aws

Guia do Desenvolvedor

OpenSearch Serviço Amazon

OpenSearch Serviço Amazon: Guia do Desenvolvedor

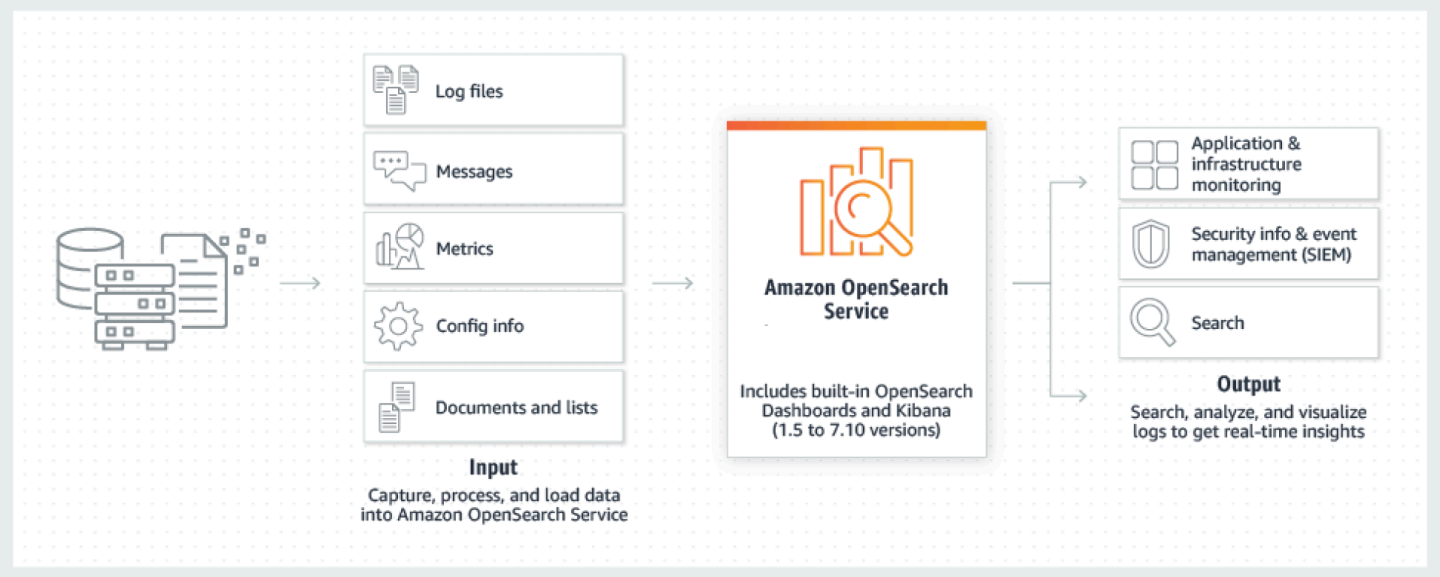
Table of Contents

O que é o Amazon OpenSearch Service?

O Amazon OpenSearch Service é um serviço gerenciado que facilita a implantação, a operação e a escalabilidade de clusters do OpenSearch na Nuvem AWS. O Amazon OpenSearch Service oferece suporte ao OpenSearch e ao Elasticsearch OSS legado (até a 7.10, a versão final de código aberto do software). Ao criar um cluster, você tem a opção de escolher qual mecanismo de pesquisa deseja usar.

O OpenSearch é um conhecido mecanismo de pesquisa e análise com código totalmente aberto para casos de uso como análise de logs, monitoramento de aplicações em tempo real e análise de fluxos de cliques. Para obter mais informações, consulte a documentação do OpenSearch.

O Amazon OpenSearch Service provisiona todos os recursos para seu cluster do OpenSearch e o inicia. Ele também detecta e substitui automaticamente os nós do OpenSearch Service que apresentam falhas, reduzindo os custos indiretos associados a infraestruturas autogerenciadas. Você pode dimensionar seu cluster com uma única chamada de API ou alguns cliques no console.



Para começar a usar o OpenSearch Service, é necessário criar um domínio do OpenSearch Service, que é equivalente a um cluster OpenSearch. Cada instância do EC2 no cluster atua como um nó do OpenSearch Service.

Você pode usar o console do OpenSearch Service para definir e configurar um domínio em questão de minutos. Se preferir o acesso programático, use a AWS CLI ou os AWS SDKs.

Recursos do Amazon OpenSearch Service

O OpenSearch Service inclui os seguintes recursos:

Dimensionar

- Várias configurações de CPU, memória e capacidade de armazenamento conhecidas como tipos de instância, incluindo instâncias do Graviton mais econômicas.
- Até 3 PB de armazenamento vinculado
- Armazenamento UltraWarm e armazenamento de baixa atividade econômicos para dados somente leitura

Segurança

- Controle de acesso do AWS Identity and Access Management (IAM)
- Integração fácil à Amazon VPC e aos grupos de segurança da VPC
- Criptografia de dados em repouso e a criptografia de nó a nó
- Autenticação do Amazon Cognito, HTTP básica ou SAML para OpenSearch Dashboards
- Segurança no nível do índice, no nível do documento e no nível do campo
- Logs de auditoria
- Multilocação do Dashboards

Estabilidade

- Vários locais geográficos para os recursos, conhecidos como regiões e zonas de disponibilidade
- A alocação de nós em duas ou três zonas de disponibilidade na mesma região da AWS, recurso conhecido como Multi-AZ
- Nós principais dedicados para descarregar tarefas de gerenciamento de cluster
- Snapshots automatizados para fazer backup e restaurar domínios do OpenSearch Service

Flexibilidade

- Suporte SQL para a integração com aplicativos de business intelligence (BI)
- Pacotes personalizados para melhorar os resultados da pesquisa

Integração com serviços populares

- Visualização de dados usando o OpenSearch Dashboards
- Integração ao Amazon CloudWatch para monitoramento das métricas de domínio do OpenSearch Service e definição de alarmes
- Integração ao AWS CloudTrail para auditoria de chamadas de API de configuração para domínios do OpenSearch Service
- Integração ao Amazon S3, Amazon Kinesis e Amazon DynamoDB para carregar dados de streaming no OpenSearch Service
- Alertas do Amazon SNS quando os dados excedem determinados limites

Amazon OpenSearch Sem Servidor

O Amazon OpenSearch Sem Servidor é uma configuração de tecnologia sem servidor com escalabilidade automática sob demanda para o Amazon OpenSearch Service. A tecnologia sem servidor remove as complexidades operacionais de provisionamento, configuração e ajuste de seus clusters do OpenSearch. Para obter mais informações, consulte Amazon sem OpenSearch servidor.

Ingestão do Amazon OpenSearch

A Ingestão do Amazon OpenSearch é um coletor de dados totalmente gerenciado, desenvolvido pelo Data Prepper, que fornece dados de log e rastreamento em tempo real para domínios do Amazon OpenSearch Service e coleções OpenSearch Sem Servidor. Ele permite filtrar, enriquecer, transformar, normalizar e agregar dados para análise e visualização posteriores. Para obter mais informações, consulte Ingestão do Amazon OpenSearch.

Versões compatíveis do OpenSearch e do Elasticsearch.

O OpenSearch Service oferece suporte às seguintes versões do OpenSearch:

- 2,11, 2.9, 2.7, 2.5, 2.3, 1.3, 1.3, 1.3, 1.2, 1.1, 1.0

O OpenSearch Service também oferece suporte às seguintes versões antigas do Elasticsearch OSS:

- 7.10, 7.9, 7.9, 7.8, 7.7, 7.4, 7.1
- 6.8, 6.7, 6.5, 6.4, 6.3, 6.2, 6.0

- 5.6, 5.5, 5.3, 5.1
- 2.3
- 1.5

Para obter mais informações, consulte the section called “Operações compatíveis”, the section called “Recursos por versão do mecanismo” e the section called “Plug-ins por versão do mecanismo”.

Se você iniciar um novo projeto no OpenSearch Service, é recomendável escolher a última versão compatível do OpenSearch Service. Se já houver um domínio existente que usa uma versão mais antiga do Elasticsearch, você poderá optar por manter o domínio ou migrar seus dados. Para obter mais informações, consulte the section called “Atualização de domínios”.

Preços do Amazon OpenSearch Service

No OpenSearch Service, você paga por hora de uso de uma instância do EC2 e pelo tamanho cumulativo de todos os volumes de armazenamento do EBS anexados a suas instâncias. Cobranças padrão de transferência de dados na AWS também se aplicam.

No entanto, existem algumas exceções notáveis de transferência de dados. Se um domínio usa várias zonas de disponibilidade, o OpenSearch Service não cobra pelo tráfego entre as zonas de disponibilidade. Um volume significativo de transferência de dados ocorre em um domínio durante a alocação de fragmentos e o rebalanceamento. O OpenSearch Service não mede nem cobra por este tráfego. Da mesma forma, o OpenSearch Service não cobra pela transferência de dados entre nós UltraWarm/de baixa atividade e o Amazon S3.

Para obter informações detalhadas sobre preços, consulte Preços do Amazon OpenSearch Service. Para obter informações sobre encargos incorridos durante as alterações de configuração, consulte the section called “Cobranças para alterações de configuração”.

Conceitos básicos do Amazon OpenSearch Service

Para começar, cadastre-se em uma Conta da AWS, se ainda não tiver uma. Depois de configurar uma conta, siga o tutorial de conceitos básicos para o Amazon OpenSearch Service. Enquanto você se informa sobre o serviço, consulte os tópicos introdutórios a seguir se precisar de mais informações:

- Crie um domínio

- Dimensione o domínio de forma apropriada para sua workload
- Controle o acesso ao seu domínio usando uma política de acesso ao domínio ou um controle de acesso refinado
- Indexar dados manualmente ou de outros serviços da AWS
- Usar o OpenSearch Dashboards para pesquisar seus dados e criar visualizações

Para obter informações sobre como migrar para o OpenSearch Service de um cluster autogerenciado do OpenSearch, consulte the section called “Migração para o OpenSearch Service”.

Serviços relacionados

O OpenSearch Service normalmente é usado com os seguintes serviços:

Amazon CloudWatch

Domínios do OpenSearch Service enviam métricas automaticamente para o CloudWatch para que você possa monitorar a integridade e a performance do domínio. Para obter mais informações, consulte Monitorar métricas de cluster do OpenSearch com o Amazon CloudWatch.

O CloudWatch Logs também pode ir para outra direção. É possível configurar o CloudWatch Logs para transmitir dados para o OpenSearch Service para análise. Para saber mais, consulte the section called “Carregando dados de streaming da Amazon CloudWatch”.

AWS CloudTrail

Use o AWS CloudTrail para obter um histórico das chamadas de API de configuração do OpenSearch Service e de eventos correspondentes de sua conta. Para obter mais informações, consulte Monitoramento de chamadas de API do Amazon OpenSearch Service com o AWS CloudTrail.

Amazon Kinesis

O Kinesis é um serviço totalmente gerenciado para processamento em tempo real de dados de streaming em altíssima escala. Para obter mais informações, consulte the section called “Carregamento dados de transmissão do Amazon Kinesis Data Streams” e the section called “Carregamento de dados de streaming do Amazon Data Firehose”.

Amazon S3

O Amazon Simple Storage Service (Amazon S3) fornece armazenamento para a Internet. Esse guia oferece código de exemplo do Lambda para integração com o Amazon S3. Para obter mais

informações, consulte the section called “Carregamento de dados de transmissão do Amazon S3”.

AWSIAM

O AWS Identity and Access Management (IAM) é um serviço da Web que você pode usar para gerenciar o acesso a seus domínios do OpenSearch Service. Para obter mais informações, consulte the section called “Identity and Access Management”.

AWS Lambda

O AWS Lambda é um serviço de computação que permite executar código sem o provisionamento ou gerenciamento de servidores. Esse guia fornece código de exemplo do Lambda para transmitir dados do DynamoDB, Amazon S3 e Kinesis Para obter mais informações, consulte the section called “Carregando dados de streaming no OpenSearch Serviço”.

Amazon DynamoDB

O Amazon DynamoDB é um serviço de banco de dados NoSQL totalmente gerenciado que fornece uma performance rápida e previsível com escalabilidade integrada. Para saber mais sobre transmissão de dados para o OpenSearch Service, consulte the section called “Carregamento de dados de transmissão do Amazon DynamoDB”.

Amazon QuickSight

Você pode visualizar dados do OpenSearch Service usando painéis do Amazon QuickSight. Para obter mais informações, consulte Uso do Amazon OpenSearch Service com o Amazon QuickSight no Manual do usuário do Amazon QuickSight.

> **Note**
>
> O OpenSearch inclui determinado código Elasticsearch licenciado pelo Apache do Elasticsearch B.V. e outro código-fonte. O Elasticsearch B.V. não é a fonte desse outro código-fonte. ELASTICSEARCH é uma marca registrada da Elasticsearch B.V.

Configurar o Amazon OpenSearch Service

Tópicos

Cadastrar-se em uma Conta da AWS

Se você ainda não tem uma Conta da AWS, siga as etapas a seguir para criar uma.

Para se cadastrar em uma Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

   Quando você se cadastra em uma Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua acesso administrativo a um usuário administrativo e use somente o usuário raiz para realizar as tarefas que exigem acesso do usuário raiz.

A AWS envia um e-mail de confirmação depois que o processo de cadastramento é concluído. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Crie um usuário administrador

Após se inscrever em uma Conta da AWS, garanta seu Usuário raiz da conta da AWS, habilite o AWS IAM Identity Center e crie um usuário administrativo para não usar o usuário raiz nas tarefas diárias.

Proteger seu Usuário raiz da conta da AWS

1. Faça login no AWS Management Console como o proprietário da conta ao escolher a opção Usuário raiz e inserir o endereço de e-mail da Conta da AWS. Na próxima página, digite sua senha.

   Para obter ajuda ao fazer login usando o usuário raiz, consulte Fazer login como usuário raiz no Guia do usuário do Início de Sessão da AWS.
2. Ative a autenticação multifator (MFA) para o usuário raiz.c

   Para obter instruções, consulte Habilitar um dispositivo MFA virtual para o usuário raiz de sua conta da Conta da AWS para seu (console) no Guia do usuário do IAM.

Criar um usuário administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Configurar AWS IAM Identity Center no Guia do Usuário do AWS IAM Identity Center.
2. No IAM Identity Center, conceda acesso administrativo a um usuário administrativo.

   Para obter um tutorial sobre o uso do Diretório do Centro de Identidade do IAM como fonte de identidades, consulte Configurar acesso do usuário com o Diretório do Centro de Identidade do IAM padrão no Guia do Usuário do AWS IAM Identity Center.

Login como usuário administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda com o login utilizando um usuário do Centro de Identidade do IAM, consulte Fazer login no portal de acesso da AWS, no Guia do usuário do Início de Sessão da AWS.

Conceder permissões

Em ambientes de produção, recomendamos que você use políticas mais refinadas. Para saber mais sobre gerenciamento de acesso, consulte Gerenciamento de acesso para recursos da AWS no Guia do usuário do IAM.

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos no AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Create a permission set (Criação de um conjunto de permissões) no Guia do usuário do AWS IAM Identity Center.
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Creating a role for an IAM user (Criação de um perfil para um usuário do IAM) no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Conceder acesso programático

Os usuários precisam de acesso programático se quiserem interagir com a AWS de fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando a AWS.

Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

Qual usuário precisa de acesso programático?	Para	Por
Identificação da força de trabalho (Usuários gerenciados no Centro de Identidade do IAM)	Use credenciais temporárias para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS.	Siga as instruções da interface que deseja utilizar. • Para a AWS CLI, consulte Configuração da AWS CLI para usar o AWS IAM Identity Center no AWS Command Line Interface Guia do usuário da .

Qual usuário precisa de acesso programático?	Para	Por
		• Para os SDKs da AWS, ferramentas e APIs da AWS, consulte Autenticação do Centro de Identidade do IAM no Guia de referência de ferramentas e SDKs da AWS.
IAM	Use credenciais temporárias para assinar solicitações programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS.	Siga as instruções em Como usar credenciais temporárias com recursos da AWS no Guia do usuário do IAM.

Qual usuário precisa de acesso programático?	Para	Por
IAM	(Não recomendado) Use credenciais de longo prazo para assinar solicitaç ões programáticas para a AWS CLI, os SDKs da AWS ou as APIs da AWS.	Siga as instruções da interface que deseja utilizar. • Para a AWS CLI, consulte Autenticação usando as credenciais de usuário do IAM no Guia do usuário da AWS Command Line Interface. • Para as ferramentas e SDKs da AWS, consulte Autenticação usando as credenciais de longo prazo no Guia de referência de ferramentas e SDKs da AWS. • Para as APIs da AWS, consulte Gerenciamento de chaves de acesso de usuários do IAM no Guia do usuário do IAM.

Instalar e configurar a AWS CLI

Se quiser usar as APIs do OpenSearch Service, você deve instalar a versão mais recente do AWS Command Line Interface (AWS CLI). Você não precisa da AWS CLI para usar o OpenSearch Service a partir do console e pode começar sem a CLI seguindo as etapas em Conceitos básicos do Amazon OpenSearch Service.

Para configurar a AWS CLI

1. Para instalar a versão mais recente da AWS CLI para macOS, Linux ou Windows, consulte Instalar ou atualizar a versão mais recente da AWS CLI.

2. Para configurar a AWS CLI e proteger seu acesso aos Serviços da AWS, incluindo o OpenSearch Service, consulte Configuração rápida com `aws configure`.
3. Para verificar a configuração, insira o comando a seguir no prompt de comando do DataBrew.

```
aws opensearch help
```

Os comandos AWS CLI usam o padrão da Região da AWS da sua configuração, a menos que você o defina com um parâmetro ou um perfil. Para definir sua Região da AWS com um parâmetro, você pode adicionar o parâmetro `--region` a cada comando.

Para definir sua Região da AWS com um perfil, primeiro adicione um perfil nomeado nos arquivos `~/.aws/config` ou `%UserProfile%/.aws/config` (para Microsoft Windows). Siga as etapas em Perfis nomeados para a AWS CLI. Em seguida, defina sua Região da AWS e outras configurações com um comando semelhante ao do exemplo a seguir.

```
[profile opensearch]
aws_access_key_id = ACCESS-KEY-ID-OF-IAM-USER
aws_secret_access_key = SECRET-ACCESS-KEY-ID-OF-IAM-USER
region = us-east-1
output = text
```

Abra o console do

A maioria dos tópicos orientados ao console nesta seção começa no console do OpenSearch Service. Se você ainda não estiver conectado à sua Conta da AWS, fala login, abra o console do OpenSearch Service e prossiga para a próxima seção para começar a usar o OpenSearch Service.

Conceitos básicos do Amazon OpenSearch Service

Este tutorial mostra como usar o Amazon OpenSearch Service para criar e configurar um domínio de teste. Um domínio do OpenSearch Service é sinônimo de cluster do OpenSearch. Domínios são clusters com configurações, tipos de instância, contagens de instâncias e recursos de armazenamento especificados por você.

O tutorial orienta você pelas etapas básicas de como montar rapidamente um domínio do OpenSearch Service. Para obter informações mais detalhadas, consulte Criação e gerenciamento de domínios e outros tópicos neste guia. Para obter informações sobre como migrar para o OpenSearch Service de um cluster autogerenciado do OpenSearch, consulte the section called “Migração para o OpenSearch Service”.

Você pode concluir as etapas deste tutorial usando o console do OpenSearch Service, a AWS CLI ou o AWS SDK: Para obter informações sobre a instalação e a configuração da AWS CLI, consulte o Manual do usuário da AWS Command Line Interface.

Etapa 1: criar um domínio do Amazon OpenSearch Service

> **Important**
>
> Este é um tutorial conciso sobre a configuração de um domínio de teste do Amazon OpenSearch Service. Não use esse processo para criar domínios de produção. Para obter uma versão abrangente do mesmo processo, consulte Criação e gerenciamento de domínios.

Um domínio do OpenSearch Service é sinônimo de cluster do OpenSearch. Domínios são clusters com configurações, tipos de instância, contagens de instâncias e recursos de armazenamento especificados por você. Você pode criar um domínio do OpenSearch Service usando o console, a AWS CLI ou os AWS SDK.

Para criar um domínio do OpenSearch Service usando o console

1. Acesse http://aws.amazon.com e escolha Fazer login no console.
2. Em Análise, escolha Amazon OpenSearch Service.

3. Escolha Criar domínio.
4. Informe um nome para o domínio. Os exemplos neste tutorial usam o nome movies.
5. Como método de criação de domínio, escolha Criação padrão.

> **Note**
>
> Para configurar rapidamente um domínio de produção com as melhores práticas, você pode escolher Criação fácil. Para fins de desenvolvimento e teste deste tutorial, usaremos a Criação padrão.

6. Para modelos, escolha dev/teste.
7. Para a opção de implantação, escolha Domínio com modo de espera.
8. Em Versão, escolha a versão mais recente.
9. Por enquanto, ignore as seções Nós de dados, Armazenamento de dados com maior e menor atividade, Nós mestres dedicados, configuração de instantâneos e endpoint personalizado.
10. Para simplificar este tutorial, use um domínio de acesso público. Sob Rede, selecione Acesso público.
11. Nas configurações de controle de acesso detalhado, mantenha a caixa de seleção Habilitar o controle de acesso refinado. Selecione Criar usuário principal e forneça um nome de usuário e senha.
12. Por enquanto, ignore as seções Autenticação SAML e Autenticação do Amazon Cognito.
13. Para Política de acesso), escolha Use somente controle de acesso refinado. Neste tutorial, o controle de acesso refinado processa a autenticação, não a política de acesso ao domínio.
14. Ignore o restante das configurações e escolha Criar. Os novos domínios normalmente levam de 15 a 30 minutos para inicializar, mas podem demorar mais dependendo da configuração. Após a inicialização do domínio, selecione-o para abrir o painel de configuração. Anote o endpoint do domínio em Informações gerais (p. ex., `https://search-`*`my-domain`*`.us-east-1.es.amazonaws.com`), você vai usá-lo na próxima etapa.

Próximo: fazer upload de dados em um domínio do OpenSearch Service para indexação

Etapa 2: carregar dados no Amazon OpenSearch Service para indexação

> **Important**
>
> Este é um tutorial conciso sobre como carregar uma pequena quantidade de dados de teste no Amazon OpenSearch Service. Para obter mais informações sobre como carregar dados em um domínio de produção, consulte Indexação de dados.

Você pode carregar os dados em um domínio do OpenSearch Service usando a linha de comando ou a maioria das linguagens de programação.

Os exemplos de solicitações a seguir usam curl, um cliente HTTP muito comum, para proporcionar agilidade e conveniência. Os clientes como o curl não podem executar a assinatura de solicitações exigida se as políticas de acesso especificam usuários ou funções do IAM. Para concluir esse processo com êxito, você deverá usar o controle de acesso refinado com um nome de usuário primário e uma senha, conforme configurados na Etapa 1.

Você pode instalar o curl no Windows e usá-lo no prompt de comando, mas recomendamos usar uma ferramenta como Cygwin ou o Windows Subsystem for Linux. O macOS e a maioria das distribuições do Linux já vêm com curl pré-instalado.

Opção 1: Carregar um único documento

Execute o comando a seguir para adicionar um único documento ao domínio movies:

```
curl -XPUT -u 'master-user:master-user-password' 'domain-endpoint/movies/_doc/1' -d
 '{"director": "Burton, Tim", "genre": ["Comedy","Sci-Fi"], "year": 1996, "actor":
 ["Jack Nicholson","Pierce Brosnan","Sarah Jessica Parker"], "title": "Mars Attacks!"}'
 -H 'Content-Type: application/json'
```

No comando, forneça o nome do usuário e a senha que você criou na etapa 1.

Para obter uma explicação detalhada desse comando e como fazer solicitações assinadas ao OpenSearch Service, consulte Indexação de dados.

Opção 2: Fazer upload de vários documentos

Para fazer upload de um arquivo JSON que contém vários documentos para um domínio do OpenSearch Service

1. Crie um arquivo local chamado `bulk_movies.json`. Copie e cole o seguinte conteúdo no arquivo, adicionando uma nova linha no final:

```
{ "index" : { "_index": "movies", "_id" : "2" } }
{"director": "Frankenheimer, John", "genre": ["Drama", "Mystery", "Thriller",
 "Crime"], "year": 1962, "actor": ["Lansbury, Angela", "Sinatra, Frank", "Leigh,
 Janet", "Harvey, Laurence", "Silva, Henry", "Frees, Paul", "Gregory, James",
 "Bissell, Whit", "McGiver, John", "Parrish, Leslie", "Edwards, James", "Flowers,
 Bess", "Dhiegh, Khigh", "Payne, Julie", "Kleeb, Helen", "Gray, Joe", "Nalder,
 Reggie", "Stevens, Bert", "Masters, Michael", "Lowell, Tom"], "title": "The
 Manchurian Candidate"}
{ "index" : { "_index": "movies", "_id" : "3" } }
{"director": "Baird, Stuart", "genre": ["Action", "Crime", "Thriller"], "year":
 1998, "actor": ["Downey Jr., Robert", "Jones, Tommy Lee", "Snipes, Wesley",
 "Pantoliano, Joe", "Jacob, Ir\u00e8ne", "Nelligan, Kate", "Roebuck, Daniel",
 "Malahide, Patrick", "Richardson, LaTanya", "Wood, Tom", "Kosik, Thomas",
 "Stellate, Nick", "Minkoff, Robert", "Brown, Spitfire", "Foster, Reese",
 "Spielbauer, Bruce", "Mukherji, Kevin", "Cray, Ed", "Fordham, David", "Jett,
 Charlie"], "title": "U.S. Marshals"}
{ "index" : { "_index": "movies", "_id" : "4" } }
{"director": "Ray, Nicholas", "genre": ["Drama", "Romance"], "year": 1955, "actor":
 ["Hopper, Dennis", "Wood, Natalie", "Dean, James", "Mineo, Sal", "Backus, Jim",
 "Platt, Edward", "Ray, Nicholas", "Hopper, William", "Allen, Corey", "Birch,
 Paul", "Hudson, Rochelle", "Doran, Ann", "Hicks, Chuck", "Leigh, Nelson",
 "Williams, Robert", "Wessel, Dick", "Bryar, Paul", "Sessions, Almira", "McMahon,
 David", "Peters Jr., House"], "title": "Rebel Without a Cause"}
```

2. Execute o comando a seguir no diretório local em que o arquivo está armazenado para fazer upload para o domínio movies:

```
curl -XPOST -u 'master-user:master-user-password' 'domain-endpoint/_bulk' --data-
binary @bulk_movies.json -H 'Content-Type: application/json'
```

Para obter mais informações sobre o formato de arquivo em massa, consulte Indexação de dados.

Próximo: Pesquisar documentos

Etapa 3: pesquisar documentos no Amazon OpenSearch Service

Para pesquisar documentos em um domínio do Amazon OpenSearch Service, use a API de pesquisa do OpenSearch. Como alternativa, você pode usar o OpenSearch Dashboards para pesquisar documentos no domínio.

Para pesquisar documentos via linha de comando

Execute o comando a seguir para realizar uma pesquisa no domínio movies usando a palavra mars:

```
curl -XGET -u 'master-user:master-user-password' 'domain-endpoint/movies/_search?
q=mars&pretty=true'
```

Se você usou dados em massa na página anterior, tente pesquisar rebeldes.

Você verá uma resposta semelhante à seguinte:

```
{
  "took" : 5,
  "timed_out" : false,
  "_shards" : {
    "total" : 5,
    "successful" : 5,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 1,
      "relation" : "eq"
    },
    "max_score" : 0.2876821,
    "hits" : [
      {
        "_index" : "movies",
        "_type" : "_doc",
        "_id" : "1",
        "_score" : 0.2876821,
        "_source" : {
          "director" : "Burton, Tim",
          "genre" : [
            "Comedy",
```

```
            "Sci-Fi"
          ],
          "year" : 1996,
          "actor" : [
            "Jack Nicholson",
            "Pierce Brosnan",
            "Sarah Jessica Parker"
          ],
          "title" : "Mars Attacks!"
        }
      }
    ]
  }
}
```

Pesquisar documentos usando o OpenSearch Dashboards

O OpenSearch Dashboards é uma popular ferramenta de visualização de código aberto projetada para funcionar com o OpenSearch. Ele fornece uma interface de usuário útil para você pesquisar e monitorar seus índices.

Para pesquisar documentos em um domínio do OpenSearch Service usando o Dashboards

1. Acesse o URL do OpenSearch Dashboards para seu domínio. O URL está disponível no painel do domínio no console do OpenSearch Service. O URL segue este formato:

   ```
   domain-endpoint/_dashboards/
   ```

2. Faça login usando o nome de usuário principal e a respectiva senha.
3. Para usar o Dashboards, é necessário criar pelo menos um padrão de índice. O Dashboards usa esses padrões para identificar quais índices você deseja analisar. Abra o menu esquerdo de navegação, escolha Gerenciamento de pilhas, escolha Padrões de índice e, em seguida, escolha Criar padrão de índice. Para este tutorial, insira movies.
4. Escolha Próxima etapa e, em seguida, Criar padrão de índice. Depois que o padrão é criado, você pode visualizar os vários campos do documento, como `actor` e `director`.
5. Volte para a página Padrões de índice e verifique se `movies` está definido como o valor padrão. Caso não esteja, selecione o padrão e escolha o ícone de estrela para torná-lo o valor padrão.
6. Para começar a pesquisar seus dados, abra novamente o menu esquerdo de navegação e escolha Descobrir.

7. Na barra de pesquisa, insira mars se você carregou um único documento, ou rebel se você fez upload de vários documentos. Em seguida, pressione Enter. Você pode tentar pesquisar outros termos, como nomes de atores ou diretores.

Próximo: Excluir um domínio

Etapa 4: excluir um domínio do Amazon OpenSearch Service

Como o domínio movies deste tutorial é usado apenas para fins de teste, você deverá excluí-lo quando terminar os testes para evitar cobranças.

Para excluir um domínio do OpenSearch Service usando o console

1. Faça login no console do Amazon OpenSearch Service.
2. Sob Domínios, selecione o domínio movies (filmes).
3. Escolha Excluir e confirme a exclusão.

Próximas etapas

Agora que você sabe como criar um domínio e indexar dados, talvez você queira tentar alguns dos seguintes exercícios:

- Saiba mais sobre opções mais avançadas para criar um domínio. Para obter mais informações, consulte Criação e gerenciamento de domínios.
- Descubra como gerenciar os índices em seu domínio. Para obter mais informações, consulte Gerenciamento de índices.
- Experimente um dos tutoriais para trabalhar com o Amazon OpenSearch Service. Para obter mais informações, consulte Tutoriais.

