elastic

O Guia do Elastic Observability para AWS

elastic.co/pt →

Índice

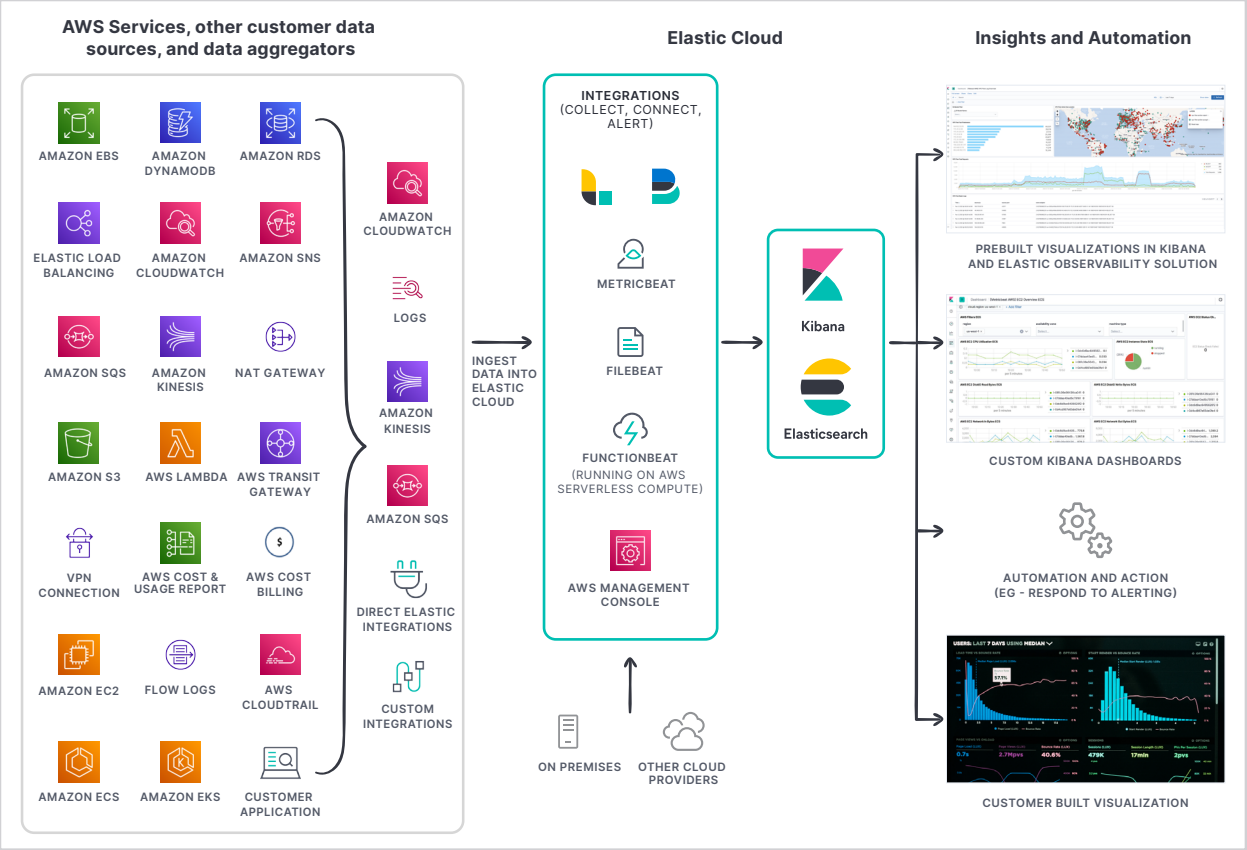
Introdução

Gerar insights e ações com base em dados é essencial para se beneficiar totalmente da agilidade e da flexibilidade proporcionadas pela nuvem. Com a solução de observabilidade da Elastic, você pode unificar a visibilidade em todos os seus ambientes locais e da AWS, permitindo uma melhor compreensão da disponibilidade, do desempenho e da integridade geral de sua infraestrutura, aplicações e negócios.

A AWS oferece uma ampla gama de logs e métricas em seus serviços de nuvem para você monitorar sua implantação de nuvem e tomar decisões mais informadas. O Elastic Observability se integra a essas fontes de dados para reunir seus dados de maneira unificada, permitindo que você obtenha insights práticos sobre a TI, operações e negócios continuamente. Analise facilmente seus dados em dashboards e ferramentas pré-criados ou crie visualizações customizadas para poder reagir rapidamente em relação às suas necessidades de negócios.

Este guia explica como configurar da melhor forma o Elastic Observability com serviços da AWS para que você possa monitorar com mais eficácia e reagir mais rapidamente aos eventos conforme eles ocorrem. Continue lendo para saber mais sobre esses serviços da AWS, os benefícios de usar a Elastic para monitoramento e as práticas recomendadas que podem ajudar a maximizar o valor dos seus investimentos em ambos.

Com a Elastic, você aproveita melhor os seus dados da AWS



Monitore e analise o Amazon CloudWatch Logs com a Elastic

Centralize os logs de toda a sua infraestrutura, aplicações e serviços da AWS que você usa em um único serviço escalável com o Amazon CloudWatch.

Com o Amazon CloudWatch Logs, você pode, de forma rápida e fácil:

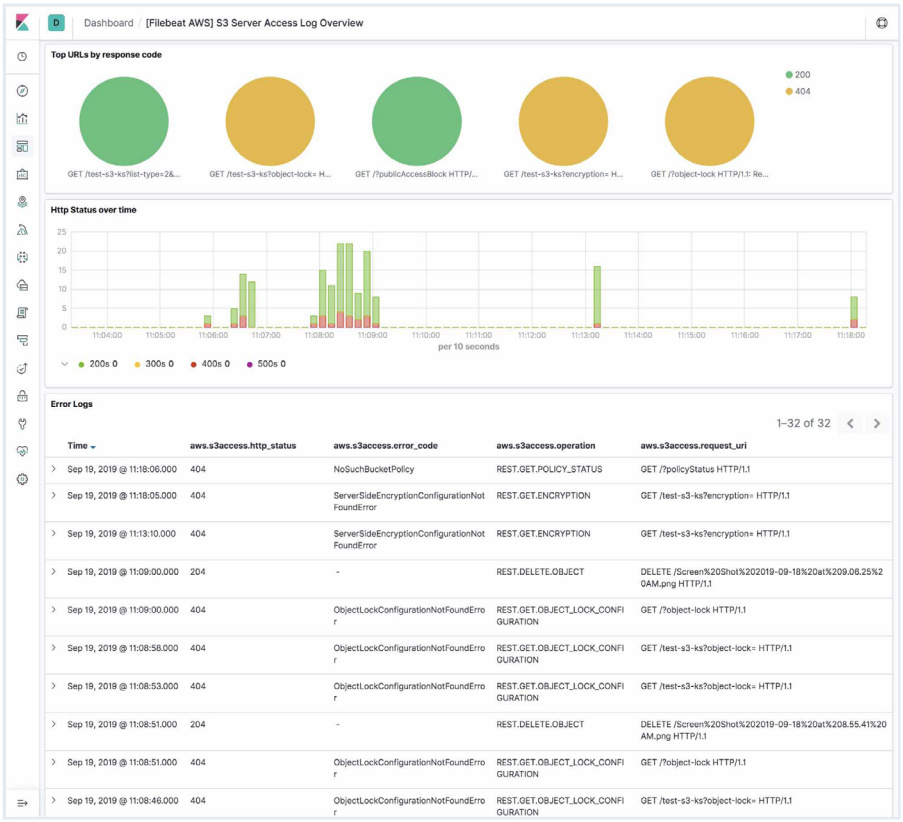
Reunir, armazenar e acessar arquivos de log de fontes distintas

Monitorar a integridade e o desempenho da infraestrutura e das aplicações

Observar o Amazon CloudWatch Logs diretamente de diferentes grupos de log da AWS

elastic

Como enviar Amazon CloudWatch Logs para a Elastic:



Primeiro, você precisará coletar informações sobre o seu ambiente da AWS e a sua implantação do Elastic Cloud. Consulte o **Apêndice A** abaixo para saber detalhes sobre esses pré-requisitos. Para começar a usar o Amazon CloudWatch Logs, siga as etapas no **Apêndice B** abaixo para obter um passo a passo com detalhes de como:

1. Configurar um bucket do Amazon Simple Storage Service (Amazon S3) e criar uma fila do Amazon Simple Queue Service (Amazon SQS)
2. Baixar e instalar o Filebeat
3. Conectar ao Elastic Stack
4. Configurar o Filebeat para coletar Amazon CloudWatch Logs
5. Habilitar e configurar os seus módulos de coleta de dados
6. Definir os seus dashboards do Kibana pré-configurados e iniciar o Filebeat
7. Analisar dados do Amazon CloudWatch no Kibana

Analise a atividade de log do Amazon S3 e monitore o acesso com a Elastic

O Amazon S3 permite que você armazene dados e aplicações de negócios, além de hospedar websites estáticos. Com o Amazon S3, há dois tipos de fluxos de trabalho que você pode implementar: a coleta de logs customizados armazenados com o Amazon S3 e o monitoramento de métricas e acesso a serviços do Amazon S3.

