AWS Guide de décision

AWS CloudTrail ou Amazon CloudWatch ?

AWS CloudTrail ou Amazon CloudWatch ?: AWS Guide de décision

Table of Contents

AWS CloudTrail ou Amazon CloudWatch ?

Comprenez les différences et choisissez celui qui vous convient

Objectif	Pour vous aider à déterminer si AWS CloudTrail Amazon CloudWatch est le bon choix pour maintenir la visibilité, la sécurité et l'efficacité opérationnelle de votre environnement cloud.
Dernière mise à jour	20 septembre 2024
Services couverts	• AWS CloudTrail • Amazon CloudWatch

Introduction

Lorsque vous déployez des charges de travail professionnelles critiques sur le AWS Cloud, il est essentiel de maintenir la visibilité, la sécurité et l'efficacité opérationnelle dans votre environnement cloud. Il y a un certain nombre de domaines clés à aborder :

- Transparence opérationnelle : suivre qui fait quoi dans votre environnement cloud et surveiller les performances de vos ressources.
- Garantie de sécurité : détection des appels d'API inhabituels ou de l'utilisation des ressources susceptibles d'indiquer une menace pour la sécurité.
- Conformité réglementaire — Tenir à jour des journaux détaillés des activités des utilisateurs et des modifications de l'infrastructure à des fins d'audit.
- Gestion des performances : surveillance de l'utilisation des ressources et des indicateurs de performance des applications.
- Réponse aux incidents : données et alertes permettant d'identifier et de résoudre rapidement les problèmes opérationnels.
- Contrôle des coûts : informations sur l'utilisation des ressources pour aider à gérer les dépenses liées au cloud.
- Automatisation : réponses automatisées à des événements ou à des seuils de performance spécifiques.

AWS propose deux services essentiels pour répondre à ces préoccupations :

- AWS CloudTrailest principalement axé sur la gouvernance, la conformité et l'audit opérationnel. Il enregistre tous les appels d'API effectués dans votre AWS environnement. Fonctions principales :
  - Suit toutes les Compte AWS activités, y compris les appels d'API AWS Management Console AWS SDKs, les actions entreprises dans les outils de ligne de commande et les autres AWS services.
  - Fournit un journal détaillé de chaque action, y compris l'auteur de l'appel, le service utilisé et les ressources affectées.
  - Utile pour l'audit de sécurité, le suivi de l'activité des utilisateurs et l'identification des actions potentiellement malveillantes.
- Amazon CloudWatch est un service de surveillance et d'observabilité qui fournit des données et des informations exploitables pour AWS les applications et infrastructures sur site et hybrides. Les principales fonctionnalités sont les suivantes :
  - Surveille les AWS ressources et les applications exécutées AWS en temps réel, notamment les métriques, les journaux et les alarmes.
  - Fournit des informations détaillées sur les performances du système, les taux d'erreur, l'utilisation des ressources, etc.
  - Permet de configurer des alarmes pour déclencher des actions (par exemple, le dimensionnement des ressources) en fonction de conditions spécifiques.

Bien que les deux services soient essentiels à un environnement cloud robuste et sécurisé, ils diffèrent quant à leurs cas d'utilisation et aux fonctionnalités qu'ils offrent.

Voici un aperçu général des principales différences entre ces services pour vous aider à démarrer.

Catégorie	CloudTrail	CloudWatch
Objectif principal	Suivi et audit de l'activité des API	Surveillance en temps réel et gestion des performances
Données collectées	Journaux des appels d'API, y compris qui a effectué l'appel, quand et quelles ressources ont été affectées	Métriques, journaux et événements liés aux performances des ressources et au comportement des applications

Catégorie	CloudTrail	CloudWatch
Cas d’utilisation	Audit de sécurité, conformité et suivi des modifications de l'environnement	Surveillance de l'utilisation des ressources, définition des alarmes et gestion des performances
Sécurité et conformité	Permet de répondre aux exigences de sécurité et de conformité en fournissant des journaux d'activité détaillés	Surveille les performances du système pour détecter les anomalies de sécurité et contribue à maintenir l'intégrité opérationnelle
Conservation de journal	Historique des événement s des 90 derniers jours. Peut créer des magasins de données sur les sentiers et les événements (à l'aide de CloudTrail Lake) pour conserver un enregistrement de l'activité pendant plus de 90 jours.	Conservation des données à court terme pour une surveilla nce et un dépannage en temps réel
Alarmes et notifications	Non principalement utilisé pour les alarmes, mais peut déclencher des actions en fonction de l'activité de l'API	Permet de définir des alarmes pour des mesures spécifiques ou des événements de journal, avec des réponses automatis ées
Integration	Souvent utilisé avec des services de sécurité tels que AWS Config l'IAM pour une gestion améliorée de la sécurité	S'intègre à une large gamme de AWS services pour une surveillance et une automatis ation complètes
Considérations de coût	Coûts basés sur le volume de journaux générés et stockés	Coûts basés sur le nombre de métriques, de journaux et d'alarmes surveillés

