AWS 决策指南

AWS CloudTrail 或 Amazon CloudWatch？

AWS CloudTrail 或 Amazon CloudWatch？: AWS 決策指南

Table of Contents

AWS CloudTrail 或 Amazon CloudWatch？

了解差異並挑選適合您的差異

用途	為了協助您判斷 AWS CloudTrail 或 Amazon CloudWatch 是維持雲端環境可見性、安全性和營運效率的正確選擇。
上次更新	2024 年 9 月 20 日
涵蓋的服務	• AWS CloudTrail • Amazon CloudWatch

簡介

將關鍵業務工作負載部署到 時 AWS 雲端，請務必在雲端環境中維持可見性、安全性和營運效率。有幾個關鍵領域需要解決：

- 營運透明度 — 追蹤誰在雲端環境中執行作業，並監控資源的效能。
- 安全保證 — 偵測可能表示安全威脅的異常 API 呼叫或資源使用率。
- 合規 — 維護使用者活動和基礎設施變更的詳細日誌，以供稽核之用。
- 效能管理 — 監控資源使用率和應用程式效能指標。
- 事件回應 — 資料和提醒，以快速識別和回應操作問題。
- 成本控制 — 深入了解資源用量，以協助管理雲端支出。
- 自動化 — 自動化對特定事件或效能閾值的回應。

AWS 提供兩種關鍵服務，以協助解決這些問題：

- AWS CloudTrail 主要專注於控管、合規和營運稽核。它會記錄在您 AWS 環境中進行的所有 API 呼叫。主要特色
  - 追蹤所有 AWS 帳戶 活動，包括 API 呼叫、在 AWS 管理主控台、 AWS SDKs、命令列工具和其他 AWS 服務中採取的動作。
  - 提供每個動作的詳細日誌，包括撥打電話的人員、使用的服務，以及受影響的資源。
  - 可用於安全稽核、追蹤使用者活動，以及識別潛在的惡意動作。

- Amazon CloudWatch 是一種監控和可觀測性服務 AWS，可為內部部署和混合式應用程式和基礎設施提供資料和可行的洞見。主要特色包括：
  - AWS 即時監控 AWS 資源和在 上執行的應用程式，包括指標、日誌和警示。
  - 提供系統效能、錯誤率、資源使用率等的詳細洞見。
  - 允許設定警示，根據特定條件觸發動作（例如擴展資源）。

雖然這兩種服務對強大、安全的雲端環境都至關重要，但它們的使用案例和提供的功能有所不同。

以下是這些服務之間主要差異的高階檢視，讓您開始使用。

類別	CloudTrail	CloudWatch
主要用途	API 活動追蹤和稽核	即時監控和效能管理
收集的資料	API 呼叫的日誌，包括撥打電話的人員、時間以及受影響的資源	與資源效能和應用程式行為相關的指標、日誌和事件
使用案例	環境中的安全稽核、合規和追蹤變更	監控資源使用率、設定警示和效能管理
安全與合規	透過提供詳細的活動日誌，協助滿足安全和合規要求	監控系統效能是否有安全性異常，並協助維持操作完整性
日誌保留	事件歷史記錄的最後 90 天。可以建立線索和事件資料存放區（使用 CloudTrail Lake)，以保留活動記錄超過 90 天。	用於即時監控和故障診斷的短期資料保留
警示和通知	不主要用於警示，但可以根據 API 活動觸發動作	透過自動回應，啟用特定指標或日誌事件的設定警示
整合	通常與 AWS Config 和 IAM 等安全服務搭配使用，以增強安全管理	與各種 AWS 服務整合，以實現全方位的監控和自動化
成本考量	根據產生和存放之日誌數量的成本	根據監控指標、日誌和警示數量的成本

類別	CloudTrail	CloudWatch
資料精細程度	提供每個 API 呼叫的詳細日誌，其中包含精細資訊	提供彙總指標和日誌資料以進行即時監控
存取控制	可讓您追蹤存取模式和使用者許可的變更	協助您根據效能指標監控和最佳化對 資源的存取
資源涵蓋範圍	AWS 帳戶全 範圍	個別 AWS 資源
即時追蹤	近乎即時 (5 分鐘內)	即時或近乎即時
視覺效果	有限；經常與其他工具搭配使用	內建儀表板和圖形