Use a Elastic com o Amazon S3 para:

Capturar detalhes de solicitações como IP remoto, solicitante, nome do bucket e outros para entender melhor a natureza do tráfego em relação aos seus buckets

Estabelecer linhas de base, analisar padrões de acesso e identificar tendências nos dashboards predefinidos do Kibana

Identificar problemas de segurança e conformidade, bem como conduzir análises de causa raiz em sua organização

Analisar logs customizados específicos de uma determinada aplicação ou negócio armazenados no **Amazon S3**

Como enviar logs do Amazon S3 para a Elastic:

Primeiro, você precisará coletar informações sobre seu ambiente da AWS, bem como sobre sua implantação do Elastic Cloud. Consulte o **Apêndice A** para saber mais detalhes sobre esses pré-requisitos. Para começar a usar os logs do Amazon S3, siga as etapas do passo a passo no **Apêndice B** com detalhes de como:

1. Configurar um bucket do Amazon S3 e criar uma fila do Amazon SQS
2. Baixar e instalar o Filebeat
3. Conectar ao Elastic Stack
4. Habilitar e configurar os seus módulos de coleta de dados
5. Configurar o Filebeat para coletar logs do Amazon S3
6. Definir os seus dashboards do Kibana pré-configurados e iniciar o Filebeat
7. Analisar dados de log do Amazon S3 no Kibana

Transmita dados para o Elasticsearch com o Amazon Kinesis

O Amazon Kinesis é um serviço totalmente gerenciado para fornecer fontes de dados de streaming em tempo real para destinos como o Amazon S3 e a Elastic.

Com o Amazon Kinesis, você pode:

Transmitir logs em tempo real e analisá-los com o Elasticsearch e o Kibana para obter insights rapidamente e tomar decisões mais informadas

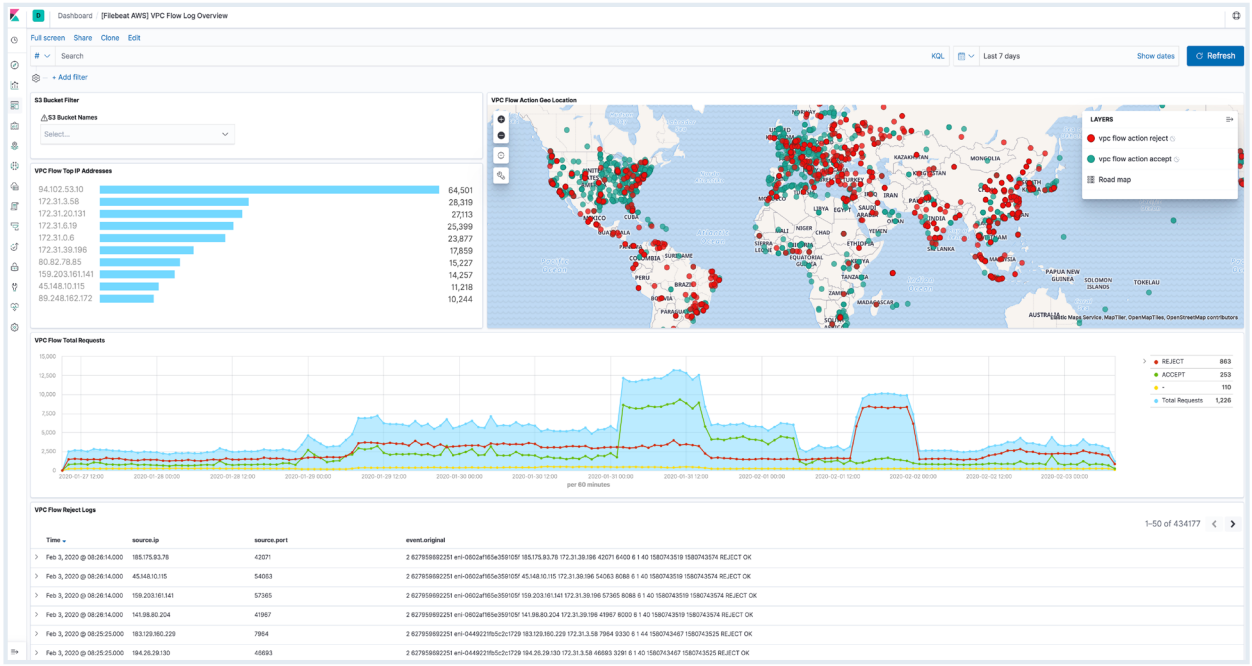
Compactar, converter e criptografar os dados em trânsito para reduzir a quantidade de armazenamento usado e, ao mesmo tempo, aumentar a segurança

Como transmitir dados para a Elastic usando o Amazon Kinesis:

Você precisará de informações sobre seu ambiente da AWS, bem como sobre sua implantação do Elastic Cloud antes de começar. Consulte o **Apêndice A** para saber mais detalhes sobre esses pré-requisitos. Para começar a usar o Amazon Kinesis, siga as etapas do passo a passo no **Apêndice C** com detalhes de como:

1. Baixar e instalar o Metricbeat
2. Conectar ao Elastic Stack
3. Configurar o Metricbeat para transmitir dados
4. Habilitar e configurar os seus módulos de coleta de dados
5. Definir os seus dashboards do Kibana pré-configurados e iniciar o Filebeat
6. Analisar dados no Kibana

Monitore o tráfego de rede com Amazon VPC Flow Logs e a Elastic



O Elastic Observability permite buscar, visualizar e filtrar logs de fluxo da Amazon Virtual Private Cloud (Amazon VPC) rapidamente para monitorar o tráfego de rede na Amazon VPC com o Kibana. Com essa integração, você pode analisar os dados do log de fluxo e compará-los com as configurações do grupo de segurança para manter e melhorar a segurança da nuvem.

A ingestão de Amazon VPC Flow Logs na Elastic permite:

Realizar uma análise melhor para tomar decisões mais informadas

Avaliar as regras dos grupos de segurança e descobrir brechas na segurança

Definir alarmes que alertam quando certos tipos de tráfego são detectados

Identificar problemas de latência e estabelecer linhas de base para garantir um desempenho consistente

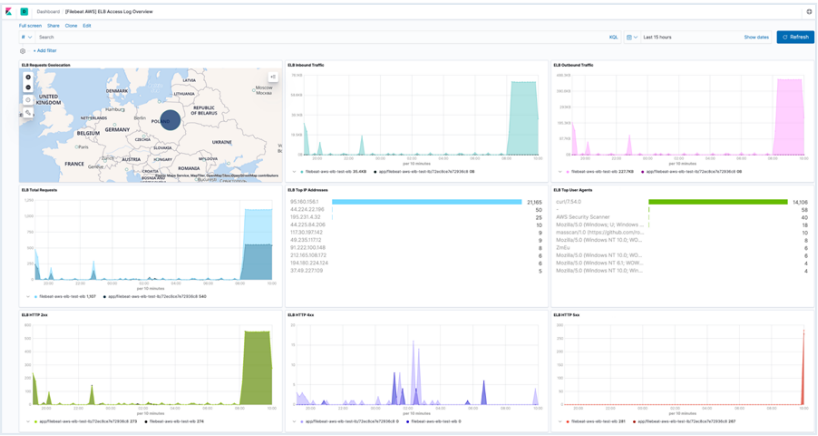
elastic

Como ingerir logs do Amazon VPC na Elastic:

Comece reunindo informações sobre seu ambiente da AWS, bem como sobre sua implantação do Elastic Cloud. Consulte o **Apêndice A** para saber mais detalhes sobre esses pré-requisitos. Para começar a usar Amazon VPC Flow Logs, siga as etapas do passo a passo no **Apêndice B** com detalhes de como:

1. Configurar um bucket do Amazon S3 e criar uma fila do Amazon SQS
2. Baixar e instalar o Filebeat
3. Conectar ao Elastic Stack
4. Configurar o Filebeat para coletar Amazon VPC Flow Logs
5. Habilitar e configurar os seus módulos de coleta de dados
6. Definir os seus dashboards do Kibana pré-configurados e iniciar o Filebeat
7. Analisar logs no Kibana

Observe as operações de balanceamento de carga na Elastic com o Amazon ELB



O serviço Elastic Load Balancing (ELB) na AWS permite balancear automaticamente o tráfego de rede em um conjunto de recursos de nuvem.

