

Exam Readiness: AWS Certified Security Specialty (Portuguese)

25% CONCLUIR

▼ CONTEÚDO MODULAR

≡ Introdução



Para o exame, você deve saber como:

- 1 Projetar e implementar monitoramento e alertas de segurança.
- 2 Solucionar problemas de monitoramento e alerta de segurança.
- 3 Projetar e implementar uma solução de logs.
- 4 Solucionar problemas de soluções de logs.

Logs e monitoramento

Este vídeo apresenta os principais tópicos no domínio Logs e monitoramento.

Domínio 2:
Registro e monitoramento

aws training and certification

© 2022, Amazon Web Services, Inc. ou suas afiliadas. Todos os direitos reservados.

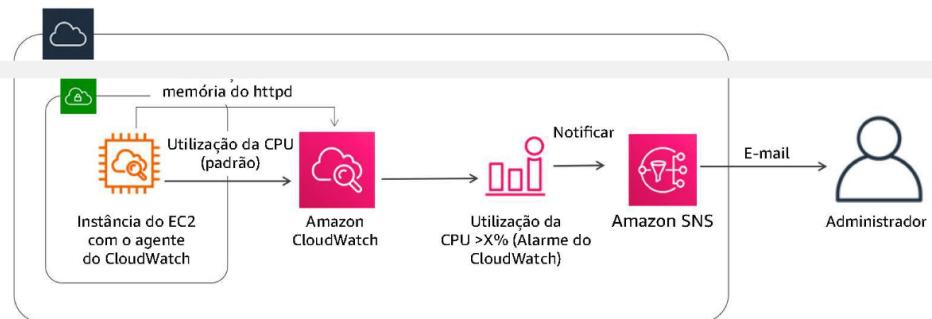
Ferramentas da AWS para monitoramento

 Amazon CloudWatch	 AWS Config	 AWS CloudTrail
--	--	---

Modelo de responsabilidade compartilhada

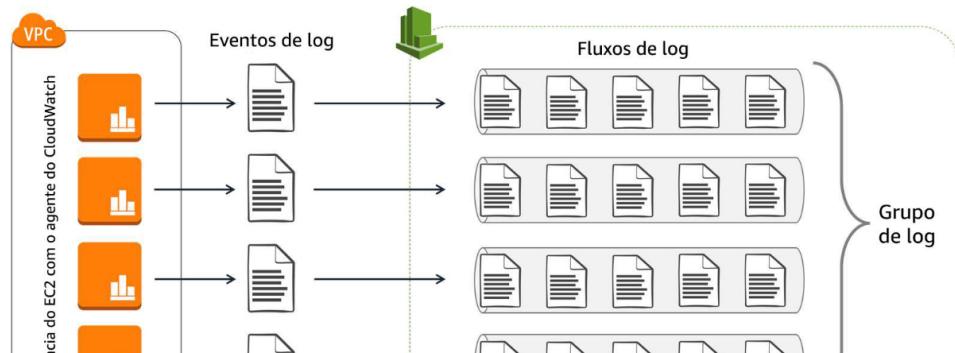


Como o CloudWatch funciona



Para obter mais informações sobre a arquitetura e os conceitos do CloudWatch, consulte https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/cloudwatch_architecture.html.

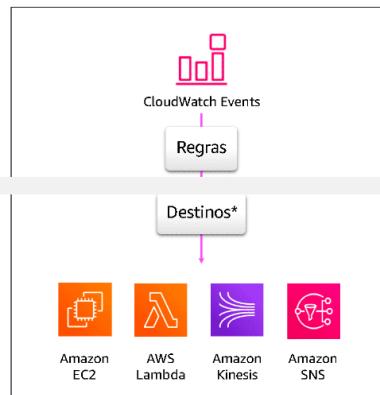
Como o CloudWatch Logs funciona





Depois que o agente do CloudWatch for instalado, iniciado e tiver os filtros de métrica configurados, a instância ou o servidor que está sendo monitorado enviará eventos de log para o CloudWatch Logs.

