AWS Guida decisionale

AWS CloudTrail o Amazon CloudWatch?

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS CloudTrail o Amazon CloudWatch?: AWS Guida decisionale

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e il trade dress di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in qualsiasi modo che possa causare confusione tra i clienti o in qualsiasi modo che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

AWS CloudTrail o Amazon CloudWatch?

Comprendi le differenze e scegli quella più adatta a te

Scopo	Per aiutarti a determinare se AWS CloudTrai l Amazon CloudWatch è la scelta giusta per mantenere la visibilità, la sicurezza e l'efficienza operativa del tuo ambiente cloud.
Ultimo aggiornamento	20 settembre 2024
Servizi coperti	• AWS CloudTrail • Amazon CloudWatch

Introduzione

Quando si distribuiscono carichi di lavoro aziendali critici su Cloud AWS, è essenziale mantenere visibilità, sicurezza ed efficienza operativa nell'ambiente cloud. Esistono diverse aree chiave da affrontare:

- Trasparenza operativa: monitoraggio di chi sta facendo cosa nel tuo ambiente cloud e monitoraggio delle prestazioni delle tue risorse.
- Garanzia di sicurezza: rilevamento di chiamate API insolite o utilizzo di risorse che potrebbero indicare una minaccia alla sicurezza.
- Conformità alle normative: mantenimento di registri dettagliati delle attività degli utenti e delle modifiche all'infrastruttura a fini di controllo.
- Gestione delle prestazioni: monitoraggio dell'utilizzo delle risorse e delle metriche prestazionali delle applicazioni.
- Risposta agli incidenti: dati e avvisi per identificare e rispondere rapidamente ai problemi operativi.
- Controllo dei costi: approfondimenti sull'utilizzo delle risorse per aiutare a gestire la spesa per il cloud.
- Automazione: risposte automatizzate a eventi o soglie di prestazioni specifici.

AWS offre due servizi chiave per aiutare a risolvere questi problemi:

- AWS CloudTrailsi concentra principalmente sulla governance, la conformità e il controllo operativo. Registra tutte le chiamate API effettuate all'interno dell'ambiente AWS . Caratteristiche principali:
  - Tiene traccia di tutte le Account AWS attività, incluse le chiamate API, le azioni intraprese negli strumenti a riga di comando e altri AWS servizi. Console di gestione AWS AWS SDKs
  - Fornisce un registro dettagliato di ogni azione, incluso chi ha effettuato la chiamata, il servizio utilizzato e le risorse interessate.
  - Utile per il controllo della sicurezza, il monitoraggio delle attività degli utenti e l'identificazione di azioni potenzialmente dannose.
- Amazon CloudWatch è un servizio di monitoraggio e osservabilità che fornisce dati e approfondimenti utilizzabili per applicazioni AWS e infrastrutture locali e ibride. Le caratteristiche principali includono:
  - Monitora AWS le risorse e le applicazioni in esecuzione AWS in tempo reale, inclusi parametri, registri e allarmi.
  - Fornisce informazioni dettagliate sulle prestazioni del sistema, sui tassi di errore, sull'utilizzo delle risorse e altro ancora.
  - Consente di impostare allarmi per attivare azioni (ad esempio, il ridimensionamento delle risorse) in base a condizioni specifiche.

Sebbene entrambi i servizi siano fondamentali per un ambiente cloud solido e sicuro, differiscono nei casi d'uso e nelle funzionalità che offrono.

Ecco una panoramica di alto livello delle principali differenze tra questi servizi per iniziare.

Categoria	CloudTrail	CloudWatch
Scopo principale	Monitoraggio e controllo delle attività delle API	Monitoraggio e gestione delle prestazioni in tempo reale
Dati raccolti	Registri delle chiamate API, inclusi chi ha effettuato la chiamata, quando e quali risorse sono state interessate	Metriche, log ed eventi relativi alle prestazioni delle risorse e al comportamento delle applicazioni
Casi d'uso	Controllo della sicurezza, conformità e monitoraggio delle modifiche nell'ambiente	Monitoraggio dell'utilizzo delle risorse, impostazione