Ao centralizar os logs do ELB com a Elastic, você pode:

Observar informações detalhadas sobre as solicitações enviadas ao balanceador de carga

Analisar os padrões de tráfego para descobrir problemas de desempenho

Fazer uma avaliação detalhada dos logs do ELB para descobrir respostas do servidor etc.

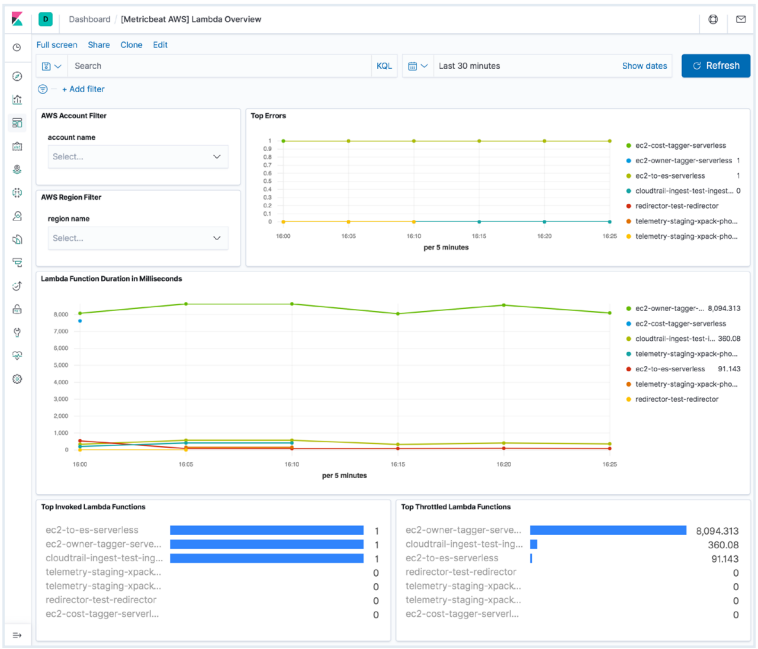
elastic

Como enviar dados do Elastic Load Balancing para a Elastic:

Antes de começar, você precisará coletar algumas informações sobre seu ambiente da AWS, bem como sobre sua implantação do Elastic Cloud. Consulte o **Apêndice A** para saber mais detalhes sobre esses pré-requisitos. Para começar a usar o ELB na AWS, siga as etapas do passo a passo no **Apêndice B** com detalhes de como:

1. Configurar um bucket do Amazon S3 e criar uma fila do Amazon SQS
2. Baixar e instalar o Filebeat
3. Conectar ao Elastic Stack
4. Configurar o Filebeat para coletar logs do ELB na AWS
5. Habilitar e configurar os seus módulos de coleta de dados
6. Definir os seus dashboards do Kibana pré-configurados e iniciar o Filebeat
7. Analisar logs do ELB no Kibana

Otimize os fluxos de trabalho operacionais usando o AWS Lambda na Elastic



Com o AWS Lambda, você pode aproveitar as vantagens de um serviço de computação sem servidor que permite executar códigos dinamicamente em resposta a eventos e otimizar fluxos de trabalho operacionais. Execute tarefas de computação, gerencie automaticamente seus recursos com código para qualquer aplicação e beneficie-se de não precisar de nenhuma tarefa administrativa.

Ao usar o AWS Lambda na Elastic, você pode:

Monitorar o desempenho de diferentes aplicações sem servidor

Processar logs e métricas em tempo real

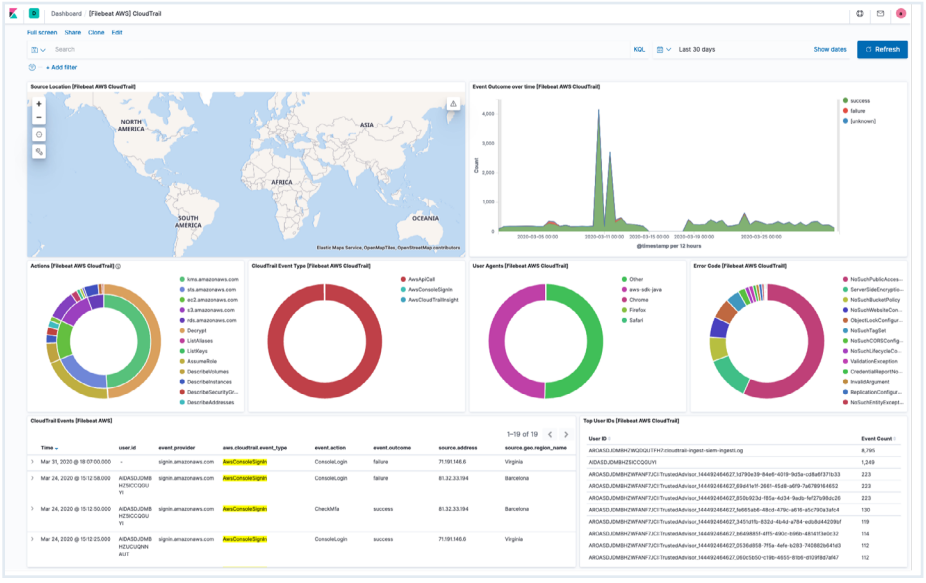
Capturar dados de desempenho e correlacioná-los com soluções da Elastic

Como começar a usar o AWS Lambda na Elastic:

Primeiro, reúna informações sobre o seu ambiente da AWS, bem como sobre a sua implantação do Elastic Cloud. Consulte o **Apêndice A** para saber mais detalhes sobre esses pré-requisitos. Para começar a usar o AWS Lambda, siga as etapas do passo a passo no **Apêndice D** com detalhes de como:

1. Baixar e instalar o Functionbeat
2. Conectar ao Elastic Stack
3. Configurar funções de nuvem
4. Habilitar e configurar módulos de coleta de dados
5. Definir ativos e implantar o Functionbeat
6. Criar dashboards do Kibana para análise

Garanta os padrões de governança e conformidade com o AWS CloudTrail na Elastic



elastic

O AWS CloudTrail possibilita governança, conformidade, auditoria operacional e auditoria de risco da sua conta da AWS.

