AWS Guia de decisão

AWS CloudTrail ou Amazon CloudWatch?

AWS CloudTrail ou Amazon CloudWatch?: AWS Guia de decisão

Table of Contents

AWS CloudTrail ou Amazon CloudWatch?

Entenda as diferenças e escolha a mais adequada para você

Finalidade	Para ajudá-lo a determinar se AWS CloudTrail a Amazon CloudWatch é a escolha certa para manter a visibilidade, a segurança e a eficiênci a operacional do seu ambiente de nuvem.
Última atualização	20 de setembro de 2024
Serviços cobertos	• AWS CloudTrail • Amazon CloudWatch

Introdução

Ao implantar cargas de trabalho comerciais críticas no Nuvem AWS, é essencial manter a visibilidade, a segurança e a eficiência operacional em seu ambiente de nuvem. Há várias áreas principais a serem abordadas:

- Transparência operacional — Rastreando quem está fazendo o quê em seu ambiente de nuvem e monitorando o desempenho de seus recursos.
- Garantia de segurança — Detectar chamadas de API incomuns ou utilização de recursos que possam indicar uma ameaça à segurança.
- Conformidade regulatória — Manter registros detalhados das atividades do usuário e das mudanças na infraestrutura para fins de auditoria.
- Gerenciamento de desempenho — monitorando a utilização de recursos e as métricas de desempenho do aplicativo.
- Resposta a incidentes — dados e alertas para identificar e responder rapidamente aos problemas operacionais.
- Controle de custos — insights sobre o uso de recursos para ajudar a gerenciar os gastos com a nuvem.
- Automação — respostas automatizadas a eventos específicos ou limites de desempenho.

AWS oferece dois serviços principais para ajudar a lidar com essas preocupações:

- AWS CloudTrailestá focado principalmente em governança, conformidade e auditoria operacional. Ele registra todas as chamadas de API feitas em seu AWS ambiente. Principais recursos:
  - Acompanha todas as Conta da AWS atividades, incluindo chamadas de API Console de gerenciamento da AWS AWS SDKs, ações realizadas nas ferramentas de linha de comando e outros AWS serviços.
  - Fornece um registro detalhado de cada ação, incluindo quem fez a chamada, o serviço usado e quais recursos foram afetados.
  - Útil para auditoria de segurança, rastreamento da atividade do usuário e identificação de ações potencialmente maliciosas.
- CloudWatchA Amazon é um serviço de monitoramento e observabilidade que fornece dados e insights acionáveis para AWS aplicativos e infraestrutura locais e híbridos. Os principais recursos incluem:
  - Monitora os AWS recursos e os aplicativos AWS em execução em tempo real, incluindo métricas, registros e alarmes.
  - Fornece informações detalhadas sobre desempenho do sistema, taxas de erro, utilização de recursos e muito mais.
  - Permite configurar alarmes para acionar ações (por exemplo, escalar recursos) com base em condições específicas.

Embora os dois serviços sejam essenciais para um ambiente de nuvem robusto e seguro, eles diferem em seus casos de uso e nos recursos que oferecem.

Aqui está uma visão geral das principais diferenças entre esses serviços para você começar.

Categoria	CloudTrail	CloudWatch
Objetivo principal	Rastreamento e auditoria de atividades de API	Monitoramento em tempo real e gerenciamento de desempenho
Dados coletados	Registros de chamadas de API, incluindo quem fez a chamada, quando e quais recursos foram afetados	Métricas, registros e eventos relacionados ao desempenho dos recursos e ao comportam ento do aplicativo

Categoria	CloudTrail	CloudWatch
Casos de uso	Auditoria de segurança, conformidade e rastreamento de mudanças no ambiente	Monitoramento da utilização de recursos, configuração de alarmes e gerenciamento de desempenho
Segurança e conformidade	Ajuda a atender aos requisitos de segurança e conformidade fornecendo registros detalhados de atividades	Monitora o desempenho do sistema em busca de anomalias de segurança e ajuda a manter a integridade operacional
Retenção de log	Últimos 90 dias do histórico do evento. Pode criar trilhas e armazenamentos de dados de eventos (usando o CloudTrail Lake) para manter um registro da atividade por mais de 90 dias.	Retenção de dados de curto prazo para monitoramento e solução de problemas em tempo real
Alarmes e notificações	Não é usado principalmente para alarmes, mas pode acionar ações com base na atividade da API	Permite definir alarmes para métricas específicas ou eventos de registro, com respostas automatizadas
Integração	Frequentemente usado com serviços de segurança como AWS Config o IAM para aprimorar o gerenciamento de segurança	Integra-se a uma ampla variedade de AWS serviços para monitoramento e automação abrangentes
Considerações sobre custos	Custos com base no volume de registros gerados e armazenados	Custos com base no número de métricas, registros e alarmes monitorados

