使用者指南

# AWS CloudTrail

版本 1.0

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

# AWS CloudTrail: 使用者指南

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

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

# Table of Contents

什麼是 AWS CloudTrail？ ..... 1
存取 CloudTrail ..... 2
CloudTrail 主控台 ..... 2
AWS CLI ..... 3
CloudTrail API ..... 3
AWS SDKs ..... 3
CloudTrail 運作方式 ..... 3
CloudTrail 事件歷史記錄 ..... 4
CloudTrail Lake 和事件資料存放區 ..... 4
CloudTrail Lake 儀表板 ..... 7
CloudTrail 追蹤 ..... 7
CloudTrail Insights 事件 ..... 11
CloudTrail 通道 ..... 12
概念 ..... 13
CloudTrail 事件 ..... 13
事件歷史記錄 ..... 41
線索 ..... 42
組織追蹤 ..... 43
CloudTrail Lake 和事件資料存放區 ..... 45
CloudTrail Insights ..... 45
Tags (標籤) ..... 45
AWS Security Token Service 和 CloudTrail ..... 46
全球服務事件 ..... 46
支援的區域 ..... 47
支援的服務和整合 ..... 51
AWS 服務與 CloudTrail 日誌的整合 ..... 51
CloudTrail 與 Amazon EventBridge 整合 ..... 53
CloudTrail 與 整合 AWS Organizations ..... 54
CloudTrail 與 整合 AWS Control Tower ..... 54
CloudTrail 與 Amazon Security Lake 整合 ..... 54
CloudTrail Lake 與 Amazon Athena 整合 ..... 54
CloudTrail Lake 與 整合 AWS Config ..... 54
CloudTrail Lake 與 整合 AWS Audit Manager ..... 55
AWS CloudTrail 的服務主題 ..... 55

不支援的服務 ..... 77
中的配額 AWS CloudTrail ..... 78
CloudTrail 資源配額 ..... 78
CloudTrail 中的每秒交易數 (TPS) 配額 ..... 82
CloudTrail 教學 ..... 83
授予使用 CloudTrail 的許可 ..... 83
檢視事件歷史記錄 ..... 84
建立追蹤以記錄管理事件 ..... 86
檢視您的日誌檔案 ..... 90
建立 S3 資料事件的事件資料存放區 ..... 91
檢視 CloudTrail 成本和用量 ..... 98
使用 AWS Budgets 來管理成本 ..... 101
為 CloudTrail Lake 事件資料存放區建立使用者定義的成本分配標籤 ..... 102
管理 CloudTrail 追蹤成本 ..... 102
追蹤組態 ..... 102
另請參閱 ..... 103
管理 CloudTrail Lake 成本 ..... 103
事件資料存放區定價選項 ..... 104
了解 CloudTrail Lake 費用 ..... 105
有關如何降低成本的建議 ..... 106
另請參閱 ..... 108
使用 CloudTrail 事件歷史記錄 ..... 109
事件歷史記錄的限制 ..... 109
使用主控台檢視最近的管理事件 ..... 110
導覽頁面 ..... 112
自訂顯示 ..... 112
篩選 CloudTrail 事件 ..... 113
檢視事件的詳細資訊 ..... 115
下載事件 ..... 115
檢視使用 參考的資源 AWS Config ..... 116
使用 檢視最近的管理事件 AWS CLI ..... 117
先決條件 ..... 118
取得命令列說明 ..... 118
查詢事件 ..... 119
指定要傳回的事件數目 ..... 120
依時間範圍查詢事件 ..... 120

依屬性查詢事件 ..... 120
指定下一頁的結果 ..... 122
從檔案取得 JSON 輸入 ..... 123
查詢輸出欄位 ..... 124
使用 CloudTrail Insights ..... 126
Insights 事件的成本 ..... 127
Insights 事件的交付 ..... 130
使用 CloudTrail 主控台記錄 Insights 事件 ..... 131
使用主控台在現有線索上啟用 CloudTrail Insights ..... 131
使用主控台在現有事件資料存放區上啟用 CloudTrail Insights ..... 132
使用 記錄 Insights 事件 AWS CLI ..... 132
使用 記錄線索的 Insights 事件 AWS CLI ..... 133
使用 記錄事件資料存放區的 Insights 事件 AWS CLI ..... 134
檢視追蹤的 Insights 事件 ..... 138
使用主控台檢視線索的 Insights 事件 ..... 139
使用 檢視線索的 Insights 事件 AWS CLI ..... 146
檢視事件資料存放區的 Insights 事件 ..... 163
檢視事件資料存放區的 Insights 儀表板 ..... 163
檢視 Insights 事件的範例查詢 ..... 164
使用 CloudTrail Lake ..... 166
CloudTrail Lake 事件資料存放區 ..... 166
CloudTrail Lake 查詢 ..... 167
CloudTrail Lake 儀表板 ..... 167
CloudTrail Lake 整合 ..... 168
其他資源 ..... 168
CloudTrail Lake 支援的區域 ..... 169
CloudTrail Lake 概念和術語 ..... 171
事件資料存放區 ..... 171
整合 ..... 172
查詢 ..... 173
儀表板 ..... 174
事件資料存放區 ..... 174
使用主控台建立、更新和管理事件資料存放區 ..... 176
使用 建立、更新和管理事件資料存放區 AWS CLI ..... 220
管理事件資料存放區生命週期 ..... 249
將追蹤事件複製到事件資料存放區 ..... 250

聯合事件資料存放區 ..... 268
組織事件資料存放區 ..... 278
整合 ..... 284
使用主控台建立與 CloudTrail 合作夥伴的整合 ..... 285
建立與主控台的自訂整合 ..... 287
使用 建立、更新和管理 CloudTrail Lake 整合 AWS CLI ..... 291
整合合作夥伴的其他資訊 ..... 299
CloudTrail Lake 整合事件結構描述 ..... 300
儀表板 ..... 306
先決條件 ..... 308
限制 ..... 308
區域支援 ..... 308
所需的許可 ..... 309
檢視受管儀表板 ..... 313
啟用反白儀表板 ..... 327
停用反白儀表板 ..... 328
建立自訂儀表板 ..... 328
設定自訂儀表板的重新整理排程 ..... 331
停用自訂儀表板的重新整理排程 ..... 332
變更終止保護 ..... 332
刪除自訂儀表板 ..... 333
使用 建立、更新和管理儀表板 AWS CLI ..... 334
查詢 ..... 167
查詢編輯器工具 ..... 350
從自然語言提示建立 CloudTrail Lake 查詢 ..... 351
檢視範例查詢 ..... 358
建立或編輯查詢 ..... 361
執行查詢並儲存查詢結果 ..... 363
檢視查詢結果 ..... 367
以自然語言摘要查詢結果 ..... 368
下載已儲存的查詢結果 ..... 370
驗證已儲存查詢結果 ..... 372
最佳化查詢 ..... 386
使用 執行和管理 CloudTrail Lake 查詢 AWS CLI ..... 389
CloudTrail Lake SQL 限制條件 ..... 394
支援的函數、條件和聯結運算子 ..... 395

進階的多重資料表查詢支援 ..... 396
事件資料存放區的受支援 SQL 結構描述 ..... 397
支援的 CloudTrail 事件記錄欄位結構描述 ..... 397
CloudTrail Insights 事件記錄欄位的受支援結構描述 ..... 401
AWS Config 支援組態項目記錄欄位的結構描述 ..... 403
AWS Audit Manager 證據記錄欄位支援的結構描述 ..... 404
非AWS 事件欄位支援的結構描述 ..... 405
支援的 CloudWatch 指標 ..... 407
使用 CloudTrail 追蹤 ..... 409
為您的 建立線索 AWS 帳戶 ..... 410
使用主控台建立和更新線索 ..... 411
使用 建立、更新和管理線索 AWS CLI ..... 438
建立多個線索 ..... 468
建立組織追蹤 ..... 470
從成員帳戶追蹤移至組織追蹤 ..... 473
準備建立組織追蹤 ..... 473
使用主控台建立組織追蹤 ..... 477
使用 為組織建立線索 AWS CLI ..... 485
疑難排解 ..... 491
了解多區域追蹤和選擇加入區域 ..... 494
多區域線索的優點有哪些？ ..... 494
當您建立多區域追蹤時會發生什麼情況？ ..... 494
當您啟用選擇加入區域時會發生什麼情況？ ..... 495
當您停用選擇加入區域時會發生什麼情況？ ..... 495
將追蹤事件複製到 CloudTrail Lake ..... 495
複製追蹤事件的考量 ..... 497
複製追蹤事件所需的許可 ..... 498
使用 CloudTrail 主控台將追蹤事件複製到現有的事件資料存放區 ..... 502
取得和檢視 CloudTrail 日誌檔案 ..... 504
尋找 CloudTrail 日誌檔案 ..... 505
下載 CloudTrail 日誌檔案 ..... 507
設定 CloudTrail 的 Amazon SNS 通知 ..... 508
設定 CloudTrail 傳送通知 ..... 509
AWS CloudTrail 搭配界面 VPC 端點使用 ..... 510
大區 (Regions) ..... 511
為 CloudTrail 建立 VPC 端點 ..... 511

建立 CloudTrail 的 VPC 端點政策 ..... 511
共用子網路 ..... 515
命名要求 ..... 515
CloudTrail 資源命名要求 ..... 516
Amazon S3 儲存貯體命名需求 ..... 516
AWS KMS 別名命名要求 ..... 517
AWS 帳戶 關閉和追蹤 ..... 517
設定 CloudTrail 設定 ..... 519
組織委派的管理員 ..... 519
指派委派管理員所需的許可 ..... 522
新增 CloudTrail 委派的管理員 ..... 523
移除 CloudTrail 委派的管理員 ..... 524
服務連結通道 ..... 525
使用主控台檢視服務連結通道 ..... 525
使用 檢視服務連結頻道 AWS CLI ..... 526
了解 CloudTrail 事件 ..... 529
管理事件 ..... 529
資料事件 ..... 532
支援的資料事件 AWS CloudTrail ..... 533
網路活動事件 ..... 559
Insights 事件 ..... 563
管理事件 ..... 565
管理事件 ..... 566
讀取和寫入事件 ..... 567
使用 記錄管理事件 AWS 管理主控台 ..... 568
使用 記錄管理事件 AWS CLI ..... 571
使用 AWS SDKs 記錄管理事件 ..... 585
資料事件 ..... 585
資料事件 ..... 587
唯讀和唯寫事件 ..... 614
使用 記錄資料事件 AWS 管理主控台 ..... 615
使用 記錄資料事件 AWS Command Line Interface ..... 623
使用進階事件選取器篩選資料事件 ..... 635
彙總資料事件 ..... 646
記錄資料事件以實現 AWS Config 合規 ..... 650
使用 AWS SDKs 記錄資料事件 ..... 650

網路活動事件 ..... 651
網路活動事件的進階事件選取器欄位 ..... 654
使用 記錄網路活動事件 AWS 管理主控台 ..... 657
使用 記錄網路活動事件 AWS Command Line Interface ..... 660
使用 AWS SDKs 記錄事件 ..... 682
將資源標籤索引鍵和 IAM 全域條件索引鍵新增至事件 ..... 682
AWS 服務 支援資源標籤 ..... 683
AWS 服務 支援 IAM 全域條件金鑰 ..... 684
事件範例 ..... 688
CloudTrail 記錄管理、資料和網路活動事件的內容 ..... 689
事件大小上限為 1 MB 的欄位截斷順序 ..... 701
sharedEventID 範例 ..... 702
彙總事件的 CloudTrail 記錄內容 ..... 703
彙總事件範例 ..... 707
追蹤的 Insights 事件 CloudTrail 記錄內容 ..... 709
範例 `insightDetails` 區塊 ..... 714
事件資料存放區的 Insights 事件 CloudTrail 記錄內容 ..... 716
CloudTrail userIdentity 元素 ..... 720
範例 ..... 720
欄位 ..... 722
具有 SAML 和 Web 聯合身分 AWS STS APIs 值 ..... 729
AWS STS 來源身分 ..... 731
CloudTrail 擷取的非 API 事件 ..... 733
AWS 服務 事件 ..... 734
AWS 管理主控台 登入事件 ..... 735
CloudTrail 日誌檔案 ..... 750
從多個區域接收 CloudTrail 日誌檔案 ..... 751
管理資料一致性 ..... 752
使用 Amazon CloudWatch Logs 監控 CloudTrail 日誌檔案 ..... 753
傳送事件到 CloudWatch Logs ..... 754
建立 CloudTrail 事件的 CloudWatch 警示：範例 ..... 761
停止 CloudTrail 將事件傳送至 CloudWatch Logs ..... 768
CloudTrail 的 CloudWatch Logs 日誌群組和日誌串流命名 ..... 769
讓 CloudTrail 能使用 CloudWatch Logs 進行監控的角色政策文件 ..... 770
從多個帳戶接收 CloudTrail 日誌檔案 ..... 772
編輯其他帳戶呼叫之資料事件的儲存貯體擁有者帳戶 ID ..... 772

設定多帳戶的儲存貯體政策 ..... 774
在其他帳戶中建立追蹤 ..... 776
在 AWS 帳戶之間共用 CloudTrail 日誌檔案 ..... 777
擔任角色以在帳戶之間共享日誌 ..... 778
驗證 CloudTrail 日誌檔案完整性 ..... 787
為什麼使用它？ ..... 787
運作方式 ..... 788
啟用 CloudTrail 的日誌檔案完整性驗證 ..... 788
使用 驗證 CloudTrail 日誌檔案完整性 AWS CLI ..... 789
CloudTrail 摘要檔案結構 ..... 800
CloudTrail 日誌檔案完整性驗證的自訂實作 ..... 806
CloudTrail 日誌檔案範例 ..... 818
CloudTrail 記錄檔名稱格式 ..... 818
日誌檔案範例 ..... 818
使用 CloudTrail Processing Library ..... 831
最低需求 ..... 832
處理 CloudTrail 日誌 ..... 832
進階主題 ..... 837
其他資源 ..... 842
安全 ..... 844
資料保護 ..... 844
身分和存取權管理 ..... 845
目標對象 ..... 846
使用身分驗證 ..... 846
使用政策管理存取權 ..... 848
AWS CloudTrail 如何使用 IAM ..... 849
身分型政策範例 ..... 855
資源型政策範例 ..... 870
適用於 CloudTrail 的 Amazon S3 儲存貯體政策 ..... 878
適用於 CloudTrail Lake 查詢結果的 Amazon S3 儲存貯體政策 ..... 885
適用於 CloudTrail 索的 Amazon SNS 主題政策 ..... 888
疑難排解 ..... 894
使用服務連結角色 ..... 898
AWS 受管政策 ..... 903
法規遵循驗證 ..... 905
恢復能力 ..... 906

基礎設施安全性 ..... 906
預防跨服務混淆代理人 ..... 907
安全最佳實務 ..... 908
CloudTrail 偵測性安全最佳實務 ..... 908
CloudTrail 預防性安全最佳實務 ..... 910
使用 AWS KMS 金鑰加密 CloudTrail 日誌檔案、摘要檔案和事件資料存放區 (SSE-KMS) ..... 913
啟用日誌檔案加密 ..... 914
授與建立 KMS 金鑰的許可 ..... 915
設定 CloudTrail 的 AWS KMS 金鑰政策 ..... 915
更新資源以搭配 主控台使用您的 KMS 金鑰 ..... 930
使用 啟用和停用 CloudTrail 日誌檔案、摘要檔案和事件資料存放區的加密 AWS CLI ..... 933
AWS CloudTrail 如何使用 AWS KMS ..... 936
文件歷史紀錄 ..... 943
舊版更新 ..... 989
..... mv

# 什麼是 AWS CloudTrail？

AWS CloudTrail 是 AWS 服務 ，可協助您啟用 的操作和風險稽核、控管和合規 AWS 帳戶。使用者、角色或 AWS 服務所執行的動作會在 CloudTrail 中記錄為事件。事件包括在 AWS 管理主控台 AWS Command Line Interface、 和 AWS SDKs和 APIs中採取的動作。

CloudTrail 提供三種記錄事件的方式：

- 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。

  檢視事件歷史記錄不會產生 CloudTrail 費用。

- CloudTrail Lake – AWS CloudTrail Lake 是受管資料湖，用於擷取、儲存、存取和分析 上的使用者和 API 活動， AWS 以用於稽核和安全性目的。CloudTrail Lake 會將分列式 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 建立事件資料存放區 AWS 帳戶 AWS Organizations。您可以從 S3 儲存貯體將任何現有的 CloudTrail 日誌匯入到現有的或新的事件資料存放區。您還可以使用 Lake 儀表板對熱門的 CloudTrail 事件趨勢進行視覺化呈現。如需詳細資訊，請參閱使用 AWS CloudTrail Lake。

  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 Lake 成本。

- 線索 – 線索會擷取 AWS 活動記錄，交付這些事件並將其儲存在 Amazon S3 儲存貯體中，並選擇性交付至 CloudWatch Logs 和 Amazon EventBridge。您可以輸入這些事件到您的安全監控解決方案。您還可以使用您自己的第三方解決方案，或 Amazon Athena 等解決方案來搜尋並分析您的 CloudTrail 日誌。您可以使用 為單一 AWS 帳戶 或多個 建立線索 AWS 帳戶 AWS Organizations。您可以記錄 Insights 事件，以分析 API 呼叫率和錯誤率中異常行為的管理事件。如需詳細資訊，請參閱為您的 建立線索 AWS 帳戶。

您可以透過建立線索，從 CloudTrail 免費將一份持續管理事件的副本交付至 S3 儲存貯體，不過，需要支付 Amazon S3 儲存費用。如需 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 AWS 帳戶活動的可見性是安全和操作最佳實務的關鍵層面。您可以使用 CloudTrail 來檢視、搜尋、下載、封存、分析和回應整個 AWS 基礎設施的帳戶活動。您可以識別誰或什麼採取了哪些動作、採取了哪些資源、事件發生的時間，以及其他詳細資訊，以協助您分析和回應 AWS 帳戶中的活動。

您可以使用 API 將 CloudTrail 整合到應用程式、自動建立您組織的追蹤或事件資料存放區、檢查您所建立事件資料存放區和追蹤的狀態，以及控制使用者如何檢視 CloudTrail 事件。

# 存取 CloudTrail

您可以透過下列任何方式使用 CloudTrail。

主題

- CloudTrail 主控台
- AWS CLI
- CloudTrail API
- AWS SDKs

## CloudTrail 主控台

登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。

CloudTrail 主控台提供用於執行許多 CloudTrail 任務的使用者介面，例如：

- 檢視您 AWS 帳戶的最新事件和事件歷史記錄。
- 從事件歷史記錄下載過去 90 天管理事件的篩選或完整檔案。
- 建立和編輯 CloudTrail 追蹤。
- 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，包含：
  - 為追蹤選取 Amazon S3 儲存貯體。

- 設定前綴。
- 設定交付至 CloudWatch Logs。
- 使用 AWS KMS 金鑰來加密追蹤資料。
- 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 CloudTrail 合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 的詳細資訊 AWS 管理主控台，請參閱 AWS 管理主控台。

## AWS CLI

AWS Command Line Interface 是一個統一的工具，您可以用來從命令列與 CloudTrail 互動。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《 AWS CLI 命令參考》中的 cloudtrail 和 cloudtrail-data。

## CloudTrail API

除了主控台和 CLI 之外，您也可以使用 CloudTrail RESTful API 直接編寫 CloudTrail。如需詳細資訊，請參閱 AWS CloudTrail API 參考和 CloudTrail-Data API 參考。

## AWS SDKs

除了使用 CloudTrail API 之外，您也可以使用其中一個 AWS SDKs。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。開發套件提供便捷方法來建立對 CloudTrail 的程式化存取。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，請參閱建置工具頁面 AWS。

# CloudTrail 運作方式

建立 時，您會自動存取 CloudTrail 事件歷史記錄 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 AWS 帳戶 過去 90 天內持續記錄的事件，請建立線索或 CloudTrail Lake 事件資料存放區。

主題

- CloudTrail 事件歷史記錄
- CloudTrail Lake 和事件資料存放區
- CloudTrail Lake 儀表板
- CloudTrail 追蹤
- CloudTrail Insights 事件
- CloudTrail 通道

## CloudTrail 事件歷史記錄

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`命令不會產生 CloudTrail 費用。

## CloudTrail Lake 和事件資料存放區

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、網路活動事件）、CloudTrail Insights 事件、AWS Audit Manager 證據、AWS Config 組態項目或 外部的事件 AWS。

事件資料存放區可以記錄來自目前 AWS 區域或您 AWS 區域 AWS 帳戶中所有 的事件。您用來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，您可以建立組織事件資料存放區，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，請參閱了解組織事件資料存放區。

依預設，CloudTrail 會加密事件資料存放區中的所有事件。當您設定事件資料存放區時，您可以選擇使用自己的 AWS KMS key。使用您自己的 KMS 金鑰會產生加密和解密 AWS KMS 的成本。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 日誌檔案、摘要檔案和事件資料存放區 (SSE-KMS)。

下表提供您可以在事件資料存放區上執行之任務的相關資訊。

| 任務 | Description |
| --- | --- |
| 檢視和建立儀表板 | 您可以使用 CloudTrail Lake 儀表板來查看帳戶中事件資料存放區的事件趨勢。您可以檢視受管儀表板、建立自訂儀表板，並啟用醒目提示儀表板，以查看 CloudTrail Lake 所策劃和管理之事件資料的醒目提示。 |
| 日誌管理事件 | 將事件資料存放區設定為記錄唯讀、唯讀或所有管理事件。根據預設，事件資料會存放日誌管理事件。<br><br>您可以在下列進階事件選取器欄位上篩選管理事件：`eventName` 、`eventSource` 、`eventType` `readOnly`、`sessionCredentialFromConsole` 、 和 `userIdentity.arn` 。 |
| 日誌資料事件 | 您可以使用進階事件選取器來建立精細選取器，只記錄感興趣的資料事件。例如，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。如需詳細資訊，請參閱使用進階事件選取器篩選資料事件。 |
| 記錄網路活動事件 | 設定事件資料存放區以記錄網路活動事件。您可以使用進階事件選取器來篩選 `eventName` 、 和 `vpcEndpointId` 欄位`errorCode` ，以僅記錄這些感興趣的事件。 |
| Log Insights 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，請參閱使用 CloudTrail Insights。<br><br>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。 |

| 任務 | Description |
| --- | --- |
| 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，以建立記錄到追蹤事件的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，在 AWS Glue 資料目錄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 Data Catalog 中的資料表中繼資料可讓 Athena 查詢引擎了解如何尋找、讀取和處理您要查詢的資料。 |
| 在事件資料存放區上停止或開始事件擷取 | 您可以在收集 CloudTrail 管理和資料事件或 AWS Config 組態項目的事件資料存放區上停止和開始事件擷取。 |
| 在 外部建立與事件來源的整合 AWS | 您可以使用 CloudTrail Lake 整合，從外部記錄和存放使用者活動資料 AWS；從混合環境中的任何來源，例如內部或 SaaS 應用程式託管在內部部署或雲端、虛擬機器或容器中。如需可用整合合作夥伴的詳細資訊，請參閱 AWS CloudTrail Lake Integrations。 |
| 在 CloudTrail 主控台中檢視 Lake 範例查詢 | CloudTrail 主控台提供許多範例查詢，可協助您開始自行編寫查詢。 |
| 建立或編輯查詢 | CloudTrail 中的查詢是以 SQL 撰寫而成。您可以在 CloudTrail Lake Editor (編輯器) 索引標籤上建置查詢，方法是從頭開始以 SQL 中編寫查詢，或開啟已儲存的查詢或範例查詢並對其加以編輯。 |
| 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。 |
| 下載已儲存的查詢結果 | 您可以下載包含已儲存 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，來判斷在 CloudTrail 傳遞查詢結果到 S3 儲存貯體之後，查詢結果是否經過修改、遭到刪除或保持不變。 |

如需有關 CloudTrail Lake 的詳細資訊，請參閱 使用 AWS CloudTrail Lake。

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 Lake 成本。

## CloudTrail Lake 儀表板

您可以使用 CloudTrail Lake 儀表板來查看帳戶中事件資料存放區的事件趨勢。CloudTrail Lake 提供下列儀表板類型：

- 受管儀表板 – 您可以檢視受管儀表板，以查看收集管理事件、資料事件或 Insights 事件的事件資料存放區的事件趨勢。這些儀表板會自動提供給您，並由 CloudTrail Lake 管理。CloudTrail 提供 14 個受管儀表板供您選擇。您可以手動重新整理受管儀表板。您無法修改、新增或移除這些儀表板的小工具，不過，如果您想要修改小工具或設定重新整理排程，則可以將受管儀表板儲存為自訂儀表板。
- 自訂儀表板 – 自訂儀表板可讓您查詢任何事件資料存放區類型中的事件。您最多可以將 10 個小工具新增至自訂儀表板。您可以手動重新整理自訂儀表板，也可以設定重新整理排程。
- 反白儀表板 – 啟用反白儀表板，以檢視您帳戶中事件資料存放區所收集的 AWS 活動at-a-glance。醒目提示儀表板由 CloudTrail 管理，並包含與您帳戶相關的小工具。反白儀表板上顯示的小工具對於每個帳戶都是唯一的。這些小工具可能會浮現偵測到的異常活動或異常。例如，您的 Highlights 儀表板可能包含跨帳戶存取總數小工具，這會顯示異常跨帳戶活動是否增加。CloudTrail 每 6 小時更新一次反白儀表板。儀表板會顯示上次更新後的最後 24 小時的資料。

每個儀表板都包含一或多個小工具，每個小工具代表 SQL 查詢。

如需詳細資訊，請參閱CloudTrail Lake 儀表板。

## CloudTrail 追蹤

追蹤是一種組態，能讓事件交付到您指定的 Amazon S3 儲存貯體。您也可以使用 Amazon CloudWatch Logs 和 Amazon EventBridge 在線索中交付和分析事件。

線索可以記錄 CloudTrail 管理事件、資料事件、網路活動事件和 Insights 事件。

您可以為 建立多區域和單一區域追蹤 AWS 帳戶。

多區域追蹤

當您建立多區域追蹤時，CloudTrail 會在 中啟用的所有 中記錄事件 AWS 區域 ， AWS 帳戶 並將 CloudTrail 事件日誌檔案交付至您指定的 S3 儲存貯體。根據最佳實務，我們建議您建立多區域追

蹤，因為它會擷取所有啟用區域中的活動。使用 CloudTrail 主控台建立的所有線索都是多區域線索。您可以使用 將單一區域線索轉換為多區域線索 AWS CLI。如需詳細資訊，請參閱了解多區域追蹤和選擇加入區域、使用主控台建立追蹤及將單一區域追蹤轉換為多區域追蹤。

單一區域追蹤

當您建立單一區域追蹤時，CloudTrail 只會記錄該區域中的事件。其接著會將 CloudTrail 事件日誌檔案交付到您指定的 Amazon S3 儲存貯體。您只能使用 AWS CLI建立單一區域追蹤。如果您建立其他單一線索，則可以讓這些線索將 CloudTrail 事件日誌檔案傳送到相同的 S3 儲存貯體或單獨的儲存貯體。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，請參閱使用 建立、更新和管理線索 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，您可以建立組織追蹤，記錄該組織中所有 AWS 帳戶的所有事件。組織追蹤可以套用至所有 AWS 區域或目前區域。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。成員帳戶可以查看組織線索，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，您的事件日誌檔案和摘要檔案會使用 KMS 金鑰加密。如果您選擇不啟用 SSE-KMS 加密，您的事件日誌檔案和摘要檔案會使用 Amazon S3 伺服器端加密 (SSE) 進行加密。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 會在一小時內每隔 5 分鐘多次發佈日誌檔案。這些日誌檔案包含帳戶中支援 CloudTrail 之服務的 API 呼叫。如需詳細資訊，請參閱CloudTrail 支援的服務和整合。

> **Note**
>
> CloudTrail 通常會在 API 呼叫的平均約 5 分鐘內傳遞日誌。此時間無法保證。如需詳細資訊，請參閱 AWS CloudTrail 服務水準協議。
>
> 如果您的追蹤設定錯誤 (例如，S3 儲存貯體無法連線)，CloudTrail 會在 30 天內嘗試重新傳遞日誌檔案到您的 S3 儲存貯體，且您需要為這些嘗試傳遞事件支付標準 CloudTrail 費用。若要避免支付追蹤設定錯誤費用，您需要刪除追蹤。

CloudTrail 會擷取使用者直接進行、或 AWS 服務代替使用者進行的動作。例如，呼叫 CloudFormation `CreateStack`可能會導致額外 API 呼叫 Amazon EC2、Amazon RDS、Amazon EBS 或其他 CloudFormation 範本所需的服務。這是正常且預期的行為。您可以識別 AWS 服務是否在 CloudTrail 事件中使用 `invokedby` 欄位採取動作。

下表提供您可以在線索上執行之任務的相關資訊。

| 任務 | Description |
| --- | --- |
| 記錄管理事件 | 設定您的線索以記錄唯讀、唯讀或所有管理事件。 |
| 日誌資料事件 | 您可以使用進階事件選取器來建立精細選取器，只記錄感興趣的資料事件。例如，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。如需詳細資訊，請參閱使用進階事件選取器篩選資料事件。 |
| 記錄網路活動事件 | 設定您的線索以記錄網路活動事件。您可以設定進階事件選取器來篩選 `eventName` 、 和 `vpcEndpointId` 欄位`errorCode` ，以僅記錄這些感興趣的事件。 |
| Log Insights 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。<br><br>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 Insights 事件 | 在線索上啟用 CloudTrail Insights 之後，您可以使用 CloudTrail 主控台或 AWS CLI檢視最多 90 天的 Insights 事件。 |

| 任務 | Description |
| --- | --- |
| 下載 Insights 事件 | 在追蹤上啟用 CloudTrail Insights 後，您可以為您的追蹤下載最多包含過去 90 天 Insights 事件的 CSV 或 JSON 檔案。 |
| 將追蹤事件複製到 CloudTrail Lake | 您可以將現有追蹤事件複製到 CloudTrail Lake 事件資料存放區，以建立記錄至追蹤之事件的時間點快照。 |
| 建立和訂閱 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。<br><br>**Note**<br>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 Processing Library」。 |
| 檢視您的日誌檔案 | 從 S3 儲存貯體尋找並下載您的日誌檔案。 |
| 使用 CloudWatch Logs 監控事件 | 設定您的追蹤以傳送事件到 CloudWatch Logs。然後，您可以使用 CloudWatch Logs 監控您帳戶中的特定 API 呼叫和事件。<br><br>**Note**<br>如果您設定多區域追蹤將事件傳送至 CloudWatch Logs 日誌群組，CloudTrail 會將所有區域的事件傳送至單一日誌群組。 |

| 任務 | Description |
| --- | --- |
| 啟用 SSE-KMS 加密 | 使用 KMS 金鑰加密日誌檔案和摘要檔案可為 CloudTrail 資料提供多一層安全性。 |
| 啟用日誌檔案完整性 | 日誌檔案完整性驗證可協助您驗證日誌檔案在 CloudTrail 交付後保持不變。 |
| 與其他 共用日誌檔案 AWS 帳戶 | 您可以在帳戶之間共享日誌檔案。 |
| 從多個帳戶彙總日誌 | 您可以將多個帳戶的日誌檔案彙整至單一儲存貯體。 |
| 使用合作夥伴解決方案 | 使用與 CloudTrail 整合的合作夥伴解決方案來分析您的 CloudTrail 輸出。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。 |

您可以透過建立線索，從 CloudTrail 免費將一份持續管理事件的副本交付至 S3 儲存貯體，不過，需要支付 Amazon S3 儲存費用。如需 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 Insights 事件

AWS CloudTrail Insights 透過持續分析 CloudTrail 管理事件，協助 AWS 使用者識別和回應與 API 呼叫率和 API 錯誤率相關的異常活動。CloudTrail Insights 會分析您的 API 呼叫量和 API 錯誤率的一般模式，也稱為基準，並在呼叫量或錯誤率處於正常模式之外時產生 Insights 事件。系統會針對`write`管理 APIs 產生 API 呼叫率上的 Insights 事件，並針對 `readwrite`和管理 APIs 產生 API 錯誤率上的 Insights 事件。

根據預設，CloudTrail 追蹤和事件資料存放區不會記錄 Insights 事件。您必須設定追蹤或事件資料存放區來記錄 Insights 事件。如需詳細資訊，請參閱使用 CloudTrail 主控台記錄 Insights 事件及使用 記錄 Insights 事件 AWS CLI。

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 Insights 事件

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

檢視追蹤的 Insights 事件

如果您已在追蹤上啟用 Insights 事件，且 CloudTrail 偵測到異常的活動，則會將 Insights 事件記錄到追蹤之目的地 S3 儲存貯體的不同資料夾或字首。當您在 CloudTrail 主控台上檢視 Insights 事件 時，也可以查看洞察類型和事件時段。如需詳細資訊，請參閱使用主控台檢視線索的 Insights 事件。

在您第一次在線索上啟用 CloudTrail Insights 之後，CloudTrail 最多可能需要 36 小時才能在線索上啟用 Insights 事件後開始交付 Insights 事件，前提是在此期間偵測到異常活動。

檢視事件資料存放區的 Insights 事件

若要在 CloudTrail Lake 中記錄 Insights 事件，您需要會記錄 Insights 事件的目的地事件資料存放區和啟用 Insights 和日誌管理事件的來源事件資料存放區。如需詳細資訊，請參閱使用主控台建立 Insights 事件的事件資料存放區。

在來源事件資料存放區上第一次啟用 CloudTrail Insights 之後，CloudTrail 最多可能需要 7 天才能開始交付 Insights 事件，前提是在此期間偵測到異常活動。

如果您已在來源事件資料存放區上啟用 CloudTrail Insights，而且 CloudTrail 偵測到異常活動，CloudTrail 會傳遞 Insights 事件至您的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，也可以選擇將查詢結果儲存至 S3 儲存貯體。如需詳細資訊，請參閱使用 CloudTrail 主控台建立或編輯查詢及使用 CloudTrail 主控台檢視範例查詢。

您可以檢視 Insights 事件儀表板，以視覺化目的地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 CloudTrail Lake 儀表板。

## CloudTrail 通道

CloudTrail 支援兩種類型的通道：

CloudTrail Lake 與 外部事件來源整合的頻道 AWS

> CloudTrail Lake 使用頻道，將來自 外部的事件從使用 CloudTrail 的外部合作夥伴，或從您自己的來源 AWS 帶入 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，請參閱在 外部建立與事件來源的整合 AWS和 AWS CloudTrail API 參考中的 `CreateChannel`。

服務連結通道

AWS 服務可以建立服務連結頻道，以代表您接收 CloudTrail 事件。建立服務連結頻道 AWS 的服務會設定頻道的進階事件選取器，並指定頻道是否套用至所有區域或目前區域。

您可以使用 CloudTrail 主控台或 AWS CLI 檢視由 建立之任何 CloudTrail 服務連結頻道的相關資訊 AWS 服務。

# CloudTrail 概念

本節摘要說明與 CloudTrail 相關的基本概念。

概念：

- CloudTrail 事件
- 事件歷史記錄
- 線索
- 組織追蹤
- CloudTrail Lake 和事件資料存放區
- CloudTrail Insights
- Tags (標籤)
- AWS Security Token Service 和 CloudTrail
- 全球服務事件

## CloudTrail 事件

CloudTrail 中的事件是 AWS 帳戶中活動的記錄。此活動可以是 CloudTrail 得以監控之 IAM 身分或服務所採取的動作。CloudTrail 事件提供透過 AWS 管理主控台、 AWS SDKs、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 日誌檔案不是公有 API 呼叫的已排序堆疊追蹤，因此事件不會以任何特定順序顯示。

CloudTrail 會記錄四種類型的事件：

- 管理事件
- 資料事件
- 網路活動事件
- Insights 事件

所有事件類型都使用 CloudTrail JSON 日誌格式。

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。

如需如何與 CloudTrail AWS 服務 整合的資訊，請參閱 AWS CloudTrail 的服務主題。

## 管理事件

管理事件提供有關對 AWS 帳戶中資源執行的管理操作的資訊。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 API AWS Identity and Access Management `AttachRolePolicy` 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 API AWS CloudTrail `CreateTrail` 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，CloudTrail 就會記錄 `ConsoleLogin` 事件的日誌。如需詳細資訊，請參閱CloudTrail 擷取的非 API 事件。

根據預設，CloudTrail 追蹤和 CloudTrail Lake 事件資料會存放日誌管理事件。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 儲存貯體中物件的 Amazon S3 物件層級 API 活動 （例如，`DeleteObject`、 `GetObject`和 `PutObject` API 操作）。 S3
- AWS Lambda 函數執行活動（`Invoke` API)。

- 用於記錄 AWS外部事件的 CloudTrail Lake 通道上的 CloudTrail PutAuditEvents 活動。
- 主題上的 Amazon SNS Publish 和 PublishBatch API 操作。

下表顯示線索和事件資料存放區可用的資源類型。資源類型 （主控台） 欄會在主控台中顯示適當的選擇。resources.type 值欄會顯示您要指定的resources.type值，以使用 AWS CLI 或 CloudTrail APIs 在線索或事件資料存放區中包含該類型的資料事件。

對於線索，您可以使用基本或進階事件選取器，在一般用途儲存貯體、Lambda 函數和 DynamoDB 資料表中記錄 Amazon S3 物件的資料事件 （如資料表的前三列所示）。您只能使用進階事件選取器來記錄剩餘資料列中顯示的資源類型。

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。

支援的資料事件 AWS CloudTrail

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon RDS | 資料庫叢集上的 Amazon RDS API 活動。 | RDS 資料 API - 資料庫叢集 | AWS::RDS::DBCluster |
| Amazon S3 | 一般用途儲存貯體中物件的 Amazon S3 物件層級 API 活動 （例如 DeleteObject 、 GetObject 和 PutObject API 操作）。 | S3 | AWS::S3::Object |
| Amazon S3 | 存取點上的 Amazon S3 API 活動。 | S3 存取點 | AWS::S3::AccessPoint |
| Amazon S3 | 目錄儲存貯體中物件的 Amazon S3 物件層級 API 活動 （例如 DeleteObject 、 GetObject | S3 Express | AWS::S3Express::Object |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| | 和 PutObject API 操作）。 | | |
| Amazon S3 | Amazon S3 Object Lambda 存取點 API 活動，例如對 CompleteMultipartUpload 和 的呼叫GetObject 。 | S3 Object Lambda | AWS::S3ObjectLambda::AccessPoint |
| Amazon S3 | 磁碟區上的 Amazon FSx API 活動。 | FSx 磁碟區 | AWS::FSx::Volume |
| Amazon S3 Tables | 資料表上的 Amazon S3 API 活動。 | S3 資料表 | AWS::S3Tables::Table |
| Amazon S3 Tables | 資料表儲存貯體上的 Amazon S3 API 活動。 | S3 資料表儲存貯體 | AWS::S3Tables::TableBucket |
| Amazon S3 Vectors | 向量儲存貯體上的 Amazon S3 API 活動。 | S3 向量儲存貯體 | AWS::S3Vectors::VectorBucket |
| Amazon S3 Vectors | 向量索引上的 Amazon S3 API 活動。 | S3 向量索引 | AWS::S3Vectors::Index |
| Amazon S3 on Outposts | Outposts 上 Amazon S3 物件層級的 API 活動。 | S3 Outposts | AWS::S3Outposts::Object |
| Amazon SNS | 平台端點上的 Amazon SNS Publish API 操作。 | SNS 平台端點 | AWS::SNS::PlatformEndpoint |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon SNS | 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 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 | AWS::SWF::Domain |
| AWS AppConfig | 組態操作的 AWS AppConfig API 活動，例如呼叫 StartConfiguration Session 和 GetLatestConfiguration 。 | AWS AppConfig | AWS::AppConfig::Configuration |
| AWS AppSync | AppSync GraphQL API APIs AWS AppSync 活動。 | AppSync GraphQL | AWS::AppSync::GraphQLApi |
| Amazon Aurora DSQL | 叢集資源上的 Amazon Aurora DSQL API 活動。 | Amazon Aurora DSQL | AWS::DSQL::Cluster |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| AWS B2B 資料交換 | 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 Backup | AWS Backup 在搜尋任務上搜尋資料 API 活動。 | AWS Backup 搜尋資料 APIs | AWS::Backup::SearchJob |
| 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 |
| Amazon Bedrock | 非同步調用上的 Amazon Bedrock API 活動。 | Bedrock 非同步調用 | AWS::Bedrock::AsyncInvoke |
| Amazon Bedrock | 流程別名上的 Amazon Bedrock API 活動。 | Bedrock 流程別名 | AWS::Bedrock::FlowAlias |
| Amazon Bedrock | 護欄上的 Amazon Bedrock API 活動。 | Bedrock 護欄 | AWS::Bedrock::Guardrail |
| Amazon Bedrock | 內嵌代理程式上的 Amazon Bedrock API 活動。 | Bedrock 調用內嵌代理程式 | AWS::Bedrock::InlineAgent |
| Amazon Bedrock | 知識庫中的 Amazon Bedrock API 活動。 | Bedrock 知識庫 | AWS::Bedrock::KnowledgeBase |
| Amazon Bedrock | 模型上的 Amazon Bedrock API 活動。 | Bedrock 模型 | AWS::Bedrock::Model |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Bedrock | 提示上的 Amazon Bedrock API 活動。 | Bedrock 提示 | AWS::Bedrock::PromptVersion |
| Amazon Bedrock | 工作階段上的 Amazon Bedrock API 活動。 | Bedrock 工作階段 | AWS::Bedrock::Session |
| Amazon Bedrock | 流程執行上的 Amazon Bedrock API 活動。 | Bedrock 流程執行 | AWS::Bedrock::FlowExecution |
| Amazon Bedrock | 自動推理政策上的 Amazon Bedrock API 活動。 | Bedrock 自動化推理政策 | AWS::Bedrock::AutomatedReasoningPolicy |
| Amazon Bedrock | 自動推理政策版本的 Amazon Bedrock API 活動。 | Bedrock 自動化推理政策版本 | AWS::Bedrock::AutomatedReasoningPolicyVersion |
| Amazon Bedrock | Amazon Bedrock 資料自動化專案 API 活動。 | Bedrock 資料自動化專案 | AWS::Bedrock::DataAutomationProject |
| Amazon Bedrock | Bedrock 資料自動化調用 API 活動。 | Bedrock 資料自動化調用 | AWS::Bedrock::DataAutomationInvocation |
| Amazon Bedrock | Amazon Bedrock 資料自動化設定檔 API 活動。 | Bedrock 資料自動化設定檔 | AWS::Bedrock::DataAutomationProfile |
| Amazon Bedrock | Amazon Bedrock 藍圖 API 活動。 | Bedrock 藍圖 | AWS::Bedrock::Blueprint |
| Amazon Bedrock | Amazon Bedrock Code-Interpreter API 活動。 | Bedrock-AgentCore Code-Interpreter | AWS::BedrockAgentCore::CodeInterpreter |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
|---|---|---|---|
| Amazon Bedrock | Amazon Bedrock 瀏覽器 API 活動。 | Bedrock-AgentCore 瀏覽器 | `AWS::BedrockAgentCore::Browser` |
| Amazon Bedrock | Amazon Bedrock 工作負載身分 API 活動。 | Bedrock-AgentCore 工作負載身分 | `AWS::BedrockAgentCore::WorkloadIdentity` |
| Amazon Bedrock | Amazon Bedrock 工作負載身分目錄 API 活動。 | Bedrock-AgentCore 工作負載身分目錄 | `AWS::BedrockAgentCore::WorkloadIdentityDirectory` |
| Amazon Bedrock | Amazon Bedrock Token Vault API 活動。 | Bedrock-AgentCore 權杖保存庫 | `AWS::BedrockAgentCore::TokenVault` |
| Amazon Bedrock | Amazon Bedrock APIKey CredentialProvider API 活動。 | Bedrock-AgentCore APIKey CredentialProvider | `AWS::BedrockAgentCore::APIKeyCredentialProvider` |
| Amazon Bedrock | Amazon Bedrock 執行時間 API 活動。 | Bedrock-AgentCore 執行期 | `AWS::BedrockAgentCore::Runtime` |
| Amazon Bedrock | Amazon Bedrock Runtime-Endpoint API 活動。 | Bedrock-AgentCore 執行時間端點 | `AWS::BedrockAgentCore::RuntimeEndpoint` |
| Amazon Bedrock | Amazon Bedrock Gateway API 活動。 | Bedrock-AgentCore 閘道 | `AWS::BedrockAgentCore::Gateway` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Bedrock | Amazon Bedrock 記憶體 API 活動。 | Bedrock-AgentCore 記憶體 | `AWS::BedrockAgentCore::Memory` |
| Amazon Bedrock | Amazon Bedrock Oauth2 CredentialProvider API 活動。 | Bedrock-AgentCore Oauth2 CredentialProvider | `AWS::BedrockAgentCore::OAuth2CredentialProvider` |
| Amazon Bedrock | Amazon Bedrock 瀏覽器自訂 API 活動。 | Bedrock-AgentCore 瀏覽器自訂 | `AWS::BedrockAgentCore::BrowserCustom` |
| Amazon Bedrock | Amazon Bedrock Code-Interpreter-Custom API 活動。 | Bedrock-AgentCore Code-Interpreter-Custom | `AWS::BedrockAgentCore::CodeInterpreterCustom` |
| Amazon Bedrock | Amazon Bedrock Tool API 活動。 | Bedrock 工具 | `AWS::Bedrock::Tool` |
| AWS Cloud Map | 命名空間上的 AWS Cloud Map API 活動。 | AWS Cloud Map 命名空間 | `AWS::ServiceDiscovery::Namespace` |
| AWS Cloud Map | 服務上的 AWS Cloud Map API 活動。 | AWS Cloud Map 服務 | `AWS::ServiceDiscovery::Service` |
| Amazon CloudFront | KeyValueStore 上的 CloudFront API 活動。 | CloudFront KeyValueStore | `AWS::CloudFront::KeyValueStore` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| AWS CloudTrail | 用於記錄 AWS外部事件的 CloudTrail Lake 通道上的 CloudTrail `PutAuditEvents` 活動。 | CloudTrail 頻道 | `AWS::CloudTrail::Channel` |
| Amazon CloudWatch | 指標上的 Amazon CloudWatch API 活動。 | CloudWatch 指標 | `AWS::CloudWatch::Metric` |
| Amazon CloudWatch 網路流量監控 | 監控上的 Amazon CloudWatch Network Flow Monitor API 活動。 | 網路流量監控監視器 | `AWS::NetworkFlowMonitor::Monitor` |
| Amazon CloudWatch 網路流量監控 | 範圍上的 Amazon CloudWatch Network Flow Monitor API 活動。 | 網路流量監控範圍 | `AWS::NetworkFlowMonitor::Scope` |
| Amazon CloudWatch RUM | 應用程式監視器上的 Amazon CloudWatch RUM API 活動。 | RUM 應用程式監控 | `AWS::RUM::AppMonitor` |
| Amazon CodeGuru Profiler | 分析群組上的 CodeGuru Profiler API 活動。 | CodeGuru Profiler 分析群組 | `AWS::CodeGuruProfiler::ProfilingGroup` |
| Amazon CodeWhisperer | 自訂上的 Amazon CodeWhisperer API 活動。 | CodeWhisperer 自訂 | `AWS::CodeWhisperer::Customization` |
| Amazon CodeWhisperer | 設定檔上的 Amazon CodeWhisperer API 活動。 | CodeWhisperer | `AWS::CodeWhisperer::Profile` |

| AWS 服務 | Description | 資源類型 (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` |
| AWS Data Exchange | AWS Data Exchange 資產上的 API 活動。 | Data Exchange 資產 | `AWS::DataExchange::Asset` |
| Amazon Data Firehose | Amazon Data Firehose 交付串流 API 活動。 | Amazon Data Firehose | `AWS::KinesisFirehose::DeliveryStream` |
| AWS Deadline Cloud | Deadline Cloud 機群上的 API 活動。 | Deadline Cloud 機群 | `AWS::Deadline::Fleet` |
| AWS Deadline Cloud | Deadline Cloud 任務上的 API 活動。 | Deadline Cloud 任務 | `AWS::Deadline::Job` |
| AWS Deadline Cloud | Deadline Cloud 佇列上的 API 活動。 | Deadline Cloud 佇列 | `AWS::Deadline::Queue` |
| AWS Deadline Cloud | Deadline Cloud 工作者上的 API 活動。 | Deadline Cloud 工作者 | `AWS::Deadline::Worker` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon DynamoDB | 資料表上的 Amazon DynamoDB 項目層級 API 活動（例如 DeleteItem 、 PutItem和 UpdateItem API 操作）。<br><br>**Note**<br>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。 | DynamoDB | AWS::DynamoDB::Table |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| | 若要排除串流事件，請在 eventName 欄位上新增篩選條件。 | | |
| 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 Elastic Compute Cloud | Amazon EC2 執行個體連接端點 API 活動。 | EC2 執行個體連線端點 | AWS::EC2::InstanceConnectEndpoint |
| Amazon Elastic Container Service | 容器執行個體上的 Amazon Elastic Container Service API 活動。 | ECS 容器執行個體 | AWS::ECS::ContainerInstance |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Elastic Kubernetes Service | 儀表板上的 Amazon Elastic Kubernetes Service API 活動。 | Amazon Elastic Kubernetes Service 儀表板 | `AWS::EKS::Dashboard` |
| Amazon EMR | 預先寫入日誌工作區上的 Amazon EMR API 活動。 | EMR 預寫日誌工作區 | `AWS::EMRWAL::Workspace` |
| AWS 最終使用者傳訊簡訊 | 起始身分上的AWS 最終使用者簡訊 SMS API 活動。 | SMS 語音來源身分 | `AWS::SMSVoice::OriginationIdentity` |
| AWS 最終使用者傳訊簡訊 | 訊息上的最終AWS 使用者簡訊 SMS API 活動。 | SMS 語音訊息 | `AWS::SMSVoice::Message` |
| AWS 最終使用者傳訊社交 | 電話號碼 IDs 上的AWS 最終使用者傳訊社交 API 活動。 | 社交訊息電話號碼 ID | `AWS::SocialMessaging::PhoneNumberId` |
| AWS 最終使用者傳訊社交 | AWS Waba IDs 上的最終使用者傳訊社交 API 活動。 | 社交訊息 Waba ID | `AWS::SocialMessaging::WabaId` |
| Amazon FinSpace | 環境上的 Amazon FinSpace API 活動。 | FinSpace | `AWS::FinSpace::Environment` |
| Amazon GameLift Streams | 應用程式上的 Amazon GameLift Streams 串流 API 活動。 | GameLift Streams 應用程式 | `AWS::GameLiftStreams::Application` |
| Amazon GameLift Streams | 串流群組上的 Amazon GameLift Streams 串流 API 活動。 | GameLift Streams 串流群組 | `AWS::GameLiftStreams::StreamGroup` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| AWS Glue | AWS Glue Lake Formation 所建立資料表上的 API 活動。 | Lake Formation | `AWS::Glue::Table` |
| Amazon GuardDuty | 偵測器的 Amazon GuardDuty API 活動。 | GuardDuty 偵測器 | `AWS::GuardDuty::Detector` |
| AWS HealthImaging | AWS HealthImaging 資料存放區上的 API 活動。 | MedicalImaging 資料存放區 | `AWS::MedicalImaging::Datastore` |
| AWS HealthImaging | AWS HealthImaging 映像集 API 活動。 | MedicalImaging 影像集 | `AWS::MedicalImaging::ImageSet` |
| AWS IoT | 憑證上的 AWS IoT API 活動。 | IoT 憑證 | `AWS::IoT::Certificate` |
| AWS IoT | 物件上的 AWS IoT API 活動。 | IoT 物件 | `AWS::IoT::Thing` |
| AWS IoT Greengrass Version 2 | 元件版本上來自 Greengrass 核心裝置的 Greengrass API 活動。<br>**Note**<br>Greengrass 不會記錄存取遭拒的事件。 | IoT Greengrass 元件版本 | `AWS::GreengrassV2::ComponentVersion` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| AWS IoT Greengrass Version 2 | 部署上來自 Greengrass 核心裝置的 Greengrass API 活動。<br><br>**Note**<br>Greengrass 不會記錄存取遭拒的事件。 | IoT Greengrass 部署 | `AWS::GreengrassV2::Deployment` |
| AWS IoT SiteWise | 資產上的 IoT SiteWise API 活動。 | IoT SiteWise 資產 | `AWS::IoTSiteWise::Asset` |
| AWS IoT SiteWise | 時間序列上的 IoT SiteWise API 活動。 | IoT SiteWise 時間序列 | `AWS::IoTSiteWise::TimeSeries` |
| AWS IoT SiteWise 助理 | 對話上的 Sitewise Assistant API 活動。 | Sitewise 助理對話 | `AWS::SitewiseAssistant::Conversation` |
| AWS IoT TwinMaker | 實體上的 IoT TwinMaker API 活動。 | IoT TwinMaker 實體 | `AWS::IoTTwinMaker::Entity` |
| AWS IoT TwinMaker | 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` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Keyspaces (適用於 Apache Cassandra) | 資料表上的 Amazon Keyspaces API 活動。 | Cassandra 資料表 | `AWS::Cassandra::Table` |
| Amazon Keyspaces (適用於 Apache Cassandra) | Cassandra CDC 串流上的 Amazon Keyspaces （適用於 Apache Cassandra) API 活動。 | Cassandra CDC 串流 | `AWS::Cassandra::Stream` |
| Amazon Kinesis Data Streams | 串流上的 Kinesis Data Streams API 活動。 | Kinesis 串流 | `AWS::Kinesis::Stream` |
| Amazon Kinesis Data Streams | 串流消費者上的 Kinesis Data Streams API 活動。 | Kinesis 串流消費者 | `AWS::Kinesis::StreamConsumer` |
| Amazon Kinesis Video Streams | 視訊串流上的 Kinesis Video Streams API 活動，例如對 `GetMedia`和 的呼叫`PutMedia`。 | Kinesis 視訊串流 | `AWS::KinesisVideo::Stream` |
| Amazon Kinesis Video Streams | Kinesis Video Streams 影片訊號頻道 API 活動。 | Kinesis 影片訊號頻道 | `AWS::KinesisVideo::SignalingChannel` |
| AWS Lambda | AWS Lambda 函數執行活動 ( `Invoke` API)。 | Lambda | `AWS::Lambda::Function` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Location Maps | Amazon Location Maps API 活動。 | 地理地圖 | `AWS::GeoMaps::Provider` |
| Amazon Location Places | Amazon Location Places API 活動。 | 地理位置 | `AWS::GeoPlaces::Provider` |
| Amazon Location Routes | Amazon Location Routes API 活動。 | Geo Routes | `AWS::GeoRoutes::Provider` |
| Amazon Machine Learning | ML 模型上的Machine Learning API 活動。 | 修補 Learning MlModel | `AWS::MachineLearning::MlModel` |
| Amazon Managed Blockchain | 網路上的 Amazon Managed Blockchain API 活動。 | Managed Blockchain 網路 | `AWS::ManagedBlockchain::Network` |
| Amazon Managed Blockchain | 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 Managed Blockchain Query | Amazon Managed Blockchain Query API 活動。 | 受管區塊鏈查詢 | `AWS::ManagedBlockchainQuery::QueryAPI` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Managed Workflows for Apache Airflow | 環境上的 Amazon MWAA API 活動。 | 受管 Apache Airflow | `AWS::MWAA::Environment` |
| 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` |
| Amazon One Enterprise | UKey 上的 Amazon One Enterprise API 活動。 | Amazon One UKey | `AWS::One::UKey` |
| Amazon One Enterprise | 使用者上的 Amazon One Enterprise API 活動。 | Amazon One 使用者 | `AWS::One::User` |
| AWS Payment Cryptography | AWS Payment Cryptography 別名上的 API 活動。 | 付款密碼編譯別名 | `AWS::PaymentCryptography::Alias` |
| AWS Payment Cryptography | AWS Payment Cryptography 金鑰上的 API 活動。 | 付款密碼編譯金鑰 | `AWS::PaymentCryptography::Key` |
| Amazon Pinpoint | 行動目標應用程式上的 Amazon Pinpoint API 活動。 | 行動目標應用程式 | `AWS::Pinpoint::App` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| AWS 私有 CA | AWS 私有 CA 適用於 Active Directory API 活動的連接器。 | AWS 私有 CA 適用於 Active Directory 的連接器 | `AWS::PCAConnectorAD::Connector` |
| AWS 私有 CA | AWS 私有 CA Connector for SCEP API 活動。 | AWS 私有 CA 適用於 SCEP 的連接器 | `AWS::PCAConnectorSCEP::Connector` |
| Amazon Q Apps | Amazon Q 應用程式上的資料 API 活動。 | Amazon Q 應用程式 | `AWS::QApps::QApp` |
| Amazon Q Apps | Amazon Q App 工作階段上的資料 API 活動。 | Amazon Q 應用程式工作階段 | `AWS::QApps::QAppSession` |
| 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` |
| Amazon Q Business | 資料來源上的 Amazon Q Business API 活動。 | Amazon Q Business 資料來源 | `AWS::QBusiness::DataSource` |
| Amazon Q Business | 索引上的 Amazon Q Business API 活動。 | Amazon Q Business 索引 | `AWS::QBusiness::Index` |
| Amazon Q Business | Web 體驗上的 Amazon Q Business API 活動。 | Amazon Q Business Web 體驗 | `AWS::QBusiness::WebExperience` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Q Business | Amazon Q Business 整合 API 活動。 | Amazon Q Business 整合 | `AWS::QBusiness::Integration` |
| Amazon Q Developer | 整合上的 Amazon Q Developer API 活動。 | Q 開發人員整合 | `AWS::QDeveloper::Integration` |
| Amazon Q Developer | 有關操作調查的 Amazon Q Developer API 活動。 | AIOps 調查群組 | `AWS::AIOps::InvestigationGroup` |
| Amazon Quick | 動作連接器上的 Amazon Quick API 活動。 | AWS QuickSuite 動作 | `AWS::Quicksight::ActionConnector` |
| Amazon Quick | Amazon Quick Flow API 活動。 | QuickSight 流程 | `AWS::QuickSight::Flow` |
| Amazon Quick | Amazon Quick FlowSession API 活動。 | QuickSight 流程工作階段 | `AWS::QuickSight::FlowSession` |
| Amazon SageMaker AI | 端點上的 Amazon SageMaker AI `InvokeEndpointWithResponseStream` 活動。 | SageMaker AI 端點 | `AWS::SageMaker::Endpoint` |
| Amazon SageMaker AI | 功能存放區上的 Amazon SageMaker AI API 活動。 | SageMaker AI 功能存放區 | `AWS::SageMaker::FeatureGroup` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon SageMaker AI | 實驗試驗元件上的 Amazon SageMaker AI API 活動。 | SageMaker AI 指標實驗試驗元件 | `AWS::SageMaker::ExperimentTrialComponent` |
| Amazon SageMaker AI | Amazon SageMaker AI MLflow API 活動。 | SageMaker MLflow | `AWS::SageMaker::MlflowTrackingServer` |
| AWS Signer | 簽署任務時的簽署者 API 活動。 | 簽署者簽署任務 | `AWS::Signer::SigningJob` |
| AWS Signer | 簽署設定檔時的簽署者 API 活動。 | 簽署者簽署設定檔 | `AWS::Signer::SigningProfile` |
| Amazon Simple Email Service | 組態集上的 Amazon Simple Email Service (Amazon SES) API 活動。 | SES 組態設定 | `AWS::SES::ConfigurationSet` |
| Amazon Simple Email Service | 電子郵件身分上的 Amazon Simple Email Service (Amazon SES) API 活動。 | SES 身分 | `AWS::SES::EmailIdentity` |
| Amazon Simple Email Service | 範本上的 Amazon Simple Email Service (Amazon SES) API 活動。 | SES 範本 | `AWS::SES::Template` |
| Amazon SimpleDB | 網域上的 Amazon SimpleDB API 活動。 | SimpleDB 網域 | `AWS::SDB::Domain` |
| AWS Step Functions | Step Functions API 活動。 | 步驟函數 | `AWS::StepFunctions::Activity` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| AWS Step Functions | 在狀態機器上的 Step Functions API 活動。 | Step Functions 狀態機器 | AWS::StepFunctions::StateMachine |
| AWS Systems Manager | 控制頻道上的 Systems Manager API 活動。 | Systems Manager | AWS::SSMMessages::ControlChannel |
| AWS Systems Manager | 影響評估上的 Systems Manager API 活動。 | SSM 影響評估 | AWS::SSM::ExecutionPreview |
| AWS Systems Manager | 受管節點上的 Systems Manager API 活動。 | Systems Manager 受管節點 | AWS::SSM::ManagedNode |
| Amazon Timestream | 資料庫上的 Amazon Timestream Query API 活動。 | Timestream 資料庫 | AWS::Timestream::Database |
| Amazon Timestream | 區域端點上的 Amazon Timestream API 活動。 | Timestream 區域端點 | AWS::Timestream::RegionalEndpoint |
| Amazon Timestream | 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 精簡型客戶端 | 裝置上的 WorkSpaces 精簡型客戶端 API 活動。 | 精簡型客戶端裝置 | AWS::ThinClient::Device |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon WorkSpaces 精簡型客戶端 | 環境上的 WorkSpaces 精簡型客戶端 API 活動。 | 精簡型客戶端環境 | `AWS::ThinClient::Environment` |
| AWS X-Ray | 追蹤上的 X-Ray API 活動。 | X-Ray 追蹤 | `AWS::XRay::Trace` |
| Amazon AIDevOps | 代理程式空間上的 AIDevOps API 活動。 | 客服人員空間 | `AWS::AIDevOps::AgentSpace` |
| Amazon AIDevOps | 關聯上的 AIDevOps API 活動。 | AIDevOps 關聯 | `AWS::AIDevOps::Association` |
| Amazon AIDevOps | 操作員應用程式團隊上的 AIDevOps API 活動。 | AIDevOps 運算子應用程式團隊 | `AWS::AIDevOps::OperatorAppTeam` |
| Amazon AIDevOps | 管道中繼資料上的 AIDevOps API 活動。 | AIDevOps 管道中繼資料 | `AWS::AIDevOps::PipelineMetadata` |
| Amazon AIDevOps | 服務上的 AIDevOps API 活動。 | AIDevOps 服務 | `AWS::AIDevOps::Service` |
| Amazon Bedrock | 進階最佳化提示任務上的 Bedrock API 活動。 | AdvancedOptimizePromptJob | `AWS::Bedrock::AdvancedOptimizePromptJob` |
| Amazon Bedrock AgentCore | 評估者上的 Bedrock AgentCore API 活動。 | Bedrock-AgentCore 評估器 | `AWS::BedrockAgentCore::Evaluator` |
| Amazon 成本最佳化 | 設定檔上的 CloudOptimization API 活動。 | CloudOptimization 設定檔 | `AWS::CloudOptimization::Profile` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon 成本最佳化 | 建議的 CloudOptimization API 活動。 | CloudOptimization 建議 | AWS::CloudOptimization::Recommendation |
| Amazon GuardDuty | 惡意軟體掃描上的 GuardDuty API 活動。 | GuardDuty 惡意軟體掃描 | AWS::GuardDuty::MalwareScan |
| Amazon NovaAct | 工作流程定義的 Amazon NovaAct API 活動。 | 工作流程定義 | AWS::NovaAct::WorkflowDefinition |
| Amazon NovaAct | 工作流程執行上的 Amanzon NovaAct API 活動。 | 工作流程執行 | AWS::NovaAct::WorkflowRun |
| Amazon Redshift | 叢集上的 Redshift API 活動。 | Amazon Redshift 叢集 | AWS::Redshift::Cluster |
| Amazon Support | 租用戶上的 SupportAccess API 活動。 | SupportAccess 租用戶 | AWS::SupportAccess::Tenant |
| Amazon Support | 信任帳戶的 SupportAccess API 活動。 | SupportAccess 信任帳戶 | AWS::SupportAccess::TrustingAccount |
| Amazon Support | 信任角色的 SupportAccess API 活動。 | SupportAccess 信任角色 | AWS::SupportAccess::TrustingRole |
| Amazon 轉換 | 轉換代理程式執行個體上的 API 活動。 | 轉換代理程式執行個體 | AWS::Transform::AgentInstance |
| Amazon 轉換自訂 | 轉換行銷活動上的自訂 API 活動。 | Transform-Custom 行銷活動 | AWS::TransformCustom::Campaign |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon 轉換自訂 | 在對話上轉換自訂 API 活動。 | 轉換自訂對話 | `AWS::TransformCustom::Conversation` |
| Amazon 轉換自訂 | 在知識項目上轉換自訂 API 活動。 | Transform-Custom 知識項目 | `AWS::TransformCustom::KnowledgeItem` |
| Amazon 轉換自訂 | 轉換套件上的自訂 API 活動。 | Transform-Custom 套件 | `AWS::TransformCustom::Package` |

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 CloudTrail 資料事件，您必須明確新增要收集活動的每個資源類型。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。

## 網路活動事件

CloudTrail 網路活動事件可讓 VPC 端點擁有者記錄使用其 VPC 端點從私有 VPC 到 的 AWS API 呼叫 AWS 服務。網路活動事件可讓您了解在 VPC 內執行的資源操作。

您可以記錄下列服務的網路活動事件：

- AWS AppConfig
- AWS App Mesh
- Amazon Athena
- AWS B2B 資料交換
- AWS Backup gateway
- Amazon Bedrock
- Billing and Cost Management
- AWS 定價計算工具
- AWS Cost Explorer
- AWS 雲端控制 API

- AWS CloudHSM
- AWS Cloud Map
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- CloudWatch Application Signals
- AWS CodeDeploy
- Amazon Comprehend Medical
- AWS Config
- AWS 資料匯出
- Amazon Data Firehose
- AWS Directory Service
- Amazon DynamoDB
- Amazon EC2
- Amazon Elastic Container Service
- Amazon Elastic File System
- Elastic Load Balancing
- Amazon EventBridge
- Amazon EventBridge 排程器
- Amazon Fraud Detector
- AWS 免費方案
- Amazon FSx
- AWS Glue
- AWS HealthLake
- AWS IoT FleetWise
- AWS IoT Secure Tunneling
- AWS Invoicing
- Amazon Keyspaces (適用於 Apache Cassandra)
- AWS KMS

- AWS Lake Formation
- AWS Lambda
- AWS License Manager
- Amazon Lookout for Equipment
- Amazon Lookout for Vision
- Amazon Personalize
- Amazon Q Business
- Amazon Rekognition
- Amazon Relational Database Service
- Amazon S3

> **Note**
>
> 不支援 Amazon S3 多區域存取點。

- Amazon SageMaker AI
- AWS Secrets Manager
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Workflow Service
- AWS Storage Gateway
- AWS Systems Manager Incident Manager
- Amazon Textract
- Amazon Transcribe
- Amazon Translate
- AWS Transform
- Amazon Verified Permissions
- Amazon WorkMail

當您建立追蹤或事件資料存放區時，預設不會記錄網路活動事件。若要記錄 CloudTrail 網路活動事件，您必須明確設定要收集活動的事件來源。如需詳細資訊，請參閱記錄網路活動事件。

記錄網路活動事件需支付額外費用。如需 CloudTrail 定價，請參閱 AWS CloudTrail 定價。

### Insights 事件

CloudTrail Insights 事件會透過分析 CloudTrail 管理活動，擷取您的 AWS 帳戶中的異常 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的事件不同，只有在 CloudTrail 偵測到帳戶 API 使用情況或錯誤率記錄變化，且與帳戶的一般使用模式有很大差異時，才會記錄 Insights 事件。如需詳細資訊，請參閱使用 CloudTrail Insights。

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 使用 CloudTrail 主控台建立追蹤。如需有關建立事件資料存放區的詳細資訊，請參閱 使用主控台建立 Insights 事件的事件資料存放區。

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。

## 事件歷史記錄

CloudTrail 事件歷史記錄提供過去 90 天發生的 AWS 區域 CloudTrail 管理事件的可檢視、可搜尋、可下載而且不可變的記錄。您可以使用此歷史記錄來了解 AWS 管理主控台、 AWS SDKs、命令列工具

和其他 AWS 服務中在您 AWS 帳戶中採取的動作。您可以選取要顯示的欄位，自訂事件歷史記錄在 CloudTrail 主控台中的檢視畫面。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄。

## 線索

線索是一種組態，可讓 CloudTrail 事件交付至 S3 儲存貯體，並可選擇性交付至 CloudWatch Logs 和 Amazon EventBridge。您可以使用線索來選擇您要交付的 CloudTrail 事件、使用 AWS KMS 金鑰加密 CloudTrail 事件日誌檔案，以及設定日誌檔案交付的 Amazon SNS 通知。如需建立及管理追蹤的詳細資訊，請參閱為您的 建立線索 AWS 帳戶。

### 多區域和單一區域追蹤

您可以為 建立多區域和單一區域追蹤 AWS 帳戶。

多區域追蹤

當您建立多區域追蹤時，CloudTrail 會在 中啟用的所有 中記錄事件 AWS 區域 ， AWS 帳戶 並將 CloudTrail 事件日誌檔案交付至您指定的 S3 儲存貯體。根據最佳實務，我們建議您建立多區域追蹤，因為它會擷取所有啟用區域中的活動。使用 CloudTrail 主控台建立的所有線索都是多區域線索。您可以使用 將單一區域線索轉換為多區域線索 AWS CLI。如需詳細資訊，請參閱了解多區域追蹤和選擇加入區域、使用主控台建立追蹤及將單一區域追蹤轉換為多區域追蹤。

單一區域追蹤

當您建立單一區域追蹤時，CloudTrail 只會記錄該區域中的事件。其接著會將 CloudTrail 事件日誌檔案交付到您指定的 Amazon S3 儲存貯體。您只能使用 AWS CLI建立單一區域追蹤。如果您建立其他單一線索，則可以讓這些線索將 CloudTrail 事件日誌檔案交付到相同的 S3 儲存貯體或單獨的儲存貯體。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，請參閱使用 建立、更新和管理線索 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。

多區域追蹤具有下列優點：

- 線索的組態設定會一致地套用至所有已啟用 AWS 區域的項目。
- 您會從單一 Amazon S3 儲存貯 AWS 區域 體中啟用的所有 ，以及選擇性地在 CloudWatch Logs 日誌群組中接收 CloudTrail 事件。

- 您可以從 AWS 區域 單一位置管理所有啟用的線索組態。

建立多區域追蹤時， 具有下列效果：

- CloudTrail 會將帳戶活動的日誌檔案從所有啟用 AWS 區域 交付至您指定的單一 Amazon S3 儲存貯體，並選擇性地交付至 CloudWatch Logs 日誌群組。
- 如果您為線索設定了 Amazon SNS 主題，所有啟用的日誌檔案交付 SNS 通知 AWS 區域 都會傳送至該單一 SNS 主題。
- 您可以在所有啟用的 中看到多區域線索 AWS 區域，但您只能在建立線索的主區域中修改線索。

無論追蹤是多區域或單一區域，傳送至 Amazon EventBridge 的事件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 在每個區域可支援五個追蹤。多區域追蹤計為每個區域一個追蹤。

以下是具有五個線索的區域範例：

- 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。
- 您在美國西部 （ 加利佛尼亞北部 ） 區域建立另外兩個多區域線索。
- 您在亞太區域 （ 雪梨 ） 區域建立另一個多區域線索。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 主控台的追蹤頁面中檢視 中的 AWS 區域 追蹤清單。 如需詳細資訊，請參閱使用 CloudTrail 主控台更新線索。如需 CloudTrail 定價，請參閱 AWS CloudTrail 定價。

## 組織追蹤

組織追蹤是一種組態，可讓管理帳戶中的 CloudTrail 事件和 AWS Organizations 組織中的所有成員帳戶交付至相同的 Amazon S3 儲存貯體、CloudWatch Logs 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線索都是多區域組織線索，可從組織中每個成員帳戶中啟用 AWS 區域 的記錄事件。若要在組織的所有 AWS 分割區中記錄事件，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線索 AWS CLI。如果您建立單一區域追蹤，則只會在追蹤的 AWS 區域 （ 也稱為主區域 ） 中記錄活動。

雖然您的 預設 AWS 區域 會啟用大多數 AWS 帳戶，但您必須手動啟用特定區域 （ 也稱為選擇加入區域)。如需預設啟用哪些區域的資訊，請參閱《 AWS 帳戶管理 參考指南》中的啟用和停用區域的考量事項。如需 CloudTrail 支援的 區域清單，請參閱 CloudTrail 支援的區域。

當您建立組織線索時，會在屬於您組織的成員帳戶中建立具有您指定名稱的線索副本。

- 如果組織線索適用於單一區域，且線索的主區域不是選擇加入區域，則會在每個成員帳戶中的組織線索的主區域中建立線索副本。
- 如果組織線索適用於單一區域，且線索的主區域是選擇加入區域，則會在已啟用該區域的成員帳戶中的組織線索的主區域中建立線索副本。
- 如果組織線索是多區域，且線索的主區域不是選擇加入區域，則會在每個成員帳戶中啟用的每個 AWS 區域 中建立線索的副本。當成員帳戶啟用選擇加入區域時，會在該區域啟用完成後，在成員帳戶的新選擇區域中建立多區域追蹤的複本。
- 如果組織線索是多區域，而主要區域是選擇加入區域，成員帳戶將不會將活動傳送至組織線索，除非他們選擇加入建立多區域線索 AWS 區域 的 。例如，如果您建立多區域追蹤並選擇歐洲 （ 西班牙 ） 區域作為追蹤的主要區域，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活動傳送至組織追蹤。

> **Note**
>
> 即使資源驗證失敗，CloudTrail 仍會在成員帳戶中建立組織追蹤。驗證失敗的範例包括：
>
> - 不正確的 Amazon S3 儲存貯體政策
> - 不正確的 Amazon SNS 主題政策
> - 無法交付至 CloudWatch Logs 日誌群組
> - 使用 KMS 金鑰加密的許可不足
>
> 具有 CloudTrail 許可的成員帳戶可以透過在 CloudTrail 主控台上檢視追蹤的詳細資訊頁面，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 許可的使用者，當他們從其 AWS 帳戶登入 CloudTrail 主控台時，或當他們執行 AWS CLI 命令時，將能夠查看組織追蹤 （ 包括追蹤 ARN)，例如 `describe-trails` ( 雖然

成員帳戶在使用 時，必須針對組織追蹤使用 ARN，而非名稱 AWS CLI)。不過，成員帳戶中的使用者將沒有足夠的許可來刪除組織線索、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線索。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 Lake 和事件資料存放區

CloudTrail Lake 可讓您對事件執行精細的 SQL 型查詢，並從外部來源記錄事件 AWS，包括來自您自己的應用程式，以及來自與 CloudTrail 整合的合作夥伴。您不需要在您的帳號中設定追蹤，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 也可以將來自組織的事件存放在事件資料存放 AWS Organizations 區中的 ，或來自多個區域和帳戶的事件。CloudTrail Lake 是稽核解決方案的一部分，可協助您執行安全調查和故障診斷。如需詳細資訊，請參閱使用 AWS CloudTrail Lake及CloudTrail Lake 概念和術語。

## CloudTrail Insights

CloudTrail Insights 透過持續分析 CloudTrail 管理事件，協助 AWS 使用者識別和回應異常數量的 API 呼叫或記錄於 API 呼叫的錯誤。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。依預設，追蹤和事件資料存放區不會記錄 CloudTrail Insights 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。當您使用 CloudTrail API 時，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 Insights 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 使用 CloudTrail Insights 和 AWS CloudTrail 定價。

## Tags (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、事件資料存放區和頻道、用於存放 CloudTrail 日誌檔案的 S3 儲存貯體、 AWS Organizations 組織和組織單位等。透過將相同的標籤新增至線索和用於存放線索日誌檔案的 S3 儲存貯體，您可以使用 更輕鬆地管理、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 資源的最佳實務。

# AWS Security Token Service 和 CloudTrail

AWS Security Token Service (AWS STS) 是一種服務，具有全域端點，也支援區域特定的端點。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 AWS STS 區域特定的端點時，該區域中的線索只會交付在該區域中發生的 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 AWS STS 區域端點的詳細資訊，請參閱《IAM 使用者指南》中的AWS STS 在 AWS 區域中啟用和停用。

如需 AWS 區域端點的完整清單，請參閱《》中的AWS 區域和端點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 變更了線索擷取全球服務事件的方式。現在，Amazon CloudFront 建立的事件 AWS Identity and Access Management和 AWS STS 會記錄在建立它們的區域中，美國東部 （ 維吉尼亞北部 ） 區域 us-east-1。這使得 CloudTrail 如何處理這些服務與其他 AWS 全球服務一致的服務。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」。
>
> 相反地，CloudTrail 主控台中的事件歷史記錄和 aws cloudtrail lookup-events命令會在事件發生 AWS 區域 的 中顯示這些事件。

對於大多數服務，事件會記錄在動作所發生的區域。對於 AWS Identity and Access Management (IAM) AWS STS和 Amazon CloudFront 等全域服務，事件會交付到包含全域服務的任何線索。

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：

- 根據預設，全球服務事件會交付至使用 CloudTrail 主控台所建立的追蹤。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。
- 如果您將多區域追蹤轉換為單一區域追蹤，則該追蹤的全域服務事件記錄會自動關閉。同樣地，如果您將單一區域線索轉換為多區域線索，則全域服務事件記錄會自動為該線索開啟。

  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，請參閱使用 建立、更新和管理線索 AWS CLI。

> **Note**
>
> 當您使用 AWS CLI、 AWS SDKs或 CloudTrail API 建立或更新追蹤時，您可以指定是否要包含或排除追蹤的全域服務事件。您無法從 CloudTrail 主控台設定全球服務事件記錄日誌。

# CloudTrail 支援的區域

> **Note**
>
> 如需有關 CloudTrail Lake 支援區域的資訊，請參閱 CloudTrail Lake 支援的區域。
> 如需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 |

| 區域名稱 | 區域 | 控制平面端點 | 通訊協定 | 支援日期 |
| --- | --- | --- | --- | --- |
| 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 |
| Africa (Cape Town) | af-south-1 | cloudtrail.af-south-1.amazonaws.com | HTTPS | 04/22/2020 |
| 亞太地區 (香港) | ap-east-1 | cloudtrail.ap-east-1.amazonaws.com | HTTPS | 2019/04/24 |
| 亞太地區 (海德拉巴) | ap-south-2 | cloudtrail.ap-south-2.amazonaws.com | HTTPS | 11/22/2022 |
| 亞太地區 (雅加達) | ap-southeast-3 | cloudtrail.ap-southeast-3.amazonaws.com | HTTPS | 12/13/2021 |
| 亞太地區 (馬來西亞) | ap-southeast-5 | cloudtrail.ap-southeast-5.amazonaws.com | HTTPS | 08/22/2024 |
| 亞太地區 (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 |
| 亞太地區 (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 |

| 區域名稱 | 區域 | 控制平面端點 | 通訊協定 | 支援日期 |
|---|---|---|---|---|
| 亞太地區 (悉尼) | ap-southeast-2 | cloudtrail.ap-southeast-2.amazonaws.com | HTTPS | 2014/05/13 |
| 亞太區域 (泰國) | ap-southeast-7 | cloudtrail.ap-southeast-7.amazonaws.com | HTTPS | 01/07/2025 |
| 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 |
| 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 |
| Europe (Paris) | 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 |

| 區域名稱 | 區域 | 控制平面端點 | 通訊協定 | 支援日期 |
| --- | --- | --- | --- | --- |
| Europe (Stockholm) | 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 |
| 墨西哥 (中部) | mx-central-1 | cloudtrail.mx-central-1.amazonaws.com | HTTPS | 01/13/2025 |
| Middle East (Bahrain) | 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 | 08/30/2022 |
| 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 |
| AWS GovCloud （美國西部） | us-gov-west-1 | cloudtrail.us-gov-west-1.amazonaws.com | HTTPS | 2011/08/16 |

如需在 中使用 CloudTrail 的詳細資訊 AWS GovCloud (US) Regions，請參閱AWS GovCloud (US)《 使用者指南》中的服務端點。

如需在中國 （北京） 區域中使用 CloudTrail 的詳細資訊，請參閱《》AWS 中的中國的端點和 ARNsAmazon Web Services 一般參考。

# CloudTrail 支援的服務和整合

CloudTrail 支援許多 的記錄事件 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 CloudTrail 的服務主題。此外，有些 AWS 服務 可用於分析 CloudTrail 日誌中收集的資料並對其採取行動。

> **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 服務與 CloudTrail 日誌的整合
- CloudTrail 與 Amazon EventBridge 整合
- CloudTrail 與 整合 AWS Organizations
- CloudTrail 與 整合 AWS Control Tower
- CloudTrail 與 Amazon Security Lake 整合
- CloudTrail Lake 與 Amazon Athena 整合
- CloudTrail Lake 與 整合 AWS Config
- CloudTrail Lake 與 整合 AWS Audit Manager
- AWS CloudTrail 的服務主題
- CloudTrail 不支援的服務


## AWS 服務與 CloudTrail 日誌的整合

> **Note**
>
> 您還可以使用 CloudTrail Lake 來查詢和分析您的事件。與事件歷史記錄中單純的索引鍵和值查詢或執行 `LookupEvents` 相比，CloudTrail Lake 查詢提供了更深入、自訂功能更多的事件檢視畫面。CloudTrail Lake 使用者可以在 CloudTrail 事件中跨多個欄位執行複雜的標準查詢語言 (SQL) 查詢。如需詳細資訊，請參閱使用 AWS CloudTrail Lake及將追蹤事件複製到 CloudTrail Lake。

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，以進一步分析和處理 CloudTrail 日誌中收集的事件資料。如需詳細資訊，請參閱下列主題。

| AWS 服務 | 主題 | Description |
| --- | --- | --- |
| Amazon Athena | 查詢 AWS CloudTrail 日誌 | 搭配 CloudTrail 日誌使用 Athena 是增強服務活動分析的強大方式 AWS 。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。<br><br>您可以自動建立資料表以直接從 CloudTrail 主控台查詢日誌，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》中的在 CloudTrail 主控台中建立 CloudTrail 日誌的資料表。<br><br>**Note**<br>在 Amazon Athena 中執行查詢會產生額外的成本。如需詳細資訊，請參閱 Amazon Athena 定價。 |
| Amazon CloudWatch Logs | 使用 Amazon CloudWatch Logs 監控 CloudTrail 日誌檔案 | 您可以設定含 CloudWatch Logs 的 CloudTrail 監控您的追蹤日誌，並在發生特定活動時通知您。例如，您可以定義 |

| AWS 服務 | 主題 | Description |
| --- | --- | --- |
| | | CloudWatch Logs 指標篩選條件，以觸發 CloudWatch 警示，並在觸發這些警示時將通知傳送給您。<br><br>**Note**<br>Amazon CloudWatch 和 Amazon CloudWatch Logs 適用的標準定價。如需詳細資訊，請參閱 Amazon CloudWatch 定價。 |

## CloudTrail 與 Amazon EventBridge 整合

Amazon EventBridge 是一項 AWS 服務，可提供近乎即時的系統事件串流，描述 AWS 資源的變更。在 EventBridge 中，您可以建立回應 CloudTrail 記錄之事件的規則。如需詳細資訊，請參閱在 Amazon EventBridge 中建立規則。

您可以使用 EventBridge 主控台建立規則，將您在追蹤中訂閱的事件交付至 EventBridge。

從 EventBridge 主控台：

- 選擇`AWS API Call via CloudTrail`詳細資訊類型，以使用 `eventType`的 交付 CloudTrail 資料和管理事件`AwsApiCall`。若要記錄詳細資訊類型值為 的事件`AWS API Call via CloudTrail`，您必須擁有目前正在記錄管理或資料事件的線索。
- 選擇 `AWS Console Sign In via CloudTrail` detail-type 以傳遞AWS 管理主控台 登入事件。若要使用 的詳細資訊類型記錄事件`AWS Console Sign In via CloudTrail`，您必須具有目前正在記錄管理事件的線索。
- 選擇`AWS Insight via CloudTrail`詳細資訊類型以交付 Insights 事件。若要記錄詳細資訊類型值為 的事件`AWS Insight via CloudTrail`，您必須擁有目前正在記錄 Insights 事件的線索。如需有關記錄 Insights 事件的詳細資訊，請參閱 使用 CloudTrail Insights。

如需有關如何建立追蹤的詳細資訊，請參閱 使用 CloudTrail 主控台建立追蹤。

## 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。建立組織追蹤或組織事件資料存放區可協助您為組織定義統一的事件記錄策略。

## CloudTrail 與 整合 AWS Control Tower

AWS Control Tower 當您設定登陸區域時， 會設定新的 CloudTrail 組織追蹤記錄管理事件。當您註冊帳戶時 AWS Control Tower，您的帳戶會受組織的組織追蹤管理 AWS Control Tower 。如果您在該帳戶中有現有的組織線索，除非您在註冊該帳戶之前刪除該帳戶的現有線索，否則可能會看到重複費用 AWS Control Tower。您可以在 CloudTrail 主控台上檢視線索頁面，以查看是否已建立任何組織線索。如需 的詳細資訊 AWS Control Tower，請參閱AWS CloudTrail 《 使用者指南》中的關於登入 AWS Control Tower。

## CloudTrail 與 Amazon Security Lake 整合

Security Lake 可以收集與 S3 和 Lambda 的 CloudTrail 管理事件和 CloudTrail 資料事件相關聯的日誌。 S3 如需詳細資訊，請參閱《Amazon Security Lake 使用者指南》中的 CloudTrail 事件日誌。

若要在 Security Lake 中收集 CloudTrail 管理事件，您必須擁有至少一個 CloudTrail 多區域組織線索，以收集讀取和寫入 CloudTrail 管理事件。

## CloudTrail Lake 與 Amazon Athena 整合

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 Data Catalog 中的資料表中繼資料可讓 Athena 查詢引擎了解如何尋找、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。

## CloudTrail Lake 與 整合 AWS Config

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。如需詳細資訊，請參閱使用主控台為組態項目建立事件資料存放區。

## CloudTrail Lake 與 整合 AWS Audit Manager

您可以使用 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 在 CloudTrail Lake 中彙總證據的詳細資訊，請參閱 AWS Audit Manager 使用者指南中的了解證據搜尋工具如何與 CloudTrail Lake 搭配運作。

## AWS CloudTrail 的服務主題

您可以進一步了解如何在 CloudTrail 日誌中記錄個別 AWS 服務的事件，包括日誌檔案中該服務的範例事件。如需特定 AWS 服務如何與 CloudTrail 整合的詳細資訊，請參閱該服務個別指南中的整合相關主題。

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。

> **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 | 使用 記錄對 Amazon API Gateway 的 API 管理呼叫 AWS CloudTrail | 2015/07/09 |
| Amazon AppFlow | 使用 AWS CloudTrail記錄 Amazon AppFlow API 呼叫 | 04/22/2020 |
| Amazon WorkSpaces 應用程式 | 使用 記錄 Amazon WorkSpaces 應用程式 API 呼叫 AWS CloudTrail | 2019/04/25 |
| Amazon Athena | 使用 記錄 Amazon Athena API 呼叫 AWS CloudTrail | 2017/05/19 |

| AWS 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| Amazon Aurora | 在 中監控 Amazon Aurora API 呼叫 AWS CloudTrail | 08/31/2018 |
| Amazon Bedrock | 使用 記錄 Amazon Bedrock API 呼叫 AWS CloudTrail | 10/23/2023 |
| Amazon Braket | 使用 CloudTrail 的 Amazon Braket API 記錄 | 08/12/2020 |
| Amazon Chime | 使用 記錄 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 | 使用 AWS CloudTrail 擷取傳送至 CloudFront API 的請求 | 2014/05/28 |
| Amazon CloudSearch | 使用 記錄 Amazon CloudSearch 組態服務呼叫 AWS CloudTrail | 2014/10/16 |
| Amazon CloudWatch | 在 中記錄 Amazon CloudWatch API 呼叫 AWS CloudTrail | 2014/04/30 |
| Amazon CloudWatch Logs | 在 中記錄 Amazon CloudWatch Logs API 呼叫 AWS CloudTrail | 2016/03/10 |
| Amazon CodeCatalyst | AWS 帳戶 使用 在 連線的 中記錄 CodeCatalyst API 呼叫 AWS CloudTrail | 12/01/2022 |
| Amazon CodeGuru Reviewer | 使用 AWS CloudTrail記錄 Amazon CodeGuru Reviewer API 呼叫 | 12/02/2019 |

| AWS 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| Amazon Cognito | 使用 記錄 Amazon Cognito API 呼叫 AWS CloudTrail | 2016/02/18 |
| Amazon Comprehend | 使用 記錄 Amazon Comprehend API 呼叫 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 Data Firehose | 使用 監控 Amazon Data Firehose API 呼叫 AWS CloudTrail | 2016/03/17 |
| 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 Guru | 使用 記錄 Amazon DevOps Guru API 呼叫 AWS CloudTrail | 05/04/2021 |
| 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 操作 AWS CloudTrail | 2015/05/28 |

| AWS 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| Amazon EC2 | 使用 記錄 Amazon EC2 API 呼叫 AWS CloudTrail | 11/13/2013 |
| Amazon EC2 Auto Scaling | 使用 CloudTrail 記錄 Auto Scaling API 呼叫 | 2014/07/16 |
| Amazon EC2 容量區塊 | 使用 記錄容量區塊 API 呼叫 AWS CloudTrail | 10/31/2023 |
| Amazon EC2 Image Builder | 使用 CloudTrail 記錄 EC2 Image Builder API 呼叫 | 12/02/2019 |
| Amazon Elastic Block Store (Amazon EBS)<br><br>EBS 直接 API | 使用 記錄 API 呼叫 AWS CloudTrail<br><br>使用 AWS CloudTrail記錄 EBS 直接 API 的 API 呼叫 | Amazon EBS：2013/11/13<br><br>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 |
| 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 記錄 Amazon EKS API 呼叫 AWS CloudTrail | 2018/06/05 |
| Amazon Elastic Transcoder | 使用 記錄 Amazon Elastic Transcoder API 呼叫 AWS CloudTrail | 2014/10/27 |
| Amazon ElastiCache | 使用 記錄 Amazon ElastiCache API 呼叫 AWS CloudTrail | 2014/09/15 |

| AWS 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| Amazon EMR | 使用 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 日誌 | 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 | 使用 記錄 Amazon FSx for Lustre API 呼叫 AWS CloudTrail | 01/11/2019 |
| Amazon FSx for Windows File Server | 使用 監控 AWS CloudTrail | 2018/11/28 |
| Amazon GameLift Servers | 使用 記錄 Amazon GameLift Servers API 呼叫 AWS CloudTrail | 2016/01/27 |
| Amazon GameLift Streams | 使用 記錄 Amazon GameLift Streams API 呼叫 AWS CloudTrail | 03/05/2025 |
| Amazon GuardDuty | 使用 記錄 Amazon GuardDuty API 呼叫 AWS CloudTrail | 2018/02/12 |

| AWS 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| Amazon Inspector | 使用 記錄 Amazon Inspector API 呼叫 AWS CloudTrail | 11/29/2021 |
| Amazon Inspector Classic | 使用 記錄 Amazon Inspector Classic API 呼叫 AWS CloudTrail | 2016/04/20 |
| Amazon Inspector 掃描 | CloudTrail 中的 Amazon Inspector 掃描資訊 | 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 記錄 Amazon Kendra API 呼叫 AWS CloudTrail，並使用 AWS CloudTrail 日誌記錄 Amazon Kendra Intelligent Ranking API 呼叫 | 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 | 使用 記錄 Managed Service for Apache Flink API 呼叫 AWS CloudTrail | 2019/03/22 |
| Amazon Kinesis Data Streams | 使用 記錄 Amazon Kinesis Data Streams API 呼叫 AWS CloudTrail | 2014/04/25 |
| Amazon Kinesis Video Streams | 使用 記錄 Kinesis Video Streams API 呼叫 AWS CloudTrail | 2018/05/24 |
| Amazon Lex | 使用 CloudTrail 記錄 Amazon Lex API 呼叫 | 2017/08/15 |

| AWS 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| 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 Amazon Lookout for Equipment | 12/01/2020 |
| Amazon Lookout for Metrics | 在 中檢視 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<br><br>使用 AWS CloudTrail記錄 Ethereum 的 Managed Blockchain API 呼叫 (預覽版) | 04/01/2019 |
| Amazon Managed Grafana | 使用 AWS CloudTrail記錄 Amazon Managed Grafana API 呼叫 | 12/15/2020 |

| AWS 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| 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 | 在 中檢視稽核日誌 AWS CloudTrail | 11/24/2020 |
| Amazon MemoryDB | 使用 記錄 Amazon MemoryDB API 呼叫 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 One Enterprise | 使用 記錄 Amazon One Enterprise API 呼叫 AWS CloudTrail | 11/27/2023 |
| Amazon OpenSearch Service | 使用 監控 Amazon OpenSearch Service API 呼叫 AWS CloudTrail | 2015/10/01 |
| Amazon Personalize | 使用 記錄 Amazon Personalize API 呼叫 AWS CloudTrail | 2018/11/28 |
| 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 |

| AWS 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| Amazon Polly | 使用 記錄 Amazon Polly API 呼叫 AWS CloudTrail | 11/30/2016 |
| Amazon Q Business | 使用 記錄 Amazon Q Business API 呼叫 AWS CloudTrail | 11/28/2023 |
| Amazon Q Developer | 使用 記錄 Amazon Q Developer API 呼叫 AWS CloudTrail | 11/28/2023 |
| Amazon Quantum Ledger Database (Amazon QLDB) | 使用 記錄 Amazon QLDB API 呼叫 AWS CloudTrail | 09/10/2019 |
| Amazon Quick | 使用 CloudTrail 記錄操作 | 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<br><br>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 |
| Amazon Application Recovery Controller (ARC) | 使用 記錄 Amazon Application Recovery Controller (ARC) API 呼叫 AWS CloudTrail | 07/27/2021 |

| AWS 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| Amazon S3 | 使用 記錄 Amazon S3 API 呼叫 AWS CloudTrail | 管理事件：2015/09/01<br>資料事件：2016/11/21 |
| Amazon Glacier | 使用 記錄 Amazon Glacier API 呼叫 AWS CloudTrail | 2014/12/11 |
| Amazon SageMaker AI | 使用 記錄 Amazon SageMaker AI API 呼叫 AWS CloudTrail | 2018/01/11 |
| Amazon Security Lake | 使用 CloudTrail 記錄 Amazon Security Lake API 呼叫 | 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：05/13/2014<br>資料事件：02/14/2024 |
| Amazon Textract | 使用 記錄 Amazon Textract API 呼叫 AWS CloudTrail | 2019/05/29 |
| Amazon Timestream | 使用 記錄 Timestream API 呼叫 AWS CloudTrail | 09/30/2020 |
| Amazon Transcribe | 使用 記錄 Amazon Transcribe API 呼叫 AWS CloudTrail | 2018/06/28 |
| Amazon Translate | 使用 AWS CloudTrail記錄 Amazon Translate API 呼叫 | 2018/04/04 |

| AWS 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| Amazon Verified Permissions | 使用 記錄 Amazon Verified Permissions API 呼叫 AWS CloudTrail | 06/13/2023 |
| Amazon Virtual Private Cloud (Amazon VPC) | 使用 記錄 API 呼叫 AWS CloudTrail<br><br>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 | 使用 記錄 Reachability Analyzer API 呼叫 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 CloudTrail 記錄 Amazon WorkSpaces API 呼叫 | 2015/04/09 |
| Amazon WorkSpaces 精簡型客戶端 | 使用 記錄 Amazon WorkSpaces 精簡型客戶端 API 呼叫 AWS CloudTrail | 11/26/2023 |
| Amazon WorkSpaces Web | 使用 AWS CloudTrail記錄 Amazon WorkSpaces Web API 呼叫 | 11/30/2021 |
| Application Auto Scaling | 使用 記錄 Application Auto Scaling API 呼叫 AWS CloudTrail | 2016/10/31 |

| AWS 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| AWS 帳戶管理 | 使用 記錄 AWS 帳戶管理 API 呼叫 AWS CloudTrail | 10/01/2021 |
| 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<br>App Mesh Envoy 管理服務 03/18/2022 |
| AWS App Runner | 使用 記錄 App Runner API 呼叫 AWS CloudTrail | 05/18/2021 |
| AWS AppConfig | 使用 記錄 AWS AppConfig API 呼叫 AWS CloudTrail | 管理事件：07/31/2020<br>資料事件：01/04/2024 |
| AWS AppFabric | 使用 記錄 AWS AppFabric API 呼叫 AWS CloudTrail | 06/27/2023 |
| AWS Application Discovery Service | 使用 AWS CloudTrail記錄 Application Discovery Service API 呼叫 | 2016/05/12 |
| AWS 應用程式轉換服務 | ( AWS 工具使用的後端服務，例如適用於 .NET 的 AWS Microservice Extractor) | 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 Audit Manager | 使用 記錄 AWS Audit Manager API 呼叫 AWS CloudTrail | 12/07/2020 |

| AWS 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| AWS Auto Scaling | 使用 CloudTrail 記錄 AWS Auto Scaling API 呼叫 | 08/15/2018 |
| AWS B2B 資料交換 | 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 帳單與成本管理 | 使用 記錄 AWS 帳單與成本管理 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 CloudTrail 記錄 BugBust API 呼叫 | 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 CloudFormation | 在 中記錄 AWS CloudFormation API 呼叫 AWS CloudTrail | 2014/04/02 |

| AWS 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| AWS CloudHSM | 使用 記錄 AWS CloudHSM API 呼叫 AWS CloudTrail | 2015/01/08 |
| AWS CloudShell | 在 中記錄和監控 AWS CloudShell | 12/15/2020 |
| AWS CloudTrail | AWS CloudTrail API 參考 (CloudTrail 會記錄所有 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 | 使用 監控部署 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 | 使用 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 AWS CloudTrail | 2015/02/10 |
| AWS 控制目錄 | 使用 記錄 AWS Control Catalog API 呼叫 AWS CloudTrail | 04/08/2024 |

| AWS 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| AWS Control Tower | 使用 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 Deadline Cloud | 使用 記錄 Deadline Cloud API 呼叫 AWS CloudTrail | 04/02/2024 |
| AWS Device Farm | 使用 記錄 AWS Device Farm API 呼叫 AWS CloudTrail | 2015/07/13 |
| Direct Connect | 在 中記錄 Direct Connect API 呼叫 AWS CloudTrail | 2014/03/08 |
| Directory Service | 使用 CloudTrail 記錄 Directory Service API 呼叫 | 2015/05/14 |
| Directory Service 資料 | 使用 記錄 Directory Service 資料 API 呼叫 AWS CloudTrail | 09/18/2024 |
| AWS Elastic Beanstalk (Elastic Beanstalk) | 搭配 使用 Elastic Beanstalk API 呼叫 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 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| AWS Elemental MediaConnect | 使用 記錄 AWS Elemental MediaConnect API 呼叫 AWS CloudTrail | 11/27/2018 |
| AWS Elemental MediaConvert | 使用 CloudTrail 記錄 AWS Elemental MediaConvert API 呼叫 | 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 CloudTrail 記錄 AWS Elemental MediaStore API 呼叫 | 2017/11/27 |
| AWS Elemental MediaTailor | 使用 記錄 AWS Elemental MediaTailor API 呼叫 AWS CloudTrail | 2019/02/11 |
| AWS 最終使用者傳訊簡訊 | 使用 記錄 AWS 最終使用者簡訊 SMS API 呼叫 AWS CloudTrail | 10/10/2024 |
| AWS 最終使用者傳訊社交 | 使用 記錄 AWS 最終使用者傳訊社交 API 呼叫 AWS CloudTrail | 10/10/2024 |
| AWS 實體解析 | 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 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| AWS Firewall Manager | 使用 記錄 AWS Firewall Manager API 呼叫 AWS CloudTrail | 2018/04/05 |
| AWS Global Accelerator | 使用 記錄 AWS Global Accelerator API 呼叫 AWS CloudTrail | 11/26/2018 |
| AWS Glue | 使用 記錄 AWS Glue 操作 AWS CloudTrail | 2017/11/07 |
| AWS Ground Station | 使用 記錄 AWS Ground Station API 呼叫 AWS CloudTrail | 05/31/2019 |
| AWS Health | 使用 記錄 AWS Health API 呼叫 AWS CloudTrail | 2016/11/21 |
| AWS Health 儀板表 | 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 Identity Center API 呼叫 AWS CloudTrail | 2017/12/07 |
| AWS IAM Identity Center – SCIM | 使用 記錄 IAM Identity Center API 呼叫 AWS CloudTrail | 10/28/2024 |

| AWS 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| 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 Events | 了解 AWS IoT Events 日誌檔案項目 | 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 的 Log AWS IoT Greengrass V2 API 呼叫 AWS CloudTrail | 12/14/2020 |
| 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<br>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 AWS License Manager API 呼叫 AWS CloudTrail | 2019/03/01 |

| AWS 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| AWS Mainframe Modernization | 使用 記錄 AWS Mainframe Modernization API 呼叫 AWS CloudTrail | 06/08/2022 |
| 的受管整合 AWS IoT Device Management | 使用 記錄受管整合 API 呼叫 AWS CloudTrail | 03/03/2025 |
| AWS Managed Services | AMS Accelerate 中的日誌管理 | 2016/12/21 |
| AWS Marketplace 協議 | 使用 記錄協議 API 呼叫 AWS CloudTrail | 09/01/2023 |
| AWS Marketplace 部署服務 | 使用 CloudTrail 記錄 AWS Marketplace 部署服務呼叫 | 11/29/2023 |
| AWS Marketplace 探索 | 使用 記錄 AWS Marketplace Discovery 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 Migration Hub | 使用 記錄 AWS Migration Hub API 呼叫 AWS CloudTrail | 2017/08/14 |
| AWS Migration Hub 旅程 | 使用 記錄 AWS Migration Hub 旅程 API 呼叫 AWS CloudTrail | 12/03/2024 |
| 多方核准 | 使用 記錄多方核准 API 呼叫 AWS CloudTrail | 06/17/2025 |
| AWS Network Firewall | 使用 記錄對 AWS Network Firewall API 的呼叫 AWS CloudTrail | 11/17/2020 |

| AWS 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| 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 | 使用 記錄 Puppet Enterprise API 呼叫的 OpsWorks AWS CloudTrail | 2018/07/16 |
| AWS OpsWorks Stacks | 使用 記錄 AWS OpsWorks Stacks API 呼叫 AWS CloudTrail | 2014/06/04 |
| Oracle Database@AWS | 使用 記錄 Oracle Database@AWS API 呼叫 AWS CloudTrail | 12/01/2024 |
| 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 私有 5G | 使用 記錄 AWS 私有 5G API 呼叫 AWS CloudTrail | 08/11/2022 |
| AWS 私有憑證授權單位 (AWS 私有 CA) | 使用 CloudTrail | 2018/04/04 |
| AWS Proton | 在 中記錄和監控 AWS Proton | 06/09/2021 |

| AWS 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| AWS re:Post 私有 | 使用 記錄 AWS re:Post 私有 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 | 資源群組中的記錄和監控 | 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 CSPM | 使用 記錄 AWS Security Hub CSPM API 呼叫 AWS CloudTrail | 11/27/2018 |
| AWS 安全事件回應 | 使用 記錄 AWS 安全事件回應 API 呼叫 AWS CloudTrail | 12/01/2024 |
| AWS Security Token Service (AWS STS) | 使用 記錄 IAM 事件 AWS CloudTrail<br><br>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 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| AWS Shield | 使用 記錄 Shield 進階 API 呼叫 AWS CloudTrail | 2018/02/08 |
| AWS Snowball Edge Edge | 使用 記錄 AWS Snowball Edge Edge 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 支援 | 使用 記錄 AWS 支援 API 呼叫 AWS CloudTrail | 2016/04/21 |
| 支援 建議 （預覽） | 使用 支援 記錄建議 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 Incident Manager API 呼叫 AWS CloudTrail | 05/10/2021 |
| AWS 電信網路建置器 (AWS TNB) | 使用 AWS 記錄 Telco Network Builder API 呼叫 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 服務 | CloudTrail 主題 | 支援開始時間 |
| --- | --- | --- |
| AWS Transit Gateway | 使用 AWS CloudTrail記錄 Transit Gateway 的 API 呼叫 | 11/26/2018 |
| AWS Trusted Advisor | 使用 記錄 AWS Trusted Advisor 主控台動作 AWS CloudTrail | 10/22/2020 |
| 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 CloudTrail 記錄 AWS X-Ray API 呼叫 | 2018/04/25 |
| Elastic Load Balancing | AWS CloudTrail 記錄 Classic Load Balancer 和AWS CloudTrail 記錄 Application Load Balancer | 2014/04/04 |
| FreeRTOS 無線更新 (OTA) | 使用 AWS IoT 記錄 OTA API 呼叫 AWS CloudTrail | 2019/05/22 |
| Service Quotas | 使用 記錄 Service Quotas API 呼叫 AWS CloudTrail | 06/24/2019 |

## CloudTrail 不支援的服務

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

如需支援的 AWS 服務清單，請參閱 AWS CloudTrail 的服務主題。

# 中的配額 AWS CloudTrail

本節說明 CloudTrail 中的資源配額（先前稱為限制）。如需 CloudTrail 中所有配額的相關資訊，請參閱《》中的服務配額AWS 一般參考。

> **Note**
>
> CloudTrail 沒有可調整的配額。

## CloudTrail 資源配額

下表說明 CloudTrail 中的資源配額。

| 資源 | 預設配額 | 說明 |
| --- | --- | --- |
| 每個區域的追蹤數目 | 5 | 每個 的線索數目上限 AWS 區域。<br><br>在陰影區域中，若要取得最新的資源計數指標，請呼叫 `ListTrails` API。<br><br>此配額無法增加。 |
| 事件資料存放區 | 10 | 每個 的事件資料存放區數目上限 AWS 區域。這包括 區域的單一區域事件資料存放區、跨所有 的多區域事件資料存放區 AWS 區域，以及組織事件資料存放區。它還包括處於任 |

| 資源 | 預設配額 | 說明 |
| --- | --- | --- |
| | | 何生命週期階段的事件資料存放區。<br><br>在陰影區域中，若要取得最新的資源計數指標，請呼叫 `ListEventDataStores` API。<br><br>此配額無法增加。 |
| 頻道 | 25 | 此配額適用於用於 CloudTrail Lake 與 外部事件來源整合的頻道 AWS，不適用於服務連結頻道。<br><br>此配額無法增加。 |
| 每個區域的儀表板 | 100 | 每個 CloudTrail Lake 自訂儀表板的數量上限 AWS 區域。<br><br>在陰影區域中，若要取得最新的資源計數指標，請呼叫 `ListDashboards` API。<br><br>此配額無法增加。 |
| 每個儀表板的小工具 | 10 | 每個 CloudTrail Lake 儀表板的小工具數量上限。<br><br>此配額無法增加。 |
| 並行儀表板重新整理 | 1 | 每個儀表板的持續重新整理數量上限。<br><br>此配額無法增加。 |

| 資源 | 預設配額 | 說明 |
| --- | --- | --- |
| 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的數目上限。<br><br>此配額無法增加。 |
| 每個 PutAuditEvents 請求的事件數 | 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)。<br><br>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。 |
| 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。<br><br>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 | 如果您選擇使用事件選取器來限制資料事件，則追蹤中所有事件選取器的資料資源總數不能超過 250。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。<br><br>範例：<br><br>• 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)<br>• 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)<br>• 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)<br><br>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。<br><br>此配額無法增加。<br><br>如果您選擇在所有資源 (例如所有 S3 儲存貯體或所有 Lambda 函數) 上記錄資料事件，則此配額不適用。 |

| 資源 | 預設配額 | 說明 |
| --- | --- | --- |
| 事件大小 | 所有事件版本：無法將超過 256 KB 的事件傳送至 CloudWatch Logs<br><br>事件版本 1.05 及更新版本：總事件大小限制為 256 KB | Amazon CloudWatch Logs 和 Amazon EventBridge 各允許事件大小上限為 256 KB。CloudTrail 不會將超過 256 KB 的事件傳送至 CloudWatch Logs 或 EventBridge。<br><br>從事件版本 1.05 開始，事件的大小上限為 256 KB。這是為了幫助防止惡意行為者利用，並允許其他 AWS 服務使用，例如 CloudWatch Logs 和 EventBridge。 |
| 傳送到 Amazon S3 的 CloudTrail 檔案大小 | 壓縮前 50 MB | 對於管理、資料和網路活動事件，CloudTrail 會以壓縮的 gzip 檔案將事件傳送至 S3。壓縮前的檔案大小上限為 50 MB。<br><br>如果在追蹤上啟用 ，在 CloudTrail 將 gzip 檔案傳送至 S3 之後，Amazon SNS 會傳送日誌交付通知。 |

## CloudTrail 中的每秒交易數 (TPS) 配額

AWS 一般參考 列出 AWS APIs 的每秒交易數 (TPS) 配額。API 的每秒交易 (TPS) 配額代表您可以為指定的 API 每秒提出多少請求，而不會受到調節。例如，CloudTrail `LookupEvents` API 的 TPS 配額為 2。

如需每個 CloudTrail API 的 TPS 配額相關資訊，請參閱 中的服務配額AWS 一般參考。

# AWS CloudTrail 教學課程入門

如果您是初次使用 AWS CloudTrail，這些教學課程可協助您了解如何使用其功能。若要使用 CloudTrail 功能，您需要擁有足夠的許可。此頁面說明適用於 CloudTrail 的受管政策，並提供有關如何授予許可的資訊。

範例：

- 授予使用 CloudTrail 的許可
- 檢視事件歷史記錄
- 建立追蹤以記錄管理事件
- 建立 S3 資料事件的事件資料存放區

## 授予使用 CloudTrail 的許可

若要建立、更新和管理追蹤、事件資料存放區和頻道等 CloudTrail 資源，您需要授予使用 CloudTrail 的許可。本節提供有關適用於 CloudTrail 的受管政策的資訊。

> **Note**
>
> 您授予使用者執行 CloudTrail 管理任務的許可，和 CloudTrail 所需要以便傳遞日誌檔案到 Amazon S3 儲存貯體或傳送通知給 Amazon SNS 主題的許可不相同。如需這些許可的詳細資訊，請參閱 適用於 CloudTrail 的 Amazon S3 儲存貯體政策。
> 如果您設定與 Amazon CloudWatch Logs 整合，CloudTrail 還需要它可擔任的角色，將事件交付到 Amazon CloudWatch Logs 日誌群組。您必須建立 CloudTrail 使用的角色。如需詳細資訊，請參閱授與在 CloudTrail 主控台上檢視和設定 Amazon CloudWatch Logs 資訊的許可及傳送事件到 CloudWatch Logs。

下列 AWS 受管政策適用於 CloudTrail：

- AWSCloudTrail_FullAccess – 此政策提供對 CloudTrail 資源 (例如追蹤、事件資料存放區和通道等) 執行 CloudTrail 動作的完整存取權。此政策提供建立、更新和刪除 CloudTrail 追蹤、事件資料存放區和通道所需的許可。

  此政策還提供管理 Amazon S3 儲存貯體、CloudWatch Logs 的日誌群組，以及追蹤的 Amazon SNS 主題的許可。不過，`AWSCloudTrail_FullAccess` 受管政策不提供刪除 Amazon S3 儲存貯

體、CloudWatch Logs 的日誌群組，以及 Amazon SNS 主題的許可。如需其他 AWS 服務的受管政策相關資訊，請參閱 AWS 受管政策參考指南。

> **Note**
>
> 此AWSCloudTrail_FullAccess政策不適用於在您的 之間廣泛共用 AWS 帳戶。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 – 此政策授予檢視 CloudTrail 主控台 (包括近期事件和事件歷史記錄) 的許可。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：

- 中的使用者和群組 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。遵循《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。
- 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。
  - (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。

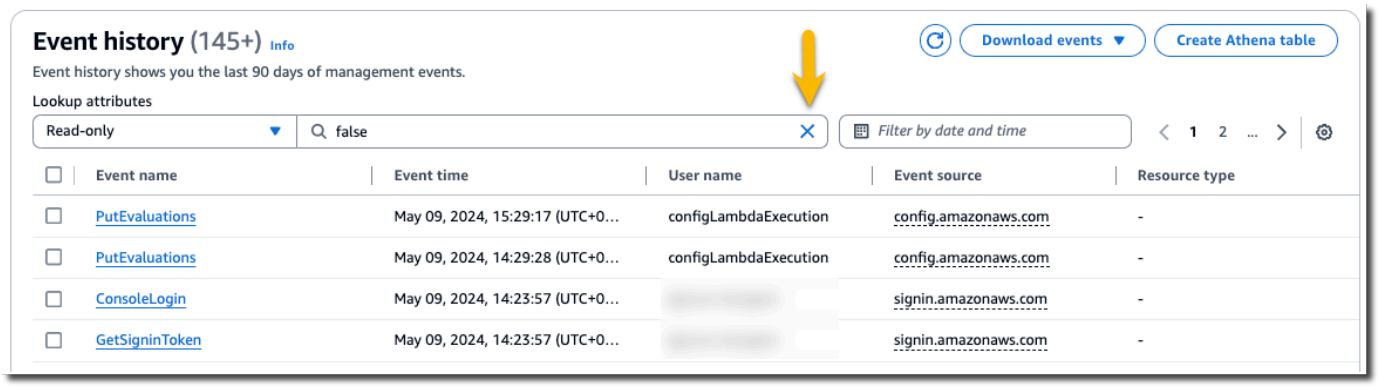
# 檢視事件歷史記錄

本節說明如何使用 CloudTrail 主控台上的 CloudTrail 事件歷史記錄頁面，檢視 AWS 帳戶 目前 過去 90 天的管理事件 AWS 區域。

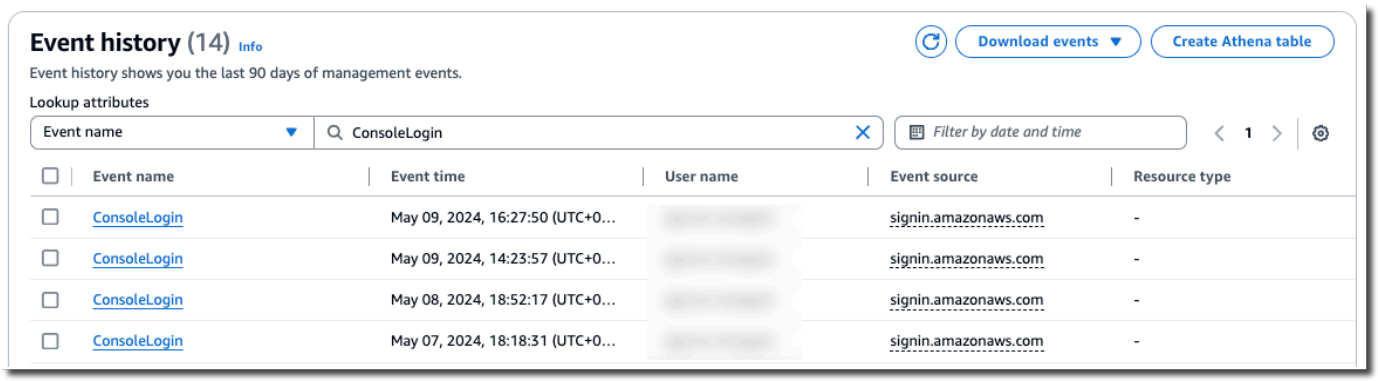
檢視事件歷史記錄

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。

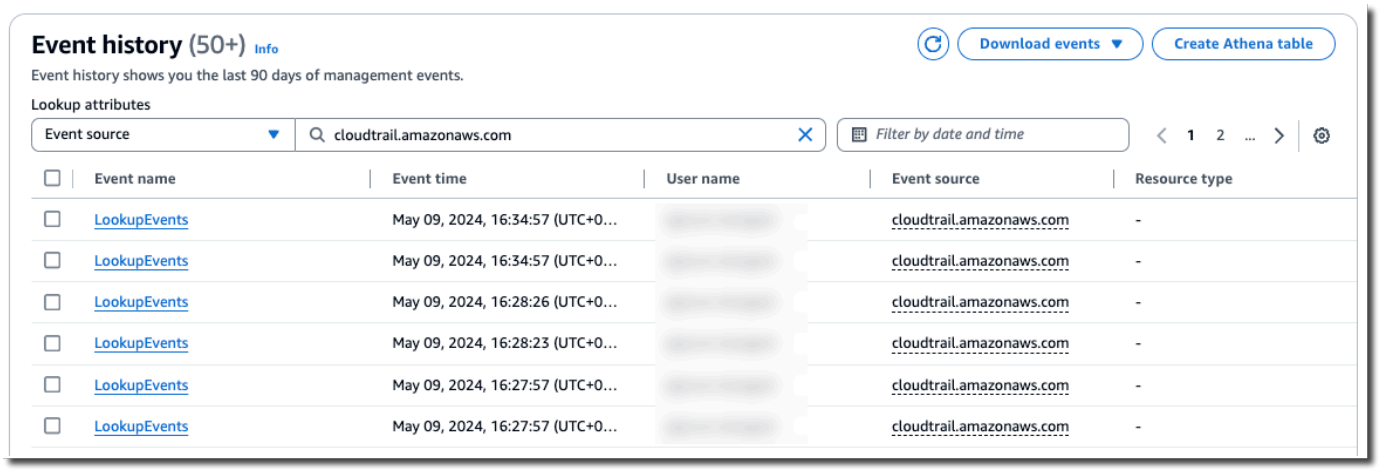
2. 在導覽窗格中，選擇 Event history (事件歷史記錄)。您可以看到已篩選的事件清單，並最先顯示最近的事件。事件的預設篩選條件為唯讀，並設為 false。您可以選擇過濾器右側的 X 來清除該篩選條件。您可以篩選單一屬性上的事件，以搜尋事件歷史記錄中的事件



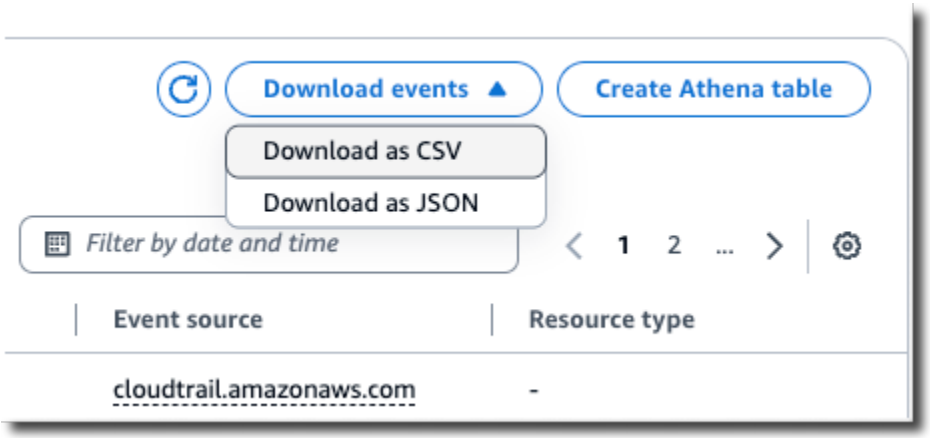

3. 選擇要篩選的屬性，然後輸入屬性的完整值。CloudTrail 無法篩選部分值。例如，若要檢視所有主控台登入事件，請選擇事件名稱篩選條件，並為屬性值指定 ConsoleLogin。




或者，若要檢視最近的 CloudTrail 管理事件，請選擇事件來源，並指定 `cloudtrail.amazonaws.com`。如需有關服務記錄到 CloudTrail 的事件資訊，請參閱服務的 API 參考。



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中side-by-side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。

## 建立追蹤以記錄管理事件

對於您的第一個線索，我們建議您建立線索，以記錄所有管理事件，且不記錄任何資料事件或 Insights 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。您將建立用於儲存追蹤日誌檔案的 Amazon S3 儲存貯體，以做為在 CloudTrail 主控台中建立追蹤的一部分。

> **Note**
>
> AWS Control Tower 當您設定登陸區域時， 會設定新的 CloudTrail 追蹤記錄管理事件。這是組織層級追蹤，這表示它會記錄管理帳戶和組織中所有成員帳戶的所有管理事件。如需詳細資訊，請參閱AWS CloudTrail 《 使用者指南》中的關於登入 AWS Control Tower。
> 此教學課程將假設您正在建立第一個追蹤。根據您 AWS 帳戶中的線索數量，以及這些線索的設定方式，下列程序可能會產生費用，也可能不會產生費用。CloudTrail 會將日誌檔案儲存在 Amazon S3 儲存貯體中，因此會產生成本。如需定價的詳細資訊，請參閱 AWS CloudTrail 定價和 Amazon S3 定價。

建立追蹤記錄

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
2. 在區域選擇器中，選擇您要建立追蹤 AWS 的區域。這是該追蹤的主要區域。

   > **Note**
   >
   > 主要區域是唯一您可以在建立追蹤之後更新追蹤 AWS 區域 的地方。

3. 在 CloudTrail 服務首頁上，Trails (追蹤) 頁面，或 Dashboard (儀表板) 頁面的 Trails (追蹤) 區段上，選擇Create trail (建立追蹤)。
4. 在線索名稱中，為您的線索命名，例如 *`management-events`*。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。當您建立儲存貯體時，CloudTrail 會建立和套用所需的儲存貯體政策。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`動作的許可，因為預設會為儲存貯體啟用伺服器端加密。為您的儲存貯體命名，以方便識別。

   若要更容易地找到您的記錄，請在現有的儲存貯體中建立新的資料夾 (也稱為prefix ) 來存儲您的 CloudTrail 日誌。

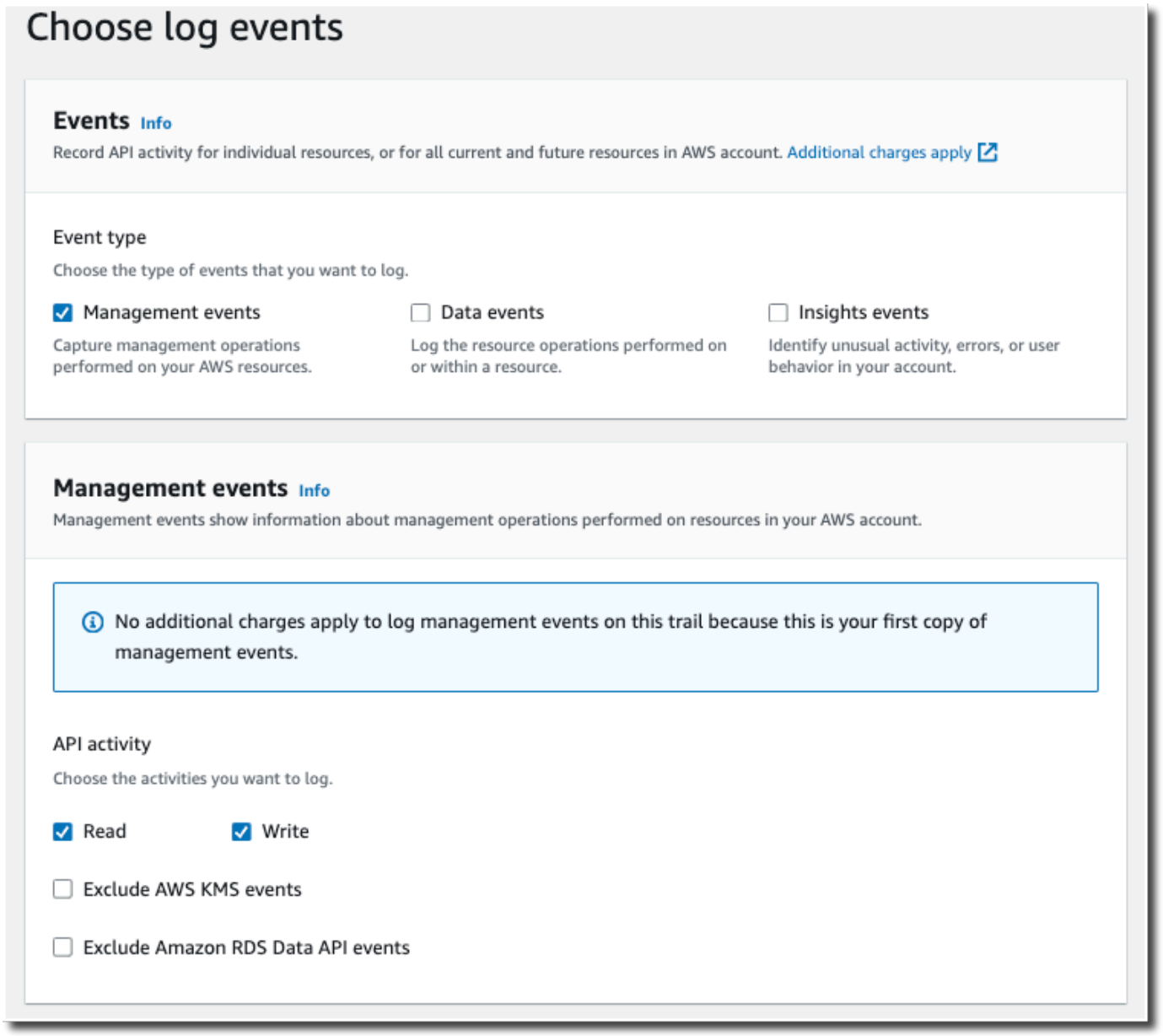
   > **Note**
   >
   > 您 Amazon S3 儲存貯體的名稱在全域中都必須是唯一的。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的儲存貯體命名規則。