CloudTrail 與 CloudWatch 之間的差異

探索 CloudTrail 和 CloudWatch 在許多關鍵領域之間的差異。

Primary purpose

AWS CloudTrail

- 提供 內所有 API 活動的完整稽核線索 AWS 帳戶。專注於記錄執行動作的人員、時間和地點。這包括透過 AWS 管理主控台、 AWS SDKs、命令列工具和其他 AWS 服務採取的動作。CloudTrail 回答以下問題：「誰終止了此 EC2 執行個體？」 或「對此 IAM 政策進行了哪些變更？」

Amazon CloudWatch

- 監控資源和應用程式的運作狀態和效能 AWS 。CloudWatch 會收集和追蹤指標、收集和監控日誌檔案，以及設定警示。它可協助您了解應用程式的效能，並回應整個系統的效能變更。CloudWatch 回答以下問題：「我的 Amazon EC2 執行個體的 CPU 使用率太高嗎？」 或「我的 Lambda 函數會產生多少錯誤？」

摘要

CloudTrail 可協助您追蹤和稽核使用者活動的安全性和合規性，而 CloudWatch 負責監控和最佳化系統效能和運作狀態。這兩種工具在管理雲端環境時提供不同但互補的角色。

Data collected

AWS CloudTrail

- 專注於擷取 AWS 環境中所有 API 活動的詳細日誌。這包括發出 API 呼叫的人員、發出時間、採取的動作，以及涉及的資源等相關資訊。CloudTrail 的日誌提供全面的稽核線索，對於追蹤變更、確保合規性和調查安全事件至關重要。

Amazon CloudWatch

- 從您的 AWS 資源和應用程式收集效能和操作資料。這包括 CPU 用量、記憶體使用率、網路流量和應用程式日誌等指標，以及您可以定義的自訂指標。CloudWatch 收集的資料用於即時監控、效能最佳化和設定警示，以根據特定條件觸發自動化動作。

摘要

CloudTrail 會收集與使用者活動和 API 使用量相關的資料，用於稽核和安全性目的，而 CloudWatch 會收集指標和日誌，以監控、管理和最佳化系統效能和運作狀態。兩者都提供重要的洞見，但提供不同的雲端管理層面。

Use cases

AWS CloudTrail

- 主要用於安全稽核、合規和操作稽核。CloudTrail 提供您 AWS 環境中 API 呼叫和使用者活動的詳細記錄，這對於追蹤變更、調查安全事件以及確保您的組織符合法規要求至關重要。例如，CloudTrail 在您需要監控誰存取特定資源、追蹤對組態所做的變更或跨多個稽核活動的情況下非常有用 AWS 帳戶。

Amazon CloudWatch

- 專為即時監控、效能管理和營運效率而設計。CloudWatch 用於透過收集和追蹤指標、日誌和事件來監控 AWS 資源和應用程式的運作狀態。CloudWatch 可讓您設定觸發自動動作的警示，例如擴展資源，或在達到特定閾值時傳送通知。CloudWatch 的使用案例包括監控應用程式效能、管理資源使用率、偵測異常情況，以及確保系統以最佳方式執行以防止停機。

Security and compliance

AWS CloudTrail

- 在 AWS 環境中維護安全與合規的關鍵。CloudTrail 提供所有 API 呼叫的完整稽核線索，包括誰進行呼叫、何時進行呼叫，以及採取的動作。此詳細記錄對於符合合規標準、執行安全稽核和調查事件至關重要。透過追蹤使用者活動和資源的變更，CloudTrail 有助於確保責任和透明度，這是許多法規架構的關鍵要求。

Amazon CloudWatch

- 透過啟用操作異常的偵測，在安全性中扮演角色。例如，您可以使用 CloudWatch 來監控指出潛在安全問題的指標，例如網路流量或 CPU 用量異常激增。此外，CloudWatch 可以在達到特定閾值時觸發警示和自動回應，允許主動事件管理。CloudWatch 中擷取的日誌也可用於追蹤操作事件，這對於了解安全事件的內容至關重要。