Catégorie	CloudTrail	CloudWatch
Granularité des données	Fournit des journaux détaillés de chaque appel d'API avec des informations détaillées	Fournit des mesures agrégées et des données de journal pour une surveillance en temps réel
Contrôle d’accès	Vous permet de suivre les modèles d'accès et les modifications des autorisations des utilisateurs	Vous aide à surveiller et à optimiser l'accès aux ressources en fonction des indicateurs de performance
Couverture des ressources	Compte AWS-wide	AWS Ressources individuelles
Suivi en temps réel	Quasiment en temps réel (dans les 5 minutes)	En temps réel ou en temps quasi réel
Visualisation	Limité ; souvent utilisé avec d'autres outils	Tableaux de bord et graphique s intégrés

Différences entre CloudTrail et CloudWatch

Explorez les différences entre CloudTrail et CloudWatch dans un certain nombre de domaines clés.

Primary purpose

AWS CloudTrail

- Fournit une piste d'audit complète de toutes les activités des API au sein d'un Compte AWS. Se concentre sur l'enregistrement de qui a fait quoi, quand et d'où. Cela inclut les actions entreprises par le biais AWS Management Console des AWS SDKs outils de ligne de commande et d'autres AWS services. CloudTrail répond à des questions telles que « Qui a résilié cette EC2 instance ? » ou « Quelles modifications ont été apportées à cette politique IAM ? »

Amazon CloudWatch

- Surveille la santé opérationnelle et les performances des AWS ressources et des applications. CloudWatch collecte et suit les métriques, collecte et surveille les fichiers journaux et définit des alarmes. Il vous aide à comprendre les performances de vos applications et à réagir aux changements de performances à l'échelle du système. CloudWatch répond à des questions telles que « L'utilisation du processeur de mon EC2 instance Amazon est-elle trop élevée ? » ou « Combien d'erreurs ma fonction Lambda génère-t-elle ? »

Récapitulatif

CloudTrail vous aide à suivre et à auditer l'activité des utilisateurs pour des raisons de sécurité et de conformité, tout en CloudWatch surveillant et en optimisant les performances du système et la santé opérationnelle. Les deux outils jouent des rôles distincts mais complémentaires dans la gestion d'un environnement cloud.

Data collected

AWS CloudTrail

- Se concentre sur la capture de journaux détaillés de toutes les activités des API au sein de votre AWS environnement. Cela inclut des informations sur la personne qui a effectué l'appel d'API, la date à laquelle il a été effectué, les mesures prises et les ressources impliquées. CloudTrailLes journaux fournissent une piste d'audit complète, essentielle pour suivre les modifications, garantir la conformité et enquêter sur les incidents de sécurité.

Amazon CloudWatch

- Collecte des données opérationnelles et de performance à partir de vos AWS ressources et applications. Cela inclut des mesures telles que l'utilisation du processeur, l'utilisation de la mémoire, le trafic réseau et les journaux des applications, ainsi que des mesures personnalisées que vous pouvez définir. Les données collectées par CloudWatch sont utilisées pour la surveillance en temps réel, l'optimisation des performances et la configuration d'alarmes pour déclencher des actions automatisées en fonction de conditions spécifiques.

Récapitulatif

CloudTrail collecte des données relatives à l'activité des utilisateurs et à l'utilisation des API à des fins d'audit et de sécurité, tout en CloudWatch collectant des métriques et des journaux pour surveiller, gérer et optimiser les performances du système et la santé opérationnelle. Les deux

fournissent des informations essentielles mais répondent à différents aspects de la gestion du cloud.

Use cases

AWS CloudTrail

- Principalement utilisé pour l'audit de sécurité, la conformité et l'audit opérationnel. CloudTrailfournit un enregistrement détaillé des appels d'API et de l'activité des utilisateurs au sein de votre AWS environnement, ce qui le rend essentiel pour suivre les modifications, enquêter sur les incidents de sécurité et garantir que votre organisation respecte les exigences réglementaires. Par exemple, CloudTrail il est utile dans les scénarios où vous devez surveiller qui a accédé à des ressources spécifiques, suivre les modifications apportées aux configurations ou auditer les activités sur plusieurs sites Comptes AWS.