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。如需此設定的詳細資訊，請參閱搭配使用伺服器端加密與 Amazon S3 受管金鑰 (SSE-S3)。
8. 保留其他設定的預設設定。
9. 保留 CloudWatch Logs 的預設設定。目前，請勿將日誌傳送到 Amazon CloudWatch Logs。
10. （選用 ） 在標籤中，您最多可以新增 50 個標籤金鑰對，以協助您識別、排序和控制對線索的存取。標籤可協助您辨識 CloudTrail 追蹤和其他資源，像是包含 CloudTrail 日誌檔案的 Amazon S3 儲存貯體。例如，您可以附加名稱為 **`Compliance`**，值為 **`Auditing`** 的標籤。

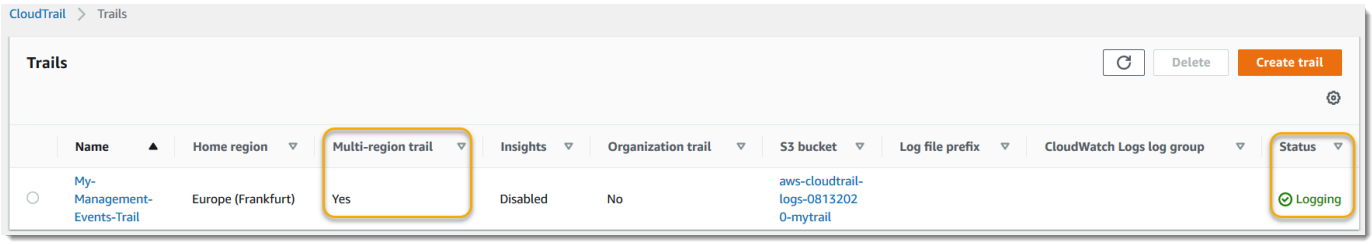
> **Note**
>
> 雖然當透過 CloudTrail 主控台建立追蹤時，您可以將標籤加入其中，而且您可以建立 Amazon S3 儲存貯體來儲存 CloudTrail 主控台的日誌檔案，不過，您無法透過 CloudTrail 主控台將標籤加入 Amazon S3 儲存貯體。如需檢視和變更 Amazon S3 儲存貯體屬性 (包括將標籤新增至儲存貯體) 的詳細資訊，請參閱《Amazon S3 使用者指南》。

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 Data 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、 Insights 事件和網路活動事件的預設設定。此線索不會記錄任何資料事件、Insights 事件或網路活動事件。選擇下一步。
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。




如需追蹤的詳細資訊，請參閱 使用 CloudTrail 追蹤。

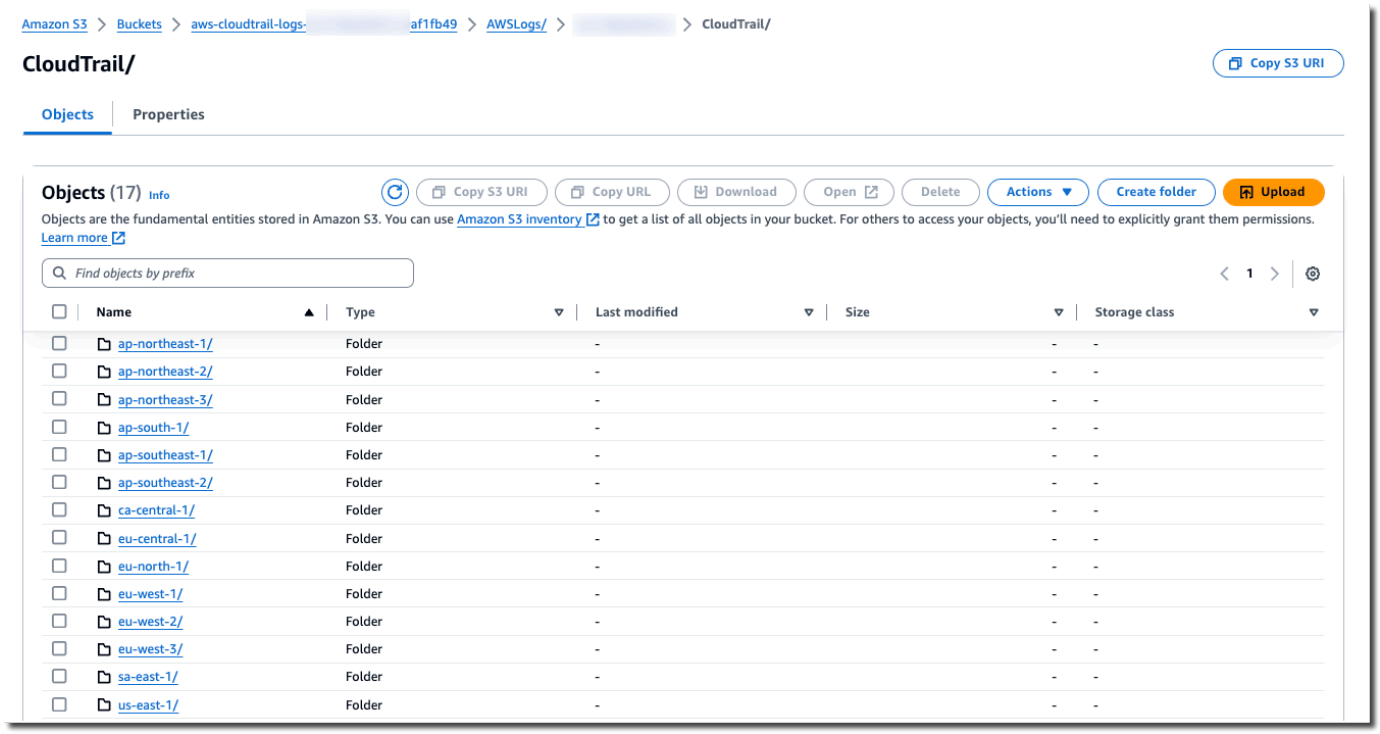
## 檢視您的日誌檔案

在您建立第一個追蹤的平均約 5 分鐘內，CloudTrail 即會為您的追蹤提供第一組日誌檔案到 Amazon S3 儲存貯體。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 呼叫的平均約 5 分鐘內傳遞日誌。此時間無法保證。如需詳細資訊，請參閱 AWS CloudTrail 服務水準協議。
> 如果您的追蹤設定錯誤 (例如，S3 儲存貯體無法連線)，CloudTrail 會在 30 天內嘗試重新傳遞日誌檔案到您的 S3 儲存貯體，且您需要為這些嘗試傳遞事件支付標準 CloudTrail 費用。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. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
2. 在導覽窗格中，選擇 Trails (追蹤記錄)。在線索頁面上，尋找您剛建立的線索名稱 （ 在範例中為 *management-events*)。
3. 在線索的 列中，選擇 S3 儲存貯體的值。
4. Amazon S3 主控台會開啟，並顯示儲存貯體的兩個資料夾： `CloudTrail-Digest`和 `CloudTrail`。選擇 CloudTrail 資料夾以檢視日誌檔案。
5. 如果您建立了多區域線索，則每個線索都有一個資料夾 AWS 區域。選擇 AWS 區域 您要檢閱日誌檔案之 的資料夾。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。




6. 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。檔案的名稱以您的 AWS 帳戶 ID 開頭，並以副檔名 結尾.gz。例如，如果您的帳戶 ID 為 *123456789012*，您會看到具有類似名稱的檔案：*123456789012*_CloudTrail_*us-east-2_20240512T0000Z_EXAMPLE*.json.gz。

   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。我們建議您使用 JSON 檢視器，因為它可讓您更輕鬆地剖析 CloudTrail 日誌檔案中的資訊。

# 建立 S3 資料事件的事件資料存放區

您可以建立一個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 組態項目或非AWS 事件。

當您為資料事件建立事件資料存放區時，您可以選擇要記錄資料事件的 AWS 服務 和資源類型。如需 AWS 服務 該日誌資料事件的資訊，請參閱 資料事件。

此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。

若要為 S3 資料事件建立事件資料存放區

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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，請在一般詳細資訊中為您的事件資料存放區提供一個名稱，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。如需有關 CloudTrail 命名要求的資訊，請參閱 CloudTrail 資源、S3 儲存貯體和 KMS 金鑰的命名需求。
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 Lake 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。在 366 天之後，延長保留將依用量計費定價。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 會透過檢查事件的 `eventTime` 是否在指定保留期以內，決定是否要保留該事件。例如，如果您指定的保留期為 90 天，CloudTrail 將移除 `eventTime` 早於 90 天的事件。
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。根據預設，事件資料存放區中的所有事件都會由 CloudTrail 使用 AWS 擁有和管理的 KMS 金鑰來加密。

   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。選擇新增以為您 AWS KMS key 建立 ，或選擇現有以使用現有的 KMS 金鑰。在 Enter KMS alias (輸入 KMS 別名) 中，指定別名，格式為 `alias/`*`MyAliasName`*。使用您自己的 KMS 金鑰時，您必須編輯您的 KMS 金鑰政策，以允許對 CloudTrail 日誌進行加密和解密。如需詳細資訊，請參閱設定

CloudTrail 的 AWS KMS 金鑰政策。CloudTrail 也支援 AWS KMS 多區域金鑰。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 AWS KMS 的成本。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**
>
> 若要啟用組織事件資料存放區的 AWS Key Management Service 加密，您必須使用管理帳戶的現有 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 Data Catalog 中的資料表中繼資料可讓 Athena 查詢引擎了解如何尋找、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 會自動建立具有必要許可的角色。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）選擇啟用資源政策，將資源型政策新增至您的事件資料存放區。以資源為基礎的政策可讓您控制哪些主體可以在事件資料存放區上執行動作。例如，您可以新增資源型政策，允許其他帳戶中的根使用者查詢此事件資料存放區並檢視查詢結果。如需範例政策，請參閱 事件資料存放區的資源型政策範例。

   以資源為基礎的政策包含一或多個陳述式。政策中的每個陳述式都會定義允許或拒絕存取事件資料存放區的委託人，以及委託人可以對事件資料存放區資源執行的動作。

   事件資料存放區的資源型政策支援下列動作：

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`

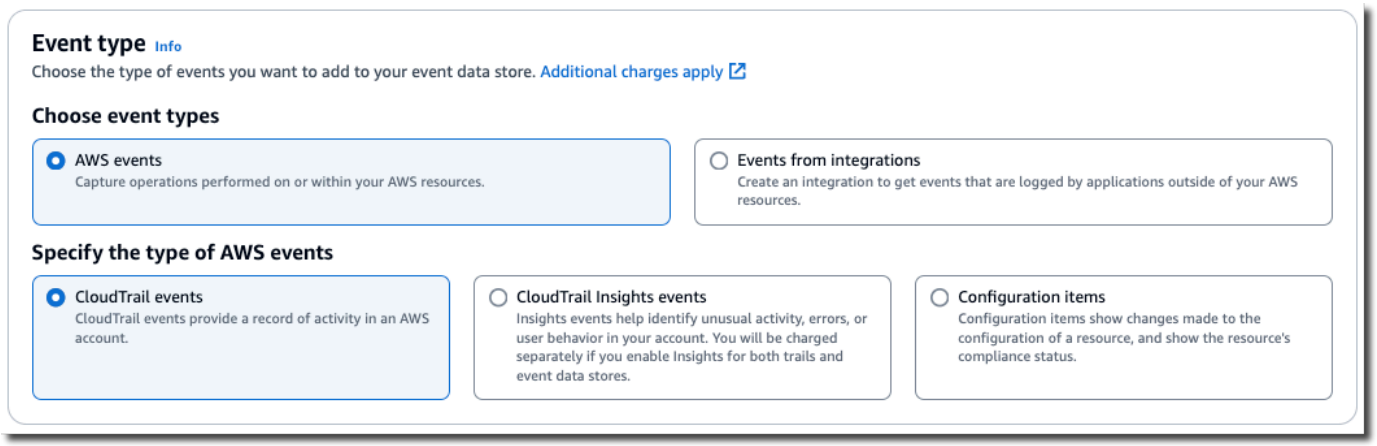
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

對於組織事件資料存放區，CloudTrail 會建立預設資源型政策，列出允許委派管理員帳戶在組織事件資料存放區上執行的動作。此政策中的許可衍生自 中的委派管理員許可 AWS Organizations。此政策會在組織事件資料存放區或組織變更後自動更新 （ 例如，CloudTrail 委派管理員帳戶已註冊或移除 ）。

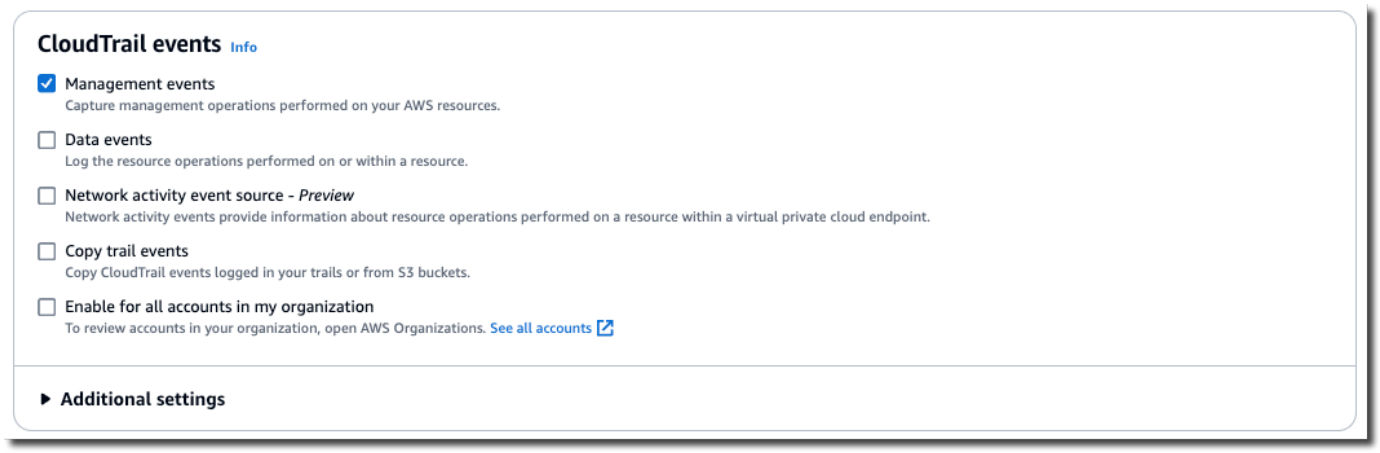
10. (選用) 在標籤中，新增一或多個自訂標籤 (鍵值組) 至您的事件資料存放區。標籤可協助您識別 CloudTrail 事件資料存放區。例如，您可以附加名稱為 **`stage`**，值為 **`prod`** 的標籤。您可以使用標籤來限制對事件資料存放區的存取。您還可以使用標籤來追蹤事件資料存放區的查詢和擷取成本。

    如需有關如何使用標籤追蹤成本的資訊，請參閱 為 CloudTrail Lake 事件資料存放區建立使用者定義的成本分配標籤。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。如需有關如何在 中使用標籤的資訊 AWS，請參閱《標記 AWS 資源使用者指南》中的標記您的 AWS 資源。

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




13. 對於 CloudTrail 事件，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。

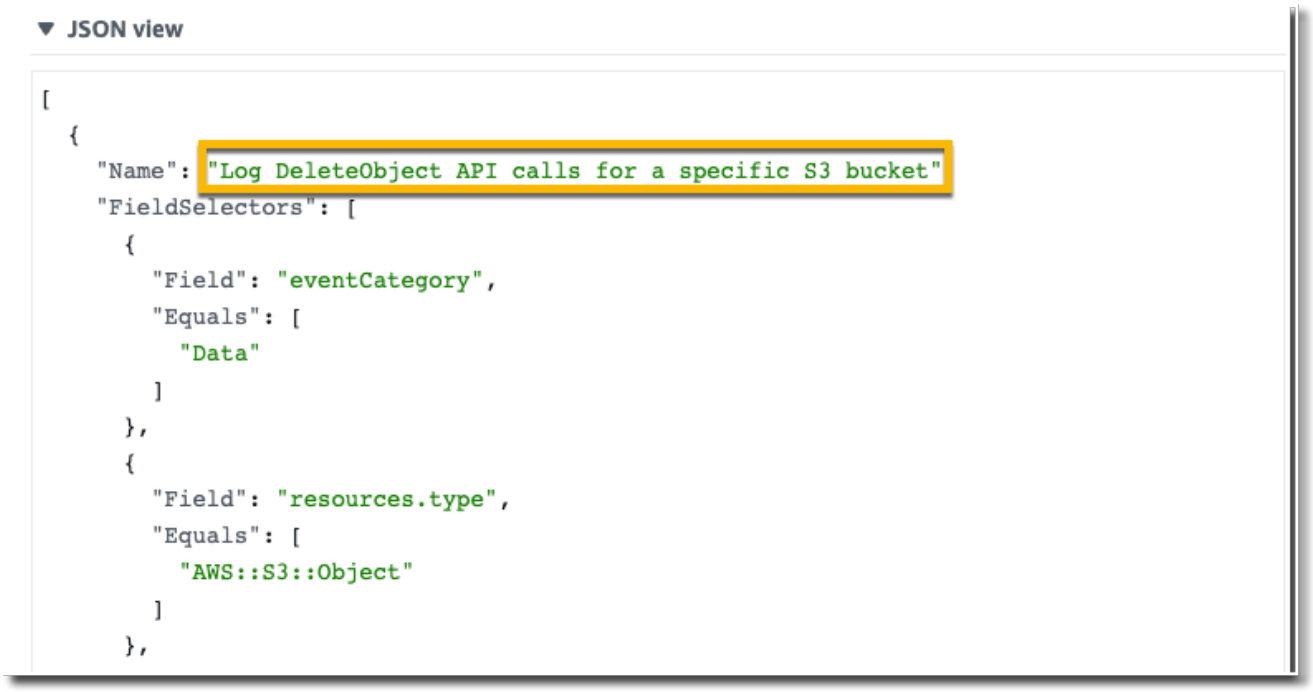



14. 保留複製追蹤事件的預設設定。您可以使用此選項，將現有追蹤事件複製到您的事件資料存放區。如需詳細資訊，請參閱將追蹤事件複製到事件資料存放區。
15. 如果這是組織事件資料存放區，選擇針對組織中的所有帳戶啟用。除非您已在 AWS Organizations 中設定帳戶，否則此選項將無法變更。
16. 對於其他設定，保留預設選項。根據預設，事件資料存放區會收集所有 的事件， AWS 區域 並在建立事件時開始擷取事件。
17. 對於資料事件，請執行下列選擇：

    a. 在資源類型中，選擇 S3。資源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。如需有關這些欄位的資訊，請參閱《AWS CloudTrail API 參考》中的 AdvancedFieldSelector。

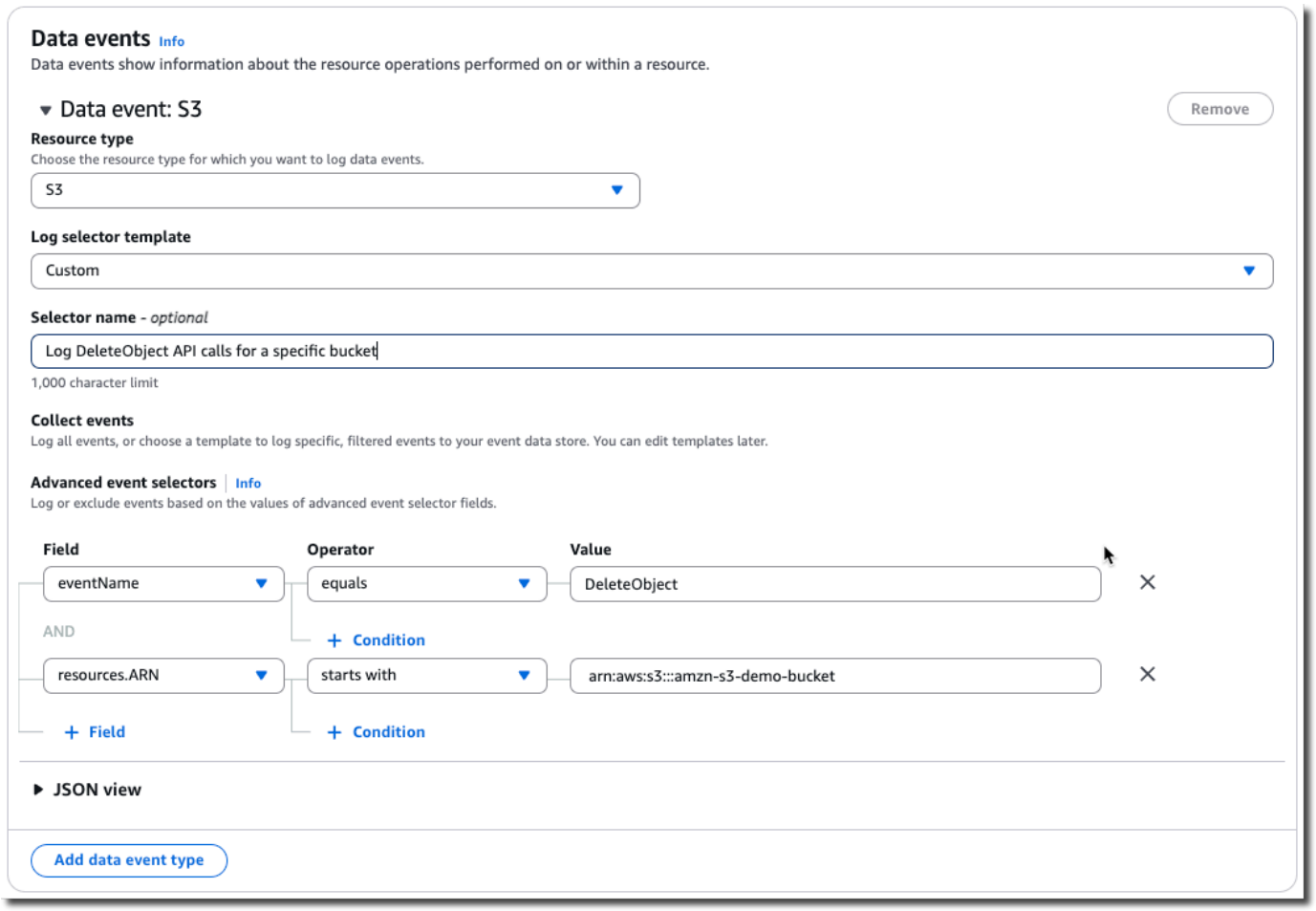
    c. (選用) 在選取器名稱中，輸入用於識別選取器的名稱。選取器名稱是進階事件選擇器的描述性名稱，例如「記錄特定 S3 儲存貯體的 DeleteObject API 呼叫」。選取器名稱會被作為 `Name` 列在進階事件選取器中，您在展開 JSON 檢視時可檢視該名稱。




d. 在進階事件選取器中，我們會建置自訂事件選取器，以篩選 `eventName`和 `resources.ARN` 欄位。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。針對值，輸入儲存貯體的 ARN（例如 arn：aws：s3：：*`amzn-s3-demo-bucket`*)。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。




18. 選擇 Next (下一步) 以檢閱您的選項。
19. 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)。
20. 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 使用 CloudTrail 主控台檢視範例查詢。

如需有關 CloudTrail Lake 的詳細資訊，請參閱 使用 AWS CloudTrail Lake。

# 使用 檢視您的 CloudTrail 成本和用量 AWS Cost Explorer

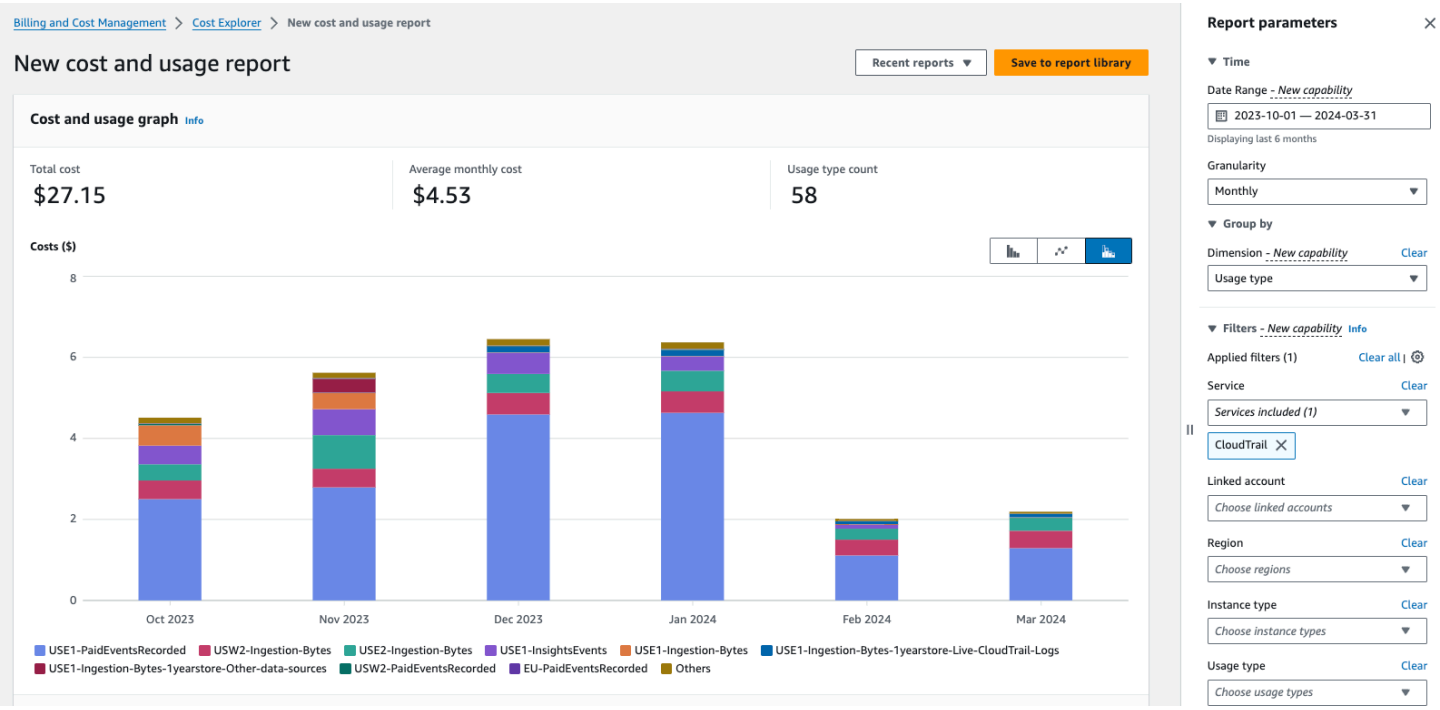
本節說明如何使用 檢視 CloudTrail 成本和用量AWS Cost Explorer。Cost Explorer 可讓您視覺化、了解和管理一段時間內的 AWS 成本和用量。

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

使用 Cost Explorer 檢視 CloudTrail 成本和用量

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cost-management/home#/custom 的 Cost Explorer 主控台。
2. 在時間下，選擇您要分析的日期範圍。
3. 在分組依據下，針對維度，選擇用量類型。
4. 在篩選條件下，針對服務選擇 CloudTrail。

下圖顯示針對 CloudTrail 篩選並依用量類型分組的成本報告範例。




檢閱用量類型，以查看哪些 CloudTrail 功能產生了最多的成本。每個用量類型都以產生 AWS 區域 費用的 代碼開頭。

下表說明每個 CloudTrail 功能的 CloudTrail 用量類型。

| CloudTrail 功能 | 用量類型 | Description |
| --- | --- | --- |
| CloudTrail 追蹤 | *region*-FreeEventsRecorded | 第一份免費交付至的管理事件副本 AWS 區域。 |
| CloudTrail 追蹤 | *region*-PaidEventsRecorded | 交付至 之管理事件的額外副本費用 AWS 區域。 |
| CloudTrail 追蹤 | *region*-DataEventsRecorded | 將資料事件交付至 的費用 AWS 區域。資料事件一律會產生費用。 |
| CloudTrail 追蹤 | *region*-NetworkEventsRecorded | 將網路活動事件交付至 的費用 AWS 區域。網路活動事件一律會產生費用。 |
| CloudTrail Lake | *region*-Ingestion-Bytes | 使用七年保留定價選項將事件擷取至 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，且所有事件類型都相同。 |
| CloudTrail Lake | *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、網路活動事件和管理事件擷取至 CloudTrail Lake 事 |

| CloudTrail 功能 | 用量類型 | Description |
| --- | --- | --- |
| | | 件資料存放區的費用。 |
| CloudTrail Lake | *region*-Ingestion-Bytes-1yearstore-Other-data-sources | 使用一年可延長保留定價選項，將其他事件來源擷取至 CloudTrail Lake 事件資料存放區的費用。這包括 CloudTrail Insights 事件、來自 的組態項目 AWS Config、來自 的證據 AWS Audit Manager、從 S3 匯入（未壓縮）歷史 CloudTrail 日誌，以及 外部的事件 AWS。 |
| CloudTrail Lake | *region*-QueryScanned-Bytes | 執行 CloudTrail Lake 查詢的費用。當您在 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 功能 | 用量類型 | Description |
| --- | --- | --- |
| CloudTrail Insights | *region*-InsightsEvents | CloudTrail Insights 事件的費用。對於 Insights 事件，根據每個 Insight 類型分析的管理事件數量，會產生費用。如需詳細資訊，請參閱Insights 事件的成本。 |

# 使用 AWS Budgets 來管理成本

AWS Budgets 的功能可讓您設定自訂預算 AWS 帳單與成本管理，在成本或用量超過 （或預測超過） 預算金額時提醒您。

使用 為 CloudTrail 建立預算 AWS Budgets 是建議的最佳實務，可協助您追蹤 CloudTrail 支出。成本型預算有助於了解 CloudTrail 的使用可能會向您收取多少費用。預算提醒會在帳單達到您定義的閾值時通知您。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。

> **Note**
>
> 雖然您可以將標籤套用至 CloudTrail 追蹤，但 AWS Billing 目前無法使用套用至追蹤的標籤進行成本分配。Cost Explorer 可以顯示 CloudTrail Lake 事件資料存放區的成本，以及 CloudTrail 服務的總體成本。

若要開始使用 AWS Budgets，請開啟 AWS 帳單與成本管理，然後在左側導覽列中選擇 Budgets。我們建議您在建立預算時設定預算提醒，以追蹤 CloudTrail 花費。如需如何使用 AWS Budgets 的詳細資訊，請參閱使用 管理成本 AWS Budgets和 的最佳實務 AWS Budgets。

## 為 CloudTrail Lake 事件資料存放區建立使用者定義的成本分配標籤

您可以建立使用者定義的成本分配標籤，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。啟用成本分配標籤之後，AWS 會使用標籤來整理成本分配報告中的資源成本。

- 若要在主控台中建立標籤，請參閱「若要為 CloudTrail 事件建立事件資料存放區」程序中的步驟 9。
- 若要使用 CloudTrail API 來建立標籤，請參閱《AWS CloudTrail API 參考》中的 CreateEventDataStore 和 AddTags。
- 若要使用 建立標籤 AWS CLI，請參閱《 AWS CLI 命令參考》中的 create-event-data-store 和 add-tags。

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。

# 管理 CloudTrail 追蹤成本

您可以透過擷取所需資料的方式設定和管理 CloudTrail 追蹤，同時保持成本效益。如需 CloudTrail 定價的詳細資訊，請參閱 AWS CloudTrail 定價。

## 追蹤組態

CloudTrail 提供如何設定帳戶內追蹤的彈性。您在設定流程中所做的某些決策，需要您了解對於 CloudTrail 帳單的影響。以下是追蹤組態如何影響您 CloudTrail 帳單的範例。

建立多重追蹤

每個區域內管理事件的第一個副本是免費的。例如，如果您的帳戶有 2 個單一區域追蹤、 中的追蹤us-east-1和 中的另一個追蹤us-west-2，則無需支付 CloudTrail 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。

如果您建立更多將相同的事件傳遞至其他目的地的追蹤，這些後續交付會產生 CloudTrail 費用。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。若是資料事件，所有交付都會產生 CloudTrail 費用，包括第一次交付。

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 CloudTrail 中發生大量 AWS KMS 管理事件。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線索的事件數量，您可以在建立線索 AWS KMS 或更新線索頁面上選擇排除 AWS KMS 事件或排除 Amazon RDS Data API 事件，以篩選掉 或 Amazon RDS Data 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來包含或排除資料事件，讓您僅記錄感興趣的資料事件。如需詳細資訊，請參閱使用進階事件選取器篩選資料事件。

您可以使用進階事件選取器，根據 `eventName`、`resources.type`、`errorCode`、`resources.ARN` 和 `vpcEndpointId` 欄位來包含或排除網路活動事件，讓您僅記錄感興趣的資料事件。如需詳細資訊，請參閱記錄網路活動事件。

如需建立或更新追蹤的詳細資訊，請參閱本指南中的 使用 CloudTrail 主控台建立追蹤 或 使用 CloudTrail 主控台更新線索。

AWS Organizations

使用 CloudTrail 設定 Organizations 追蹤時，CloudTrail 會將追蹤複寫至組織內的各成員帳戶。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
- 使用 管理您的成本 AWS Budgets
- Cost Explorer 入門
- 準備建立組織追蹤

# 管理 CloudTrail Lake 成本

AWS CloudTrail Lake 事件資料存放區和查詢會產生費用。您可以採用擷取所需資料的方式設定事件資料存放區，同時保持成本效益。如需有關 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
- 了解 CloudTrail Lake 費用
- 有關如何降低成本的建議
- 另請參閱


## 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) | Description |
| --- | --- | --- |
| 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。<br><br>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。在 366 天之後，延長保留將依用量計費定價。<br><br>此為預設選項。<br><br>預設保留期：366 天<br><br>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。<br><br>保留已包含在擷取定價中，無須額外付費。 |

| 定價選項 (主控台) | BillingMode (API) | Description |
| --- | --- | --- |
| | | 預設保留期：2,557 天<br><br>最長保留期：2,557 天 |

## 了解 CloudTrail Lake 費用

下表提供有關 CloudTrail Lake 事件資料存放區和查詢如何產生費用的資訊。如需有關 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) | 如果使用 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：<br><br>• 一年可延長保留定價：根據事件類型提供擷取定價。<br>• 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。<br><br>複製追蹤事件<br><br>當您複製追蹤事件到 CloudTrail Lake 時，CloudTrail 會解壓縮以 gzip (已壓縮) 格式存放的日誌。CloudTrail 會將日誌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。<br><br>**Note**<br>如果事件的事件時間超過指定的保留期，則 CloudTrail 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：<br>保留期 = *oldest-event-in-days* + *number-days-to-retain* |

| 收費類型 | 如何產生費用 |
| --- | --- |
| | 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 Lake 會將分列式 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。<br><br>事件資料存放區的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。CloudTrail Lake 會檢查事件的事件時間是否在指定的保留期內，從而決定是否要保留該事件。舉例來說，如果您指定的保留期為 90 天，則 CloudTrail 會在事件時間超過 90 天時移除事件。<br><br>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。<br><br>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。在 366 天之後，儲存將以依用量計費定價提供，並根據事件資料存放區中的最佳化和壓縮資料收費。 |
| 在 CloudTrail Lake 中執行查詢 (最佳化和壓縮的資料) | 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，我們通常會建議此選項 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、AWS CLI 或 UpdateEventDataStore API 操作來變更定價選項。

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 管理事件、資料事件或網路活動事件設定事件資料存放區時，您可以使用進階事件選取器來篩選掉不感興趣的事件。

您可以在下列進階事件選取器欄位上篩選管理事件：`eventName`、`eventSource`、`eventTypereadOnly`、`sessionCredentialFromConsole`、和 `userIdentity.arn`。

您可以在下列進階事件選取器欄位上篩選資料事件：`eventName`、`eventSource`、`eventTyperesources.type`、`resources.ARN`、`readOnly`、`sessionCredentialFromConsole`和 `userIdentity.arn`。如需詳細資訊，請參閱使用進階事件選取器篩選資料事件。

您可以在下列進階事件選取器欄位上篩選網路活動事件：`eventName`、 `errorCode`和 `vpcEndpointId`。如需詳細資訊，請參閱記錄網路活動事件。

在複製追蹤事件時選擇較短的時間範圍

在將追蹤事件複製到 CloudTrail Lake 時，縮小從開始事件到結束事件的指定時間範圍以減少資料擷取量。

如果您複製追蹤事件到 CloudTrail Lake 以執行歷史分析，而且您不想擷取未來事件，則可以取消選取擷取事件的選項，因此擷取任何額外事件將不會產生費用。

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。

## 另請參閱

- AWS CloudTrail 定價
- 支援的 CloudWatch 指標
- 使用 管理您的成本 AWS Budgets
- Cost Explorer 入門

# 使用 CloudTrail 事件歷史記錄

根據預設， AWS 您的帳戶會啟用 CloudTrail，而且您會自動存取 CloudTrail 事件歷史記錄。事件歷史記錄提供過去 90 天的管理事件的可檢視、可搜尋、可下載和不可變記錄 AWS 區域。這些事件會擷取透過 AWS 管理主控台 AWS Command Line Interface、 和 AWS SDKs和 APIs進行的活動。事件歷史記錄會在事件發生 AWS 區域 的 中記錄事件。檢視事件歷史記錄無需支付 CloudTrail 費用。

您可以檢視事件歷史記錄頁面，在 CloudTrail 主控台上 AWS 帳戶 依區域查詢與建立、修改或刪除 中資源（例如 IAM 使用者或 Amazon EC2 執行個體）相關的事件。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 主控台上的事件歷史記錄頁面來檢視、搜尋、下載、封存、分析和回應整個 AWS 基礎設施的帳戶活動。您可以透過選取每個頁面上要顯示的事件數量，以及要顯示或隱藏的資料欄，在主控台上自訂事件歷史記錄頁面的檢視。 您也可以side-by-side比較事件歷史記錄中的事件詳細資訊。您可以使用 AWS SDKs或 以程式設計方式查詢事件 AWS Command Line Interface。

> **Note**
>
> 隨著時間的推移， AWS 服務 可能會新增其他事件。CloudTrail 會在事件歷史記錄中記錄這些事件，但包含新增事件的完整 90 天活動記錄在新增事件後 90 天內無法使用。
> 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 主控台和 查詢最近的管理事件 AWS CLI，以及如何下載事件檔案。如需有關使用 `LookupEvents` API 從 CloudTrail 事件擷取資訊的資訊，請參閱《AWS CloudTrail API 參考》中的 LookupEvents。

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
- 使用 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 主控台上的事件歷史記錄頁面只會顯示管理事件。它不會顯示資料事件、 Insights 事件或網路活動事件。
- 事件歷史記錄僅限於過去 90 天的事件。若要持續記錄 中的事件 AWS 帳戶，請建立事件資料存放區或追蹤。
- 當您從 CloudTrail 主控台的事件歷史記錄頁面下載事件時，您可以在單一檔案中下載最多 200，000 個事件。如果您達到 200，000 個事件限制，CloudTrail 主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。
- 事件歷史記錄搜尋僅限於單一 AWS 帳戶，只會傳回來自單一的事件 AWS 區域，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 事件資料存放區，以跨多個屬性和 進行查詢 AWS 區域。您也可以在 AWS Organizations 組織中跨多個 AWS 帳戶 進行查詢。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、 Insights 事件、 AWS Config 組態項目、Audit Manager 證據和非AWS 事件。CloudTrail Lake 查詢在事件歷史記錄頁面上或透過執行 ，提供比簡單索引鍵和值查詢更深入且更可自訂的事件檢視LookupEvents。如需詳細資訊，請參閱使用 AWS CloudTrail Lake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 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 主控台的事件歷史記錄頁面檢視過去 90 天在 AWS 區域中發生的管理事件。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。您可以透過選取每個頁面上要顯示的事件數量，然後選擇要在主控台上顯示的資料欄，來自訂事件歷史記錄的檢視。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。您也可以並排比較Event history (事件歷史記錄) 中的事件詳細資訊。

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，事件將不再顯示在事件歷史記錄中。您無法從事件歷史記錄手動刪除事件。

您可以透過諮詢特定服務的文件，來進一步了解 CloudTrail 如何記錄該服務的事件之詳細資訊。如需詳細資訊，請參閱AWS CloudTrail 的服務主題。

> **Note**
>
> 若要持續記錄超過 90 天的活動和事件，請建立事件資料存放區或追蹤。

若要檢視事件歷史記錄

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
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. 您可以在單一屬性上篩選事件，您可以從下拉式清單中選擇。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條件，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條件，並指定 `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中side-by-side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
- 自訂顯示
- 篩選 CloudTrail 事件
- 檢視事件的詳細資訊
- 下載事件
- 檢視使用 參考的資源 AWS Config

## 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 主控台上自訂事件歷史記錄的檢視。

- 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. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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

用來簽署請求的 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 ID。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

提出請求 AWS 的服務，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，資源名稱可能是「auto-scaling-test-group」(用於 Auto Scaling 群組) 或「i-12345678910」(用於 EC2 執行個體)。

Resource Type (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 服務的資源類型各不相同。

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。您可以在單一檔案中下載最多 200，000 個事件。如果您達到 200，000 個事件限制，CloudTrail 主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 事件歷史記錄檔案屬資料檔案，內含個別使用者可設定的資訊 (如資源名稱)。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，將 CloudTrail 事件匯出至 CSV 並匯入至試算表程式時，該程式可能會提醒您關於安全方面的考量。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。

## 檢視使用 參考的資源 AWS Config

AWS Config 會記錄 資源 AWS 的組態詳細資訊、關係和變更。

在資源參考窗格中，選擇AWS Config 資源時間軸欄

中

的 ，

以在 AWS Config 主控台中檢視資源。

如

果

圖

示為灰色、 AWS Config 未開啟，或未記錄資源類型。選擇圖示前往 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 最近新增對資源類型的支援，但尚無法從 CloudTrail 主控台取得。您可以在 AWS Config 主控台中查詢資源，以查看資源的時間軸。
- 資源由另一個資源擁有 AWS 帳戶。
- 資源由另一個 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。

若要授予使用者在 AWS Config 主控台中檢視資源的唯讀許可，請參閱 授予在 CloudTrail 主控台上檢視 AWS Config 資訊的許可。

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

# 使用 檢視最近的管理事件 AWS CLI

您可以使用 aws cloudtrail lookup-events 命令為目前的 AWS 區域 查詢過去 90 天的 CloudTrail 管理事件。aws cloudtrail lookup-events 命令會在事件發生 AWS 區域 的 中顯示事件。

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
- Resource Type (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。產生的 JSON 骨架在 版本之間不穩定，AWS CLI 而且在產生的 JSON 骨架中沒有回溯相容性保證。
- `--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。

如需使用 AWS 命令列界面的一般資訊，請參閱 AWS Command Line Interface 使用者指南。

內容


- 先決條件
- 取得命令列說明
- 查詢事件
- 指定要傳回的事件數目
- 依時間範圍查詢事件
- 依屬性查詢事件
  - 屬性查詢範例
- 指定下一頁的結果
- 從檔案取得 JSON 輸入
- 查詢輸出欄位


## 先決條件

- 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。
- 請確定您的 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 帳戶 AWS 區域，以及 AWS CLI 工作階段的預設輸出格式，請使用 aws configure命令。如需詳細資訊，請參閱設定 AWS 命令列界面。

> **Note**
>
> CloudTrail AWS CLI 命令區分大小寫。

## 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 記錄管理、資料和網路活動事件的內容。

## 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

的長度上限為 AttributeValue 2000 個字元。下列字元 ('_'、' '、','、'\\n') 計算為 2000 個字元限制的兩個字元。

### 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所指定 CloudTrail EventId 的事件。

```
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

AWS CLI 某些 AWS 服務的 有兩個參數 `--generate-cli-skeleton`和 `--cli-input-json`，可用來產生 JSON 範本，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`。如需更多詳細資訊，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
   ```

   所產生的範本檔案 (在此情況下為 LookupEvents.txt) 如下：

   ```
   {
       "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。每個項目都會包含查詢請求的資訊，以及包含以字串呈現所擷取的 CloudTrail 事件。

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

提出請求的 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。

# 使用 CloudTrail Insights

AWS CloudTrail Insights 透過持續分析 CloudTrail 管理和資料事件，協助 AWS 使用者識別和回應與 API 呼叫率和 API 錯誤率相關的異常活動。CloudTrail Insights 會分析您過去的管理和資料事件，以建立 API 呼叫率和 API 錯誤率的正常模式，也稱為基準。然後，當目前的 API 呼叫率或錯誤率偏離基準時，CloudTrail 會產生 Insights 事件。

您可以收集兩種類型的 Insights，每個都用於管理和資料事件。

管理事件洞見

- API 呼叫率 – 針對基準 API 呼叫量，測量每分鐘發生的唯寫管理 API 呼叫。若要在管理事件的 API 呼叫率上記錄 Insights 事件，追蹤或事件資料存放區必須啟用 Insights 和日誌`write`管理事件。
- API 錯誤率 – 導致錯誤碼的管理 API 呼叫的測量。如果 API 呼叫失敗，則顯示錯誤。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啟用 Insights 和日誌`read`或`write`管理事件，或同時啟用 `read` `write`和管理事件。

資料事件洞見

- API 呼叫率 – 針對基準 API 呼叫量，測量每分鐘發生的資料 API 呼叫。若要在 API 呼叫率上記錄 Insights 事件，追蹤必須啟用 Insights 和記錄資料事件。
- API 錯誤率 – 測量導致錯誤碼的資料 API 呼叫。如果 API 呼叫失敗，則顯示錯誤。若要在 API 錯誤率上記錄 Insights 事件，線索必須啟用 Insights 和日誌`read`或`write`資料事件，或同時啟用 `read`和 `write` 資料事件。

> **Note**
>
> 資料事件的 Insights 事件僅支援追蹤，不支援事件資料存放區。

CloudTrail Insights 會分析每個區域中發生的管理和資料事件，並在偵測到異常活動偏離基準時產生 Insights 事件。CloudTrail Insights 事件會在與其支援管理或資料事件產生的相同區域中產生。

Insights 事件會產生額外費用。如果您同時為線索和事件資料存放區以及資料事件 Insights 啟用管理事件 Insights，則會另外向您收取費用。如需詳細資訊，請參閱AWS CloudTrail 定價。

主題

- Insights 事件的成本
- Insights 事件的交付
- 使用 CloudTrail 主控台記錄 Insights 事件
- 使用 記錄 Insights 事件 AWS CLI
- 檢視追蹤的 Insights 事件
- 檢視事件資料存放區的 Insights 事件


# Insights 事件的成本

> **Note**
>
> 資料事件的 Insights 事件僅支援追蹤。

當您在現有的線索或事件資料存放區上啟用 Insights 事件時，CloudTrail 會分析過去 28 天的管理和由線索或事件資料存放區收集的資料事件，以建立正常活動的基準。建立初始基準之後，基準會在資料過去 28 天內每天重新計算。基準分析不收取 CloudTrail 費用。

在基準分析之後，您會針對 CloudTrail 分析的任何未來管理和資料事件產生 CloudTrail 費用。根據針對已啟用的 Insights 類型分析的管理和資料事件數量，會產生費用。

如果您選擇為記錄和管理事件的線索或事件資料存放區記錄 API 呼叫率`read`和 API 錯誤率 Insights 類型，則分析的事件`write`總數將大於記錄的管理事件總數。這是因為 CloudTrail 會分析唯寫管理事件兩次，一次用於計算 API 呼叫率，另一次用於判斷 API 錯誤率。唯讀管理事件將分析一次，以計算 API 錯誤率。

同樣地，如果您選擇為記錄和資料事件的線索記錄 API 呼叫率`read`和 API 錯誤率 Insights 類型`write`，則分析的事件總數將大於記錄的資料事件總數。這是因為 CloudTrail 會分析所有資料事件兩次，一次用於計算 API 呼叫率，另一次用於判斷 API 錯誤率。

您可以分別尋找 和 `InsightsEventsDataInsightsEvents`用量類型，以識別 帳單上 Insights 的管理和資料事件費用。如需詳細資訊，請參閱使用 檢視您的 CloudTrail 成本和用量 AWS Cost Explorer。

您將針對線索和事件資料存放區產生個別的 Insights 費用，以及針對線索產生個別的資料事件 Insights。如需定價的詳細資訊，請參閱AWS CloudTrail 定價。

範例 1：針對追蹤的 API 呼叫率和 API 錯誤率啟用管理事件的洞見

在此第一個範例中，您會在線索記錄管理事件上啟用 Insights，並選擇收集這兩種 Insights 類型。此範例中的線索同時記錄 readwrite和管理事件。

- CloudTrail 會分析過去 28 天內記錄的管理事件，以形成基準。分析無需支付 CloudTrail 費用。
- 建立基準後，線索會記錄 300，000 個管理事件，其中 270，000 個是read管理事件，30，000 個是write管理事件。
  - write 管理事件會分析兩次，一次用於 API 呼叫率，一次用於 API 錯誤率 (30，000 * 2=60，000)。
  - read 管理事件會針對 API 錯誤率 (270，000 *1=270，000) 分析一次。
  - 分析的總管理事件為 330，000 (60，000 + 270，000)。分析此線索的 330，000 個管理事件會產生成本。如果您為其他線索或事件資料存放區啟用 Insights，則會另外收費。

範例 2 – 啟用兩個線索管理事件的洞見

在此下一個範例中，您會在兩個線索記錄管理事件上啟用 Insights，即線索 A 和線索 B。您可以選擇僅在線索 A 上啟用 API 呼叫率 Insights，並在線索 B 上啟用 API 錯誤率 Insights。兩個線索都記錄readwrite和管理事件。

- CloudTrail 會分析過去 28 天內記錄的write管理事件，以形成基準。分析無需支付 CloudTrail 費用。
- 建立基準後，線索會記錄 800，000 個管理事件，其中 710，000 個是read事件，90，000 個是write事件。

  對於線索 A，會發生下列分析：
  - write 管理事件會針對 API 呼叫率 (90，000 * 1=90，000) 分析一次。
  - 不會分析read管理事件，因為 CloudTrail 只會分析 API 呼叫率 Insights 的write管理事件。
  - 分析的總管理事件為 90，000。分析線索 A 的 90，000 個管理事件會產生成本。

  對於線索 B，會發生下列分析：
  - write 管理事件會針對 API 錯誤率 (90，000 * 1=90，000) 分析一次。
  - read 管理事件會針對 API 錯誤率 (710，000 *1=710，000) 分析一次。
  - 分析的總管理事件為 800，000 (90，000 + 710，000)。分析線索 B 的 800，000 個管理事件會產生成本。

範例 3：針對追蹤和事件資料存放區上的 API 呼叫率和 API 錯誤率啟用管理事件的洞見

在此範例中，您會在線索和事件資料存放區記錄管理事件上啟用 Insights for API 呼叫率和 API 錯誤率。追蹤和事件資料存放區都是記錄readwrite和管理事件。當您在兩者上啟用 Insights 時，會針對追蹤和事件資料存放區分別產生 CloudTrail Insights 的費用。

- CloudTrail 會分析過去 28 天內記錄的管理事件，以形成基準。分析無需支付 CloudTrail 費用。
- 建立基準後，追蹤和事件資料存放區日誌 500，000 個管理事件，其中 380，000 個是read管理事件，120，000 個是write管理事件。

  對於線索，會發生下列分析：

  - write 管理事件會針對線索分析兩次，一次針對 API 呼叫率，一次針對 API 錯誤率 (120，000 * 2=240，000)。
  - read 管理事件會針對 API 錯誤率 (380，000 *1=380，000) 的線索分析一次。
  - 針對追蹤分析的總管理事件為 620，000 (240，000 + 380，000)。分析線索的 620，000 個管理事件會產生成本。

  對於事件資料存放區，會發生下列分析：

  - write 管理事件會針對事件資料存放區分析兩次，一次針對 API 呼叫率，一次針對 API 錯誤率 (120，000 * 2=240，000)。
  - read 管理事件會針對 API 錯誤率的事件資料存放區分析一次 (380，000 *1=380，000)。
  - 針對事件資料存放區分析的總管理事件為 620，000 (240，000 + 380，000)。分析事件資料存放區的 620，000 個管理事件會產生成本。

範例 4 – 在線索上啟用管理事件 Insights 和資料事件 Insights for API 呼叫率和 API 錯誤率

在此最終範例中，您會在管理和資料事件上啟用 Insights。此範例中的線索是記錄readwrite和管理與資料事件。

- CloudTrail 會分析過去 28 天內記錄的管理和資料事件，以形成基準。分析無需支付 CloudTrail 費用。
- 建立基準後，線索會記錄 300，000 個管理事件，其中 270，000 個是讀取管理事件，30，000 個是寫入管理事件。追蹤也會記錄 400，000 個資料事件，其中 340，000 個是讀取資料事件，60，000 個是寫入資料事件。
  - write 管理事件會分析兩次，一次用於 API 呼叫率，一次用於 API 錯誤率 (30，000 * 2=60，000)。read 管理事件會針對 API 錯誤率 (270，000 *1=270，000) 分析一次。分析的總管理事件為 330，000 (60，000 + 270，000)。

- `read` 和 `write`資料事件會分析兩次，一次用於 API 呼叫率，一次用於 API 錯誤率 (400，000 * 2)。分析的資料事件總數為 800，000。
- 分析此線索的 1，130，000 個管理和資料事件會產生成本。

# Insights 事件的交付

與 CloudTrail 擷取的其他類型的事件不同，只有在 CloudTrail 偵測到帳戶 API 使用方式發生變更，且與帳戶的一般使用模式有很大差異時，才會加以記錄。

在不同的追蹤和事件資料存放區之間，CloudTrail 在何處傳遞事件以及接收 Insights 事件所需的時間會有所不同。

> **Note**
>
> 資料事件的 Insights 事件僅支援追蹤。

追蹤的 Insights 事件傳遞

如果您已啟用追蹤上的 Insights 事件，且 CloudTrail 偵測到異常的活動，CloudTrail 會為您的追蹤將 Insights 事件傳遞至所選目的地 S3 儲存貯體中的 `/CloudTrail-Insight` 資料夾。在線索上第一次啟用 CloudTrail Insights 之後，CloudTrail 最多可能需要 36 小時才能開始交付 Insights 事件，前提是在此期間偵測到異常活動。

如果您關閉追蹤記錄的 Insights 事件，然後重新啟用 Insights 事件，或停止並重新啟動追蹤記錄，CloudTrail 最多可能需要 36 小時才能重新啟動傳遞 Insights 事件，前提是在此期間偵測到異常活動。

事件資料存放區的 Insights 事件傳遞

如果您已啟用來源事件資料存放區上的 Insights 事件，CloudTrail 會將 Insights 事件傳遞到目的地事件資料存放區。在您第一次在來源事件資料存放區上啟用 CloudTrail Insights 之後，CloudTrail 最多可能需要 7 天才能開始將 Insights 事件交付至目的地事件資料存放區，前提是在此期間偵測到異常活動。

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，則 CloudTrail 最多可能需要 7 天才能重新啟動傳遞 Insights 事件，前提是在此期間偵測到異常活動。擷取 CloudTrail Lake 中的 Insights 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。如需有關 CloudTrail 定價的資訊，請參閱 AWS CloudTrail 定價。

# 使用 CloudTrail 主控台記錄 Insights 事件

本節說明如何使用 CloudTrail 主控台在現有的線索或事件資料存放區上啟用 Insights 事件。

如需如何建立新的線索以記錄 Insights 事件的詳細資訊，請參閱 使用主控台建立追蹤。

如需如何建立新的事件資料存放區以收集 Insights 事件的詳細資訊，請參閱 使用主控台建立 Insights 事件的事件資料存放區。

主題


- 使用主控台在現有線索上啟用 CloudTrail Insights
- 使用主控台在現有事件資料存放區上啟用 CloudTrail Insights


## 使用主控台在現有線索上啟用 CloudTrail Insights

使用下列程序在現有線索上啟用 CloudTrail Insights。

1. 在 CloudTrail 主控台的左導覽窗格中，開啟追蹤頁面，選擇追蹤名稱。
2. 在 Insights 事件中，選擇編輯。

> **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 事件中選擇管理事件或資料事件
5. 在 Insights 類型下，選擇 API 呼叫率、API 錯誤率或兩者。您的線索必須記錄寫入管理或資料事件，以記錄 API 呼叫速率的 Insights 事件。您的線索必須記錄讀取或寫入管理或資料，以記錄 API 錯誤率的 Insights 事件。
6. 選擇儲存變更，以儲存您所做的變更。

在線索上啟用 Insights 事件後，CloudTrail 最多可能需要 36 小時才能開始交付 Insights 事件，前提是在此期間偵測到異常活動。

## 使用主控台在現有事件資料存放區上啟用 CloudTrail Insights

使用下列程序在現有事件資料存放區上啟用 CloudTrail Insights。

擷取 CloudTrail Lake 中的 Insights 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。如需有關 CloudTrail 定價的資訊，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。您無法在其他事件資料存放區類型上啟用 CloudTrail Insights。

1. 在 CloudTrail 主控台的左側導覽窗格中，選擇 Lake 下方的事件資料存放區。
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 事件擷取。
5. 選擇將收集 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。
6. 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。
7. 選擇儲存變更，以儲存您所做的變更。

CloudTrail 最多可能需要 7 天才能開始交付 Insights 事件，前提是在此期間偵測到異常活動。

## 使用 記錄 Insights 事件 AWS CLI

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**
>
> 對於管理事件 Insights：若要在 API 呼叫率上記錄 Insights 事件，追蹤或事件資料存放區必須記錄`write`管理事件。若要以 API 錯誤率記錄 Insights 事件，追蹤或事件資料存放區必須記錄`read`或`write`管理。

對於資料事件 Insights：若要在 API 呼叫率或 API 錯誤率上記錄 Insights 事件，追蹤必須記錄 `read`或 `write` 資料事件。

主題


- 使用 記錄線索的 Insights 事件 AWS CLI
- 使用 記錄事件資料存放區的 Insights 事件 AWS CLI


## 使用 記錄線索的 Insights 事件 AWS CLI

若要傳回線索的目前 Insights 選擇器，請執行 `get-insight-selectors`命令。

```
aws cloudtrail get-insight-selectors --trail-name TrailName
```

下列範例回應顯示名為 之線索的 Insights 選擇器`insights-trail`。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/insights-trail",
    "InsightSelectors": [
        {
            "InsightType": "ApiCallRateInsight",
            "EventCategories": [
                "Management",
                "Data"
            ]
        },
        {
            "InsightType": "ApiErrorRateInsight",
            "EventCategories": [
                "Management",
                "Data"
            ]
        }
    ]
}
```

如果追蹤未啟用 Insights，get-insight-selectors命令會傳回下列錯誤訊息：「呼叫 GetInsightSelectors 操作時發生錯誤 (InsightNotEnabledException)：Trail arn：aws：cloudtrail：us-east-1：123456789012：trail/trailName 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。)

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)。每個 InsightType 都可以為管理 EventCategory 或資料 EventCategory 或兩者啟用。

```
aws cloudtrail put-insight-selectors --trail-name TrailName --insight-selectors
 '[{"InsightType": "ApiCallRateInsight", "EventCategories": ["Data"]},{"InsightType":
 "ApiErrorRateInsight", "EventCategories": ["Data", "Management"]}]'
```

下列結果顯示針對追蹤設定的 Insights 事件選取器。

```
{
  "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName",
  "InsightSelectors":
      [
         {
            "InsightType": "ApiErrorRateInsight",
            "EventCategories": [
                "Data"
            ]
         },
         {
            "InsightType": "ApiCallRateInsight",
            "EventCategories": [
                "Data",
                "Management"
            ]
         }
      ]
 }
```

## 使用 記錄事件資料存放區的 Insights 事件 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
```

如果事件資料存放區設定為接收 Insights 事件，`eventCategory`則會將其設定為 `Insight`。

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`。使用您希望在事件資料存放區中保留事件的天數來替換 *`retention-period-days`*。

   若您要用 AWS Organizations 組織的管理帳戶登入，請加入 `--organization-enabled` 參數 (如果您希望向委派的管理員授予存取事件資料存放區的權限)。

   ```
   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。使用您希望在事件資料存放區中保留事件的天數來替換 *retention-period-days*。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"
         }
      ]
}
```

在您第一次在事件資料存放區上啟用 CloudTrail Insights 之後，CloudTrail 最多可能需要 7 天才能開始交付 Insights 事件，前提是在此期間偵測到異常活動。

# 檢視追蹤的 Insights 事件

本節說明如何在啟用 CloudTrail Insights 的情況下，查詢追蹤過去 90 天的 Insights 事件。如需如何檢視事件資料存放區的 CloudTrail Insights 的詳細資訊，請參閱 檢視事件資料存放區的 Insights 儀表板。

您可以從 主控台的 Insights 頁面檢視、篩選和下載過去 90 天的 Insights 事件。

您可以以程式設計方式擷取 Insights 事件的最後 90 天：

- 對於透過執行 AWS CLI lookup-events命令或 LookupEvents API 操作的線索記錄管理事件。
- 對於透過執行 AWS CLI list-insights-data命令或 ListInsightsData API 操作記錄資料事件的線索。

如需追蹤的 Insights 事件記錄欄位說明，請參閱 追蹤的 Insights 事件 CloudTrail 記錄內容。

> **Note**
>
> 如果您已在記錄管理或資料事件的線索上啟用 Insights， Insights 頁面和 AWS CLI `lookup-events` 或 `list-insights-data`命令只會列出 Insights 事件。如需在線索上啟用 Insights 的詳細資訊，請參閱 使用主控台在現有線索上啟用 CloudTrail Insights和 使用 記錄線索的 Insights 事件 AWS CLI。
>
> 若要在 API 呼叫率上記錄 Insights 事件，線索必須記錄`write`管理或資料事件。若要以 API 錯誤率記錄 Insights 事件，追蹤必須記錄`read`或`write`管理 或 資料事件。

主題

- 使用主控台檢視線索的 Insights 事件
- 使用 檢視線索的 Insights 事件 AWS CLI


# 使用主控台檢視線索的 Insights 事件

本節說明如何從 CloudTrail 主控台的 Insights 頁面檢視、查詢和下載過去 90 天的 Insights 事件。如需如何檢視事件資料存放區的 CloudTrail Insights 的詳細資訊，請參閱 檢視事件資料存放區的 Insights 儀表板。

記錄線索的 Insights 事件後，事件會在 Insights 頁面上顯示 90 天。您無法從 Insights (深入分析) 頁面手動刪除事件。由於針對線索啟用的 Insights 事件會存放在針對該線索設定的 Amazon S3 儲存貯體中，因此從儲存貯體中移除 Insights 事件將會刪除這些事件。

您可以啟用 CloudWatch Logs 來監控追蹤日誌，並在發生特定 Insights 事件時收到通知。如需詳細資訊，請參閱使用 Amazon CloudWatch Logs 監控 CloudTrail 日誌檔案。

> **Note**
>
> - CloudTrail Insights 事件必須在您的線索中啟用，才能在主控台中查看 Insights 事件。如果在此期間偵測到異常活動，CloudTrail 最多需要 36 小時才能交付第一個 Insights 事件。
> - 對於管理事件 Insights：若要在 API 呼叫率上記錄 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。
> - 對於資料事件 Insights：若要在 API 呼叫率或 API 錯誤率上記錄 Insights 事件，追蹤必須記錄 `read`或 `write` 資料事件。

檢視 Insights 事件

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/home/ 的 CloudTrail 主控台。
2. 在導覽窗格中，選擇 Insights 以查看您帳戶在過去 90 天內記錄的所有 Insights 事件。您也可以從儀表板頁面檢視五個最新的 Insights 事件。
3. 在 Insights 頁面上，您可以選取管理事件 Insights 或資料事件 Insights 索引標籤
4. 您可以依事件來源、事件名稱或事件 ID 篩選 Insights 事件。如需有關篩選 Insights 事件的詳細資訊，請參閱篩選 Insights 事件。
5. 您可以進一步將清單限制為相對範圍或絕對範圍。

內容


- 篩選 Insights 事件
- 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

根據預設， Insights 頁面上的事件會依事件開始時間的反向時間順序顯示。

您可以從下列三個屬性中選擇其中一個來篩選清單：

事件名稱

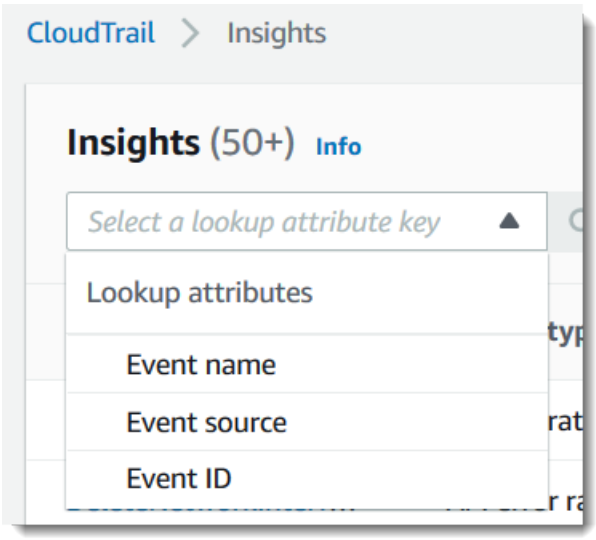
事件的名稱，通常是記錄異常活動層級的 AWS API。

事件來源

提出請求 AWS 的服務，例如 `iam.amazonaws.com`或 `s3.amazonaws.com`。如果您選擇依事件來源篩選，您可以捲動事件來源清單。

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。分析以產生 Insights 事件的管理事件或資料事件的事件 IDs 與 Insights 事件的事件 IDs 不同。




下列清單說明無法篩選之事件的屬性：

洞見類型

CloudTrail Insights 事件的類型可以是 API 呼叫率或 API 錯誤率。API 呼叫率洞見類型會根據基準 API 呼叫量，分析每分鐘彙總的唯寫管理或資料 API 呼叫。API 錯誤率洞見類型會分析導致錯誤代碼的管理或資料 API 呼叫。如果 API 呼叫失敗，則顯示錯誤。

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

基準代表 API 呼叫率或錯誤率活動的正常模式，每日計算。基準平均值是 Insights 事件開始前七天內這些每日基準的平均值。雖然此期間通常為七天，但 CloudTrail 會將計算期間四捨五入為整數天數，因此確切的基準持續時間可能會略有不同。

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 Insights 平均值是觸發 Insights 事件的發生率。一般而言，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，請從下拉式選單中選擇查詢屬性，然後在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。

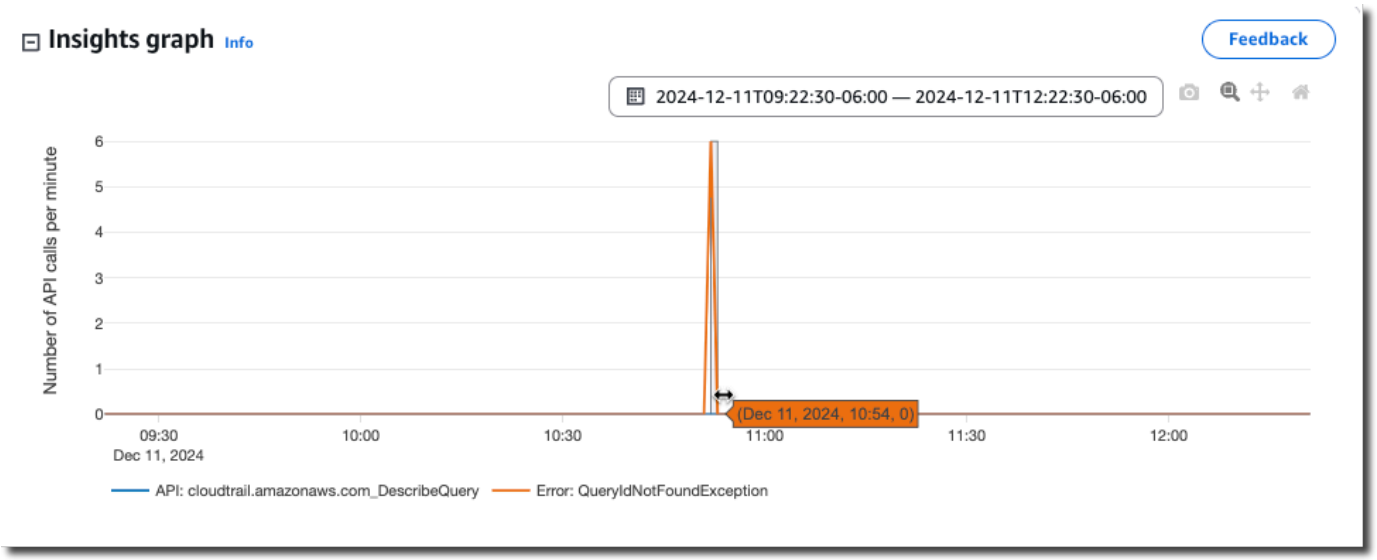
依開始與結束日期及時間進行篩選

1. 從依日期和時間篩選中，選擇下列其中一項：
   - 絕對範圍 - 可讓您選擇特定時間。繼續進行下一個步驟。
   - 相對範圍 - 預設選取。可讓您選擇與 Insights 事件開始時間相關的時段。繼續步驟 3。
2. 若要設定絕對範圍，請執行下列動作。
   a. 選擇您希望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。
3. 若要設定相對範圍，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。預設時間範圍包括 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)。
   b. 設定您想要的相對時間後，選擇 Apply (套用)。
4. 若要移除時間範圍篩選條件，請選擇依日期和時間篩選方塊右側的行事曆圖示，然後選擇清除並關閉。

# 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，其中列出為了判斷發生異常活動而分析的管理或資料事件。
- 每分鐘 API 呼叫或每分鐘錯誤
  - 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 Insights 平均值是觸發 Insights 事件之 API 的每分鐘呼叫率或錯誤率。一般而言，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 呼叫次數或錯誤 AWS 的服務端點。在上述影像中，來源為 `ec2.amazonaws.com`，這是 Amazon EC2 的服務端點。
- 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。
- Shared event ID (共用事件 ID) - 在 Insights 事件中，Shared event ID (共用事件 ID) 是由 CloudTrail Insights 產生的 GUID，用於唯一識別一組開始和結束 Insights 事件。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。
4. 在 CloudTrail 事件索引標籤上，檢視 CloudTrail 所分析的相關事件，以判斷發生的異常活動。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 管理或與主體 API 相關的資料事件，這些事件發生在 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。

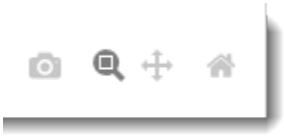
   當您在圖表中選取其他 Insights 事件時，CloudTrail 事件資料表中顯示的事件變更。這些事件可協助您執行更深入的分析，以判斷 Insights 事件的可能原因，以及異常 API 活動的原因。

   若要顯示 Insights 事件持續期間記錄的所有 CloudTrail 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。

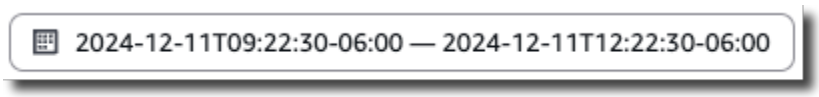


圖表工具列上的命令按鈕從左到右執行以下作業：

- 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。




## 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 事件歷史記錄檔案屬資料檔案，內含個別使用者可設定的資訊 (如資源名稱)。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，將 CloudTrail 事件匯出至 CSV 並匯入至試算表程式時，該程式可能會提醒您關於安全方面的考量。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`，並指定過去 12 小時活動的時間範圍。
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)。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，請選擇取消。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。

## 使用 檢視線索的 Insights 事件 AWS CLI

本節說明如何使用 AWS CLI `lookup-events`和 `list-insights-data`命令來查詢過去 90 天的 Insights 事件，以取得已啟用 Insights 事件的線索。如需有關如何在線索上啟用 CloudTrail Insights 的資訊，請參閱 使用 記錄線索的 Insights 事件 AWS CLI。

> **Note**
>
> 您無法使用 `lookup-events`或 `list-insights-data`命令來查詢事件資料存放區的 Insights 事件，不過，CloudTrail Lake 為 Insights 事件資料存放區提供許多範例查詢。如需詳細資訊，請參閱檢視 Insights 事件的範例查詢。

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`

此 `list-insights-data` 命令提供以下選項：

- `--end-time`
- `--data-type`
- `--max-results`
- `--start-time`
- `--dimensions`
- `--next-token`
- `--generate-cli-skeleton`
- `--cli-input-json`

如需使用 的一般資訊 AWS Command Line Interface，請參閱AWS Command Line Interface 《使用者指南》。

內容


- 先決條件
- 取得命令列說明
- 查詢管理事件的 Insights 事件
- 查詢 Insights 事件以取得資料事件
- 指定要傳回的管理事件 Insights 事件數量
- 指定要傳回的資料事件 Insights 事件數目
- 依時間範圍查詢管理事件的 Insights 事件
- 依時間範圍查詢資料事件的 Insights 事件
- 依屬性查詢管理事件的 Insights 事件
  - 屬性查詢範例
- 依維度查詢資料事件的 Insights 事件
  - 維度查詢範例
- 為管理事件指定 Insights 事件結果的下一頁
- 為管理事件指定 Insights 事件結果的下一頁
- 從管理事件的 Insights 事件檔案中取得 JSON 輸入

- 從資料事件的 Insights 事件檔案中取得 JSON 輸入
- 查詢輸出欄位

## 先決條件

- 若要執行 AWS CLI 命令，您必須安裝 AWS CLI。如需詳細資訊，請參閱 Get started with the AWS CLI。
- 請確定您的 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命令。如需詳細資訊，請參閱設定 AWS 命令列界面。
- 若要在 API 呼叫率上記錄 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**
>
> CloudTrail AWS CLI 命令區分大小寫。

## 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
```

## 查詢管理事件的 Insights 事件

若要查看 50 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": "1.09",
```

```
            "eventTime": "2024-12-11T16:52:00Z",
            "awsRegion": "us-east-1",
            "eventID": "18378b1e-3653-433d-ba1e-aa11a5958f0c",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "888888888888",
            "sharedEventID": "fccb064f-dd07-4822-97c0-11115d8b91d4",
            "insightDetails": {
                "state": "Start",
                "eventSource": "cloudtrail.amazonaws.com",
                "eventName": "DescribeQuery",
                "insightType": "ApiErrorRateInsight",
                "errorCode": "QueryIdNotFoundException",
                "sourceEventCategory": "Management",
                "insightContext": {
                    "statistics": {
                        "baseline": {
                            "average": 0
                        },
                        "insight": {
                            "average": 1.2
                        },
                        "insightDuration": 5,
                        "baselineDuration": 11092
                    },
                    "attributions": [
                        {
                            "attribute": "userIdentityArn",
                            "insight": [
                                {
                                    "value": "arn:aws:sts::888888888888:assumed-role/
Admin",
                                    "average": 1.2
                                }
                            ],
                            "baseline": []
                        },
                        {
                            "attribute": "userAgent",
                            "insight": [
                                {
                                    "value": "Mozilla/5.0 (Macintosh; Intel Mac OS X
 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36",
                                    "average": 1.2
                                }
```

```
                            ],
                            "baseline": []
                        }
                    ]
                }
            },
            "eventCategory": "Insight"
        },
        {
            "eventVersion": "1.09",
            "eventTime": "2024-12-11T16:53:00Z",
            "awsRegion": "us-east-1",
            "eventID": "b32f10a0-f039-419a-bad7-e95468930a4f",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "888888888888",
            "sharedEventID": "fccb064f-dd07-4822-97c0-11115d8b91d4",
            "insightDetails": {
                "state": "End",
                "eventSource": "cloudtrail.amazonaws.com",
                "eventName": "DescribeQuery",
                "insightType": "ApiErrorRateInsight",
                "errorCode": "QueryIdNotFoundException",
                "sourceEventCategory": "Management",
                "insightContext": {
                    "statistics": {
                        "baseline": {
                            "average": 0
                        },
                        "insight": {
                            "average": 6
                        },
                        "insightDuration": 1,
                        "baselineDuration": 11092
                    },
                    "attributions": [
                        {
                            "attribute": "userIdentityArn",
                            "insight": [
                                {
                                    "value": "arn:aws:sts::888888888888:assumed-role/
Admin",
                                    "average": 6
                                }
                            ],
```

```
                            "baseline": []
                        },
                        {
                            "attribute": "userAgent",
                            "insight": [
                                {
                                    "value": "Mozilla/5.0 (Macintosh; Intel Mac OS X
 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36",
                                    "average": 6
                                }
                            ],
                            "baseline": []
                        }
                    ]
                }
            },
            "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 追蹤的 Insights 事件 CloudTrail 記錄內容。

## 查詢 Insights 事件以取得資料事件

若要查看 50 個最新的 Insights 事件，請輸入下列命令。

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName
```

傳回的事件看起來類似下列範例：

```
    {
    "NextToken": "kbOt5LlZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP

    "Events": [
        {
            "eventVersion": "1.09",
            "eventTime": "2024-12-11T16:52:00Z",
            "awsRegion": "us-east-2",
```

```
            "eventID": "18378b1e-3653-433d-ba1e-aa11a5958f0c",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "123456789012",
            "sharedEventID": "fccb064f-dd07-4822-97c0-11115d8b91d4",
            "insightDetails": {
                "state": "Start",
                "eventSource": "s3.amazonaws.com",
                "eventName": "PutObject",
                "insightType": "ApiErrorRateInsight",
                "errorCode": "InvalidRequest",
                "sourceEventCategory": "Data",
                "insightContext": {
                    "statistics": {
                        "baseline": {
                            "average": 0
                        },
                        "insight": {
                            "average": 1.2
                        },
                        "insightDuration": 5,
                        "baselineDuration": 11092
                    },
                    "attributions": [
                        {
                            "attribute": "userIdentityArn",
                            "insight": [
                                {
                                    "value": "arn:aws:sts::123456789012:assumed-role/
Admin",
                                    "average": 1.2
                                }
                            ],
                            "baseline": []
                        },
                        {
                            "attribute": "userAgent",
                            "insight": [
                                {
                                    "value": "Mozilla/5.0 (Macintosh; Intel Mac OS X
 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36",
                                    "average": 1.2
                                }
                            ],
                            "baseline": []
```

```
                        }
                    ]
                },

                "insightSource": "arn:aws:cloudtrail:us-
east-2:123456789012:trail/TrailName"
            },
            "eventCategory": "Insight"
        },
        {
            "eventVersion": "1.09",
            "eventTime": "2024-12-11T16:53:00Z",
            "awsRegion": "us-east-1",
            "eventID": "b32f10a0-f039-419a-bad7-e95468930a4f",
            "eventType": "AwsCloudTrailInsight",
            "recipientAccountId": "123456789012",
            "sharedEventID": "fccb064f-dd07-4822-97c0-11115d8b91d4",
            "insightDetails": {
                "state": "End",
                "eventSource": "s3.amazonaws.com",
                "eventName": "PutObject",
                "insightType": "ApiErrorRateInsight",
                "errorCode": "InvalidRequest",
                "sourceEventCategory": "Data",
                "insightContext": {
                    "statistics": {
                        "baseline": {
                            "average": 0
                        },
                        "insight": {
                            "average": 6
                        },
                        "insightDuration": 1,
                        "baselineDuration": 11092
                    },
                    "attributions": [
                        {
                            "attribute": "userIdentityArn",
                            "insight": [
                                {
                                    "value": "arn:aws:sts::123456789012:assumed-role/
Admin",
                                    "average": 6
                                }
```

```
                            ],
                            "baseline": []
                        },
                        {
                            "attribute": "userAgent",
                            "insight": [
                                {
                                    "value": "Mozilla/5.0 (Macintosh; Intel Mac OS X
 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36",
                                    "average": 6
                                }
                            ],
                            "baseline": []
                        }
                    ]
                },

                "insightSource": "arn:aws:cloudtrail:us-
east-2:123456789012:trail/TrailName"
            },
            "eventCategory": "Insight"
        }
    ]
}
```

## 指定要傳回的管理事件 Insights 事件數量

若要為要傳回的管理事件指定 Insights 事件數量，請輸入下列命令。

```
aws cloudtrail lookup-events --event-category insight --max-results <integer>
```

若未指定 *<integer>* 的預設值為 50。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
```

## 指定要傳回的資料事件 Insights 事件數目

若要為要傳回的資料事件指定 Insights 事件數量，請輸入下列命令。

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName --max-results <integer>
```

若未指定 *<integer>* 的預設值為 50。可能值為 1 到 50。下列範例會傳回一個結果。

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName --max-results 1
```

### 依時間範圍查詢管理事件的 Insights 事件

過去 90 天的管理事件洞見事件可供查詢。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。

### 依時間範圍查詢資料事件的 Insights 事件

過去 90 天的資料事件洞見事件可供查詢。若要指定時間範圍，請輸入下列命令。

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName --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。

## 依屬性查詢管理事件的 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`

的長度上限為 `AttributeValue` 2000 個字元。下列字元 ('_'、' '、','、'\\n') 計算為 2000 個字元限制的兩個字元。

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
```

## 依維度查詢資料事件的 Insights 事件

若要依維度篩選，請輸入下列命令。

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName
       --dimensions <DimensionKey>=<DimensionValue>
```

每個list-insights-events命令只能指定一個維度鍵/值對。以下是 DimensionKey 的有效 Insights 事件值。值名稱區分大小寫。

- EventId
- EventName
- EventSource

的長度上限為 DimensionValue 2000 個字元。下列字元 ('_'、' '、','、'\\n') 計算為 2000 個字元限制的兩個字元。

維度查詢範例

下列範例命令會傳回 EventName 值為 PutObject 的 Insights 事件。

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName --dimensions
 EventName=PutObject
```

下列範例命令會傳回 EventId 值為 b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002 的 Insights 事件。

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName --dimensions
 EventId=b5cc8c40-12ba-4d08-a8d9-2bceb9a3e002
```

下列範例命令會傳回 EventSource 值為 s3.amazonaws.com 的 Insights 事件。

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName --dimensions
 EventSource=s3.amazonaws.com
```

### 為管理事件指定 Insights 事件結果的下一頁

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
```

### 為管理事件指定 Insights 事件結果的下一頁

若要從 list-insights-data 命令取得下一頁的結果，請輸入下列命令。

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName<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 list-insights-data --data-type InsightsEvents --insight-source
 arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName --dimensions
 EventName=PutObject
```

若要取得下一頁的結果，您的下一個命令會如下所示。

```
aws cloudtrail list-insights-data --data-type InsightsEvents --insight-
source arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName
 --dimensions EventName=PutObject --next-token=EXAMPLEZe+
+mErCebpy2TgaMgmDvF1kYGFcH64JSjIbZFjsuvrSqg66b5YGssKutDYIyII4lrP4IDbeQdiObkp9YAlju3oXd12juEXAMP
```

## 從管理事件的 Insights 事件檔案中取得 JSON 輸入

AWS CLI 某些 AWS 服務的 有兩個參數 `--generate-cli-skeleton`和 `--cli-input-json`，可用來產生 JSON 範本，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
   ```

   所產生的範本檔案 (在此情況下為 LookupEvents.txt) 如下。

   ```
   {
       "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。

## 從資料事件的 Insights 事件檔案中取得 JSON 輸入

AWS CLI 某些 AWS 服務的 有兩個參數 `--generate-cli-skeleton`和 `--cli-input-json`，可用來產生 JSON 範本，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 list-insights-data`。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 `list-insights-data` 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 list-insights-data --data-type InsightsEvents --generate-cli-
skeleton > ListInsightsData.txt
```

產生的範本檔案（在此案例中為 ListInsightsData.txt) 如下所示。

```
{
```

```
   "InsightSource": "",
    "DataType": "InsightsEvents",
    "Dimensions":
    {
        "KeyName": ""
    },
    "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。

```
{

   "InsightSource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName",
    "DataType": "InsightsEvents",
    "Dimensions":
    {
        "EventName": "PutObject"
    },
    "StartTime": "2025-11-01",
    "EndTime": "2025-11-05",
    "MaxResults": 1
}
```

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 list-insights-data --data-type InsightsEvents --cli-input-json
 file://ListInsightsData.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。每個項目都會包含查詢請求的資訊，以及包含以字串呈現所擷取的 CloudTrail 事件。

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

提出請求的 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 Insights 事件的詳細資訊，請參閱此指南中的 使用 CloudTrail Insights。

# 檢視事件資料存放區的 Insights 事件

本節說明如何透過檢視 Insights 事件儀表板和執行範例查詢，來檢視 Insights 事件資料存放區的 Insights 事件。如需有關如何在事件資料存放區上啟用 CloudTrail Insights 的資訊，請參閱 使用主控台在現有事件資料存放區上啟用 CloudTrail Insights。

CloudTrail 查詢會依據掃描的資料量而產生費用。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 CloudTrail 定價的詳細資訊，請參閱 AWS CloudTrail 定價。

如需事件資料存放區的 Insights 事件記錄欄位說明，請參閱 事件資料存放區的 Insights 事件 CloudTrail 記錄內容。

主題

- 檢視事件資料存放區的 Insights 儀表板
- 檢視 Insights 事件的範例查詢

## 檢視事件資料存放區的 Insights 儀表板

Insights 事件儀表板會顯示依 Insights 類型分類的 Insights 事件整體比例、最高使用者和服務依 Insights 類型分類的 Insights 事件比例，以及每天的 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。

> **Note**
>
> - 在您第一次在來源事件資料存放區上啟用 CloudTrail Insights 之後，CloudTrail 最多可能需要 7 天才能開始交付 Insights 事件，前提是在此期間偵測到異常活動。如需詳細資訊，請參閱Insights 事件的交付。

- Insights 事件儀表板只會顯示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。

檢視 Insights 事件儀表板

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
2. 在左側導覽窗格中，選擇 Lake 下方的儀表板。
3. 選擇受管和自訂儀表板索引標籤。
4. 從AWS 受管儀表板中，選擇 Insights 事件儀表板。
5. 選擇您的 Insights 事件資料存放區。
6. 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 CloudTrail 定價的詳細資訊，請參閱 AWS CloudTrail 定價。

7. 選擇重新整理圖示以填入儀表板小工具的圖形。每個小工具都會指出重新整理的狀態。

如需有關 Lake 儀表板的詳細資訊，請參閱 CloudTrail Lake 儀表板。

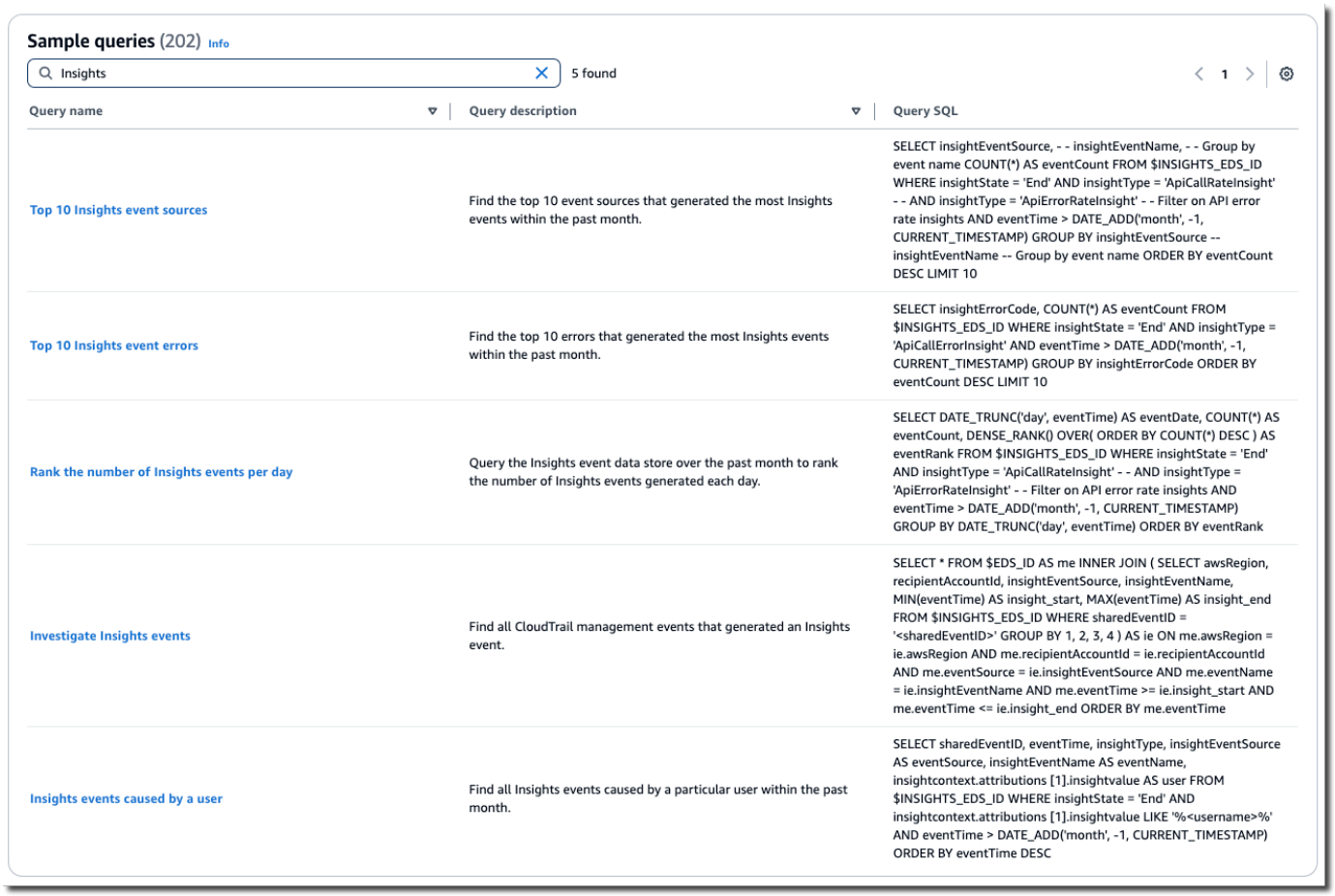
## 檢視 Insights 事件的範例查詢

CloudTrail 主控台為 Insights 事件提供許多範例查詢，可協助您開始撰寫自己的查詢。

檢視 Insights 事件的範例查詢

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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. 搜尋 Insights 事件的查詢。選擇查詢名稱以在編輯器索引標籤中開啟查詢。




5. 在編輯器索引標籤上，選擇 Insights 事件資料存放區。當您在清單中選擇事件資料存放區時，CloudTrail 會自動在查詢編輯器的 FROM 列填入事件資料存放區 ID。
6. 選擇執行以執行查詢。查詢完成後，您可以檢視命令輸出和查詢結果。

   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 使用 CloudTrail 主控台建立或編輯查詢。如需有關執行查詢和儲存查詢結果的詳細資訊，請參閱 使用主控台執行查詢並儲存查詢結果。

# 使用 AWS CloudTrail Lake

AWS CloudTrail Lake 可讓您在事件上執行 SQL 型查詢。CloudTrail Lake 會將分列式 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)。套用於事件資料存放區的選取器控制哪些事件持續存在並可供您查詢。CloudTrail Lake 是稽核解決方案，可以補充您的合規性堆疊，並協助您進行接近即時的故障診斷。

## CloudTrail Lake 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 （管理事件、資料事件、網路活動事件）、CloudTrail Insights 事件、AWS Config 組態項目、AWS Audit Manager 證據或來自外部的事件 AWS。每個事件資料存放區只能包含特定事件類別 （例如 AWS Config 組態項目），因為事件結構描述對事件類別是唯一的。您可以將來自組織的事件存放在組織的事件資料存放 AWS Organizations 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全新和現有的事件資料存放區，以建立記錄到追蹤之事件的時間點快照。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 Data Catalog 中的資料表中繼資料可讓 Athena 查詢引擎知道如何尋找、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。

您可以將資源型政策連接至事件資料存放區，以提供所選主體的跨帳戶存取權。您可以在 CloudTrail 主控台上建立或更新事件資料存放區時，或執行 AWS CLI `put-resource-policy`命令來新增資源型政策。如需詳細資訊，請參閱事件資料存放區的資源型政策範例。

依預設，CloudTrail 會加密事件資料存放區中的所有事件。當您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 AWS KMS 的成本。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。

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 Lake 成本。

CloudTrail Lake 支援 Amazon CloudWatch 指標，這些指標可提供擷取之資料和儲存位元組的相關資訊。如需支援的 CloudWatch 指標的詳細資訊，請參閱支援的 CloudWatch 指標。

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

## CloudTrail Lake 查詢

與事件歷史記錄中單純的索引鍵和值查詢或執行 `LookupEvents` 相比，CloudTrail Lake 查詢提供了更深入、自訂功能更多的事件檢視畫面。事件歷史記錄搜尋僅限於單一 AWS 帳戶，只會傳回來自單一的事件 AWS 區域，且無法查詢多個屬性。相比之下，CloudTrail Lake 使用者可以跨多個事件欄位執行複雜的 SQL 查詢。CloudTrail Lake 支援所有有效的 Trino `SELECT`陳述式和函數。如需支援的 SQL 函數和運算子的詳細資訊，請參閱 Trino 文件網站上的函數和運算子。

您可以在 CloudTrail Lake Editor 索引標籤上建置查詢，方法是從頭開始在 SQL 中寫入查詢、開啟已儲存或範例查詢並進行編輯，或使用查詢產生器從英文語言提示產生查詢。如需詳細資訊，請參閱使用 CloudTrail 主控台建立或編輯查詢及從自然語言提示建立 CloudTrail Lake 查詢。

您可以儲存 CloudTrail Lake 查詢以供將來使用，並可查看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。

CloudTrail 主控台提供許多範例查詢，可協助您開始自行編寫查詢。如需詳細資訊，請參閱使用 CloudTrail 主控台檢視範例查詢。

CloudTrail Lake 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 Lake 成本。

## CloudTrail Lake 儀表板

您可以使用 CloudTrail Lake 儀表板來查看帳戶中事件資料存放區的事件趨勢。CloudTrail Lake 提供下列儀表板類型：

- 受管儀表板 – 您可以檢視受管儀表板，以查看收集管理事件、資料事件或 Insights 事件的事件資料存放區的事件趨勢。這些儀表板會自動提供給您，並由 CloudTrail Lake 管理。CloudTrail 提供 14 個受管儀表板供您選擇。您可以手動重新整理受管儀表板。您無法修改、新增或移除這些儀表板的小工具，不過，如果您想要修改小工具或設定重新整理排程，則可以將受管儀表板儲存為自訂儀表板。
- 自訂儀表板 – 自訂儀表板可讓您查詢任何事件資料存放區類型中的事件。您最多可以將 10 個小工具新增至自訂儀表板。您可以手動重新整理自訂儀表板，也可以設定重新整理排程。
- 反白儀表板 – 啟用反白儀表板可at-a-glance檢視您帳戶中事件資料存放區所收集的 AWS 活動概觀。醒目提示儀表板由 CloudTrail 管理，並包含與您帳戶相關的小工具。醒目提示儀表板上顯示的小工具對於每個帳戶都是唯一的。這些小工具可能會浮現偵測到的異常活動或異常。例如，醒目提示儀表板可能包含跨帳戶存取總數小工具，這會顯示異常跨帳戶活動是否增加。CloudTrail 每 6 小時更新一次反白儀表板。儀表板會顯示上次更新後的最後 24 小時的資料。

每個儀表板都包含一或多個小工具，每個小工具代表 SQL 查詢。

如需詳細資訊，請參閱CloudTrail Lake 儀表板。

# CloudTrail Lake 整合

您可以使用 CloudTrail Lake 整合，從 外部記錄和存放使用者活動資料 AWS；從混合環境中的任何來源，例如內部或 SaaS 應用程式託管在內部部署或雲端、虛擬機器或容器中。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 將您的應用程式活動擷取到 CloudTrail。然後，您可以使用 CloudTrail Lake 來搜尋、查詢和分析從應用程式記錄的資料。

整合還可以將來自十幾個 CloudTrail 合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，將事件交付至您 AWS 帳戶的事件資料存放區。透過解決方案整合，應用程式會在您的帳戶中執行，AWS 而應用程式會呼叫 `PutAuditEvents` API，將事件交付至您 AWS 帳戶的事件資料存放區。

如需整合的詳細資訊，請參閱在 外部建立與事件來源的整合 AWS。

# 其他資源

以下資源可協助您進一步了解什麼是 CloudTrail Lake 及其使用方式。

- 使用 CloudTrail Lake 實現稽核日誌管理現代化 (YouTube 影片)
- 記錄 AWS CloudTrail Lake 中非AWS 來源的活動事件 (YouTube 影片 )

- 使用 AWS CloudTrail Lake 和 Amazon Athena 分析活動日誌 (YouTube 影片 )
- 了解員工和客戶身分的活動日誌 (AWS 部落格 )
- 使用 AWS CloudTrail Lake 識別 AWS 較舊的服務端點 TLS 連線 (AWS 部落格 )
- Arctic Wolf 如何使用 AWS CloudTrail Lake 來簡化安全性和操作 (AWS 部落格 )
- CloudTrail Lake 常見問答集
- AWS CloudTrail API 參考
- AWS CloudTrail 資料 API 參考
- AWS CloudTrail 合作夥伴加入指南

# CloudTrail Lake 支援的區域

目前，以下支援 CloudTrail Lake 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 |
| Africa (Cape Town) | af-south-1 |
| 亞太地區 (香港) | ap-east-1 |
| 亞太地區 (海德拉巴) | ap-south-2 |
| 亞太地區 (雅加達) | ap-southeast-3 |
| 亞太地區 (墨爾本) | ap-southeast-4 |
| 亞太區域 (孟買) | ap-south-1 |
| 亞太地區 (大阪) | ap-northeast-3 |
| 亞太區域 (首爾) | ap-northeast-2 |

| 區域名稱 | 區域 |
| --- | --- |
| 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 |
| Europe (Paris) | eu-west-3 |
| 歐洲 (西班牙) | eu-south-2 |
| Europe (Stockholm) | eu-north-1 |
| 歐洲 (蘇黎世) | eu-central-2 |
| 以色列 (特拉維夫) | il-central-1 |
| Middle East (Bahrain) | 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 |

如需有關 CloudTrail 服務端點的詳細資訊，請參閱 AWS CloudTrail 端點與配額。

如需在 中使用 CloudTrail 的詳細資訊 AWS GovCloud (US) Regions，請參閱AWS GovCloud (US)《 使用者指南》中的服務端點。

# CloudTrail Lake 概念和術語

本節說明協助您使用 AWS CloudTrail Lake 的重要概念和術語。

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 事件（管理事件、資料事件、網路活動事件）、CloudTrail Insights 事件、AWS Audit Manager 證據、AWS Config 組態項目或外部事件 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。

對於管理事件、資料事件和網路活動事件，您可以使用進階事件選取器來篩選事件。例如，如果您要建立事件資料存放區來收集管理事件，您可以篩選 out AWS Key Management Service (AWS KMS) 或 Amazon Relational Database Service (Amazon RDS) Data API 事件。一般而言，`Encrypt`、 `Decrypt`和 等 AWS KMS 動作`GenerateDataKey`會產生超過 99% 的事件。

對於 AWS Config 組態項目、Audit Manager 證據或 外部的事件 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 資料目錄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 Data Catalog 中的資料表中繼資料可讓 Athena 查詢引擎了解如何尋找、讀取和處理您要查詢的資料。

當您啟用 Lake 查詢聯合時，CloudTrail 會代替您建立聯合資源，並向 AWS Lake Formation 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 Lake 成本。

保留期間

事件資料存放區的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。CloudTrail Lake 會透過檢查事件的 `eventTime` 是否在指定保留期以內，決定是否要保留該事件。例如，如果您指定的保留期為 90 天，CloudTrail 將移除 `eventTime` 早於 90 天的事件。

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，儲存的定價將為按使用量付費。

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 整合來記錄和儲存來自下列來源的使用者活動資料：

- 外部 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。設定整合後，請呼叫 PutAuditEvents API 操作，將您的應用程式活動擷取至 CloudTrail。然後，您可以使用 CloudTrail Lake 來搜尋、查詢和分析從應用程式記錄的資料。如需詳細資訊，請參閱在 外部建立與事件來源的整合 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 中執行，AWS 帳戶 而應用程式會呼叫 PutAuditEvents API 操作，將事件交付至 的事件資料存放區 AWS 帳戶。

頻道

來自 AWS 工作外部來源的活動事件，方法是使用頻道將事件從使用 CloudTrail 的外部合作夥伴，或從您自己的來源帶入 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 Lake 中的查詢是以 SQL 撰寫而成。您可以在 CloudTrail Lake Editor 索引標籤上建置查詢，方法是從頭開始在 SQL 中寫入查詢、開啟已儲存或範例查詢並進行編輯，或使用查詢產生器從英文語言提示產生查詢。如需詳細資訊，請參閱使用 CloudTrail 主控台建立或編輯查詢及從自然語言提示建立 CloudTrail Lake 查詢。

CloudTrail Lake 支援所有有效的 Trino SELECT 陳述式和函數。如需支援之 SQL 函數和運算子的詳細資訊，請參閱 Trino 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CloudTrail Lake 儀表板。

儀表板類型

CloudTrail Lake 提供下列儀表板類型：

- 受管儀表板 – 您可以檢視受管儀表板，以查看收集管理事件、資料事件或 Insights 事件的事件資料存放區的事件趨勢。這些儀表板會自動提供給您，並由 CloudTrail Lake 管理。CloudTrail 提供 14 個受管儀表板供您選擇。您可以手動重新整理受管儀表板。您無法修改、新增或移除這些儀表板的小工具，不過，如果您想要修改小工具或設定重新整理排程，則可以將受管儀表板儲存為自訂儀表板。
- 自訂儀表板 – 自訂儀表板可讓您查詢任何事件資料存放區類型中的事件。您最多可以將 10 個小工具新增至自訂儀表板。您可以手動重新整理自訂儀表板，也可以設定重新整理排程。
- 反白儀表板 – 啟用反白儀表板可at-a-glance檢視您帳戶中事件資料存放區所收集的 AWS 活動概觀。醒目提示儀表板由 CloudTrail 管理，並包含與您帳戶相關的小工具。醒目提示儀表板上顯示的小工具對於每個帳戶都是唯一的。這些小工具可能會浮現偵測到的異常活動或異常。例如，您的 Highlights 儀表板可能包含跨帳戶存取總數小工具，顯示異常跨帳戶活動是否增加。CloudTrail 每 6 小時更新一次反白儀表板。儀表板會顯示上次更新後的最後 24 小時的資料。

小工具

小工具是組成儀表板並提供視覺化的元件，例如折線圖或長條圖。每個小工具對應至 SQL 查詢。當您重新整理儀表板時，CloudTrail 會對儀表板上的每個小工具執行查詢，以填入小工具的資料。

# CloudTrail Lake 事件資料存放區

在 CloudTrail Lake 中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（管理事件、資料事件或網路活動事件）、CloudTrail Insights 事件、 AWS Config 組態項目或外部事件 AWS。每個事件資料存放區類型只能包含特定事件類別（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) | Description |
| --- | --- | --- |
| CloudTrail 事件 | `Management`<br>`Data`<br>`NetworkActivity` | 此事件資料存放區類型可以收集 CloudTrail 管理事件、資料事件和網路活動事件。如需詳細資訊，請參閱為 CloudTrail 事件建立事件資料存放區。 |
| CloudTrail Insights 事件 | `Insight` | 此事件資料存放區類型可以收集 CloudTrail Insights 事件。若要接收 Insights 事件，您需要一個記錄 CloudTrail 管理事件並啟用 Insights 的來源事件資料存放區。如需有關建立來源和目的地事件資料存放區的資訊，請參閱為 CloudTrail Insights 事件建立一個事件資料存放區。 |
| 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 外部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 在 CloudTrail Lake 中彙總證據的詳細資訊，請參閱 AWS Audit Manager 使用者指南中的了解證據搜尋工具如何與 CloudTrail Lake 搭配運作。

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 Lake 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
- 使用 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
- 了解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 主控台來建立、更新、刪除和還原事件資料存放區。

您可以使用 CloudTrail 主控台更新下列設定：

- 您可以將定價選項從七年保留定價變更為一年可延長保留定價。
- 您可以更新事件資料存放區的保留期間。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。
- 您可以將多區域事件資料存放區轉換為單一區域事件資料存放區，或將單一區域事件資料存放區轉換為多區域事件資料存放區。
- AWS Organizations 組織的管理帳戶可以將帳戶層級事件資料存放區轉換為組織事件資料存放區，也可以將組織事件資料存放區轉換為帳戶層級事件資料存放區。此設定不適用於收集 外部事件的事件資料存放區 AWS。
- 您可以啟用或停用 Lake 查詢聯合。聯合事件資料存放區可讓您從 Amazon Athena 查詢事件資料。
- 您可以新增或編輯事件資料存放區的資源型政策，以提供事件資料存放區的跨帳戶存取權。如需詳細資訊，請參閱事件資料存放區的資源型政策範例。
- 您可以在收集管理事件、資料事件或 AWS Config 組態項目的事件資料存放區上停止事件擷取並重新啟動事件擷取。
- 您可以啟用或停用終止保護。啟用終止保護可防止意外刪除事件資料存放區。預設會啟用終止保護。
- 您可以還原待刪除的事件資料存放區。
- 您可以新增或移除標籤。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。
- 您可以新增 KMS 金鑰來加密事件資料存放區。您無法從事件資料存放區移除 KMS 金鑰。

使用 CloudTrail 主控台建立或更新事件資料存放區可提供下列優點：

- 如果您要設定事件資料存放區來收集資料事件，則使用 CloudTrail 主控台可讓您檢視可用的資料事件資源類型。如需詳細資訊，請參閱記錄資料事件。

- 如果您要設定事件資料存放區來收集網路活動事件，則使用 CloudTrail 主控台可讓您檢視可記錄網路活動事件的事件來源。如需詳細資訊，請參閱記錄網路活動事件。
- 如果您要設定事件資料存放區以收集外部的事件 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 外部的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
- 使用主控台建立 Insights 事件的事件資料存放區
- 使用主控台為組態項目建立事件資料存放區
- AWS 使用 主控台為 外部的事件建立事件資料存放區
- 使用主控台更新事件資料存放區
- 使用主控台停止和啟動事件擷取
- 使用 主控台變更終止保護
- 使用主控台刪除事件資料存放區
- 使用主控台還原事件資料存放區
- 從 CloudTrail Lake Event Data Store 匯出資料至 CloudWatch


## 使用主控台為 CloudTrail 事件建立事件資料存放區

CloudTrail 事件的事件資料存放區可以包含 CloudTrail 管理事件、資料事件和網路活動事件。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 Lake 成本。

若要為 CloudTrail 事件建立事件資料存放區

使用此程序建立記錄 CloudTrail 管理事件、資料事件或網路活動事件的事件資料存放區。

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。

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 Lake 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。在 366 天之後，延長保留將依用量計費定價。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 會透過檢查事件的 `eventTime` 是否在指定保留期以內，決定是否要保留該事件。例如，如果您指定的保留期為 90 天，CloudTrail 將移除 `eventTime` 早於 90 天的事件。

   > **Note**
   >
   > 如果您要將追蹤事件複製到此事件資料存放區，CloudTrail 不會複製 `eventTime` 早於指定保留期的事件。若要決定適當的保留期，請加總您要複製的最舊事件所經歷的天數與要在事件資料存放區中保留事件的天數 (保留期 = *#########* + *####*)。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）若要使用 啟用加密 AWS Key Management Service，請選擇使用我自己的 AWS KMS key。選擇新增以為您 AWS KMS key 建立 ，或選擇現有以使用現有的 KMS 金鑰。在 Enter KMS alias (輸入 KMS 別名) 中，指定別名，格式為 `alias/`*`MyAliasName`*。使用您自己的 KMS 金鑰需要您編輯 KMS 金鑰政策，以允許加密和解密您的事件資料存放區。如需詳細資訊，請參閱設定

CloudTrail 的 AWS KMS 金鑰政策。CloudTrail 也支援 AWS KMS 多區域金鑰。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 AWS KMS 的成本。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**
>
> 若要啟用組織事件資料存放區的 AWS Key Management Service 加密，您必須使用管理帳戶的現有 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 Data Catalog 中的資料表中繼資料可讓 Athena 查詢引擎了解如何尋找、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 會自動建立具有必要許可的角色。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）選擇啟用資源政策，將資源型政策新增至您的事件資料存放區。以資源為基礎的政策可讓您控制哪些委託人可以在事件資料存放區上執行動作。例如，您可以新增資源型政策，允許其他帳戶中的根使用者查詢此事件資料存放區並檢視查詢結果。如需範例政策，請參閱 事件資料存放區的資源型政策範例。

   以資源為基礎的政策包含一或多個陳述式。政策中的每個陳述式都會定義允許或拒絕存取事件資料存放區的委託人，以及委託人可以對事件資料存放區資源執行的動作。

   事件資料存放區的資源型政策支援下列動作：

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`

- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

對於組織事件資料存放區，CloudTrail 會建立預設資源型政策，列出允許委派管理員帳戶在組織事件資料存放區上執行的動作。此政策中的許可衍生自 中的委派管理員許可 AWS Organizations。此政策會在組織事件資料存放區或組織變更後自動更新 （ 例如，CloudTrail 委派管理員帳戶已註冊或移除 ）。

10. (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。如需如何在 中使用標籤的詳細資訊 AWS，請參閱《標記 AWS 資源使用者指南》中的標記 AWS 資源。
11. 選擇 Next (下一步) 以設定事件資料存放區。
12. 在選擇事件頁面上，選擇 AWS 事件，然後選擇 CloudTrail 事件。
13. 針對 CloudTrail events (CloudTrail 事件)，請至少選擇一種事件類型。根據預設，管理事件已選取。您可以將管理事件、資料事件和網路活動事件新增至事件資料存放區。
14. (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。
15. 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。

16. 展開其他設定以選擇您希望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 AWS 區域，然後選擇事件資料存放區是否擷取事件。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。

17. 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. 選擇簡易事件集合或進階事件集合：

       - 如果您想要記錄所有事件、僅記錄讀取事件或僅記錄寫入事件，請選擇簡易事件收集。您也可以選擇排除 AWS Key Management Service 和 Amazon RDS Data API 事件。
       - 如果您想要根據進階事件選取器欄位的值包含或排除管理事件，包括 、、、 和 欄位，請選擇進階事件集合。 `eventName` `eventType` `eventSource` `sessionCredentialFromConsole` `userIdentity.arn`

    b. 如果您選取簡易事件集合，請選擇是否要記錄所有事件、僅記錄讀取事件，或僅記錄寫入事件。您也可以選擇排除 AWS KMS 和 Amazon RDS Data API 事件。

    c. 如果您選取進階事件集合，請進行下列選擇：

       i. 在日誌選取器範本中，選擇預先定義的範本，或自訂以根據進階事件選取器欄位值建置自訂組態。

          您可以從下列預先定義的範本中選擇：

          - 記錄所有事件：選擇此範本記錄所有事件。
          - 僅記錄讀取事件 – 選擇此範本以僅記錄讀取事件。唯讀事件是不會變更資源狀態的事件，例如 `Get*`或 `Describe*`事件。
          - 僅記錄寫入事件 – 選擇此範本僅記錄寫入事件。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。
          - 僅記錄 AWS 管理主控台 事件 – 選擇此範本僅記錄源自 的事件 AWS 管理主控台。
          - 排除 AWS 服務 啟動的事件 – 選擇此範本以排除具有 `eventType`之 AWS 服務 的事件`AwsServiceEvent`，以及使用連結角色 (SLRs) AWS 服務啟動的事件。

       ii. (選用) 在選取器名稱中，輸入用於識別選取器的名稱。選擇器名稱是進階事件選擇器的描述性名稱，例如「從 AWS 管理主控台 工作階段記錄管理事件」。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。

       iii. 如果您選擇自訂，在進階事件選取器中，會根據進階事件選取器欄位值建立表達式。

> **Note**
>
> 選取器不支援使用萬用字元，例如 * 。若要將多個值與單一條件比對，您可以使用 StartsWith、NotStartsWith、 EndsWith或 NotEndsWith來明確比對事件欄位的開頭或結尾。

A. 從下列欄位選取。

- **readOnly** – readOnly可設定為等於 true或 的值false。設定為 時false，事件資料存放區會記錄唯讀管理事件。唯讀管理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。若要同時記錄讀取和寫入事件，請勿新增readOnly選取器。
- **eventName** – eventName 可以使用任何運算子。您可以使用它來包含或排除任何管理事件，例如 CreateAccessPoint或 GetAccessPoint。
- **userIdentity.arn** – 包含或排除特定 IAM 身分所採取動作的事件。如需更多詳細資訊，請參閱 CloudTrail userIdentity 元素。
- **sessionCredentialFromConsole** – 包含或排除源自 AWS 管理主控台 工作階段的事件。此欄位可以設定為等於或不等於 的值true。
- **eventSource** – 您可以使用它來包含或排除特定事件來源。eventSource 通常是簡短形式的服務名稱，不含空格加 .amazonaws.com。例如，您可以將eventSource等於 設定為僅ec2.amazonaws.com記錄 Amazon EC2 管理事件。
- **eventType** – 要包含或排除的 eventType。例如，您可以將此欄位設定為不等於AwsServiceEvent排除AWS 服務 事件。

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。

如需有關 CloudTrail 如何評估多個條件的資訊，請參閱 CloudTrail 如何評估欄位的多項條件。

> **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。

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

d. 選擇啟用 Insights 事件擷取以啟用 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. 選擇將記錄 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。

18. 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. 選擇資源類型。這是記錄資料事件的 AWS 服務 和資源。

b. 在日誌選取器範本中，選擇預先定義的範本，或選擇自訂，根據進階事件選取器欄位的值定義您自己的事件收集條件。

您可以從下列預先定義的範本中選擇：

- 記錄所有事件：選擇此範本記錄所有事件。
- 僅記錄讀取事件 – 選擇此範本以僅記錄讀取事件。唯讀事件是不會變更資源狀態的事件，例如 `Get*`或 `Describe*`事件。
- 僅記錄寫入事件 – 選擇此範本僅記錄寫入事件。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。
- 僅記錄 AWS 管理主控台 事件 – 選擇此範本僅記錄源自 的事件 AWS 管理主控台。
- 排除 AWS 服務 啟動的事件 – 選擇此範本以排除具有 `eventType`之 AWS 服務 的事件`AwsServiceEvent`，以及使用連結角色 (SLRs) AWS 服務啟動的事件。

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. 如果您選取自訂，在進階事件選取器中會根據進階事件選取器欄位的值來建置表達式。

> **Note**
>
> 選取器不支援使用萬用字元，例如 * 。若要將多個值與單一條件比對，您可以使用 StartsWith、NotStartsWith、 EndsWith或 NotEndsWith來明確比對事件欄位的開頭或結尾。

i. 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任何記錄到 CloudTrail 的資料事件，例如 PutBucket、GetItem 或 GetSnapshotBlock。
- **eventSource** – 要包含或排除的事件來源。此欄位可以使用任何運算子。
- eventType – 要納入或排除的事件類型。例如，您可以將此欄位設定為不等於AwsServiceEvent排除 AWS 服務 事件。如需事件類型的清單，請參閱 eventType中的 CloudTrail 記錄管理、資料和網路活動事件的內容。
- sessionCredentialFromConsole – 包含或排除源自 AWS 管理主控台 工作階段的事件。此欄位可以設定為等於或不等於 的值true。
- userIdentity.arn – 針對特定 IAM 身分執行的動作納入或排除事件。如需更多詳細資訊，請參閱 CloudTrail userIdentity 元素。
- **resources.ARN** - 您可以將任何運算子與 搭配使用resources.ARN，但如果您使用等於或不等於，則值必須完全符合您在範本中指定之類型之有效資源的 ARN，做為的值resources.type。

> **Note**
>
> 您無法使用 resources.ARN 欄位來篩選沒有 ARNs的資源類型。

如需資料事件資源 ARN 格式的詳細資訊，請參閱《服務授權參考》中的 的動作、資源和條件索引鍵 AWS 服務。

ii. 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，若要從記錄於事件資料存放區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，設定 的運算子不會以 開頭，然後貼入您不想記錄事件的 S3 儲存貯體 ARN。

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。

如需有關 CloudTrail 如何評估多個條件的資訊，請參閱 CloudTrail 如何評估欄位的多項條件。

> **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。

iii. 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。

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. 若要新增要記錄資料事件的其他資源類型，請選擇新增資料事件類型。透過此步驟重複步驟 a，為資源類型設定進階事件選取器。

19. 若要在您的事件資料存放區中包含網路活動事件，請執行下列動作。

a. 從網路活動事件來源中，選擇網路活動事件的來源。

b. 在日誌選取器範本中，選擇範本。您可以選擇記錄所有網路活動事件、記錄所有網路活動存取遭拒的事件，或選擇自訂以建置自訂日誌選取器來篩選多個欄位，例如 `eventName`和 `vpcEndpointId`。

c. （選用）輸入名稱以識別選取器。選擇器名稱在進階事件選擇器中列為名稱，如果您展開 JSON 檢視，則可檢視。

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。如果您使用預先定義的日誌範本，則可略過此步驟。

i. 對於排除或包含網路活動事件，您可以在 主控台中選擇下列欄位。

- **eventName** – 您可以將任何運算子與 搭配使用eventName。您可以使用它來包含或排除任何事件，例如 CreateKey。
- **errorCode** – 您可以使用它來篩選錯誤碼。目前，唯一支援的errorCode是VpceAccessDenied。
- **vpcEndpointId** – 識別操作通過的 VPC 端點。您可以搭配 使用任何運算子vpcEndpointId。

ii. 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。

iii. 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。

e. 若要新增要記錄網路活動事件的其他事件來源，請選擇新增網路活動事件選取器。

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

20. 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 只會複製包含在 S3 儲存貯體CloudTrail字首和CloudTrail字首內的字首中的 CloudTrail 事件，而不會檢查其他服務的字首 AWS 。如果您要複製其他字首中包含的 CloudTrail 事件，請選擇 Enter S3 URI (輸入 S3 URI)，然後選擇 Browse S3 (瀏覽 S3) 以瀏覽至字首。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 金鑰政策允許 CloudTrail 解密資料。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。

b. 選擇複製事件的時間範圍。CloudTrail 會在嘗試複製追蹤事件之前檢查字首和日誌檔案名稱，以確認名稱包含介於所選開始日期和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 只會複製 eventTime 在事件資料存放區保留期內的追蹤事件。例如，如果事件資料存放區的保留期為 90 天，則 CloudTrail 將不會複製 eventTime 早於 90 天的任何追蹤事件。

- 如果選擇相對範圍，您可以選擇複製過去 6 個月、1 年、2 年、7 年或自訂範圍內記錄的事件。CloudTrail 會複製所選時段內記錄的事件。
- 如果選擇 Absolute range (絕對範圍)，您可以選擇特定的開始和結束日期。CloudTrail 會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。對於 Enter IAM role name (輸入 IAM 角色名稱)，請輸入角色的名稱。CloudTrail 會自動為此新角色建立必要的許可。
- 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。

21. 選擇下一步，透過新增資源標籤索引鍵和 IAM 全域條件索引鍵來豐富您的事件。
22. 在富集事件中，新增最多 50 個資源標籤金鑰和 50 個 IAM 全域條件金鑰，以提供事件的其他中繼資料。這可協助您分類和分組相關事件。

    如果您新增資源標籤索引鍵，CloudTrail 將包含與 API 呼叫中所涉及資源相關聯的所選標籤索引鍵。與已刪除資源相關的 API 事件將不會有資源標籤。

    如果您新增 IAM 全域條件金鑰，CloudTrail 將包含授權程序期間評估之所選條件金鑰的相關資訊，包括委託人、工作階段、網路和請求本身的其他詳細資訊。

    資源標籤索引鍵和 IAM 全域條件索引鍵的相關資訊會顯示在事件的 `eventContext` 欄位中。如需詳細資訊，請參閱透過新增資源標籤索引鍵和 IAM 全域條件索引鍵來豐富 CloudTrail 事件。

    > **Note**
    >
    > 如果事件包含不屬於事件區域的資源，CloudTrail 將不會填入此資源的標籤，因為標籤擷取僅限於事件區域。

23. 選擇展開事件大小，將事件承載從 256 KB 擴展至 1 MB。當您新增資源標籤金鑰或 IAM 全域條件金鑰時，此選項會自動啟用，以確保所有新增的金鑰都包含在事件中。

擴展事件大小有助於分析和疑難排解事件，因為它可讓您查看下列欄位的完整內容，只要事件承載小於 1 MB：

- annotation
- requestID
- additionalEventData
- serviceEventDetails
- userAgent
- errorCode
- responseElements
- requestParameters
- errorMessage

如需這些欄位的詳細資訊，請參閱 CloudTrail 記錄內容。

24. 選擇 Next (下一步) 以檢閱您的選項。
25. 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)。
26. 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 使用 CloudTrail 主控台建立或編輯查詢。

您也可以檢視受管儀表板，或建立自訂儀表板以視覺化事件趨勢。如需有關 Lake 儀表板的詳細資訊，請參閱 CloudTrail Lake 儀表板。

## 使用主控台建立 Insights 事件的事件資料存放區

AWS CloudTrail Insights 透過持續分析 CloudTrail 管理事件，協助 AWS 使用者識別和回應與 API 呼叫率和 API 錯誤率相關的異常活動。CloudTrail Insights 會分析 API 呼叫率和 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產生 Insights 事件。系統會針對write管

理 APIs 產生 API 呼叫率上的 Insights 事件，並針對 `readwrite`和管理 APIs 產生 API 錯誤率上的 Insights 事件。

若要在 CloudTrail Lake 中記錄 Insights 事件，您需要會記錄 Insights 事件的目的地事件資料存放區和啟用 Insights 和日誌管理事件的來源事件資料存放區。

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

如果您已在來源事件資料存放區上啟用 CloudTrail Insights，而且 CloudTrail 偵測到異常活動，CloudTrail 會傳遞 Insights 事件至您的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的事件不同，只有在 CloudTrail 偵測到帳戶 API 使用方式與帳戶的一般使用模式有很大差異時，才會加以記錄。

在事件資料存放區上第一次啟用 CloudTrail Insights 之後，CloudTrail 最多可能需要 7 天才能開始交付 Insights 事件，前提是在此期間偵測到異常活動。

CloudTrail Insights 會分析事件資料存放區在每個區域中發生的管理事件，並在偵測到異常活動偏離基準時產生 Insights 事件。CloudTrail Insights 事件會在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，CloudTrail Insights 會分析組織中每個區域每個成員帳戶的管理事件，並在偵測到異常活動偏離帳戶和區域的基準時產生 Insights 事件。

擷取 CloudTrail Lake 中的 Insights 事件需支付額外費用。如果您同時為追蹤和 CloudTrail Lake 事件資料存放區啟用 Insights，則將分別支付它們的費用。如需有關 CloudTrail 定價的資訊，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. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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 Lake 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。在 366 天之後，延長保留將依用量計費定價。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. （選用）若要使用 啟用加密 AWS Key Management Service，請選擇使用我自己的 AWS KMS key。選擇新增以為您 AWS KMS key 建立 ，或選擇現有以使用現有的 KMS 金鑰。在 Enter KMS alias (輸入 KMS 別名) 中，指定別名，格式為 `alias/MyAliasName`。使用您自己的 KMS 金鑰需要您編輯 KMS 金鑰政策，以允許加密和解密您的事件資料存放區。如需詳細資訊，請參閱設定 CloudTrail 的 AWS KMS 金鑰政策。CloudTrail 也支援 AWS KMS 多區域金鑰。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 AWS KMS 的成本。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**
>
> 若要啟用組織事件資料存放區的 AWS Key Management Service 加密，您必須使用管理帳戶的現有 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 Data Catalog 中的資料表中繼資料可讓 Athena 查詢引擎了解如何尋找、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 會自動建立具有必要許可的角色。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）選擇啟用資源政策，將資源型政策新增至您的事件資料存放區。以資源為基礎的政策可讓您控制哪些委託人可以在事件資料存放區上執行動作。例如，您可以新增資源型政策，允許其他帳戶中的根使用者查詢此事件資料存放區並檢視查詢結果。如需範例政策，請參閱 事件資料存放區的資源型政策範例。

   以資源為基礎的政策包含一或多個陳述式。政策中的每個陳述式都會定義允許或拒絕存取事件資料存放區的委託人，以及委託人可以對事件資料存放區資源執行的動作。

   事件資料存放區的資源型政策支援下列動作：

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`
   - `cloudtrail:GetQueryResults`
   - `cloudtrail:GenerateQuery`
   - `cloudtrail:GenerateQueryResultsSummary`
   - `cloudtrail:GetEventDataStore`

對於組織事件資料存放區，CloudTrail 會建立預設資源型政策，列出允許委派管理員帳戶在組織事件資料存放區上執行的動作。此政策中的許可衍生自 中的委派管理員許可 AWS Organizations。此政策會在組織事件資料存放區或組織變更後自動更新 （ 例如，CloudTrail 委派管理員帳戶已註冊或移除 ）。

10. (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。如需如何在 中使用標籤的詳細資訊 AWS，請參閱《標記 AWS 資源使用者指南》中的標記 AWS 資源。
11. 選擇 Next (下一步) 以設定事件資料存放區。
12. 在選擇事件頁面上，選擇 AWS 事件，然後選擇 CloudTrail Insights 事件。
13. 在 CloudTrail Insights 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。只有在您使用 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。
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。

17. 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. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
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 Lake 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。在 366 天之後，延長保留將依用量計費定價。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 會透過檢查事件的 `eventTime` 是否在指定保留期以內，決定是否要保留該事件。例如，如果您指定的保留期為 90 天，CloudTrail 將移除 `eventTime` 早於 90 天的事件。
7. （選用）若要使用 啟用加密 AWS Key Management Service，請選擇使用我自己的 AWS KMS key。選擇新增以為您 AWS KMS key 建立 ，或選擇現有以使用現有的 KMS 金鑰。在 Enter KMS alias (輸入 KMS 別名) 中，指定別名，格式為 `alias/`*`MyAliasName`*。使用您自己的 KMS 金鑰需要您編輯 KMS 金鑰政策，以允許加密和解密您的事件資料存放區。如需詳細資訊，請參閱設定

CloudTrail 的 AWS KMS 金鑰政策。CloudTrail 也支援 AWS KMS 多區域金鑰。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 AWS KMS 的成本。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**
>
> 若要啟用組織事件資料存放區的 AWS Key Management Service 加密，您必須使用管理帳戶的現有 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 Data Catalog 中的資料表中繼資料可讓 Athena 查詢引擎知道如何尋找、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 會自動建立具有必要許可的角色。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）選擇啟用資源政策，將資源型政策新增至您的事件資料存放區。以資源為基礎的政策可讓您控制哪些主體可以在事件資料存放區上執行動作。例如，您可以新增資源型政策，允許其他帳戶中的根使用者查詢此事件資料存放區並檢視查詢結果。如需範例政策，請參閱 事件資料存放區的資源型政策範例。

   以資源為基礎的政策包含一或多個陳述式。政策中的每個陳述式都會定義允許或拒絕存取事件資料存放區的委託人，以及委託人可以對事件資料存放區資源執行的動作。

   事件資料存放區的資源型政策支援下列動作：

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`

- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

對於組織事件資料存放區，CloudTrail 會建立預設資源型政策，列出允許委派管理員帳戶在組織事件資料存放區上執行的動作。此政策中的許可衍生自 中的委派管理員許可 AWS Organizations。此政策會在組織事件資料存放區或組織變更後自動更新 （例如，CloudTrail 委派管理員帳戶已註冊或移除）。

10. (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。如需如何在 中使用標籤的詳細資訊 AWS，請參閱《標記 AWS 資源使用者指南》中的標記 AWS 資源。
11. 選擇 Next (下一步) 以設定事件資料存放區。
12. 在選擇事件頁面上，選擇 AWS 事件，然後選擇 CloudTrail 事件。
13. 在 CloudTrail 事件中，維持選取管理事件。
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，才能建立會啟用 Insights 的事件資料存放區。
15. 展開其他設定，選擇您希望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 AWS 區域，然後選擇事件資料存放區是否擷取事件。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。
16. 選擇簡易事件集合或進階事件集合：
    - 如果您想要記錄所有事件、僅記錄讀取事件或僅記錄寫入事件，請選擇簡易事件收集。您也可以選擇排除 AWS Key Management Service 和 Amazon RDS Data API 事件。
    - 如果您想要根據進階事件選取器欄位的值包含或排除管理事件，包括 、、、 和 欄位，請選擇進階事件集合。 `eventName` `eventType` `eventSource` `sessionCredentialFromConsole` `userIdentity.arn`

17. 如果您選取簡易事件集合，請選擇是否要記錄所有事件、僅記錄讀取事件，或僅記錄寫入事件。您也可以選擇排除 AWS KMS 和 Amazon RDS Data API 事件。
18. 如果您選取進階事件集合，請進行下列選擇：

    a. 在日誌選取器範本中，選擇預先定義的範本，或選擇自訂，根據進階事件選取器欄位的值來撰寫您自己的事件收集條件。

       您可以從下列預先定義的範本中選擇：

       - 記錄所有事件：選擇此範本記錄所有事件。
       - 僅記錄讀取事件 – 選擇此範本以僅記錄讀取事件。唯讀事件是不會變更資源狀態的事件，例如 `Get*`或 `Describe*`事件。
       - 僅記錄寫入事件 – 選擇此範本以僅記錄寫入事件。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。
       - 僅記錄 AWS 管理主控台 事件 – 選擇此範本僅記錄源自 的事件 AWS 管理主控台。
       - 排除 AWS 服務 啟動的事件 – 選擇此範本以排除具有 `eventType`之 AWS 服務 的事件`AwsServiceEvent`，以及使用連結角色 (SLRs) AWS 服務啟動的事件。

    b. (選用) 在選取器名稱中，輸入用於識別選取器的名稱。選擇器名稱是進階事件選擇器的描述性名稱，例如「從 AWS 管理主控台 工作階段記錄管理事件」。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。

    c. 如果您選擇自訂，在進階事件選取器中會根據進階事件選取器欄位值建立表達式。

       > **Note**
       >
       > 選取器不支援使用萬用字元，例如 `*` 。若要以單一條件比對多個值，您可以使用 `StartsWith`、`NotStartsWith`、 `EndsWith`或 `NotEndsWith`來明確比對事件欄位的開頭或結尾。

       i. 從下列欄位選取。

          - **`readOnly`** – `readOnly`可設定為等於 `true`或 的值`false`。設定為 時`false`，事件資料存放區會記錄唯讀管理事件。唯讀管理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。若要同時記錄讀取和寫入事件，請勿新增`readOnly`選取器。

- **eventName** – eventName 可以使用任何運算子。您可以使用它來包含或排除任何管理事件，例如 CreateAccessPoint或 GetAccessPoint。
- **userIdentity.arn** – 包含或排除特定 IAM 身分所採取動作的事件。如需更多詳細資訊，請參閱 CloudTrail userIdentity 元素。
- **sessionCredentialFromConsole** – 包含或排除源自 AWS 管理主控台 工作階段的事件。此欄位可以設定為等於或不等於 的值true。
- **eventSource** – 您可以使用它來包含或排除特定事件來源。eventSource 通常是簡短形式的服務名稱，不含空格加 .amazonaws.com。例如，您可以將eventSource等於 設定為僅ec2.amazonaws.com記錄 Amazon EC2 管理事件。
- **eventType** – 要包含或排除的 eventType。例如，您可以將此欄位設定為不等於AwsServiceEvent排除AWS 服務 事件。

ii. 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。

如需有關 CloudTrail 如何評估多個條件的資訊，請參閱 CloudTrail 如何評估欄位的多項條件。

> **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。

iii. 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。

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

19. 選擇啟用 Insights 事件擷取。
20. 選擇將記錄 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。
21. 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。
22. 選擇下一步，透過新增資源標籤索引鍵和 IAM 全域條件索引鍵來豐富您的事件。

23. 在富集事件中，新增最多 50 個資源標籤金鑰和 50 個 IAM 全域條件金鑰，以提供事件的其他中繼資料。這可協助您分類和分組相關事件。

    如果您新增資源標籤索引鍵，CloudTrail 將包含與 API 呼叫中所涉及資源相關聯的所選標籤索引鍵。與已刪除資源相關的 API 事件將不會有資源標籤。

    如果您新增 IAM 全域條件金鑰，CloudTrail 將包含授權程序期間評估之所選條件金鑰的相關資訊，包括委託人、工作階段、網路和請求本身的其他詳細資訊。

    資源標籤索引鍵和 IAM 全域條件索引鍵的相關資訊會顯示在事件的 `eventContext` 欄位中。如需詳細資訊，請參閱透過新增資源標籤索引鍵和 IAM 全域條件索引鍵來豐富 CloudTrail 事件。

    > **Note**
    >
    > 如果事件包含不屬於事件區域的資源，CloudTrail 將不會填入此資源的標籤，因為標籤擷取僅限於事件區域。

24. 選擇展開事件大小，將事件承載從 256 KB 擴展到 1 MB。當您新增資源標籤金鑰或 IAM 全域條件金鑰時，此選項會自動啟用，以確保所有新增的金鑰都包含在事件中。

    擴展事件大小有助於分析和疑難排解事件，因為它可讓您查看下列欄位的完整內容，只要事件承載小於 1 MB：

    - `annotation`
    - `requestID`
    - `additionalEventData`
    - `serviceEventDetails`
    - `userAgent`
    - `errorCode`
    - `responseElements`
    - `requestParameters`
    - `errorMessage`

    如需這些欄位的詳細資訊，請參閱 CloudTrail 記錄內容。

25. 選擇 Next (下一步) 以檢閱您的選項。

26. 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)。
27. 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。在您第一次在來源事件資料存放區上啟用 CloudTrail Insights 之後，CloudTrail 最多可能需要 7 天才能開始交付 Insights 事件，前提是在此期間偵測到異常活動。

    您可以檢視 CloudTrail Lake 儀表板，對目的地事件資料存放區內的 Insights 事件進行視覺化呈現。如需有關 Lake 儀表板的詳細資訊，請參閱 CloudTrail Lake 儀表板。

擷取 CloudTrail Lake 中的 Insights 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。如需有關 CloudTrail 定價的資訊，請參閱 AWS CloudTrail 定價。

## 使用主控台為組態項目建立事件資料存放區

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。組態項目代表存在於您帳戶中的支援 AWS 資源屬性point-in-time檢視。 會在偵測到正在記錄的資源類型變更時 AWS Config 建立組態項目。 AWS Config 也會在擷取組態快照時建立組態項目。

您可以使用 AWS Config 和 CloudTrail Lake 對組態項目執行查詢。您可以使用 根據單一 AWS 帳戶 和或跨多個帳戶和區域的組態屬性 AWS 區域， AWS Config 來查詢 AWS 資源的目前組態狀態。相比之下，您可以使用 CloudTrail Lake 來跨各種資料來源進行查詢，例如 CloudTrail 事件、組態項目和規則評估。CloudTrail Lake 查詢涵蓋所有 AWS Config 組態項目，包括資源組態和合規歷史記錄。

為組態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。您可以使用 繼續執行進階查詢 AWS Config，並繼續將歷史記錄檔案 AWS Config 交付至 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 Lake 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

先決條件

建立事件資料存放區之前，請先為所有帳戶和區域設定 AWS Config 記錄。您可以使用 Quick Setup 功能 AWS Systems Manager，快速建立採用 技術的組態記錄器 AWS Config。

> **Note**
>
> AWS Config 開始記錄組態時，需支付服務費用。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 AWS Config 您要用來評估所記錄資源類型合規資訊的規則。的數個 CloudTrail Lake 範例查詢 AWS Config 需要 AWS Config 規則 評估 AWS 資源的合規狀態。如需詳細資訊 AWS Config 規則，請參閱《 AWS Config 開發人員指南》中的使用 評估資源 AWS Config 規則。

若要為組態項目建立事件資料存放區

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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 Lake 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。在 366 天之後，延長保留將依用量計費定價。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 會透過檢查事件的 `eventTime` 是否在指定保留期以內，決定是否要保留該事件。例如，如果您指定的保留期為 90 天，CloudTrail 將移除 `eventTime` 早於 90 天的事件。

7. （選用）若要使用 啟用加密 AWS Key Management Service，請選擇使用我自己的 AWS KMS key。選擇新增以為您 AWS KMS key 建立 ，或選擇現有以使用現有的 KMS 金鑰。在 Enter KMS alias (輸入 KMS 別名) 中，指定別名，格式為 `alias/`*`MyAliasName`*。使用您自己的 KMS 金鑰需要您編輯 KMS 金鑰政策，以允許加密和解密您的事件資料存放區。如需詳細資訊，請參閱設定 CloudTrail 的 AWS KMS 金鑰政策。CloudTrail 也支援 AWS KMS 多區域金鑰。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 AWS KMS 的成本。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**
   >
   > 若要啟用組織事件資料存放區的 AWS Key Management Service 加密，您必須使用管理帳戶的現有 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 Data Catalog 中的資料表中繼資料可讓 Athena 查詢引擎知道如何尋找、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 會自動建立具有必要許可的角色。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）選擇啟用資源政策，將資源型政策新增至您的事件資料存放區。以資源為基礎的政策可讓您控制哪些主體可以在事件資料存放區上執行動作。例如，您可以新增資源型政策，允許其他帳戶中的根使用者查詢此事件資料存放區並檢視查詢結果。如需範例政策，請參閱 事件資料存放區的資源型政策範例。

   以資源為基礎的政策包含一或多個陳述式。政策中的每個陳述式都會定義允許或拒絕存取事件資料存放區的委託人，以及委託人可以對事件資料存放區資源執行的動作。

   事件資料存放區的資源型政策支援下列動作：

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`
   - `cloudtrail:GetQueryResults`
   - `cloudtrail:GenerateQuery`
   - `cloudtrail:GenerateQueryResultsSummary`
   - `cloudtrail:GetEventDataStore`

   對於組織事件資料存放區，CloudTrail 會建立預設資源型政策，列出允許委派管理員帳戶在組織事件資料存放區上執行的動作。此政策中的許可衍生自 中的委派管理員許可 AWS Organizations。此政策會在組織事件資料存放區或組織變更後自動更新（例如，CloudTrail 委派管理員帳戶已註冊或移除）。

10. (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。如需如何在 中使用標籤的詳細資訊 AWS，請參閱《標記 AWS 資源使用者指南》中的標記 AWS 資源。

11. 選擇下一步。

12. 在選擇事件頁面上，選擇 AWS 事件，然後選擇組態項目。

13. CloudTrail 會將事件資料存放區資源儲存在您建立該資源的區域中，但在預設情況下，資料存放區中收集的組態項目來自已啟用記錄的帳戶中的所有區域。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。
14. 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。
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。

    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。

### 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。`eventData` 的內容由您的組態項目提供；其他欄位則在擷取後由 CloudTrail 提供。

CloudTrail 記錄管理、資料和網路活動事件的內容 將詳細說明 CloudTrail 事件記錄內容。

- 擷取後由 CloudTrail 提供的欄位
- 您的事件提供的欄位

#### 擷取後由 CloudTrail 提供的欄位

| 欄位名稱 | 輸入類型 | 需求 | Description |
| --- | --- | --- | --- |
| 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 |

| 欄位名稱 | 輸入類型 | 需求 | Description |
| --- | --- | --- | --- |
| | | | 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 | 要指派事件 AWS 區域的 。 |
| recipientAccountId | string | 必要 | 代表收到此事件的 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 | Description |
| --- | --- | --- | --- |
| eventData | - | 必要 | eventData 中的欄位由您的組態項目提供。 |

| 欄位名稱 | 輸入類型 | 需求 | Description |
| --- | --- | --- | --- |
| • configurationItemVersion | string | 選用 | 來自其來源的組態項目版本。 |
| • configurationItemCaptureTime | 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 | 與資源相關聯的 12 位數 AWS 帳戶 ID。 |
| • 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 參考中的 ConfigurationItem。 |
| • 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)。 |

| 欄位名稱 | 輸入類型 | 需求 | Description |
| --- | --- | --- | --- |
| • awsRegion | string | 選用 | AWS 區域 資源所在的 。 |
| • 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 AWS Config 傳回的組態屬性，以補充針對組態參數傳回的資訊。 |
| • relatedEvents | string | 選用 | CloudTrail 事件 ID 的清單。 |
| • relationships | - | 選用 | 相關 AWS 資源的清單。 |
| • • 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 外部的事件建立事件資料存放區

您可以建立事件資料存放區以包含 外部的事件 AWS，然後使用 CloudTrail Lake 來搜尋、查詢和分析從應用程式記錄的資料。

您可以使用 CloudTrail Lake 整合，從 外部記錄和存放使用者活動資料 AWS；從混合環境中的任何來源，例如內部或 SaaS 應用程式託管在內部部署或雲端、虛擬機器或容器中。

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 Lake 成本。

為 外部的事件建立事件資料存放區 AWS

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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 Lake 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。在 366 天之後，延長保留將依用量計費定價。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 會透過檢查事件的 `eventTime` 是否在指定保留期以內，決定是否要保留該事件。例如，如果您指定的保留期為 90 天，CloudTrail 將移除 `eventTime` 早於 90 天的事件。

7. （選用）若要使用 啟用加密 AWS Key Management Service，請選擇使用我自己的 AWS KMS key。選擇新增以為您 AWS KMS key 建立 ，或選擇現有以使用現有的 KMS 金鑰。在 Enter KMS alias (輸入 KMS 別名) 中，指定別名，格式為 `alias/MyAliasName`。使用您自己的 KMS 金鑰需要您編輯 KMS 金鑰政策，以允許加密和解密您的事件資料存放區。如需詳細資訊，請參閱設定 CloudTrail 的 AWS KMS 金鑰政策。CloudTrail 也支援 AWS KMS 多區域金鑰。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 AWS KMS 的成本。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**
   >
   > 若要啟用組織事件資料存放區的 AWS Key Management Service 加密，您必須使用管理帳戶的現有 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 Data Catalog 中的資料表中繼資料可讓 Athena 查詢引擎了解如何尋找、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 會自動建立具有必要許可的角色。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）選擇啟用資源政策，將資源型政策新增至您的事件資料存放區。以資源為基礎的政策可讓您控制哪些主體可以在事件資料存放區上執行動作。例如，您可以新增資源型政策，允許其他帳

戶中的根使用者查詢此事件資料存放區並檢視查詢結果。如需範例政策，請參閱 事件資料存放區的資源型政策範例。

以資源為基礎的政策包含一或多個陳述式。政策中的每個陳述式都會定義允許或拒絕存取事件資料存放區的委託人，以及委託人可以對事件資料存放區資源執行的動作。

事件資料存放區的資源型政策支援下列動作：

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

對於組織事件資料存放區，CloudTrail 會建立預設資源型政策，列出允許委派管理員帳戶在組織事件資料存放區上執行的動作。此政策中的許可衍生自 中的委派管理員許可 AWS Organizations。此政策會在組織事件資料存放區或組織變更後自動更新 （例如，CloudTrail 委派管理員帳戶已註冊或移除）。

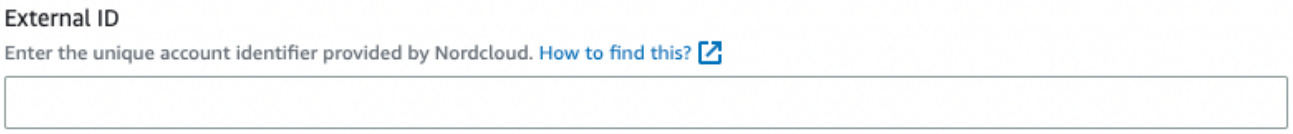
10. (選用) 在 Tags (標籤) 區段中，您最多可以新增 50 個標籤金鑰對，以協助您識別、排序和控制對事件資料存放區的存取權限。如需使用 IAM 政策，對以標籤為基礎的事件資料存放區授與存取權限的詳細資訊，請參閱範例：拒絕以標籤為基礎建立或刪除事件資料存放區的存取權限。如需如何在 中使用標籤的詳細資訊 AWS，請參閱《標記 AWS 資源使用者指南》中的標記 AWS 資源。
11. 選擇 Next (下一步) 以設定事件資料存放區。
12. 在 Choose events (選擇事件) 頁面上，選擇 Events from integrations (來自整合的事件)。
13. 從 Events 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。
14. 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。
15. 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。對於方向整合，CloudTrail 會自動新增合作夥伴 AWS 的帳戶 IDs，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，您必須指定至少一個 AWS 帳戶 ID 作為委託人，並且可以選擇輸入外部 ID 以防止混淆代理人。

> **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. 針對解決方案整合，選擇新增 AWS 帳戶以指定要新增為政策中主體的每個 AWS 帳戶 ID。

16. 選擇 Next (下一步) 以檢閱您的選項。
17. 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)。
18. 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。
19. 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在通道上呼叫 PutAuditEvents API 時，事件資料存放區就會開始透過整合的通道將合作夥伴事件擷取到 CloudTrail 中。

## 使用主控台更新事件資料存放區

本節說明如何使用 AWS 管理主控台更新事件資料存放區的設定。如需有關如何使用 更新事件資料存放區的資訊 AWS CLI，請參閱 使用 更新事件資料存放區 AWS CLI。

更新事件資料存放區

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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 Lake 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，CloudTrail 將移除 eventTime 早於新保留期的任何事件。例如，如果先前的保留期為 365 天，而您將其縮短到 100 天，則 CloudTrail 會移除 eventTime 早於 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，CloudTrail 會加密事件資料存放區中的所有事件。使用您自己的 KMS 金鑰會產生加密和解密 AWS KMS 的成本。

  > **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，請為組織中的所有帳戶選擇啟用。只有在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 CloudTrail 事件或組態項目時，才能使用此選項。

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 AWS Glue 資料目錄中檢視事件資料存放區的中繼資料，並使用 Amazon Athena 對事件資料執行 SQL 查詢。停用 Lake 查詢聯合會會停用與 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，系統不會刪除任何 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許可的角色。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. 在資源政策中，選擇編輯以新增或修改事件資料存放區的資源型政策。

   以資源為基礎的政策可讓您控制哪些主體可以在事件資料存放區上執行動作。例如，您可以新增資源型政策，允許其他帳戶中的根使用者查詢此事件資料存放區並檢視查詢結果。如需範例政策，請參閱 事件資料存放區的資源型政策範例。

以資源為基礎的政策包含一或多個陳述式。政策中的每個陳述式都會定義允許或拒絕存取事件資料存放區的委託人，以及委託人可以對事件資料存放區資源執行的動作。

事件資料存放區的資源型政策支援下列動作：

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

對於組織事件資料存放區，CloudTrail 會建立預設資源型政策，列出允許委派管理員帳戶在組織事件資料存放區上執行的動作。此政策中的許可衍生自 中的委派管理員許可 AWS Organizations。此政策會在組織事件資料存放區或組織變更後自動更新（例如，CloudTrail 委派管理員帳戶已註冊或移除）。

7. 編輯事件資料存放區事件類型特有的任何其他設定。

   CloudTrail 事件的設定

   - 若要變更事件資料存放區記錄的事件，請在 CloudTrail 事件中選擇編輯。
   - 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，請參閱更新現有事件資料存放區的管理事件設定。
   - 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源類型，然後選擇要使用的日誌選取器範本。如需詳細資訊，請參閱更新現有的事件資料存放區，以使用主控台記錄資料事件。
   - 在網路活動事件中，選擇編輯以變更網路活動事件的設定。您可以選擇要記錄的網路活動事件類型，然後選擇要使用的日誌選取器範本。如需詳細資訊，請參閱更新現有的事件資料存放區以記錄網路活動事件。
   - 在富集事件中，展開事件大小，選擇編輯以新增或移除資源標籤和 IAM 全域條件索引鍵，然後展開事件大小。

在富集事件中，新增最多 50 個資源標籤金鑰和 50 個 IAM 全域條件金鑰，以提供事件的其他中繼資料。這可協助您分類和分組相關事件。

如果您新增資源標籤金鑰，CloudTrail 將包含與 API 呼叫中所涉及資源相關聯的所選標籤金鑰。與已刪除資源相關的 API 事件將不會有資源標籤。

如果您新增 IAM 全域條件金鑰，CloudTrail 將包含授權程序期間評估之所選條件金鑰的相關資訊，包括委託人、工作階段、網路和請求本身的其他詳細資訊。

資源標籤索引鍵和 IAM 全域條件索引鍵的相關資訊會顯示在事件的 `eventContext` 欄位中。如需詳細資訊，請參閱[透過新增資源標籤索引鍵和 IAM 全域條件索引鍵來豐富 CloudTrail 事件]。

> **Note**
>
> 如果事件包含不屬於事件區域的資源，CloudTrail 將不會填入此資源的標籤，因為標籤擷取僅限於事件區域。

選擇展開事件大小，將事件承載從 256 KB 擴展到 1 MB。當您新增資源標籤金鑰或 IAM 全域條件金鑰時，此選項會自動啟用，以確保所有新增的金鑰都包含在事件中。

擴展事件大小有助於分析和疑難排解事件，因為它可讓您查看下列欄位的完整內容，只要事件承載小於 1 MB：

- `annotation`
- `requestID`
- `additionalEventData`
- `serviceEventDetails`
- `userAgent`
- `errorCode`
- `responseElements`
- `requestParameters`
- `errorMessage`

如需這些欄位的詳細資訊，請參閱 CloudTrail 記錄內容。

完成後，請選擇儲存變更。

整合事件的設定

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 使用主控台建立與 CloudTrail 合作夥伴的整合。

8. 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。

## 使用主控台停止和啟動事件擷取

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 APIs 來停止事件資料存放區擷取事件。

開始擷取和停止擷取的選項僅適用於包含 CloudTrail 事件 （管理事件、資料事件和網路活動事件） 或 AWS Config 組態項目的事件資料存放區。

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 （如果只包含 CloudTrail 事件）。

若要使事件資料存放區停止擷取事件

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
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會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 管理主控台 AWS CLI或 API 操作來停用終止保護。

關閉終止保護

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
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. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
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 CloudTrail 主控台刪除事件資料存放區。如需如何使用 刪除事件資料存放區的資訊 AWS CLI，請參閱 使用 刪除事件資料存放區 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 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。如需詳細資訊，請參閱刪除頻道以刪除與 的整合 AWS CLI

刪除事件資料存放區

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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。待刪除的事件資料存放區會計入一個 中可能存在的事件資料存放區的配額 AWS 區域。

## 使用主控台還原事件資料存放區

在您刪除 AWS CloudTrail Lake 中的事件資料存放區之後，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 AWS 管理主控台 AWS CLI或 RestoreEventDataStore API 操作來還原事件資料存放區。

本節說明如何使用主控台還原事件資料存放區。如需有關如何使用 還原事件資料存放區的資訊 AWS CLI，請參閱 使用 還原事件資料存放區 AWS CLI。

還原事件資料存放區

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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。

## 從 CloudTrail Lake Event Data Store 匯出資料至 CloudWatch

讓 CloudTrail Lake 資料可供 CloudWatch 使用提供多種優點：

- 集中式日誌管理 - 將 CloudTrail 事件與 CloudWatch 中的應用程式日誌、基礎設施日誌和其他資料來源合併。
- 簡化整合 - CloudWatch 只需幾個步驟即可處理匯入程序 - 指定事件資料存放區和資料範圍。
- 歷史資料存取 - 匯入歷史 CloudTrail Lake 資料，以分析過去的事件與目前的操作資料。
- 無需額外 CloudTrail 成本 - 簡化 CloudTrail Lake 資料的匯入無需額外 CloudTrail 成本。不過，套用不常存取自訂日誌定價時，會產生 CloudWatch 成本。

本節說明如何使用 CloudTrail 主控台從事件資料存放區匯出資料。如需有關如何透過 SDK 或 執行此操作的資訊 AWS CLI，請參閱 CloudWatch 文件

從事件資料存放區匯出資料

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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，選擇匯出至 CloudWatch。
5. 選擇要匯出 EDS 資料的時間範圍。
6. 使用指示來建立或提供 IAM 角色，CloudTrail 將使用該角色來存取您的資料以進行匯出。
7. 選擇 Export (匯出)。

讓 CloudTrail Lake 資料可供匯出至 CloudWatch 時，請考慮下列事項：

- 定價 - 雖然 CloudTrail Lake 資料的簡化匯出無需額外 CloudTrail 成本，但會根據自訂日誌定價產生 CloudWatch 費用
- 資料保留 - 確保您的 CloudTrail Lake 事件資料存放區保留期間涵蓋您要匯出的歷史資料
- 區域可用性 - 檢查 CloudWatch 文件以取得此功能支援 AWS 的區域
- 事件資料存放區存取 - 您必須能夠存取要從中匯出資料的事件資料存放區。

## 使用 建立、更新和管理事件資料存放區 AWS CLI

本節說明可用來建立、更新和管理 CloudTrail Lake 事件資料存放區的 AWS CLI 命令。

使用 時 AWS CLI，請記住，您的命令會在為設定檔 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。

### 事件資料存放區的可用命令

在 CloudTrail Lake 中建立和更新事件資料存放區的命令包括：

- `create-event-data-store` 來建立事件資料存放區。
- `get-event-data-store` 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` 變更現有事件資料存放區的組態。
- `list-event-data-stores` 列出事件資料存放區。
- `delete-event-data-store` 刪除事件資料存放區。
- `restore-event-data-store` 還原待刪除的事件資料存放區。
- `start-import` 開始將追蹤事件匯入事件資料存放區，或重試失敗的匯入。
- `get-import` 傳回特定匯入的相關資訊。
- `stop-import` 停止將追蹤事件匯入至事件資料存放區。
- `list-imports` 傳回所有匯入的資訊，或由 `ImportStatus`或 選取的匯入集`Destination`。
- `list-import-failures` 列出指定匯入的匯入失敗。
- `stop-event-data-store-ingestion` 停止事件資料存放區上的事件擷取。
- `start-event-data-store-ingestion` 在事件資料存放區上重新啟動事件擷取。
- `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 在事件資料存放區上停用聯合。停用聯合之後，您無法再對 Amazon Athena 中的事件資料存放區資料進行查詢。您可以繼續在 CloudTrail Lake 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 傳回為事件資料存放區設定的 Insights 事件選取器相關資訊。
- add-tags 將一或多個標籤（鍵/值對）新增至現有的事件資料存放區。
- remove-tags 從事件資料存放區移除一或多個標籤。
- list-tags 傳回與事件資料存放區相關聯的標籤清單。
- get-event-configuration 傳回為事件資料存放區設定的任何資源標籤金鑰和 IAM 全域條件金鑰。命令也會傳回事件資料存放區是否設定為收集Standard大小事件或Large大小事件。
- put-event-configuration 以展開事件大小，並新增或移除資源標籤金鑰和 IAM 全域條件金鑰。如需詳細資訊，請參閱透過新增資源標籤索引鍵和 IAM 全域條件索引鍵來豐富 CloudTrail 事件。
- put-resource-policy 將資源型政策連接到事件資料存放區。以資源為基礎的政策可讓您控制哪些主體可以在事件資料存放區上執行動作。如需範例政策，請參閱 事件資料存放區的資源型政策範例。
- get-resource-policy 以取得連接至事件資料存放區的資源型政策。
- delete-resource-policy 刪除連接至事件資料存放區的資源型政策。

如需 CloudTrail Lake 查詢的可用命令清單，請參閱 CloudTrail Lake 查詢的可用命令。

如需 CloudTrail Lake 儀表板的可用命令清單，請參閱 儀表板的可用命令。

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

## 使用 建立事件資料存放區 AWS CLI

本節說明如何使用 create-event-data-store命令來建立事件資料存放區，並提供您可以建立的不同事件資料存放區類型範例。

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 參考中的 AdvancedEventSelectors。

- `--kms-key-id` - 指定用來加密 CloudTrail 交付事件的 KMS 金鑰 ID。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，記錄 AWS 區域 您帳戶中所有 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。如果您未指定 `--retention-period`，CloudTrail 會使用 `--billing-mode` 的預設保留期。
- `--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。

範例：

- 使用 建立 S3 資料事件的事件資料存放區 AWS CLI
- 使用 建立 KMS 網路活動事件的事件資料存放區 AWS CLI
- 使用 為 AWS Config 組態項目建立事件資料存放區 AWS CLI

- 使用 建立管理事件的組織事件資料存放區 AWS CLI
- 使用 建立 Insights 事件的事件資料存放區 AWS CLI

### 使用 建立 S3 資料事件的事件資料存放區 AWS CLI

下列 example 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`，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"
}
```

