AWS Leitfaden zur Entscheidungsfindung

AWS CloudTrail oder Amazon CloudWatch?

AWS CloudTrail oder Amazon CloudWatch?: AWS Leitfaden zur Entscheidungsfindung

Table of Contents

AWS CloudTrail oder Amazon CloudWatch?

Verstehen Sie die Unterschiede und wählen Sie den für Sie richtigen aus

Zweck	Um Ihnen bei der Entscheidung zu helfen, ob Amazon AWS CloudTrail oder Amazon die richtige Wahl CloudWatch ist, um die Transparenz, Sicherheit und betriebliche Effizienz Ihrer Cloud-Umgebung aufrechtzuerhalten.
Letzte Aktualisierung	20. September 2024
Abgedeckte Dienstleistungen	• AWS CloudTrail • Amazon CloudWatch

Einführung

Bei der Bereitstellung kritischer Geschäftsworkloads in der ist es wichtig AWS Cloud, die Transparenz, Sicherheit und betriebliche Effizienz in Ihrer Cloud-Umgebung aufrechtzuerhalten. Es gibt eine Reihe von Schlüsselbereichen, die angegangen werden müssen:

- Betriebliche Transparenz — Verfolgen Sie, wer was in Ihrer Cloud-Umgebung tut, und überwachen Sie die Leistung Ihrer Ressourcen.
- Sicherheit — Erkennung ungewöhnlicher API-Aufrufe oder Ressourcennutzung, die auf eine Sicherheitsbedrohung hinweisen könnten.
- Einhaltung gesetzlicher Vorschriften — Aufbewahrung detaillierter Protokolle über Benutzeraktivitäten und Infrastrukturänderungen zu Prüfungszwecken.
- Leistungsmanagement — Überwachung der Ressourcennutzung und der Leistungskennzahlen von Anwendungen.
- Reaktion auf Vorfälle — Daten und Warnmeldungen zur schnellen Identifizierung und Behebung betrieblicher Probleme.
- Kostenkontrolle — Einblicke in die Ressourcennutzung zur Verwaltung der Cloud-Ausgaben.
- Automatisierung — automatisierte Reaktionen auf bestimmte Ereignisse oder Leistungsschwellenwerte.

AWS bietet zwei wichtige Dienste an, die Sie bei der Lösung dieser Probleme unterstützen:

- AWS CloudTrailkonzentriert sich hauptsächlich auf Unternehmensführung, Compliance und Betriebsprüfung. Es protokolliert alle API-Aufrufe in Ihrer AWS Umgebung. Wichtigste Funktionen:
  - Verfolgt alle AWS-Konto Aktivitäten, einschließlich API-Aufrufe, Aktionen, die in den Befehlszeilentools AWS-Managementkonsole AWS SDKs,, ausgeführt wurden, und anderer AWS Dienste.
  - Stellt ein detailliertes Protokoll aller Aktionen bereit, einschließlich der Person, die den Anruf getätigt hat, der verwendete Dienst und die betroffenen Ressourcen.
  - Nützlich für Sicherheitsüberprüfungen, die Nachverfolgung von Benutzeraktivitäten und die Identifizierung potenziell bösartiger Aktionen.
- Amazon CloudWatch ist ein Überwachungs- und Beobachtbarkeitsservice, der Daten und umsetzbare Erkenntnisse für AWS lokale und hybride Anwendungen und Infrastrukturen bereitstellt. Zu den wichtigsten Funktion gehören:
  - Überwacht AWS Ressourcen und laufende Anwendungen AWS in Echtzeit, einschließlich Metriken, Protokollen und Alarmen.
  - Bietet detaillierte Einblicke in die Systemleistung, Fehlerraten, Ressourcennutzung und mehr.
  - Ermöglicht die Einrichtung von Alarmen, um Aktionen (z. B. Skalierung von Ressourcen) auf der Grundlage bestimmter Bedingungen auszulösen.

Beide Dienste sind zwar entscheidend für eine robuste, sichere Cloud-Umgebung, unterscheiden sich jedoch in ihren Anwendungsfällen und den Funktionen, die sie bieten.