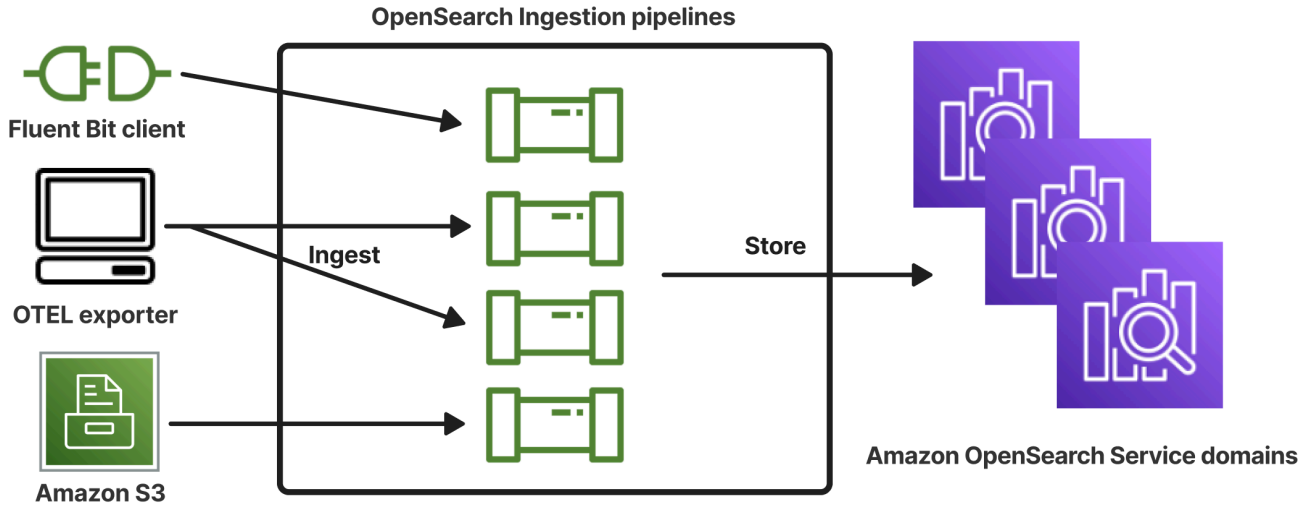
OpenSearch Ingestão da Amazon

O Amazon OpenSearch Ingestion é um coletor de dados totalmente gerenciado e sem servidor que fornece dados de log, métricas e rastreamento em tempo real para domínios do Amazon OpenSearch Service e coleções sem servidor. OpenSearch

Com o OpenSearch Ingestion, você não precisa mais usar soluções de terceiros, como Logstash ou Jaeger, para ingerir dados em seus OpenSearch domínios de serviço e coleções sem servidor. OpenSearch Você configura seus produtores de dados para enviar dados para o OpenSearch Ingestion. Em seguida, ele entrega automaticamente os dados para o domínio ou coleção que você especificar. Você também pode configurar a OpenSearch ingestão para transformar seus dados antes de entregá-los.

Além disso, com o OpenSearch Ingestion, você não precisa se preocupar em provisionar servidores, gerenciar e corrigir software ou escalar seu cluster de servidores. Você provisiona pipelines de ingestão diretamente no AWS Management Console, e o OpenSearch Ingestion se encarrega de gerenciá-los e escalá-los.

OpenSearch A ingestão é um subconjunto do Amazon OpenSearch Service. Ele é desenvolvido pelo Data Prepper, que é um coletor de dados de código aberto que pode filtrar, enriquecer, transformar, normalizar e agregar dados para análise e visualização posteriores.



Tópicos

- Principais conceitos
- Benefícios da OpenSearch ingestão
- Limitações

- Versões do Data Prepper compatíveis
- Pipelines de escalabilidade
- OpenSearch Preços de ingestão
- Suportado Regiões da AWS
- OpenSearch Cotas de ingestão
- Configurar funções e usuários na Ingestão do Amazon OpenSearch
- Conceitos básicos da Ingestão do Amazon OpenSearch
- Visão geral dos recursos do pipeline no Amazon OpenSearch Ingestion
- Criação de pipelines OpenSearch de ingestão da Amazon
- Visualizar pipelines da Ingestão do Amazon OpenSearch
- Atualização dos pipelines OpenSearch de ingestão da Amazon
- Interromper e iniciar os pipelines de Ingestão do Amazon OpenSearch
- Ingestão do Amazon OpenSearch
- Plugins e opções compatíveis para pipelines OpenSearch de ingestão da Amazon
- Trabalhando com integrações de pipeline OpenSearch de ingestão da Amazon
- Migração de dados entre domínios e coleções usando o Amazon Ingestion OpenSearch
- Uso de SDKs da AWS para interagir com a Ingestão do Amazon OpenSearch
- Casos de uso da Ingestão do Amazon OpenSearch
- Segurança na Ingestão do Amazon OpenSearch
- Uso de tags nos pipelines de Ingestão do Amazon OpenSearch
- Log e monitoramento da Ingestão do Amazon OpenSearch com o Amazon CloudWatch
- Práticas recomendadas para Ingestão do Amazon OpenSearch

Principais conceitos

Ao começar a usar o OpenSearch Ingestion, você pode se beneficiar da compreensão dos seguintes conceitos:

Pipeline

> Do ponto de vista da OpenSearch ingestão, um pipeline se refere a um único coletor de dados provisionado que você cria no Service. OpenSearch Pense nisso como o arquivo de configuração

YAML completo, que inclui um ou mais subpipelines. Para ver as etapas para criar um pipeline de ingestão, consulte the section called “Como criar pipelines”.

Subpipeline

Você define subpipelines em um arquivo de configuração YAML. Cada subpipeline é uma combinação de uma fonte, um buffer, zero ou mais processadores e um ou mais coletores. Você pode definir vários subpipelines em um único arquivo YAML, cada um com fontes, processadores e coletores exclusivos. Para ajudar no monitoramento com CloudWatch e outros serviços, recomendamos que você especifique um nome de pipeline que seja diferente de todos os seus subpipelines.

Você pode agrupar vários subpipelines em um único arquivo YAML, de forma que a origem de um subpipeline seja outro subpipeline e seu coletor seja um terceiro subpipeline. Para ver um exemplo, consulte the section called “OpenTelemetry Colecionador”.

Origem

O componente de entrada de um subpipeline. Ele define o mecanismo pelo qual um pipeline consome registros. A fonte pode consumir eventos recebendo-os por HTTPS ou lendo em endpoints externos, como o Amazon S3. Existem dois tipos de fontes: baseadas em push e baseadas em pull. Fontes baseadas em push, como logs HTTP e OTel, transmitem registros para endpoints de ingestão. Fontes baseadas em pull, como rastreamento de OTel e S3, extraem dados da fonte.

Processadores

Unidades de processamento intermediárias que podem filtrar, transformar e enriquecer registros no formato desejado antes de publicá-los no coletor. O processador é um componente opcional de um pipeline. Se você não definir um processador, os registros serão publicados no formato definido na fonte. Você pode usar mais de um processador. Um pipeline executa os processadores na ordem em que são definidos.

Sink

O componente de saída de um subpipeline. Ele define um ou mais destinos nos quais um subpipeline publica registros. OpenSearch A ingestão oferece suporte a domínios OpenSearch de serviço como coletores. Ele também é compatível com subtubulações como coletores. Isso significa que você pode agrupar vários subpipelines em um único pipeline de OpenSearch ingestão (arquivo YAML). OpenSearch Clusters autogerenciados não são suportados como coletores.

Buffer

A parte de um processador que atua como a camada entre a fonte e o coletor. Você não pode configurar um buffer no seu pipeline manualmente. OpenSearch A ingestão usa uma configuração de buffer padrão.

Rota

A parte de um processador que permite que os autores do pipeline enviem somente eventos que correspondam a determinadas condições para diferentes coletores.

Uma definição de subpipeline válida deve conter uma fonte e um coletor. Para obter mais informações sobre cada um desses elementos do pipeline, consulte a referência de configuração.

Benefícios da OpenSearch ingestão

OpenSearch A ingestão tem os seguintes benefícios principais:

- Elimina a necessidade de gerenciar manualmente um pipeline autoprovisionado.
- Dimensiona automaticamente seus pipelines com base nos limites de capacidade definidos por você.
- Mantém seu pipeline atualizado com correções de segurança e bugs.
- Oferece a opção de conectar pipelines à sua nuvem privada virtual (VPC) para uma camada adicional de segurança.
- Permite que você pare e inicie pipelines para controlar os custos.
- Fornece esquemas de configuração de pipeline para casos de uso populares para ajudar você a começar a trabalhar com mais rapidez.
- Permite que você interaja programaticamente com seus pipelines por meio dos vários AWS SDKs e da API de ingestão. OpenSearch
- Oferece suporte ao monitoramento de desempenho na Amazon CloudWatch e ao registro de erros no CloudWatch Logs.

Limitações

OpenSearch A ingestão tem as seguintes limitações:

- Você só pode ingerir dados em domínios que executam OpenSearch 1.0 ou posterior, ou Elasticsearch 6.8 ou posterior. Se você estiver usando a fonte de rastreamento OTel, recomendamos usar o Elasticsearch 7.9 ou posterior para poder usar o plug-in Dashboards. OpenSearch
- Se um pipeline estiver gravando em um domínio de OpenSearch serviço dentro de uma VPC, o pipeline deverá ser criado da Região da AWS mesma forma que o domínio.
- Você pode configurar uma única fonte de dados dentro de uma definição de pipeline.
- Você não pode especificar OpenSearch clusters autogerenciados como coletores.
- Não é possível especificar um endpoint personalizado como coletor. Você ainda pode gravar em um domínio que tenha endpoints personalizados habilitados, mas deve especificar seu endpoint padrão.
- Você não pode especificar recursos em regiões opcionais como fontes ou coletores.
- Há algumas restrições nos parâmetros que você pode incluir em uma configuração de pipeline. Para ter mais informações, consulte the section called “Requisitos e restrições de configuração”.

Versões do Data Prepper compatíveis

OpenSearch Atualmente, o Inestion é compatível com as seguintes versões principais do Data Prepper:

- 2.x

Ao criar um pipeline, use a opção de `version` necessária para especificar a versão principal do Data Prepper a ser usada. Por exemplo,`version: "2"`. OpenSearch A ingestão recupera a versão secundária mais recente compatível dessa versão principal e provisiona o pipeline com essa versão. Para ter mais informações, consulte the section called “Como especificar a versão do pipeline”.

Atualmente, os pipelines de OpenSearch ingestão são provisionados com a versão 2.7 do Data Prepper. Para obter informações, consulte as notas de versão 2.7. Para obter informações sobre os atributos e as correções de erros que estão em cada versão do Data Prepper, consulte a página de Versões. Nem todas as versões secundárias de uma versão principal específica são suportadas pelo OpenSearch Ingestion.

Quando você atualiza o arquivo de configuração YAML de um pipeline, se houver suporte para uma nova versão secundária do Data Prepper, o OpenSearch Ingestion atualizará automaticamente

o pipeline para a versão secundária mais recente compatível da versão principal especificada na configuração do pipeline. Por exemplo, você pode ter `version: "2"` em sua configuração de pipeline, e a OpenSearch Ingestion inicialmente provisionou o pipeline com a versão 2.6.0. Quando o suporte para a versão 2.7.0 é adicionado e você faz uma alteração na configuração do pipeline, o OpenSearch Ingestion atualiza o pipeline para a versão 2.7.0. Esse processo mantém seu pipeline atualizado com as últimas correções de bugs e melhorias de desempenho. OpenSearch A ingestão não pode atualizar a versão principal do seu pipeline, a menos que você altere manualmente a `version` opção na configuração do pipeline. Para ter mais informações, consulte the section called “Atualizar pipelines”.

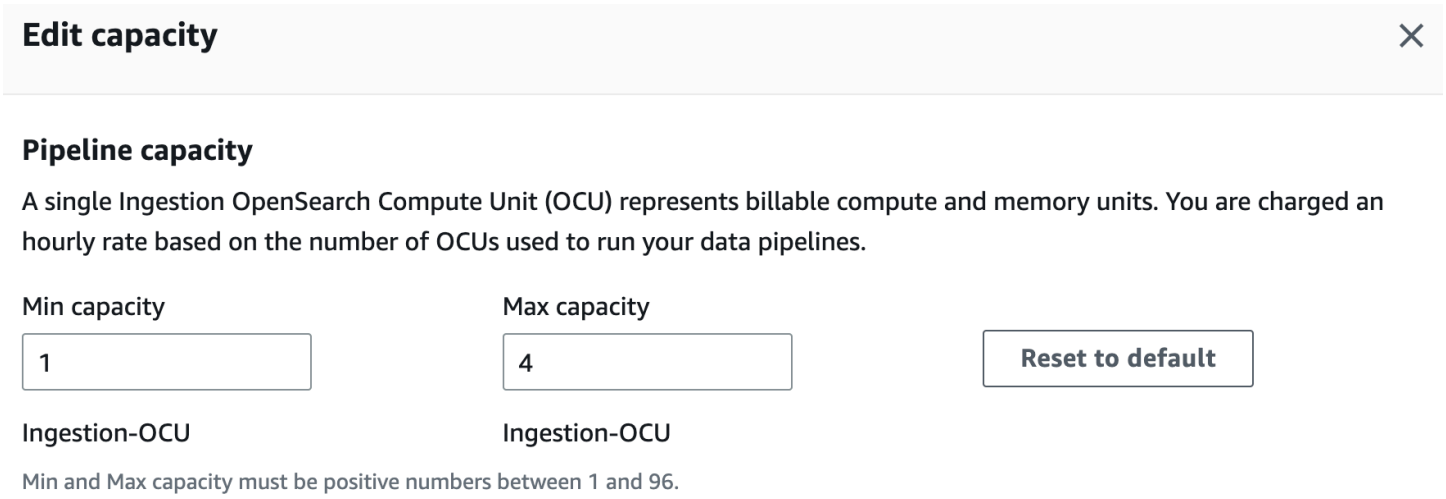
Pipelines de escalabilidade

Você não precisa provisionar e gerenciar a capacidade do pipeline sozinho. OpenSearch A ingestão escala automaticamente a capacidade do pipeline de acordo com sua carga de trabalho estimada, com base nas unidades OpenSearch computacionais de ingestão mínimas e máximas (OCUs de ingestão) que você especificar.

Cada OCU de ingestão é uma combinação de aproximadamente 8 GiB de memória e 2 vCPUs. Você pode especificar os valores mínimo e máximo de OCU para um pipeline, e o OpenSearch Ingestion escala automaticamente a capacidade do pipeline com base nesses limites.

Especifique os seguintes valores:

- Capacidade mínima: o pipeline pode reduzir a capacidade até esse número de OCUs de ingestão. A capacidade mínima especificada também é a capacidade inicial de uma pipeline.
- Capacidade máxima: o pipeline pode aumentar a capacidade até esse número de OCUs de ingestão.



Assegure-se de garantir que a capacidade máxima do pipeline seja alta o suficiente para lidar com picos da workload, e a capacidade mínima seja baixa o suficiente para minimizar os custos quando o pipeline não estiver ocupado. Com base nas suas configurações, o OpenSearch Inestion escala automaticamente o número de OCUs de ingestão do seu pipeline para processar a carga de trabalho de ingestão. A qualquer momento específico, você será cobrado apenas pelas OCUs de ingestão que estão sendo usadas ativamente pelo seu pipeline.

A capacidade alocada para o pipeline de OpenSearch ingestão aumenta e diminui com base nos requisitos de processamento do pipeline e na carga gerada pelo aplicativo cliente. Quando a capacidade é restrita, o OpenSearch Ingestion aumenta alocando mais unidades de computação (GiB de memória). Quando seu pipeline está processando cargas de trabalho menores ou não processando nenhum dado, ele pode reduzir a escala verticalmente até as OCUs de ingestão mínimas configuradas.

Você pode especificar um mínimo de 1 OCU de ingestão, um máximo de 96 OCUs de ingestão para pipelines sem estado e um máximo de 48 OCUs de ingestão para pipelines com estado. Recomendamos um mínimo de pelo menos 2 OCUs de ingestão para fontes baseadas em push. Quando o buffer persistente está habilitado, é possível especificar no mínimo 2 e no máximo 384 OCUs de ingestão.

Com um pipeline de log padrão com uma única fonte, um padrão Grok simples e um coletor, cada unidade computacional pode suportar até 2 MiB por segundo. Para pipelines de log mais complexos com vários processadores, cada unidade computacional pode suportar menos carga de ingestão. Com base na capacidade do pipeline e na utilização de recursos, o processo de escalabilidade OpenSearch de ingestão entra em ação.

Para garantir a alta disponibilidade, as OCUs de ingestão são distribuídas entre zonas de disponibilidade (AZs). O número de AZs depende da capacidade mínima que você especificar.

Por exemplo, se você especificar um mínimo de 2 unidades de computação, as OCUs de ingestão que estão em uso a qualquer momento serão distribuídas uniformemente em 2 AZs. Se você especificar um mínimo de 3 ou mais unidades de computação, as OCUs de ingestão serão distribuídas uniformemente em 3 AZs. Recomendamos que você provisione pelo menos duas OCUs de ingestão para garantir 99,9% de disponibilidade para seus pipelines de ingestão.

Você não paga pelas OCUs de ingestão quando um pipeline está nos estados `Create failed`, `Creating`, `Deleting` e `Stopped`.

Para obter instruções sobre como definir e recuperar as configurações de capacidade de um pipeline, consulte the section called “Como criar pipelines”.

OpenSearch Preços de ingestão

Em qualquer momento específico, você paga apenas pelo número de OCUs de ingestão alocadas a um pipeline, independentemente de haver dados fluindo pelo pipeline. OpenSearch A ingestão acomoda imediatamente suas cargas de trabalho, aumentando ou diminuindo a capacidade do pipeline com base no uso.

Para obter detalhes completos sobre preços, consulte os preços OpenSearch do Amazon Service.

Suportado Regiões da AWS

OpenSearch A ingestão está disponível em um subconjunto Regiões da AWS desse OpenSearch serviço disponível em. Para obter uma lista das regiões suportadas, consulte os endpoints e cotas do Amazon OpenSearch Service no. Referência geral da AWS

OpenSearch Cotas de ingestão

Para obter uma lista de cotas padrão para recursos OpenSearch de ingestão, consulte Cotas do Amazon OpenSearch Service.

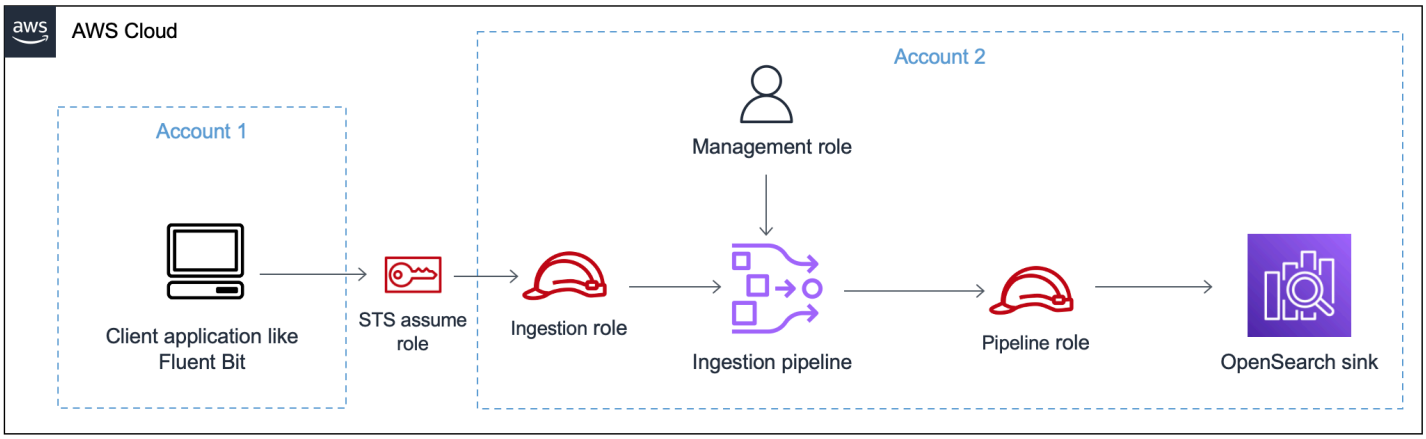
Configurar funções e usuários na Ingestão do Amazon OpenSearch

A Ingestão do Amazon OpenSearch usa uma variedade de modelos de permissões e perfis do IAM para permitir que os aplicativos de origem gravem em pipelines e para permitir que os pipelines gravem em coletores. Antes de começar a ingerir dados, você precisa criar um ou mais perfis do IAM com permissões específicas com base no seu caso de uso.

No mínimo, os seguintes perfis são necessários para configurar um pipeline bem-sucedido.

Nome	Descrição
Perfil de gerenciamento	Qualquer entidade principal que esteja gerenciando pipelines (geralmente um "administrador de pipeline") precisa de acesso de gerenciamento, que inclui permissões como `osis:CreatePipeline` e `osis:UpdatePipeline`. Essas permissões permitem que um usuário administre pipelines, mas não necessariamente grave dados neles.
Perfis do pipeline	O perfil do pipeline, que você especifica na configuração YAML do pipeline, fornece as permissões necessárias para que um pipeline grave no domínio ou no coletor de coleções e leia de fontes baseadas em pull. Para obter informações, consulte os tópicos a seguir: • the section called "Concedendo acesso aos pipelines aos domínios" • the section called "Concedendo aos oleodutos acesso às coleções"
Perfil de ingestão	O perfil de ingestão contém a permissão `osis:Ingest` para o recurso de pipeline. Essa permissão permite que fontes baseadas em push consumam dados em um pipeline.

A imagem a seguir demonstra uma configuração típica de pipeline, em que uma fonte de dados, como Amazon S3 ou Fluent Bit, está gravando em um pipeline em uma conta diferente. Nesse caso, o cliente precisa assumir o perfil de ingestão para acessar o pipeline. Para obter mais informações, consulte the section called "Ingestão entre contas".



Para obter um guia de configuração simples, consulte the section called “Tutorial: ingerir dados em um domínio”.

Tópicos

- the section called “Perfil de gerenciamento”
- the section called “Perfil de ingestão”
- the section called “Perfis do pipeline”
- the section called “Ingestão entre contas”

Perfil de gerenciamento

Além das `osis:*` permissões básicas necessárias para criar e modificar um pipeline, você também precisa da `iam:PassRole` permissão para o recurso de perfil do pipeline. Qualquer AWS service (Serviço da AWS) que aceite um perfil deve usar essa permissão. A Ingestão do OpenSearch assume o perfil sempre que necessário para gravar dados em um coletor. Isso ajuda os administradores a garantir que apenas usuários aprovados possam configurar a Ingestão do OpenSearch com uma função que concede permissões. Para obter mais informações, consulte Conceder a um usuário permissões para transmitir uma função a um AWS service (Serviço da AWS).

Se estiver usando o AWS Management Console (usando esquemas e depois verificando seu pipeline), você precisará das seguintes permissões para criar e atualizar um pipeline:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
```

```
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:CreatePipeline",
            "osis:GetPipelineBlueprint",
            "osis:ListPipelineBlueprints",
            "osis:GetPipeline",
            "osis:ListPipelines",
            "osis:GetPipelineChangeProgress",
            "osis:ValidatePipeline",
            "osis:UpdatePipeline"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/pipeline-role"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
   ]
}
```

Se estiver usando o AWS CLI (sem pré-validar seu pipeline ou usando esquemas), você precisará das seguintes permissões para criar e atualizar um pipeline:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:CreatePipeline",
            "osis:UpdatePipeline"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/pipeline-role"
         ],
```

```
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
   ]
}
```

Perfis do pipeline

Um pipeline precisa de certas permissões para gravar no coletor. Essas permissões dependem se o coletor é um domínio do OpenSearch Service ou uma coleção OpenSearch Sem Servidor.

Além disso, um pipeline pode precisar de permissões para extrair do aplicativo de origem (se a fonte for um plug-in baseado em pull) e permissões para gravar em uma fila de mensagens não entregues do S3, se configurado.

Tópicos

- Gravar em um coletor de domínios
- Gravação em um coletor de coleções
- Gravar em uma fila de mensagens não entregues

Gravar em um coletor de domínios

Um pipeline de Ingestão do OpenSearch precisa de permissão para gravar em um domínio do OpenSearch Service que esteja configurado como seu coletor. Essas permissões incluem a capacidade de descrever o domínio e enviar solicitações HTTP para ele.

Para fornecer ao seu pipeline as permissões necessárias para gravar em um coletor, primeiro crie um perfil do IAM AWS Identity and Access Management com as permissões necessárias. Essas permissões são as mesmas para pipelines públicos e VPC. Em seguida, especifique o perfil do pipeline na política de acesso ao domínio para que o domínio possa aceitar solicitações de gravação do pipeline.

Por fim, especifique o ARN do perfil como o valor da opção sts_role_arn na configuração do pipeline:

```
version: "2"
source:
```

```
  http:
    ...
processor:
  ...
sink:
  - opensearch:
      ...
      aws:
        sts_role_arn: arn:aws:iam::{your-account-id}:role/pipeline-role
```

Para obter instruções sobre como concluir cada uma dessas etapas, consulte Como permitir que os pipelines acessem domínios.

Gravação em um coletor de coleções

Um pipeline de Ingestão do OpenSearch precisa de permissão para gravar em uma coleção OpenSearch Sem Servidor que esteja configurada como seu coletor. Essas permissões incluem a capacidade de descrever a coleção e enviar solicitações HTTP para ela.

Primeiro, crie um perfil do IAM que tenha a permissão de `aoss:BatchGetCollection` para todos os recursos (*). Em seguida, inclua esse perfil em uma política de acesso a dados e forneça permissões para criar índices, atualizar índices, descrever índices e escrever documentos na coleção. Por fim, especifique o ARN do perfil como o valor da opção sts_role_arn na configuração do pipeline.

Para obter instruções sobre como concluir cada uma dessas etapas, consulte Como permitir que os pipelines acessem as coleções.

Gravar em uma fila de mensagens não entregues

Se configurar seu pipeline para gravar em uma fila de mensagens não entregues (DLQ), você deverá incluir a opção `sts_role_arn` na configuração da DLQ. As permissões incluídas nesse perfil permitem que o pipeline acesse o bucket do S3 que você especifica como destino para eventos do DLQ.

Você deve usar o mesmo `sts_role_arn` em todos os componentes do pipeline. Portanto, você deve anexar uma política de permissões separada ao seu perfil de pipeline que forneça acesso ao DLQ. No mínimo, o perfil deve ter permissão para a ação `S3:PutObject` no recurso do bucket:

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "WriteToS3DLQ",
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::my-dlq-bucket/*"
    }
  ]
}
```

Em seguida, você pode especificar o perfil na configuração do DLQ do pipeline:

```
  ...
  sink:
    opensearch:
      dlq:
        s3:
          bucket: "my-dlq-bucket"
          key_path_prefix: "dlq-files"
          region: "us-west-2"
          sts_role_arn: "arn:aws:iam::123456789012:role/pipeline-role"
```

Perfil de ingestão

Todos os plug-ins de origem que a Ingestão do OpenSearch suporta atualmente, com exceção do S3, usam uma arquitetura baseada em push. Isso significa que o aplicativo de origem envia os dados para o pipeline, em vez de o pipeline extrair os dados da fonte.

Portanto, você deve conceder aos aplicativos de origem as permissões necessárias para ingerir dados em um pipeline de Ingestão do OpenSearch. No mínimo, o perfil que assina a solicitação deve receber permissão para a ação `osis:Ingest`, o que permite enviar dados para um pipeline. As mesmas permissões são necessárias para endpoints de pipelines públicos e VPC.

O exemplo de política a seguir permite que a entidade principal associada consuma dados em um único pipeline `my-pipeline` chamado:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Sid": "PermitsWriteAccessToPipeline",
      "Effect": "Allow",
      "Action": "osis:Ingest",
      "Resource": "arn:aws:osis:us-west-2:{your-account-id}:pipeline/my-pipeline"
    }
  ]
}
```

Para obter mais informações, consulte the section called “Trabalhar com integrações de pipeline”.

Ingestão entre contas

Talvez seja necessário ingerir dados em um pipeline de outra Conta da AWS, como uma conta de aplicativo. Para configurar a ingestão entre contas, defina uma perfil de ingestão na mesma conta do pipeline e estabeleça uma relação de confiança entre o perfil de ingestão e a conta do aplicativo:

```
{
  "Version": "2012-10-17",
  "Statement": [{
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::{external-account-id}:root"
      },
     "Action": "sts:AssumeRole"
  }]
}
```

Em seguida, configure seu aplicativo para assumir o perfil de ingestão. A conta do aplicativo deve conceder ao perfil do aplicativo as permissões AssumeRole para o perfil de ingestão na conta do pipeline.

Para obter etapas detalhadas e exemplos de políticas do IAM, consulte the section called “Concessão de acesso de ingestão entre contas”.

Concedendo acesso aos pipelines OpenSearch do Amazon Ingestion aos domínios

Um pipeline OpenSearch de ingestão da Amazon precisa de permissão para gravar no domínio do OpenSearch serviço que está configurado como seu coletor. Para fornecer acesso, você configura uma função AWS Identity and Access Management (IAM) com uma política de permissões restritiva

que limita o acesso ao domínio para o qual um pipeline está enviando dados. Por exemplo, talvez você queira limitar um pipeline de ingestão somente ao domínio e aos índices necessários para ser compatível com seu caso de uso.

Antes de especificar a função na configuração do pipeline, você deve configurá-la com uma relação de confiança apropriada e, em seguida, conceder a ela acesso ao domínio dentro da política de acesso ao domínio.

Tópicos

Etapa 1: Criar um pipeline

A função que você especifica no parâmetro sts_role_arn de uma configuração de pipeline deve ter uma política de permissões anexada que permita enviar dados para o coletor de domínio. Ele também deve ter uma relação de confiança que permita que o OpenSearch Inestion assuma a função. Para obter instruções de como associar uma política gerenciada a uma função, consulte Adição de permissões de identidade do IAM no Manual do usuário do IAM.

O exemplo de política a seguir demonstra o privilégio mínimo que você pode fornecer na função sts_role_arn de uma configuração de pipeline para que ela grave em um único domínio:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "es:DescribeDomain",
            "Resource": "arn:aws:es:*:{your-account-id}:domain/*"
        },
        {
            "Effect": "Allow",
            "Action": "es:ESHttp*",
            "Resource": "arn:aws:es:*:{your-account-id}:domain/{domain-namedomain}/*"
        }
```

```
    ]
}
```

Se planeja reutilizar a função para gravar em vários domínios, você pode tornar a política mais ampla substituindo o nome do domínio por um caractere curinga (*).

A função deve ter a seguinte relação de confiança, o que permite que o OpenSearch Inestion assuma a função do pipeline:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"osis-pipelines.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

Recomendamos que você adicione as chaves de condição `aws:SourceAccount` e `aws:SourceArn` na política para se proteger contra o problema confused deputy. O ID de conta da do proprietário do de origem.

Por exemplo, você poderia adicionar o bloco de condições a seguir na política:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "{your-account-id}"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:osis:{region}:{your-account-id}:pipeline/*"
    }
}
```

Etapa 2: incluir a função do pipeline na política de acesso ao domínio

Para que um pipeline grave dados em um domínio, o domínio deve ter uma política de acesso em nível de domínio que permita que a função de pipeline sts_role_arn o acesse.