使用 建立 KMS 網路活動事件的事件資料存放區 AWS CLI

下列範例示範如何建立事件資料存放區，以包含其VpceAccessDenied網路活動事件 AWS KMS。此範例會將 errorCode 欄位設定為等於 VpceAccessDenied 事件，而 eventSource 欄位設定為等於 kms.amazonaws.com。

```
aws cloudtrail create-event-data-store \
--name EventDataStoreName \
--advanced-event-selectors '[
     {
        "Name": "Audit AccessDenied AWS KMS events over a VPC endpoint",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            },
            {
```

```
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]'
```

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": "Audit AccessDenied AWS KMS events over a VPC endpoint",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "kms.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
```

```
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

如需網路活動事件的詳細資訊，請參閱 記錄網路活動事件。

使用 為 AWS Config 組態項目建立事件資料存放區 AWS CLI

下列範例 AWS CLI create-event-data-store命令會建立名為 的事件資料存放區config-items-eds，以選取 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"
}
```

使用 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命令會建立組織事件資料存放區，收集所有管理事件並將 `--billing-mode` 參數設定為 `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 建立 Insights 事件的事件資料存放區 AWS CLI

若要在 CloudTrail Lake 中記錄 Insights 事件，您需要會收集 Insights 事件的目的地事件資料存放區和啟用 Insights 和日誌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`。使用您希望在事件資料存放區中保留事件的天數來替換 *`retention-period-days`*。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。如果您未指定 `--retention-period`，CloudTrail 會使用 `--billing-mode` 的預設保留期。

   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。使用您希望在事件資料存放區中保留事件的天數來替換 *retention-period-days*。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。如果您未指定 `--retention-period`，CloudTrail 會使用 `--billing-mode` 的預設保留期。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"
         }
      ]
}
```

在您第一次在事件資料存放區上啟用 CloudTrail Insights 之後，CloudTrail 最多可能需要 7 天才能開始交付 Insights 事件，前提是在此期間偵測到異常活動。

CloudTrail Insights 會分析在單一區域 (而非全球) 發生的管理事件。CloudTrail Insights 事件會在產生其支援管理事件的相同區域產生。

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

擷取 CloudTrail Lake 中的 Insights 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。如需有關 CloudTrail 定價的資訊，請參閱 AWS CloudTrail 定價。

## 使用 將追蹤事件匯入事件資料存放區 AWS CLI

本節說明如何執行 create-event-data-store命令來建立和設定事件資料存放區，然後如何使用 start-import命令將事件匯入至該事件資料存放區。如需匯入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。

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至 CloudTrail Lake 時，CloudTrail 會解壓縮以 gzip (已壓縮) 格式儲存的日誌。CloudTrail 會將日誌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。如果事件的 `eventTime` 早於指定的保留期，則 CloudTrail 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 = *`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`。對於`--import-source`指定包含追蹤日誌之 S3 S3儲存貯體的 S3 URI、S3 儲存貯 AWS 區域 體的 ，以及用於匯入追蹤事件之角色的 ARN。

```
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，CloudTrail 會在發生失敗的位置繼續匯入。

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

## 使用 更新事件資料存放區 AWS CLI

本節提供範例，示範如何透過執行 AWS CLI update-event-data-store 命令來更新事件資料存放區的設定。

範例：

- 使用 更新帳單模式 AWS CLI
- 更新保留模式、啟用終止保護，並使用 指定 AWS KMS key AWS CLI
- 使用 停用終止保護 AWS CLI

### 使用 更新帳單模式 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 Lake 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命令會將事件資料存放--billing-mode區的 FIXED_RETENTION_PRICING變更為 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，並使用 指定 AWS KMS key AWS CLI

下列範例 AWS CLI update-event-data-store命令會更新事件資料存放區，將保留期間變更為 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，並透過將 `--kms-key-id` 新增至 命令，以及將 KMS 金鑰 ARN 指定為 值 AWS KMS key 來指定 。 `--termination-protection-enabled` 會新增，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，無法更新記錄 AWS 事件的事件資料存放區，以從外部記錄事件 AWS。

> **Note**
>
> 如果您縮短事件資料存放區的保留期，CloudTrail 將移除 `eventTime` 早於新保留期的任何事件。例如，如果先前的保留期為 365 天，而您將其縮短到 100 天，則 CloudTrail 會移除 `eventTime` 早於 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"
}
```

### 使用 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"
}
```

## 使用 管理事件資料存放區 AWS CLI

本節說明您可以執行的數個其他命令，以取得事件資料存放區的相關資訊、啟動和停止事件資料存放區的擷取，以及啟用和停用事件資料存放區的聯合。

主題

- 使用 取得事件資料存放區 AWS CLI
- 使用 列出帳戶中的所有事件資料存放區 AWS CLI
- 新增資源標籤索引鍵和 IAM 全域條件索引鍵，並展開事件大小
- 取得事件資料存放區的事件組態
- 使用 取得事件資料存放區的資源型政策 AWS CLI
- 使用 將資源型政策連接至事件資料存放區 AWS CLI
- 使用 刪除連接至事件資料存放區的資源型政策 AWS CLI
- 使用 在事件資料存放區上停止擷取 AWS CLI
- 使用 在事件資料存放區上開始擷取 AWS CLI
- 在事件資料存放區上啟用聯合
- 在事件資料存放區上停用聯合
- 使用 還原事件資料存放區 AWS CLI

使用 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，該參數接受 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:::amzn-s3-demo-bucket"
                    ]
                },
                {
                    "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"
}
```

使用 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命令會傳回目前區域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"
        }
    ]
}
```

新增資源標籤索引鍵和 IAM 全域條件索引鍵，並展開事件大小

執行 AWS CLI put-event-configuration命令來擴展事件大小上限，並新增最多 50 個資源標籤金鑰和 50 個 IAM 全域條件金鑰，以提供事件的其他中繼資料。

put-event-configuration 命令接受下列引數：

- --event-data-store – 指定事件資料存放區的 ARN 或 ARN 的 ID 尾碼。此為必要參數。
- --max-event-size – 設定為 Large ，將事件大小上限設定為 1 MB。根據預設，值為 Standard，指定事件大小上限為 256 KB。

> **Note**
>
> 若要新增資源標籤金鑰或 IAM 全域條件金鑰，您必須將事件大小設定為 Large，以確保所有新增的金鑰都包含在事件中。

- `--context-key-selectors` – 指定您要包含在事件資料存放區所收集事件中的金鑰類型。您可以包含資源標籤索引鍵和 IAM 全域條件索引鍵。新增資源標籤和 IAM 全域條件索引鍵的相關資訊會顯示在事件的 `eventContext` 欄位中。如需詳細資訊，請參閱透過新增資源標籤索引鍵和 IAM 全域條件索引鍵來豐富 CloudTrail 事件。
  - Type 將 設定為 `TagContext` ，以傳入最多 50 個資源標籤金鑰的陣列。如果您新增資源標籤，CloudTrail 事件將包含與 API 呼叫中所涉及資源相關聯的所選標籤索引鍵。與已刪除資源相關的 API 事件將不會有資源標籤。
  - 將 Type設定為 `RequestContext`，以傳入最多 50 個 IAM 全域條件金鑰的陣列。如果您新增 IAM 全域條件金鑰，CloudTrail 事件將包含授權程序期間評估之所選條件金鑰的相關資訊，包括有關主體、工作階段、網路和請求本身的其他詳細資訊。

下列範例會將事件大小上限設定為 ，`Large`並新增兩個資源標籤索引鍵 `myTagKey1`和 `myTagKey2`。

```
aws cloudtrail put-event-configuration \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--max-event-size Large \
--context-key-selectors '[{"Type":"TagContext", "Equals":["myTagKey1","myTagKey2"]}]'
```

下一個範例會將事件大小上限設定為 ，`Large`並新增 IAM； 全域條件金鑰 (`aws:MultiFactorAuthAge`)。

```
aws cloudtrail put-event-configuration \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--max-event-size Large \
--context-key-selectors '[{"Type":"RequestContext", "Equals":
["aws:MultiFactorAuthAge"]}]'
```

最後一個範例會移除所有資源標籤金鑰和 IAM 全域條件金鑰，並將事件大小上限設定為 `Standard`。

```
aws cloudtrail put-event-configuration \
```

```
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--max-event-size Standard \
--context-key-selectors
```

取得事件資料存放區的事件組態

執行 AWS CLI `get-event-configuration`命令，以傳回收集 CloudTrail 事件之事件資料存放區的事件組態。此命令會傳回事件大小上限，並列出包含在 CloudTrail 事件中的資源標籤金鑰和 IAM 全域條件金鑰 （ 如果有的話 ）。

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

使用 取得事件資料存放區的資源型政策 AWS CLI

下列範例會在組織事件資料存放區上執行 `get-resource-policy`命令。

```
aws cloudtrail get-resource-policy --resource-arn arn:aws:cloudtrail:us-
east-1:888888888888:eventdatastore/example6-d493-4914-9182-e52a7934b207
```

由於命令是在組織事件資料存放區上執行，輸出會顯示提供的資源型政策和為委派管理員帳戶`DelegatedAdminResourcePolicy`產生的 。

使用 將資源型政策連接至事件資料存放區 AWS CLI

若要在手動或排程重新整理期間對儀表板執行查詢，您需要將資源型政策連接到與儀表板上小工具相關聯的每個事件資料存放區。這可讓 CloudTrail Lake 代表您執行查詢。如需資源型政策的詳細資訊，請參閱 範例：允許 CloudTrail 執行查詢以重新整理儀表板。

下列範例會將資源型政策連接至事件資料存放區，允許 CloudTrail 在儀表板重新整理時對儀表板執行查詢。此政策是在單獨的檔案 *`policy.json`* 中建立，並具有下列範例政策陳述式：

JSON

```
{ "Version":"2012-10-17",       "Statement": [{ "Sid": "EDSPolicy", "Effect":
    "Allow", "Principal": { "Service": "cloudtrail.amazonaws.com" }, "Resource":
    "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
event_data_store_ID",
```

```
    "Action": "cloudtrail:StartQuery", "Condition": { "StringEquals":
 { "AWS:SourceArn":
    "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE",
    "AWS:SourceAccount": "123456789012" } } } ] }
```

將 *123456789012* 取代為您的帳戶 ID，將 *arn#aws#cloudtrail#us-east-1#123456789012#eventdatastore/event_data_store_ID* 取代為 CloudTrail 將執行查詢之事件資料存放區的 ARN，並將 *arn#aws#cloudtrail#us-east-1#123456789012#eventdatastore/EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE* 取代為儀表板的 ARN。

```
aws cloudtrail put-resource-policy \
--resource-arn eds-arn \
--resource-policy file://policy.json
```

以下是回應範例。

```
{ "ResourceArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE", "ResourcePolicy": "policy-statement" }
```

如需其他政策範例，請參閱 事件資料存放區的資源型政策範例。

使用 刪除連接至事件資料存放區的資源型政策 AWS CLI

下列範例會刪除連接至事件資料存放區的資源型政策。將 *eds-arn* 取代為事件資料存放區的 ARN。

```
aws cloudtrail delete-resource-policy --resource-arn eds-arn
```

此命令如果成功就不會產生輸出。

使用 在事件資料存放區上停止擷取 AWS CLI

下列範例 AWS CLI stop-event-data-store-ingestion命令會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。

使用 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開始事件擷取。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。

使用 還原事件資料存放區 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。

## 使用 刪除事件資料存放區 AWS CLI

本節示範如何執行 命令來 AWS CLI `delete-event-data-store`刪除事件資料存放區

若要刪除事件資料存放區，`--event-data-store`請提供事件資料存放區 ARN 或 ARN 的 ID 尾碼來指定 。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。事件資料存放區在等待刪除 AWS 區域 時，會計入 中最多十個事件資料存放區的 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。

若要刪除具有 eventCategory之 的事件資料存放區ActivityAuditLog，您必須先刪除整合的頻道。您可以使用 aws cloudtrail delete-channel命令刪除頻道。如需詳細資訊，請參閱刪除頻道以刪除與 的整合 AWS CLI。

```
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。

## 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。

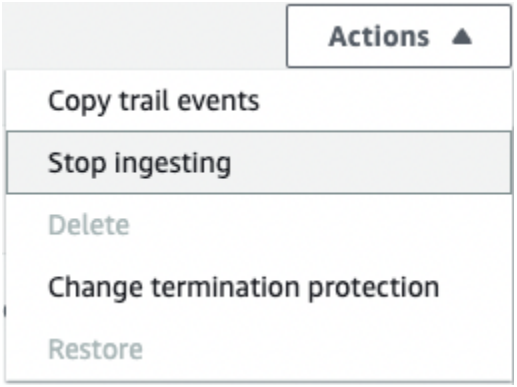
- CREATED – 指示已建立事件資料存放區的短期狀態。
- ENABLED – 事件資料存放區在作用中並擷取事件。您可以執行查詢並將追蹤事件複製到事件資料存放區。
- STARTING_INGESTION – 短期狀態指示事件資料存放區將開始擷取即時事件。
- STOPPING_INGESTION – 短期狀態指示事件資料存放區將停止擷取即時事件。
- STOPPED_INGESTION – 事件資料存放區不在擷取事件。您仍然可以對已在事件資料存放區內的任何事件執行查詢，並將追蹤事件複製到事件資料存放區。
- PENDING_DELETION – 事件資料存放區處於 ENABLED 或 STOPPED_INGESTION 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。不過，待刪除的事件資料存放區會計入一個 中可能存在的事件資料存放區的配額 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，或開啟或關閉事件資料存放區終止保護，請使用事件資料存放區詳細資訊頁面的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 事件的事件資料存放區。開始擷取和停止擷取的選項僅適用於包含 CloudTrail 事件（管理和資料事件）或 AWS Config 組態項目的事件資料存放區。

## 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，以建立記錄至追蹤之事件的時間點快照。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為 CloudTrail 事件設定的現有事件資料存放區，或者您可以建立一個新的 CloudTrail 事件資料存放區，然後在建立事件資料存放區的過程中選擇複製追蹤事件選項。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。

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 Lake 成本。

在將追蹤事件複製到 CloudTrail Lake 事件資料存放區時，您需要按事件資料存放區擷取的未壓縮的資料量支付費用。

當您將追蹤事件複製到 CloudTrail Lake 時，CloudTrail 會解壓縮以 gzip (已壓縮) 格式存放的日誌，然後將日誌中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 Lake 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？ |
| --- | --- |
| 分析並查詢 CloudTrail Lake 中的歷史追蹤事件，而不擷取新事件 | 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的現有追蹤 | 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。<br><br>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。<br><br>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
- 複製追蹤事件所需的許可
- 使用主控台將追蹤事件複製到現有的事件資料存放區
- 使用主控台將追蹤事件複製到新的事件資料存放區
- 使用 CloudTrail 主控台檢視事件複製詳細資訊

## 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 操作來擷取來源 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。

- 當您將追蹤事件複製到事件資料存放區時，無論目的地事件資料存放區的事件類型、進階事件選取器或組態為何，CloudTrail 都會複製所有追蹤事件 AWS 區域。
- 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 只會複製 `eventTime` 在事件資料存放區保留期內的追蹤事件。若要決定適當的保留期，請加總您要複製的最舊事件所經歷的天數與要在事件資料存放區中保留事件的天數 (保留期 = ######### + ### #)。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 壓縮日誌檔案複製追蹤事件。CloudTrail 不會從未壓縮的日誌檔案或使用 Gzip 以外格式壓縮的日誌檔案複製追蹤事件。
- 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 只會複製包含在 S3 儲存貯體`CloudTrail`字首和`CloudTrail`字首內的字首中的 CloudTrail 事件，而不會檢查其他服務的字首 AWS 。如果您要複製其他字首中包含的 CloudTrail 事件，則必須在複製追蹤事件時選擇字首。
- 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 角色所需的所有必要許可。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，CloudTrail 會為角色提供所需的所有許可。

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，則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，CloudTrail 會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。

如果您選擇現有的角色，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。將 *amzn-s3-demo-bucket*、*myAccountID*、 *region*、 *prefix* 和 *eventDataStoreId* 取代為您的組態的適當值。*myAccountID* 是用於 CloudTrail Lake AWS 的帳戶 ID，可能與 S3 儲存貯體 AWS 的帳戶 ID 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:::amzn-s3-demo-bucket"
      ],
      "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:::amzn-s3-demo-bucket/prefix",
        "arn:aws:s3:::amzn-s3-demo-bucket/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，允許 CloudTrail 擔任 IAM 角色，從來源 S3 儲存貯體複製追蹤事件。將 *myAccountID*、*region* 和 *eventDataStoreArn* 取代為適當的組態值。*myAccountID* 是用於 CloudTrail Lake 的 AWS 帳戶 ID，可能與 S3 儲存貯體 AWS 的帳戶 ID 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。

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，以授予這些許可。將 *roleArn* 和 *amzn-s3-demo-bucket* 取代為您的組態的適當值。

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
```

```
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket",
    "arn:aws:s3:::amzn-s3-demo-bucket/*"
  ]
},
```

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 金鑰政策為 CloudTrail 提供從已啟用 SSE-KMS 加密的 S3 儲存貯體複製追蹤事件所需的 `kms:Decrypt` 和 `kms:GenerateDataKey` 許可。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 金鑰政策可讓 CloudTrail 解密來源 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，該政策允許 CloudTrail 解密來源 S3 儲存貯體中的資料。將 *roleArn*、*amzn-s3-demo-bucket*、*myAccountID*、*region* 和 *eventDataStoreId* 取代為您的組態的適當值。*myAccountID* 是用於 CloudTrail Lake AWS 的帳戶 ID，可能與 S3 儲存貯體 AWS 的帳戶 ID 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:::amzn-s3-demo-bucket/*"
    },
    "StringEquals": {
      "aws:SourceAccount": "myAccountID",
      "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:eventdatastore/eventDataStoreId"
    }
```

```
  }
}
```

## 使用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 只會複製 `eventTime` 在事件資料存放區保留期內的追蹤事件。若要決定適當的保留期，請加總您要複製的最舊事件所經歷的天數與要在事件資料存放區中保留事件的天數 (保留期 = ######## + ####)。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. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
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 只會複製包含在 S3 儲存貯體`CloudTrail`字首和`CloudTrail`字首內的字首中的 CloudTrail 事件，而不會檢查其他服務的字首 AWS 。如果您要複製其他字首中包含的 CloudTrail 事件，請選擇 Enter S3 URI (輸入 S3 URI)，然後選擇 Browse S3 (瀏覽 S3) 以瀏覽至字首。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 金鑰政策允許 CloudTrail 解密資料。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。

S3 儲存貯體政策必須授予 CloudTrail 存取權，才能從 S3 儲存貯體複製追蹤事件。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. 針對指定事件的時間範圍，選擇複製事件的時間範圍。CloudTrail 會在嘗試複製追蹤事件之前檢查字首和日誌檔案名稱，以確認名稱包含介於所選開始日期和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 只會複製 `eventTime` 在事件資料存放區保留期內的追蹤事件。例如，如果事件資料存放區的保留期為 90 天，則 CloudTrail 將不會複製 `eventTime` 早於 90 天的任何追蹤事件。

   - 如果選擇相對範圍，您可以選擇複製過去 6 個月、1 年、2 年、7 年或自訂範圍內記錄的事件。CloudTrail 會複製所選時段內記錄的事件。
   - 如果選擇 Absolute range (絕對範圍)，您可以選擇特定的開始和結束日期。CloudTrail 會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 會自動為此新角色建立必要的許可。
   - 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 會在事件複製的過程中逐步更新詳細資訊。

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)。當您重試複製時，CloudTrail 會在發生失敗的位置繼續複製。

如需檢視追蹤事件複製之詳細資訊，請參閱 使用 CloudTrail 主控台檢視事件複製詳細資訊。

## 使用主控台將追蹤事件複製到新的事件資料存放區

本演練說明如何將追蹤事件複製到新的 CloudTrail Lake 事件資料存放區，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. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
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，請在一般詳細資訊中為您的事件資料存放區提供一個名稱，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。如需有關 CloudTrail 命名要求的資訊，請參閱 CloudTrail 資源、S3 儲存貯體和 KMS 金鑰的命名需求。
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 Lake 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。在 366 天之後，延長保留將依用量計費定價。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 會透過檢查事件的 `eventTime` 是否在指定保留期以內，決定是否要保留該事件。例如，如果您指定的保留期為 90 天，CloudTrail 將移除 `eventTime` 早於 90 天的事件。

   > **Note**
   >
   > 如果事件的 `eventTime` 早於指定的保留期，則 CloudTrail 不會複製該事件。
   > 若要決定適當的保留期，請加總您要複製的最舊事件所經歷的天數與要在事件資料存放區中保留事件的天數 (保留期 = *#########* + *####*)。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。根據預設，事件資料存放區中的所有事件都會由 CloudTrail 使用 AWS 擁有和管理的 KMS 金鑰來加密。

   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。選擇新增以為您 AWS KMS key 建立 ，或選擇現有以使用現有的 KMS 金鑰。在 Enter KMS alias (輸入 KMS 別名) 中，指定別名，格式為 `alias/`*`MyAliasName`*。使用您自己的 KMS 金鑰時，您必須編輯您的 KMS 金鑰政策，以允許對 CloudTrail 日誌進行加密和解密。如需詳細資訊，請參閱設定 CloudTrail 的 AWS KMS 金鑰政策。CloudTrail 也支援 AWS KMS 多區域金鑰。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 AWS KMS 的成本。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**
   >
   > 若要啟用組織事件資料存放區的 AWS Key Management Service 加密，您必須使用管理帳戶的現有 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 Data Catalog 中的資料表中繼資料可讓 Athena 查詢引擎了解如何尋找、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 會自動建立具有必要許可的角色。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）選擇啟用資源政策，將資源型政策新增至您的事件資料存放區。以資源為基礎的政策可讓您控制哪些主體可以在事件資料存放區上執行動作。例如，您可以新增資源型政策，允許其他帳戶中的根使用者查詢此事件資料存放區並檢視查詢結果。如需範例政策，請參閱 事件資料存放區的資源型政策範例。

   以資源為基礎的政策包含一或多個陳述式。政策中的每個陳述式都會定義允許或拒絕存取事件資料存放區的委託人，以及委託人可以在事件資料存放區資源上執行的動作。

   事件資料存放區的資源型政策支援下列動作：

   - `cloudtrail:StartQuery`
   - `cloudtrail:CancelQuery`
   - `cloudtrail:ListQueries`
   - `cloudtrail:DescribeQuery`
   - `cloudtrail:GetQueryResults`
   - `cloudtrail:GenerateQuery`
   - `cloudtrail:GenerateQueryResultsSummary`
   - `cloudtrail:GetEventDataStore`

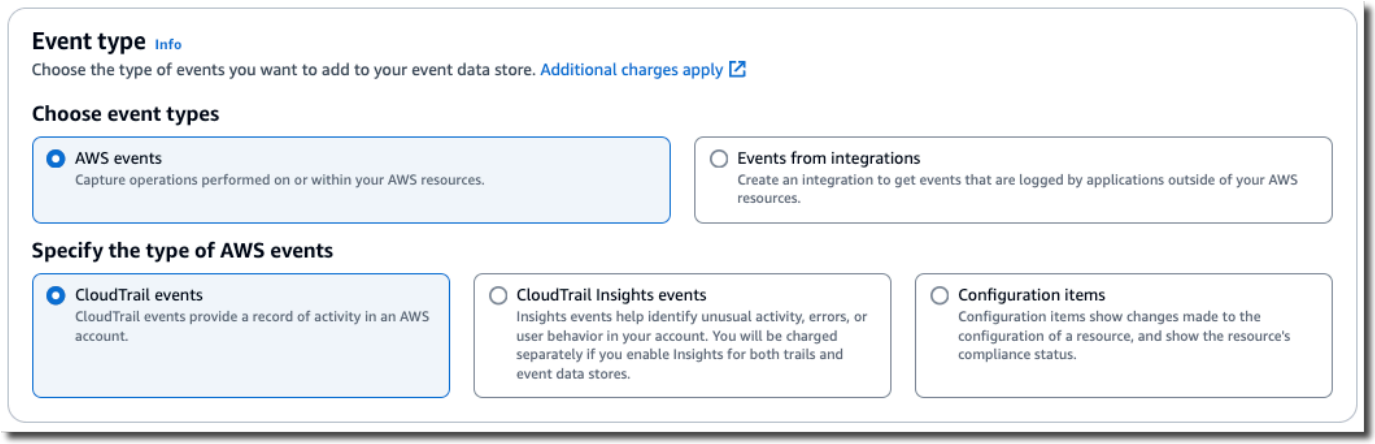
   對於組織事件資料存放區，CloudTrail 會建立預設資源型政策，列出允許委派管理員帳戶在組織事件資料存放區上執行的動作。此政策中的許可衍生自 中的委派管理員許可 AWS Organizations。此政策會在組織事件資料存放區或組織變更後自動更新（例如，CloudTrail 委派管理員帳戶已註冊或移除）。

10. (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 事件資料存放區建立使用者定義的成本分配標籤。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。如需有關如何在 中使用標籤的資訊 AWS，請參閱《標記 AWS 資源使用者指南》中的標記您的 AWS 資源。

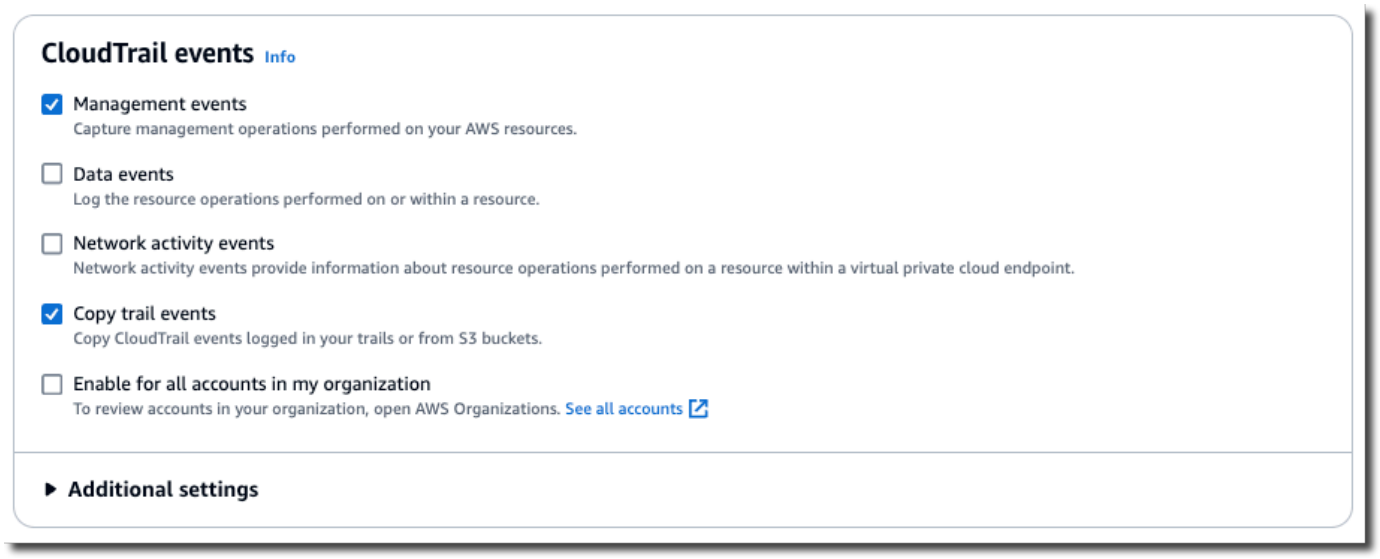
11. 選擇 Next (下一步) 以設定事件資料存放區。

12. 在選擇事件頁面上，保留事件類型的預設選項。




13. 對於 CloudTrail 事件，我們將維持選取管理事件，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。




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。

> **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。

15. 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。根據預設，事件資料存放區會收集所有 的事件， AWS 區域 並在建立事件時開始擷取事件。
16. 對於管理事件，我們將保留預設設定。
17. 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。

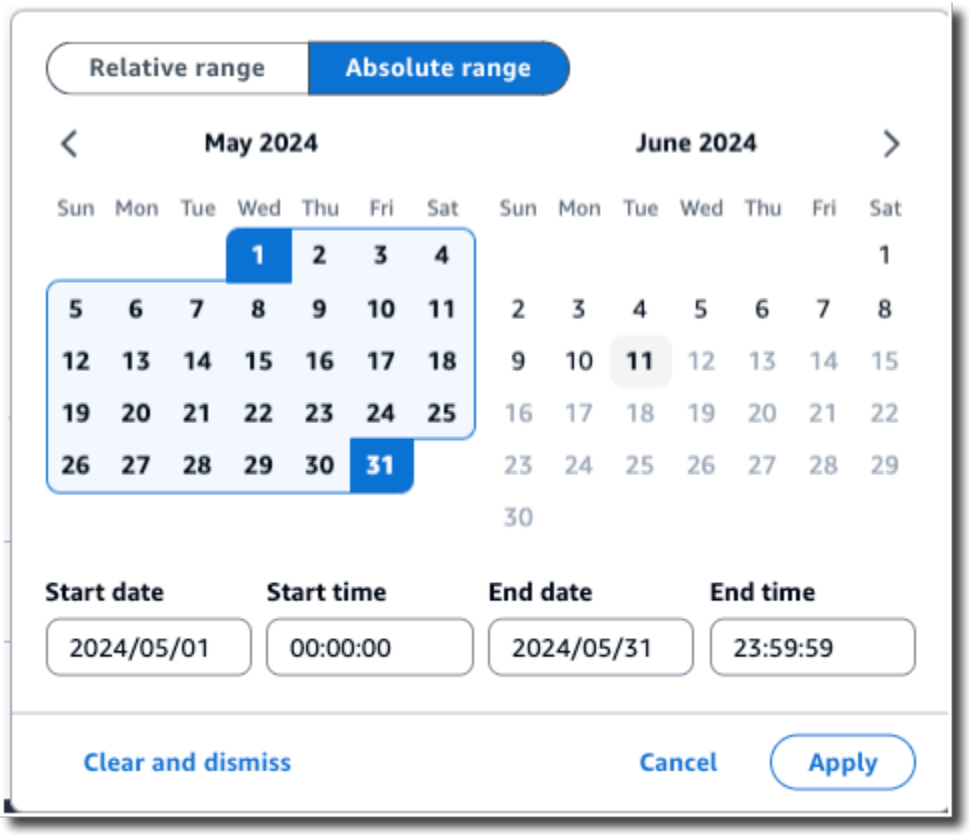
    根據預設，CloudTrail 只會複製包含在 S3 儲存貯體`CloudTrail`字首和`CloudTrail`字首內的字首中的 CloudTrail 事件，而不會檢查其他服務的字首 AWS 。如果您要複製其他字首中包含的 CloudTrail 事件，請選擇 Enter S3 URI (輸入 S3 URI)，然後選擇 Browse S3 (瀏覽 S3) 以瀏覽至字首。如果追蹤的來源 S3 儲存貯體使用 KMS 金鑰進行資料加密，請確保 KMS 金鑰政策允許 CloudTrail 解密資料。如果您的來源 S3 儲存貯體使用多個 KMS 金鑰，則必須更新每個金鑰的政策以允許 CloudTrail 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。

    b. 選擇複製事件的時間範圍。CloudTrail 會在嘗試複製追蹤事件之前檢查字首和日誌檔案名稱，以確認名稱包含介於所選開始日期和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。

- 如果選擇相對範圍，您可以選擇複製過去 6 個月、1 年、2 年、7 年或自訂範圍內記錄的事件。CloudTrail 會複製所選時段內記錄的事件。
- 如果選擇 Absolute range (絕對範圍)，您可以選擇特定的開始和結束日期。CloudTrail 會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，並選取整個 5 月。

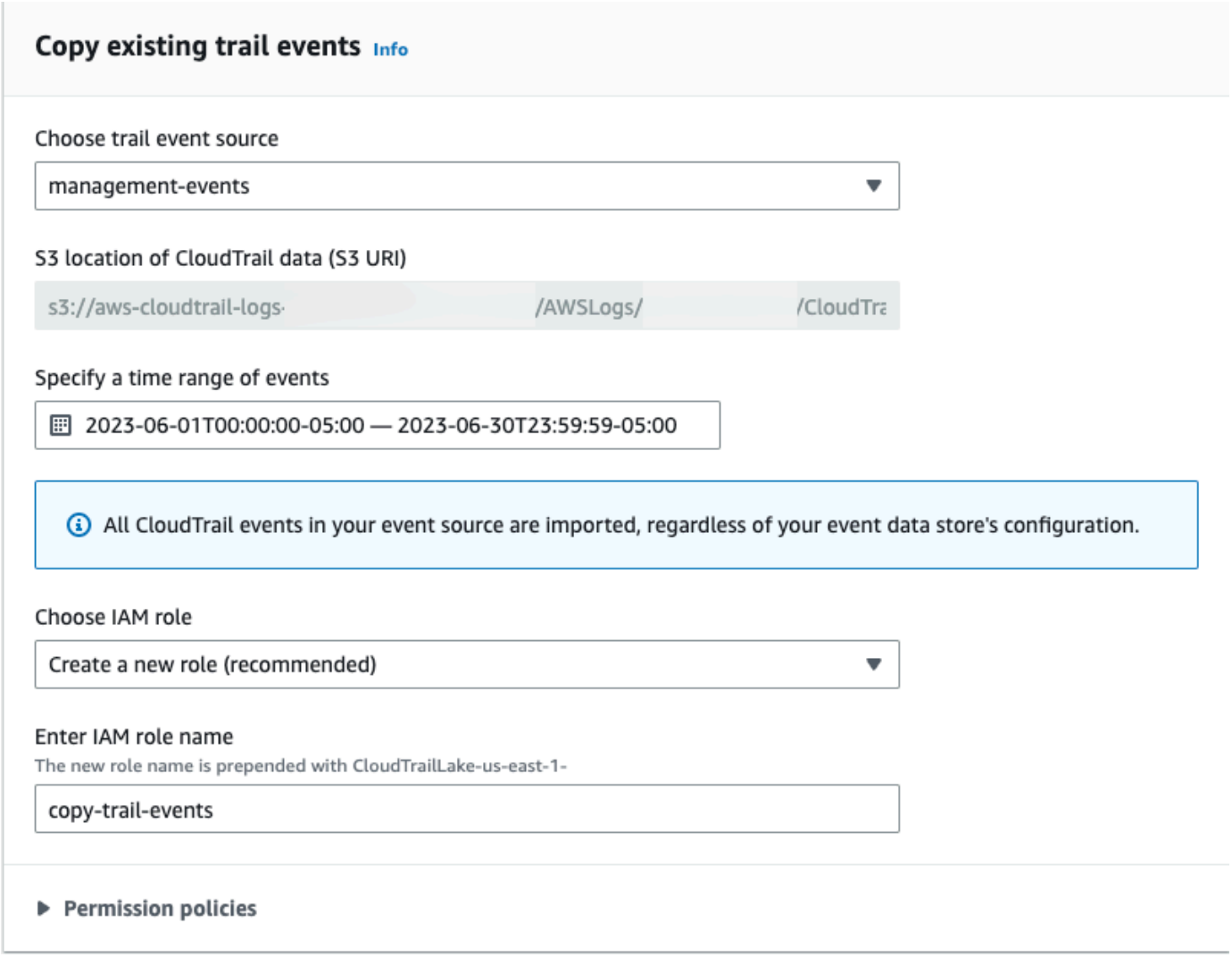



c. 對於 Permissions (許可)，從下列 IAM 角色選項中選擇。如果您選擇現有的 IAM 角色，請確認 IAM 角色政策提供必要的許可。如需更新 IAM 角色許可的詳細資訊，請參閱[複製追蹤事件的 IAM 許可]。

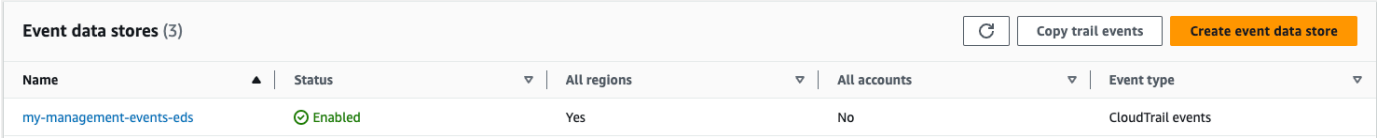
- 選擇 Create a new role (recommended) (建立新角色 (建議使用)) 以建立新的 IAM 角色。對於 Enter IAM role name (輸入 IAM 角色名稱)，請輸入角色的名稱。CloudTrail 會自動為此新角色建立必要的許可。
- 選擇使用自訂 IAM 角色 ARN，以使用未列出的自訂 IAM 角色。對於 Enter IAM role ARN (輸入 IAM 角色 ARN)，輸入 IAM ARN。

- 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**。

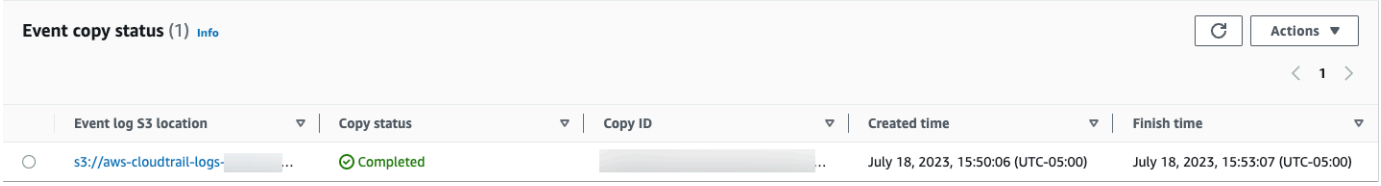



18. 選擇 Next (下一步) 以檢閱您的選項。
19. 在 Review and create (檢閱和建立) 頁面上，檢閱您的選擇。選擇 Edit (編輯) 以對區段進行變更。當您準備建立事件資料存放區時，請選擇 Create event data store (建立事件資料存放區)。
20. 新的事件資料存放區出現在事件資料存放區頁面上的事件資料存放區表格中。

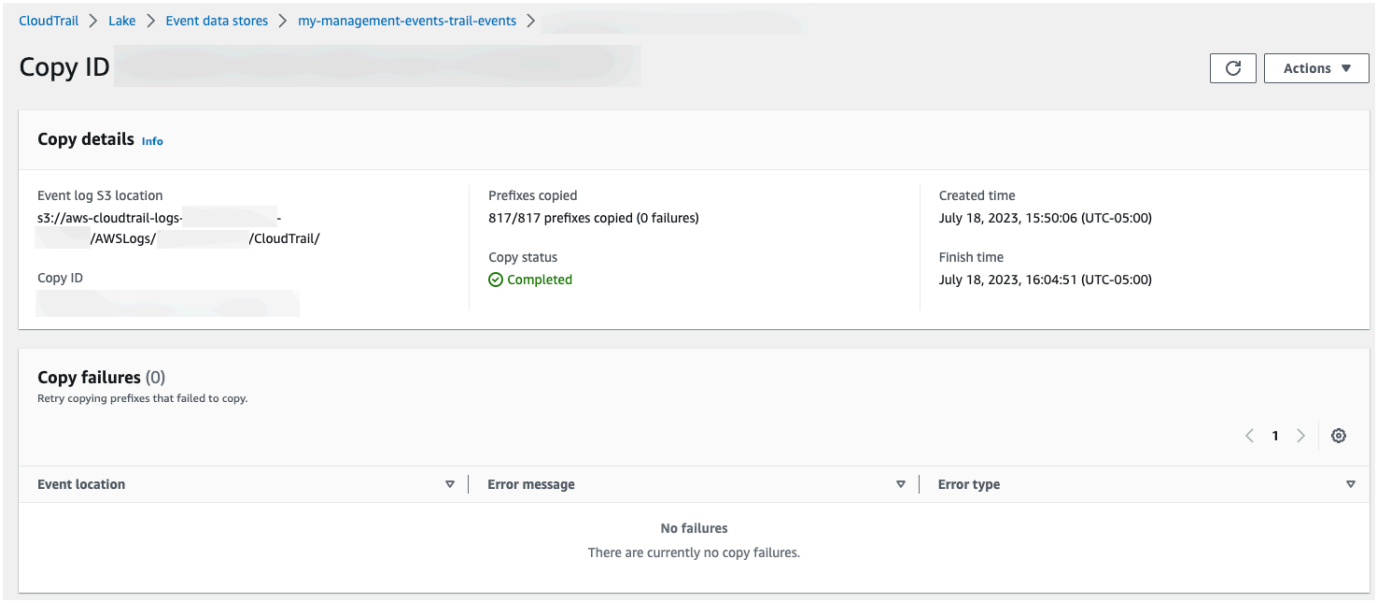


21. 選擇事件資料存放區名稱，以檢視其詳細資訊頁面。詳細資訊頁面顯示您的事件資料存放區的詳細資訊以及複製狀態。事件複製狀態顯示在事件複製狀態區域中。

    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)。




22. 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 [使用 CloudTrail 主控台檢視事件複製詳細資訊]。




23. 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)。當您重試複製時，CloudTrail 會在發生失敗的位置繼續複製。

## 使用 CloudTrail 主控台檢視事件複製詳細資訊

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 會在事件複製的過程中逐步更新詳細資訊。

### 存取事件複製詳細資訊頁面

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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，CloudTrail 會複製追蹤日誌檔案中儲存在字首中的事件。
- 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)。當您重試複製時，CloudTrail 會在發生失敗的位置繼續複製。
  - 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 字首是否包含未壓縮的檔案，或者其中包含 CloudTrail 以外之服務提供的檔案。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 CloudTrail 匯入事件的存取權，您將得到 `AccessDenied` 錯誤。

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)。當您重試複製時，CloudTrail 會在發生失敗的位置繼續複製。

## 聯合事件資料存放區

聯合事件資料存放區可讓您在 Data Catalog 中 AWS Glue 檢視與事件資料存放區相關聯的中繼資料、向 註冊 Data Catalog AWS Lake Formation，以及可讓您使用 Amazon Athena 針對事件資料執行 SQL 查詢。儲存在 AWS Glue Data Catalog 中的資料表中繼資料可讓 Athena 查詢引擎了解如何尋找、讀取和處理您要查詢的資料。

您可以使用 CloudTrail 主控台 AWS CLI或 EnableFederation API 操作來啟用聯合。當您啟用 Lake 查詢聯合時，CloudTrail 會在 AWS Glue Data Catalog 中建立名為 的受管資料庫 `aws:cloudtrail`（如果資料庫不存在） 和受管聯合資料表。事件資料存放區 ID 會用於資料表名稱。CloudTrail 會在 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 AWS Glue 資料目錄中的聯合資源進行精細存取控制。

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 會自動建立具有必要許可的角色。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 DisableFederation API 操作 AWS CLI來停用聯合。當您停用聯合時，CloudTrail 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 中查詢事件資料。當您停用聯合時，系統不會刪除任何 CloudTrail Lake 資料，而且您可以繼續在 CloudTrail Lake 中執行查詢。

聯合 CloudTrail Lake 事件資料存放區不會產生 CloudTrail 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 Lake 和 Amazon Athena 分析活動日誌

主題


- 考量事項
- 聯合的所需許可
- 啟用 Lake 查詢聯合
- 停用 Lake 查詢聯合
- 使用 管理 CloudTrail Lake 聯合資源 AWS Lake Formation


## 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 事件資料存放區不會產生 CloudTrail 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 撤銷資源的許可 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，請參閱使用 管理 CloudTrail Lake 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。 AWS 受管政策：AmazonAthenaFullAccess 允許此動作。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 `aws:cloudtrail` 資料庫是由 CloudTrail 管理。

- 若要在 Amazon Quick 中建立資料集，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，CloudTrail 會為角色提供所需的所有許可。

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，CloudTrail 會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。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFederationEDSDataAccess",
            "Effect": "Allow",
            "Action": "cloudtrail:GetEventDataStoreData",
            "Resource": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/eds-id"
        },
        {
            "Sid": "LakeFederationKMSDecryptAccess",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-east-1:111111111111: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。

JSON

```
{
  "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。此政策允許 CloudTrail 在事件資料存放區上啟用聯合、在 AWS Glue Data Catalog 中 AWS Glue 建立聯合資源，以及 AWS Lake Formation 管理資源註冊。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CloudTrailEnableFederation",
            "Effect": "Allow",
            "Action": "cloudtrail:EnableFederation",
            "Resource": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/eds-id"
        },
        {
            "Sid": "FederationRoleAccess",
            "Effect": "Allow",
            "Action": [
                "iam:PassRole",
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/federation-role-name"
        },
        {
            "Sid": "GlueResourceCreation",
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:CreateTable",
                "glue:PassConnection"
            ],
            "Resource": [
                "arn:aws:glue:us-east-1:111111111111:catalog",
                "arn:aws:glue:us-east-1:111111111111:database/aws:cloudtrail",
```

```
                "arn:aws:glue:us-east-1:111111111111:table/aws:cloudtrail/eds-
id",
                "arn:aws:glue:us-east-1:111111111111:connection/aws:cloudtrail"
            ]
        },
        {
            "Sid": "LakeFormationRegistration",
            "Effect": "Allow",
            "Action": [
                "lakeformation:RegisterResource",
                "lakeformation:DeregisterResource"
            ],
            "Resource":
 "arn:aws:lakeformation:region:111111111111:catalog:111111111111"
        }
    ]
}
```

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。此政策允許 CloudTrail 在事件資料存放區上停用聯合、 AWS Glue 刪除 AWS Glue Data Catalog 中的受管聯合資料表，以及 Lake Formation 取消註冊聯合資源。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CloudTrailDisableFederation",
            "Effect": "Allow",
            "Action": "cloudtrail:DisableFederation",
            "Resource": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/eds-id"
        },
        {
            "Sid": "GlueTableDeletion",
            "Effect": "Allow",
            "Action": "glue:DeleteTable",
            "Resource": [
```

```
                "arn:aws:glue:us-east-1:111111111111:catalog",
                "arn:aws:glue:us-east-1:111111111111:database/aws:cloudtrail",
                "arn:aws:glue:us-east-1:111111111111:table/aws:cloudtrail/eds-id"
            ]
        },
        {
            "Sid": "LakeFormationDeregistration",
            "Effect": "Allow",
            "Action": "lakeformation:DeregisterResource",
            "Resource": "arn:aws:lakeformation:us-
east-1:111111111111:catalog:111111111111"
        }
    ]
}
```

## 啟用 Lake 查詢聯合

您可以使用 CloudTrail 主控台或 EnableFederation API 操作 AWS CLI來啟用 Lake 查詢聯合。當您啟用 Lake 查詢聯合時，CloudTrail 會在 AWS Glue Data Catalog 中建立名為 的受管資料庫 `aws:cloudtrail`（如果資料庫不存在） 和受管聯合資料表。事件資料存放區 ID 會用於資料表名稱。CloudTrail 會在 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 AWS Glue 資料目錄中的聯合資源進行精細存取控制。

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. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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許可的角色。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 DisableFederation API 操作 AWS CLI來停用聯合。當您停用聯合時，CloudTrail 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 中查詢事件資料。當您停用聯合時，系統不會刪除任何 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. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
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。

## 使用 管理 CloudTrail Lake 聯合資源 AWS Lake Formation

當您聯合事件資料存放區時，CloudTrail 會在其中註冊聯合角色 ARN 和事件資料存放區 AWS Lake Formation，該服務負責允許對 AWS Glue 資料目錄中的聯合資源進行精細存取控制。本節說明如何使用 Lake Formation 來管理 CloudTrail Lake 聯合資源。

當您啟用聯合時，CloudTrail 會在 AWS Glue Data Catalog 中建立下列資源。

- 受管資料庫 – CloudTrail 會為每個帳戶建立 1 個名稱為 aws:cloudtrail 的資料庫。CloudTrail 會管理資料庫。您無法刪除或修改 中的資料庫 AWS Glue。
- 受管聯合資料表 – CloudTrail 會為每個聯合事件資料存放區建立 1 個資料表，並將事件資料存放區 ID 用於資料表名稱。CloudTrail 會管理資料表。您無法刪除或修改其中的資料表 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 如何使用 AWS Glue IAM 的詳細資訊，請參閱 AWS Glue 如何使用 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。如需詳細資訊，請參閱《 AWS Lake Formation 開發人員指南》中的使用資料列層級存取控制保護資料湖。
  - 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

當您首次啟用聯合時，CloudTrail 會使用 Lake Formation 資料湖設定建立受管資料庫和受管聯合資料表。

CloudTrail 啟用聯合後，您可以檢查這些資源的許可，藉此確認要用於受管資料庫和受管聯合資料表的許可方法。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. 如果與您的 共用 Data Catalog 資源， AWS 帳戶 且您的帳戶與共用帳戶不在同一個 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 RAM AWS 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. 如果與您的 共用 Data Catalog 資源， AWS 帳戶 且您的帳戶與共用帳戶不在同一個 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 RAM AWS 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。

擁有資料表的帳戶可以從 Lake Formation 移除外部帳戶的許可，或在 CloudTrail 中停用聯合，藉此隨時撤銷共用。

## 了解組織事件資料存放區

如果您已在 中建立組織 AWS Organizations，您可以建立組織事件資料存放區，以記錄 AWS 帳戶 該組織中所有 的所有事件。組織事件資料存放區可以套用至所有 AWS 區域或目前區域。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存放區，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功能。

| 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 |
| 為事件或 AWS Config 組態項目建立組織 AWS CloudTrail 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開始和停止事件擷取。 | 是 | 是 |
| 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 |

| 功能 | 管理帳戶 | 委派管理員帳戶 |
| --- | --- | --- |
| 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受管儀表板。 | 是 | 否 |
| 啟用組織事件資料存放區的醒目提示儀表板。 | 是 | 否 |
| 為查詢組織事件資料存放區的自訂儀表板建立小工具。 | 是 | 否 |

[1]只有管理帳戶可以將組織事件資料存放區轉換為帳戶層級事件資料存放區，或將帳戶層級事件資料存放區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。當組織事件資料存放區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存放區。同樣地，只有管理帳戶中的帳戶層級事件資料存放區可以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。

## 建立組織事件資料存放區

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 AWS Config 組態項目。

> **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

使用主控台建立組織事件資料存放區

1. 請遵循為 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

遵循 為 AWS Config 組態項目建立事件資料存放區程序中的步驟，為組態項目建立組織事件資料存放區 AWS Config 。

2. 在選擇事件頁面上，為組織中的所有帳戶選擇啟用。

### AWS CLI

若要建立組織事件資料存放區，請執行 create-event-data-store命令並包含 `--organization-enabled`選項。

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 CloudTrail 預設會記錄管理事件，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`命令會建立名為 的組織事件資料存放區`config-items-org-eds`，以收集 AWS Config 組態項目。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的事件資料存放區，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. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
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. 為組織中的所有帳戶選擇啟用。
6. 選擇儲存變更。

如需更新事件資料存放區的詳細資訊，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存放區以將其套用至組織，請執行 update-event-data-store 命令並包含 --organization-enabled選項。

```
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
```

## 委派管理員的預設資源政策

CloudTrail 會自動DelegatedAdminResourcePolicy為組織事件資料存放區產生名為 的資源政策，列出允許委派管理員帳戶在組織事件資料存放區上執行的動作。中的許可DelegatedAdminResourcePolicy衍生自 中的委派管理員許可 AWS Organizations。

DelegatedAdminResourcePolicy 的目的在於確保委派管理員帳戶可以代表組織管理組織事件資料存放區，而且當以資源為基礎的政策連接到允許或拒絕主體對組織事件資料存放區執行動作的組織事件資料存放區時，不會意外拒絕存取組織事件資料存放區。

CloudTrail DelegatedAdminResourcePolicy 會與為組織事件資料存放區提供的任何資源型政策一起評估。委派管理員帳戶只有在提供的資源型政策包含明確拒絕委派管理員帳戶對委派管理員帳戶可執行的組織事件資料存放區執行動作的陳述式時，才會被拒絕存取。

此DelegatedAdminResourcePolicy政策會在下列情況下自動更新：

- 管理帳戶會將組織事件資料存放區轉換為帳戶層級事件資料存放區，或將帳戶層級事件資料存放區轉換為組織事件資料存放區。
- 有組織變更。例如，管理帳戶會註冊或移除 CloudTrail 委派管理員帳戶。

您可以在 CloudTrail 主控台的委派管理員資源政策區段上檢視up-to-date政策，或執行 AWS CLI get-resource-policy命令並傳遞組織事件資料存放區的 ARN。

下列範例會在組織事件資料存放區上執行 get-resource-policy命令。

```
aws cloudtrail get-resource-policy --resource-arn arn:aws:cloudtrail:us-east-1:888888888888:eventdatastore/example6-d493-4914-9182-e52a7934b207
```

此命令的輸出會顯示資源型政策，以及為委派管理員帳戶產生的`DelegatedAdminResourcePolicy`政策。

### 其他資源

- 組織委派的管理員
- 新增 CloudTrail 委派的管理員
- 移除 CloudTrail 委派的管理員

## 在 外部建立與事件來源的整合 AWS

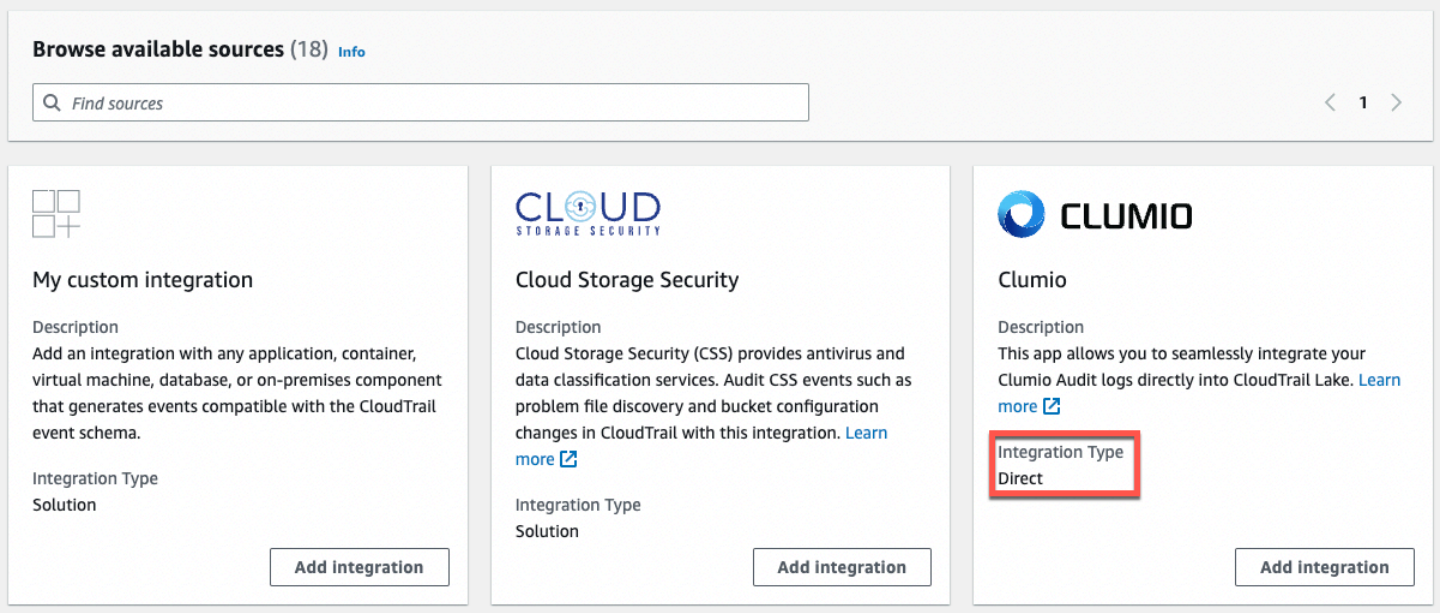
您可以使用 CloudTrail 來記錄和儲存來自混合環境中任何來源 (例如在內部部署或雲端、虛擬機器或容器中託管的內部或 SaaS 應用程式) 的使用者活動資料。您可以針對此資料進行儲存、存取、分析、疑難排解和採取行動，而不需維護多個日誌彙總工具和報告工具。

來自非AWS 來源的活動事件的運作方式是使用頻道，將事件從使用 CloudTrail 的外部合作夥伴，或從您自己的來源帶入 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 已與許多事件來源提供者合作，例如 Okta 和 LaunchDarkly。當您在外部建立與事件來源的整合時 AWS，您可以選擇其中一個合作夥伴做為您的事件來源，或選擇我的自訂整合，將自有來源的事件整合到 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，將事件交付至您 AWS 帳戶的事件資料存放區。透過解決方案整合，應用程式會在您的帳戶中執行， AWS 而應用程式會呼叫 `PutAuditEvents` API，將事件交付至您 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)。




首先，請使用 CloudTrail 主控台建立整合，以記錄來自合作夥伴或其他應用程式來源的事件。

主題

- 使用主控台建立與 CloudTrail 合作夥伴的整合
- 建立與主控台的自訂整合
- 使用 建立、更新和管理 CloudTrail Lake 整合 AWS CLI
- 整合合作夥伴的其他資訊
- CloudTrail Lake 整合事件結構描述

## 使用主控台建立與 CloudTrail 合作夥伴的整合

當您在外部建立與事件來源的整合時 AWS，您可以選擇其中一個合作夥伴做為您的事件來源。當您在 CloudTrail 中與合作夥伴應用程式建立整合時，合作夥伴需要您在此工作流程中所建立通道的 Amazon Resource Name (ARN)，才能將事件傳送至 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。合作夥伴在整合的通道上呼叫 `PutAuditEvents` 之後，整合就會開始將合作夥伴事件擷取到 CloudTrail 中。

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
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。

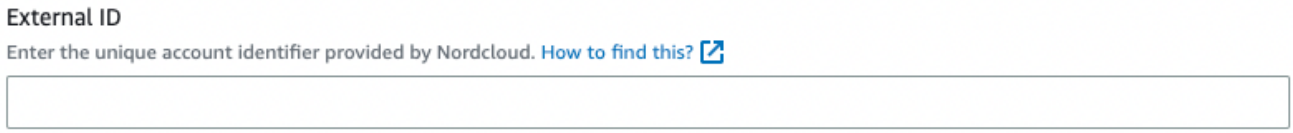
   如果您選擇將活動事件記錄到一或多個現有事件資料存放區，請從清單中選擇事件資料存放區。事件資料存放區只能包含活動事件。主控台中的事件類型必須是 Events from integrations (來自整合的事件)。在 API 中，`eventCategory` 值必須是 `ActivityAuditLog`。
6. 在 Resource policy (資源政策) 中，為整合的通道設定資源政策。資源政策是 JSON 政策文件，這些文件會指出指定的主體可對資源執行哪些動作以及相關條件。在資源政策中定義為主體的帳戶可以呼叫 `PutAuditEvents` API，將事件傳送至您的通道。如果資源擁有者的 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。對於方向整合，CloudTrail 會自動新增合作夥伴 AWS 的帳戶 IDs，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，您必須指定至少一個 AWS 帳戶 ID 作為委託人，並且可以選擇輸入外部 ID 以防止混淆代理人。

   > **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. 針對解決方案整合，選擇新增 AWS 帳戶以指定 AWS 帳戶 ID，以在政策中新增為委託人。

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。如需如何在 中使用標籤的詳細資訊 AWS，請參閱《》中的標記 AWS 資源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)。沒有檢閱頁面。CloudTrail 會建立整合，但您必須提供通道 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。

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。活動事件傳送後，您可以使用 CloudTrail Lake 來搜尋、查詢和分析從應用程式記錄的資料。您的事件資料包含與 CloudTrail 事件承載相符的欄位，例如 `eventVersion`、`eventSource` 和 `userIdentity`。

## 建立與主控台的自訂整合

您可以使用 CloudTrail 來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。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，並提供您的通道 ARN 和事件承載。使用 `PutAuditEvents` API 將應用程式活動擷取到 CloudTrail 之後，您可以使用 CloudTrail Lake 來搜尋、查詢和分析從應用程式記錄的資料。

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
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 帳戶，以指定要在頻道的資源政策中新增為主體的每個 AWS 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。如需如何在 中使用標籤的詳細資訊 AWS，請參閱《》中的標記您的 AWS 資源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)。沒有檢閱頁面。CloudTrail 會建立整合，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，將您的活動事件擷取到 CloudTrail 中。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、希望 CloudTrail 新增的事件承載，以及外部 ID (如有為您的資源政策指定)。將事件擷取到 CloudTrail 之前，請確定事件承載中沒有任何敏感或個人識別資訊。您擷取到 CloudTrail 中的事件必須遵循 CloudTrail Lake 整合事件結構描述。

> **Tip**
>
> 使用 AWS CloudShell 以確保您執行的是最新的 AWS APIs。

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)。--audit-events 的值為事件物件的 JSON 陣列。--audit-events 包含來自事件的必要 ID、必要的事件承載 (作為 EventData 的值)，以及選用總和檢查碼 (可在擷取至 CloudTrail 後協助驗證事件完整性)。

```
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

您在 PutAuditEvents 請求中指定為 EventDataChecksum 值的總和檢查碼可協助您驗證 CloudTrail 是否接收到與總和檢查碼相符的事件；這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。下列是 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，CloudTrail 就會拒絕事件並顯示 InvalidChecksum 錯誤。

## 使用 建立、更新和管理 CloudTrail Lake 整合 AWS CLI

本節說明您可以使用 建立、更新和管理 CloudTrail Lake 整合的命令 AWS CLI。

使用 時 AWS CLI，請記住，您的命令會在為設定檔 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 Lake 整合的可用命令

在 CloudTrail Lake 中建立、更新和管理整合的命令包括：

- create-event-data-store 為 外部的事件建立事件資料存放區 AWS。
- delete-channel 刪除用於整合的頻道。
- delete-resource-policy 刪除連接至頻道的資源政策以進行 CloudTrail Lake 整合。
- get-channel 傳回 CloudTrail 頻道的相關資訊。
- get-resource-policy 擷取連接至 CloudTrail 頻道之資源型政策文件的 JSON 文字。
- list-channels 列出目前帳戶中的頻道及其來源名稱。
- put-audit-events 將應用程式事件擷取至 CloudTrail Lake。必要參數 auditEvents接受您希望 CloudTrail 擷取之事件的 JSON 記錄 （ 也稱為承載 ）。每個PutAuditEvents請求最多可以新增 100 個事件 （ 或最多 1 MB)。
- put-resource-policy 將資源型許可政策連接至 CloudTrail 頻道，用於與 外部的事件來源整合 AWS。如需資源型政策的詳細資訊，請參閱AWS CloudTrail 資源型政策範例。
- update-channel 更新所需頻道 ARN 或 UUID 指定的頻道。

如需 CloudTrail Lake 事件資料存放區的可用命令清單，請參閱 事件資料存放區的可用命令。

如需 CloudTrail Lake 查詢的可用命令清單，請參閱 CloudTrail Lake 查詢的可用命令。

如需 CloudTrail Lake 儀表板的可用命令清單，請參閱 儀表板的可用命令。

## AWS 使用 建立從外部記錄事件的整合 AWS CLI

本節說明如何使用 AWS CLI 建立 CloudTrail Lake 整合，以從 外部記錄事件 AWS。

在 中 AWS CLI，您可以在四個命令中建立整合 （ 如果您已有符合條件的事件資料存放區，則為三個）。您用作整合目的地的事件資料存放區必須用於單一區域和單一帳戶；它們不能是多區域，不能記錄組織的事件 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，請參閱在 外部建立與事件來源的整合 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 命令會建立事件資料存放區，記錄來自外部的事件 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。根據預設，事件資料存放區會從所有區域收集事件，但由於這是收集非AWS 事件，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 create-channel 命令以建立通道，讓合作夥伴或來源應用程式將事件傳送到 CloudTrail 中的事件資料存放區。

   通道具有下列元件：

   來源

   CloudTrail 會使用此資訊來判斷代表您將事件資料傳送至 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

目的地是從通道接收事件的 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。若要從 CloudTrail 合作夥伴擷取事件，請將合作夥伴的名稱指定為 --source 的值。若要從外部您自己的應用程式擷取事件 AWS，請將 指定Custom為 的值--source。

```
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 put-resource-policy 命令，將資源政策連接至通道。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。

- 對於方向整合，CloudTrail 要求政策包含合作夥伴 AWS 的帳戶 IDs，並要求您輸入合作夥伴提供的唯一外部 ID。當您使用 CloudTrail 主控台建立整合時，CloudTrail 會自動將合作夥伴 AWS 的帳戶 IDs 新增至資源政策。請參閱合作夥伴的文件，了解如何取得政策所需的 AWS 帳號。
- 對於解決方案整合，您必須指定至少一個 AWS 帳戶 ID 作為委託人，並且可以選擇輸入外部 ID 以防止混淆代理人。

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。
- 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。

```
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 PutAuditEvents API，將您的活動事件擷取到 CloudTrail 中。您將需要 CloudTrail 要新增的事件承載。將事件擷取到 CloudTrail 之前，請確定事件承載中沒有任何敏感或個人識別資訊。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。--audit-events 的值為事件物件的 JSON 陣列。--audit-events 包含來自事件的必要 ID、必要的事件承載 (作為 EventData 的值)，以及選用總和檢查碼 (可在擷取至 CloudTrail 後協助驗證事件完整性)。

```
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。get-channel 的輸出顯示 CloudTrail 接收到事件的最新時間戳記。

```
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

您在 PutAuditEvents 請求中指定為 EventDataChecksum 值的總和檢查碼可協助您驗證 CloudTrail 是否接收到與總和檢查碼相符的事件；這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。下列是 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，CloudTrail 就會拒絕事件並顯示 InvalidChecksum 錯誤。

## 使用 更新頻道 AWS CLI

本節說明如何使用 AWS CLI 更新 CloudTrail Lake 整合的頻道。您可以執行 update-channel命令來更新頻道的名稱，或指定不同的目的地事件資料存放區。您無法更新通道的來源。

當您執行 命令時，需要 --channel 參數。

以下是示範如何更新頻道名稱和目的地的範例。

```
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 的整合 AWS CLI

本節說明如何執行 `delete-channel`命令來刪除 CloudTrail Lake 整合的頻道。如果您想要停止擷取外部的合作夥伴或其他活動事件，您可以刪除頻道 AWS。您要刪除的通道的 ARN 或通道 ID (ARN 字尾) 是必要項目。

下列範例顯示如何刪除頻道。

```
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 |
| Netskope | `NetskopeCloudExchange` | 解決方案 |

| 合作夥伴名稱 (主控台) | 來源名稱 (API) | 整合類型 |
| --- | --- | --- |
| 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. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
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 Lake 整合事件結構描述

下表說明符合 CloudTrail 事件記錄內容的必要和選用結構描述元素。eventData 的內容由您的事件提供；其他欄位則在擷取後由 CloudTrail 提供。

CloudTrail 記錄管理、資料和網路活動事件的內容 將詳細說明 CloudTrail 事件記錄內容。

- 擷取後由 CloudTrail 提供的欄位
- 您的事件提供的欄位

CloudTrail 會在擷取後提供下列欄位：

| 欄位名稱 | 輸入類型 | 需求 | Description |
| --- | --- | --- | --- |
| 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 | 進行`PutAuditEvents` 呼叫 AWS 區域的。 |
| recipientAccountId | string | 必要 | 代表收到此事件的帳戶 ID。CloudTrail 會根據事件承載進行計算，以填入此欄位。 |
| 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，則附錄區塊會包含缺少的資訊，以及缺失的原因。 |

| 欄位名稱 | 輸入類型 | 需求 | Description |
| --- | --- | --- | --- |
| • 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。 |

下列欄位由客戶事件提供：

| 欄位名稱 | 輸入類型 | 需求 | Description |
| --- | --- | --- | --- |
| eventData | - | 必要 | 在 PutAuditEvents 呼叫中傳送 |

| 欄位名稱 | 輸入類型 | 需求 | Description |
| --- | --- | --- | --- |
| | | | 至 CloudTrail 的稽核資料。 |
| • version | string | 必要 | 來自來源的事件版本。<br><br>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。<br><br>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。<br><br>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。<br><br>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。<br><br>長度限制：長度上限為 1024。 |

| 欄位名稱 | 輸入類型 | 需求 | Description |
| --- | --- | --- | --- |
| • 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。<br><br>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。<br><br>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 | Description |
| --- | --- | --- | --- |
| • errorCode | string | 選用 | 代表事件錯誤的字串。<br><br>長度限制：長度上限為 256。 |
| • errorMessage | string | 選用 | 錯誤的描述。<br><br>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。帳戶 ID 必須與擁有頻道 AWS 的帳戶 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。 |

以下範例展示符合 CloudTrail 事件記錄內容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": {
```

```
        "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
        }
    }
}
```

# CloudTrail Lake 儀表板

您可以使用 CloudTrail Lake 儀表板來查看帳戶中事件資料存放區的事件趨勢。CloudTrail Lake 提供下列儀表板類型：

- 受管儀表板 – 您可以檢視受管儀表板，以查看收集管理事件、資料事件或 Insights 事件的事件資料存放區的事件趨勢。這些儀表板會自動提供給您，並由 CloudTrail Lake 管理。CloudTrail 提供 14 個受管儀表板供您選擇。您可以手動重新整理受管儀表板。您無法修改、新增或移除這些儀表板的小工具，不過，如果您想要修改小工具或設定重新整理排程，則可以將受管儀表板儲存為自訂儀表板。
- 自訂儀表板 – 自訂儀表板可讓您查詢任何事件資料存放區類型中的事件。您最多可以將 10 個小工具新增至自訂儀表板。您可以手動重新整理自訂儀表板，也可以設定重新整理排程。
- 反白儀表板 – 啟用反白儀表板可at-a-glance檢視您帳戶中事件資料存放區所收集的 AWS 活動概觀。醒目提示儀表板由 CloudTrail 管理，並包含與您帳戶相關的小工具。反白儀表板上顯示的小工具對於每個帳戶都是唯一的。這些小工具可能會浮現偵測到的異常活動或異常。例如，您的醒目提示儀表板可能包含跨帳戶存取總數小工具，這會顯示異常跨帳戶活動是否增加。CloudTrail 每 6 小時更新一次反白儀表板。儀表板會顯示上次更新後的最後 24 小時的資料。

每個儀表板都包含一或多個小工具，每個小工具提供 SQL 查詢結果的圖形表示。若要檢視小工具的查詢，請選擇檢視和編輯查詢以開啟查詢編輯器。

重新整理儀表板時，CloudTrail Lake 會執行查詢以填入儀表板的小工具。由於執行查詢會產生成本，CloudTrail 會要求您確認與執行查詢相關聯的成本。如需 CloudTrail 定價的詳細資訊，請參閱 CloudTrail 定價。

主題


- 先決條件
- 限制
- 區域支援
- 所需的許可
- 使用 CloudTrail 主控台檢視受管儀表板
- 使用 CloudTrail 主控台啟用反白儀表板
- 使用 CloudTrail 主控台停用反白儀表板
- 使用 CloudTrail 主控台建立自訂儀表板
- 使用 CloudTrail 主控台設定自訂儀表板的重新整理排程
- 使用 CloudTrail 主控台停用自訂儀表板的重新整理排程
- 使用 CloudTrail 主控台變更終止保護
- 使用 CloudTrail 主控台刪除自訂儀表板
- 使用 建立、更新和管理儀表板 AWS CLI

## 先決條件

下列先決條件適用於 CloudTrail Lake 儀表板：

- 若要檢視與使用 Lake 儀表板，您必須建立至少一個 CloudTrail Lake 事件資料存放區。您可以使用主控台 AWS CLI或 SDKs建立事件資料存放區。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。如需使用 建立事件資料存放區的資訊 AWS CLI，請參閱 使用 建立事件資料存放區 AWS CLI。
- 您必須擁有足夠的許可才能檢視、建立、更新和重新整理儀表板。如需詳細資訊，請參閱所需的許可。

## 限制

下列限制適用於 CloudTrail Lake 儀表板：

- 您只能為帳戶中存在的事件資料存放區啟用反白儀表板。
- 您只能檢視存在於您帳戶中的事件資料存放區的受管儀表板。
- 對於自訂儀表板，您只能新增範例小工具或建立新的小工具，以查詢存在於您帳戶中的事件資料存放區。
- AWS Organizations 組織的委派管理員無法檢視或管理管理帳戶所擁有的儀表板。

## 區域支援

支援 CloudTrail Lake 的所有 都支援 AWS 區域 CloudTrail Lake 儀表板。

下列區域支援醒目提示儀表板上的活動摘要小工具：

- 亞太區域 (東京) 區域 (ap-northeast-1)
- 美國東部 (維吉尼亞北部) (us-east-1)
- 美國西部 （ 奧勒岡 ） 區域 (us-west-1)

支援 AWS 區域 CloudTrail Lake 的所有 都支援所有其他小工具。

如需 CloudTrail Lake 支援區域的詳細資訊，請參閱 CloudTrail Lake 支援的區域。

# 所需的許可

本節說明 CloudTrail Lake 儀表板的必要許可，並討論兩種 IAM 政策類型：

- 身分型政策，可讓您執行建立、管理和刪除儀表板的動作。
- 以資源為基礎的政策，允許 CloudTrail 在儀表板重新整理時在您的事件資料存放區上執行查詢，並代表您執行自訂儀表板和反白儀表板的排程重新整理。當您使用 CloudTrail 主控台建立儀表板時，您可以選擇連接資源型政策。您也可以執行 AWS CLI `put-resource-policy`命令，將資源型政策新增至事件資料存放區或儀表板。

## 身分型政策需求

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

若要檢視和管理 CloudTrail Lake 儀表板，您需要下列其中一個政策：

- `CloudTrailFullAccess` 受管政策。
- `AdministratorAccess` 受管政策。
- 自訂政策，其中包含以下各節所述的一或多個特定許可。

主題

- 建立儀表板所需的許可
- 更新儀表板所需的許可
- 重新整理儀表板所需的許可

### 建立儀表板所需的許可

下列範例政策提供建立儀表板所需的最低許可。將*###*、*##*、*account-id* 和 *eds-id* 取代為組態的值。

- `StartQuery` 只有在請求包含小工具時，才需要 許可。為小工具查詢中包含的所有事件資料存放區提供`StartQuery`許可。
- `StartDashboardRefresh` 只有在儀表板有重新整理排程時，才需要 許可。
- 對於反白儀表板，發起人必須擁有帳戶中所有事件資料存放區的`StartQuery`許可。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateDashboard",
                "cloudtrail:StartDashboardRefresh",
                "cloudtrail:StartQuery"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-1:111111111111:dashboard/*",
                "arn:aws:cloudtrail:us-east-1:111111111111:eventdatastore/eds-id"
            ]
        }
    ]
}
```

更新儀表板所需的許可

下列範例政策提供更新儀表板所需的最低許可。將*###*、*##*、*account-id* 和 *eds-id* 取代為組態的值。

- StartQuery 只有在請求包含小工具時，才需要 許可。為小工具查詢中包含的所有事件資料存放區提供StartQuery許可。
- StartDashboardRefresh 只有在儀表板有重新整理排程時，才需要 許可。
- 對於反白儀表板，發起人必須擁有帳戶中所有事件資料存放區的StartQuery許可。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
```

```
            "Action": [
                "cloudtrail:UpdateDashboard",
                "cloudtrail:StartDashboardRefresh",
                "cloudtrail:StartQuery"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-1:111111111111:dashboard/*",
                "arn:aws:cloudtrail:us-east-1:111111111111:eventdatastore/eds-id"
            ]
        }
    ]
}
```

重新整理儀表板所需的許可

下列範例政策提供重新整理儀表板所需的最低許可。將*###*、*##*、*## ID*、*#####*和 *eds-id* 取代為組態的值。

- 對於自訂儀表板和醒目提示儀表板，發起人必須具有 cloudtrail:StartDashboardRefresh permissions。
- 對於受管儀表板，發起人必須擁有重新整理所涉及事件資料存放區的cloudtrail:StartDashboardRefresh許可和cloudtrail:StartQuery許可。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:StartDashboardRefresh",
                "cloudtrail:StartQuery"
            ],
            "Resource": [
                "arn:aws:cloudtrail:us-east-1:111111111111:dashboard/dashboard-
name",
                "arn:aws:cloudtrail:us-east-1:111111111111:eventdatastore/eds-id"
            ]
```

```
        }
    ]
}
```

## 儀表板和事件資料存放區的資源型政策

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。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。

若要在手動或排程重新整理期間對儀表板執行查詢，您必須將資源型政策連接至與儀表板上小工具相關聯的每個事件資料存放區。這可讓 CloudTrail Lake 代表您執行查詢。當您建立自訂儀表板，或使用 CloudTrail 主控台啟用反白儀表板時，CloudTrail 可讓您選擇要套用許可的事件資料存放區。如需資源型政策的詳細資訊，請參閱 範例：允許 CloudTrail 執行查詢以重新整理儀表板。

若要設定儀表板的重新整理排程，您必須將資源型政策連接至儀表板，以允許 CloudTrail Lake 代表您重新整理儀表板。當您設定自訂儀表板的重新整理排程，或使用 CloudTrail 主控台啟用反白儀表板時，CloudTrail 可讓您選擇將資源型政策連接至儀表板。如需政策範例，請參閱 儀表板的資源型政策範例。