Hier finden Sie einen Überblick über die wichtigsten Unterschiede zwischen diesen Diensten, um Ihnen den Einstieg zu erleichtern.

Kategorie	CloudTrail	CloudWatch
Hauptzweck	Verfolgung und Prüfung von API-Aktivitäten	Überwachung und Leistungs management in Echtzeit
Gesammelte Daten	Protokolle von API-Aufrufen, einschließlich der Person, die den Anruf getätigt hat, wann und welche Ressourcen betroffen waren	Metriken, Protokolle und Ereignisse im Zusammenhang mit der Ressourcenleistung und dem Anwendungsverhalte n

Kategorie	CloudTrail	CloudWatch
Anwendungsfälle	Sicherheitsprüfung, Einhaltung von Vorschriften und Nachverfolgung von Änderungen in der Umgebung	Überwachung der Ressourcennutzung, Einstellung von Alarmen und Leistungsmanagement
Sicherheits und Compliance	Hilft bei der Erfüllung von Sicherheits- und Compliance-Anforderungen durch die Bereitstellung detaillierter Aktivitätsprotokolle	Überwacht die Systemleistung auf Sicherheitsanomalien und trägt zur Aufrechterhaltung der Betriebsintegrität bei
Aufbewahrung von Protokollen	Ereignisverlauf der letzten 90 Tage. Kann Pfade und Ereignisdatenspeicher (mithilfe von CloudTrail Lake) erstellen, um Aktivitäten länger als 90 Tage aufzuzeichnen.	Kurzfristige Datenspeicherung für Überwachung und Fehlerbehebung in Echtzeit
Alarme und Benachrichtigungen	Wird nicht hauptsächlich für Alarme verwendet, kann aber Aktionen auslösen, die auf API-Aktivitäten basieren	Ermöglicht die Einstellung von Alarmen für bestimmte Metriken oder Protokollereignisse mit automatisierten Antworten
Integration	Wird häufig zusammen mit Sicherheitsdiensten wie AWS Config IAM für ein verbessertes Sicherheitsmanagement verwendet	Lässt sich in eine breite Palette von AWS Diensten für umfassende Überwachung und Automatisierung integrieren
Kostenüberlegungen	Die Kosten basieren auf der Menge der generierten und gespeicherten Protokolle	Die Kosten basieren auf der Anzahl der überwachten Messwerte, Protokolle und Alarme

Kategorie	CloudTrail	CloudWatch
Datengranularität	Bietet detaillierte Protokolle jedes API-Aufrufs mit detaillierten Informationen	Bietet aggregierte Metriken und Protokolldaten für die Überwachung in Echtzeit
Zugriffskontrolle	Ermöglicht die Nachverfolgung von Zugriffsmustern und Änderungen der Benutzerberechtigungen	Hilft Ihnen, den Zugriff auf Ressourcen auf der Grundlage von Leistungskennzahlen zu überwachen und zu optimieren
Ressourcenabdeckung	AWS-Konto-breit	Individuelle Ressourcen AWS
Tracking in Echtzeit	Nahezu in Echtzeit (innerhalb von 5 Minuten)	In Echtzeit oder fast in Echtzeit
Visualisierung	Eingeschränkt; wird oft mit anderen Tools verwendet	Integrierte Dashboards und Grafiken

Unterschiede zwischen und CloudTrail CloudWatch

Erkunden Sie die Unterschiede zwischen CloudTrail und CloudWatch in einer Reihe von Schlüsselbereichen.