Categoria	CloudTrail	CloudWatch
Granularidade de dados	Fornece registros detalhados de cada chamada de API com informações granulares	Fornece métricas agregadas e dados de registro para monitoramento em tempo real
Controle de acesso	Permite que você acompanhe padrões de acesso e alteraçõe s nas permissões do usuário	Ajuda você a monitorar e otimizar o acesso aos recursos com base em métricas de desempenho
Cobertura de recursos	Conta da AWS-largo	AWS Recursos individuais
Acompanhamento em tempo real	Quase em tempo real (em 5 minutos)	Em tempo real ou quase em tempo real
Visualização	Limitado; frequentemente usado com outras ferramentas	Painéis e gráficos integrados

Diferenças entre CloudTrail e CloudWatch

Explore as diferenças entre CloudTrail e CloudWatch em várias áreas importantes.

Primary purpose

AWS CloudTrail

- Fornece uma trilha de auditoria abrangente de todas as atividades de API em um Conta da AWS. Concentra-se em registrar quem fez o quê, quando e de onde. Isso inclui ações realizadas por meio de Console de gerenciamento da AWS, AWS SDKs, ferramentas de linha de comando e outros AWS serviços. CloudTrail responde a perguntas como “Quem encerrou essa EC2 instância?” ou “Quais mudanças foram feitas nessa política do IAM?”

Amazon CloudWatch

- Monitora a integridade operacional e o desempenho de AWS recursos e aplicativos. CloudWatch coleta e rastreia métricas, coleta e monitora arquivos de log e define alarmes. Ele ajuda você a entender o desempenho de seus aplicativos e a responder às mudanças de

desempenho em todo o sistema. CloudWatch responde a perguntas como “A utilização da CPU da minha EC2 instância Amazon está muito alta?” ou “Quantos erros minha função Lambda está gerando?”

Resumo

CloudTrail ajuda você a monitorar e auditar a atividade do usuário para fins de segurança e conformidade, além CloudWatch de monitorar e otimizar o desempenho do sistema e a integridade operacional. Ambas as ferramentas desempenham funções distintas, mas complementares, no gerenciamento de um ambiente de nuvem.

Data collected

AWS CloudTrail

- Concentra-se na captura de registros detalhados de todas as atividades da API em seu AWS ambiente. Isso inclui informações sobre quem fez a chamada à API, quando ela foi feita, a ação tomada e os recursos envolvidos. CloudTrailOs registros da fornecem uma trilha de auditoria abrangente, essencial para rastrear mudanças, garantir a conformidade e investigar incidentes de segurança.

Amazon CloudWatch

- Coleta dados operacionais e de desempenho de seus AWS recursos e aplicativos. Isso inclui métricas como uso da CPU, utilização da memória, tráfego de rede e registros de aplicativos, além de métricas personalizadas que você pode definir. Os dados coletados pelo CloudWatch são usados para monitoramento em tempo real, otimização de desempenho e configuração de alarmes para acionar ações automatizadas com base em condições específicas.

Resumo

CloudTrail coleta dados relacionados à atividade do usuário e ao uso da API para fins de auditoria e segurança, enquanto CloudWatch coleta métricas e registros para monitorar, gerenciar e otimizar o desempenho do sistema e a integridade operacional. Ambos fornecem informações essenciais, mas atendem a diferentes aspectos do gerenciamento da nuvem.

Use cases

AWS CloudTrail

- Usado principalmente para auditoria de segurança, conformidade e auditoria operacional. CloudTrailfornece um registro detalhado das chamadas de API e da atividade do usuário em seu AWS ambiente, tornando-o essencial para rastrear alterações, investigar incidentes de segurança e garantir que sua organização atenda aos requisitos regulatórios. Por exemplo, CloudTrail é útil em cenários em que você precisa monitorar quem acessou recursos específicos, rastrear alterações feitas nas configurações ou auditar atividades em vários Contas da AWS.