您可以使用 CloudTrail 主控台、 AWS CLI或 PutResourcePolicy API 操作來連接資源型政策。

## 解密事件資料存放區中資料的 KMS 金鑰許可

如果查詢的事件資料存放區使用 KMS 金鑰加密，請確定 KMS 金鑰政策允許 CloudTrail 解密事件資料存放區中的資料。下列範例政策陳述式允許 CloudTrail 服務主體解密事件資料存放區。

```
{
      "Sid": "AllowCloudTrailDecryptAccess",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

# 使用 CloudTrail 主控台檢視受管儀表板

CloudTrail Lake 提供受管儀表板，顯示收集管理事件、資料事件和 Insights 事件的事件資料存放區的事件趨勢。這些儀表板由 CloudTrail Lake 管理。您無法修改、新增或移除這些儀表板的小工具，不過，如果您想要修改小工具或設定重新整理排程，則可以將受管儀表板儲存為自訂儀表板。

> **Note**
>
> 您只能檢視存在於您帳戶中的事件資料存放區的受管儀表板。

檢視受管儀表板

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
2. 在左側導覽窗格中，選擇 Lake 下方的儀表板。
3. 選擇受管和自訂儀表板索引標籤。
4. 從受管儀表板中，選擇您要檢視的儀表板。如需詳細資訊，請參閱可用的受管儀表板。

   > **Note**
   >
   > 下拉式清單只會顯示所選儀表板的相關事件資料存放區。例如，如果您選擇著重於資料事件的儀表板，例如 S3 資料事件，下拉式清單只會顯示設定為收集資料事件的事件資料存放區。

5. 選擇儀表板的事件資料存放區。重新整理儀表板時，CloudTrail 將在此儀表板上執行查詢。
6. 若要檢視小工具的查詢，請選擇小工具底部的檢視和編輯查詢。
7. 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 CloudTrail 定價的詳細資訊，請參閱 AWS CloudTrail 定價。

8. 選擇重新整理圖示以填入儀表板小工具的圖形。每個小工具都會指出重新整理的狀態。

## 將受管儀表板儲存為自訂儀表板

您無法修改受管儀表板，但可以將副本儲存為自訂儀表板。這可讓您設定儀表板的重新整理排程，並修改小工具。

將受管儀表板儲存為自訂儀表板

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
2. 在左側導覽窗格中，選擇 Lake 下方的儀表板。
3. 選擇受管和自訂儀表板索引標籤。
4. 選擇您要建立複本的受管儀表板。
5. 選擇另存為新儀表板。
6. 提供名稱以識別儀表板。
7. （選用）在標籤區段中，您最多可以新增 50 個標籤金鑰對，以協助您識別和排序儀表板。如需如何在 中使用標籤的詳細資訊 AWS，請參閱《標記 AWS 資源使用者指南》中的標記 AWS 資源。
8. 針對許可，選擇您要套用許可的事件資料存放區。由於 CloudTrail 執行查詢以填入儀表板上小工具的資料，CloudTrail 需要許可，才能在與儀表板小工具相關聯的事件資料存放區上執行查詢。針對此步驟中選取的每個事件資料存放區，CloudTrail 會將資源型政策連接至事件資料存放區，以允許 CloudTrail 執行查詢。如果您不想允許許可，您可以取消選取事件資料存放區。
9. 選擇 Create dashboard (建立儀表板)。

建立自訂儀表板後，您可以新增小工具、移除小工具，以及設定儀表板的重新整理排程。

## 可用的受管儀表板

本節提供可用受管儀表板的相關資訊，並提供每個儀表板上特色小工具的相關資訊。

可用的受管儀表板：

- 安全性監控儀表板
- IAM 活動儀表板
- 使用者活動儀表板
- 豐富事件儀表板
- 錯誤分析儀表板
- EC2 活動儀表板

- Organizations 活動儀表板
- 資源變更儀表板
- 資料事件概觀儀表板
- Lambda 資料事件儀表板
- DynamoDB 資料事件儀表板
- S3 資料事件儀表板
- Insights 事件儀表板
- 管理事件儀表板
- 概觀儀表板

安全性監控儀表板

此儀表板提供關鍵安全重點小工具的集中式檢視，例如最高存取遭拒事件、失敗的主控台登入嘗試及其相關聯的 IP 地址、根使用者主控台登入嘗試、破壞性動作、跨帳戶存取和其他關鍵安全重點小工具。它提供快速的事件偵測和回應，以增強您的整體安全狀態。

此儀表板適用於收集管理事件的事件資料存放區，並包含下列小工具：

拒絕最高存取事件

追蹤最常發生的拒絕存取事件，依 API 分組。

ConsoleLogin嘗試失敗

追蹤一段時間內失敗主控台登入嘗試的趨勢，其中包含 MFA 和非 MFA 驗證來電者的明細。

依 IP 地址的失敗 ConsoleLogin 嘗試

追蹤與失敗主控台登入嘗試相關聯的 IP 地址，並依失敗的登入計數顯示最違規的 IP 地址。

根使用者 ConsoleLogin 嘗試

追蹤根使用者隨著時間嘗試主控台登入的頻率。

破壞性動作

追蹤一段時間內刪除操作的頻率。

熱門跨帳戶存取

依發起人帳戶 ID 和動作追蹤前 個跨帳戶活動。

停用 MFA 的使用者

追蹤最近停用 MFA 的使用者。

最近的 EC2 SecurityGroup 和 NetworkAcl 變更

追蹤最新的 EC2 SecurityGroup 和 NetworkAcl 變更。

允許公開存取的最近 EC2 SecurityGroup 變更

追蹤具有允許公有 (0.0.0.0/0) 存取規則的最新 EC2 安全群組。

潛在的 CloudTrail 停用動作

追蹤近期可能會中斷 CloudTrail 記錄的動作。

IAM 活動儀表板

此儀表板可讓您查看常用的 IAM APIs、API 錯誤、IAM 實體的變更，以及最高呼叫者 IP 地址，進而識別非預期的 IAM 動作和合規問題。

此儀表板適用於收集管理事件的事件資料存放區，並包含下列小工具：

熱門 IAM APIs

追蹤最常用的 IAM APIs。

最高 IAM 呼叫者

追蹤最常用的 IAM API 呼叫者。

IAM 成功與失敗趨勢

追蹤一段時間內成功和失敗 IAM API 呼叫的趨勢。

排名前列的 IAM API 錯誤

追蹤呼叫 IAM APIs 時最常見的錯誤。

Top AccessDenied IAM APIs

追蹤因存取遭拒錯誤而失敗的最常見 IAM API 呼叫。

IAM 呼叫的熱門 IP 地址

追蹤進行 IAM API 呼叫的主要來源 IP 地址。

最近的 IAM 政策變更

追蹤 IAM 政策的最新變更，依促進變更的特定 IAM API 操作、與政策變更相關聯的 IAM 資源（使用者、角色或群組），以及使用的政策名稱或 ARN 進行分類。

最近的 IAM 使用者變更

追蹤 IAM 使用者的最新變更，依特定 IAM API 分類，以促進使用者管理、受變更影響的 IAM 使用者，以及事件時間。

最高擔任的 IAM 角色

追蹤最常擔任的 IAM 角色。

使用者活動儀表板

此儀表板提供使用者活動趨勢的可見性、主要作用中使用者、使用者流量模式、存取遭拒的使用者、最近的使用者操作、執行破壞性活動和 IAM 政策變更的使用者，以及特殊權限使用者動作等關鍵領域的洞見。它有助於偵測意外的使用者動作和安全性風險。

此儀表板適用於收集管理事件的事件資料存放區，並包含下列小工具：

使用者 ARN 的使用者活動趨勢

追蹤使用者 ARN 隨著時間的使用者活動趨勢。

依 API 的使用者活動趨勢

追蹤 API 隨時間推移的使用者活動趨勢。

最近的使用者活動

追蹤最新的使用者動作。

發生錯誤的熱門使用者

追蹤錯誤數目最高的使用者。

出現 AccessDenied 錯誤的熱門使用者

追蹤 AccessDenied 錯誤數目最高的使用者。

進行破壞性動作的熱門使用者

追蹤進行最高數量破壞性動作的使用者。

變更 IAM 政策的熱門使用者

追蹤經常執行 IAM 政策變更的 IAM 使用者。

潛在 IAM 特殊權限使用者執行的熱門動作

追蹤高權限 IAM 使用者最常見的動作，例如管理員。

豐富事件儀表板

此豐富的事件儀表板提供已標記資源、主體活動和 AWS 全域條件索引鍵的趨勢洞察。這些洞見可協助您分析最常見的資源和主體標籤分佈，以及在請求內容中角色工作階段、請求和主體中常用的全域條件索引鍵。

此儀表板適用於收集管理事件的事件資料存放區，並包含下列小工具：

隨著時間的推移，富集事件

追蹤一段時間內擴充事件的計數。

最常用的資源標籤索引鍵值對

顯示富集事件中最常使用的資源標籤鍵值對。

與相關聯資源和使用者的最常見資源標籤鍵值對

顯示最常使用的資源標籤鍵/值對，顯示哪些資源使用這些標籤，以及哪些使用者與其相關聯。

最常見的主體標籤鍵值對

顯示富集事件中最常用的主體標籤鍵值對。

依委託人標籤索引鍵值對分組的最常存取遭拒動作

顯示依主體標籤索引鍵/值對分組的最頻繁存取拒絕動作，橫跨豐富事件。

IAM 全域條件索引鍵中最常見的主體屬性

顯示委託人屬性最常用的 IAM 全域條件索引鍵，顯示其索引鍵值對和所有事件的計數。

IAM 全域條件索引鍵中最常見的請求屬性

顯示請求屬性最常用的 IAM 全域條件索引鍵，顯示其索引鍵值對和所有事件的計數。

IAM 全域條件索引鍵中最常見的角色工作階段屬性

顯示角色工作階段屬性最常用的 IAM 全域條件金鑰，顯示其金鑰值對和所有事件的計數。

錯誤分析儀表板

此儀表板提供跨 服務、APIs、使用者、錯誤代碼和限流 APIs錯誤趨勢的完整洞見。可見性可快速識別和疑難排解潛在可用性問題，以獲得最佳系統效能。

此儀表板適用於收集管理事件的事件資料存放區，並包含下列小工具：

服務錯誤計數

依服務追蹤活動的錯誤計數。

依 API 的錯誤計數

依 API 追蹤活動的錯誤計數。

依錯誤碼排序的熱門錯誤

依錯誤碼追蹤最常發生的錯誤。

依錯誤訊息列出的最高錯誤

依錯誤訊息追蹤最常見的錯誤。

熱門AccessDenied錯誤

使用最常報告的存取遭拒錯誤追蹤 APIs。

依 API 列出的最高限流錯誤

使用最常報告的調節錯誤追蹤 APIs。

發生錯誤的熱門使用者

使用最常報告的錯誤追蹤使用者。

EC2 活動儀表板

此儀表板提供 EC2 管理活動的全面可見性，例如 API 趨勢、存取錯誤、熱門執行個體啟動器、安全變更和網路修改。洞見有助於識別安全風險和操作問題。

此儀表板適用於收集管理事件的事件資料存放區，並包含下列小工具：

EC2 執行個體管理活動概觀

監控指定時間內 EC2 執行個體管理活動的概觀，並反白顯示啟動、停止和終止等關鍵操作。

EC2 API 成功與失敗趨勢

追蹤一段時間內成功和失敗 EC2 API 呼叫的趨勢。

熱門 EC2 錯誤

追蹤 EC2 API 呼叫期間最常發生的錯誤代碼。

熱門 EC2 AccessDenied 事件

追蹤存取遭拒錯誤最多的 EC2 APIs。

啟動 EC2 執行個體的熱門使用者

追蹤在啟動新的 EC2 執行個體時最活躍的使用者。

最近的 EC2 SecurityGroup 和 NetworkInterface 變更

追蹤最新的 EC2 安全群組和網路介面變更。

最近的 VPC 管理和路由表變更

追蹤最新的 VPC 管理活動和路由表變更。

根使用者最近的 EC2 動作

追蹤具有高權限許可的根使用者執行的最新 EC2 動作。

Organizations 活動儀表板

此儀表板專為組織事件資料存放區而設計，提供組織活動和趨勢的可見性，包括對作用中成員、帳戶管理、存取模式、政策變更，以及使用之常用服務和 APIs洞察。

此儀表板可用於組織事件資料存放區，並包含下列小工具：

組織中的活動趨勢

追蹤整個 AWS Organizations 組織隨時間的整體活動趨勢，提供高或低活動層級期間的可見性。

成員帳戶管理摘要

追蹤組織內成員帳戶管理活動的分佈，根據每個活動類型的計數進行分類。

整個組織最常使用的服務

追蹤整個組織中 AWS 服務 已使用最多的 。

依服務分類的最作用中帳戶

使用 AWS 服務 整個組織的 追蹤最活躍的帳戶。

整個組織最常使用的 APIs

反白顯示在整個組織中最常調用 AWS APIs。

最作用中的成員帳戶

追蹤組織內已呈現最高活動計數的成員帳戶。

存取整個組織的拒絕錯誤趨勢

追蹤一段時間內組織內發生的存取遭拒錯誤模式。

存取遭拒錯誤最多的帳戶

追蹤組織內遇到最多存取遭拒錯誤的帳戶。

最近的服務控制政策變更

追蹤對組織內服務控制政策 SCPs) 所做的最新變更。

資源變更儀表板

此儀表板提供資源管理活動的全方位檢視，監控跨服務佈建、刪除和修改的趨勢。它會反白顯示重大變更，包括透過 CloudFormation手動進行的變更，以及對 S3 儲存貯體和 KMS 存取等政策所做的變更。

此儀表板適用於收集管理事件的事件資料存放區，並包含下列小工具：

資源建立和刪除趨勢

追蹤帳戶內資源隨時間的建立和刪除。

執行資源建立的熱門使用者

追蹤最主動建立新資源的使用者。

用於建立資源APIs

追蹤最常用於在帳戶中建立新資源的 APIs。

用於刪除資源APIs

追蹤最常用於刪除帳戶中資源的 APIs。

在 CloudFormation 外部建立的最新資源

追蹤在 CloudFormation 控管之外建立的新資源，強調非透過 CloudFormation 範本管理的變更。

使用主控台進行的最新資源變更

追蹤透過 對 資源所做的最新變更 AWS 管理主控台。

最新的 S3 儲存貯體存取變更

追蹤最新的 S3 儲存貯體存取變更。

最新的 KMS 金鑰存取變更

追蹤最新的 KMS 金鑰政策變更。

資料事件概觀儀表板

此儀表板提供事件資料存放區中資料事件的集中檢視，包括整體活動趨勢、熱門服務、APIs、區域、限流資料平面 APIs 和主要資料平面使用者。此儀表板可協助您監控資料平面 API 活動，以進行稽核和故障診斷。

此儀表板適用於收集資料事件的事件資料存放區，並包含下列小工具：

整體資料事件趨勢

追蹤帳戶內隨時間發生的整體資料事件趨勢。

產生資料事件的熱門服務

追蹤在帳戶中產生最高資料活動量的服務。

產生資料事件APIs

追蹤在帳戶中產生最高資料活動量的 APIs。

產生資料事件的熱門區域

追蹤在帳戶中產生最高資料活動量的區域。

最高限流資料平面 APIs

追蹤帳戶內經常發生限流的資料平面 APIs。

資料平面 APIs 的熱門使用者

追蹤在帳戶中使用最多資料平面 APIs 的前幾名使用者。

Lambda 資料事件儀表板

此儀表板提供 Lambda 資料平面 API 活動的可見性，包括最高使用者、經常調用的函數、常見的 API 錯誤。這些洞見可協助您稽核 Lambda 用量、偵測異常，以及降低營運或安全風險。

此儀表板適用於收集 Lambda 資料事件的事件資料存放區，並包含下列小工具：

Lambda 資料平面 API 活動

追蹤帳戶內 Lambda 資料平面 API 活動的趨勢。

Lambda 調用成功與失敗趨勢

追蹤一段時間內成功和失敗 Lambda 調用的趨勢。

Lambda 調用的主要使用者

追蹤在整個帳戶中對 Lambda 函數進行最多調用的使用者。

最高調用 Lambda 函數

追蹤帳戶內最常調用的 Lambda 函數。

前 10 個 Lambda 調用 API 錯誤

追蹤 Lambda 調用 API 呼叫期間遇到的前 10 個錯誤。

Lambda 調用的最限流使用者

追蹤遇到 Lambda 調用限流事件次數最高的使用者。

DynamoDB 資料事件儀表板

此儀表板提供 DynamoDB 資料平面 API 活動的可見性，包括使用趨勢、熱門 APIs，以及涉及使用者和資料表的限流模式。這些洞見可協助您稽核 DynamoDB 用量、偵測異常，並降低營運或安全風險。

此儀表板適用於收集 DynamoDB 資料事件的事件資料存放區，並包含下列小工具：

DynamoDB 帳戶資料活動

追蹤帳戶內隨時間發生的 DynamoDB 資料事件趨勢。

DynamoDB 資料平面 APIs成功與失敗趨勢

追蹤一段時間內 DynamoDB 資料平面 API 呼叫成功和失敗的趨勢。

前 10 大 DynamoDB 資料平面 APIs

列出前 10 個 DynamoDB 資料平面 API 呼叫。

DynamoDB 資料平面 APIs 的熱門使用者

追蹤在帳戶中對 DynamoDB 資料平面 APIs 進行最高次數呼叫的使用者。

前 10 個 DynamoDB 資料平面 API 錯誤

追蹤呼叫 DynamoDB 資料平面 APIs 時發生的前 10 個錯誤。

DynamoDB 資料平面 APIs 的最限流使用者

追蹤呼叫 DynamoDB 資料平面 APIs 時最常限流的使用者。

最高限流 DynamoDB 資料平面 APIs

追蹤帳戶內頻繁調節的 DynamoDB 資料平面 APIs。

最高限流 DynamoDB 資料表

追蹤帳戶中調節速率最高的 DynamoDB 資料表。

S3 資料事件儀表板

此儀表板提供 S3 資料平面 API 活動的可見性，包括用量趨勢、最常存取的 S3 物件、熱門 S3 使用者和熱門 S3 動作。這些洞見可協助您稽核 S3 用量、偵測異常，以及降低營運或安全風險。

此儀表板適用於收集 Amazon S3 資料事件的事件資料存放區，並包含下列小工具：

S3 帳戶活動

追蹤 S3 帳戶活動。

最常存取的物件

列出最常存取的 S3 物件。

S3 最高使用者

追蹤前 個 S3 使用者。

最佳 S3 動作

追蹤前 個 S3 動作。

Insights 事件儀表板

此儀表板可讓您依類型了解 Insights 事件的整體明細，以及產生這些事件類型的熱門使用者和服務。此外，它會顯示 Insights 事件的每日計數，以及 Insights 指標的 30 天歷史檢視。

> **Note**
>
> - 您第一次在來源事件資料存放區上啟用 CloudTrail Insights 後，如果偵測到異常活動，CloudTrail 可能需要最多 7 天才能傳遞第一個 Insights 事件。
> - 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。

此儀表板適用於收集 Insights 事件的事件資料存放區，並包含下列小工具：

Insight 類型

依 Insights 類型追蹤事件。

依日期的洞見

依日期追蹤 Insights 事件。

API 呼叫率 依事件來源的 Insights

依事件來源追蹤 API 呼叫率 Insights。若要檢視此小工具的資料，您的 Insights 事件資料存放區必須設定為收集 API 呼叫速率的 Insights。

事件來源的 API 錯誤率 Insights

依事件來源追蹤 API 錯誤率 Insights。若要檢視此小工具，您的 Insights 事件資料存放區必須設定為收集 API 錯誤率的 Insights。

依最高使用者的洞見

列出產生 Insights 事件之請求的前 位使用者。

Insights 事件

列出最近的 Insights 事件。

管理事件儀表板

此儀表板重點介紹有關存取遭拒事件、破壞性動作、主控台登入事件、使用者的熱門錯誤、TLS 版本用量，以及使用者過期的 TLS 呼叫的洞察。

此儀表板適用於收集管理事件的事件資料存放區，並包含下列小工具：

拒絕最高存取事件

追蹤導致存取遭拒錯誤的熱門事件。

使用者的熱門錯誤

依使用者追蹤熱門錯誤。

主控台登入事件

顯示主控台登入事件。

破壞性動作

追蹤導致破壞性動作的動作。

TLS 版本控制

顯示 TLS 版本。

使用者過期的 TLS 呼叫

依使用者使用過期的 TLS 版本追蹤呼叫。

概觀儀表板

此儀表板重點介紹有關存取遭拒事件、破壞性動作、主控台登入事件、使用者的熱門錯誤、TLS 版本用量，以及使用者過期的 TLS 呼叫的洞察。

此儀表板適用於收集管理事件的事件資料存放區，並包含下列小工具：

帳戶活動

追蹤您帳戶的讀取和寫入活動。

熱門錯誤

列出最常見的錯誤。

最作用中的區域

顯示最作用中的 AWS 區域。

熱門服務

顯示最佳服務。

大多數限流事件

列出最限流的事件。

最高使用者

列出最高使用者。

## 使用 CloudTrail 主控台啟用反白儀表板

啟用醒目提示儀表板，檢視您帳戶中事件資料存放區所收集的 AWS 活動at-a-glance。醒目提示儀表板由 CloudTrail 管理，並包含與您帳戶相關的小工具。醒目提示儀表板上顯示的小工具對於每個帳戶都是唯一的。這些小工具可能會浮現偵測到的異常活動或異常。例如，您的 Highlights 儀表板可能包含跨帳戶存取總數小工具，顯示異常跨帳戶活動是否增加。

CloudTrail 每 6 小時更新一次反白儀表板。儀表板會顯示上次更新後的最後 24 小時的資料。

> **Note**
>
> 您只能為帳戶中存在的事件資料存放區啟用反白儀表板。
> 您無法設定反白儀表板的重新整理排程，或新增或移除小工具。

### 啟用反白儀表板

使用下列程序來啟用反白儀表板。

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
2. 在左側導覽窗格中，選擇 Lake 下方的儀表板。
3. 選擇反白標籤。
4. 由於執行查詢會產生 CloudTrail 費用，CloudTrail 會要求您在啟用反白儀表板之前檢閱成本資訊。如需有關 CloudTrail 定價的資訊，請參閱 AWS CloudTrail 定價。

   選擇同意並啟用反白以啟用反白儀表板。
5. 針對許可，選擇您要套用許可的事件資料存放區。CloudTrail 需要許可，才能在事件資料存放區上執行查詢，並代表您重新整理儀表板。為了提供許可，CloudTrail 會將預設資源型政策連接到此步驟中選取的每個事件資料存放區，以允許 CloudTrail 在事件資料存放區上執行查詢。CloudTrail 會將資源型政策連接到儀表板，以允許 CloudTrail 每 6 小時重新整理儀表板。

您可以從事件資料存放區的詳細資訊頁面修改以資源為基礎的政策。您可以從儀表板的動作功能表中選取編輯政策，以修改儀表板的資源型政策。

6. 選擇確認。

當您啟用反白儀表板時，會自動啟用終止保護。終止保護可防止儀表板意外遭到刪除。如果您想要停用儀表板，則需要停用終止保護。

## 使用 CloudTrail 主控台停用反白儀表板

本節說明如何停用反白儀表板。由於會自動為 Highlights 儀表板啟用終止保護，因此您必須先停用終止保護，然後停用 Highlights 儀表板。

停用反白儀表板

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
2. 在左側導覽窗格中，選擇 Lake 下方的儀表板。
3. 選擇反白標籤。
4. 在動作中，選擇變更終止保護。
5. 選擇停用。
6. 選擇儲存。
7. 在動作中，選擇停用反白顯示。

## 使用 CloudTrail 主控台建立自訂儀表板

您可以建立自訂儀表板，並為每個自訂儀表板新增最多 10 個小工具。您可以選擇新增範例小工具，或從 SQL 查詢建立新的小工具。

新增小工具完成後，您可以手動重新整理儀表板或設定重新整理排程。

欲建立自訂儀表板

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
2. 在左側導覽窗格中，選擇 Lake 下方的儀表板。
3. 選擇受管和自訂儀表板索引標籤。

4. 選擇建置自己的儀表板。
5. 提供儀表板名稱以識別您的儀表板。
6. 針對許可，選擇您要套用許可的事件資料存放區。由於 CloudTrail 會執行查詢來填入儀表板上小工具的資料，因此 CloudTrail 需要許可，才能在與儀表板小工具相關聯的事件資料存放區上執行查詢。對於此步驟中選取的每個事件資料存放區，CloudTrail 會將資源型政策連接至事件資料存放區，讓 CloudTrail 能夠在此儀表板的事件資料存放區上執行查詢。
7. （選用）在標籤區段中，您最多可以新增 50 個標籤金鑰對，以協助您識別和排序儀表板。如需如何在 中使用標籤的詳細資訊 AWS，請參閱《標記 AWS 資源使用者指南》中的標記 AWS 資源。
8. 選擇 Create dashboard (建立儀表板)。

   接下來，您可以新增小工具並設定重新整理排程。

主題

- 使用 CloudTrail 主控台新增範例小工具
- 使用 CloudTrail 主控台從 SQL 查詢建立新的小工具
- 使用 CloudTrail 主控台從儀表板移除小工具

## 使用 CloudTrail 主控台新增範例小工具

本節說明如何將範例小工具新增至儀表板。您最多可以將 10 個小工具新增至自訂儀表板。

> **Note**
>
> 範例小工具僅限於存在於您帳戶中的單一事件資料存放區。若要在帳戶中的多個事件資料存放區之間進行查詢，請建立新的小工具。

將範例小工具新增至儀表板

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
2. 在左側導覽窗格中，選擇 Lake 下方的儀表板。
3. 選擇受管和自訂儀表板索引標籤。
4. 在自訂儀表板中，選擇您要新增小工具的儀表板。
5. 在動作中，選擇編輯儀表板。

6. 在動作中，選擇新增範例小工具。
7. 選擇您要執行查詢的事件資料存放區。您只能選擇存在於您帳戶中的事件資料存放區。
8. 選擇您要新增的範例小工具。根據預設，會顯示所有範例小工具。您可以依小工具類型（例如 IAM 小工具）進行篩選。
9. 選擇檢視查詢以檢視所選小工具的查詢。
10. 選擇新增至儀表板，將小工具新增至儀表板。
11. 選擇儲存以儲存儀表板。

## 使用 CloudTrail 主控台從 SQL 查詢建立新的小工具

本節說明如何透過撰寫或貼上 SQL 查詢並選擇圖表類型來建立新的小工具。您最多可以將 10 個小工具新增至自訂儀表板。

從 SQL 查詢建立新的小工具

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
2. 在左側導覽窗格中，選擇 Lake 下方的儀表板。
3. 選擇受管和自訂儀表板索引標籤。
4. 在自訂儀表板中，選擇您要為其建立小工具的儀表板。
5. 在動作中，選擇編輯儀表板。
6. 在動作中，選擇建立新的小工具。
7. 選擇您要執行查詢的事件資料存放區。只要事件資料存放區存在於您的帳戶中，您就可以跨多個事件資料存放區進行查詢。
8. 撰寫或複製 SQL 查詢。

   您也可以提供英文的自然語言提示，然後選擇產生查詢，從您的提示產生 SQL 查詢。如需詳細資訊，請參閱從自然語言提示建立 CloudTrail Lake 查詢。
9. 選擇執行以執行查詢並預覽查詢結果。

> **Note**
>
> 當您執行查詢時，會根據掃描的最佳化和壓縮資料量產生費用。為了協助控制成本，建議您將開始和結束`eventTime`時間戳記新增至查詢，以限制查詢。

10. 選擇視覺化工具索引標籤，以選取小工具的圖表類型。您可以從這些圖表類型中選擇：資料表、長條圖、折線圖和圓餅圖。
11. 選擇新增至儀表板，將小工具新增至儀表板。
12. 選擇儲存以儲存儀表板。

### 使用 CloudTrail 主控台從儀表板移除小工具

本節說明從自訂儀表板移除小工具。

從儀表板移除小工具

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
2. 在左側導覽窗格中，選擇 Lake 下方的儀表板。
3. 選擇受管和自訂儀表板索引標籤。
4. 在自訂儀表板中，選擇您要移除小工具的儀表板。
5. 在動作中，選擇編輯儀表板。
6. 在您要移除的小工具上，選擇移除圖示 (⋮)，然後選擇移除。
7. 選擇儲存以儲存儀表板。

## 使用 CloudTrail 主控台設定自訂儀表板的重新整理排程

本節說明如何設定儀表板重新整理排程。您可以設定重新整理排程，以允許 CloudTrail Lake 每 1 小時、6 小時、12 小時或 24 小時 (1 天） 重新整理儀表板。

當您使用 CloudTrail 主控台設定重新整理排程時，CloudTrail 會將資源型政策連接至儀表板，以允許 CloudTrail 代表您重新整理儀表板。

設定重新整理排程

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
2. 在左側導覽窗格中，選擇 Lake 下方的儀表板。

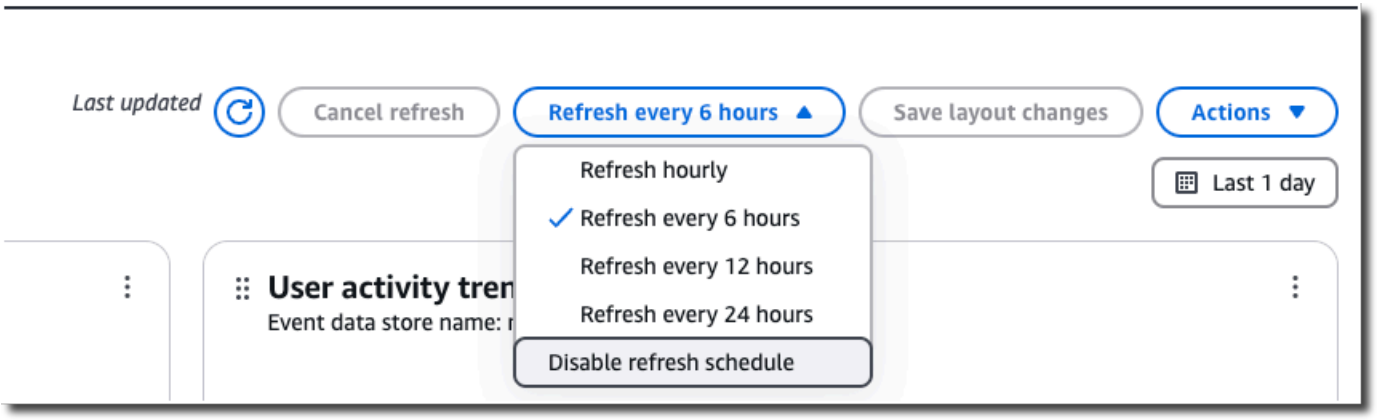
3. 選擇受管和自訂儀表板索引標籤。
4. 在自訂儀表板中，選擇您要為其設定重新整理排程的儀表板。
5. 從下拉式清單中選擇重新整理頻率。
6. 若要建立重新整理排程，CloudTrail 會將資源型政策連接至儀表板，以允許 CloudTrail 代表您重新整理儀表板。展開儀表板資源政策，以檢視 CloudTrail 將連接到儀表板的資源型政策。
7. 由於執行查詢會產生成本，CloudTrail 會要求您確認您希望 CloudTrail 執行排程頻率的查詢。選擇確認以設定重新整理排程。

## 使用 CloudTrail 主控台停用自訂儀表板的重新整理排程

如果您不再希望 CloudTrail 自動重新整理儀表板，而是希望手動重新整理儀表板，您可以停用重新整理排程。

停用重新整理排程

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
2. 在左側導覽窗格中，選擇 Lake 下方的儀表板。
3. 選擇受管和自訂儀表板索引標籤。
4. 在自訂儀表板中，選擇您要停用重新整理排程的儀表板。
5. 從下拉式清單中選擇停用重新整理排程。




## 使用 CloudTrail 主控台變更終止保護

終止保護可防止儀表板意外刪除。如果您想要刪除自訂儀表板，或停用反白儀表板，則必須停用終止保護。

關閉終止保護

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
2. 在導覽窗格中的 Lake 下，選擇儀表板。
3. 選擇您要停用終止保護的儀表板。
4. 在動作中，選擇變更終止保護。
5. 選擇停用。
6. 選擇儲存。

開啟終止保護

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
2. 在導覽窗格中的 Lake 下，選擇儀表板。
3. 選擇您要啟用終止保護的儀表板。
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 CloudTrail 主控台刪除自訂儀表板

本節說明如何使用 CloudTrail 刪除儀表板。

> **Note**
>
> 如果啟用終止保護，則無法刪除事件資料存放區。

刪除儀表板

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
2. 在導覽窗格的 Lake 下，選擇儀表板。
3. 選擇受管和自訂儀表板索引標籤。

4. 選擇您要刪除的自訂儀表板。
5. 對於 Actions (動作)，選擇 Delete (刪除)。
6. 選擇刪除以確認您想要刪除儀表板。

## 使用 建立、更新和管理儀表板 AWS CLI

本節說明可用來建立、更新和管理 CloudTrail Lake 儀表板的 AWS CLI 命令。

使用 時 AWS CLI，請記住，您的命令會在為設定檔 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。

### 儀表板的可用命令

在 CloudTrail Lake 中建立和更新儀表板的命令包括：

- `create-dashboard` 建立自訂儀表板或啟用反白儀表板。
- `update-dashboard` 更新自訂儀表板或醒目提示儀表板。
- `delete-dashboard` 刪除自訂儀表板或醒目提示儀表板。
- `get-dashboard` 會傳回指定儀表板的相關資訊。
- `list-dashboards` 會列出您 AWS 帳戶或指定篩選條件的所有儀表板。
- `start-dashboard-refresh` 會開始重新整理儀表板。
- `get-resource-policy` 取得連接至儀表板的資源型政策。
- `put-resource-policy` 將資源型政策連接到儀表板，以允許 CloudTrail 代表您以非同步方式重新整理儀表板。您也可以將資源型政策連接到事件資料存放區，以允許 CloudTrail 在事件資料存放區上執行查詢，以填入儀表板小工具的資料。
- `delete-resource-policy` 會移除連接至儀表板的資源型政策。
- `add-tags` 新增標籤以識別儀表板。
- `remove-tags` 從儀表板移除標籤。
- `list-tags` 列出儀表板的標籤。

如需 CloudTrail Lake 事件資料存放區的可用命令清單，請參閱 事件資料存放區的可用命令。

如需 CloudTrail Lake 查詢的可用命令清單，請參閱 CloudTrail Lake 查詢的可用命令。

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

主題：

- 使用 建立儀表板 AWS CLI
- 使用 管理儀表板 AWS CLI
- 使用 刪除儀表板 AWS CLI

## 使用 建立儀表板 AWS CLI

本節說明如何使用 `create-dashboard`命令來建立自訂儀表板或醒目提示儀表板。

使用 時 AWS CLI，請記住，您的命令會在為設定檔 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 在手動或排程重新整理期間執行查詢以填入儀表板的小工具。必須授予 CloudTrail 許可，才能在與儀表板小工具相關聯的每個事件資料存放區上執行 `StartQuery`操作。若要提供許可，請執行 `put-resource-policy`命令，將資源型政策連接至每個事件資料存放區，或在 CloudTrail 主控台上編輯事件資料存放區的政策。如需政策範例，請參閱 範例：允許 CloudTrail 執行查詢以重新整理儀表板。

若要設定重新整理排程， CloudTrail 必須授予執行 `StartDashboardRefresh`操作的許可，才能代表您重新整理儀表板。若要提供許可，請執行 `put-resource-policy`操作，將資源型政策連接至儀表板，或在 CloudTrail 主控台上編輯儀表板的政策。如需政策範例，請參閱 儀表板的資源型政策範例。

範例：

- 使用 建立自訂儀表板 AWS CLI
- 使用 啟用反白儀表板 AWS CLI
- 檢視小工具的屬性

### 使用 建立自訂儀表板 AWS CLI

下列程序說明如何建立自訂儀表板、將所需的資源型政策連接至事件資料存放區和儀表板，以及更新儀表板以設定和啟用重新整理排程。

1. 執行 `create-dashboard` 以建立儀表板。

   建立自訂儀表板時，您最多可以傳入 10 個小工具的陣列。小工具提供查詢結果的圖形表示。每個小工具都包含 `ViewProperties`、 `QueryStatement`和 `QueryParameters`。

   - `ViewProperties` – 指定檢視類型的屬性。如需詳細資訊，請參閱檢視小工具的屬性。

- QueryStatement – CloudTrail 在儀表板重新整理時執行的查詢。只要事件資料存放區存在於您的帳戶中，您就可以跨多個事件資料存放區進行查詢。
- QueryParameters – 自訂儀表板支援下列QueryParameters值：$Period$、$StartTime$和 $EndTime$。若要使用 ，請在QueryStatement您要取代 參數的?中QueryParameters放置 。執行查詢時，CloudTrail 會填入參數。

下列範例會建立具有四個小工具的儀表板，每種檢視類型之一。

> **Note**
>
> 在此範例中，？被單引號包圍，因為它與 搭配使用eventTime。根據您執行的作業系統，您可能需要使用逸出引號括住單引號。如需詳細資訊，請參閱 中的使用引號和常值搭配字串 AWS CLI。

```
aws cloudtrail create-dashboard --name AccountActivityDashboard \
--widgets '[
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "TopErrors",
        "View": "Table"
      },
      "QueryStatement": "SELECT errorCode, COUNT(*) AS eventCount FROM eds WHERE
 eventTime > '?' AND eventTime < '?' AND (errorCode is not null) GROUP BY errorCode
 ORDER BY eventCount DESC LIMIT 100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    },
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "MostActiveRegions",
        "View": "PieChart",
        "LabelColumn": "awsRegion",
        "ValueColumn": "eventCount",
        "FilterColumn": "awsRegion"
      },
```

```
     "QueryStatement": "SELECT awsRegion, COUNT(*) AS eventCount FROM eds where
eventTime > '?' and eventTime < '?' GROUP BY awsRegion ORDER BY eventCount LIMIT
100",
     "QueryParameters": ["$StartTime$", "$EndTime$"]
   },
   {
     "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "AccountActivity",
       "View": "LineChart",
       "YAxisColumn": "eventCount",
       "XAxisColumn": "eventDate",
       "FilterColumn": "readOnly"
     },
     "QueryStatement": "SELECT DATE_TRUNC('?', eventTime) AS eventDate,
IF(readOnly, 'read', 'write') AS readOnly, COUNT(*) as eventCount FROM eds WHERE
eventTime > '?' AND eventTime < '?' GROUP BY DATE_TRUNC('?', eventTime), readOnly
ORDER BY DATE_TRUNC('?', eventTime), readOnly",
     "QueryParameters": ["$Period$", "$StartTime$", "$EndTime$", "$Period$",
"$Period$"]
   },
   {
     "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "TopServices",
       "View": "BarChart",
       "LabelColumn": "service",
       "ValueColumn": "eventCount",
       "FilterColumn": "service",
       "Orientation": "Horizontal"
     },
     "QueryStatement": "SELECT REPLACE(eventSource, '.amazonaws.com') AS service,
COUNT(*) AS eventCount FROM eds WHERE eventTime > '?' AND eventTime < '?' GROUP BY
eventSource ORDER BY eventCount DESC LIMIT 100",
     "QueryParameters": ["$StartTime$", "$EndTime$"]
   }
 ]'
```

2. 使用小工具 中包含的每個事件資料存放區所需的資源政策來建立個別檔案QueryStatement。使用下列範例政策陳述式命名檔案 *policy.json*：

將 *123456789012* 取代為您的帳戶 ID，*arn#aws#cloudtrail#us-east-1#123456789012#dashboard/exampleDashboard* 取代為儀表板的 ARN。

如需儀表板資源型政策的詳細資訊，請參閱 範例：允許 CloudTrail 執行查詢以重新整理儀表板。

3. 執行 put-resource-policy命令以連接政策。您也可以在 CloudTrail 主控台上更新事件資料存放區的資源型政策。

   下列範例會將資源型政策連接至事件資料存放區。

```
aws cloudtrail put-resource-policy \
--resource-arn eds-arn \
--resource-policy file://policy.json
```

4. 執行 put-resource-policy命令，將資源型政策連接至儀表板。如需政策範例，請參閱 儀表板的資源型政策範例。

   下列範例會將資源型政策連接至儀表板。將 *account-id* 取代為您的帳戶 ID，將 *dashboard-arn* 取代為儀表板的 ARN。

```
aws cloudtrail put-resource-policy \
--resource-arn dashboard-arn \
--resource-policy '{"Version": "2012-10-17",        "Statement":
 [{"Sid": "DashboardPolicy", "Effect": "Allow", "Principal": { "Service":
 "cloudtrail.amazonaws.com" }, "Action": "cloudtrail:StartDashboardRefresh",
 "Condition": { "StringEquals": { "AWS:SourceArn": "dashboard-arn",
 "AWS:SourceAccount": "account-id"}}}]}'
```

5. 執行 update-dashboard命令，透過設定 --refresh-schedule 參數來設定和啟用重新整理排程。

   --refresh-schedule 包含下列選用參數：

   - Frequency – 排程Value的 Unit和 。

     對於自訂儀表板，單位可以是 HOURS或 DAYS。

     對於自訂儀表板，當單位為 1、、6、 時12，以下值有效HOURS： 24

     對於自訂儀表板，單位DAYS為 時的唯一有效值。 1

- `Status` – 指定是否啟用重新整理排程。將值設定為 ENABLED 以啟用重新整理排程，或設定為 DISABLED 以關閉重新整理排程。
- `TimeOfDay` – 一天中執行排程的時間，每小時僅參考分鐘；預設值為 00：00。

下列範例會設定每六小時的重新整理排程，並啟用排程。

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \
--refresh-schedule '{"Frequency": {"Unit": "HOURS", "Value": 6}, "Status":
 "ENABLED"}'
```

使用 啟用反白儀表板 AWS CLI

下列程序說明如何建立反白儀表板、將所需的資源型政策連接至事件資料存放區和儀表板，以及更新儀表板以設定和啟用重新整理排程。

1. 執行 `create-dashboard`命令來建立反白儀表板。若要建立此儀表板， `--name` 必須是 `AWSCloudTrail-Highlights`。

   ```
   aws cloudtrail create-dashboard --name AWSCloudTrail-Highlights
   ```

2. 針對您帳戶中的每個事件資料存放區，執行 `put-resource-policy`命令，將資源型政策連接至事件資料存放區。您也可以在 CloudTrail 主控台上更新事件資料存放區的資源型政策。如需政策範例，請參閱 範例：允許 CloudTrail 執行查詢以重新整理儀表板。

   下列範例會將資源型政策連接至事件資料存放區。將 *account-id* 取代為您的帳戶 ID、將 *eds-arn* 取代為事件資料存放區的 ARN，並將 *dashboard-arn* 取代為儀表板的 ARN。

   ```
   aws cloudtrail put-resource-policy \
   --resource-arn eds-arn \
   --resource-policy '{"Version": "2012-10-17",        "Statement":
    [{"Sid": "EDSPolicy", "Effect": "Allow", "Principal": { "Service":
    "cloudtrail.amazonaws.com" }, "Action": "cloudtrail:StartQuery", "Condition":
    { "StringEquals": { "AWS:SourceArn": "dashboard-arn", "AWS:SourceAccount":
    "account-id"}}} ]}'
   ```

3. 執行 `put-resource-policy`命令，將資源型政策連接至儀表板。如需政策範例，請參閱 儀表板的資源型政策範例。

下列範例會將資源型政策連接至儀表板。將 *account-id* 取代為您的帳戶 ID，將 *dashboard-arn* 取代為儀表板的 ARN。

```
aws cloudtrail put-resource-policy \
--resource-arn dashboard-arn \
--resource-policy '{"Version": "2012-10-17",        "Statement":
 [{"Sid": "DashboardPolicy", "Effect": "Allow", "Principal": { "Service":
 "cloudtrail.amazonaws.com" }, "Action": "cloudtrail:StartDashboardRefresh",
 "Condition": { "StringEquals": { "AWS:SourceArn": "dashboard-arn",
 "AWS:SourceAccount": "account-id"}}}]}'
```

4. 執行 update-dashboard命令，透過設定 --refresh-schedule 參數來設定和啟用重新整理排程。對於醒目提示儀表板，唯一有效的 UNIT是 HOURS，而唯一有效的 Value是 6。

```
aws cloudtrail update-dashboard --dashboard-id AWSCloudTrail-Highlights \
--refresh-schedule '{"Frequency": {"Unit": "HOURS", "Value": 6}, "Status":
 "ENABLED"}'
```

檢視小工具的屬性

本節說明 4 種檢視類型的可設定檢視屬性：資料表、折線圖、圓餅圖和長條圖。

檢視類型：

- 資料表
- 折線圖
- 圓餅圖
- 長條圖

資料表

下列範例顯示設定為資料表的小工具。

```
{
    "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "TopErrors",
       "View": "Table"
```

```
    },
    "QueryStatement": "SELECT errorCode, COUNT(*) AS eventCount FROM eds WHERE
 eventTime > '?' AND eventTime < '?' AND (errorCode is not null) GROUP BY errorCode
 ORDER BY eventCount DESC LIMIT 100",
    "QueryParameters": ["$StartTime$", "$EndTime$"]
}
```

下表說明資料表的可設定檢視屬性。

| 參數 | 必要 | Value |
| --- | --- | --- |
| Height | 是 | 資料表的高度，以英吋為單位。 |
| Width | 是 | 資料表的寬度，以英吋為單位。 |
| Title | 是 | 資料表的標題。 |
| View | 是 | 小工具檢視類型。對於資料表，值為 Table。 |

### 折線圖

下列範例顯示設定為折線圖的小工具。

```
{
    "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "AccountActivity",
       "View": "LineChart",
       "YAxisColumn": "eventCount",
       "XAxisColumn": "eventDate",
       "FilterColumn": "readOnly"
    },
    "QueryStatement": "SELECT DATE_TRUNC('?', eventTime) AS eventDate, IF(readOnly,
 'read', 'write') AS readOnly, COUNT(*) as eventCount FROM eds WHERE eventTime >
 '?' AND eventTime < '?' GROUP BY DATE_TRUNC('?', eventTime), readOnly ORDER BY
 DATE_TRUNC('?', eventTime), readOnly",
    "QueryParameters": ["$Period$", "$StartTime$", "$EndTime$", "$Period$", "$Period$"]
```

```
}
```

下表說明折線圖的可設定檢視屬性。

| 參數 | 必要 | Value |
| --- | --- | --- |
| Height | 是 | 折線圖的高度，以英吋為單位。 |
| Width | 是 | 折線圖的寬度，以英吋為單位。 |
| Title | 是 | 折線圖的標題。 |
| View | 是 | 小工具檢視類型。對於折線圖，值為 LineChart 。 |
| YAxisColumn | 是 | 您要用於 Y 軸欄之查詢結果的欄位。例如 eventCount 。 |
| XAxisColumn | 是 | 您要用於 X 軸欄之查詢結果的欄位。例如 eventDate 。 |
| FilterColumn | 否 | 您要篩選之查詢結果中的 欄位。例如 readOnly。 |

### 圓餅圖

下列範例顯示設定為圓餅圖的小工具。

```
{
    "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "MostActiveRegions",
       "View": "PieChart",
       "LabelColumn": "awsRegion",
       "ValueColumn": "eventCount",
       "FilterColumn": "awsRegion"
    },
```

```
    "QueryStatement": "SELECT awsRegion, COUNT(*) AS eventCount FROM eds where
 eventTime > '?' and eventTime < '?' GROUP BY awsRegion ORDER BY eventCount LIMIT 100",
    "QueryParameters": ["$StartTime$", "$EndTime$"]
}
```

下表說明圓餅圖的可設定檢視屬性。

| 參數 | 必要 | Value |
| --- | --- | --- |
| Height | 是 | 圓餅圖的高度，以英吋為單位。 |
| Width | 是 | 圓餅圖的寬度，以英吋為單位。 |
| Title | 是 | 圓餅圖的標題。 |
| View | 是 | 小工具檢視類型。對於圓餅圖，值為 PieChart。 |
| LabelColumn | 是 | 圓餅圖中區段的標籤。例如 awsRegion 。 |
| ValueColumn | 是 | 圓餅圖中區段的值。例如 ValueColumn 。 |
| FilterColumn | 否 | 您要篩選之查詢結果中的 欄位。例如 awsRegion 。 |

長條圖

下列範例顯示設定為長條圖的小工具。

```
{
    "ViewProperties": {
       "Height": "2",
       "Width": "4",
       "Title": "TopServices",
       "View": "BarChart",
       "LabelColumn": "service",
```

```
       "ValueColumn": "eventCount",
       "FilterColumn": "service",
       "Orientation": "Horizontal"
    },
    "QueryStatement": "SELECT REPLACE(eventSource, '.amazonaws.com') AS service,
 COUNT(*) AS eventCount FROM eds WHERE eventTime > '?' AND eventTime < '?' GROUP BY
 eventSource ORDER BY eventCount DESC LIMIT 100",
    "QueryParameters": ["$StartTime$", "$EndTime$"]
}
```

下表說明長條圖的可設定檢視屬性。

| 參數 | 必要 | Value |
| --- | --- | --- |
| Height | 是 | 長條圖的高度，以英吋為單位。 |
| Width | 是 | 長條圖的寬度，以英吋為單位。 |
| Title | 是 | 長條圖的標題。 |
| View | 是 | 小工具檢視類型。對於長條圖，值為 BarChart。 |
| LabelColumn | 是 | 長條圖中長條的標籤。例如 service。 |
| ValueColumn | 是 | 長條圖中長條的值。例如 eventCount 。 |
| FilterColumn | 否 | 您要篩選之查詢結果中的 欄位。例如 service。 |
| Orientation | 否 | 長條圖的方向，Horizontal 或 Vertical。 |

## 使用 管理儀表板 AWS CLI

本節說明您可以執行以管理儀表板的數個其他命令，包括取得儀表板、列出儀表板、重新整理儀表板，以及更新儀表板。

使用 時 AWS CLI，請記住，您的命令會在為設定檔 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。

範例：

- 使用 取得儀表板 AWS CLI
- 使用 列出儀表板 AWS CLI
- 使用 將資源型政策連接至事件資料存放區或儀表板 AWS CLI
- 使用 手動重新整理儀表板 AWS CLI
- 使用 更新儀表板 AWS CLI

### 使用 取得儀表板 AWS CLI

執行 `get-dashboard`命令以傳回儀表板。`--dashboard-id` 提供儀表板 ARN 或儀表板名稱來指定 。

```
aws cloudtrail get-dashboard --dashboard-id arn:aws:cloudtrail:us-
east-1:123456789012:dashboard/exampleDash
```

### 使用 列出儀表板 AWS CLI

執行 `list-dashboards`命令來列出您帳戶的儀表板。

- 包含 `--type` 參數，以僅檢視 `CUSTOM`或 `MANAGED`儀表板。
- 包含 `--max-results` 參數以限制結果的數量。有效值為 1-100。
- 包含 `--name-prefix`以傳回符合指定字首的儀表板。

下列範例列出所有儀表板。

```
aws cloudtrail list-dashboards
```

此範例僅列出`CUSTOM`儀表板。

```
aws cloudtrail list-dashboards --type CUSTOM
```

下一個範例只會列出MANAGED儀表板。

```
aws cloudtrail list-dashboards --type MANAGED
```

最後一個範例會列出符合指定字首的儀表板。

```
aws cloudtrail list-dashboards --name-prefix ExamplePrefix
```

使用 將資源型政策連接至事件資料存放區或儀表板 AWS CLI

執行 put-resource-policy命令，將資源型政策套用至事件資料存放區或儀表板。

將資源型政策連接至事件資料存放區

若要在手動或排程重新整理期間對儀表板執行查詢，您需要將資源型政策連接至與儀表板上小工具相關聯的每個事件資料存放區。這可讓 CloudTrail Lake 代表您執行查詢。如需資源型政策的詳細資訊，請參閱 範例：允許 CloudTrail 執行查詢以重新整理儀表板。

下列範例會將資源型政策連接至事件資料存放區。將 *account-id* 取代為您的帳戶 ID、將 *eds-arn* 取代為 CloudTrail 將執行查詢的事件資料存放區的 ARN，並將 *dashboard-arn* 取代為儀表板的 ARN。

```
aws cloudtrail put-resource-policy \
--resource-arn eds-arn \
--resource-policy '{"Version": "2012-10-17",        "Statement": [{"Sid": "EDSPolicy",
 "Effect": "Allow", "Principal": { "Service": "cloudtrail.amazonaws.com" }, "Action":
 "cloudtrail:StartQuery", "Condition": { "StringEquals": { "AWS:SourceArn": "dashboard-
arn", "AWS:SourceAccount": "account-id"}}} ]}'
```

將資源型政策連接至儀表板

若要設定儀表板的重新整理排程，您需要將資源型政策連接至儀表板，以允許 CloudTrail Lake 代表您重新整理儀表板。如需資源型政策的詳細資訊，請參閱 儀表板的資源型政策範例。

下列範例會將資源型政策連接至儀表板。將 *account-id* 取代為您的帳戶 ID，將 *dashboard-arn* 取代為儀表板的 ARN。

```
aws cloudtrail put-resource-policy \
```

```
--resource-arn dashboard-arn \
--resource-policy '{"Version": "2012-10-17",        "Statement":
 [{"Sid": "DashboardPolicy", "Effect": "Allow", "Principal": { "Service":
 "cloudtrail.amazonaws.com" }, "Action": "cloudtrail:StartDashboardRefresh",
 "Condition": { "StringEquals": { "AWS:SourceArn": "dashboard-arn",
 "AWS:SourceAccount": "account-id"}}}]}'
```

使用 手動重新整理儀表板 AWS CLI

執行 start-dashboard-refresh命令以手動重新整理儀表板。您必須先將資源型政策連接至與儀表板小工具相關聯的每個事件資料存放區，才能執行此命令。

下列範例示範如何手動重新整理自訂儀表板。

```
aws cloudtrail start-dashboard-refresh \
--dashboard-id  dashboard-id \
--query-parameter-values '{"$StartTime$": "2024-11-05T10:45:24.00Z"}'
```

下一個範例顯示如何手動重新整理受管儀表板。由於受管儀表板是由 CloudTrail 設定，重新整理請求需要包含查詢將在其中執行的事件資料存放區的 ID。

```
aws cloudtrail start-dashboard-refresh \
--dashboard-id dashboard-id  \
--query-parameter-values '{"$StartTime$": "2024-11-05T10:45:24.00Z", "$EventDataStoreId
$": "eds-id"}'
```

使用 更新儀表板 AWS CLI

執行 update-dashboard命令以更新儀表板。您可以更新儀表板以設定重新整理排程、啟用或停用重新整理排程、修改小工具，以及啟用或停用終止保護。

使用 更新重新整理排程 AWS CLI

下列範例會更新名為 之自訂儀表板的重新整理排程AccountActivityDashboard。

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \
--refresh-schedule '{"Frequency": {"Unit": "HOURS", "Value": 6}, "Status": "ENABLED"}'
```

使用 在自訂儀表板上停用終止保護和重新整理排程 AWS CLI

下列範例會停用名為 之自訂儀表板的終止保護AccountActivityDashboard，以允許刪除儀表板。它也會關閉重新整理排程。

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \
--refresh-schedule '{ "Status": "DISABLED"}' \
--no-termination-protection-enabled
```

將小工具新增至自訂儀表板

下列範例會將名為 的新小工具新增至名為 TopServices的自訂儀表板AccountActivityDashboard。Widgets 陣列包含為儀表板建立的兩個 Widget，以及新的 Widget。

> **Note**
>
> 在此範例中，？被單引號包圍，因為它與 搭配使用eventTime。根據您執行的作業系統，您可能需要使用逸出引號括住單引號。如需詳細資訊，請參閱 中的使用引號和常值搭配字串 AWS CLI。

```
aws cloudtrail update-dashboard --dashboard-id AccountActivityDashboard \
--widgets '[
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "TopErrors",
        "View": "Table"
      },
      "QueryStatement": "SELECT errorCode, COUNT(*) AS eventCount FROM eds WHERE
 eventTime > '?' AND eventTime < '?' AND (errorCode is not null) GROUP BY errorCode
 ORDER BY eventCount DESC LIMIT 100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    },
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "MostActiveRegions",
        "View": "PieChart",
        "LabelColumn": "awsRegion",
        "ValueColumn": "eventCount",
        "FilterColumn": "awsRegion"
      },
```

```
      "QueryStatement": "SELECT awsRegion, COUNT(*) AS eventCount FROM eds where
eventTime > '?' and eventTime < '?' GROUP BY awsRegion ORDER BY eventCount LIMIT 100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    },
    {
      "ViewProperties": {
        "Height": "2",
        "Width": "4",
        "Title": "TopServices",
        "View": "BarChart",
        "LabelColumn": "service",
        "ValueColumn": "eventCount",
        "FilterColumn": "service",
        "Orientation": "Vertical"
      },
      "QueryStatement": "SELECT replace(eventSource, '.amazonaws.com') AS service,
COUNT(*) as eventCount FROM eds WHERE eventTime > '?' AND eventTime < '?' GROUP BY
eventSource ORDER BY eventCount DESC LIMIT 100",
      "QueryParameters": ["$StartTime$", "$EndTime$"]
    }
 ]'
```

### 使用 刪除儀表板 AWS CLI

本節說明如何使用 AWS CLI `delete-dashboard`命令來刪除 CloudTrail Lake 儀表板。

若要刪除儀表板，`--dashboard-id`請提供儀表板 ARN 或儀表板名稱來指定 。

```
aws cloudtrail delete-dashboard --dashboard-id arn:aws:cloudtrail:us-
east-1:123456789012:dashboard/exampleDash
```

如果操作成功，則不會有回應。

> **Note**
>
> 如果`--termination-protection-enabled`已設定 ，則無法刪除儀表板。

## CloudTrail Lake 查詢

CloudTrail Lake 中的查詢是以 SQL 撰寫而成。您可以在 CloudTrail Lake Editor 索引標籤上建置查詢，方法是從頭開始在 SQL 中寫入查詢、開啟已儲存或範例查詢並進行編輯，或使用查詢產生器從英

文語言提示產生查詢。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 Lake SQL 限制條件。

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'
```

如需如何最佳化查詢的資訊，請參閱 最佳化 CloudTrail Lake 查詢。

主題


- 查詢編輯器工具
- 從自然語言提示建立 CloudTrail Lake 查詢
- 使用 CloudTrail 主控台檢視範例查詢
- 使用 CloudTrail 主控台建立或編輯查詢
- 使用主控台執行查詢並儲存查詢結果
- 使用主控台檢視查詢結果
- 以自然語言摘要查詢結果
- 下載已儲存的查詢結果
- 驗證 CloudTrail Lake 儲存的查詢結果
- 最佳化 CloudTrail Lake 查詢
- 使用 執行和管理 CloudTrail Lake 查詢 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。

## 從自然語言提示建立 CloudTrail Lake 查詢

您可以使用 CloudTrail Lake 查詢產生器，從您提供的英文提示產生查詢。查詢產生器使用生成式人工智慧 （ 生成式 AI) 從您的提示產生ready-to-use SQL 查詢，然後您可以選擇在 Lake 的查詢編輯器中執行，或進一步微調。您不需要具備 SQL 或 CloudTrail 事件欄位的廣泛知識，即可使用查詢產生器。

提示可以是有關 CloudTrail Lake 事件資料存放區中事件資料的問題或陳述式。例如，您可以輸入提示，例如 "What are my top errors in the past month?"和 “Give me a list of users that used SNS.”

提示最少可以有 3 個字元，最多 500 個字元。

產生查詢不收取費用；不過，當您執行查詢時，會根據掃描的最佳化和壓縮資料量產生費用。為了協助控制成本，建議您將開始和結束`eventTime`時間戳記新增至查詢，以限制查詢。

> **Note**
>
> 您可以選擇出現在所產生查詢下方的拇指向上或拇指向下按鈕，以提供所產生查詢的意見回饋。當您提供意見回饋時，CloudTrail 會儲存您的提示和產生的查詢。
> 請勿在提示中包含任何個人識別、機密或敏感資訊。
> 此功能使用生成式 AI 大型語言模型 LLMs)；我們建議再次檢查 LLM 回應。

> **Note**
>
> CloudTrail 會自動選取您地理位置內的最佳區域，以在產生查詢時處理推論請求。這可將可用的運算資源、模型可用性最大化，並提供最佳客戶體驗。您的資料只會存放在發出請求的區域，但輸入提示和輸出結果可能會在該區域之外處理。所有資料都會透過 Amazon 的安全網路進行加密傳輸。
> CloudTrail 會將您的推論請求安全地路由到發出請求的地理區域內可用的運算資源，如下所示：

- 來自美國的推論請求將在美國境內處理
- 來自日本的推論請求將在日本內處理
- 來自澳洲的推論請求將在澳洲處理。
- 源自歐盟的推論請求將在歐盟內處理
- 來自印度的推論請求將在印度處理

若要選擇退出查詢產生功能，您可以明確拒絕或移除您正在使用的 iam 政策中的`cloudtrail:GenerateQuery`動作。

您可以使用 CloudTrail 主控台 和 存取查詢產生器 AWS CLI。

CloudTrail console

在 CloudTrail 主控台上使用查詢產生器

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
2. 在導覽窗格中，選擇 Lake 下方的查詢。
3. 在查詢頁面上，選擇編輯器索引標籤。
4. 選擇您要為其建立查詢的事件資料存放區。
5. 在查詢產生器區域中，輸入純英文提示。如需範例，請參閱 範例提示。
6. 選擇產生查詢。查詢產生器將嘗試從您的提示產生查詢。如果成功，查詢產生器會在編輯器中提供 SQL 查詢。如果提示失敗，請重新說出您的提示，然後再試一次。
7. （選用）您可以提供有關所產生查詢的意見回饋。若要提供意見回饋，請選擇出現在提示下方的拇指向上或拇指向下按鈕。當您提供意見回饋時，CloudTrail 會儲存您的提示和產生的查詢。
8. （選用）選擇執行以執行查詢。

> **Note**
>
> 當您執行查詢時，會根據掃描的最佳化和壓縮資料量產生費用。為了協助控制成本，建議您將開始和結束`eventTime`時間戳記新增至查詢，以限制查詢。

9. （選用）如果您執行查詢且有結果，您可以選擇摘要結果，以產生查詢結果的英文自然語言摘要。此選項使用生成式人工智慧（生成式 AI) 來產生摘要。如需有關此選項的詳細資訊，請參閱 以自然語言摘要查詢結果。

   您可以選擇出現在所產生摘要下方的拇指向上或拇指向下按鈕，以提供有關摘要的意見回饋。

   > **Note**
   >
   > 查詢摘要功能目前為 CloudTrail Lake 的預覽版本，可能會有所變更。此功能適用於下列區域：亞太區域（東京）、美國東部（維吉尼亞北部）和美國西部（奧勒岡）。

AWS CLI

使用 產生查詢 AWS CLI

執行 generate-query命令，從英文提示產生查詢。針對 --event-data-stores，提供您要查詢的事件資料存放區的 ARN（或 ARN 的 ID 尾碼）。您只能指定一個事件資料存放區。對於 --prompt，請以英文提供提示。

```
aws cloudtrail generate-query
--event-data-stores arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-ee54-4813-92d5-999aeEXAMPLE \
--prompt "Show me all console login events for the past week?"
```

如果成功，命令會輸出 SQL 陳述式QueryAlias，並提供您將與 start-query命令搭配使用的 ，以針對您的事件資料存放區執行查詢。

```
{
  "QueryStatement": "SELECT * FROM $EDS_ID WHERE eventname = 'ConsoleLogin' AND
 eventtime >= timestamp '2024-09-16 00:00:00' AND eventtime <= timestamp '2024-09-23
 00:00:00' AND eventSource = 'signin.amazonaws.com'",
  "QueryAlias": "AWSCloudTrail-UUID"
}
```

使用 執行查詢 AWS CLI

在上一個範例中，使用 start-query命令QueryAlias輸出的 執行 generate-query命令。您也可以選擇透過提供 來執行 start-query命令QueryStatement。

```
aws cloudtrail start-query --query-alias AWSCloudTrail-UUID
```

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。

```
{
    "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。如果您使用選用的 --delivery-s3uri 參數將查詢結果傳送到 S3 儲存貯體，則儲存貯體政策必須授予 CloudTrail 許可，才能將查詢結果傳送到儲存貯體。如需手動編輯儲存貯體政策的資訊，請參閱「適用於 CloudTrail Lake 查詢結果的 Amazon S3 儲存貯體政策」。

## 所需的許可

AWSCloudTrail_FullAccess 和 AdministratorAccess受管政策都提供使用此功能的必要許可。

也可以在新的或現有的客戶管理政策或內嵌政策中包含 cloudtrail:GenerateQuery 動作。

## 區域支援

下列支援此功能 AWS 區域：

- 亞太區域 (孟買) 區域 (ap-south-1)
- 亞太區域 (雪梨) 區域 (ap-southeast-2)
- 亞太區域 (東京) 區域 (ap-northeast-1)
- 加拿大 (中部) 區域 (ca-central-1)
- 歐洲 (倫敦) 區域 (eu-west-2)
- 美國東部 (維吉尼亞北部) 區域 (us-east-1)
- 美國西部 (奧勒岡) 區域 (us-west-2)

## 限制

以下是查詢產生器的限制：

- 查詢產生器只能接受英文提示。
- 查詢產生器只能為收集 CloudTrail 事件（管理事件、資料事件、網路活動事件）的事件資料存放區產生查詢。
- 查詢產生器無法針對與 CloudTrail Lake 事件資料無關的提示產生查詢。

## 範例提示

本節提供範例提示，以及從提示產生的 SQL 查詢。

如果您選擇執行本節中的範例查詢，請將 *eds-id* 取代為您要查詢的事件資料存放區的 ID，並將時間戳記取代為您的使用案例的適當時間戳記。時間戳記的格式如下：YYYY-MM-DD HH:MM:SS。

提示：What are my top errors in the past month?

SQL 查詢：

```
SELECT
    errorMessage,
    COUNT(*) as eventCount
FROM
    eds-id
WHERE
    errorMessage IS NOT NULL
AND eventTime >= timestamp '2024-05-01 00:00:00'
AND eventTime <= timestamp '2024-05-31 23:59:59'
GROUP BY 1
ORDER BY 2 DESC
LIMIT 2;
```

提示：Give me a list of users that used Amazon SNS.

SQL 查詢：

```
SELECT
    DISTINCT userIdentity.arn AS user
FROM
    eds-id
```

```
WHERE
    eventSource = 'sns.amazonaws.com'
```

提示：What are my API counts each day for read and write events in the past month?

SQL 查詢：

```
SELECT date(eventTime) AS event_date,
    SUM(
        CASE
            WHEN readonly = true THEN 1
            ELSE 0
        END
    ) AS read_events,
    SUM(
        CASE
            WHEN readonly = false THEN 1
            ELSE 0
        END
    ) AS write_events
FROM
    eds-id
WHERE
    eventTime >= timestamp '2024-05-04 00:00:00'
AND eventTime <= timestamp '2024-06-04 23:59:59'
GROUP BY 1
ORDER BY 1 ASC;
```

提示：Show any events with access denied errors for the past three weeks.

SQL 查詢：

```
SELECT *
FROM
  eds-id
WHERE
  WHERE (errorCode = 'AccessDenied' OR errorMessage = 'Access Denied')
AND eventTime >= timestamp '2024-05-16 01:00:00'
AND eventTime <= timestamp '2024-06-06 01:00:00'
```

提示：Query the number of calls each operator performed on the date 2024-05-01. The operator is a principal tag.

SQL 查詢：

```
SELECT element_at(
        eventContext.tagContext.principalTags,
        'operator'
    ) AS operator,
    COUNT(*) AS eventCount
FROM
    eds-id
WHERE eventtime >= '2024-05-01 00:00:00'
    AND eventtime < '2024-05-01 23:59:59'
GROUP BY 1
ORDER BY 2 DESC;
```

提示：Give me all event IDs that touched resources within the CloudFormation stack with name myStack on the date 2024-05-01.

SQL 查詢：

```
SELECT eventID
FROM
    eds-id
WHERE any_match(
        eventContext.tagcontext.resourcetags,
        rt->element_at(rt.tags, 'aws:cloudformation:stack-name') = 'myStack'
    )
    AND eventtime >= '2024-05-01 00:00:00'
    AND eventtime < '2024-05-01 23:59:59'
```

提示：Count the number of events grouped by resource tag 'solution' values, listing them in descending order of count.

SQL 查詢：

```
SELECT element_at(rt.tags, 'solution'),
    count(*) as event_count
FROM
    eds-id,
    unnest(eventContext.tagContext.resourceTags) as rt
WHERE eventtime < '2025-05-14 19:00:00'
GROUP BY 1
ORDER BY 2 DESC;
```

提示：Find all Amazon S3 data events where resource tag Environment has value prod.

SQL 查詢：

```
SELECT *
FROM
    eds-id
WHERE eventCategory = 'Data'
    AND eventSource = 's3.amazonaws.com'
    AND eventtime >= '2025-05-14 00:00:00'
    AND eventtime < '2025-05-14 20:00:00'
    AND any_match(
        eventContext.tagContext.resourceTags,
        rt->element_at(rt.tags, 'Environment') = 'prod'
    )
```

## 使用 CloudTrail 主控台檢視範例查詢

CloudTrail 主控台提供許多範例查詢，可協助您開始自行編寫查詢。

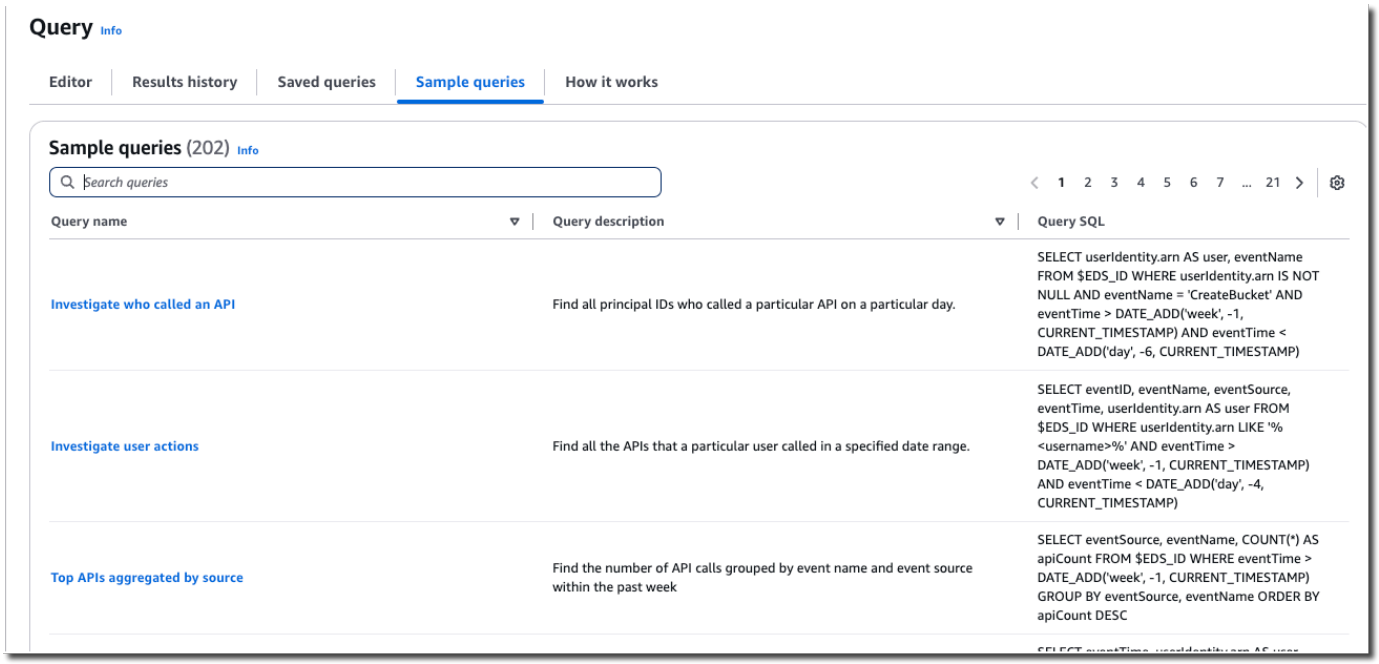
CloudTrail 查詢會依據掃描的資料量而產生費用。為了協助控制成本，我們建議您對查詢新增開始和結束 `eventTime` 時間戳記來限制查詢。如需 CloudTrail 定價的詳細資訊，請參閱 AWS CloudTrail 定價。

> **Note**
>
> 您也可以檢視 GitHub 社群所建立的查詢。如需詳細資訊，請參閱 GitHub 網站上的 CloudTrail Lake 範例查詢。 AWS CloudTrail 尚未評估 GitHub 中的查詢。

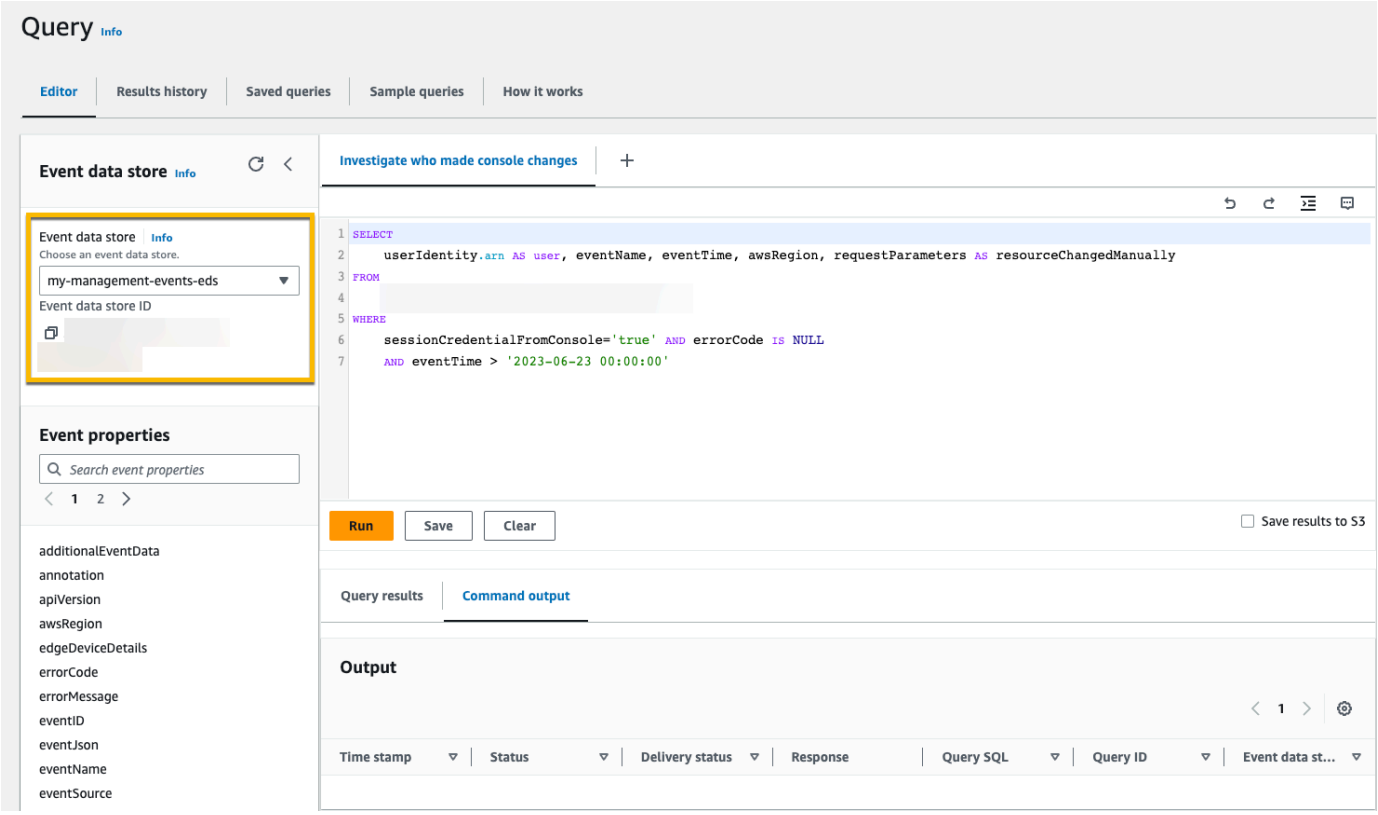
若要檢視與執行範例查詢

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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. 從清單中選擇範例查詢，或輸入要搜尋的片語。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。

> **Note**
>
> 根據預設，此頁面會使用基本搜尋功能。如果您的許可政策尚未提供動作的許可，您可以新增該`cloudtrail:SearchSampleQueries`動作的許可來改善搜尋功能。`AWSCloudTrail_FullAccess` 受管政策提供執行`cloudtrail:SearchSampleQueries`動作的許可。

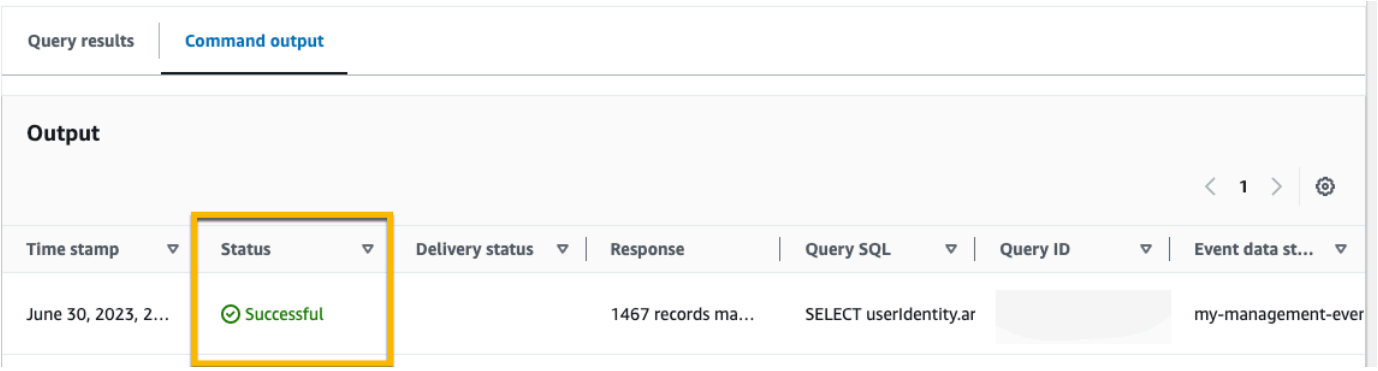



5. 在編輯器索引標籤上，選擇您想要為哪個事件資料存放區執行查詢。當您在清單中選擇事件資料存放區時，CloudTrail 會自動在查詢編輯器的 FROM 列填入事件資料存放區 ID。

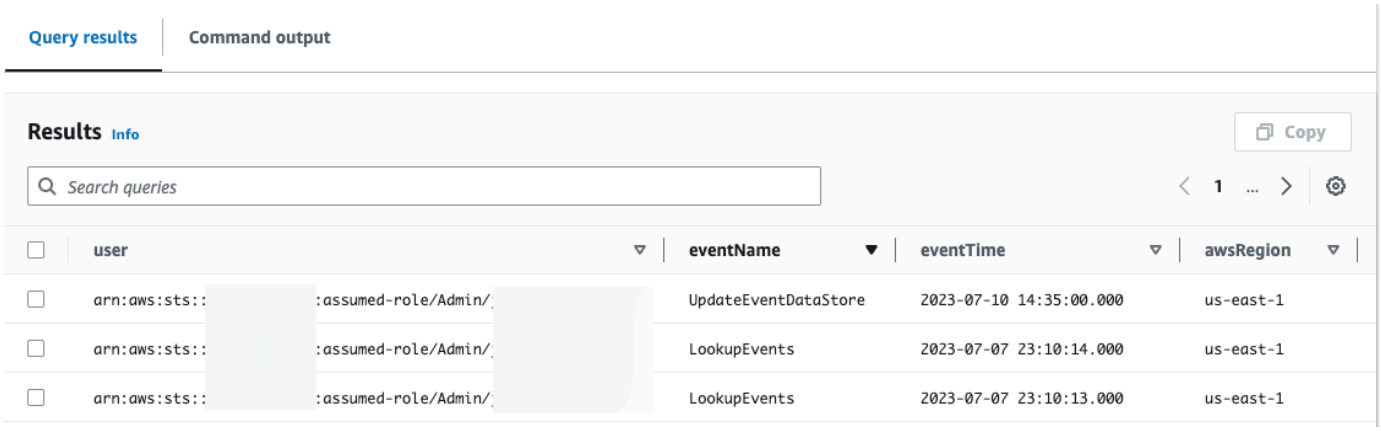



6. 選擇執行以執行查詢。

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 使用 CloudTrail 主控台建立或編輯查詢。如需有關執行查詢和儲存查詢結果的詳細資訊，請參閱 使用主控台執行查詢並儲存查詢結果。

## 使用 CloudTrail 主控台建立或編輯查詢

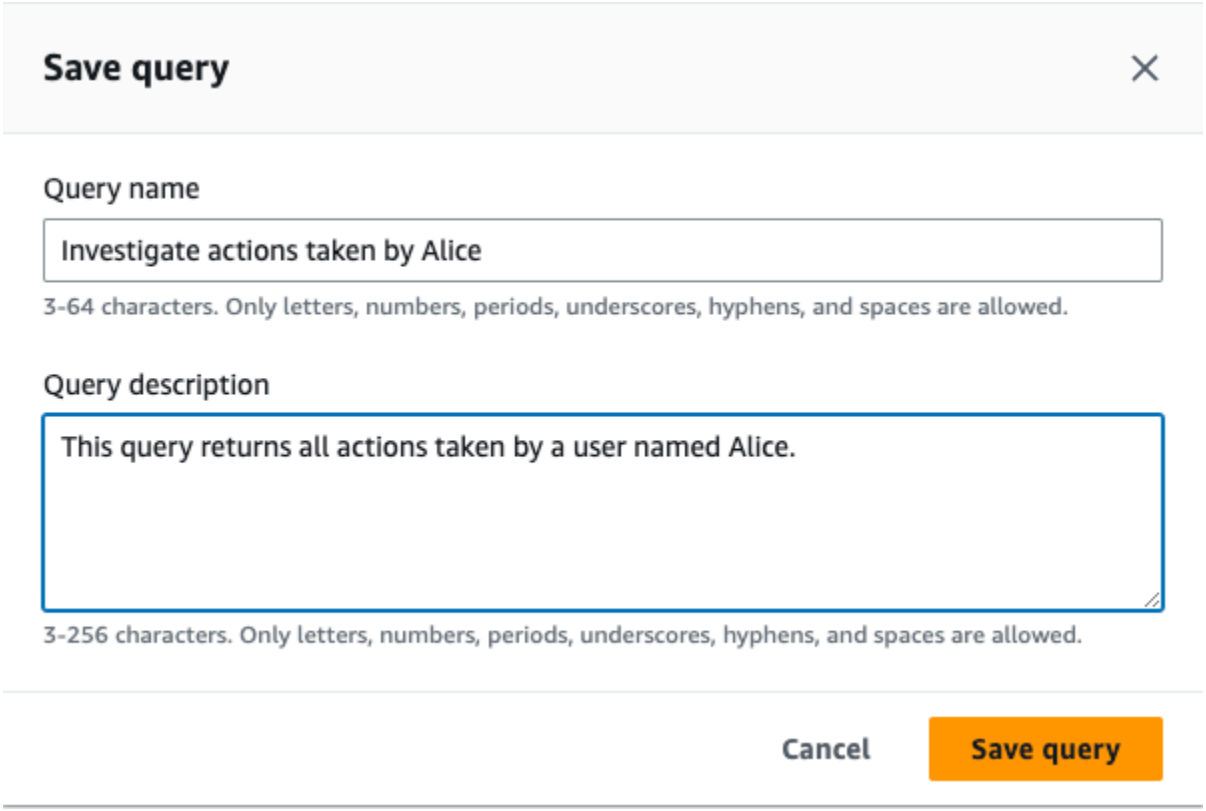
在這次逐步解說中，我們會打開其中一個範例查詢，進行編輯以查找名為 `Alice` 的特定使用者所做的動作，然後將其儲存為新查詢。您也可以在 Saved queries (已儲存的查詢) 索引標籤編輯已儲存的查詢 (如果有已儲存的查詢)。為了協助控制成本，我們建議您對查詢新增開始和結束 `eventTime` 時間戳記來限制查詢。

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
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。`FROM` 的值是事件資料存放區 ARN 的 ID 部分，會在您選擇該事件資料存放區時由 CloudTrail 自動填入。

```
SELECT
    eventID, eventName, eventSource, eventTime, userIdentity.arn AS user
FROM
    event-data-store-id
WHERE
    userIdentity.arn LIKE '%Alice%'
```

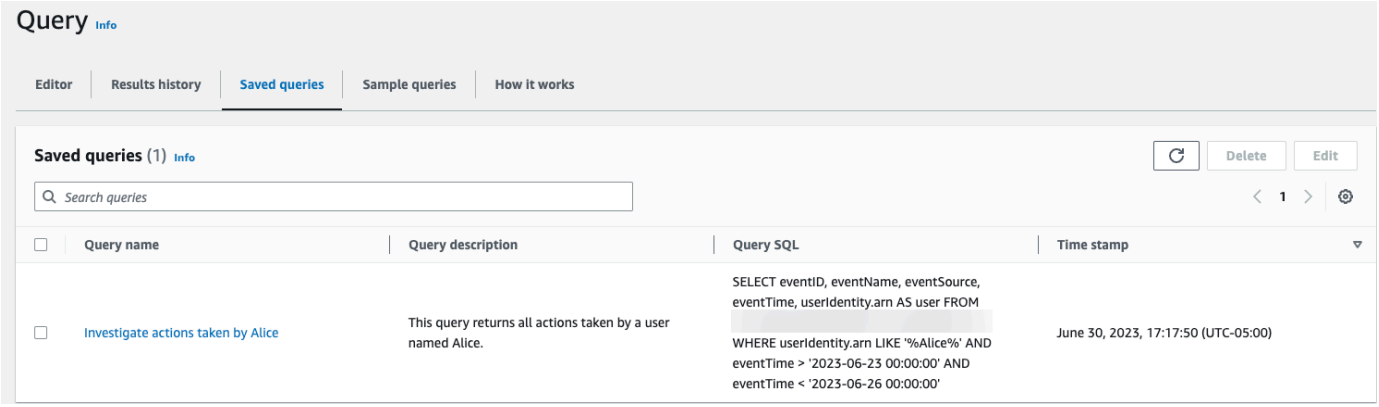
```
    AND eventTime > '2023-06-23 00:00:00' AND eventTime < '2023-06-26 00:00:00'
```

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**
>
> 已儲存的查詢與您的瀏覽器相關；如果您使用不同的瀏覽器或其他裝置存取 CloudTrail 主控台，則無法存取先前已儲存的查詢。

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。




# 使用主控台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。當您在 CloudTrail Lake 中執行查詢時，會根據查詢所掃描的資料量而產生費用。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，查詢結果可能會先顯示在 CloudTrail 主控台中，隨後才能在 S3 儲存貯體中檢視，因為 CloudTrail 會在查詢掃描完成後傳送查詢結果。儘管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，CloudTrail 將查詢結果傳送到 S3 儲存貯體可能需要更長的時間。CloudTrail 會以壓縮的 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 Lake 執行查詢

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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 會建立和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`動作的許可，因為預設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。儲存貯體政策必須授予 CloudTrail 許可，才能將查詢結果傳送至儲存貯體。如需手動編輯儲存貯體政策的資訊，請參閱「適用於 CloudTrail Lake 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送至 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，以判斷在 CloudTrail 傳送查詢結果之後，查詢結果是否經過修改、遭到刪除或保持不變。如需有關驗證已儲存查詢結果的詳細資訊，請參閱驗證 CloudTrail Lake 儲存的查詢結果。

## 範例：將查詢結果儲存至 Amazon S3 儲存貯體

此逐步解說說明如何將查詢結果儲存到 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. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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。當您在清單中選擇事件資料存放區時，CloudTrail 會自動在 `From` 列填入事件資料存放區 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。

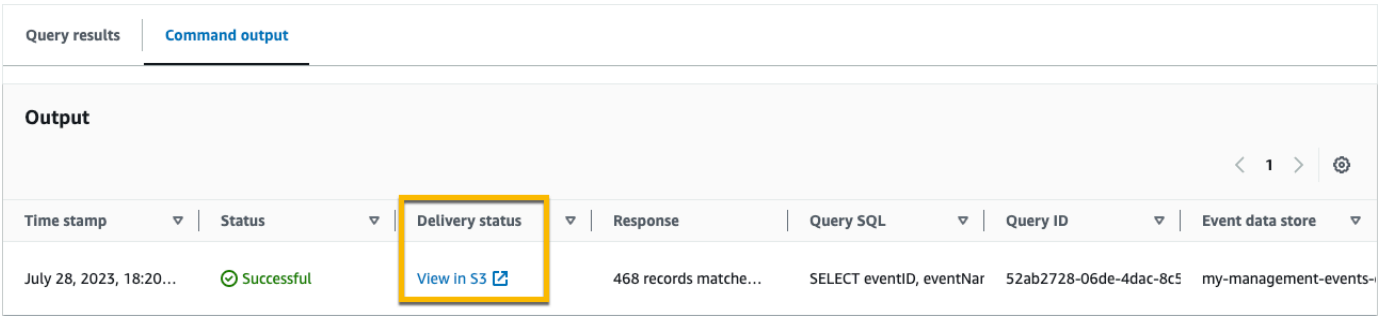
6. 選擇將結果儲存至 S3，以便將查詢結果儲存至 S3 儲存貯體。當您選擇預設 S3 儲存貯體時，CloudTrail 會建立和套用所需的儲存貯體政策。如果您選擇預設 S3 儲存貯體，您的 IAM 政策需要包含 `s3:PutEncryptionConfiguration`動作的許可，因為預設會為儲存貯體啟用伺服器端加密。在此範例中，我們使用預設的 S3 儲存貯體。

> **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。儲存貯體政策必須授予 CloudTrail 許可，才能將查詢結果傳送至儲存貯體。如需手動編輯儲存貯體政策的資訊，請參閱「適用於 CloudTrail Lake 查詢結果的 Amazon S3 儲存貯體政策」。

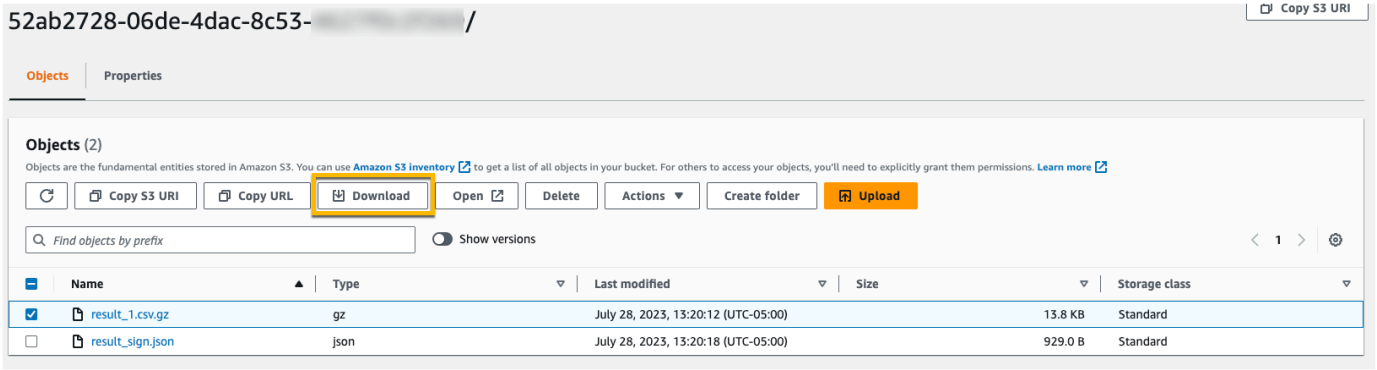
7. 選擇執行。根據事件資料存放區的大小及其中包含的資料天數，查詢可能需要幾分鐘才能執行。所以 Command output (命令輸出) 索引標籤會顯示查詢的狀態，以及查詢是否已完成執行。查詢完成執行後，開啟 Query results (查詢結果) 索引標籤查看作用中查詢 (目前編輯器中顯示的查詢) 的結果表格。

8. 當 CloudTrail 完成將儲存的查詢結果傳遞至您的 S3 儲存貯體時，傳遞狀態欄會提供一個包含已儲存查詢結果檔案的 S3 儲存貯體連結，以及一個您可以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**
>
> 儲存查詢結果時，查詢結果可能會先顯示在 CloudTrail 主控台中，隨後才能在 S3 儲存貯體中檢視，因為 CloudTrail 會在查詢掃描完成後傳遞查詢結果。儘管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，CloudTrail 將查詢結果傳送到 S3 儲存貯體可能需要更長的時間。CloudTrail 會以壓縮的 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 CloudTrail Lake 儲存的查詢結果]。

## 使用主控台檢視查詢結果

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，查詢結果可能會先顯示在 CloudTrail 主控台中，隨後才能在 S3 儲存貯體中檢視，因為 CloudTrail 會在查詢掃描完成後傳送查詢結果。儘管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，CloudTrail 將查詢結果傳送到 S3 儲存貯體可能需要更長的時間。CloudTrail 會以壓縮的 gzip 格式將查詢結果傳遞至 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。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送至 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。

檢視查詢結果

1. 如果尚未選取查詢結果，請選擇查詢編輯器上的查詢結果索引標籤。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. （選用）選擇摘要結果，以產生查詢結果的自然語言摘要。摘要以英文提供。此選項使用生成式人工智慧（生成式 AI) 來產生摘要。如需有關此選項的詳細資訊，請參閱 以自然語言摘要查詢結果。

   您可以選擇出現在所產生摘要下方的拇指向上或拇指向下按鈕，以提供有關摘要的意見回饋。

   > **Note**
   >
   > 查詢摘要功能目前為 CloudTrail Lake 的預覽版本，可能會有所變更。此功能適用於下列區域：亞太區域（東京）、美國東部（維吉尼亞北部）和美國西部（奧勒岡）。

3. 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。

## 以自然語言摘要查詢結果

> **Note**
>
> 查詢摘要功能目前為 CloudTrail Lake 的預覽版本，可能會有所變更。

> **Note**
>
> CloudTrail 會自動選取您地理位置內的最佳區域，以處理推論請求，同時摘要查詢。這可將可用的運算資源、模型可用性最大化，並提供最佳客戶體驗。您的資料只會存放在發出請求的區

域，但輸入提示和輸出結果可能會在該區域之外處理。所有資料都會透過 Amazon 的安全網路進行加密傳輸。
CloudTrail 會將您的推論請求安全地路由到發出請求的地理區域內可用的運算資源，如下所示：

- 來自美國的推論請求將在美國境內處理
- 來自日本的推論請求將在日本內處理

若要選擇退出查詢摘要功能，您可以明確拒絕或移除您正在使用的 iam 政策中的`cloudtrail:GenerateQueryResultsSummary`動作。

查詢完成後，您可以從查詢編輯器的查詢結果索引標籤中，以自然語言取得查詢結果的摘要。此選項使用生成式人工智慧（生成式 AI) 來產生摘要。

摘要查詢結果

1. 從查詢編輯器的查詢結果索引標籤中，選擇摘要結果以產生查詢結果的自然語言摘要。摘要以英文提供。
2. （選用）選擇出現在所產生摘要下方的拇指向上或拇指向下按鈕，以提供有關摘要的意見回饋。

如果相關的事件資料存放區使用 KMS 金鑰加密，則無法使用 KMS 金鑰來加密查詢結果和摘要。查詢結果和摘要會改為由 CloudTrail 加密。

根據 `GetQueryResults`、 `GenerateQueryResultsSummary`和 KMS 許可授權對產生的摘要的存取（如果相關事件日期存放區使用 KMS 金鑰加密）。產生摘要時，CloudTrail 會記錄名為 的事件，`GenerateQueryResultsSummary`以取得可見性。

## 所需的許可

AWSCloudTrail_FullAccess 和 AdministratorAccess受管政策都提供使用此功能的必要許可。

您也可以在新的或現有的客戶受管或內嵌政策中包含`cloudtrail:GenerateQueryResultsSummary`和 `cloudtrail:GetQueryResults`動作。

如果與所摘要查詢結果相關的事件資料存放區使用 KMS 金鑰加密，您也需要 KMS 金鑰的許可。

### 區域支援

此功能可在下列位置使用 AWS 區域：

- 亞太區域 (東京) 區域 (ap-northeast-1)
- 美國東部 (維吉尼亞北部) 區域 (us-east-1)
- 美國西部 (奧勒岡) 區域 (us-west-2)

### 限制

以下是此功能的限制：

- 摘要僅以英文顯示。
- 摘要僅限於收集 CloudTrail 事件（管理事件、資料事件、網路活動事件）的事件資料存放區。
- 每個摘要適用於單一查詢的結果。
- 查詢結果大小必須小於 250 KB。
- 可以摘要的查詢結果每月配額為 3 MB。

## 下載已儲存的查詢結果

儲存查詢結果後，您必須能夠找到包含查詢結果的檔案。CloudTrail 會將您的查詢結果傳送至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，查詢結果可能會先顯示在主控台中，隨後才能在 S3 儲存貯體中檢視，因為 CloudTrail 會在查詢掃描完成後傳送查詢結果。儘管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，CloudTrail 將查詢結果傳送到 S3 儲存貯體可能需要更長的時間。CloudTrail 會以壓縮的 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

- 尋找您的 CloudTrail Lake 已儲存查詢結果
- 下載您的 CloudTrail Lake 已儲存查詢結果

## 尋找您的 CloudTrail Lake 已儲存查詢結果

CloudTrail 會將查詢結果和簽署檔案發佈到您的 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 CloudTrail Lake 儲存的查詢結果。

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
    amzn-s3-demo-bucket
        AWSLogs
            Account_ID;
                CloudTrail-Lake
                    Query
                        2022
                            06
                              20
                                Query_ID
```

## 下載您的 CloudTrail Lake 已儲存查詢結果

當您儲存查詢結果時，CloudTrail 會將兩種類型的檔案傳送到您的 Amazon S3 儲存貯體。

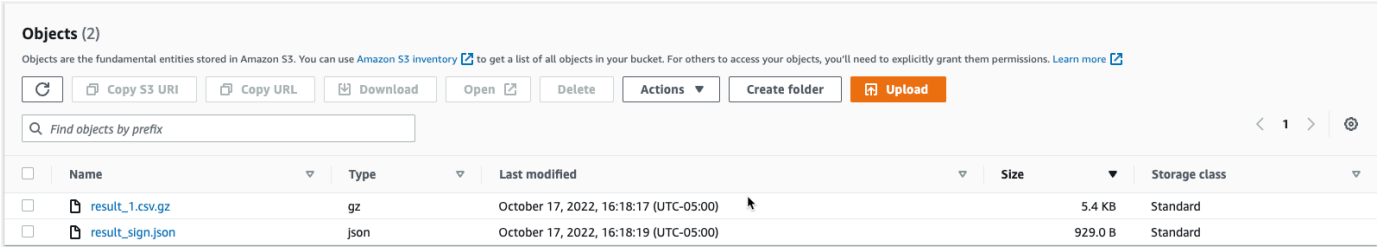
- 一個 JSON 格式的簽署檔案，可供您用於驗證查詢結果檔案。簽署檔案命名為 result_sign.json。如需簽署檔案的詳細資訊，請參閱 CloudTrail 簽署檔案結構。
- 一或多個 CSV 格式的查詢結果檔案，其中包含查詢的結果。傳送的查詢結果檔案數量取決於查詢結果的總大小。查詢結果檔案的檔案大小上限為 1 TB。每個查詢結果檔案都會命名為 result_*number*.csv.gz。例如，如果查詢結果的總大小為 2 TB，您將有兩個查詢結果檔案，result_1.csv.gz 和 result_2.csv.gz。

CloudTrail 查詢結果和簽署檔案是 Amazon S3 物件。您可以使用 S3 主控台、 AWS Command Line Interface (CLI) 或 S3 API 來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 CloudTrail Lake 儲存的查詢結果

若要判斷在 CloudTrail 傳送查詢結果之後，查詢結果是否經過修改、遭到刪除或保持不變，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。這可透過運算方式防止修改、刪除或偽造 CloudTrail 查詢結果檔案，而無需偵測。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可讓您知道查詢結果檔案是否已遭刪除或變更。

主題

- 使用 驗證已儲存的查詢結果 AWS CLI
- CloudTrail 簽署檔案結構
- CloudTrail 查詢結果檔案完整性驗證的自訂實作

## 使用 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。

先決條件

若要使用命令列驗證查詢結果完整性，必須符合下列條件：

- 您必須擁有 的線上連線 AWS。
- 您必須使用第 2 AWS CLI 版。
- 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 amzn-s3-demo-bucket --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 已儲存查詢結果。

```
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 | Description |
| --- | --- | --- |
| 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://amzn-s3-demo-bucket/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

以下範例簽署檔案包含 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 AWS 的帳戶區域。

`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 CloudTrail 將查詢結果傳送至 S3 儲存貯體的時間。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、公開使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 查詢結果檔案的完整性。當您將查詢結果儲存到 Amazon S3 儲存貯體時，CloudTrail 會將簽署檔案傳送到您的 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。

了解如何簽署 CloudTrail 簽署檔案

CloudTrail 簽署檔案使用 RSA 數位簽章進行簽署。針對每個簽署檔案，CloudTrail 會執行下列操作：

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

若要取得公有金鑰來驗證簽署檔案，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 CloudTrail 針對每個區域使用不同的私有/公有金鑰對，因此每個簽署檔案都使用其區域唯一的私有金鑰進行簽署。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 擷取公 AWS CLI 有金鑰

若要使用 擷取簽署檔案的公有金鑰 AWS CLI，請使用 `cloudtrail list-public-keys`命令。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 擷取公有金鑰

若要使用 CloudTrail API 擷取簽署檔案的公有金鑰，請將開始時間和結束時間值傳遞到 `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 | 選擇地指定要查詢 CloudTrail 簽署檔案公有金鑰之時間範圍的開始時間 (UTC)。如果未指定 StartTime，則會使用目前的時間，並傳回目前的公有金鑰。<br><br>類型：DateTime |
| EndTime | 選擇地指定要查詢 CloudTrail 簽署檔案公有金鑰之時間範圍的結束時間 (UTC)。如果未指定 EndTime，則會使用目前的時間。<br><br>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。<br><br>類型：Blob |
| ValidityStartTime | 公有金鑰的有效開始時間。<br><br>類型：DateTime |
| ValidityEndTime | 公有金鑰的有效結束時間。<br><br>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。<br><br>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 交付後已修改，SHA-256 雜湊將會變更，因此簽署檔案的簽章將會不符。

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驗證 CloudTrail 簽署和查詢結果檔案的骨架程式碼。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.");
```

```
    }
}
```

# 最佳化 CloudTrail Lake 查詢

此頁面提供如何最佳化 CloudTrail Lake 查詢以改善效能和可靠性的指引。它涵蓋了特定最佳化技術，以及常見查詢失敗的解決方法。

主題


- 最佳化查詢的建議
- 查詢失敗的解決方法


## 最佳化查詢的建議

請遵循本節中的建議來最佳化您的查詢。

建議：


- 最佳化彙總
- 使用近似技術
- 限制查詢結果
- 最佳化 LIKE 查詢
- 使用 UNION ALL 而非 UNION
- 僅包含必填資料欄
- 減少視窗函數範圍


### 最佳化彙總

排除子GROUP BY句中的備援資料欄可以提高效能，因為較少的資料欄需要較少的記憶體。例如，在以下查詢中，我們可以在像是 的備援資料欄上使用 arbitrary函數eventType來改善效能。上的 arbitrary函數eventType用於從群組隨機挑選欄位值，因為值相同，不需要包含在 GROUP BY子句中。

```
SELECT eventName, eventSource, arbitrary(eventType), count(*)
FROM $EDS_ID
GROUP BY eventName, eventSource
```

您可以透過GROUP BY依唯一值計數（基數）的遞減順序排序 中的欄位清單，來改善GROUP BY函數的效能。例如，在取得每個類型的事件數量時 AWS 區域，可以使用 來改善效能eventName，在GROUP BY函數中awsRegion排序 而非 awsRegion，eventName因為 比 eventName 更唯一值awsRegion。

```
SELECT eventName, awsRegion, count(*)
FROM $EDS_ID
GROUP BY eventName, awsRegion
```

使用近似技術

每當計算不同值時不需要確切的值時，請使用近似彙總函數來尋找最常用的值。例如，approx_distinct使用的記憶體比 操作少得多，而且執行速度比 COUNT(DISTINCT fieldName)操作快。

限制查詢結果

如果查詢只需要範例回應，請使用 LIMIT條件將結果限制為少量資料列。否則，查詢會傳回大型結果，並花費更多時間來執行查詢。

LIMIT 搭配 使用 ORDER BY可以更快地提供最上方或最下方 N 記錄的結果，因為它可減少排序所需的記憶體量和時間。

```
SELECT * FROM $EDS_ID
ORDER BY eventTime
LIMIT 100;
```

最佳化 LIKE 查詢

您可以使用 LIKE 來查找相符字串，但對於長字串而言，此為計算密集型。在大多數情況下，regexp_like函數是更快的替代方案。

通常，您可以透過錨定您要尋找的子字串來最佳化搜尋。例如，如果您正在尋找字首，最好使用 'substr%' 而非 '%substr%' 搭配 LIKE 運算子和 '^substr' 搭配 regexp_like函數。

使用 **UNION ALL** 而非 **UNION**

UNION ALL 和 UNION 是將兩個查詢的結果合併為一個結果，但UNION移除重複項目的兩種方式。UNION需要處理所有記錄並尋找重複項目，這是記憶體和運算密集型，但UNION ALL操作相對快速。除非您需要重複記錄，否則請使用 UNION ALL 以獲得最佳效能。

僅包含必填資料欄

如果您不需要資料欄，請不要將其包含在查詢中。查詢必須處理的資料越少，執行速度就越快。如果您有在最外部查詢SELECT *中執行的查詢，您應該將 * 變更為您需要的資料欄清單。

ORDER BY 子句會以排序順序傳回查詢的結果。排序大量資料時，如果沒有可用的必要記憶體，會將中繼排序結果寫入磁碟，這可能會減慢查詢執行速度。如果您並不需要對結果進行排序，請避免新增 ORDER BY 子句。此外，如果不需要的話，請避免ORDER BY將 新增至內部查詢。

減少視窗函數範圍

視窗函數會將其操作的所有記錄保留在記憶體中，以計算其結果。當視窗非常大時，視窗函數可能會耗盡記憶體。為了確保查詢在可用的記憶體限制內執行，請新增 PARTITION BY子句來減少視窗函數操作的視窗大小。

有時，具有視窗函數的查詢可以在沒有視窗函數的情況下重寫。例如，您可以使用彙總函數，例如 row_number或 rank，而不是使用 max_by或 min_by。

下列查詢會使用 尋找最近指派給每個 KMS 金鑰的別名max_by。

```
SELECT element_at(requestParameters, 'targetKeyId') as keyId,
max_by(element_at(requestParameters, 'aliasName'), eventTime) as mostRecentAlias
FROM $EDS_ID
WHERE eventsource = 'kms.amazonaws.com'
AND eventName in ('CreateAlias', 'UpdateAlias')
AND eventTime > DATE_ADD('week', -1, CURRENT_TIMESTAMP)
GROUP BY element_at(requestParameters, 'targetKeyId')
```

在此情況下， max_by函數會傳回具有群組內最新事件時間的記錄別名。與具有視窗函數的對等查詢相比，此查詢執行速度更快，而且使用的記憶體更少。

## 查詢失敗的解決方法

本節提供常見查詢失敗的解決方法。

查詢失敗：

- 查詢失敗，因為回應太大
- 查詢因資源耗盡而失敗

查詢失敗，因為回應太大

如果回應太大而導致訊息 ，查詢可能會失敗**Query response is too large**。如果發生這種情況，您可以減少彙總範圍。

這類彙總函數`array_agg`可能會導致查詢回應中的至少一列非常大，導致查詢失敗。例如，使用`array_agg(eventName)`而非 `array_agg(DISTINCT eventName)`會因為所選 CloudTrail 事件中的重複事件名稱而大幅增加回應大小。

查詢因資源耗盡而失敗

如果在執行聯結、彙總和視窗函數等記憶體密集型操作期間沒有足夠的記憶體可用，則中繼結果會溢出到磁碟，但溢出會減慢查詢執行速度，並不足以防止查詢因 而失敗**Query exhausted resources at this scale factor**。您可以透過重試查詢來修正此問題。

如果上述錯誤即使在最佳化查詢後仍持續存在，您可以使用事件`eventTime`的 縮小查詢範圍，並以原始查詢時間範圍的較小間隔多次執行查詢。

## 使用 執行和管理 CloudTrail Lake 查詢 AWS CLI

您可以使用 AWS CLI 來執行和管理 CloudTrail Lake 查詢。使用 時 AWS CLI，請記住，您的命令會在為您的設定檔 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 Lake 查詢的可用命令

在 CloudTrail Lake 中執行和管理查詢的命令包括：

- `start-query` 執行查詢。
- `describe-query` 傳回有關查詢的中繼資料。
- `generate-query` 從英文提示產生查詢。如需詳細資訊，請參閱從自然語言提示建立 CloudTrail Lake 查詢。
- `get-query-results` 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` 取消執行中的查詢。

如需 CloudTrail Lake 事件資料存放區的可用命令清單，請參閱 事件資料存放區的可用命令。

如需 CloudTrail Lake 儀表板的可用命令清單，請參閱 儀表板的可用命令。

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

## 使用 從自然語言提示產生查詢 AWS CLI

執行 generate-query命令，從英文提示產生查詢。針對 --event-data-stores，提供您要查詢的事件資料存放區的 ARN （或 ARN 的 ID 尾碼）。您只能指定一個事件資料存放區。對於 --prompt，請以英文提供提示。

```
aws cloudtrail generate-query
--event-data-stores arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-ee54-4813-92d5-999aeEXAMPLE \
--prompt "Show me all console login events for the past week?"
```

如果成功，命令會輸出 SQL 陳述式QueryAlias，並提供您將與 start-query命令搭配使用的 ，以針對您的事件資料存放區執行查詢。

```
{
  "QueryStatement": "SELECT * FROM $EDS_ID WHERE eventname = 'ConsoleLogin' AND
 eventtime >= timestamp '2024-09-16 00:00:00' AND eventtime <= timestamp '2024-09-23
 00:00:00' AND eventSource = 'signin.amazonaws.com'",
  "QueryAlias": "AWSCloudTrail-UUID"
}
```

## 使用 啟動查詢 AWS CLI

下列範例 AWS CLI start-query命令會在 查詢陳述式中指定為 ID 的事件資料存放區上執行查詢，並將查詢結果傳送到指定的 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-s3-uri，用於將查詢結果傳送到指定的 S3 儲存貯體。如需可在 CloudTrail Lake 中使用之查詢語言的詳細資訊，請參閱 CloudTrail Lake SQL 限制條件。

```
aws cloudtrail start-query
--query-statement 'SELECT eventID, eventTime FROM EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE
 LIMIT 10'
--delivery-s3-uri "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。如果您使用選用的 `--delivery-s3-uri` 參數將查詢結果傳送到 S3 儲存貯體，則儲存貯體政策必須授予 CloudTrail 許可，才能將查詢結果傳送到儲存貯體。如需手動編輯儲存貯體政策的資訊，請參閱「適用於 CloudTrail Lake 查詢結果的 Amazon S3 儲存貯體政策」。

## 使用 取得有關查詢的中繼資料 AWS CLI

下列範例 AWS CLI describe-query命令會取得查詢的中繼資料，包括以毫秒為單位的查詢執行時間、掃描和比對的事件數、掃描的總位元組數，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"
    }
```

```
}
```

## 使用 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"
}
```

## 使用 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"
}
```

## 使用 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 的查詢RUNNING。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 Lake SQL 限制條件

CloudTrail Lake 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。

SELECT 陳述式的 CloudTrail Lake 語法如下所示。事件資料存放區 ID - 事件資料存放區 ARN 的 ID 部分會指定為 FROM值。

```
SELECT [ DISTINCT ] columns [ Aggregate ]
[ FROM table event_data_store_ID]
[ WHERE columns [ Conditions ] ]
[ GROUP BY columns [ DISTINCT | Aggregate ] ]
[ HAVING columns [ Aggregate | Conditions ] ]
[ ORDER BY columns [ Aggregate | ASC | DESC | NULLS | FIRST | LAST ]
[ LIMIT [ INT ] ]
```

CloudTrail Lake 支援所有有效的 Trino SQL SELECT陳述式、函數和運算子。如需支援的 SQL 函數和運算子的詳細資訊，請參閱 Trino 文件網站上的函數和運算子。

CloudTrail 主控台提供許多範例查詢，可協助您開始自行編寫查詢。如需詳細資訊，請參閱使用 CloudTrail 主控台檢視範例查詢。

如需如何最佳化查詢的資訊，請參閱 最佳化 CloudTrail Lake 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 Lake 支援所有 Trino 函數。如需支援函數的詳細資訊，請參閱 Trino 文件網站上的函數和運算子。

## 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

- 支援的 CloudTrail 事件記錄欄位結構描述
- CloudTrail Insights 事件記錄欄位的受支援結構描述
- AWS Config 支援組態項目記錄欄位的結構描述
- AWS Audit Manager 證據記錄欄位支援的結構描述
- 非AWS 事件欄位支援的結構描述

## 支援的 CloudTrail 事件記錄欄位結構描述

以下是 CloudTrail 管理、資料和網路活動事件記錄欄位的有效 SQL 結構描述。如需有關 CloudTrail 事件記錄欄位的詳細資訊，請參閱 CloudTrail 記錄管理、資料和網路活動事件的內容。

```
[
    {
        "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>,onbehalfof:struct<userid:string,identitystorearn:string>,
```

```
inscopeof:struct<sourcearn:string,sourceaccount:string,issuertype:string,
                credentiaisissuedto: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": "vpcendpointaccountid",
        "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 Insights 事件記錄欄位的受支援結構描述

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`。如需這些欄位的說明，請參閱 [事件資料存放區的 Insights 事件 CloudTrail 記錄內容](#)。

> **Note**
>
> 欄位內的 `insightvalue`、`baselinevalue`、 `insightaverage`和 `baselineaverage` 欄位`attributionsinsightContext`將於 2025 年 6 月 23 日開始棄用。

```
[
    {
        "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,
                 insight:struct<value:string,average:double>,
                 baseline:struct<value:string,average:double>>>"
    }
```

```
]
```

## AWS Config 支援組態項目記錄欄位的結構描述

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>>"
    }
]
```

## AWS Audit Manager 證據記錄欄位支援的結構描述

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 在 CloudTrail Lake 中彙總證據的詳細資訊，請參閱 AWS Audit Manager 使用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 事件欄位支援的結構描述

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`，而 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>>"
    }
]
```

# 支援的 CloudWatch 指標

CloudTrail Lake 支援 Amazon CloudWatch 指標。CloudWatch 是 AWS 資源的監控服務。您可以使用 CloudWatch 來收集和追蹤指標、設定警示，並自動回應 AWS 資源的變更。

AWS/CloudTrail 命名空間包含 CloudTrail Lake 的下列指標。

| 指標 | Description | 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。<br><br>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。<br><br>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。<br><br>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。<br><br>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 | 位元組 |

| 指標 | Description | 單位 |
| --- | --- | --- |
| | 保留期) 的儲存已包含在擷取定價中，無須額外付費。在 366 天之後，儲存將為按使用量付費。如需關於定價的資訊，請參閱AWS CloudTrail 定價。<br><br>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 Insights 所分析的事件總數。此指標每小時更新一次。<br><br>此指標適用於啟用 CloudTrail Insights 的 CloudTrail 事件資料存放區。 | 計數 |

如需 CloudWatch 指標的詳細資訊，請參閱下列主題。

- 使用 Amazon CloudWatch 指標
- 使用 Amazon CloudWatch 警示

# 使用 CloudTrail 追蹤

線索會擷取 AWS 活動記錄，在 Amazon S3 儲存貯體中交付和存放這些事件，並選擇性交付至 CloudWatch Logs 和 Amazon EventBridge。

您可以透過建立線索，從 CloudTrail 免費將一份持續管理事件的副本交付至 S3 儲存貯體，不過，需要支付 Amazon S3 儲存費用。如需 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 建立多區域和單一區域線索 AWS 帳戶。

多區域追蹤

當您建立多區域追蹤時，CloudTrail 會在 中啟用的所有 中記錄事件 AWS 區域 ， AWS 帳戶 並將 CloudTrail 事件日誌檔案交付至您指定的 S3 儲存貯體。根據最佳實務，我們建議您建立多區域追蹤，因為它會擷取所有啟用區域中的活動。使用 CloudTrail 主控台建立的所有線索都是多區域線索。您可以使用 將單一區域線索轉換為多區域線索 AWS CLI。如需詳細資訊，請參閱了解多區域追蹤和選擇加入區域、使用主控台建立追蹤及將單一區域追蹤轉換為多區域追蹤。

單一區域追蹤

當您建立單一區域追蹤時，CloudTrail 只會記錄該區域中的事件。其接著會將 CloudTrail 事件日誌檔案交付到您指定的 Amazon S3 儲存貯體。您只能使用 AWS CLI建立單一區域追蹤。如果您建立其他單一線索，則可以讓這些線索將 CloudTrail 事件日誌檔案傳送到相同的 S3 儲存貯體或單獨的儲存貯體。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，請參閱使用 建立、更新和管理線索 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，您可以建立組織追蹤，記錄該組織中所有 AWS 帳戶的所有事件。組織追蹤可以套用至所有 AWS 區域或目前區域。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。成員帳戶可以查看組織線索，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。如需詳細資訊，請參閱建立組織追蹤。

主題

- 為您的 建立線索 AWS 帳戶
- 建立組織追蹤
- 了解多區域追蹤和選擇加入區域
- 將追蹤事件複製到 CloudTrail Lake
- 取得和檢視 CloudTrail 日誌檔案
- 設定 CloudTrail 的 Amazon SNS 通知
- AWS CloudTrail 搭配界面 VPC 端點使用
- CloudTrail 資源、S3 儲存貯體和 KMS 金鑰的命名需求
- AWS 帳戶 關閉和追蹤


# 為您的 建立線索 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。
- 可透過將事件記錄傳送到 Amazon CloudWatch Logs 的方式，自動針對指定事件進行監控和發出警示的選項。
- 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，您只能在記錄事件的 AWS 區域中檢視追蹤。如果您建立多區域追蹤，它會顯示在您帳戶中 AWS 區域 啟用的所有 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。根據最佳實務，我們建議您建立多區域追蹤，因為它會擷取所有啟用區域中的活動。使用 CloudTrail 主控台建立的所有線索都是多區域線索。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。建立組織的線索，將自動啟用 CloudTrail 和 Organizations 之間的整合。如需詳細資訊，請參閱建立組織追蹤。

如果您的追蹤設定錯誤 (例如，S3 儲存貯體無法連線)，CloudTrail 會在 30 天內嘗試重新傳遞日誌檔案到您的 S3 儲存貯體，且您需要為這些嘗試傳遞事件支付標準 CloudTrail 費用。若要避免支付追蹤設定錯誤費用，您需要刪除追蹤。

主題


- 使用主控台建立和更新線索
- 使用 建立、更新和管理線索 AWS CLI
- 建立多個線索


## 使用主控台建立和更新線索

您可以使用 CloudTrail 主控台建立、更新或刪除您的追蹤。使用主控台建立的追蹤為多區域追蹤。若要建立僅記錄事件的線索 AWS 區域，請使用 AWS CLI。

每個區域最多可以建立五個追蹤。在您建立線索後，CloudTrail 會自動開始將您帳戶中的 API 呼叫及相關事件記錄到您指定的 Amazon S3 儲存貯體。

您可以使用 CloudTrail 主控台變更追蹤的下列設定：

- 您可以變更 S3 儲存貯體位置並指定字首。
- AWS Organizations 組織的管理帳戶可以將帳戶層級追蹤轉換為組織追蹤，也可以將組織追蹤轉換為帳戶層級追蹤。
- 您可以啟用或停用 KMS 金鑰加密。
- 您可以啟用或停用日誌檔案驗證。日誌檔案驗證可讓您判斷日誌檔案是否在 CloudTrail 交付後遭到修改、刪除或保持不變。預設會啟用日誌檔案驗證。
- 您可以設定線索，將通知傳送至 Amazon SNS 主題。
- 您可以設定線索，將事件傳送至 CloudWatch Logs 日誌群組。日誌群組和 IAM 角色都必須存在於您自己的帳戶中。
- 您可以更新管理事件、資料事件、網路活動事件和 Insights 事件的設定。
- 您可以新增或移除標籤。您最多可以新增 50 個標籤金鑰對，以協助您識別追蹤。

使用 CloudTrail 主控台建立或更新追蹤具有下列優點。

- 如果這是您第一次建立線索，則使用 CloudTrail 主控台可讓您檢視可用的功能和選項。

- 如果您要設定線索來記錄資料事件，則使用 CloudTrail 主控台可讓您檢視可用的資料類型。如需詳細資訊，請參閱記錄資料事件。
- 如果您要設定網路活動事件的線索，使用 CloudTrail 主控台可讓您檢視可用的事件來源。如需詳細資訊，請參閱記錄網路活動事件。

如需在 中為組織建立追蹤的特定資訊 AWS Organizations，請參閱 建立組織追蹤。

主題

- 使用 CloudTrail 主控台建立追蹤
- 使用 CloudTrail 主控台更新線索
- 使用 CloudTrail 主控台刪除線索
- 關閉記錄線索

## 使用 CloudTrail 主控台建立追蹤

線索可以套用至在您的 中啟用的所有 AWS 區域 AWS 帳戶，也可以套用至單一區域。套用至 中所有啟用 AWS 區域 的線索 AWS 帳戶 稱為多區域線索。根據最佳實務，我們建議您建立多區域追蹤，因為它會擷取所有啟用區域中的活動。使用 CloudTrail 主控台建立的所有線索都是多區域線索。您只能使用 AWS CLI 或 `CreateTrail` API 操作建立單一區域追蹤。

> **Note**
>
> 建立追蹤之後，您可以設定其他 AWS 服務 以進一步分析和處理 CloudTrail 日誌中收集的事件資料。如需詳細資訊，請參閱AWS 服務與 CloudTrail 日誌的整合。

主題

- 使用主控台建立追蹤
- 後續步驟

### 使用主控台建立追蹤

使用下列程序建立多區域追蹤。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 追蹤 AWS 管理主控台

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
2. 在 CloudTrail 服務首頁上，Trails (追蹤) 頁面，或 Dashboard (儀表板) 頁面的 Trails (追蹤) 區段上，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CloudTrail 資源、S3 儲存貯體和 KMS 金鑰的命名需求。
4. 如果這是 AWS Organizations 組織線索，您可以為組織中的所有帳戶啟用線索。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。當您建立儲存貯體時，CloudTrail 會建立和套用所需的儲存貯體政策。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`動作的許可，因為預設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。儲存貯體政策必須授予 CloudTrail 寫入的許可。如需手動編輯儲存貯體政策的資訊，請參閱「適用於 CloudTrail 的 Amazon S3 儲存貯體政策」。

   若要更容易地找到您的記錄，請在現有的儲存貯體中建立新的資料夾 (也稱為prefix ) 來存儲您的 CloudTrail 日誌。在字首中輸入字首。
6. 對於日誌檔案 SSE-KMS 加密，如果您想要使用 SSE-KMS 加密而非 SSE-S3 加密來加密日誌檔案和摘要檔案，請選擇已啟用。預設為啟用。如果您未啟用 SSE-KMS 加密，您的日誌檔案和摘要檔案會使用 SSE-S3 加密進行加密。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，指定別名，格式為 `alias/MyAliasName`。如需詳細資訊，請參閱更新資源以搭配 主控台使用您的 KMS 金鑰。CloudTrail 也支援 AWS KMS 多區域金鑰。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**
>
> 您也可以輸入來自另一個帳戶的金鑰 ARN。如需詳細資訊，請參閱更新資源以搭配 主控台使用您的 KMS 金鑰。金鑰政策必須允許 CloudTrail 使用金鑰來加密您的日誌檔案和摘要檔案，並允許您指定的使用者以未加密的形式讀取日誌檔案或摘要檔案。如需手動編輯金鑰政策的資訊，請參閱「設定 CloudTrail 的 AWS KMS 金鑰政策」。

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。您可以使用摘要檔案來驗證您的日誌檔案在 CloudTrail 交付以後未變更。如需詳細資訊，請參閱 驗證 CloudTrail 日誌檔案完整性。

   b. 針對 SNS notification delivery (SNS 通知傳送)，若要在每次日誌交付至您的儲存貯體時收到通知，請選擇 Enabled (啟用)。CloudTrail 會在日誌檔案存放多個事件。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 CloudTrail 的 Amazon SNS 通知。

      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。如果您要建立多區域追蹤，所有已啟用區域的日誌檔案交付 SNS 通知會傳送至您建立的單一 SNS 主題。

      如果選擇 New (新的)，CloudTrail 會為您指定新主題的名稱，或者您可以輸入名稱。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 適用於 CloudTrail 索的 Amazon SNS 主題政策。

      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. 選擇性地設定 CloudTrail 以將日誌檔案傳送至 CloudWatch Logs，方法是選擇CloudWatch Logs 中的 Enabled (啟用)。如需詳細資訊，請參閱 傳送事件到 CloudWatch Logs。

   a. 如果您啟用與 CloudWatch Logs 整合功能，請選擇 New (新的) 建立新日誌群組，或 Existing (現有) 以使用現有的群組。如果選擇 New (新的)，CloudTrail 會為您指定新日誌群組的名稱，或者您可以輸入名稱。

   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 New (新的) 為將日誌傳送至 CloudWatch Logs 的許可建立新的 IAM 角色。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 讓 CloudTrail 能使用 CloudWatch Logs 進行監控的角色政策文件。

> **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，如果您要 CloudTrail 將事件交付至 CloudWatch Logs 日誌群組，則必須選擇存在於目前帳戶中的日誌群組。
> - 只有管理帳戶可以為使用主控台的組織追蹤設定 CloudWatch Logs 日誌群組。委派管理員可以使用 AWS CLI 或 CloudTrail 或 API 操作來設定 CloudWatch Logs 日誌群組。 CloudTrail `CreateTrail` `UpdateTrail`

9. 對於標籤，您最多可以新增 50 個標籤金鑰對，以協助您識別、排序和控制對線索的存取。標籤可協助您辨識 CloudTrail 追蹤和包含 CloudTrail 日誌檔案的 Amazon S3 儲存貯體。然後，您可以對 CloudTrail 資源使用資源群組。如需詳細資訊，請參閱AWS Resource Groups及Tags (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) 事件篩選出您的線索。預設設定為包含所有 AWS KMS 事件。

    只有在您的線索上記錄管理 AWS KMS 事件時，才提供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 `Encrypt`、 `Decrypt`和 等動作`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。少量的相關 AWS KMS 動作，例如 `Disable`、 `Delete`和 `ScheduleKey`（通常佔 AWS KMS 事件量的 0.5% 以下） 會記錄為寫入事件。

    若要排除大量事件`Decrypt`，例如 `Encrypt`、 和 `GenerateDataKey`，但仍會記錄相關事件，例如 `Disable`、 `Delete`和 `ScheduleKey`，請選擇記錄寫入管理事件，並清除排除 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源類型，並對線索擷取的資料事件提供精細的控制。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。

針對資源類型，選擇您要記錄資料事件的資源類型。如需可用資源類型的詳細資訊，請參閱 資料事件。

13. 選擇日誌選取器範本。您可以選擇預先定義的範本，或選擇自訂來定義您自己的事件集合條件。

    您可以從下列預先定義的範本中選擇：

    - 記錄所有事件：選擇此範本記錄所有事件。
    - 僅記錄讀取事件 – 選擇此範本以僅記錄讀取事件。唯讀事件是不會變更資源狀態的事件，例如 `Get*`或 `Describe*`事件。
    - 僅記錄寫入事件 – 選擇此範本僅記錄寫入事件。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。
    - 僅記錄 AWS 管理主控台 事件 – 選擇此範本僅記錄源自 的事件 AWS 管理主控台。
    - 排除 AWS 服務 啟動的事件 – 選擇此範本以排除具有 `eventType`之 AWS 服務 的事件`AwsServiceEvent`，以及使用連結角色 (SLRs) AWS 服務啟動的事件。

> **Note**
>
> 選擇 S3 儲存貯體的預先定義範本，可讓您 AWS 帳戶中目前所有儲存貯體的資料事件記錄，以及您在完成建立追蹤後建立的任何儲存貯體。它也可以記錄您 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 帳戶的儲存貯體上執行。

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。它不會記錄您 AWS 帳戶中其他區域中 Amazon S3 儲存貯體的資料事件。
如果您要建立多區域線索，選擇 Lambda 函數的預先定義範本，可啟用 AWS 目前帳戶中所有函數的資料事件記錄，以及在完成建立線索後，您可以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線索 （使用 完成 AWS CLI)，則此選擇會啟用 AWS 帳戶中目前該區域中所有函數的資料事件記錄，以及在您完成建立線索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. 如果您選取自訂，在進階事件選取器中，會根據進階事件選取器欄位的值來建置表達式。

> **Note**
>
> 選取器不支援使用萬用字元，例如 * 。若要將多個值與單一條件比對，您可以使用 StartsWith、NotStartsWith、 EndsWith或 NotEndsWith來明確比對事件欄位的開頭或結尾。

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任何記錄到 CloudTrail 的資料事件，例如 PutBucket、GetItem 或 GetSnapshotBlock。
- **eventSource** – 要包含或排除的事件來源。此欄位可以使用任何運算子。

- eventType – 要納入或排除的事件類型。例如，您可以將此欄位設定為不等於AwsServiceEvent排除 AWS 服務 事件。如需事件類型的清單，請參閱 eventType中的 CloudTrail 記錄管理、資料和網路活動事件的內容。
- sessionCredentialFromConsole – 包含或排除源自 AWS 管理主控台 工作階段的事件。此欄位可以設定為等於或不等於 的值true。
- userIdentity.arn – 針對特定 IAM 身分執行的動作納入或排除事件。如需更多詳細資訊，請參閱 CloudTrail userIdentity 元素。
- **resources.ARN** - 您可以將任何運算子與 搭配使用resources.ARN，但如果您使用等於或不等於，則該值必須完全符合您在範本中指定之類型之有效資源的 ARN，做為 的值resources.type。

> **Note**
>
> 您無法使用 resources.ARN 欄位來篩選沒有 ARNs的資源類型。

如需資料事件資源 ARN 格式的詳細資訊，請參閱《服務授權參考》中的 的動作、資源和條件索引鍵 AWS 服務。

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，若要從記錄於事件資料存放區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 的運算子設定為 不以 開頭，然後貼入您不想記錄事件的 S3 儲存貯體 ARN。

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。

如需有關 CloudTrail 如何評估多個條件的資訊，請參閱 CloudTrail 如何評估欄位的多項條件。

> **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。

16. 若要新增要記錄資料事件的其他資源類型，請選擇新增資料事件類型。重複步驟 12 到此步驟，為資源類型設定進階事件選取器。

17. 若要在資料事件上啟用彙總，請選擇一或多個彙總範本。這些範本會定義資料事件的摘要方式。您可以從下列範本中選擇：

    a. API 活動，根據所做的 API 呼叫，取得資料事件的 5 分鐘摘要。使用此選項來了解您的 API 使用模式，包括頻率、呼叫者和來源。

    b. 資源存取，以取得 AWS 資源上的活動模式。使用此項目來了解您的 AWS 資源如何被存取、在 5 分鐘的時段中被存取多少次、誰正在存取資源，以及正在執行哪些動作。

    c. 使用者動作，根據在您帳戶中進行 API 呼叫的 IAM 主體來取得活動模式。

    > **Note**
    >
    > 彙總適用於追蹤中收集的所有資料事件。

18. 若要記錄網路活動事件，請選擇網路活動事件。網路活動事件可讓 VPC 端點擁有者記錄使用其 VPC 端點從私有 VPC 到 的 AWS API 呼叫 AWS 服務。記錄網路活動事件需支付額外費用。如需詳細資訊，請參閱AWS CloudTrail 定價。

    若要記錄網路活動事件，請執行下列動作：

    a. 從網路活動事件來源中，選擇網路活動事件的來源。

    b. 在日誌選取器範本中，選擇範本。您可以選擇記錄所有網路活動事件、記錄所有網路活動存取遭拒的事件，或選擇自訂以建置自訂日誌選取器來篩選多個欄位，例如 `eventName`和 `vpcEndpointId`。

    c. （選用）輸入名稱以識別選取器。選擇器名稱在進階事件選擇器中列為名稱，如果您展開 JSON 檢視，則可檢視。

    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。如果您使用預先定義的日誌範本，則可略過此步驟。

        i. 對於排除或包含網路活動事件，您可以在 主控台中選擇下列欄位。

- **eventName** – 您可以將任何運算子與 搭配使用eventName。您可以使用它來包含或排除任何事件，例如 CreateKey。
- **errorCode** – 您可以使用它來篩選錯誤碼。目前，唯一支援的errorCode是VpceAccessDenied。
- **vpcEndpointId** – 識別操作通過的 VPC 端點。您可以搭配 使用任何運算子vpcEndpointId。

ii. 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。

iii. 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。

e. 若要新增要記錄網路活動事件的其他事件來源，請選擇新增網路活動事件選取器。

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

19. 如果您想要追蹤記錄 CloudTrail Insights 事件，請選擇 Insights 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，請參閱使用 CloudTrail Insights。記錄 Insights 事件需支付額外費用。如需 CloudTrail 定價，請參閱 AWS CloudTrail 定價。

    Insights 事件會傳遞到相同 S3 儲存貯體上名為 /CloudTrail-Insight 的不同資料夾，此資料夾是在追蹤詳細資訊頁面的 Storage location (儲存位置) 區域中指定的。CloudTrail 會為您建立新的前綴。例如，如果您目前的目的地 S3 儲存貯體名為 amzn-s3-demo-bucket/AWSLogs/CloudTrail/，則具有新前綴的 S3 儲存貯體名稱會被命名為 amzn-s3-demo-bucket/AWSLogs/CloudTrail-Insight/。

20. 當您完成選擇要記錄的事件類型時，請選擇 Next (下一頁)。

21. 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)。

22. 新的追蹤會出現在 Trails (追蹤) 頁面上。約 5 分鐘後，CloudTrail 會發佈日誌檔案，其中顯示您帳戶中曾進行的 AWS API 呼叫。您可以在所指定之 S3 儲存貯體中看到日誌檔案。

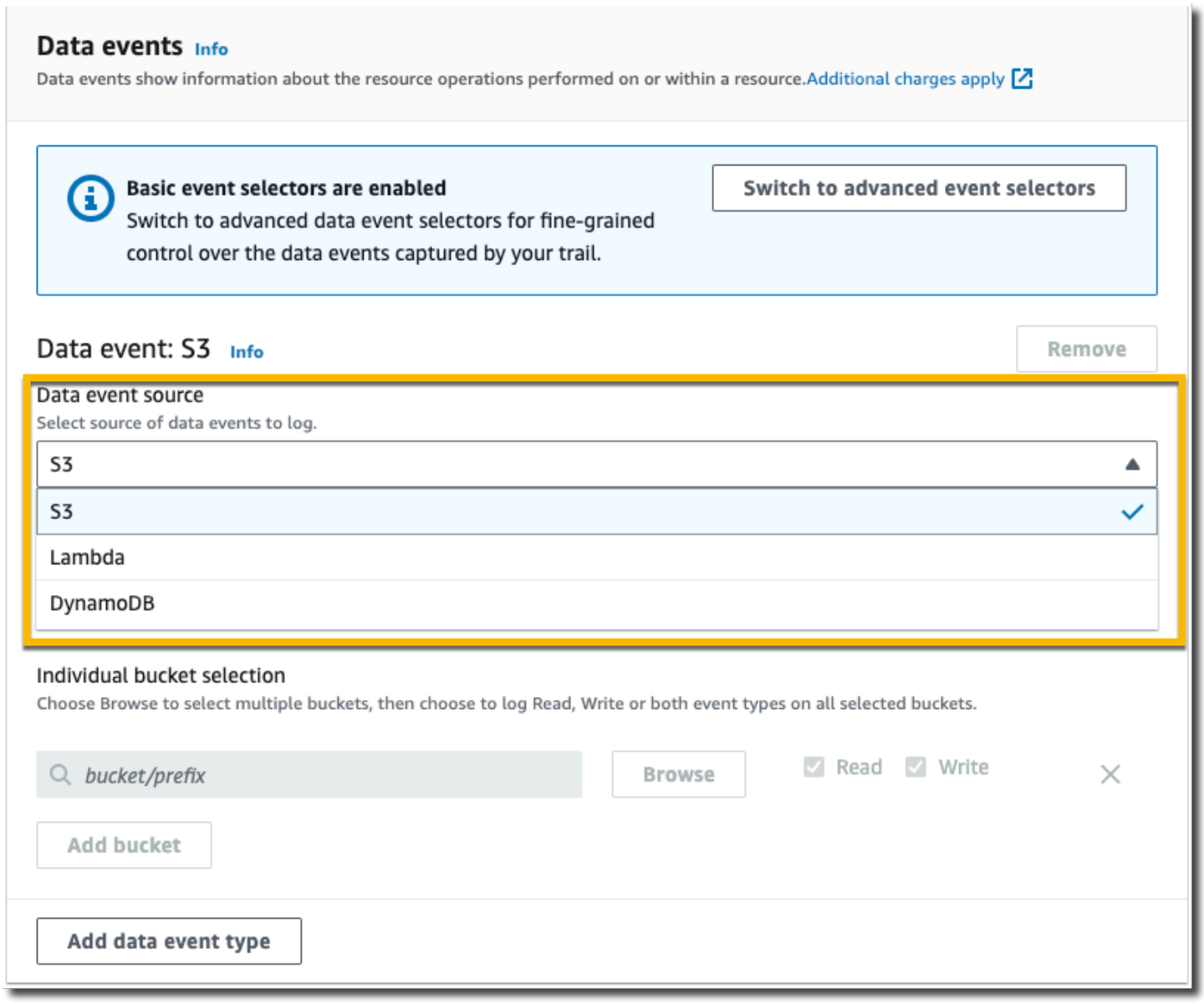
    如果您為線索啟用 Insights 事件，CloudTrail 最多可能需要 36 小時才能開始交付這些事件，前提是在此期間偵測到異常活動。

> **Note**
>
> CloudTrail 通常會在 API 呼叫的平均約 5 分鐘內傳遞日誌。此時間無法保證。如需詳細資訊，請參閱 AWS CloudTrail 服務水準協議。
> 如果您的追蹤設定錯誤 (例如，S3 儲存貯體無法連線)，CloudTrail 會在 30 天內嘗試重新傳遞日誌檔案到您的 S3 儲存貯體，且您需要為這些嘗試傳遞事件支付標準 CloudTrail 費用。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以及網路活動事件。進階事件選取器可讓您建立精細選取器，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，則僅限於記錄 Amazon S3 儲存貯體、 AWS Lambda 函數和 Amazon DynamoDB 資料表的資料事件。您無法使用基本事件選取器篩選 `eventName` 欄位。您也無法記錄網路活動事件。




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 所有目前和未來的 S3 儲存貯體選項會啟用您 AWS 帳戶中目前所有儲存貯體的資料事件記錄，以及您在完成建立追蹤後建立的任何儲存貯體。它也可以記錄您 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 帳戶的儲存貯體上執行。
> 如果您要為單一區域建立追蹤（使用 完成 AWS CLI)，請選擇所有目前和未來的 S3 儲存貯體，以啟用與追蹤相同區域中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。它不會記錄您 AWS 帳戶中其他區域中 Amazon S3 儲存貯體的資料事件。

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. 若要新增要記錄資料事件的其他資源類型，請選擇新增資料事件類型。