O exemplo de política de acesso ao domínio a seguir permite que a função de pipeline chamada`pipeline-role`, que você criou na etapa anterior, grave dados no domínio chamado `ingestion-domain`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{your-account-id}:role/{pipeline-role}"
      },
      "Action": ["es:DescribeDomain", "es:ESHttp*"],
      "Resource": "arn:aws:es:{region}:{your-account-id}:domain/{domain-name}/*"
    }
  ]
}
```

Etapa 3: mapear a função do pipeline (somente para domínios que usam controle de acesso refinado)

Se seu domínio usa controle de acesso refinado para autenticação, há etapas adicionais que você precisa seguir para fornecer acesso ao pipeline a um domínio. As etapas variam de acordo com a configuração do seu domínio:

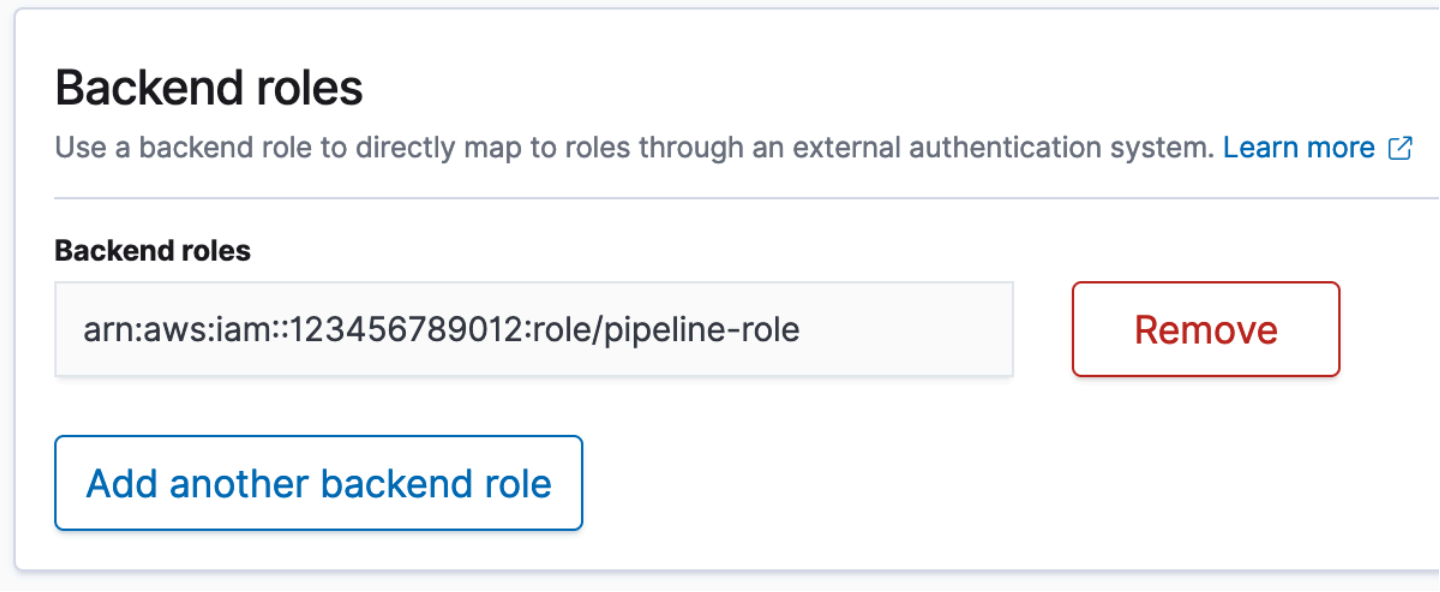
Cenário 1: função de mestre e função de pipeline diferentes — Se você estiver usando um Amazon Resource Name (ARN) do IAM como usuário principal e ele for diferente da função do pipeline (`sts_role_arn`), você precisará mapear a função do pipeline para a função de OpenSearch `all_access` back-end. Basicamente, isso adiciona a função de pipeline como usuário principal adicional. Para obter mais informações, consulte Usuários principais adicionais.

Cenário 2: Usuário principal no banco de dados de usuário interno — Se seu domínio usa um usuário mestre no banco de dados de usuário interno e autenticação básica HTTP para OpenSearch painéis, você não pode passar o nome de usuário e a senha principais diretamente para a configuração do pipeline. Em vez disso, você precisa mapear a função do pipeline (`sts_role_arn`) para a função de OpenSearch `all_access` back-end. Basicamente, isso adiciona a função de pipeline como usuário principal adicional. Para obter mais informações, consulte Usuários principais adicionais.

Cenário 3: mesma função principal e função de pipeline (incomum) — se você estiver usando um ARN do IAM como usuário principal e for o mesmo ARN que você está usando como função de

pipeline (`sts_role_arn`), você não precisa realizar nenhuma ação adicional. O pipeline tem as permissões necessárias para gravar no domínio. Esse cenário é incomum porque a maioria dos ambientes usa uma função de administrador ou alguma outra função como a função principal.

A imagem a seguir mostra como mapear a função do pipeline para uma função de back-end:



Etapa 4: especificar a função na configuração do pipeline

Para criar um pipeline com sucesso, você deve especificar a função do pipeline que você criou na etapa 1 como o parâmetro sts_role_arn na configuração do pipeline. O pipeline assume essa função para assinar solicitações no coletor de domínio do OpenSearch serviço.

No campo `sts_role_arn`, especifique o ARN da função do pipeline do IAM:

```
version: "2"
log-pipeline:
  source:
    http:
      path: "/${pipelineName}/logs"
  processor:
    - grok:
        match:
          log: [ "%{COMMONAPACHELOG}" ]
  sink:
    - opensearch:
        hosts: [ "https://search-{domain-name}.us-east-1.es.amazonaws.com" ]
        index: "my-index"
```

```
        aws:
          region: "[region}"
          sts_role_arn: "arn:aws:iam::{your-account-id}:role/{pipeline-role}"
```

Para obter uma referência completa dos parâmetros necessários e não compatíveis, consulte the section called “Plug-ins e opções compatíveis”.

Concedendo aos pipelines do Amazon OpenSearch Ingestion acesso às coleções

Um pipeline OpenSearch de ingestão da Amazon precisa de permissão para gravar na coleção OpenSearch Serverless que está configurada como seu coletor. Para fornecer acesso, você configura uma função AWS Identity and Access Management (IAM) com uma política de permissões restritiva que limita o acesso à coleção para a qual um pipeline está enviando dados. OpenSearch A ingestão pode ingerir dados tanto para uma coleção pública quanto para uma coleção de VPC.

Antes de especificar o perfil na configuração do pipeline, você deve configurá-lo com uma relação de confiança apropriada e, em seguida, conceder a ele permissões de acesso aos índices da coleção.

Tópicos

Limitações

As limitações a seguir se aplicam aos pipelines que gravam em coleções OpenSearch sem servidor:

- Atualmente, o processador de grupos de rastreamento OTel não funciona com coletores de coleta OpenSearch sem servidor.
- Atualmente, o OpenSearch Ingestion suporta apenas a `_template` operação legada, enquanto o OpenSearch Serverless oferece suporte à operação composable. `_index_template` Portanto, se a configuração do pipeline incluir a opção `index_type`, ela deverá ser definida como `management_disabled`.

Etapa 1: Criar um pipeline

A função que você especifica no parâmetro sts_role_arn de uma configuração de pipeline deve ter uma política de permissões anexada que permita enviar dados para o coletor de coleta. Ele também deve ter uma relação de confiança que permita que o OpenSearch Inestion assuma a função. Para obter instruções de como associar uma política gerenciada a uma função, consulte Adição de permissões de identidade do IAM no Manual do usuário do IAM.

O exemplo de política a seguir demonstra o privilégio mínimo que você pode fornecer na função sts_role_arn de uma configuração de pipeline para que ela grave em coleções:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aoss:BatchGetCollection"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:aoss:{region}:{your-account-
id}:collection/{collection-id}"
        },
        {
            "Action": [
                "aoss:CreateSecurityPolicy",
                "aoss:GetSecurityPolicy",
                "aoss:UpdateSecurityPolicy",
                "aoss:APIAccessAll"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:collection": "{collection-name}"
                }
            }
        }
    ]
}
```

A função deve ter a seguinte relação de confiança, que permita que a OpenSearch Inestion a assuma:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "osis-pipelines.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Recomendamos que você adicione as chaves de condição `aws:SourceAccount` e `aws:SourceArn` na política para se proteger contra o problema confused deputy. O ID de conta da do proprietário do de origem.

Por exemplo, você poderia adicionar o bloco de condições a seguir na política:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "{your-account-id}"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:osis:{region}:{your-account-id}:pipeline/*"
    }
}
```

Etapa 2: criar uma coleção

Crie uma coleção OpenSearch Serverless com as seguintes configurações:

- A seguinte política de acesso a dados, que concede as permissões necessárias para a função de pipeline:

```
[
  {
    "Rules": [
```

```
      {
        "Resource": [
          "index/{collection-name}/*"
        ],
        "Permission": [
          "aoss:CreateIndex",
          "aoss:UpdateIndex",
          "aoss:DescribeIndex",
          "aoss:WriteDocument",
        ],
        "ResourceType": "index"
      }
    ],
    "Principal": [
      "arn:aws:iam::{account-id}:role/{pipeline-role}"
    ],
    "Description": "Pipeline role access"
  }
]
```

> **Note**
>
> No elemento `Principal`, especifique o nome do recurso da Amazon (ARN) do perfil do pipeline criado na etapa anterior.

- Uma política de acesso à rede. Você pode ingerir dados em uma coleção pública ou em uma coleção de VPC. Se você usa uma coleção de VPC, a política de rede deve permitir que um ou mais endpoints de VPC acessem a coleção. Por exemplo, você pode adicionar a seguinte política de rede, que permite que um VPC endpoint acesse a coleção:

```
[
   {
      "Description":"VPC access",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/{collection-name}"
            ]
         }
      ],
      "AllowFromPublic": false,
```

```
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ]
   }
]
```

> **Note**
>
> Além disso, você deve especificar o nome da política de rede na `network_policy_name` opção na configuração do pipeline. Consulte a etapa 3 para ver um exemplo de configuração de pipeline.

Para obter instruções sobre como criar uma coleção, consultethe section called “Criação de coleções”.

Etapa 3: Criar um pipeline

Por fim, crie um pipeline no qual você especifica a função do pipeline e os detalhes da coleção. O pipeline assume essa função para assinar solicitações no coletor de coleta OpenSearch Serverless.

Não deixe de fazer o seguinte:

- Para a opção `hosts`, especifique o endpoint da coleção que você criou na etapa 2.
- Para a opção `sts_role_arn`, especifique o nome do recurso da Amazon (ARN) do perfil do pipeline criado na etapa 1.
- Defina a opção `serverless` como `true`.
- Defina a `network_policy_name` opção como o nome da política de rede anexada à coleção.

```
version: "2"
log-pipeline:
  source:
    http:
        path: "/log/ingest"
  processor:
    - date:
        from_time_received: true
        destination: "@timestamp"
  sink:
```

```
    - opensearch:
        hosts: [ "https://{collection-id}.{region}.aoss.amazonaws.com" ]
        index: "my-index"
        aws:
          serverless: true
          serverless_options:
            network_policy_name: "{network-policy-name}" # If the policy doesn't exist,
a new policy is created.
          region: "us-east-1"
          sts_role_arn: "arn:aws:iam::{account-id}:role/{pipeline-role}"
```

Para obter uma referência completa dos parâmetros necessários e não compatíveis, consulte the section called “Plug-ins e opções compatíveis”.

Conceitos básicos da Ingestão do Amazon OpenSearch

A Ingestão do Amazon OpenSearch suporta a ingestão de dados em domínios gerenciados do OpenSearch Service e coleções tecnologia sem servidor do OpenSearch. Os tutoriais a seguir orientam você nas etapas básicas para colocar um pipeline em funcionamento para cada um desses casos de uso.

> **Note**
>
> A criação de pipeline falhará se você não configurar as permissões corretas. Consulte the section called “Configurar funções e usuários” para entender melhor as funções necessárias antes de criar um pipeline.

Tópicos

Tutorial: ingestão de dados em um domínio usando a Ingestão do Amazon OpenSearch

Este tutorial mostra como usar a Ingestão do Amazon OpenSearch para configurar um pipeline simples e ingerir dados em um domínio do Amazon OpenSearch Service. Um pipeline é um recurso que a Ingestão do OpenSearch provisiona e gerencia. Você pode usar um pipeline para filtrar,

enriquecer, transformar, normalizar e agregar dados para análises e visualizações posteriores no OpenSearch Service.

Este tutorial orienta você pelas etapas básicas de como conseguir montar um pipeline rapidamente. Para obter mais informações detalhadas, consulte the section called “Como criar pipelines”.

Você concluirá as seguintes etapas neste tutorial:

1. Criar a função do pipeline.
2. Crie um domínio.
3. Crie um pipeline.
4. Ingerir alguns dados de amostra.

Neste tutorial, você vai criar os recursos a seguir:

- Um pipeline chamado `ingestion-pipeline`
- Um domínio chamado `ingestion-domain` no qual o pipeline fará a gravação
- Uma perfil do IAM chamado `PipelineRole` determinou que o pipeline assumirá para gravar no domínio

Permissões obrigatórias

Para concluir este tutorial, você deve ter as permissões corretas do IAM. Seu usuário ou função deve ter uma política baseada em identidade anexada com as seguintes permissões mínimas: Essas permissões permitem que você crie uma função de pipeline (`iam:Create`), crie ou modifique um domínio (`es:*`) e trabalhe com pipelines (`osis:*`).

Além disso, a permissão `iam:PassRole` é necessária no recurso de perfil do pipeline. Essa permissão permite que você passe a função do pipeline para a Ingestão do OpenSearch para que ele possa gravar dados no domínio.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
```

```
            "osis:*",
            "iam:Create*",
            "es:*"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/PipelineRole"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
   ]
}
```

Etapa 1: Criar a função de pipeline

Primeiro, crie uma função que o pipeline assumirá para acessar o coletor de domínio do OpenSearch Service. Neste tutorial, você incluirá esse perfil posteriormente na configuração do pipeline.

Para criar a função de pipeline

1. Abra o console do AWS Identity and Access Management em https://console.aws.amazon.com/iamv2/.
2. Escolha Políticas e, depois, Criar política.
3. Neste tutorial, você consumirá dados em um domínio chamado `ingestion-domain`, que você criará na próxima etapa. Selecione JSON e cole a política a seguir no editor. Substitua `{your-account-id}` pelo ID da sua conta e modifique a região, se necessário.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "es:DescribeDomain",
            "Resource": "arn:aws:es:us-east-1:{your-account-id}:domain/ingestion-
domain"
        },
        {
            "Effect": "Allow",
```

```
            "Action": "es:ESHttp*",
            "Resource": "arn:aws:es:us-east-1:{your-account-id}:domain/ingestion-
domain/*"
        }
    ]
}
```

Se quiser gravar dados em um domínio existente, `ingestion-domain` substitua pelo nome do seu domínio.

> **Note**
>
> Para simplificar este tutorial, usaremos uma política de acesso bem ampla. Em ambientes de produção, no entanto, recomendamos que você aplique uma política de acesso mais restritiva à sua função de pipeline. Para obter um exemplo de política que fornece as permissões mínimas necessárias, consulte the section called “Concedendo acesso aos pipelines aos domínios”.

4. Escolha Próximo, então Próximo, e nomeie sua política pipeline-policy.
5. Escolha Criar política.
6. Depois, crie um perfil e anexe a política à ele. Selecione Funções e, em seguida, Criar função.
7. Escolha Política de confiança personalizada e cole a política a seguir no editor:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"osis-pipelines.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

8. Escolha Próximo. Em seguida, pesquise e selecione pipeline-policy (que você acabou de criar).
9. Escolha Próximo e nomeie a função PipelineRole.
10. Selecione Criar função.

Lembre-se do nome do recurso da Amazon (ARN) do perfil (por exemplo, `arn:aws:iam::{your-account-id}:role/PipelineRole`). Você precisará dele quando criar seu pipeline.

Etapa 2: Criar um domínio

Em seguida, crie um domínio chamado `ingestion-domain` para ingerir dados.

Navegue até o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home e crie um domínio que atenda às seguintes configurações:

- Está executando OpenSearch 1.0 ou posterior ou Elasticsearch 7.4 ou posterior
- Usa o acesso público
- Não use controle de acesso detalhado.

> **Note**
>
> Esses requisitos têm como objetivo garantir a simplicidade deste tutorial. Em ambientes de produção, você pode configurar um domínio com acesso à VPC e/ou usar um controle de acesso refinado. Para obter instruções, consulte o restante dos tópicos nesse capítulo.

O domínio deve ter uma política de acesso que conceda a permissão `PipelineRole`, que você criou na etapa anterior. O pipeline assumirá essa função (chamada sts_role_arn na configuração do pipeline) para enviar dados para o coletor de domínio do OpenSearch Service.

Certifique-se de que o domínio tenha a seguinte política de acesso em nível de domínio, concedendo acesso de `PipelineRole` ao domínio. Substitua a região e a ID da conta com seus dados:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{your-account-id}:role/PipelineRole"
      },
      "Action": "es:*",
      "Resource": "arn:aws:es:us-east-1:{your-account-id}:domain/ingestion-domain/*"
    }
  ]
```

```
}
```

Para obter mais informações sobre a criação de políticas de acesso em nível de domínio, consulte Políticas de acesso com base em recursos.

Se você já tiver um domínio criado, modifique sua política de acesso existente para fornecer as permissões acima para a `PipelineRole`.

> **Note**
>
> Lembre-se do endpoint do domínio (por exemplo, `https://search-ingestion-domain.us-east-1.es.amazonaws.com`). Você o usará na próxima etapa para configurar o pipeline.

Etapa 3: Criar um pipeline

Agora que você tem um domínio e uma função com os direitos de acesso apropriados, você pode criar um pipeline.

Como criar um pipeline do

1. No console do Amazon OpenSearch Service, escolha Pipelines no painel de navegação à esquerda.
2. Selecione Criar pipeline.
3. Nomeie o pipeline ingestion-pipeline e mantenha as configurações de capacidade como padrão.
4. Neste tutorial, você criará um subpipeline simples chamada `log-pipeline` que usa o plug-in de origem HTTP. Este plug-in aceita dados de log em formato de matriz JSON. Você especificará um único domínio do OpenSearch Service como coletor e ingerirá todos os dados no índice `application_logs`.

   Em Configuração do pipeline, cole a seguinte configuração de YAML no editor:

   ```
   version: "2"
   log-pipeline:
     source:
       http:
         path: "/${pipelineName}/test_ingestion_path"
     processor:
   ```

```
    - date:
        from_time_received: true
        destination: "@timestamp"
  sink:
    - opensearch:
        hosts: [ "https://search-ingestion-domain.us-east-1.es.amazonaws.com" ]
        index: "application_logs"
        aws:
          sts_role_arn: "arn:aws:iam::{your-account-id}:role/PipelineRole"
          region: "us-east-1"
```

> **Note**
>
> A opção `path` especifica o caminho do URI para ingestão. Essa opção é necessária para fontes baseadas em pull. Para obter mais informações, consulte the section called "Como especificar o caminho de ingestão".

5. Substitua o URL `hosts` pelo endpoint do domínio que você criou (ou modificou) na seção anterior. Substitua o parâmetro `sts_role_arn` pelo ARN de `PipelineRole`.
6. Escolha Validar pipeline e certifique-se de que a validação seja bem-sucedida.
7. Para simplificar neste tutorial, configuraremos o acesso público do pipeline. Sob Rede, selecione Acesso público.

   Para obter mais informações sobre como configurar VPC, consulte the section called "Como proteger pipelines em uma VPC".
8. Mantenha a publicação de logs ativada caso encontre algum problema ao concluir este tutorial. Para obter mais informações, consulte the section called "Monitoramento dos logs de pipeline".

   Especifique o seguinte nome do grupo de logs: `/aws/vendedlogs/OpenSearchIngestion/ingestion-pipeline/audit-logs`
9. Escolha Próximo. Revise sua configuração do pipeline e escolha Criar pipeline. O pipeline leva de 5 a 10 minutos para se tornar ativo.

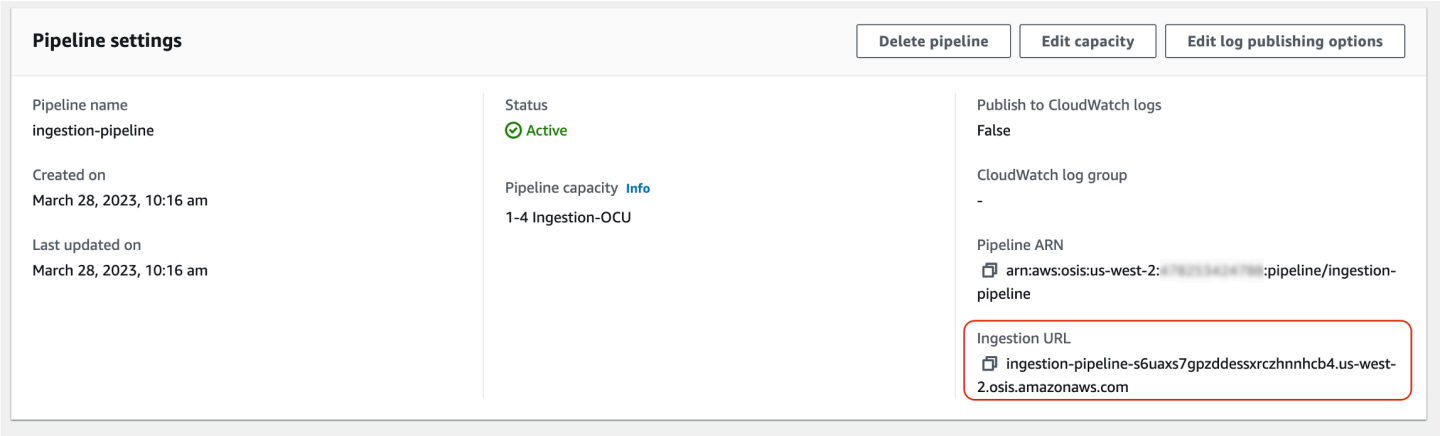
Etapa 4: ingestão de dados de exemplo

Quando o status do pipeline é `Active`, você pode começar a ingerir dados nele. Você deve assinar todas as solicitações HTTP no pipeline usando o Signature Version 4. Use uma ferramenta HTTP, como o Postman ou awscurl, para enviar alguns dados para o pipeline. Assim como acontece com a

indexação de dados diretamente em um domínio, a ingestão de dados em um pipeline sempre exige um perfil do IAM ou uma chave de acesso e chave secreta do IAM.

> **Note**
>
> A entidade principal responsável pela assinatura da solicitação deve ter a permissão `osis:Ingest` do IAM.

Primeiro, obtenha o URL de ingestão na página Configurações do Pipeline:



Em seguida, faça a ingestão de alguns dados de exemplo. A solicitação a seguir usa awscurl para enviar um único arquivo de log para o índice: `application_logs`

```
awscurl --service osis --region us-east-1 \
    -X POST \
    -H "Content-Type: application/json" \
    -d
 '[{"time":"2014-08-11T11:40:13+00:00","remote_addr":"122.226.223.69","status":"404","request":
 http://www.k2proxy.com//hello.html HTTP/1.1","http_user_agent":"Mozilla/4.0
 (compatible; WOW64; SLCC2;)"}]' \
    https://{pipeline-endpoint}.us-east-1.osis.amazonaws.com/log-pipeline/
test_ingestion_path
```

Você obterá uma resposta `200 OK`. Se você receber um erro de autenticação, pode ser porque está ingerindo dados de uma conta diferente daquela em que o pipeline está. Consulte the section called "Corrigindo problemas de permissão".

Agora, consulte o índice `application_logs` para garantir que sua entrada de log tenha sido ingerida com sucesso:

```
awscurl --service es --region us-east-1 \
     -X GET \
     https://search-{ingestion-domain}.us-east-1.es.amazonaws.com/application_logs/
_search | json_pp
```

Resposta de exemplo:


```
{
   "took":984,
   "timed_out":false,
   "_shards":{
      "total":1,
      "successful":5,
      "skipped":0,
      "failed":0
   },
   "hits":{
      "total":{
         "value":1,
         "relation":"eq"
      },
      "max_score":1.0,
      "hits":[
         {
            "_index":"application_logs",
            "_type":"_doc",
            "_id":"z6VY_IMBRpceX-DU6V4O",
            "_score":1.0,
            "_source":{
               "time":"2014-08-11T11:40:13+00:00",
               "remote_addr":"122.226.223.69",
               "status":"404",
               "request":"GET http://www.k2proxy.com//hello.html HTTP/1.1",
               "http_user_agent":"Mozilla/4.0 (compatible; WOW64; SLCC2;)",
               "@timestamp":"2022-10-21T21:00:25.502Z"
            }
         }
      ]
   }
}
```

Corrigindo problemas de permissão

Se você seguiu as etapas do tutorial e ainda vê erros de autenticação ao tentar ingerir dados, talvez seja porque a função que está gravando em um pipeline está em uma Conta da AWS diferente do próprio pipeline. Nesse caso, você precisa criar e assumir uma função que permita especificamente a ingestão de dados. Para obter instruções, consulte the section called “Concessão de acesso de ingestão entre contas”.

Recursos relacionados

Este tutorial apresentou um caso de uso simples de ingestão de um único documento via HTTP. Em cenários de produção, você configurará seus aplicativos cliente (como Fluent Bit, Kubernetes ou o OpenTelemetry Collector) para enviar dados para um ou mais pipelines. Seus pipelines provavelmente serão mais complexos do que o exemplo simples deste tutorial.

Para começar a configurar seus clientes e ingerir dados, consulte os seguintes recursos:

- Criação e gerenciamento de pipelines
- Configurar seus clientes para enviar dados para a Ingestão do OpenSearch
- Documentação do Data Prepper

Tutorial: Ingestão de dados em uma coleção usando o Amazon OpenSearch Ingestion

Este tutorial mostra como usar o Amazon OpenSearch Ingestion para configurar um pipeline simples e ingerir dados em uma coleção Amazon OpenSearch Serverless. Um pipeline é um recurso que o OpenSearch Ingestion provisiona e gerencia. Você pode usar um pipeline para filtrar, enriquecer, transformar, normalizar e agregar dados para análises e visualizações posteriores no Service. OpenSearch

Para ver um tutorial que demonstra como ingerir dados em um domínio de OpenSearch serviço provisionado, consulte. the section called “Tutorial: ingerir dados em um domínio”

Você concluirá as seguintes etapas neste tutorial:

1. Criar a função do pipeline.
2. Crie uma coleção.
3. Crie um pipeline

4. Ingira alguns dados de exemplo.

Neste tutorial, você vai criar os recursos a seguir:

- Um pipeline chamado `ingestion-pipeline-serverless`
- Um coleção chamada `ingestion-collection` no qual o pipeline fará a gravação
- Um perfil do IAM chamado `PipelineRole` e que o pipeline assumirá para gravar na coleção

Permissões obrigatórias

Para concluir este tutorial, você deve ter as permissões corretas do IAM. Seu usuário ou função deve ter uma política baseada em identidade anexada com as seguintes permissões mínimas: Essas permissões permitem que você crie um perfil de pipeline (`iam:Create*`), crie ou modifique uma coleção (`aoss:*`) e trabalhe com pipelines (`osis:*`).

Além disso, a permissão `iam:PassRole` é necessária no recurso de perfil do pipeline. Essa permissão permite que você passe a função do pipeline para o OpenSearch Ingestion para que ele possa gravar dados na coleção.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:*",
            "iam:Create*",
            "aoss:*"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/PipelineRole"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
```

```
    ]
}
```

Etapa 1: Criar a função de pipeline

Primeiro, crie uma função que o pipeline assumirá para acessar o coletor de coleta OpenSearch Serverless. Neste tutorial, você incluirá esse perfil posteriormente na configuração do pipeline.

Para criar a função de pipeline

1. Abra o AWS Identity and Access Management console em https://console.aws.amazon.com/iamv2/.
2. Escolha Políticas e, depois, Criar política.
3. Selecione JSON e cole a política a seguir no editor.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aoss:BatchGetCollection",
        "aoss:APIAccessAll"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:aoss:{region}:{your-account-id}:collection/{collection-
id}"
    },
    {
      "Action": [
        "aoss:CreateSecurityPolicy",
        "aoss:GetSecurityPolicy",
        "aoss:UpdateSecurityPolicy"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aoss:collection": "{collection-name}"
        }
      }
    }
  ]
```

```
}
```

4. Escolha Avançar, escolha Avançar e nomeie sua política collection-pipeline-policy.
5. Escolha Criar política.
6. Depois, crie um perfil e anexe a política à ele. Selecione Funções e, em seguida, Criar função.
7. Escolha Política de confiança personalizada e cole a política a seguir no editor:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"osis-pipelines.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

8. Escolha Próximo. Em seguida, pesquise e selecione collection-pipeline-policy(que você acabou de criar).
9. Escolha Avançar e nomeie a função PipelineRole.
10. Selecione Criar função.

Lembre-se do nome do recurso da Amazon (ARN) do perfil (por exemplo, `arn:aws:iam::{your-account-id}:role/PipelineRole`). Você precisará dele quando criar seu pipeline.

Etapa 2: criar uma coleção

Em seguida, crie uma coleção para ingerir dados. Daremos o nome da coleção de `ingestion-collection`.

1. Navegue até o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. Escolha Coleções no painel de navegação à esquerda e escolha Criar coleção.
3. Nomeie a coleção ingestion-collection.
4. Em Configurações de acesso à rede, altere o tipo de acesso para Público .

5. Mantenha todas as outras configurações em seus valores padrão e escolha Próximo.
6. Para Método de definição, escolha JSON e cole a seguinte política no editor. Essa política faz duas coisas:

   - Permite que o perfil de pipeline faça gravações na coleção.
   - Permite que você leia a coleção. Posteriormente, depois de ingerir alguns dados de amostra no pipeline, você consultará a coleção para garantir que os dados foram ingeridos e gravados com sucesso no índice.

```
[
  {
    "Rules": [
      {
        "Resource": [
          "index/ingestion-collection/*"
        ],
        "Permission": [
          "aoss:CreateIndex",
          "aoss:UpdateIndex",
          "aoss:DescribeIndex",
          "aoss:ReadDocument",
          "aoss:WriteDocument"
        ],
        "ResourceType": "index"
      }
    ],
    "Principal": [
      "arn:aws:iam::{your-account-id}:role/PipelineRole",
      "arn:aws:iam::{your-account-id}:role/Admin"
    ],
    "Description": "Rule 1"
  }
]
```

7. Substitua os elementos `Principal`. A entidade principal deve especificar o perfil do pipeline que você criou. A entidade secundária deve especificar um usuário ou perfil que você possa usar para consultar a coleção posteriormente.
8. Escolha Próximo. Nomeie a política de acesso pipeline-domain-accesse escolha Avançar novamente.
9. Reveja sua configuração da coleção e escolha Enviar.

Quando a coleção estiver ativa, anote o OpenSearch endpoint em Endpoint (por exemplo,`https://{collection-id}.us-east-1.aoss.amazonaws.com`). Você precisará dele quando criar seu pipeline.

Etapa 3: Criar um pipeline

Agora que você tem uma coleção e um perfil com os direitos de acesso apropriados, pode criar um pipeline.

Para criar um pipeline

1. No console do Amazon OpenSearch Service, escolha Pipelines no painel de navegação esquerdo.
2. Selecione Criar pipeline.
3. Nomeie o pipeline como serverless-ingestion e mantenha as configurações de capacidade como padrão.
4. Neste tutorial, criaremos um subpipeline simples chamado `log-pipeline`, que usa o plug-in de fonte do HTTP. Este plug-in aceita dados de log em formato de matriz JSON. Vamos especificar uma única coleção OpenSearch Serverless como coletor e ingerir todos os dados no índice. `my_logs`

   Em Configuração do pipeline, cole a seguinte configuração de YAML no editor:

```
version: "2"
log-pipeline:
  source:
    http:
      path: "/${pipelineName}/test_ingestion_path"
  processor:
    - date:
        from_time_received: true
        destination: "@timestamp"
  sink:
    - opensearch:
        hosts: [ "https://{collection-id}.us-east-1.aoss.amazonaws.com" ]
        index: "my_logs"
        aws:
          sts_role_arn: "arn:aws:iam::{your-account-id}:role/PipelineRole"
          region: "us-east-1"
          serverless: true
```

5. Substitua o URL `hosts` pelo endpoint da coleção criada na seção anterior. Substitua o parâmetro `sts_role_arn` pelo ARN de `PipelineRole`. Opcionalmente, modifique o `region`.
6. Escolha Validar pipeline e certifique-se de que a validação seja bem-sucedida.
7. Para simplificar neste tutorial, configuraremos o acesso público do pipeline. Sob Rede, selecione Acesso público.

   Para obter mais informações sobre como configurar VPC, consulte the section called “Como proteger pipelines em uma VPC”.
8. Mantenha a publicação de logs ativada caso encontre algum problema ao concluir este tutorial. Para ter mais informações, consulte the section called “Monitoramento dos logs de pipeline”.