Ao centralizar os logs do AWS CloudTrail na Elastic, você pode facilmente:

Visualizar seus logs do AWS CloudTrail, bem como a atividade da conta e do usuário, em dashboards pré-criados do Kibana para uma análise mais rápida

Registrar informações sobre todas as ações tomadas para controlar alterações e resolver problemas

Proteger e monitorar suas conexões de rede

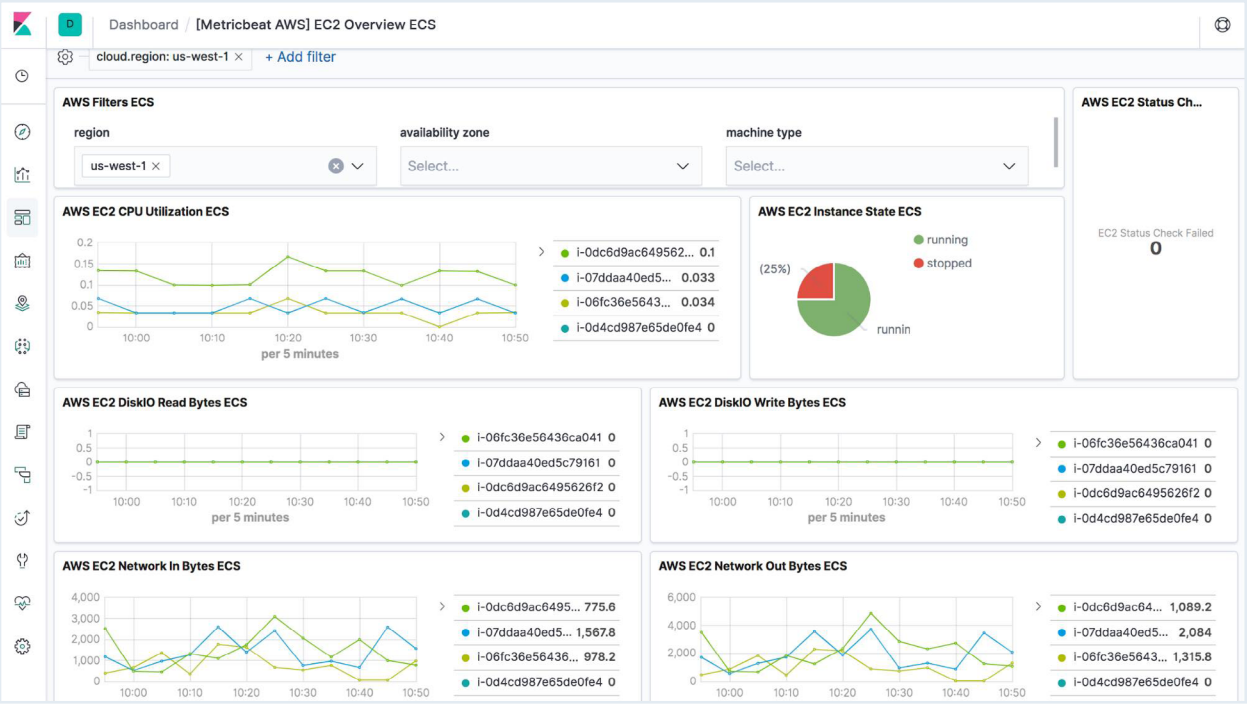
Garantir a conformidade com normas e políticas regulatórias

Como ingerir dados do AWS CloudTrail no Elastic:

Antes de começar, você precisará coletar algumas informações sobre o seu ambiente da AWS, bem como sobre a sua implantação do Elastic Cloud. Consulte o **Apêndice A** para saber mais detalhes sobre esses pré-requisitos. Para começar a usar o AWS CloudTrail, siga as etapas do passo a passo no **Apêndice B** com detalhes de como:

1. Configurar um bucket do Amazon S3 e criar uma fila do Amazon SQS
2. Baixar e instalar o Filebeat
3. Conectar ao Elastic Stack
4. Configurar o Filebeat para coletar logs do AWS CloudTrail
5. Habilitar e configurar os seus módulos de coleta de dados
6. Definir os seus dashboards do Kibana pré-configurados e iniciar o Filebeat
7. Analisar logs do AWS CloudTrail no Kibana

Ingira e unifique métricas em todo o seu ambiente da AWS para obter insights abrangentes



Com as integrações e os dashboards pré-criados da Elastic para AWS, você pode coletar métricas da AWS como uso, desempenho, faturamento e outras para ver como cada sinal se correlaciona, permitindo que você tome decisões de negócios mais informadas.

Por meio do monitoramento e análise contínuos das suas métricas de computação, armazenamento, rede e dados da AWS, você pode reagir rapidamente conforme suas necessidades de negócios evoluem:

- Amazon Relational Database Service (Amazon RDS)
- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Gateway de conversão de endereços de rede (NAT) da Amazon VPC
- Amazon CloudWatch
- Amazon S3
- Amazon DynamoDB
- Amazon Simple Notification Service (SNS)
- Amazon SQS
- Relatório de custo e uso da AWS
- AWS Billing and Cost Management
- AWS Virtual Private Network (AWS VPN)
- AWS Transit Gateway

elastic

As métricas da AWS ajudam a realizar uma análise abrangente, permitindo que você tome decisões mais informadas com a capacidade de:

Correlacionar métricas entre serviços de computação, armazenamento e dados para resolução de problemas de maneira unificada

Avaliar restrições de capacidade, desempenho e uso para tomar decisões holísticas de redimensionamento

Monitorar e manter uma implantação de nuvem otimizada com análise e alerta automatizados, usando um conjunto de dados unificado

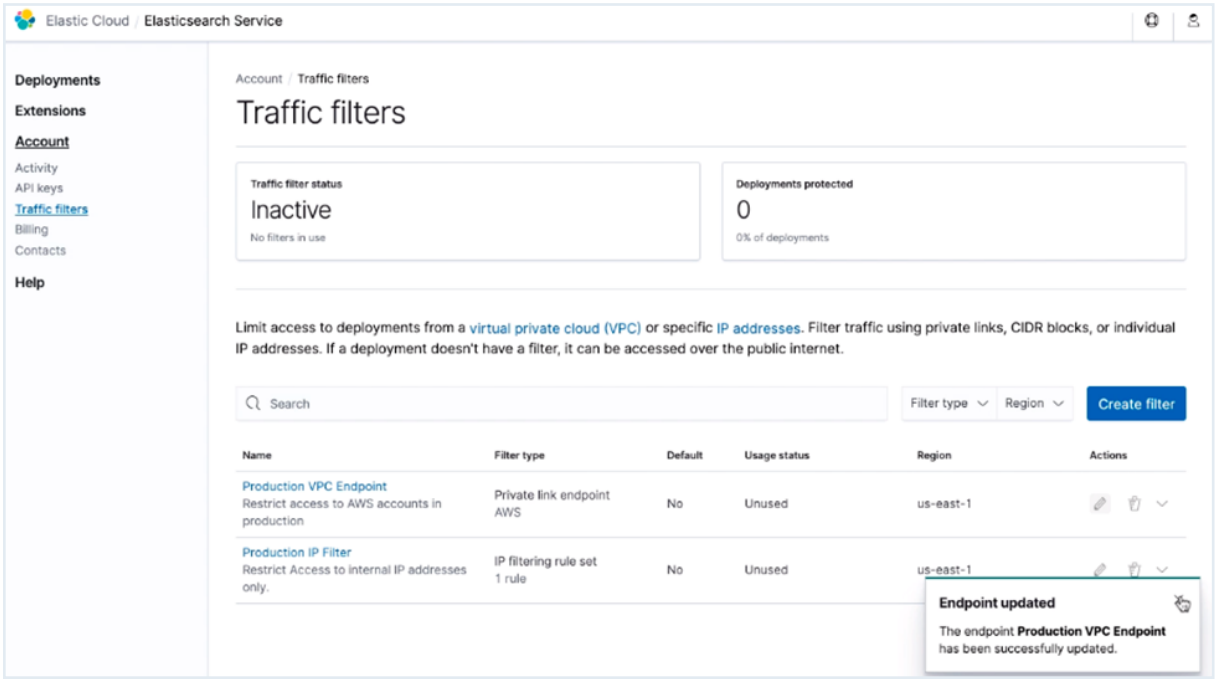
Como começar a usar as métricas da AWS e dashboards customizados:

Você precisará de informações sobre seu ambiente da AWS, bem como sobre sua implantação do Elastic Cloud antes de começar. Consulte o **Apêndice A** para saber mais detalhes sobre esses pré-requisitos. Para começar a criar o seu dashboard, siga as etapas do passo a passo no **Apêndice C** com detalhes de como:

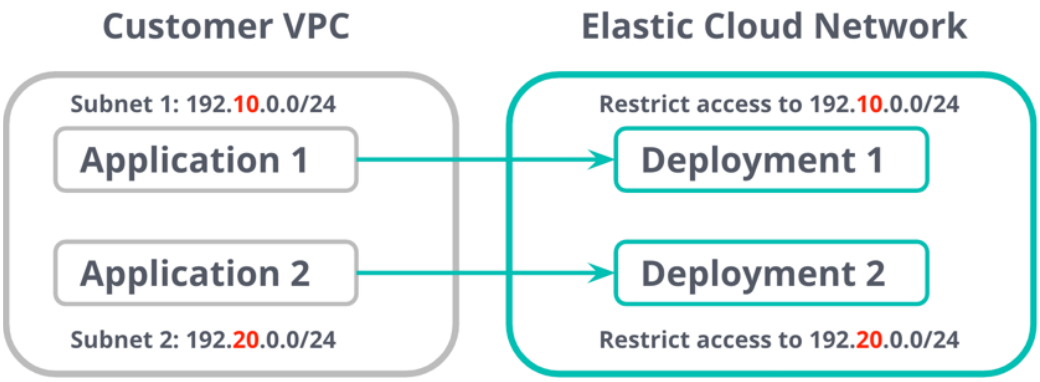
1. Baixar e instalar o Metricbeat
2. Conectar ao Elastic Stack
3. Configurar o Metricbeat para coletar métricas
4. Habilitar e configurar os seus módulos de coleta de dados
5. Definir os seus dashboards do Kibana pré-configurados e iniciar o Filebeat
6. Analisar métricas no Kibana

Para saber como criar um dashboard customizado para atender às suas necessidades, consulte a nossa **documentação**. Você também pode assistir a este rápido **tutorial em vídeo**.