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**
>
> 如果您要建立多區域線索，此選擇會啟用 AWS 目前帳戶中所有函數的資料事件記錄，以及在您完成建立線索後，您可以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線索（使用 完成 AWS CLI)，此選擇會啟用 AWS 帳戶中目前該區域中所有函數的資料事件記錄，以及在您完成建立線索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於 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命令來設定特定 Lambda 函數的資料事件記錄。如需詳細資訊，請參閱使用管理線索 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 將日誌檔案傳送到 CloudWatch Logs。如需詳細資訊，請參閱 傳送事件到 CloudWatch Logs。
- 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》中的在 CloudTrail 主控台中建立 CloudTrail 日誌的資料表。
- 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。

## 使用 CloudTrail 主控台更新線索

本節將描述如何變更追蹤設定。

若要將單一區域線索轉換為多區域線索，或更新多區域線索以僅記錄單一區域中的事件，您必須使用 AWS CLI。如需如何將單一區域線索轉換為多區域線索的詳細資訊，請參閱 將單一區域追蹤轉換為多區域追蹤。如需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，則需要維護至少一個多區域，會同時記錄 `read` 和 `write` 管理事件的組織追蹤。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**
>
> 即使資源驗證失敗，CloudTrail 也會更新成員帳戶中的組織線索。驗證失敗的範例包括：
>
> - 不正確的 Amazon S3 儲存貯體政策
> - 不正確的 Amazon SNS 主題政策
> - 無法交付至 CloudWatch Logs 日誌群組
> - 使用 KMS 金鑰加密的許可不足
>
> 具有 CloudTrail 許可的成員帳戶可以透過在 CloudTrail 主控台上檢視追蹤的詳細資訊頁面，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 更新線索 AWS 管理主控台

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。

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。

   - 將線索套用至我的組織 - 變更此線索是否為 AWS Organizations 組織線索。

     > **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. 若要將線索變更為 AWS Organizations 組織線索，您可以選擇為組織中的所有帳戶啟用線索。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。當您建立儲存貯體時，CloudTrail 會建立和套用所需的儲存貯體政策。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`動作的許可，因為預設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。儲存貯體政策必須授予 CloudTrail 寫入的許可。如需手動編輯儲存貯體政策的資訊，請參閱「適用於 CloudTrail 的 Amazon S3 儲存貯體政策」。

      若要更容易地找到您的記錄，請在現有的儲存貯體中建立新的資料夾 (也稱為prefix ) 來存儲您的 CloudTrail 日誌。在字首中輸入字首。

   c. 對於日誌檔案 SSE-KMS 加密，如果您想要使用 SSE-KMS 加密而非 SSE-S3 加密來加密日誌檔案和摘要檔案，請選擇已啟用。預設為啟用。如果您未啟用 SSE-KMS 加密，您的日誌檔案和摘要檔案會使用 SSE-S3 加密進行加密。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，指定別名，格式為 `alias/MyAliasName`。如需詳細資訊，請參閱更新資源以搭配 主控台使用您的 KMS 金鑰。CloudTrail 也支援 AWS KMS 多區域金鑰。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**
>
> 您也可以輸入來自另一個帳戶的金鑰 ARN。如需詳細資訊，請參閱更新資源以搭配主控台使用您的 KMS 金鑰。金鑰政策必須允許 CloudTrail 使用金鑰來加密您的日誌檔案和摘要檔案，並允許您指定的使用者以未加密的形式讀取日誌檔案或摘要檔案。如需手動編輯金鑰政策的資訊，請參閱「設定 CloudTrail 的 AWS KMS 金鑰政策」。

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。您可以使用摘要檔案來驗證您的日誌檔案在 CloudTrail 交付以後未變更。如需詳細資訊，請參閱 驗證 CloudTrail 日誌檔案完整性。

e. 針對 SNS notification delivery (SNS 通知傳送)，若要在每次日誌交付至您的儲存貯體時收到通知，請選擇 Enabled (啟用)。CloudTrail 會在日誌檔案存放多個事件。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 CloudTrail 的 Amazon SNS 通知。

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。如果您要建立多區域追蹤，所有已啟用區域的日誌檔案交付 SNS 通知會傳送至您建立的單一 SNS 主題。

如果選擇 New (新的)，CloudTrail 會為您指定新主題的名稱，或者您可以輸入名稱。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 適用於 CloudTrail 索的 Amazon SNS 主題政策。

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 Logs 中，選擇 Edit (編輯)，以變更將 CloudTrail 日誌檔案傳送至 CloudWatch Logs 的設定。選擇 CloudWatch Logs 中的 Enabled (已啟用)，以啟用傳送日誌檔案。如需詳細資訊，請參閱 傳送事件到 CloudWatch Logs。

   a. 如果您啟用與 CloudWatch Logs 整合功能，請選擇 New (新的) 建立新日誌群組，或 Existing (現有) 以使用現有的群組。如果選擇 New (新的)，CloudTrail 會為您指定新日誌群組的名稱，或者您可以輸入名稱。

   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 New (新的) 為將日誌傳送至 CloudWatch Logs 的許可建立新的 IAM 角色。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 讓 CloudTrail 能使用 CloudWatch Logs 進行監控的角色政策文件。

   > **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，如果您要 CloudTrail 將事件交付至 CloudWatch Logs 日誌群組，則必須選擇存在於目前帳戶中的日誌群組。
   > - 只有管理帳戶可以為使用主控台的組織追蹤設定 CloudWatch Logs 日誌群組。委派管理員可以使用 AWS CLI 或 CloudTrail 或 API 操作來設定 CloudWatch Logs 日誌群組。 CloudTrail `CreateTrail` `UpdateTrail`

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。您最多可以新增 50 個標籤金鑰對，以協助您識別、排序和控制對線索的存取。標籤可協助您辨識 CloudTrail 追蹤和包含 CloudTrail 日誌檔案的 Amazon S3 儲存貯體。然後，您可以對 CloudTrail 資源使用資源群組。如需詳細資訊，請參閱AWS Resource Groups及Tags (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 KMS) 事件篩選 AWS Key Management Service 出您的線索。預設設定是包含所有 AWS KMS 事件。

      只有在您的線索上記錄管理 AWS KMS 事件時，才提供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 Encrypt、 Decrypt和 等動作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。少量的相關 AWS KMS 動作，例如 Disable、 Delete和 ScheduleKey （通常佔 AWS KMS 事件量的 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**
>
> 步驟 7-11 是使用進階事件選取器來設定資料事件，這是預設值。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。如果您打算記錄網路活動事件，則必須使用進階事件選取器。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。

針對資源類型，選擇您要記錄資料事件的資源類型。如需可用資源類型的詳細資訊，請參閱 資料事件。

8. 選擇日誌選取器範本。您可以選擇預先定義的範本，或選擇自訂來定義您自己的事件集合條件。

   您可以從下列預先定義的範本中選擇：

   - 記錄所有事件：選擇此範本記錄所有事件。
   - 僅記錄讀取事件 – 選擇此範本以僅記錄讀取事件。唯讀事件是不會變更資源狀態的事件，例如 Get*或 Describe*事件。
   - 僅記錄寫入事件 – 選擇此範本僅記錄寫入事件。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。
   - 僅記錄 AWS 管理主控台 事件 – 選擇此範本僅記錄源自 的事件 AWS 管理主控台。

- 排除 AWS 服務 啟動的事件 – 選擇此範本以排除具有 `eventType`之 AWS 服務 的事件`AwsServiceEvent`，以及使用連結角色 (SLRs) AWS 服務啟動的事件。

> **Note**
>
> 選擇 S3 儲存貯體的預先定義範本，可為您 AWS 帳戶中目前的所有儲存貯體以及您在完成建立追蹤後建立的任何儲存貯體啟用資料事件記錄。它也可以記錄您 AWS 帳戶中任何使用者或角色執行的資料事件活動，即使該活動是在屬於另一個 AWS 帳戶的儲存貯體上執行。
>
> 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。
>
> 如果您要建立多區域線索，請為 Lambda 函數選擇預先定義的範本，以啟用 AWS 目前帳戶中所有函數的資料事件記錄，以及在您完成建立線索後，您可以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線索 （使用 完成 AWS CLI)，此選擇會啟用帳戶中 AWS 目前該區域中所有函數的資料事件記錄，以及在您完成建立線索後，您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。

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. 如果您選取自訂，在進階事件選取器中會根據進階事件選取器欄位的值來建置表達式。

> **Note**
>
> 選取器不支援使用萬用字元，例如 `*` 。若要將多個值與單一條件比對，您可以使用 `StartsWith`、`NotStartsWith`、 `EndsWith`或 `NotEndsWith`來明確比對事件欄位的開頭或結尾。

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任何記錄到 CloudTrail 的資料事件，例如 PutBucket、GetItem 或 GetSnapshotBlock。
- **eventSource** – 要包含或排除的事件來源。此欄位可以使用任何運算子。
- eventType – 要納入或排除的事件類型。例如，您可以將此欄位設定為不等於AwsServiceEvent排除 AWS 服務 事件。如需事件類型的清單，請參閱 eventType中的 CloudTrail 記錄管理、資料和網路活動事件的內容。
- sessionCredentialFromConsole – 包含或排除源自 AWS 管理主控台 工作階段的事件。此欄位可以設定為等於或不等於 的值true。
- userIdentity.arn – 針對特定 IAM 身分執行的動作納入或排除事件。如需更多詳細資訊，請參閱 CloudTrail userIdentity 元素。
- **resources.ARN** - 您可以將任何運算子與 搭配使用resources.ARN，但如果您使用等於或不等於，則值必須完全符合您在範本中指定之類型之有效資源的 ARN，做為 的值resources.type。

  > **Note**
  >
  > 您無法使用 resources.ARN 欄位來篩選沒有 ARNs的資源類型。

  如需資料事件資源 ARN 格式的詳細資訊，請參閱《服務授權參考》中的 的動作、資源和條件索引鍵 AWS 服務。

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，若要從記錄於事件資料存放區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 的運算子設定為 不以 開頭，然後貼入您不想記錄事件的 S3 儲存貯體 ARN。

   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。

   如需有關 CloudTrail 如何評估多個條件的資訊，請參閱 CloudTrail 如何評估欄位的多項條件。

> **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。

11. 若要新增要記錄資料事件的其他資源類型，請選擇新增資料事件類型。重複步驟 3 到此步驟來設定資源類型的進階事件選取器。

12. 在網路活動事件中，選擇編輯以變更網路活動事件記錄設定。根據預設，線索不會記錄網路活動事件。記錄網路活動事件需支付額外費用。如需詳細資訊，請參閱AWS CloudTrail 定價。

    若要記錄網路活動事件，請執行下列動作：

    a. 從網路活動事件來源中，選擇網路活動事件的來源。

    b. 在日誌選取器範本中，選擇範本。您可以選擇記錄所有網路活動事件、記錄所有網路活動存取遭拒的事件，或選擇自訂以建置自訂日誌選取器來篩選多個欄位，例如 eventName和 vpcEndpointId。

    c. （選用）輸入名稱以識別選取器。選擇器名稱在進階事件選擇器中列為名稱，如果您展開 JSON 檢視，則可檢視。

    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。如果您使用預先定義的日誌範本，則可略過此步驟。

       i. 若要排除或包含網路活動事件，您可以在 主控台中選擇下列欄位。

          - **eventName** – 您可以將任何運算子與 搭配使用eventName。您可以使用它來包含或排除任何事件，例如 CreateKey。
          - **errorCode** – 您可以使用它來篩選錯誤碼。目前，唯一支援的errorCode是 VpceAccessDenied。
          - **vpcEndpointId** – 識別操作通過的 VPC 端點。您可以搭配 使用任何運算子vpcEndpointId。

       ii. 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。

iii. 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。

e. 若要新增要記錄網路活動事件的其他事件來源，請選擇新增網路活動事件選取器。

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

13. 在 Insights 事件中，如果您希望追蹤記錄 CloudTrail Insights 事件，請選擇編輯。

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，請參閱使用 CloudTrail Insights。記錄 Insights 事件需支付額外費用。如需 CloudTrail 定價，請參閱 AWS CloudTrail 定價。

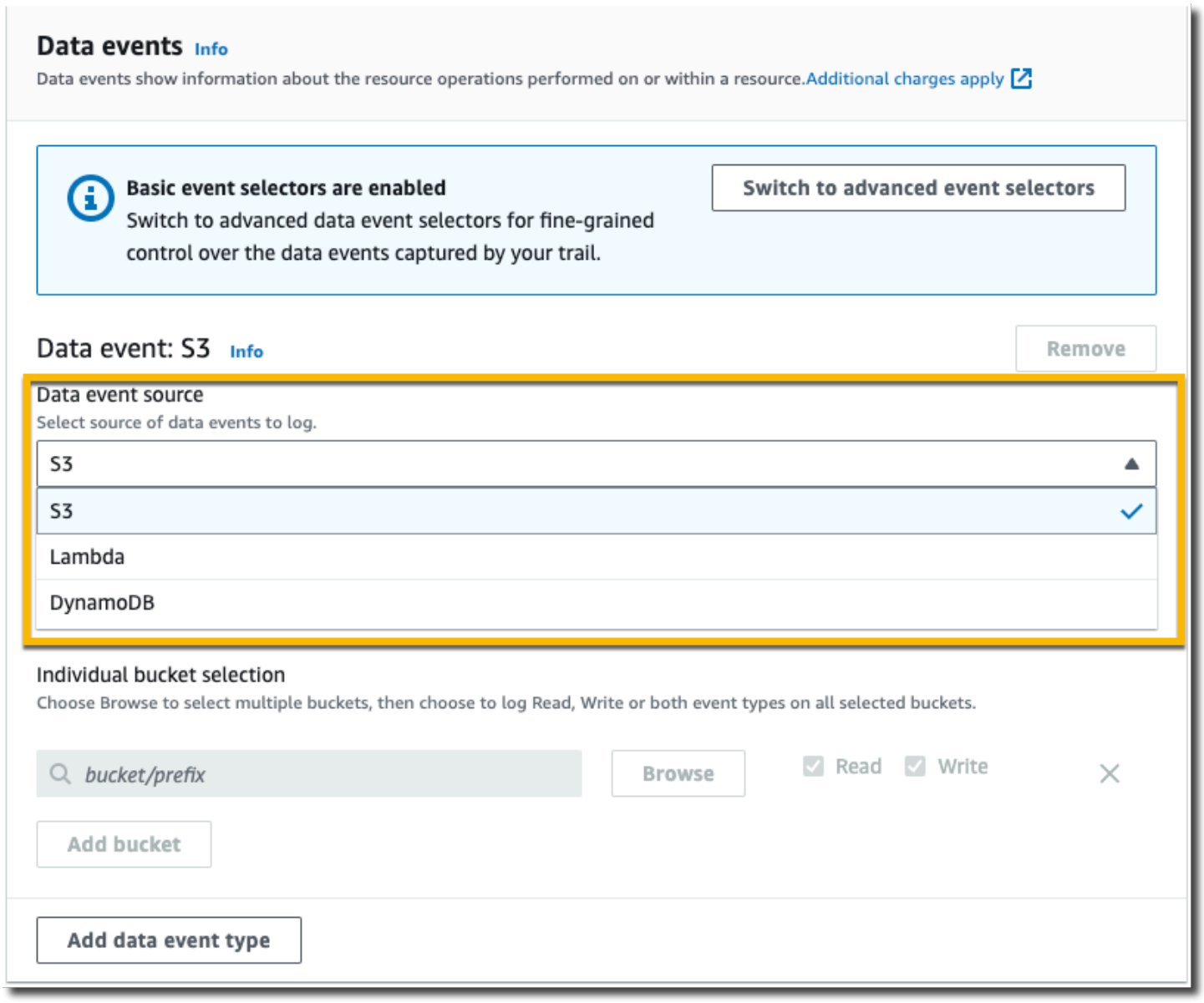
Insights 事件會傳遞到相同 S3 儲存貯體上名為 `/CloudTrail-Insight` 的不同資料夾，此資料夾是在追蹤詳細資訊頁面的 Storage location (儲存位置) 區域中指定的。CloudTrail 會為您建立新的前綴。例如，如果您目前的目的地 S3 儲存貯體名為 `amzn-s3-demo-bucket/AWSLogs/CloudTrail/`，則具有新前綴的 S3 儲存貯體名稱會被命名為 `amzn-s3-demo-bucket/AWSLogs/CloudTrail-Insight/`。

14. 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以及網路活動事件。進階事件選取器可讓您建立精細選取器，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，則僅限於記錄 Amazon S3 儲存貯體、 AWS Lambda 函數和 Amazon DynamoDB 資料表的資料事件。您無法使用基本事件選取器篩選 `eventName` 欄位。您也無法記錄網路活動事件。




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資源類型。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 所有目前和未來的 S3 儲存貯體選項會啟用您 AWS 帳戶中目前所有儲存貯體的資料事件記錄，以及您在完成建立追蹤後建立的任何儲存貯體。它也可以記錄您 AWS 帳戶中任何使用者或角色執行的資料事件活動，即使該活動是在屬於另一個 AWS 帳戶的儲存貯體上執行。
> 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。它不會記錄您 AWS 帳戶中其他區域中 Amazon S3 儲存貯體的資料事件。

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. 若要新增要記錄資料事件的其他資源類型，請選擇新增資料事件類型。

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**
>
> 如果您要建立多區域線索，此選擇會啟用 AWS 目前帳戶中所有函數的資料事件記錄，以及在您完成建立線索後，您可以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線索（使用 完成 AWS CLI)，則此選擇會啟用 AWS 帳戶中目前該區域中所有函數的資料事件記錄，以及在您完成建立線索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於 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，請參閱使用 管理線索 AWS CLI。

4. 若要新增要記錄資料事件的其他資源類型，請選擇新增資料事件類型。
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 使用 CloudTrail 主控台更新線索。

## 使用 CloudTrail 主控台刪除線索

使用 CloudTrail 主控台刪除線索。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。

> **Important**
>
> 雖然刪除 CloudTrail 追蹤是不可復原的動作，但 CloudTrail 不會刪除該追蹤的 Amazon S3 儲存貯體、Amazon S3 儲存貯體本身或追蹤交付事件的 CloudWatch 日誌群組中的日誌檔案。刪除多區域追蹤將停止記錄 中啟用的所有 AWS 區域中的事件 AWS 帳戶。刪除單一區域追蹤只會停止記錄該區域中的事件。它不會停止記錄其他區域中的事件，即使這些其他區域中的線索與已刪除的線索具有相同的名稱。
> 如需關閉和刪除 CloudTrail 追蹤的相關資訊，請參閱 AWS 帳戶 關閉和追蹤。

如果您已在 Amazon Security Lake 中啟用 CloudTrail 管理事件，則需要維護至少一個多區域，會同時記錄 `read` 和 `write` 管理事件的組織追蹤。如果它是您擁有的唯一符合此要求的追蹤，除非在 Security Lake 中關閉 CloudTrail 管理事件，否則您無法刪除該追蹤。

使用 CloudTrail 主控台刪除線索

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
2. 開啟 CloudTrail 主控台的 Trails (線索) 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。已交付至 Amazon S3 儲存貯體的日誌檔案不會刪除並繼續產生 S3 費用。

> **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。 Amazon S3

## 關閉記錄線索

當您建立線索時，會自動開啟記錄。您可以從追蹤的詳細資訊頁面關閉追蹤的記錄。

> **Note**
>
> 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。如需 S3 定價的資訊，請參閱 Amazon S3 定價。

> **停止記錄後的事件交付**
>
> 關閉線索的記錄後，線索仍然可以接收在記錄關閉之前發生的事件。事件可能會因為多種原因而延遲，包括高網路流量、連線問題、服務中斷或現有事件的更新。CloudTrail 會使用最近關閉記錄的時間來判斷是否交付延遲事件，而不是事件發生時追蹤的記錄狀態。因此，上次關閉記錄之前發生的延遲事件仍然可以傳送到追蹤。如需延遲事件交付的詳細資訊，請參閱 中的 addendum 欄位CloudTrail 記錄管理、資料和網路活動事件的內容。
>
> 此外，事件選取器和進階事件選取器不會在記錄關閉後評估傳送到線索的延遲事件。這表示無論追蹤的事件選取器組態為何，追蹤都可以接收在日誌關閉之前發生的任何類型的事件。

使用 CloudTrail 主控台關閉記錄線索

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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. 出現確認提示時，選擇 Stop logging (停止記錄)。CloudTrail 會停止記錄該線索的活動。
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)。

## 使用 建立、更新和管理線索 AWS CLI

您可以使用 AWS CLI 來建立、更新和管理追蹤。使用 時 AWS CLI，請記住您的命令會在為設定檔設定的 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 AWS 命令列工具才能執行本主題中的 AWS Command Line Interface (AWS CLI) 命令。請確定您 AWS CLI 已安裝最新版本的 。如需詳細資訊，請參閱「AWS Command

Line Interface 使用者指南」。如需命令 AWS CLI 列 CloudTrail 命令的說明，請輸入 `aws cloudtrail help`。

## 建立及管理追蹤的常用命令與狀態

CloudTrail 中有一些較常用來建立及更新追蹤的命令，其中包括：

- 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 傳回 AWS 區域中線索的相關資訊。
- 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，您應該建立追蹤記錄所有 AWS 區域中的事件。
- 使用 --is-organization-trail選項建立接收組織中所有 AWS 帳戶日誌的線索。
- 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。選項會指定您已建立的金鑰，以及您已連接允許 CloudTrail 加密日誌的政策的 AWS KMS 金鑰。如需詳細資訊，請參閱使用 啟用和停用 CloudTrail 日誌檔案、摘要檔案和事件資料存放區的加密 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 日誌檔案完整性。
- 指定 CloudWatch Logs 日誌群組和角色，讓 CloudTrail 可以將事件交付到 CloudWatch Logs 群組。如需詳細資訊，請參閱使用 Amazon CloudWatch Logs 監控 CloudTrail 日誌檔案。

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`命令來建立線索

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。

建立多區域追蹤

線索可以套用至在您的 中啟用的所有 AWS 區域 AWS 帳戶，也可以套用至單一區域。套用至 中所有啟用 AWS 區域 的線索 AWS 帳戶 稱為多區域線索。根據最佳實務，我們建議您建立多區域追蹤，因為它會擷取所有啟用區域中的活動。

若要建立多區域追蹤，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，您應該建立追蹤來記錄所有 AWS 區域中的事件。

> **Note**
>
> 當您建立追蹤時，若指定的 Amazon S3 儲存貯體並非透過 CloudTrail 所建立，則需連接適當的政策。請參閱 適用於 CloudTrail 的 Amazon S3 儲存貯體政策。

下列範例會建立名為 *my-trail* 的多區域線索，以及具有名為 *Group* 之索引鍵的標籤，該索引鍵值為 *Marketing*，可將您帳戶中所有已啟用區域的日誌傳送至名為 *amzn-s3-demo-bucket* 的現有儲存貯體。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket --is-multi-region-trail --tags-list [key=Group,value=Marketing]
```

若要確認您的線索是多區域線索，請確認輸出中的 IsMultiRegionTrail元素顯示 true。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-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**
>
> 您在 CloudTrail 主控台中建立追蹤時，即自動開啟記錄日誌。

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，而且已套用適當的 CloudTrail 許可。如需詳細資訊，請參閱適用於 CloudTrail 的 Amazon S3 儲存貯體政策。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket
```

以下為範例輸出。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": false,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

建立已啟用日誌檔案驗證的多區域追蹤

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 日誌檔案完整性。

下列範例會建立多區域追蹤，將日誌傳送到指定的儲存貯體。此命令會採用 --enable-log-file-validation 選項。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-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": "amzn-s3-demo-bucket"
}
```

## 使用 **update-trail**命令更新線索

> **Important**
>
> 截至 2021 年 11 月 22 日， AWS CloudTrail 變更了線索擷取全球服務事件的方式。現在，Amazon CloudFront 建立的事件 AWS Identity and Access Management AWS STS 會記錄在建立它們的區域中，即美國東部（維吉尼亞北部）區域 us-east-1。這使得 CloudTrail 如何處理這些服務與其他 AWS 全球服務一致的服務。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」。
>
> 相反地，CloudTrail 主控台中的事件歷史記錄和 aws cloudtrail lookup-events命令會在事件發生 AWS 區域 的 中顯示這些事件。

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。您只能從建立追蹤的 AWS 區域（其主區域）更新追蹤。使用 時 AWS CLI，請記住，您的命令會在為設定檔設定的 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，則需要維護至少一個多區域，會同時記錄 `read` 和 `write` 管理事件的組織追蹤。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 SDKs 來修改線索，請確定線索的儲存貯體政策是up-to-date。為了讓您的儲存貯體自動接收來自新的事件 AWS 區域，政策必須包含完整的服務名稱 `cloudtrail.amazonaws.com`。如需詳細資訊，請參閱適用於 CloudTrail 的 Amazon S3 儲存貯體政策。

主題

- 將單一區域追蹤轉換為多區域追蹤
- 將多區域追蹤轉換成單一區域追蹤
- 啟用及停用全球服務事件記錄
- 啟用日誌檔案驗證
- 停用日誌檔案驗證

### 將單一區域追蹤轉換為多區域追蹤

若要將現有的單一區域線索變更為多區域線索，請使用 `--is-multi-region-trail`選項。

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

若要確認線索現在是多區域線索，請確認輸出中的 `IsMultiRegionTrail`元素顯示 `true`。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-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": "amzn-s3-demo-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": "amzn-s3-demo-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* 更改為適合您組態的追蹤名稱。

```
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 AWS STS 事件：

```
aws cloudtrail --region us-east-1 create-trail --include-global-service-events --
name myTrail --s3-bucket-name amzn-s3-demo-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": "amzn-s3-demo-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": "amzn-s3-demo-bucket"
}
```

若要使用 驗證日誌檔案 AWS CLI，請參閱 使用 驗證 CloudTrail 日誌檔案完整性 AWS CLI。

## 使用 管理線索 AWS CLI

AWS CLI 包含數個其他命令，可協助您管理線索。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。您必須從建立追蹤的相同 AWS 區域 （其主區域） 執行這些命令。使用 時 AWS CLI，請記住您的命令會在為設定檔設定的 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 Insights 事件選取器
- 設定進階事件選取器
- 設定基本事件選取器
- 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 describe-trails命令來擷取 AWS 區域中線索的相關資訊。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": "amzn-s3-demo-bucket1",
      "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": "amzn-s3-demo-bucket2",
      "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": "amzn-s3-demo-bucket3",
      "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": "amzn-s3-demo-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。您必須從建立該命令的區域（主區域）執行此命令 AWS ，或者您必須新增 --region 參數來指定該區域。

> **Note**
>
> 如果線索是組織線索，而且您是組織中的成員帳戶 AWS Organizations，您必須提供該線索的完整 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 CloudTrail 無法將日誌檔案交付到儲存貯體時由 Amazon S3 發出的錯誤。

### 設定 CloudTrail Insights 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。您必須從建立線索 AWS 的區域（主區域）執行此命令，或者您必須將 --region 參數新增至命令來指定該區域。

> **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

下列範例使用 put-insight-selectors，為名為 *TrailName3* 的追蹤建立 Insights 事件選取器。這會啟用 *TrailName3* 追蹤的 Insights 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

下列範例使用 put-insight-selectors，為名為 *TrailName3* 的追蹤移除 Insights 事件選取器。清除 Insights 選取器的 JSON 字串會停用 *TrailName3* 追蹤的 Insights 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"
}
```

設定進階事件選取器

您可以使用進階事件選取器來記錄管理事件、所有資源類型的資料事件，以及網路活動事件。相反地，您可以使用基本事件選取器來記錄 AWS::DynamoDB::Table、 和資源AWS::S3::Object類型的管理事件AWS::Lambda::Function和資料事件。您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使用基本事件選取器的線索，則會覆寫基本事件選取器。

若要將線索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，然後設定進階事件選取器以符合先前事件選取器的範圍，然後新增任何其他選取器。

您必須從建立追蹤 AWS 區域 的 （ 主區域 ） 執行 get-event-selectors命令，或者您必須新增 --region 參數來指定該區域。

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> 如果線索是組織線索，而且您使用組織中的成員帳戶登入 AWS Organizations，您必須提供線索的完整 ARN，而不只是名稱。

下列範例顯示使用進階事件選取器記錄管理事件之線索的設定。根據預設，線索會設定為記錄所有管理事件，而不會記錄資料事件或網路活動事件。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/management-events-
trail",
    "AdvancedEventSelectors": [
        {
            "Name": "Management events selector",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
```

```
            ]

        }
    ]
}
```

若要建立進階事件選取器，請執行 put-event-selectors 命令。當您的帳戶發生事件時，CloudTrail 會評估您的追蹤組態。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及記錄網路活動事件。

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記錄 Amazon S3 AWS Outposts 資料事件的範例追蹤
- 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 Data API 管理事件的範例追蹤

使用特定進階事件選取器的範例追蹤

下列範例會為名為 *TrailName* 的線索建立自訂進階事件選取器，以包含讀取和寫入管理事件（省略選取readOnly器）PutObject，以及所有 Amazon S3 儲存貯體/字首組合DeleteObject的資料事件，除了名為 的儲存貯體amzn-s3-demo-bucket、名為 之 AWS Lambda 函數的資料事件MyLambdaFunction，以及透過 VPC 端點 AWS KMS 存取遭拒事件的網路活動事件。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:::amzn-s3-demo-
bucket/"] }
    ]
  },
  {
    "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"] }
    ]
  },
  {
     "Name": "Audit AccessDenied AWS KMS events over a VPC endpoint",
     "FieldSelectors": [
       { "Field": "eventCategory", "Equals": ["NetworkActivity"]},
       { "Field": "eventSource", "Equals": ["kms.amazonaws.com"]},
       { "Field": "errorCode", "Equals": ["VpceAccessDenied"]}
     ]
  }
]'
```

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:::amzn-s3-demo-bucket/" ]
        },
      ]
    },
    {
      "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-2:123456789012:function/
MyLambdaFunction" ]
        }
      ]
    },
    {
       "Name": "Audit AccessDenied AWS KMS events over a VPC endpoint",
       "FieldSelectors": [
         {
           "Field": "eventCategory",
           "Equals": ["NetworkActivity"]
         },
         {
           "Field": "eventSource",
           "Equals": ["kms.amazonaws.com"]
         },
```

```
          {
            "Field": "errorCode",
            "Equals": ["VpceAccessDenied"]
          }
        ]
      }
  ],
  "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/TrailName"
}
```

使用自訂進階事件選取器記錄 Amazon S3 AWS Outposts 資料事件的範例追蹤

下列範例顯示如何設定您的線索，以將所有 Amazon S3 AWS Outposts 物件上的所有資料事件包含在前哨站中。在此版本中， `resources.type` 欄位的 S3 on AWS Outposts 事件支援的值為 `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

下列範例會為名為 *TrailName* 的線索建立進階事件選取器，以包含唯讀和唯寫管理事件 （省略`readOnly`選取器），但會排除 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，因此如果您有多個擷取管理事件的線索，它們可能會對 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 事件記錄到線索，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 Data API 管理事件的範例追蹤

下列範例會為名為 *TrailName* 的線索建立進階事件選取器，以包含唯讀和唯寫管理事件（省略選取readOnly器），但會排除 Amazon RDS Data API 管理事件。若要排除 Amazon RDS Data API 管理事件，請在 eventSource 欄位的字串值中指定 Amazon RDS Data 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 Data API 管理事件，而且您無法變更 Amazon RDS Data API 事件記錄設定。

若要再次開始將 Amazon RDS Data API 管理事件記錄到線索，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"] }
    ]
  }
]'
```

設定基本事件選取器

您只能使用基本事件選取器來記錄 AWS::DynamoDB::Table、 和資源AWS::S3::Object類型的管理事件AWS::Lambda::Function和資料事件。您可以使用進階事件選取器來記錄管理事件、所有資料資源類型和網路活動事件。

您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。如果您將基本事件選取器套用至使用進階事件選取器的線索，則會覆寫進階事件選取器。

若要檢視追蹤的事件選取器設定，請執行 get-event-selectors 命令。您必須從建立命令 AWS 區域 的 （主區域） 執行此命令，或使用 --region 參數指定該區域。

```
aws cloudtrail get-event-selectors --trail-name TrailName
```

> **Note**
>
> 如果線索是組織線索，而且您是組織中的成員帳戶 AWS Organizations，您必須提供該線索的完整 ARN，而不只是名稱。

下列範例顯示使用基本事件選取器記錄管理事件的線索設定。

```
{
    "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 使用 CloudTrail Insights。

當您的帳戶發生事件時，CloudTrail 會評估您的追蹤組態。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
- 記錄相關少量 AWS Key Management Service 事件的範例追蹤
- 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 *TrailName* 的線索建立事件選取器，以包含唯讀和唯讀管理事件、兩個 Amazon S3 儲存貯體/字首組合的資料事件，以及名為 *hello-world-python-function* 的單一 AWS Lambda 函數的資料事件。

```
aws cloudtrail put-event-selectors --trail-name TrailName --event-selectors
 '[{"ReadWriteType": "All","IncludeManagementEvents": true,"DataResources":
 [{"Type":"AWS::S3::Object", "Values": ["arn:aws:s3:::amzn-s3-
demo-bucket/prefix","arn:aws:s3:::amzn-s3-demo-bucket2/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:::amzn-s3-demo-bucket/prefix",
                        "arn:aws:s3:::amzn-s3-demo-bucket2/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* 的線索建立事件選取器，其中包含所有管理事件，包括唯讀和唯寫管理事件，以及 中所有 Amazon S3 儲存貯體、 AWS Lambda 函數和 Amazon DynamoDB 資料表的資料事件 AWS 帳戶。由於此範例使用基本事件選取器，因此無法設定 S3 事件的日誌記錄 AWS Outposts、Ethereum 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。您也無法使用基本事件選取器記錄網路活動事件。您必須使用進階事件選取器來記錄所有其他資源類型的網路活動事件和資料事件。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

下列範例會為名為 *TrailName* 的線索建立事件選取器，以包含唯讀和唯寫管理事件，但會排除 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，因此如果您有多個擷取管理事件的線索，它們可能會對 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。

若要再次開始將 AWS KMS 事件記錄到線索，請傳遞空陣列做為 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"
}
```

若要再次開始將 AWS KMS 事件記錄到線索，請傳遞空陣列做為 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]}]'
```

記錄相關少量 AWS Key Management Service 事件的範例追蹤

下列範例會為名為 *TrailName* 的線索建立事件選取器，以包含唯寫管理事件和 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，因此如果您有多個擷取管理事件的線索，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，其中包含 `Disable`、 `Delete`和 `ScheduleKey`，但不再包含大量動作，例如 `Encrypt`、 `Decrypt`和 `GenerateDataKey`（這些現在視為讀取事件）。

```
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 *TrailName* 的追蹤建立事件選取器，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，而且可能會有大量的事件，因此如果您有多個追蹤用來擷取管理事件，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。

若要再次開始將 Amazon RDS Data API 管理事件記錄到線索，請傳遞空陣列做為 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"
}
```

若要再次開始將 Amazon RDS Data API 管理事件記錄到線索，請傳遞空陣列做為 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]}]'
```

停止及啟動追蹤的記錄功能

下列命令可用來啟動及停止 CloudTrail 記錄功能。

```
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。如果您未停止記錄日誌，CloudTrail 會嘗試在有限期間內將日誌檔案交付到具有相同名稱的儲存貯體。
> 如果您停止記錄或刪除追蹤，該追蹤會停用 CloudTrail Insights。

> **停止記錄後的事件交付**
>
> 停止記錄追蹤之後，追蹤仍然可以接收停止記錄之前發生的事件。事件可能會因為多種原因而延遲，包括高網路流量、連線問題、服務中斷或現有事件的更新。CloudTrail 會使用最近停止記錄的時間來判斷是否交付延遲事件，而不是事件發生時追蹤的記錄狀態。因此，上次停止記錄之前發生的延遲事件仍然可以傳送到追蹤。如需延遲事件交付的詳細資訊，請參閱 中的 addendum 欄位CloudTrail 記錄管理、資料和網路活動事件的內容。
> 此外，事件選取器和進階事件選取器不會在停止記錄後評估傳送到追蹤的延遲事件。這表示追蹤可以接收停止記錄之前發生的任何類型的事件，無論追蹤的事件選取器組態為何。

刪除追蹤

如果您已在 Amazon Security Lake 中啟用 CloudTrail 管理事件，則需要維護至少一個多區域，會同時記錄 `read` 和 `write` 管理事件的組織追蹤。如果它是您擁有的唯一符合此要求的追蹤，除非在 Security Lake 中關閉 CloudTrail 管理事件，否則您無法刪除該追蹤。

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。

> **Important**
>
> 雖然刪除 CloudTrail 追蹤是不可復原的動作，但 CloudTrail 不會刪除該追蹤的 Amazon S3 儲存貯體、Amazon S3 儲存貯體本身或追蹤交付事件的 CloudWatch 日誌群組中的日誌檔案。刪除多區域追蹤將停止記錄 中啟用的所有 AWS 區域中的事件 AWS 帳戶。刪除單一區域追蹤只會停止記錄該區域中的事件。它不會停止記錄其他區域中的事件，即使這些其他區域中的線索與已刪除的線索具有相同的名稱。
> 如需有關關閉和刪除 CloudTrail 追蹤的資訊，請參閱 AWS 帳戶 關閉和追蹤。

```
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 CLI AWS 管理主控台、 或服務 API 分別刪除這些資源。

## 建立多個線索

您可以使用 CloudTrail 日誌檔案為您 AWS 帳戶中的操作或安全問題進行故障診斷。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。

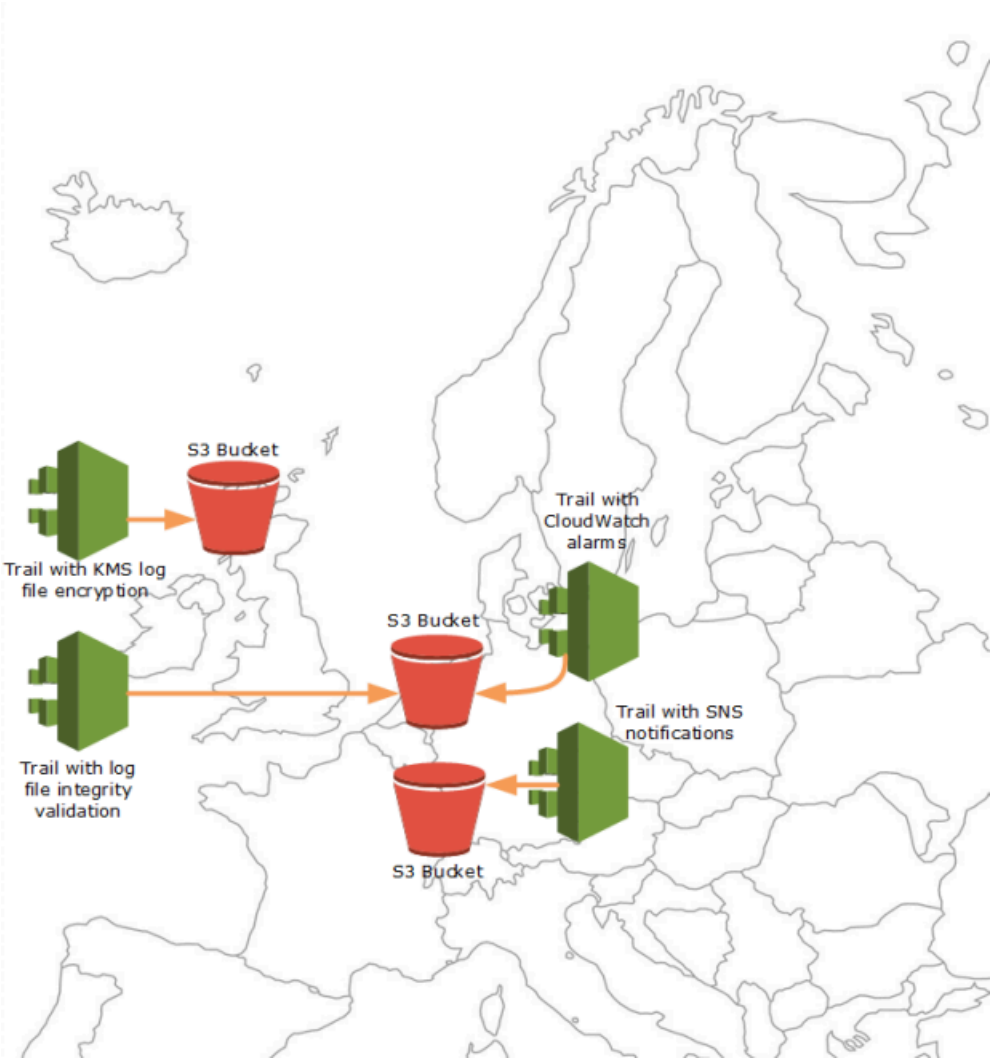
> **Note**
>
> AWS 區域 帳戶每個 中管理事件的第一個副本是免費的。如果您建立更多將相同的事件傳遞至其他目的地的追蹤，這些後續交付會產生 CloudTrail 費用。如需 CloudTrail 成本的詳細資訊，請參閱 AWS CloudTrail 定價和 管理 CloudTrail 追蹤成本。

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 稽核員在歐洲 (愛爾蘭) 區域中建立追蹤，並設定日誌檔案完整性驗證，以確保日誌檔案自 CloudTrail 交付後未經變更。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 最多可以建立五個線索 AWS 區域。多區域追蹤計為每個區域一個追蹤。

您可以使用資源層級許可管理使用者在 CloudTrail 上執行特定操作的能力。

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」。

如需多個線索的詳細資訊，請參閱 CloudTrail FAQs。

## 建立組織追蹤

如果您已在 中建立組織 AWS Organizations，您可以建立追蹤記錄 AWS 帳戶 該組織中所有 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 委派的管理員。

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 的詳細資訊 AWS Organizations，請參閱組織術語和概念。

> **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。您還必須擁有足夠的許可，才能讓管理或委派管理員帳戶中的使用者或角色建立線索。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線索都是多區域組織線索，可從組織中每個成員帳戶中啟用 AWS 區域 的記錄事件。若要在組織的所有 AWS 分割區中記錄事件，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線索 AWS CLI。如果您建立單一區域追蹤，則只會在追蹤的 AWS 區域 （ 也稱為主區域 ） 中記錄活動。

雖然您的 預設 AWS 區域 會啟用大多數 AWS 帳戶，但您必須手動啟用特定區域 （ 也稱為選擇加入區域)。如需預設啟用哪些區域的資訊，請參閱《 AWS 帳戶管理 參考指南》中的啟用和停用區域的考量事項。如需 CloudTrail 支援的 區域清單，請參閱 CloudTrail 支援的區域。

當您建立組織線索時，會在屬於您組織的成員帳戶中建立具有您指定名稱的線索副本。

- 如果組織線索適用於單一區域，且線索的主區域不是選擇加入區域，則會在每個成員帳戶中的組織線索的主區域中建立線索副本。
- 如果組織線索適用於單一區域，且線索的主區域是選擇加入區域，則會在已啟用該區域的成員帳戶中的組織線索的主區域中建立線索副本。

- 如果組織線索是多區域，且線索的主區域不是選擇加入區域，則會在每個成員帳戶中啟用的每個 AWS 區域 中建立線索的副本。當成員帳戶啟用選擇加入區域時，會在該區域啟用完成後，在成員帳戶的新選擇區域中建立多區域追蹤的複本。
- 如果組織線索是多區域，而主要區域是選擇加入區域，成員帳戶將不會將活動傳送至組織線索，除非他們選擇加入建立多區域線索 AWS 區域 的 。例如，如果您建立多區域追蹤並選擇歐洲 （西班牙） 區域作為追蹤的主要區域，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活動傳送至組織追蹤。

> **Note**
>
> 即使資源驗證失敗，CloudTrail 仍會在成員帳戶中建立組織追蹤。驗證失敗的範例包括：
>
> - 不正確的 Amazon S3 儲存貯體政策
> - 不正確的 Amazon SNS 主題政策
> - 無法交付至 CloudWatch Logs 日誌群組
> - 使用 KMS 金鑰加密的許可不足
>
> 具有 CloudTrail 許可的成員帳戶可以透過在 CloudTrail 主控台上檢視追蹤的詳細資訊頁面，或執行 AWS CLI get-trail-status命令，來查看組織追蹤的任何驗證失敗。

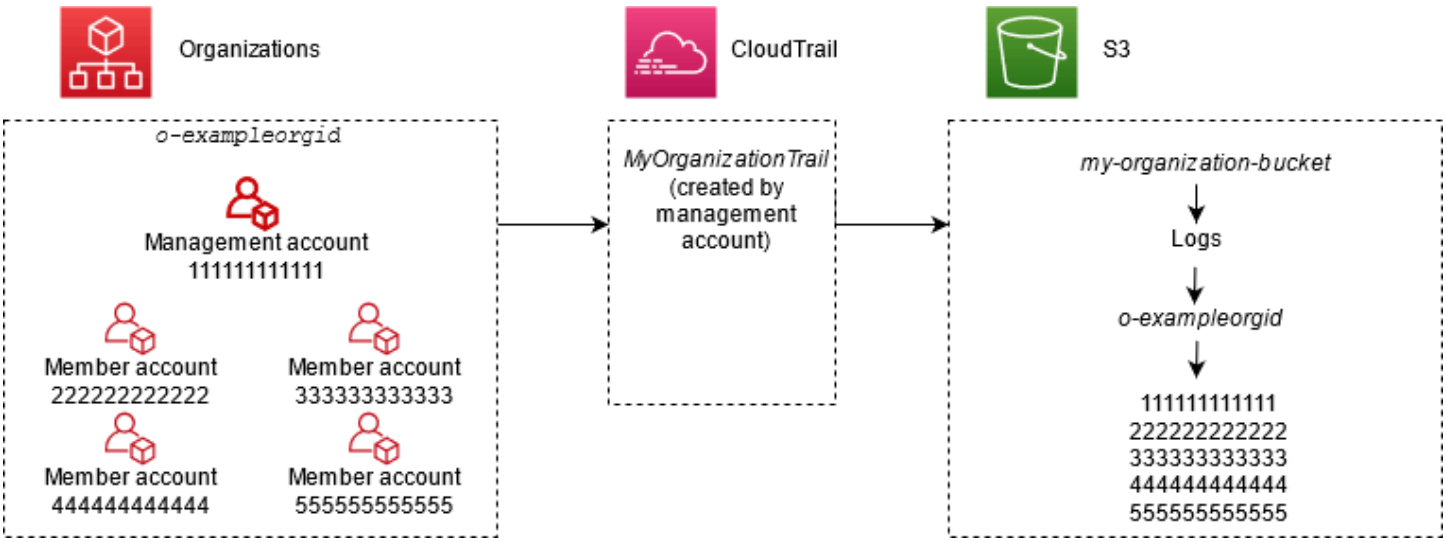
在成員帳戶中具有 CloudTrail 許可的使用者，可以在從他們的 登入 CloudTrail 主控台， AWS 帳戶或執行 等 AWS CLI 命令時查看組織線索`describe-trails`。不過，成員帳戶中的使用者沒有足夠的許可來刪除組織線索、開啟或關閉記錄、變更記錄的事件類型，或以任何方式變更組織線索。

當您在主控台中建立組織追蹤時，CloudTrail 會建立服務連結角色，以在組織的成員帳戶中執行記錄任務。此角色已命名為 AWSServiceRoleForCloudTrail，而且是 CloudTrail 記錄組織事件的必要角色。如果 AWS 帳戶 將 新增至組織，則會將組織追蹤和服務連結角色新增至該角色 AWS 帳戶，並在組織追蹤中自動開始該帳戶的記錄。如果從組織中移除 AWS 帳戶 ，則會從 AWS 帳戶 不再屬於組織的 中刪除組織追蹤和服務連結角色。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組織追蹤，但隨後做為組織的管理帳戶移除，則使用其帳戶建立的任何組織追蹤都會變成非組織追蹤。

在下列範例中，組織的管理帳戶 111111111111 會為組織 *o-exampleorgid* 建立名為 *MyOrganizationTrail* 的追蹤。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在其追蹤清單中查看 *MyOrganizationTrail*，但是成員帳戶無法移除或修改該組織追蹤。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，根據預設，只有管理帳戶可以存取追蹤的 Amazon S3 儲存貯體，以及其中包含的日誌。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 444444444444 從組織中移除，*MyOrganizationTrail* 和服務連結角色不會再出現在 AWS 帳戶 444444444444 中，而且組織追蹤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線索，並選擇是否建立多區域或單一區域組織線索，以及您想要登入組織線索的事件類型，就像任何其他線索一樣。不過，還是有一些差異。例如，當在主控台內建立線索並選擇是否要記錄 Amazon S3 儲存貯體或 AWS Lambda 函數的資料事件時，CloudTrail 主控台中只會列出管理帳戶的資源，但您可以選擇新增成員帳戶中資源的 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，請參閱 記錄管理事件、 記錄資料事件和 使用 CloudTrail Insights。

> **Note**
>
> 在 主控台中，您可以建立多區域追蹤。建議最佳實務是在 中所有啟用的區域中記錄活動 AWS 帳戶，因為它可協助您更安全地保護 AWS 環境。若要建立單一區域追蹤，請使用 AWS CLI。

當您在 中檢視組織事件歷史記錄中的事件時 AWS Organizations，您只能檢視您登入 AWS 帳戶 的 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，以進一步分析和處理 CloudTrail 日誌中針對組織線索所收集的事件資料，就像針對任何其他線索一樣。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 服務與 CloudTrail 日誌的整合。

主題


- 從成員帳戶追蹤移至組織追蹤
- 準備建立組織追蹤
- 使用主控台建立組織追蹤
- 使用 為組織建立線索 AWS CLI
- 對組織線索的問題進行故障診斷


## 從成員帳戶追蹤移至組織追蹤

如果您已經為個別成員帳戶設定了 CloudTrail 追蹤，但是想要移動到組織追蹤，以記錄所有帳戶中的事件，您不希望在建立組織追蹤之前，由於刪除個別成員帳戶追蹤而遺失事件。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。這個角色是您在建立組織時由 Organizations 所自動建立，而且是 CloudTrail 用來記錄組織事件的必要角色。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，
您的政策也需要包含 `s3:PutEncryptionConfiguration`
動作，因為預設會為儲存貯體啟用伺服器端加密。下列範例政策顯示最少的必要許可。

> **Note**
>
> 您不應該在 之間廣泛共用AWSCloudTrail_FullAccess政策 AWS 帳戶。由於 CloudTrail 會收集高度敏感的資訊，您應限制僅 AWS 帳戶 管理員才能使用這類政策。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。

JSON

```
{
    "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 APIs 建立組織線索，您必須在 Organizations 中啟用 CloudTrail 的受信任存取，而且您必須手動建立 Amazon S3 儲存貯體，其政策允許記錄組織線索。如需詳細資訊，請參閱使用 為組織建立線索 AWS CLI。

- 若要使用現有的 IAM 角色，在 Amazon CloudWatch Logs 中新增組織追蹤的監控，IAM 角色必須透過手動修改，允許將成員帳戶的 CloudWatch Logs 傳遞到管理帳戶的 CloudWatch Logs 群組，如下列範例所示。

> **Note**
>
> 您必須使用存在於您自己帳戶中的 IAM 角色和 CloudWatch Logs 日誌群組。您無法使用不同帳戶所擁有的 IAM 角色和 CloudWatch Logs 日誌群組。

JSON

```
{
    "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 使用 Amazon CloudWatch Logs 監控 CloudTrail 日誌檔案 中進一步了解 CloudTrail 和 Amazon CloudWatch Logs。此外，請先考慮 CloudWatch Logs 限制和定價考量等因素，再決定啟用組織追蹤的功能。如需詳細資訊，請參閱 CloudWatch Logs 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。

您也應該先考慮管理帳戶與成員帳戶中已存在多少個線索，再建立組織線索。CloudTrail 會限制每個區域內能夠建立的追蹤數目。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 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：

- 適用於 CloudTrail 的 Amazon S3 儲存貯體政策

- 設定 CloudTrail 的 AWS KMS 金鑰政策
- 適用於 CloudTrail 索的 Amazon SNS 主題政策

## 使用主控台建立組織追蹤

若要從 CloudTrail 主控台建立組織追蹤，您必須使用管理或委派的管理員帳戶中的使用者或角色，以足夠的許可登入主控台。如果您不是使用管理或委派的管理員帳戶登入，則當您從 CloudTrail 主控台建立或編輯追蹤時，將不會看到將追蹤套用到組織的選項。

使用 建立組織追蹤 AWS 管理主控台

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。

   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 CloudTrail 資源、S3 儲存貯體和 KMS 金鑰的命名需求。
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。當您建立儲存貯體時，CloudTrail 會建立和套用所需的儲存貯體政策。

   > **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儲存貯體，但儲存貯體政策必須授予 CloudTrail 寫入的許可。如需手動編輯儲存貯體政策的資訊，請參閱「適用於 CloudTrail 的 Amazon S3 儲存貯體政策」。

   若要更容易地找到您的記錄，請在現有的儲存貯體中建立新的資料夾 (也稱為prefix ) 來存儲您的 CloudTrail 日誌。在字首中輸入字首。

6. 對於日誌檔案 SSE-KMS 加密，如果您想要使用 SSE-KMS 加密而非 SSE-S3 加密來加密日誌檔案和摘要檔案，請選擇已啟用。預設為啟用。如果您未啟用 SSE-KMS 加密，您的日誌檔案和摘要檔案會使用 SSE-S3 加密進行加密。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，指定別名，格式為 `alias/MyAliasName`。如需詳細資訊，請參閱 更新資源以搭配 主控台使用您的 KMS 金鑰。

   > **Note**
   >
   > 您也可以輸入來自另一個帳戶的金鑰 ARN。如需詳細資訊，請參閱更新資源以搭配 主控台使用您的 KMS 金鑰。金鑰政策必須允許 CloudTrail 使用金鑰來加密您的日誌檔案和摘要檔案，並允許您指定的使用者以未加密的形式讀取日誌檔案或摘要檔案。如需手動編輯金鑰政策的資訊，請參閱「設定 CloudTrail 的 AWS KMS 金鑰政策」。

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。您可以使用摘要檔案來驗證您的日誌檔案在 CloudTrail 交付以後未變更。如需詳細資訊，請參閱 驗證 CloudTrail 日誌檔案完整性。

   b. 針對 SNS notification delivery (SNS 通知傳送)，若要在每次日誌交付至您的儲存貯體時收到通知，請選擇 Enabled (啟用)。CloudTrail 會在日誌檔案存放多個事件。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 CloudTrail 的 Amazon SNS 通知。

      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。如果您要建立多區域追蹤，所有區域的日誌檔案交付 SNS 通知會傳送到您建立的單一 SNS 主題。

      如果選擇 New (新的)，CloudTrail 會為您指定新主題的名稱，或者您可以輸入名稱。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 適用於 CloudTrail 索的 Amazon SNS 主題政策。

      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. 選擇性地設定 CloudTrail 以將日誌檔案傳送至 CloudWatch Logs，方法是選擇CloudWatch Logs 中的 Enabled (啟用)。如需詳細資訊，請參閱傳送事件到 CloudWatch Logs。

> **Note**
>
> 只有管理帳戶可以為使用主控台的組織追蹤設定 CloudWatch Logs 日誌群組。委派管理員可以使用 AWS CLI 或 CloudTrail 或 API 操作來設定 CloudWatch Logs 日誌群組。CloudTrail `CreateTrail` `UpdateTrail`

   a. 如果您啟用與 CloudWatch Logs 整合功能，請選擇 New (新的) 建立新日誌群組，或 Existing (現有) 以使用現有的群組。如果選擇 New (新的)，CloudTrail 會為您指定新日誌群組的名稱，或者您可以輸入名稱。

   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 New (新的) 為將日誌傳送至 CloudWatch Logs 的許可建立新的 IAM 角色。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 讓 CloudTrail 能使用 CloudWatch Logs 進行監控的角色政策文件。

> **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，如果您要 CloudTrail 將事件交付至 CloudWatch Logs 日誌群組，則必須選擇存在於目前帳戶中的日誌群組。

9. 對於標籤，您最多可以新增 50 個標籤金鑰對，以協助您識別、排序和控制對線索的存取。標籤可協助您辨識 CloudTrail 追蹤和包含 CloudTrail 日誌檔案的 Amazon S3 儲存貯體。然後，您可以對 CloudTrail 資源使用資源群組。如需詳細資訊，請參閱AWS Resource Groups及Tags (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 KMS) 事件篩選 AWS Key Management Service 出您的線索。預設設定是包含所有 AWS KMS 事件。

只有在您的線索上記錄管理 AWS KMS 事件時，才提供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 `Encrypt`、 `Decrypt`和 等動作`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。少量的相關 AWS KMS 動作，例如 `Disable`、 `Delete`和 `ScheduleKey` （通常佔 AWS KMS 事件量的 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源類型，並對線索擷取的資料事件提供精細的控制。如果您打算記錄網路活動事件，則必須使用進階事件選取器。如果您使用基本事件選取器，請完成 中的步驟使用基本事件選取器執行資料事件設定，然後返回此程序的步驟 17。

針對資源類型，選擇您要記錄資料事件的資源類型。如需可用資源類型的詳細資訊，請參閱 資料事件。

13. 選擇日誌選取器範本。您可以選擇預先定義的範本，或選擇自訂來定義您自己的事件集合條件。

您可以從下列預先定義的範本中選擇：

- 記錄所有事件：選擇此範本記錄所有事件。
- 僅記錄讀取事件 – 選擇此範本以僅記錄讀取事件。唯讀事件是不會變更資源狀態的事件，例如 `Get*`或 `Describe*`事件。
- 僅記錄寫入事件 – 選擇此範本僅記錄寫入事件。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。

- 僅記錄 AWS 管理主控台 事件 – 選擇此範本僅記錄源自 的事件 AWS 管理主控台。
- 排除 AWS 服務 啟動的事件 – 選擇此範本以排除具有 `eventType`之 AWS 服務 的事件`AwsServiceEvent`，以及使用連結角色 (SLRs) AWS 服務啟動的事件。

> **Note**
>
> 選擇 S3 儲存貯體的預先定義範本，可讓您 AWS 帳戶中目前所有儲存貯體的資料事件記錄，以及您在完成建立追蹤後建立的任何儲存貯體。它也可以記錄您 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 帳戶的儲存貯體上執行。
>
> 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。
>
> 如果您要建立多區域線索，請為 Lambda 函數選擇預先定義的範本，以啟用 AWS 目前帳戶中所有函數的資料事件記錄，以及在您完成建立線索後，您可以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線索 （ 使用 完成 AWS CLI)，則此選擇會啟用帳戶中 AWS 目前該區域中所有函數的資料事件記錄，以及在您完成建立線索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. 如果您選取自訂，在進階事件選取器中，會根據進階事件選取器欄位的值來建置表達式。

> **Note**
>
> 選取器不支援使用萬用字元，例如 `*` 。若要以單一條件比對多個值，您可以使用 `StartsWith`、`NotStartsWith`、 `EndsWith`或 `NotEndsWith`來明確比對事件欄位的開頭或結尾。

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任何記錄到 CloudTrail 的資料事件，例如 PutBucket、GetItem 或 GetSnapshotBlock。
- **eventSource** – 要包含或排除的事件來源。此欄位可以使用任何運算子。
- eventType – 要納入或排除的事件類型。例如，您可以將此欄位設定為不等於AwsServiceEvent排除 AWS 服務 事件。如需事件類型的清單，請參閱 eventType中的 CloudTrail 記錄管理、資料和網路活動事件的內容。
- sessionCredentialFromConsole – 包含或排除源自 AWS 管理主控台 工作階段的事件。此欄位可以設定為等於或不等於 的值true。
- userIdentity.arn – 針對特定 IAM 身分執行的動作納入或排除事件。如需更多詳細資訊，請參閱 CloudTrail userIdentity 元素。
- **resources.ARN** - 您可以將任何運算子與 搭配使用resources.ARN，但如果您使用等於或不等於，則值必須完全符合您在範本中指定之類型之有效資源的 ARN，做為 的值resources.type。

  > **Note**
  >
  > 您無法使用 resources.ARN 欄位來篩選沒有 ARNs的資源類型。

  如需資料事件資源 ARN 格式的詳細資訊，請參閱《服務授權參考》中的 的動作、資源和條件索引鍵 AWS 服務。

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，若要從記錄於事件資料存放區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，設定 的運算子不會以 開頭，然後貼入您不想記錄事件的 S3 儲存貯體 ARN。

   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。

   如需有關 CloudTrail 如何評估多個條件的資訊，請參閱 CloudTrail 如何評估欄位的多項條件。

> **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。

16. 若要新增要記錄資料事件的資源類型，請選擇新增資料事件類型。重複步驟 12 到此步驟，為資源類型設定進階事件選取器。

17. 若要記錄網路活動事件，請選擇網路活動事件。網路活動事件可讓 VPC 端點擁有者記錄使用其 VPC 端點從私有 VPC 到 的 AWS API 呼叫 AWS 服務。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。

    若要記錄網路活動事件，請執行下列動作：

    a. 從網路活動事件來源中，選擇網路活動事件的來源。

    b. 在日誌選取器範本中，選擇範本。您可以選擇記錄所有網路活動事件、記錄所有網路活動存取遭拒的事件，或選擇自訂以建置自訂日誌選取器來篩選多個欄位，例如 eventName和 vpcEndpointId。

    c. （選用）輸入名稱以識別選取器。選擇器名稱在進階事件選擇器中列為名稱，如果您展開 JSON 檢視，則可檢視。

    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。如果您使用預先定義的日誌範本，則可略過此步驟。

        i. 對於排除或包含網路活動事件，您可以在 主控台中選擇下列欄位。

        - **eventName** – 您可以將任何運算子與 搭配使用eventName。您可以使用它來包含或排除任何事件，例如 CreateKey。
        - **errorCode** – 您可以使用它來篩選錯誤碼。目前，唯一支援的errorCode是 VpceAccessDenied。
        - **vpcEndpointId** – 識別操作通過的 VPC 端點。您可以搭配 使用任何運算子vpcEndpointId。

        ii. 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。

iii. 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。

e. 若要新增要記錄網路活動事件的其他事件來源，請選擇新增網路活動事件選取器。

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

18. 如果您想要追蹤記錄 CloudTrail Insights 事件，請選擇 Insights 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，請參閱使用 CloudTrail Insights。記錄 Insights 事件需支付額外費用。如需 CloudTrail 定價，請參閱 AWS CloudTrail 定價。

Insights 事件會傳遞到相同 S3 儲存貯體上名為 `/CloudTrail-Insight` 的不同資料夾，此資料夾是在追蹤詳細資訊頁面的 Storage location (儲存位置) 區域中指定的。CloudTrail 會為您建立新的前綴。例如，如果您目前的目的地 S3 儲存貯體名為 `amzn-s3-demo-destination-bucket/AWSLogs/CloudTrail/`，則具有新前綴的 S3 儲存貯體名稱會被命名為 `amzn-s3-demo-destination-bucket/AWSLogs/CloudTrail-Insight/`。

19. 當您完成選擇要記錄的事件類型時，請選擇 Next (下一頁)。

20. 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)。

21. 新的追蹤會出現在 Trails (追蹤) 頁面上。在所有成員帳戶中啟用的所有區域中建立組織追蹤最多可能需要 24 小時。Trails (追蹤) 頁面會顯示您帳戶中所有區域內的追蹤。約 5 分鐘後，CloudTrail 會發佈日誌檔案，其中顯示您組織中曾進行的 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，請參閱使用 CloudTrail 主控台更新線索。
- 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 日誌檔案。
- 設定 CloudTrail 將日誌檔案傳送至 CloudWatch Logs 如需詳細資訊，請參閱 準備建立組織追蹤 中的 傳送事件到 CloudWatch Logs 和 CloudWatch Logs 項目。

> **Note**
>
> 只有管理帳戶可以為組織追蹤設定 CloudWatch Logs 日誌群組。

- 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》中的在 CloudTrail 主控台中建立 CloudTrail 日誌的資料表。
- 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，如果您要 CloudTrail 將事件交付至 CloudWatch Logs 日誌群組，則必須選擇存在於目前帳戶中的日誌群組。

## 使用 為組織建立線索 AWS CLI

您可以使用 AWS CLI來建立組織追蹤。 AWS CLI 會使用其他功能和命令定期更新 。為了確保成功，請務必先安裝或更新至最新版本， AWS CLI 再開始。

> **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 AWS CLI 管理線索的範例，請參閱 使用 管理線索 AWS CLI和 使用 設定 CloudWatch Logs 監控 AWS CLI。使用 建立或更新組織線索時 AWS CLI，您必須使用管理帳戶或委派管理員帳戶中具有足夠許可的 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。這個儲存貯體必須具備特定政策，允許 CloudTrail 將組織的日誌檔案放入儲存貯體。

以下是名為 amzn-s3-demo-bucket 的 Amazon S3 儲存貯體的範例政策，該儲存貯體為組織的管理帳戶所擁有。 將 *amzn-s3-demo-bucket*、*region*、 *managementAccountID*、 *trailName* 和 *o-organizationID* 取代為組織的值

此儲存貯體政策包含三個陳述式。

- 第一個陳述式允許 CloudTrail 在 Amazon S3 儲存貯體上呼叫 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 CloudTrail 僅針對特定追蹤寫入 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。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "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:::amzn-s3-demo-bucket/
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:::amzn-s3-demo-bucket/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 日誌檔案。

### 在 中啟用 CloudTrail 做為信任的服務 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 設定成信任 CloudTrail 做為信任的服務。

若要在 AWS Organizations 和 CloudTrail 之間建立信任的服務關係，請開啟終端機或命令列，並使用管理帳戶中的設定檔。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，您必須在管理帳戶或委派管理員帳戶中使用具有足夠許可的 AWS CLI 設定檔。

以下範例會建立組織追蹤，將所有區域的日誌傳遞到名為 *amzn-s3-demo-bucket* 的現有儲存貯體：

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-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": "amzn-s3-demo-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

下列命令會建立組織追蹤，只會在單一 中記錄事件 AWS 區域，也稱為單一區域追蹤。記錄事件 AWS 的區域是 組態設定檔中指定的區域 AWS CLI。

```
aws cloudtrail create-trail --name my-trail --s3-bucket-name amzn-s3-demo-bucket --is-organization-trail
```

如需詳細資訊，請參閱CloudTrail 資源、S3 儲存貯體和 KMS 金鑰的命名需求。

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": "amzn-s3-demo-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 SDKs來更新線索，請確定線索的儲存貯體政策是up-to-date。如需詳細資訊，請參閱使用 為組織建立線索 AWS CLI。
> 當您使用 更新組織線索時 AWS CLI，您必須在管理帳戶或委派管理員帳戶中使用 AWS CLI 具有足夠許可的設定檔。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，因為管理帳戶是所有組織資源的擁有者。
> 即使資源驗證失敗，CloudTrail 也會更新成員帳戶中的組織線索。驗證失敗的範例包括：
>
> - 不正確的 Amazon S3 儲存貯體政策
> - 不正確的 Amazon SNS 主題政策
> - 無法交付至 CloudWatch Logs 日誌群組
> - 使用 KMS 金鑰加密的許可不足
>
> 具有 CloudTrail 許可的成員帳戶可以透過在 CloudTrail 主控台上檢視追蹤的詳細資訊頁面，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

若要變更現有的線索，使其也適用於組織而非單一 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": "amzn-s3-demo-bucket"
}
```

在上述範例中，線索已設定為多區域線索 ("IsMultiRegionTrail": true)。只套用到單一區域的追蹤，將在輸出中顯示 "IsMultiRegionTrail": false。

將單一區域組織線索轉換為多區域組織線索

若要將現有的單一區域組織線索轉換為多區域組織線索，請新增 --is-multi-region-trail選項，如下列範例所示。

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

若要確認線索現在是多區域，請檢查輸出中的 IsMultiRegionTrail 參數是否具有 的值true。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": true,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

## 對組織線索的問題進行故障診斷

本節提供如何疑難排解組織線索問題的相關資訊。

主題

- CloudTrail 未交付事件
- CloudTrail 不會為組織中的成員帳戶傳送 Amazon SNS 通知

## CloudTrail 未交付事件

如果 CloudTrail 未將 CloudTrail 日誌檔案交付至 Amazon S3 儲存貯體

檢查 S3 儲存貯體是否有問題。

- 從 CloudTrail 主控台，檢查追蹤的詳細資訊頁面。如果 S3 儲存貯體發生問題，詳細資訊頁面會包含傳遞至 S3 儲存貯體失敗的警告。
- 從 AWS CLI執行 get-trail-status命令。如果發生故障，命令輸出會包含 `LatestDeliveryError` 欄位，其中會顯示 CloudTrail 在嘗試將日誌檔案交付至指定的儲存貯體時遇到的任何 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，且逾時的請求不會發生此錯誤。若要解決問題，請修正儲存貯體政策，以便 CloudTrail 可以寫入儲存貯體；或建立新的儲存貯體，然後呼叫 `update-trail` 來指定新的儲存貯體。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，以用於存放組織追蹤的日誌檔案。

> **Note**
>
> 如果您的追蹤設定錯誤 (例如，S3 儲存貯體無法連線)，CloudTrail 會在 30 天內嘗試重新傳遞日誌檔案到您的 S3 儲存貯體，且您需要為這些嘗試傳遞事件支付標準 CloudTrail 費用。若要避免支付追蹤設定錯誤費用，您需要刪除追蹤。

如果 CloudTrail 未將日誌交付至 CloudWatch Logs

檢查 CloudWatch Logs 角色政策的組態是否有問題。

- 從 CloudTrail 主控台，檢查追蹤的詳細資訊頁面。如果 CloudWatch Logs 發生問題，詳細資訊頁面會包含警告，指出 CloudWatch Logs 交付失敗。
- 從 中 AWS CLI，執行 get-trail-status命令。如果發生故障，命令輸出會包含 `LatestCloudWatchLogsDeliveryError` 欄位，其中會顯示 CloudTrail 在嘗試將日誌交付至 CloudWatch Logs 時遇到的任何 CloudWatch Logs 錯誤。若要解決此問題，請修正 CloudWatch Logs 角色政策。如需 CloudWatch Logs 角色政策的相關資訊，請參閱 讓 CloudTrail 能使用 CloudWatch Logs 進行監控的角色政策文件。

如果您在組織追蹤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：

- 檢查追蹤的主區域，以查看它是否為選擇加入區域

  雖然您的 預設 AWS 區域 會啟用大多數 AWS 帳戶，但您必須手動啟用特定區域（也稱為選擇加入區域)。如需預設啟用哪些區域的資訊，請參閱《 AWS 帳戶管理 參考指南》中的啟用和停用區域的考量事項。如需 CloudTrail 支援的 區域清單，請參閱 CloudTrail 支援的區域。

  如果組織線索是多區域，而主要區域是選擇加入區域，成員帳戶將不會將活動傳送至組織線索，除非他們選擇加入建立多區域線索 AWS 區域 的 。例如，如果您建立多區域追蹤並選擇歐洲（西班牙）區域作為追蹤的主要區域，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活動傳送至組織追蹤。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 帳戶管理 參考指南》中的啟用或停用組織中的區域。

- 檢查組織資源型政策是否與 CloudTrail 服務連結角色政策衝突

  CloudTrail 使用名為 的服務連結角色`AWSServiceRoleForCloudTrail`來支援組織追蹤。此服務連結角色可讓 CloudTrail 對組織資源執行動作，例如`organizations:DescribeOrganization`。如果組織的資源型政策拒絕服務連結角色政策中允許的動作，CloudTrail 將無法執行動作，即使該動作在服務連結角色政策中允許。若要解決問題，請修正組織的資源型政策，使其不會拒絕服務連結角色政策中允許的動作。

## CloudTrail 不會為組織中的成員帳戶傳送 Amazon SNS 通知

當具有 AWS Organizations 組織線索的成員帳戶未傳送 Amazon SNS 通知時，SNS 主題政策的組態可能會發生問題。即使資源驗證失敗，CloudTrail 仍會在成員帳戶中建立組織線索，例如，組織線索的 SNS 主題不包含所有成員帳戶 IDs。如果 SNS 主題政策不正確，則會發生授權失敗。

若要檢查追蹤的 SNS 主題政策是否有授權失敗：

- 從 CloudTrail 主控台，檢查追蹤的詳細資訊頁面。如果發生授權失敗，詳細資訊頁面會包含警告，`SNS authorization failed`並指示 修正 SNS 主題政策。
- 從 AWS CLI中，執行 get-trail-status命令。如果發生授權失敗，命令輸出會包含值為`LastNotificationError`的欄位`AuthorizationError`。若要解決問題，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 適用於 CloudTrail 索的 Amazon SNS 主題政策。

如需 SNS 主題和訂閱主題的詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》中的 Amazon SNS 入門。

# 了解多區域追蹤和選擇加入區域

線索可以套用至在您的 中啟用的所有 AWS 區域 AWS 帳戶，也可以套用至單一區域。套用至 中所有啟用 AWS 區域 的線索 AWS 帳戶 稱為多區域線索。根據最佳實務，我們建議您建立多區域追蹤，因為它會擷取所有啟用區域中的活動。使用 CloudTrail 主控台建立的所有線索都是多區域線索。您只能使用 AWS CLI 或 `CreateTrail` API 操作建立單一區域追蹤。

雖然您的 預設 AWS 區域 會啟用大多數 AWS 帳戶，但您必須手動啟用特定區域（也稱為選擇加入區域)。如需有關預設啟用哪些區域的資訊，請參閱《 AWS 帳戶管理 參考指南》中的啟用和停用區域的考量事項。如需 CloudTrail 支援的 區域清單，請參閱 CloudTrail 支援的區域。

主題

- 多區域線索的優點有哪些？
- 當您建立多區域追蹤時會發生什麼情況？
- 當您啟用選擇加入區域時會發生什麼情況？
- 當您停用選擇加入區域時會發生什麼情況？

## 多區域線索的優點有哪些？

多區域追蹤具有下列優點：

- 線索的組態設定會一致地套用至所有已啟用的 AWS 區域。
- 您會從單一 Amazon S3 儲存貯 AWS 區域 體中啟用的所有 ，以及選擇性地在 CloudWatch Logs 日誌群組中接收 CloudTrail 事件。
- 您可以從 AWS 區域 單一位置管理所有啟用的線索組態。

## 當您建立多區域追蹤時會發生什麼情況？

建立多區域追蹤具有下列效果：

- CloudTrail 會將帳戶活動的日誌檔案從已啟用的所有 交付 AWS 區域 至您指定的單一 Amazon S3 儲存貯體，並選擇性地交付至 CloudWatch Logs 日誌群組。

- 如果您為線索設定了 Amazon SNS 主題，所有已啟用的日誌檔案交付 SNS 通知 AWS 區域 都會傳送至該單一 SNS 主題。
- 您可以在所有啟用的 中看到多區域線索 AWS 區域，但只能在建立線索的主區域中修改線索。

### 當您啟用選擇加入區域時會發生什麼情況？

在您啟用選擇加入區域之後，CloudTrail 會在您啟用的選擇加入區域中建立每個多區域追蹤的相同複本。

CloudTrail 使用稱為最終一致性的分散式運算模型。由於啟用區域需要幾分鐘到幾個小時，因此您可能不會立即在日誌中看到新啟用區域的所有事件。CloudTrail 可能需要數小時才能交付新啟用區域的所有日誌。在此期間，您可以透過檢視 CloudTrail 事件歷史記錄或執行 命令，來檢視該區域最近 90 天的管理事件。 aws cloudtrail lookup-events --region <region>事件歷史記錄預設會在您的 中處於作用中狀態 AWS 帳戶、擷取最近 90 天的在區域中記錄的管理事件，而且不需要追蹤。

如需有關為 啟用選擇加入區域的資訊 AWS 帳戶，請參閱啟用或停用獨立帳戶的區域，或啟用或停用組織中的區域。

### 當您停用選擇加入區域時會發生什麼情況？

由於您的帳戶在您停用的區域中可能有活動，例如 AWS 服務 移除資源的動作，CloudTrail 將繼續擷取活動，並嘗試針對區域停用之前未刪除的任何線索，將事件交付至 S3 儲存貯體。

## 將追蹤事件複製到 CloudTrail Lake

您可以將現有追蹤事件複製到 CloudTrail Lake 事件資料存放區，以建立記錄至追蹤之事件的時間點快照。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為 CloudTrail 事件設定的現有事件資料存放區，或者您可以建立一個新的 CloudTrail 事件資料存放區，然後在建立事件資料存放區的過程中選擇複製追蹤事件選項。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。與事件歷史記錄中單純的索引鍵和值查詢或執行 `LookupEvents` 相比，CloudTrail Lake 查詢提供了更深入、自訂功能更多的事件檢視畫面。如需有關 CloudTrail Lake 的詳細資訊，請參閱 使用 AWS CloudTrail Lake。

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 Lake 成本。

在將追蹤事件複製到 CloudTrail Lake 事件資料存放區時，您需要按事件資料存放區擷取的未壓縮的資料量支付費用。

當您將追蹤事件複製到 CloudTrail Lake 時，CloudTrail 會解壓縮以 gzip (已壓縮) 格式存放的日誌，然後將日誌中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 Lake 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？ |
| --- | --- |
| 分析並查詢 CloudTrail Lake 中的歷史追蹤事件，而不擷取新事件 | 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的現有追蹤 | 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。<br><br>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。<br><br>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
- 複製追蹤事件所需的許可
- 使用 CloudTrail 主控台將追蹤事件複製到現有的事件資料存放區

## 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 操作來擷取來源 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。
- 當您將追蹤事件複製到事件資料存放區時，CloudTrail 會複製所有追蹤事件，無論目的地事件資料存放區的事件類型、進階事件選取器或組態為何 AWS 區域。
- 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 只會複製 `eventTime` 在事件資料存放區保留期內的追蹤事件。若要決定適當的保留期，請加總您要複製的最舊事件所經歷的天數與要在事件資料存放區中保留事件的天數 (保留期 = `#########` + `###`)。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 壓縮日誌檔案複製追蹤事件。CloudTrail 不會從未壓縮的日誌檔案或使用 Gzip 以外格式壓縮的日誌檔案複製追蹤事件。

- 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 只會複製包含在 S3 儲存貯體`CloudTrail`字首和`CloudTrail`字首內的字首中的 CloudTrail 事件，而不會檢查其他服務的字首 AWS 。如果您要複製其他字首中包含的 CloudTrail 事件，則必須在複製追蹤事件時選擇字首。
- 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 角色所需的所有必要許可。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，CloudTrail 會為角色提供所需的所有許可。

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，則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，CloudTrail 會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。

如果您選擇現有的角色，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。將 *amzn-s3-demo-bucket*、*myAccountID*、 *region*、 *prefix* 和 *eventDataStoreId* 取代為您的組態的適當值。*myAccountID* 是用於 CloudTrail Lake AWS 的帳戶 ID，可能與 S3 儲存貯體 AWS 的帳戶 ID 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:::amzn-s3-demo-bucket"
      ],
      "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:::amzn-s3-demo-bucket/prefix",
        "arn:aws:s3:::amzn-s3-demo-bucket/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，允許 CloudTrail 擔任 IAM 角色，從來源 S3 儲存貯體複製追蹤事件。將 *myAccountID*、*region* 和 *eventDataStoreArn* 取代為適當的組態值。*myAccountID* 是用於 CloudTrail Lake 的 AWS 帳戶 ID，可能與 S3 儲存貯體 AWS 的帳戶 ID 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。

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，以授予這些許可。將 *roleArn* 和 *amzn-s3-demo-bucket* 取代為您的組態的適當值。

```
{
  "Sid": "AWSCloudTrailImportBucketAccess",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket",
    "s3:GetBucketAcl",
    "s3:GetObject"
  ],
  "Principal": {
    "AWS": "roleArn"
  },
  "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket",
    "arn:aws:s3:::amzn-s3-demo-bucket/*"
  ]
},
```

## 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 金鑰政策為 CloudTrail 提供從已啟用 SSE-KMS 加密的 S3 儲存貯體複製追蹤事件所需的 `kms:Decrypt` 和 `kms:GenerateDataKey` 許可。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 金鑰政策可讓 CloudTrail 解密來源 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，該政策允許 CloudTrail 解密來源 S3 儲存貯體中的資料。將 *roleArn*、*amzn-s3-demo-bucket*、*myAccountID*、*region* 和 *eventDataStoreId* 取代為您的組態的適當值。*myAccountID* 是用於 CloudTrail Lake AWS 的帳戶 ID，可能與 S3 儲存貯體 AWS 的帳戶 ID 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:::amzn-s3-demo-bucket/*"
    },
    "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 只會複製 `eventTime` 在事件資料存放區保留期內的追蹤事件。若要決定適當的保留期，請加總您要複製的最舊事件所經歷的天數與要在事件資料存放區中保留事件的天數 (保留期 = ####### ## + ####)。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. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
2. 在 CloudTrail 主控台的左側導覽窗格中選擇 Trails (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，則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. （選用）根據預設，CloudTrail 只會複製包含在 S3 儲存貯體`CloudTrail`字首和`CloudTrail`字首內的字首中的 CloudTrail 事件，而不會檢查其他服務的字首 AWS 。如果您要複製其他字首中包含的 CloudTrail 事件，請選擇 Enter S3 URI (輸入 S3 URI)，然後選擇 Browse S3 (瀏覽 S3) 以瀏覽至字首。

   S3 儲存貯體政策必須授予 CloudTrail 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. 針對指定事件的時間範圍，選擇複製事件的時間範圍。CloudTrail 會在嘗試複製追蹤事件之前檢查字首和日誌檔案名稱，以確認名稱包含介於所選開始日期和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 只會複製 `eventTime` 在事件資料存放區保留期內的追蹤事件。例如，如果事件資料存放區的保留期為 90 天，則 CloudTrail 將不會複製 `eventTime` 早於 90 天的任何追蹤事件。

   - 如果選擇相對範圍，您可以選擇複製過去 6 個月、1 年、2 年、7 年或自訂範圍內記錄的事件。CloudTrail 會複製所選時段內記錄的事件。
   - 如果選擇 Absolute range (絕對範圍)，您可以選擇特定的開始和結束日期。CloudTrail 會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 會自動為此新角色建立必要的許可。

- 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 會在事件複製的過程中逐步更新詳細資訊。

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)。當您重試複製時，CloudTrail 會在發生失敗的位置繼續複製。

如需檢視追蹤事件複製之詳細資訊，請參閱 使用 CloudTrail 主控台檢視事件複製詳細資訊。

# 取得和檢視 CloudTrail 日誌檔案

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 會將您的日誌檔案交付至您在建立線索時指定的 Amazon S3 儲存貯體。CloudTrail 通常會在 API 呼叫的平均約 5 分鐘內傳遞日誌。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**
>
> 如果您的追蹤設定錯誤 (例如，S3 儲存貯體無法連線)，CloudTrail 會在 30 天內嘗試重新傳遞日誌檔案到您的 S3 儲存貯體，且您需要為這些嘗試傳遞事件支付標準 CloudTrail 費用。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 CloudTrail 日誌檔案
- 下載 CloudTrail 日誌檔案


## 尋找 CloudTrail 日誌檔案

CloudTrail 會將日誌檔案以 gzip 封存形式發佈至 S3 儲存貯體。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：

- 在您建立線索時指定的儲存貯體名稱 (位於 CloudTrail 主控台的 Trails (線索) 頁面上)
- 在您建立線索時指定的 (選用) 前綴
- 字串 "AWSLogs"
- 帳戶號碼
- 資料、管理事件的字串 "CloudTrail"
- 洞察事件的字串 "CloudTrail-Insight"
- 網路活動事件的字串 "CloudTrail-NetworkActivity"
- 資料事件彙總事件的字串 "CloudTrail-Aggregated"
- 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

下列範例顯示資料、管理事件的完整日誌檔案物件名稱：

```
amzn-s3-demo-bucket/prefix_name/AWSLogs/Account ID/
CloudTrail/region/YYYY/MM/DD/file_name.json.gz
```

下列範例顯示洞見事件的完整日誌檔案物件名稱：

```
amzn-s3-demo-bucket/prefix_name/AWSLogs/Account ID/CloudTrail-
Insight/region/YYYY/MM/DD/file_name.json.gz
```

下列範例顯示網路活動事件的完整日誌檔案物件名稱：

```
amzn-s3-demo-bucket/prefix_name/AWSLogs/Account ID/CloudTrail-
NetworkActivity/region/YYYY/MM/DD/file_name.json.gz
```

下列範例顯示資料事件彙總的完整日誌檔案物件名稱：

```
amzn-s3-demo-bucket/prefix_name/AWSLogs/Account ID/CloudTrail-
Aggregated/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案物件名稱會在路徑中包含組織單位 ID，如下所示：
>
> ```
> amzn-s3-demo-bucket/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
```

```
    amzn-s3-demo-bucket
        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 記錄管理、資料和網路活動事件的內容。

## 下載 CloudTrail 日誌檔案

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 日誌檔案是 Amazon S3 物件。您可以使用 Amazon S3 主控台、 AWS Command Line Interface (CLI) 或 Amazon S3 API 來擷取日誌檔案。

如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的 Amazon S3 物件概觀。

下列程序說明如何使用 AWS 管理主控台下載日誌檔案。

下載和讀取日誌檔案

1. 開啟位於 https://console.aws.amazon.com/s3/ 的 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 記錄管理、資料和網路活動事件的內容」。

AWS 與第三方記錄和分析專家合作，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。
> 如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄。

# 設定 CloudTrail 的 Amazon SNS 通知

當 CloudTrail 發佈新的日誌檔案到您的 Amazon S3 儲存貯體時，您會收到通知。您可以使用 Amazon Simple Notification Service (Amazon SNS) 來管理通知。

通知為選用。如果想要接到通知，您要設定每當傳送新的日誌檔案，CloudTrail 就會傳送更新資訊到 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

# 設定 CloudTrail 傳送通知

在 CloudTrail 主控台上，您可以在建立或更新追蹤時啟用 SNS 通知交付選項，將追蹤設定為使用 Amazon SNS 主題。如果您選擇使用新主題，CloudTrail 會為您建立 Amazon SNS 主題並連接適當的政策，以便 CloudTrail 具有發佈至該主題的許可。

使用 AWS CLI，您可以指定 `--sns-topic-name` 參數的值來建立或更新線索，以使用 Amazon SNS 主題。您可以指定 Amazon SNS 主題的名稱或 ARN。

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

當您設定多區域追蹤的通知時，所有區域的通知都會傳送至您指定的 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。

若要收到通知，請訂閱 Amazon SNS 主題或 CloudTrail 所使用的主題。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**
>
> 在日誌檔案寫入 Amazon S3 儲存貯體時，CloudTrail 會傳送通知。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": "amzn-s3-demo-bucket","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": "amzn-s3-demo-bucket",
    "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 Simple Notification Service 開發人員指南》中的散發至 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 建立線索，則可以使用 `CreateTrail` 或 `UpdateTrail` 操作，指定您想要 CloudTrail 將通知傳送至其中的現有 Amazon SNS 主題。您必須先確定該主題已存在，且其具有允許 CloudTrail 傳送通知的許可。請參閱 適用於 CloudTrail 索的 Amazon SNS 主題政策。

### 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。

# AWS CloudTrail 搭配界面 VPC 端點使用

如果您使用 Amazon Virtual Private Cloud (Amazon VPC) 託管 AWS 資源，您可以在 VPC 與 之間建立私有連線 AWS CloudTrail。您可以使用此連線來啟用 CloudTrail 不用透過公有網際網路在 VPC 與您的資源進行通訊。

Amazon VPC 是一種 AWS 服務，可用來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。透過 VPC 端點，VPC 和 AWS 服務之間的路由由 AWS 網路處理，您可以使用 IAM 政策來控制對服務資源的存取。

若要將您的 VPC 連接到 CloudTrail，請定義 CloudTrail 的 VPC 端點界面。界面端點是具有私有 IP 地址的彈性網路界面，可做為目的地為支援 AWS 服務之流量的進入點。端點能為 CloudTrail 提供可靠、可擴展性的連線，無須使用網際網路閘道、網路位址轉譯 (NAT) 執行個體或 VPN 連接。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 端點採用 AWS PrivateLink 技術，這項 AWS 技術可使用具有私有 IP 地址的彈性網路介面，在 AWS 服務之間進行私有通訊。如需詳細資訊，請參閱 AWS PrivateLink。

下列各節適用於 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。

主題


- 大區 (Regions)
- 為 CloudTrail 建立 VPC 端點
- 建立 CloudTrail 的 VPC 端點政策
- 共用子網路


## 大區 (Regions)

AWS CloudTrail 在支援 CloudTrail 的所有 AWS 區域 中支援 VPC 端點和 VPC 端點政策。

## 為 CloudTrail 建立 VPC 端點

若要以 VPC 開始使用 CloudTrail，請建立 CloudTrail 的 VPC 端點界面。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的 AWS 服務 使用介面 VPC 端點存取 。

您不需要變更 CloudTrail 的設定。CloudTrail AWS 服務 使用公有端點或私有介面 VPC 端點呼叫其他 ，以使用中者為準。

## 建立 CloudTrail 的 VPC 端點政策

VPC 端點政策是您可以連接到介面 VPC 端點的 IAM 資源。預設端點政策可讓您透過介面 VPC 端點完整存取 CloudTrail APIs。若要控制從 VPC 授予 CloudTrail 的存取權，請將自訂端點政策連接至介面 VPC 端點。

端點政策會指定以下資訊：

- 可執行動作 (AWS 帳戶、IAM 使用者和 IAM 角色) 的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需 VPC 端點政策的詳細資訊，包括如何更新政策，請參閱《Amazon VPC 使用者指南》中的使用 VPC 端點控制對 服務的存取。

以下是 CloudTrail 的自訂 VPC 端點政策範例。

範例政策：

- 範例：允許所有 CloudTrail 動作
- 範例：允許特定的 CloudTrail 動作
- 範例：拒絕所有 CloudTrail 動作
- 範例：拒絕特定 CloudTrail 動作
- 範例：允許來自特定 VPC 的所有 CloudTrail 動作
- 範例：允許來自特定 VPC 端點的所有 CloudTrail 動作

## 範例：允許所有 CloudTrail 動作

下列範例 VPC 端點政策會授予所有資源上所有主體所有 CloudTrail 動作的存取權。

JSON

```
{
     "Version":"2012-10-17",
     "Statement": [
         {
             "Action": "cloudtrail:*",
             "Effect": "Allow",
             "Resource": "*",
             "Principal": "*"
         }
     ]
}
```

## 範例：允許特定的 CloudTrail 動作

下列範例 VPC 端點政策會授予在所有資源上執行 `cloudtrail:ListTrails`和 `cloudtrail:ListEventDataStores`動作的存取權。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": ["cloudtrail:ListTrails",
 "cloudtrail:ListEventDataStores"],
            "Effect": "Allow",
            "Principal": "*",
            "Resource": "*"
        }
    ]
}
```

## 範例：拒絕所有 CloudTrail 動作

下列範例 VPC 端點政策拒絕存取所有資源上所有主體的所有 CloudTrail 動作。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": "cloudtrail:*",
            "Effect": "Deny",
            "Principal": "*",
            "Resource": "*"
        }
    ]
}
```

## 範例：拒絕特定 CloudTrail 動作

下列範例 VPC 端點政策會拒絕所有資源上所有主體的 `cloudtrail:CreateTrail`和 `cloudtrail:CreateEventDataStore`動作。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": ["cloudtrail:CreateTrail",
 "cloudtrail:CreateEventDataStore"],
            "Effect": "Deny",
            "Principal": "*",
            "Resource": "*"
        }
    ]
}
```

## 範例：允許來自特定 VPC 的所有 CloudTrail 動作

下列範例 VPC 端點政策授予存取權，以對所有資源上的所有主體執行所有 CloudTrail 動作，但前提是請求者使用指定的 VPC 提出請求。將 *vpc-id* 取代為您的 VPC ID。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "cloudtrail:*",
      "Resource": "*",
      "Principal": "*",
      "Condition": {
        "StringEquals": {
        "aws:SourceVpc": "vpc-1234567890abcdef0"
        }
      }
```

```
    }
  ]
}
```

### 範例：允許來自特定 VPC 端點的所有 CloudTrail 動作

下列範例 VPC 端點政策授予存取權，以對所有資源上的所有主體執行所有 CloudTrail 動作，但前提是請求者使用指定的 VPC 端點提出請求。將 *vpc-endpoint-id* 取代為您的 VPC 端點 ID。

JSON

```
{
     "Version":"2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Action": "cloudtrail:*",
         "Resource": "*",
         "Condition": {
             "StringEquals": {
                "aws:SourceVpce": "vpce-1a2b3c4d"
             }
         }
       }
    ]
  }
```

## 共用子網路

與任何其他 VPC 端點類似，只有共用子網路的擁有者帳戶才能建立 CloudTrail VPC 端點。不過，參與者帳戶可以使用子網路中與參與者帳戶共用的 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。

# CloudTrail 資源、S3 儲存貯體和 KMS 金鑰的命名需求

本節將提供 CloudTrail 資源、Amazon S3 儲存貯體和 KMS 金鑰命名要求的相關資訊。

**主題**

- CloudTrail 資源命名要求
- Amazon S3 儲存貯體命名需求
- AWS KMS 別名命名要求

## CloudTrail 資源命名要求

CloudTrail 資源名稱必須符合下列要求：

- 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

您用來存放 CloudTrail 日誌檔案的 Amazon S3 儲存貯體，其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 別名命名要求

建立 時 AWS KMS key，您可以選擇別名來識別它。例如，您可以選擇別名 "KMS-CloudTrail-us-west-2" 來加密特定線索的日誌。

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。

# AWS 帳戶 關閉和追蹤

AWS CloudTrail 會持續監控和記錄任何 使用者、角色或 所產生的帳戶活動事件 AWS 服務 AWS 帳戶。使用者可以建立 CloudTrail 追蹤，以取得在其擁有的 S3 儲存貯體中此類事件的複本。

CloudTrail 是一種基礎安全服務，因此，即使 AWS 帳戶 關閉 ，使用者建立的線索仍會繼續存在並交付事件，除非使用者在關閉線索 AWS 帳戶 之前明確刪除其 中的線索。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。

關閉您的 之前 AWS 帳戶，請考慮下列事項：

- 即使在關閉後期間過後，追蹤仍會繼續存在。關閉後期間是指您關閉帳戶到 AWS 永久關閉帳戶之間的 90 天 AWS 帳戶。
- 此行為也適用於管理帳戶或委派管理員建立的組織線索，以及在組織成員帳戶中建立的多區域組織線索。
- 對於將事件交付至相同帳戶中 S3 儲存貯體的追蹤，即使帳戶關閉，追蹤仍會繼續存在。不過，由於 S3 儲存貯體會在帳戶關閉時刪除，因此追蹤不會繼續交付事件。
- 對於將事件交付到不同帳戶中 S3 儲存貯體的線索，即使帳戶關閉，線索仍會繼續存在。如果事件可以交付，線索也會繼續將事件交付到 S3 儲存貯體。例如，如果您關閉組織中的成員帳戶，但未關閉管理帳戶，組織追蹤仍會繼續將事件交付至 S3 儲存貯體。
- 對於使用 加密的線索 AWS KMS keys，除了 KMS 金鑰之外，在帳戶關閉後，線索仍會繼續存在。

使用者可以選擇在關閉線索之前刪除線索 AWS 帳戶，或在線索 AWS 帳戶 關閉後聯絡 AWS 支援請求刪除線索。

如需有關關閉 的資訊 AWS 帳戶，請參閱《 AWS 帳戶管理 參考指南》中的關閉 AWS 帳戶。

> **Note**
>
> 如果 CloudTrail 日誌檔案驗證已經啟用，使用者會持續收到每小時摘要檔案，其中會指出是否建立了任何 CloudTrail 日誌。
> CloudTrail Lake 事件資料存放區、用於整合的 CloudTrail Lake 通道、CloudTrail 服務連結通道，以及為追蹤建立的資源 （例如，Amazon CloudWatch Logs 日誌群組和封閉帳戶中現有的 Amazon S3 儲存貯體），請遵循帳戶關閉的標準 AWS 行為，並在關閉後期間 （通常為 90 天） 之後永久刪除。

# 設定 CloudTrail 設定

您可以使用 CloudTrail 主控台的設定頁面來設定和檢閱 CloudTrail 設定，例如管理 AWS Organizations 組織的委派管理員，以及檢視為您的帳戶建立的任何服務連結管道。

存取設定頁面

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
2. 在 CloudTrail 主控台的左側導覽窗格中選擇 Settings (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 AWS Organizations 組織，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的管理員。

     組織的管理帳戶可以指派組織內的任何帳戶，以擔任 CloudTrail 委派管理員，代表組織管理組織的追蹤和事件資料存放區。
   - 檢視服務連結頻道 – 您可以檢視為您的帳戶建立的任何服務連結管道。

     AWS 服務 可以建立服務連結頻道來代表您接收 CloudTrail 事件。建立服務連結頻道 AWS 的服務會設定頻道的進階事件選取器 AWS 區域，並指定頻道是否套用至所有 或單一 AWS 區域。

## 組織委派的管理員

當您將 CloudTrail 與 AWS Organizations 組織搭配使用時，您可以指派組織內的任何帳戶做為 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。委派管理員是組織中的成員帳戶，可以在 CloudTrail 中執行與管理帳戶相同的管理工作 (註明的除外)。

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。

當您第一次在 CloudTrail 主控台中新增委派管理員，或使用 AWS CLI 或 CloudTrail API 時，CloudTrail 會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，則 CloudTrail 會為管理帳戶建立服務連結角色。如需服務連結角色的詳細資訊，請參閱使用 CloudTrail 的服務連結角色。

> **Note**
>
> 當您使用 CLI 或 API AWS Organizations 操作新增委派管理員時，如果 CloudTrail 服務連結角色不存在，則不會自動建立這些角色。只有在您直接從管理帳戶呼叫 CloudTrail 服務時，才會建立服務連結角色。例如，當您使用 CloudTrail 主控台或 CloudTrail API 新增委派管理員或建立組織追蹤 AWS CLI 或事件資料存放區時，即會建立AWSServiceRoleForCloudTrail服務連結角色。
>
> 當您使用 AWS CloudTrail；CLI 或 API 操作新增委派管理員時，CloudTrail AWSServiceRoleForCloudTrailEventContext 會同時建立 AWSServiceRoleForCloudTrail和服務連結角色。如需詳細資訊，請參閱 使用 CloudTrail 的服務連結角色。

請注意下列定義委派管理員如何在 CloudTrail 中運作的因素。

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 (例如線索和事件資料存放區) 的擁有者。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，不會刪除委派的管理員建立的組織線索和事件資料存放區，因為管理帳戶始終都是 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。

每個組織最多可以有三個 CloudTrail 委派的管理員。如需委派的管理員的詳細資訊，請參閱 移除 CloudTrail 委派的管理員。

下表顯示管理帳戶、委派管理員帳戶和 AWS Organizations 組織中成員帳戶的功能。

| 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 |

| 功能 | 管理帳戶 | 委派管理員帳戶 | 成員帳戶 |
| --- | --- | --- | --- |
| 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 |
| 為 CloudTrail 事件或 AWS Config 組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 |
| 在組織事件資料存放區上開始和停止事件擷取。 | 是 | 是 | 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受管儀表板。 | 是 | 否 | 否 |

| 功能 | 管理帳戶 | 委派管理員帳戶 | 成員帳戶 |
| --- | --- | --- | --- |
| 啟用組織事件資料存放區的醒目提示儀表板。 | 是 | 否 | 否 |
| 為查詢組織事件資料存放區的自訂儀表板建立小工具。 | 是 | 否 | 否 |

[1] 委派管理員只能使用 AWS CLI 或 CloudTrail 或 API 操作來設定 CloudWatch Logs 日誌群組。CloudTrail `CreateTrail` `UpdateTrail` 呼叫帳戶中必須存在 CloudWatch Logs 日誌群組和日誌角色。

[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。當組織線索或事件資料存放區轉換為帳戶層級的線索或事件資料存放區時，只有管理帳戶可以存取線索或事件資料存放區。

[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
- 新增 CloudTrail 委派的管理員
- 移除 CloudTrail 委派的管理員


## 指派委派管理員所需的許可

指派 CloudTrail 委派管理員時，您必須擁有在 CloudTrail 中新增和移除委派管理員的許可，以及下列政策陳述式中列出的特定 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": "*"
}
```

### 使用條件索引鍵搭配委派管理員許可的政策陳述式時的考量事項

在新增政策陳述式以新增和移除 CloudTrail 中的委派管理員時，您可以考慮使用 IAM 全域條件金鑰，以提高安全性。執行此操作時，請記得在 條件中包含兩個服務主體名稱 (SPNs)。例如：

```
{
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": [
            "context.cloudtrail.amazonaws.com",
            "cloudtrail.amazonaws.com"
          ]
        }
      },
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow"
}
```

如需詳細資訊，請參閱的 Identity and Access Management AWS CloudTrail。

## 新增 CloudTrail 委派的管理員

您可以新增委派的管理員，以管理您組織的 CloudTrail 資源，例如線索和事件資料存放區。

您可以使用 CloudTrail 主控台或 AWS CLI為您的 AWS 組織新增 CloudTrail 委派的管理員。

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。如需有關如何為組織建立新 AWS 帳戶的資訊，請參閱在組織中建立 AWS 帳戶。如需有關如何邀請現有 AWS 帳戶加入組織的資訊，請參閱邀請 AWS 帳戶加入您的組織。

CloudTrail console

下列程序說明如何使用 CloudTrail 主控台新增 CloudTrail 委派的管理員。

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
2. 在 CloudTrail 主控台的左側導覽窗格中選擇 Settings (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線索和事件資料存放區的 CloudTrail 委派管理員之帳戶的 12 位數 AWS 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 委派的管理員

您可以使用 CloudTrail 主控台或 AWS CLI新增 CloudTrail 委派的管理員。

CloudTrail console

下列程序說明如何使用 CloudTrail 主控台移除 CloudTrail 委派的管理員。

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
2. 在 CloudTrail 主控台的左側導覽窗格中選擇 Settings (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。

# 檢視服務連結頻道

AWS 服務可以建立服務連結頻道，以代表您接收 CloudTrail 事件。建立服務連結頻道 AWS 的服務會設定頻道的進階事件選取器，並指定頻道是否套用至所有 AWS 區域或單一 AWS 區域。

主題

- 使用主控台檢視服務連結通道
- 使用 檢視服務連結頻道 AWS CLI

## 使用主控台檢視服務連結通道

使用 CloudTrail 主控台，您可以檢視由 AWS 服務建立之任何 CloudTrail 服務連結頻道的相關資訊。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 主控台的左側導覽窗格中選擇 Settings (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。頻道名稱格式為 `aws-service-channel/`*`AWS_service_name`*`/slc`，其中 *`AWS_service_name`*代表管理頻道 AWS 的服務名稱。
   - 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 service - 管理頻道 AWS 的服務名稱。

- 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 檢視服務連結頻道 AWS CLI

使用 AWS CLI，您可以檢視 AWS 服務建立之任何 CloudTrail 服務連結頻道的相關資訊。

主題


- 取得 CloudTrail 服務連結管道
- 列出所有 CloudTrail 服務連結管道
- AWS 服務連結頻道上的 服務事件


## 取得 CloudTrail 服務連結管道

下列範例 AWS CLI 命令會傳回特定 CloudTrail 服務連結頻道的相關資訊，包括目的地 AWS 服務的名稱、為頻道設定的任何進階選擇器，以及該頻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`代表建立頻道 AWS 的服務名稱。

```
{
    "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 服務連結管道

下列範例 AWS CLI 命令會傳回代表您建立之所有 CloudTrail 服務連結頻道的相關資訊。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`代表建立頻道 AWS 的服務名稱。

```
{
    "Channels": [
        {
            "ChannelArn": "arn:aws:cloudtrail:us-east-1:111122223333:channel/EXAMPLE-
ee54-4813-92d5-999aeEXAMPLE",
            "Name": "aws-service-channel/AWS_service_name/slc"
        }
    ]
}
```

## AWS 服務連結頻道上的 服務事件

管理服務連結頻道 AWS 的服務可以在服務連結頻道上啟動動作 （例如，建立或更新服務連結頻道）。CloudTrail 會將這些動作記錄為 AWS 服務事件，並將這些事件傳送到 Event history (事件歷史

記錄)，以及為管理事件設定的任何作用中線索和事件資料存放區。對於這些事件，eventType 欄位是 AwsServiceEvent。

以下是用於建立 AWS 服務連結頻道之服務事件的日誌檔案項目範例。


```
{
   "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

CloudTrail 中的事件是 AWS 帳戶中活動的記錄。此活動可以是 CloudTrail 得以監控之 IAM 身分或服務所採取的動作。CloudTrail 事件提供透過 AWS 管理主控台、 AWS SDKs、命令列工具和其他 進行的 API 和非 API 帳戶活動的歷史記錄 AWS 服務。

CloudTrail 日誌檔案不是公有 API 呼叫的已排序堆疊追蹤，因此事件不會以任何特定順序顯示。

CloudTrail 事件有四種類型：

- 管理事件
- 資料事件
- 網路活動事件
- Insights 事件

根據預設，線索和事件資料會存放日誌管理事件，但不會存放資料事件、網路活動事件或 Insights 事件。

所有事件類型都使用 CloudTrail JSON 日誌格式。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。

如需管理、資料和網路活動事件的 CloudTrail 事件記錄欄位相關資訊，請參閱 CloudTrail 記錄管理、資料和網路活動事件的內容。

如需追蹤 Insights 事件的 CloudTrail 事件記錄欄位的相關資訊，請參閱 追蹤的 Insights 事件 CloudTrail 記錄內容。

如需事件資料存放區之 Insights 事件的 CloudTrail 事件記錄欄位的相關資訊，請參閱 事件資料存放區的 Insights 事件 CloudTrail 記錄內容。

## 管理事件

管理事件提供有關對 AWS 帳戶中資源執行的管理操作的資訊。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 API AWS Identity and Access Management `AttachRolePolicy` 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 API AWS CloudTrail `CreateTrail` 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，CloudTrail 就會記錄 `ConsoleLogin` 事件的日誌。如需詳細資訊，請參閱CloudTrail 擷取的非 API 事件。

根據預設，CloudTrail 追蹤和 CloudTrail Lake 事件資料會存放日誌管理事件。如需記錄管理事件的詳細資訊，請參閱 記錄管理事件。

下列範例顯示管理事件的單一日誌記錄。在這種情形中，名為 `Mary_Major` 的 IAM 使用者會執行 aws cloudtrail start-logging 命令來呼叫 CloudTrail `StartLogging` 動作，以便在名為 `myTrail` 的追蹤上啟動記錄程序。


```
{
    "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 儲存貯體中物件的 Amazon S3 物件層級 API 活動（例如，DeleteObject、 GetObject和 PutObject API 操作）。 S3
- AWS Lambda 函數執行活動（Invoke API)。
- 用於記錄 AWS外部事件的 CloudTrail Lake 通道上的 CloudTrail PutAuditEvents 活動。
- 主題上的 Amazon SNS Publish 和 PublishBatch API 操作。

下表顯示線索和事件資料存放區可用的資源類型。資源類型（主控台）欄會在主控台中顯示適當的選擇。resources.type 值欄會顯示您要指定的resources.type值，以使用 AWS CLI 或 CloudTrail APIs 在線索或事件資料存放區中包含該類型的資料事件。

對於線索，您可以使用基本或進階事件選取器，在一般用途儲存貯體、Lambda 函數和 DynamoDB 資料表（顯示於資料表的前三列）中記錄 Amazon S3 物件的資料事件。您只能使用進階事件選取器來記錄剩餘資料列中顯示的資源類型。

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。

# 支援的資料事件 AWS CloudTrail

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon RDS | 資料庫叢集上的 Amazon RDS API 活動。 | RDS 資料 API - 資料庫叢集 | `AWS::RDS::DBCluster` |
| Amazon S3 | 一般用途儲存貯體中物件的 Amazon S3 物件層級 API 活動（例如 `DeleteObject`、`GetObject` 和 `PutObject` API 操作）。 | S3 | `AWS::S3::Object` |
| Amazon S3 | 存取點上的 Amazon S3 API 活動。 | S3 存取點 | `AWS::S3::AccessPoint` |
| Amazon S3 | 目錄儲存貯體中物件的 Amazon S3 物件層級 API 活動（例如 `DeleteObject`、`GetObject` 和 `PutObject` API 操作）。 | S3 Express | `AWS::S3Express::Object` |
| Amazon S3 | Amazon S3 Object Lambda 存取點 API 活動，例如對 `CompleteMultipartUpload` 和的呼叫`GetObject`。 | S3 Object Lambda | `AWS::S3ObjectLambda::AccessPoint` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon S3 | 磁碟區上的 Amazon FSx API 活動。 | FSx 磁碟區 | AWS::FSx::Volume |
| Amazon S3 Tables | 資料表上的 Amazon S3 API 活動。 | S3 資料表 | AWS::S3Tables::Table |
| Amazon S3 Tables | 資料表儲存貯體上的 Amazon S3 API 活動。 | S3 資料表儲存貯體 | AWS::S3Tables::TableBucket |
| Amazon S3 Vectors | 向量儲存貯體上的 Amazon S3 API 活動。 | S3 向量儲存貯體 | AWS::S3Vectors::VectorBucket |
| Amazon S3 Vectors | 向量索引上的 Amazon S3 API 活動。 | S3 向量索引 | AWS::S3Vectors::Index |
| Amazon S3 on Outposts | Outposts 上 Amazon S3 物件層級的 API 活動。 | S3 Outposts | AWS::S3Outposts::Object |
| Amazon SNS | 平台端點上的 Amazon SNS Publish API 操作。 | SNS 平台端點 | AWS::SNS::PlatformEndpoint |
| Amazon SNS | 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 Supply Chain | AWS Supply Chain 執行個體上的 API 活動。 | 供應鏈 | AWS::SCN::Instance |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon SWF | 網域上的 Amazon SWF API 活動。 | SWF 網域 | AWS::SWF::Domain |
| AWS AppConfig | 組態操作的 AWS AppConfig API 活動，例如呼叫 StartConfiguration Session 和 GetLatestConfiguration 。 | AWS AppConfig | AWS::AppConfig::Configuration |
| AWS AppSync | AppSync GraphQL API APIs AWS AppSync 活動。 | AppSync GraphQL | AWS::AppSync::GraphQLApi |
| Amazon Aurora DSQL | 叢集資源上的 Amazon Aurora DSQL API 活動。 | Amazon Aurora DSQL | AWS::DSQL::Cluster |
| AWS B2B 資料交換 | 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 Backup | AWS Backup 在搜尋任務上搜尋資料 API 活動。 | AWS Backup 搜尋資料 APIs | AWS::Backup::SearchJob |
| 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 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Bedrock | 非同步調用上的 Amazon Bedrock API 活動。 | Bedrock 非同步調用 | AWS::Bedrock::AsyncInvoke |
| Amazon Bedrock | 流程別名上的 Amazon Bedrock API 活動。 | Bedrock 流程別名 | AWS::Bedrock::FlowAlias |
| Amazon Bedrock | 護欄上的 Amazon Bedrock API 活動。 | Bedrock 護欄 | AWS::Bedrock::Guardrail |
| Amazon Bedrock | 內嵌代理程式上的 Amazon Bedrock API 活動。 | Bedrock 調用內嵌代理程式 | AWS::Bedrock::InlineAgent |
| Amazon Bedrock | 知識庫中的 Amazon Bedrock API 活動。 | Bedrock 知識庫 | AWS::Bedrock::KnowledgeBase |
| Amazon Bedrock | 模型上的 Amazon Bedrock API 活動。 | Bedrock 模型 | AWS::Bedrock::Model |
| Amazon Bedrock | 提示上的 Amazon Bedrock API 活動。 | Bedrock 提示 | AWS::Bedrock::PromptVersion |
| Amazon Bedrock | 工作階段上的 Amazon Bedrock API 活動。 | Bedrock 工作階段 | AWS::Bedrock::Session |
| Amazon Bedrock | 流程執行的 Amazon Bedrock API 活動。 | Bedrock 流程執行 | AWS::Bedrock::FlowExecution |
| Amazon Bedrock | 自動推理政策上的 Amazon Bedrock API 活動。 | Bedrock 自動化推理政策 | AWS::Bedrock::AutomatedReasoningPolicy |
| Amazon Bedrock | 自動推理政策版本的 Amazon Bedrock API 活動。 | Bedrock 自動化推理政策版本 | AWS::Bedrock::AutomatedReasoningPolicyVersion |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Bedrock | Amazon Bedrock 資料自動化專案 API 活動。 | Bedrock 資料自動化專案 | `AWS::Bedrock::DataAutomationProject` |
| Amazon Bedrock | Bedrock 資料自動化調用 API 活動。 | Bedrock 資料自動化調用 | `AWS::Bedrock::DataAutomationInvocation` |
| Amazon Bedrock | Amazon Bedrock 資料自動化設定檔 API 活動。 | Bedrock 資料自動化設定檔 | `AWS::Bedrock::DataAutomationProfile` |
| Amazon Bedrock | Amazon Bedrock 藍圖 API 活動。 | Bedrock 藍圖 | `AWS::Bedrock::Blueprint` |
| Amazon Bedrock | Amazon Bedrock Code-Interpreter API 活動。 | Bedrock-AgentCore Code-Interpreter | `AWS::BedrockAgentCore::CodeInterpreter` |
| Amazon Bedrock | Amazon Bedrock 瀏覽器 API 活動。 | Bedrock-AgentCore 瀏覽器 | `AWS::BedrockAgentCore::Browser` |
| Amazon Bedrock | Amazon Bedrock 工作負載身分 API 活動。 | Bedrock-AgentCore 工作負載身分 | `AWS::BedrockAgentCore::WorkloadIdentity` |
| Amazon Bedrock | Amazon Bedrock 工作負載身分目錄 API 活動。 | Bedrock-AgentCore 工作負載身分目錄 | `AWS::BedrockAgentCore::WorkloadIdentityDirectory` |
| Amazon Bedrock | Amazon Bedrock Token Vault API 活動。 | Bedrock-AgentCore 權杖保存庫 | `AWS::BedrockAgentCore::TokenVault` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Bedrock | Amazon Bedrock APIKey CredentialProvider API 活動。 | Bedrock-AgentCore APIKey CredentialProvider | `AWS::BedrockAgentCore::APIKeyCredentialProvider` |
| Amazon Bedrock | Amazon Bedrock 執行時間 API 活動。 | Bedrock-AgentCore 執行期 | `AWS::BedrockAgentCore::Runtime` |
| Amazon Bedrock | Amazon Bedrock Runtime-Endpoint API 活動。 | Bedrock-AgentCore 執行時間端點 | `AWS::BedrockAgentCore::RuntimeEndpoint` |
| Amazon Bedrock | Amazon Bedrock Gateway API 活動。 | Bedrock-AgentCore 閘道 | `AWS::BedrockAgentCore::Gateway` |
| Amazon Bedrock | Amazon Bedrock 記憶體 API 活動。 | Bedrock-AgentCore 記憶體 | `AWS::BedrockAgentCore::Memory` |
| Amazon Bedrock | Amazon Bedrock Oauth2 CredentialProvider API 活動。 | Bedrock-AgentCore Oauth2 CredentialProvider | `AWS::BedrockAgentCore::OAuth2CredentialProvider` |
| Amazon Bedrock | Amazon Bedrock 瀏覽器自訂 API 活動。 | Bedrock-AgentCore 瀏覽器自訂 | `AWS::BedrockAgentCore::BrowserCustom` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Bedrock | Amazon Bedrock Code-Interpreter-Custom API 活動。 | Bedrock-AgentCore Code-Interpreter-Custom | `AWS::BedrockAgentCore::CodeInterpreterCustom` |
| Amazon Bedrock | Amazon Bedrock Tool API 活動。 | Bedrock 工具 | `AWS::Bedrock::Tool` |
| AWS Cloud Map | 命名空間上的 AWS Cloud Map API 活動。 | AWS Cloud Map 命名空間 | `AWS::ServiceDiscovery::Namespace` |
| AWS Cloud Map | 服務上的 AWS Cloud Map API 活動。 | AWS Cloud Map 服務 | `AWS::ServiceDiscovery::Service` |
| Amazon CloudFront | KeyValueStore 上的 CloudFront API 活動。 | CloudFront KeyValueStore | `AWS::CloudFront::KeyValueStore` |
| AWS CloudTrail | 用於記錄 AWS外部事件的 CloudTrail Lake 通道上的 CloudTrail `PutAuditEvents` 活動。 | CloudTrail 頻道 | `AWS::CloudTrail::Channel` |
| Amazon CloudWatch | 指標上的 Amazon CloudWatch API 活動。 | CloudWatch 指標 | `AWS::CloudWatch::Metric` |
| Amazon CloudWatch 網路流量監控 | 監控上的 Amazon CloudWatch Network Flow Monitor API 活動。 | 網路流量監控監視器 | `AWS::NetworkFlowMonitor::Monitor` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon CloudWatch 網路流量監控 | 範圍上的 Amazon CloudWatch Network Flow Monitor API 活動。 | 網路流量監控範圍 | AWS::NetworkFlowMonitor::Scope |
| Amazon CloudWatch RUM | 應用程式監視器上的 Amazon CloudWatch RUM API 活動。 | RUM 應用程式監控 | AWS::RUM::AppMonitor |
| Amazon CodeGuru Profiler | 分析群組上的 CodeGuru Profiler API 活動。 | CodeGuru Profiler 分析群組 | AWS::CodeGuruProfiler::ProfilingGroup |
| Amazon CodeWhisperer | 自訂上的 Amazon CodeWhisperer API 活動。 | CodeWhisperer 自訂 | AWS::CodeWhisperer::Customization |
| Amazon CodeWhisperer | 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 Data Exchange | AWS Data Exchange 資產上的 API 活動。 | Data Exchange 資產 | AWS::DataExchange::Asset |
| Amazon Data Firehose | Amazon Data Firehose 交付串流 API 活動。 | Amazon Data Firehose | AWS::KinesisFirehose::DeliveryStream |
| AWS Deadline Cloud | Deadline Cloud 機群上的 API 活動。 | Deadline Cloud 機群 | AWS::Deadline::Fleet |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| AWS Deadline Cloud | Deadline Cloud 任務上的 API 活動。 | Deadline Cloud 任務 | `AWS::Deadline::Job` |
| AWS Deadline Cloud | Deadline Cloud 佇列上的 API 活動。 | Deadline Cloud 佇列 | `AWS::Deadline::Queue` |
| AWS Deadline Cloud | Deadline Cloud 工作者上的 API 活動。 | Deadline Cloud 工作者 | `AWS::Deadline::Worker` |

| AWS 服務 | Description | 資源類型 (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）。<br><br>**Note**<br>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。 | DynamoDB | `AWS::DynamoDB::Table` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| | 若要排除串流事件，請在 eventName 欄位上新增篩選條件。 | | |
| 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 Elastic Compute Cloud | Amazon EC2 執行個體連接端點 API 活動。 | EC2 執行個體連線端點 | AWS::EC2::InstanceConnectEndpoint |
| Amazon Elastic Container Service | 容器執行個體上的 Amazon Elastic Container Service API 活動。 | ECS 容器執行個體 | AWS::ECS::ContainerInstance |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Elastic Kubernetes Service | 儀表板上的 Amazon Elastic Kubernetes Service API 活動。 | Amazon Elastic Kubernetes Service 儀表板 | `AWS::EKS::Dashboard` |
| Amazon EMR | 預先寫入日誌工作區上的 Amazon EMR API 活動。 | EMR 預寫日誌工作區 | `AWS::EMRWAL::Workspace` |
| AWS 最終使用者傳訊簡訊 | 起始身分上的AWS 最終使用者簡訊 SMS API 活動。 | SMS 語音來源身分 | `AWS::SMSVoice::OriginationIdentity` |
| AWS 最終使用者傳訊簡訊 | 訊息上的最終AWS 使用者簡訊 SMS API 活動。 | SMS 語音訊息 | `AWS::SMSVoice::Message` |
| AWS 最終使用者傳訊社交 | 電話號碼 IDs 上的AWS 最終使用者傳訊社交 API 活動。 | 社交訊息電話號碼 ID | `AWS::SocialMessaging::PhoneNumberId` |
| AWS 最終使用者傳訊社交 | AWS Waba IDs 上的最終使用者傳訊社交 API 活動。 | 社交訊息 Waba ID | `AWS::SocialMessaging::WabaId` |
| Amazon FinSpace | 環境上的 Amazon FinSpace API 活動。 | FinSpace | `AWS::FinSpace::Environment` |
| Amazon GameLift Streams | Amazon GameLift Streams 應用程式上的串流 API 活動。 | GameLift Streams 應用程式 | `AWS::GameLiftStreams::Application` |
| Amazon GameLift Streams | 串流群組上的 Amazon GameLift Streams 串流 API 活動。 | GameLift Streams 串流群組 | `AWS::GameLiftStreams::StreamGroup` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| AWS Glue | AWS Glue Lake Formation 所建立資料表上的 API 活動。 | Lake Formation | `AWS::Glue::Table` |
| Amazon GuardDuty | 偵測器的 Amazon GuardDuty API 活動。 | GuardDuty 偵測器 | `AWS::GuardDuty::Detector` |
| AWS HealthImaging | AWS HealthImaging 資料存放區上的 API 活動。 | MedicalImaging 資料存放區 | `AWS::MedicalImaging::Datastore` |
| AWS HealthImaging | AWS HealthImaging 映像集 API 活動。 | MedicalImaging 影像集 | `AWS::MedicalImaging::ImageSet` |
| AWS IoT | 憑證上的 AWS IoT API 活動。 | IoT 憑證 | `AWS::IoT::Certificate` |
| AWS IoT | 物件上的 AWS IoT API 活動。 | IoT 物件 | `AWS::IoT::Thing` |
| AWS IoT Greengrass Version 2 | 元件版本上來自 Greengrass 核心裝置的 Greengrass API 活動。<br>**Note**<br>Greengrass 不會記錄存取遭拒的事件。 | IoT Greengrass 元件版本 | `AWS::GreengrassV2::ComponentVersion` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| AWS IoT Greengrass Version 2 | 部署上來自 Greengrass 核心裝置的 Greengrass API 活動。<br><br>**Note**<br>Greengrass 不會記錄存取遭拒的事件。 | IoT Greengrass 部署 | `AWS::GreengrassV2::Deployment` |
| AWS IoT SiteWise | 資產上的 IoT SiteWise API 活動。 | IoT SiteWise 資產 | `AWS::IoTSiteWise::Asset` |
| AWS IoT SiteWise | 時間序列上的 IoT SiteWise API 活動。 | IoT SiteWise 時間序列 | `AWS::IoTSiteWise::TimeSeries` |
| AWS IoT SiteWise 助理 | 對話上的 Sitewise Assistant API 活動。 | Sitewise 助理對話 | `AWS::SitewiseAssistant::Conversation` |
| AWS IoT TwinMaker | 實體上的 IoT TwinMaker API 活動。 | IoT TwinMaker 實體 | `AWS::IoTTwinMaker::Entity` |
| AWS IoT TwinMaker | 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` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Keyspaces (適用於 Apache Cassandra) | 資料表上的 Amazon Keyspaces API 活動。 | Cassandra 資料表 | `AWS::Cassandra::Table` |
| Amazon Keyspaces (適用於 Apache Cassandra) | Cassandra CDC 串流上的 Amazon Keyspaces （適用於 Apache Cassandra) API 活動。 | Cassandra CDC 串流 | `AWS::Cassandra::Stream` |
| Amazon Kinesis Data Streams | 串流上的 Kinesis Data Streams API 活動。 | Kinesis 串流 | `AWS::Kinesis::Stream` |
| Amazon Kinesis Data Streams | 串流消費者上的 Kinesis Data Streams API 活動。 | Kinesis 串流消費者 | `AWS::Kinesis::StreamConsumer` |
| Amazon Kinesis Video Streams | 視訊串流上的 Kinesis Video Streams API 活動，例如對 `GetMedia`和 的呼叫`PutMedia`。 | Kinesis 視訊串流 | `AWS::KinesisVideo::Stream` |
| Amazon Kinesis Video Streams | Kinesis Video Streams 影片訊號頻道 API 活動。 | Kinesis 影片訊號頻道 | `AWS::KinesisVideo::SignalingChannel` |
| AWS Lambda | AWS Lambda 函數執行活動 ( `Invoke` API)。 | Lambda | `AWS::Lambda::Function` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Location Maps | Amazon Location Maps API 活動。 | 地理地圖 | `AWS::GeoMaps::Provider` |
| Amazon Location Places | Amazon Location Places API 活動。 | 地理位置 | `AWS::GeoPlaces::Provider` |
| Amazon Location Routes | Amazon Location Routes API 活動。 | 地理路由 | `AWS::GeoRoutes::Provider` |
| Amazon Machine Learning | ML 模型上的Machine Learning API 活動。 | 修補 Learning MlModel | `AWS::MachineLearning::MlModel` |
| Amazon Managed Blockchain | 網路上的 Amazon Managed Blockchain API 活動。 | Managed Blockchain 網路 | `AWS::ManagedBlockchain::Network` |
| Amazon Managed Blockchain | 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 Managed Blockchain Query | Amazon Managed Blockchain Query API 活動。 | 受管區塊鏈查詢 | `AWS::ManagedBlockchainQuery::QueryAPI` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Managed Workflows for Apache Airflow | 環境上的 Amazon MWAA API 活動。 | 受管 Apache Airflow | `AWS::MWAA::Environment` |
| 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` |
| Amazon One Enterprise | UKey 上的 Amazon One Enterprise API 活動。 | Amazon One UKey | `AWS::One::UKey` |
| Amazon One Enterprise | 使用者上的 Amazon One Enterprise API 活動。 | Amazon One 使用者 | `AWS::One::User` |
| AWS Payment Cryptography | AWS Payment Cryptography 別名上的 API 活動。 | 付款密碼編譯別名 | `AWS::PaymentCryptography::Alias` |
| AWS Payment Cryptography | AWS Payment Cryptography 金鑰上的 API 活動。 | 付款密碼編譯金鑰 | `AWS::PaymentCryptography::Key` |
| Amazon Pinpoint | 行動目標應用程式上的 Amazon Pinpoint API 活動。 | 行動目標應用程式 | `AWS::Pinpoint::App` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| AWS 私有 CA | AWS 私有 CA 適用於 Active Directory API 活動的連接器。 | AWS 私有 CA 適用於 Active Directory 的連接器 | `AWS::PCAConnectorAD::Connector` |
| AWS 私有 CA | AWS 私有 CA Connector for SCEP API 活動。 | AWS 私有 CA 適用於 SCEP 的連接器 | `AWS::PCAConnectorSCEP::Connector` |
| Amazon Q Apps | Amazon Q 應用程式上的資料 API 活動。 | Amazon Q 應用程式 | `AWS::QApps::QApp` |
| Amazon Q Apps | Amazon Q App 工作階段上的資料 API 活動。 | Amazon Q 應用程式工作階段 | `AWS::QApps::QAppSession` |
| 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` |
| Amazon Q Business | 資料來源上的 Amazon Q Business API 活動。 | Amazon Q Business 資料來源 | `AWS::QBusiness::DataSource` |
| Amazon Q Business | 索引上的 Amazon Q Business API 活動。 | Amazon Q Business 索引 | `AWS::QBusiness::Index` |
| Amazon Q Business | Web 體驗上的 Amazon Q Business API 活動。 | Amazon Q Business Web 體驗 | `AWS::QBusiness::WebExperience` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Q Business | Amazon Q Business 整合 API 活動。 | Amazon Q Business 整合 | `AWS::QBusiness::Integration` |
| Amazon Q Developer | 整合上的 Amazon Q Developer API 活動。 | Q 開發人員整合 | `AWS::QDeveloper::Integration` |
| Amazon Q Developer | 有關操作調查的 Amazon Q Developer API 活動。 | AIOps 調查群組 | `AWS::AIOps::InvestigationGroup` |
| Amazon Quick | 動作連接器上的 Amazon Quick API 活動。 | AWS QuickSuite 動作 | `AWS::Quicksight::ActionConnector` |
| Amazon Quick | Amazon Quick Flow API 活動。 | QuickSight 流程 | `AWS::QuickSight::Flow` |
| Amazon Quick | Amazon Quick FlowSession API 活動。 | QuickSight 流程工作階段 | `AWS::QuickSight::FlowSession` |
| Amazon SageMaker AI | 端點上的 Amazon SageMaker AI `InvokeEndpointWithResponseStream` 活動。 | SageMaker AI 端點 | `AWS::SageMaker::Endpoint` |
| Amazon SageMaker AI | 功能存放區上的 Amazon SageMaker AI API 活動。 | SageMaker AI 功能存放區 | `AWS::SageMaker::FeatureGroup` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon SageMaker AI | 實驗試驗元件上的 Amazon SageMaker AI API 活動。 | SageMaker AI 指標實驗試驗元件 | `AWS::SageMaker::ExperimentTrialComponent` |
| Amazon SageMaker AI | Amazon SageMaker AI MLflow API 活動。 | SageMaker MLflow | `AWS::SageMaker::MlflowTrackingServer` |
| AWS Signer | 簽署任務時的簽署者 API 活動。 | 簽署者簽署任務 | `AWS::Signer::SigningJob` |
| AWS Signer | 簽署設定檔時的簽署者 API 活動。 | 簽署者簽署設定檔 | `AWS::Signer::SigningProfile` |
| Amazon Simple Email Service | 組態集上的 Amazon Simple Email Service (Amazon SES) API 活動。 | SES 組態設定 | `AWS::SES::ConfigurationSet` |
| Amazon Simple Email Service | 電子郵件身分上的 Amazon Simple Email Service (Amazon SES) API 活動。 | SES 身分 | `AWS::SES::EmailIdentity` |
| Amazon Simple Email Service | 範本上的 Amazon Simple Email Service (Amazon SES) API 活動。 | SES 範本 | `AWS::SES::Template` |
| Amazon SimpleDB | 網域上的 Amazon SimpleDB API 活動。 | SimpleDB 網域 | `AWS::SDB::Domain` |
| AWS Step Functions | Step Functions API 活動。 | 步驟函數 | `AWS::StepFunctions::Activity` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| AWS Step Functions | Step Functions API 在狀態機器上的活動。 | Step Functions 狀態機器 | AWS::StepFunctions::StateMachine |
| AWS Systems Manager | 控制頻道上的 Systems Manager API 活動。 | Systems Manager | AWS::SSMMessages::ControlChannel |
| AWS Systems Manager | 影響評估上的 Systems Manager API 活動。 | SSM 影響評估 | AWS::SSM::ExecutionPreview |
| AWS Systems Manager | 受管節點上的 Systems Manager API 活動。 | Systems Manager 受管節點 | AWS::SSM::ManagedNode |
| Amazon Timestream | 資料庫上的 Amazon Timestream Query API 活動。 | Timestream 資料庫 | AWS::Timestream::Database |
| Amazon Timestream | 區域端點上的 Amazon Timestream API 活動。 | Timestream 區域端點 | AWS::Timestream::RegionalEndpoint |
| Amazon Timestream | 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 精簡型客戶端 | 裝置上的 WorkSpaces 精簡型客戶端 API 活動。 | 精簡型客戶端裝置 | AWS::ThinClient::Device |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon WorkSpaces 精簡型客戶端 | 環境上的 WorkSpaces 精簡型客戶端 API 活動。 | 精簡型客戶端環境 | `AWS::ThinClient::Environment` |
| AWS X-Ray | 追蹤上的 X-Ray API 活動。 | X-Ray 追蹤 | `AWS::XRay::Trace` |
| Amazon AIDevOps | 代理程式空間上的 AIDevOps API 活動。 | 客服人員空間 | `AWS::AIDevOps::AgentSpace` |
| Amazon AIDevOps | 關聯上的 AIDevOps API 活動。 | AIDevOps 關聯 | `AWS::AIDevOps::Association` |
| Amazon AIDevOps | 操作員應用程式團隊上的 AIDevOps API 活動。 | AIDevOps 運算子應用程式團隊 | `AWS::AIDevOps::OperatorAppTeam` |
| Amazon AIDevOps | 管道中繼資料上的 AIDevOps API 活動。 | AIDevOps 管道中繼資料 | `AWS::AIDevOps::PipelineMetadata` |
| Amazon AIDevOps | 服務上的 AIDevOps API 活動。 | AIDevOps 服務 | `AWS::AIDevOps::Service` |
| Amazon Bedrock | 進階最佳化提示任務上的 Bedrock API 活動。 | AdvancedOptimizePromptJob | `AWS::Bedrock::AdvancedOptimizePromptJob` |
| Amazon Bedrock AgentCore | 評估器上的 Bedrock AgentCore API 活動。 | Bedrock-AgentCore 評估器 | `AWS::BedrockAgentCore::Evaluator` |
| Amazon 成本最佳化 | 設定檔上的 CloudOptimization API 活動。 | CloudOptimization 設定檔 | `AWS::CloudOptimization::Profile` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon 成本最佳化 | 建議的 CloudOptimization API 活動。 | CloudOptimization 建議 | AWS::CloudOptimization::Recommendation |
| Amazon GuardDuty | 惡意軟體掃描上的 GuardDuty API 活動。 | GuardDuty 惡意軟體掃描 | AWS::GuardDuty::MalwareScan |
| Amazon NovaAct | 工作流程定義的 Amazon NovaAct API 活動。 | 工作流程定義 | AWS::NovaAct::WorkflowDefinition |
| Amazon NovaAct | 工作流程執行上的 Amanzon NovaAct API 活動。 | 工作流程執行 | AWS::NovaAct::WorkflowRun |
| Amazon Redshift | 叢集上的 Redshift API 活動。 | Amazon Redshift 叢集 | AWS::Redshift::Cluster |
| Amazon Support | 租用戶上的 SupportAccess API 活動。 | SupportAccess 租用戶 | AWS::SupportAccess::Tenant |
| Amazon Support | 信任帳戶的 SupportAccess API 活動。 | SupportAccess 信任帳戶 | AWS::SupportAccess::TrustingAccount |
| Amazon Support | 信任角色的 SupportAccess API 活動。 | SupportAccess 信任角色 | AWS::SupportAccess::TrustingRole |
| Amazon 轉換 | 轉換代理程式執行個體上的 API 活動。 | 轉換代理程式執行個體 | AWS::Transform::AgentInstance |
| Amazon 轉換自訂 | 轉換行銷活動上的自訂 API 活動。 | Transform-Custom 行銷活動 | AWS::TransformCustom::Campaign |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon 轉換自訂 | 在對話上轉換自訂 API 活動。 | 轉換自訂對話 | AWS::TransformCustom::Conversation |
| Amazon 轉換自訂 | 在知識項目上轉換自訂 API 活動。 | Transform-Custom 知識項目 | AWS::TransformCustom::KnowledgeItem |
| Amazon 轉換自訂 | 轉換套件上的自訂 API 活動。 | Transform-Custom 套件 | AWS::TransformCustom::Package |