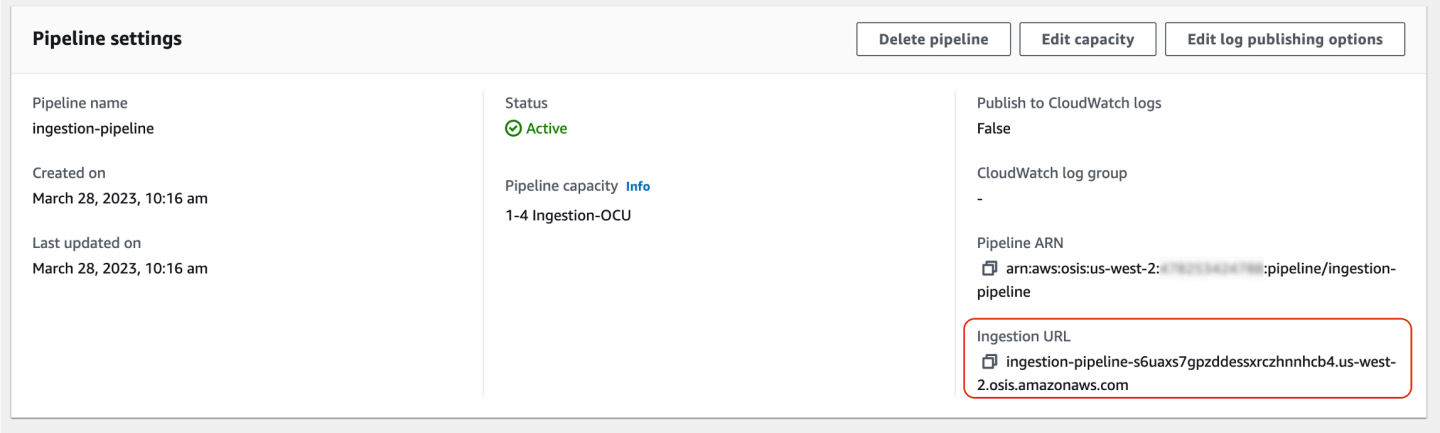
   Especifique o seguinte nome do grupo de logs: `/aws/vendedlogs/OpenSearchIngestion/serverless-ingestion/audit-logs`
9. Escolha Próximo. Revise sua configuração do pipeline e escolha Criar pipeline. O pipeline leva de 5 a 10 minutos para se tornar ativo.

Etapa 4: ingestão de dados de exemplo

Quando o status do pipeline é `Active`, você pode começar a ingerir dados nele. Você deve assinar todas as solicitações HTTP no pipeline usando o Signature Version 4. Use uma ferramenta HTTP, como o Postman ou awscurl, para enviar alguns dados para o pipeline. Assim como acontece com a indexação de dados diretamente em uma coleção, a ingestão de dados em um pipeline sempre requer um perfil do IAM, uma chave de acesso do IAM e uma chave secreta.

> **Note**
>
> A entidade principal responsável pela assinatura da solicitação deve ter a permissão `osis:Ingest` do IAM.

Primeiro, obtenha o URL de ingestão na página Configurações do Pipeline:



Em seguida, faça a ingestão de alguns dados de exemplo. O exemplo de solicitação a seguir usa awscurl para enviar um único arquivo de log para o índice `my_logs`:

```
awscurl --service osis --region us-east-1 \
    -X POST \
    -H "Content-Type: application/json" \
    -d
 '[{"time":"2014-08-11T11:40:13+00:00","remote_addr":"122.226.223.69","status":"404","request":
 http://www.k2proxy.com//hello.html HTTP/1.1","http_user_agent":"Mozilla/4.0
 (compatible; WOW64; SLCC2;)"}]' \
    https://{pipeline-endpoint}.us-east-1.osis.amazonaws.com/log-pipeline/
test_ingestion_path
```

Você obterá uma resposta `200 OK`.

Agora, consulte o índice `my_logs` para garantir que a entrada do log tenha sido ingerida com sucesso:

```
awscurl --service aoss --region us-east-1 \
     -X GET \
     https://{collection-id}.us-east-1.aoss.amazonaws.com/my_logs/_search | json_pp
```

Resposta de exemplo:

```
{
   "took":348,
   "timed_out":false,
   "_shards":{
      "total":0,
```

```
      "successful":0,
      "skipped":0,
      "failed":0
   },
   "hits":{
      "total":{
         "value":1,
         "relation":"eq"
      },
      "max_score":1.0,
      "hits":[
         {
            "_index":"my_logs",
            "_id":"1%3A0%3ARJgDvIcBTy5m12xrKE-y",
            "_score":1.0,
            "_source":{
               "time":"2014-08-11T11:40:13+00:00",
               "remote_addr":"122.226.223.69",
               "status":"404",
               "request":"GET http://www.k2proxy.com//hello.html HTTP/1.1",
               "http_user_agent":"Mozilla/4.0 (compatible; WOW64; SLCC2;)",
               "@timestamp":"2023-04-26T05:22:16.204Z"
            }
         }
      ]
   }
}
```


Recursos relacionados

Este tutorial apresentou um caso de uso simples de ingestão de um único documento via HTTP. Em cenários de produção, você configurará seus aplicativos cliente (como Fluent Bit, Kubernetes ou OpenTelemetry Collector) para enviar dados para um ou mais pipelines. Seus pipelines provavelmente serão mais complexos do que o exemplo simples deste tutorial.

Para começar a configurar seus clientes e ingerir dados, consulte os seguintes recursos:

- Criação e gerenciamento de pipelines
- Configurando seus clientes para enviar dados para OpenSearch o Inestion
- Documentação do Data Prepper

Visão geral dos recursos do pipeline no Amazon OpenSearch Ingestion

O Amazon OpenSearch Ingestion provisiona pipelines, que consistem em uma fonte, um buffer, zero ou mais processadores e um ou mais coletores. Os pipelines de ingestão são alimentados pelo Data Prepper como mecanismo de dados. Para obter uma visão geral de vários componentes de um pipeline, consulte the section called “Principais conceitos”.

As seções a seguir fornecem uma visão geral de alguns dos recursos mais usados no Amazon OpenSearch Ingestion.

> **Note**
>
> Esta não é uma lista completa de atributos disponíveis para pipelines. Para obter uma documentação abrangente de todas as funcionalidades disponíveis do pipeline, consulte a documentação do Data Prepper. Observe que o OpenSearch Inestion impõe algumas restrições aos plug-ins e às opções que você pode usar. Para ter mais informações, consulte the section called “Plug-ins e opções compatíveis”.

Tópicos

Armazenamento em buffer persistente

Um buffer persistente armazena seus dados em um buffer baseado em disco em várias zonas de disponibilidade para adicionar durabilidade aos seus dados. Você pode usar o buffer persistente para ingerir dados de todas as fontes baseadas em push suportadas sem a necessidade de configurar

um buffer independente. Isso inclui HTTP e OpenTelemetry fontes para registros, rastreamentos e métricas.

Para ativar o buffer persistente, escolha Ativar buffer persistente ao criar ou atualizar um pipeline. Para obter mais informações, consultethe section called “Como criar pipelines”. OpenSearch A ingestão determina automaticamente a capacidade de armazenamento em buffer necessária com base nas unidades de OpenSearch processamento de ingestão (OCUs de ingestão) que você especifica para o pipeline.

Por padrão, os pipelines usam an Chave pertencente à AWS para criptografar dados do buffer. Esses pipelines não precisam de nenhuma permissão adicional para a função do pipeline. Como alternativa, você pode especificar uma chave gerenciada pelo cliente e adicionar as seguintes permissões do IAM à função do pipeline:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "KeyAccess",
            "Effect": "Allow",
            "Action": [
              "kms:Decrypt",
              "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "arn:aws:kms:{region}:{aws-account-
id}:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

Para obter mais informações, consulte Chaves mestras do cliente (CMKs) no AWS Key Management Service Guia do desenvolvedor.

> **Note**
>
> Se desabilitar o armazenamento em buffer persistente, seu pipeline será atualizado para ser executado inteiramente no armazenamento em buffer na memória.

Ajustar o tamanho máximo da carga útil da solicitação

Se você ativar o buffer persistente para um pipeline, terá a opção de ajustar o tamanho máximo da carga útil da solicitação. Essa configuração limita o tamanho dos registros enviados ao coletor em uma única solicitação, evitando assim o envio de solicitações enormes. Para ajustar o tamanho máximo da carga útil, defina a `max_request_length` opção na configuração de origem. Assim como o buffer persistente, essa opção só é compatível com HTTP e OpenTelemetry fontes para registros, rastreamentos e métricas.

Os únicos valores válidos para a `max_request_length` opção são 1 MB, 1,5 MB, 2 MB, 2,5 MB, 3 MB, 3,5 MB e 4 MB. Se você especificar um valor diferente, receberá um erro.

O exemplo a seguir demonstra como configurar o tamanho máximo da carga útil em uma configuração de pipeline:

```
...
log-pipeline:
  source:
    http:
      path: "/${pipelineName}/logs"
      max_request_length: "4mb"
  processor:
...
```

Se você ativar o buffer persistente e não especificar a `max_request_length` opção, o valor padrão será de 1 MB.

Dividindo

Você pode configurar um pipeline de OpenSearch ingestão para dividir os eventos recebidos em um subpipeline, permitindo que você execute diferentes tipos de processamento no mesmo evento de entrada.

O exemplo de pipeline a seguir divide os eventos recebidos em dois subpipelines. Cada subpipeline usa seu próprio processador para enriquecer e manipular os dados e, em seguida, envia os dados para índices diferentes. OpenSearch

```
version: "2"
log-pipeline:
```

```
  source:
    http:
    ...
  sink:
    - pipeline:
        name: "logs_enriched_one_pipeline"
    - pipeline:
        name: "logs_enriched_two_pipeline"

logs_enriched_one_pipeline:
  source:
    log-pipeline
  processor:
   ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
        index: "enriched_one_logs"

logs_enriched_two_pipeline:
  source:
    log-pipeline
  processor:
   ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
          index: "enriched_two_logs"
```

Encadeamento

Você pode encadear vários subpipelines para realizar o processamento e o enriquecimento de dados em partes. Em outras palavras, você pode enriquecer um evento de entrada com determinados recursos de processamento em um subpipeline, enviá-lo para outro subpipeline para enriquecimento adicional com um processador diferente e, finalmente, enviá-lo para o coletor. OpenSearch

No exemplo a seguir, o `log_pipeline` subpipeline enriquece um evento de log de entrada com um conjunto de processadores e, em seguida, envia o evento para um índice chamado. OpenSearch `enriched_logs` O pipeline envia o mesmo evento para o `log_advanced_pipeline` subpipeline, que o processa e o envia para um OpenSearch índice diferente chamado`enriched_advanced_logs`.

```
version: "2"
log-pipeline:
  source:
    http:
    ...
  processor:
    ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
          index: "enriched_logs"
    - pipeline:
        name: "log_advanced_pipeline"

log_advanced_pipeline:
  source:
    log-pipeline
  processor:
   ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
          index: "enriched_advanced_logs"
```

Filas de mensagens mortas

As filas de mensagens não entregues (DLQs) são destinos para eventos que um pipeline não consegue gravar em um coletor. Em OpenSearch Ingestão, você deve especificar um bucket do

Amazon S3 com permissões de gravação apropriadas para ser usado como DLQ. Você pode adicionar uma configuração de DLQ a cada coletor em um pipeline. Quando um pipeline encontra erros de gravação, ele cria objetos DLQ no bucket S3 configurado. Os objetos DLQ existem em um arquivo JSON como uma matriz de eventos com falha.

Um pipeline grava eventos na DLQ quando uma das condições a seguir é atendida:

- Os `max_retries` quatro da OpenSearch pia estão esgotados. OpenSearch A ingestão requer um mínimo de 16 para essa opção.
- Os eventos são rejeitados pelo coletor devido a uma condição de erro.

Configuração

Para configurar uma fila de mensagens não entregues para um subpipeline, especifique a opção `dlq` na configuração do coletor: `opensearch`

```
apache-log-pipeline:
  ...
  sink:
    opensearch:
      dlq:
        s3:
          bucket: "my-dlq-bucket"
          key_path_prefix: "dlq-files"
          region: "us-west-2"
          sts_role_arn: "arn:aws:iam::123456789012:role/dlq-role"
```

Os arquivos gravados nessa DLQ do S3 terão o seguinte padrão de nomenclatura:

```
dlq-v${version}-${pipelineName}-${pluginId}-${timestampIso8601}-${uniqueId}
```

Para obter mais informações, consulte Filas de mensagens não entregues (DLQ).

Para obter instruções sobre como configurar a função `sts_role_arn`, consulte the section called “Gravar em uma fila de mensagens não entregues”.

Exemplo

Considere o seguinte exemplo de arquivo DLQ:

```
dlq-v2-apache-log-pipeline-opensearch-2023-04-05T15:26:19.152938Z-e7eb675a-
f558-4048-8566-dac15a4f8343
```

Aqui está um exemplo de dados que não foram gravados no coletor e foram enviados ao bucket DLQ S3 para análise posterior:

```
Record_0
pluginId            "opensearch"
pluginName          "opensearch"
pipelineName        "apache-log-pipeline"
failedData
index    "logs"
indexId   null
status    0
message  "Number of retries reached the limit of max retries (configured value 15)"
document
log      "sample log"
timestamp     "2023-04-14T10:36:01.070Z"

Record_1
pluginId            "opensearch"
pluginName          "opensearch"
pipelineName        "apache-log-pipeline"
failedData
index               "logs"
indexId   null
status    0
message  "Number of retries reached the limit of max retries (configured value 15)"
document
log                 "another sample log"
timestamp           "2023-04-14T10:36:01.071Z"
```

Gerenciamento de índices

O Amazon OpenSearch Ingestion tem muitos recursos de gerenciamento de índices, incluindo os seguintes.

Criar índices

Você pode especificar um nome de índice em um coletor de pipeline e o OpenSearch Ingestion cria o índice ao provisionar o pipeline. Se um índice já existir, o pipeline o usará para indexar eventos

recebidos. Se você parar e reiniciar um pipeline ou atualizar sua configuração YAML, o pipeline tentará criar novos índices, caso eles ainda não existam. Um pipeline nunca pode excluir um índice.

Os coletores de exemplo a seguir criam dois índices quando o pipeline é provisionado:

```
sink:
  - opensearch:
      index: apache_logs
  - opensearch:
      index: nginx_logs
```

Geração de nomes e padrões de índice

Você pode gerar nomes de índices dinâmicos usando variáveis dos campos de eventos recebidos. Na configuração do coletor, use o formato `string${}` para sinalizar a interpolação de strings e use um ponteiro JSON para extrair campos de eventos. As opções para `index_type` são `custom` ou`management_disabled`. Como o `index_type` padrão é `custom` para OpenSearch domínios e `management_disabled` coleções OpenSearch sem servidor, ele pode ser deixado sem definição.

Por exemplo, o pipeline a seguir seleciona o campo `metadataType` dos eventos recebidos para gerar nomes de índice.

```
pipeline:
  ...
  sink:
    opensearch:
      index: "metadata-${metadataType}"
```

A configuração a seguir continua gerando um novo índice a cada dia ou a cada hora.

```
pipeline:
  ...
  sink:
    opensearch:
      index: "metadata-${metadataType}-%{yyyy.MM.dd}"

pipeline:
  ...
  sink:
    opensearch:
      index: "metadata-${metadataType}-%{yyyy.MM.dd.HH}"
```

O nome do índice também pode ser uma string simples com um padrão de data e hora como sufixo, como `my-index-%{yyyy.MM.dd}`. Quando o coletor envia dados para OpenSearch, ele substitui o padrão de data e hora pela hora UTC e cria um novo índice para cada dia, como. `my-index-2022.01.25` Para obter mais informações, consulte a DateTimeFormatteraula.

Esse nome de índice também pode ser uma string formatada (com ou sem um sufixo de padrão de data e hora), como `my-${index}-name`. Quando o coletor envia dados para OpenSearch, ele substitui a `"${index}"` parte pelo valor no evento que está sendo processado. Se o formato for `"${index1/index2/index3}"`, ele substituirá o campo `index1/index2/index3` por seu valor no evento.

Gerar IDs de documentos

Um pipeline pode gerar uma ID de documento ao indexar OpenSearch documentos em. Ele pode inferir esses IDs de documentos a partir dos campos nos eventos recebidos.

Este exemplo usa o campo `uuid` de um evento recebido para gerar um ID do documento.

```
pipeline:
  ...
  sink:
    opensearch:
      index_type: custom
      index: "metadata-${metadataType}-%{yyyy.MM.dd}"
      document_id_field: "uuid"
```

No exemplo a seguir, o processador Adicionar entradas mescla os campos `uuid` e `other_field` do evento recebido para gerar um ID do documento.

A ação `create` garante que documentos com IDs idênticos não sejam substituídos. O pipeline elimina documentos duplicados sem nenhuma nova tentativa ou evento de DLQ. Essa é uma expectativa razoável para autores de pipelines que usam essa ação, pois o objetivo é evitar a atualização de documentos existentes.

```
pipeline:
  ...
  processor:
   - add_entries:
      entries:
        - key: "my_doc_id_field"
```

```
          format: "${uuid}-${other_field}"
  sink:
    - opensearch:
        ...
        action: "create"
        document_id_field: "my_doc_id_field"
```

Talvez você queira definir o ID do documento de um evento como um campo de um subobjeto. No exemplo a seguir, o plug-in OpenSearch sink usa o subobjeto `info/id` para gerar uma ID de documento.

```
sink:
  - opensearch:
        ...
        document_id_field: info/id
```

Dado o evento a seguir, o pipeline gerará um documento com o campo `_id` definido como `json001`:

```
{
   "fieldA":"arbitrary value",
   "info":{
      "id":"json001",
      "fieldA":"xyz",
      "fieldB":"def"
   }
}
```

Gerar IDs de roteamento

Você pode usar a `routing_field` opção no plug-in de OpenSearch coletor para definir o valor de uma propriedade de roteamento de documentos (`_routing`) como um valor de um evento de entrada.

O roteamento é compatível com a sintaxe de ponteiro do JSON, portanto, campos aninhados também estão disponíveis, e não apenas campos de nível superior.

```
sink:
  - opensearch:
        ...
        routing_field: metadata/id
```

```
        document_id_field: id
```

Dado o evento a seguir, o plug-in gerará um documento com o campo `_routing` definido como `abcd`:

```
{
   "id":"123",
   "metadata":{
      "id":"abcd",
      "fieldA":"valueA"
   },
   "fieldB":"valueB"
}
```

Para obter instruções sobre como criar modelos de índice que os pipelines podem usar durante a criação do índice, consulte Modelos de índice.

E nd-to-end reconhecimento

OpenSearch A ingestão garante a durabilidade e a confiabilidade dos dados, rastreando sua entrega da origem aos sumidouros em pipelines sem estado usando reconhecimento. end-to-end Atualmente, somente o plug-in de origem do S3 suporta end-to-end reconhecimento.

Com a end-to-end confirmação, o plug-in de origem do pipeline cria um conjunto de confirmações para monitorar um lote de eventos. Ele recebe uma confirmação positiva quando esses eventos são enviados com sucesso para seus coletores ou uma confirmação negativa quando nenhum dos eventos pôde ser enviado para seus coletores.

No caso de um evento negativo ou falha de um componente do pipeline, ou se uma fonte não receber uma confirmação, a fonte atinge o tempo limite e toma as medidas necessárias, como tentar novamente ou registrar a falha. Se o pipeline tiver vários coletores ou vários subpipelines configurados, as confirmações em nível de evento serão enviadas somente após o evento ser enviado para todos os coletores em todos os subpipelines. Se um coletor tiver uma DLQ configurada, as end-to-end confirmações também rastrearão eventos gravados na DLQ.

Para ativar a end-to-end confirmação, inclua a `acknowledgments` opção na configuração de origem:

```
s3-pipeline:
```

```
  source:
    s3:
      acknowledgments: true
...
```

Contrapressão da fonte

Um pipeline pode sofrer contrapressão quando está ocupado processando dados ou se seus sumidouros estão temporariamente inativos ou lentos para ingerir dados. OpenSearch A ingestão tem maneiras diferentes de lidar com a contrapressão, dependendo do plug-in de origem que um pipeline está usando.

Origem HTTP

Os pipelines que usam o plug-in de origem HTTP lidam com a pressão oposta de maneira diferente, dependendo de qual componente do pipeline está congestionado:

- Buffers: quando os buffers estão cheios, o pipeline começa a retornar o status HTTP `REQUEST_TIMEOUT` com o código de erro 408 de volta ao endpoint de origem. À medida que os buffers são liberados, o pipeline começa a processar eventos HTTP novamente.
- Threads de origem: quando todos os threads de origem HTTP estão ocupados executando solicitações e o tamanho da fila de solicitações não processadas excede o número máximo permitido de solicitações, o pipeline começa a retornar o status HTTP `TOO_MANY_REQUESTS` com o código de erro 429 de volta ao endpoint de origem. Quando a fila de solicitações fica abaixo do tamanho máximo permitido, o pipeline começa a processar as solicitações novamente.

Origem OTel

Quando os buffers estão cheios para pipelines que usam OpenTelemetry fontes (registros OTel, métricas OTel e rastreamento OTel), o pipeline começa a retornar o status HTTP `REQUEST_TIMEOUT` com o código de erro 408 para o endpoint de origem. À medida que os buffers são liberados, o pipeline começa a processar eventos novamente.

Origem do S3

Quando os buffers estão cheios para pipelines com uma origem do S3, os pipelines param de processar notificações SQS. À medida que os buffers são liberados, os pipelines começam a processar as notificações novamente.

Se um coletor estiver inativo ou não conseguir ingerir dados e a end-to-end confirmação for ativada para a origem, o pipeline interromperá o processamento das notificações do SQS até receber uma confirmação bem-sucedida de todos os coletores.

Criação de pipelines OpenSearch de ingestão da Amazon

Um pipeline é o mecanismo que o Amazon OpenSearch Ingeston usa para mover dados da fonte (de onde vêm os dados) para o coletor (para onde vão os dados). Na OpenSearch ingestão, o coletor sempre será um único domínio do Amazon OpenSearch Service, enquanto a fonte de seus dados pode ser clientes como Amazon S3, Fluent Bit ou Collector. OpenTelemetry

Para obter mais informações, consulte Pipelines na OpenSearch documentação.

Tópicos

Pré-requisitos e funções obrigatórias

Para criar um pipeline OpenSearch de ingestão, você precisa ter os seguintes recursos:

- Uma função do IAM que o OpenSearch Ingestion assumirá para gravar no coletor. Você incluirá esse ARN do perfil na sua configuração do pipeline.
- Um domínio OpenSearch de serviço ou coleção OpenSearch sem servidor para atuar como coletor. Se você estiver gravando em um domínio, ele deverá estar executando a OpenSearch versão 1.0 ou posterior, ou o Elasticsearch 7.4 ou posterior. O coletor deve ter uma política de acesso que conceda as permissões apropriadas à sua perfil de pipeline do IAM.

Para obter instruções sobre como criar esses recursos, consulte os tópicos a seguir:

- the section called “Concedendo acesso aos pipelines aos domínios”

- the section called “Concedendo aos oleodutos acesso às coleções”

> **Note**
>
> Se você estiver escrevendo para um domínio que usa controle de acesso detalhado, há etapas extras que você precisa concluir. Consulte the section called “Etapa 3: mapear a função do pipeline (somente para domínios que usam controle de acesso refinado)”.

Permissões obrigatórias

OpenSearch A ingestão usa as seguintes permissões do IAM para criar pipelines:

- `osis:CreatePipeline` – crie um pipeline.
- `osis:ValidatePipeline` – verifica se a configuração do pipeline é válida.
- `iam:PassRole`— passe a função do pipeline para o OpenSearch Ingestion para que ele possa gravar dados no domínio. Essa permissão deve estar no recurso de perfil de pipeline (o ARN que você especifica para a opção `sts_role_arn` na configuração do pipeline) ou simplesmente `*`, se você planeja usar funções diferentes em cada pipeline.

Por exemplo, a política a seguir concede permissão para criar um pipeline:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:CreatePipeline",
            "osis:ListPipelineBlueprints",
            "osis:ValidatePipeline"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/{pipeline-role}"
         ],
         "Effect":"Allow",
```

```
         "Action":[
            "iam:PassRole"
         ]
      }
   ]
}
```

OpenSearch A ingestão também inclui uma permissão chamada`osis:Ingest`, que é necessária para enviar solicitações assinadas ao pipeline usando o Signature Version 4. Para ter mais informações, consulte the section called “Criação de uma função de ingestão”.

> **Note**
>
> Além disso, o primeiro usuário a criar um pipeline em uma conta precisa ter permissões para a ação `iam:CreateServiceLinkedRole`. Para obter mais informações, consulte Recurso de perfil de pipeline.

Para obter mais informações sobre cada permissão, consulte Ações, recursos e chaves de condição para OpenSearch ingestão na Referência de autorização de serviço.

Como especificar a versão do pipeline

Ao configurar um pipeline, você deve especificar a versão principal do Data Prepper que o pipeline executará. Para especificar a versão, inclua a opção `version` na configuração do pipeline:

```
version: "2"
log-pipeline:
  source:
    ...
```

Quando você escolhe Criar, a OpenSearch ingestão determina a última versão secundária disponível da versão principal especificada e provisiona o pipeline com essa versão. Por exemplo, se você especificar `version: "2"` e a versão mais recente compatível do Data Prepper for 2.1.1, o OpenSearch Ingestion provisionará seu pipeline com a versão 2.1.1. Não exibimos publicamente a versão secundária que seu pipeline está executando.

Para atualizar seu pipeline quando uma nova versão principal do Data Prepper estiver disponível, edite a configuração do pipeline e especifique a nova versão. Você não pode fazer o downgrade de um pipeline para uma versão anterior.

> **Note**
>
> OpenSearch O Inestion não oferece suporte imediato às novas versões do Data Prepper assim que elas são lançadas. Haverá algum atraso entre o momento em que uma nova versão estará disponível publicamente e o momento em que ela será suportada no OpenSearch Ingestion. Além disso, o OpenSearch Inestion pode explicitamente não oferecer suporte total a determinadas versões principais ou secundárias. Para obter uma lista abrangente, consulte the section called “Versões do Data Prepper compatíveis”.

Sempre que você fizer uma alteração no pipeline que inicie uma implantação azul/verde, o OpenSearch Ingestion poderá atualizá-la para a versão secundária mais recente da versão principal que está atualmente configurada no arquivo YAML do pipeline. Para obter mais informações, consultethe section called “Implantações azul/verde para atualizações de pipeline”. OpenSearch A ingestão não pode alterar a versão principal do seu pipeline, a menos que você atualize explicitamente a `version` opção na configuração do pipeline.

Como especificar o caminho de ingestão

Para fontes baseadas em pull, como rastreamento de oTel e métricas de oTel, a OpenSearch ingestão requer a `path` opção adicional em sua configuração de origem. O caminho é uma string como `/log/ingest`, que representa o caminho do URI para ingestão. Esse caminho define o URI que você usa para enviar dados para o pipeline.

Por exemplo, digamos que você especifique o seguinte subpipeline de entrada para um pipeline de ingestão chamado: `logs`

```
entry-pipeline:
  source:
    http:
      path: "/my/test_path"
```

Ao ingerir dados no pipeline, você deve especificar o seguinte endpoint na configuração do seu cliente:. `https://logs-abcdefgh.us-west-2.osis.amazonaws.com/my/test_path`

O caminho deve começar com uma barra (/) e pode conter os caracteres especiais '-', '_', ' . 'e'/', bem como o placeholder `${pipelineName}`. Se você usar `${pipelineName}` (como `path: "/${pipelineName}/test_path"`), a variável será substituída pelo nome do subpipeline

associado. Neste exemplo, seria `https://logs.us-west-2.osis.amazonaws.com/`*`entry-pipeline`*`/`*`test_path`*.

Como criar pipelines

Esta seção descreve como criar pipelines OpenSearch de ingestão usando o console OpenSearch de serviço e o. AWS CLI

Console

Para criar um pipeline

1. Faça login no console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. Escolha Pipelines no painel de navegação à esquerda e, depois, Criar pipeline.
3. Insira um nome para o pipeline.
4. (Opcional) Escolha Habilitar buffer persistente. Um buffer persistente armazena seus dados em um buffer baseado em disco entre várias AZs. Para obter informações, consulte Armazenamento em buffer persistente. Se você ativar o buffer persistente, selecione a AWS Key Management Service chave para criptografar os dados do buffer.
5. Configure a capacidade mínima e máxima do pipeline em Unidades de OpenSearch Computação de Ingestão (OCUs). Para ter mais informações, consulte the section called “Pipelines de escalabilidade”.
6. Em Configuração do pipeline, forneça a configuração do pipeline no formato YAML. Um único arquivo de configuração do pipeline pode conter de 1 a 10 subpipelines. Cada subpipeline é uma combinação de uma única fonte, zero ou mais processadores e um único coletor. Para OpenSearch ingestão, o coletor deve sempre ser um domínio OpenSearch de serviço. Para ver uma lista das opções compatíveis, consulte the section called “Plug-ins e opções compatíveis”.

> **Note**
>
> Você deve incluir as opções `sts_role_arn` e `sigv4` em cada subpipeline. O pipeline assume a regra definida em `sts_role_arn` para assinar solicitações no domínio. Para ter mais informações, consulte the section called “Concedendo acesso aos pipelines aos domínios”.

O exemplo de arquivo de configuração a seguir usa a fonte HTTP e os plug-ins Grok para processar dados de log não estruturados e enviá-los para um domínio de OpenSearch serviço. O subpipeline é nomeado `log-pipeline`.