Categoria	CloudTrail	CloudWatch
		degli allarmi e gestione delle prestazioni
Conformità e sicurezza	Aiuta a soddisfare i requisiti di sicurezza e conformità fornendo registri dettagliati delle attività	Monitora le prestazioni del sistema per rilevare eventuali anomalie di sicurezza e aiuta a mantenere l'integrità operativa
Retention dei log	Ultimi 90 giorni di cronologi a degli eventi. Può creare percorsi e archivi di dati sugli eventi (utilizzando CloudTrail Lake) per tenere traccia delle attività per più di 90 giorni.	Conservazione dei dati a breve termine per monitorag gio e risoluzione dei problemi in tempo reale
Allarmi e notifiche	Non vengono utilizzati principalmente per gli allarmi, ma possono attivare azioni basate sull'attività delle API	Consente di impostare allarmi per metriche specifiche o eventi di registro, con risposte automatiche
Integrazione	Spesso utilizzato con servizi di sicurezza come AWS Config IAM per una migliore gestione della sicurezza	Si integra con un'ampia gamma di AWS servizi per il monitoraggio e l'automazione completi
Considerazioni sui costi	Costi basati sul volume di log generati e archiviati	Costi basati sul numero di metriche, registri e allarmi monitorati
Granularità dei dati	Fornisce registri dettaglia ti di ogni chiamata API con informazioni granulari	Fornisce metriche aggregate e dati di registro per il monitorag gio in tempo reale

Categoria	CloudTrail	CloudWatch
Controllo degli accessi	Consente di tenere traccia dei modelli di accesso e delle modifiche nelle autorizzazioni degli utenti	Ti aiuta a monitorare e ottimizzare l'accesso alle risorse in base alle metriche delle prestazioni
Copertura delle risorse	Account AWS-ampio	Risorse individuali AWS
Localizzazione in tempo reale	Quasi in tempo reale (entro 5 minuti)	In tempo reale o quasi in tempo reale
Visualizzazione	Limitato; spesso utilizzato con altri strumenti	Dashboard e grafici integrati

Differenze tra e CloudTrail CloudWatch

Esplora le differenze tra CloudTrail e CloudWatch in una serie di aree chiave.

Primary purpose

AWS CloudTrail

- Fornisce un audit trail completo di tutte le attività delle API all'interno di un Account AWS. Si concentra sulla registrazione di chi ha fatto cosa, quando e da dove. Ciò include le azioni eseguite tramite Console di gestione AWS AWS SDKs gli strumenti a riga di comando e altri AWS servizi. CloudTrail risponde a domande come «Chi ha chiuso questa EC2 istanza?» o «Quali modifiche sono state apportate a questa politica IAM?»

Amazon CloudWatch

- Monitora lo stato operativo e le prestazioni di AWS risorse e applicazioni. CloudWatch raccoglie e tiene traccia delle metriche, raccoglie e monitora i file di registro e imposta gli allarmi. Ti aiuta a capire le prestazioni delle tue applicazioni e a rispondere ai cambiamenti delle prestazioni a livello di sistema. CloudWatch risponde a domande come «L'utilizzo della CPU della mia EC2 istanza Amazon è troppo elevato?» o «Quanti errori genera la mia funzione Lambda?»

Riepilogo

CloudTrail aiuta a tracciare e controllare l'attività degli utenti per motivi di sicurezza e conformità, mentre CloudWatch si occupa del monitoraggio e dell'ottimizzazione delle prestazioni del sistema e dello stato operativo. Entrambi gli strumenti svolgono ruoli distinti ma complementari nella gestione di un ambiente cloud.

Data collected

AWS CloudTrail

- Si concentra sull'acquisizione di registri dettagliati di tutte le attività delle API all'interno dell'ambiente. AWS Ciò include informazioni su chi ha effettuato la chiamata API, quando è stata effettuata, sull'azione intrapresa e sulle risorse coinvolte. CloudTrailI log forniscono una pista di controllo completa, essenziale per tenere traccia delle modifiche, garantire la conformità e indagare sugli incidenti di sicurezza.

Amazon CloudWatch

- Raccoglie dati operativi e prestazionali dalle risorse e dalle applicazioni AWS . Ciò include metriche come l'utilizzo della CPU, l'utilizzo della memoria, il traffico di rete e i registri delle applicazioni, oltre a metriche personalizzate che è possibile definire. I dati raccolti da vengono utilizzati per CloudWatch il monitoraggio in tempo reale, l'ottimizzazione delle prestazioni e l'impostazione di allarmi per attivare azioni automatizzate in base a condizioni specifiche.

Riepilogo

CloudTrail raccoglie dati relativi all'attività degli utenti e all'utilizzo delle API per scopi di controllo e sicurezza, mentre CloudWatch raccoglie metriche e registri per monitorare, gestire e ottimizzare le prestazioni del sistema e lo stato operativo. Entrambi forniscono informazioni fondamentali ma servono diversi aspetti della gestione del cloud.