Amazon CloudWatch

- Projetado para monitoramento em tempo real, gerenciamento de desempenho e eficiência operacional. CloudWatch é usado para monitorar a integridade de seus AWS recursos e aplicativos coletando e rastreando métricas, registros e eventos. CloudWatch permite que você defina alarmes que acionam ações automatizadas, como escalar recursos ou enviar notificações quando determinados limites são atingidos. Os casos de uso CloudWatch incluem o monitoramento do desempenho do aplicativo, o gerenciamento da utilização de recursos, a detecção de anomalias e a garantia de que seus sistemas estejam funcionando de maneira ideal para evitar o tempo de inatividade.

Security and compliance

AWS CloudTrail

- Crucial para manter a segurança e a conformidade nos AWS ambientes. CloudTrail fornece uma trilha de auditoria abrangente de todas as chamadas de API, incluindo quem fez a chamada, quando ela foi feita e as ações tomadas. Esse registro detalhado é essencial para atender aos padrões de conformidade, conduzir auditorias de segurança e investigar incidentes. Ao rastrear a atividade do usuário e as alterações nos recursos, CloudTrail ajuda a garantir a responsabilidade e a transparência, que são requisitos essenciais para muitas estruturas regulatórias.

Amazon CloudWatch

- Desempenha um papel na segurança, permitindo a detecção de anomalias operacionais. Por exemplo, você pode usar CloudWatch para monitorar métricas que indicam possíveis problemas de segurança, como picos incomuns no tráfego de rede ou no uso da CPU. Além disso, CloudWatch pode acionar alarmes e respostas automatizadas quando determinados

limites são atingidos, permitindo o gerenciamento proativo de incidentes. Os registros capturados também CloudWatch podem ser usados para rastrear eventos operacionais, o que pode ser vital para entender o contexto dos incidentes de segurança.

Resumo

Juntos, CloudTrail fornecem os registros de auditoria necessários para a conformidade e CloudWatch oferecem monitoramento em tempo real que ajuda a detectar e responder às ameaças à segurança, contribuindo para um ambiente de nuvem seguro e compatível.

Log retention

AWS CloudTrail

- Por padrão, o histórico de CloudTrail eventos registra os últimos 90 dias de eventos de gerenciamento da sua conta.
- Os usuários podem criar uma trilha para armazenar registros indefinidamente em um bucket do S3.
- Não há exclusão automática de registros armazenados no Amazon S3, permitindo a retenção a longo prazo.
- Os usuários podem implementar políticas de ciclo de vida em buckets S3 para gerenciar os custos de armazenamento a longo prazo.
- CloudTrail pode ser configurado para enviar registros ao CloudWatch Logs para opções de retenção mais flexíveis.

Amazon CloudWatch

- A retenção de CloudWatch registros no Logs é mais flexível e configurável.
- O período de retenção padrão varia de acordo com o grupo de registros, geralmente definido como “Nunca expira”.
- Os usuários podem definir períodos de retenção personalizados que variam de um dia a 10 anos ou escolher a retenção indefinida.
- Grupos de registros diferentes podem ter períodos de retenção diferentes.
- Após o período de retenção, os registros são excluídos automaticamente para gerenciar os custos de armazenamento.

- CloudWatch Os registros podem ser exportados para o Amazon S3 para armazenamento de longo prazo, se necessário.

Alarms and notifications

AWS CloudTrail

- Concentra-se principalmente no registro da atividade da API e não tem recursos integrados de alarme ou notificação. No entanto, você pode fazer a integração com CloudWatch registros e CloudWatch alarmes para configurar alarmes para CloudTrail eventos. Essa configuração geralmente é usada para alertá-lo sobre eventos relacionados à segurança, como tentativas de acesso não autorizado ou alterações em recursos essenciais.