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 CloudTrail 資料事件，您必須明確地新增欲收集之活動的受支援資源或資源類型。如需詳細資訊，請參閱使用 CloudTrail 主控台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"
}
```

# 網路活動事件

CloudTrail 網路活動事件可讓 VPC 端點擁有者記錄使用其 VPC 端點從私有 VPC 到 的 AWS API 呼叫 AWS 服務。網路活動事件可讓您查看在 VPC 內執行的資源操作。

您可以記錄下列服務的網路活動事件：

- AWS AppConfig
- AWS App Mesh
- Amazon Athena
- AWS B2B 資料交換
- AWS Backup gateway
- Amazon Bedrock
- Billing and Cost Management
- AWS 定價計算工具
- AWS Cost Explorer
- AWS 雲端控制 API
- AWS CloudHSM
- AWS Cloud Map
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- CloudWatch Application Signals
- AWS CodeDeploy
- Amazon Comprehend Medical
- AWS Config
- AWS 資料匯出
- Amazon Data Firehose
- AWS Directory Service
- Amazon DynamoDB
- Amazon EC2

- Amazon Elastic Container Service
- Amazon Elastic File System
- Elastic Load Balancing
- Amazon EventBridge
- Amazon EventBridge 排程器
- Amazon Fraud Detector
- AWS 免費方案
- Amazon FSx
- AWS Glue
- AWS HealthLake
- AWS IoT FleetWise
- AWS IoT Secure Tunneling
- AWS Invoicing
- Amazon Keyspaces (適用於 Apache Cassandra)
- AWS KMS
- AWS Lake Formation
- AWS Lambda
- AWS License Manager
- Amazon Lookout for Equipment
- Amazon Lookout for Vision
- Amazon Personalize
- Amazon Q Business
- Amazon Rekognition
- Amazon Relational Database Service
- Amazon S3

> **Note**
>
> 不支援 Amazon S3 多區域存取點。

- Amazon SageMaker AI

- AWS Secrets Manager
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Workflow Service
- AWS Storage Gateway
- AWS Systems Manager Incident Manager
- Amazon Textract
- Amazon Transcribe
- Amazon Translate
- AWS Transform
- Amazon Verified Permissions
- Amazon WorkMail

當您建立線索或事件資料存放區時，預設不會記錄網路活動事件。若要記錄 CloudTrail 網路活動事件，您必須明確設定要收集活動的事件來源。如需詳細資訊，請參閱記錄網路活動事件。

記錄網路活動事件需支付額外費用。如需 CloudTrail 定價，請參閱 AWS CloudTrail 定價。

下列範例顯示周遊 VPC 端點的成功 AWS KMS `ListKeys`事件。`vpcEndpointId` 欄位會顯示 VPC 端點的 ID。`vpcEndpointAccountId` 欄位會顯示 VPC 端點擁有者的帳戶 ID。在此範例中，請求是由 VPC 端點擁有者提出。


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "ASIAIOSFODNN7EXAMPLE:role-name",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/role-name",
        "accountId": "123456789012",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "ASIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
```

```
            },
            "attributes": {
                "creationDate": "2024-06-04T23:10:46Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-06-04T23:12:50Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ListKeys",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "requestID": "16bcc089-ac49-43f1-9177-EXAMPLE23731",
    "eventID": "228ca3c8-5f95-4a8a-9732-EXAMPLE60ed9",
    "eventType": "AwsVpceEvent",
    "recipientAccountId": "123456789012",
    "sharedEventID": "a1f3720c-ef19-47e9-a5d5-EXAMPLE8099f",
    "vpcEndpointId": "vpce-EXAMPLE08c1b6b9b7",
    "vpcEndpointAccountId": "123456789012",
    "eventCategory": "NetworkActivity"
}
```

下一個範例顯示 VPC 端點政策違規的失敗 AWS KMS `ListKeys`事件。由於發生 VPC 政策違規，因此 `errorCode`和 `errorMessage` 欄位都存在。`recipientAccountId` 和 `vpcEndpointAccountId` 欄位中的帳戶 ID 相同，這表示事件已傳送至 VPC 端點擁有者。`userIdentity` 元素`accountId`中的 不是 `vpcEndpointAccountId`，這表示提出請求的使用者不是 VPC 端點擁有者。

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSAccount",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "accountId": "777788889999"
    },
    "eventTime": "2024-07-15T23:57:12Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ListKeys",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "errorCode": "VpceAccessDenied",
    "errorMessage": "The request was denied due to a VPC endpoint policy",
```

```
    "requestID": "899003b8-abc4-42bb-ad95-EXAMPLE0c374",
    "eventID": "7c6e3d04-0c3b-42f2-8589-EXAMPLE826c0",
    "eventType": "AwsVpceEvent",
    "recipientAccountId": "123456789012",
    "sharedEventID": "702f74c4-f692-4bfd-8491-EXAMPLEb1ac4",
    "vpcEndpointId": "vpce-EXAMPLE08c1b6b9b7",
    "vpcEndpointAccountId": "123456789012",
    "eventCategory": "NetworkActivity"
}
```

# Insights 事件

CloudTrail Insights 事件會透過分析 CloudTrail 管理活動，擷取您的 AWS 帳戶中的異常 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的事件不同，只有在 CloudTrail 偵測到帳戶 API 使用情況或錯誤率記錄變化，且與帳戶的一般使用模式有很大差異時，才會記錄 Insights 事件。如需詳細資訊，請參閱使用 CloudTrail Insights。

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 使用 CloudTrail 主控台建立追蹤。如需有關建立事件資料存放區的詳細資訊，請參閱 使用主控台建立 Insights 事件的事件資料存放區。

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。

CloudTrail Insights 中會記錄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 追蹤的 Insights 事件 CloudTrail 記錄內容。


```
{
        "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
- 讀取和寫入事件
- 使用 記錄管理事件 AWS 管理主控台
  - 更新現有追蹤的管理事件設定
  - 更新現有事件資料存放區的管理事件設定
- 使用 記錄管理事件 AWS CLI
  - 範例：記錄追蹤的管理事件
    - 範例：使用進階事件選取器記錄線索的管理事件
    - 範例：使用基本事件選取器記錄線索的管理事件
  - 範例：記錄事件資料存放區的管理事件
    - 範例：排除 AWS KMS 管理事件
    - 範例：排除 Amazon RDS 管理事件
    - 範例：從 AWS 管理主控台 工作階段排除 AWS 服務 事件和事件
    - 範例：排除特定 IAM 身分的管理事件
- 使用 AWS SDKs 記錄管理事件


## 管理事件

管理事件可讓您查看在 AWS 帳戶中資源上執行的管理操作。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 API AWS CloudTrail `CreateTrail` 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，CloudTrail 就會記錄 `ConsoleLogin` 事件。如需詳細資訊，請參閱CloudTrail 擷取的非 API 事件。

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 Event history (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 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。

## 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 `amzn-s3-demo-bucket1` 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 `amzn-s3-demo-bucket2` 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 並將事件交付至 `amzn-s3-demo-bucket1`。
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 並將事件交付至 `amzn-s3-demo-bucket2`。

# 使用 記錄管理事件 AWS 管理主控台

本節說明如何更新現有線索或事件資料存放區的管理事件設定。

主題


- 更新現有追蹤的管理事件設定
- 更新現有事件資料存放區的管理事件設定


## 更新現有追蹤的管理事件設定

使用下列程序更新現有線索的管理事件設定。

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
2. 開啟 CloudTrail 主控台的線索頁面，選擇線索名稱。
3. 針對管理活動，選擇 Edit (編輯)。
   - 如果您想要記錄讀取事件、寫入事件或兩者都記錄，請選擇 。
   - 選擇排除 AWS KMS 事件以篩選出 traiL 中的 AWS Key Management Service (AWS KMS) 事件。預設設定為包含所有 AWS KMS 事件。

     只有在您的線索上記錄管理 AWS KMS 事件時，才提供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 `Encrypt`、 `Decrypt`和 等動作`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。少量的相關 AWS KMS 動作，例如 `Disable`、 `Delete`和 `ScheduleKey` （通常少於 AWS KMS 事件磁碟區的 0.5%) 會記錄為寫入事件。

     若要排除大量事件`Decrypt`，例如 `Encrypt`、 和 `GenerateDataKey`，但仍會記錄相關事件，例如 `Disable`、 `Delete`和 `ScheduleKey`，請選擇記錄寫入管理事件，並清除排除 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。
4. 完成時，請選擇儲存變更。

## 更新現有事件資料存放區的管理事件設定

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
2. 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. 針對管理事件，選擇編輯，然後設定下列設定：

   a. 選擇簡易事件集合或進階事件集合：

      - 如果您想要記錄所有事件、僅記錄讀取事件或僅記錄寫入事件，請選擇簡單事件集合。您也可以選擇排除 AWS Key Management Service 和 Amazon RDS Data API 管理事件。
      - 如果您想要根據進階事件選取器欄位的值包含或排除管理事件，包括 、、 和 欄位，請選擇進階事件集合。 `eventName` `eventType` `eventSource` `userIdentity.arn`

   b. 如果您選擇簡易事件集合，請選擇您是否要記錄所有事件、僅記錄讀取事件，或僅記錄寫入事件。您也可以選擇排除 AWS KMS 和 Amazon RDS 管理事件。

   c. 如果您選取進階事件集合，請進行下列選擇：

      i. 在日誌選取器範本中，選擇預先定義的範本，或選擇自訂以根據進階事件選取器欄位值建置自訂組態。

         您可以從下列預先定義的範本中選擇：

         - 記錄所有事件：選擇此範本記錄所有事件。
         - 僅記錄讀取事件 – 選擇此範本以僅記錄讀取事件。唯讀事件是不會變更資源狀態的事件，例如 `Get*`或 `Describe*`事件。
         - 僅記錄寫入事件 – 選擇此範本以僅記錄寫入事件。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。
         - 僅記錄 AWS 管理主控台 事件 – 選擇此範本僅記錄源自 的事件 AWS 管理主控台。
         - 排除 AWS 服務 啟動的事件 – 選擇此範本以排除具有 `eventType`之 AWS 服務 的事件`AwsServiceEvent`，以及使用連結角色 (SLRs) AWS 服務啟動的事件。

      ii. (選用) 在選取器名稱中，輸入用於識別選取器的名稱。選擇器名稱是進階事件選擇器的描述性名稱，例如「從 AWS 管理主控台 工作階段記錄管理事件」。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。

      iii. 如果您選擇自訂，在進階事件選取器中會根據進階事件選取器欄位值建立表達式。

> **Note**
>
> 選取器不支援使用萬用字元，例如 * 。若要將多個值與單一條件比對，您可以使用 StartsWith、NotStartsWith、 EndsWith或 NotEndsWith來明確比對事件欄位的開頭或結尾。

A. 從下列欄位選取。

- **readOnly** – readOnly 可設定為等於 true或 的值false。設定為 時false，事件資料存放區會記錄唯讀管理事件。唯讀管理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。若要同時記錄讀取和寫入事件，請勿新增readOnly選取器。
- **eventName** – eventName 可以使用任何運算子。您可以使用它來包含或排除任何管理事件，例如 CreateAccessPoint或 GetAccessPoint。
- **userIdentity.arn** – 包含或排除特定 IAM 身分所採取動作的事件。如需更多詳細資訊，請參閱 CloudTrail userIdentity 元素。
- **sessionCredentialFromConsole** – 包含或排除源自 AWS 管理主控台 工作階段的事件。此欄位可以設定為等於或不等於 的值true。
- **eventSource** – 您可以使用它來包含或排除特定事件來源。eventSource 通常是簡短形式的服務名稱，不含空格加 .amazonaws.com。例如，您可以將eventSource等於 設定為僅ec2.amazonaws.com記錄 Amazon EC2 管理事件。
- **eventType** – 要包含或排除的 eventType。例如，您可以將此欄位設定為不等於AwsServiceEvent排除AWS 服務 事件。

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。

如需有關 CloudTrail 如何評估多個條件的資訊，請參閱 CloudTrail 如何評估欄位的多項條件。

> **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。

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

d. 選擇啟用 Insights 事件擷取以啟用 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. 選擇將記錄 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。

4. 完成時，請選擇儲存變更。

## 使用 記錄管理事件 AWS CLI

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線索的管理事件
- 範例：使用基本事件選取器記錄線索的管理事件

範例：使用進階事件選取器記錄線索的管理事件

下列範例會為名為 *TrailName* 的線索建立進階事件選取器，以包含唯讀和唯寫管理事件（省略`readOnly`選取器），但排除 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，因此如果您有一個以上的線索擷取管理事件，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 事件記錄到線索，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"] }
```

```
    ]
  }
]'
```

下一個範例會為名為 *TrailName* 的線索建立進階事件選取器，以包含唯讀和唯寫管理事件（省略選取`readOnly`器），但會排除 Amazon RDS Data API 管理事件。若要排除 Amazon RDS Data API 管理事件，請在 `eventSource` 欄位的字串值中指定 Amazon RDS Data 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 Data API 管理事件，而且您無法變更 Amazon RDS Data API 事件記錄設定。

若要再次開始將 Amazon RDS Data API 管理事件記錄到線索，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線索的管理事件

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:::amzn-s3-demo-bucket/prefix",
 "arn:aws:s3:::amzn-s3-demo-bucket2/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:::amzn-s3-demo-bucket/prefix",
                        "arn:aws:s3:::amzn-s3-demo-bucket2/prefix2",
                    ]
                }
            ],
            "ExcludeManagementEventSources": []
        }
    ]
}
```

若要從線索日誌中排除 AWS Key Management Service (AWS KMS) 事件，請執行 `put-event-selectors`命令，並新增值`ExcludeManagementEventSources`為 的 屬性`kms.amazonaws.com`。下列範例會為名為 *TrailName* 的線索建立事件選取器，以包含唯讀和唯寫管理事件，但排除 AWS KMS 事件。由於 AWS KMS 可以產生大量事件，因此此範例中的使用者可能想要限制事件以管理線索的成本。

```
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"
            ]
        }
    ]
```

```
}
```

若要從線索的日誌中排除 Amazon RDS Data API 管理事件，請執行 `put-event-selectors`命令，並新增值`ExcludeManagementEventSources`為 的 屬性`rdsdata.amazonaws.com`。下列範例會為名為 *TrailName* 的線索建立事件選取器，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"
            ]
        }
    ]
}
```

若要再次開始記錄 AWS KMS 或 Amazon RDS Data API 管理事件至線索，請將空字串傳遞為 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 `Disable`、 `Delete`和 等線索`ScheduleKey`，但排除 `Encrypt`、`Decrypt`和 等大量 AWS KMS 事件`GenerateDataKey`、記錄唯寫管理事件，並保留預設設定以記錄 AWS KMS 事件，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

您可以透過設定進階事件選取器來記錄事件資料存放區的管理事件。

在事件資料存放區上記錄管理事件時，支援下列進階事件選取器欄位：

- **eventCategory** – 您必須Management將eventCategory等於 設定為日誌管理事件。此為必要欄位。
- **readOnly** – readOnly 可以設定為 Equals true或 的值false。設定為 時false，事件資料存放區會記錄唯讀管理事件。唯讀管理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。若要同時記錄讀取和寫入事件，請勿新增readOnly選取器。
- **eventName** – eventName 可以使用任何運算子。您可以使用它來包含或排除任何管理事件，例如CreateAccessPoint或 GetAccessPoint。您可以搭配此欄位使用任何運算子。
- **userIdentity.arn** – 包含或排除特定 IAM 身分所採取動作的事件。如需更多詳細資訊，請參閱CloudTrail userIdentity 元素。
- **sessionCredentialFromConsole** – 包含或排除源自 AWS 管理主控台 工作階段的事件。此欄位可以設定為等於或NotEquals值為 true。
- **eventSource** – 您可以使用它來包含或排除特定事件來源。eventSource 通常是簡短形式的服務名稱，不含空格加 .amazonaws.com。例如，您可以將 eventSource Equals 設定為ec2.amazonaws.com，以僅記錄 Amazon EC2 管理事件。
- **eventType** – 要包含或排除的 eventType。例如，您可以將此欄位設定為NotEqualsAwsServiceEvent以排除AWS 服務 事件。您可以搭配此欄位使用任何運算子。

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"
}
```

範例：

- 範例：排除 AWS KMS 管理事件
- 範例：排除 Amazon RDS 管理事件
- 範例：從 AWS 管理主控台 工作階段排除 AWS 服務 事件和事件
- 範例：排除特定 IAM 身分的管理事件

範例：排除 AWS KMS 管理事件

若要建立排除 AWS Key Management Service (AWS KMS) 事件的事件資料存放區，請執行 `create-event-data-store`命令並指定 `eventSource` 不等於 `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，但不包括 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"
}
```

範例：排除 Amazon RDS 管理事件

若要建立排除 Amazon RDS Data 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` 不等於 `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"
}
```

範例：從 AWS 管理主控台 工作階段排除 AWS 服務 事件和事件

下列範例會建立事件資料存放區，記錄管理事件，但排除源自 AWS 管理主控台 工作階段 AWS 服務的事件和事件。

```
aws cloudtrail create-event-data-store --name event-data-store-name --advanced-event-
selectors '[
    {
        "Name": "Exclude AWS ## and console events",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "eventType","NotEquals": ["AwsServiceEvent"]},
            {"Field": "sessionCredentialFromConsole","NotEquals": ["true"]}
        ]
    }
]'
```

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": "Exclude AWS ## and console events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                },
                {
                    "Field": "eventType",
                    "NotEquals": [
                        "AwsServiceEvent"
                    ]
                },
                {
                    "Field": "sessionCredentialFromConsole",
                    "NotEquals": [
                        "true"
                    ]
                }
            ]
        }
```

```
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2024-11-13T17:02:02.241000+00:00"
}
```

範例：排除特定 IAM 身分的管理事件

下列範例會建立記錄管理事件的事件資料存放區，但會排除 所產生的事件bucket-scanner-roleuserIdentity。

```
aws cloudtrail create-event-data-store --name event-data-store-name --advanced-event-
selectors '[
    {
        "Name": "Exclude events generated by bucket-scanner-role userIdentity",
        "FieldSelectors": [
            {"Field": "eventCategory","Equals": ["Management"]},
            {"Field": "userIdentity.arn","NotStartsWith":
 ["arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"]}
        ]
    }
]'
```

以下是回應範例。

```
{
    "EventDataStoreArn": "arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/
EXAMPLE-f852-4e8f-8bd1-bcf6cEXAMPLE",
    "Name": "event-data-store-name",
    "Status": "CREATED",
    "AdvancedEventSelectors": [
        {
            "Name": "Exclude events generated by bucket-scanner-role userIdentity",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
```

```
                    ]
                },
                {
                    "Field": "userIdentity.arn",
                    "NotStartsWith": [
                        "arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-11-13T17:02:02.067000+00:00",
    "UpdatedTimestamp": "2024-11-13T17:02:02.241000+00:00"
}
```

## 使用 AWS SDKs 記錄管理事件

使用 GetEventSelectors 操作查看您的線索是否為線索記錄管理事件。您可以使用 PutEventSelectors 操作，設定您的線索來記錄管理事件。如需詳細資訊，請參閱 AWS CloudTrail API 參考。

執行 GetEventDataStore 操作以檢視您的事件資料存放區是否包括管理事件。您可以透過執行 CreateEventDataStore 或 UpdateEventDataStore 操作，設定您的事件資料存放區以包括管理事件。如需詳細資訊，請參閱使用 建立、更新和管理事件資料存放區 AWS CLI和 AWS CloudTrail API 參考。

# 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 儲存貯體中物件的 Amazon S3 物件層級 API 活動（例如 DeleteObject、 GetObject和 PutObject API 操作）。 S3
- AWS Lambda 函數執行活動（Invoke API)。
- 用於記錄 AWS外部事件的 CloudTrail Lake 通道上的 CloudTrail PutAuditEvents 活動。
- 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選取器，這可協助您僅記錄使用案例的特定關注事件來控制成本。例如，您可以使用進階事件選取器，透過在 eventName 欄位中新增篩選條件來記錄特定 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**
>
> 您的追蹤所記錄的事件可在 Amazon EventBridge 中取得。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 EventBridge 中取得。如需詳細資訊，請參閱《Amazon EventBridge 使用者指南》中的AWS 透過 CloudTrail 交付的服務事件和AWS 事件參考。

內容


- 資料事件
  - 支援的資料事件 AWS CloudTrail
  - 範例：記錄 Amazon S3 物件的資料事件
  - 記錄其他 AWS 帳戶中 S3 物件的資料事件
- 唯讀和唯寫事件
- 使用 記錄資料事件 AWS 管理主控台
- 使用 記錄資料事件 AWS Command Line Interface
  - 使用 記錄線索的資料事件 AWS CLI
    - 使用進階事件選取器記錄線索的資料事件
    - 使用進階Amazon S3事件選取器記錄 Amazon S3 儲存貯體的所有 Amazon S3 事件
    - 使用進階 AWS Outposts 事件選取器在事件上記錄 Amazon S3
    - 使用基本事件選取器記錄事件
  - 使用 記錄事件資料存放區的資料事件 AWS CLI
    - 包含特定儲存貯體的所有 Amazon S3 事件

        - 在 AWS Outposts 事件上包含 Amazon S3
- 使用進階事件選取器篩選資料事件
  - CloudTrail 如何評估欄位的多項條件
    - 顯示 resources.ARN 欄位多個條件的範例
  - AWS CLI 用於篩選資料事件的範例
    - 範例 1：篩選 eventName 欄位
    - 範例 2：篩選 resources.ARN和 userIdentity.arn 欄位
    - 範例 3：篩選 resources.type和 eventName 欄位以排除由 Amazon S3 DeleteObjects 事件刪除的個別物件
- 彙總資料事件
  - 使用主控台啟用資料事件的彙總
  - 使用 啟用資料事件的彙總 AWS CLI
    - 範例：API_ACTIVITY 彙總事件
    - 範例：RESOURCE_ACCESS 彙總事件
- 記錄資料事件以實現 AWS Config 合規
- 使用 AWS SDKs 記錄資料事件


# 資料事件

下表顯示線索和事件資料存放區可用的資源類型。資源類型（主控台）欄會在主控台中顯示適當的選擇。resources.type 值欄會顯示您要指定的`resources.type`值，以使用 AWS CLI 或 CloudTrail APIs 在線索或事件資料存放區中包含該類型的資料事件。

對於線索，您可以使用基本或進階事件選取器，在一般用途儲存貯體、Lambda 函數和 DynamoDB 資料表（顯示於資料表的前三列）中記錄 Amazon S3 物件的資料事件。您只能使用進階事件選取器來記錄剩餘資料列中顯示的資源類型。

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。

# 支援的資料事件 AWS CloudTrail

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon RDS | 資料庫叢集上的 Amazon RDS API 活動。 | RDS 資料 API - 資料庫叢集 | `AWS::RDS::DBCluster` |
| Amazon S3 | 一般用途儲存貯體中物件的 Amazon S3 物件層級 API 活動（例如 `DeleteObject`、`GetObject` 和 `PutObject` API 操作）。 | S3 | `AWS::S3::Object` |
| Amazon S3 | 存取點上的 Amazon S3 API 活動。 | S3 存取點 | `AWS::S3::AccessPoint` |
| Amazon S3 | 目錄儲存貯體中物件的 Amazon S3 物件層級 API 活動（例如 `DeleteObject`、`GetObject` 和 `PutObject` API 操作）。 | S3 Express | `AWS::S3Express::Object` |
| Amazon S3 | Amazon S3 Object Lambda 存取點 API 活動，例如對 `CompleteMultipartUpload` 和 的呼叫`GetObject` 。 | S3 Object Lambda | `AWS::S3ObjectLambda::AccessPoint` |
| Amazon S3 | 磁碟區上的 Amazon FSx API 活動。 | FSx 磁碟區 | `AWS::FSx::Volume` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon S3 Tables | 資料表上的 Amazon S3 API 活動。 | S3 資料表 | `AWS::S3Tables::Table` |
| Amazon S3 Tables | 資料表儲存貯體上的 Amazon S3 API 活動。 | S3 資料表儲存貯體 | `AWS::S3Tables::TableBucket` |
| Amazon S3 Vectors | 向量儲存貯體上的 Amazon S3 API 活動。 | S3 向量儲存貯體 | `AWS::S3Vectors::VectorBucket` |
| Amazon S3 Vectors | 向量索引上的 Amazon S3 API 活動。 | S3 向量索引 | `AWS::S3Vectors::Index` |
| Amazon S3 on Outposts | Outposts 上 Amazon S3 物件層級的 API 活動。 | S3 Outposts | `AWS::S3Outposts::Object` |
| Amazon SNS | 平台端點上的 Amazon SNS `Publish` API 操作。 | SNS 平台端點 | `AWS::SNS::PlatformEndpoint` |
| Amazon SNS | 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 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 | `AWS::SWF::Domain` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| AWS AppConfig | 組態操作的 AWS AppConfig API 活動，例如呼叫 StartConfiguration Session 和 GetLatest Configuration 。 | AWS AppConfig | AWS::AppConfig::Configuration |
| AWS AppSync | AppSync GraphQL API APIs AWS AppSync 活動。 | AppSync GraphQL | AWS::AppSync::GraphQLApi |
| Amazon Aurora DSQL | 叢集資源上的 Amazon Aurora DSQL API 活動。 | Amazon Aurora DSQL | AWS::DSQL::Cluster |
| AWS B2B 資料交換 | 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 Backup | AWS Backup 在搜尋任務上搜尋資料 API 活動。 | AWS Backup 搜尋資料 APIs | AWS::Backup::SearchJob |
| 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 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Bedrock | 非同步調用上的 Amazon Bedrock API 活動。 | Bedrock 非同步調用 | AWS::Bedrock::AsyncInvoke |
| Amazon Bedrock | 流程別名上的 Amazon Bedrock API 活動。 | Bedrock 流程別名 | AWS::Bedrock::FlowAlias |
| Amazon Bedrock | 護欄上的 Amazon Bedrock API 活動。 | Bedrock 護欄 | AWS::Bedrock::Guardrail |
| Amazon Bedrock | 內嵌代理程式上的 Amazon Bedrock API 活動。 | Bedrock 調用內嵌代理程式 | AWS::Bedrock::InlineAgent |
| Amazon Bedrock | 知識庫中的 Amazon Bedrock API 活動。 | Bedrock 知識庫 | AWS::Bedrock::KnowledgeBase |
| Amazon Bedrock | 模型上的 Amazon Bedrock API 活動。 | Bedrock 模型 | AWS::Bedrock::Model |
| Amazon Bedrock | 提示上的 Amazon Bedrock API 活動。 | Bedrock 提示 | AWS::Bedrock::PromptVersion |
| Amazon Bedrock | 工作階段上的 Amazon Bedrock API 活動。 | Bedrock 工作階段 | AWS::Bedrock::Session |
| Amazon Bedrock | 流程執行上的 Amazon Bedrock API 活動。 | Bedrock 流程執行 | AWS::Bedrock::FlowExecution |
| Amazon Bedrock | 自動推理政策上的 Amazon Bedrock API 活動。 | Bedrock 自動化推理政策 | AWS::Bedrock::AutomatedReasoningPolicy |
| Amazon Bedrock | 自動推理政策版本的 Amazon Bedrock API 活動。 | Bedrock 自動化推理政策版本 | AWS::Bedrock::AutomatedReasoningPolicyVersion |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Bedrock | Amazon Bedrock 資料自動化專案 API 活動。 | Bedrock 資料自動化專案 | `AWS::Bedrock::DataAutomationProject` |
| Amazon Bedrock | Bedrock 資料自動化調用 API 活動。 | Bedrock 資料自動化調用 | `AWS::Bedrock::DataAutomationInvocation` |
| Amazon Bedrock | Amazon Bedrock 資料自動化設定檔 API 活動。 | Bedrock 資料自動化設定檔 | `AWS::Bedrock::DataAutomationProfile` |
| Amazon Bedrock | Amazon Bedrock 藍圖 API 活動。 | Bedrock 藍圖 | `AWS::Bedrock::Blueprint` |
| Amazon Bedrock | Amazon Bedrock Code-Interpreter API 活動。 | Bedrock-AgentCore Code-Interpreter | `AWS::BedrockAgentCore::CodeInterpreter` |
| Amazon Bedrock | Amazon Bedrock 瀏覽器 API 活動。 | Bedrock-AgentCore 瀏覽器 | `AWS::BedrockAgentCore::Browser` |
| Amazon Bedrock | Amazon Bedrock 工作負載身分 API 活動。 | Bedrock-AgentCore 工作負載身分 | `AWS::BedrockAgentCore::WorkloadIdentity` |
| Amazon Bedrock | Amazon Bedrock 工作負載身分目錄 API 活動。 | Bedrock-AgentCore 工作負載身分目錄 | `AWS::BedrockAgentCore::WorkloadIdentityDirectory` |
| Amazon Bedrock | Amazon Bedrock Token Vault API 活動。 | Bedrock-AgentCore 字符保存庫 | `AWS::BedrockAgentCore::TokenVault` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Bedrock | Amazon Bedrock APIKey CredentialProvider API 活動。 | Bedrock-AgentCore APIKey CredentialProvider | `AWS::BedrockAgentCore::APIKeyCredentialProvider` |
| Amazon Bedrock | Amazon Bedrock 執行期 API 活動。 | Bedrock-AgentCore 執行期 | `AWS::BedrockAgentCore::Runtime` |
| Amazon Bedrock | Amazon Bedrock Runtime-Endpoint API 活動。 | Bedrock-AgentCore 執行時間端點 | `AWS::BedrockAgentCore::RuntimeEndpoint` |
| Amazon Bedrock | Amazon Bedrock Gateway API 活動。 | Bedrock-AgentCore 閘道 | `AWS::BedrockAgentCore::Gateway` |
| Amazon Bedrock | Amazon Bedrock 記憶體 API 活動。 | Bedrock-AgentCore 記憶體 | `AWS::BedrockAgentCore::Memory` |
| Amazon Bedrock | Amazon Bedrock Oauth2 CredentialProvider API 活動。 | Bedrock-AgentCore Oauth2 CredentialProvider | `AWS::BedrockAgentCore::OAuth2CredentialProvider` |
| Amazon Bedrock | Amazon Bedrock 瀏覽器自訂 API 活動。 | Bedrock-AgentCore 瀏覽器自訂 | `AWS::BedrockAgentCore::BrowserCustom` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Bedrock | Amazon Bedrock Code-Interpreter-Custom API 活動。 | Bedrock-AgentCore Code-Interpreter-Custom | `AWS::BedrockAgentCore::CodeInterpreterCustom` |
| Amazon Bedrock | Amazon Bedrock Tool API 活動。 | Bedrock 工具 | `AWS::Bedrock::Tool` |
| AWS Cloud Map | 命名空間上的 AWS Cloud Map API 活動。 | AWS Cloud Map 命名空間 | `AWS::ServiceDiscovery::Namespace` |
| AWS Cloud Map | 服務上的 AWS Cloud Map API 活動。 | AWS Cloud Map 服務 | `AWS::ServiceDiscovery::Service` |
| Amazon CloudFront | KeyValueStore 上的 CloudFront API 活動。 | CloudFront KeyValueStore | `AWS::CloudFront::KeyValueStore` |
| AWS CloudTrail | 用於記錄 AWS外部事件的 CloudTrail Lake 通道上的 CloudTrail `PutAuditEvents` 活動。 | CloudTrail 頻道 | `AWS::CloudTrail::Channel` |
| Amazon CloudWatch | 指標上的 Amazon CloudWatch API 活動。 | CloudWatch 指標 | `AWS::CloudWatch::Metric` |
| Amazon CloudWatch 網路流量監控 | 監控上的 Amazon CloudWatch Network Flow Monitor API 活動。 | 網路流量監控監視器 | `AWS::NetworkFlowMonitor::Monitor` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon CloudWatch 網路流量監控 | 範圍上的 Amazon CloudWatch Network Flow Monitor API 活動。 | 網路流量監控範圍 | `AWS::NetworkFlowMonitor::Scope` |
| Amazon CloudWatch RUM | 應用程式監視器上的 Amazon CloudWatch RUM API 活動。 | RUM 應用程式監控 | `AWS::RUM::AppMonitor` |
| Amazon CodeGuru Profiler | 分析群組上的 CodeGuru Profiler API 活動。 | CodeGuru Profiler 分析群組 | `AWS::CodeGuruProfiler::ProfilingGroup` |
| Amazon CodeWhisperer | 自訂上的 Amazon CodeWhisperer API 活動。 | CodeWhisperer 自訂 | `AWS::CodeWhisperer::Customization` |
| Amazon CodeWhisperer | 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 Data Exchange | AWS Data Exchange 資產上的 API 活動。 | 資料交換資產 | `AWS::DataExchange::Asset` |
| Amazon Data Firehose | Amazon Data Firehose 交付串流 API 活動。 | Amazon Data Firehose | `AWS::KinesisFirehose::DeliveryStream` |
| AWS Deadline Cloud | Deadline Cloud 機群上的 API 活動。 | Deadline Cloud 機群 | `AWS::Deadline::Fleet` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| AWS Deadline Cloud | Deadline Cloud 任務上的 API 活動。 | Deadline Cloud 任務 | `AWS::Deadline::Job` |
| AWS Deadline Cloud | Deadline Cloud 佇列上的 API 活動。 | Deadline Cloud 佇列 | `AWS::Deadline::Queue` |
| AWS Deadline Cloud | Deadline Cloud 工作者上的 API 活動。 | Deadline Cloud 工作者 | `AWS::Deadline::Worker` |

| AWS 服務 | Description | 資源類型 (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）。<br><br>**Note**<br>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。 | DynamoDB | `AWS::DynamoDB::Table` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| | 若要排除串流事件，請在 eventName 欄位上新增篩選條件。 | | |
| 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 Elastic Compute Cloud | Amazon EC2 執行個體連接端點 API 活動。 | EC2 執行個體連線端點 | AWS::EC2::InstanceConnectEndpoint |
| Amazon Elastic Container Service | 容器執行個體上的 Amazon Elastic Container Service API 活動。 | ECS 容器執行個體 | AWS::ECS::ContainerInstance |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Elastic Kubernetes Service | 儀表板上的 Amazon Elastic Kubernetes Service API 活動。 | Amazon Elastic Kubernetes Service 儀表板 | `AWS::EKS::Dashboard` |
| Amazon EMR | 預先寫入日誌工作區上的 Amazon EMR API 活動。 | EMR 預寫日誌工作區 | `AWS::EMRWAL::Workspace` |
| AWS 最終使用者傳訊簡訊 | 起始身分上的AWS 最終使用者簡訊 SMS API 活動。 | SMS 語音起始身分 | `AWS::SMSVoice::OriginationIdentity` |
| AWS 最終使用者傳訊簡訊 | 訊息上的最終AWS 使用者簡訊 SMS API 活動。 | SMS 語音訊息 | `AWS::SMSVoice::Message` |
| AWS 最終使用者傳訊社交 | 電話號碼 IDs 上的AWS 最終使用者傳訊社交 API 活動。 | 社交訊息電話號碼 ID | `AWS::SocialMessaging::PhoneNumberId` |
| AWS 最終使用者傳訊社交 | AWS Waba IDs 上的最終使用者傳訊社交 API 活動。 | 社交訊息 Waba ID | `AWS::SocialMessaging::WabaId` |
| Amazon FinSpace | 環境上的 Amazon FinSpace API 活動。 | FinSpace | `AWS::FinSpace::Environment` |
| Amazon GameLift Streams | Amazon GameLift Streams 串流應用程式上的 API 活動。 | GameLift Streams 應用程式 | `AWS::GameLiftStreams::Application` |
| Amazon GameLift Streams | 串流群組上的 Amazon GameLift Streams 串流 API 活動。 | GameLift Streams 串流群組 | `AWS::GameLiftStreams::StreamGroup` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| AWS Glue | AWS Glue Lake Formation 所建立資料表上的 API 活動。 | Lake Formation | `AWS::Glue::Table` |
| Amazon GuardDuty | 偵測器的 Amazon GuardDuty API 活動。 | GuardDuty 偵測器 | `AWS::GuardDuty::Detector` |
| AWS HealthImaging | AWS HealthImaging 資料存放區上的 API 活動。 | MedicalImaging 資料存放區 | `AWS::MedicalImaging::Datastore` |
| AWS HealthImaging | AWS HealthImaging 映像集 API 活動。 | MedicalImaging 影像集 | `AWS::MedicalImaging::ImageSet` |
| AWS IoT | 憑證上的 AWS IoT API 活動。 | IoT 憑證 | `AWS::IoT::Certificate` |
| AWS IoT | 物件上的 AWS IoT API 活動。 | IoT 物件 | `AWS::IoT::Thing` |
| AWS IoT Greengrass Version 2 | 元件版本上來自 Greengrass 核心裝置的 Greengrass API 活動。<br>**Note**<br>Greengrass 不會記錄存取遭拒的事件。 | IoT Greengrass 元件版本 | `AWS::GreengrassV2::ComponentVersion` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| AWS IoT Greengrass Version 2 | 部署上來自 Greengrass 核心裝置的 Greengrass API 活動。<br><br>**Note**<br>Greengrass 不會記錄存取遭拒的事件。 | IoT Greengrass 部署 | `AWS::GreengrassV2::Deployment` |
| AWS IoT SiteWise | 資產上的 IoT SiteWise API 活動。 | IoT SiteWise 資產 | `AWS::IoTSiteWise::Asset` |
| AWS IoT SiteWise | 時間序列上的 IoT SiteWise API 活動。 | IoT SiteWise 時間序列 | `AWS::IoTSiteWise::TimeSeries` |
| AWS IoT SiteWise 助理 | 對話上的 Sitewise Assistant API 活動。 | Sitewise 助理對話 | `AWS::SitewiseAssistant::Conversation` |
| AWS IoT TwinMaker | 實體上的 IoT TwinMaker API 活動。 | IoT TwinMaker 實體 | `AWS::IoTTwinMaker::Entity` |
| AWS IoT TwinMaker | 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` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Keyspaces (適用於 Apache Cassandra) | 資料表上的 Amazon Keyspaces API 活動。 | Cassandra 資料表 | `AWS::Cassandra::Table` |
| Amazon Keyspaces (適用於 Apache Cassandra) | Cassandra CDC 串流上的 Amazon Keyspaces （適用於 Apache Cassandra) API 活動。 | Cassandra CDC 串流 | `AWS::Cassandra::Stream` |
| Amazon Kinesis Data Streams | 串流上的 Kinesis Data Streams API 活動。 | Kinesis 串流 | `AWS::Kinesis::Stream` |
| Amazon Kinesis Data Streams | 串流消費者上的 Kinesis Data Streams API 活動。 | Kinesis 串流消費者 | `AWS::Kinesis::StreamConsumer` |
| Amazon Kinesis Video Streams | 視訊串流上的 Kinesis Video Streams API 活動，例如對 `GetMedia`和 的呼叫`PutMedia`。 | Kinesis 視訊串流 | `AWS::KinesisVideo::Stream` |
| Amazon Kinesis Video Streams | Kinesis Video Streams 影片訊號頻道 API 活動。 | Kinesis 影片訊號頻道 | `AWS::KinesisVideo::SignalingChannel` |
| AWS Lambda | AWS Lambda 函數執行活動 ( `Invoke` API)。 | Lambda | `AWS::Lambda::Function` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Location Maps | Amazon Location Maps API 活動。 | 地理地圖 | `AWS::GeoMaps::Provider` |
| Amazon Location Places | Amazon Location Places API 活動。 | 地理位置 | `AWS::GeoPlaces::Provider` |
| Amazon Location Routes | Amazon Location Routes API 活動。 | 地理路由 | `AWS::GeoRoutes::Provider` |
| Amazon Machine Learning | ML 模型上的Machine Learning API 活動。 | 修補 Learning MlModel | `AWS::MachineLearning::MlModel` |
| Amazon Managed Blockchain | 網路上的 Amazon Managed Blockchain API 活動。 | Managed Blockchain 網路 | `AWS::ManagedBlockchain::Network` |
| Amazon Managed Blockchain | 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 Managed Blockchain Query | Amazon Managed Blockchain Query API 活動。 | 受管區塊鏈查詢 | `AWS::ManagedBlockchainQuery::QueryAPI` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Managed Workflows for Apache Airflow | 環境上的 Amazon MWAA API 活動。 | 受管 Apache Airflow | `AWS::MWAA::Environment` |
| 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` |
| Amazon One Enterprise | UKey 上的 Amazon One Enterprise API 活動。 | Amazon One UKey | `AWS::One::UKey` |
| Amazon One Enterprise | 使用者上的 Amazon One Enterprise API 活動。 | Amazon One 使用者 | `AWS::One::User` |
| AWS Payment Cryptography | AWS Payment Cryptography 別名上的 API 活動。 | 付款密碼編譯別名 | `AWS::PaymentCryptography::Alias` |
| AWS Payment Cryptography | AWS Payment Cryptography 金鑰上的 API 活動。 | 付款密碼編譯金鑰 | `AWS::PaymentCryptography::Key` |
| Amazon Pinpoint | 行動目標應用程式上的 Amazon Pinpoint API 活動。 | 行動目標應用程式 | `AWS::Pinpoint::App` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| AWS 私有 CA | AWS 私有 CA 適用於 Active Directory API 活動的連接器。 | AWS 私有 CA 適用於 Active Directory 的連接器 | `AWS::PCAConnectorAD::Connector` |
| AWS 私有 CA | AWS 私有 CA Connector for SCEP API 活動。 | AWS 私有 CA 適用於 SCEP 的連接器 | `AWS::PCAConnectorSCEP::Connector` |
| Amazon Q Apps | Amazon Q 應用程式上的資料 API 活動。 | Amazon Q 應用程式 | `AWS::QApps::QApp` |
| Amazon Q Apps | Amazon Q App 工作階段上的資料 API 活動。 | Amazon Q 應用程式工作階段 | `AWS::QApps::QAppSession` |
| 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` |
| Amazon Q Business | 資料來源上的 Amazon Q Business API 活動。 | Amazon Q Business 資料來源 | `AWS::QBusiness::DataSource` |
| Amazon Q Business | 索引上的 Amazon Q Business API 活動。 | Amazon Q Business 索引 | `AWS::QBusiness::Index` |
| Amazon Q Business | Web 體驗上的 Amazon Q Business API 活動。 | Amazon Q Business Web 體驗 | `AWS::QBusiness::WebExperience` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon Q Business | Amazon Q Business 整合 API 活動。 | Amazon Q Business 整合 | `AWS::QBusiness::Integration` |
| Amazon Q Developer | 整合上的 Amazon Q Developer API 活動。 | Q 開發人員整合 | `AWS::QDeveloper::Integration` |
| Amazon Q Developer | 有關操作調查的 Amazon Q Developer API 活動。 | AIOps 調查群組 | `AWS::AIOps::InvestigationGroup` |
| Amazon Quick | 動作連接器上的 Amazon Quick API 活動。 | AWS QuickSuite 動作 | `AWS::Quicksight::ActionConnector` |
| Amazon Quick | Amazon Quick Flow API 活動。 | QuickSight 流程 | `AWS::QuickSight::Flow` |
| Amazon Quick | Amazon Quick FlowSession API 活動。 | QuickSight 流程工作階段 | `AWS::QuickSight::FlowSession` |
| Amazon SageMaker AI | 端點上的 Amazon SageMaker AI `InvokeEndpointWithResponseStream` 活動。 | SageMaker AI 端點 | `AWS::SageMaker::Endpoint` |
| Amazon SageMaker AI | 功能存放區上的 Amazon SageMaker AI API 活動。 | SageMaker AI 功能存放區 | `AWS::SageMaker::FeatureGroup` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon SageMaker AI | 實驗試驗元件上的 Amazon SageMaker AI API 活動。 | SageMaker AI 指標實驗試驗元件 | `AWS::SageMaker::ExperimentTrialComponent` |
| Amazon SageMaker AI | Amazon SageMaker AI MLflow API 活動。 | SageMaker MLflow | `AWS::SageMaker::MlflowTrackingServer` |
| AWS Signer | 簽署任務時的簽署者 API 活動。 | 簽署者簽署任務 | `AWS::Signer::SigningJob` |
| AWS Signer | 簽署設定檔時的簽署者 API 活動。 | 簽署者簽署設定檔 | `AWS::Signer::SigningProfile` |
| Amazon Simple Email Service | 組態集上的 Amazon Simple Email Service (Amazon SES) API 活動。 | SES 組態設定 | `AWS::SES::ConfigurationSet` |
| Amazon Simple Email Service | 電子郵件身分上的 Amazon Simple Email Service (Amazon SES) API 活動。 | SES 身分 | `AWS::SES::EmailIdentity` |
| Amazon Simple Email Service | 範本上的 Amazon Simple Email Service (Amazon SES) API 活動。 | SES 範本 | `AWS::SES::Template` |
| Amazon SimpleDB | 網域上的 Amazon SimpleDB API 活動。 | SimpleDB 網域 | `AWS::SDB::Domain` |
| AWS Step Functions | Step Functions API 活動。 | 步驟函數 | `AWS::StepFunctions::Activity` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| AWS Step Functions | Step Functions 在狀態機器上的 API 活動。 | Step Functions 狀態機器 | AWS::StepFunctions::StateMachine |
| AWS Systems Manager | 控制頻道上的 Systems Manager API 活動。 | Systems Manager | AWS::SSMMessages::ControlChannel |
| AWS Systems Manager | 影響評估上的 Systems Manager API 活動。 | SSM 影響評估 | AWS::SSM::ExecutionPreview |
| AWS Systems Manager | 受管節點上的 Systems Manager API 活動。 | Systems Manager 受管節點 | AWS::SSM::ManagedNode |
| Amazon Timestream | 資料庫上的 Amazon Timestream Query API 活動。 | Timestream 資料庫 | AWS::Timestream::Database |
| Amazon Timestream | 區域端點上的 Amazon Timestream API 活動。 | Timestream 區域端點 | AWS::Timestream::RegionalEndpoint |
| Amazon Timestream | 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 精簡型客戶端 | 裝置上的 WorkSpaces 精簡型客戶端 API 活動。 | 精簡型客戶端裝置 | AWS::ThinClient::Device |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon WorkSpaces 精簡型客戶端 | 環境上的 WorkSpaces 精簡型客戶端 API 活動。 | 精簡型客戶端環境 | `AWS::ThinClient::Environment` |
| AWS X-Ray | 追蹤上的 X-Ray API 活動。 | X-Ray 追蹤 | `AWS::XRay::Trace` |
| Amazon AIDevOps | 代理程式空間上的 AIDevOps API 活動。 | 客服人員空間 | `AWS::AIDevOps::AgentSpace` |
| Amazon AIDevOps | 關聯上的 AIDevOps API 活動。 | AIDevOps 關聯 | `AWS::AIDevOps::Association` |
| Amazon AIDevOps | 操作員應用程式團隊上的 AIDevOps API 活動。 | AIDevOps 運算子應用程式團隊 | `AWS::AIDevOps::OperatorAppTeam` |
| Amazon AIDevOps | 管道中繼資料上的 AIDevOps API 活動。 | AIDevOps 管道中繼資料 | `AWS::AIDevOps::PipelineMetadata` |
| Amazon AIDevOps | 服務上的 AIDevOps API 活動。 | AIDevOps 服務 | `AWS::AIDevOps::Service` |
| Amazon Bedrock | 進階最佳化提示任務上的 Bedrock API 活動。 | AdvancedOptimizePromptJob | `AWS::Bedrock::AdvancedOptimizePromptJob` |
| Amazon Bedrock AgentCore | 評估器上的 Bedrock AgentCore API 活動。 | Bedrock-AgentCore 評估器 | `AWS::BedrockAgentCore::Evaluator` |
| Amazon 成本最佳化 | 設定檔上的 CloudOptimization API 活動。 | CloudOptimization 設定檔 | `AWS::CloudOptimization::Profile` |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon 成本最佳化 | 建議的 CloudOptimization API 活動。 | CloudOptimization 建議 | AWS::CloudOptimization::Recommendation |
| Amazon GuardDuty | 惡意軟體掃描上的 GuardDuty API 活動。 | GuardDuty 惡意軟體掃描 | AWS::GuardDuty::MalwareScan |
| Amazon NovaAct | 工作流程定義的 Amazon NovaAct API 活動。 | 工作流程定義 | AWS::NovaAct::WorkflowDefinition |
| Amazon NovaAct | 工作流程執行上的 Amanzon NovaAct API 活動。 | 工作流程執行 | AWS::NovaAct::WorkflowRun |
| Amazon Redshift | 叢集上的 Redshift API 活動。 | Amazon Redshift 叢集 | AWS::Redshift::Cluster |
| Amazon Support | 租用戶上的 SupportAccess API 活動。 | SupportAccess 租用戶 | AWS::SupportAccess::Tenant |
| Amazon Support | 信任帳戶的 SupportAccess API 活動。 | SupportAccess 信任帳戶 | AWS::SupportAccess::TrustingAccount |
| Amazon Support | 信任角色的 SupportAccess API 活動。 | SupportAccess 信任角色 | AWS::SupportAccess::TrustingRole |
| Amazon 轉換 | 轉換代理程式執行個體上的 API 活動。 | 轉換代理程式執行個體 | AWS::Transform::AgentInstance |
| Amazon 轉換自訂 | 轉換行銷活動上的自訂 API 活動。 | Transform-Custom 行銷活動 | AWS::TransformCustom::Campaign |

| AWS 服務 | Description | 資源類型 (主控台) | resources.type 值 |
| --- | --- | --- | --- |
| Amazon 轉換自訂 | 在對話上轉換自訂 API 活動。 | 轉換自訂對話 | `AWS::TransformCustom::Conversation` |
| Amazon 轉換自訂 | 在知識項目上轉換自訂 API 活動。 | 轉換自訂知識項目 | `AWS::TransformCustom::KnowledgeItem` |
| Amazon 轉換自訂 | 轉換套件上的自訂 API 活動。 | Transform-Custom 套件 | `AWS::TransformCustom::Package` |

若要記錄 CloudTrail 資料事件，您必須明確新增要收集活動的每個資源類型。如需詳細資訊，請參閱使用 CloudTrail 主控台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 儲存貯體是全域的，但 AWS Lambda 函數和 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 `amzn-s3-demo-bucket` 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 使用者指定了空的前綴，選擇記錄讀和寫資料事件。

1. 使用者將物件上傳至 `amzn-s3-demo-bucket`。
2. `PutObject` API 操作是 Amazon S3 物件層級的 API。它在 CloudTrail 中會記錄為資料事件。因為 CloudTrail 使用者使用空的字首指定了 S3 儲存貯體，所以會記錄該儲存貯體中任何物件發生的事件。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 `amzn-s3-demo-bucket2`。
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 使用者指定名為 的 S3 儲存貯體amzn-s3-demo-bucket3，字首為 *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:::amzn-s3-demo-bucket3/my-images/example.jpg。
2. DeleteObject API 操作是 Amazon S3 物件層級的 API。它在 CloudTrail 中會記錄為寫資料事件。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:::amzn-s3-demo-bucket3/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:::amzn-s3-demo-bucket3/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。它在 CloudTrail 中記錄為讀取資料事件，但追蹤或事件資料存放區未設定記錄讀取事件。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 傳遞日誌時，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。
>
> 為了避免記錄 Amazon S3 儲存貯體的資料事件，如果您設定追蹤記錄 AWS 帳戶中的所有 Amazon S3 資料事件，請考慮設定將日誌檔案交付到屬於另一個 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 日誌檔案。

## 記錄其他 AWS 帳戶中 S3 物件的資料事件

當您設定追蹤記錄資料事件時，您也可以指定屬於其他 AWS 帳戶的 S3 物件。當指定的物件上發生事件時，CloudTrail 會評估事件是否符合各帳戶的任何追蹤。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 帳戶的 Amazon S3 物件的資料事件

下列範例顯示兩個 AWS 帳戶如何設定 CloudTrail 來記錄相同 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 `amzn-s3-demo-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。因為目前有兩個事件複本 (一個記錄於 Bob 的追蹤中，另一個記錄於您的追蹤)，所以 CloudTrail 會針對資料事件的兩個複本收取費用。
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. 因為事件不是發生在 Bob 的帳戶中，而且此 S3 儲存貯體不屬於他，所以 Bob 的追蹤不會記錄此事件。CloudTrail 只會針對此資料事件的一個副本收費。

範例：記錄所有儲存貯體的資料事件，包括兩個 AWS 帳戶所使用的 S3 儲存貯體

下列範例顯示針對在帳戶中收集資料事件的線索啟用選取您帳戶中的所有 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。因為目前有兩個事件複本 (一個記錄於 Bob 的追蹤中，另一個記錄於您的追蹤)，所以 CloudTrail 會針對資料事件的複本，對每個帳戶收取費用。
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. 因為事件不是發生在 Bob 的帳戶中，而且此 S3 儲存貯體不屬於他，所以 Bob 的追蹤不會記錄此事件。CloudTrail 只會針對您帳戶中此資料事件的一份副本收費。
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 CloudTrail 會記錄其追蹤中的資料事件。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，您會在追蹤中收到關於 Mary 叫用 `GetObject` 操作的事件。CloudTrail 會針對每個資料事件複本 (一個在 Mary 的追蹤中，一個在您的追蹤中)，向您的帳戶和 Mary 的帳戶收取費用。

## 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

下列範例示範如何設定線索，將帳戶的日誌活動分割為單獨的 S3 儲存貯體：一個名為 amzn-s3-demo-bucket1 的儲存貯體會收到唯讀事件，第二個 amzn-s3-demo-bucket2 會收到唯讀事件。

1. 您可以建立線索，然後選擇名為 的 S3 儲存貯體amzn-s3-demo-bucket1來接收日誌檔案。接著，您要更新追蹤，指定您要讀管理事件和資料事件。
2. 您可以建立第二個線索，然後選擇要接收日誌檔案的 S3 amzn-s3-demo-bucket2 儲存貯體。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 amzn-s3-demo-bucket1。
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 amzn-s3-demo-bucket2 。

## 使用 記錄資料事件 AWS 管理主控台

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 管理主控台記錄資料事件。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 使用主控台建立追蹤。

對於線索，記錄資料事件的步驟會根據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源類型的資料事件，但如果您使用基本事件選取器，則僅限於記錄 Amazon S3 儲存貯體和儲存貯體物件、 AWS Lambda 函數和 Amazon DynamoDB 資料表的資料事件。

更新現有的事件資料存放區，以使用主控台記錄資料事件

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. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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 CloudTrail 事件的事件資料存放區上啟用資料事件。您無法在 CloudTrail 事件資料存放區上為 AWS Config 組態項目、CloudTrail Insights 事件或非AWS 事件啟用資料事件。

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. 針對資源類型，選擇您要記錄資料事件的資源類型。
7. 選擇日誌選取器範本。您可以選擇預先定義的範本，或選擇自訂來定義您自己的事件集合條件。

   您可以從下列預先定義的範本中選擇：

   - 記錄所有事件：選擇此範本記錄所有事件。
   - 僅記錄讀取事件 – 選擇此範本以僅記錄讀取事件。唯讀事件是不會變更資源狀態的事件，例如 `Get*`或 `Describe*`事件。
   - 僅記錄寫入事件 – 選擇此範本以僅記錄寫入事件。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。
   - 僅記錄 AWS 管理主控台 事件 – 選擇此範本僅記錄源自 的事件 AWS 管理主控台。
   - 排除 AWS 服務 啟動的事件 – 選擇此範本以排除具有 `eventType`之 AWS 服務 的事件`AwsServiceEvent`，以及使用連結角色 (SLRs) AWS 服務啟動的事件。
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. 如果您選取自訂，在進階事件選取器中，會根據進階事件選取器欄位的值來建置表達式。

> **Note**
>
> 選取器不支援使用萬用字元，例如 `*` 。若要將多個值與單一條件比對，您可以使用 `StartsWith`、`NotStartsWith`、 `EndsWith`或 `NotEndsWith`來明確比對事件欄位的開頭或結尾。

   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任何記錄到 CloudTrail 的資料事件，例如 PutBucket、GetItem 或 GetSnapshotBlock。
- **eventSource** – 要包含或排除的事件來源。此欄位可以使用任何運算子。
- eventType – 要納入或排除的事件類型。例如，您可以將此欄位設定為不等於AwsServiceEvent排除 AWS 服務 事件。如需事件類型的清單，請參閱 eventType中的 CloudTrail 記錄管理、資料和網路活動事件的內容。
- sessionCredentialFromConsole – 包含或排除源自 AWS 管理主控台 工作階段的事件。此欄位可以設定為等於或不等於 的值true。
- userIdentity.arn – 針對特定 IAM 身分執行的動作納入或排除事件。如需更多詳細資訊，請參閱 CloudTrail userIdentity 元素。
- **resources.ARN** - 您可以將任何運算子與 搭配使用resources.ARN，但如果您使用等於或不等於，則該值必須完全符合您在範本中指定之類型之有效資源的 ARN，做為 的值resources.type。

  > **Note**
  >
  > 您無法使用 resources.ARN 欄位來篩選沒有 ARNs的資源類型。

  如需資料事件資源 ARN 格式的詳細資訊，請參閱《服務授權參考》中的 的動作、資源和條件索引鍵 AWS 服務。

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，若要從記錄於事件資料存放區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，設定 的運算子不會以 開頭，然後貼入您不想記錄事件的 S3 儲存貯體 ARN。

   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。

   如需有關 CloudTrail 如何評估多個條件的資訊，請參閱 CloudTrail 如何評估欄位的多項條件。

> **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. 若要新增要記錄資料事件的其他資源類型，請選擇新增資料事件類型。重複步驟 6 到此步驟，以設定另一個資源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。

使用主控台更新現有的線索，以使用進階事件選取器記錄資料事件

在 中 AWS 管理主控台，如果您的線索使用進階事件選取器，您可以選擇預先定義的範本，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，選擇您想要更新的追蹤。
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. 針對資源類型，選擇您要記錄資料事件的資源類型。
5. 選擇日誌選取器範本。您可以選擇預先定義的範本，或選擇自訂來定義您自己的事件集合條件。

   您可以從下列預先定義的範本中選擇：

   - 記錄所有事件：選擇此範本記錄所有事件。
   - 僅記錄讀取事件 – 選擇此範本以僅記錄讀取事件。唯讀事件是不會變更資源狀態的事件，例如 `Get*`或 `Describe*`事件。
   - 僅記錄寫入事件 – 選擇此範本僅記錄寫入事件。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。
   - 僅記錄 AWS 管理主控台 事件 – 選擇此範本僅記錄源自 的事件 AWS 管理主控台。
   - 排除 AWS 服務 啟動的事件 – 選擇此範本以排除具有 `eventType`之 AWS 服務 的事件`AwsServiceEvent`，以及使用連結角色 (SLRs) AWS 服務啟動的事件。

> **Note**
>
> 選擇 S3 儲存貯體的預先定義範本，可讓您 AWS 帳戶中目前所有儲存貯體的資料事件記錄，以及您在完成建立追蹤後建立的任何儲存貯體。它也可以記錄您 AWS 帳戶中任何使用者或角色執行的資料事件活動，即使該活動是在屬於另一個 AWS 帳戶的儲存貯體上執行。
>
> 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。它不會記錄您 AWS 帳戶中其他區域中 Amazon S3 儲存貯體的資料事件。
>
> 如果您要為所有區域建立線索，請為 Lambda 函數選擇預先定義的範本，以啟用目前在您 AWS 帳戶中所有函數的資料事件記錄，以及在您完成建立線索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線索（對於線索，這只能透過使用 來完成 AWS CLI)，則此選擇會啟用目前在您 AWS 帳戶中該區域的所有函數的資料事件記錄，以及在您完成建立線索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以記錄您 AWS 帳戶中任何使用者或角色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。

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. 如果您選取自訂，在進階事件選取器中，會根據進階事件選取器欄位的值來建置表達式。

> **Note**
>
> 選取器不支援使用萬用字元，例如 * 。若要將多個值與單一條件比對，您可以使用 `StartsWith`、`NotStartsWith`、 `EndsWith`或 `NotEndsWith`來明確比對事件欄位的開頭或結尾。

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任何記錄到 CloudTrail 的資料事件，例如 PutBucket、GetItem 或 GetSnapshotBlock。
- **eventSource** – 要包含或排除的事件來源。此欄位可以使用任何運算子。
- eventType – 要納入或排除的事件類型。例如，您可以將此欄位設定為不等於AwsServiceEvent排除 AWS 服務 事件。如需事件類型的清單，請參閱 eventType中的 CloudTrail 記錄管理、資料和網路活動事件的內容。
- sessionCredentialFromConsole – 包含或排除源自 AWS 管理主控台 工作階段的事件。此欄位可以設定為等於或不等於 的值true。
- userIdentity.arn – 針對特定 IAM 身分執行的動作納入或排除事件。如需更多詳細資訊，請參閱 CloudTrail userIdentity 元素。
- **resources.ARN** - 您可以將任何運算子與 搭配使用resources.ARN，但如果您使用等於或不等於，則該值必須完全符合您在範本中指定之類型之有效資源的 ARN，做為 的值resources.type。

> **Note**
>
> 您無法使用 resources.ARN 欄位來篩選沒有 ARNs的資源類型。

如需資料事件資源 ARN 格式的詳細資訊，請參閱《服務授權參考》中的 的動作、資源和條件索引鍵 AWS 服務。

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，若要從記錄於事件資料存放區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 的運算子設定為 不以 開頭，然後貼入您不想記錄事件的 S3 儲存貯體 ARN。

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。

如需有關 CloudTrail 如何評估多個條件的資訊，請參閱 CloudTrail 如何評估欄位的多項條件。

> **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。

8. 若要新增要記錄資料事件的其他資源類型，請選擇新增資料事件類型。重複步驟 4 到此步驟，為資源類型設定進階事件選取器。
9. 檢閱並驗證您的選擇後，選擇儲存變更。

使用主控台更新現有的線索，以使用基本事件選取器記錄資料事件

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. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
2. 開啟 CloudTrail 主控台的追蹤頁面，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 所有目前和未來的 S3 儲存貯體選項會啟用您 AWS 帳戶中目前所有儲存貯體的資料事件記錄，以及您在完成建立追蹤後建立的任何儲存貯體。它也可以記錄

您 AWS 帳戶中任何使用者或角色執行的資料事件活動，即使該活動是在屬於另一個 AWS 帳戶的儲存貯體上執行。
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，為與追蹤相同區域中的所有儲存貯體以及稍後在該區域中建立的任何儲存貯體啟用資料事件記錄。它不會記錄您 AWS 帳戶中其他區域中 Amazon S3 儲存貯體的資料事件。

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. 若要新增要記錄資料事件的其他資源類型，請選擇新增資料事件類型。

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線索（使用 完成 AWS CLI)，則此選擇會啟用 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

立線索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以記錄您 AWS 帳戶中任何使用者或角色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於 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命令來設定特定 Lambda 函數的資料事件記錄。如需詳細資訊，請參閱使用管理線索 AWS CLI。

7. 若要新增要記錄資料事件的其他資源類型，請選擇新增資料事件類型。
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。

## 使用 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

- 使用 記錄線索的資料事件 AWS CLI
- 使用 記錄事件資料存放區的資料事件 AWS CLI

# 使用 記錄線索的資料事件 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，根據支援的進階事件選取器欄位支援進階事件選取器欄位的值進行篩選，讓您能夠僅記錄感興趣的資料事件。如需設定這些欄位的詳細資訊，請參閱《AWS CloudTrail API 參考AdvancedFieldSelector》中的 和本指南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
```

命令會傳回線索的事件選取器。

主題

- 使用進階事件選取器記錄線索的資料事件
- 使用進階Amazon S3事件選取器記錄 Amazon S3 儲存貯體的所有 Amazon S3 事件
- 使用進階 AWS Outposts 事件選取器在事件上記錄 Amazon S3
- 使用基本事件選取器記錄事件

使用進階事件選取器記錄線索的資料事件

> **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。

下列範例會為名為 *TrailName* 的線索建立自訂進階事件選取器，以包含讀取和寫入管理事件（省略選取readOnly器），PutObject以及所有 Amazon S3 儲存貯體/字首組合DeleteObject的資料事件，但名為 的儲存貯體amzn-s3-demo-bucket和名為 之 AWS Lambda 函數的資料事件除外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:::amzn-s3-demo-
bucket/"] }
    ]
  },
  {
    "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:::amzn-s3-demo-bucket/" ]
        },
      ]
    },
{
      "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Amazon S3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:::amzn-s3-
demo-bucket/"] }
            ]
        }
]'
```

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:::amzn-s3-demo-bucket/"
                    ]
                }
            ]
        }
    ]
}
```

使用進階 AWS Outposts 事件選取器在事件上記錄 Amazon S3

> **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。根據預設，當您使用 建立線索時 AWS CLI，線索會記錄所有管理事件。根據預設，線索不會記錄資料事件。

```
{
    "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:::amzn-s3-demo-bucket1/prefix",
 "arn:aws:s3:::amzn-s3-demo-bucket2;/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:::amzn-s3-demo-bucket1/prefix",
                        "arn:aws:s3:::amzn-s3-demo-bucket2/prefix2",
                    ],
                    "Type": "AWS::S3::Object"
                }
            ],
            "ReadWriteType": "All"
        }
    ]
```

```
}
```

## 使用 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。

您可以設定進階事件選取器來記錄事件資料存放區上的資料事件。如需支援欄位的清單，請參閱 使用進階事件選取器篩選資料事件。

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

- 包含特定儲存貯體的所有 Amazon S3 事件
- 在 AWS Outposts 事件上包含 Amazon S3

包含特定儲存貯體的所有 Amazon S3 事件

下列範例示範如何建立事件資料存放區，以包含特定一般用途 Amazon S3 S3 物件的所有資料事件，並排除 產生的 AWS 服務 事件和事件bucket-scanner-roleuserIdentity。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:::amzn-s3-
demo-bucket/"] },
            { "Field": "userIdentity.arn", "NotStartsWith":
 ["arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"]},
            { "Field": "eventType","NotEquals": ["AwsServiceEvent"]}
        ]
    }
]'
```

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:::amzn-s3-demo-bucket/"
                    ]
                },
                {
                    "Field": "resources.type",
                    "Equals": [
                        "AWS::S3::Object"
                    ]
                },
                {
                    "Field": "userIdentity.arn",
                    "NotStartsWith": [
                        "arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"
                     ]
                },
                {
                    "Field": "eventType",
                    "NotEquals": [
                        "AwsServiceEvent"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "BillingMode": "EXTENDABLE_RETENTION_PRICING",
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
```

```
    "CreatedTimestamp": "2024-11-04T15:57:33.701000+00:00",
    "UpdatedTimestamp": "2024-11-20T20:49:21.766000+00:00"
}
```

在 AWS Outposts 事件上包含 Amazon S3

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用於記錄資料事件的精細選取器，這可協助您僅記錄感興趣的特定資料事件來控制成本。

例如：

- 您可以在 `eventName` 欄位中新增篩選條件，以包含或排除特定 API 呼叫。
- 您可以在 `resources.ARN` 欄位中新增篩選條件，以包含或排除特定資源的記錄。例如，如果您正在記錄 S3 資料事件，您可以排除追蹤的 S3 儲存貯體記錄。
- 您可以在 `readOnly` 欄位上新增篩選條件，以選擇僅記錄唯讀事件或唯讀事件。

下表說明篩選資料事件的支援欄位。如需每個 CloudTrail 事件類型的支援欄位清單，請參閱 AWS CloudTrail API 參考中的 AdvancedEventSelector。

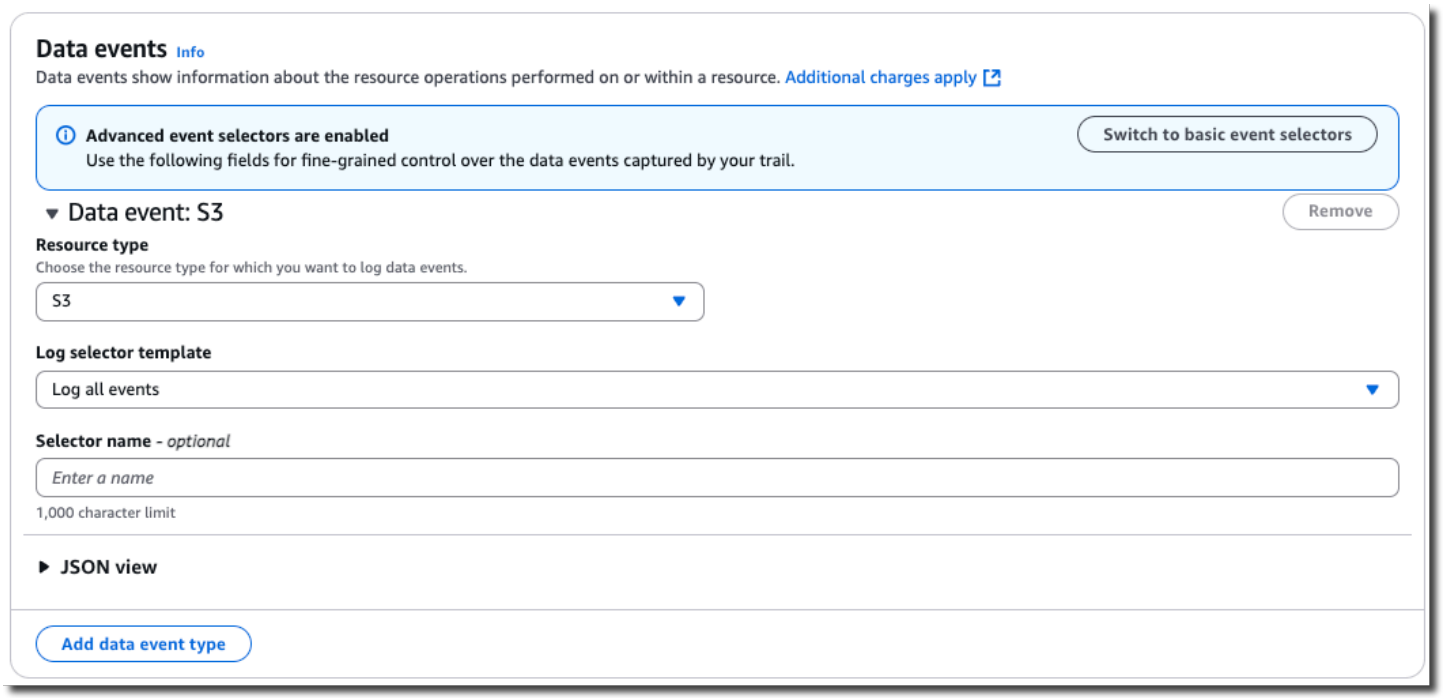
| 欄位 | 必要 | 有效運算子 | Description |
| --- | --- | --- | --- |
| **eventCategory** | 是 | Equals | 此欄位設定為 Data以記錄資料事件。 |
| **resources.type** | 是 | Equals | 此欄位用於選取您要記錄資料事件的資源類型。資料事件資料表會顯示可能的值。 |
| **readOnly** | 否 | Equals | 這是選用欄位，用於根據 readOnly值包含或排除資料事件。僅true記錄讀取事件的值。false 僅日誌寫入事件的值 |

| 欄位 | 必要 | 有效運算子 | Description |
| --- | --- | --- | --- |
| | | | 。如果您未新增此欄位，CloudTrail 會同時記錄讀取和寫入事件。 |
| **eventName** | 否 | EndsWith<br>Equals<br>NotEndsWith<br>NotEquals<br>NotStartsWith<br>StartsWith | 這是選用的封存檔，用於篩選或篩選任何記錄到 CloudTrail 的資料事件，例如 PutBucket 或 GetSnapshotBlock 。<br>如果您使用的是 AWS CLI，則可以使用逗號分隔每個值來指定多個值。<br>如果您使用的是 主控台，您可以為eventName 要篩選的每個 建立條件來指定多個值。 |
| **resources.ARN** | 否 | EndsWith<br>Equals<br>NotEndsWith<br>NotEquals<br>NotStartsWith<br>StartsWith | 這是選用欄位，用於透過提供 來排除或包含特定資源的資料事件resources.ARN 。您可以搭配 使用任何運算子resources.ARN ，但如果您使用Equals或 NotEquals ，該值必須完全符合您resources.type 指定之 的有效資源 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。<br>如果您使用的是 AWS CLI，則可以使用逗號分隔每個值來指定多個值。<br>如果您使用的是 主控台，您可以為resources.ARN 要篩選的每個 建立條件來指定多個值。 |

| 欄位 | 必要 | 有效運算子 | Description |
| --- | --- | --- | --- |
| **eventSource** | 否 | EndsWith<br><br>Equals<br><br>NotEndsWith<br><br>NotEquals<br><br>NotStartsWith<br><br>StartsWith | 您可以使用它來包含或排除特定事件來源。eventSource 通常是簡短形式的服務名稱，不含空格加 .amazonaws.com 。例如，您可以將 eventSource Equals 設定為 ec2.amazonaws.com ，以僅記錄 Amazon EC2 資料事件。 |
| **eventType** | 否 | EndsWith<br><br>Equals<br><br>NotEndsWith<br><br>NotEquals<br><br>NotStartsWith<br><br>StartsWith | 要包含或排除的 eventType。例如，您可以將此欄位設定為 NotEquals AwsServiceEvent 以排除AWS 服務事件。 |
| **sessionCredentialFromConsole** | 否 | Equals<br><br>NotEquals | 包含或排除源自 AWS 管理主控台 工作階段的事件。此欄位可以設定為 Equals或NotEquals 值為 true。 |

| 欄位 | 必要 | 有效運算子 | Description |
| --- | --- | --- | --- |
| **userIdentity.arn** | 否 | EndsWith<br>Equals<br>NotEndsWith<br>NotEquals<br>NotStartsWith<br>StartsWith | 包含或排除特定 IAM 身分所採取動作的事件。如需更多詳細資訊，請參閱 CloudTrail userIdentity 元素。 |

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源類型。資料事件資料表顯示您可以在 CloudTrail 主控台中選擇的可能資源類型。



若要使用 記錄資料事件 AWS CLI，請設定 `--advanced-event-selector` 參數來設定`eventCategory`等於 `Data`且`resources.type`值等於您要記錄資料事件的資源類型值。資料事件資料表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。您可以進一步精簡進階事件選取器，以篩選 `eventName`、 和 `resources.ARN` 欄位`readOnly`，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，根據多個欄位篩選資料事件。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。將 *`amzn-s3-demo-bucket`* 取代為您的儲存貯體名稱。

```
--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:::amzn-s3-demo-
bucket/"] }
    ]
  }
]'
```

您也可以為欄位包含多個條件。如需如何評估多個條件的資訊，請參閱 CloudTrail 如何評估欄位的多項條件。

您可以使用進階事件選取器來記錄管理和資料事件。若要記錄多個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擇器陳述式。

> **Note**
>
> 線索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。
> 選取器不支援使用萬用字元，例如 * 。若要以單一條件比對多個值，您可以使用 `StartsWith`、`NotStartsWith`、 `EndsWith`或 `NotEndsWith`來明確比對事件欄位的開頭或結尾。

主題


- CloudTrail 如何評估欄位的多項條件
- AWS CLI 用於篩選資料事件的範例


## CloudTrail 如何評估欄位的多項條件

對於進階事件選取器，CloudTrail 會評估欄位的多個條件，如下所示：

- DESELECT 運算子是 AND'd 在一起的。如果符合任何 DESELECT 運算子條件，則不會交付事件。以下是進階事件選取器的有效 DESELECT 運算子：
  - `NotEndsWith`
  - `NotEquals`
  - `NotStartsWith`
- SELECT 運算子是 OR'd 在一起。以下是進階事件選取器的有效 SELECT 運算子：
  - `EndsWith`
  - `Equals`
  - `StartsWith`
- SELECT 和 DESELECT 運算子的組合遵循上述規則，兩個群組是 AND'd 在一起。

### 顯示 **`resources.ARN`** 欄位多個條件的範例

下列範例事件選取器陳述式會收集`AWS::S3::Object`資源類型的資料事件，並在 `resources.ARN` 欄位上套用多個條件。

```
{
    "Name": "S3Select",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "Data"
        ]
      },
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      },
      {
        "Field": "resources.ARN",
        "Equals": [
          "arn:aws:s3:::amzn-s3-demo-bucket/object1"
        ],
        "StartsWith": [
          "arn:aws:s3:::amzn-s3-demo-bucket/"
        ],
        "EndsWith": [
          "object3"
        ],
        "NotStartsWith": [
          "arn:aws:s3:::amzn-s3-demo-bucket/deselect"
        ],
        "NotEndsWith": [
          "object5"
        ],
        "NotEquals": [
          "arn:aws:s3:::amzn-s3-demo-bucket/object6"
        ]
      }
    ]
  }
```

在上述範例中，如果符合下列條件，則會交付`AWS::S3::Object`資源的 Amazon S3 資料事件：

1. 不符合這些 DESELECT 運算子條件：

- resources.ARN 欄位 NotStartsWith 值 arn:aws:s3:::amzn-s3-demo-bucket/deselect
- resources.ARN 欄位 NotEndsWith 值 object5
- resources.ARN 欄位 NotEquals 值 arn:aws:s3:::amzn-s3-demo-bucket/object6

2. 至少符合下列其中一個 SELECT 運算子條件：
   - resources.ARN 欄位 Equals 值 arn:aws:s3:::amzn-s3-demo-bucket/object1
   - resources.ARN 欄位 StartsWith 值 arn:aws:s3:::amzn-s3-demo-bucket/
   - resources.ARN 欄位 EndsWith 值 object3

根據評估邏輯：

1. 的資料事件amzn-s3-demo-bucket/object1將交付，因為它符合Equals運算子的值，且不符合NotStartsWith、 NotEndsWith和 NotEquals運算子的任何值。
2. 的資料事件amzn-s3-demo-bucket/object2將交付，因為它符合StartsWith運算子的值，且不符合 NotStartsWith、 NotEndsWith和 NotEquals運算子的任何值。
3. 的資料事件amzn-s3-demo-bucket1/object3將交付，因為它符合EndsWith運算子，且不符合NotStartsWith、 NotEndsWith和 NotEquals運算子的任何值。
4. 的資料事件arn:aws:s3:::amzn-s3-demo-bucket/deselectObject4將不會交付，因為它符合 的條件，NotStartsWith即使它符合StartsWith運算子的條件。
5. 的資料事件arn:aws:s3:::amzn-s3-demo-bucket/object5將不會交付，因為它符合 的條件，NotEndsWith即使它符合StartsWith運算子的條件。
6. 的資料事件arn:aws:s3:::amzn-s3-demo-bucket/object6將不會交付，因為它符合NotEquals運算子的條件，即使它符合StartsWith運算子的條件。

## AWS CLI 用於篩選資料事件的範例

本節提供 AWS CLI 範例，示範如何篩選不同欄位的資料事件。如需其他 AWS CLI 範例，請參閱 使用進階事件選取器記錄線索的資料事件和 使用 記錄事件資料存放區的資料事件 AWS CLI。

如需如何使用 主控台記錄資料事件的資訊，請參閱 使用 記錄資料事件 AWS 管理主控台。

範例：

- 範例 1：篩選 eventName 欄位
- 範例 2：篩選 resources.ARN和 userIdentity.arn 欄位

- 範例 3：篩選 resources.type和 eventName 欄位以排除由 Amazon S3 DeleteObjects 事件刪除的個別物件

**範例 1：篩選 eventName 欄位**

在第一個範例中，線索--advanced-event-selectors的 設定為僅記錄一般用途儲存貯體中 Amazon S3 物件的 GetObjectPutObject、 和 DeleteObject API 呼叫。

```
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，記錄 EBS Direct APIs 的資料事件，但排除 ListChangedBlocks API 呼叫。您可以使用 update-event-data-store命令來更新現有的事件資料存放區。

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

### 範例 2：篩選 **resources.ARN**和 **userIdentity.arn** 欄位

下列範例顯示如何在特定一般用途 Amazon S3 S3 物件的所有資料事件，但排除 所產生的事件bucket-scanner-roleuserIdentity。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，因此您必須新增的StartsWith運算子resources.ARN。

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
--advanced-event-selectors \
'[
    {
        "Name": "S3EventSelector",
        "FieldSelectors": [
            { "Field": "eventCategory", "Equals": ["Data"] },
            { "Field": "resources.type", "Equals": ["AWS::S3::Object"] },
            { "Field": "resources.ARN", "StartsWith": ["arn:partition:s3:::amzn-s3-
demo-bucket/"] },
            { "Field": "userIdentity.arn", "NotStartsWith":
 ["arn:aws:sts::123456789012:assumed-role/bucket-scanner-role"]}
        ]
    }
]'
```

### 範例 3：篩選 **resources.type**和 **eventName** 欄位以排除由 Amazon S3 DeleteObjects 事件刪除的個別物件

下列範例顯示如何在特定的一般用途 Amazon S3 儲存貯體中包含所有 Amazon S3 物件的所有資料事件，但排除 DeleteObject操作刪除的個別物件。resources.type 欄位的 S3 事件的值是 AWS::S3::Object。事件名稱的值為 DeleteObject。

```
aws cloudtrail put-event-selectors \
--trail-name trailName \
--advanced-event-selectors \

{
    "Name": "Exclude Events for DeleteObject operation",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "Data"
```

```
        ]
      },
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      },
      {
        "Field": "eventName",
        "NotEquals": [
          "DeleteObject"
        ]
      }
    ]
  },
  {
    "Name": "Exclude DeleteObject Events for individual objects deleted by
DeleteObjects Operation",
    "FieldSelectors": [
      {
        "Field": "eventCategory",
        "Equals": [
          "Data"
        ]
      },
      {
        "Field": "resources.type",
        "Equals": [
          "AWS::S3::Object"
        ]
      },
      {
        "Field": "eventName",
        "Equals": [
          "DeleteObject"
        ]
      },
      {
        "Field": "eventType",
        "NotEquals": [
          "AwsServiceEvent"
        ]
      }
```

```
    ]
  }
] (edited)
```

# 彙總資料事件

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。

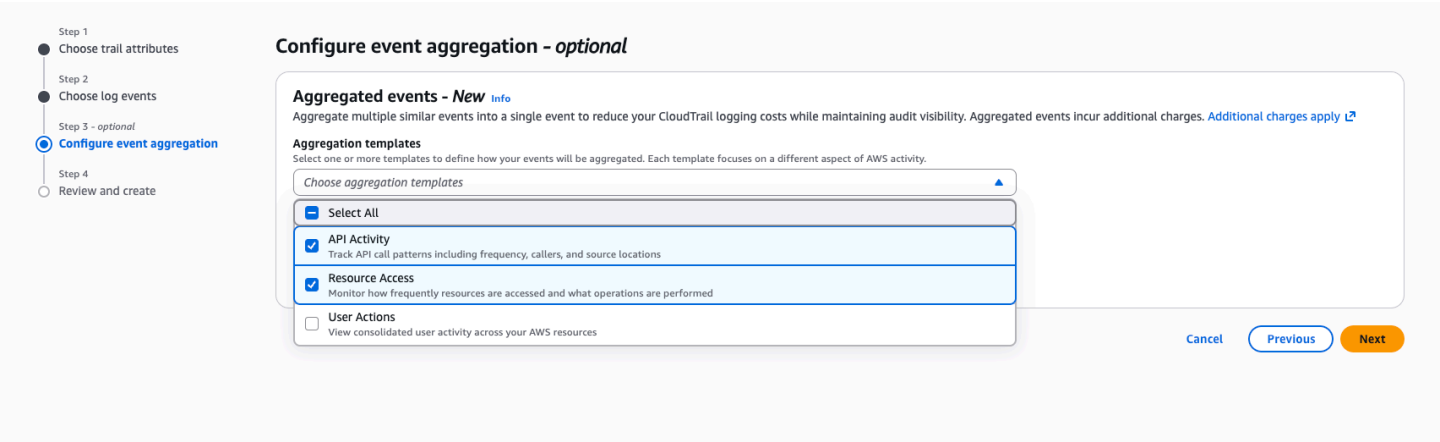
透過在資料事件上啟用彙總，您可以有效率地監控大量資料存取模式，而無需處理大量個別事件。此功能會自動將資料事件合併為 5 分鐘摘要，顯示存取頻率、錯誤率和最常用動作等主要趨勢。例如，您會收到顯示最高使用者和動作的合併摘要，而不是處理數千個個別 S3 儲存貯體存取事件以了解使用模式。

您可以在建立新的線索或更新收集資料事件的現有線索時，啟用資料事件的彙總。您可以選擇三個out-of-the-box範本之一或全部，以彙總資料事件：

- API 活動，可根據 API 呼叫取得 5 分鐘的資料事件摘要。使用此選項來了解您的 API 使用模式，包括頻率、呼叫者和來源。
- 資源存取，以取得 AWS 資源上的活動模式。使用此項目來了解您的 AWS 資源如何被存取、在 5 分鐘的時段中被存取多少次、誰正在存取資源，以及正在執行哪些動作。
- 使用者動作，根據在您帳戶中進行 API 呼叫的 IAM 主體來取得活動模式。

## 使用主控台啟用資料事件的彙總

若要在線索上啟用彙總，請先在建立或更新線索時選擇資料事件記錄，並設定資料事件以在線索中記錄事件。然後，在設定事件彙總步驟中，您可以從彙總範本下拉式清單中選取範本，例如 API 活動和資源存取，如以下螢幕擷取畫面所示。



## 使用 啟用資料事件的彙總 AWS CLI

您可以使用 設定追蹤以彙總事件 AWS CLI。

若要查看您的線索是否正在彙總資料事件，請執行 get-event-configurations命令。

```
aws cloudtrail get-event-configuration --region us-east-1 --trail-name TrailName
```

命令會傳回線索的彙總組態。

啟用事件彙總之前，您必須先建立追蹤並在其中設定資料事件。

若要在線索上啟用事件彙總，請遵循以下步驟。追蹤會根據 API_ACTIVITY和 RESOURCE_ACCESS 彙總範本彙總事件。

```
aws cloudtrail put-event-configuration --region us-east-1 --trail TrailName \
--aggregation-configurations \
'[
    {
        "EventCategory": "Data",
        "Templates":
        [
            "API_ACTIVITY",
            "RESOURCE_ACCESS"
        ]
    }
]'
```

範例：API_ACTIVITY 彙總事件

以下顯示API_ACTIVITY範本的彙總事件範例：

```
{
    "eventVersion": "1.0",
    "accountId": "111122223333",
    "eventId": "62759c1a-6248-48e1-a6b3-d5fb7e6c4bc0",
    "eventCategory": "Aggregated",
    "eventType": "AwsAggregatedEvent",
    "awsRegion": "us-west-2",
    "eventSource": "s3.amazonaws.com",
    "timeWindow":
    {
        "windowStart": "2025-11-17T19:20:00Z",
```

```
        "windowEnd": "2025-11-17T19:25:00Z",
        "windowSize": "PT5M"
    },
    "summary":
    {
        "primaryDimension":
        {
            "dimension": "eventName",
            "statistics":
            [
                {
                    "name": "PutObject",
                    "value": 1000
                }
            ],
            "aggregationType": "Count"
        },
        "details":
        [
            {
                "dimension": "resourceARN",
                "statistics":
                [
                    {
                        "name": "arn:aws:s3:::bucket-1",
                        "value": 800
                    },
                    {
                        "name": "arn:aws:s3:::bucket-2",
                        "value": 150
                    },
                    {
                        "name": "arn:aws:s3:::bucket-3",
                        "value": 50
                    }
                ],
                "aggregationType": "Count"
            }
        ]
    }
}
```

## 範例：RESOURCE_ACCESS 彙總事件

以下顯示RESOURCE_ACCESS範本彙總事件的範例：


```
{
    "eventVersion": "1.0",
    "accountId": "111122223333",
    "eventId": "2ed87efa-45c1-412d-bc38-7e0879faa6df",
    "eventCategory": "Aggregated",
    "eventType": "AwsAggregatedEvent",
    "awsRegion": "us-west-2",
    "eventSource": "s3.amazonaws.com",
    "timeWindow":
    {
        "windowStart": "2025-11-17T19:20:00Z",
        "windowEnd": "2025-11-17T19:25:00Z",
        "windowSize": "PT5M"
    },
    "summary":
    {
        "primaryDimension":
        {
            "dimension": "resourceARN",
            "statistics":
            [
                {
                    "name": "arn:aws:s3:::bucket-1",
                    "value": 800
                }
            ],
            "aggregationType": "Count"
        },
        "details":
        [
            {
                "dimension": "eventName",
                "statistics":
                [
                    {
                        "name": "PutObject",
                        "value": 800
                    }
                ],
                "aggregationType": "Count"
```

```
            }
        ]
    }
}
```

## 記錄資料事件以實現 AWS Config 合規

如果您使用一致性套件來協助企業維持遵循正式標準，例如聯邦風險與授權管理計劃 AWS Config (FedRAMP) 或國家標準與技術研究所 (NIST) 所需的標準，合規架構的一致性套件通常會要求您至少記錄 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。

- AWS Well-Architected Framework 安全支柱的操作最佳實務
- 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 中可用之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 SDKs 記錄資料事件

執行 GetEventSelectors 操作以查看您的追蹤是否記錄資料事件。您可以執行 PutEventSelectors 操作來設定您的追蹤記錄資料事件。如需詳細資訊，請參閱 AWS CloudTrail API 參考。

執行 GetEventDataStore 操作以查看您的事件資料存放區是否記錄資料事件。您可以透過執行 CreateEventDataStore 或 UpdateEventDataStore 操作並指定進階事件選取器，設定您的事件資料存放區以包括資料事件。如需詳細資訊，請參閱使用 建立、更新和管理事件資料存放區 AWS CLI和 AWS CloudTrail API 參考。

# 記錄網路活動事件

CloudTrail 網路活動事件可讓 VPC 端點擁有者記錄使用其 VPC 端點從私有 VPC 到 的 AWS API 呼叫 AWS 服務。網路活動事件可讓您了解 VPC 內執行的資源操作。例如，記錄網路活動事件可協助 VPC 端點擁有者偵測組織外部的登入資料何時嘗試存取其 VPC 端點。

您可以記錄下列服務的網路活動事件：

- AWS AppConfig
- AWS App Mesh
- Amazon Athena
- AWS B2B 資料交換
- AWS Backup gateway
- Amazon Bedrock
- Billing and Cost Management
- AWS 定價計算工具
- AWS Cost Explorer
- AWS 雲端控制 API
- AWS CloudHSM
- AWS Cloud Map
- AWS CloudFormation
- AWS CloudTrail
- Amazon CloudWatch
- CloudWatch Application Signals
- AWS CodeDeploy
- Amazon Comprehend Medical
- AWS Config
- AWS 資料匯出
- Amazon Data Firehose
- AWS Directory Service
- Amazon DynamoDB
- Amazon EC2

- Amazon Elastic Container Service
- Amazon Elastic File System
- Elastic Load Balancing
- Amazon EventBridge
- Amazon EventBridge 排程器
- Amazon Fraud Detector
- AWS 免費方案
- Amazon FSx
- AWS Glue
- AWS HealthLake
- AWS IoT FleetWise
- AWS IoT Secure Tunneling
- AWS Invoicing
- Amazon Keyspaces (適用於 Apache Cassandra)
- AWS KMS
- AWS Lake Formation
- AWS Lambda
- AWS License Manager
- Amazon Lookout for Equipment
- Amazon Lookout for Vision
- Amazon Personalize
- Amazon Q Business
- Amazon Rekognition
- Amazon Relational Database Service
- Amazon S3

> **Note**
>
> 不支援 Amazon S3 多區域存取點。

- Amazon SageMaker AI
- AWS Secrets Manager

- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Workflow Service
- AWS Storage Gateway
- AWS Systems Manager Incident Manager
- Amazon Textract
- Amazon Transcribe
- Amazon Translate
- AWS Transform
- Amazon Verified Permissions
- Amazon WorkMail

您可以同時設定線索和事件資料存放區，以記錄網路活動事件。

根據預設，線索和事件資料存放區不會記錄網路活動事件。網路活動事件需支付額外費用。如需詳細資訊，請參閱AWS CloudTrail 定價。

內容


- 網路活動事件的進階事件選取器欄位
- 使用 記錄網路活動事件 AWS 管理主控台
  - 更新現有的線索以記錄網路活動事件
  - 更新現有的事件資料存放區以記錄網路活動事件
- 使用 記錄網路活動事件 AWS Command Line Interface
  - 範例：記錄線索的網路活動事件
    - 範例：記錄 CloudTrail 操作的網路活動事件
    - 範例： 的日誌VpceAccessDenied事件 AWS KMS
    - 範例：Amazon S3 的日誌VpceAccessDenied事件
    - 範例：記錄特定 VPC 端點上的 EC2 VpceAccessDenied事件
    - 範例：記錄多個事件來源的所有管理事件和網路活動事件
  - 範例：記錄事件資料存放區的網路活動事件
    - 範例：記錄 CloudTrail 操作的所有網路活動事件
    - 範例： 的日誌VpceAccessDenied事件 AWS KMS

    - 範例：記錄特定 VPC 端點上的 EC2 VpceAccessDenied事件
    - 範例：Amazon S3 的日誌VpceAccessDenied事件
    - 範例：記錄多個事件來源的所有管理事件和網路活動事件
- 使用 AWS SDKs 記錄事件

## 網路活動事件的進階事件選取器欄位

您可以指定要記錄活動的事件來源，藉此設定進階事件選取器來記錄網路活動事件。您可以使用 AWS SDKs AWS CLI或 CloudTrail 主控台來設定進階事件選取器。

記錄網路活動事件時，需要下列進階事件選取器欄位：

- eventCategory – 若要記錄網路活動事件，值必須為 NetworkActivity。 eventCategory 只能使用 Equals 運算子。
- eventSource – 您要記錄網路活動事件的事件來源。 eventSource 只能使用 Equals 運算子。如果您想要記錄多個事件來源的網路活動事件，您必須為每個事件來源建立個別的欄位選擇器。

  有效值包含：

  - aco-automation.amazonaws.com
  - appconfig.amazonaws.com
  - application-signals.amazonaws.com
  - appmesh.amazonaws.com
  - athena.amazonaws.com
  - b2bi.amazonaws.com
  - backup-gateway.amazonaws.com
  - bcm-data-exports.amazonaws.com
  - bcm-pricing-calculator.amazonaws.com
  - bedrock-agentcore.amazonaws.com
  - bedrock.amazonaws.com
  - billing.amazonaws.com
  - cassandra.amazonaws.com
  - ce.amazonaws.com
  - cloudcontrolapi.amazonaws.com

- cloudformation.amazonaws.com
- cloudhsm.amazonaws.com
- cloudoptimization.amazonaws.com
- cloudtrail.amazonaws.com
- codedeploy.amazonaws.com
- comprehend.amazonaws.com
- comprehendmedical.amazonaws.com
- config.amazonaws.com
- ds.amazonaws.com
- dynamodb.amazonaws.com
- ec2.amazonaws.com
- ecs.amazonaws.com
- elasticfilesystem.amazonaws.com
- elasticloadbalancing.amazonaws.com
- events.amazonaws.com
- firehose.amazonaws.com
- frauddetector.amazonaws.com
- freetier.amazonaws.com
- fsx.amazonaws.com
- glue.amazonaws.com
- healthlake.amazonaws.com
- invoicing.amazonaws.com
- iot.amazonaws.com
- iotfleetwise.amazonaws.com
- iotsecuredtunneling.amazonaws.com
- kms.amazonaws.com
- lakeformation.amazonaws.com
- lambda.amazonaws.com
- license-manager.amazonaws.com
- lookoutequipment.amazonaws.com

- lookoutvision.amazonaws.com
- monitoring.amazonaws.com
- nova-act.amazonaws.com
- personalize.amazonaws.com
- qbusiness.amazonaws.com
- rds.amazonaws.com
- rekognition.amazonaws.com
- rolesanywhere.amazonaws.com
- s3.amazonaws.com
- sagemaker.amazonaws.com
- scheduler.amazonaws.com
- secretsmanager.amazonaws.com
- servicediscovery.amazonaws.com
- sns.amazonaws.com
- sqs.amazonaws.com
- ssm-contacts.amazonaws.com
- ssm.amazonaws.com
- storagegateway.amazonaws.com
- swf.amazonaws.com
- textract.amazonaws.com
- transcribe.amazonaws.com
- transcribestreaming.amazonaws.com
- transform-agents.amazonaws.com
- transform-custom.amazonaws.com
- transform.amazonaws.com
- translate.amazonaws.com
- user-subscriptions.amazonaws.com
- verifiedpermissions.amazonaws.com
- voiceid.amazonaws.com
- workmail.amazonaws.com

- workmailmessageflow.amazonaws.com

下列進階事件選取器欄位為選用：

- eventName – 您要篩選的請求動作。例如， CreateKey或 ListKeys。 eventName 可以使用任何運算子。
- errorCode – 您要篩選的請求錯誤代碼。目前，唯一有效的errorCode是 VpceAccessDenied。您只能搭配 使用 Equals運算子errorCode。
- vpcEndpointId – 識別操作通過的 VPC 端點。您可以搭配 使用任何運算子vpcEndpointId。

當您建立追蹤或事件資料存放區時，預設不會記錄網路活動事件。若要記錄 CloudTrail 網路活動事件，您必須明確設定要收集活動的每個事件來源。

記錄網路活動事件需支付額外費用。如需 CloudTrail 定價，請參閱 AWS CloudTrail 定價。

## 使用 記錄網路活動事件 AWS 管理主控台

您可以使用 主控台更新現有的線索或事件資料存放區，以記錄網路活動事件。

主題


- 更新現有的線索以記錄網路活動事件
- 更新現有的事件資料存放區以記錄網路活動事件


### 更新現有的線索以記錄網路活動事件

使用下列程序更新現有的線索，以記錄網路活動事件。

> **Note**
>
> 記錄網路活動事件需支付額外費用。如需 CloudTrail 定價，請參閱 AWS CloudTrail 定價。

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
2. 在 CloudTrail 主控台的左導覽窗格中，開啟追蹤頁面，選擇追蹤名稱。
3. 如果您的線索使用基本事件選取器記錄資料事件，您將需要切換到進階事件選取器來記錄網路活動事件。

採取下列步驟切換到進階事件選取器：

a. 在資料事件區域中，記下目前的資料事件選取器。切換到進階事件選取器將清除任何現有的資料事件選取器。

b. 選擇編輯，然後選擇切換到進階事件選取器。

c. 使用進階事件選取器重新套用您的資料事件選取項目。如需詳細資訊，請參閱使用主控台更新現有的線索，以使用進階事件選取器記錄資料事件。

4. 在網路活動事件中，選擇編輯。

若要記錄網路活動事件，請執行下列步驟：

a. 從網路活動事件來源中，選擇網路活動事件的來源。

b. 在日誌選取器範本中，選擇範本。您可以選擇記錄所有網路活動事件、記錄所有網路活動存取遭拒的事件，或選擇自訂以建置自訂日誌選取器來篩選多個欄位，例如 `eventName`和 `vpcEndpointId`。

c. （選用）輸入名稱以識別選取器。選擇器名稱在進階事件選擇器中列為名稱，如果您展開 JSON 檢視，則可檢視。

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。如果您使用預先定義的日誌範本，則可略過此步驟。

   i. 對於排除或包含網路活動事件，您可以在 主控台中選擇下列欄位。

      - **eventName** – 您可以將任何運算子與 搭配使用`eventName`。您可以使用它來包含或排除任何事件，例如 `CreateKey`。
      - **errorCode** – 您可以使用它來篩選錯誤碼。目前，唯一支援的`errorCode`是 `VpceAccessDenied`。
      - **vpcEndpointId** – 識別操作通過的 VPC 端點。您可以搭配 使用任何運算子`vpcEndpointId`。

   ii. 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。

   iii. 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。

e. 若要新增要記錄網路活動事件的其他事件來源，請選擇新增網路活動事件選取器。

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

5. 選擇儲存變更，以儲存您所做的變更。

## 更新現有的事件資料存放區以記錄網路活動事件

使用下列程序更新現有的事件資料存放區，以記錄網路活動事件。

> **Note**
>
> 您只能在 CloudTrail 事件類型的事件資料存放區上記錄網路活動事件。

1. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
2. 在 CloudTrail 主控台的左側導覽窗格中，選擇 Lake 下方的事件資料存放區。
3. 選擇事件資料存放區名稱。
4. 在網路活動事件中，選擇編輯。

   若要記錄網路活動事件，請執行下列步驟：

   a. 從網路活動事件來源中，選擇網路活動事件的來源。

   b. 在日誌選取器範本中，選擇範本。您可以選擇記錄所有網路活動事件、記錄所有網路活動存取遭拒的事件，或選擇自訂以建置自訂日誌選取器來篩選多個欄位，例如 `eventName`和 `vpcEndpointId`。

   c. （選用）輸入名稱以識別選取器。選擇器名稱在進階事件選擇器中列為名稱，如果您展開 JSON 檢視，則可檢視。

   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。如果您使用預先定義的日誌範本，則可略過此步驟。

      i. 對於排除或包含網路活動事件，您可以在 主控台中選擇下列欄位。

      - **eventName** – 您可以將任何運算子與 搭配使用`eventName`。您可以使用它來包含或排除任何事件，例如 `CreateKey`。
      - **errorCode** – 您可以使用它來篩選錯誤碼。目前，唯一支援的`errorCode`是 `VpceAccessDenied`。
      - **vpcEndpointId** – 識別操作通過的 VPC 端點。您可以搭配 使用任何運算子`vpcEndpointId`。

      ii. 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。

iii. 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。

e. 若要新增您要記錄網路活動事件的其他事件來源，請選擇新增網路活動事件選取器。

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

5. 選擇儲存變更，以儲存您所做的變更。

## 使用 記錄網路活動事件 AWS Command Line Interface

您可以設定追蹤或事件資料存放區，以使用 記錄網路活動事件 AWS CLI。

主題

- 範例：記錄線索的網路活動事件
- 範例：記錄事件資料存放區的網路活動事件

### 範例：記錄線索的網路活動事件

您可以使用 設定追蹤記錄網路活動事件 AWS CLI。執行 put-event-selectors命令來設定追蹤的進階事件選取器。

若要查看您的線索是否正在記錄網路活動事件，請執行 `get-event-selectors`命令。

主題

- 範例：記錄 CloudTrail 操作的網路活動事件
- 範例： 的日誌VpceAccessDenied事件 AWS KMS
- 範例：Amazon S3 的日誌VpceAccessDenied事件
- 範例：記錄特定 VPC 端點上的 EC2 VpceAccessDenied事件
- 範例：記錄多個事件來源的所有管理事件和網路活動事件

#### 範例：記錄 CloudTrail 操作的網路活動事件

下列範例示範如何設定您的線索，以包含 CloudTrail API 操作的所有網路活動事件，例如 `CreateTrail`和 `CreateEventDataStore`呼叫。`eventSource` 欄位的值為 `cloudtrail.amazonaws.com`。

```
aws cloudtrail put-event-selectors /
```

```
--trail-name TrailName /
--region region /
--advanced-event-selectors '[
    {
        "Name": "Audit all CloudTrail API calls through VPC endpoints",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["cloudtrail.amazonaws.com"]
            }
        ]
    }
]'
```

命令會傳回下列範例輸出。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Audit all CloudTrail API calls through VPC endpoints",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "cloudtrail.amazonaws.com"
                    ]
                }
            ]
        }
    ]
}
```

### 範例： 的日誌**VpceAccessDenied**事件 AWS KMS

下列範例顯示如何設定您的線索以包含 VpceAccessDenied的事件 AWS KMS。此範例會將 errorCode 欄位設定為等於 VpceAccessDenied 事件，而 eventSource 欄位設定為等於 kms.amazonaws.com。

```
aws cloudtrail put-event-selectors \
--region region /
--trail-name TrailName /
--advanced-event-selectors '[
    {
        "Name": "Audit AccessDenied AWS KMS events through VPC endpoints",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]'
```

命令會傳回下列範例輸出。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Audit AccessDenied AWS KMS events through VPC endpoints",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
```

```
                {
                    "Field": "eventSource",
                    "Equals": [
                        "kms.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
            ]
        }
    ]
}
```

### 範例：Amazon S3 的日誌**VpceAccessDenied**事件

下列範例顯示如何設定您的線索以包含 Amazon S3 VpceAccessDenied的事件。此範例會將 errorCode 欄位設定為等於 VpceAccessDenied 事件，而 eventSource 欄位設定為等於 s3.amazonaws.com。

```
aws cloudtrail put-event-selectors \
--region region /
--trail-name TrailName /
--advanced-event-selectors '[
    {
        "Name": "Log S3 access denied network activity events",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["s3.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
```

```
        ]
    }
]'
```

命令會傳回下列範例輸出。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Log S3 access denied network activity events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "s3.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
            ]
        }
    ]
}
```

範例：記錄特定 VPC 端點上的 EC2 **VpceAccessDenied**事件

下列範例示範如何設定您的線索，以包含特定 VPC 端點的 Amazon EC2 VpceAccessDenied事件。此範例會設定等於VpceAccessDenied事件errorCode的欄位、等於 eventSource的欄位ec2.amazonaws.com，以及vpcEndpointId等於感興趣的 VPC 端點。

```
aws cloudtrail put-event-selectors \
```

```
--region region /
--trail-name TrailName /
--advanced-event-selectors '[
    {
        "Name": "Audit AccessDenied EC2 events over a specific VPC endpoint",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["ec2.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            },
            {
                "Field": "vpcEndpointId",
                "Equals": ["vpce-example8c1b6b9b7"]
            }
        ]
    }
]'
```

命令會傳回下列範例輸出。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:111122223333:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Audit AccessDenied EC2 events over a specific VPC endpoint",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
```

```
                        "ec2.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                },
                {
                    "Field": "vpcEndpointId",
                    "Equals": [
                        "vpce-example8c1b6b9b7"
                    ]
                }
            ]
        }
    ]
}
```

**範例：記錄多個事件來源的所有管理事件和網路活動事件**

下列範例會設定追蹤記錄 CloudTrail AWS KMS AWS Secrets Manager、Amazon EC2 和 Amazon S3 事件來源的管理事件和所有網路活動事件。

```
aws cloudtrail put-event-selectors \
--region region /
--trail-name TrailName /
--advanced-event-selectors '[
    {
        "Name": "Log all management events",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["Management"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for CloudTrail APIs",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
```

```
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["cloudtrail.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for EC2",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["ec2.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for KMS",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for S3",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["s3.amazonaws.com"]
```

```
            }
        ]
    },
    {
        "Name": "Log all network activity events for Secrets Manager",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["secretsmanager.amazonaws.com"]
            }
        ]
    }
]'
```

命令會傳回下列範例輸出。

```
{
    "TrailARN": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TrailName",
    "AdvancedEventSelectors": [
        {
            "Name": "Log all management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for CloudTrail APIs",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
```

```
                {
                    "Field": "eventSource",
                    "Equals": [
                        "cloudtrail.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for EC2",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "ec2.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for KMS",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "kms.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for S3",
```

```
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "s3.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for Secrets Manager",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "secretsmanager.amazonaws.com"
                    ]
                }
            ]
        }
    ]
}
```

## 範例：記錄事件資料存放區的網路活動事件

您可以使用 將事件資料存放區設定為包含網路活動事件 AWS CLI。使用 [create-event-data-store](#)命令建立新的事件資料存放區，以記錄網路活動事件。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。

若要查看您的事件資料存放區是否包含網路活動事件，請執行 [get-event-data-store](#)命令。

```
aws cloudtrail get-event-data-store --event-data-store EventDataStoreARN
```

主題

- 範例：記錄 CloudTrail 操作的所有網路活動事件
- 範例： 的日誌VpceAccessDenied事件 AWS KMS
- 範例：記錄特定 VPC 端點上的 EC2 VpceAccessDenied事件
- 範例：Amazon S3 的日誌VpceAccessDenied事件
- 範例：記錄多個事件來源的所有管理事件和網路活動事件

### 範例：記錄 CloudTrail 操作的所有網路活動事件

下列範例示範如何建立事件資料存放區，其中包含與 CloudTrail 操作相關的所有網路活動事件，例如對 CreateTrail和 的呼叫CreateEventDataStore。eventSource 欄位的值設定為 cloudtrail.amazonaws.com。

```
aws cloudtrail create-event-data-store \
--name "EventDataStoreName" \
--advanced-event-selectors '[
    {
        "Name": "Audit all CloudTrail API calls over VPC endpoint",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["cloudtrail.amazonaws.com"]
            }
        ]
    }
]'
```

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": "Audit all CloudTrail API calls over VPC endpoint",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "cloudtrail.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

範例： 的日誌**VpceAccessDenied**事件 AWS KMS

下列範例示範如何建立事件資料存放區以包含 VpceAccessDenied的事件 AWS KMS。此範例會將 errorCode 欄位設定為等於 VpceAccessDenied 事件，而 eventSource 欄位設定為等於 kms.amazonaws.com。

```
aws cloudtrail create-event-data-store \
--name EventDataStoreName \
--advanced-event-selectors '[
     {
        "Name": "Audit AccessDenied AWS KMS events over VPC endpoints",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
```

```
            },
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]'
```

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": "Audit AccessDenied AWS KMS events over VPC endpoints",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "kms.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                }
            ]
```

```
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

範例：記錄特定 VPC 端點上的 EC2 **VpceAccessDenied**事件

下列範例示範如何建立事件資料存放區，以包含特定 VPC 端點的 Amazon EC2 VpceAccessDenied事件。此範例會設定等於VpceAccessDenied事件errorCode的欄位、等於eventSource的欄位ec2.amazonaws.com，以及vpcEndpointId等於感興趣的 VPC 端點。

```
aws cloudtrail create-event-data-store \
--name EventDataStoreName \
--advanced-event-selectors '[
     {
        "Name": "Audit AccessDenied EC2 events over a specific VPC endpoint",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["ec2.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            },
            {
                "Field": "vpcEndpointId",
                "Equals": ["vpce-example8c1b6b9b7"]
            }
        ]
    }
]'
```

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": "Audit AccessDenied EC2 events over a specific VPC endpoint",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "ec2.amazonaws.com"
                    ]
                },
                {
                    "Field": "errorCode",
                    "Equals": [
                        "VpceAccessDenied"
                    ]
                },
                {
                    "Field": "vpcEndpointId",
                    "Equals": [
                        "vpce-example8c1b6b9b7"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

### 範例：Amazon S3 的日誌**VpceAccessDenied**事件

下列範例示範如何建立事件資料存放區，以包含 Amazon S3 VpceAccessDenied的事件。此範例會將 errorCode 欄位設定為等於 VpceAccessDenied 事件，而 eventSource 欄位設定為等於 s3.amazonaws.com。

```
aws cloudtrail create-event-data-store \
--name EventDataStoreName \
--advanced-event-selectors '[
    {
        "Name": "Log S3 access denied network activity events",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["s3.amazonaws.com"]
            },
            {
                "Field": "errorCode",
                "Equals": ["VpceAccessDenied"]
            }
        ]
    }
]'
```

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": "Log S3 access denied network activity events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
```

```
                ]
            },
            {
                "Field": "eventSource",
                "Equals": [
                    "s3.amazonaws.com"
                ]
            },
            {
                "Field": "errorCode",
                "Equals": [
                    "VpceAccessDenied"
                ]
            }
        ]
    }
 ],
 "MultiRegionEnabled": true,
 "OrganizationEnabled": false,
 "RetentionPeriod": 366,
 "TerminationProtectionEnabled": true,
 "CreatedTimestamp": "2024-05-20T21:00:17.673000+00:00",
 "UpdatedTimestamp": "2024-05-20T21:00:17.820000+00:00"
}
```

範例：記錄多個事件來源的所有管理事件和網路活動事件

下列範例會更新目前僅記錄管理事件的事件資料存放區，以記錄多個事件來源的網路活動事件。若要更新事件資料存放區以新增事件選取器，請執行 get-event-data-store命令以傳回目前的進階事件選取器。然後，執行 update-event-data-store命令並傳入 --advanced-event-selectors，其中包含目前的選擇器和任何新的選擇器。若要記錄多個事件來源的網路活動事件，請針對您要記錄的每個事件來源包含一個選擇器。

```
aws cloudtrail update-event-data-store \
--event-data-store arn:aws:cloudtrail:us-east-1:123456789012:eventdatastore/EXAMPLE-
f852-4e8f-8bd1-bcf6cEXAMPLE \
--advanced-event-selectors '[
    {
        "Name": "Log all management events",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["Management"]
```

```
            }
        ]
    },
    {
        "Name": "Log all network activity events for CloudTrail APIs",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["cloudtrail.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for EC2",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["ec2.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for KMS",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]},
            {
                "Field": "eventSource",
                "Equals": ["kms.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for S3",
        "FieldSelectors": [
```

```
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["s3.amazonaws.com"]
            }
        ]
    },
    {
        "Name": "Log all network activity events for Secrets Manager",
        "FieldSelectors": [
            {
                "Field": "eventCategory",
                "Equals": ["NetworkActivity"]
            },
            {
                "Field": "eventSource",
                "Equals": ["secretsmanager.amazonaws.com"]
            }
        ]
    }
]'
```

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": "Log all management events",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "Management"
                    ]
                }
            ]
```

```
        },
        {
            "Name": "Log all network activity events for CloudTrail APIs",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "cloudtrail.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for EC2",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "ec2.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for KMS",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
```

```
                {
                    "Field": "eventSource",
                    "Equals": [
                        "kms.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for S3",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "s3.amazonaws.com"
                    ]
                }
            ]
        },
        {
            "Name": "Log all network activity events for Secrets Manager",
            "FieldSelectors": [
                {
                    "Field": "eventCategory",
                    "Equals": [
                        "NetworkActivity"
                    ]
                },
                {
                    "Field": "eventSource",
                    "Equals": [
                        "secretsmanager.amazonaws.com"
                    ]
                }
            ]
        }
    ],
    "MultiRegionEnabled": true,
```

```
    "OrganizationEnabled": false,
    "RetentionPeriod": 366,
    "TerminationProtectionEnabled": true,
    "CreatedTimestamp": "2024-11-20T21:00:17.673000+00:00",
    "UpdatedTimestamp": "2024-11-20T21:00:17.820000+00:00"
}
```

## 使用 AWS SDKs 記錄事件

執行 GetEventSelectors 操作，查看您的線索是否正在記錄網路活動事件。您可以執行 PutEventSelectors 操作，將線索設定為記錄網路活動事件。如需詳細資訊，請參閱 AWS CloudTrail API 參考。

執行 GetEventDataStore 操作，查看您的事件資料存放區是否正在記錄網路活動事件。您可以透過執行 CreateEventDataStore 或 UpdateEventDataStore 操作並指定進階事件選取器，將事件資料存放區設定為包含網路活動事件。如需詳細資訊，請參閱使用 建立、更新和管理事件資料存放區 AWS CLI和 AWS CloudTrail API 參考。

