AWS Guía de decisiones

AWS CloudTrail ¿o Amazon CloudWatch?

AWS CloudTrail ¿o Amazon CloudWatch?: AWS Guía de decisiones

Table of Contents

AWS CloudTrail ¿o Amazon CloudWatch?

Comprenda las diferencias y elija la que sea adecuada para usted

Finalidad	Para ayudarlo a determinar AWS CloudTrail si Amazon CloudWatch es la opción correcta para mantener la visibilidad, la seguridad y la eficiencia operativa de su entorno de nube.
Última actualización	20 de septiembre de 2024
Servicios cubiertos	• AWS CloudTrail • Amazon CloudWatch

Introducción

Al implementar cargas de trabajo empresariales críticas en el entorno de nube Nube de AWS, es esencial mantener la visibilidad, la seguridad y la eficiencia operativa en su entorno de nube. Hay una serie de áreas clave que abordar:

- Transparencia operativa: realiza un seguimiento de quién hace qué en su entorno de nube y supervisa el rendimiento de sus recursos.
- Garantía de seguridad: detectar llamadas a la API o el uso de recursos inusuales que puedan indicar una amenaza a la seguridad.
- Cumplimiento normativo: mantener registros detallados de las actividades de los usuarios y los cambios en la infraestructura con fines de auditoría.
- Gestión del rendimiento: supervisión de la utilización de los recursos y las métricas de rendimiento de las aplicaciones.
- Respuesta a incidentes: datos y alertas para identificar y responder rápidamente a los problemas operativos.
- Control de costes: información sobre el uso de los recursos para ayudar a gestionar el gasto en la nube.
- Automatización: respuestas automatizadas a eventos o umbrales de rendimiento específicos.

AWS ofrece dos servicios clave para ayudar a abordar estas preocupaciones:

- AWS CloudTrailse centra principalmente en la gobernanza, el cumplimiento y la auditoría operativa. Registra todas las llamadas a la API realizadas en su AWS entorno. Características clave:
  - Realiza un seguimiento de todas Cuenta de AWS las actividades, incluidas las llamadas a la API Consola de administración de AWS AWS SDKs, las acciones realizadas en las herramientas de línea de comandos y otros AWS servicios.
  - Proporciona un registro detallado de cada acción, incluida la persona que realizó la llamada, el servicio utilizado y los recursos afectados.
  - Resulta útil para realizar auditorías de seguridad, realizar un seguimiento de la actividad de los usuarios e identificar posibles acciones maliciosas.
- Amazon CloudWatch es un servicio de monitoreo y observabilidad que proporciona datos e información procesable para AWS infraestructuras y aplicaciones locales e híbridas. Entre las características principales se incluyen:
  - Supervisa AWS los recursos y las aplicaciones que se ejecutan AWS en tiempo real, incluidas las métricas, los registros y las alarmas.
  - Proporciona información detallada sobre el rendimiento del sistema, las tasas de error, la utilización de los recursos y mucho más.
  - Permite configurar alarmas para activar acciones (por ejemplo, escalar los recursos) en función de condiciones específicas.

Si bien ambos servicios son fundamentales para un entorno de nube sólido y seguro, difieren en sus casos de uso y en las capacidades que ofrecen.

A continuación, le ofrecemos una vista general de las principales diferencias entre estos servicios para que pueda empezar.

Categoría	CloudTrail	CloudWatch
Propósito principal	Seguimiento y auditoría de la actividad de la API	Supervisión y gestión del rendimiento en tiempo real
Datos recopilados	Registros de las llamadas a la API, incluidos quién realizó	Métricas, registros y eventos relacionados con el rendimien to de los recursos y el

Categoría	CloudTrail	CloudWatch
	la llamada, cuándo y qué recursos se vieron afectados	comportamiento de las aplicaciones
Casos de uso	Auditoría de seguridad, cumplimiento y seguimiento de los cambios en el entorno	Supervisión de la utilización de los recursos, configura ción de alarmas y gestión del rendimiento
Seguridad y conformidad	Ayuda a cumplir los requisito s de seguridad y conformidad al proporcionar registros de actividad detallados	Supervisa el rendimiento del sistema para detectar anomalías de seguridad y ayuda a mantener la integrida d operativa
Retención de registros	Historial de eventos de los últimos 90 días. Puede crear senderos y almacenes de datos de eventos (con CloudTrail Lake) para mantener un registro de la actividad durante más de 90 días.	Retención de datos a corto plazo para la supervisión y la resolución de problemas en tiempo
Alarmas y notificaciones	No se usa principalmente para alarmas, pero puede activar acciones en función de la actividad de la API	Permite configurar alarmas para métricas específicas o registrar eventos, con respuestas automatizadas
Integración	AWS Config Suele utilizars e con servicios de seguridad como el IAM para mejorar la gestión de la seguridad	Se integra con una amplia gama de AWS servicios para una supervisión y automatiz ación integrales
Consideraciones sobre costos	Los costos se basan en el volumen de registros generados y almacenados	Los costos se basan en la cantidad de métricas, registros y alarmas monitoreados