Amazon CloudWatch

- Conçu pour la surveillance en temps réel, la gestion des performances et l'efficacité opérationnelle. CloudWatch est utilisé pour surveiller l'état de vos AWS ressources et de vos applications en collectant et en suivant les métriques, les journaux et les événements. CloudWatch vous permet de définir des alarmes qui déclenchent des actions automatisées, telles que le dimensionnement des ressources ou l'envoi de notifications lorsque certains seuils sont atteints. Les cas d'utilisation CloudWatch incluent la surveillance des performances des applications, la gestion de l'utilisation des ressources, la détection des anomalies et la garantie du fonctionnement optimal de vos systèmes afin d'éviter les temps d'arrêt.

Security and compliance

AWS CloudTrail

- Essentiel pour le maintien de la sécurité et de la conformité dans AWS les environnements. CloudTrail fournit une piste d'audit complète de tous les appels d'API, y compris l'auteur de l'appel, le moment où il a été effectué et les actions entreprises. Cette journalisation détaillée est essentielle pour respecter les normes de conformité, effectuer des audits de sécurité et enquêter sur les incidents. En suivant l'activité des utilisateurs et les modifications apportées aux ressources, il CloudTrail contribue à garantir la responsabilité et la transparence, qui sont des exigences essentielles pour de nombreux cadres réglementaires.

Amazon CloudWatch

- Joue un rôle dans la sécurité en permettant la détection des anomalies opérationnelles. Par exemple, vous pouvez l'utiliser CloudWatch pour surveiller les mesures qui indiquent des problèmes de sécurité potentiels, tels que des pics inhabituels de trafic réseau ou d'utilisation du processeur. En outre, il CloudWatch peut déclencher des alarmes et des réponses automatisées lorsque certains seuils sont atteints, ce qui permet une gestion proactive des incidents. Les journaux capturés CloudWatch peuvent également être utilisés pour suivre les événements opérationnels, ce qui peut être essentiel pour comprendre le contexte des incidents de sécurité.

Récapitulatif

Ensemble, ils CloudTrail fournissent les journaux d'audit nécessaires à la conformité, tout en CloudWatch offrant une surveillance en temps réel qui aide à détecter les menaces de sécurité et à y répondre, contribuant ainsi à un environnement cloud sécurisé et conforme.

Log retention

AWS CloudTrail

- Par défaut, l'historique des CloudTrail événements enregistre les 90 derniers jours d'événements de gestion de votre compte.
- Les utilisateurs peuvent créer une trace pour stocker les journaux indéfiniment dans un compartiment S3.
- Il n'y a pas de suppression automatique des journaux stockés dans Amazon S3, ce qui permet de les conserver à long terme.
- Les utilisateurs peuvent mettre en œuvre des politiques de cycle de vie sur les compartiments S3 afin de gérer les coûts de stockage à long terme.
- CloudTrail peut être configuré pour envoyer des CloudWatch journaux à Logs pour des options de conservation plus flexibles.

Amazon CloudWatch

- La conservation des CloudWatch journaux dans Logs est plus flexible et plus configurable.
- La période de conservation par défaut varie en fonction du groupe de journaux, généralement définie sur « Ne jamais expirer ».

- Les utilisateurs peuvent définir des périodes de conservation personnalisées allant d'un jour à 10 ans, ou choisir une conservation indéfinie.
- Les différents groupes de journaux peuvent avoir des durées de conservation différentes.
- Après la période de conservation, les journaux sont automatiquement supprimés pour gérer les coûts de stockage.
- CloudWatch Les journaux peuvent être exportés vers Amazon S3 pour un stockage à long terme si nécessaire.

Alarms and notifications

AWS CloudTrail

- Se concentre principalement sur la journalisation de l'activité de l'API et ne dispose pas de fonctionnalités d'alarme ou de notification intégrées. Cependant, vous pouvez intégrer les CloudWatch journaux et les CloudWatch alarmes pour configurer les alarmes en fonction CloudTrail des événements. Cette configuration est généralement utilisée pour vous avertir d'événements liés à la sécurité, tels que des tentatives d'accès non autorisées ou des modifications apportées à des ressources critiques.

Amazon CloudWatch

- Spécialement conçu pour la surveillance en temps réel et comprend des fonctionnalités d'alarme et de notification robustes. CloudWatch vous permet de définir des alarmes en fonction de métriques, de données de journal ou de seuils personnalisés. Lorsque ces seuils sont dépassés, CloudWatch vous pouvez envoyer des notifications via Amazon SNS (Amazon Simple Notification Service), déclencher des actions automatisées telles que le dimensionnement des instances ou effectuer des étapes de correction personnalisées à l'aide de. AWS Lambda Cela en fait CloudWatch un outil essentiel pour une gestion proactive du système, en vous alertant en cas de problèmes de performance ou d'anomalies opérationnelles au fur et à mesure qu'ils surviennent.