Amazon CloudWatch

- Projetado especificamente para monitoramento em tempo real e inclui recursos robustos de alarme e notificação. CloudWatch permite que você defina alarmes com base em métricas, dados de registro ou limites personalizados. Quando esses limites são violados, CloudWatch pode enviar notificações via Amazon SNS (Amazon Simple Notification Service), acionar ações automatizadas, como escalar instâncias, ou realizar etapas de remediação personalizadas usando. AWS Lambda Isso é CloudWatch uma ferramenta essencial para o gerenciamento proativo do sistema, alertando você sobre problemas de desempenho ou anomalias operacionais à medida que elas acontecem.

Integration

CloudTrail e CloudWatch oferecem amplas opções de integração com outros AWS serviços e ferramentas externas, aprimorando sua funcionalidade e utilidade.

CloudTrail integrações

- Amazon S3: armazene registros de longo prazo para arquivamento e análise
- CloudWatch Registros: habilite análises e alertas de registros em tempo real
- Amazon EventBridge: acione ações automatizadas com base em eventos de API
- AWS Config: Forneça informações para controle e conformidade da configuração
- AWS Security Hub CSPM: Contribuir para o gerenciamento centralizado da postura de segurança

- AWS Lake Formation: Habilite a governança de CloudTrail registros em data lake
- Amazon Athena: execute consultas SQL em CloudTrail logs armazenados no Amazon S3

CloudWatch integrações

- Amazon SNS: envie notificações para alarmes e eventos
- AWS Lambda: acione funções sem servidor com base em métricas ou registros
- Amazon EC2 Auto Scaling: ajuste a capacidade com base nas métricas de desempenho
- AWS Systems Manager: automatize tarefas operacionais com base em dados CloudWatch
- AWS X-Ray: Combine com dados de rastreamento para obter informações detalhadas sobre a aplicação
- Serviços de contêineres (Amazon ECS, Amazon EKS): monitore aplicativos em contêineres
- Ferramentas de terceiros: exporte métricas e registros para plataformas externas de monitoramento

Cost considerations

AWS CloudTrail

- CloudTrail o preço é baseado principalmente no número de eventos registrados e armazenados. Por padrão, o histórico de CloudTrail eventos registra e armazena, sem cobrança, os últimos 90 dias de eventos de gerenciamento da sua conta. No entanto, se você habilitar eventos de dados (como ações em nível de objeto do S3) ou criar várias trilhas, você incorrerá em cobranças com base no volume de eventos e no armazenamento exigido no Amazon S3. Custos adicionais podem surgir se você usar recursos avançados como o CloudTrail Insights, que fornecem uma análise mais profunda da atividade incomum da API.

Amazon CloudWatch

- CloudWatch tem uma estrutura de preços mais complexa com base em vários fatores, incluindo o número de métricas personalizadas que você monitora, o número de eventos de log ingeridos e armazenados e o uso de alarmes e painéis. O monitoramento básico AWS dos serviços é gratuito, mas o monitoramento detalhado e as métricas personalizadas incorrem em cobranças. O preço do armazenamento de registros é baseado no volume de dados ingeridos e retidos, com custos adicionais para configurar e manter alarmes ou usar o CloudWatch Logs Insights para análise avançada de registros.

Data granularity

AWS CloudTrail

- CloudTrail fornece alta granularidade ao registrar cada chamada de API individual feita em seu AWS ambiente. Cada entrada de registro inclui informações detalhadas, como quem fez a solicitação, a ação executada, os recursos afetados e a hora da ação. Esse nível de detalhe é crucial para auditoria, monitoramento de segurança e conformidade, pois permite rastrear ações e alterações específicas do usuário até a chamada exata da API.

Amazon CloudWatch

- CloudWatch concentra-se em dados agregados para monitoramento e gerenciamento de desempenho. Ele coleta métricas em intervalos regulares (normalmente a cada minuto ou cinco minutos) e registra dados operacionais dos AWS recursos. Embora CloudWatch forneça informações detalhadas sobre o desempenho do sistema e o comportamento do aplicativo, seus dados são mais agregados em comparação com o. CloudTrail Por exemplo, você pode monitorar o uso médio da CPU ao longo do tempo, em vez de solicitações ou ações individuais. CloudWatch No entanto, os registros podem fornecer dados mais granulares semelhantes, CloudTrail mas geralmente são usados para analisar registros operacionais em vez de rastrear chamadas de API.