# 透過新增資源標籤索引鍵和 IAM 全域條件索引鍵來豐富 CloudTrail 事件

您可以在建立或更新事件資料存放區時新增資源標籤索引鍵、主體標籤索引鍵和 IAM 全域條件索引鍵，以豐富 CloudTrail 管理事件和資料事件。這可讓您根據業務內容來分類、搜尋和分析 CloudTrail 事件，例如成本分配和財務管理、操作和資料安全需求。您可以在 CloudTrail Lake 中執行查詢來分析事件。您也可以選擇聯合事件資料存放區，並在 Amazon Athena 中執行查詢。您可以使用 CloudTrail 主控台、 和 SDKs，將資源標籤金鑰AWS CLI和 IAM 全域條件金鑰新增至事件資料存放區。

> **Note**
>
> 您在資源建立或更新之後新增的資源標籤可能會在 CloudTrail 事件中反映這些標籤之前遇到延遲。刪除資源的 CloudTrail 事件可能不會包含標籤資訊。
> IAM 全域條件金鑰一律會顯示在查詢的輸出中，但資源擁有者可能無法看見。

當您將資源標籤索引鍵新增至擴充事件時，CloudTrail 會包含與 API 呼叫中所涉及資源相關聯的所選標籤索引鍵。

當您將 IAM 全域條件金鑰新增至事件資料存放區時，CloudTrail 會包含授權程序期間評估之所選條件金鑰的相關資訊，包括主體、工作階段和請求本身的其他詳細資訊。

> **Note**
>
> 設定 CloudTrail 包含條件索引鍵或主體標籤，並不表示每個事件都會出現此條件索引鍵或主體標籤。例如，如果您已設定 CloudTrail 包含特定全域條件金鑰，但未在特定事件中看到，這表示該金鑰與該動作的 IAM 政策評估無關。

新增資源標籤金鑰或 IAM 條件金鑰後，CloudTrail 會在 CloudTrail 事件中包含 `eventContext` 欄位，以提供 API 動作的所選內容資訊。

當事件不包含 `eventContext` 欄位時，有一些例外狀況，包括下列項目：

- 與已刪除資源相關的 API 事件可能有也可能沒有資源標籤。
- `eventContext` 欄位不會有延遲事件的資料，也不會出現於 API 呼叫後更新的事件。例如，如果 Amazon EventBridge 發生延遲或中斷，則在解決中斷之後，事件的標籤可能會保留一段時間。有些 AWS 服務將會遇到較長的延遲。如需詳細資訊，請參閱CloudTrail 中豐富事件的資源標籤更新。
- 如果您修改或刪除用於豐富事件的 AWSServiceRoleForCloudTrailEventContext 服務連結角色，CloudTrail 不會將任何資源標籤填入 `eventContext` 。

> **Note**
>
> `eventContext` 欄位只會出現在設定為包含資源標籤索引鍵、主體標籤索引鍵和 IAM 全域條件索引鍵的事件資料存放區事件中。交付至事件歷史記錄、Amazon EventBridge、可使用 AWS CLI `lookup-events`命令檢視，以及交付至追蹤的事件，將不會包含 `eventContext` 欄位。

主題

- AWS 服務 支援資源標籤
- AWS 服務 支援 IAM 全域條件金鑰
- 事件範例

## AWS 服務 支援資源標籤

所有 AWS 服務 支援資源標籤。如需詳細資訊，請參閱支援 的 服務 AWS Resource Groups Tagging API。

### CloudTrail 中豐富事件的資源標籤更新

設定為這樣做時，CloudTrail 會擷取資源標籤的相關資訊，並使用它們在豐富的事件中提供資訊。使用資源標籤時，在某些情況下，系統請求事件時可能無法準確反映資源標籤。在標準操作期間，在資源建立時間套用的標籤一律存在，而且會有極少或沒有延遲。不過，下列服務預期在 CloudTrail 事件中出現資源標籤變更的延遲：

- Amazon Chime Voice Connector
- AWS CloudTrail
- AWS CodeConnections
- Amazon DynamoDB
- Amazon ElastiCache
- Amazon Keyspaces (適用於 Apache Cassandra)
- Amazon Kinesis
- Amazon Lex
- Amazon MemoryDB
- Amazon S3
- Amazon Security Lake
- AWS Direct Connect
- AWS IAM Identity Center
- AWS Key Management Service
- AWS Lambda
- AWS Marketplace 廠商洞見
- AWS Organizations
- AWS Payment Cryptography
- Amazon Simple Queue Service

服務中斷也可能導致資源標籤資訊的更新延遲。如果發生服務中斷延遲，後續 CloudTrail 事件將包含 `addendum` 欄位，其中包含資源標籤變更的相關資訊。此額外資訊將依指定使用，以提供富集的 CloudTrailevents。

## AWS 服務 支援 IAM 全域條件金鑰

下列 AWS 服務 支援擴充事件的 IAM 全域條件索引鍵：

- AWS Certificate Manager
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch Logs
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- Amazon Cognito Sync
- Amazon Comprehend
- Amazon Comprehend Medical
- Amazon Connect Voice ID
- AWS Control Tower
- Amazon Data Firehose
- Amazon Elastic Block Store
- Elastic Load Balancing
- AWS 終端用戶訊息社交服務
- Amazon EventBridge
- Amazon EventBridge 排程器
- Amazon Data Firehose
- Amazon FSx
- AWS HealthImaging
- AWS IoT Events
- AWS IoT FleetWise
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS IoT Wireless
- Amazon Kendra
- AWS KMS

- AWS Lambda
- AWS License Manager
- Amazon Lookout for Equipment
- Amazon Lookout for Vision
- AWS Network Firewall
- AWS Payment Cryptography
- Amazon Personalize
- AWS Proton
- Amazon Rekognition
- Amazon SageMaker AI
- AWS Secrets Manager
- Amazon Simple Email Service (Amazon SES)
- Amazon Simple Notification Service (Amazon SNS)
- Amazon SQS
- AWS Step Functions
- AWS Storage Gateway
- Amazon SWF
- AWS Supply Chain
- Amazon Timestream
- InfluxDB 的 Amazon Timestream
- Amazon Transcribe
- AWS Transfer Family
- AWS Trusted Advisor
- Amazon WorkSpaces
- AWS X-Ray

## 適用於豐富事件的支援 IAM 全域條件索引鍵

下表列出 CloudTrail 擴充事件支援的 IAM 全域條件索引鍵，其中包含範例值：

全域條件金鑰和範例值

| 金鑰 | 範例值 |
| --- | --- |
| aws:FederatedProvider | 「*IdP*」 |
| aws:TokenIssueTime | "*123456789* " |
| aws:MultiFactorAuthAge | "99" |
| aws:MultiFactorAuthPresent | 「*true*」 |
| aws:SourceIdentity | "*UserName*" |
| aws:PrincipalAccount | "111122223333" |
| aws:PrincipalArn | "arn：aws：iam：：*555555555555#role/myRole* " |
| aws:PrincipalIsAWSService | "*false*" |
| aws:PrincipalOrgI D | "*o-rganization* " |
| aws:PrincipalOrgPaths | 【「*####/path-of-org* 」】 |
| aws:PrincipalServiceName | "*cloudtrail.amazonaws.com* " |
| aws:PrincipalServiceNamesList | 【"*cloudtrail.amazonaws.com"#" s3.amazonaws.com* "】 |
| aws:PrincipalType | 「*AssumedRole* 」 |
| aws:userid | "*userid*" |
| aws:username | "*username*" |
| aws:RequestedRegion | *us-east-2* " |
| aws:SecureTransport | 「*true*」 |
| aws:ViaAWSService | "*false*" |

| 金鑰 | 範例值 |
| --- | --- |
| aws:CurrentTime | "*2025-04-30 15#30#00* " |
| aws:EpochTime | "*1746049800* " |
| aws:SourceAccount | "*111111111111* " |
| aws:SourceOrgID | "*o-rganization* " |

## 事件範例

在下列範例中， eventContext 欄位包含值aws:ViaAWSService為 的 IAM 全域條件金鑰false，這表示 API 呼叫不是由 進行 AWS 服務。


```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "ASIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/admin",
        "accountId": "123456789012",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "ASIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/admin",
                "accountId": "123456789012",
                "userName": "admin"
            },
            "attributes": {
                "creationDate": "2025-01-22T22:05:56Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2025-01-22T22:06:16Z",
    "eventSource": "cloudtrail.amazonaws.com",
    "eventName": "GetTrailStatus",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "192.168.0.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:133.0)
 Gecko/20100101 Firefox/133.0",
    "requestParameters": {
        "name": "arn:aws:cloudtrail:us-east-1:123456789012:trail/myTrail"
    },
    "responseElements": null,
    "requestID": "d09c4dd2-5698-412b-be7a-example1a23",
    "eventID": "9cb5f426-7806-46e5-9729-exampled135d",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "cloudtrail.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true",
    "eventContext": {
        "requestContext": {
            "aws:ViaAWSService": "false"
        },
        "tagContext": {}
    }
}
```


# CloudTrail 記錄管理、資料和網路活動事件的內容

此頁面說明管理、資料或網路活動事件的記錄內容。

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。

> **Note**
>
> 等豐富事件的欄位`eventContext`僅適用於管理事件和資料事件。它們不適用於網路事件。

**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） 區域中執行的 CreateBucket API 事件，會從執行 Amazon S3 端點 的 AWS 主機取得其時間戳記`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。目前版本為 1.11。

`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 `1.10` 的 `eventVersion`，其中 `1` 是主要版本，`10` 是次要版本。

如果 CloudTrail 對不向下相容的事件結構進行變更，主要版本就會增加。這包括已經存在的 JSON 欄位，或變更欄位內容的呈現方式 (例如，日期格式)。如果 CloudTrail 將新欄位新增至事件結構，次要版本就會增加。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 引進新的事件類型，但卻未修改事件結構，則事件版本不會變更。

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。為確保您的應用程式預期的欄位存在，我們建議您對次要版本執行「大於或等於」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：

- 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，Amazon CloudWatch 的 eventSource 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**

提出請求 AWS 區域 的 ，例如 us-east-2。請參閱 CloudTrail 支援的區域。

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

發出請求的代理程式，例如 AWS 管理主控台、 AWS 服務、 AWS SDKs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。對於設定為事件大小上限為 1 MB 的事件資料存放區，只有在事件承載超過 1 MB 且超過欄位大小上限時，才會截斷欄位內容。

範例值如下：

- `lambda.amazonaws.com` - 使用 AWS Lambda提出請求。
- `aws-sdk-java` - 使用 適用於 Java 的 AWS SDK提出請求。
- `aws-sdk-ruby` - 使用 適用於 Ruby 的 AWS SDK提出請求。
- `aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5` – 使用 AWS CLI Linux 上安裝的 提出請求。

> **Note**
>
> 對於源自 的事件 AWS，如果 CloudTrail 知道是哪個 AWS 服務 呼叫，則此欄位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

如果請求傳回錯誤，則表示 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。對於設定為事件大小上限為 1 MB 的事件資料存放區，只有在事件承載超過 1 MB 且超過欄位大小上限時，才會截斷欄位內容。

對於網路活動事件，發生 VPC 端點政策違規時，錯誤碼為 `VpceAccessDenied`。

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 會擷取服務在處理例外狀況時所記錄的訊息。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。對於設定為事件大小上限為 1 MB 的事件資料存放區，只有在事件承載超過 1 MB 且超過欄位大小上限時，才會截斷欄位內容。

對於網路活動事件，當發生 VPC 端點政策違規時， `errorMessage` 一律會是下列訊息：`The request was denied due to a VPC endpoint policy`。如需 VPC 端點政策違規存取遭拒事件的詳細資訊，請參閱《IAM 使用者指南》中的存取遭拒錯誤訊息範例。如需顯示 VPC 端點政策違規的網路活動事件範例，請參閱本指南中的網路活動事件。

> **Note**
>
> 有些 AWS 服務會在事件中提供 `errorCode`和 `errorMessage`做為最上層欄位。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)。這些參數會記錄在適當 AWS 服務的 API 參考文件中。此欄位的大小上限為 100 KB。當欄位大小超過 100 KB 時，會省略`requestParameters`內容。對於設定為事件大小上限為 1 MB 的事件資料存放區，只有在事件承載超過 1 MB 且超過欄位大小上限時，才會省略欄位內容。

來自：1.0

選用：False

### responseElements

對於進行變更的動作（建立、更新或刪除動作），如果有回應元素。對於 `readOnly` APIs，此欄位為 `null`。如果動作

不會傳回回應元素，此欄位為 null。動作的回應元素記錄在 API 參考中
文件 AWS 服務。

此欄位的大小上限為 100 KB。當欄位大小超過 100 KB 時，會省略reponseElements內容。對於設定為事件大小上限為 1 MB 的事件資料存放區，只有在事件承載超過 1 MB 且超過欄位大小上限時，才會省略欄位內容。

此responseElements值可協助您追蹤請求
搭配 AWS 支援。x-amz-request-id 和 x-amz-id-2
包含的資訊可協助您使用 追蹤請求 支援。這些值為
與 服務在回應請求時傳回的請求相同
會啟動事件，因此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。當欄位大小超過 28 KB 時，會省略additionalEventData內容。對於設定為事件大小上限為 1 MB 的事件資料存放區，只有在事件承載超過 1 MB 且超過欄位大小上限時，才會省略欄位內容。

的內容additionalEventData是可變的。例如，對於AWS 管理主控台 登入事件，Yes如果請求是由根使用者或 IAM 使用者使用多重要素驗證 (MFA) 提出， additionalEventData可以包含值為 MFAUsed的欄位。

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。對於設定為事件大小上限為 1 MB 的事件資料存放區，只有在事件承載超過 1 MB 且超過欄位大小上限時，才會截斷欄位內容。

來自：1.01

選用：True

**eventID**

CloudTrail 所產生的 GUID 可唯一識別每個事件。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` - 您帳戶中登入 AWS 管理主控台的使用者 (根、IAM、聯合、SAML 或 SwitchRole)。
- `AwsVpceEvents` – CloudTrail 網路活動事件可讓 VPC 端點擁有者記錄使用其 VPC 端點從私有 VPC 到 的 AWS API 呼叫 AWS 服務。若要記錄網路活動事件，VPC 端點擁有者必須為事件來源啟用網路活動事件。

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 resources欄位中的範例日誌，請參閱《IAM 使用者指南AWS STS 》中的 CloudTrail 日誌檔案中的 API 事件或《 AWS Key Management Service 開發人員指南》中的記錄 AWS KMS 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。當欄位大小超過 100 KB 時，會省略serviceEventDetails內容。對於設定為事件大小上限為 1 MB 的事件資料存放區，只有在事件承載超過 1 MB 且超過欄位大小上限時，才會省略欄位內容。

來自：1.05

選用：True

**sharedEventID**

CloudTrail 產生的 GUID，可從傳送至不同 AWS 帳戶的相同 AWS 動作唯一識別 CloudTrail 事件。

例如，帳戶使用屬於另一個帳戶的 AWS KMS key 時，使用 KMS 金鑰的帳戶以及擁有 KMS 金鑰的帳戶會收到相同動作的個別 CloudTrail 事件。針對此 AWS 動作傳遞的每個 CloudTrail 事件都會共用相同的 sharedEventID，但也有唯一的 eventID和 recipientAccountID。

如需詳細資訊，請參閱sharedEventID 範例。

> **Note**
>
> 只有在 CloudTrail 事件交付至多個帳戶時，才會顯示 sharedEventID 欄位。如果發起人和擁有者是相同的 AWS 帳戶，則 CloudTrail 只會傳送一個事件，而且不會顯示 sharedEventID 欄位。

來自：1.03

選用：True

### vpcEndpointId

識別 VPC 向其他服務提出請求的 VPC 端點 AWS ，例如 Amazon EC2。

> **Note**
>
> 對於由 AWS 和 透過 AWS 服務的 VPC 產生的事件，此欄位通常是 AWS Internal或服務名稱。

來自：1.04

選用：True

### vpcEndpointAccountId

識別請求已周遊之對應端點的 VPC 端點擁有者 AWS 帳戶 ID。

> **Note**
>
> 對於由 AWS 和 透過 AWS 服務的 VPC 產生的事件，此欄位通常是 AWS Internal或服務名稱。

開始日期：1.09

選用：True

### eventCategory

顯示事件類別。事件類別用於 LookupEvents呼叫，以篩選管理事件。

- 對於管理事件，值為 Management。
- 對於資料事件，值為 Data。

- 對於網路活動事件，值為 NetworkActivity。

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**- 將事件記錄到 CloudTrail 的服務發生中斷，無法將事件記錄到 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**

值為 `true`或 的字串`false`，顯示事件是否來自 AWS 管理主控台 工作階段。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

**eventContext**

對於已設定為包含資源標籤金鑰或 IAM 全域條件金鑰的事件資料存放區，此欄位會出現在記錄的擴充事件中。如需詳細資訊，請參閱[透過新增資源標籤索引鍵和 IAM 全域條件索引鍵來豐富 CloudTrail 事件]。

內容包括下列項目：

- `requestContext` – 包含授權程序期間評估之 IAM 全域條件金鑰的相關資訊，包括委託人、工作階段、網路和請求本身的其他詳細資訊。
- `tagContext` – 包括與 API 呼叫所涉及資源相關聯的標籤，以及與 IAM 主體相關聯的標籤，例如角色或使用者。如需詳細資訊，請參閱控制 IAM 主體的存取。

  與已刪除資源相關的 API 事件將不會有資源標籤。

> **Note**
>
> `eventContext` 欄位僅存在於設定為包含資源標籤金鑰和 IAM 全域條件金鑰的事件資料存放區的事件中。交付至事件歷史記錄、Amazon EventBridge、可使用 AWS CLI `lookup-events`命令檢視，以及交付至追蹤的事件，將不會包含 `eventContext` 欄位。

原因：1.11

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。對於設定為事件大小上限為 1 MB 的事件資料存放區，只有在事件承載超過 1 MB 且超過欄位大小上限時，才會截斷欄位內容。

自：1.08

選用：True

**`tlsDetails`**

顯示服務 API 呼叫中用戶端所提供主機名稱的 Transport Layer Security (TLS) 版本、加密套件，以及完整網域名稱 (FQDN) 的相關資訊，而這通常會是服務端點的 FQDN。如果預期的資訊遺失或空白，CloudTrail 仍會記錄部分 TLS 詳細資訊。例如，如果 TLS 版本和加密套件存在，但 `HOST` 標頭為空，則可用的 TLS 詳細資訊仍會記錄在 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。

- **keyExchange** - TLS 交握中使用的金鑰交換方法。此欄位指出連線是使用傳統密碼編譯還是後量子密碼編譯。範例值X25519MLKEM768包括後量子 TLS 1.3、傳統 x25519 TLS 1.3 和 secp256r1 TLS 1.2。

> **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 AWS 服務 代表您進行，則 tlsDetails 欄位不存在。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

## 事件大小上限為 1 MB 的欄位截斷順序

當您使用 CloudTrail 主控台、 和 SDKs 建立或更新事件資料存放區時AWS CLI，您可以將事件大小上限從 256 KB 擴展到 1 MB。

擴展事件大小有助於分析和疑難排解事件，因為它可讓您查看通常會被截斷或省略的欄位的完整內容。

當事件承載超過 1 MB 時，CloudTrail 會依下列順序截斷欄位：

- annotation
- requestID
- additionalEventData
- serviceEventDetails
- userAgent
- errorCode
- eventContext
- responseElements
- requestParameters

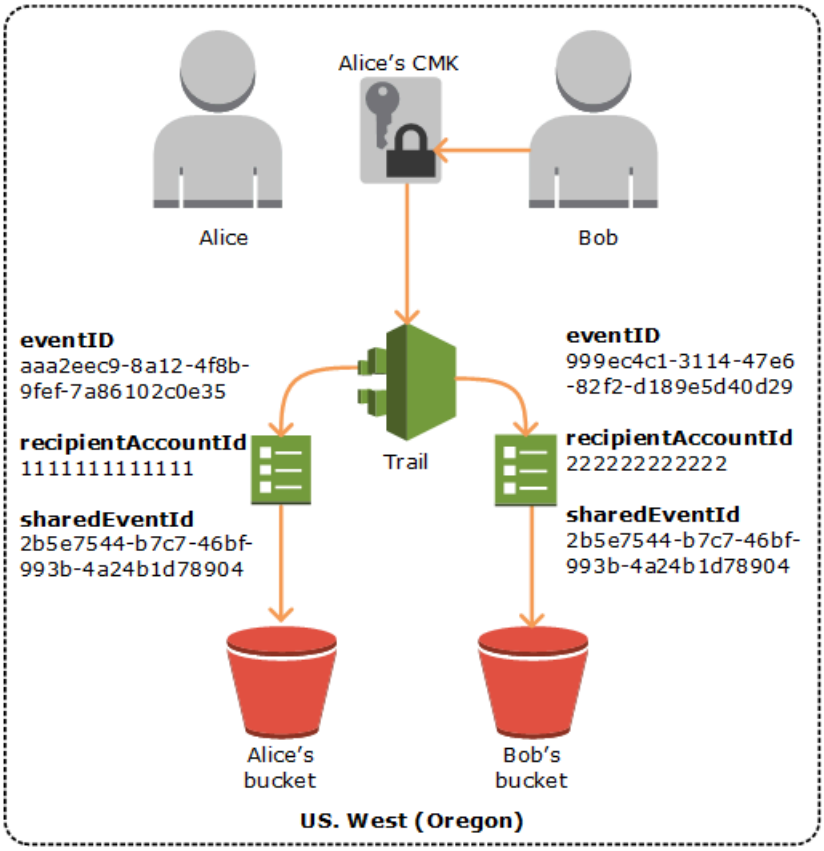
- `errorMessage`

如果即使在截斷之後，事件承載仍無法減少到 1 MB 以下，則會發生錯誤。

## sharedEventID 範例

下列範例說明 CloudTrail 如何傳送交付動作的兩個事件：

1. Alice 有 AWS 帳戶 ((111111111111) 並建立 AWS KMS key。她是此 KMS 金鑰的擁有者。
2. Bob 有 AWS 帳戶 ((222222222222)。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 傳送兩個不同的事件。
    - 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。



# 彙總事件的 CloudTrail 記錄內容

AWS CloudTrail 彙總事件記錄包含的欄位與其 JSON 承載中的其他 CloudTrail 事件不同。彙總事件包含下列欄位：

**`eventVersion`**

彙總事件的版本。

來自：1.0

選用：False

**`accountId`**

收到此事件的帳戶 ID。

來自：1.0

選用：False

**`eventId`**

CloudTrail 產生的 GUID，可唯一識別每個彙總事件。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：1.0

選用：False

**`eventCategory`**

識別事件的類別。對於彙總的事件，此值一律為 `Aggregated`。當您依類別查詢事件時，請使用此欄位進行篩選。

來自：1.0

選用：False

**`eventType`**

識別彙總事件的類型。對於彙總的事件，此值為 `AwsAggregatedEvent`。

來自：1.0

選用：False

**awsRegion**

彙總到此記錄中 AWS 區域 的原子 CloudTrail 事件的 ，例如 ap-northeast-1。這通常是進行服務 API 呼叫的區域。

來自：1.0

選用：False

**eventSource**

記錄基礎事件 AWS 的服務。

來自：1.0

選用：False

**timeWindow**

將原子 CloudTrail 事件彙總到此彙總事件記錄中的時間間隔。timeWindow 欄位包含視窗開始時間、視窗結束時間和視窗大小等詳細資訊。

來自：1.0

選用：False

**windowStart**

彙總視窗的開頭，包含國際時間 (UTC)，以 ISO-8601 格式表示。

來自：1.0

選用：False

**windowEnd**

彙總視窗的結尾，以 UTC 表示，以 ISO-8601 格式表示。

來自：1.0

選用：False

**windowSize**

彙總視窗的持續時間。差異windowEnd – windowStart應對應至 windowSize。以 ISO-8601 格式windowSize表示。

來自：1.0

選用：False

**summary**

基礎原子事件的彙總摘要，依主要維度 （例如 resourceARN或 userIdentity) 分組eventName，並選擇性地依其他維度 （例如 userAgent、sourceIpAddress、) 細分errorCodes。

來自：1.0

選用：False

摘要包含下列欄位：

**primaryDimension**

此 的主要彙總維度AwsAggregatedEvent。這是彙總資料的主要檢視。例如，在API_ACTIVITY彙總範本中，主要維度為 eventName；在RESOURCE_ACCESS範本中，其為 resourceARN；在USER_ACTIONS範本中，其為 userIdentity。

來自：1.0

選用：False

**details**

提供彙總原子事件詳細資訊的其他維度。每個詳細資訊物件可能會根據彙總範本提供相同基礎事件的額外檢視，例如 userIdentity、、 eventName resourceARNuserAgent和 sourceIpAddress 。

來自：1.0

選用：False

每個詳細資訊都提供下列資訊：

**dimension**

用於將彙總事件分組的維度名稱。常見值包括：

- eventName
- resourceARN
- userIdentity
- userAgent
- sourceIpAddress

來自：1.0

選用：False

**statistics**

此維度的統計資料清單，其中每個項目代表一個儲存貯體 （例如，一個事件名稱或一個資源 ARN) 及其彙總值。

來自：1.0

選用：False

統計資料中的每個項目都包含下列資訊：

**name**

關聯維度內此統計資料的儲存貯體識別符或索引鍵。

**value**

指定維度中指定名稱的彙總數值。

**aggregationType**

套用至此維度運算`statistics.value`的彙總類型。允許的值：

- `Count` – 事件數量。

來自：1.0

選用：False

**addendum**

承載有關延遲交付或更新現有 AggregatedEvent 的中繼資料。

來自：1.0

選用：False

**reason**

`AwsAggregatedEvent` 延遲、更新或以其他方式補充 的原因。常見值可以包括 （非詳盡）：

- `DELIVERY_DELAY` – 彙總資料的交付延遲 （例如網路問題或大量）。
- `UPDATED_DATA` – 已重新計算或更正彙總的資料。
- `SERVICE_OUTAGE` – 基礎服務中斷會影響事件可用性。

來自：1.0

選用：True

## 彙總事件範例

以下是 CloudTrail 彙總事件 () 的範例AwsAggregatedEvent。在此範例中，CloudTrail 會在 us-east-1 區域的cloudtrail-data.amazonaws.com五分鐘時段內彙總對 的PutAuditEvents呼叫。摘要區塊會顯示主要彙總維度 (eventName)，並在時段內發生 30 次PutAuditEvents呼叫。詳細資訊項目會進一步依 resourceARN、userAgent、 userIdentity和 細分這些呼叫sourceIpAddress，以顯示活動如何分散到資源、委託人和用戶端。

```
{
    "eventVersion": "1.0",
    "accountId": "111122223333",
    "eventId": "4da798a8-1db6-4d17-8b51-4c33df06b56d",
    "eventCategory": "Aggregated",
    "eventType": "AwsAggregatedEvent",
    "awsRegion": "us-east-1",
    "eventSource": "cloudtrail-data.amazonaws.com",
    "timeWindow":
    {
        "windowStart": "2025-10-30 23:45:00",
        "windowEnd": "2025-10-30 23:50:00",
        "windowSize": "PT5M"
    },
    "summary":
    {
        "primaryDimension":
        {
            "dimension": "eventName",
            "statistics":
            [
                {
                    "name": "PutAuditEvents",
                    "value": 30
                }
            ],
            "aggregationType": "Count"
        },
        "details":
        [
```

```
            {
                "dimension": "resourceARN",
                "statistics":
                [
                    {
                        "name": "arn:aws:cloudtrail:us-
east-1:111122223333:channel/1234abcd-12ab-34cd-56ef-1234567890ab",
                        "value": 20
                    },
                    {
                        "name": "arn:aws:cloudtrail:us-
east-1:111122223333:channel/6789abcd-12ab-34cd-56ef-6789012345ab",
                        "value": 10
                    }
                ],
                "aggregationType": "Count"
            },
            {
                "dimension": "userIdentity",
                "statistics":
                [
                    {
                        "name": "AWSAccount:111122223333",
                        "value": 20
                    },
                    {
                        "name": "AWSService:AWS Internal",
                        "value": 10
                    }
                ],
                "aggregationType": "Count"
            },
            {
                "dimension": "userAgent",
                "statistics":
                [
                    {
                        "name": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0)
 Gecko/20100101 Firefox/102.0",
                        "value": 20
                    },
                    {
                        "name": "AWS Internal",
                        "value":10
```

```
                    }
                ],
                "aggregationType": "Count"
            },
            {
                "dimension": "sourceIpAddress",
                "statistics":
                [
                    {
                        "name": "1.2.3.4",
                        "value": 20
                    },
                    {
                        "name": "AWS Internal",
                        "value": 10
                    }
                ],
                "aggregationType": "Count"
            }
        ]
    }
}
```

# 追蹤的 Insights 事件 CloudTrail 記錄內容

線索的AWS CloudTrail Insights 事件記錄包括與其 JSON 結構中其他 CloudTrail 事件不同的欄位，有時稱為承載。追蹤的 CloudTrail Insights 事件包含下列欄位：

- **`eventVersion`** – 事件的版本。

  自：1.07

  選用：False

- **`eventType`** – 事件類型。值一律`AwsCloudTrailInsight`適用於 Insights 事件。

  自：1.07

  選用：False

- **`eventID`** – CloudTrail 產生的 GUID，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。

自：1.07

選用：False

- **eventTime** – Insights 事件開始或停止的時間，以國際標準時間 (UTC) 表示。

  自：1.07

  選用：False

- **awsRegion** – 發生 Insights 事件 AWS 區域 的 ，例如 us-east-2。

  自：1.07

  選用：False

- **recipientAccountId** – 代表收到此事件的帳戶 ID。

  自：1.07

  選用：True

- **sharedEventID** – CloudTrail Insights 產生的 GUID，用於唯一識別 Insights 事件。 在起始和結束 Insights 事件之間sharedEventID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** – 線索的 CloudTrail Insights 事件記錄包含一個insightDetails區塊，其中包含 Insights 事件的基礎觸發條件的相關資訊，例如事件來源、使用者身分、使用者代理程式、歷史平均值或基準、統計資料、API 名稱，以及事件是 Insights 事件的開始還是結束。

  自：1.07

  選用：False

  - **state** – 事件是開始或結束 Insights 事件。此值可以為 Start 或 End。

    自：1.07

    選用：False

  - **eventSource** – 做為異常活動來源 AWS 的服務，例如 ec2.amazonaws.com。

自：1.07

選用：False

- **eventName** – Insights 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`。

  自：1.07

  選用：False

- **errorCode** – 異常活動的錯誤代碼。另請參閱 `errorCode` 中的 CloudTrail 記錄管理、資料和網路活動事件的內容。

  自：1.07

  選用：True

- **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）的相關資訊，以及與 CloudTrail 分析以產生 Insights 事件之事件相關聯的錯誤代碼。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，或帳戶在基準期間測量的對主體 API 的呼叫或錯誤的典型平均速率、觸發 Insights 事件的呼叫或錯誤的平均速率、以分鐘為單位的 Insights 事件持續時間，以及基準測量期間的持續時間，以分鐘為單位。

    自：1.07

    選用：False

    - **baseline** – 在 Insights 事件之帳戶主體 API 的基準期間，每分鐘 API 呼叫或錯誤，計算時間是 Insights 事件開始之前的七天。

      自：1.07

選用：False

- **average** – 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

- **insight** – 對於開始的 Insights 事件，此值是異常活動開始期間每分鐘 API 呼叫或錯誤的平均數量。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

- **average** – 在異常活動期間每分鐘記錄的平均 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（主體 API 上異常活動的開始到結束期間）。 `insightDuration`同時發生在開始和結束 Insights 事件中。

  自：1.07

  選用：False

- **baselineDuration** – 基準期間（在主體 API 上測量正常活動的期間）的持續時間，以分鐘為單位。 至少`baselineDuration`為 Insights 事件之前的七天 (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** – 包括與異常和基準活動相關的使用者身分、使用者代理程式和錯誤碼的相關資訊。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。如果存在，這些值只會出現在個別屬性中一次。不同的屬性值可以有不同的 userIdentityArn、 userAgent或 errorCode值，但每個屬性執行個體只會包含一個 userIdentityArn、 userAgent或 的值errorCode。

  自：1.07

  選用：False

- **insight** – 顯示最多前五個屬性值的區塊，這些值導致在異常活動期間進行的 API 呼叫或錯誤，從最大數量的 API 呼叫或錯誤降至最小。它也會顯示異常活動期間屬性值進行的 API 呼叫或錯誤的平均次數。

  自：1.07

  選用：False

  - **value** – 導致 API 呼叫或在異常活動期間進行的錯誤的屬性。

    自：1.07

    選用：False False

  - **average** – 在 value 欄位中屬性的異常活動期間，每分鐘 API 呼叫或錯誤的次數。

    自：1.07

    選用：False False

- **baseline** – 區塊，顯示在正常活動期間對 API 呼叫或錯誤貢獻最多的前五個屬性值，從 API 呼叫的最大數量或錯誤降至最小。它也會顯示正常活動期間屬性值所做的 API 呼叫或錯誤的平均數量。

  自：1.07

  選用：False False

  - **value** – 在正常活動期間導致 API 呼叫或錯誤的屬性。

    自：1.07

    選用：False False

  - **average** – value欄位中屬性的 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

Optional：False False

- **eventCategory** – 事件的類別。值一律Insight適用於 Insights 事件。

  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 Insights 事件。

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。attributions 區塊也會顯示使用者代理程式是 codedeploy.amazonaws.com，這表示使用 AWS CodeDeploy 主控台執行 API 呼叫的最上層使用者身分。

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
                }
              ]
            }
          ]
        }
      }
```

# 事件資料存放區的 Insights 事件 CloudTrail 記錄內容

事件資料存放區的AWS CloudTrail Insights 事件記錄包括與其 JSON 結構中其他 CloudTrail 事件不同的欄位，有時稱為承載。事件資料存放區的 CloudTrail Insights 事件記錄包含下列欄位：

> **Note**
>
> `insightValue`、`baselineValue`、 `insightAverage`和 `baselineAverage` 欄位內的 `attributionsinsightContext`將於 2025 年 6 月 23 日開始棄用。

- **`eventVersion`** – 日誌事件格式的版本。

  選用：False
- **`eventCategory`** – 事件的類別。值一律`Insight`適用於 Insights 事件。

  選用：False
- **`eventType`** – 事件類型。值一律`AwsCloudTrailInsight`適用於 Insights 事件。

  選用：False

- **eventID** – CloudTrail 產生的 GUID，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。

  選用：False

- **eventTime** – Insights 事件開始或停止的時間，以國際標準時間 (UTC) 表示。

  選用：False

- **awsRegion** – Insights 事件發生 AWS 區域 的 ，例如 us-east-2。

  選用：False

- **recipientAccountId** – 代表收到此事件的帳戶 ID。

  選用：True

- **sharedEventID** – CloudTrail Insights 產生的 GUID，用於唯一識別 Insights 事件。 在起始和結束 Insights 事件之間sharedEventID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。

  選用：False

- **addendum** – 如果事件交付延遲，或記錄事件後現有事件的其他資訊變成可用，則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。另請參閱 addendum 中的 CloudTrail 記錄管理、資料和網路活動事件的內容。

  選用：True

- **insightSource** – 收集已分析之管理事件的來源事件資料存放區。

  選用：False

- **insightState** – 事件是開始或結束 Insights 事件。此值可以為 Start 或 End。

  選用：False

- **insightEventSource** – AWS 服務 是異常活動的來源，例如 ec2.amazonaws.com。

  選用：False

- **insightEventName** – Insights 事件的名稱，通常是異常活動來源的 API 名稱。

  選用：False

- **insightErrorCode** – 異常活動的錯誤代碼。另請參閱 errorCode 中的 CloudTrail 記錄管理、資料和網路活動事件的內容。

選用：True

- **insightType** – Insights 事件的類型。此值可以為 ApiCallRateInsight 或 ApiErrorRateInsight。

  選用：False

- **insightContext** – 包含 Insights 事件基礎觸發的相關資訊，例如使用者身分、使用者代理程式、歷史平均值或基準，以及 Insights 持續時間和平均值。

  選用：False

  - **baselineAverage** – 在 Insights 事件之帳戶主體 API 的基準期間，每分鐘 API 呼叫或錯誤的平均次數，計算時間是 Insights 事件開始之前的七天。

    選用：False

  - **insightAverage** – 對於開始的 Insights 事件，此值是異常活動開始期間每分鐘 API 呼叫或錯誤的平均數量。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。

    選用：False

  - **baselineDuration** – 基準期間（在主體 API 上測量正常活動的期間）的持續時間，以分鐘為單位。 至少baselineDuration為 Insights 事件之前的七天 (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。

    選用：False

  - **insightDuration** – Insights 事件的持續時間，以分鐘為單位（主體 API 上異常活動的開始到結束期間）。 insightDuration同時發生在開始和結束 Insights 事件中。

    選用：False

  - **attributions** – 包括與異常和基準活動相關的使用者身分、使用者代理程式或錯誤碼的相關資訊。

    選用：True

    > **Note**
    >
    > insightValue、baselineValue、 insightAverage和 baselineAverage 欄位內的 attributionsinsightContext將於 2025 年 6 月 23 日開始棄用。

- **attribute** – 包含屬性類型。此值可以是 userIdentityArn、userAgent 或 errorCode。如果存在，這些值只會出現在個別屬性中一次。不同的屬性值可以有不同的 userIdentityArn、 userAgent或 errorCode值，但每個屬性執行個體只會包含一個 userIdentityArn、 userAgent或 的值errorCode。

  選用：False

- **insightValue** – 在異常活動期間進行的 API 呼叫或錯誤上發生的首要屬性值。

  選用：False

- **insightAverage** – 在 insightValue 欄位中屬性的異常活動期間，每分鐘 API 呼叫或錯誤的次數。

  選用：False

- **baselineValue** – 導致正常活動期間所記錄的 API 呼叫或錯誤的主要屬性值。

  選用：False

- **baselineAverage** – baselineValue欄位中屬性的 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。

  選用：False

- **insight** – 造成 API 呼叫的前五個屬性值，或在異常活動期間進行的錯誤。它也會顯示屬性在異常活動期間所做的 API 呼叫或錯誤的平均數量。

  選用：False

  - **value** – 導致 API 呼叫或在異常活動期間進行的錯誤的屬性。

    選用：False

  - **average** – 在 value 欄位中屬性的異常活動期間，每分鐘 API 呼叫或錯誤的平均數量。

    選用：False

- **baseline** – 在正常活動期間對 API 呼叫或錯誤做出最大貢獻的前五個屬性值。它也會顯示正常活動期間屬性值所記錄的 API 呼叫或錯誤的平均數量。

  選用：False

  - **value** – 在正常活動期間導致 API 呼叫或錯誤的屬性。

    選用：False

- **average** – value欄位中屬性的 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。

  選用：False

# CloudTrail userIdentity 元素

AWS Identity and Access Management (IAM) 提供不同類型的身分。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


- 範例
- 欄位
- 具有 SAML 和 Web 聯合身分 AWS STS APIs 值
- AWS STS 來源身分


## 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": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAIDPPEZS35WEXAMPLE",
            "arn": "arn:aws:iam::123456789012:role/RoleToBeAssumed",
            "accountId": "123456789012",
            "userName": "RoleToBeAssumed"
        },
        "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "20131102T010628Z"
        }
    }
}
```

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"
}
```

若要進一步了解如何使用 `userId`、 `identityStoreArn`和 `credentialId`，請參閱《IAM Identity Center 使用者指南》中的在 IAM Identity Center 使用者起始的 CloudTrail 事件中識別使用者和工作階段。

**`userIdentity`** 使用產品提供者起始的請求

產品提供者使用暫時委派存取執行的所有動作都會自動記錄在 CloudTrail 中。這可讓您帳戶中產品提供者活動的完整可見性和可稽核性 AWS 。您可以識別產品提供者所採取的動作、發生的時間，以及執行這些動作的產品提供者帳戶。

為了協助您區分您自己的 IAM 主體所採取的動作，以及具有委派存取權的產品提供者所採取的動作，CloudTrail 事件會在 `userIdentity`元素`invokedByDelegate`下包含名為 的新欄位。此欄位包含產品提供者 AWS 的帳戶 ID，讓您輕鬆篩選和稽核所有委派的動作。

下列範例顯示產品提供者使用暫時委派存取所執行動作的 `userIdentity` 元素。

```
"userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI...",
    "arn": "arn:aws:sts::123456789012:assumed-role/Alice/Session",
    "accountId": "123456789012",
    "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAI...",
            "arn": "arn:aws:iam::123456789012:role/Alice",
            "accountId": "123456789012",
            "userName": "Alice"
        },
        "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "20131102T010628Z"
        }
    },
    "invokedByDelegate": {
        "accountId": "999999999999"
    }
}
```

`invokedByDelegate` 欄位包含使用委派存取執行動作之產品提供者 AWS 的帳戶 ID。在此範例中，帳戶 999999999999 （產品提供者） 在帳戶 123456789012 （客戶帳戶） 中執行動作。

## 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 – 使用您的 AWS 帳戶 登入資料提出請求。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。這可以包含 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 – 使用從呼叫 API 取得的 AWS STS GetFederationToken臨時安全登入資料提出請求。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。目錄服務包括下列項目：Amazon WorkDocs 和 Amazon Quick。
- AWSAccount – 請求是由另一個 提出 AWS 帳戶
- AWSService – 請求是由屬於 AWS 帳戶 的 提出 AWS 服務。例如， AWS Elastic Beanstalk 假設您帳戶中的 IAM 角色 AWS 服務 代表您呼叫其他 。
- IdentityCenterUser – 代表 IAM Identity Center 使用者提出請求。
- Unknown – 使用 CloudTrail 無法判斷的身分類型提出請求。

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：由另一個帳戶啟動的跨帳戶存取 AWS

1. 您在帳戶中擁有 IAM 角色。
2. 另一個 AWS 帳戶會切換到該角色，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。如需範例日誌項目，請參閱 CloudTrail 日誌檔案中的AWS STS API 事件。

範例：由 AWS 服務啟動的跨帳戶存取

1. 您在帳戶中擁有 IAM 角色。
2. AWS 服務擁有 AWS 的帳戶會擔任該角色。

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 | Description |
| --- | --- | --- |
| Root (未設定別名) | 不存在 | 如果您尚未設定 的別名 AWS 帳戶，則不會顯示 userName 欄位。如需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 | |
| AssumedRole | 不存在 | 對於 AssumedRole 類型，您可以在 sessionIssuer 元素sessionContext 中找到 中的 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 | |

| type | userName | Description |
| --- | --- | --- |
| 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。若要進一步了解如何使用這兩個欄位，請參閱在 IAM Identity Center 使用者起始的 CloudTrail 事件中識別使用者和工作階段 IAM Identity Center 使用者指南中的 。<br><br>* IAM Identity Center 會在兩個登入 CloudTrail 事件的 additionalEventData 元素下發出 userName 欄位。如需詳細資訊，請參閱《IAM Identity Center 使用者指南》中的登入 CloudTrail 事件中的使用者名稱。 |
| 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。在此情況下，CloudTrail 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。下列屬性可能會出現在中sessionContext：

- sessionIssuer – 如果使用者使用臨時安全登入資料提出請求， sessionIssuer會提供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** | Description |
| --- | --- | --- |
| 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AWS 您的帳戶 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 | IAM 使用者擔任的角色 AWS 服務，或角色工作階段中的 Web 聯合身分使用者。 |

  - 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。
- webIdFederationData – 如果使用 Web 聯合身分取得的臨時安全登入資料提出請求，會webIdFederationData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**
>
> 省略此欄位或存在具有空值的此欄位表示沒有身分提供者的相關資訊。

- assumedRoot – 值true適用於管理帳戶或委派管理員呼叫時的暫時工作階段 AWS STS AssumedRoot。如需詳細資訊，請參閱《IAM 使用者指南》中的在 CloudTrail 中追蹤特殊權限任務。此為選用欄位。
- attributes – 工作階段的屬性。
  - 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 來源身分。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》中的監控和控制使用擔任角色所採取的動作。
- 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) 提供的憑證包含 ec2：RoleDelivery IAM 內容金鑰。此內容索引鍵可讓您在 IAM 政策、資源政策或服務 AWS Organizations 控制政策中使用內容索引鍵作為條件，輕鬆地在service-by-service逐項資源的基礎上強制使用新方案。resource-by-resource 如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的執行個體中繼資料與使用者資料。

選用：True

**invokedBy**

AWS 服務 發出請求的 名稱，當 發出請求時， AWS 服務 例如 Amazon EC2 Auto Scaling 或 AWS Elastic Beanstalk。只有在 提出請求時，才會出現此欄位 AWS 服務。這包括 服務使用轉送存取工作階段 (FAS)、 AWS 服務 委託人、服務連結角色或 使用的服務角色提出的請求 AWS 服務。

選用：True

**invokedByDelegate**

追蹤產品供應商在您 AWS 帳戶中使用暫時委派存取提出的請求。只有當產品提供者使用委派的許可啟動 API 請求時，才會顯示此欄位。如果有的話， invokedByDelegate會提供發出請求之產品提供者帳戶的相關資訊。此元素具有下列屬性：

- accountId – 啟動請求之產品提供者 AWS 的帳戶 ID。

如需 CloudTrail 事件中委派存取的詳細資訊和 JSON 範例，請參閱《IAM 使用者指南》中的暫時安全登入資料的 CloudTrail 項目。

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

**`inScopeOf`**

如果請求是在 範圍內提出 AWS 服務，例如 Lambda 或 Amazon ECS，則會提供與請求相關的資源或登入資料的相關資訊。此元素可以包含下列屬性：

- `sourceArn` – 叫用service-to-service請求之資源的 ARN。
- `sourceAccount` – 的擁有者帳戶 ID`sourceArn`。它與 一起顯示`sourceArn`。
- `issuerType` – 的資源類型`credentialsIssuedTo`。例如 `AWS::Lambda::Function`。
- `credentialsIssuedTo` – 與發出登入資料的環境相關的資源。

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

## 具有 SAML 和 Web 聯合身分 AWS STS APIs 值

AWS CloudTrail 支援使用安全性聲明標記語言 (SAML AWS STS) 和 Web 聯合身分進行的 logging AWS Security Token Service () API 呼叫。當使用者呼叫 `AssumeRoleWithSAML` 和 `AssumeRoleWithWebIdentity` API 時， CloudTrail 會記錄呼叫並將事件傳遞到您的 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"
```

```
}
```

如需 userIdentity 元素如何顯示 SAMLUser和 WebIdentityUser類型的範例日誌，請參閱使用記錄 IAM 和 AWS STS API 呼叫 AWS CloudTrail。

## AWS STS 來源身分

IAM 管理員可以設定 ， AWS Security Token Service 要求使用者在使用臨時登入資料擔任角色時指定身分。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 管理員設定後 AWS STS，CloudTrail 會在事件記錄中的下列事件和位置中記錄sourceIdentity資訊：

- 使用者身分在擔任角色時發出的 AssumeRoleWithSAML、 AWS STS AssumeRole或 AssumeRoleWithWebIdentity呼叫。 sourceIdentity 位於 AWS STS 呼叫的 requestParameters區塊中。
- 如果使用者身分使用角色擔任另一個角色，稱為角色鏈結 AWS STS AssumeRole，則使用者身分進行的 AssumeRoleWithSAML、 或 AssumeRoleWithWebIdentity呼叫。 sourceIdentity 可在 AWS STS 呼叫的 requestParameters 區塊中找到。
- AWS 服務 API 會在使用者身分擔任角色並使用 指派的暫時登入資料時呼叫 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。

如需如何設定 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》中的監控和控制使用擔任角色採取的動作。如需記錄到 CloudTrail AWS STS 之事件的詳細資訊，請參閱《IAM 使用者指南》中的使用 記錄 IAM 和 AWS STS API 呼叫 AWS CloudTrail。

以下是事件的範例片段，其中顯示 sourceIdentity 欄位。

範例 **requestParameters** 區段

在下列範例事件程式碼片段中，使用者提出 AWS STS AssumeRole請求，並設定來源身分，此處由 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

在下列範例事件程式碼片段中，使用者提出請求 AWS STS AssumeRole以擔任名為 的角色Developer_Role，並設定來源身分 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**

在下列範例事件程式碼片段中，使用者擔任名為 的角色DevRole來呼叫 AWS 服務 API。使用者會設定來源身分，此處由 *source-identity-value-set* 表示。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 擷取的非 API 事件

除了記錄 AWS API 呼叫之外，CloudTrail 還會擷取可能對 AWS 您的帳戶造成安全或合規影響的其他相關事件，或可協助您疑難排解操作問題。

- AWS 服務 事件 – CloudTrail 支援記錄非 API 服務事件。這些事件是由 AWS 服務建立，但不會由對公有 AWS API 的請求直接觸發。對於這些事件，eventType 欄位是 AwsServiceEvent。
- AWS 管理主控台 登入事件 – CloudTrail 日誌會嘗試登入 AWS 管理主控台、 AWS 開發論壇和 AWS 支援中心。所有 IAM 使用者和根使用者登入事件，以及所有聯合身分使用者登入事件，都會在 CloudTrail 中產生記錄。對於登入事件， eventType 欄位為 AwsConsoleSignIn。

## AWS 服務 事件

CloudTrail 支援記錄非 API 服務事件。這些事件是由 AWS 服務建立，但不會由對公有 AWS API 的請求直接觸發。對於這些事件，eventType 欄位是 AwsServiceEvent。

以下是在 AWS Key Management Service () 中自動輪換客戶受管金鑰時， AWS 服務事件的範例案例 AWS KMS。如需有關轉換 KMS 金鑰的詳細資訊，請參閱 轉換 KMS 金鑰。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-01-14T01:41:59Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RotateKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "a24b3967-ddad-417f-9b22-2332b918db06",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
```

```
        "rotationType": "AUTOMATIC",
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "eventCategory": "Management"
}
```

## AWS 管理主控台 登入事件

CloudTrail 日誌會嘗試登入 AWS 管理主控台、 AWS 開發論壇和 AWS 支援中心。所有 IAM 使用者和根使用者登入事件，以及所有聯合身分使用者登入事件，會在 CloudTrail 日誌檔案中產生記錄。如需有關尋找與檢視日誌的資訊，請參閱 尋找 CloudTrail 日誌檔案 和 下載 CloudTrail 日誌檔案。

您可以使用 AWS 使用者通知 來設定交付管道，以取得 AWS CloudTrail 事件的通知。當事件符合您指定的規則時，便會收到通知。您可以透過多個管道接收事件通知，包括電子郵件、聊天應用程式中的 Amazon Q Developer 聊天通知或 AWS Console Mobile Application 推送通知。您也可在 Console Notifications Center 中看到通知。 使用者通知 支援彙總，可減少您在特定事件期間收到的通知數目。

> **Note**
>
> `ConsoleLogin` 事件中記錄的區域會根據使用者類型以及您是否使用全域或區域端點登入而有所不同。
>
> - 如果您以根使用者身分登入，CloudTrail 會在 us-east-1 中記錄事件。
> - 如果您使用 IAM 使用者登入並使用全域端點，CloudTrail 會記錄`ConsoleLogin`事件的區域，如下所示：
>   - 如果瀏覽器中存在帳戶別名 Cookie，CloudTrail 會在下列其中一個區域中記錄`ConsoleLogin`事件：us-east-2、eu-north-1 或 ap-southeast-2。這是因為主控台代理會根據來自使用者登入位置的延遲來重新導向使用者。
>   - 如果瀏覽器中沒有帳戶別名 Cookie，CloudTrail 會在 us-east-1 中記錄`ConsoleLogin`事件。這是因為主控台代理會重新導向回全域登入。
> - 如果您使用 IAM 使用者登入並使用區域端點，CloudTrail 會將`ConsoleLogin`事件記錄在端點的適當區域中。如需 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
- 根使用者的範例事件紀錄

- 聯合身分使用者的範例事件紀錄

## 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
- IAM 使用者，在使用 MFA 的情況下成功登入
- IAM 使用者，登入失敗
- IAM 使用者，登入程序檢查 MFA (單一 MFA 裝置類型)
- IAM 使用者，登入程序檢查 MFA (多個 MFA 裝置類型)

### 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 管理主控台 而無需使用多重要素驗證 (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 AWS 管理主控台 使用多重要素驗證 (MFA) 登入 。

```
{
    "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。當您以根使用者身分登入時，CloudTrail 會在 us-east-1 中記錄 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。聯合身分使用者會獲得臨時安全登入資料，以透過 `AssumeRole`請求存取 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。

> **Note**
>
> 在此範例中， `mfaAuthenticated`值為 `false`， `MFAUsed`值為 ，`No`因為該請求是由聯合身分使用者提出。只有在 IAM 使用者或根使用者使用 MFA 提出請求時，這些欄位才會設為 true。

```
{
    "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 日誌檔案

您可以使用 CloudTrail 檔案執行更進階的任務。

- 透過將 CloudTrail 日誌檔案傳送到 CloudWatch Logs 進行監控。
- 在帳戶之間共享日誌檔案。
- 使用 AWS CloudTrail Processing Library 在 Java 中寫入日誌處理應用程式。
- 驗證您的日誌檔案，以確認其在 CloudTrail 交付後未曾變更。

當您的帳戶發生事件時，CloudTrail 會評估事件是否符合您的追蹤設定。只有符合您追蹤設定的事件才會交付到您的 Amazon S3 儲存貯體和 Amazon CloudWatch Logs 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：管理事件可讓您了解在 AWS 帳戶中資源上執行的管理操作。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，CloudTrail 就會記錄 `ConsoleLogin` 事件。如需詳細資訊，請參閱CloudTrail 擷取的非 API 事件。
- 網路活動事件：CloudTrail 網路活動事件可讓 VPC 端點擁有者記錄使用其 VPC 端點從私有 VPC 到的 AWS API 呼叫 AWS 服務。網路活動事件可讓您查看在 VPC 內執行的資源操作。
- Insights 事件：Insights 事件會擷取在您的帳戶中偵測到的異常活動。如果您已啟用 Insights 事件且 CloudTrail偵測到異常活動，則會將 Insights 事件記錄到追蹤之目的地 S3 儲存貯體的不同資料夾。當您在 CloudTrail 主控台上檢視 Insights 事件時，也可以查看 Insights 事件的類型。與 CloudTrail 追蹤中擷取的其他類型的事件不同，只有在 CloudTrail 偵測到帳戶 API 使用方式與帳戶的一般使用模式有很大差異時，才會加以記錄。

  僅針對管理 API 產生 Insights 事件。如需詳細資訊，請參閱使用 CloudTrail Insights。

> **Note**
>
> CloudTrail 通常會在 API 呼叫的平均約 5 分鐘內傳遞日誌。此時間無法保證。如需詳細資訊，請參閱 AWS CloudTrail 服務水準協議。
> 如果您的追蹤設定錯誤 (例如，S3 儲存貯體無法連線)，CloudTrail 會在 30 天內嘗試重新傳遞日誌檔案到您的 S3 儲存貯體，且您需要為這些嘗試傳遞事件支付標準 CloudTrail 費用。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 日誌檔案
- 在 CloudTrail 中管理資料一致性
- 使用 Amazon CloudWatch Logs 監控 CloudTrail 日誌檔案
- 從多個帳戶接收 CloudTrail 日誌檔案
- 在 AWS 帳戶之間共用 CloudTrail 日誌檔案
- 驗證 CloudTrail 日誌檔案完整性
- CloudTrail 日誌檔案範例
- 使用 CloudTrail Processing Library


# 從多個區域接收 CloudTrail 日誌檔案

當您建立多區域追蹤時，CloudTrail 會從您帳戶中啟用的所有區域記錄事件。CloudTrail 會將日誌檔案傳送至相同的 S3 儲存貯體和 CloudWatch Logs 群組。只要 CloudTrail 具有寫入 S3 儲存貯體的許可，多區域追蹤的儲存貯體就不必位於追蹤的主區域。

雖然您的 預設 AWS 區域 會啟用大多數 AWS 帳戶，但您必須手動啟用特定區域 （ 也稱為選擇加入區域)。如需預設啟用哪些區域的資訊，請參閱《 AWS 帳戶管理 參考指南》中的啟用和停用區域的考量事項。如需 CloudTrail 支援的 區域清單，請參閱 CloudTrail 支援的區域。

在您啟用選擇加入區域之後，CloudTrail 會在您啟用的選擇加入區域中建立每個多區域追蹤的相同複本。如需詳細資訊，請參閱當您啟用選擇加入區域時會發生什麼情況？。

如果您稍後停用選擇加入區域，該區域中的多區域線索副本將會保留。由於您的帳戶在您停用的區域中可能有活動，例如 AWS 服務 移除資源的動作，CloudTrail 將繼續擷取活動，並嘗試針對區域停用之前未刪除的任何線索，將事件交付至 S3 儲存貯體。

若要將現有的單一區域線索轉換為多區域線索，您必須使用 AWS CLI。

若要變更現有的線索以套用至所有已啟用的區域，請將 `--is-multi-region-trail`選項新增至 update-trail命令。

```
aws cloudtrail update-trail --name my-trail --is-multi-region-trail
```

若要確認線索現在是多區域線索，請確認輸出中的 `IsMultiRegionTrail`元素顯示 `true`。

```
{
    "IncludeGlobalServiceEvents": true,
    "Name": "my-trail",
    "TrailARN": "arn:aws:cloudtrail:us-east-2:123456789012:trail/my-trail",
    "LogFileValidationEnabled": false,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "S3BucketName": "amzn-s3-demo-bucket"
}
```

如需詳細資訊，請參閱下列資源：

- 了解多區域追蹤和選擇加入區域
- 為您的 建立線索 AWS 帳戶
- CloudTrail 常見問答集

# 在 CloudTrail 中管理資料一致性

CloudTrail 使用稱為最終一致性的分散式運算模型。您對 CloudTrail 組態 （或其他 AWS 服務） 所做的任何變更，包括屬性型存取控制 (ABAC) 中使用的標籤，都需要時間才能從所有可能的端點中顯示。從伺服器到伺服器，以及從區域到世界各地的區域傳送資料所花費的時間，會產生一些延遲。CloudTrail 也會使用快取以提升效能，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。這類變更包括啟用選擇加入區域、建立或更新線索或事件資料存放區、更新事件選取器，以及開始或停止記錄。當您建立或更新追蹤或事件資料存放區時，CloudTrail 會根據上次已知的組態將日誌傳送至 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。

如需這如何影響其他 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：AWS 大數據部落格中的在將 Amazon S3 和 Amazon Elastic MapReduce 用於 ETL 工作流程時確保一致性。
- AWS Identity and Access Management (IAM)：IAM 使用者指南中不一定會立即顯示我所做的變更。
- 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 Logs 監控 CloudTrail 日誌檔案

您可以使用 Amazon CloudWatch Logs 從 CloudTrail 監控、存放和存取您的日誌檔案。

CloudWatch Logs 可讓您將來自所有系統、應用程式和 AWS 服務 您使用的日誌集中在單一、高度可擴展的服務中。然後，您可以輕鬆檢視日誌、在日誌中搜尋特定的錯誤碼或模式、根據特定欄位篩選日誌，或安全封存日誌以供日後分析。CloudWatch Logs 可讓您將所有日誌 (無論其來源為何) 視為依時間排序的單一且一致的事件流量。

完成下列步驟，以使用 CloudWatch Logs 設定 CloudTrail 來監控您的追蹤日誌，並在發生特定活動時收到通知。

1. 設定您的線索將日誌事件傳送到 CloudWatch Logs。
2. 定義 CloudWatch Logs 指標篩選條件，以評估詞彙、片語或數值中符合項目的日誌事件。例如，您可以監控 `ConsoleLogin` 事件。
3. 將 CloudWatch 指標指派給指標篩選條件。
4. 建立根據您指定的閾值和時段所觸發的 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 自動執行動作，以回應警示。

Amazon CloudWatch 和 Amazon CloudWatch Logs 適用的標準定價。如需詳細資訊，請參閱 Amazon CloudWatch 定價。

如需有關您可以在哪些區域中設定追蹤，以將日誌傳送到 CloudWatch Logs 的詳細資訊，請參閱《AWS 一般參考》中的 Amazon CloudWatch Logs 日誌區域和配額。

主題


- 傳送事件到 CloudWatch Logs
- 建立 CloudTrail 事件的 CloudWatch 警示：範例
- 停止 CloudTrail 將事件傳送至 CloudWatch Logs
- CloudTrail 的 CloudWatch Logs 日誌群組和日誌串流命名
- 讓 CloudTrail 能使用 CloudWatch Logs 進行監控的角色政策文件


## 傳送事件到 CloudWatch Logs

當您將追蹤設定為將事件傳送到 CloudWatch Logs 時，CloudTrail 只會傳送符合您追蹤設定的事件。例如，如果您設定線索只記錄資料事件，您的線索只會將資料事件傳送到您的 CloudWatch Logs 日誌群組。CloudTrail 支援將資料、Insights 和管理事件傳送到 CloudWatch Logs。如需詳細資訊，請參閱使用 CloudTrail 日誌檔案。

> **Note**
>
> 只有管理帳戶可以為使用主控台的組織追蹤設定 CloudWatch Logs 日誌群組。委派管理員可以使用 AWS CLI 或 CloudTrail 或 API 操作來設定 CloudWatch Logs 日誌群組。 CloudTrail `CreateTrail` `UpdateTrail`

將事件傳送到 CloudWatch Logs 日誌群組：

- 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 CloudTrail 主控台上檢視和設定 Amazon CloudWatch Logs 資訊的許可。
- 如果您使用 設定 CloudWatch Logs 日誌群組 AWS CLI，請確定您有足夠的許可在指定的日誌群組中建立 CloudWatch Logs 日誌串流，並將 CloudTrail 事件交付至該日誌串流。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


- 使用主控台設定 CloudWatch Logs 監控
  - 建立日誌群組或指定現有的日誌群組
  - 指定 IAM 角色
  - 在 CloudWatch 主控台中檢視事件
- 使用 設定 CloudWatch Logs 監控 AWS CLI
  - 建立日誌群組
  - 建立角色
  - 建立政策文件
  - 更新線索
- 限制


## 使用主控台設定 CloudWatch Logs 監控

您可以使用 AWS 管理主控台 來設定追蹤，以將事件傳送至 CloudWatch Logs 進行監控。

### 建立日誌群組或指定現有的日誌群組

CloudTrail 使用 CloudWatch Logs 日誌群組做為日誌事件的交付端點。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. 請確定您使用具有足夠許可，可以設定 CloudWatch Logs 整合的管理使用者或角色登入。如需詳細資訊，請參閱授與在 CloudTrail 主控台上檢視和設定 Amazon CloudWatch Logs 資訊的許可。

   > **Note**
   >
   > 只有管理帳戶可以為使用主控台的組織追蹤設定 CloudWatch Logs 日誌群組。委派管理員可以使用 AWS CLI 或 CloudTrail 或 API 操作來設定 CloudWatch Logs 日誌群組。CloudTrail `CreateTrail` `UpdateTrail`

2. 前往 https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
3. 選擇線索名稱。如果您選擇多區域線索，系統會將您重新導向至建立線索的區域。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**
>
> 多區域追蹤會將 中所有已啟用區域的日誌檔案 AWS 帳戶 傳送至您指定的 CloudWatch Logs 日誌群組。

4. 在 CloudWatch Logs 中，選擇 Edit (編輯)。
5. 對於 CloudWatch Logs，選擇已啟用。
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 New (新的)，CloudTrail 會為您指定新日誌群組的名稱，或者您可以輸入名稱。如需有關命名的詳細資訊，請參閱 CloudTrail 的 CloudWatch Logs 日誌群組和日誌串流命名。
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，為將日誌傳送至 CloudWatch Logs 的許可建立新的 IAM 角色。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 讓 CloudTrail 能使用 CloudWatch Logs 進行監控的角色政策文件。

> **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，如果您要 CloudTrail 將事件交付至 CloudWatch Logs 日誌群組，則必須選擇存在於目前帳戶中的日誌群組。

9. 選擇儲存變更。

### 指定 IAM 角色

您可以指定角色，讓擔任的 CloudTrail 可以將事件交付到日誌串流。

#### 指定角色

1. 預設會為您指定 `CloudTrail_CloudWatchLogs_Role`。預設角色政策具備必要的許可，可在您指定的日誌群組中建立 CloudWatch Logs 日誌串流，並將 CloudTrail 事件交付到該日誌串流。

> **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，請前往位於 https：//https://console.aws.amazon.com/iam/ 的 AWS Identity and Access Management 主控台。

b. 選擇 Roles (角色)，然後選擇 CloudTrail_CloudWatchLogs_Role。

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，但若要使用它將事件傳送到 CloudWatch Logs，則必須將必要的角色政策連接到現有的角色。如需詳細資訊，請參閱讓 CloudTrail 能使用 CloudWatch Logs 進行監控的角色政策文件。

在 CloudWatch 主控台中檢視事件

設定線索將事件傳送到 CloudWatch Logs 日誌群組之後，您可以在 CloudWatch 主控台中檢視事件。CloudTrail 通常會在 API 呼叫的平均約 5 分鐘內將事件傳遞到您的日誌群組。此時間無法保證。如需詳細資訊，請參閱 AWS CloudTrail 服務水準協議。

在 CloudWatch 主控台中檢視事件

1. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
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 Time (UTC) (時間 (UTC)) 欄顯示事件交付到日誌群組的時間。若要查看 CloudTrail 記錄事件的實際時間，請查看 `eventTime` 欄位。

## 使用 設定 CloudWatch Logs 監控 AWS CLI

您可以使用 AWS CLI 設定 CloudTrail 將事件傳送至 CloudWatch Logs 進行監控。

### 建立日誌群組

1. 如果您還沒有日誌群組，請使用 CloudWatch Logs `create-log-group` 命令，建立 CloudWatch Logs 日誌群組做為日誌事件的交付端點。

   ```
   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

建立角色，讓啟用它的 CloudTrail 可以將事件傳送到 CloudWatch Logs 日誌群組。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提供 `AssumeRole` 許可給 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。

JSON

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

```
    }
  ]
}
```

執行下列命令為 CloudTrail 建立具備 AssumeRole 許可的角色。

```
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

建立下列適用於 CloudTrail 的角色政策文件。此文件會授予 CloudTrail 必要的許可，以在您指定的日誌群組中建立 CloudWatch Logs 日誌串流，並將 CloudTrail 事件交付到該日誌串流。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream2014110",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111111111111:log-
group:log_group_name:log-stream:111111111111_CloudTrail_us-east-1*"
            ]
        },
        {
            "Sid": "AWSCloudTrailPutLogEvents20141101",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:111111111111:log-
group:log_group_name:log-stream:111111111111_CloudTrail_us-east-1*"
```

```
            ]
        }
    ]
}
```

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。例如，下列政策會授予 CloudTrail 在您指定的日誌群組中建立 CloudWatch Logs 日誌串流所需的許可，以及針對 AWS 帳戶 111111111111 中兩個線索以及在 111111111111 帳戶中建立的組織線索，將 CloudTrail 事件交付至該日誌串流，這些線索會套用到 ID 為 *o-exampleorgid* AWS Organizations 的組織：

JSON

```
{
    "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-aa111bb222_*"
            ]
        },
        {
            "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-aa111bb222_*"
```

```
            ]
        }
    ]
}
```

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 CloudTrail `update-trail` 命令，更新線索中的日誌群組和角色資訊。

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-
arn log_group_arn --cloud-watch-logs-role-arn role_arn
```

如需 AWS CLI 命令的詳細資訊，請參閱 AWS CloudTrail 命令列參考。

### 限制

CloudWatch Logs 和 EventBridge 各允許事件大小上限為 256 KB。雖然大多數服務事件的大小上限為 256 KB，但某些服務仍有較大的事件。CloudTrail 不會將這些事件傳送至 CloudWatch Logs 或 EventBridge。

從 CloudTrail 事件版本 1.05 開始，事件的大小上限為 256 KB。這是為了協助防止惡意行為者利用，並允許 AWS 其他服務消耗事件，例如 CloudWatch Logs 和 EventBridge。

## 建立 CloudTrail 事件的 CloudWatch 警示：範例

此主題說明如何設定 CloudTrail 事件的警示，並包含範例。

主題

- 先決條件
- 建立指標篩選條件並建立警示
- 範例：安全群組組態變更
- AWS 管理主控台 登入失敗範例

- 範例：IAM 政策變更
- 設定 CloudWatch Logs 警示的通知

## 先決條件

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 使用 CloudTrail 主控台建立追蹤。
- 指定或建立 IAM 角色以將下列許可授予 CloudTrail：在您指定的日誌群組中建立 CloudWatch Logs 日誌串流，以及將 CloudTrail 事件傳送至該日誌串流。預設 `CloudTrail_CloudWatchLogs_Role` 會為您妥善處理。

如需詳細資訊，請參閱傳送事件到 CloudWatch Logs。本節中的範例會在 Amazon CloudWatch Logs 主控台中執行。如需建立指標篩選條件和警示的詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的使用篩選條件從日誌事件建立指標和使用 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 CloudTrail 日誌事件指標篩選條件和模式之語法的詳細資訊，請參閱 Amazon CloudWatch Logs 使用者指南中篩選條件和模式語法的 JSON 相關小節。

## 範例：安全群組組態變更

遵循此程序，以建立在安全群組發生組態變更時觸發的 Amazon CloudWatch 警示。

建立指標篩選條件

1. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
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

建立指標篩選條件之後，CloudTrail 線索日誌群組的 CloudWatch Logs 日誌群組詳細資訊頁面就會開啟。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。選擇下一步。
3. 在設定動作頁面上，選擇通知，然後選擇警示中，表示當超過 5 分鐘內 1 個變更事件的閾值時，會採取動作，而 SecurityGroupEventCount 處於警示狀態。
   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。

建立警示後，CloudWatch 會開啟 Alarms (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 管理主控台 登入失敗範例

依照此程序建立 Amazon CloudWatch 警示，該警示會在五分鐘期間內發生三個或更多 AWS 管理主控台 登入失敗時觸發。

建立指標篩選條件

1. 透過 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
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

建立指標篩選條件之後，CloudTrail 線索日誌群組的 CloudWatch Logs 日誌群組詳細資訊頁面就會開啟。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。選擇下一步。
3. 在設定動作頁面上，對於通知，選擇警示中，表示當超過 5 分鐘內 3 個變更事件的閾值時，會採取動作，而 ConsoleSigninFailureCount 處於警示狀態。
   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。

   建立警示後，CloudWatch 會開啟 Alarms (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

遵循此程序，以建立在進行 API 呼叫來變更 IAM 政策時觸發的 Amazon CloudWatch 警示。

建立指標篩選條件

1. 在 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
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

建立指標篩選條件之後，CloudTrail 線索日誌群組的 CloudWatch Logs 日誌群組詳細資訊頁面就會開啟。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。選擇下一步。
   i.
3. 在設定動作頁面上，對於通知，選擇警示中，表示當超過 5 分鐘內 1 個變更事件的閾值時，會採取動作，而 IAMPolicyEventCount 處於警示狀態。
   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。

   建立警示後，CloudWatch 會開啟 Alarms (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 Logs 警示的通知

您可以設定 CloudWatch Logs 在每次 CloudTrail 警示觸發時傳送通知。這可讓您快速回應在 CloudTrail 事件中擷取到和 CloudWatch Logs 偵測到的重要操作事件。CloudWatch 使用 Amazon Simple Notification Service (SNS) 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。

## 停止 CloudTrail 將事件傳送至 CloudWatch Logs

您可以更新線索以停用 CloudWatch Logs 設定，停止將 AWS CloudTrail 事件傳送至 Amazon CloudWatch Logs。 Amazon CloudWatch

### 停止傳送事件到 CloudWatch Logs (主控台)

停止將 CloudTrail 事件傳送至 CloudWatch Logs

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
2. 在導覽窗格中，選擇 Trails (追蹤記錄)。
3. 選擇您要停用 CloudWatch Logs 整合的線索名稱。

4. 在 CloudWatch Logs 中，選擇 Edit (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 Logs (CLI)

您可以使用 update-trail 命令移除做為交付端點的 CloudWatch Logs 日誌群組。下列命令會以空白值取代日誌串流 ARN 和 CloudWatch Logs 角色 ARN 的值，從而從線索組態中清除日誌群組和角色的值。

```
aws cloudtrail update-trail --name trail_name --cloud-watch-logs-log-group-arn="" --
cloud-watch-logs-role-arn=""
```

## CloudTrail 的 CloudWatch Logs 日誌群組和日誌串流命名

Amazon CloudWatch 會顯示您為 CloudTrail 事件建立的日誌群組，以及您在區域中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 建立日誌群組的日誌串流時，會根據下列格式來命名日誌串流：*account_ID*_CloudTrail_*trail_region*。

> **Note**
>
> 如果 CloudTrail 日誌數量很大，則可以建立多個日誌串流，將日誌資料交付至您的日誌群組。當有多個日誌串流時，CloudTrail 會根據下列格式來命名每個日誌串流：*account_ID*_CloudTrail_*trail_region_number*。

如需 CloudWatch 日誌群組的詳細資訊，請參閱Amazon CloudWatch Logs 使用者指南中的使用日誌群組和日誌串流和 Amazon CloudWatch Logs API 參考中的 CreateLogGroup。

# 讓 CloudTrail 能使用 CloudWatch Logs 進行監控的角色政策文件

本節說明 CloudTrail 角色要能向 CloudWatch Logs 傳送日誌事件所需的許可政策。當您設定 CloudTrail 傳送事件時，可以將政策文件連接至角色，如 傳送事件到 CloudWatch Logs 中的說明。您也可以使用 IAM 建立角色。如需詳細資訊，請參閱建立角色以將許可委派給 AWS 服務或建立 IAM 角色 (AWS CLI)。

下列範例政策文件包含在您指定之日誌群組中建立 CloudWatch 日誌串流的必要許可，以及將 CloudTrail 事件傳遞到美國東部 (俄亥俄) 區域中該日誌串流的必要許可。(這是用於預設 IAM 角色 `CloudTrail_CloudWatchLogs_Role` 的預設政策。)

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailCreateLogStream2014110",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": [
                "arn:aws:logs:us-east-2:111122223333: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-2:111122223333: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。例如，下列政策會授予 CloudTrail 在您指定為 *log_group_name* 值的日誌群組中建立 CloudWatch Logs 日誌串流所需的許可，以及針對 AWS 帳戶 111111111111 中的兩個線索，以及在 111111111111 帳戶中建立的組織線索，將 CloudTrail 事件交付至該日誌串流，這些線索會套用到 ID 為 *o-exampleorgid* AWS Organizations 的組織：

JSON

```
{
    "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 日誌檔案

您可以讓 CloudTrail 從多個 將日誌檔案交付 AWS 帳戶 至單一 Amazon S3 儲存貯體。例如，您有四個帳戶 IDs AWS 帳戶 為 111111111111、222222222222、333333333333 和 444444444444，而且您想要設定 CloudTrail 將所有四個帳戶的日誌檔案交付到屬於帳戶 111111111111 的儲存貯體。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，請參閱使用主控台建立追蹤。

2. 更新您目標儲存貯體上的儲存貯體政策，授予 CloudTrail 跨帳戶許可。

   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 金鑰政策必須允許 CloudTrail 使用金鑰來加密您的日誌檔案和摘要檔案，並允許您指定的使用者以未加密的形式讀取日誌檔案或摘要檔案。如需手動編輯金鑰政策的資訊，請參閱「設定 CloudTrail 的 AWS KMS 金鑰政策」。

## 編輯其他帳戶呼叫之資料事件的儲存貯體擁有者帳戶 ID

過去，如果 CloudTrail 資料事件是在 Amazon S3 資料事件 API 發起 AWS 帳戶 人的 中啟用，CloudTrail 會在資料事件 （ 例如 ) 中顯示 S3 儲存貯體擁有者的帳戶 IDPutObject。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，如果同時滿足以下兩個條件，CloudTrail 會移除 `resources` 區塊中 S3 儲存貯體擁有者的帳戶 ID：

- 資料事件 API 呼叫來自與 Amazon S3 儲存貯體擁有者 AWS 帳戶 不同的 。
- 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:::amzn-s3-demo-bucket2/"
    },
    {
        "accountId": "123456789012",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::amzn-s3-demo-bucket2"
    }
]
```

以下為當前行為。

```
# Current

"resources": [
    {
        "type": "AWS::S3::Object",
        "ARNPrefix": "arn:aws:s3:::amzn-s3-demo-bucket2/"
    },
    {
        "accountId": "",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::amzn-s3-demo-bucket2"
    }
]
```

主題

- 設定多帳戶的儲存貯體政策
- 在其他帳戶中建立追蹤

# 設定多帳戶的儲存貯體政策

儲存貯體若要接收多個帳戶的日誌檔案，其儲存貯體政策必須授予 CloudTrail 許可，從您指定的所有帳戶寫入日誌檔案。這表示您必須修改目標儲存貯體的儲存貯體政策，授予從各指定帳戶寫入日誌檔案的 CloudTrail 許可。

> **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 管理主控台 使用此範例中擁有儲存貯體 (111111111111 的帳戶登入)，然後開啟 Amazon S3 主控台。
2. 選擇 CloudTrail 交付您日誌檔案的儲存貯體，然後選擇 Permissions (許可)。
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 12 位數字，包括前導零。

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20131101",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
```

```
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "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:::amzn-s3-demo-
bucket/optionalLogFilePrefix/AWSLogs/111111111111/*",
                "arn:aws:s3:::amzn-s3-demo-
bucket/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

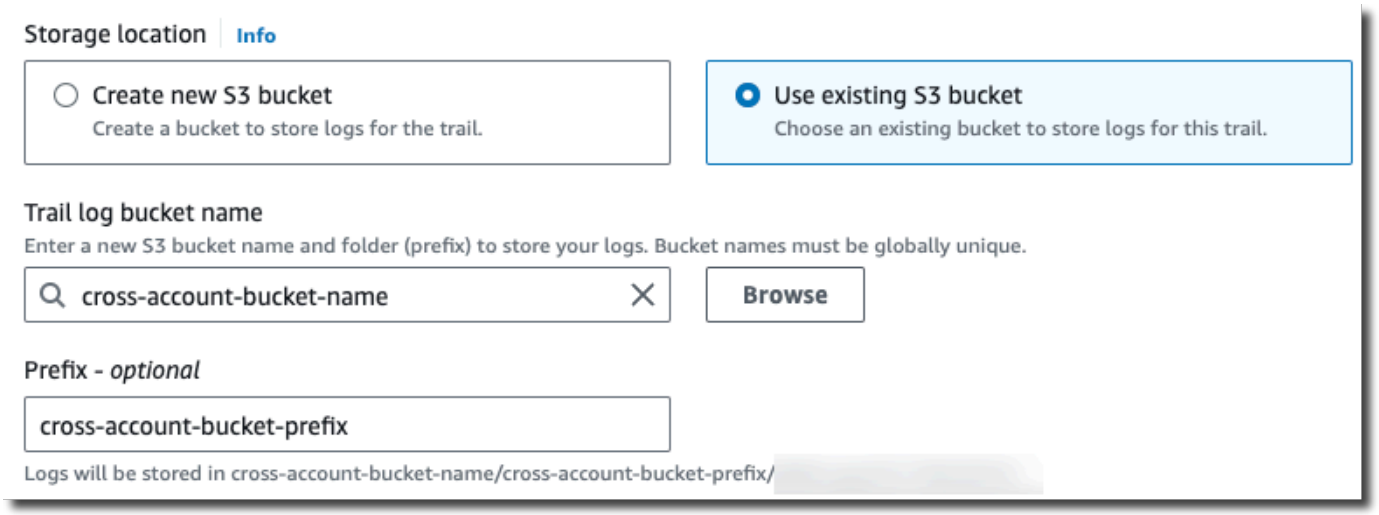
您可以使用 主控台或 AWS CLI 在其他 中建立線索 AWS 帳戶 ，並將其日誌檔案彙總到一個 Amazon S3 儲存貯體。或者，您可以建立組織線索來記錄組織 AWS 帳戶 中的所有 AWS Organizations。如需詳細資訊，請參閱建立組織追蹤。

## 使用 主控台在其他 AWS 帳戶中建立追蹤

您可以使用 CloudTrail 主控台在其他帳戶中建立追蹤。

1. AWS 管理主控台 使用您要為其建立追蹤的帳戶登入 。遵循 使用主控台建立追蹤 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**
>
> 儲存貯體政策必須授予 CloudTrail 寫入的許可。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。如果您選擇使用的字首與在儲存貯體政策中指定的不同，則必須編輯目的地儲存貯體上的儲存貯體政策，以允許 CloudTrail 使用這個新字首將日誌檔案寫入儲存貯體。

### 使用 CLI 在其他 AWS 帳戶中建立追蹤

您可以使用 AWS 命令列工具在其他帳戶中建立追蹤，並將其日誌檔案彙總到一個 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` 指定此線索將記錄您正在使用的分割區中所有 AWS 區域中的事件。

您可以為帳戶正在執行 AWS 資源的每個區域建立一個線索。

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 amzn-s3-demo-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": "amzn-s3-demo-bucket"
}
```

如需從 AWS 命令列工具使用 CloudTrail 的詳細資訊，請參閱 CloudTrail 命令列參考。

## 在 AWS 帳戶之間共用 CloudTrail 日誌檔案

本節說明如何在多個 AWS 帳戶之間共用 CloudTrail 日誌檔案。您在 之間共用日誌的方法 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 透過擔任角色在多個 之間共用 CloudTrail 日誌檔案，並描述共用日誌檔案的案例。

- 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 AmazonS3ReadOnlyAccess 政策。

> **Note**
>
> AmazonS3ReadOnlyAccess 政策預設會將擷取和列出權限授予您帳戶內的所有 Amazon S3 儲存貯體。

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》中的如何在將 AWS 資源的存取權授予第三方時使用外部 ID。
   - 選擇 AmazonS3ReadOnlyAccess 政策。

   > **Note**
   >
   > AmazonS3ReadOnlyAccess 政策預設會將擷取和列出權限授予您帳戶內的所有 Amazon S3 儲存貯體。

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 日誌檔案

## 建立存取政策將存取權授予您擁有的帳戶

作為 Amazon S3 儲存貯體擁有者，您對於 CloudTrail 用來將其他帳戶的日誌檔案寫入的 Amazon S3 儲存貯體有完全的控制權。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。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333: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，Resource (資源) ARN 包含帳戶 B 的 12 位數帳戶 ID，以及您在彙整程序期間為帳戶 B 開啟 CloudTrail 時指定的字首 (如有)。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**
>
> 您必須確認存取政策中的前綴與您為帳戶 B 開啟 CloudTrail 時指定的前綴完全相同。若不相同，您就必須編輯您帳戶中的 IAM 角色存取政策，以納入帳戶 B 的實際前綴。如果角色存取政策中的前綴與您為帳戶 B 開啟 CloudTrail 時指定的前綴不完全相同，帳戶 B 就無法存取其日誌檔案。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/account-B-id/
*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
}
```

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， 建立的信任關係會 AWS 指定信任第三方帳戶 （此範例中的帳戶 Z) 來擔任您建立的角色。信任政策範例如下：

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333: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》中的如何在將 AWS 資源的存取權授予第三方時使用外部 ID。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Sid": "",
```

```
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::111111111111: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。

JSON

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

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 API 的 AWS STS `AssumeRole`許可。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。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/Test"
```

```
        }
    ]
}
```

編輯客戶受管政策 (主控台)

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/iam/ 開啟 IAM 主控台。
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、要擔任角色的 Amazon Resource Number (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》中的如何在將 AWS 資源的存取權授予第三方時使用外部 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 傳回暫時憑證，用於存取擁有帳戶中的資源。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 適用於 Python (Boto) 的 AWS SDK) 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 日誌檔案

若要停止與另一個帳戶共用日誌檔案 AWS 帳戶，請刪除您為該帳戶建立的角色。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 日誌檔案完整性

若要判斷在 CloudTrail 交付日誌檔案之後，日誌檔案是否已修改、已刪除或保持不變，您可以使用 CloudTrail 日誌檔案完整性驗證。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。這可透過運算方式防止修改、刪除或偽造 CloudTrail 日誌檔案，而無需偵測。您可以使用 AWS CLI 驗證 CloudTrail 交付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。CloudTrail 日誌檔案完整性驗證程序也可讓您知道日誌檔案是否已刪除或變更，或積極宣告在指定的一段期間沒有日誌檔案交付至您的帳戶。

# 運作方式

當您啟用日誌檔案完整性驗證時，CloudTrail 會為它所交付的每個日誌檔案建立一個雜湊。CloudTrail 也會在每個小時建立和交付檔案，檔案參考前一小時的日誌檔案，並包含每個日誌檔案的雜湊。此檔案稱為摘要檔案。CloudTrail 會使用公有和私有金鑰對的私有金鑰來簽署每個摘要檔案。在交付之後，您可以使用公有金鑰來驗證摘要檔案。CloudTrail 會對每個金鑰對使用不同的金鑰對 AWS 區域。

摘要檔案會交付至與您線索相關聯的 Amazon S3 儲存貯體，其與交付您 CloudTrail 日誌檔案的儲存貯體相同。如果將您的日誌檔案從所有區域或多個帳戶交付至單一 Amazon S3 儲存貯體，則 CloudTrail 會將摘要檔案從那些區域和帳戶傳遞至相同的儲存貯體。

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 日誌檔案和摘要檔案儲存在 Amazon S3 或 Amazon Glacier 中，無限期以安全、耐用且經濟實惠的方式存放。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

若要啟用日誌檔案完整性驗證，您可以使用 AWS 管理主控台 AWS CLI、 或 CloudTrail API。啟用日誌檔完整性驗證可讓 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 CloudTrail 的日誌檔案完整性驗證。

若要驗證 CloudTrail 日誌檔案的完整性，您可以使用 AWS CLI 或建立您自己的解決方案。 AWS CLI 將驗證 CloudTrail 交付檔案的位置。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 驗證日誌的相關資訊 AWS CLI，請參閱 使用 驗證 CloudTrail 日誌檔案完整性 AWS CLI。如需開發 CloudTrail 日誌檔案驗證之自訂實作的資訊，請參閱 CloudTrail 日誌檔案完整性驗證的自訂實作。

# 啟用 CloudTrail 的日誌檔案完整性驗證

您可以使用 AWS 管理主控台、 AWS 命令列界面 (AWS CLI) 或 CloudTrail API 來啟用日誌檔案完整性驗證。CloudTrail 會在大約一小時內開始交付摘要檔案。

### AWS 管理主控台

若要透過 CloudTrail 主控台啟用日誌檔案完整性驗證，請在建立或更新線索時，針對 Enable log file validation (啟用日誌檔案驗證) 選擇 Yes (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

若要使用 啟用日誌檔案完整性驗證 AWS CLI，請使用 `--enable-log-file-validation`選項搭配 create-trail 或 update-trail 命令。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 啟用日誌檔案完整性驗證，請在呼叫 `CreateTrail` 或 `UpdateTrail` 時，將 `EnableLogFileValidation` 請求參數設定為 `true`。

如需詳細資訊，請參閱 AWS CloudTrail API 參考中的 CreateTrail 和 UpdateTrail。

## 使用 驗證 CloudTrail 日誌檔案完整性 AWS CLI

若要使用 驗證日誌 AWS Command Line Interface，請使用 CloudTrail `validate-logs`命令。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 日誌檔案
- 修改或刪除 CloudTrail 摘要檔案
- 修改或刪除上述兩者

> **Note**
>
> 只會 AWS CLI 驗證摘要檔案所參考的日誌檔案。如需詳細資訊，請參閱檢查特定檔案是否由 CloudTrail 交付。

## 先決條件

若要使用 驗證日誌檔案完整性 AWS CLI，必須符合下列條件：

- 您必須擁有 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。
- 在 CloudTrail 交付摘要和日誌檔案後，不得自原始的 Amazon S3 位置再行移動。
- 執行命令的角色必須具有呼叫 `ListObjects`、 和 的許可`GetObject`，以`GetBucketLocation`用於追蹤所參考的每個 S3 儲存貯體。

> **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 日誌檔案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 <amzn-s3-demo-bucket>] [--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`全域選項來驗證特定 的日誌 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 交付。

--s3-bucket

選擇性指定摘要檔案要存放的 Amazon S3 儲存貯體。如果未指定儲存貯體名稱， AWS CLI 會呼叫來擷取它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 會呼叫 來擷取它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。`validate-logs` 命令會先在標準摘要鏈上操作。完成標準摘要驗證後，如果有，它會驗證回填摘要檔案。回填摘要會形成單獨的驗證鏈，並與標準摘要獨立處理。

## 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
```

主輸出的每一行都包含單一摘要或日誌檔案的驗證結果，格式如下。字首為 的行(backfill)表示回填摘要檔案，這會與標準摘要檔案形成單獨的驗證鏈。

```
<optional (backfill)> <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 | Description |
| --- | --- | --- |
| 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。 |
| 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。 |

| 檔案類型 | 驗證訊息 | Description |
| --- | --- | --- |
| 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。在 CloudTrail 交付之後，日誌檔案已修改。 |
| 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://amzn-s3-demo-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://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1925Z_WZZw1RymnjCRjxXc.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_POuvV87nu6pfAV2W.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1930Z_l2QgXhAKVm1QXiIA.json.gz valid
```

```
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_eQJteBBrfpBCqOqw.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1950Z_9g5A6qlR2B5KaRdq.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1920Z_i4DNCC12BuXd6Ru7.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1915Z_Sg5caf2RH6Jdx0EJ.json.gz valid
Digest file    s3://amzn-s3-demo-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://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/09/01/111111111111_CloudTrail_us-
east-2_20150901T1910Z_YYSFiuFQk4nrtnEW.json.gz valid
[...]
Log file       s3://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1055Z_0Sfy6m9f6iBzmoPF.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T1040Z_lLa3QzVLpOed7igR.json.gz valid

Digest file    s3://amzn-s3-demo-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://amzn-s3-demo-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://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2015/09/01/144218288521_CloudTrail_us-
east-2_20150901T0830Z_eaFvO3dwHo4NCqqc.json.gz valid
Digest file    s3://amzn-s3-demo-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://amzn-s3-demo-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://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2245Z_mbJkEO5kNcDnVhGh.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2225Z_IQ6kXy8sKU03RSPr.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2230Z_eRPVRTxHQ5498ROA.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2015/08/31/111111111111_CloudTrail_us-
east-2_20150831T2255Z_IlWawYZGvTWB5vYN.json.gz valid
Digest file    s3://amzn-s3-demo-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
```

下列範例validate-logs命令會在存在回填摘要檔案的期間使用 --verbose旗標，並產生後續的範例輸出。回填摘要會以(backfill)字首顯示，並與標準摘要鏈分開驗證。 [...]表示範例輸出已縮寫。

```
aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:us-
east-2:111111111111:trail/example-trail-name --start-time 2024-07-31T22:00:00Z --end-
time 2024-08-01T19:17:29Z --verbose
```

```
Validating log files for trail arn:aws:cloudtrail:us-east-2:111111111111:trail/example-
trail-name between 2024-07-31T22:00:00Z and 2024-08-01T19:17:29Z

Digest file    s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2024/08/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20240801T201728Z.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/08/01/111111111111_CloudTrail_us-
east-2_20240801T1925Z_Xm3pK9vN2wQ5rT8h.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/08/01/111111111111_CloudTrail_us-
east-2_20240801T1915Z_Bj7cL4nM6pR9sU2v.json.gz valid
```

```
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/08/01/111111111111_CloudTrail_us-
east-2_20240801T1930Z_Fy1dG8kN3qT6wX0z.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/08/01/111111111111_CloudTrail_us-
east-2_20240801T1920Z_Hn5jM2pQ7sV9yB4e.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/08/01/111111111111_CloudTrail_us-
east-2_20240801T1950Z_Kp8rN1tW4xZ7aC3f.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/08/01/111111111111_CloudTrail_us-
east-2_20240801T1920Z_Mq6sP9uX2yB5dE8g.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/08/01/111111111111_CloudTrail_us-
east-2_20240801T1915Z_Rt4vQ7wZ0aC3fG6h.json.gz valid
Digest file    s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2024/08/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20240801T191728Z.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/08/01/111111111111_CloudTrail_us-
east-2_20240801T1910Z_Uw9xR2yB5dH8jK1m.json.gz valid
[...]
Log file       s3://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2024/08/01/144218288521_CloudTrail_us-
east-2_20240801T1055Z_Vz3aS6cE9fL2nP5q.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2024/08/01/144218288521_CloudTrail_us-
east-2_20240801T1040Z_Xy7bT0dG3hM6pR9s.json.gz valid

Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2024/08/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20240801T101728Z.json.gz INVALID: signature verification failed

Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2024/08/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20240801T091728Z.json.gz valid
Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2024/08/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20240801T081728Z.json.gz valid
Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/us-
east-2/2024/08/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20240801T071728Z.json.gz valid
[...]
```

```
Digest file    s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail-Digest/us-
east-2/2024/07/31/111111111111_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20240731T221728Z.json.gz valid
(backfill) Digest file    s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail-
Digest/us-east-2/2024/08/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-
name_us-east-2_20240801T201728Z_backfill.json.gz valid
(backfill) Digest file    s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail-
Digest/us-east-2/2024/08/01/111111111111_CloudTrail-Digest_us-east-2_example-trail-
name_us-east-2_20240801T191728Z_backfill.json.gz valid
[...]

(backfill) Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-
Digest/us-east-2/2024/08/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-
name_us-east-2_20240801T101728Z_backfill.json.gz INVALID: signature verification failed

(backfill) Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-
Digest/us-east-2/2024/08/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-
name_us-east-2_20240801T091728Z_backfill.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/144218288521/
CloudTrail/us-east-2/2024/08/01/144218288521_CloudTrail_us-
east-2_20240801T0830Z_Rn6uk0wY5aD9fJ3n.json.gz valid
(backfill) Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-
Digest/us-east-2/2024/08/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-
name_us-east-2_20240801T081728Z_backfill.json.gz valid
(backfill) Digest file    s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-
Digest/us-east-2/2024/08/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-
name_us-east-2_20240801T071728Z_backfill.json.gz valid
[...]
(backfill) Digest file    s3://amzn-s3-demo-bucket/AWSLogs/111111111111/CloudTrail-
Digest/us-east-2/2024/07/31/111111111111_CloudTrail-Digest_us-east-2_example-trail-
name_us-east-2_20240731T221728Z_backfill.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/07/31/111111111111_CloudTrail_us-
east-2_20240731T2145Z_Sp3vm7xZ2bE6gK0p.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/07/31/111111111111_CloudTrail_us-
east-2_20240731T2125Z_Tq0wn4ya9cF3hL7q.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/07/31/111111111111_CloudTrail_us-
east-2_20240731T2130Z_Ur7xp1zb6dG0jM4r.json.gz valid
Log file       s3://amzn-s3-demo-bucket/AWSLogs/111111111111/
CloudTrail/us-east-2/2024/07/31/111111111111_CloudTrail_us-
east-2_20240731T2155Z_Vs4yq8ac3eH7kN1s.json.gz valid
```

```
Results requested for 2024-07-31T22:00:00Z to 2024-08-01T19:17:29Z
Results found for 2024-07-31T22:17:28Z to 2024-08-01T20:17:28Z:

22/23 digest files valid, 1/23 digest files INVALID
22/23 backfill digest files valid, 1/23 backfill 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://amzn-s3-demo-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

(backfill) Digest file s3://amzn-s3-demo-bucket/AWSLogs/144218288521/CloudTrail-Digest/
us-east-2/2024/08/01/144218288521_CloudTrail-Digest_us-east-2_example-trail-name_us-
east-2_20240801T101728Z_backfill.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
22/23 backfill digest files valid, 1/23 backfill digest files INVALID
63/63 log files valid
```

## 檢查特定檔案是否由 CloudTrail 交付

**若要檢查儲存貯體中的特定檔案是否由 CloudTrail 交付，請在包含該檔案的期間以詳細資訊模式執行 validate-logs。如果檔案出現在 validate-logs 的輸出中，則該檔案確實是由 CloudTrail 交付。**

# 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://amzn-s3-demo-bucket/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://amzn-s3-demo-bucket/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
> ```

> **Note**
>
> 當 CloudTrail 需要包含原始摘要中因處理延遲而未參考的日誌檔案時，會交付回填摘要檔案。回填摘要檔案在其檔案名稱中使用_backfill尾碼，如下所示：
>
> ```
> s3://amzn-s3-demo-bucket/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_backfill.json.gz
> ```

## 範例摘要檔案內容

下例的摘要檔案包含 CloudTrail 日誌的資訊。


```
{
  "awsAccountId": "111122223333",
  "digestStartTime": "2015-08-17T14:01:31Z",
  "digestEndTime": "2015-08-17T15:01:31Z",
  "digestS3Bucket": "amzn-s3-demo-bucket",
  "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": "amzn-s3-demo-bucket",
  "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": "amzn-s3-demo-bucket",
      "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`

已交付摘要檔案 AWS 的帳戶 ID。

`digestStartTime`

摘要檔案涵蓋的 UTC 時間範圍起點，做為 CloudTrail 已交付日誌檔案的時間參考。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`

摘要檔案涵蓋的 UTC 時間範圍終點，做為 CloudTrail 已交付日誌檔案的時間參考。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 CloudTrail API，擷取與摘要檔案對應的時間範圍的公有金鑰。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。如需擷取摘要檔案公有金鑰的相關資訊，請參閱 AWS CLI `list-public-keys`命令或 CloudTrail `ListPublicKeys` API。

> **Note**
>
> CloudTrail 在每個區域都使用不同的私有/公有金鑰對。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

即使您的帳戶在摘要檔案代表的一小時期限內沒有任何 API 活動，CloudTrail 仍會交付摘要檔案。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": "amzn-s3-demo-bucket",
  "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": "amzn-s3-demo-bucket",
  "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

- x-amz-meta-backfill-generation-timestamp

  產生回填摘要時的 UTC 時間戳記。此中繼資料屬性僅存在於回填摘要檔案中，用於識別用於簽章驗證的正確公有金鑰。以下是範例時間戳記：

  2025-05-20T00:00:00.000Z

### 摘要檔案鏈結

每個摘要檔案都包含其先前摘要檔案的參考，可讓「鏈結」允許像是 的驗證工具 AWS CLI 偵測摘要檔案是否已刪除。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**
>
> 當您停用日誌檔案完整性驗證時，摘要檔案鏈結會在 1 小時後中斷。CloudTrail 不會為在日誌檔案完整性驗證停用期間內交付的日誌檔案建立摘要檔案。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。您每次停止 CloudTrail 記錄或刪除追蹤時，也是同樣的情況。

如果線索的 S3 儲存貯體政策設定錯誤，或 CloudTrail 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。若要確認您的線索是否有任何摘要交付錯誤，請執行 `get-trail-status`命令並檢查 `LatestDigestDeliveryError` 參數是否有錯誤。解決交付問題後（例如，透過修正儲存貯體政策），CloudTrail 會嘗試重新交付任何缺少的摘要檔案。在重新傳遞期間，摘要檔案可能會不按順序交付，因此鏈可能會暫時中斷。

如果停止記錄或刪除追蹤，CloudTrail 會交付最終的摘要檔案。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 日誌檔案完整性驗證的自訂實作

由於 CloudTrail 使用業界標準、公開使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 日誌檔案的完整性。啟用日誌檔案完整性驗證時，CloudTrail 會將摘要檔案交付到

您的 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。

## 了解如何簽署 CloudTrail 摘要檔案

CloudTrail 摘要檔案使用 RSA 數位簽章進行簽署。針對每個摘要檔案，CloudTrail 會執行下列操作：

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

資料簽署字串包含下列 CloudTrail 物件：

- 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 AmazonS3Client 類別 （例如），從 Amazon S3 儲存貯體取得您想要驗證的時間範圍的最新摘要檔案。
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

若要取得公有金鑰來驗證摘要檔案，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 CloudTrail 針對每個區域使用不同的私有/公有金鑰對，因此每個摘要檔案都使用其區域唯一的私有金鑰進行簽署。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 擷取公 AWS CLI 有金鑰

若要使用 擷取摘要檔案的公有金鑰 AWS CLI，請使用 `cloudtrail list-public-keys`命令。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 擷取公有金鑰

若要使用 CloudTrail API 擷取摘要檔案的公有金鑰，請將開始時間和結束時間值傳遞到 `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 | 選擇地指定要查詢 CloudTrail 摘要檔案公有金鑰之時間範圍的開始時間 (UTC)。如果未指定 StartTime，則會使用目前的時間，並傳回目前的公有金鑰。<br><br>類型：DateTime |
| EndTime | 選擇地指定要查詢 CloudTrail 摘要檔案公有金鑰之時間範圍的結束時間 (UTC)。如果未指定 EndTime，則會使用目前的時間。<br><br>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。<br><br>類型：Blob |
| ValidityStartTime | 公有金鑰的有效開始時間。<br><br>類型：DateTime |
| ValidityEndTime | 公有金鑰的有效結束時間。<br><br>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。<br><br>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
amzn-s3-demo-bucket/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。如果其中一個日誌檔案在 CloudTrail 交付後已修改，SHA-256 雜湊將會變更，因此摘要檔案的簽章將會不符。

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：

- 由於先前摘要檔案的數位簽章位在目前摘要檔案中，請從倒數第二個摘要檔案開始驗證。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驗證 CloudTrail 摘要和日誌檔案的骨架程式碼。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 日誌檔案範例

CloudTrail 會監控您帳戶的事件。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 中建立事件資料存放區，事件會記錄到事件資料存放區中。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
- 日誌檔案範例


## CloudTrail 記錄檔名稱格式

CloudTrail 會將下列檔案名稱格式用於它交付至您 Amazon S3 儲存貯體的日誌檔案物件：

```
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。

CloudTrail 日誌檔案名稱

```
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。

如需有關 CloudTrail 事件記錄欄位的資訊，請參閱 CloudTrail 記錄管理、資料和網路活動事件的內容。

內容


- Amazon EC2 日誌範例
- IAM 日誌範例
- 錯誤代碼和訊息日誌範例
- CloudTrail Insights 事件記錄範例


## 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《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包含金鑰對的雜湊，並 AWS 移除金鑰材料。

```
{"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) 是一種 Web 服務，可協助您安全地控制對 資源的 AWS 存取。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": "policy-statement",
            "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 Insights 事件記錄範例

下列範例顯示 CloudTrail Insights 事件日誌。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 `UpdateInstanceInformation` 與 CloudTrail 分析管理事件以判斷發生異常活動的 AWS Systems Manager API 名稱相同。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。如需使用 CloudTrail Insights 的詳細資訊，請參閱 使用 CloudTrail Insights。


```
{
    "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 Processing Library

CloudTrail Processing Library 是 Java 程式庫，可讓您輕鬆處理 AWS CloudTrail 日誌。您提供 CloudTrail SQS 佇列的組態詳細資訊，並編寫程式碼來處理事件。CloudTrail Processing Library 會執行其餘作業。它會輪詢您的 Amazon SQS 佇列、讀取和剖析佇列訊息、下載 CloudTrail 日誌檔案、剖析日誌檔案中的事件，並將事件傳遞至您的程式碼做為 Java 物件。

CloudTrail Processing Library 具有高度可擴展性並容錯。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。

下列主題顯示如何使用 CloudTrail Processing Library 來處理 Java 專案中的 CloudTrail 日誌。

此程式庫做為 Apache-licensed open-source 專案，可在 GitHub 上取得：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 日誌
- 進階主題
- 其他資源

## 最低需求

若要使用 CloudTrail Processing Library，您必須具有下列項目：

- 適用於 Java 的 AWS SDK 1.11.830
- Java 1.8 (Java SE 8)

## 處理 CloudTrail 日誌

在 Java 應用程式中處理 CloudTrail 日誌：

1. 將 CloudTrail Processing Library 新增至您的專案
2. 設定 CloudTrail Processing Library
3. 實作事件處理器
4. 實例化和執行處理執行器

### 將 CloudTrail Processing Library 新增至您的專案

若要使用 CloudTrail Processing Library，請將它新增至 Java 專案的 classpath。

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

將 CloudTrail Processing Library 新增至 Apache Ant 專案

1. 從 GitHub 下載或複製 CloudTrail Processing Library 的原始程式碼：
   - 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 Processing Library 適用於 Apache 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。

將 CloudTrail Processing Library 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

將 CloudTrail Processing Library 新增至 Eclipse 專案

1. 從 GitHub 下載或複製 CloudTrail Processing Library 的原始程式碼：
   - 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. 將建置的 aws-cloudtrail-processing-library-1.6.1.jar 複製至您專案中的目錄 (通常是 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. 選擇新增 JAR...，然後導覽至您已複製 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

將 CloudTrail Processing Library 新增至 IntelliJ 專案

1. 從 GitHub 下載或複製 CloudTrail Processing Library 的原始程式碼：
   - 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。

## 設定 CloudTrail Processing Library

您可以建立在執行階段載入的 classpath 屬性檔案，或手動建立 `ClientConfiguration` 物件並設定選項，來設定 CloudTrail Processing Library。

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` – 您帳戶的唯一識別符，例如 wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY。

`accessKey` 和 `secretKey` 參數會將您的 AWS 登入資料提供給程式庫，讓程式庫可以 AWS 代表您存取 。

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。

建立 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 日誌，您必須實作收到 CloudTrail 日誌資料的 EventsProcessor。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()));
        }
    }
}
```

實作 EventsProcessor 時，請實作 process() 用來將 CloudTrail 事件傳送給您的 AWSCloudTrailProcessingExecutor 回呼。事件是以 CloudTrailClientEvent 物件清單形式提供。

CloudTrailClientEvent 物件提供 CloudTrailEvent 和 CloudTrailEventMetadata，以用來讀取 CloudTrail 事件和交付資訊。

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

在您寫入 EventsProcessor 並設定 CloudTrail Processing Library 的組態值 (在屬性檔案中或使用 ClientConfiguration 類別) 後，可以使用這些元素來初始化和使用 AWSCloudTrailProcessingExecutor。

使用 **AWSCloudTrailProcessingExecutor** 處理 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。CloudTrail 提供您可實作的選用界面，以篩選用來取得 CloudTrail 日誌的來源，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()。

在程式庫輪詢 Amazon SQS 佇列上的日誌之後，CloudTrail Processing Library 會呼叫 filterSource() 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

您可以實作 EventFilter 界面，選擇是否要將 CloudTrail 事件傳送給您的 EventsProcessor。EventFilter 會宣告可接收 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()。

在程式庫輪詢 Amazon SQS 佇列上的日誌和來源篩選之後，CloudTrail Processing Library 會呼叫 filterEvent() 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

當 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) 或 float (一個包含十進制的數字)。在資料事件欄位中包含整數的事件中，CloudTrail 過去會將這些數字處理為浮點數。目前，CloudTrail 會透過保留其原始格式來處理這些欄位中的數字。

最佳實務是，為了避免破壞自動化，請在您用來處理或篩選 CloudTrail 資料事件的任何程式碼或自動化中保持彈性，並允許 int 和 float 格式化的數字。若要獲得最佳效果，請使用 CloudTrail Processing Library 1.4.0 版或更新版本。

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 界面，自訂 CloudTrail 進度的報告。ProgressReporter 宣告兩種方法：reportStart() 和 reportEnd()，以在下列操作開始和結束時呼叫：

- 輪詢 Amazon SQS 中的訊息
- 剖析 Amazon SQS 中的訊息
- 處理 CloudTrail 日誌的 Amazon SQS 來源
- 刪除 Amazon SQS 中的訊息
- 下載 CloudTrail 日誌檔案

- 處理 CloudTrail 日誌檔案

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` 參數是 `true`，則 CloudTrail Processing Library 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，您沒有存取可接收 CloudTrail 日誌檔案之 S3 儲存貯體的必要許可。因為您沒有必要許可，所以會擲回 `AmazonServiceException`。CloudTrail Processing Library 會將這個項目包裝在 `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 Processing Library 會將這個項目視為處理錯誤，並刪除訊息，即使訊息包含有效的 CloudTrail 日誌檔案。
>
> 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 CloudTrail Processing Library 的相關詳細資訊，請參閱以下：。

- CloudTrail Processing Library GitHub 專案，其中包含示範如何實作 CloudTrail Processing Library 應用程式的範本程式碼。
- CloudTrail Processing Library Java 套件文件。

# 中的安全性 AWS CloudTrail

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

安全性是 AWS 與您之間的共同責任。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 Cloud 中執行 AWS 服務的基礎設施。 AWS 也為您提供可安全使用的服務。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。若要了解適用的合規計劃 AWS CloudTrail，請參閱AWS 合規計劃範圍內的服務。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件有助於您了解如何在使用 CloudTrail 時套用共同責任模型。下列主題將顯示如何配置 CloudTrail 以達到您的安全和合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 CloudTrail 資源。

主題


- 中的資料保護 AWS CloudTrail
- 的 Identity and Access Management AWS CloudTrail
- 的合規驗證 AWS CloudTrail
- 中的彈性 AWS CloudTrail
- 中的基礎設施安全 AWS CloudTrail
- 預防跨服務混淆代理人
- 中的安全最佳實務 AWS CloudTrail
- 使用 AWS KMS 金鑰加密 CloudTrail 日誌檔案、摘要檔案和事件資料存放區 (SSE-KMS)


## 中的資料保護 AWS CloudTrail

AWS 共同責任模型適用於 中的資料保護 AWS CloudTrail。如此模型所述， AWS 負責保護執行所有 的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱AWS 安全性部落格上的AWS 共同責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 CloudTrail 或使用主控台、API AWS CLI或 AWS SDKs的其他 AWS 服務 時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

根據預設，CloudTrail 事件日誌檔案和摘要檔案會使用 Amazon S3 伺服器端加密 (SSE) 進行加密。您也可以選擇使用 AWS Key Management Service (AWS KMS) 金鑰加密日誌檔案和摘要檔案。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。

以下安全最佳實務也可用來解決 CloudTrail 中的資料保護問題：

- 使用 AWS KMS 金鑰加密 CloudTrail 日誌檔案、摘要檔案和事件資料存放區 (SSE-KMS)
- 適用於 CloudTrail 的 Amazon S3 儲存貯體政策
- 驗證 CloudTrail 日誌檔案完整性
- 在 AWS 帳戶之間共用 CloudTrail 日誌檔案

由於 CloudTrail 日誌檔案存放在儲存貯體或 Amazon S3 的儲存貯體，因此您也應該檢視 Amazon Simple Storage Service 使用者指南中的資料保護資訊。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) 是 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員會控制誰經過身分身分驗證 (已登入) 並得到授權 (具有許可) 來使用 CloudTrail 資源。IAM 是 AWS 服務 您可以免費使用的 。

主題


- 目標對象
- 使用身分驗證
- 使用政策管理存取權
- AWS CloudTrail 如何使用 IAM
- 的身分型政策範例 AWS CloudTrail
- AWS CloudTrail 資源型政策範例
- 適用於 CloudTrail 的 Amazon S3 儲存貯體政策
- 適用於 CloudTrail Lake 查詢結果的 Amazon S3 儲存貯體政策
- 適用於 CloudTrail 索的 Amazon SNS 主題政策
- 對 AWS CloudTrail 身分和存取進行故障診斷
- 使用 CloudTrail 的服務連結角色
- AWS 的 受管政策 AWS CloudTrail


## 目標對象

使用方式 AWS Identity and Access Management (IAM) 會根據您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 對 AWS CloudTrail 身分和存取進行故障診斷)
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 AWS CloudTrail 如何使用 IAM)
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 的身分型政策範例 AWS CloudTrail)

## 使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色身分進行身分驗證。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的如何登入您的 AWS 帳戶。

對於程式設計存取， AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的 API 請求的AWS 第 4 版簽署程序。

### AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分可完整存取所有 AWS 服務 和資源。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

### 聯合身分

最佳實務是要求人類使用者使用聯合身分提供者，以 AWS 服務 使用臨時憑證存取 。

聯合身分是來自您的企業目錄、Web 身分提供者的使用者，或使用來自身分來源的 AWS 服務 憑證存取 Directory Service 的使用者。聯合身分會擔任角色，而該角色會提供臨時憑證。

若需集中化管理存取權限，建議使用 AWS IAM Identity Center。如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的什麼是 IAM Identity Center？。

### IAM 使用者和群組

IAM 使用者https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取 。

IAM 群組會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

### IAM 角色

IAM 角色https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過從使用者切換到 IAM 角色 （主控台） 或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

# 使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS ， 會評估這些政策。大多數政策會以 JSON 文件 AWS 形式存放在 中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的 JSON 政策概觀。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

## 身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的在受管政策與內嵌政策之間選擇。

## 資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 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。您必須在資源型政策中指定主體。

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

## 其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《 IAM 使用者指南》中的 IAM 實體許可界限。
- 服務控制政策 (SCP) — 為 AWS Organizations中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的資源控制政策 (RCP)。
- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參《IAM 使用者指南》中的工作階段政策。

### 多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 在涉及多個政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

## AWS CloudTrail 如何使用 IAM

在您使用 IAM 管理 CloudTrail 的存取之前，請了解有哪些 IAM 功能可以與 CloudTrail 搭配使用。

您可以搭配 使用的 IAM 功能 AWS CloudTrail

| IAM 功能 | CloudTrail 支援 |
| --- | --- |
| 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) | 是 |
| 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 |

若要全面了解 CloudTrail 和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《IAM 使用者指南》中的AWS 與 IAM 搭配使用的 服務。

### 適用於 CloudTrail 的身分型政策

支援身分型政策：是

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

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。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。

適用於 CloudTrail 的身分型政策範例

若要檢視 CloudTrail 身分類型政策的範例，請參閱 的身分型政策範例 AWS CloudTrail。

## CloudTrail 內的資源型政策

支援資源型政策：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。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以在其他帳戶內指定所有帳戶或 IAM 實體作為資源型政策的主體。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

CloudTrail 支援下列類型的資源型政策：

- 用於 CloudTrail Lake 與 外部事件來源整合之頻道的資源型政策 AWS。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。如需與 CloudTrail Lake 建立整合的詳細資訊，請參閱在 外部建立與事件來源的整合 AWS。
- 以資源為基礎的政策，以控制哪些委託人可以在您的事件資料存放區上執行動作。您可以使用資源型政策來提供事件資料存放區的跨帳戶存取權。
- 儀表板上的資源型政策，允許 CloudTrail 在您為儀表板設定重新整理排程時，以您定義的間隔重新整理 CloudTrail Lake 儀表板。如需詳細資訊，請參閱使用 CloudTrail 主控台設定自訂儀表板的重新整理排程。

範例

若要檢視 CloudTrail 資源型政策範例，請參閱 AWS CloudTrail 資源型政策範例。

## 適用於 CloudTrail 的政策動作

支援政策動作：是

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

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。政策會使用動作來授予執行相關聯動作的許可。

如要查看 CloudTrail 動作的清單，請參閱《服務授權參考》中的 AWS CloudTrail定義的動作。

CloudTrail 中的政策動作會在動作前使用以下字首：

```
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 會定義自己的一組動作，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*"
```

## CloudTrail 的政策資源

支援政策資源：是

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

Resource JSON 政策元素可指定要套用動作的物件。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

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

如要查看 CloudTrail 資源類型及其 ARN 的清單，請參閱《服務授權參考》中的 AWS CloudTrail定義的資源。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 CloudTrail 中，有四種資源類型：線索、事件資料存放區、儀表板和頻道。每個資源都有一個相關聯的唯一 Amazon Resource Name (ARN)。在政策中，您可以使用 ARN 識別要套用政策的資源。CloudTrail 目前不支援其他資源類型，因此有時稱為子資源。

CloudTrail 追蹤資源具有以下 ARN：

```
arn:${Partition}:cloudtrail:${Region}:${Account}:trail/{TrailName}
```

CloudTrail 事件資料存放區資源具有以下 ARN：

```
arn:${Partition}:cloudtrail:${Region}:${Account}:eventdatastore/{EventDataStoreId}
```

CloudTrail 儀表板資源具有下列 ARN：

```
arn:${Partition}:cloudtrail:${Region}:${Account}:dashboard/{DashboardName}
```

CloudTrail 通道資源具有以下 ARN：

```
arn:${Partition}:cloudtrail:${Region}:${Account}:channel/{ChannelId}
```

如需 ARNs 格式的詳細資訊，請參閱 Amazon Resource Name (ARNs) AWS 和服務命名空間。

例如，對於 ID 為 *123456789012* AWS 帳戶 的 ，若要指定存在於陳述式中美國東部 （俄亥俄） 區域中名為 *My-Trail* 的線索，請使用下列 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線索 AWS 區域，請使用萬用字元 (*)：

```
"Resource": "arn:aws:cloudtrail:us-east-2:123456789012:trail/*"
```

有些 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 動作都涉及多個資源。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"
```

## CloudFront 的政策條件索引鍵

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` 元素會根據定義的條件，指定陳述式的執行時機。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。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

CloudTrail 不會定義自己的條件索引鍵，但是支援使用一些全域條件索引鍵。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。

如要查看 CloudTrail 條件索引鍵的清單，請參閱《服務授權參考》中的 AWS CloudTrail的條件索引鍵。若要了解您可以使用條件金鑰的動作和資源，請參閱 定義的動作 AWS CloudTrail。

## CloudTrail 中的 ACL

支援 ACL：否

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

## ABAC 與 CloudTrail

支援 ABAC (政策中的標籤)：是

屬性型存取控制 (ABAC) 是一種授權策略，依據稱為標籤的屬性來定義許可。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

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

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

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

您可以將標籤連接到 CloudTrail 資源，或是在請求中將標籤傳遞給 CloudTrail。如需標記 CloudTrail 資源的詳細資訊，請參閱 使用 CloudTrail 主控台建立追蹤 與 使用 建立、更新和管理線索 AWS CLI。

### 將暫時登入資料與 CloudTrail 搭配使用

支援臨時憑證：是

臨時登入資料提供 AWS 資源的短期存取權，當您使用聯合或切換角色時，會自動建立。 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 使用者指南》中的 IAM 中的臨時安全憑證與可與 IAM 搭配運作的AWS 服務。

### 轉送 CloudTrail 的存取工作階段

支援轉寄存取工作階段 (FAS)：是

轉送存取工作階段 (FAS) 使用呼叫 的委託人許可 AWS 服務，並結合 AWS 服務 請求向下游服務提出請求。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。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務。

> **Warning**
>
> 變更服務角色的許可有可能會中斷 CloudTrail 功能。只有在 CloudTrail 提供指引時，才能編輯服務角色。

### CloudTrail 的服務連結角色

支援服務連結角色：是

服務連結角色是連結至 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

CloudTrail 支援與 整合的服務連結角色 AWS Organizations。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存放 AWS 帳戶 組織中所有 的日誌事件。如需有關建立或管理 CloudTrail 服務連結角色的詳細資訊，請參閱 使用 CloudTrail 的服務連結角色。

## 的身分型政策範例 AWS CloudTrail

依預設，使用者和角色不具備建立或修改 CloudTrail 資源的許可。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。

如需了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策 (主控台)。

如需 CloudTrail 所定義之動作和資源類型的詳細資訊，包括每種資源類型的 ARN 格式，請參閱《服務授權參考》中的適用於 AWS CloudTrail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
- 授予 CloudTrail 使用者的自訂許可

### 政策最佳實務

以身分為基礎的政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 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 受管政策並轉向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，進一步減少許可。如需更多資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 等使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的透過 MFA 的安全 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱《IAM 使用者指南》中的 IAM 安全最佳實務。

CloudTrail 沒有可在政策陳述式的 `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。此線索是在美國東部（俄亥俄）區域（其主區域）建立，AWS 帳戶 其 ID 為 *123456789012*。

JSON

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

下列範例會示範政策，明確拒絕未命名 *My-First-Trail* 的任何追蹤的 CloudTrail 動作。

JSON

```
{
  "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

您可以使用許可和政策，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。

JSON

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

在第二個政策中，允許對所有 CloudTrail 資源執行 DescribeTrails 和 GetTrailStatus 動作：

JSON

```
{
    "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。

下列範例顯示名為 的 AWS CLI 設定檔中設定的開發人員群組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": "amzn-s3-demo-bucket",
            "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。

JSON

```
{
```

```
    "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。

JSON

```
{
    "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，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 中 CloudTrail 資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

授予 CloudTrail 管理許可

若要允許 IAM 使用者管理 CloudTrail 資源，例如追蹤、事件資料存放區或通道，您必須明確授予執行與 CloudTrail 任務相關聯之動作的許可。在大多數情況下，您可以使用包含預先定義許可的 AWS 受管政策。

> **Note**
>
> 您授予使用者執行 CloudTrail 管理任務的許可，和 CloudTrail 所需要以便傳遞日誌檔案到 Amazon S3 儲存貯體或傳送通知給 Amazon SNS 主題的許可不相同。如需這些許可的詳細資訊，請參閱 適用於 CloudTrail 的 Amazon S3 儲存貯體政策。
> 如果您設定與 Amazon CloudWatch Logs 整合，CloudTrail 還需要它可擔任的角色，將事件交付到 Amazon CloudWatch Logs 日誌群組。您必須建立 CloudTrail 使用的角色。如需詳細資訊，請參閱授與在 CloudTrail 主控台上檢視和設定 Amazon CloudWatch Logs 資訊的許可及傳送事件到 CloudWatch Logs。

下列 AWS 受管政策適用於 CloudTrail：

- AWSCloudTrail_FullAccess – 此政策提供對 CloudTrail 資源 (例如追蹤、事件資料存放區和通道等) 執行 CloudTrail 動作的完整存取權。此政策提供建立、更新和刪除 CloudTrail 追蹤、事件資料存放區和通道所需的許可。

  此政策還提供管理 Amazon S3 儲存貯體、CloudWatch Logs 的日誌群組，以及追蹤的 Amazon SNS 主題的許可。不過，AWSCloudTrail_FullAccess 受管政策不提供刪除 Amazon S3 儲存貯體、CloudWatch Logs 的日誌群組，以及 Amazon SNS 主題的許可。如需其他 受管政策的相關資訊 AWS 服務，請參閱 AWS 受管政策參考指南。

  > **Note**
  >
  > 此AWSCloudTrail_FullAccess政策不適用於在您的 之間廣泛共用 AWS 帳戶。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 – 此政策授予檢視 CloudTrail 主控台 (包括近期事件和事件歷史記錄) 的許可。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：

- 中的使用者和群組 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。遵循《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。

- 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。
  - (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 來提供身分，例如使用者和角色、存取您帳戶中的資源，請參閱《IAM 使用者指南》中的設定 IAM 和存取 AWS 資源的管理。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合您嘗試執行之 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。此政策包含在主控台或使用 或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

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

# 授予 CloudTrail 使用者的自訂許可

CloudTrail 政策會將許可授予使用 CloudTrail 的使用者。如果您需要將不同的許可授予使用者，則可以將 CloudTrail 政策連接至 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
- 授予在 CloudTrail 主控台上檢視 AWS Config 資訊的許可
- 授與在 CloudTrail 主控台上檢視和設定 Amazon CloudWatch Logs 資訊的許可
- 其他資訊


## 唯讀存取

下列範例顯示可授予 CloudTrail 追蹤唯讀存取的政策。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。

JSON

```
{
    "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 AWS 的資源。對於 CloudTrail 動作的控制存取政策，Resource 元素通常會設定為 *，這是表示「所有資源」的萬用字元。

Action 元素中的值對應至服務所支援的 API。這些動作的前面會加上 cloudtrail:，意指其參照 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"]

  這允許結尾為 "Logging" 的所有 CloudTrail 動作 (StartLogging、StopLogging)。
- "Action": ["cloudtrail:*"]

  這允許所有 CloudTrail 動作，但不允許其他 AWS 服務的動作。
- "Action": ["*"]

  這允許所有 AWS 動作。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。如需完整 CloudTrail 動作清單，請參閱 AWS CloudTrail API 參考。

完整 存取

下列範例顯示可授予 CloudTrail 完整存取權限的政策。這相當於受管政策 AWSCloudTrail_FullAccess。政策會將執行所有 CloudTrail 動作的許可授予使用者。另外也可讓使用者記錄 Amazon S3 和 AWS Lambda中的資料事件、管理 Amazon S3 儲存貯體中的檔案、管理 CloudWatch Logs 如何監控 CloudTrail 日誌事件，以及管理與使用者相關聯之帳戶中的 Amazon SNS 主題。

> **Important**
>
> AWSCloudTrail_FullAccess 政策或同等許可不適用於在您的 AWS 帳戶之間廣泛共用。具有此角色或同等存取權的使用者能夠停用或重新設定 AWS 帳戶中最敏感和重要的稽核函數。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。

JSON

```
{
```

```
    "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:::amzn-s3-demo-logging-bucket1*"
            ]
        },
        {
            "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": "*"
        }
    ]
}
```

授予在 CloudTrail 主控台上檢視 AWS Config 資訊的許可

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軸。將此政策連接到您的使用者，以授予他們唯讀 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。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "config:Get*",
            "config:Describe*",
            "config:List*"
        ],
        "Resource": "*"
    }]
}
```