Obtenha mais segurança e flexibilidade da Elastic usando o AWS PrivateLink



O AWS PrivateLink fornece conectividade segura entre as suas Amazon VPCs, outros recursos da AWS e aplicações locais. Isso facilita a proteção das conexões de rede entre as suas aplicações e a implantação da Elastic. O tráfego entre a rede virtual e a implantação da Elastic viaja pela rede da AWS em vez da Internet pública, eliminando a exposição de dados e fornecendo segurança adicional.



Com o AWS PrivateLink, você pode:

Criar endpoints com endereços IP privados, para que as cargas de trabalho pareçam estar em execução dentro da sua rede

Garantir que todo o tráfego permaneça dentro da rede da Amazon e não saia em nenhum ponto

Beneficiar-se do gerenciamento de rede simplificado para não precisar mais manter uma infraestrutura complexa (gateways NAT, controles de acesso)

Restringir o tráfego das redes virtuais do cliente para o endpoint (o tráfego do AWS PrivateLink é unidirecional, ao contrário do tráfego no emparelhamento da Amazon VPC, que é bidirecional)

Como começar a usar o AWS PrivateLink:

Confira a nossa **documentação** para obter instruções passo a passo.

elastic

Por que a Elastic?

Implante as soluções da Elastic para trazer um conjunto de recursos complementares para a nuvem que ajudam a maximizar o valor dos seus investimentos na AWS.

O Elastic Observability e seus recursos de plataforma de busca subjacentes complementam as inovações da infraestrutura de nuvem

Desde seus primórdios, a Elastic entregou um fluxo constante de inovações em busca e análise de dados e redefiniu o valor da busca. A Elastic, a empresa que criou o Elasticsearch e o Kibana, está sempre adicionando novos recursos, atualizações de segurança e melhorias de desempenho a esses produtos. As inovações da Elastic em busca na camada da aplicação de software complementam as inovações da AWS na camada da infraestrutura de nuvem. Com a combinação de ambas, você pode responder rapidamente aos dados operacionais e de negócios, o que contribui para que a sua organização se torne mais ágil e orientada por dados.

Escolha e flexibilidade entre provedores de serviços em nuvem e ambientes locais

A plataforma de busca da Elastic foi construída para dar aos desenvolvedores e clientes flexibilidade de execução no local de sua escolha. Fortes investimentos permitem que isso agregue recursos essenciais à plataforma e, ao mesmo tempo, desenvolva integrações profundas na nuvem. A plataforma de busca da Elastic também oferece uma experiência consistente na nuvem e no local. Essa consistência híbrida é valiosa à medida que você aumenta gradualmente o uso da nuvem, um processo que pode levar anos em empresas de grande porte.

A consistência entre várias nuvens também poderá facilitar a expansão da sua solução se você optar por expandir seu uso da nuvem adicionando os melhores serviços de diferentes provedores. Isso é particularmente valioso para casos de uso de observabilidade e segurança, nos quais uma visão unificada entre os locais pode ajudar os clientes a acelerar a solução de problemas e reduzir os riscos.

Soluções de busca empresarial, observabilidade e segurança prontas para uso

A Elastic oferece aplicações pré-criadas e prontas para casos de uso do Enterprise Search, incluindo Workplace Search, App Search e Site Search; casos de uso do Observability, incluindo logging e monitoramento de performance de aplicação (APM); e casos de uso do Security, incluindo SIEM e proteção de endpoint.

Todos os recursos e integrações externas que possibilitam essas aplicações específicas das soluções são incorporados à plataforma de busca da Elastic e estão disponíveis para os clientes que optam por criar suas próprias aplicações customizadas de acordo com suas necessidades. Isso inclui integrações amplas para ingerir os dados necessários para as soluções Observability e Security na AWS.

Comunidade e talento técnico

A plataforma de busca da Elastic é um padrão de fato para soluções baseadas em busca. A comunidade Elasticsearch no GitHub tem mais de 1.500 membros. Além disso, os conjuntos de habilidades relacionados ao Elasticsearch e ao Kibana estão bem estabelecidos no mercado. O Elasticsearch também inclui integrações prontamente disponíveis para fontes de dados e aplicações adjacentes comumente usadas. A combinação do Elastic Observability com a AWS dá a você a possibilidade de usar esses recursos — o pool de talentos, as integrações e a comunidade Elasticsearch colaborativa — enquanto você expande a sua solução baseada em busca.

Como se conectar com a comunidade Elastic

Fóruns de discussão

Encontre conselhos ou ajude o próximo. Faça as suas perguntas mais urgentes sobre todos os assuntos da Elastic e compartilhe seus conhecimentos com outros usuários nos nossos **fóruns de discussão**, que também estão disponíveis no seu idioma nativo.

Slack e comunidades locais

Entre no nosso **Elastic Slack**, que está crescendo rapidamente, para conversar com outros usuários e pedir conselhos em vários canais: #elasticsearch, #kubernetes, #kibana-development e outros.

Além disso, surgiram muitas **outras comunidades online** no mundo todo! Participe de uma na sua região para compartilhar sua história na Elastic com a comunidade local.

Continue aprendendo

Está começando agora com o Elastic Stack? Procurando análises detalhadas? Coloque a mão na massa com o **repositório de exemplos da Elastic** e explore conjuntos de dados selecionados e instruções passo a passo. Além disso, veja o que está circulando na nossa equipe de desenvolvimento por meio do nosso **boletim informativo da comunidade**.

Adoraríamos ouvir você

A tecnologia evolui, e a Elastic também. Ouvir a nossa comunidade é realmente muito importante para nós. **Entre em contato conosco** para obter ajuda ou compartilhar feedback sobre a sua experiência com a Elastic.

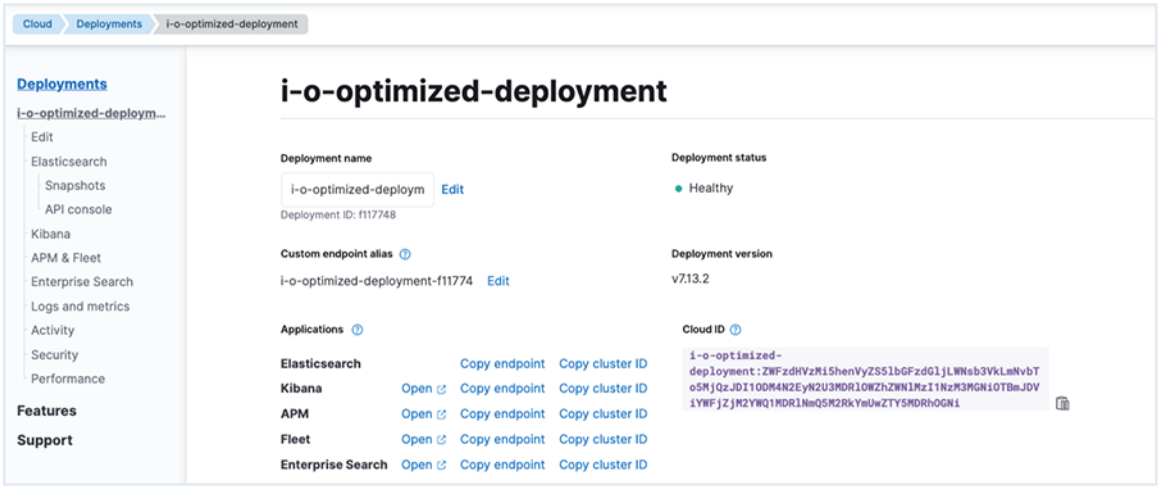
Apêndice A — Pré-requisitos para começar