```
version: "2"
log-pipeline:
  source:
    http:
      path: "/log/ingest"
  processor:
    - grok:
        match:
          log: [ '%{COMMONAPACHELOG}' ]
    - date:
        from_time_received: true
        destination: "@timestamp"
  sink:
    - opensearch:
        hosts: [ "https://search-my-domain.us-east-1.es.amazonaws.com" ]
        index: "apache_logs"
        aws:
          sts_role_arn: "arn:aws:iam::123456789012:role/{pipeline-role}"
          region: "us-east-1"
```

> **Note**
>
> Se você especificar vários coletores em uma definição de pipeline YAML, todos eles deverão ser do mesmo domínio de OpenSearch serviço. Um pipeline OpenSearch de ingestão não pode gravar em vários domínios diferentes.

Você pode criar sua própria configuração do pipeline ou escolher Carregar arquivo e importar uma configuração existente para um pipeline autogerenciado do Data Prepper. Como alternativa, você pode usar um esquema de configuração.

7. Depois de configurar seu pipeline, escolha Validar pipeline para confirmar se sua configuração está correta. Se a validação falhar, corrija os erros e execute a validação novamente.
8. Na seção Rede, escolha Acesso via VPC ou Acesso público. Se você selecionar Acesso público, vá para a próxima etapa. Se você escolher Acesso à VPC, defina as seguintes configurações:

Configuração	Descrição
VPC	Escolha o ID da nuvem privada virtual (VPC) que deseja usar. A VPC e o pipeline devem estar na mesma Região da AWS.
Subredes	Escolha uma ou mais sub-redes. OpenSearch O serviço colocará um endpoint VPC e interfaces de rede elástica nas sub-redes.
Grupos de segurança	Escolha um ou mais grupos de segurança de VPC que permitam que o aplicativo necessário alcance o pipeline de OpenSearch ingestão nas portas (80 ou 443) e protocolos (HTTP ou HTTPs) expostos pelo pipeline.

Para ter mais informações, consulte the section called “Como proteger pipelines em uma VPC”.

9. (Opcional) Em Tags, adicione uma ou mais tags (pares de chave/valor) ao seu pipeline. Para ter mais informações, consulte the section called “Uso de tags com pipelines”.
10. (Opcional) Em Opções de publicação de registros, ative a publicação de registros de pipeline no Amazon CloudWatch Logs. Recomendamos que você habilite a publicação de logs para poder solucionar problemas de pipeline com mais facilidade. Para ter mais informações, consulte the section called “Monitoramento dos logs de pipeline”.
11. Escolha Próximo.
12. Revise sua configuração do pipeline e escolha Criar.

OpenSearch A ingestão executa um processo assíncrono para criar o pipeline. Quando o status do pipeline for `Active`, você pode começar a ingerir dados.

AWS CLI

O comando create-pipeline aceita a configuração do pipeline como uma string ou em um arquivo .yaml. Se você fornecer a configuração como uma string, cada nova linha deverá ser escapada com `\n`. Por exemplo, `"log-pipeline:\n source:\n http:\n processor:\n - grok:\n ...`.

O exemplo de comando a seguir cria um pipeline com a seguinte configuração:

- Mínimo de 4 OCUs de ingestão, máximo de 10 OCUs de ingestão

- Provisionado em uma nuvem privada virtual (VPC)
- Publicação de logs habilitada

```
aws osis create-pipeline \
  --pipeline-name my-pipeline \
  --min-units 4 \
  --max-units 10 \
  --log-publishing-options
 IsLoggingEnabled=true,CloudWatchLogDestination={LogGroup="MyLogGroup"} \
  --vpc-options
 SecurityGroupIds={sg-12345678,sg-9012345},SubnetIds=subnet-1212234567834asdf \
  --pipeline-configuration-body "file://pipeline-config.yaml"
```

OpenSearch A ingestão executa um processo assíncrono para criar o pipeline. Quando o status do pipeline for `Active`, você pode começar a ingerir dados. Para verificar o status do pipeline, use o GetPipelinecomando.

OpenSearch API de ingestão

Para criar um pipeline OpenSearch de ingestão usando a API OpenSearch de ingestão, chame a CreatePipelineoperação.

Depois que seu pipeline for criado com sucesso, você poderá configurar seu cliente e começar a ingerir dados em seu domínio OpenSearch de serviço. Para ter mais informações, consulte the section called “Trabalhar com integrações de pipeline”.

Acompanhar o status da criação do pipeline

Você pode acompanhar o status de um pipeline à medida que o OpenSearch Inestion o provisiona e o prepara para ingerir dados.

Console

Depois de criar inicialmente um pipeline, ele passa por vários estágios à medida que o OpenSearch Inestion o prepara para ingerir dados. Para visualizar os vários estágios da criação do pipeline, escolha o nome do pipeline para ver sua página Configurações do pipeline. Em Status, escolha Exibir detalhes.

Um pipeline passa pelos seguintes estágios antes de estar disponível para ingestão de dados:

- Validação: valida a configuração do pipeline. Quando esse estágio estiver concluído, todas as validações serão bem-sucedidas.
- Criação de um ambiente: prepara e provisiona recursos Quando esse estágio estiver concluído, o novo ambiente de pipeline será criado.
- Implantação do pipeline: implanta o pipeline. Quando esse estágio estiver concluído, o pipeline foi implantado com sucesso.
- Verificação da integridade do pipeline: verifica a integridade da pipeline. Quando esse estágio estiver concluído, todas as verificações de integridade serão aprovadas.
- Habilitação de tráfego: permite que o pipeline consuma dados. Quando este estágio for concluído, você pode começar a ingerir dados no pipeline.

CLI

Use o get-pipeline-change-progresscomando para verificar o status de um pipeline. A AWS CLI solicitação a seguir verifica o status de um pipeline chamadomy-pipeline:

```
aws osis get-pipeline-change-progress \
    --pipeline-name my-pipeline
```

Resposta:

```
{
   "ChangeProgressStatuses": {
      "ChangeProgressStages": [
         {
            "Description": "Validating pipeline configuration",
            "LastUpdated": 1.671055851E9,
            "Name": "VALIDATION",
            "Status": "PENDING"
         }
      ],
      "StartTime": 1.671055851E9,
      "Status": "PROCESSING",
      "TotalNumberOfStages": 5
   }
}
```

OpenSearch API de ingestão

Para acompanhar o status da criação do pipeline usando a API OpenSearch de ingestão, chame a GetPipelineChangeProgressoperação.

Usar esquemas para criar um pipeline

Em vez de criar uma definição de pipeline do zero, você pode usar esquemas de configuração, que são modelos YAML pré-configurados para cenários comuns de ingestão, como Trace Analytics ou logs do Apache. Os esquemas de configuração ajudam você a provisionar pipelines facilmente, sem precisar criar uma configuração do zero.

Console

Como usar um esquema de pipeline

1. Faça login no console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. Escolha Pipelines no painel de navegação à esquerda e, depois, Criar pipeline.
3. Em Configuração do pipeline, escolha Esquemas de configuração.
4. Selecione um esquema. A configuração do pipeline é preenchida com um subpipeline para o caso de uso selecionado.
5. Revise o texto comentado que orienta você na configuração do esquema.

> **Important**
>
> O esquema do pipeline não é válido no estado em que se encontra. Você precisa fazer algumas modificações, como fornecer o ARN Região da AWS e a função a serem usados para autenticação, caso contrário, a validação do pipeline falhará.

CLI

Para obter uma lista de todos os blueprints disponíveis usando o AWS CLI, envie uma list-pipeline-blueprintssolicitação.

```
aws osis list-pipeline-blueprints
```

A solicitação retorna uma lista com todos os esquemas disponíveis.

Para obter informações mais detalhadas sobre um blueprint específico, use o get-pipeline-blueprintcomando:

```
aws osis get-pipeline-blueprint --blueprint-name AWS-ApacheLogPipeline
```

Essa solicitação retorna o conteúdo do esquema do pipeline de log do Apache:

```
{
   "Blueprint":{
      "PipelineConfigurationBody":"###\n  # Limitations: https://docs.aws.amazon.com/
opensearch-service/latest/ingestion/ingestion.html#ingestion-limitations\n###\n###\n
 # apache-log-pipeline:\n    # This pipeline receives logs via http (e.g. FluentBit),
 extracts important values from the logs by matching\n    # the value in the 'log' key
 against the grok common Apache log pattern. The grokked logs are then sent\n    # to
 OpenSearch to an index named 'logs'\n###\n\nversion: \"2\"\napache-log-pipeline:\n
 source:\n    http:\n      # Provide the path for ingestion. ${pipelineName} will be
 replaced with pipeline name configured for this pipeline.\n      # In this case it
 would be \"/apache-log-pipeline/logs\". This will be the FluentBit output URI value.
\n      path: \"/${pipelineName}/logs\"\n  processor:\n    - grok:\n        match:\n
          log: [ \"%{COMMONAPACHELOG_DATATYPED}\" ]\n  sink:\n    - opensearch:\n
   # Provide an AWS OpenSearch Service domain endpoint\n        # hosts: [ \"https://
search-mydomain-1a2a3a4a5a6a7a8a9a0a9a8a7a.us-east-1.es.amazonaws.com\" ]\n
 aws:\n          # Provide a Role ARN with access to the domain. This role should have
 a trust relationship with osis-pipelines.amazonaws.com\n          # sts_role_arn:
 \"arn:aws:iam::123456789012:role/Example-Role\"\n          # Provide the region of the
 domain.\n          # region: \"us-east-1\"\n          # Enable the 'serverless' flag
 if the sink is an Amazon OpenSearch Serverless collection\n          # serverless:
 true\n        index: \"logs\"\n        # Enable the S3 DLQ to capture any failed
 requests in an S3 bucket\n        # dlq:\n          # s3:\n            # Provide an
 S3 bucket\n            # bucket: \"your-dlq-bucket-name\"\n            # Provide a key
 path prefix for the failed requests\n            # key_path_prefix: \"${pipelineName}/
logs/dlq\"\n            # Provide the region of the bucket.\n            # region:
 \"us-east-1\"\n            # Provide a Role ARN with access to the bucket. This role
 should have a trust relationship with osis-pipelines.amazonaws.com\n            #
 sts_role_arn: \"arn:aws:iam::123456789012:role/Example-Role\"\n",
      "BlueprintName":"AWS-ApacheLogPipeline"
   }
}
```

OpenSearch API de ingestão

Para obter informações sobre esquemas de pipeline usando a API de OpenSearch ingestão, use as operações ListPipelineBlueprintse. GetPipelineBlueprint

Visualizar pipelines da Ingestão do Amazon OpenSearch

Você pode ver os detalhes sobre um pipeline da Ingestão do Amazon OpenSearch usando o AWS Management Console, a AWS CLI ou o API de Ingestão de OpenSearch.

Console

Para visualizar um pipeline

1. Faça login no console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. No painel de navegação à esquerda, selecione Pipelines.
3. (Opcional) Para visualizar pipelines com um status específico, escolha Qualquer status e selecione um status para filtrar.

   Um pipeline pode ter os seguintes status:

   - `Creating`: o pipeline está sendo criado.
   - `Active`: o pipeline está ativo e pronto para ingerir dados.
   - `Updating`: o pipeline está sendo atualizado.
   - `Deleting`: o pipeline está sendo excluído.
   - `Create failed`: o pipeline não pôde ser criado.
   - `Update failed`: o pipeline não pôde ser atualizado.
   - `Starting`: o pipeline está sendo iniciado.
   - `Start failed`: o pipeline não pôde ser iniciado.
   - `Stopping`: o pipeline está sendo interrompido.
   - `Stopped`: o pipeline está parado e pode ser reiniciado a qualquer momento.

Você não paga pelas OCUs de ingestão quando um pipeline está nos estados `Create failed`, `Creating`, `Deleting` e `Stopped`.

CLI

Para visualizar pipelines usando a AWS CLI, envie uma solicitação list-pipelines:

```
aws osis list-pipelines
```

A solicitação retorna uma lista de todos os pipelines existentes:

```
{
    "NextToken": null,
    "Pipelines": [
        {,
            "CreatedAt": 1.671055851E9,
            "LastUpdatedAt": 1.671055851E9,
            "MaxUnits": 4,
            "MinUnits": 2,
            "PipelineArn": "arn:aws:osis:us-west-2:123456789012:pipeline/log-pipeline",
            "PipelineName": "log-pipeline",
            "Status": "ACTIVE",
            "StatusReason": {
                "Description": "The pipeline is ready to ingest data."
            }
        },
            "CreatedAt": 1.671055851E9,
            "LastUpdatedAt": 1.671055851E9,
            "MaxUnits": 2,
            "MinUnits": 8,
            "PipelineArn": "arn:aws:osis:us-west-2:123456789012:pipeline/another-
pipeline",
            "PipelineName": "another-pipeline",
            "Status": "CREATING",
            "StatusReason": {
                "Description": "The pipeline is being created. It is not able to ingest
 data."
            }
        }
    ]
}
```

Para obter informações sobre um único pipeline, use o comando get-pipeline:

```
aws osis get-pipeline --pipeline-name "my-pipeline"
```

A solicitação retorna informações de configuração para o pipeline especificado:

```
{
    "Pipeline": {
        "PipelineName": "my-pipeline",
        "PipelineArn": "arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline",
        "MinUnits": 9,
        "MaxUnits": 10,
        "Status": "ACTIVE",
        "StatusReason": {
            "Description": "The pipeline is ready to ingest data."
        },
        "PipelineConfigurationBody": "log-pipeline:\n source:\n http:\n processor:\n
 - grok:\n match:\nlog: [ '%{COMMONAPACHELOG}' ]\n - date:\n from_time_received: true
\n destination: \"@timestamp\"\n  sink:\n - opensearch:\n hosts: [ \"https://search-
mdp-performance-test-duxkb4qnycd63rpy6svmvyvfpi.us-east-1.es.amazonaws.com\" ]\n index:
 \"apache_logs\"\n aws_sts_role_arn: \"arn:aws:iam::123456789012:role/my-domain-role
\"\n  aws_region: \"us-east-1\"\n  aws_sigv4: true",,
        "CreatedAt": "2022-10-01T15:28:05+00:00",
        "LastUpdatedAt": "2022-10-21T21:41:08+00:00",
        "IngestEndpointUrls": [
            "my-pipeline-123456789012.us-east-1.osis.amazonaws.com"
        ]
    }
}
```

API de Ingestão de OpenSearch

Para visualizar os pipelines da Ingestão do OpenSearch usando a API de Ingestão de OpenSearch, chame as operações ListPipelines e GetPipeline.

Atualização dos pipelines OpenSearch de ingestão da Amazon

Você pode atualizar os pipelines OpenSearch de ingestão da Amazon usando a API AWS Management Console AWS CLI, a ou a API de OpenSearch ingestão. OpenSearch A ingestão inicia uma implantação azul/verde quando você atualiza a configuração YAML de um pipeline. Para ter mais informações, consulte the section called “Implantações azul/verde para atualizações de pipeline”.

Tópicos

- Permissões obrigatórias
- Atualizar pipelines
- Implantações azul/verde para atualizações de pipeline

Considerações

Considere o seguinte ao atualizar um pipeline:

- Você pode editar os limites de capacidade, as opções de publicação de logs e a configuração do YAML de um pipeline. Você não pode editar o nome ou as configurações de rede.
- Se o pipeline gravar em um coletor de domínio da VPC, você não pode voltar e alterar o coletor para um domínio de VPC diferente após a criação do pipeline. Você deve excluir e recriar o pipeline com o novo coletor. Você ainda pode mudar o coletor de um domínio da VPC para um domínio público, de um domínio público para um domínio VPC ou de um domínio público para outro domínio público.
- Você pode alternar o coletor do pipeline a qualquer momento entre um domínio OpenSearch de serviço público e uma OpenSearch coleção sem servidor.
- Quando você atualiza a configuração YAML de um pipeline, o OpenSearch Inestion inicia uma implantação azul/verde. Para ter mais informações, consulte the section called “Implantações azul/verde para atualizações de pipeline”.
- Quando você atualiza a configuração YAML de um pipeline, o OpenSearch Ingestion atualiza automaticamente seu pipeline para a versão secundária mais recente compatível da versão principal do Data Prepper especificada na configuração do pipeline. Esse processo mantém seu pipeline atualizado com as últimas correções de bugs e melhorias de desempenho.
- Você ainda pode fazer atualizações no seu pipeline quando ele estiver parado.

Permissões obrigatórias

OpenSearch A ingestão usa as seguintes permissões do IAM para atualizar os pipelines:

- `osis:UpdatePipeline` – atualizar um pipeline.
- `osis:ValidatePipeline` – verifica se a configuração do pipeline é válida.
- `iam:PassRole`— passe a função do pipeline para o OpenSearch Ingestion para que ele possa gravar dados no domínio. Essa permissão só é necessária se você estiver atualizando a

configuração YAML do pipeline, não se estiver modificando outras configurações, como publicação de logs ou limites de capacidade.

Por exemplo, a política a seguir concede permissão para atualizar um pipeline:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:UpdatePipeline",
            "osis:ValidatePipeline"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/{pipeline-role}"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
   ]
}
```

Atualizar pipelines

Você pode atualizar os pipelines OpenSearch de ingestão da Amazon usando a API AWS Management Console AWS CLI, a ou a API de OpenSearch ingestão.

Console

Como atualizar um pipeline

1. Faça login no console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. No painel de navegação à esquerda, selecione Pipelines.

3. Escolhe um pipeline para abrir suas configurações. Você pode editar os limites de capacidade, as opções de publicação de logs e a configuração do YAML de um pipeline. Você não pode editar o nome ou as configurações de rede.
4. Quando terminar de fazer as alterações, selecione Salvar.

CLI

Para atualizar um pipeline usando o AWS CLI, envie uma solicitação update-pipeline. O exemplo de solicitação a seguir carrega um novo arquivo de configuração e atualiza os valores de capacidade mínima e máxima:

```
aws osis update-pipeline \
  --pipeline-name "my-pipeline" \
  --pipline-configuration-body "file://new-pipeline-config.yaml" \
  --min-units 11 \
  --max-units 18
```

OpenSearch API de ingestão

Para atualizar um pipeline OpenSearch de ingestão usando a API OpenSearch de ingestão, chame a UpdatePipelineoperação.

Implantações azul/verde para atualizações de pipeline

OpenSearch A ingestão inicia um processo de implantação azul/verde quando você atualiza a configuração YAML de um pipeline.

Azul/verde refere-se à prática de criar um novo ambiente para atualizações de pipeline e rotear o tráfego para o novo ambiente assim que essas atualizações são concluídas. Essa prática minimiza o tempo de inatividade e mantém o ambiente original caso a implantação no novo ambiente seja malsucedida. As implantações azul/verde em si não têm nenhum impacto no desempenho, mas o desempenho poderá mudar se a configuração do pipeline mudar de uma forma que altere o desempenho.

OpenSearch A ingestão bloqueia o escalonamento automático durante implantações em azul/verde. Você continua sendo cobrado somente pelo tráfego do pipeline antigo até que ele seja redirecionado para o novo pipeline. Depois que o tráfego for redirecionado, você será cobrado apenas pelo novo pipeline. Você nunca será cobrado por dois pipelines simultaneamente.

Quando você atualiza o arquivo de configuração YAML de um pipeline, o OpenSearch Ingestion pode atualizar automaticamente seu pipeline para a versão secundária mais recente compatível da versão principal do Data Prepper especificada na configuração do pipeline. Por exemplo, você pode ter `version: "2"` na configuração do pipeline e a OpenSearch Ingestion inicialmente provisionou o pipeline com a versão 2.1.0. Quando o suporte para a versão 2.1.1 é adicionado e você faz uma alteração na configuração do pipeline, o OpenSearch Ingestion atualiza seu pipeline para a versão 2.1.1.

Esse processo mantém seu pipeline atualizado com as últimas correções de bugs e melhorias de desempenho. OpenSearch A ingestão não pode atualizar a versão principal do seu pipeline, a menos que você altere manualmente a `version` opção na configuração do pipeline.

Interromper e iniciar os pipelines de Ingestão do Amazon OpenSearch

Interromper e iniciar os pipelines de Ingestão do Amazon OpenSearch ajuda a gerenciar os custos dos ambientes de desenvolvimento e teste. Você pode interromper temporariamente um pipeline em lugar de configurá-lo e destruí-lo cada vez que você usa um pipeline.

Tópicos

Visão geral de como interromper e iniciar um pipeline da Ingestão do OpenSearch

Você pode interromper um pipeline durante períodos em que não precisa ingerir dados nele. Você pode iniciar o pipeline novamente a qualquer momento, sempre que precisar usá-lo. Iniciar e interromper simplifica os processos de configuração e destruição dos pipelines usados em desenvolvimento, teste ou atividades afins que não exijam disponibilidade contínua.

Enquanto seu pipeline estiver interrompido, você não será cobrado por nenhuma hora da OCU de ingestão. Você ainda pode atualizar pipelines interrompidos, e eles recebem atualizações automáticas de versões secundárias e patches de segurança.

Evite iniciar e interromper se você precisar manter seu pipeline em execução mas ele tiver mais capacidade do que o necessário. Se seu pipeline for muito caro ou não estiver muito ocupado, considere reduzir seus limites máximos de capacidade. Para obter mais informações, consulte the section called “Pipelines de escalabilidade”.

Interromper um pipeline da Ingestão do OpenSearch

Para usar ou realizar a administração de um pipeline da Ingestão do OpenSearch, você sempre começa com um pipeline ativo, depois interrompe e, em seguida, reinicia o pipeline. Enquanto seu pipeline estiver interrompido, você não precisará pagar por nenhuma hora da OCU de ingestão.

Console

Para interromper um pipeline

1. Faça login no console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. No painel de navegação, escolha Pipelines e, em seguida, escolha um pipeline. Você pode executar a operação de interrupção nesta página ou navegar até a página de detalhes do pipeline de banco de dados que você deseja interromper.
3. Em Ações, escolha Parar pipeline.

   Se um pipeline não puder ser interrompido e iniciado, a ação Stop pipeline não estará disponível.

AWS CLI

Para interromper um pipeline usando AWS CLI, chame o comando stop-pipeline com os seguintes parâmetros:

- `--pipeline-name` – nome do pipeline.

Example

```
aws osis stop-pipeline --pipeline-name my-pipeline
```

API de Ingestão do OpenSearch

Para interromper um pipeline usando a API de Ingestão do OpenSearch, chame a operação StopPipeline com o seguinte parâmetro:

- `PipelineName` – nome do pipeline.

Iniciar um pipeline da Ingestão do OpenSearch

Você deve sempre iniciar um pipeline da Ingestão do OpenSearch da Ingestão do OpenSearch começando com um pipeline do que já esteja em estado interrompido. O pipeline mantém suas configurações, como limites de capacidade, configurações de rede e opções de publicação de logs.

A reinicialização de um pipeline normalmente leva vários minutos.

Console

Para iniciar um pipeline

1. Faça login no console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. No painel de navegação, escolha Pipelines e, em seguida, escolha um pipeline. É possível executar a operação de início nesta página ou navegar até a página de detalhes do pipeline que você deseja iniciar.
3. Em Ações, escolha Iniciar pipeline.

AWS CLI

Para iniciar um pipeline usando a AWS CLI, chame o comando start-pipeline com os seguintes parâmetros:

- `--pipeline-name` – nome do pipeline.

Example

```
aws osis start-pipeline --pipeline-name my-pipeline
```

API de Ingestão de OpenSearch

Para iniciar um pipeline da Ingestão do OpenSearch usando a API de Ingestão de OpenSearch, chame a operação StartPipeline com o seguinte parâmetro:

- `PipelineName` – nome do pipeline.

Ingestão do Amazon OpenSearch

Você pode excluir um pipeline da Ingestão do Amazon OpenSearch usando AWS Management Console, AWS CLI ou a API de Ingestão de OpenSearch. Você não pode excluir um pipeline quando tem um status de `Creating` ou `Updating`.

Console

Para excluir um pipeline.

1. Faça login no console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. No painel de navegação à esquerda, selecione Pipelines.
3. Selecione o pipeline que deseja excluir e escolha Excluir.
4. Confirme a exclusão e escolha Excluir.

CLI

Para excluir um pipeline usando a AWS CLI, envie uma solicitação delete-pipeline:

```
aws osis delete-pipeline --pipeline-name "my-pipeline"
```

API de Ingestão do OpenSearch

Para excluir um pipeline da Ingestão do OpenSearch usando a API de Ingestão de OpenSearch, chame a operação DeletePipeline, com o seguinte parâmetro:

- `PipelineName` – nome do pipeline.

Plugins e opções compatíveis para pipelines OpenSearch de ingestão da Amazon

O Amazon OpenSearch Ingestion oferece suporte a um subconjunto de fontes, processadores e coletores em comparação com o Data Prepper de código aberto. Além disso, há algumas restrições que o OpenSearch Inestion impõe às opções disponíveis para cada plug-in compatível. As seções a seguir descrevem os plug-ins e as opções associadas compatíveis com o OpenSearch Inestion.

> **Note**
>
> OpenSearch A ingestão não oferece suporte a nenhum plug-in de buffer porque configura automaticamente um buffer padrão. Você receberá um erro de validação se incluir um buffer na configuração do pipeline.

Tópicos

Plug-ins compatíveis

OpenSearch O Inestion é compatível com os seguintes plug-ins do Data Prepper:

Sources (Origens):

- Dynamodb
- OpenSearch

- HTTP
- Kafka
- OTel logs (Logs do OTel)
- OTel metrics (Métricas do OTel)
- OTel trace (Rastreamento OTel)

- S3

Processadores:

- Aggregate
- Detector de anomalias
- CSV
- Data
- Descomprimir
- Dissecar
- Descarte eventos
- IP geográfico
- Grok
- Valor da chave
- Mapa para listar
- Evento de mutação (série de processadores)
- Mutate string (série de processadores)
- Obfuscate (Ofuscar)
- OTel metrics (Métricas do OTel)
- OTel trace group (Grupo de rastreamento OTel)
- OTel trace (Rastreamento OTel)
- Íon de análise
- Parse JSON (Analisar JSON)
- Analisar XML
- Selecionar entradas
- Mapa de serviço
- Rastrear o remetente entre os pares
- Truncar
- Agente de usuário

Coletores:

- OpenSearch(compatível com OpenSearch Service, OpenSearch Serverless e Elasticsearch 6.8 ou posterior)
- S3

Codecs Sink:

- Avro
- NDJSON
- JSON
- Parquet

Processadores sem estado x processadores com estado

Os processadores sem estado realizam operações como transformações e filtragem, enquanto os processadores com estado realizam operações como agregações, que lembram o resultado da execução anterior. OpenSearch A ingestão suporta os processadores com estado Aggregate e Service-MAP. Todos os outros processadores compatíveis são sem estado.

Para pipelines que contêm somente processadores sem estado, o limite máximo de capacidade é 96 OCUs de ingestão. Se um pipeline contiver algum processador com estado, o limite máximo de capacidade será de 48 OCUs de ingestão. No entanto, se um pipeline tiver o buffer persistente ativado, ele poderá ter no máximo 384 OCUs de ingestão com apenas processadores sem estado ou 192 OCUs de ingestão se contiver algum processador com estado. Para ter mais informações, consulte the section called “Pipelines de escalabilidade”.

O nd-to-end reconhecimento E só é suportado para processadores sem estado. Para ter mais informações, consulte the section called “E nd-to-end reconhecimento”.

Requisitos e restrições de configuração

A menos que especificado de outra forma abaixo, todas as opções descritas na referência de configuração do Data Prepper para os plug-ins compatíveis listados acima são permitidas nos pipelines OpenSearch de ingestão. As seções a seguir explicam as restrições que o OpenSearch Inestion impõe a determinadas opções de plug-in.

> **Note**
>
> OpenSearch A ingestão não oferece suporte a nenhum plug-in de buffer porque configura automaticamente um buffer padrão. Você receberá um erro de validação se incluir um buffer na configuração do pipeline.

Muitas opções são configuradas e gerenciadas internamente pelo OpenSearch Inestion, como e. `authentication` `acm_certificate_arn` Outras opções, como `thread_count` e `request_timeout`, sofrem impactos no desempenho se alteradas manualmente. Portanto, esses valores são definidos internamente para garantir o desempenho ideal de seus pipelines.

Por fim, algumas opções não podem ser passadas para a OpenSearch Ingestão, como `ism_policy_file` `esink_template`, porque são arquivos locais quando executados no Data Prepper de código aberto. Não oferece suporte a esses valores.

Tópicos

- Opções gerais de pipeline
- Processador Grok
- Origem HTTP
- OpenSearch pia
- Fonte de métricas do OTel, fonte de rastreamento do OTel e fonte de logs do OTel
- Processador de grupos de rastreamento OTel
- Processador OTel trace
- Processador de mapas de serviços
- Origem do S3

Opções gerais de pipeline

As seguintes opções gerais de pipeline são definidas pela OpenSearch Ingestão e não são suportadas nas configurações de pipeline:

- `workers`
- `delay`

Processador Grok

As seguintes opções do processador Grok não são compatíveis:

- `patterns_directories`
- `patterns_files_glob`

Origem HTTP

O plug-in de origem HTTP tem os seguintes requisitos e restrições:

- A opção `path` é obrigatória. O caminho é uma string como `/log/ingest`, que representa o caminho do URI para ingestão de logs. Esse caminho define o URI que você usa para enviar dados para o pipeline. Por exemplo, `https://log-pipeline.us-west-2.osis.amazonaws.com/log/ingest`. O caminho deve começar com uma barra (/) e pode conter os caracteres especiais '-', '_', ' . 'e'/', bem como o placeholder `${pipelineName}`.
- As seguintes opções de origem HTTP são definidas pelo OpenSearch Inestion e não são compatíveis com as configurações de pipeline:
  - `port`
  - `ssl`
  - `ssl_key_file`
  - `ssl_certificate_file`
  - `aws_region`
  - `authentication`
  - `unauthenticated_health_check`
  - `use_acm_certificate_for_ssl`
  - `thread_count`
  - `request_timeout`
  - `max_connection_count`
  - `max_pending_requests`
  - `health_check_service`
  - `acm_private_key_password`
  - `acm_certificate_timeout_millis`
  - `acm_certificate_arn`

OpenSearch pia

O plug-in OpenSearchsink tem os seguintes requisitos e limitações.

- A opção `aws` é obrigatória e deve conter as opções a seguir.
  - `sts_role_arn`
  - `region`
  - `hosts`
  - `serverless`(se o coletor for uma OpenSearch coleção sem servidor)
- A opção `sts_role_arn` deve apontar para a mesma função para cada coletor em um arquivo de definição YAML.
- A `hosts` opção deve especificar um endpoint OpenSearch de domínio de serviço ou um endpoint de coleta OpenSearch sem servidor. Todos os hosts em um arquivo de definição YAML devem apontar para o mesmo endpoint. Você não pode especificar um endpoint personalizado para um domínio; ele deve ser o endpoint padrão.
- Se a opção `hosts` for um endpoint de coleta de tecnologia sem servidor, você deverá definir a opção `serverless` como `true`. Além disso, se o arquivo de definição YAML contiver a opção `index_type`, ela deverá ser definida como `management_disabled`, caso contrário, a validação falhará.
- As seguintes opções não são compatíveis:
  - `username`
  - `password`
  - `cert`
  - `proxy`
  - `dlq_file`: se quiser transferir eventos com falha para uma fila de mensagens não entregues (DLQ), você deve usar a opção `dlq` e especificar um bucket do S3.
  - `ism_policy_file`
  - `socket_timeout`
  - `template_file`
  - `insecure`
  - `bulk_size`

Fonte de métricas do OTel, fonte de rastreamento do OTel e fonte de logs do OTel

Os plug-ins OTel metrics source, OTel trace source e OTel logs source têm os seguintes requisitos e limitações:

- A opção `path` é obrigatória. O caminho é uma string como `/log/ingest`, que representa o caminho do URI para ingestão de logs. Esse caminho define o URI que você usa para enviar dados para o pipeline. Por exemplo, `https://log-pipeline.us-west-2.osis.amazonaws.com/log/ingest`. O caminho deve começar com uma barra (/) e pode conter os caracteres especiais '-', '_', ' . 'e'/', bem como o placeholder `${pipelineName}`.
- As opções a seguir são definidas pelo OpenSearch Ingestion e não são compatíveis com as configurações de pipeline:
  - `port`
  - `ssl`
  - `sslKeyFile`
  - `sslKeyCertChainFile`
  - `authentication`
  - `unauthenticated_health_check`
  - `useAcmCertForSSL`
  - `unframed_requests`
  - `proto_reflection_service`
  - `thread_count`
  - `request_timeout`
  - `max_connection_count`
  - `acmPrivateKeyPassword`
  - `acmCertIssueTimeOutMillis`
  - `health_check_service`
  - `acmCertificateArn`
  - `awsRegion`

Processador de grupos de rastreamento OTel

O processador OTel trace group (Grupo de rastreamento OTel) apresenta os seguintes requisitos e limitações:

- A opção `aws` é obrigatória e deve conter as opções a seguir.
  - `sts_role_arn`
  - `region`
  - `hosts`
- A `sts_role_arn` opção especifica a mesma função do pipeline que você especifica na configuração do OpenSearch coletor.
- As opções `username`, `password`, `cert` e `insecure` não são compatíveis.
- A opção `aws_sigv4` é obrigatória e deve ser definida como verdadeira.
- A `serverless` opção dentro do plug-in do OpenSearch coletor não é suportada. Atualmente, o processador de grupos de rastreamento da Otel não funciona com coleções sem OpenSearch servidor.
- O número de processadores `otel_trace_group` dentro do corpo de configuração do pipeline não pode exceder 8.

Processador OTel trace

O processador OTel trace (Rastreamento OTel) apresenta os seguintes requisitos e limitações:

- O valor da opção `trace_flush_interval` não pode exceder 300 segundos.

Processador de mapas de serviços

O processador Service-map (Mapa de serviços) apresenta os seguintes requisitos e limitações:

- O valor da opção `window_duration` não pode exceder 300 segundos.

Origem do S3

O plug-in de origem do S3 tem os seguintes requisitos e limitações:

- A opção `aws` é obrigatória e deve conter as opções `region` e `sts_role_arn`.

- O valor da opção `records_to_accumulate` não pode exceder 200.
- O valor da opção `maximum_messages` não pode exceder 10.
- Se especificada, a opção `disable_bucket_ownership_validation` deve ser definida como falsa.
- Se especificada, a opção `input_serialization` deve ser definida como `parquet`.