摘要

CloudTrail 共同提供合規所需的稽核日誌，而 CloudWatch 則提供即時監控，協助偵測和回應安全威脅，為安全且合規的雲端環境做出貢獻。

Log retention

AWS CloudTrail

- 根據預設，CloudTrail 事件歷史記錄會記錄您帳戶過去 90 天的管理事件。
- 使用者可以建立追蹤，無限期地將日誌存放在 S3 儲存貯體中。
- 不會自動刪除存放在 Amazon S3 中的日誌，允許長期保留。
- 使用者可以在 S3 儲存貯體上實作生命週期政策，以管理長期儲存成本。
- CloudTrail 可設定為將日誌傳送至 CloudWatch Logs，以取得更靈活的保留選項。

Amazon CloudWatch

- CloudWatch Logs 中的日誌保留更靈活且可設定。
- 預設保留期間因日誌群組而異，通常設定為「永不過期」。
- 使用者可以設定從一天到 10 年的自訂保留期間，或選擇無限期保留。
- 不同的日誌群組可以有不同的保留期間。

- 保留期間過後，日誌會自動刪除以管理儲存成本。
- 如有需要，CloudWatch Logs 可以匯出至 Amazon S3 以進行長期儲存。

Alarms and notifications

AWS CloudTrail

- 主要著重於記錄 API 活動，並且沒有內建警示或通知功能。不過，您可以與 CloudWatch Logs 和 CloudWatch 警示整合，以設定 CloudTrail 事件的警示。此設定通常用於提醒您與安全相關的事件，例如未經授權的存取嘗試或對關鍵資源的變更。

Amazon CloudWatch

- 專為即時監控而設計，並包含強大的警示和通知功能。CloudWatch 可讓您根據指標、日誌資料或自訂定義的閾值來設定警示。違反這些閾值時，CloudWatch 可以透過 Amazon SNS (Amazon Simple Notification Service) 傳送通知、觸發自動動作，例如擴展執行個體，或使用 執行自訂修復步驟 AWS Lambda。這使得 CloudWatch 成為主動系統管理的重要工具，在發生效能問題或操作異常時提醒您。

Integration

CloudTrail 和 CloudWatch 提供與其他 AWS 服務和外部工具的廣泛整合選項，增強其功能和公用程式。

CloudTrail 整合

- Amazon S3：長期儲存日誌以進行封存和分析
- CloudWatch Logs：啟用即時日誌分析和提醒
- Amazon EventBridge：根據 API 事件觸發自動化動作
- AWS Config：提供組態追蹤和合規的輸入
- AWS Security Hub CSPM：有助於集中式安全狀態管理
- AWS Lake Formation：啟用 CloudTrail 日誌的資料湖控管
- Amazon Athena：對存放在 Amazon S3 中的 CloudTrail 日誌執行 SQL 查詢

CloudWatch 整合

- Amazon SNS：傳送警示和事件的通知
- AWS Lambda：根據指標或日誌觸發無伺服器函數
- Amazon EC2 Auto Scaling：根據效能指標調整容量
- AWS Systems Manager：根據 CloudWatch 資料自動化操作任務
- AWS X-Ray：結合追蹤資料以取得深入的應用程式洞見
- 容器服務 (Amazon ECS、Amazon EKS)：監控容器化應用程式
- 第三方工具：將指標和日誌匯出至外部監控平台

Cost considerations

AWS CloudTrail

- CloudTrail 的定價主要取決於記錄和儲存的事件數量。根據預設，CloudTrail 事件歷史記錄會記錄並免費存放您帳戶過去 90 天的管理事件。不過，如果您啟用資料事件 （例如 S3 物件層級動作） 或建立多個線索，則會根據事件量和 Amazon S3 中所需的儲存體產生費用。如果您使用 CloudTrail Insights 等進階功能，可提供異常 API 活動的更深入分析，則可能會產生額外的成本。

Amazon CloudWatch

- 根據幾個因素，CloudWatch 具有更複雜的定價結構，包括您監控的自訂指標數量、擷取和儲存的日誌事件數量，以及警示和儀表板的使用。 AWS 服務的基本監控是免費的，但詳細的監控和自訂指標會產生費用。日誌儲存會根據擷取和保留的資料量來定價，而設定和維護警示或使用 CloudWatch Logs Insights 進行進階日誌分析時，需支付額外費用。

Data granularity

AWS CloudTrail

- CloudTrail 透過記錄您 AWS 環境中所做的每個個別 API 呼叫來提供高精細度。每個日誌項目都包含詳細資訊，例如提出請求的人員、執行的動作、受影響的資源，以及動作的時間。此詳細程度對於稽核、安全性監控和合規至關重要，因為它可讓您追蹤特定使用者動作，並變更為確切的 API 呼叫。