Real-time tracking

AWS CloudTrail

- CloudTrail não é inerentemente projetado para rastreamento em tempo real, mas pode ser configurado para fornecer near-real-time alertas. Por padrão, CloudTrail registra a atividade da API, mas há um pequeno atraso na entrega dos registros. Para um rastreamento mais imediato, você pode se integrar CloudTrail ao Amazon CloudWatch Events ou AWS Lambda acionar ações com base em chamadas ou atividades de API específicas assim que elas forem registradas. Essa configuração permite o near-real-time monitoramento de eventos críticos de segurança ou alterações na configuração.

Amazon CloudWatch

- CloudWatch, por outro lado, foi desenvolvido para rastrear em tempo real o desempenho do sistema e do aplicativo. Ele monitora continuamente as métricas dos AWS recursos e

pode acionar instantaneamente alarmes ou notificações quando os limites predefinidos são excedidos. CloudWatch também coleta e analisa dados de registro em tempo real, permitindo monitorar registros de aplicativos, detectar anomalias e responder aos problemas operacionais à medida que eles ocorrem. Isso é CloudWatch uma ferramenta essencial para manter a saúde e o desempenho do seu AWS ambiente em tempo real.

Use

Agora que você leu sobre os critérios de escolha entre a Amazon AWS CloudTrail e a Amazon CloudWatch, você pode selecionar o serviço que atende às suas necessidades e usar as informações a seguir para ajudá-lo a começar a usar cada um deles.

AWS CloudTrail

- Começando com AWS CloudTrail

  AWS CloudTrail é um AWS serviço que ajuda você a viabilizar a auditoria operacional e de risco, a governança e a conformidade do seu Conta da AWS. Veja como começar a usá-lo.

  Explore o guia

- Conta da AWS Atividade de revisão

  Saiba como analisar a atividade recente AWS da API no recurso de histórico CloudTrail de eventos de seu Conta da AWS usuário.

  Use o tutorial

- Criar uma trilha

  Saiba como criar uma trilha para registrar a atividade AWS da API em todas as regiões, incluindo dados e eventos do Insights.

  Use o tutorial

- Melhores práticas de segurança em AWS CloudTrail

  Este guia fornece as melhores práticas de segurança preventiva e de detetive para uso AWS CloudTrail em sua organização.

  Explore o guia

Amazon CloudWatch

- Começando com a Amazon CloudWatch

  Monitore seus AWS recursos e os aplicativos em que você executa AWS em tempo real usando a Amazon CloudWatch. Você pode usar CloudWatch para coletar e monitorar métricas, que são variáveis que você pode medir para seus recursos e aplicativos.

  Explore o guia

- Comece a usar o Amazon CloudWatch Metrics

  Este guia discute o monitoramento básico e o monitoramento detalhado, como representar graficamente as métricas e como usar a detecção de CloudWatch anomalias.

  Explore o guia

- Configure o Container Insights no Amazon EKS e no Kubernetes

  Configure o complemento Amazon CloudWatch Observability ESK e o ADTO em seu cluster EKS para o qual enviar métricas. CloudWatch Você também aprenderá como configurar o Fluent Bit ou o Fluentd para enviar registros para o Logs. CloudWatch

  Explore o guia

- Introdução ao Amazon CloudWatch Application Insights

  Aprenda a usar o console para permitir que o CloudWatch Application Insights gerencie seus aplicativos para monitoramento.

  Explore o guia

- Usar o Container Insights

  Saiba como o CloudWatch Container Insights coleta, agrega e resume métricas e registros de seus aplicativos e microsserviços em contêineres.

  Explore o guia

- Configurando o Container Insights no Amazon ECS

  Aprenda a configurar métricas de cluster e de nível de serviço, implantar o ADOT para coletar métricas em nível de EC2 instância e configurar FireLens para enviar CloudWatch registros para o Logs.

Explore o guia

Histórico de documentos para AWS CloudTrail nossa Amazon CloudWatch?

A tabela a seguir descreve as mudanças importantes nesse guia de decisão. Para receber notificações sobre atualizações deste guia, você pode assinar um feed RSS.

Alteração	Descrição	Data
Lançamento inicial	Lançamento inicial do guia de decisão.	20 de setembro de 2024

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.