如需詳細資訊，請參閱 檢視使用 參考的資源 AWS Config。

授與在 CloudTrail 主控台上檢視和設定 Amazon CloudWatch Logs 資訊的許可

如果您有足夠許可，您可以在 CloudTrail 主控台中檢視和設定到 CloudWatch Logs 的事件交付。這些許可可能超出 CloudTrail 管理員可以授與的範圍。將此政策連接到將設定和管理 CloudTrail 與 CloudWatch Logs 整合的管理員。該政策不會直接在 CloudTrail 和 CloudWatch Logs 為他們授與許可，而是受與建立和設定角色 CloudTrail 所需的許可，以便該角色成功將事件傳遞給您的 CloudWatch 群組。

JSON

```
{
    "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 Logs 監控 CloudTrail 日誌檔案。

其他資訊

若要進一步了解如何使用 IAM 來提供身分，例如使用者和角色、存取您帳戶中的資源，請參閱《IAM 使用者指南》中的 資源的入門和存取管理。 AWS

## AWS CloudTrail 資源型政策範例

本節提供 CloudTrail Lake 儀表板、事件資料存放區和頻道的範例資源型政策。

CloudTrail 支援下列類型的資源型政策：

- 用於 CloudTrail Lake 與 外部事件來源整合之頻道的資源型政策 AWS。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。如需與 CloudTrail Lake 建立整合的詳細資訊，請參閱在 外部建立與事件來源的整合 AWS。
- 以資源為基礎的政策，以控制哪些委託人可以在您的事件資料存放區上執行動作。您可以使用資源型政策來提供事件資料存放區的跨帳戶存取權。
- 儀表板上的資源型政策，允許 CloudTrail 在您為儀表板設定重新整理排程時，以您定義的間隔重新整理 CloudTrail Lake 儀表板。如需詳細資訊，請參閱使用 CloudTrail 主控台設定自訂儀表板的重新整理排程。

範例：

- 頻道的資源型政策範例
- 事件資料存放區的資源型政策範例
- 儀表板的資源型政策範例

## 頻道的資源型政策範例

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。

政策所需的資訊取決於整合類型。

- 對於直接整合，CloudTrail 會要求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。當您使用 CloudTrail 主控台建立整合時，CloudTrail 會自動將合作夥伴的 AWS 帳戶 IDs 新增至資源政策。請參閱合作夥伴的文件，了解如何取得政策所需的 AWS 帳戶 號碼。
- 對於解決方案整合，您必須指定至少一個 AWS 帳戶 ID 作為委託人，並且可以選擇輸入外部 ID 以防止混淆代理人。

資源型政策的需求如下：

- 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。委託人是帳戶、使用者、角色或聯合身分使用者。陳述式最多可以有 50 個主體。
- 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`

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

下列範例將許可授與具有 ARN arn:aws:iam::111122223333:root、arn:aws:iam::444455556666:root 和 arn:aws:iam::123456789012:root 的主體，以在具有 ARN arn:aws:cloudtrail:us-east-1:777788889999:channel/EXAMPLE-80b5-40a7-ae65-6e099392355b 的 CloudTrail 通道上呼叫 PutAuditEvents API。

JSON

```
{
    "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。

下列範例將許可授與具有 ARN `arn:aws:iam::111122223333:root`、`arn:aws:iam::444455556666:root` 和 `arn:aws:iam::123456789012:root` 的主體，以在 CloudTrail 通道資源上呼叫 PutAuditEvents API (如果對 `PutAuditEvents` API 的呼叫含有在政策中定義的外部 ID 值)。

JSON

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

## 事件資料存放區的資源型政策範例

以資源為基礎的政策可讓您控制哪些委託人可以在事件資料存放區上執行動作。

您可以使用資源型政策來提供跨帳戶存取權，以允許選取的委託人查詢您的事件資料存放區、列出和取消查詢，以及檢視查詢結果。

對於 CloudTrail Lake 儀表板，資源型政策用於允許 CloudTrail 在事件資料存放區上執行查詢，以在儀表板重新整理時填入儀表板小工具的資料。當您在 CloudTrail 主控台上建立自訂儀表板或啟用反白儀表板時，CloudTrail Lake 可讓您選擇將預設資源型政策連接至事件資料存放區。

事件資料存放區的資源型政策支援下列動作：

- `cloudtrail:StartQuery`
- `cloudtrail:CancelQuery`
- `cloudtrail:ListQueries`
- `cloudtrail:DescribeQuery`
- `cloudtrail:GetQueryResults`
- `cloudtrail:GenerateQuery`
- `cloudtrail:GenerateQueryResultsSummary`
- `cloudtrail:GetEventDataStore`

當您在 CloudTrail 主控台上建立或更新事件資料存放區，或管理儀表板時，您可以選擇將資源型政策新增至事件資料存放區。您也可以執行 put-resource-policy 命令，將資源型政策連接至事件資料存放區。

以資源為基礎的政策包含一或多個陳述式。例如，它可以包含一個允許 CloudTrail 查詢儀表板事件資料存放區的陳述式，以及另一個允許跨帳戶存取查詢事件資料存放區的陳述式。您可以從 CloudTrail 主控台的事件資料存放區詳細資訊頁面更新現有事件資料存放區的資源型政策。

對於組織事件資料存放區，CloudTrail 會建立預設資源型政策，列出允許委派管理員帳戶在組織事件資料存放區上執行的動作。此政策中的許可衍生自 中的委派管理員許可 AWS Organizations。此政策會在組織事件資料存放區或組織變更後自動更新（例如，CloudTrail 委派管理員帳戶已註冊或移除）。

範例：

- 範例：允許 CloudTrail 執行查詢以重新整理儀表板
- 範例：允許其他帳戶查詢事件資料存放區並檢視查詢結果

### 範例：允許 CloudTrail 執行查詢以重新整理儀表板

若要在重新整理期間填入 CloudTrail Lake 儀表板上的資料，您需要允許 CloudTrail 代表您執行查詢。若要這樣做，請將資源型政策連接至與儀表板小工具相關聯的每個事件資料存放區，其中包含允許 CloudTrail 執行`StartQuery`操作以填入小工具資料的陳述式。

以下是 陳述式的要求：

- 唯一的`Principal`是 `cloudtrail.amazonaws.com`。
- 唯一`Action`允許的是 `cloudtrail:StartQuery`。
- `Condition` 僅包含儀表板 ARN (s) 和 AWS 帳戶 ID。對於 `AWS:SourceArn`，您可以提供儀表板 ARNs的陣列。

下列範例政策包含一個陳述式，允許 CloudTrail 針對名為 `example-dashboard1`和 的兩個自訂儀表板`example-dashboard2`，以及`AWSCloudTrail-Highlights`針對帳戶 的 Highlights 儀表板，在事件資料存放區上執行查詢`123456789012`。

JSON

```
{
    "Version":"2012-10-17",
    "Statement":
    [
        {
            "Effect": "Allow",
            "Principal":
            {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action":
            [
                "cloudtrail:StartQuery"
            ],
            "Resource": "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/*",
            "Condition": {
               "StringLike": {
                  "AWS:SourceArn": [
                     "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/
example-dashboard1",
```

```
                    "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/
example-dashboard2",
                    "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/
AWSCloudTrail-Highlights"
                ],
                "AWS:SourceAccount": "123456789012"
            }
        }
    }
  ]
}
```

範例：允許其他帳戶查詢事件資料存放區並檢視查詢結果

您可以使用資源型政策來提供事件資料存放區的跨帳戶存取權，以允許其他帳戶在您的事件資料存放區上執行查詢。

下列範例政策包含一個陳述式，允許帳戶 111122223333、999999999999、 777777777777和中的根使用者111111111111對帳戶 ID 擁有的事件資料存放區執行查詢並取得查詢結果555555555555。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "policy1",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::777777777777:root",
            "arn:aws:iam::999999999999:root",
            "arn:aws:iam::111111111111:root"
        ]
      },
      "Action": [
        "cloudtrail:StartQuery",
        "cloudtrail:GetEventDataStore",
        "cloudtrail:GetQueryResults"
```

```
      ],
      "Resource": "arn:aws:cloudtrail:us-east-1:555555555555:eventdatastore/
example80-699f-4045-a7d2-730dbf313ccf"
    }
  ]
}
```

## 儀表板的資源型政策範例

您可以為 CloudTrail Lake 儀表板設定重新整理排程，這可讓 CloudTrail 在您設定重新整理排程時，以您定義的間隔代表您重新整理儀表板。若要這樣做，您需要將資源型政策連接至儀表板，以允許 CloudTrail 在儀表板上執行`StartDashboardRefresh`操作。

資源型政策的需求如下：

- 唯一的`Principal`是 `cloudtrail.amazonaws.com`。
- 政策中唯一`Action`允許的是 `cloudtrail:StartDashboardRefresh`。
- `Condition` 僅包含儀表板 ARN 和 AWS 帳戶 ID。

下列範例政策允許 CloudTrail 重新整理帳戶 名為 `exampleDash`的儀表板`123456789012`。

JSON

```
{
    "Version":"2012-10-17",
    "Statement":
    [
        {
            "Effect": "Allow",
            "Principal":
            {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action":
            [
                "cloudtrail:StartDashboardRefresh"
            ],
            "Resource": "arn:aws:cloudtrail:us-east-1:123456789012:dashboard/*",
            "Condition": {
                "StringEquals": {
```

```
                    "AWS:SourceArn": "arn:aws:cloudtrail:us-
east-1:123456789012:dashboard/exampleDash",
                    "AWS:SourceAccount":"123456789012"
                }
            }
        }
    ]
}
```

## 適用於 CloudTrail 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 使用 為組織建立線索 AWS CLI。

若要將日誌檔案交付到 S3 儲存貯體，CloudTrail 必須具備必要的許可，而且不得設定為申請者付款儲存貯體。

CloudTrail 會在政策中為您新增下列欄位：

- 允許的 SID
- 儲存貯體名稱
- CloudTrail 的服務委託人名稱
- 存放日誌檔案的資料夾名稱，包括儲存貯體名稱、字首 （ 如果您指定了 ） 和 AWS 您的帳戶 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 CloudTrail 僅針對特定追蹤寫入 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。

> **Note**
>
> 如果您的追蹤設定錯誤 (例如，S3 儲存貯體無法連線)，CloudTrail 會在 30 天內嘗試重新傳遞日誌檔案到您的 S3 儲存貯體，且您需要為這些嘗試傳遞事件支付標準 CloudTrail 費用。若要避免支付追蹤設定錯誤費用，您需要刪除追蹤。

下列政策允許 CloudTrail 從支援的 將日誌檔案寫入儲存貯體 AWS 區域。將 *amzn-s3-demo-bucket*、*#optionalPrefix#/*、*myAccountID*、*region* 和 *trailName* 取代為您的組態的適當值。

S3 儲存貯體政策

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "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:::amzn-s3-demo-
bucket/[optionalPrefix]/AWSLogs/myAccountID/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceArn":
 "arn:aws:cloudtrail:region:myAccountID:trail/trailName"
                }
            }
        }
    ]
}
```

如需 的詳細資訊 AWS 區域，請參閱 CloudTrail 支援的區域。

內容


- 指定 CloudTrail 日誌交付的現有儲存貯體
- 從其他帳戶接收日誌檔案
- 建立或更新 Amazon S3 儲存貯體以存放組織追蹤的日誌檔案
- 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 CloudTrail 日誌交付的現有儲存貯體

如果您指定現有的 S3 儲存貯體做為日誌檔案交付的儲存位置，您必須將政策連接到儲存貯體以允許 CloudTrail 寫入儲存貯體。

> **Note**
>
> 最佳實務是使用 CloudTrail 日誌專用的 S3 儲存貯體。

將必要的 CloudTrail 政策新增至 Amazon S3 儲存貯體

1. 開啟位於 https://console.aws.amazon.com/s3/ 的 Amazon S3 主控台。
2. 選擇您想要讓 CloudTrail 交付日誌檔案的目標儲存貯體，然後選擇 Permissions (許可)。
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**
   >
   > 如果現有的儲存貯體已連接一或多個政策，請將 CloudTrail 存取陳述式新增至這些政策。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 將日誌檔案從多個 AWS 帳戶交付到單一 S3 儲存貯體。如需詳細資訊，請參閱從多個帳戶接收 CloudTrail 日誌檔案。

## 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。這個儲存貯體必須具備特定政策，允許 CloudTrail 將組織的日誌檔案放入儲存貯體。

以下是名為 amzn-s3-demo-bucket 的 Amazon S3 儲存貯體的範例政策，該儲存貯體為組織的管理帳戶所擁有。 將 *amzn-s3-demo-bucket*、 *region*、 *managementAccountID*、 *trailName* 和 *o-organizationID* 取代為組織的值

此儲存貯體政策包含三個陳述式。

- 第一個陳述式允許 CloudTrail 在 Amazon S3 儲存貯體上呼叫 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 CloudTrail 僅針對特定追蹤寫入 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。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "cloudtrail.amazonaws.com"
                ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "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:::amzn-s3-demo-bucket/
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:::amzn-s3-demo-bucket/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 日誌檔案。

## 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。

> **Note**
>
> 如果您的追蹤設定錯誤 (例如，S3 儲存貯體無法連線)，CloudTrail 會在 30 天內嘗試重新傳遞日誌檔案到您的 S3 儲存貯體，且您需要為這些嘗試傳遞事件支付標準 CloudTrail 費用。若要避免支付追蹤設定錯誤費用，您需要刪除追蹤。

常見的 Amazon S3 政策設定錯誤

當您在建立或更新追蹤的過程中建立新的儲存貯體時，CloudTrail 會將必要的許可連接到您的儲存貯體。儲存貯體政策使用服務主體名稱 `"cloudtrail.amazonaws.com"`，其允許 CloudTrail 傳遞所有區域的日誌。

如果 CloudTrail 未傳遞某個區域的日誌，可能是您的儲存貯體具有為每個區域指定 CloudTrail 帳戶 ID 的舊版政策。此政策授予 CloudTrail 許可，只能傳遞指定區域的日誌。

最佳實務是更新政策以搭配 CloudTrail 服務委託人使用許可。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"`。這會授予 CloudTrail 許可，以傳遞目前和新區域的日誌。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。將 *`amzn-s3-demo-bucket`*、*`#optionalPrefix#/`*、*`myAccountID`*、*`region`* 和 *`trailName`* 取代為您的組態的適當值。

Example儲存貯體政策與服務主體名稱範例

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailAclCheck20150319",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "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:::amzn-s3-demo-
bucket/[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綴，然後使用 CloudTrail 主控台指定與追蹤中的儲存貯體相同的前綴。

更新 Amazon S3 儲存貯體的日誌檔案前綴

1. 開啟位於 https://console.aws.amazon.com/s3/ 的 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:::amzn-s3-demo-bucket/prefix/AWSLogs/myAccountID/*",
```

5. 選擇儲存。
6. 前往 https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
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。

## 適用於 CloudTrail Lake 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 查詢結果傳送到 S3 儲存貯體，CloudTrail 必須具備必要的許可，而且不得設定為申請者付款儲存貯體。

CloudTrail 會在政策中為您新增下列欄位：

- 允許的 SID
- 儲存貯體名稱
- CloudTrail 的服務委託人名稱

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 全域條件索引鍵 `aws:SourceArn` 有助於確保 CloudTrail 僅針對事件資料存放區寫入 S3 儲存貯體。

下列政策允許 CloudTrail 將查詢結果傳遞到受支援 AWS 區域中的儲存貯體。將 *amzn-s3-demo-bucket*、*myAccountID* 和 *myQueryRunningRegion* 取代為您的組態的適當值。*myAccountID* 是用於 CloudTrail AWS 的帳戶 ID，可能與 S3 儲存貯體 AWS 的帳戶 ID 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， 會 AWS KMS 解析請求者帳戶中的金鑰。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

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailLake1",
            "Effect": "Allow",
            "Principal": {"Service": "cloudtrail.amazonaws.com"},
            "Action": [
                "s3:PutObject*",
                "s3:Abort*"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
```

```
            "Condition": {
                "StringEquals": {
                    "aws:sourceAccount": "111111111111"
                },
                "ArnLike": {
                    "aws:sourceArn": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/*"
                }
            }
        },
        {
            "Sid": "AWSCloudTrailLake2",
            "Effect": "Allow",
            "Principal": {"Service":"cloudtrail.amazonaws.com"},
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:sourceAccount": "111111111111"
                },
                "ArnLike": {
                    "aws:sourceArn": "arn:aws:cloudtrail:us-
east-1:111111111111:eventdatastore/*"
                }
            }
        }
    ]
}
```

內容


- 為 CloudTrail Lake 查詢結果指定現有的儲存貯體
- 其他資源


## 為 CloudTrail Lake 查詢結果指定現有的儲存貯體

如果您指定現有的 S3 儲存貯體做為 CloudTrail Lake 查詢結果傳送的儲存位置，您必須將政策連接到儲存貯體，以允許 CloudTrail 將查詢結果傳送到儲存貯體。

> **Note**
>
> 最佳實務是使用 CloudTrail Lake 查詢結果專用的 S3 儲存貯體。

將必要的 CloudTrail 政策新增至 Amazon S3 儲存貯體

1. 開啟位於 https://console.aws.amazon.com/s3/ 的 Amazon S3 主控台。
2. 選擇您想要讓 CloudTrail 傳送查詢結果的目標儲存貯體，然後選擇 Permissions (許可)。
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**
>
> 如果現有的儲存貯體已連接一或多個政策，請將 CloudTrail 存取陳述式新增至這些政策。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。

## 適用於 CloudTrail 索的 Amazon SNS 主題政策

若要將通知傳送給 SNS 主題，CloudTrail 必須具有必要的許可。當您在 CloudTrail 主控台建立或更新線索的過程中建立 Amazon SNS 主題時，CloudTrail 會自動將必要的許可連接到儲存貯體。

> **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 新增以下陳述式到政策為您提供下列欄位：

- 允許的 SID。
- CloudTrail 的服務委託人名稱。
- SNS 主題，包含區域、帳戶 ID 和主題名稱。

下列政策允許 CloudTrail 傳送有關受支援區域之日誌檔案傳遞的通知。如需詳細資訊，請參閱 CloudTrail 支援的區域。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

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSCloudTrailSNSPolicy20131101",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:us-east-1:111111111111:SNSTopicName"
        }
    ]
}
```

若要使用加密的 Amazon SNS 主題來傳送通知，您還必須將下列陳述 AWS KMS式新增至 政策，以啟用事件來源 (CloudTrail) 與加密主題之間的相容性 AWS KMS key。

KMS 金鑰政策

JSON

```
{
    "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 服務和加密主題的事件來源之間的相容性。

內容


- SNS 主題政策的安全最佳實務
- 指定用於傳送通知的現有主題
- 針對 SNS 主題政策進行故障診斷
  - CloudTrail 不會傳送區域的通知
  - CloudTrail 不會傳送組織中成員帳戶的通知
- 其他資源


## SNS 主題政策的安全最佳實務

根據預設，CloudTrail 附加到 Amazon SNS 主題的 IAM 政策聲明允許 CloudTrail 服務主體發佈到由 ARN 識別的 SNS 主題。若要協助防止攻擊者存取您的 SNS 主題，並代表 CloudTrail 傳送通知給主題收件人，請手動編輯您的 CloudTrail SNS 主題政策，以新增 `aws:SourceArn` 條件金鑰新增至由 CloudTrail 附加的政策聲明。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。在將條件金鑰新增至 SNS 主題政策之前，請從 CloudTrail 主控台中的線索設定取得 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。aws:SourceAccount 的值是擁有 CloudTrail 線索的帳戶 ID。此範例限制只能登入 AWS 帳戶 123456789012 的使用者存取 SNS 主題。

```
    {
      "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

您可以在 Amazon SNS 主控台中將許可手動新增至主題政策，然後在 CloudTrail 主控台中指定主題。

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政策。
4. 使用區域、帳戶 ID SNS topic policy 和主題名稱的適當值，從 新增陳述式。
5. 如果您的主題是加密主題，您必須允許 CloudTrail 擁有 `kms:GenerateDataKey*` 和 `kms:Decrypt` 許可。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 CloudTrail 主控台，並指定線索的主題。

## 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 不會傳送區域的通知
- CloudTrail 不會傳送組織中成員帳戶的通知

CloudTrail 不會傳送區域的通知

當您在建立或更新線索的過程中建立新的主題時，CloudTrail 會將必要的許可連接至您的主題。主題政策使用服務主體名稱 `"cloudtrail.amazonaws.com"`，允許 CloudTrail 傳送所有區域的通知。

如果 CloudTrail 未傳送某個區域的通知，則可能是您的主題具有為每個區域指定 CloudTrail 帳戶 ID 的舊版政策。這種類型的政策提供 CloudTrail 僅針對指定區域傳送通知的許可。

最佳實務是更新政策以搭配 CloudTrail 服務委託人使用許可。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"`。

下列範例政策提供 CloudTrail 許可，以傳送目前和新區域的通知：

Example主題政策與服務主體名稱

JSON

```
{
```

```
    "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 不會傳送組織中成員帳戶的通知

當具有 AWS Organizations 組織線索的成員帳戶未傳送 Amazon SNS 通知時，SNS 主題政策的組態可能會發生問題。即使資源驗證失敗，CloudTrail 仍會在成員帳戶中建立組織線索，例如，組織線索的 SNS 主題不包含所有成員帳戶 IDs。如果 SNS 主題政策不正確，則會發生授權失敗。

若要檢查追蹤的 SNS 主題政策是否有授權失敗：

- 從 CloudTrail 主控台，檢查追蹤的詳細資訊頁面。如果發生授權失敗，詳細資訊頁面會包含警告，SNS authorization failed並指示 修正 SNS 主題政策。
- 從 AWS CLI中，執行 get-trail-status命令。如果發生授權失敗，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》。

## 對 AWS CloudTrail 身分和存取進行故障診斷

請使用以下資訊來協助您診斷和修復使用 CloudTrail 和 IAM 時發生的常見問題。

主題

- 我未獲授權，不得在 CloudTrail 中執行動作

- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 以外的人員 AWS 帳戶 存取我的 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

## 我未獲授權，不得在 CloudTrail 中執行動作

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 管理員。您的管理員提供您的簽署憑證。

如果 AWS 管理主控台 告訴您未獲授權執行 動作，則您必須聯絡管理員尋求協助。您的管理員是為您提供簽署憑證的人員。

以下錯誤範例發生的時候為 mateojackson IAM 使用者嘗試使用主控台檢視追蹤的相關詳細資訊，但沒有適當的 CloudTrail 受管政策 (AWSCloudTrail_FullAccess 或 AWSCloudTrail_ReadOnlyAccess)，也沒有套用至其帳戶的同等許可。

```
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受管政策或其同等許可的 IAM 使用者或角色登入，且無法設定 AWS Config 或 Amazon CloudWatch Logs 與線索的整合，則您可能缺少與這些服務整合所需的許可。如需詳細資訊，請參閱授予在 CloudTrail 主控台上檢視 AWS Config 資訊的許可及授與在 CloudTrail 主控台上檢視和設定 Amazon CloudWatch Logs 資訊的許可。

## 我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行 iam:PassRole 動作，則必須更新您的政策，以便您將角色傳遞至 CloudTrail。

有些 AWS 服務 可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 marymajor 的 IAM 使用者嘗試使用主控台在 CloudTrail 中執行動作時，就發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞給服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

## 我想要允許 以外的人員 AWS 帳戶 存取我的 CloudTrail 資源

您可以建立角色並和多個 AWS 帳戶之間共用 CloudTrail 資訊。如需詳細資訊，請參閱在 AWS 帳戶之間共用 CloudTrail 日誌檔案。

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 CloudTrail 是否支援這些功能，請參閱 AWS CloudTrail 如何使用 IAM。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 IAM 使用者中提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有。
- 如需了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

## 我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行 iam:PassRole 動作，則必須更新您的政策，以便您將角色傳遞至 CloudTrail。

有些 AWS 服務 可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 marymajor 的 IAM 使用者嘗試使用主控台在 CloudTrail 中執行動作時，就發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞給服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

## 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 CLI 或 API AWS Organizations 操作新增委派管理員時，如果 CloudTrail 服務連結角色不存在，則不會自動建立這些角色。只有在您直接從管理帳戶呼叫 CloudTrail 服務時，才會建立服務連結角色。例如，當您使用 CloudTrail 主控台或 CloudTrail API 新增委派管理員或建立組織追蹤 AWS CLI 或事件資料存放區時，即會建立AWSServiceRoleForCloudTrail服務連結角色。

當您使用 AWS CloudTrail；CLI 或 API 操作新增委派管理員時，CloudTrail AWSServiceRoleForCloudTrailEventContext 會同時建立 AWSServiceRoleForCloudTrail和服務連結角色。

當您使用組織的管理帳戶在 CloudTrail 主控台中新增委派管理員或建立組織線索或事件資料存放區，或使用 AWS CLI 或 CloudTrail API 時，如果管理帳戶尚不存在，CloudTrail 會自動建立 AWSServiceRoleForCloudTrail服務連結角色。如需詳細資訊，請參閱使用 CloudTrail 的服務連結角色。

如果您尚未新增委派管理員，請使用 CloudTrail 主控台 AWS CLI 或 CloudTrail API 來新增委派管理員。如需有關新增委派的管理員的詳細資訊，請參閱 新增 CloudTrail 委派的管理員 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。如需有關建立組織追蹤的詳細資訊，請參閱 使用主控台建立組織追蹤、使用 為組織建立線索 AWS CLI 和 CreateTrail (API)。

# 使用 CloudTrail 的服務連結角色

AWS CloudTrail use AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 CloudTrail 的一種特殊 IAM 角色類型。服務連結角色由 CloudTrail 預先定義，並包含服務代表您呼叫其他 AWS 服務所需的所有許可。

主題

- 使用角色在 CloudTrail 中建立和管理 CloudTrail 組織線索和 CloudTrail Lake CloudTrail 組織事件資料存放區
- CloudTrail 服務連結角色的支援區域
- 使用角色在 CloudTrail 中建立和管理 CloudTrail 事件內容
- CloudTrail 服務連結角色的支援區域

## 使用角色在 CloudTrail 中建立和管理 CloudTrail 組織線索和 CloudTrail Lake CloudTrail 組織事件資料存放區

AWS CloudTrail use AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 CloudTrail 的一種特殊 IAM 角色類型。服務連結角色由 CloudTrail 預先定義，並包含服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓設定 CloudTrail 更為簡單，因為您不必手動新增必要的許可。CloudTrail 定義其服務連結角色的許可，除非另有定義，否則僅有 許可 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。這可保護您的 CloudTrail 資源，因為您不會不小心移除存取資源的許可。

如需有關支援服務連結角色的其他 服務的資訊，請參閱AWS 使用 IAM 的服務，並在服務連結角色欄中尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

CloudTrail 的服務連結角色許可

CloudTrail 使用名為 AWSServiceRoleForCloudTrail 的服務連結角色 – 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。

AWSServiceRoleForCloudTrail 服務連結角色信任下列服務擔任該角色：

- `cloudtrail.amazonaws.com`

名為 CloudTrailServiceRolePolicy 的角色許可政策允許 CloudTrail 對指定的資源完成下列動作：

- 所有 CloudTrail 資源上的動作：
  - `All`
- 所有 AWS Organizations 資源的動作：
  - `organizations:DescribeAccount`
  - `organizations:DescribeOrganization`
  - `organizations:ListAccounts`
  - `organizations:ListAWSServiceAccessForOrganization`
- CloudTrail 服務主體的所有 Organizations 資源上的動作，用於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，以允許您的使用者、群組或角色建立、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。

如需 AWSServiceRoleForCloudTrail 相關受管政策的詳細資訊，請參閱 AWS 的 受管政策 AWS CloudTrail。

建立 CloudTrail 的服務連結角色

您不需要手動建立服務連結角色，當您建立組織追蹤或組織事件資料存放區，或在 CloudTrail 主控台、、 AWS CLI或 AWS API AWS 管理主控台中新增委派管理員時，CloudTrail 會為您建立服務連結角色。

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，或在 CloudTrail 主控台中新增委派管理員時，CloudTrail 會再次為您建立服務連結角色。

編輯 CloudTrail 的服務連結角色

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。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

刪除 CloudTrail 的服務連結角色

您不需要手動刪除 AWSServiceRoleForCloudTrail 角色。如果從 Organizations 組織中移除 AWS 帳戶 ，該AWSServiceRoleForCloudTrail角色會自動從該中移除 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**
>
> 若 CloudTrail 服務在您試圖刪除資源時正在使用該角色，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：

- AWS 帳戶 從 Organizations 中的組織移除 。
- 更新追蹤，因此不再是組織追蹤。如需詳細資訊，請參閱使用 CloudTrail 主控台更新線索。
- 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，請參閱使用 CloudTrail 主控台刪除線索。
- 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 AWS CLI、 或 AWS API 來刪除AWSServiceRoleForCloudTrail服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

## CloudTrail 服務連結角色的支援區域

CloudTrail 支援在所有可使用 CloudTrail 和 Organizations AWS 區域 的 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 區域與端點。

## 使用角色在 CloudTrail 中建立和管理 CloudTrail 事件內容

AWS CloudTrail use AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至 CloudTrail 的一種特殊 IAM 角色類型。服務連結角色由 CloudTrail 預先定義，並包含服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓設定 CloudTrail 更為簡單，因為您不必手動新增必要的許可。CloudTrail 定義其服務連結角色的許可，除非另有定義，否則僅有 許可 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除服務連結角色的相關資源，才能將其刪除。這可保護您的 CloudTrail 資源，因為您不會不小心移除存取資源的許可。

如需有關支援服務連結角色的其他 服務的資訊，請參閱AWS 使用 IAM 的服務，並在服務連結角色欄中尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

CloudTrail 的服務連結角色許可

CloudTrail 使用名為 AWSServiceRoleForCloudTrailEventContext 的服務連結角色 – 此服務連結角色用於管理 CloudTrail 事件內容和 EventBridge 規則。

AWSServiceRoleForCloudTrailEventContext 服務連結角色信任下列服務擔任該角色：

- `context.cloudtrail.amazonaws.com`

名為 CloudTrailEventContext 的角色許可政策可讓 CloudTrail 對指定的資源完成下列動作：

- 資源標籤的動作：
  - `tag:GetResources`
- CloudTrail 服務主體在所有 Amazon EventBridge 資源上建立規則的動作：
  - `events:PutRule`
- CloudTrail 服務主體對所有 Amazon EventBridge 資源執行動作，以管理其建立的規則：
  - `events:PutTargets`
  - `events:DeleteRule`
  - `events:RemoveTargets`
  - `events:RemoveTargets`
- CloudTrail 服務主體對所有 Amazon EventBridge 資源執行動作，以描述其建立的規則：
  - `events:DescribeRule`

  - `events:DeRegisterResource`
- 所有 Amazon EventBridge 資源的動作：
  - `events:ListRules`

您必須設定許可，以允許您的使用者、群組或角色建立、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。

如需 AWSServiceRoleForCloudTrailEventContext 相關受管政策的詳細資訊，請參閱 AWS 的 受管政策 AWS CloudTrail。

建立 CloudTrail 的服務連結角色

您不需要手動建立服務連結角色，當您開始使用 AWS 管理主控台、 AWS CLI或 AWS API 中的內容事件功能時，CloudTrail 會為您建立服務連結角色。

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。當您開始使用內容事件功能時，CloudTrail 會再次為您建立服務連結角色。

編輯 CloudTrail 的服務連結角色

CloudTrail 不允許您編輯 AWSServiceRoleForCloudTrailEventContext 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。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

刪除 CloudTrail 的 AWSServiceRoleForCloudTrailEventContext 服務連結角色

如果您不再需要使用需要 AWSServiceRoleForCloudTrailEventContext 服務連結角色的功能或服務，建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。不過，您必須先清除服務連結角色的資源，才能透過從事件資料存放區移除 TagContext 金鑰來手動刪除它。

> **Note**
>
> 如果 CloudTrail 服務在您嘗試刪除資源時使用角色，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。

刪除 CloudTrail 服務連結角色所使用的 CloudTrail 資源 AWSServiceRoleForCloudTrailEventContext

1. 在終端機或命令列，針對您要從中移除`TagContext`金鑰的事件存放區執行 put-event-configuration命令。例如，若要將`TagContext`金鑰從美國東部（俄亥俄）區域中

*111122223333* 帳戶中的事件存放區中移除，且 ARN 為 *arn#aws#cloudtrail#us-east-2#111122223333#eventdatastore/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111*，其中 TagContext是唯一的內容金鑰選取器，您可以使用 put-event-configuration命令，而沒有為 指定值--context-key-selectors：

```
 aws cloudtrail put-event-configuration --event-data-store arn:aws:cloudtrail:us-east-2:111122223333:eventdatastore/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --max-event-size Large --context-key-selectors
```

2. 對分割區中每個區域中的每個資料存放區重複此命令。如需詳細資訊，請參閱使用 Amazon Resource Name (ARNs) 識別 AWS 資源。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台 AWS CLI、 或 AWS API 來刪除 AWSServiceRoleForCloudTrailEventContext 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

### CloudTrail 服務連結角色的支援區域

CloudTrail 支援在所有可使用 CloudTrail 和 EventBridge 的區域中使用服務連結角色。如需詳細資訊，請參閱 AWS Regions and endpoints。

## AWS 的 受管政策 AWS CloudTrail

若要新增許可給使用者、群組和角色，使用 AWS 受管政策比自行撰寫政策更容易。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 受管政策。您無法變更 AWS 受管政策中的許可。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 受管政策中移除許可，因此政策更新不會破壞您現有的許可。

此外， AWS 支援跨多個 服務之任務函數的受管政策。例如，ReadOnlyAccess AWS 受管政策提供所有 AWS 服務和資源的唯讀存取權。當服務啟動新功能時， 會為新操作和資源 AWS 新增唯讀許可。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 受管政策： **AWSCloudTrail_FullAccess**

已將AWSCloudTrail_FullAccess政策連接至其角色的使用者身分，在 CloudTrail 中具有完整的管理存取權。

如需政策詳細資訊的 JSON 清單，請參閱《 AWS 受管政策參考指南AWSCloudTrail_FullAccess》中的 。

## AWS 受管政策： **AWSCloudTrail_ReadOnlyAccess**

如果使用者身分的角色已連接至 AWSCloudTrail_ReadOnlyAccess 政策，使用者可以在 CloudTrail 中執行唯讀操作，例如對線索、CloudTrail Lake 事件資料存放區或 Lake 查詢執行 `Get*`、`List*` 和 `Describe*` 操作。

如需政策詳細資訊的 JSON 清單，請參閱《 AWS 受管政策參考指南AWSCloudTrail_ReadOnlyAccess》中的 。

## AWS 受管政策： **AWSServiceRoleForCloudTrail**

此CloudTrailServiceRolePolicy政策允許 代表您對組織追蹤和組織事件資料存放區 AWS CloudTrail 執行動作。此政策包含描述和列出組織中組織帳戶和委派管理員的必要 AWS Organizations 許可 AWS Organizations 。

此政策還包括在組織事件資料存放區上停用 Lake 聯合的必要 AWS Glue 和 AWS Lake Formation 許可。

此政策會連接到 AWSServiceRoleForCloudTrail 服務連結角色，而此角色可讓 CloudTrail 代表您執行動作。您無法將此政策連接至使用者、群組或角色。

如需政策詳細資訊的 JSON 清單，請參閱《 AWS 受管政策參考指南CloudTrailServiceRolePolicy》中的 。

## AWS 受管政策： **CloudTrailEventContext**

此CloudTrailEventContext政策允許 代表您 AWS CloudTrail 管理 CloudTrail 事件內容和 EventBridge 規則。此政策包含建立、管理和描述其為您建立之規則所需的 EventBridge 許可。

此政策會連接到 AWSServiceRoleForCloudTrailEventContext 服務連結角色，而此角色可讓 CloudTrail 代表您執行動作。您無法將此政策連接至使用者、群組或角色。

如需政策詳細資訊的 JSON 清單，請參閱《 AWS 受管政策參考指南CloudTrailEventContext》中的 。

## AWS 受管政策的 CloudTrail 更新

檢視 CloudTrail AWS 受管政策更新的詳細資訊。如要在此頁面內容有所異動時收到自動提醒，請訂閱 CloudTrail 文件歷史紀錄 頁面的 RSS 摘要。

| 變更 | 描述 | Date |
| --- | --- | --- |
| CloudTrailEventContext – AWSServiceRoleForCloudTrailEventContext 服務連結角色使用的新政策 | 新增了用於 CloudTrail 擴充事件功能的新政策和角色。 | 2025 年 5 月 19 日 |
| 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：<br>• glue:DeleteTable<br>• lakeformation:DeregisterResource | 2023 年 11 月 26 日 |
| AWSCloudTrail_ReadOnlyAccess – 更新現有政策 | CloudTrail 已將 AWSCloudTrailReadOnlyAccess 政策名稱變更為 AWSCloudTrail_ReadOnlyAccess 。此外，政策的許可範圍已縮減至 CloudTrail 操作，它不再包含 Amazon S3 AWS KMS 或 AWS Lambda 動作許可。 | 2022 年 6 月 6 日 |
| CloudTrail 開始記錄異動情形 | CloudTrail 開始追蹤其 AWS 受管政策的變更。 | 2022 年 6 月 6 日 |

# 的合規驗證 AWS CloudTrail

在多個合規計畫 AWS CloudTrail 中，第三方稽核人員會評估 的安全與 AWS 合規。這些計劃包括 SOC、PCI、FedRAMP、HIPAA 等等。

若要了解 AWS 服務 是否在特定合規計劃範圍內，請參閱AWS 服務 合規計劃範圍內然後選擇您感興趣的合規計劃。如需一般資訊，請參閱AWS 合規計劃。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載報告 in AWS Artifact

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。如需使用 時合規責任的詳細資訊 AWS 服務，請參閱 AWS 安全文件。

# 中的彈性 AWS CloudTrail

AWS 全球基礎設施是以 AWS 區域和可用區域為基礎建置。 AWS 區域提供多個實體分隔和隔離的可用區域，這些可用區域以低延遲、高輸送量和高備援聯網連接。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。如果您特別需要以更大的地理距離複寫 CloudTrail 日誌檔案，則可以為線索 Amazon S3 儲存貯體使用跨區域複寫，以啟用在不同 AWS 區域中跨儲存貯體自動、非同步地複製物件。

如需 AWS 區域和可用區域的詳細資訊，請參閱 AWS 全球基礎設施。

除了 AWS 全球基礎設施之外，CloudTrail 還提供數種功能，以協助支援您的資料彈性和備份需求。

記錄所有 AWS 區域中事件的線索和事件資料存放區

當您建立多區域追蹤時，CloudTrail 會在您帳戶中啟用的所有 中建立具有相同組態 AWS 區域 的追蹤。

當您建立多區域事件資料存放區時，CloudTrail 會收集 AWS 區域 您帳戶中所有 中發生的事件。

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，您也可以使用 Amazon S3 提供的功能，協助支援您的資料備援和備份需求。如需詳細資訊，請參閱 Amazon S3 的恢復能力。

# 中的基礎設施安全 AWS CloudTrail

作為受管服務， AWS CloudTrail 受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及 如何 AWS 保護基礎設施的相關資訊，請參閱AWS 雲端安全。若要使用基礎設施安全的最佳實務來設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的基礎設施保護。

您可以使用 AWS 發佈的 API 呼叫，透過網路存取 CloudTrail。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。

以下安全最佳實務也可用來解決 CloudTrail 中的基礎設施安全問題：

- 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政策控制 VPC 端點的存取。
- 識別和稽核所有包含 CloudTrail 日誌檔的 Amazon S3 儲存貯體。考慮使用標籤協助您辨識 CloudTrail 線索和包含 CloudTrail 日誌檔的 Amazon S3 儲存貯體。然後，您可以對 CloudTrail 資源使用資源群組。如需詳細資訊，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代理人問題。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。

我們建議在資源政策中使用 `aws:SourceArn`和 `aws:SourceAccount`全域條件內容索引鍵，以限制將另一個 服務 AWS CloudTrail 提供給資源的許可。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。

下列範例示範如何使用 CloudTrail 中的 `aws:SourceArn` 和 `aws:SourceAccount` 全域條件內容索引鍵，來預防混淆代理人問題：適用於 CloudTrail Lake 查詢結果的 Amazon S3 儲存貯體政策。

# 中的安全最佳實務 AWS CloudTrail

AWS CloudTrail 提供許多安全功能，供您在開發和實作自己的安全政策時考慮。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 偵測性安全最佳實務
- CloudTrail 預防性安全最佳實務


## CloudTrail 偵測性安全最佳實務

建立線索

若要持續記錄 AWS 帳戶中的事件，您必須建立追蹤。雖然 CloudTrail 提供 CloudTrail 主控台 90 天的事件歷史記錄資訊供管理事件且無須建立線索，但這不是永久記錄，而且這不提供所有可能類型事件的資訊。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。

為了協助管理您的 CloudTrail 資料，請考慮建立一個記錄所有管理事件的線索 AWS 區域，然後建立其他線索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。

建立多區域追蹤

若要取得您 AWS 帳戶中 IAM 身分或服務所採取事件的完整記錄，請建立多區域追蹤。多區域追蹤 AWS 區域 會在您的 中啟用的所有 中記錄事件 AWS 帳戶。透過在所有已啟用的 中記錄事件 AWS 區域，您可以確保在 中的所有已啟用區域中擷取活動 AWS 帳戶。這包括記錄全域服務事件，這些事件會記錄到該服務 AWS 區域 特定的 。使用 CloudTrail 主控台建立的所有線索都是多區域線索。

以下是您可進行的一些步驟：

- 為您的 AWS 帳戶建立線索。
- 將現有的單一區域追蹤轉換為多區域追蹤。

- 實作持續的偵測性控制，以協助確保建立的所有線索都 AWS 區域 使用multi-region-cloud-trail-enabled規則記錄所有 中的事件 AWS Config。

### 啟用 CloudTrail 日誌檔案完整性

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。CloudTrail 日誌檔案完整性驗證程序也可讓您知道日誌檔案是否已刪除或變更，或積極宣告在指定的一段期間沒有日誌檔案交付至您的帳戶。CloudTrail 日誌檔案完整性驗證使用產業標準演算法：SHA-256 進行雜湊，而使用含 RSA 的 SHA-256 進行數位簽署。這可透過運算方式防止修改、刪除或偽造 CloudTrail 日誌檔案，而無需偵測。如需詳細資訊，請參閱 啟用驗證並驗證檔案。

### 與 Amazon CloudWatch Logs 整合

CloudWatch Logs 可讓您監控和接收透過 CloudTrail 擷取特定事件的警示。傳送至 CloudWatch Logs 的事件是設定為由追蹤記錄的事件，因此請確定您已設定您的追蹤記錄您有興趣監控的事件類型 （管理事件資料事件和/或網路活動事件）。

例如，您可以監控金鑰安全和網路相關管理事件，例如失敗的 AWS 管理主控台 登入事件。

以下是您可進行的一些步驟：

- 檢閱範例 CloudTrail 的 CloudWatch Logs 整合。
- 設定您的線索到 傳送事件到 CloudWatch Logs。
- 考慮實作持續的偵測性控制，以協助確保所有線索傳送事件到 CloudWatch Logs 以進行監控，方法是使用cloud-trail-cloud-watch-logs-enabled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 會持續監控不同的日誌來源，以識別環境中的潛在安全風險和惡意活動的優先順序。

例如，如果 GuardDuty 透過執行個體啟動角色偵測專門為 Amazon EC2 執行個體建立的登入資料，但正從 中的另一個帳戶使用，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 CSPM

透過使用 AWS Security Hub CSPM 監視您的 CloudTrail 使用狀況，因為它關係到安全最佳實務。Security Hub CSPM 使用偵測性安全控制來評估資源組態和安全標準，以協助您遵守各種合規架構。如需使用 Security Hub CSPM 評估 CloudTrail 資源的詳細資訊，請參閱AWS Security Hub 《使用者指南》中的AWS CloudTrail 控制項。

## CloudTrail 預防性安全最佳實務

以下 CloudTrail 最佳實務有助於預防安全事件的發生。

記錄到專用和集中式的 Amazon S3 儲存貯體

CloudTrail 日誌檔案為 IAM 身分或 AWS 服務所執行動作的稽核日誌。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：

- 建立個別 AWS 帳戶做為日誌封存帳戶。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來記錄組織中所有 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，請建立線索來記錄此日誌封存帳戶中的活動。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。
- 在建立線索時，無論是組織線索還是單一 AWS 帳戶的線索，請建立專用 Amazon S3 儲存貯體來存放此線索的日誌檔案。
- 如果您想要記錄多個 AWS 帳戶的活動，請修改儲存貯體政策，以允許記錄和儲存您要記錄 AWS 帳戶活動之所有 AWS 帳戶的日誌檔案。
- 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。

搭配 AWS KMS 受管金鑰使用伺服器端加密

根據預設，CloudTrail 交付至 S3 儲存貯體的日誌檔案會使用伺服器端加密搭配 KMS 金鑰 (SSE-KMS) 進行加密。若要將 SSE-KMS 搭配 CloudTrail 使用，您可以建立並管理 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測性控制，以協助確保所有線索使用啟用 cloud-trail-encryption-enabled規則來加密 SSE-KMS 的日誌檔案 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，CloudTrail 會在您的 SNS 主題存取政策新增政策聲明，讓 CloudTrail 能夠將內容傳送至 SNS 主題。作為安全最佳實務，我們建議將 `aws:SourceArn`（或選用的 `aws:SourceAccount`) 條件金鑰新增至 Amazon SNS 主題政策陳述式。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 適用於 CloudTrail 索的 Amazon SNS 主題政策。

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 追蹤記錄事件到您指定的 Amazon S3 儲存貯體。這些日誌檔案包含 IAM 身分 AWS 和服務所採取動作的稽核日誌。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。為了協助確保完整性，當您建立或修改存取任何 Amazon S3 儲存貯體用於存放 CloudTrail 日誌檔案時，應該遵循最低權限原則。

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 主控台建立線索，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 適用於 CloudTrail 的 Amazon S3 儲存貯體政策。
- 如果您使用相同的 Amazon S3 儲存貯體存放多個 AWS 帳戶的日誌檔案，請遵循接收多個帳戶日誌檔案的指引。
- 如果您使用組織線索，確保您遵循組織線索，並檢閱 使用 為組織建立線索 AWS CLI 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 線索預設是在 Amazon S3 為線索設定的儲存貯體中無限期存放日誌檔案。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。

限制存取 AWSCloudTrail_FullAccess 政策

具有 AWSCloudTrail_FullAccess 政策的使用者能夠停用或重新設定 AWS 帳戶中最敏感和重要的稽核函數。此政策在您的 AWS 帳戶中不應共用或廣泛套用至 IAM 身分。將此政策的套用限制為盡可能少的個人，也就是您預期作為 AWS 帳戶管理員的人員。

# 使用 AWS KMS 金鑰加密 CloudTrail 日誌檔案、摘要檔案和事件資料存放區 (SSE-KMS)

根據預設，CloudTrail 交付至儲存貯體的日誌檔案和摘要檔案會使用伺服器端加密搭配 KMS 金鑰 (SSE-KMS) 進行加密。如果您未啟用 SSE-KMS 加密，您的日誌檔案和摘要檔案會使用 SSE-S3 加密進行加密。

> **Note**
>
> 如果您使用現有的 S3 儲存貯體搭配 S3 儲存貯體金鑰，則必須在金鑰政策中允許 CloudTrail 使用 AWS KMS 動作 `GenerateDataKey`和 的許可`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 CloudTrail 使用 SSE-KMS，您可以建立和管理 AWS KMS key。您可以將政策連接至金鑰，以決定哪些使用者可以使用金鑰來加密和解密 CloudTrail 日誌檔案和摘要檔案。解密是透過 S3 無縫進行。當金鑰的授權使用者讀取 CloudTrail 日誌檔案或摘要檔案時，S3 會管理解密，授權使用者能夠以未加密的形式讀取檔案。

這種方法具有下列優勢：

- 您可以自行建立和管理 KMS 金鑰。
- 您可以使用單一 KMS 金鑰來加密和解密所有區域中多個帳戶的日誌檔案和摘要檔案。
- 您可以控制誰可以使用您的金鑰來加密和解密 CloudTrail 日誌檔案和摘要檔案。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。使用此功能時，若要讀取日誌檔案或摘要檔案，需要下列許可：
  - 使用者必須擁有包含日誌檔案和摘要檔案之儲存貯體的 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 金鑰之使用者的日誌檔案和摘要檔案，因此檔案的 SSE-KMS 加密與讀取 CloudTrail 日誌資料的應用程式回溯相容。

> **Note**
>
> 您選擇的 KMS 金鑰必須在與接收日誌檔案和摘要檔案的 Amazon S3 儲存貯體相同的 AWS 區域中建立。例如，如果日誌檔案和摘要檔案將存放在美國東部（俄亥俄）區域的儲存貯體

中，您必須建立或選擇在該區域中建立的 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。

根據預設，CloudTrail 會加密事件資料存放區。建立或更新事件資料存放區時，您可以選擇使用自己的 KMS 金鑰進行加密。

## 啟用日誌檔案加密

> **Note**
>
> 如果您在 CloudTrail 主控台中建立 KMS 金鑰，CloudTrail 會為您新增必要的 KMS 金鑰政策區段。如果您在 IAM 主控台或 中建立金鑰， AWS CLI 而且需要手動新增必要的政策區段，請遵循這些程序。

若要啟用 CloudTrail 日誌檔案的 SSE-KMS 加密，請執行下列高階步驟：

1. 建立 KMS 金鑰。
   - 如需有關使用 建立 KMS 金鑰的資訊 AWS 管理主控台，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 金鑰的資訊 AWS CLI，請參閱 create-key。

   > **Note**
   >
   > 您選擇的 KMS 金鑰必須與接收日誌檔案和摘要檔案的 S3 儲存貯體位於相同的區域。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. 將政策區段新增至金鑰，讓 CloudTrail 加密和使用者解密日誌檔案和摘要檔案。
   - 如需政策中所含項目的資訊，請參閱「設定 CloudTrail 的 AWS KMS 金鑰政策」。

   > **Warning**
   >
   > 請務必針對需要讀取日誌檔案或摘要檔案的所有使用者，在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 將政策連接至 KMS 金鑰的資訊 AWS CLI，請參閱 put-key-policy。

3. 更新您的線索或事件資料存放區，以使用您為 CloudTrail 修改的政策的 KMS 金鑰。

   - 若要使用 CloudTrail 主控台更新線索或事件資料存放區，請參閱 更新資源以搭配 主控台使用您的 KMS 金鑰。
   - 若要使用 更新線索或事件資料存放區 AWS CLI，請參閱 使用 啟用和停用 CloudTrail 日誌檔案、摘要檔案和事件資料存放區的加密 AWS CLI。

CloudTrail 也支援 AWS KMS 多區域金鑰。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。

下節說明您 KMS 金鑰政策與 CloudTrail 搭配使用所需的政策區段。

## 授與建立 KMS 金鑰的許可

您可以授予使用者使用 `AWSKeyManagementServicePowerUser`政策建立 AWS KMS key 的許可。

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. 選擇許可索引標籤。
4. 從新增許可清單中，選擇連接政策。
5. 搜尋 AWSKeyManagementServicePowerUser，選擇政策，然後選擇連接政策。

   使用者現在具備建立 KMS 金鑰的許可。如需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 CloudTrail 的 AWS KMS 金鑰政策

您可以透過 AWS KMS key 三種方式建立 ：

- CloudTrail 主控台
- AWS 管理主控台

- 的 AWS CLI

> **Note**
>
> 如果您在 CloudTrail 主控台中建立 KMS 金鑰，CloudTrail 會為您新增必要的 KMS 金鑰政策。您不需要手動新增政策陳述式。請參閱 在 CloudTrail 主控台中建立的預設金鑰政策。

如果您在 AWS 管理主控台 或 中建立 KMS 金鑰 AWS CLI，則必須將政策區段新增至金鑰，才能搭配 CloudTrail 使用。此政策必須允許 CloudTrail 使用 金鑰來加密您的日誌檔案、摘要檔案和事件資料存放區，並允許您指定的使用者以未加密的形式讀取日誌檔案和摘要檔案。

請參閱下列資源：

- 若要使用 建立 KMS 金鑰 AWS CLI，請參閱 create-key。
- 若要編輯 CloudTrail 的 KMS 金鑰政策，請參閱《AWS Key Management Service 開發人員指南》中的編輯金鑰政策。
- 如需 CloudTrail 使用方式的技術詳細資訊 AWS KMS，請參閱 AWS CloudTrail 如何使用 AWS KMS。

主題


- 搭配 CloudTrail 使用的必要的 KMS 金鑰政策區段
- 授予追蹤的加密許可
- 授予事件資料存放區的加密許可
- 授予追蹤的解密許可
- 授予事件資料存放區的解密許可
- 啟用 CloudTrail 以描述 KMS 金鑰屬性
- 在 CloudTrail 主控台中建立的預設金鑰政策


## 搭配 CloudTrail 使用的必要的 KMS 金鑰政策區段

如果您使用 AWS 管理主控台或 建立 KMS 金鑰 AWS CLI，則必須至少將下列陳述式新增至您的 KMS 金鑰政策，才能搭配 CloudTrail 使用。

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. 授予加密 CloudTrail 日誌和摘要檔案的許可。如需詳細資訊，請參閱授予追蹤的加密許可。
2. 授予解密 CloudTrail 日誌和摘要檔案的許可。如需詳細資訊，請參閱授予追蹤的解密許可。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 以描述 KMS 金鑰屬性。如需詳細資訊，請參閱啟用 CloudTrail 以描述 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` 可協助確保 CloudTrail 僅針對特定追蹤使用 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。
> 若追蹤已啟用加密，但 KMS 金鑰已停用或 CloudTrail 的 KMS 金鑰政策設定不正確，則 CloudTrail 不會交付日誌。

適用於事件資料存放區的必要 KMS 金鑰政策

1. 授予加密 CloudTrail Lake 事件資料存放區的許可。如需詳細資訊，請參閱授予事件資料存放區的加密許可。
2. 授予解密 CloudTrail Lake 事件資料存放區的許可。如需詳細資訊，請參閱授予事件資料存放區的解密許可。

   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 金鑰政策必須擁有 CloudTrail 的存取權，而且 KMS 金鑰應由在事件資料存放區上執行操作 (例如查詢) 的使用者來管理。

3. 啟用 CloudTrail 以描述 KMS 金鑰屬性。如需詳細資訊，請參閱[啟用 CloudTrail 以描述 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。
> 若事件資料存放區已啟用加密，但 KMS 金鑰已停用或刪除，或者 CloudTrail 的 KMS 金鑰政策設定不正確，則 CloudTrail 不會將事件傳送到事件資料存放區。

## 授予追蹤的加密許可

Example允許 CloudTrail 代表特定帳戶加密日誌檔案和摘要檔案

CloudTrail 需要明確許可，才能使用 KMS 金鑰來代表特定帳戶加密日誌檔案和摘要檔案。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。您可以將其他帳戶 IDs 新增至 `EncryptionContext`區段，讓這些帳戶能夠使用 CloudTrail 使用您的 KMS 金鑰來加密日誌檔案和摘要檔案。

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` 可協助確保 CloudTrail 僅針對特定追蹤使用 KMS 金鑰。

```
{
   "Sid": "AllowCloudTrailEncryptLogs",
   "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/*"
         }
    }
```

```
}
```

Example

下列範例政策陳述式說明另一個帳戶如何使用 KMS 金鑰來加密 CloudTrail 日誌檔案和摘要檔案。

案例

- 您的 KMS 金鑰在帳戶 *111111111111* 中。
- 您和帳戶 *222222222222* 都要加密日誌。

在該政策中，您要將使用您金鑰加密的一或多個帳戶新增至 CloudTrail EncryptionContext。這會將 CloudTrail 限制為您指定的帳戶使用金鑰來加密日誌檔案和摘要檔案。當您授予帳戶 *222222222222* 的根許可來加密日誌檔案和摘要檔案時，它會將許可委派給帳戶管理員，以加密該帳戶中其他使用者的必要許可。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 全域條件索引鍵 `aws:SourceArn` 可協助確保 CloudTrail 僅針對特定追蹤使用 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": "EnableCloudTrailEncryptPermissions",
  "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 KMS 金鑰政策以搭配 CloudTrail 使用的詳細資訊，請參閱《 AWS Key Management Service 開發人員指南》中的編輯金鑰政策。

### 授予事件資料存放區的加密許可

用於加密 CloudTrail Lake 事件資料存放區的 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": "AllowCloudTrailEncryptEds",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
     },
     "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*"
}
```

### 授予追蹤的解密許可

在您將自己的 KMS 金鑰新增至 CloudTrail 組態之前，請務必將解密許可授予所有需要該許可的使用者。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。

#### 允許 CloudTrail 日誌解密許可

您的金鑰使用者必須擁有明確的許可，才能讀取 CloudTrail 加密的日誌檔案。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": "EnableCloudTrailLogDecryptPermissions",
  "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 服務主體解密追蹤日誌所需的範例政策。

```
{
      "Sid": "AllowCloudTrailDecryptTrail",
      "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。
- 您要授予 IAM 使用者 Bob 解密 S3 儲存貯體中之 CloudTrail 日誌的許可。

在金鑰政策中，您要為 IAM 使用者 Bob 允許 CloudTrail 日誌解密許可。

KMS 金鑰政策聲明：

```
{
  "Sid": "EnableCloudTrailLogDecryptPermissions",
  "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 金鑰來解密追蹤日誌。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。

在此案例中，您要授予在帳戶 *222222222222* 下解密日誌的 CloudTrail 許可，再授予 Alice 的 IAM 使用者政策使用您金鑰 *KeyA* (在帳戶 *111111111111* 中) 的許可。

KMS 金鑰政策聲明：

```
{
  "Sid": "EnableEncryptedCloudTrailLogReadAccess",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::222222222222:root"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:111111111111:key/key-id",
```

```
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

Alice 的 IAM 使用者政策陳述式：

JSON

```
{
  "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。

若要進行此案例，您要為您帳戶中的 IAM 角色 CloudTrailReadRole 允許解密許可，再授予其他帳戶擔任該角色的許可。

KMS 金鑰政策聲明：

```
{
  "Sid": "EnableEncryptedCloudTrailLogReadAccess",
```

```
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111111111111:role/CloudTrailReadRole"
    ]
  },
  "Action": "kms:Decrypt",
  "Resource": "arn:aws:kms:region:account-id:key/key-id",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:cloudtrail:arn": "false"
    }
  }
}
```

CloudTrailReadRole 信任實體政策陳述式：

JSON

```
{
 "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 KMS 金鑰政策以搭配 CloudTrail 使用的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的編輯金鑰政策。

## 授予事件資料存放區的解密許可

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如下內容。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": "EnableUserKeyPermissionsEds"
      "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所需的範例政策。

```
{
      "Sid": "AllowCloudTrailDecryptEds",
      "Effect": "Allow",
      "Principal": {
          "Service": "cloudtrail.amazonaws.com"
        },
      "Action": "kms:Decrypt",
      "Resource": "*"
}
```

## 啟用 CloudTrail 以描述 KMS 金鑰屬性

CloudTrail 需要描述 KMS 金鑰屬性的能力。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。此陳述式不會授予 CloudTrail 您指定之其他許可以外的任何許可。

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` 可協助確保 CloudTrail 僅針對特定追蹤使用 KMS 金鑰。

```
{
  "Sid": "AllowCloudTrailAccess",
  "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 主控台中建立的預設金鑰政策

如果您在 CloudTrail 主控台 AWS KMS key 中建立 ，系統會自動為您建立下列政策。此政策允許這些許可：

- KMS 金鑰的 Allow AWS 帳戶 (root) 許可。
- 允許 CloudTrail 在 KMS 金鑰下加密日誌檔案和摘要檔案，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和摘要檔案。
- 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

- 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 金鑰政策

### 適用於追蹤的預設 KMS 金鑰政策

以下是針對您搭配線索使用的 AWS KMS key 所建立的預設政策。

> **Note**
>
> 此政策包含允許跨帳戶使用 KMS 金鑰解密日誌檔案和摘要檔案的陳述式。

JSON

```
{
    "Version":"2012-10-17",
    "Id": "Key policy created by CloudTrail",
```

```
    "Statement": [
        {
            "Sid": "Enable IAM user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111111111111:root",
                    "arn:aws:iam::111111111111: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:us-
east-1:111111111111:trail/trail-name"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:111111111111: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": "111111111111"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:111111111111:trail/*"
                }
            }
        },
        {
            "Sid": "Enable cross account log decryption",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:Decrypt",
                "kms:ReEncryptFrom"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "111111111111"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:111111111111:trail/*"
                }
            }
        }
    ]
}
```

CloudTrail Lake 事件資料存放區的預設 KMS 金鑰政策

以下是 AWS KMS key 您用於 CloudTrail Lake 中事件資料存放區之 的預設政策。

JSON

```
{
      "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::111111111111:root"
          },
          "Action": "kms:*",
          "Resource": "*"
        },
        {
          "Sid": "Enable user to have permissions",
          "Effect": "Allow",
          "Principal": {
               "AWS" : "arn:aws:sts::111111111111:assumed-role/example-role-name"
        },
          "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
           ],
          "Resource": "*"
```

```
        }
      ]
    }
```

# 更新資源以搭配 主控台使用您的 KMS 金鑰

在 CloudTrail 主控台上，更新追蹤或事件資料存放區以使用 KMS 金鑰。請注意，使用您自己的 KMS 金鑰會產生加密和解密 AWS KMS 的成本。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

若要更新線索以使用您為 CloudTrail 修改 AWS KMS key 的 ，請在 CloudTrail 主控台中完成下列步驟。

> **Note**
>
> 如果您使用帶有S3 儲存貯體金鑰的 S3 儲存貯體，則必須在金鑰政策中允許 CloudTrail 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 更新線索 AWS CLI，請參閱 使用 啟用和停用 CloudTrail 日誌檔案、摘要檔案和事件資料存放區的加密 AWS CLI。

更新追蹤以使用您的 KMS 金鑰

1. 登入 AWS 管理主控台 ，並在 https：//https://console.aws.amazon.com/cloudtrail/ 開啟 CloudTrail 主控台。
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. 對於日誌檔案 SSE-KMS 加密，如果您想要使用 SSE-KMS 加密而非 SSE-S3 加密來加密日誌檔案和摘要檔案，請選擇已啟用。預設為啟用。如果您未啟用 SSE-KMS 加密，您的日誌檔案和摘

要檔案會使用 SSE-S3 加密進行加密。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)。

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**
>
> 您也可以輸入來自另一個帳戶的金鑰 ARN。如需詳細資訊，請參閱更新資源以搭配 主控台使用您的 KMS 金鑰。金鑰政策必須允許 CloudTrail 使用金鑰來加密您的日誌檔案和摘要檔案，並允許您指定的使用者以未加密的形式讀取日誌檔案或摘要檔案。如需手動編輯金鑰政策的資訊，請參閱「設定 CloudTrail 的 AWS KMS 金鑰政策」。

在 AWS KMS Alias (別名) 中，指定您為其變更政策以與 CloudTrail 搭配使用的別名，格式為 `alias/MyAliasName`。如需詳細資訊，請參閱更新資源以搭配 主控台使用您的 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/12345678-1234-1234-1234-123456789`
- 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

若要更新事件資料存放區以使用您為 CloudTrail 修改 AWS KMS key 的 ，請在 CloudTrail 主控台中完成下列步驟。

若要使用 更新事件資料存放區 AWS CLI，請參閱 使用 更新事件資料存放區 AWS CLI。

> **Important**
>
> 停用或刪除 KMS 金鑰，或移除該金鑰的 CloudTrail 許可，會導致 CloudTrail 無法將事件擷取到事件資料存放區，並導致使用者無法查詢使用該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. 登入 AWS 管理主控台 並開啟位於 https：//https://console.aws.amazon.com/cloudtrail/ 的 CloudTrail 主控台。
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，如果尚未啟用，請選擇使用我自己的 AWS KMS key KMS 金鑰來加密事件資料存放區。

   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，指定您變更政策以搭配 CloudTrail 使用的別名，格式為 `alias/MyAliasName`。如需詳細資訊，請參閱更新資源以搭配 主控台使用您的 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/12345678-1234-1234-1234-123456789012`
   - 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。

# 使用 啟用和停用 CloudTrail 日誌檔案、摘要檔案和事件資料存放區的加密 AWS CLI

本主題說明如何使用 啟用和停用 CloudTrail 日誌檔案、摘要檔案和事件資料存放區的 SSE-KMS 加密 AWS CLI。如需背景資訊，請參閱使用 AWS KMS 金鑰加密 CloudTrail 日誌檔案、摘要檔案和事件資料存放區 (SSE-KMS)。

主題


- 使用 啟用 CloudTrail 日誌檔案、摘要檔案和事件資料存放區的加密 AWS CLI
- 使用 停用日誌檔案和摘要檔案的加密 AWS CLI


## 使用 啟用 CloudTrail 日誌檔案、摘要檔案和事件資料存放區的加密 AWS CLI

- 啟用追蹤的日誌檔案和摘要檔案加密
- 啟用事件資料存放區的加密

### 啟用追蹤日誌檔案和摘要檔案的加密

1. 使用 AWS CLI建立金鑰。您建立的金鑰必須位在與收到您 CloudTrail 日誌檔案之 S3 儲存貯體相同的區域中。在此步驟中 AWS KMS create-key，您可以使用 命令。
2. 取得現有金鑰政策，讓您可以將其修改以搭配 CloudTrail 使用。您可以使用 命令擷取金鑰政策 AWS KMS get-key-policy。
3. 將必要的區段新增至金鑰政策，以便 CloudTrail 加密，使用者可以解密您的日誌檔案和摘要檔案。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 CloudTrail 的 AWS KMS 金鑰政策。
4. 使用 命令將修改過的 AWS KMS put-key-policy JSON 政策檔案連接至金鑰。

5. 執行具有 --kms-key-id 參數的 CloudTrail create-trail 或 update-trail 命令。此命令會啟用日誌檔案和摘要檔案的加密。

```
aws cloudtrail update-trail --name Default --kms-key-id alias/MyKmsKey
```

--kms-key-id 參數指定您針對 CloudTrail 修改其政策的金鑰。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": "amzn-s3-demo-bucket"
}
```

KmsKeyId 元素的存在表示已啟用日誌檔案的加密。如果日誌檔案驗證已啟用 （由設定為 true 的 LogFileValidationEnabled元素表示），這也表示已啟用摘要檔案的加密。加密的日誌檔案和摘要檔案應該會在大約 5 分鐘內出現在為追蹤設定的 S3 儲存貯體中。

## 啟用事件資料存放區的加密

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。在此步驟中 AWS KMS create-key，請執行 命令。
2. 取得現有金鑰政策對其進行編輯以搭配 CloudTrail 使用。您可以執行 AWS KMS get-key-policy 命令來取得金鑰政策。

3. 將必要的區段新增至金鑰政策，以便 CloudTrail 加密，使用者可以解密您的事件資料存放區。確定讀取事件資料存放區的所有使用者都獲得解密許可。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 CloudTrail 的 AWS KMS 金鑰政策。
4. 執行 AWS KMS put-key-policy 命令，將編輯的 JSON 政策檔案連接至金鑰。
5. 執行 CloudTrail `create-event-data-store` 或 `update-event-data-store` 命令，並新增 `--kms-key-id` 參數。此命令會啟用事件資料存放區的加密。

```
aws cloudtrail update-event-data-store --name my-event-data-store --kms-key-id
 alias/MyKmsKey
```

`--kms-key-id` 參數指定您針對 CloudTrail 修改其政策的金鑰。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 元素的存在表示事件資料存放區的加密已啟用。

### 使用 停用日誌檔案和摘要檔案的加密 AWS CLI

若要停止加密追蹤的日誌檔案和摘要檔案，請執行並update-trail傳遞空字串至 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": "amzn-s3-demo-bucket"
}
```

缺少 KmsKeyId值表示日誌檔案和摘要檔案的加密不再啟用。

> **Important**
>
> 您無法停止事件資料存放區的加密。

## AWS CloudTrail 如何使用 AWS KMS

本節說明如何 AWS KMS 使用以 SSE-KMS 金鑰加密的 CloudTrail 追蹤。

> **Important**
>
> AWS CloudTrail 和 Amazon S3 僅支援對稱 AWS KMS keys。您無法使用非對稱 KMS 金鑰來加密您的 CloudTrail 日誌。如需判斷 KMS 金鑰是對稱金鑰還是非對稱金鑰的說明，請參閱《AWS Key Management Service 開發人員指南》中的 Identify different key types。

當 CloudTrail 讀取或寫入使用 SSE-KMS 金鑰加密的日誌檔案時，您無需支付金鑰使用費。不過，當您存取使用 SSE-KMS 金鑰加密的 CloudTrail 日誌檔案時，您要支付金鑰使用費。如需 AWS KMS 定價的資訊，請參閱 AWS Key Management Service 定價。如需 CloudTrail 定價的資訊，請參閱 AWS CloudTrail 定價。

## 了解您的 KMS 金鑰何時用於您的線索

在稱為伺服器端加密的 Amazon S3 功能上使用 AWS KMS key (SSE-KMS) AWS KMS 建置來加密 CloudTrail 日誌檔案。若要進一步了解 SSE-KMS，請參閱《Amazon Simple Storage Service 使用者指南》中的使用伺服器端加密與 AWS KMS 金鑰 (SSE-KMS)。

當您設定 AWS CloudTrail 使用 SSE-KMS 加密日誌檔案時，CloudTrail 和 Amazon S3 會在您使用這些服務執行特定動作 AWS KMS keys 時使用 。以下章節說明這些服務使用您的 KMS 金鑰的時機和方法，並提供您可用來驗證此說明的額外資訊。

導致 CloudTrail 和 Amazon S3 使用 KMS 金鑰的動作

- 您可以將 CloudTrail 設定為使用 加密日誌檔案 AWS KMS key
- CloudTrail 將日誌檔案放到您的 S3 儲存貯體
- 您從 S3 儲存貯體取得加密的日誌檔

您可以將 CloudTrail 設定為使用 加密日誌檔案 AWS KMS key

當您更新 CloudTrail 組態以使用 KMS 金鑰時，CloudTrail 會向 傳送GenerateDataKey請求 AWS KMS ，以驗證 KMS 金鑰是否存在，以及 CloudTrail 是否具有使用該金鑰進行加密的許可。CloudTrail 不會使用產生的資料金鑰。

GenerateDataKey 請求包含加密內容的下列資訊：

- CloudTrail 追蹤的 Amazon Resource Name (ARN)
- 交付 CloudTrail 日誌檔案的 S3 儲存貯體 ARN 和路徑

GenerateDataKey 請求會在您的 CloudTrail 日誌中產生類似以下範例的項目。當您看到像這樣的日誌項目時，您可以判斷 CloudTrail AWS KMS GenerateDataKey已針對特定線索呼叫 操作。 已在特定 KMS 金鑰下 AWS KMS 建立資料金鑰。

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
```

```
        "invokedBy": "cloudtrail.amazonaws.com"
    },
    "eventTime": "2024-12-06T20:14:46Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "cloudtrail.amazonaws.com",
    "userAgent": "cloudtrail.amazonaws.com",
    "requestParameters": {
        "keySpec": "AES_256",
        "keyId": "arn:aws:kms:us-east-1:123456789012:key/example1-6736-4661-bf00-
exampleeb770",
        "encryptionContext": {
            "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-east-1:123456789012:trail/
management-events",
            "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-logging-
bucket-123456789012-9af1fb49/AWSLogs/123456789012/CloudTrail/us-
east-1/2024/12/06/123456789012_CloudTrail_us-
east-1_20241206T2010Z_TO50OLMG1hIQ1png.json.gz"
        }
    },
    "responseElements": null,
    "requestID": "a0555e85-7e8a-4765-bd8f-2222295558e1",
    "eventID": "e4f3557e-7dbd-4e37-a00a-d86c137d1111",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:123456789012:key/example1-6736-4661-bf00-
exampleeb770"
         }],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "sharedEventID": "ce71d6be-0846-498e-851f-111a1af9078f",
    "eventCategory": "Management"
}
```


CloudTrail 將日誌檔案放到您的 S3 儲存貯體

每次 CloudTrail 將日誌檔案放入 S3 儲存貯體時，Amazon S3 都會 AWS KMS 代表 CloudTrail 傳送GenerateDataKey請求至 。為了回應此請求， AWS KMS 會產生唯一的資料金鑰，然後傳送兩個

資料金鑰複本給 Amazon S3，一個為純文字，另一個使用指定的 KMS 金鑰加密。Amazon S3 使用純文字資料金鑰來加密 CloudTrail 日誌檔案，然後在使用後盡快從記憶體移除純文字資料金鑰。Amazon S3 會將加密的資料金鑰以中繼資料形式跟加密 CloudTrail 日誌檔案一起存放。

GenerateDataKey 請求包含加密內容的下列資訊：

- CloudTrail 追蹤的 Amazon Resource Name (ARN)
- S3 物件的 ARN (CloudTrail 日誌檔案)

每個 GenerateDataKey 請求會在您的 CloudTrail 日誌中產生類似以下範例的項目。當您看到像這樣的日誌項目時，您可以判斷 CloudTrail 已針對特定線索呼叫 AWS KMS GenerateDataKey 操作，以保護特定日誌檔案。 在指定的 KMS 金鑰下 AWS KMS 建立資料金鑰，在同一日誌項目中顯示兩次。

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "cloudtrail.amazonaws.com"
    },
    "eventTime": "2024-12-06T21:49:28Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "cloudtrail.amazonaws.com",
    "userAgent": "cloudtrail.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-east-1::trail/insights-trail",
            "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-logging-
bucket1-123456789012-7867ab0c/AWSLogs/123456789012/CloudTrail/us-
east-1/2024/12/06/123456789012_CloudTrail_us-
east-1_20241206T2150Z_hVXmrJzjZk2wAM2V.json.gz"
        },
        "keySpec": "AES_256",
        "keyId": "arn:aws:kms:us-east-1:123456789012:key/example9-16ef-48ba-9163-
example67a5a"
    },
    "responseElements": null,
    "requestID": "11117d14-9232-414a-b3d1-01bab4dc9f99",
    "eventID": "999e9a50-512c-4e2a-84a3-111a5f511111",
    "readOnly": true,
    "resources": [
```

```
        {
            "accountId": "123456789012",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:123456789012:key/example9-16ef-48ba-9163-
example67a5a"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "sharedEventID": "5e663acc-b7fd-4cdd-8328-0eff862952fa",
    "eventCategory": "Management"
}
```

您從 S3 儲存貯體取得加密的日誌檔

每次從 S3 儲存貯體取得加密的 CloudTrail 日誌檔案時，Amazon S3 都會 AWS KMS 代表您傳送Decrypt請求至 ，以解密日誌檔案的加密資料金鑰。為了回應此請求， AWS KMS 會使用 KMS 金鑰來解密資料金鑰，然後將純文字資料金鑰傳送至 Amazon S3。Amazon S3 使用純文字資料金鑰來解密 CloudTrail 日誌檔案，然後在使用後盡快從記憶體移除純文字資料金鑰。

Decrypt 請求包含加密內容的下列資訊：

- CloudTrail 追蹤的 Amazon Resource Name (ARN)
- S3 物件的 ARN (CloudTrail 日誌檔案)

每個 Decrypt 請求會在您的 CloudTrail 日誌中產生類似以下範例的項目。當您看到像這樣的日誌項目時，您可以判斷 擔任的角色是否針對特定線索和特定日誌檔案呼叫 AWS KMS Decrypt 操作。 已在特定 KMS 金鑰下 AWS KMS 解密資料金鑰。

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
```

```
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-12-06T22:04:04Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2024-12-06T22:26:34Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "encryptionContext": {
            "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-east-1:123456789012:trail/
insights-trail",
            "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-logging-
bucket1-123456789012-7867ab0c/AWSLogs/123456789012/CloudTrail/us-
east-1/2024/12/06/123456789012_CloudTrail_us-
east-1_20241206T0000Z_aAAsHbGBdye3jp2R.json.gz"
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "1ab2d2d2-111a-2222-a59b-11a2b3832b53",
    "eventID": "af4d4074-2849-4b3d-1a11-a1aaa111a111",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:123456789012:key/example9-16ef-48ba-9163-
example67a5a"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
```

```
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}
```

# 文件歷史紀錄

下表說明 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
-

| 變更 | 描述 | 日期 |
| --- | --- | --- |
| 已新增的功能 | 您現在可以記錄其他 CloudTrail 網路活動事件。如需詳細資訊，請參閱網路活動事件。 | 2025 年 10 月 15 日 |
| 已新增的功能 | 您現在可以記錄 Amazon Bedrock Amazon Elastic Container Service 和 Amazon Quick 的其他 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2025 年 10 月 15 日 |
| 已新增的功能 | 您現在可以記錄其他 CloudTrail 網路活動事件。如需詳細資訊，請參閱網路活動事件。 | 2025 年 9 月 15 日 |
| 已新增的功能 | 您現在可以記錄 Amazon Q Business、Amazon Quick、Amazon SageMaker AI、Amazon Bedrock、Amazon Elastic Compute Cloud 和 Amazon Kinesis Video Streams 的其他 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2025 年 9 月 12 日 |
| 已新增的功能 | 您現在可以記錄 Amazon Aurora DSQL、Amazon Bedrock、Amazon Elastic | 2025 年 7 月 1 日 |

| | | |
|---|---|---|
| | Kubernetes Service、Amazon S3 和 Amazon Keyspaces（適用於 Apache Cassandra) 的其他 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | |
| 已新增的服務支援 | 此版本支援記錄多方核准 API 呼叫。如需詳細資訊，請參閱 CloudTrail 支援的服務和整合。 | 2025 年 6 月 17 日 |
| 已新增的功能 | 記錄 Amazon S3 資料事件`DeleteObject` 操作現在包含呼叫刪除的所有個別物件的相關資訊。您可以選擇篩選掉此額外資訊。如需詳細資訊，請參閱AWS CLI 篩選資料事件的範例。 | 2025 年 6 月 9 日 |
| 已新增的功能 | 您現在可以記錄其他服務的網路活動事件。如需詳細資訊，請參閱網路活動事件。 | 2025 年 5 月 30 日 |
| 新功能 | 您現在可以充實 CloudTrail 管理事件和資料事件，以便在分類、搜尋和分析 CloudTrail 事件時增強結果。如需詳細資訊，請參閱新增資源標籤索引鍵和 IAM 全域條件索引鍵來豐富 CloudTrail 事件。 | 2025 年 5 月 29 日 |

| | | |
|---|---|---|
| 新功能 | 新增AWSServiceRoleForCloudTrailEventContext 服務連結角色的文件和政策資訊。如需詳細資訊，請參閱使用角色在 CloudTrail 中建立和管理 CloudTrail 事件內容。 | 2025 年 5 月 29 日 |
| 已新增的功能 | 您現在可以使用 AWS KMS keys (SSE-KMS) 加密日誌檔案和摘要檔案。如需詳細資訊，請參閱使用 AWS KMS keys (SSE-KMS) 加密 CloudTrail 日誌檔案。 | 2025 年 5 月 22 日 |
| 已新增的功能 | 您現在可以使用其他進階事件選取器和預先定義的範本，將資料事件記錄到您的線索。如需詳細資訊，請參閱資料事件。 | 2025 年 4 月 10 日 |
| 已新增的功能 | 您現在可以記錄 AWS Lambda 和 Amazon Comprehend 的網路活動事件。如需詳細資訊，請參閱網路活動事件。 | 2025 年 4 月 10 日 |
| 已新增的功能 | 您現在可以在 Amazon Simple Email Service 組態集、電子郵件身分和範本上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2025 年 4 月 10 日 |
| 已新增的功能 | AWS CloudTrail 現在支援 VPC 端點政策。如需詳細資訊，請參閱搭配使用 AWS CloudTrail 與 Amazon VPC 端點。 | 2025 年 4 月 9 日 |

| | | |
|---|---|---|
| 已新增的功能 | 您現在可以記錄 的 CloudTrail 網路活動事件 AWS IoT FleetWise。 | 2025 年 4 月 8 日 |
| 已新增的功能 | 您現在可以使用進階事件選取器，在 Amazon Bedrock 工作階段上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2025 年 3 月 19 日 |
| 已更新的文件 | 更新 CloudTrail Lake Insights 事件的 SQL 結構描述。新增主題，以描述追蹤和事件資料存放區的 Insights 事件記錄欄位。如需 CloudTrail Lake Insights 事件支援的 SQL 結構描述的詳細資訊，請參閱 CloudTrail Insights 事件記錄欄位的支援結構描述。 | 2025 年 3 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 GameLift Streams 應用程式和串流群組上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2025 年 3 月 7 日 |
| 已新增的服務支援 | 此版本支援 的受管整合 AWS IoT Device Management。如需詳細資訊，請參閱 AWS 服務 CloudTrail 的主題。 | 2025 年 3 月 3 日 |
| 已新增的功能 | 您現在可以使用進階事件選取器，在以 Amazon Pinpoint 行動裝置為目標的應用程式上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2025 年 2 月 24 日 |

| | | |
|---|---|---|
| 網路活動事件的一般可用性 | 網路活動事件現已正式推出。如需詳細資訊，請參閱記錄網路活動事件。 | 2025 年 2 月 13 日 |
| 已更新的文件 | 新增了解多區域追蹤和選擇加入區域主題，以描述多區域追蹤和選擇加入區域。 | 2025 年 2 月 10 日 |
| 已新增的功能 | 您現在可以使用進階事件選取器，在 Amazon Timestream 區域端點上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2025 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，在 Amazon Bedrock 提示和 AWS Step Functions 活動上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2025 年 1 月 24 日 |
| 已更新的文件 | 新增最佳化 CloudTrail Lake 查詢主題，提供如何最佳化 CloudTrail Lake 查詢以改善效能和可靠性的指引。本主題涵蓋特定最佳化技術，以及常見查詢失敗的解決方法。 | 2025 年 1 月 22 日 |
| 新區域支援 | CloudTrail 將支援擴展到新的 區域：墨西哥（中部）區域。如需詳細資訊，請參閱 CloudTrail 支援區域。 | 2025 年 1 月 13 日 |
| 新區域支援 | CloudTrail 將支援擴展至亞太區域（泰國）區域。如需詳細資訊，請參閱 CloudTrail 支援區域。 | 2025 年 1 月 7 日 |

| | | |
|---|---|---|
| 已新增的功能 | 您現在可以使用進階事件選取器，在 AWS Backup 搜尋任務上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2024 年 12 月 30 日 |
| 已更新的文件 | 將 Logging Insights 事件主題轉換為名為使用 CloudTrail Insights 的章節。本章包含有關 Insights 事件成本和檢視事件資料存放區的 Insights 事件的新章節。 | 2024 年 12 月 23 日 |
| 支援 IPv6 | CloudTrail 新增對 IPv6 的支援。 | 2024 年 12 月 20 日 |
| 已新增的功能 | 您現在可以使用進階事件選取器，在 AWS Signer 簽署任務和設定檔時記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2024 年 12 月 20 日 |
| 已更新的文件 | 更新 CloudTrail 支援的服務和整合區段，以包含 的描述 AWS Config AWS Audit Manager，以及與 CloudTrail Lake 的 Amazon Athena 整合。 | 2024 年 12 月 18 日 |
| 已新增的服務支援 | 此版本支援 AWS Migration Hub 旅程。如需詳細資訊，請參閱使用 AWS 服務 CloudTrail 和記錄旅程 API 呼叫的主題。 AWS Migration HubAWS CloudTrail | 2024 年 12 月 3 日 |

| | | |
|---|---|---|
| 已新增的服務支援 | 此版本支援 Oracle Database@AWS。如需詳細資訊，請參閱 AWS 服務 CloudTrail 和使用 記錄 Oracle Database@API 呼叫的主題。AWSAWS CloudTrail | 2024 年 12 月 1 日 |
| 已新增的服務支援 | 此版本支援 AWS 安全事件回應。如需詳細資訊，請參閱使用 AWS 服務 CloudTrail 和記錄安全事件回應 API 呼叫的主題。 AWSAWS CloudTrail | 2024 年 12 月 1 日 |
| 已新增的功能 | CloudTrail Lake 新增對自訂儀表板、醒目提示儀表板和新受管儀表板的支援。您可以建立自訂儀表板，並為每個自訂儀表板新增最多 10 個小工具。您可以啟用醒目提示儀表板，檢視您帳戶中事件資料存放區所收集的 AWS 活動at-a-glance。如需詳細資訊，請參閱 CloudTrail Lake 儀表板。 | 2024 年 11 月 21 日 |
| 已新增的功能 | CloudTrail Lake 新增對事件資料存放區上資源型政策的支援。您可以使用資源型政策來提供跨帳戶存取權，以允許選取的委託人查詢您的事件資料存放區、列出和取消查詢，以及檢視查詢結果。如需詳細資訊，請參閱事件資料存放區的資源型政策範例。 | 2024 年 11 月 21 日 |

| | | |
|---|---|---|
| 已新增的功能 | 您現在可以使用進階事件選取器，在 AWS AppSync GraphQL APIs 上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2024 年 11 月 19 日 |
| 已新增的功能 | 您現在可以使用進階事件選取器，在 AWS IoT SiteWise 助理對話上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2024 年 11 月 18 日 |
| 已新增的功能 | 您現在可以使用進階事件選取器，在 AWS 最終使用者簡訊簡訊上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2024 年 11 月 15 日 |
| 已新增的功能 | 新增對 `userIdentity` 元素`assumedRoot` 之 `sessionContext` 欄位的支援。如需詳細資訊，請參閱本指南中的 CloudTrail userIdentity 元素，以及《IAM 使用者指南》中的在 CloudTrail 中追蹤特殊權限任務。 | 2024 年 11 月 14 日 |
| CloudTrail Lake 查詢助理的一般可用性 | CloudTrail Lake 查詢助理現已正式推出。查詢助理可讓您從英文的自然語言提示建立 SQL 查詢。如需詳細資訊，請參閱從自然語言提示建立 CloudTrail Lake 查詢。 | 2024 年 11 月 12 日 |

| | | |
|---|---|---|
| 已新增的功能 | 介紹 CloudTrail Lake 查詢的預覽功能，其使用生成式人工智慧 （生成式 AI) 功能來摘要查詢結果。如需詳細資訊，請參閱以自然語言摘要查詢結果。 | 2024 年 11 月 12 日 |
| 已新增的功能 | 您現在可以為 CloudTrail Lake 事件資料存放區設定其他進階事件選取器欄位，讓您更能控制哪些 CloudTrail 事件會擷取到您的事件資料存放區。您可以篩選下列進階事件選取器欄位的管理事件： `eventName` （新）`eventSource`、、 `eventType`（新）`readOnly`、、`sessionCredentialFromConsole`（新）和 `userIdentity.arn` （新）。您可以篩選下列進階事件選取器欄位的資料事件：`eventName`、 `eventSource` （新）、 `eventType` （新）`resources.type`、、`readOnly`、`sessionCredentialFromConsole` （新）和 `resources.ARN` `userIdentity.arn` （新）。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 （步驟 16 和 17)。 | 2024 年 11 月 11 日 |

| | | |
|---|---|---|
| 已更新事件版本 | 已更新`eventVersion` 至 `1.11` 並新增 `userIdentity` 元素`inScopeOf` 的欄位。如需更多詳細資訊，請參閱 CloudTrail userIdentity 元素。 | 2024 年 10 月 29 日 |
| 已新增的服務支援 | 此版本支援 AWS 最終使用者傳訊簡訊。如需詳細資訊，請參閱使用 AWS 服務 CloudTrail 和記錄最終使用者傳訊 SMS API 呼叫的主題。 AWSAWS CloudTrail | 2024 年 10 月 22 日 |
| 已新增的功能 | 您現在可以使用進階事件選取器，在 AWS 最終使用者簡訊簡訊來源身分上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2024 年 10 月 22 日 |
| 已新增的服務支援 | 此版本支援 AWS 最終使用者傳訊社交。如需詳細資訊，請參閱 AWS 服務 CloudTrail 主題和使用 記錄 AWS 最終使用者傳訊社交 API 呼叫 AWS CloudTrail。 | 2024 年 10 月 10 日 |
| 已新增的功能 | 您現在可以使用進階事件選取器，在 AWS 最終使用者傳訊社交電話號碼 IDs 上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2024 年 10 月 10 日 |

| | | |
|---|---|---|
| 已新增的功能 | 您現在可以使用進階事件選取器，在 Amazon Bedrock 模型和 AWS Data Exchange 資產上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2024 年 9 月 27 日 |
| 已新增的功能 | 您現在可以設定追蹤和事件資料存放區，以記錄 CloudTrail 網路活動事件（預覽）。網路活動事件可讓 VPC 端點擁有者記錄使用其 VPC 端點從私有 VPC 到 的 AWS API 呼叫 AWS 服務。此版本支援下列事件來源的網路活動事件記錄：`cloudtrail.amazonaws.com` 、`kms.amazonaws.com` 、 `ec2.amazonaws.com` 和 `secretsmanager.amazonaws.com` 。如需詳細資訊，請參閱記錄網路活動事件。 | 2024 年 9 月 24 日 |
| 已新增的服務支援 | 此版本支援 Directory Service 資料。如需詳細資訊，請參閱使用 AWS 服務 CloudTrail 和記錄資料 API 呼叫的主題。 Directory ServiceAWS CloudTrail | 2024 年 9 月 18 日 |
| 新區域支援 | CloudTrail 將支援擴展到新的區域：亞太區域（馬來西亞）區域。如需詳細資訊，請參閱 CloudTrail 支援區域。 | 2024 年 8 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 CloudWatch RUM 應用程式監視器上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2024 年 7 月 25 日 |
| 已新增的功能 | 您現在可以使用標籤控制對線索的存取。如需詳細資訊，請參閱 ABAC with CloudTrail。 | 2024 年 7 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 One Enterprise 使用者和 UKeys 上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2024 年 7 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 Bedrock 流程別名和護欄上記錄 CloudTrail 資料事件，以及在目錄儲存貯體上記錄 Amazon S3 物件層級 API 活動。如需詳細資訊，請參閱資料事件。 | 2024 年 7 月 9 日 |
| 已新增的功能 | 您現在可以使用進階事件選取器，在 AWS Payment Cryptography 金鑰和別名上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2024 年 7 月 5 日 |
| 已新增的功能 | 介紹 CloudTrail Lake 查詢的預覽功能，該功能使用生成式人工智慧（生成式 AI) 功能，從英文語言提示產生 SQL 查詢。如需詳細資訊，請參閱從英文提示建立 CloudTrail Lake 查詢。 | 2024 年 6 月 11 日 |

| | | |
|---|---|---|
| 已新增的功能 | 您現在可以 AWS 私有 CA 使用進階事件選取器，在 Amazon CloudWatch 指標、Amazon Machine Learning ML 模型上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2024 年 6 月 5 日 |
| 已更新的文件 | 新增章節，說明如何使用進階事件選取器來篩選資料事件。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 Data Streams 串流和串流取用者上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2024 年 5 月 21 日 |
| 已更新的文件 | 更新 CloudTrail Lake 支援的區域頁面，新增亞太區域（海德拉巴）區域 (ap-south-2)、歐洲（蘇黎世）區域 (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 | 新增有關使用 檢視 CloudTrail 成本和用量的章節 AWS Cost Explorer。如需詳細資訊，請參閱使用 檢視 CloudTrail 成本和用量 AWS Cost Explorer。 | 2024 年 5 月 14 日 |
| 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 | 使用者指南章節和頁面標題的一般組織改進，包括以下內容：將 CloudTrail 日誌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。變更設定頁面的標題以設定 CloudTrail 設定。將記錄資料事件、記錄管理事件和記錄 Insights 事件頁面移至了解 CloudTrail 事件區段。將 CloudTrail 日誌檔案範例頁面移至 CloudTrail 日誌檔案區段。新增個別頁面，列出 AWS CLI CloudTrail Lake 事件資料存放區、查詢和整合的命令。 | 2024 年 4 月 10 日 |
| 已更新的文件 | 更新 CloudTrail Lake 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 Control Catalog。如需詳細資訊，請參閱使用 AWS 服務 CloudTrail 和記錄 Control Catalog API 呼叫的主題。 AWSAWS CloudTrail | 2024 年 4 月 8 日 |
| 已新增的服務支援 | 此版本支援 AWS 截止日期雲端。如需詳細資訊，請參閱 AWS 服務 CloudTrail 的主題。 | 2024 年 4 月 2 日 |
| 已更新事件版本 | AWS CloudTrail 事件版本現在為 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，請參閱 AWS 服務 CloudTrail 和使用 記錄 API 呼叫的主題。 AWS Billing ConductorAWS CloudTrail | 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 新增了 `ListInsightsMetricData` API。`ListInsightsMetricData` API 會傳回已啟用 Insights 之線索的 Insights 指標資料。如需詳細資訊，請參閱 AWS CloudTrail API 參考中的 ListInsightsMetricData。 | 2024 年 2 月 6 日 |
| 已新增的功能 | 您現在可以 AWS AppConfig 使用進階事件選取器 AWS IoT AWS IoT SiteWise記錄 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 AWS IoT Greengrass 使用進階事件選取器記錄 的 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 將支援擴展到新的區域：加拿大西部（卡加利）區域。如需詳細資訊，請參閱 CloudTrail 支援區域。 | 2023 年 12 月 20 日 |
| 已新增的功能 | 您現在可以 AWS Supply Chain 使用進階事件選取器記錄 Amazon Keyspaces（適用於 Apache Cassandra）、Amazon RDS 和 AWS IoT TwinMaker的 CloudTrail 資料事件。如需詳細資訊，請參閱資料事件。 | 2023 年 12 月 20 日 |

| | | |
|---|---|---|
| 更新 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 AWS Glue 資料目錄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 Data Catalog 中的資料表中繼資料可讓 Athena 查詢引擎了解如何尋找、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 AWS Cloud Map 使用進階事件選取器記錄 的 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 現在為事件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、AWS CLI 或 UpdateEventDataStore API 作業，將事件資料存放區使用的選項從七年保留定價切換為一年可延長保留定價。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 Lake 中收集 Insights 事件。 AWS CloudTrail Insights 透過持續分析 CloudTrail 管理事件，協助 AWS 使用者識別和回應與 API 呼叫率和 API 錯誤率相關的異常活動。若要在 CloudTrail Lake 中收集 Insights 事件，您需要會記錄管理事件並啟用 Insights 的來源事件資料存放區，以及會依據來源事件資料存放區中的異常管理事件活動收集 Insights 事件的目的地事件資料存放區。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 Insights 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，請參閱 CloudTrail 的AWS 服務 主題和使用 AWS CloudTrail記錄 AWS Launch Wizard API 呼叫。 | 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 CloudTrail 的AWS 服務 主題和使用 AWS CloudTrail記錄 Amazon Bedrock API 呼叫。 | 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 資料庫和資料表上記錄 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 | 新增資料表，以顯示管理帳戶、委派管理員帳戶和 AWS Organizations 組織內的成員帳戶可在 CloudTrail 中執行的任務。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 協議。如需詳細資訊，請參閱 CloudTrail 的AWS 服務 主題和使用 AWS CloudTrail記錄協議 API 呼叫。 | 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 AI 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 Application Transformation Service。AWS Application Transformation Service 是 AWS Microservice Extractor for .NET 等服務使用的一項後端服務。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器，在 AWS 私有 CA Connector for Active Directory 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，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，以及使用 將查詢結果儲存至 Amazon S3 儲存貯體 AWS 管理主控台。如需詳細資訊，請參閱 CloudTrail Lake 的案例 | 2023 年 8 月 16 日 |
| 新區域支援 | CloudTrail 已經將支援擴展到新的區域，亦即以色列 (特拉維夫) 區域。如需詳細資訊，請參閱 CloudTrail 支援區域。 | 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 支援的服務和整合與使用 AWS CloudTrail記錄 AWS HealthImaging API 呼叫。 | 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 資料存放區上記錄 CloudTrail 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 控制頻道和 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 命令確認您的 CloudTrail Lake 已儲存查詢結果。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 支援的服務和整合與使用 AWS CloudTrail記錄 Amazon Verified Permissions API 呼叫。 | 2023 年 6 月 13 日 |
| 已新增的功能 | 您現在可以使用 CloudTrail Lake 儀表板對事件資料存放區內的事件進行視覺化呈現。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 Verified Permissions 政策存放區上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。 | 2023 年 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 | 您現在可以開始與停止 CloudTrail 事件資料存放區上的事件擷取。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 支援的服務和整合與使用 AWS CloudTrail記錄 Amazon Security Lake API 呼叫。 | 2023 年 5 月 30 日 |
| 已更新事件版本 | 現在`eventVersion` 為 1.09。 | 2023 年 5 月 23 日 |
| 已更新的文件 | 更新的 CloudTrail userIdentity 元素主題包含代表 IAM Identity Center 使用者提出請求的範例和欄位描述。如需更多詳細資訊，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 處理程式庫修補程式版本：aws-cloudtrail-processing-library-1.6.1.jar。如需詳細資訊，請參閱 GitHub 上的使用 CloudTrail 處理程式庫和 CloudTrail 處理程式庫。 | 2023 年 5 月 23 日 |
| 已新增的功能 | CloudTrail Lake 現在支援全部 Presto 函數和運算子。如需詳細資訊，請參閱 CloudTrail Lake SQL 限制。 | 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，請參閱記錄資料事件和使用 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 事件資料存放區建立使用者定義的成本分配標籤。 | 2023 年 3 月 24 日 |
| 已新增的服務支援 | 此版本支援 AWS Telco Network Builder (AWS TNB)。如需詳細資訊，請參閱 CloudTrail 支援的服務和整合，以及使用 AWS 記錄 Telco Network Builder API 呼叫 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 | 您現在可以建立 CloudTrail Lake 與 外部事件來源的整合 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，在 CloudTrail Lake 通道上記錄 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 已經將支援擴展到新的區域，亦即亞太區域 (墨爾本) 區域。如需詳細資訊，請參閱 CloudTrail 支援區域。 | 2023 年 1 月 24 日 |
| 已更新的文件 | 已新增有關在 CloudTrail 中管理資料一致性的新章節，請參閱在 CloudTrail 中管理資料一致性。 | 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 AI 功能存放區上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。 | 2022 年 12 月 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 AI 指標實驗試驗元件上記錄 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來包含 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 已經將支援擴展到新的地區，亦即亞太區域 (海德拉巴) 區域。如需詳細資訊，請參閱 CloudTrail 支援區域。 | 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 環境中記錄 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 已經將支援擴展到新的區域，亦即歐洲 (西班牙) 區域。如需詳細資訊，請參閱 CloudTrail 支援區域。 | 2022 年 11 月 16 日 |
| 新區域支援 | CloudTrail 已經將支援擴展到新的區域，亦即歐洲 (蘇黎世) 區域。如需詳細資訊，請參閱 CloudTrail 支援區域。 | 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管理員來管理組織的 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 | 您現在可以啟用 CloudTrail Lake 事件資料存放區的 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 Lake 查詢結果儲存至 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，請參閱將追蹤事件複製到 CloudTrail Lake。 | 2022 年 9 月 19 日 |

| | | |
|---|---|---|
| 已更新的文件 | 已新增適用於 CloudTrail Lake 的支援 Amazon CloudWatch 指標清單。如需詳細資訊，請參閱支援的 CloudWatch 指標。 | 2022 年 9 月 16 日 |
| 已新增的功能 | 您現在可以使用 檢視 CloudTrail 服務連結頻道 AWS CLI。如需詳細資訊，請參閱使用 AWS CLI檢視 CloudTrail 的服務連結通道。 | 2022 年 9 月 9 日 |
| 新區域支援 | CloudTrail 已經將支援擴展到新的區域，亦即中東 (阿拉伯聯合大公國) 區域。如需詳細資訊，請參閱 CloudTrail 支援區域。 | 2022 年 8 月 30 日 |
| 已變更的功能 | CloudTrail 已將受管政策的名稱從 `AWSCloudTrailReadOnlyAccess` 變更為 `AWSCloudTrail_ReadOnlyAccess`。此政策中的許可範圍已有所縮減。根據預設，政策不會再授予列出所有 Amazon S3 AWS KMS 儲存貯體、 AWS Lambda 函數或別名的許可。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，請參閱設定適用於 CloudTrail 的 Amazon S3 儲存貯體政策。 | 2022 年 5 月 11 日 |
| 已變更的功能 | 從 2022 年 2 月 24 日開始， AWS CloudTrail 開始在源自使用代理用戶端的 AWS 管理主控台 工作階段的任何事件中變更 `userAgent` 和 `sourceIPAddress` 欄位值。對於這些事件，CloudTrail 會將 `userAgent` 和 `sourceIPAddress` 欄位的值替換成 `AWS Internal`。CloudTrail 進行了此變更，以標準化它如何記錄所有服務的服務動作資訊 AWS 。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 | 此版本支援 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 | 此版本支援 AWS App Mesh Envoy Management Service。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 | 已將新的查詢範例新增至 CloudTrail Lake，這項新功能可讓您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 | 如果滿足下列兩個條件，CloudTrail 現在會移除資料事件`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，且 API 發起人收到僅適用於發起人帳戶的`AccessDenied` 錯誤。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 處理庫的以下版本：新增了對實作自訂 S3 管理器的支援、用於記錄檔案剖析相關異常的事件日誌記錄、支援剖析 `insightDetails` 中的選用 `errorCode` 欄位，並更新了帳戶 ID 剖析規則運算式以接受非數值。如需詳細資訊，請參閱 GitHub 上的使用 CloudTrail 處理程式庫和 CloudTrail 處理程式庫。 | 2022 年 1 月 28 日 |

| | | |
|---|---|---|
| 已新增的功能 | CloudTrail 引入了 CloudTrail Lake，這項新功能可讓您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 已經將支援擴展到新的區域，亦即亞太區域 (雅加達)。如需詳細資訊，請參閱 CloudTrail 支援區域。 | 2021 年 12 月 13 日 |
| 已新增的服務支援 | 此版本支援 Amazon WorkSpaces Web。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 AWS Glue 資料表上記錄 CloudTrail 資料事件。如需詳細資訊，請參閱記錄資料事件。 | 2021 年 11 月 30 日 |
| 已變更的功能 | 作為安全最佳實務，您現在可以將 `aws:SourceArn` 或 `aws:SourceAccount` 條件金鑰新增至 AWS KMS 金鑰政策和 Amazon S3 儲存貯體政策。如需詳細資訊，請參閱設定 CloudTrail 的 AWS KMS 金鑰政策以及設定 CloudTrail 的 Amazon S3 儲存貯體政策。 | 2021 年 11 月 15 日 |

| | | |
|---|---|---|
| 已新增的服務支援 | 此版本支援 AWS Resilience Hub。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 Insights 事件類型可供使用：錯誤率 Insights 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 Streams 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，CloudTrail 會在您的 SNS 主題存取政策新增政策聲明，讓 CloudTrail 能夠將內容傳送至 SNS 主題。我們建議的安全最佳實務是，新增 `aws:SourceArn` 或 `aws:SourceAccount` 條件金鑰至 CloudTrail 政策聲明。如需詳細資訊，請參閱適用於 CloudTrail 的 Amazon SNS 主題政策。 | 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 | 當 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`) 或`float`。在資料事件欄位中包含整數的事件中，CloudTrail 過去會將這些數字處理為浮點數。現在，CloudTrail 會在資料事件中保留整數的原始格式。如需詳細資訊，請參閱使用 CloudTrail Processing Library。 | 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 | 此版本支援 AWS App Runner。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 Incident Manager。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 | 此更新說明一致性套件的資料事件記錄需求，特別是 HIPAA AWS Config 或 FedRAMP 等合規架構。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 AWS STS 後，當使用者擔任 IAM 角色或使用假定角色執行任何動作時，CloudTrail 會在事件中記錄 `sourceIdentity` 資訊。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 AWS STS 後，當使用者擔任 IAM 角色或使用假定角色執行任何動作時，CloudTrail 會在事件中記錄 `sourceIdentity` 資訊。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 Fault Injection Simulator。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 處理程式庫修補程式版本：在使用者指南中更新 .jar 檔案引用，使用最新版本：aws-cloudtrail-processing-library-1.4.0.jar。如需詳細資訊，請參閱 GitHub 上的使用 CloudTrail 處理程式庫和 CloudTrail 處理程式庫。 | 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 AWS Well-Architected Tool和 Amazon Location Service。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 | 此版本支援 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 |
| 已更新事件版本 | AWS CloudTrail 事件版本現在為 1.08。版本 1.08 為 CloudTrail 引入了新的領域。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 APIs 以登入您的追蹤。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 使用者的自訂許可。 | 2020 年 9 月 29 日 |

| | | |
|---|---|---|
| 已更新的文件 | 此更新支援下列 CloudTrail 處理程式庫修補程式版本：在使用者指南中更新 .jar 檔案引用，使用最新版本：aws-cloudtrail-processing-library-1.3.0.jar。如需詳細資訊，請參閱 GitHub 上的使用 CloudTrail 處理程式庫和 CloudTrail 處理程式庫。 | 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 Insights 引入 CloudTrail Insights 事件的屬性欄位。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 Insights 事件。 | 2020 年 8 月 13 日 |
| 已新增的功能 | AWS CloudTrail 主控台具有全新的外觀，旨在讓您更輕鬆地使用。 AWS CloudTrail 使用者指南已更新，其中包含如何在主控台中執行任務的程序變更，例如建立追蹤、更新追蹤和下載事件歷史記錄。 | 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 | 此版本支援 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 | Encrypt、 Decrypt和等大量 AWS KMS 動作現在GenerateDataKey 會記錄為讀取事件。如果您選擇在線索上記錄所有 AWS KMS 事件，也選擇記錄寫入管理事件，則線索會記錄相關 AWS KMS 動作，例如 Disable、Delete和 ScheduleKey 。 | 2020 年 4 月 7 日 |
| 已新增的服務支援 | 此版本支援 Amazon CodeGuru Reviewer。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 處理程式庫修補程式版本：在使用者指南中更新 .jar 檔案引用，使用最新版本：aws-cloudtrail-processing-library-1.2.0.jar。如需詳細資訊，請參閱 GitHub 上的使用 CloudTrail 處理程式庫和 CloudTrail 處理程式庫。 | 2019 年 11 月 21 日 |

| | | |
|---|---|---|
| 已新增的功能 | 此版本支援 AWS CloudTrail Insights，可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 | 此版本新增從線索篩選 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 | 此版本支援 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 主控台或 API，此版本都會支援在 CloudTrail 中建立追蹤時可新增標籤。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，僅包含目前未在 CloudTrail 中記錄事件 AWS 的服務。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 | 本文件已更新新主題管理 CloudTrail 成本，以協助您記錄所需的 CloudTrail 資料，同時不超出預算。 | 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 | 文件已更新關於 CloudTrail 安全性的相關資訊。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 WorkSpaces Applications。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 | 此版本支援 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 CloudTrail 中建立追蹤，用於記錄 AWS Organizations組織中所有 AWS 帳戶的事件。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 處理程式庫修補程式版本：在使用者指南中更新 .jar 檔案引用，使用最新版本：aws-cloudtrail-processing-library-1.1.3.jar。如需詳細資訊，請參閱 GitHub 上的使用 CloudTrail 處理程式庫和 CloudTrail 處理程式庫。 | 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。請參閱搭配使用 AWS CloudTrail 與介面 VPC 端點。 | 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 Mobile CLI。請參閱 AWS CloudTrail 支援的服務和整合。 | 2018 年 6 月 29 日 |
| AWS CloudTrail 文件歷史記錄通知可透過 RSS 摘要取得 | 您現在可以訂閱 RSS 摘要，接收 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 AWS CloudTrail 日之前的文件發行歷史記錄。

| 變更 | Description | 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 | 此版本支援在事件歷史記錄中記錄所有 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 帳單與成本管理。請參閱 CloudTrail 支援的服務和整合。 | 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 支援的服務和整合。 | 2018 年 6 月 5 日 |
| 已更新的文件 | 此更新支援下列 CloudTrail 處理程式庫修補程式版本：<br>• 在使用者指南中更新 .jar 檔案引用，使用最新版本：aws-cloudtrail-processing-library-1.1.2.jar。<br><br>如需詳細資訊，請參閱 使用 CloudTrail Processing Library 和 GitHub 上的 CloudTrail 處理程式庫。 | 2018 年 5 月 16 日 |

| 變更 | Description | 版本日期 |
| --- | --- | --- |
| 已新增的服務支援 | 此版本支援 AWS 帳單與成本管理。請參閱 CloudTrail 支援的服務和整合。 | 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 支援的服務和整合。 | 2018 年 6 月 5 日 |
| 已更新的文件 | 此更新支援下列 CloudTrail 處理程式庫修補程式版本：<br>• 在使用者指南中更新 .jar 檔案引用，使用最新版本：aws-cloudtrail-processing-library-1.1.2.jar。<br><br>如需詳細資訊，請參閱 使用 CloudTrail Processing Library 和 GitHub 上的 CloudTrail 處理程式庫。 | 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 支援的服務和整合。 | 2018 年 4 月 25 日 |
| 已新增的服務支援 | 此版本支援 AWS IoT Analytics。請參閱 CloudTrail 支援的服務和整合。 | 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 支援的服務和整合。 | 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 支援的服務和整合。 | 2018 年 4 月 6 日 |
| 已新增的服務支援 | 此版本支援 AWS 私有憑證授權機構 (PCA)。請參閱 CloudTrail 支援的服務和整合。 | 2018 年 4 月 4 日 |
| 已新增的功能 | 此版本支援使用 Amazon Athena更輕鬆地搜尋 CloudTrail 日誌檔案。您可以自動建立資料表以直接從 CloudTrail 主控台查詢日誌，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 支援的服務和整合 和 在 CloudTrail 主控台中建立 CloudTrail 日誌的資料表。 | 2018 年 3 月 15 日 |

| 變更 | Description | 版本日期 |
| --- | --- | --- |
| 已新增的服務支援 | 此版本支援 AWS AppSync。請參閱 CloudTrail 支援的服務和整合。 | 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 支援的區域。 | 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 支援的服務和整合。 | 2018 年 2 月 12 日 |
| 已新增的服務支援 | 此版本支援 Amazon SageMaker AI。請參閱 CloudTrail 支援的服務和整合。 | 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 支援的服務和整合。 | 2018 年 1 月 10 日 |
| 已新增的功能 | 此版本支援將 CloudTrail 事件歷史記錄中可用的帳戶活動數量延伸為 90 天。您也可以自訂欄的顯示以改善您 CloudTrail 事件的檢視畫面。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 | 此版本支援 Amazon WorkMail。請參閱 CloudTrail 支援的服務和整合。 | 2017 年 12 月 12 日 |
| 已新增的服務支援 | 此版本支援 Alexa for Business AWS Elemental MediaConvert、 和 AWS Elemental MediaStore。請參閱 CloudTrail 支援的服務和整合。 | 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。<br><br>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。<br><br>如需詳細資訊，請參閱記錄資料事件。 | 2017 年 11 月 30 日 |

| 變更 | Description | 版本日期 |
| --- | --- | --- |
| 新增功能與文件 | 此版本支援下列 CloudTrail 處理程式庫更新：<br>• 新增管理事件之布林值識別的支援。<br>• 將 CloudTrail 事件版本更新為 1.06。<br><br>如需詳細資訊，請參閱 使用 CloudTrail Processing Library 和 GitHub 上的 CloudTrail 處理程式庫。 | 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 支援的服務和整合。 | 2017 年 11 月 7 日 |
| 新增文件 | 此版本會新增主題：中的配額 AWS CloudTrail。 | 2017 年 10 月 19 日 |
| 已更新的文件 | 此版本會更新 Amazon Athena、Amazon AWS CodeBuild Elastic Container Registry 和 的 CloudTrail 事件歷史記錄中支援的 APIs 文件 AWS Migration Hub。 | 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 支援的服務和整合。 | 2017 年 9 月 27 日 |
| 新增功能與文件 | 此版本支援為您 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 支援的服務和整合。 | 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 支援的服務和整合。 | 2017 年 8 月 14 日 |
| 新增功能與文件 | 根據預設，此版本支援針對所有 AWS 帳戶所啟用的 CloudTrail。CloudTrail 事件歷史記錄中會提供過去 7 天的帳戶活動，而且最新事件會出現在主控台儀表板上。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 | Description | 版本日期 |
| --- | --- | --- |
| 新增功能與文件 | 此版本支援從 CloudTrail 主控台的 API 活動歷史記錄頁面下載事件。您可以下載 JSON 或 CSV 格式的事件。<br><br>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。<br><br>如需詳細資訊，請參閱 使用 CloudTrail 日誌檔案。 | 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詢 Amazon CloudWatch Events 的 API。 | 2017 年 6 月 27 日 |
| 新增功能與文件 | 此版本支援下列服務之 CloudTrail API 活動歷史記錄功能中的其他 API：<br><br>• AWS CloudHSM<br>• Amazon Cognito<br>• Amazon DynamoDB<br>• Amazon EC2<br>• Kinesis<br>• 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 支援的服務和整合。 | 2017 年 6 月 14 日 |

| 變更 | Description | 版本日期 |
| --- | --- | --- |
| 新增功能與文件 | 此版本支援下列 CloudTrail 處理程式庫更新：<br>• 新增相同 SQS 佇列中不同 SQS 訊息格式的支援來識別 CloudTrail 日誌檔案。下列是支援的格式：<br>  • CloudTrail 傳送至 SNS 主題的通知<br>  • Amazon S3 傳送至 SNS 主題的通知<br>  • Amazon S3 直接傳送至 SQS 佇列的通知<br>• 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。<br><br>如需詳細資訊，請參閱 使用 CloudTrail Processing Library 和 GitHub 上的 CloudTrail 處理程式庫。 | 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 支援的服務和整合。 | 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 Logs。<br><br>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」。<br><br>如需有關將事件傳送至 CloudWatch Logs 的詳細資訊，請參閱 使用 Amazon CloudWatch Logs 監控 CloudTrail 日誌檔案。 | 2017 年 5 月 9 日 |
| 已新增的服務支援 | 此版本支援 AWS Marketplace 計量服務。請參閱 CloudTrail 支援的服務和整合。 | 2017 年 5 月 2 日 |
| 已新增的服務支援 | 此版本支援 Amazon Quick。請參閱 CloudTrail 支援的服務和整合。 | 2017 年 4 月 28 日 |

| 變更 | Description | 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 使用 CloudTrail 主控台建立追蹤。 | 2017 年 4 月 11 日 |
| 已新增的文件 | 如果 CloudTrail 未將日誌傳遞至 S3 儲存貯體，或傳送您帳戶中部分區域的 SNS 通知，則您可能需要更新政策。<br><br>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」。<br><br>若要進一步了解如何更新 SNS 主題政策，請參閱「CloudTrail 不會傳送區域的通知」。 | 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 支援的服務和整合。 | 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 日誌檔案。 | 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 支援的服務和整合。 | 2017 年 1 月 26 日 |
| 新增功能與文件 | 此版本支援在 CloudTrail APIs 活動歷史記錄中查詢 AWS CodeCommit、Amazon GameLift 伺服器和 AWS Managed Services 的 API。 | 2017 年 1 月 26 日 |

| 變更 | Description | 版本日期 |
| --- | --- | --- |
| 已新增的功能 | 此版本支援與 AWS Health 儀板表整合。<br>您可以使用 Health 儀板表 來識別您的線索是否無法將日誌交付至 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。 會 Health 儀板表 通知您受影響的線索，並建議修正政策的方法。<br><br>如需詳細資訊，請參閱「AWS Health 使用者指南」。 | 2017 年 1 月 24 日 |
| 新增功能與文件 | 此版本支援在 CloudTrail 主控台中依事件來源進行篩選。事件來源顯示提出請求 AWS 的服務。<br><br>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 支援的服務和整合。 | 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 支援的服務和整合。 | 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 支援的服務和整合。 | 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 支援的區域。 | 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 支援的區域。 | 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 支援的服務和整合。<br><br>此版本支援 AWS Health。請參閱 CloudTrail 支援的服務和整合。<br><br>此版本支援 AWS Step Functions。請參閱 CloudTrail 支援的服務和整合。 | 2016 年 12 月 1 日 |

| 變更 | Description | 版本日期 |
| --- | --- | --- |
| 已新增的服務支援 | 此版本支援 Amazon Polly。請參閱 CloudTrail 支援的服務和整合。 | 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 支援的服務和整合。 | 2016 年 11 月 23 日 |
| 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。<br><br>CloudTrail 支援記錄 Amazon S3 物件層級 API 操作，例如 `GetObject` 、`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。<br><br>如需詳細資訊，請參閱 使用 CloudTrail 日誌檔案。 | 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 支援的服務和整合。 | 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 支援的區域。 | 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 支援的資源類型 AWS Config。如需詳細資訊，請參閱檢視使用 參考的資源 AWS Config。 | 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 支援的服務和整合。 | 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 支援的服務和整合。 | 2016 年 6 月 28 日 |

| 變更 | Description | 版本日期 |
| --- | --- | --- |
| 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 支援的區域。 | 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 支援的服務和整合。 | 2016 年 5 月 12 日 |
| 已新增的服務支援 | 此版本支援南美洲 (聖保羅) 區域中的 CloudWatch Logs。如需詳細資訊，請參閱使用 Amazon CloudWatch Logs 監控 CloudTrail 日誌檔案。 | 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 支援的服務和整合。 | 2016 年 4 月 28 日 |
| 已新增的服務支援 | 此版本支援 AWS 支援。請參閱 CloudTrail 支援的服務和整合。 | 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 支援的服務和整合。 | 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 支援的服務和整合。 | 2016 年 4 月 11 日 |
| 新增功能與文件 | 此版本支援使用安全性聲明標記語言 (SAML AWS STS) 和 Web 聯合身分進行的 logging AWS Security Token Service () API 呼叫。如需詳細資訊，請參閱具有 SAML 和 Web 聯合身分 AWS STS APIs 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 支援的服務和整合。 | 2016 年 3 月 25 日 |
| 已新增的服務支援 | 此版本支援 Amazon Data Firehose。請參閱 CloudTrail 支援的服務和整合。 | 2016 年 3 月 17 日 |
| 已新增的服務支援 | 此版本支援 Amazon CloudWatch Logs。請參閱 CloudTrail 支援的服務和整合。 | 2016 年 3 月 10 日 |

| 變更 | Description | 版本日期 |
| --- | --- | --- |
| 已新增的服務支援 | 此版本支援 Amazon Cognito。請參閱 CloudTrail 支援的服務和整合。 | 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 支援的服務和整合。 | 2016 年 2 月 4 日 |
| 已新增的服務支援 | 此版本支援 Amazon GameLift 伺服器 (Amazon GameLift 伺服器 ) 。請參閱 CloudTrail 支援的服務和整合。 | 2016 年 1 月 27 日 |
| 已新增的服務支援 | 此版本支援 Amazon CloudWatch Events。請參閱 CloudTrail 支援的服務和整合。 | 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 支援的區域。 | 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 支援的服務和整合。 | 2015 年 12 月 21 日 |
| 新增功能與文件 | 此版本支援開啟所有區域的 CloudTrail 以及每個區域有多個追蹤的支援。如需詳細資訊，請參閱使用 CloudTrail 追蹤。 | 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 支援的服務和整合。 | 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 日誌檔案、摘要檔案和事件資料存放區 (SSE-KMS)、驗證 CloudTrail 日誌檔案完整性 及 使用 CloudTrail 主控台更新線索。 | 2015 年 10 月 1 日 |
| 已新增的服務支援 | 此版本支援 Amazon OpenSearch Service。請參閱 CloudTrail 支援的服務和整合。 | 2015 年 10 月 1 日 |

| 變更 | Description | 版本日期 |
| --- | --- | --- |
| 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 支援的服務和整合。 | 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 支援的服務和整合。 | 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 支援的服務和整合。 | 2015 年 7 月 9 日 |
| 已新增的服務支援 | 此版本支援 CodePipeline。請參閱 CloudTrail 支援的服務和整合。 | 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 支援的服務和整合。 | 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) 區域中的 CloudWatch Logs。如需 CloudTrail 支援 CloudWatch Logs 監控的詳細資 ，請參閱使用 Amazon CloudWatch Logs 監控 CloudTrail 日誌檔案。 | 2015 年 5 月 19 日 |
| 已新增的服務支援 | 此版本支援 Directory Service。請參閱 CloudTrail 支援的服務和整合。 | 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 支援的服務和整合。 | 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 支援的服務和整合。 | 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 支援的服務和整合。 | 2015 年 4 月 9 日 |
| 已新增的服務支援 | 此版本支援 Amazon WorkSpaces。請參閱 CloudTrail 支援的服務和整合。 | 2015 年 4 月 9 日 |

| 變更 | Description | 版本日期 |
| --- | --- | --- |
| | 此版本支援查詢 CloudTrail 擷取 AWS 的活動 (CloudTrail 事件）。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) 區域中的 Amazon CloudWatch Logs。如需詳細資訊，請參閱傳送事件到 CloudWatch Logs。 | 2015 年 3 月 5 日 |
| 新增文件 | 描述 CloudTrail 對 AWS Security Token Service (AWS STS) 區域端點支援的新區段已新增至 CloudTrail 概念頁面。 | 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 支援的服務和整合。 | 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 支援的服務和整合。 | 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 支援的服務和整合。 | 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 支援的服務和整合。 | 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 支援的服務和整合。 | 2014 年 12 月 16 日 |
| 新增了區域支援 | 此版本支援另一個區域：us-gov-west-1 (AWS GovCloud (US-West))。請參閱 CloudTrail 支援的區域。 | 2014 年 12 月 16 日 |
| 已新增的服務支援 | 此版本支援 Amazon Glacier。請參閱 CloudTrail 支援的服務和整合。 | 2014 年 12 月 11 日 |

| 變更 | Description | 版本日期 |
| --- | --- | --- |
| 已新增的服務支援 | 此版本支援 AWS Data Pipeline。請參閱 CloudTrail 支援的服務和整合。 | 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 支援的服務和整合。 | 2014 年 11 月 12 日 |
| 新增文件 | 「使用 Amazon CloudWatch Logs 監控 CloudTrail 日誌檔案」的新小節已新增至指南》。它說明如何使用 Amazon CloudWatch Logs 來監控 CloudTrail 日誌事件。 | 2014 年 11 月 10 日 |
| 新增文件 | 「使用 CloudTrail Processing Library」的新小節已新增至指南》。它提供如何使用 AWS CloudTrail Processing Library 在 Java 中寫入 CloudTrail 日誌處理器的相關資訊。 | 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 支援的服務和整合。 | 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 支援的區域。 | 2014 年 10 月 23 日 |
| 已新增的服務支援 | 此版本支援 Amazon CloudSearch。請參閱 CloudTrail 支援的服務和整合。 | 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 支援的服務和整合。 | 2014 年 10 月 09 日 |
| 已新增的服務支援 | 此版本支援 Amazon ElastiCache。請參閱 CloudTrail 支援的服務和整合。 | 2014 年 9 月 15 日 |
| 已新增的服務支援 | 此版本支援 Amazon WorkDocs。請參閱 CloudTrail 支援的服務和整合。 | 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 管理主控台 登入事件。 | 2014 年 7 月 24 日 |

| 變更 | Description | 版本日期 |
| --- | --- | --- |
| 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 記錄管理、資料和網路活動事件的內容。 | 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 支援的服務和整合)。 | 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 支援的區域。 | 2014 年 6 月 30 日 |
| 額外的服務支援 | 此版本支援 Amazon Redshift。請參閱 CloudTrail 支援的服務和整合。 | 2014 年 6 月 10 日 |
| 已新增的服務支援 | 此版本支援 OpsWorks。請參閱 CloudTrail 支援的服務和整合。 | 2014 年 6 月 5 日 |
| 已新增的服務支援 | 此版本支援 Amazon CloudFront。請參閱 CloudTrail 支援的服務和整合。 | 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 支援的區域。 | 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 支援的服務和整合。 | 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 日誌檔案。 | 2014 年 5 月 2 日 |
| 已新增的服務支援 | 此版本支援 Amazon CloudWatch。請參閱 CloudTrail 支援的服務和整合。 | 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 支援的服務和整合。 | 2014 年 4 月 22 日 |

| 變更 | Description | 版本日期 |
| --- | --- | --- |
| 已新增的服務支援 | 此版本支援 Direct Connect。請參閱 CloudTrail 支援的服務和整合。 | 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 支援的服務和整合。 | 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 支援的服務和整合。 | 2014 年 4 月 2 日 |
| 額外的服務支援 | 此版本支援 CloudFormation。請參閱 CloudTrail 支援的服務和整合。 | 2014 年 3 月 7 日 |
| 新的指南》 | 此版本推出 AWS CloudTrail。 | 2013 年 11 月 13 日 |

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。