Primary purpose

AWS CloudTrail

- Bietet einen umfassenden Prüfpfad aller API-Aktivitäten innerhalb eines AWS-Konto. Konzentriert sich auf die Aufzeichnung, wer was, wann und von wo aus getan hat. Dazu gehören Aktionen AWS-Managementkonsole, AWS SDKs die über die Befehlszeilentools,, und andere AWS Dienste ausgeführt werden. CloudTrail beantwortet Fragen wie „Wer hat diese EC2 Instanz beendet?“ oder „Welche Änderungen wurden an dieser IAM-Richtlinie vorgenommen?“

Amazon CloudWatch

- Überwacht den Betriebszustand und die Leistung von AWS Ressourcen und Anwendungen. CloudWatch sammelt und verfolgt Metriken, sammelt und überwacht Protokolldateien und setzt Alarme. Es hilft Ihnen, die Leistung Ihrer Anwendungen zu verstehen und auf systemweite Leistungsänderungen zu reagieren. CloudWatch beantwortet Fragen wie „Ist die CPU-Auslastung meiner EC2 Amazon-Instance zu hoch?“ oder „Wie viele Fehler generiert meine Lambda-Funktion?“

Übersicht

CloudTrail hilft Ihnen dabei, Benutzeraktivitäten im Hinblick auf Sicherheit und Compliance zu verfolgen und zu überprüfen. Außerdem CloudWatch geht es um die Überwachung und Optimierung der Systemleistung und des Betriebszustands. Beide Tools erfüllen unterschiedliche, sich aber ergänzende Rollen bei der Verwaltung einer Cloud-Umgebung.

Data collected

AWS CloudTrail

- Konzentriert sich auf die Erfassung detaillierter Protokolle aller API-Aktivitäten in Ihrer AWS Umgebung. Dazu gehören Informationen darüber, wer den API-Aufruf getätigt hat, wann er getätigt wurde, welche Maßnahmen ergriffen wurden und welche Ressourcen eingesetzt wurden. CloudTrailDie Protokolle bieten einen umfassenden Prüfpfad, der für die Nachverfolgung von Änderungen, die Sicherstellung der Einhaltung von Vorschriften und die Untersuchung von Sicherheitsvorfällen unerlässlich ist.

Amazon CloudWatch

- Sammelt Leistungs- und Betriebsdaten aus Ihren AWS Ressourcen und Anwendungen. Dazu gehören Messwerte wie CPU-Auslastung, Speicherauslastung, Netzwerkverkehr und Anwendungsprotokolle sowie benutzerdefinierte Metriken, die Sie definieren können. Die von CloudWatch gesammelten Daten werden für die Echtzeitüberwachung, Leistungsoptimierung und die Einrichtung von Alarmen verwendet, um automatisierte Aktionen auf der Grundlage bestimmter Bedingungen auszulösen.

Übersicht

CloudTrail sammelt Daten im Zusammenhang mit Benutzeraktivitäten und API-Nutzung zu Prüf- und Sicherheitszwecken und CloudWatch sammelt gleichzeitig Metriken und Protokolle zur

Überwachung, Verwaltung und Optimierung der Systemleistung und des Betriebszustands. Beide bieten wichtige Einblicke, dienen aber unterschiedlichen Aspekten des Cloud-Managements.

Use cases

AWS CloudTrail

- Wird hauptsächlich für Sicherheitsaudits, Compliance- und Betriebsprüfungen verwendet. CloudTrailbietet eine detaillierte Aufzeichnung der API-Aufrufe und Benutzeraktivitäten in Ihrer AWS Umgebung und ist daher unverzichtbar für die Nachverfolgung von Änderungen, die Untersuchung von Sicherheitsvorfällen und die Sicherstellung, dass Ihr Unternehmen die gesetzlichen Anforderungen erfüllt. Dies CloudTrail ist beispielsweise nützlich in Szenarien, in denen Sie überwachen müssen, wer auf bestimmte Ressourcen zugegriffen hat, Änderungen an Konfigurationen nachverfolgen oder Aktivitäten mehrerer überprüfen müssen AWS-Konten.

Amazon CloudWatch

- Konzipiert für Echtzeitüberwachung, Leistungsmanagement und betriebliche Effizienz. CloudWatch wird verwendet, um den Zustand Ihrer AWS Ressourcen und Anwendungen zu überwachen, indem Metriken, Protokolle und Ereignisse gesammelt und verfolgt werden. CloudWatch ermöglicht es Ihnen, Alarme einzurichten, die automatisierte Aktionen auslösen, z. B. die Skalierung von Ressourcen oder das Senden von Benachrichtigungen, wenn bestimmte Schwellenwerte erreicht werden. Zu den Anwendungsfällen CloudWatch gehören die Überwachung der Anwendungsleistung, die Verwaltung der Ressourcennutzung, die Erkennung von Anomalien und die Sicherstellung, dass Ihre Systeme optimal laufen, um Ausfallzeiten zu vermeiden.