Use cases

AWS CloudTrail

- Utilizzato principalmente per il controllo della sicurezza, la conformità e il controllo operativo. CloudTrailfornisce una registrazione dettagliata delle chiamate API e delle attività degli utenti all'interno dell' AWS ambiente, il che lo rende essenziale per tenere traccia delle modifiche, indagare sugli incidenti di sicurezza e garantire che l'organizzazione soddisfi i requisiti

normativi. Ad esempio, CloudTrail è utile in scenari in cui è necessario monitorare chi ha avuto accesso a risorse specifiche, tenere traccia delle modifiche apportate alle configurazioni o controllare l'attività su più piattaforme. Account AWS

Amazon CloudWatch

- Progettato per il monitoraggio in tempo reale, la gestione delle prestazioni e l'efficienza operativa. CloudWatch viene utilizzato per monitorare lo stato delle AWS risorse e delle applicazioni raccogliendo e tracciando metriche, log ed eventi. CloudWatch consente di impostare allarmi che attivano azioni automatiche, come il ridimensionamento delle risorse o l'invio di notifiche quando vengono raggiunte determinate soglie. I casi d'uso CloudWatch includono il monitoraggio delle prestazioni delle applicazioni, la gestione dell'utilizzo delle risorse, il rilevamento di anomalie e la garanzia che i sistemi funzionino in modo ottimale per prevenire i tempi di inattività.

Security and compliance

AWS CloudTrail

- Fondamentale per mantenere la sicurezza e la conformità negli ambienti. AWS CloudTrail fornisce un audit trail completo di tutte le chiamate API, incluso chi ha effettuato la chiamata, quando è stata effettuata e le azioni intraprese. Questa registrazione dettagliata è essenziale per soddisfare gli standard di conformità, condurre controlli di sicurezza e indagare sugli incidenti. Tracciando l'attività degli utenti e le modifiche alle risorse, CloudTrail aiuta a garantire la responsabilità e la trasparenza, requisiti fondamentali per molti quadri normativi.

Amazon CloudWatch

- Svolge un ruolo nella sicurezza abilitando il rilevamento di anomalie operative. Ad esempio, è possibile utilizzarlo per CloudWatch monitorare le metriche che indicano potenziali problemi di sicurezza, come picchi insoliti nel traffico di rete o nell'utilizzo della CPU. Inoltre, CloudWatch può attivare allarmi e risposte automatiche quando vengono raggiunte determinate soglie, consentendo una gestione proattiva degli incidenti. I log acquisiti CloudWatch possono essere utilizzati anche per tenere traccia degli eventi operativi, il che può essere fondamentale per comprendere il contesto degli incidenti di sicurezza.

Riepilogo

Insieme, CloudTrail fornisce i registri di controllo necessari per la conformità, mentre CloudWatch offre un monitoraggio in tempo reale che aiuta a rilevare e rispondere alle minacce alla sicurezza, contribuendo a un ambiente cloud sicuro e conforme.

Log retention

AWS CloudTrail

- Per impostazione predefinita, la cronologia CloudTrail degli eventi registra gli ultimi 90 giorni di eventi di gestione del tuo account.
- Gli utenti possono creare un percorso per archiviare i log a tempo indeterminato in un bucket S3.
- Non è prevista l'eliminazione automatica dei log archiviati in Amazon S3, il che consente la conservazione a lungo termine.
- Gli utenti possono implementare politiche del ciclo di vita sui bucket S3 per gestire i costi di storage a lungo termine.
- CloudTrail può essere configurato per inviare i log a Logs per opzioni di conservazione CloudWatch più flessibili.

Amazon CloudWatch

- La conservazione dei log in CloudWatch Logs è più flessibile e configurabile.
- Il periodo di conservazione predefinito varia in base al gruppo di log, in genere impostato su «Non scade mai».
- Gli utenti possono impostare periodi di conservazione personalizzati che vanno da un giorno a 10 anni o scegliere una conservazione a tempo indeterminato.
- Gruppi di log diversi possono avere periodi di conservazione diversi.
- Dopo il periodo di conservazione, i log vengono eliminati automaticamente per gestire i costi di archiviazione.
- CloudWatch I log possono essere esportati in Amazon S3 per lo storage a lungo termine, se necessario.

Alarms and notifications

AWS CloudTrail

- Si concentra principalmente sulla registrazione dell'attività delle API e non dispone di funzionalità di allarme o notifica integrate. Tuttavia, è possibile eseguire l'integrazione con CloudWatch Logs and CloudWatch alarms per configurare gli allarmi per gli eventi. CloudTrail Questa configurazione viene in genere utilizzata per avvisare l'utente di eventi relativi alla sicurezza, come tentativi di accesso non autorizzati o modifiche a risorse critiche.