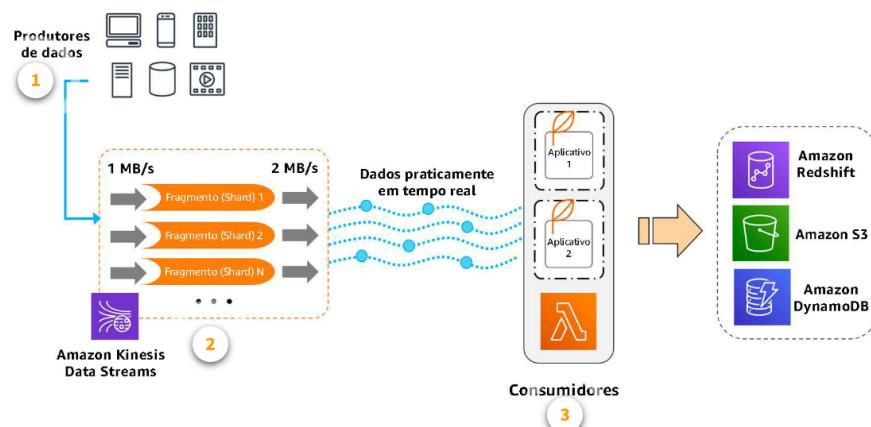
Como funciona o Eventos do CloudWatch



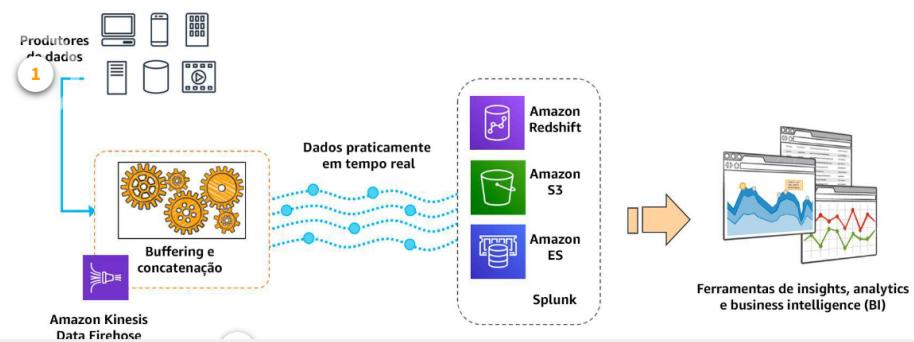
- Um *evento* é uma mudança no seu ambiente AWS.
- As *regras* direcionam os dados do evento para o alvo adequado.
- O *alvo* é o serviço que processa o evento.

Para obter uma lista completa de todas as metas de eventos CloudWatch compatíveis, consulte <https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/WhatIsCloudWatchEvents.html>.

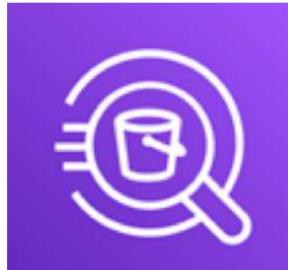
Visão geral: Amazon Kinesis Data Streams



Visão geral: Amazon Kinesis Data Firehose



Amazon Athena



Fornece um serviço de consulta interativa para analisar dados no Amazon S3 usando SQL padrão.

- Sem servidor
- Consultas entre regiões são suportadas
- Não há necessidade de carregar ou agragar dados
- Usa Presto e Apache Hive

<https://aws.amazon.com/athena/>

Exemplo de pergunta 1

Você precisa criar uma estratégia de logs para as contas da sua empresa. Os dados de logs devem ser mantidos seguros e ser facilmente utilizáveis por 90 dias. Após 90 dias, o log provavelmente não será mais necessário, mas ainda deve ser mantido para conformidade por 10 anos.

Qual solução garante que os logs sejam retidos com segurança durante toda a duração necessária da maneira mais econômica?

Você precisa criar uma estratégia de registro em log para as contas da sua empresa. Os dados de registro devem ser armazenados de forma segura e ser facilmente utilizáveis por 90 dias. Após 90 dias, o log provavelmente não será mais necessário, mas ainda deve ser mantido para conformidade por 10 anos.

Qual solução garante que os logs sejam retidos com segurança durante toda a duração necessária da maneira mais econômica?

- Ⓐ Enviar todos os logs para um bucket do Amazon S3 de uma conta de log central. Garantir que o bucket esteja protegido com uma política que permita acesso somente leitura aos administradores de segurança, negando todos os outros acessos. Criar uma política de ciclo de vida que exclua os dados automaticamente após 10 anos.

- Ⓑ Importar todos os logs para o Amazon Redshift usando fluxos de dados do Kinesis. Criar uma política de ciclo de vida que move automaticamente os dados para o Amazon S3 Glacier após 90 dias e exclua automaticamente os dados de log após 10 anos.

- Ⓒ Enviar todos os logs para um bucket do Amazon S3 de uma conta de log central. Garantir que o bucket esteja protegido

 com uma política que permita acesso somente leitura aos administradores de segurança, negando todos os outros acessos. Criar uma política de ciclo de vida que mova automaticamente os dados para o Amazon S3 Glacier após 90 dias e exclua automaticamente os dados de log após 10 anos.

-  D. Enviar todos os logs para um arquivo do Amazon S3 de uma conta de log central. Garantir que o arquivo esteja protegido com uma política de recursos que permita acesso somente leitura aos administradores de segurança, negando todos os outros acessos. Criar uma política de ciclo de vida que exclua automaticamente os dados de log após 10 anos. Garantir que todas as solicitações de dados usem as recuperações expressas do Glacier para garantir a entrega rápida dos dados de log.



Correto

REFAZER



Continue com uma explicação da resposta.