Security and compliance

AWS CloudTrail

- Entscheidend für die Aufrechterhaltung von Sicherheit und Compliance in AWS Umgebungen. CloudTrail bietet einen umfassenden Prüfpfad aller API-Aufrufe, einschließlich Informationen darüber, wer den Anruf getätigt hat, wann er getätigt wurde und welche Maßnahmen ergriffen wurden. Diese detaillierte Protokollierung ist für die Einhaltung von Compliance-Standards, die Durchführung von Sicherheitsaudits und die Untersuchung von Vorfällen unerlässlich. Durch die Nachverfolgung von Benutzeraktivitäten und Änderungen der Ressourcen werden Rechenschaftspflicht und Transparenz gewährleistet — zentrale Anforderungen für viele regulatorische Rahmenbedingungen. CloudTrail

Amazon CloudWatch

- Spielt eine wichtige Rolle bei der Sicherheit, indem es die Erkennung betrieblicher Anomalien ermöglicht. Sie können es beispielsweise verwenden, um Messwerte CloudWatch zu überwachen, die auf potenzielle Sicherheitsprobleme hinweisen, wie z. B. ungewöhnliche Spitzen im Netzwerkverkehr oder bei der CPU-Auslastung. Darüber hinaus CloudWatch können Alarme und automatische Reaktionen ausgelöst werden, wenn bestimmte Schwellenwerte erreicht werden, was ein proaktives Incident-Management ermöglicht. Die erfassten Protokolle CloudWatch können auch zur Nachverfolgung betrieblicher Ereignisse verwendet werden, was für das Verständnis des Kontextes von Sicherheitsvorfällen von entscheidender Bedeutung sein kann.

Übersicht

Together CloudTrail stellt die für die Einhaltung der Vorschriften erforderlichen Prüfprotokolle bereit und CloudWatch bietet gleichzeitig eine Echtzeitüberwachung, die dabei hilft, Sicherheitsbedrohungen zu erkennen und darauf zu reagieren, und trägt so zu einer sicheren und konformen Cloud-Umgebung bei.

Log retention

AWS CloudTrail

- Standardmäßig zeichnet der CloudTrail Ereignisverlauf die Verwaltungsereignisse der letzten 90 Tage für Ihr Konto auf.
- Benutzer können einen Trail erstellen, um Protokolle auf unbestimmte Zeit in einem S3-Bucket zu speichern.
- In Amazon S3 gespeicherte Protokolle werden nicht automatisch gelöscht, was eine langfristige Aufbewahrung ermöglicht.
- Benutzer können Lebenszyklusrichtlinien für S3-Buckets implementieren, um die langfristigen Speicherkosten zu verwalten.
- CloudTrail kann so konfiguriert werden, dass Protokolle an Logs gesendet CloudWatch werden, was flexiblere Aufbewahrungsoptionen bietet.

Amazon CloudWatch

- Die Aufbewahrung von CloudWatch Protokollen in Logs ist flexibler und konfigurierbarer.

- Die standardmäßige Aufbewahrungsdauer variiert je nach Protokollgruppe und ist in der Regel auf „Niemals ablaufen“ festgelegt.
- Benutzer können benutzerdefinierte Aufbewahrungszeiträume zwischen einem Tag und 10 Jahren festlegen oder sich für eine unbefristete Aufbewahrung entscheiden.
- Verschiedene Protokollgruppen können unterschiedliche Aufbewahrungszeiträume haben.
- Nach Ablauf der Aufbewahrungsfrist werden die Protokolle automatisch gelöscht, um die Speicherkosten im Griff zu behalten.
- CloudWatch Protokolle können bei Bedarf zur längerfristigen Speicherung nach Amazon S3 exportiert werden.