Categoría	CloudTrail	CloudWatch
Granularidad de los datos	Proporciona registros detallados de cada llamada a la API con información pormenorizada	Proporciona métricas agregadas y datos de registro para una supervisión en tiempo real
Control de acceso	Le permite realizar un seguimiento de los patrones de acceso y los cambios en los permisos de los usuarios	Le ayuda a supervisar y optimizar el acceso a los recursos en función de las métricas de rendimiento
Cobertura de recursos	Cuenta de AWS-en todo	Recursos individuales AWS
Seguimiento en tiempo real	Casi en tiempo real (en 5 minutos)	En tiempo real o casi en tiempo real
Visualización	Limitado; se usa a menudo con otras herramientas	Paneles de mando y gráficos integrados

Diferencias entre y CloudTrail CloudWatch

Explore las diferencias entre CloudTrail y CloudWatch en una serie de áreas clave.

Primary purpose

AWS CloudTrail

- Proporciona un registro de auditoría completo de toda la actividad de las API dentro de un Cuenta de AWS. Se centra en registrar quién hizo qué, cuándo y desde dónde. Esto incluye las acciones realizadas a través de las herramientas de línea de comandos y otros AWS servicios. Consola de administración de AWS AWS SDKs CloudTrail responde a preguntas como «¿Quién puso fin a esta EC2 instancia?» o «¿Qué cambios se han realizado en esta política de IAM?»

Amazon CloudWatch

- Supervisa el estado operativo y el rendimiento de AWS los recursos y las aplicaciones. CloudWatch recopila y rastrea las métricas, recopila y monitorea los archivos de registro y establece las alarmas. Le ayuda a comprender el rendimiento de sus aplicaciones y a responder a los cambios de rendimiento en todo el sistema. CloudWatch responde a preguntas como «¿El uso de la CPU de mi EC2 instancia de Amazon es demasiado alto?» o «¿Cuántos errores genera mi función Lambda?»

Resumen

CloudTrail le ayuda a rastrear y auditar la actividad de los usuarios para garantizar la seguridad y el cumplimiento, al mismo tiempo que CloudWatch supervisa y optimiza el rendimiento del sistema y el estado operativo. Ambas herramientas cumplen funciones distintas, aunque complementarias, en la gestión de un entorno de nube.

Data collected

AWS CloudTrail

- Se centra en capturar registros detallados de toda la actividad de las API en su AWS entorno. Esto incluye información sobre quién realizó la llamada a la API, cuándo se realizó, la acción realizada y los recursos involucrados. CloudTrailLos registros proporcionan una pista de auditoría completa, esencial para hacer un seguimiento de los cambios, garantizar el cumplimiento e investigar los incidentes de seguridad.

Amazon CloudWatch

- Recopila datos operativos y de rendimiento de sus AWS recursos y aplicaciones. Esto incluye métricas como el uso de la CPU, la utilización de la memoria, el tráfico de red y los registros de las aplicaciones, así como métricas personalizadas que puede definir. Los datos recopilados por CloudWatch se utilizan para la supervisión en tiempo real, la optimización del rendimiento y la configuración de alarmas para activar acciones automatizadas en función de condiciones específicas.

Resumen

CloudTrail recopila datos relacionados con la actividad de los usuarios y el uso de las API con fines de auditoría y seguridad, al tiempo que CloudWatch recopila métricas y registros para monitorear, administrar y optimizar el rendimiento y el estado operativo del sistema.

Ambos proporcionan información fundamental, pero se ocupan de diferentes aspectos de la administración de la nube.