Siga as instruções abaixo para obter as seguintes informações antes de começar a ingestão dos seus dados da AWS:

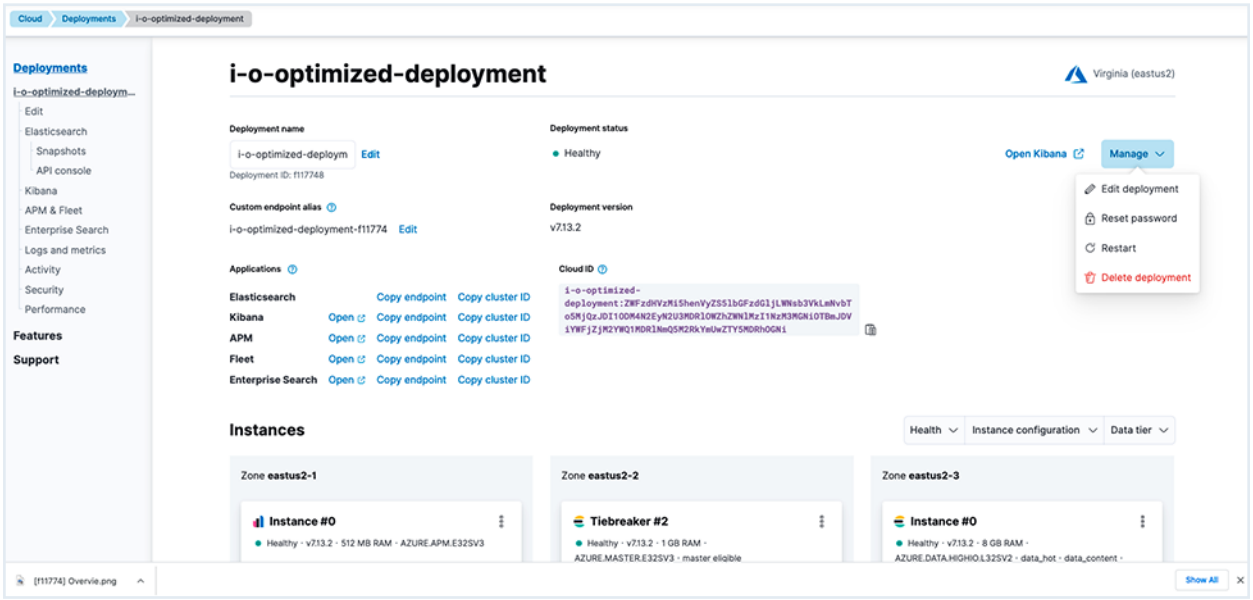
- Localize o Cloud ID
- Obtenha as credenciais de login
- Crie o ID da chave de acesso e a chave de acesso da AWS

Localize o Cloud ID

Você pode encontrar o Cloud ID navegando até cloud.elastic.co e selecionando a implantação relevante.



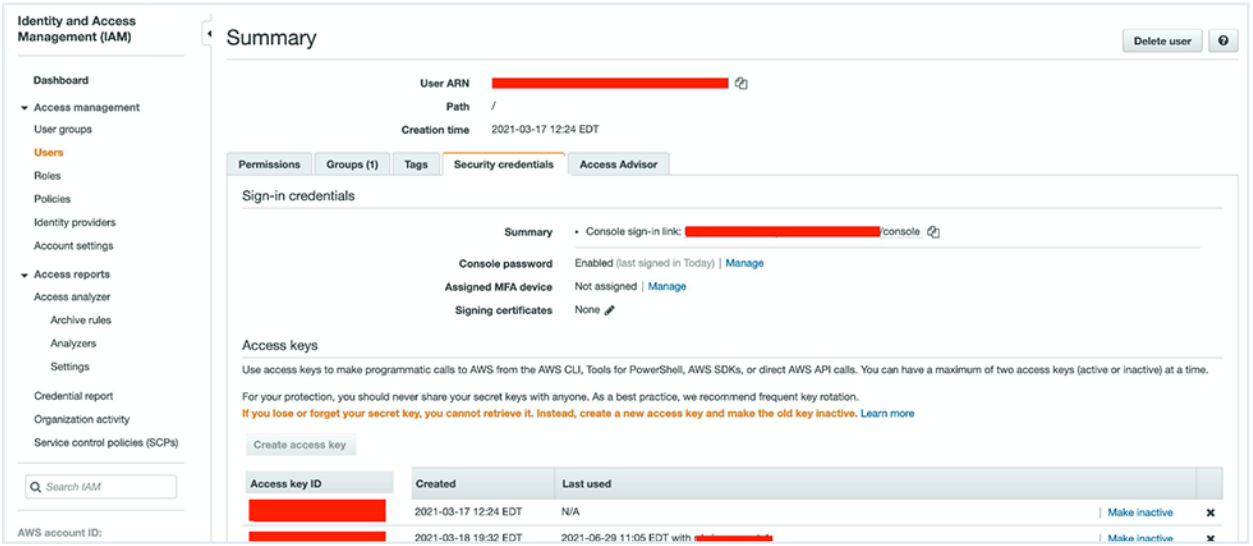
Obtenha as credenciais de login



Ao enviar dados para o Elasticsearch, você pode usar o usuário `Elastic` padrão e a senha que recebeu quando criou o cluster ou pode configurar usuários e funções dedicados, com o mínimo de privilégios necessários para realizar as tarefas. Neste exemplo, usaremos o usuário `Elastic` e a senha fornecida.

Se você não fez o download ou esqueceu a senha, pode navegar até cloud.elastic.co e redefini-la clicando em Manage (Gerenciar) e selecionando a opção Reset password (Redefinir senha).

Crie o ID da chave de acesso e a chave de acesso da AWS



O ID da chave de acesso e a chave de acesso da AWS são usados para assinar solicitações programáticas feitas à AWS. Para obtê-los:

- Faça o login no AWS Identity and Access Management e abra o console do IAM em **https://console.aws.amazon.com/iam/**
- Selecione Users (Usuários) no painel de navegação esquerdo.
- Escolha o usuário e selecione a aba Security credentials (Credenciais de segurança)
- Na seção Access Keys (Chaves de acesso), clique em Create access key (Criar chave de acesso) e, para visualizar o par de chaves de acesso, selecione Show (Mostrar). Copie e salve-as para configurar o Filebeat e o Metricbeat.

Apêndice B — Configuração do Filebeat

Abaixo, você encontrará instruções passo a passo para instalar o Filebeat e habilitar os módulos da AWS. O fluxo é o seguinte:

1. Configurar um bucket do Amazon S3 e criar uma fila do Amazon SQS
2. Baixar e instalar o Filebeat
3. Conectar ao Elastic Stack
   - É aqui que você precisará do Cloud ID e da senha da sua implantação da Elastic
4. Habilitar e configurar o seu módulo do Filebeat
5. Configurar o Filebeat para coletar os seus logs da AWS
   - É aqui que você precisará do código do módulo da AWS, bem como do ID da chave de acesso e da chave de acesso da AWS
6. Definir os seus dashboards do Kibana pré-configurados e iniciar o Filebeat
7. Visualizar e analisar os dados no Kibana

Etapa 1: configurar um bucket do Amazon S3 e criar uma fila do Amazon SQS

Para evitar uma demora significativa na sondagem de todos os arquivos de log de cada bucket do S3, o Filebeat combina a notificação e a sondagem: use o Amazon SQS para notificação do Amazon S3 quando um novo objeto do Amazon S3 for criado. Consulte **Configuring S3 event notifications using Amazon SQS** (Configurar notificações de eventos do S3 usando o Amazon SQS) para saber como configurar o bucket do Amazon S3 e a fila do Amazon SQS.

Etapa 2: baixar e instalar o Filebeat

Baixe e instale o Filebeat. Use os comandos que funcionam para o seu sistema.