Alarms and notifications

AWS CloudTrail

- Konzentriert sich hauptsächlich auf die Protokollierung von API-Aktivitäten und verfügt nicht über integrierte Alarm- oder Benachrichtigungsfunktionen. Sie können jedoch CloudWatch Protokolle und CloudWatch Alarme integrieren, um Alarme für CloudTrail Ereignisse zu konfigurieren. Diese Konfiguration wird in der Regel verwendet, um Sie über sicherheitsrelevante Ereignisse wie unbefugte Zugriffsversuche oder Änderungen an kritischen Ressourcen zu informieren.

Amazon CloudWatch

- Es wurde speziell für die Echtzeitüberwachung entwickelt und umfasst robuste Alarm- und Benachrichtigungsfunktionen. CloudWatch ermöglicht es Ihnen, Alarme auf der Grundlage von Metriken, Protokolldaten oder benutzerdefinierten Schwellenwerten festzulegen. Wenn diese Schwellenwerte überschritten werden, CloudWatch können Benachrichtigungen über Amazon SNS (Amazon Simple Notification Service) gesendet, automatisierte Aktionen wie das Skalieren von Instances ausgelöst oder benutzerdefinierte Abhilfemaßnahmen mithilfe von durchgeführt werden. AWS Lambda Dies ist CloudWatch ein unverzichtbares Tool für die proaktive Systemverwaltung, das Sie über Leistungsprobleme oder betriebliche Anomalien informiert, sobald diese auftreten.

Integration

CloudTrail und CloudWatch bieten umfangreiche Integrationsoptionen mit anderen AWS Diensten und externen Tools, wodurch deren Funktionalität und Nützlichkeit verbessert werden.

CloudTrail Integrationen

- Amazon S3: Langfristiges Speichern von Protokollen zur Archivierung und Analyse
- CloudWatch Protokolle: Ermöglichen Sie Protokollanalysen und Warnmeldungen in Echtzeit
- Amazon EventBridge: Automatisierte Aktionen basierend auf API-Ereignissen auslösen
- AWS Config: Stellen Sie Informationen zur Konfigurationsverfolgung und Einhaltung von Vorschriften bereit
- AWS Security Hub CSPM: Tragen Sie zur zentralen Verwaltung des Sicherheitsstatus bei
- AWS Lake Formation: Ermöglichen Sie die Verwaltung von CloudTrail Protokollen durch Data Lake
- Amazon Athena: Führen Sie SQL-Abfragen für in Amazon S3 gespeicherte CloudTrail Protokolle durch

CloudWatch Integrationen

- Amazon SNS: Benachrichtigungen für Alarme und Ereignisse senden
- AWS Lambda: Löst serverlose Funktionen auf der Grundlage von Metriken oder Protokollen aus
- Amazon EC2 Auto Scaling: Passen Sie die Kapazität anhand von Leistungskennzahlen an
- AWS Systems Manager: Automatisieren Sie betriebliche Aufgaben auf der Grundlage CloudWatch von Daten
- AWS X-Ray: Kombinieren Sie es mit Trace-Daten, um detaillierte Einblicke in die Anwendung zu erhalten
- Container-Services (Amazon ECS, Amazon EKS): Überwachung containerisierter Anwendungen
- Tools von Drittanbietern: Exportieren Sie Metriken und Protokolle auf externe Überwachungsplattformen

Cost considerations

AWS CloudTrail

- CloudTrail richtet sich in erster Linie nach der Anzahl der protokollierten und gespeicherten Ereignisse. Standardmäßig werden in der CloudTrail Ereignishistorie die Verwaltungsereignisse der letzten 90 Tage für Ihr Konto aufgezeichnet und kostenlos gespeichert. Wenn Sie jedoch Datenereignisse (wie S3-Aktionen auf Objektebene) aktivieren oder mehrere Trails erstellen, fallen Gebühren an, die auf dem Volumen der Ereignisse und dem in Amazon S3 benötigten Speicherplatz basieren. Zusätzliche Kosten können anfallen, wenn Sie erweiterte Funktionen wie CloudTrail Insights verwenden, die eine tiefere Analyse ungewöhnlicher API-Aktivitäten ermöglichen.