Use cases

AWS CloudTrail

- Se utiliza principalmente para la auditoría de seguridad, el cumplimiento y la auditoría operativa. CloudTrailproporciona un registro detallado de las llamadas a la API y la actividad de los usuarios en su AWS entorno, por lo que es esencial para rastrear los cambios, investigar los incidentes de seguridad y garantizar que su organización cumpla con los requisitos reglamentarios. Por ejemplo, CloudTrail resulta útil en situaciones en las que es necesario supervisar quién accedió a recursos específicos, realizar un seguimiento de los cambios realizados en las configuraciones o auditar la actividad de varios Cuentas de AWS.

Amazon CloudWatch

- Diseñada para la supervisión en tiempo real, la gestión del rendimiento y la eficiencia operativa. CloudWatch se utiliza para supervisar el estado de sus AWS recursos y aplicaciones mediante la recopilación y el seguimiento de métricas, registros y eventos. CloudWatch le permite configurar alarmas que activan acciones automatizadas, como escalar los recursos o enviar notificaciones cuando se alcanzan ciertos umbrales. Los casos de uso CloudWatch incluyen la supervisión del rendimiento de las aplicaciones, la gestión de la utilización de los recursos, la detección de anomalías y la garantía de que los sistemas funcionen de forma óptima para evitar el tiempo de inactividad.

Security and compliance

AWS CloudTrail

- Es crucial para mantener la seguridad y el cumplimiento en AWS los entornos. CloudTrail proporciona un registro de auditoría completo de todas las llamadas a la API, que incluye quién realizó la llamada, cuándo se realizó y las medidas adoptadas. Este registro detallado es esencial para cumplir con las normas de conformidad, realizar auditorías de seguridad e investigar los incidentes. Al rastrear la actividad de los usuarios y los cambios en los recursos, CloudTrail ayuda a garantizar la responsabilidad y la transparencia, que son requisitos clave para muchos marcos regulatorios.

Amazon CloudWatch

- Desempeña un papel en la seguridad al permitir la detección de anomalías operativas. Por ejemplo, se puede utilizar CloudWatch para supervisar las métricas que indican posibles problemas de seguridad, como picos inusuales en el tráfico de la red o el uso de la CPU. Además, CloudWatch puede activar alarmas y respuestas automatizadas cuando se alcanzan ciertos umbrales, lo que permite una gestión proactiva de los incidentes. Los registros capturados también se CloudWatch pueden utilizar para realizar un seguimiento de los eventos operativos, lo que puede ser vital para comprender el contexto de los incidentes de seguridad.

Resumen

En conjunto, CloudTrail proporcionan los registros de auditoría necesarios para el cumplimiento y, al mismo tiempo, CloudWatch ofrecen una supervisión en tiempo real que ayuda a detectar las amenazas a la seguridad y responder a ellas, lo que contribuye a crear un entorno de nube seguro y que cumpla con las normas.

Log retention

AWS CloudTrail

- De forma predeterminada, el historial de CloudTrail eventos registra los últimos 90 días de eventos de administración de su cuenta.
- Los usuarios pueden crear un registro para almacenar los registros de forma indefinida en un bucket de S3.
- No se eliminan automáticamente los registros almacenados en Amazon S3, lo que permite conservarlos a largo plazo.
- Los usuarios pueden implementar políticas de ciclo de vida en los depósitos de S3 para administrar los costos de almacenamiento a largo plazo.
- CloudTrail se puede configurar para enviar registros a Logs para CloudWatch disponer de opciones de retención más flexibles.

Amazon CloudWatch

- La retención de CloudWatch registros en Logs es más flexible y configurable.
- El período de retención predeterminado varía según el grupo de registros y, por lo general, se establece en «Nunca caduca».

- Los usuarios pueden establecer períodos de retención personalizados que van desde un día hasta 10 años, o elegir una retención indefinida.
- Los distintos grupos de registros pueden tener distintos períodos de retención.
- Tras el período de retención, los registros se eliminan automáticamente para gestionar los costes de almacenamiento.
- CloudWatch Si es necesario, los registros se pueden exportar a Amazon S3 para almacenarlos durante más tiempo.

Alarms and notifications

AWS CloudTrail

- Se centra principalmente en registrar la actividad de la API y no tiene funciones integradas de alarma o notificación. Sin embargo, puede integrarlo con CloudWatch los registros y CloudWatch las alarmas para configurar las alarmas de CloudTrail los eventos. Esta configuración se suele utilizar para avisarle sobre eventos relacionados con la seguridad, como intentos de acceso no autorizado o cambios en recursos críticos.