Amazon CloudWatch

- Progettata specificamente per il monitoraggio in tempo reale e include solide funzionalità di allarme e notifica. CloudWatch consente di impostare allarmi in base a metriche, dati di registro o soglie personalizzate. Quando queste soglie vengono superate, CloudWatch puoi inviare notifiche tramite Amazon SNS (Amazon Simple Notification Service), attivare azioni automatizzate come il ridimensionamento delle istanze o eseguire passaggi di riparazione personalizzati utilizzando. AWS Lambda Si tratta di uno strumento CloudWatch essenziale per la gestione proattiva del sistema, che ti avvisa in caso di problemi di prestazioni o anomalie operative non appena si verificano.

Integration

CloudTrail e CloudWatch offrono ampie opzioni di integrazione con altri AWS servizi e strumenti esterni, migliorandone funzionalità e utilità.

CloudTrail integrazioni

- Amazon S3: archivia i log a lungo termine per l'archiviazione e l'analisi
- CloudWatch Registri: abilita l'analisi e gli avvisi dei log in tempo reale
- Amazon EventBridge: attiva azioni automatizzate basate su eventi API
- AWS Config: Fornisci input per il monitoraggio e la conformità della configurazione
- AWS Security Hub CSPM: Contribuisci alla gestione centralizzata del livello di sicurezza
- AWS Lake Formation: Abilita la governance dei log tramite data lake CloudTrail
- Amazon Athena: esegui query SQL sui CloudTrail log archiviati in Amazon S3

CloudWatch integrazioni

- Amazon SNS: invio di notifiche per allarmi ed eventi
- AWS Lambda: Attiva funzioni serverless basate su parametri o log

- Amazon EC2 Auto Scaling: regola la capacità in base ai parametri delle prestazioni
- AWS Systems Manager: Automatizza le attività operative in base ai dati CloudWatch
- AWS X-Ray: Combinalo con i dati di tracciamento per informazioni approfondite sulle applicazioni
- Servizi container (Amazon ECS, Amazon EKS): monitoraggio delle applicazioni containerizzate
- Strumenti di terze parti: esporta parametri e log su piattaforme di monitoraggio esterne

Cost considerations

AWS CloudTrail

- CloudTrail viene calcolato principalmente in base al numero di eventi registrati e archiviati. Per impostazione predefinita, la cronologia degli CloudTrail eventi registra e archivia, gratuitamente, gli ultimi 90 giorni degli eventi di gestione dell'account. Tuttavia, se abiliti gli eventi relativi ai dati (come le azioni a livello di oggetto S3) o crei percorsi multipli, dovrai sostenere addebiti in base al volume degli eventi e allo storage richiesti in Amazon S3. Potrebbero sorgere costi aggiuntivi se utilizzi funzionalità avanzate come CloudTrail Insights, che forniscono un'analisi più approfondita delle attività insolite delle API.

Amazon CloudWatch

- CloudWatch ha una struttura dei prezzi più complessa basata su diversi fattori, tra cui il numero di metriche personalizzate monitorate, il numero di eventi di registro inseriti e archiviati e l'uso di allarmi e dashboard. Il monitoraggio di base dei AWS servizi è gratuito, ma il monitoraggio dettagliato e le metriche personalizzate comportano costi. Il prezzo dello storage dei log si basa sul volume di dati acquisiti e conservati, con costi aggiuntivi per l'impostazione e la manutenzione degli allarmi o l'utilizzo di Logs Insights per l'analisi avanzata dei log. CloudWatch

Data granularity

AWS CloudTrail

- CloudTrail fornisce un'elevata granularità registrando ogni singola chiamata API effettuata all'interno dell'ambiente. AWS Ogni voce di registro include informazioni dettagliate come chi ha effettuato la richiesta, l'azione eseguita, le risorse interessate e l'ora dell'azione. Questo livello di dettaglio è fondamentale per il controllo, il monitoraggio della sicurezza e la conformità, in

quanto consente di tracciare azioni e modifiche specifiche dell'utente fino all'esatta chiamata API.

Amazon CloudWatch

- CloudWatch si concentra sui dati aggregati per il monitoraggio e la gestione delle prestazioni. Raccoglie le metriche a intervalli regolari (in genere ogni minuto o cinque minuti) e registra i dati operativi dalle risorse. AWS Sebbene CloudWatch fornisca informazioni dettagliate sulle prestazioni del sistema e sul comportamento delle applicazioni, i suoi dati sono più aggregati rispetto a. CloudTrail Ad esempio, è possibile monitorare l'utilizzo medio della CPU nel tempo anziché le singole richieste o azioni. CloudWatch I log, tuttavia, possono fornire dati più granulari, simili a, CloudTrail ma vengono spesso utilizzati per analizzare i log operativi anziché tenere traccia delle chiamate API.