- Para este exemplo, usaremos comandos do Linux. Para encontrar a versão mais recente, navegue até a **documentação do Filebeat** e selecione Quick start: installation and configuration (Início rápido: instalação e configuração). Aqui você também encontrará comandos para outros sistemas operacionais.

```
curl -L -O
https.//artifacts.elastic.co/downloads/beats/filebeat/
filebeat-7.13.3-linux-x86_64.tar.gz
tar xzvf filebeat-7.13.3-linux-x86_64.tar.gz
```

Etapa 3: conectar ao Elastic Stack

As conexões com o Elasticsearch e o Kibana são necessárias para configurar o Filebeat. Você precisará modificar o arquivo de configuração, que é o arquivo filebeat.yml.

Aqui, você usará o Cloud ID e a senha que obteve. Especifique o **cloud.id** do seu Elasticsearch Service e defina **cloud.auth** (nome de usuário:senha) como um usuário que esteja autorizado a configurar o Filebeat. Por exemplo:

```
cloud.id.
"staging.dxMtZWFzdC0xLmF3cy5mb3VuZC5pbyRjZWM2ZjI2MWE3NGJmMjRjZTMzYmI4ODExY
jg0Mjk0ZiRjNmMyY2E2ZDA0MjI0OWFmMGNjN2Q3YTllOTYyNTc0Mw=="
cloud.auth. "elastic.<elastic-password>"
```

Para segurança adicional, você pode utilizar o **keystore do Filebeat** para ofuscar as credenciais (nome de usuário, senha, cloud.id etc.) e criar usuários e funções dedicados com o mínimo de permissões necessárias para a tarefa. Para este exemplo, o nome de usuário e a senha padrão que você recebeu ao criar sua implantação serão usados. Além disso, você está usando o superusuário padrão como exemplo. Para produção, configure usuários e funções com o **mínimo de privilégios necessários** para a tarefa.

Crie uma função customizada para usar para a função implantada. Por exemplo:

```
role. arn.aws.iam..123456789012.role/MyFunction
```

A função customizada deve ter as permissões necessárias para executar a função. Para obter mais informações, consulte **IAM permissions required for deployment** (Permissões de IAM necessárias para implantação).

Etapa 4: habilitar e configurar módulos de coleta de dados

Para habilitar o módulo aws, navegue até o diretório do Filebeat e insira o seguinte comando:

```
./filebeat modules enable aws
```

Etapa 5: Configurar o Filebeat para coletar os seus logs da AWS

Navegue até as configurações do módulo da AWS no diretório modules.d, arquivo aws.yml. Se o código da integração desejada estiver faltando, você poderá encontrá-lo no **Apêndice E**.

Você também precisará das suas credenciais da AWS que recebeu do Apêndice A para adicionar ao arquivo aws.yml na parte superior:

- access_key_id: "SEU ID DA CHAVE DE ACESSO DA AWS"
- secret_access_key: "SUA CHAVE DE ACESSO DA AWS"

Se preferir usar outro método de autenticação, consulte **AWS credential options** (Opções de credencial da AWS) para saber mais detalhes.

Consulte o exemplo a seguir abaixo para adicionar seu ID da chave de acesso e a chave de acesso da AWS:

```
module. aws
var.access_key_id. "XyzW4VIA6DCIEKDUNB"
var.secret_access_key. "p4873PxKFRB/enxV98PExUtQkEU82Coafo1w6"
```

Consulte o exemplo abaixo para adicionar sua função do IAM:

```
module. aws
#Função do AWS IAM a assumir
var.role_arn. arniam..123456789012.role/test-mb
```

Observe que você também pode usar o **keystore do Filebeat** para ofuscar seu ID da chave de acesso e a chave de acesso da AWS.

Etapa 6: Definir os seus dashboards do Kibana pré-configurados e iniciar o Filebeat

O Filebeat vem com ativos predefinidos para análise, indexação e visualização dos seus dados. Para carregar esses ativos:

- O usuário especificado em filebeat.yml deverá estar **autorizado a configurar o Filebeat** se você não estiver usando o usuário 'elastic' (usuário padrão)
- No diretório de instalação, execute:

```
./filebeat setup -e
```

Antes de iniciar o Filebeat, modifique as credenciais do usuário em filebeat.yml e especifique um usuário que esteja autorizado a publicar eventos.

Para iniciar o Filebeat, use os seguintes comandos:

```
sudo chown root filebeat.yml
sudo chown root modules.d/aws.yml
sudo ./filebeat -e -c filebeat.yml &
```

Etapa 7: visualizar e analisar os dados no Kibana

O Filebeat vem com dashboards do Kibana pré-criados e uma aplicação Logs dedicada para visualizar, buscar e filtrar dados de log, além de um recurso de detecção de anomalia fácil de configurar. Você carregou os dashboards anteriormente quando executou o comando de instalação.

Para executar o Kibana:

- **Faça o login** na sua conta do Elastic Cloud
- Navegue até o endpoint do Kibana na sua implantação para visualizar e analisar seus dados

Apêndice C — Configuração do Metricbeat

Abaixo, você encontrará instruções passo a passo para instalar o Metricbeat e habilitar os módulos da AWS. O fluxo é o seguinte:

1. Baixar e instalar o Metricbeat
2. Conectar ao Elastic Stack
   - É aqui que você precisará do Cloud ID e da senha da sua implantação da Elastic
3. Habilitar e configurar módulos de coleta de dados
4. Configurar o Filebeat para coletar métricas da AWS
   - É aqui que você precisará do código do módulo da AWS, bem como do ID da chave de acesso e da chave de acesso da AWS
5. Definir os seus dashboards do Kibana pré-configurados e iniciar o Metricbeat
6. Visualizar e analisar os dados no Kibana

Etapa 1: baixar e instalar o Metricbeat

Baixe e instale o Metricbeat. Use os comandos que funcionam para o seu sistema.

Para este exemplo, usaremos comandos do Linux. Para encontrar a versão mais recente, navegue até a **documentação do Metricbeat** e selecione Quick start: installation and configuration (Início rápido: instalação e configuração). Aqui você também encontrará comandos para outros sistemas operacionais.

```
curl -L -O https://artifacts.elastic.co/downloads/beats/
metricbeat/metricbeat-7.13.4-linux-x86_64.tar.gz
tar xzvf metricbeat-7.13.4-linux-x86_64.tar.gz
```

Etapa 2: Conectar ao Elastic Stack

Ao configurar o Metricbeat, você deve editar o arquivo de configuração, metricbeat.yml.

Aqui, você usará o Cloud ID e a senha que obteve. Especifique o **cloud.id** do seu Elasticsearch Service e defina **cloud.auth** (nome de usuário:senha) como um usuário que esteja autorizado a configurar o Metricbeat. Por exemplo:

```
cloud.id.
"staging.dxMtZWFzdC0xLmF3cy5mb3VuZC5pbyRjZWM2ZjI2MWE3NGJmMjRjZTMzYmI4ODExY
jg0Mjk0ZiRjNmMyY2E2ZDA0MjI0OWFmMGNjN2Q3YTllOTYyNTc0Mw=="
cloud.auth. "elastic.<elastic-password>"
```

Para segurança adicional, você pode utilizar o **keystore do Metricbeat** para ofuscar as credenciais (nome de usuário, senha, cloud.id etc.) e criar usuários e funções dedicados com o mínimo de permissões necessárias para a tarefa. Para este exemplo, o nome de usuário e a senha padrão que você recebeu ao criar sua implantação serão usados. Além disso, você está usando o superusuário padrão como exemplo. Para produção, configure usuários e funções com o **mínimo de privilégios necessários** para a tarefa.

Crie uma função customizada para usar para a função implantada. Por exemplo:

```
role. arn.aws.iam..123456789012.role/MyFunction
```

A função customizada deve ter as permissões necessárias para executar a função. Para obter mais informações, consulte **IAM permissions required for deployment** (Permissões de IAM necessárias para implantação).

Etapa 3: habilitar e configurar módulos de coleta de dados

Ao configurar o Metricbeat, você precisa especificar quais módulos executar. O Metricbeat usa módulos para coletar métricas. Para habilitar o aws config no diretório modules.d, insira o seguinte comando:

```
./metricbeat modules enable aws
```

Etapa 4: Configurar o Metricbeat para coletar as suas métricas da AWS

Navegue até as configurações do módulo da AWS no diretório modules.d, arquivo aws.yml.
Se o código da integração desejada estiver faltando, você poderá encontrá-lo no **Apêndice E**.