Amazon CloudWatch

- Diseñada específicamente para la supervisión en tiempo real e incluye sólidas funciones de alarma y notificación. CloudWatch le permite configurar las alarmas en función de métricas, datos de registro o umbrales personalizados. Cuando se superan estos umbrales, CloudWatch puede enviar notificaciones a través de Amazon SNS (Amazon Simple Notification Service), activar acciones automatizadas como escalar instancias o realizar pasos de remediación personalizados utilizando. AWS Lambda Esto lo convierte en CloudWatch una herramienta esencial para la administración proactiva del sistema, ya que le alerta sobre problemas de rendimiento o anomalías operativas a medida que se producen.

Integration

CloudTrail y CloudWatch ofrecen amplias opciones de integración con otros AWS servicios y herramientas externas, lo que mejora su funcionalidad y utilidad.

CloudTrail integraciones

- Amazon S3: almacene registros a largo plazo para archivarlos y analizarlos

- CloudWatch Registros: habilite el análisis y las alertas de registros en tiempo real
- Amazon EventBridge: desencadena acciones automatizadas en función de los eventos de la API
- AWS Config: Proporcione información para el seguimiento y el cumplimiento de la configuración
- AWS Security Hub CSPM: Contribuya a la gestión centralizada de la postura de seguridad
- AWS Lake Formation: Habilite la gobernanza de los CloudTrail registros de los lagos de datos
- Amazon Athena: Realice consultas SQL en CloudTrail los registros almacenados en Amazon S3

CloudWatch integraciones

- Amazon SNS: envíe notificaciones de alarmas y eventos
- AWS Lambda: Active funciones sin servidor en función de métricas o registros
- Amazon EC2 Auto Scaling: ajuste la capacidad en función de las métricas de rendimiento
- AWS Systems Manager: Automatice las tareas operativas en función de CloudWatch los datos
- AWS X-Ray: Combínelo con datos de rastreo para obtener información detallada sobre las aplicaciones
- Servicios de contenedores (Amazon ECS, Amazon EKS): supervise las aplicaciones en contenedores
- Herramientas de terceros: exporte métricas y registros a plataformas de monitoreo externas

Cost considerations

AWS CloudTrail

- CloudTrail su precio se basa principalmente en la cantidad de eventos registrados y almacenados. De forma predeterminada, el historial de CloudTrail eventos registra y almacena, de forma gratuita, los últimos 90 días de los eventos de gestión de tu cuenta. Sin embargo, si habilita los eventos de datos (como las acciones a nivel de objeto de S3) o crea varios seguimientos, se le cobrarán cargos en función del volumen de eventos y del almacenamiento necesarios en Amazon S3. Si utiliza funciones avanzadas como CloudTrail Insights, que proporcionan un análisis más profundo de la actividad inusual de las API, podrían generarse costes adicionales.

Amazon CloudWatch

- CloudWatch tiene una estructura de precios más compleja que se basa en varios factores, como la cantidad de métricas personalizadas que monitorizas, la cantidad de eventos de registro que se ingieren y almacenan y el uso de alarmas y paneles. La supervisión básica de AWS los servicios es gratuita, pero la supervisión detallada y las métricas personalizadas conllevan gastos. El precio del almacenamiento de registros se basa en el volumen de datos ingeridos y retenidos, con costes adicionales para configurar y mantener las alarmas o utilizar CloudWatch Logs Insights para el análisis avanzado de los registros.

Data granularity

AWS CloudTrail

- CloudTrail proporciona una gran granularidad al registrar cada llamada a la API individual realizada en su AWS entorno. Cada entrada de registro incluye información detallada, como quién realizó la solicitud, la acción realizada, los recursos afectados y la hora de la acción. Este nivel de detalle es fundamental para la auditoría, la supervisión de la seguridad y el cumplimiento, ya que permite rastrear las acciones y los cambios específicos de los usuarios hasta la llamada exacta a la API.

Amazon CloudWatch

- CloudWatch se centra en los datos agregados para la supervisión y la gestión del rendimiento. Recopila métricas a intervalos regulares (normalmente cada minuto o cinco minutos) y registra los datos operativos de AWS los recursos. Si bien CloudWatch proporciona información detallada sobre el rendimiento del sistema y el comportamiento de las aplicaciones, sus datos son más agregados en comparación con CloudTrail. Por ejemplo, puede supervisar el uso medio de la CPU a lo largo del tiempo en lugar de realizar solicitudes o acciones individuales. CloudWatch Sin embargo, los registros pueden proporcionar datos más detallados, de forma similar a CloudTrail los que se utilizan a menudo para analizar los registros operativos en lugar de realizar un seguimiento de las llamadas a la API.