Amazon CloudWatch

- CloudWatch hat eine komplexere Preisstruktur, die auf mehreren Faktoren basiert, darunter der Anzahl der von Ihnen überwachten benutzerdefinierten Metriken, der Anzahl der aufgenommenen und gespeicherten Protokollereignisse sowie der Verwendung von Alarmen und Dashboards. Die grundlegende Überwachung von AWS Diensten ist kostenlos, detaillierte Überwachung und benutzerdefinierte Metriken sind jedoch kostenpflichtig. Der Preis für die Speicherung von Protokollen richtet sich nach der Menge der aufgenommenen und gespeicherten Daten. Hinzu kommen zusätzliche Kosten für die Einrichtung und Verwaltung von Alarmen oder die Nutzung von CloudWatch Logs Insights für erweiterte Protokollanalysen.

Data granularity

AWS CloudTrail

- CloudTrail bietet eine hohe Granularität, indem jeder einzelne API-Aufruf in Ihrer AWS Umgebung protokolliert wird. Jeder Protokolleintrag enthält detaillierte Informationen, z. B. wer die Anfrage gestellt hat, welche Aktion ausgeführt wurde, welche Ressourcen betroffen sind und wann die Aktion ausgeführt wurde. Dieser Detaillierungsgrad ist für die Prüfung, Sicherheitsüberwachung und Einhaltung von Vorschriften von entscheidender Bedeutung, da Sie damit bestimmte Benutzeraktionen und -änderungen bis hin zum genauen API-Aufruf verfolgen können.

Amazon CloudWatch

- CloudWatch konzentriert sich auf aggregierte Daten für die Überwachung und das Leistungsmanagement. Es sammelt in regelmäßigen Abständen (normalerweise alle Minuten oder fünf Minuten) Kennzahlen und protokolliert Betriebsdaten von AWS

Ressourcen. Es CloudWatch bietet zwar detaillierte Einblicke in die Systemleistung und das Anwendungsverhalten, aber die Daten sind im Vergleich zu CloudTrail aggregierter. So können Sie beispielsweise die durchschnittliche CPU-Auslastung im Laufe der Zeit überwachen und nicht einzelne Anfragen oder Aktionen. CloudWatch Protokolle können jedoch detailliertere Daten liefern, die denen ähneln, die CloudTrail aber häufig zur Analyse von Betriebsprotokollen verwendet werden, anstatt API-Aufrufe zu verfolgen.

Real-time tracking

AWS CloudTrail

- CloudTrail ist nicht grundsätzlich für die Echtzeitverfolgung konzipiert, kann aber so konfiguriert werden, dass Warnmeldungen ausgegeben werden. near-real-time CloudTrail Zeichnet standardmäßig API-Aktivitäten auf, es kommt jedoch zu einer leichten Verzögerung bei der Protokollzustellung. Für eine direktere Nachverfolgung können Sie Amazon CloudWatch Events integrieren CloudTrail oder Aktionen auslösen AWS Lambda , die auf bestimmten API-Aufrufen oder Aktivitäten basieren, sobald diese protokolliert werden. Dieses Setup ermöglicht die near-real-time Überwachung kritischer Sicherheitsereignisse oder Konfigurationsänderungen.

Amazon CloudWatch

- CloudWatchist dagegen für die Echtzeitverfolgung der System- und Anwendungsleistung konzipiert. Es überwacht kontinuierlich die Kennzahlen von AWS Ressourcen und kann sofort Alarme oder Benachrichtigungen auslösen, wenn vordefinierte Schwellenwerte überschritten werden. CloudWatch sammelt und analysiert außerdem Protokolldaten in Echtzeit, sodass Sie Anwendungsprotokolle überwachen, Anomalien erkennen und auf Betriebsprobleme reagieren können, sobald sie auftreten. Dies ist CloudWatch ein unverzichtbares Tool, um den Zustand und die Leistung Ihrer AWS Umgebung in Echtzeit aufrechtzuerhalten.