Trabalhando com integrações de pipeline OpenSearch de ingestão da Amazon

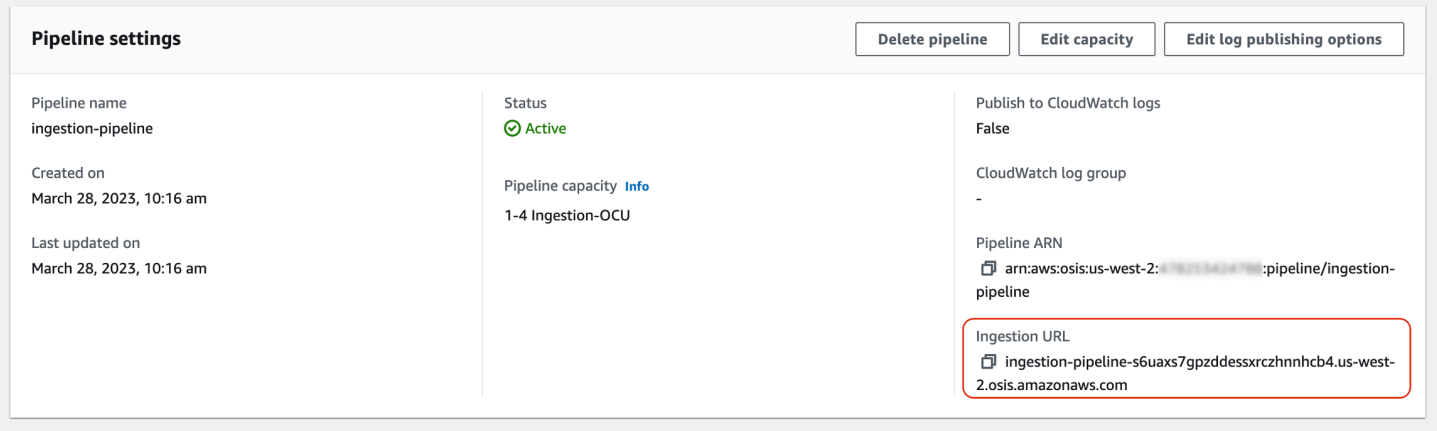
Para ingerir dados com sucesso em um pipeline de OpenSearch ingestão da Amazon, você deve configurar seu aplicativo cliente (a fonte) para enviar dados para o endpoint do pipeline. Sua fonte pode ser clientes como os registros do Fluent Bit, o OpenTelemetry Collector ou um simples bucket do S3. A configuração exata é diferente para cada cliente.

As diferenças importantes durante a configuração da fonte (em comparação com o envio de dados diretamente para um domínio de OpenSearch serviço ou coleção OpenSearch sem servidor) são o nome do AWS serviço (`osis`) e o endpoint do host, que deve ser o endpoint do pipeline.

Tópicos

Criar o endpoint de ingestão

Para ingerir dados em um pipeline, envie-os para o endpoint de ingestão. Para localizar o URL de ingestão, navegue até a página de Configurações do pipeline e copie o URL de ingestão:



Para criar o endpoint de ingestão completo para fontes baseadas em pull, como rastreamento de OTel e métricas de OTel, adicione o caminho de ingestão da configuração do pipeline ao URL de ingestão.

Por exemplo, digamos que a configuração do pipeline tem o seguinte caminho de ingestão:

```
entry-pipeline:
  source:
    http:
      path: "/my/test_path"
```

O endpoint de ingestão completo, que você especifica na configuração do seu cliente, terá o seguinte formato: `https://ingestion-pipeline-abcdefg.us-west-2.osis.amazonaws.com/my/test_path`.

Para ter mais informações, consulte the section called “Como especificar o caminho de ingestão”.

Criação de uma função de ingestão

Todas as solicitações de OpenSearch ingestão devem ser assinadas com o Signature versão 4. No mínimo, a função que assina a solicitação deve receber permissão para a `osis:Ingest` ação, o que permite que ela envie dados para um pipeline OpenSearch de ingestão.

Por exemplo, a política a seguir AWS Identity and Access Management (IAM) permite que a função correspondente envie dados para um único pipeline:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": "osis:Ingest",
      "Resource": "arn:aws:osis:us-east-1:{account-id}:pipeline/pipeline-name"
    }
  ]
}
```

> **Note**
>
> Para usar a função em todos os pipelines, substitua o ARN no elemento `Resource` por um caractere curinga (*).

Concessão de acesso de ingestão entre contas

> **Note**
>
> Você só pode fornecer acesso de ingestão entre contas para pipelines públicos, não para pipelines de VPC.

Talvez seja necessário ingerir dados em um pipeline de outro Conta da AWS, como uma conta que hospeda seu aplicativo de origem. Se a entidade principal que está gravando em um pipeline estiver em uma conta diferente do próprio pipeline, você precisará configurar a entidade principal para confiar em outro perfil do IAM para ingerir dados no pipeline.

Como configurar permissões de ingestão entre contas

1. Crie a função de ingestão com `osis:Ingest` permissão (descrita na seção anterior) dentro da Conta da AWS mesma função do pipeline. Para obter instruções, consulte Como criar perfis do IAM.
2. Vincule uma política de confiança à função de ingestão que permita que uma entidade principal em outra conta a assuma:

```
{
  "Version": "2012-10-17",
  "Statement": [{
     "Effect": "Allow",
     "Principal": {
```

```
        "AWS": "arn:aws:iam::{external-account-id}:root"
      },
     "Action": "sts:AssumeRole"
  }]
}
```

3. Na outra conta, configure seu aplicativo cliente (por exemplo, Fluent Bit) para assumir a função de ingestão. Para que isso funcione, a conta do aplicativo deve conceder permissões ao usuário ou à função do aplicativo para assumir a função de ingestão.

   O exemplo a seguir de política baseada em identidade permite que a entidade principal anexada assuma o `ingestion-role` a partir da conta do pipeline:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::{account-id}:role/ingestion-role"
    }
  ]
}
```

O aplicativo cliente pode então usar a AssumeRoleoperação para assumir `ingestion-role` e ingerir dados no pipeline associado.

Usando um pipeline de OpenSearch ingestão com o Amazon DynamoDB

Você pode usar um pipeline de OpenSearch ingestão com o DynamoDB para transmitir eventos de tabela do DynamoDB (como criar, atualizar e excluir) para domínios e coleções do Amazon Service. OpenSearch O pipeline OpenSearch de ingestão incorpora a infraestrutura de captura de dados de alteração (CDC) para fornecer uma forma de alta escala e baixa latência de transmitir dados continuamente de uma tabela do DynamoDB.

Há duas maneiras de usar o DynamoDB como origem para processar dados: com e sem um snapshot inicial completo.

Um instantâneo inicial completo é um backup de uma tabela que o DynamoDB faz com o recurso de recuperação (point-in-time PITR). O DynamoDB carrega esse snapshot no Amazon S3. A partir

daí, um pipeline de OpenSearch ingestão o envia para um índice em um domínio ou o particiona em vários índices em um domínio. Para manter os dados no DynamoDB OpenSearch e consistentes, o pipeline sincroniza todos os eventos de criação, atualização e exclusão na tabela do DynamoDB com os documentos salvos no índice ou índices. OpenSearch

Quando você usa um snapshot inicial completo, seu pipeline de OpenSearch ingestão primeiro ingere o snapshot e depois começa a ler os dados do DynamoDB Streams. Eventualmente, ele recupera e mantém a consistência de dados quase em tempo real entre o DynamoDB e. OpenSearch Ao escolher essa opção, habilite a PITR e um fluxo do DynamoDB na sua tabela.

Você também pode usar a integração do OpenSearch Ingestion com o DynamoDB para transmitir eventos sem um snapshot. Escolha essa opção se você já tiver um snapshot completo de algum outro mecanismo ou se quiser apenas transmitir eventos atuais de uma tabela do DynamoDB com o DynamoDB Streams. Ao escolher essa opção, você só precisa habilitar um fluxo do DynamoDB na sua tabela.

Para obter mais informações sobre essa integração, consulte Integração do DynamoDB Zero-ETL com o OpenSearch Amazon Service no Guia do desenvolvedor.Amazon DynamoDB

Tópicos

Pré-requisitos

Para configurar o pipeline, você precisa ter uma tabela do DynamoDB com o DynamoDB Streams habilitado. Seu fluxo deve usar o tipo de visualização de fluxo `NEW_IMAGE`. No entanto, os pipelines de OpenSearch ingestão também podem transmitir eventos `NEW_AND_OLD_IMAGES` se esse tipo de visualização de fluxo for adequado ao seu caso de uso.

Se você estiver usando instantâneos, também deverá ativar a point-in-time recuperação em sua tabela. Para obter mais informações, consulte Criar uma tabela, Habilitar a point-in-time recuperação e Habilitar um stream no Amazon DynamoDB Developer Guide.

Etapa 1: configurar a função do pipeline

Depois de configurar a tabela do DynamoDB, defina o perfil de pipeline que você deseja usar na configuração do pipeline e adicione as seguintes permissões do DynamoDB nesse perfil:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "allowRunExportJob",
            "Effect": "Allow",
            "Action": [
                "dynamodb:DescribeTable",
                "dynamodb:DescribeContinuousBackups",
                "dynamodb:ExportTableToPointInTime"
            ],
            "Resource": [
                "arn:aws:dynamodb:us-east-1:{account-id}:table/my-table"
            ]
        },
        {
            "Sid": "allowCheckExportjob",
            "Effect": "Allow",
            "Action": [
                "dynamodb:DescribeExport"
            ],
            "Resource": [
                "arn:aws:dynamodb:us-east-1:{account-id}:table/my-table/export/*"
            ]
        },
        {
            "Sid": "allowReadFromStream",
            "Effect": "Allow",
            "Action": [
                "dynamodb:DescribeStream",
                "dynamodb:GetRecords",
                "dynamodb:GetShardIterator"
            ],
            "Resource": [
                "arn:aws:dynamodb:us-east-1:{account-id}:table/my-table/stream/*"
            ]
        },
        {
```

```
            "Sid": "allowReadAndWriteToS3ForExport",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::my-bucket/export/*"
            ]
        }
    ]
}
```

Você também pode usar uma chave gerenciada pelo AWS KMS cliente para criptografar os arquivos de dados de exportação. Para descriptografar os objetos exportados, especifique `s3_sse_kms_key_id` para o ID da chave na configuração de exportação do pipeline, com o seguinte formato: `arn:aws:kms:us-west-2:{account-id}:key/my-key-id`.

Etapa 2: Criar o pipeline

Em seguida, você pode configurar um pipeline OpenSearch de ingestão como o seguinte, que especifica o DynamoDB como origem. Essa amostra de pipeline ingere dados de `table-a` com o snapshot de PITR, seguido por eventos do DynamoDB Streams. Uma posição inicial de `LATEST` indica que o pipeline deve ler os dados mais recentes do DynamoDB Streams.

```
version: "2"
cdc-pipeline:
  source:
    dynamodb:
      tables:
      - table_arn: "arn:aws:dynamodb:us-west-2:{account-id}:table/table-a"
        export:
          s3_bucket: "my-bucket"
          s3_prefix: "export/"
        stream:
          start_position: "LATEST"
      aws:
        region: "us-west-2"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
  sink:
```

```
  - opensearch:
      hosts: ["https://search-mydomain.us-east-1.es.amazonaws.com"]
      index: "${getMetadata(\"table_name\")}"
      index_type: custom
      document_id: "${getMetadata(\"primary_key\")}"
      action: "${getMetadata(\"opensearch_action\")}"
      document_version: "${getMetadata(\"document_version\")}"
      document_version_type: "external"
```

Você pode usar o blueprint do AWS-DynamoDB ChangeDataCapturePipeline ou do AWS-DynamoDB SingleTableDesignPipeline para criar esse pipeline. Para ter mais informações, consulte the section called “Usar esquemas para criar um pipeline”.

Consistência de dados

OpenSearch A ingestão suporta o end-to-end reconhecimento para garantir a durabilidade dos dados. Quando um pipeline lê snapshots ou fluxos, ele cria partições dinamicamente para processamento paralelo. O pipeline marca uma partição como concluída quando ela recebe uma confirmação após a ingestão de todos os registros no OpenSearch domínio ou na coleção.

Se quiser fazer a ingestão em uma coleção de pesquisa OpenSearch sem servidor, você pode gerar uma ID de documento no pipeline. Se você quiser fazer a ingestão em uma coleção de séries temporais OpenSearch sem servidor, observe que o pipeline não gera uma ID de documento.

Um pipeline OpenSearch de ingestão também mapeia as ações de eventos recebidos em ações de indexação em massa correspondentes para ajudar a ingerir documentos. Isso mantém os dados consistentes, de forma que cada alteração de dados no DynamoDB seja reconciliada com as alterações correspondentes no documento. OpenSearch

Mapeaar tipo de dados

OpenSearch O serviço mapeia dinamicamente os tipos de dados em cada documento recebido para o tipo de dados correspondente no DynamoDB. A tabela a seguir mostra como o OpenSearch Service mapeia automaticamente vários tipos de dados.

Tipo de dados	OpenSearch	DynamoDB
Número	OpenSearch mapeia automaticamente os dados numéricos. Se o número for	O DynamoDB é compatível com números.

Tipo de dados	OpenSearch	DynamoDB
	um número inteiro, OpenSearch mapeie-o como um valor longo. Se o número for fracionário, ele será OpenSearch mapeado como um valor flutuante. OpenSearch mapeia dinamicamente vários atributos com base no primeiro documento enviado. Se houver uma combinação de tipos de dados para o mesmo atributo no DynamoDB, como um número inteiro e um fracionário, o mapeamento poderá falhar. Por exemplo, se seu primeiro documento tiver um atributo que seja um número inteiro e um documento posterior tiver o mesmo atributo de um número fracionário, OpenSearch não conseguirá ingerir o segundo documento. Nesses casos, é necessário fornecer um modelo de mapeamento explícito, como o seguinte: `{ "template": { "mappings": { "properties": { "MixedNumberAttribute": { "type": "float" } } } } }` Se precisar de precisão dupla, use o mapeamento de campo do tipo string.	

Tipo de dados	OpenSearch	DynamoDB
	Não há nenhum tipo numérico equivalente que suporte 38 dígitos de precisão em. OpenSearch	
Number set	OpenSearch mapeia automaticamente um conjunto de números em uma matriz de valores longos ou valores flutuantes. Assim como os números escalares, isso depende de o primeiro número ingerido ser um número inteiro ou fracionário. É possível fornecer mapeamentos para conjuntos de números da mesma maneira que você mapeia strings escalares.	O DynamoDB oferece suporte a tipos que representam conjuntos de números.

Tipo de dados	OpenSearch	DynamoDB
String	OpenSearch mapeia automaticamente valores de string como texto. Em algumas situações, como valores enumerados, é possível mapear para o tipo de palavra-chave. O exemplo a seguir mostra como mapear um atributo do DynamoDB `PartType` nomeado para uma palavra-chave. OpenSearch `{ "template": { "mappings": { "properties": { "PartType": { "type": "keyword" } } } } }`	O DynamoDB é compatível com strings.
String set	OpenSearch mapeia automaticamente um conjunto de strings em uma matriz de strings. É possível fornecer mapeamentos para conjuntos de strings da mesma maneira que você mapeia strings escalares.	O DynamoDB oferece suporte a tipos que representam conjuntos de strings.

Tipo de dados	OpenSearch	DynamoDB
Binário	OpenSearch mapeia automaticamente dados binários como texto. Você pode fornecer um mapeamento para escrevê-los como campos binários OpenSearch. O exemplo a seguir mostra como mapear um atributo do DynamoDB `ImageData` nomeado para OpenSearch um campo binário. `{ "template": { "mappings": { "properties": { "ImageData": { "type": "binary" } } } } }`	O DynamoDB oferece suporte a atributos de tipo binário.
Binary Set	OpenSearch mapeia automaticamente um conjunto binário em uma matriz de dados binários como texto. É possível fornecer mapeamentos para conjuntos de números da mesma maneira que você mapeia binários escalares.	O DynamoDB oferece suporte a tipos que representam conjuntos de valores binários.
Booleano	OpenSearch mapeia um tipo booleano do DynamoDB em um tipo booleano. OpenSearch	O DynamoDB é compatível com atributos do tipo booliano.

Tipo de dados	OpenSearch	DynamoDB
Nulo	OpenSearch pode ingerir documento s com o tipo nulo do DynamoDB. Ele salva o valor como um valor nulo no documento. Não há mapeamento para esse tipo, e esse campo não é indexado nem pesquisável. Se o mesmo nome de atributo for usado para um tipo nulo e depois for alterado para um tipo diferente, como string, OpenSearch criará um mapeamento dinâmico para o primeiro valor não nulo. Os valores subsequentes ainda podem ser valores nulos do DynamoDB.	O DynamoDB oferece suporte a atributos de tipo nulo.

Tipo de dados	OpenSearch	DynamoDB
Mapa	OpenSearch mapeia os atributos do mapa do DynamoDB para campos aninhados. Os mesmos mapeamentos são aplicáveis a um campo aninhado. O exemplo a seguir mapeia uma string em um campo aninhado para um tipo de palavra-chave em OpenSearch: `{ "template": { "mappings": { "properties": { "AdditionalDescriptions": { "properties": { "PartType": { "type": "keyword" } } } } } } }`	O DynamoDB oferece suporte a atributos de tipo de mapa.

Tipo de dados	OpenSearch	DynamoDB
Lista	OpenSearch fornece resultados diferentes para as listas do DynamoDB, dependendo do que está na lista. Quando uma lista contém todos os mesmos tipos de tipos escalares (por exemplo, uma lista de todas as cadeias de caracteres), a lista é OpenSearc h ingerida como uma matriz desse tipo. Isso funciona para os tipos string, número, booliano e null. As restrições para cada um desses tipos são iguais às restrições para um escalar do mesmo tipo. Também é possível fornecer mapeament os para listas de mapas usando o mesmo mapeamento que você usaria para um mapa. Você não pode fornecer uma lista de tipos mistos.	O DynamoDB oferece suporte para atributos de tipo de lista.

Tipo de dados	OpenSearch	DynamoDB
Defina	OpenSearch fornece resultados diferentes para conjuntos do DynamoDB, dependendo do que está no conjunto. Quando um conjunto contém todos os mesmos tipos de tipos escalares (por exemplo, um conjunto de todas as cadeias de caracteres), ele OpenSearch ingere o conjunto como uma matriz desse tipo. Isso funciona para os tipos string, número, booliano e null. As restrições para cada um desses tipos são iguais às restrições para um escalar do mesmo tipo. Também é possível fornecer mapeamentos para conjuntos de mapas usando o mesmo mapeamento que você usaria para um mapa. Você não pode fornecer um conjunto de tipos mistos.	O DynamoDB oferece suporte a tipos que representam conjuntos.

Recomendamos que você configure a fila de mensagens mortas (DLQ) em seu pipeline de ingestão. OpenSearch Se você configurou a fila, o OpenSearch Service envia todos os documentos com falha que não podem ser ingeridos devido a falhas de mapeamento dinâmico para a fila.

Se os mapeamentos automáticos falharem, será possível usar `template_type` e `template_content` na configuração do pipeline para definir regras de mapeamento explícitas. Como alternativa, é possível criar modelos de mapeamento diretamente no seu domínio de pesquisa ou na sua coleção antes de iniciar o pipeline.

Limitações

Considere as seguintes limitações ao configurar um pipeline de OpenSearch ingestão para o DynamoDB:

- Atualmente, a integração de OpenSearch ingestão com o DynamoDB não oferece suporte à ingestão entre regiões. Sua tabela do DynamoDB OpenSearch e seu pipeline de ingestão devem estar no mesmo lugar. Região da AWS
- Sua tabela do DynamoDB OpenSearch e seu pipeline de ingestão devem estar no mesmo lugar. Conta da AWS
- Um pipeline OpenSearch de ingestão suporta somente uma tabela do DynamoDB como origem.
- O DynamoDB Streams apenas armazena dados em log por até 24 horas. Se a ingestão de um snapshot inicial de uma tabela grande levar 24 horas ou mais, haverá uma certa perda inicial de dados. Para mitigar essa perda de dados, estime o tamanho da tabela e configure as unidades computacionais apropriadas dos pipelines de OpenSearch ingestão.

Usando um pipeline OpenSearch de ingestão com Amazon Managed Streaming for Apache Kafka

Você pode usar o plug-in Kafka para ingerir dados do Amazon Managed Streaming for Apache Kafka (Amazon MSK) em seu pipeline de ingestão. OpenSearch Com o Amazon MSK, você pode criar e executar aplicativos que usam o Apache Kafka para processar dados em streaming. OpenSearch A ingestão é usada AWS PrivateLink para se conectar ao Amazon MSK.

Tópicos

Pré-requisitos

Antes de criar seu pipeline OpenSearch de ingestão, execute as seguintes etapas:

1. Crie um cluster do Amazon MSK seguindo as etapas em Criar um cluster no Guia do desenvolvedor do Amazon Managed Streaming para Apache Kafka.
   - Em Tipo de cluster, escolha Provisionado. OpenSearch A ingestão não é compatível com clusters MSK sem servidor.
2. Depois que o cluster tiver um status Ativo, siga as etapas em Ativar a conectividade de várias VPCs.
3. Siga as etapas em Anexar uma política de cluster ao cluster MSK para anexar uma das políticas a seguir, dependendo se o cluster e o pipeline estão na mesma Conta da AWS. Essa política permite que o OpenSearch Inestion crie uma AWS PrivateLink conexão com seu cluster Amazon MSK e leia dados de tópicos do Kafka. Lembre-se de atualizar o `resource` com seu próprio ARN.

   As políticas a seguir se aplicam quando o cluster e o pipeline estão na mesma Conta da AWS:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:us-east-1:{account-id}:cluster/cluster-name/cluster-
id"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis-pipelines.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:GetBootstrapBrokers",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2"
      ],
```

```
      "Resource": "arn:aws:kafka:us-east-1:{account-id}:cluster/cluster-name/cluster-
id"
    }
  ]
}
```

Se seu cluster MSK estiver em um local Conta da AWS diferente do seu pipeline, anexe a política a seguir. O ARN do AWS `principal` deve ser o ARN da mesma função de pipeline que você fornece à configuração YAML do pipeline:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:us-east-1:{msk-account-id}:cluster/cluster-
name/cluster-id"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis-pipelines.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:GetBootstrapBrokers",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:us-east-1:{msk-account-id}:cluster/cluster-
name/cluster-id"
    },
    {
      "Effect": "Allow",
      "Principal": {
```

```
        "AWS": "arn:aws:iam::{pipeline-account-id}:role/pipeline-role"
      },
      "Action": [
        "kafka-cluster:*",
        "kafka:*"
      ],
      "Resource": [
        "arn:aws:kafka:us-east-1:{msk-account-id}:cluster/cluster-name/cluster-id",
        "arn:aws:kafka:us-east-1:{msk-account-id}:topic/cluster-name/cluster-id/*",
        "arn:aws:kafka:us-east-1:{msk-account-id}:group/cluster-name/*"
      ]
    }
  ]
}
```

4. Crie um tópico do Kafka seguindo as etapas em Criar um tópico. Assegure-se de que *BootstrapServerString* seja um dos URLs de bootstrap do endpoint privado (VPC única). O valor de `--replication-factor` deve ser 2 ou 3, com base no número de zonas que seu cluster MSK tem. O valor de `--partitions` deve ser pelo menos 10.
5. Produza e consuma dados seguindo as etapas em Produzir e consumir dados. Novamente, verifique se *BootstrapServerString* é um dos seus URLs de bootstrap de endpoint privado (VPC única).

Etapa 1: configurar a função do pipeline

Depois de configurar seu cluster MSK, adicione as seguintes permissões do Kafka na função do pipeline que você deseja usar na configuração do pipeline:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:Connect",
                "kafka-cluster:AlterCluster",
                "kafka-cluster:DescribeCluster",
                "kafka:DescribeClusterV2",
                "kafka:GetBootstrapBrokers"
            ],
            "Resource": [
```

```
                "arn:aws:kafka:us-east-1:{account-id}:cluster/cluster-name/cluster-id"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:*Topic*",
                "kafka-cluster:ReadData"
            ],
            "Resource": [
                "arn:aws:kafka:us-east-1:{account-id}:topic/cluster-name/cluster-
id/topic-name"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:AlterGroup",
                "kafka-cluster:DescribeGroup"
            ],
            "Resource": [
                "arn:aws:kafka:us-east-1:{account-id}:group/cluster-name/*"
            ]
        }
    ]
}
```

Etapa 2: Criar o pipeline

Em seguida, você pode configurar um pipeline de OpenSearch ingestão como o seguinte, que especifica o Kafka como fonte:

```
version: "2"
log-pipeline:
  source:
    kafka:
      acknowledgements: true
      topics:
      - name: "topic-name"
        group_id: "group-id"
        serde_format: "json"/"plaintext"
      aws:
        msk:
```

```
          arn: "arn:aws:iam::{account-id}:role/cluster-role"
        region: "us-west-2"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      schema:                                # Optional
        type: "aws_glue"
  processor:
  - grok:
      match:
        log:
        - "%{COMMONAPACHELOG}"
  - date:
      destination: "@timestamp"
      from_time_received: true
  sink:
  - opensearch:
      hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
      index: "index_name"
      aws_sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      aws_region: "us-east-1"
      aws_sigv4: true
```

Você pode usar o esquema do AWS-MSKPipeline para criar esse pipeline. Para ter mais informações, consulte the section called “Usar esquemas para criar um pipeline”.

Etapa 3: (Opcional) Usar o Registro do AWS Glue Esquema

Ao usar o OpenSearch Inestion com o Amazon MSK, você pode usar o formato de dados AVRO para esquemas hospedados no Schema Registry. AWS Glue Com o registro de esquema do AWS Glue, você pode descobrir, controlar e evoluir centralmente esquemas de fluxo de dados.

Para usar essa opção, habilite o esquema `type` na configuração do seu pipeline:

```
schema:
  type: "aws_glue"
```

Você também deve AWS Glue fornecer permissões de acesso de leitura em sua função de funil. Você pode usar a política AWS gerenciada chamada AWSGlueSchemaRegistryReadonlyAccess. Além disso, seu registro deve estar na mesma Conta da AWS região do pipeline OpenSearch de ingestão.

Etapa 4: (opcional) configurar unidades computacionais (OCUs) recomendadas para o pipeline do Amazon MSK

Cada unidade computacional tem um consumidor por tópico. Os corretores equilibram as partições entre esses consumidores para um determinado tópico. No entanto, quando o número de partições é maior que o número de consumidores, o Amazon MSK hospeda várias partições em cada consumidor. OpenSearch A ingestão tem escalonamento automático integrado para aumentar ou diminuir a escala com base no uso da CPU ou no número de registros pendentes no pipeline.

Para um desempenho ideal, distribua suas partições em várias unidades de computação para processamento paralelo. Se os tópicos tiverem um grande número de partições (por exemplo, mais de 96, que é o máximo de OCUs por pipeline), recomendamos que você configure um pipeline com 1 a 96 OCUs. Isso ocorre porque ele será escalado automaticamente conforme necessário. Se um tópico tiver um número baixo de partições (por exemplo, menos de 96), mantenha o máximo de unidades computacionais igual ao número de partições.

Quando um pipeline tiver mais de um tópico, escolha o tópico com o maior número de partições como referência para configurar o máximo de unidades computacionais. Ao adicionar outro pipeline com um novo conjunto de OCUs ao mesmo tópico e grupo de consumidores, você pode escalar o throughput quase linearmente.

Usando um pipeline OpenSearch de ingestão com o Amazon S3

Com OpenSearch a ingestão, você pode usar o Amazon S3 como origem ou destino. Ao usar o Amazon S3 como fonte, você envia dados para um pipeline de OpenSearch ingestão. Ao usar o Amazon S3 como destino, você grava dados de um pipeline de OpenSearch ingestão em um ou mais buckets do S3.

Tópicos

Amazon S3 como origem

Há duas maneiras de usar o Amazon S3 como fonte para processar dados: com o processamento do S3-SQS e com escaneamentos agendados.

Use o processamento S3-SQS quando precisar escanear arquivos quase em tempo real depois que eles forem gravados no S3. Você pode configurar buckets do Amazon S3 para gerar um evento sempre que um objeto for armazenado ou modificado dentro do bucket. Use uma verificação agendada única ou recorrente para processar dados em lote em um bucket do S3.

Tópicos

Pré-requisitos

Para usar o Amazon S3 como fonte de um pipeline de OpenSearch ingestão para uma verificação programada ou processamento do S3-SQS, primeiro crie um bucket do S3.

> **Note**
>
> Se o bucket do S3 usado como fonte no pipeline de OpenSearch ingestão estiver em outro Conta da AWS, você também precisará habilitar as permissões de leitura entre contas no bucket. Isso permite que o pipeline leia e processe os dados. Para habilitar permissões entre contas, consulte Bucket owner granting cross-account bucket permissions (Conceder permissões de bucket entre contas como proprietário do bucket) no Guia do usuário do Amazon S3.
>
> Se seus buckets do S3 estiverem em várias contas, use um `bucket_owners` mapa. Para ver um exemplo, consulte Acesso ao S3 entre contas na OpenSearch documentação.

Para configurar o processamento do S3-SQS, você também precisa executar as seguintes etapas:

1. Como criar uma fila do Amazon SQS.
2. Ative as notificações de eventos no bucket do S3 com a fila SQS como destino.

Etapa 1: configurar a função do pipeline

Ao contrário de outros plug-ins de origem que enviam dados para um pipeline, o plug-in de origem do S3 tem uma arquitetura baseada em leitura na qual o pipeline extrai dados da fonte.

Portanto, para que um pipeline seja lido do S3, você deve especificar uma função na configuração de origem do S3 do pipeline que tenha acesso ao bucket do S3 e à fila do Amazon SQS. O pipeline assumirá essa função para ler os dados da fila.

> **Note**
>
> A função que você especifica na configuração de origem do S3 deve ser a função do pipeline. Portanto, sua função de pipeline deve conter duas políticas de permissões separadas: uma para gravar em um coletor e outra para extrair da origem do S3. Você deve usar o mesmo `sts_role_arn` em todos os componentes do pipeline.

O exemplo de política a seguir mostra as permissões necessárias para usar o S3 como fonte:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action":[
          "s3:ListBucket",
          "s3:GetBucketLocation",
          "s3:GetObject"
       ],
      "Resource": "arn:aws:s3:::my-bucket/*"
    },
    {
       "Effect":"Allow",
       "Action":"s3:ListAllMyBuckets",
       "Resource":"arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sqs:DeleteMessage",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility"
      ],
      "Resource": "arn:aws:sqs:us-west-2:{account-id}:MyS3EventSqsQueue"
    }
  ]
```

```
}
```

Você deve anexar essas permissões ao perfil do IAM especificado na opção `sts_role_arn` na configuração do plug-in de origem do S3:

```
version: "2"
source:
  s3:
    ...
    aws:
      ...
      sts_role_arn: arn:aws:iam::{account-id}:role/pipeline-role
processor:
  ...
sink:
  - opensearch:
      ...
```

Etapa 2: Criar o pipeline

Depois de configurar suas permissões, você pode configurar um pipeline de OpenSearch ingestão, dependendo do seu caso de uso do Amazon S3.

Processamento do S3-SQS

Para configurar o processamento do S3-SQS, configure seu pipeline para especificar o S3 como origem e configure as notificações do Amazon SQS:

```
version: "2"
s3-pipeline:
  source:
    s3:
      notification_type: "sqs"
      codec:
        newline: null
      sqs:
        queue_url: "https://sqs.us-east-1.amazonaws.com/{account-id}/ingestion-queue"
      compression: "none"
      aws:
        region: "us-east-1"
        # IAM role that the pipeline assumes to read data from the queue. This role
 must be the same as the pipeline role.
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
```

```
  processor:
  - grok:
      match:
        log:
        - "%{COMMONAPACHELOG}"
  - date:
      destination: "@timestamp"
      from_time_received: true
  sink:
  - opensearch:
      hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
      index: "index-name"
      aws:
        # IAM role that the pipeline assumes to access the domain sink
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
        region: "us-east-1"
```

Se você observar uma baixa utilização da CPU ao processar arquivos pequenos no Amazon S3, considere aumentar a taxa de transferência modificando o valor da opção. `workers` Para obter mais informações, consulte as opções de configuração do plug-in S3.

Varredura agendada

Para configurar uma verificação agendada, configure seu pipeline com uma programação no nível da verificação que se aplique a todos os seus buckets do S3 ou no nível de bucket. Uma programação em nível de bucket ou uma configuração de intervalo de escaneamento sempre substitui uma configuração em nível de escaneamento.

Você pode configurar escaneamentos agendados com um escaneamento único, que é ideal para migração de dados, ou um escaneamento recorrente, que é ideal para processamento em lote.

Para configurar seu pipeline para ler do Amazon S3, use os blueprints do Amazon S3 chamados AWS-S3 ou AWS-S3. ScanPipeline ScanSchedulePipeline Você pode editar a parte da `scan` da configuração do seu pipeline para atender às suas necessidades de agendamento. Para ter mais informações, consulte the section called “Usar esquemas para criar um pipeline”.

Digitalização única

Uma varredura agendada única é executada uma vez. Na sua configuração YAML, você pode usar `start_time` e `end_time` para especificar quando deseja que os objetos no bucket sejam digitalizados. Como alternativa, você pode usar `range` para especificar o intervalo de tempo em relação ao horário atual em que você deseja que os objetos no bucket sejam digitalizados.

Por exemplo, um intervalo definido para PT4H verificar todos os arquivos criados nas últimas quatro horas. Para configurar uma varredura única para ser executada pela segunda vez, você deve parar e reiniciar o pipeline. Se você não tiver um intervalo configurado, também deverá atualizar os horários de início e término.

A configuração a seguir configura uma varredura única para todos os buckets e todos os objetos nesses buckets:

```
version: "2"
log-pipeline:
  source:
    s3:
      codec:
        csv:
      compression: "none"
      aws:
        region: "us-east-1"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      acknowledgments: true
      scan:
        buckets:
          - bucket:
              name: my-bucket-1
              filter:
                include_prefix:
                  - Objects1/
                exclude_suffix:
                  - .jpeg
                  - .png
          - bucket:
              name: my-bucket-2
              key_prefix:
                include:
                  - Objects2/
                exclude_suffix:
                  - .jpeg
                  - .png
      delete_s3_objects_on_read: false
  processor:
    - date:
        destination: "@timestamp"
        from_time_received: true
  sink:
```

```
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index: "index-name"
        aws:
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"
        dlq:
          s3:
            bucket: "my-bucket-1"
            region: "us-east-1"
            sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
```

A configuração a seguir configura uma varredura única para todos os buckets durante uma janela de tempo especificada. Isso significa que o S3 processa somente os objetos com horários de criação que se enquadram nessa janela.

