

# AWS CloudTrail

追蹤在 AWS 以及混合雲端和多雲端環境中的使用者活動和 API 使用情形

## 優勢

### 彙總和合併多來源事件

透過 CloudTrail Lake，您可以從 AWS 和 AWS 外部來源擷取活動事件，包括其他雲端供應商、內部應用程式和在雲端或內部部署執行的 SaaS 應用程式。

### 不變地存儲值得稽核的事件

在 AWS CloudTrail Lake 中，您可以不變地儲存值得稽核的事件。輕鬆產生內部政策和外部法規所需的稽核報告。

### 獲取洞察和分析異常活動

現在，您可以更輕鬆地使用 Amazon Athena 或 SQL 型查詢來偵測未經授權的存取及分析活動日誌，這要歸功於自然語言查詢產生 (預覽版)，此工具採用生成式 AI 技術，使用者無須撰寫複雜的 SQL 查詢或 CloudTrail，即可使用。使用規則型 EventBridge 提醒和自動化工作流程進行回應。

## 使用案例

### 合規與稽核

使用 CloudTrail 日誌來證明符合法規 (如 SOC、PCI 和 HIPAA)，從而保護您的組織免受處罰。

### 安全性

透過記錄使用者活動和事件提升安全狀態，並使用 Amazon EventBridge 設定自動化工作流程規則。

### 操作

解答操作問題、加速偵錯，以及使用 SQL 型查詢、自然語言查詢產生 (預覽版)、Amazon Athena，或透過 CloudTrail Lake 中的儀表板將趨勢視覺化，藉以調查速率限制之類的問題。