Integration

CloudTrail et CloudWatch offrent des options d'intégration étendues avec d'autres AWS services et outils externes, améliorant ainsi leurs fonctionnalités et leur utilité.

CloudTrail intégrations

- Amazon S3 : stockez les journaux à long terme à des fins d'archivage et d'analyse
- CloudWatch Journaux : activez l'analyse des journaux et les alertes en temps réel
- Amazon EventBridge : déclenchez des actions automatisées en fonction des événements de l'API
- AWS Config: Fournir des informations pour le suivi de la configuration et la conformité
- AWS Security Hub CSPM: Contribuer à la gestion centralisée de la posture de sécurité
- AWS Lake Formation: Activez la gouvernance des CloudTrail journaux dans les lacs de données
- Amazon Athena : exécuter des requêtes SQL sur les CloudTrail journaux stockés dans Amazon S3

CloudWatch intégrations

- Amazon SNS : envoi de notifications en cas d'alarmes et d'événements
- AWS Lambda: Déclenchez des fonctions sans serveur en fonction de métriques ou de journaux
- Amazon EC2 Auto Scaling : ajustez la capacité en fonction des indicateurs de performance
- AWS Systems Manager: Automatisez les tâches opérationnelles en fonction CloudWatch des données
- AWS X-Ray: Combinez avec les données de trace pour obtenir des informations détaillées sur les applications
- Services de conteneurs (Amazon ECS, Amazon EKS) : surveillez les applications conteneurisées
- Outils tiers : exportez les métriques et les journaux vers des plateformes de surveillance externes

Cost considerations

AWS CloudTrail

- CloudTrail est calculé principalement en fonction du nombre d'événements enregistrés et enregistrés. Par défaut, l'historique des CloudTrail événements enregistre et stocke, sans frais, les événements de gestion de votre compte au cours des 90 derniers jours. Toutefois, si vous activez des événements de données (tels que des actions au niveau des objets S3) ou si vous créez plusieurs pistes, des frais vous seront facturés en fonction du volume d'événements et du

stockage requis dans Amazon S3. Des coûts supplémentaires peuvent survenir si vous utilisez des fonctionnalités avancées telles que CloudTrail Insights, qui fournissent une analyse plus approfondie des activités inhabituelles des API.

Amazon CloudWatch

- CloudWatch possède une structure tarifaire plus complexe basée sur plusieurs facteurs, notamment le nombre de mesures personnalisées que vous surveillez, le nombre d'événements de journal ingérés et stockés, ainsi que l'utilisation d'alarmes et de tableaux de bord. La surveillance de base des AWS services est gratuite, mais la surveillance détaillée et les mesures personnalisées entraînent des frais. Le stockage des journaux est facturé en fonction du volume de données ingérées et conservées, avec des coûts supplémentaires liés à la configuration et à la gestion des alarmes ou à l'utilisation de CloudWatch Logs Insights pour une analyse avancée des journaux.

Data granularity

AWS CloudTrail

- CloudTrail fournit une granularité élevée en enregistrant chaque appel d'API individuel effectué dans votre AWS environnement. Chaque entrée de journal inclut des informations détaillées telles que l'auteur de la demande, l'action effectuée, les ressources concernées et l'heure de l'action. Ce niveau de détail est crucial pour l'audit, la surveillance de la sécurité et la conformité, car il vous permet de suivre les actions et les modifications spécifiques des utilisateurs jusqu'à l'appel d'API exact.

Amazon CloudWatch

- CloudWatch met l'accent sur les données agrégées pour le suivi et la gestion des performances. Il collecte des métriques à intervalles réguliers (généralement toutes les minutes ou toutes les cinq minutes) et enregistre les données opérationnelles provenant AWS des ressources. Tout en CloudWatch fournissant des informations détaillées sur les performances du système et le comportement des applications, ses données sont plus agrégées que CloudTrail. Par exemple, vous pouvez surveiller l'utilisation moyenne du processeur au fil du temps plutôt que des demandes ou des actions individuelles. CloudWatch Les journaux peuvent toutefois fournir des données plus détaillées, similaires à CloudTrail celles utilisées pour analyser les journaux opérationnels plutôt que pour suivre les appels d'API.