```
scan:
  start_time: 2023-01-21T18:00:00.000Z
  end_time: 2023-04-21T18:00:00.000Z
  buckets:
    - bucket:
        name: my-bucket-1
        filter:
          include:
            - Objects1/
          exclude_suffix:
            - .jpeg
            - .png
    - bucket:
        name: my-bucket-2
        filter:
          include:
            - Objects2/
          exclude_suffix:
            - .jpeg
            - .png
```

A configuração a seguir configura uma verificação única no nível de escaneamento e no nível do bucket. Os horários de início e término no nível do bucket substituem os horários de início e término no nível do escaneamento.

```
scan:
```

```
  start_time: 2023-01-21T18:00:00.000Z
  end_time: 2023-04-21T18:00:00.000Z
  buckets:
    - bucket:
        start_time: 2023-01-21T18:00:00.000Z
        end_time: 2023-04-21T18:00:00.000Z
        name: my-bucket-1
        filter:
          include:
            - Objects1/
          exclude_suffix:
            - .jpeg
            - .png
    - bucket:
        start_time: 2023-01-21T18:00:00.000Z
        end_time: 2023-04-21T18:00:00.000Z
        name: my-bucket-2
        filter:
          include:
            - Objects2/
          exclude_suffix:
            - .jpeg
            - .png
```

A interrupção de uma tubulação remove qualquer referência preexistente de quais objetos foram escaneados pela tubulação antes da parada. Se um único pipeline de escaneamento for interrompido, ele digitalizará novamente todos os objetos após seu início, mesmo que eles já tenham sido escaneados. Se você precisar interromper um único pipeline de escaneamento, é recomendável alterar sua janela de tempo antes de iniciar o pipeline novamente.

Se você precisar filtrar objetos por hora de início e hora de término, parar e iniciar seu funil é a única opção. Se você não precisar filtrar por hora de início e hora de término, poderá filtrar objetos por nome. Filtrar por nome não exige que você pare e inicie seu funil. Para fazer isso, use `include_prefix` `exclude_suffix` e.

Escaneamento recorrente

Uma verificação agendada recorrente executa uma varredura de seus buckets S3 especificados em intervalos regulares e agendados. Você só pode configurar esses intervalos no nível de escaneamento porque não há suporte para configurações individuais em nível de bucket.

Na sua configuração YAML, o `interval` especifica a frequência da verificação recorrente e pode ser entre 30 segundos e 365 dias. A primeira dessas varreduras sempre ocorre quando você cria o pipeline. `count` define o número total de instâncias de verificação.

A configuração a seguir configura um escaneamento recorrente, com um atraso de 12 horas entre os escaneamentos:

```
scan:
  scheduling:
    interval: PT12H
    count: 4
  buckets:
    - bucket:
        name: my-bucket-1
        filter:
          include:
            - Objects1/
          exclude_suffix:
            - .jpeg
            - .png
    - bucket:
        name: my-bucket-2
        filter:
          include:
            - Objects2/
          exclude_suffix:
            - .jpeg
            - .png
```

Amazon S3 como destino

Para gravar dados de um pipeline de OpenSearch ingestão em um bucket do S3, use o blueprint chamado AWS-S3 SinkLogPipeline para criar um pipeline com um coletor do S3. Esse pipeline encaminha dados seletivos para um OpenSearch coletor e envia simultaneamente todos os dados para arquivamento no S3. Para ter mais informações, consulte the section called “Usar esquemas para criar um pipeline”.

Ao criar seu coletor S3, você pode especificar sua formatação preferida a partir de uma variedade de codecs de coletor. Por exemplo, se você quiser gravar dados em formato de coluna, escolha o codec Parquet ou Avro. Se você preferir um formato baseado em linhas, escolha JSON ou ND-JSON. Para

gravar dados no S3 em um esquema especificado, você também pode definir um esquema embutido nos codecs de coletor usando o formato Avro.

O exemplo a seguir define um esquema embutido em um coletor do S3:

```
- s3:
  codec:
    parquet:
      schema: >
        {
           "type" : "record",
           "namespace" : "org.vpcFlowLog.examples",
           "name" : "VpcFlowLog",
           "fields" : [
             { "name" : "version", "type" : "string"},
             { "name" : "srcport", "type": "int"},
             { "name" : "dstport", "type": "int"},
             { "name" : "start", "type": "int"},
             { "name" : "end", "type": "int"},
             { "name" : "protocol", "type": "int"},
             { "name" : "packets", "type": "int"},
             { "name" : "bytes", "type": "int"},
             { "name" : "action", "type": "string"},
             { "name" : "logStatus", "type" : "string"}
           ]
         }
```

Ao definir esse esquema, especifique um superconjunto de todas as chaves que podem estar presentes nos diferentes tipos de eventos que seu pipeline entrega a um coletor.

Por exemplo, se um evento tiver a possibilidade de uma chave faltar, adicione essa chave em seu esquema com um valor `null`. Declarações de valor nulo permitem que o esquema processe dados não uniformes (onde alguns eventos têm essas chaves e outros não). Quando os eventos recebidos têm essas chaves presentes, seus valores são gravados em coletores.

Essa definição de esquema atua como um filtro que só permite que chaves definidas sejam enviadas aos coletores e elimina chaves indefinidas dos eventos recebidos.

Você também pode usar `include_keys` e `exclude_keys` no seu coletor para filtrar dados que são roteados para outros coletores. Esses dois filtros são mutuamente exclusivos, então você só pode usar um por vez em seu esquema. Além disso, não é possível usá-los em esquemas definidos pelo usuário.

Para criar pipelines com esses filtros, use o AWSSinkFilterWithSchemaPipelineblueprint. Para ter mais informações, consulte the section called “Usar esquemas para criar um pipeline”.

Conta cruzada do Amazon S3 como fonte

Você pode conceder acesso a várias contas com o Amazon S3 para que os pipelines de OpenSearch ingestão possam acessar buckets do S3 em outra conta como fonte. A configuração YAML a seguir permite o acesso de várias contas a um bucket do Amazon S3 como fonte:

```
s3-pipeline:
 source:
  s3:
   notification_type: "sqs"
   codec:
    csv:
     delimiter: ","
     quote_character: "\""
     detect_header: True
   sqs:
    queue_url: "https://sqs.ap-northeast-1.amazonaws.com/401447383613/test-s3-queue"
   bucket_owners:
    user-role-1234567890: 1234567890 # User1
    user-role-12345678891: 1234567891 # User2
   compression: "gzip"
```

Usando um pipeline OpenSearch de ingestão com o Amazon Security Lake

Você pode usar o plug-in de origem do S3 para ingerir dados do Amazon Security Lake em seu pipeline de OpenSearch ingestão. O Security Lake centraliza automaticamente os dados de segurança de AWS ambientes, ambientes locais e provedores de SaaS em um data lake específico. Você pode criar uma assinatura que replica os dados do Security Lake para o pipeline de OpenSearch ingestão e, em seguida, os grava no domínio do OpenSearch Service ou na coleção OpenSearch Serverless.

Para configurar seu pipeline para ler do Security Lake, use o blueprint do Security Lake chamado AWS- SecurityLake S3ParqueToCSFPipeline. O esquema inclui uma configuração padrão para ingerir arquivos de parquet do Open Cybersecurity Schema Framework (OCSF) do Security Lake. Para ter mais informações, consulte the section called “Usar esquemas para criar um pipeline”.

Tópicos

Pré-requisitos

Antes de criar seu pipeline OpenSearch de ingestão, execute as seguintes etapas:

- Habilitar o Security Lake.
- Criar um assinante no Security Lake.
  - Escolha as fontes que você deseja ingerir em seu pipeline.
  - Em Credenciais de assinante, adicione o ID da Conta da AWS em que você pretende criar o pipeline. Para o ID externo, especifique `OpenSearchIngestion-{accountid}`.
  - Em Método de acesso a dados, escolha S3.
  - Para Detalhes de notificação, escolha SQS queue.

Quando você cria um assinante, o Security Lake cria automaticamente duas políticas de permissões em linha: uma para o S3 e outra para SQS. As políticas têm o seguinte formato: `AmazonSecurityLake-{12345}-S3` e `AmazonSecurityLake-{12345}-SQS`. Para permitir que seu pipeline acesse as origens de assinantes, você deve associar as permissões necessárias à sua função do pipeline.

Etapa 1: configurar a função do pipeline

Crie uma nova política de permissões no IAM que combine somente as permissões necessárias das duas políticas que o Security Lake criou automaticamente. O exemplo de política a seguir mostra o menor privilégio necessário para que um pipeline de OpenSearch ingestão leia dados de várias fontes do Security Lake:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject"
         ],
```

```
         "Resource":[
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/
LAMBDA_EXECUTION/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/S3_DATA/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/VPC_FLOW/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/ROUTE53/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/SH_FINDINGS/1.0/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "sqs:ReceiveMessage",
            "sqs:DeleteMessage"
         ],
         "Resource":[
            "arn:aws:sqs:{region}:{account-id}:AmazonSecurityLake-abcde-Main-Queue"
         ]
      }
   ]
}
```

> **Important**
>
> O Security Lake não gerencia a política de função do pipeline para você. Se você adicionar ou remover fontes da sua assinatura do Security Lake, deverá atualizar a política manualmente. O Security Lake cria partições para cada fonte de log, então você precisa adicionar ou remover manualmente as permissões na função de pipeline.

Você deve anexar essas permissões ao perfil do IAM que você especifica na opção `sts_role_arn` na configuração do plug-in de origem do S3, em `sqs`.

```
version: "2"
source:
  s3:
    ...
    sqs:
      queue_url: "https://sqs.{region}.amazonaws.com/{account-id}/
AmazonSecurityLake-abcde-Main-Queue"
    aws:
      ...
```

```
      sts_role_arn: arn:aws:iam::{account-id}:role/pipeline-role
processor:
  ...
sink:
  - opensearch:
      ...
```

Etapa 2: Criar o pipeline

Depois de adicionar as permissões à função do pipeline, use o blueprint AWS- SecurityLake S3ParqueToCSFPipeline para criar o pipeline. Para ter mais informações, consulte the section called "Usar esquemas para criar um pipeline".

Você deve especificar a opção `queue_url` na configuração de origem do `s3`, que é o URL da fila do Amazon SQS para leitura. Para formatar o URL, localize o endpoint da assinatura na configuração do assinante e altere `arn:aws:` para `https://`. Por exemplo, `https://sqs.{region}.amazonaws.com/{account-id}/AmazonSecurityLake-abdcef-Main-Queue`.

O `sts_role_arn` que você especifica na configuração de origem do S3 deve ser o ARN da função do pipeline.

Usando um pipeline de OpenSearch ingestão com o FluentBit

Esse exemplo de arquivo de configuração do Fluent Bit envia dados de log do Fluent Bit para um pipeline de OpenSearch ingestão. Para obter mais informações sobre a ingestão de dados de log, consulte Log Analytics na documentação do Data Prepper.

Observe o seguinte:

- O valor `host` deve ser o endpoint do seu pipeline. Por exemplo, *`pipeline-endpoint`*`.us-east-1.osis.amazonaws.com`.
- O valor de `aws_service` deve ser `osis`.
- O `aws_role_arn` valor é o ARN da função do AWS IAM que o cliente deve assumir e usar para a autenticação Signature versão 4.

```
[INPUT]
  name                  tail
  refresh_interval      5
```

```
  path                  /var/log/test.log
  read_from_head        true

[OUTPUT]
  Name http
  Match *
  Host pipeline-endpoint.us-east-1.osis.amazonaws.com
  Port 443
  URI /log/ingest
  Format json
  aws_auth true
  aws_region us-east-1
  aws_service osis
  aws_role_arn arn:aws:iam::{account-id}:role/ingestion-role
  Log_Level trace
  tls On
```

Em seguida, você pode configurar um pipeline de OpenSearch ingestão como o seguinte, que tem HTTP como origem:

```
version: "2"
unaggregated-log-pipeline:
  source:
    http:
      path: "/log/ingest"
  processor:
    - grok:
        match:
          log:
            - "%{TIMESTAMP_ISO8601:timestamp} %{NOTSPACE:network_node}
 %{NOTSPACE:network_host} %{IPORHOST:source_ip}:%{NUMBER:source_port:int} ->
 %{IPORHOST:destination_ip}:%{NUMBER:destination_port:int} %{GREEDYDATA:details}"
    - grok:
        match:
          details:
            - "'%{NOTSPACE:http_method} %{NOTSPACE:http_uri}' %{NOTSPACE:protocol}"
            - "TLS%{NOTSPACE:tls_version} %{GREEDYDATA:encryption}"
            - "%{NUMBER:status_code:int} %{NUMBER:response_size:int}"
    - delete_entries:
        with_keys: ["details", "log"]

  sink:
    - opensearch:
```

```
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index: "index_name"
        index_type: custom
        bulk_size: 20
        aws:
          # IAM role that the pipeline assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"
```

Usando um pipeline OpenSearch de ingestão com OpenTelemetry o Collector

Esse exemplo de arquivo de OpenTelemetry configuração exporta dados de rastreamento do OpenTelemetry Collector e os envia para um pipeline OpenSearch de ingestão. Para obter mais informações sobre a ingestão de dados de rastreamento, consulte Análise de rastreamento na documentação do Data Prepper.

Observe o seguinte:

- O valor `endpoint` deve incluir o endpoint do seu pipeline. Por exemplo, `https://pipeline-endpoint.us-east-1.osis.amazonaws.com`.
- O valor de `service` deve ser `osis`.
- A `compression` opção para o exportador OTLP/HTTP deve corresponder à `compression` opção na fonte do pipeline. OpenTelemetry

```
extensions:
  sigv4auth:
    region: "us-east-1"
    service: "osis"

receivers:
  jaeger:
    protocols:
      grpc:

exporters:
  otlphttp:
    traces_endpoint: "https://pipeline-endpoint.us-east-1.osis.amazonaws.com/v1/traces"
    auth:
      authenticator: sigv4auth
```

```
    compression: none

service:
  extensions: [sigv4auth]
  pipelines:
    traces:
      receivers: [jaeger]
      exporters: [otlphttp]
```

Em seguida, você pode configurar um pipeline de OpenSearch ingestão como o seguinte, que especifica o plug-in de rastreamento OTel como fonte:

```
version: "2"
otel-trace-pipeline:
  source:
    otel_trace_source:
      path: "/v1/traces"
  processor:
    - trace_peer_forwarder:
  sink:
    - pipeline:
        name: "trace-pipeline"
    - pipeline:
        name: "service-map-pipeline"
trace-pipeline:
  source:
    pipeline:
      name: "otel-trace-pipeline"
  processor:
    - otel_traces:
  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index_type: trace-analytics-raw
        aws:
          # IAM role that OpenSearch Ingestion assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"

service-map-pipeline:
  source:
    pipeline:
      name: "otel-trace-pipeline"
```

```
  processor:
    - service_map:
  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index_type: trace-analytics-service-map
        aws:
          # IAM role that the pipeline assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"
```

Para ver outro exemplo de pipeline, consulte o esquema do pipeline do Trace Analytics. Para ter mais informações, consulte the section called “Usar esquemas para criar um pipeline”.

Próximas etapas

Depois de exportar seus dados para um pipeline, você pode consultá-los no domínio OpenSearch Service que está configurado como um coletor para o pipeline. Os seguintes recursos podem ajudá-lo a começar:

- A instalação padrão do OpenSearch Dashboards para Amazon OpenSearch Service inclui o plug-in de Observabilidade, que você pode usar para visualizar eventos controlados por dados usando a Piped Processing Language (PPL) para explorar, descobrir e consultar dados armazenados no OpenSearch.
- the section called “Trace Analytics”
- the section called “Piped Processing Language”

Migração de dados entre domínios e coleções usando o Amazon Ingestion OpenSearch

Você pode usar pipelines OpenSearch de ingestão para migrar dados entre domínios do Amazon OpenSearch Service ou coleções de VPC sem servidor OpenSearch . Para fazer isso, você configura um pipeline no qual configura um domínio ou coleção como origem e outro domínio ou coleção como coletor. Isso migra efetivamente seus dados de um domínio ou coleção para outro.

Para migrar dados, você deve ter os seguintes recursos:

- Um domínio de OpenSearch serviço de origem ou uma coleção de OpenSearch VPC sem servidor. Esse domínio ou coleção contém os dados que você deseja migrar. Se você estiver

usando um domínio, ele deverá estar executando a OpenSearch versão 1.0 ou posterior, ou a versão 7.4 ou posterior do Elasticsearch. O domínio também deve ter uma política de acesso que conceda as permissões apropriadas à sua função no pipeline.

- Um domínio separado ou coleção de VPC para o qual você deseja migrar seus dados. Esse domínio ou coleção funcionará como o coletor do pipeline.
- Uma função de pipeline que o OpenSearch Ingestion usará para ler e gravar em sua coleção ou domínio. Você inclui o Amazon Resource Name (ARN) dessa função na configuração do seu pipeline. Para obter mais informações, consulte os seguintes recursos do :
  - the section called “Concedendo acesso aos pipelines aos domínios”
  - the section called “Concedendo aos oleodutos acesso às coleções”

Tópicos

Limitações

As seguintes limitações se aplicam quando você designa domínios OpenSearch de serviço ou coleções OpenSearch sem servidor como coletores:

- Um pipeline não pode gravar em mais de um domínio VPC.
- Você só pode migrar dados de ou para coleções OpenSearch sem servidor que usam acesso VPC. Não há suporte para coleções públicas.
- Você não pode especificar uma combinação de VPC e domínios públicos em uma única configuração de pipeline.
- Você pode ter no máximo 20 coletores sem tubulação em uma única configuração de tubulação.
- Você pode especificar coletores de no máximo três diferentes Regiões da AWS em uma única configuração de pipeline.
- Um pipeline com vários coletores pode sofrer uma redução na velocidade de processamento ao longo do tempo se algum dos coletores ficar inativo por muito tempo ou não for provisionado com capacidade suficiente para receber dados de entrada.

OpenSearch Serviço como fonte

O domínio ou coleção que você especifica como fonte é de onde os dados são migrados.

Criar um perfil de pipeline no IAM

Para criar seu pipeline de OpenSearch ingestão, primeiro você deve criar uma função de pipeline para conceder acesso de leitura e gravação entre domínios ou coleções. Para fazer isso, execute as seguintes etapas:

1. Crie uma nova política de permissões no IAM para anexar à função do pipeline. Certifique-se de conceder permissões para ler a partir da fonte e gravar no coletor. Para obter mais informações sobre como definir permissões de pipeline do IAM para domínios de OpenSearch serviço, consulte the section called “Concedendo acesso aos pipelines aos domínios” e. the section called “Concedendo aos oleodutos acesso às coleções”
2. Especifique as seguintes permissões na função do pipeline para ler a partir da fonte:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"es:ESHttpGet",
         "Resource":[
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_cat/indices",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_search",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_search/scroll",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/*/_search"
         ]
      },
      {
         "Effect":"Allow",
         "Action":"es:ESHttpPost",
         "Resource":[
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/*/_search/
point_in_time",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/*/_search/scroll"
         ]
      },
      {
         "Effect":"Allow",
```

```
            "Action":"es:ESHttpDelete",
            "Resource":[
               "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_search/
point_in_time",
               "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_search/scroll"
            ]
         }
      ]
}
```

Criando um pipeline

Depois de anexar a política à função do pipeline, use o blueprint de AWSOpenSearchDataMigrationPipelinemigração para criar o pipeline. Esse esquema inclui uma configuração padrão para migrar dados entre domínios ou coleções OpenSearch de serviços. Para ter mais informações, consulte the section called “Usar esquemas para criar um pipeline”.

> **Note**
>
> OpenSearch A ingestão usa a versão e a distribuição do domínio de origem para determinar qual mecanismo usar para a migração. Algumas versões oferecem suporte à `point_in_time` opção. OpenSearch O Serverless usa a `search_after` opção porque ela não suporta `point_in_time` ou. `scroll`

Novos índices podem estar sendo criados durante o processo de migração, ou documentos podem estar sendo atualizados enquanto a migração está em andamento. Por isso, talvez seja necessário fazer uma única ou várias verificações dos dados de índice do domínio para obter dados novos ou atualizados.

Especifique o número de verificações a serem executadas, definindo `index_read_count` e `interval` na configuração do pipeline. O exemplo a seguir mostra como fazer várias verificações:

```
scheduling:
    interval: "PT2H"
    index_read_count: 3
    start_time: "2023-06-02T22:01:30.00Z"
```

OpenSearch A ingestão usa a seguinte configuração para garantir que seus dados sejam gravados no mesmo índice e mantenham a mesma ID do documento:

```
index: "${getMetadata(\"opensearch-index\")}"
document_id: "${getMetadata(\"opensearch-document_id\")}"
```

Especificação de vários coletores OpenSearch de domínio de serviço

Você pode especificar vários domínios OpenSearch de serviço público como destinos para seus dados. Você pode usar esse recurso para realizar roteamento condicional ou replicar dados de entrada em vários domínios de serviço. OpenSearch Você pode especificar até 10 domínios de OpenSearch serviço público diferentes como coletores.

No exemplo a seguir, os dados recebidos são roteados condicionalmente para diferentes OpenSearch domínios de serviço:

```
...
  route:
    - 2xx_status: "/response >= 200 and /response < 300"
    - 5xx_status: "/response >= 500 and /response < 600"
  sink:
    - opensearch:
        hosts: [ "https://search-response-2xx.us-east-1.es.amazonaws.com" ]
        aws:
          sts_role_arn: "arn:aws:iam::123456789012:role/Example-Role"
          region: "us-east-1"
        index: "response-2xx"
        routes:
          - 2xx_status
    - opensearch:
        hosts: [ "https://search-response-5xx.us-east-1.es.amazonaws.com" ]
        aws:
          sts_role_arn: "arn:aws:iam::123456789012:role/Example-Role"
          region: "us-east-1"
        index: "response-5xx"
        routes:
          - 5xx_status
```

Migração de dados para uma coleção de OpenSearch VPC sem servidor

Você pode usar o OpenSearch Inestion para migrar dados de um domínio de OpenSearch serviço de origem ou de uma coleção OpenSearch sem servidor para um coletor de coleta de VPC. Você deve fornecer uma política de acesso à rede na configuração do pipeline. Para obter mais informações sobre a ingestão de dados em coleções de VPC OpenSearch sem servidor, consulte. the section called “Tutorial: Ingestão de dados em uma coleção”

Para migrar dados para uma coleção de VPC

1. Crie uma coleção OpenSearch sem servidor. Para obter instruções, consulte the section called “Tutorial: Ingestão de dados em uma coleção”.
2. Crie uma política de rede para a coleção que especifique o acesso via VPC ao endpoint da coleção e ao endpoint do Dashboards. Para obter instruções, consulte the section called “Acesso à rede”.
3. Crie o perfil de pipeline se ainda não tiver um. Para obter instruções, consulte the section called “Perfis do pipeline”.
4. Criar o pipeline. Para obter instruções, consulte the section called “Usar esquemas para criar um pipeline”.

Uso de SDKs da AWS para interagir com a Ingestão do Amazon OpenSearch

Esta seção inclui exemplos de como usar os SDKs da AWS para interagir com a Ingestão do Amazon OpenSearch. O exemplo de código demonstra como criar um domínio e um pipeline e, em seguida, ingerir dados no pipeline.

Tópicos

- Python

Python

O script de exemplo a seguir usa o AWS SDK for Python (Boto3) para criar uma função de pipeline do IAM, um domínio para gravar dados e um pipeline para ingerir dados. Em seguida, ele ingere um arquivo de log de amostra no pipeline usando a biblioteca HTTP de `requests`.

Execute os comandos a seguir para instalar as dependências necessárias:

```
pip install boto3
pip install botocore
pip install requests
pip install requests-auth-aws-sigv4
```

No script, substitua os IDs da conta nas políticas de acesso pelo seu ID da Conta da AWS. Você também pode, opcionalmente, modificar a `region`.

```
import boto3
import botocore
from botocore.config import Config
import requests
from requests_auth_aws_sigv4 import AWSSigV4
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a Region other than your default.
    region_name='us-east-1'
)

opensearch = boto3.client('opensearch', config=my_config)
iam = boto3.client('iam', config=my_config)
osis = boto3.client('osis', config=my_config)

domainName = 'test-domain'  # The name of the domain
pipelineName = 'test-pipeline' # The name of the pipeline

def createPipelineRole(iam, domainName):
    """Creates the pipeline role"""
    response = iam.create_policy(
        PolicyName='pipeline-policy',
        PolicyDocument=f'{{\"Version\":\"2012-10-17\",\"Statement\":[{{\"Effect
\":\"Allow\",\"Action\":\"es:DescribeDomain\",\"Resource\":\"arn:aws:es:us-
east-1:123456789012:domain\/{domainName}\"}},{{\"Effect\":\"Allow\",\"Action\":
\"es:ESHttp*\",\"Resource\":\"arn:aws:es:us-east-1:123456789012:domain\/{domainName}\/*
\"}}]}}'
    )
```

```
    policyarn = response['Policy']['Arn']

    response = iam.create_role(
        RoleName='PipelineRole',
        AssumeRolePolicyDocument='{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Principal\":{\"Service\":\"osis-pipelines.amazonaws.com\"},\"Action\":
\"sts:AssumeRole\"}]}'
    )
    rolename=response['Role']['RoleName']

    response = iam.attach_role_policy(
        RoleName=rolename,
        PolicyArn=policyarn
    )

    print('Creating pipeline role...')
    time.sleep(10)
    print('Role created: ' + rolename)

def createDomain(opensearch, domainName):
    """Creates a domain to ingest data into"""
    response = opensearch.create_domain(
        DomainName=domainName,
        EngineVersion='OpenSearch_2.3',
        ClusterConfig={
            'InstanceType': 't2.small.search',
            'InstanceCount': 5,
            'DedicatedMasterEnabled': True,
            'DedicatedMasterType': 't2.small.search',
            'DedicatedMasterCount': 3
        },
        # Many instance types require EBS storage.
        EBSOptions={
            'EBSEnabled': True,
            'VolumeType': 'gp2',
            'VolumeSize': 10
        },
        AccessPolicies=f'{{\"Version\":\"2012-10-17\",\"Statement\":[{{\"Effect\":
\"Allow\",\"Principal\":{{\"AWS\":\"arn:aws:iam::123456789012:role\/PipelineRole
\"}},\"Action\":\"es:*\",\"Resource\":\"arn:aws:es:us-east-1:123456789012:domain\/
{domainName}\/*\"}}]}}',
        NodeToNodeEncryptionOptions={
            'Enabled': True
        }
```

```
    )
    return(response)

def waitForDomainProcessing(opensearch, domainName):
    """Waits for the domain to be active"""
    try:
        response = opensearch.describe_domain(
            DomainName=domainName
        )
        # Every 30 seconds, check whether the domain is processing.
        while 'Endpoint' not in response['DomainStatus']:
            print('Creating domain...')
            time.sleep(60)
            response = opensearch.describe_domain(
                DomainName=domainName)

        # Once we exit the loop, the domain is ready for ingestion.
        endpoint = response['DomainStatus']['Endpoint']
        print('Domain endpoint ready to receive data: ' + endpoint)
        createPipeline(osis, endpoint)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
            print('Domain not found.')
        else:
            raise error

def createPipeline(osis, endpoint):
    """Creates a pipeline using the domain and pipeline role"""
    try:
        definition = f'version: \"2\"\nlog-pipeline:\n  source:\n    http:\n      path:
 \"/${{pipelineName}}/logs\"\n  processor:\n    - date:\n        from_time_received:
 true\n        destination: \"@timestamp\"\n  sink:\n    - opensearch:\n        hosts:
 [ \"https://{endpoint}\" ]\n        index: \"application_logs\"\n        aws:\n
     sts_role_arn: \"arn:aws:iam::123456789012:role/PipelineRole\"\n          region:
 \"us-east-1\"'
        response = osis.create_pipeline(
            PipelineName=pipelineName,
            MinUnits=4,
            MaxUnits=9,
            PipelineConfigurationBody=definition
        )

        response = osis.get_pipeline(
```

```
                PipelineName=pipelineName
        )

        # Every 30 seconds, check whether the pipeline is active.
        while response['Pipeline']['Status'] == 'CREATING':
            print('Creating pipeline...')
            time.sleep(30)
            response = osis.get_pipeline(
                PipelineName=pipelineName)

        # Once we exit the loop, the pipeline is ready for ingestion.
        ingestionEndpoint = response['Pipeline']['IngestEndpointUrls'][0]
        print('Pipeline ready to ingest data at endpoint: ' + ingestionEndpoint)
        ingestData(ingestionEndpoint)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceAlreadyExistsException':
            print('Pipeline already exists.')
            response = osis.get_pipeline(
                PipelineName=pipelineName
            )
            ingestionEndpoint = response['Pipeline']['IngestEndpointUrls'][0]
            ingestData(ingestionEndpoint)
        else:
            raise error


def ingestData(ingestionEndpoint):
    """Ingests a sample log file into the pipeline"""
    endpoint = 'https://' + ingestionEndpoint
    r = requests.request('POST', f'{endpoint}/log-pipeline/logs',

 data='[{"time":"2014-08-11T11:40:13+00:00","remote_addr":"122.226.223.69","status":"404","requ
 http://www.k2proxy.com//hello.html HTTP/1.1","http_user_agent":"Mozilla/4.0
 (compatible; WOW64; SLCC2;)"}]',
    auth=AWSSigV4('osis'))
    print('Ingesting sample log file into pipeline')
    print('Response: ' + r.text)

def main():
    createPipelineRole(iam, domainName)
    createDomain(opensearch, domainName)
    waitForDomainProcessing(opensearch, domainName)
```

```
if __name__ == "__main__":
    main()
```

Casos de uso da Ingestão do Amazon OpenSearch

Este capítulo demonstra alguns casos de uso comuns da Ingestão do Amazon OpenSearch. Essa lista não é exaustiva. Para ver os recursos completos de cada plug-in compatível, consulte Fontes, Processadores e Coletores na documentação do Data Prepper.

Tópicos

- Correspondência de padrões Grok com a Ingestão do Amazon OpenSearch
- Enriquecimento de logs com a Ingestão do Amazon OpenSearch
- Agregação de eventos com Ingestão do Amazon OpenSearch
- Derivar métricas de logs com a Ingestão do Amazon OpenSearch
- Trace Analytics com Ingestão do Amazon OpenSearch
- Derivação de métricas de rastreamento com a Ingestão do Amazon OpenSearch
- Detecção de anomalias com a Ingestão do Amazon OpenSearch
- Amostragem com Ingestão do Amazon OpenSearch
- Download seletivo com Ingestão do Amazon OpenSearch

Correspondência de padrões Grok com a Ingestão do Amazon OpenSearch

A Ingestão do Amazon OpenSearch fornece recursos de correspondência de padrões com o processador Grok. O processador Grok é baseado na biblioteca `java-grok` e suporta todos os padrões compatíveis. A biblioteca `java-grok` é criada usando a biblioteca de expressões `java.util.regex` regulares.

Você pode adicionar padrões personalizados aos seus pipelines usando a opção `patterns_definitions`. Ao depurar padrões personalizados, o Grok Debugger pode ser útil.

Além desses exemplos, você também pode usar o esquema do pipeline de log do Apache. Para obter mais informações sobre esquemas, consulte the section called “Usar esquemas para criar um pipeline”.

Tópicos

- Uso básico

- Incluir capturas nomeadas e vazias
- Sobrescrever chaves
- Usar padrões personalizados
- Armazenar capturas com uma chave principal

Uso básico

Para começar com a correspondência de padrões, crie o seguinte pipeline:

```
version: "2"
patten-matching-pipeline:
  source
    ...
  processor:
    - grok:
        match:
          message: ['%{IPORHOST:clientip} \[%{HTTPDATE:timestamp}\]
 %{NUMBER:response_status:int}']
  sink:
    - opensearch:
        # Provide an OpenSearch Service domain endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
        index: "metrics_for_traces"
        # serverless: true
```

Uma mensagem recebida no pipeline pode ter o seguinte conteúdo:

```
{"message": "127.0.0.1 198.126.12 [10/Oct/2000:13:55:36 -0700] 200"}
```

O pipeline localizará o valor na chave `message` de cada evento recebido e tentará corresponder ao padrão. As palavras-chave `IPORHOST`, `HTTPDATE` e `NUMBER` são incorporadas ao plug-in.

Quando um registro recebido corresponde ao padrão, ele gera um evento interno como o seguinte, com chaves de identificação extraídas da mensagem original.

