Serviços de monitoramento e registro em log

Amazon CloudWatch

O Amazon CloudWatch é um serviço de monitoramento para recursos de nuvem da AWS e os aplicativos que você executa na AWS.

CloudWatch é para monitoramento de desempenho (CloudTrail é para auditoria).

Usado para coletar e rastrear métricas, coletar e monitorar arquivos de log e definir alarmes.

Reaja automaticamente às alterações em seus recursos da AWS.

Monitore recursos como:

- instâncias EC2.
- Tabelas do DynamoDB.
- Instâncias de banco de dados RDS.
- Métricas personalizadas geradas por aplicativos e serviços.
- Quaisquer arquivos de log gerados por seus aplicativos.

Obtenha visibilidade de todo o sistema sobre a utilização de recursos.

O monitoramento do CloudWatch inclui o desempenho do aplicativo.

Monitorar a saúde operacional.

O CloudWatch é acessado por meio de API, interface de linha de comando, SDKs da AWS e Console de gerenciamento da AWS.

O CloudWatch se integra ao IAM.

O Amazon CloudWatch Logs permite monitorar e solucionar problemas de seus sistemas e aplicativos usando seu sistema existente, aplicativo e arquivos de log personalizados.

O CloudWatch Logs pode ser usado para monitoramento de aplicativos e sistemas em tempo real, bem como retenção de logs de longo prazo.

O CloudWatch Logs mantém os logs indefinidamente por padrão.

Os logs do CloudTrail podem ser enviados ao CloudWatch Logs para monitoramento em tempo real.

Os filtros de métrica do CloudWatch Logs podem avaliar os logs do CloudTrail para termos, frases ou valores específicos.

O CloudWatch retém dados de métrica da seguinte forma:

- Os pontos de dados com um período inferior a 60 segundos ficam disponíveis por 3 horas. Esses pontos de dados são métricas personalizadas de alta resolução.
- Os pontos de dados com um período de 60 segundos (1 minuto) ficam disponíveis por 15 dias.
- Pontos de dados com um período de 300 segundos (5 minutos) estão disponíveis por 63 dias.
- Pontos de dados com um período de 3600 segundos (1 hora) estão disponíveis por 455 dias (15 meses).

Os painéis permitem que você crie, personalize, interaja e salve gráficos de recursos da AWS e métricas personalizadas.

Os alarmes podem ser usados para monitorar qualquer métrica do Amazon CloudWatch em sua conta.

Eventos são um fluxo de eventos do sistema que descrevem alterações em seus recursos da AWS.

Os logs ajudam você a agregar, monitorar e armazenar logs.

Monitoramento básico = 5 minutos (gratuito para instâncias EC2, volumes EBS, ELBs e bancos de dados RDS).

Monitoramento detalhado = 1 min (carregável).

As métricas são fornecidas automaticamente para vários produtos e serviços da AWS.

Não há métrica padrão para uso de memória em instâncias do EC2.

Uma métrica personalizada é qualquer métrica que você fornece ao Amazon CloudWatch (por exemplo, tempo para carregar uma página da Web ou desempenho do aplicativo).

Opções para armazenar logs:

- Registros do CloudWatch.
- Sistema de registro centralizado (por exemplo, Splunk).
- Script personalizado e armazenamento no S3.

Não armazene logs em discos não permanentes:

A prática recomendada é armazenar logs no CloudWatch Logs ou S3.

A assinatura do CloudWatch Logs pode ser usada em várias contas da AWS (usando acesso entre contas).

O Amazon CloudWatch usa o Amazon SNS para enviar e-mail.

AWS CloudTrail

AWS CloudTrail é um serviço da web que registra a atividade feita em sua conta e entrega arquivos de log para um bucket do Amazon S3.

CloudTrail é para auditoria (CloudWatch é para monitoramento de desempenho).

CloudTrail trata do registro e salva um histórico de chamadas de API para sua conta da AWS.

Fornece visibilidade da atividade do usuário ao registrar as ações realizadas em sua conta.

O histórico da API permite análise de segurança, rastreamento de alterações de recursos e auditoria de conformidade.

Chamadas de API de logs feitas por meio de:

- Console de gerenciamento da AWS.
- SDKs da AWS.
- Ferramentas de linha de comando.
- Serviços da AWS de nível superior (como CloudFormation).

O CloudTrail registra a atividade da conta e os eventos de serviço da maioria dos serviços da AWS e registra os seguintes registros:

- A identidade do chamador da API.
- A hora da chamada da API.
- O endereço IP de origem do chamador da API.
- Os parâmetros de solicitação.
- Os elementos de resposta retornados pelo serviço da AWS.

CloudTrail é habilitado por padrão.

CloudTrail é por conta da AWS.

Você pode consolidar logs de várias contas usando um bucket do S3:

Ative o CloudTrail na conta paga. Crie uma política de bucket que permita acesso entre contas. Ative o CloudTrail nas outras contas e use o bucket na conta paga. Você pode integrar o CloudTrail ao CloudWatch Logs para entregar eventos de dados capturados pelo CloudTrail a um fluxo de log do CloudWatch Logs.

O recurso de validação de integridade do arquivo de log do CloudTrail permite determinar se um arquivo de log do CloudTrail foi inalterado, excluído ou modificado desde que o CloudTrail o entregou ao bucket especificado do Amazon S3.