Você também precisará das suas credenciais da AWS para adicionar ao arquivo aws.yml na parte superior:

- access_key_id: "SEU ID DA CHAVE DE ACESSO DA AWS"
- secret_access_key: "SUA CHAVE DE ACESSO DA AWS"

Se preferir usar outro método de autenticação, consulte **AWS credential options** (Opções de credencial da AWS) para saber mais detalhes.

Consulte o exemplo a seguir abaixo para adicionar seu ID da chave de acesso e a chave de acesso da AWS:

```
module. aws
access_key_id. "XyzW4VIA6DCIEKDUNB"
secret_access_key. "p4873PxKFRB/enxV98PExUtQkEU82Coafo1w6"
```

Consulte o exemplo abaixo para adicionar sua função do IAM:

```
module. aws
#Função do AWS IAM a assumir
role_arn. arniam..123456789012.role/test-mb
```

Observe que você também pode usar o **keystore do Metricbeat** para ofuscar seu ID da chave de acesso e a chave de acesso da AWS.

Etapa 5: Definir os seus dashboards do Kibana pré-configurados e iniciar o Metricbeat

O Metricbeat vem com exemplos de dashboards do Kibana, visualizações e buscas para visualizar dados de métricas da AWS no Kibana, além de recursos de alerta e detecção de anomalia fáceis de configurar.

- O usuário especificado em metricbeat.yml deverá estar **autorizado a configurar o Metricbeat** se você não estiver usando o usuário 'elastic' (usuário padrão)
- No diretório de instalação, execute:

  ```
  ./metricbeat setup -e
  ```

Para iniciar o Metricbeat, use os seguintes comandos:

```
sudo chown root metricbeat.yml
sudo chown root modules.d/aws.yml
sudo ./metricbeat -e -c metricbeat.yml &
```

Etapa 6: Visualizar e analisar os dados no Kibana

O Metricbeat vem com dashboards do Kibana pré-criados e uma aplicação dedicada para visualizar dados de métricas. Você carregou os dashboards anteriormente quando executou o comando de instalação.

Para executar o Kibana:

- **Faça o login** na sua conta do Elastic Cloud
- Navegue até o endpoint do Kibana na sua implantação

Apêndice D — Configuração do Functionbeat

Abaixo, você encontrará instruções passo a passo para instalar o Functionbeat e habilitar os módulos da AWS. O fluxo é o seguinte:

1. Baixar e instalar o Functionbeat
2. Conectar ao Elastic Stack
   - É aqui que você precisará do Cloud ID e da senha da sua implantação da Elastic
3. Configurar funções de nuvem
   - É aqui que você precisará do código do módulo da AWS, bem como do ID da chave de acesso e da chave de acesso da AWS
4. Configurar ativos e implantar o Functionbeat
5. Criar dashboards do Kibana para análise

Etapa 1: Baixar e instalar o Functionbeat

Baixe e instale o Metricbeat. Use os comandos que funcionam para o seu sistema.

- Para este exemplo, usaremos comandos do Linux. Consulte na **documentação** os comandos para outros sistemas operacionais.

```
curl -L -O https.//artifacts.elastic.co/downloads/beats/
functionbeat/functionbeat-7.13.4-linux-x86_64.tar.gz
tar xzvf functionbeat-7.13.4-linux-x86_64.tar.gz
```

Etapa 2: Conectar ao Elastic Stack

As conexões com o Elasticsearch e o Kibana são necessárias para usar o Filebeat. Você precisará modificar o arquivo de configuração, functionbeat.yml.

Aqui você usará o Cloud ID e a senha que obteve. Especifique o **cloud.id** do seu Elasticsearch Service e defina **cloud.auth** (senha) como um usuário que esteja autorizado a configurar o Functionbeat.
Por exemplo:

```
cloud.id.
"staging.dxMtZWFzdC0xLmF3cy5mb3VuZC5pbyRjZWM2ZjI2MWE3NGJmMjRjZTMzYmI4ODExY
jg0Mjk0ZiRjNmMyY2E2ZDA0MjI0OWFmMGNjN2Q3YTllOTYyNTc0Mw=="
cloud.auth. "functionbeat_setup.YOUR_PASSWORD"
```

Crie uma função customizada para usar para a função implantada. Por exemplo:

```
role. arn.aws.iam..123456789012.role/MyFunction
```

A função customizada deve ter as permissões necessárias para executar a função. Para obter mais informações, consulte **IAM permissions required for deployment** (Permissões de IAM necessárias para implantação).

Etapa 3: configurar funções de nuvem

Antes de implantar o Functionbeat na AWS, você precisa especificar detalhes sobre as funções de nuvem que planeja implantar, incluindo os nomes e tipos de função e os gatilhos que farão com que a função seja executada.

Em functionbeat.yml, configure as funções que você quer implantar. As configurações variam dependendo do tipo de função e do provedor de serviços em nuvem que você está usando. Se o código da integração desejada estiver faltando, você poderá encontrá-lo no **Apêndice E**. Esta seção fornece um exemplo de configuração.

```
functionbeat.provider.aws.endpoint. "s3.amazonaws.com"
functionbeat.provider.aws.deploy_bucket. "functionbeat-deploy"
functionbeat.provider.aws.functions.
  - name. cloudwatch
    enabled. true
    type. cloudwatch_logs
    description. "lambda function for cloudwatch logs"
    triggers.
      - log_group_name. /aws/lambda/my-lambda-function
```

Você também precisará das suas credenciais da AWS. Configure-as na parte superior do arquivo functionbeat.yml:

- access_key_id: "SEU ID DA CHAVE DE ACESSO DA AWS"
- secret_access_key: "SUA CHAVE DE ACESSO DA AWS"

Se preferir usar outro método de autenticação, consulte **AWS credential options** (Opções de credencial da AWS) para saber mais detalhes.

Veja o exemplo abaixo:

```
module. cloudwatch
enabled. true
access_key_id. "XyzW4VIA6DCIEKDUNB"
secret_access_key. "p4873PxKFRB/enxV98PExUtQkEU82Coafo1w6"
```

Etapa 4: configurar ativos e implantar o Functionbeat

O Functionbeat vem com ativos predefinidos para análise, indexação e visualização dos seus dados. Para carregar esses ativos:

O usuário especificado em functionbeat.yml deve estar **autorizado a configurar o Functionbeat**.
No diretório de instalação, execute:

```
./functionbeat setup -e
```

Para implantar as funções de nuvem, use os seguintes comandos:

```
./functionbeat -v -e -d "*" deploy cloudwatch
```

Agora a função está implantada na AWS e pronta para enviar eventos de log para a saída configurada.

Etapa 5: criar dashboards do Kibana para análise

Agora você pode criar os seus dashboards no Kibana. Para saber como visualizar e explorar seus dados, consulte o **Kibana User Guide** (Guia do Usuário do Kibana). Para executar o Kibana:

- **Faça o login** na sua conta do Elastic Cloud
- Navegue até o endpoint do Kibana na sua implantação

Apêndice E — Recursos adicionais

Para configurações avançadas da AWS nos Beats, consulte estes documentos:

- **Filebeat**
- **Metricbeat**
- **Functionbeat**

elastic

Search. Observe. Protect.

A Elastic torna os dados utilizáveis em tempo real e em escala para busca empresarial, observabilidade e segurança. As soluções da Elastic são desenvolvidas sobre uma única stack de tecnologia aberta e gratuita que pode ser implantada em qualquer lugar, possibilitando a obtenção de insights práticos instantaneamente de qualquer tipo de dados — desde encontrar documentos até monitorar a infraestrutura e caçar ameaças. Milhares de organizações em todo o mundo, incluindo Cisco, Goldman Sachs, Microsoft, The Mayo Clinic, NASA, The New York Times, Wikipédia e Verizon, usam a Elastic para operar sistemas de missão crítica. Fundada em 2012, a Elastic tem suas ações negociadas publicamente na NYSE sob o símbolo ESTC. Saiba mais no website elastic.co/pt.

ESCRITÓRIO DA EMPRESA PARA AS AMÉRICAS
800 West El Camino Real, Suite 350, Mountain View, Califórnia 94040
Telefones: +1 650 458 2620 (geral), +1 650 458 2625 (vendas)

info@elastic.co