Real-time tracking

AWS CloudTrail

- CloudTrail no está diseñado intrínsecamente para el seguimiento en tiempo real, pero se puede configurar para proporcionar near-real-time alertas. De forma predeterminada, CloudTrail registra la actividad de la API, pero hay un ligero retraso en la entrega de los registros. Para un seguimiento más inmediato, puedes integrarlo CloudTrail con Amazon CloudWatch Events o AWS Lambda activar acciones basadas en llamadas o actividades específicas a la API tan pronto como se registren. Esta configuración permite near-real-time monitorear los eventos de seguridad críticos o los cambios de configuración.

Amazon CloudWatch

- CloudWatch, por otro lado, está diseñado para el seguimiento en tiempo real del rendimiento del sistema y las aplicaciones. Supervisa continuamente las métricas de AWS los recursos y puede activar alarmas o notificaciones al instante cuando se superan los umbrales predefinidos. CloudWatch también recopila y analiza los datos de registro en tiempo real, lo que le permite supervisar los registros de las aplicaciones, detectar anomalías y responder a los problemas operativos a medida que se producen. Esto lo convierte en CloudWatch una herramienta esencial para mantener el estado y el rendimiento de su AWS entorno en tiempo real.

Uso

Ahora que has leído los criterios para elegir entre Amazon AWS CloudTrail y Amazon CloudWatch, puedes seleccionar el servicio que se adapte a tus necesidades y utilizar la siguiente información para empezar a utilizar cada uno de ellos.

AWS CloudTrail

- ¿Cómo empezar con AWS CloudTrail

  AWS CloudTrail es un AWS servicio que le ayuda a habilitar la auditoría operativa y de riesgos, la gobernanza y el cumplimiento de sus normas Cuenta de AWS. A continuación, le indicamos cómo empezar a usarlo.

  Exploración de la guía
- Revisa Cuenta de AWS la actividad

  Obtén información sobre cómo revisar la actividad reciente de la AWS API en la función de historial CloudTrail de eventos de tu Cuenta de AWS usuario.

Usa el tutorial

- Crear un registro de seguimiento

  Aprenda a crear un registro para registrar la actividad de las AWS API en todas las regiones, incluidos los datos y los eventos de Insights.

  Usa el tutorial

- Mejores prácticas de seguridad en AWS CloudTrail

  Esta guía proporciona las mejores prácticas de seguridad preventiva y de detección para su uso AWS CloudTrail en su organización.

  Exploración de la guía

Amazon CloudWatch

- Cómo empezar con Amazon CloudWatch

  Supervisa tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real con Amazon CloudWatch. Puede utilizarlas CloudWatch para recopilar y realizar un seguimiento de las métricas, que son variables que puede medir para sus recursos y aplicaciones.

  Exploración de la guía

- Cómo empezar a usar Amazon CloudWatch Metrics

  En esta guía, se explica la supervisión básica y detallada, cómo graficar las métricas y cómo utilizar la detección de CloudWatch anomalías.

  Exploración de la guía

- Configuración de Container Insights en Amazon EKS y Kubernetes

  Configure el complemento Amazon CloudWatch Observability ESK y ADTO en su clúster de EKS al que enviar las métricas. CloudWatch También aprenderá a configurar Fluent Bit o Fluentd para enviar registros a Logs. CloudWatch

  Exploración de la guía

- Primeros pasos con Amazon CloudWatch Application Insights

Aprenda a usar la consola para permitir que CloudWatch Application Insights administre sus aplicaciones para su monitoreo.

Exploración de la guía

- Uso de Información de contenedores

  Descubra cómo CloudWatch Container Insights recopila, agrega y resume las métricas y los registros de sus aplicaciones y microservicios contenerizados.

  Exploración de la guía

- Configuración de Container Insights en Amazon ECS

  Aprenda a configurar las métricas de clúster y nivel de servicio, a implementar ADOT para recopilar métricas a nivel de EC2 instancia y FireLens a configurar el envío de CloudWatch registros a Logs.

  Exploración de la guía

¿Historial de documentos para AWS CloudTrail Amazon CloudWatch?

En la siguiente tabla se describen los cambios importantes en esta guía de decisiones. Para recibir notificaciones sobre las actualizaciones de esta guía, puede suscribirse a una fuente RSS.

Cambio	Descripción	Fecha
Versión inicial	Versión inicial de la guía de decisiones.	20 de septiembre de 2024

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.