Real-time tracking

AWS CloudTrail

- CloudTrail n'est pas intrinsèquement conçu pour le suivi en temps réel, mais peut être configuré pour fournir des near-real-time alertes. Par défaut, CloudTrail enregistre l'activité de l'API, mais la livraison du journal est légèrement retardée. Pour un suivi plus immédiat, vous pouvez intégrer CloudTrail Amazon CloudWatch Events ou AWS Lambda déclencher des actions en fonction d'appels d'API ou d'activités spécifiques dès qu'ils sont enregistrés. Cette configuration permet de near-real-time surveiller les événements de sécurité critiques ou les modifications de configuration.

Amazon CloudWatch

- CloudWatch, d'autre part, est conçu pour le suivi en temps réel des performances du système et des applications. Il surveille en permanence les métriques issues AWS des ressources et peut déclencher instantanément des alarmes ou des notifications lorsque des seuils prédéfinis sont dépassés. CloudWatch collecte et analyse également les données des journaux en temps réel, ce qui vous permet de surveiller les journaux des applications, de détecter les anomalies et de répondre aux problèmes opérationnels dès qu'ils surviennent. Cela en fait CloudWatch un outil essentiel pour maintenir la santé et les performances de votre AWS environnement en temps réel.

Utiliser

Maintenant que vous avez pris connaissance des critères de choix entre Amazon AWS CloudTrail et Amazon CloudWatch, vous pouvez sélectionner le service qui répond à vos besoins et utiliser les informations suivantes pour vous aider à commencer à utiliser chacun d'entre eux.

AWS CloudTrail

- Commencer avec AWS CloudTrail

  AWS CloudTrail est un AWS service qui vous aide à permettre l'audit des opérations et des risques, la gouvernance et la conformité de votre Compte AWS. Voici comment vous y prendre pour commencer.

  Explorer le guide

- Compte AWS Activité de révision

  Découvrez comment consulter l'activité récente de AWS l'API dans la fonction Compte AWS d'historique des événements CloudTrail de votre utilisateur.

  Utilisez le didacticiel

- Créer un journal de suivi

  Découvrez comment créer un journal pour enregistrer l'activité des AWS API dans toutes les régions, y compris les données et les événements Insights.

  Utilisez le didacticiel

- Bonnes pratiques en matière de sécurité dans AWS CloudTrail

  Ce guide fournit les meilleures pratiques de sécurité en matière de détection et de prévention à utiliser AWS CloudTrail dans votre entreprise.

  Explorer le guide

Amazon CloudWatch

- Commencer à utiliser Amazon CloudWatch

  Surveillez vos AWS ressources et les applications que vous exécutez AWS en temps réel à l'aide d'Amazon CloudWatch. Vous pouvez les utiliser CloudWatch pour collecter et suivre les métriques, qui sont des variables que vous pouvez mesurer pour vos ressources et vos applications.

  Explorer le guide

- Commencer à utiliser Amazon CloudWatch Metrics

  Ce guide décrit la surveillance de base et la surveillance détaillée, comment représenter graphiquement les métriques et comment utiliser la détection des CloudWatch anomalies.

  Explorer le guide

- Configurer Container Insights sur Amazon EKS et Kubernetes

Configurez le module complémentaire Amazon CloudWatch Observability ESK et ADTO sur votre cluster EKS pour envoyer des métriques. CloudWatch Vous apprendrez également comment configurer Fluent Bit ou Fluentd pour envoyer des journaux à CloudWatch Logs.

Explorer le guide

- Commencer à utiliser Amazon CloudWatch Application Insights

  Découvrez comment utiliser la console pour permettre à CloudWatch Application Insights de gérer vos applications à des fins de surveillance.

  Explorer le guide

- Utilisation de Container Insights

  Découvrez comment CloudWatch Container Insights collecte, agrège et résume les métriques et les journaux provenant de vos applications conteneurisées et de vos microservices.

  Explorer le guide

- Configuration de Container Insights sur Amazon ECS

  Apprenez à configurer les métriques de cluster et de niveau de service, à déployer ADOT pour collecter des métriques au niveau de l' EC2instance et FireLens à configurer l'envoi de CloudWatch journaux vers Logs.

  Explorer le guide

Historique des documents pour Amazon AWS CloudTrail ou pour Amazon CloudWatch ?

Le tableau suivant décrit les modifications importantes apportées à ce guide de décision. Pour recevoir des notifications concernant les mises à jour de ce guide, vous pouvez vous abonner à un flux RSS.

Modification	Description	Date
Première version	Publication initiale du guide de décision.	20 septembre 2024

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.