Real-time tracking

AWS CloudTrail

- CloudTrail non è intrinsecamente progettato per il tracciamento in tempo reale, ma può essere configurato per fornire avvisi. near-real-time Per impostazione predefinita, CloudTrail registra l'attività delle API, ma c'è un leggero ritardo nella consegna dei log. Per un tracciamento più immediato, puoi AWS Lambda integrarti CloudTrail con Amazon CloudWatch Events o attivare azioni basate su chiamate o attività API specifiche non appena vengono registrate. Questa configurazione consente il near-real-time monitoraggio di eventi di sicurezza critici o modifiche alla configurazione.

Amazon CloudWatch

- CloudWatch, d'altra parte, è progettato per il monitoraggio in tempo reale delle prestazioni del sistema e delle applicazioni. Monitora continuamente le metriche AWS delle risorse e può attivare istantaneamente allarmi o notifiche quando vengono superate le soglie predefinite. CloudWatch raccoglie e analizza inoltre i dati di registro in tempo reale, consentendovi di monitorare i log delle applicazioni, rilevare anomalie e rispondere ai problemi operativi non appena si verificano. Si tratta di uno strumento essenziale per mantenere lo CloudWatch stato e le prestazioni dell'ambiente in tempo reale. AWS

Utilizzo

Ora che hai letto i criteri per scegliere tra Amazon AWS CloudTrail e Amazon CloudWatch, puoi selezionare il servizio che soddisfa le tue esigenze e utilizzare le seguenti informazioni per iniziare a utilizzare ciascuno di essi.

AWS CloudTrail

- Iniziare con AWS CloudTrail

  AWS CloudTrail è un AWS servizio che ti aiuta a consentire il controllo operativo e dei rischi, la governance e la conformità dei tuoi Account AWS. Ecco come iniziare.

  Esplora la guida
- Esamina Account AWS l'attività

  Scopri come rivedere le attività recenti dell' AWS API nella funzione di cronologia degli eventi CloudTrail del tuo Account AWS utilizzo.

  Usa il tutorial
- Creazione di un trail

  Scopri come creare un percorso per registrare l'attività delle AWS API in tutte le regioni, inclusi dati ed eventi Insights.

  Usa il tutorial
- Le migliori pratiche di sicurezza in AWS CloudTrail

  Questa guida fornisce le migliori pratiche di sicurezza investigative e preventive da utilizzare AWS CloudTrail nell'organizzazione.

  Esplora la guida

Amazon CloudWatch

- Guida introduttiva ad Amazon CloudWatch

  Monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale utilizzando Amazon CloudWatch. Puoi utilizzarlo CloudWatch per raccogliere e tenere traccia delle metriche, che sono variabili che puoi misurare per le tue risorse e applicazioni.

Esplora la guida

- Guida introduttiva ad Amazon CloudWatch Metrics

  Questa guida illustra il monitoraggio di base e il monitoraggio dettagliato, come rappresentare graficamente le metriche e come utilizzare CloudWatch il rilevamento delle anomalie.

  Esplora la guida

- Configura Container Insights su Amazon EKS e Kubernetes

  Configura il componente aggiuntivo Amazon CloudWatch Observability ESK e ADTO sul tuo cluster EKS a cui inviare i parametri. CloudWatch Imparerai anche come configurare Fluent Bit o Fluentd per inviare i log ai Logs. CloudWatch

  Esplora la guida

- Guida introduttiva ad Amazon CloudWatch Application Insights

  Scopri come utilizzare la console per consentire ad CloudWatch Application Insights di gestire le tue applicazioni per il monitoraggio.

  Esplora la guida

- Utilizzo di Container Insights

  Scopri come CloudWatch Container Insights raccoglie, aggrega e riepiloga metriche e log delle tue applicazioni e microservizi containerizzati.

  Esplora la guida

- Configurazione di Container Insights su Amazon ECS

  Impara a configurare i parametri dei cluster e dei livelli di servizio, a implementare ADOT per raccogliere parametri a livello di EC2 istanza e a configurare l'invio dei log FireLens ai log. CloudWatch

  Esplora la guida

Cronologia dei documenti per AWS CloudTrail o Amazon CloudWatch?

La tabella seguente descrive le modifiche importanti a questa guida decisionale. Per ricevere notifiche sugli aggiornamenti di questa guida, puoi iscriverti a un feed RSS.

Modifica	Descrizione	Data
Versione iniziale	Versione iniziale della guida decisionale.	20 settembre 2024

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.