Amazon CloudWatch

- CloudWatch 著重於監控和效能管理的彙總資料。它會定期收集指標（通常是每分鐘或五分鐘），並從 AWS 資源記錄操作資料。雖然 CloudWatch 提供系統效能和應用程式行為的詳細洞見，但其資料比 CloudTrail 更彙總。例如，您可以監控一段時間內的平均 CPU 用量，而不是個別的請求或動作。不過，CloudWatch Logs 可以提供更精細的資料，類似於 CloudTrail，但通常用於分析操作日誌，而不是追蹤 API 呼叫。

Real-time tracking

AWS CloudTrail

- CloudTrail 本身並非針對即時追蹤而設計，但可以設定為提供near-real-time提醒。根據預設，CloudTrail 會記錄 API 活動，但日誌交付會有些微延遲。如需更即時的追蹤，您可以將 CloudTrail 與 Amazon CloudWatch Events 整合 AWS Lambda ，或根據記錄的特定 API 呼叫或活動觸發動作。此設定允許near-real-time地監控關鍵安全事件或組態變更。

Amazon CloudWatch

- 另一方面，CloudWatch 是專為即時追蹤系統和應用程式效能而建置。它會持續監控來自 AWS 資源的指標，並在超過預先定義的閾值時立即觸發警示或通知。CloudWatch 也會即時收集和分析日誌資料，讓您監控應用程式日誌、偵測異常，並在發生操作問題時加以回應。這使得 CloudWatch 成為即時維護 AWS 環境運作狀態和效能的必要工具。

使用

現在您已閱讀 AWS CloudTrail 和 Amazon CloudWatch 之間的選擇條件，您可以選擇符合您需求的服務，並使用以下資訊來協助您開始使用每個服務。

AWS CloudTrail

- 入門 AWS CloudTrail

  AWS CloudTrail 是一種 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。以下是開始使用的方法。

  探索指南
- 檢閱 AWS 帳戶 活動

  了解如何 AWS 帳戶 使用 CloudTrail 的事件歷史記錄功能，在 中檢閱最近的 AWS API 活動。

使用教學課程

- 建立線索

  了解如何建立追蹤記錄所有區域中的 AWS API 活動，包括資料和 Insights 事件。

  使用教學課程

- 中的安全最佳實務 AWS CloudTrail

  本指南提供 AWS CloudTrail 在您的組織中使用 的偵測和預防性安全最佳實務。

  探索指南

Amazon CloudWatch

- Amazon CloudWatch 入門

  使用 Amazon CloudWatch AWS 即時監控您的 AWS 資源和您在 上執行的應用程式。您可以使用 CloudWatch 收集和追蹤指標，這些是您可以為您的資源和應用程式測量的變數。

  探索指南

- Amazon CloudWatch 指標入門

  本指南討論基本監控和詳細監控、如何繪製指標圖形，以及如何使用 CloudWatch 異常偵測。

  探索指南

- 在 Amazon EKS 和 Kubernetes 上設定 Container Insights

  在 EKS 叢集上設定 Amazon CloudWatch 可觀測性 ESK 附加元件和 ADTO，以將指標傳送至 CloudWatch。您也將了解如何設定 Fluent Bit 或 Fluentd 將日誌傳送至 CloudWatch Logs。

  探索指南

- Amazon CloudWatch Application Insights 入門

  了解如何使用 主控台讓 CloudWatch Application Insights 管理您的應用程式以進行監控。

  探索指南

- 使用容器洞見

了解 CloudWatch Container Insights 如何從容器化應用程式和微服務收集、彙總和摘要指標和日誌。

探索指南

- 在 Amazon ECS 上設定 Container Insights

  了解如何設定叢集和服務層級指標、部署 ADOT 以收集 EC2 執行個體層級指標，以及設定 FireLens 將日誌傳送至 CloudWatch Logs。

  探索指南

AWS CloudTrail 或 Amazon CloudWatch 的文件歷史記錄？

下表說明此決策指南的重要變更。如需有關本指南更新的通知，您可以訂閱 RSS 摘要。

變更	描述	日期
初始版本	決策指南的初始版本。	2024 年 9 月 20 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。