Verwenden Sie

Nachdem Sie sich mit den Kriterien für die Wahl zwischen Amazon AWS CloudTrail und Amazon vertraut gemacht haben CloudWatch, können Sie den Service auswählen, der Ihren Anforderungen entspricht, und die folgenden Informationen verwenden, um Ihnen den Einstieg in die Nutzung der einzelnen Dienste zu erleichtern.

AWS CloudTrail

- Erste Schritte mit AWS CloudTrail

  AWS CloudTrail ist ein AWS Service, der Sie bei der Betriebs- und Risikoprüfung, Unternehmensführung und Einhaltung Ihrer Vorschriften unterstützt AWS-Konto. Hier erfahren Sie, wie Sie damit beginnen können.

  Den Leitfaden erkunden

- AWS-Konto Aktivität überprüfen

  Erfahren Sie, wie Sie die letzten AWS API-Aktivitäten in der AWS-Konto Funktion CloudTrail „Ereignisverlauf“ Ihres Benutzers überprüfen können.

  Nutze das Tutorial

- Einen Trail anlegen

  Erfahren Sie, wie Sie einen Trail erstellen, um AWS API-Aktivitäten in allen Regionen zu protokollieren, einschließlich Daten und Insights-Ereignissen.

  Nutze das Tutorial

- Bewährte Sicherheitsmethoden in AWS CloudTrail

  Dieser Leitfaden enthält bewährte Methoden zur Erkennung und Vorbeugung von Sicherheitsvorkehrungen, die Sie AWS CloudTrail in Ihrem Unternehmen anwenden können.

  Den Leitfaden erkunden

Amazon CloudWatch

- Erste Schritte mit Amazon CloudWatch

  Überwachen Sie mit Amazon Ihre AWS Ressourcen und die Anwendungen, auf AWS denen Sie laufen, in Echtzeit CloudWatch. Sie können CloudWatch damit Metriken sammeln und verfolgen. Dabei handelt es sich um Variablen, die Sie für Ihre Ressourcen und Anwendungen messen können.

  Den Leitfaden erkunden

- Erste Schritte mit Amazon CloudWatch Metrics

In diesem Leitfaden werden die grundlegende Überwachung und die detaillierte Überwachung, die grafische Darstellung von Metriken und die Verwendung der CloudWatch Anomalieerkennung beschrieben.

Den Leitfaden erkunden

- Container Insights auf Amazon EKS und Kubernetes einrichten

  Richten Sie das Amazon CloudWatch Observability ESK-Add-on und ADTO auf Ihrem EKS-Cluster ein, an das Metriken gesendet werden sollen. CloudWatch Sie erfahren auch, wie Sie Fluent Bit oder Fluentd einrichten, um Protokolle an Logs zu senden. CloudWatch

  Den Leitfaden erkunden

- Erste Schritte mit Amazon CloudWatch Application Insights

  Erfahren Sie, wie Sie mithilfe der Konsole CloudWatch Application Insights Ihre Anwendungen für die Überwachung verwalten können.

  Den Leitfaden erkunden

- Verwenden von Container Insights

  Erfahren Sie, wie CloudWatch Container Insights Metriken und Protokolle aus Ihren containerisierten Anwendungen und Microservices sammelt, aggregiert und zusammenfasst.

  Den Leitfaden erkunden

- Container Insights auf Amazon ECS einrichten

  Erfahren Sie, wie Sie Cluster- und Service-Level-Metriken konfigurieren, ADOT zur Erfassung von Metriken auf EC2 Instanzebene einsetzen und das Senden von Protokollen an CloudWatch Logs einrichten FireLens .

  Den Leitfaden erkunden

Dokumentenverlauf für AWS CloudTrail oder Amazon CloudWatch?

In der folgenden Tabelle werden die wichtigen Änderungen an diesem Entscheidungsleitfaden beschrieben. Für Benachrichtigungen über Aktualisierungen dieses Handbuchs können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Erstversion	Erste Veröffentlichung des Entscheidungsleitfadens.	20. September 2024

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.