```
{
```

```
  "message":"127.0.0.1 198.126.12 [10/Oct/2000:13:55:36 -0700] 200",
  "response_status":200,
  "clientip":"198.126.12",
  "timestamp":"10/Oct/2000:13:55:36 -0700"
}
```

A configuração `match` do processador Grok especifica quais chaves de um registro devem corresponder a quais padrões.

No exemplo a seguir, a configuração da correspondência verifica se há uma chave `message` nos logs recebidos. Se a chave existir, ela combina o valor da chave com o padrão `SYSLOGBASE` e, em seguida, com o padrão `COMMONAPACHELOG`. Depois, ela verifica os logs em busca de uma chave `timestamp`. Se a chave existir, ela tentará comparar o valor da chave com o padrão `TIMESTAMP_ISO8601`.

```
processor:
  - grok:
      match:
        message: ['%{SYSLOGBASE}', "%{COMMONAPACHELOG}"]
        timestamp: ["%{TIMESTAMP_ISO8601}"]
```

Por padrão, o plugin continua até encontrar uma correspondência bem-sucedida. Por exemplo, se houver uma correspondência bem-sucedida com o valor na chave `message` de um padrão `SYSLOGBASE`, o plug-in não tentará corresponder aos outros padrões. Se quiser comparar os logs com cada padrão, inclua a opção `break_on_match`.

Incluir capturas nomeadas e vazias

Inclua a opção `keep_empty_captures` na configuração do pipeline para incluir capturas nulas ou a opção `named_captures_only` para incluir somente capturas nomeadas. Capturas nomeadas seguem o padrão `%{SYNTAX:SEMANTIC}`, enquanto capturas sem nome seguem o padrão `%{SYNTAX}`.

Por exemplo, você pode modificar a configuração do Grok acima para remover `clientip` do padrão `%{IPORHOST}`:

```
processor:
  - grok:
      match:
```

```
        message: ['%{IPORHOST} \[%{HTTPDATE:timestamp}\]
 %{NUMBER:response_status:int}']
```

O log do Grok resultante será semelhante ao seguinte:

```
{
  "message":"127.0.0.1 198.126.12 [10/Oct/2000:13:55:36 -0700] 200",
  "response_status":200,
  "timestamp":"10/Oct/2000:13:55:36 -0700"
}
```

Observe que a chave `clientip` não existe mais, porque o padrão `%{IPORHOST}` agora é uma captura sem nome.

No entanto, se você definir `named_captures_only` como `false`:

```
processor:
  - grok:
      match:
        named_captures_only: false
        message: ['%{IPORHOST} \[%{HTTPDATE:timestamp}\] %{NUMBER:message:int}']
```

O log do Grok resultante será semelhante ao seguinte:

```
{
  "message":"127.0.0.1 198.126.12 [10/Oct/2000:13:55:36 -0700] 200",
  "MONTH":"Oct",
  "YEAR":"2000",
  "response_status":200,
  "HOUR":"13",
  "TIME":"13:55:36",
  "MINUTE":"55",
  "SECOND":"36",
  "IPORHOST":"198.126.12",
  "MONTHDAY":"10",
  "INT":"-0700",
  "timestamp":"10/Oct/2000:13:55:36 -0700"
}
```

Observe que a captura `IPORHOST` agora aparece como uma nova chave, junto com algumas capturas internas sem nome, como `MONTH` e `YEAR`. A palavra-chave `HTTPDATE` está usando esses padrões, que você pode ver no arquivo de padrões padrão.

Sobrescrever chaves

Inclua a opção `keys_to_overwrite` para especificar quais chaves existentes de um registro devem ser substituídas se houver uma captura com o mesmo valor de chave.

Por exemplo, você pode modificar a configuração do Grok acima para substituir `%{NUMBER:response_status:int}` por `%{NUMBER:message:int}` e adicionar `message` à lista de chaves a serem substituídas.

```
processor:
  - grok:
      match:
        keys_to_overwrite: ["message"]
        message: ['%{IPORHOST:clientip} \[%{HTTPDATE:timestamp}\]
 %{NUMBER:message:int}']
```

No log isolado resultante, a mensagem original é substituída pelo número 200.

```
{
  "message":200,
  "clientip":"198.126.12",
  "timestamp":"10/Oct/2000:13:55:36 -0700"
}
```

Usar padrões personalizados

Inclua a opção `pattern_definitions` na configuração do Grok para especificar padrões personalizados.

A configuração a seguir cria padrões de regex personalizados chamados `CUSTOM_PATTERN-1` e `CUSTOM_PATTERN-2`. Por padrão, o plugin continua até encontrar uma correspondência bem-sucedida.

```
processor:
  - grok:
      pattern_definitions:
        CUSTOM_PATTERN_1: 'this-is-regex-1'
        CUSTOM_PATTERN_2: '%{CUSTOM_PATTERN_1} REGEX'
      match:
        message: ["%{CUSTOM_PATTERN_2:my_pattern_key}"]
```

Se você especificar `break_on_match` como `false`, o pipeline tentará combinar todos os padrões e extrair as chaves dos eventos recebidos:

```
processor:
  - grok:
      pattern_definitions:
        CUSTOM_PATTERN_1: 'this-is-regex-1'
        CUSTOM_PATTERN_2: 'this-is-regex-2'
        CUSTOM_PATTERN_3: 'this-is-regex-3'
        CUSTOM_PATTERN_4: 'this-is-regex-4'
      match:
        message: [ "%{PATTERN1}”, "%{PATTERN2}" ]
        log: [ "%{PATTERN3}", "%{PATTERN4}" ]
        break_on_match: false
```

Você pode definir seus próprios padrões personalizados para usar na correspondência de padrões em pipelines. No exemplo anterior, `my_pattern` será extraído após combinar os padrões personalizados.

Armazenar capturas com uma chave principal

Inclua a opção `target_key` na configuração do Grok para agrupar todas as capturas de um registro em um valor de chave externa adicional.

Por exemplo, você pode modificar a configuração do Grok acima para adicionar uma chave de destino chamada`grokked`.

```
processor:
   - grok:
       target_key: "grok"
       match:
         message: ['%{IPORHOST} \[%{HTTPDATE:timestamp}\]
 %{NUMBER:response_status:int}']
```

O log do Grok resultante será semelhante ao seguinte:

```
{
  "message":"127.0.0.1 198.126.12 [10/Oct/2000:13:55:36 -0700] 200",
  "grokked": {
     "response_status":200,
     "clientip":"198.126.12",
     "timestamp":"10/Oct/2000:13:55:36 -0700"
```

```
  }
}
```

Enriquecimento de logs com a Ingestão do Amazon OpenSearch

Você pode realizar diferentes tipos de enriquecimento de logs com a Ingestão do Amazon OpenSearch. Além desses exemplos, você também pode usar o esquema do Pipeline de log genérico. Para obter mais informações sobre esquemas, consulte the section called “Usar esquemas para criar um pipeline”.

Tópicos

Filtrar

Use o processador Drop events (Eliminar eventos) para filtrar eventos de log específicos antes de enviá-los para um coletor. Por exemplo, digamos que você esteja coletando logs de solicitações da Web e queira armazenar somente solicitações malsucedidas. Você cria o seguinte pipeline, que descarta todas as solicitações em que a resposta é menor que 400, de forma que somente eventos de log com códigos de status HTTP 400 ou superiores permaneçam.

```
version: "2"
log-pipeline:
  source:
  ...
  processor:
    - grok:
        match:
          log: [ "%{COMMONAPACHELOG_DATATYPED}" ]
    - drop:
        drop_when: "/response < 400"
  sink:
    - opensearch:
```

```
        ...
        index: failure_logs
```

A opção `drop_when` especifica quais pares devem ser retirados do pipeline.

Extrair pares de chave/valor de cadeias de caracteres

Os dados de log geralmente incluem sequências de pares de chave/valor. Um cenário comum é uma sequência de caracteres de consulta HTTP. Por exemplo, se um usuário da Web consultar um URL paginável, os logs HTTP poderão ter a seguinte string de consulta HTTP:

```
page=3&q=my-search-term
```

Para realizar a análise usando os termos de pesquisa, você pode extrair o valor de q de uma sequência de caracteres de consulta. O processador Key value (Valor de chave) fornece suporte robusto para extrair chaves e valores de cadeias de caracteres.

O exemplo a seguir combina os processadores `split_string` e `key_value` para extrair parâmetros de consulta de uma linha de log do Apache:

```
version: "2"
pipeline
 ...
  processor:
    - grok:
      match:
        message: [ "%{COMMONAPACHELOG_DATATYPED}" ]
    - split_string:
      entries:
        - source: request
          delimiter: "?"
    - key_value:
      source: "/request/1"
      field_split_characters: "&"
      value_split_characters: "="
      destination: query_params
```

Eventos mutantes

Os diferentes processadores Mutate event (Mutação de evento) permitem renomear, copiar, adicionar e excluir entradas de eventos.

Neste exemplo, o primeiro processador define o valor da chave `debug` para `true` se a chave já existir no evento. O segundo processador só define a chave `debug` para `true` se a chave não existir no evento, porque `overwrite_if_key_exists` está configurada como `true`.

```
...
processor:
  - add_entries:
    entries:
    - key: "debug"
      value: true
...
processor:
  - add_entries:
    entries:
    - key: "debug"
      value: true
      overwrite_if_key_exists: true
...
```

Você também pode usar uma string de formato para criar novas entradas a partir de entradas existentes. Por exemplo, `${date}-${time}` criará uma nova entrada com base nos valores das entradas existentes `date` e `time`.

Por exemplo, o pipeline a seguir adiciona novas entradas de eventos dinamicamente a partir de eventos existentes:

```
processor:
  - add_entries:
    entries:
    - key: "key_three"
      format: "${key_one}-${key_two}
```

Por exemplo, considere o seguinte evento recebido:

```
{
   "key_one": "value_one",
   "key_two": "value_two"
}
```

O processador o transforma em um evento com uma nova chave `key_three`, que combina valores de outras chaves no evento original.

```
{
   "key_one": "value_one",
   "key_two": "value_two",
   "key_three": "value_one-value_two"
}
```

Strings mutantes

Os vários processadores Mutate strings (Mutação de strings) oferecem ferramentas para manipular cadeias de caracteres nos dados recebidos. Por exemplo, se você precisar dividir uma string em uma matriz, use o processador `split_string`:

```
...
processor:
  - split_string:
    entries:
    - source: "message"
      delimiter: "&"
...
```

O processador transformará um string como `a&b&c` em `["a", "b", "c"]`.

Converter listas em mapas

O processador List-to-Map (Lista em mapa), que é um dos processadores de eventos Mutate, converte uma lista de objetos em um evento em um mapa.

Por exemplo, considere a seguinte configuração de processador:

```
...
processor:
    - list_to_map:
        key: "name"
        source: "A-car-as-list"
        target: "A-car-as-map"
        value_key: "value"
        flatten: true
...
```

Esse processador converterá um evento que contém uma lista de objetos como esta:

```
{
  "A-car-as-list": [
    {
      "name": "make",
      "value": "tesla"
    },
    {
      "name": "model",
      "value": "model 3"
    },
    {
      "name": "color",
      "value": "white"
    }
  ]
}
```

Em um mapa:

```
{
  "A-car-as-map": {
    "make": "tesla",
    "model": "model 3",
    "color": "white"
  }
}
```

Como outro exemplo, suponha que você tem um evento planejado com a seguinte estrutura:

```
{
  "mylist" : [
    {
      "somekey" : "a",
      "somevalue" : "val-a1",
      "anothervalue" : "val-a2"
    },
    {
      "somekey" : "b",
      "somevalue" : "val-b1",
      "anothervalue" : "val-b2"
    },
    {
```

```
      "somekey" : "b",
      "somevalue" : "val-b3",
      "anothervalue" : "val-b4"
    },
    {
      "somekey" : "c",
      "somevalue" : "val-c1",
      "anothervalue" : "val-c2"
    }
  ]
}
```

Você pode definir as seguintes opções na configuração do processador:

```
...
processor:
    - list_to_map:
        key: "somekey"
        source: "mylist"
        target: "myobject"
        value_key: "value"
        flatten: true
...
```

O processador modifica o evento removendo `mylist` e adicionando o novo objeto `myobject`:

```
{
  "myobject" : {
    "a" : [
      {
        "somekey" : "a",
        "somevalue" : "val-a1",
        "anothervalue" : "val-a2"
      }
    ],
    "b" : [
      {
        "somekey" : "b",
        "somevalue" : "val-b1",
        "anothervalue" : "val-b2"
      },
      {
        "somekey" : "b",
```

```
        "somevalue" : "val-b3",
        "anothervalue" : "val-b4"
      }
    "c" : [
      {
        "somekey" : "c",
        "somevalue" : "val-c1",
        "anothervalue" : "val-c2"
      }
    ]
  }
}
```

Em muitos casos, convém nivelar a matriz de cada chave. Nessas situações, você deve escolher apenas um objeto para ser mantido. O processador oferece a opção de primeiro ou último.

```
...
processor:
    - list_to_map:
        key: "somekey"
        source: "mylist"
        target: "myobject"
        flatten: true
...
```

A estrutura do evento planejado é então nivelada de acordo:

```
{
  "myobject" : {
    "a" : {
      "somekey" : "a",
      "somevalue" : "val-a1",
      "anothervalue" : "val-a2"
    },
    "b" : {
      "somekey" : "b",
      "somevalue" : "val-b1",
      "anothervalue" : "val-b2"
    }
    "c" : {
      "somekey" : "c",
      "somevalue" : "val-c1",
      "anothervalue" : "val-c2"
```

```
    }
  }
}
```

Você pode usar o processador List-to-Map para processar logs do AWS WAF. Por exemplo, considere um exemplo de log do WAF como este:

```
{
    "webaclId": "arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/
STMTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
    "httpRequest": {
        "headers": [
            {
                "name": "Host",
                "value": "localhost:1989"
            },
            {
                "name": "User-Agent",
                "value": "curl/7.61.1"
            }
        ]
    }
}
```

Se o pipeline a seguir processar o evento:

```
...
processor:
    - list_to_map:
        key: "name"
        source: "httpRequest/headers"
        value_key: "value"
        flatten: true
...
```

Isso criará o seguinte novo evento:

```
{
    "webaclId": "arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/
STMTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
    "httpRequest": {
        "headers": [
```

```
            {
                "name": "Host",
                "value": "localhost:1989"
            },
            {
                "name": "User-Agent",
                "value": "curl/7.61.1"
            }
        ]
    },
    "Host": "localhost:1989",
    "User-Agent": "curl/7.61.1"
}
```

Processar carimbos de data/hora futuros

O processador Date (Data) analisa a chave de registro de data e hora dos eventos recebidos, convertendo-a para o formato ISO 8601.

```
...
  processor:
    - date:
        match:
          - key: timestamp
            patterns: ["dd/MMM/yyyy:HH:mm:ss"]
        destination: "@timestamp"
        source_timezone: "America/Los_Angeles"
        destination_timezone: "America/Chicago"
        locale: "en_US"
...
```

Se o pipeline acima processar o seguinte evento:

```
{"timestamp": "10/Feb/2000:13:55:36"}
```

Ele converte o evento no seguinte formato:

```
{
  "timestamp":"10/Feb/2000:13:55:36",
  "@timestamp":"2000-02-10T15:55:36.000-06:00"
}
```

Gerar carimbos de data/hora

O processador Date pode gerar registros de data e hora para eventos recebidos se você especificar `@timestamp` para a opção `destination`.

```
...
    processor:
    - date:
        from_time_received: true
        destination: "@timestamp"
...
```

Derivar padrões de pontuação

O processador Substitute string (Substituir string), que é um dos processadores Mutate string, permite derivar um padrão de pontuação dos eventos recebidos. No exemplo de pipeline a seguir, o processador examinará os eventos de log do Apache recebidos e derivará padrões de pontuação a partir deles.

```
processor:

    - substitute_string:

        entries:

          - source: "message"

            from: "[a-zA-Z0-9_]+"

            to: ""

          - source: "message"

            from: "[ ]+"

            to: "_"
```

O seguinte log HTTP recebido do Apache gerará um padrão de pontuação:

```
[{"message":"10.10.10.11 - admin [19/Feb/2015:15:50:36 -0500] \"GET /big2.pdf
 HTTP/1.1\" 200 33973115 0.202 \"-\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_1)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.111 Safari/537.36\""}]
```

```
{"message":"..._-_[//:::_-]_\"_/._/.\"_._\"-\"_\"/._(;_)_/._(,_)_/..._/.\""}
```

Você pode contar esses padrões gerados passando-os pelo processador Aggregate (Agregar) com a ação `count`.

Agregação de eventos com Ingestão do Amazon OpenSearch

Você pode usar a Ingestão do Amazon OpenSearch para agregar dados de diferentes eventos ao longo de um período. A agregação de eventos pode ajudar a reduzir o volume desnecessário de logs e lidar com casos de uso, como logs de várias linhas que chegam como eventos separados. Aggregate é um processador com estado que agrupa eventos com base nos valores de um conjunto de chaves de identificação especificadas e executa uma ação configurável em cada grupo.

O estado no processador Aggregate é armazenado na memória. Por exemplo, para combinar quatro eventos em um, o processador precisa reter partes dos três primeiros eventos. O estado de um grupo agregado de eventos é mantido por um período de tempo configurável. Dependendo dos seus logs, da ação agregada usada e da quantidade de opções de memória na configuração do processador, a agregação pode ocorrer por um longo período de tempo.

Além desses exemplos, você também pode usar o esquema de agregação de logs com roteamento condicional. Para obter mais informações sobre esquemas, consulte the section called “Usar esquemas para criar um pipeline”.

Tópicos

Uso básico

O exemplo de pipeline a seguir extrai os campos `sourceIp`, `destinationIp` e `port`, usando o processador Grok e, em seguida, agrega esses campos por um período de 30 segundos usando o processador Aggregate e a ação `put_all`. Ao final dos 30 segundos, o log agregado é enviado para o coletor do OpenSearch.

```
version: "2"
aggregate_pipeline:
```

```
  source:
    http:
     path: "/${pipelineName}/logs"
  processor:
    - grok:
        match:
          log: ["%{IPORHOST:sourceIp} %{IPORHOST:destinationIp} %{NUMBER:port:int}"]
    - aggregate:
        group_duration: "30s"
        identification_keys: ["sourceIp", "destinationIp", "port"]
        action:
          put_all:
  sink:
    - opensearch:
        ...
        index: aggregated_logs
```

Por exemplo, considere os seguintes lotes de logs:

```
{ "log": "127.0.0.1 192.168.0.1 80", "status": 200 }
{ "log": "127.0.0.1 192.168.0.1 80", "bytes": 1000 }
{ "log": "127.0.0.1 192.168.0.1 80" "http_verb": "GET" }
```

O processador Grok extrairá as `identification_keys` para criar os seguintes logs:

```
{ "sourceIp": "127.0.0.1", "destinationIp": "192.168.0.1", "port": 80, "status": 200 }
{ "sourceIp": "127.0.0.1", "destinationIp": "192.168.0.1", "port": 80, "bytes": 1000 }
{ "sourceIp": "127.0.0.1", "destinationIp": "192.168.0.1", "port": 80, "http_verb":
 "GET" }
```

Quando o grupo termina 30 segundos após o recebimento do primeiro log pelo processador agregado, o seguinte log agregado é gravado no coletor:

```
{ "sourceIp": "127.0.0.1", "destinationIp": "192.168.0.1", "port": 80, "status": 200,
 "bytes": 1000, "http_verb": "GET" }
```

Exclusão de duplicidades

Você pode remover entradas duplicadas derivando chaves de eventos recebidos e especificando a opção `remove_duplicates` para o processador agregado. Essa ação processa imediatamente o primeiro evento de um grupo e elimina todos os eventos seguintes desse grupo.

No exemplo a seguir, o primeiro evento é processado com as chaves de identificação `sourceIp` e `destinationIp`:

```
{ "sourceIp": "127.0.0.1", "destinationIp": "192.168.0.1", "status": 200 }
```

O pipeline então eliminará o seguinte evento porque ele tem as mesmas chaves:

```
{ "sourceIp": "127.0.0.1", "destinationIp": "192.168.0.1", "bytes": 1000 }
```

O pipeline processa esse evento e cria um novo grupo porque `sourceIp` é diferente:

```
{ "sourceIp": "127.0.0.2", "destinationIp": "192.168.0.1", "bytes": 1000 }
```

Agregação de logs e roteamento condicional

Você pode usar vários plug-ins para combinar a agregação de logs com o roteamento condicional. Neste exemplo, o subpipeline `log-aggregate-pipeline` recebe logs por meio de um cliente HTTP como o FluentBit e extrai valores importantes dos logs comparando o valor na chave `log` com o padrão de log comum do Apache.

Dois dos valores que ele extrai dos logs com um padrão Grok incluem `response` e `clientip`. O processador agregado então usa o valor `clientip`, junto com a opção `remove_duplicates`, para descartar quaisquer logs que contenham um `clientip` que já tenha sido processado dentro do `group_duration` específico.

Existem três rotas, ou declarações condicionais, no pipeline. Essas rotas separam o valor da resposta em respostas 2xx/3xx, 4xx e 5xx. Registros com status 2xx e 3xx são enviados para o índice `aggregated_2xx_3xx`, logs com status 4xx são enviados para o índice `aggregated_4xx` e logs com status 5xx são enviados para o índice `aggregated_5xx`.

```
version: "2"
log-aggregate-pipeline:
  source:
    http:
      # Provide the path for ingestion. ${pipelineName} will be replaced with pipeline
 name configured for this pipeline.
      # In this case it would be "/log-aggregate-pipeline/logs". This will be the
 FluentBit output URI value.
      path: "/${pipelineName}/logs"
  processor:
```

```
    - grok:
        match:
          log: [ "%{COMMONAPACHELOG_DATATYPED}" ]
    - aggregate:
        identification_keys: ["clientip"]
        action:
          remove_duplicates:
        group_duration: "180s"
  route:
    - 2xx_status: "/response >= 200 and /response < 300"
    - 3xx_status: "/response >= 300 and /response < 400"
    - 4xx_status: "/response >= 400 and /response < 500"
    - 5xx_status: "/response >= 500 and /response < 600"
  sink:
    - opensearch:
        ...
        index: "aggregated_2xx_3xx"
        routes:
          - 2xx_status
          - 3xx_status
    - opensearch:
        ...
        index: "aggregated_4xx"
        routes:
          - 4xx_status
    - opensearch:
        ...
        index: "aggregated_5xx"
        routes:
          - 5xx_status
```

Derivar métricas de logs com a Ingestão do Amazon OpenSearch

Você pode usar a Ingestão do Amazon OpenSearch para derivar métricas de logs. O exemplo de pipeline a seguir recebe logs de entrada usando o plug-in origem do HTTP e o processador Grok. Em seguida, ele usa o processador Aggregate para extrair a métrica agregada `bytes` em um intervalo de 30 segundos e deriva histogramas dos resultados.

Em geral, os pipelines contém dois subpipelines:

- `apache-log-pipeline-with-metrics`: recebe logs por meio de um cliente HTTP como o FluentBit, extrai valores importantes dos logs comparando o valor na chave `log` com o padrão

de log comum do Grok no Apache e, em seguida, encaminha os logs do Grok para o subpipeline `log-to-metrics-pipeline` e um índice do OpenSearch chamado `logs`.

- `log-to-metrics-pipeline`: recebe logs agrupados do subpipeline `apache-log-pipeline-with-metrics`, agrega os logs e deriva as métricas do histograma `bytes` com base nos valores nas chaves `clientip` e `request`. Finalmente, ele envia as métricas do histograma para um índice do OpenSearch chamado `histogram_metrics`.

```
version: "2"
apache-log-pipeline-with-metrics:
  source:
    http:
      # Provide the path for ingestion. ${pipelineName} will be replaced with pipeline
 name configured for this pipeline.
      # In this case it would be "/apache-log-pipeline-with-metrics/logs". This will be
 the FluentBit output URI value.
      path: "/${pipelineName}/logs"
  processor:
    - grok:
        match:
          log: [ "%{COMMONAPACHELOG_DATATYPED}" ]
  sink:
    - opensearch:
        ...
        index: "logs"
    - pipeline:
        name: "log-to-metrics-pipeline"

log-to-metrics-pipeline:
  source:
    pipeline:
      name: "apache-log-pipeline-with-metrics"
  processor:
    - aggregate:
        # Specify the required identification keys
        identification_keys: ["clientip", "request"]
        action:
          histogram:
            # Specify the appropriate values for each of the following fields
            key: "bytes"
            record_minmax: true
            units: "bytes"
```

```
            buckets: [0, 25000000, 50000000, 75000000, 100000000]
        # Pick the required aggregation period
        group_duration: "30s"
sink:
  - opensearch:
        ...
        index: "histogram_metrics"
```

Além deste exemplo, você também pode usar o esquema de log do pipeline de métrica. Para obter mais informações sobre esquemas, consulte the section called “Usar esquemas para criar um pipeline”.

Trace Analytics com Ingestão do Amazon OpenSearch

Você pode usar a Ingestão do Amazon OpenSearch para coletar dados de rastreamento do OpenTelemetry e transformá-los para uso no OpenSearch Service. O exemplo de pipeline a seguir usa três subpipelines para monitorar o Trace Analytics: `entry-pipeline`, `span-pipeline` e `service-map-pipeline`.

Origem de rastreamento do OpenTelemetry

O plug-in OTel trace source (origem de rastreamento OTel) aceita dados de rastreamento do OpenTelemetry Collector. O plug-in segue o protocolo OpenTelemetry e oferece suporte oficial à criptografia HTTPS padrão do setor.

Processadores

Você pode usar os seguintes processadores para o Trace Analytics:

- OTel trace: recebe uma coleção de registros de amplitude da fonte e executa o processamento, a extração e o preenchimento de campos com estado.
- OTel trace group: preenche os campos do grupo de rastreamento ausentes na coleção de registros de extensão.
- Mapa de serviços: executa o pré-processamento de dados de rastreamento e cria metadados para exibir painéis de mapas de serviços.

OpenSearch SQL

O plug-in coletor do OpenSearch fornece índices e modelos de índice específicos do Trace Analytics. Os seguintes índices do OpenSearch são específicos do Trace Analytics:

- `otel-v1-apm-span`: armazena a saída do processador OTel trace.
- `otel-v1-apm-service-map`: armazena a saída do processador Service-map.

Configuração do pipeline

O exemplo de pipeline a seguir é compatível com a Observabilidade do OpenSearch Dashboards. O primeiro subpipeline (`entry-pipeline`) recebe dados do OpenTelemetry Collector e usa dois outros subpipelines como coletores.

O subpipeline `span-pipeline` analisa os dados de rastreamento, enriquece e ingere os documentos de extensão em um índice de extensão. O subpipeline `service-map-pipeline` agrega rastreamentos em um mapa de serviços e grava documentos em um índice de mapas de serviços.

```
version: "2"
entry-pipeline:
  source:
    otel_trace_source:
      # Provide the path for ingestion. This will be the endpoint URI path in the
 OpenTelemetry Exporter configuration.
      # ${pipelineName} will be replaced with the sub-pipeline name. In this case it
 would be "/entry-pipeline/v1/traces".
      path: "/${pipelineName}/v1/traces"
  processor:
    - trace_peer_forwarder
  sink:
    - pipeline:
        name: "span-pipeline"
    - pipeline:
        name: "service-map-pipeline"

span-pipeline:
  source:
    pipeline:
      name: "entry-pipeline"
  processor:
    - otel_traces
  sink:
    - opensearch:
        ...
        index_type: trace-analytics-raw
```

```
service-map-pipeline:
  source:
    pipeline:
      name: "entry-pipeline"
  processor:
    - service_map
  sink:
    - opensearch:
        ...
        index_type: trace-analytics-service-map
```

Você deve executar o OpenTelemetry Collector em seu ambiente para enviar dados para o endpoint de ingestão. Para ver outro exemplo de pipeline, consulte o esquema do pipeline do Trace Analytics. Para obter mais informações, consulte the section called “Usar esquemas para criar um pipeline”.

Derivação de métricas de rastreamento com a Ingestão do Amazon OpenSearch

Você pode usar a Ingestão do Amazon OpenSearch para derivar métricas de rastreamentos do OpenTelemetry. O exemplo de pipeline a seguir recebe rastreamento de entrada e extrai uma métrica chamada `durationInNanos`, agregada em uma janela em cascata de 30 segundos. Em seguida, ele deriva um histograma dos rastreamentos recebidos.

O pipeline contém os seguintes subpipelines:

- `entry-pipeline` – recebe dados de rastreamento do coletor do OpenTelemetry e os encaminha para o subpipeline `trace_to_metrics_pipeline`.
- `trace-to-metrics-pipeline` – recebe os dados de rastreamento do subpipeline `entry-pipeline`, os agrega e deriva um histograma dos rastreamentos com base no valor `durationInNanos` do campo `serviceName`. Em seguida, ele envia as métricas derivadas para o índice do OpenSearch chamado `metrics_for_traces`.

```
version: "2"
entry-pipeline:
  source:
    otel_trace_source:
      # Provide the path for ingestion. ${pipelineName} will be replaced with sub-
pipeline name.
```

```
      # In this case it would be "/entry-pipeline/v1/traces". This will be endpoint URI
 path in OpenTelemetry Exporter configuration.
      path: "/${pipelineName}/v1/traces"
  sink:
    - pipeline:
        name: "trace-to-metrics-pipeline"

trace-to-metrics-pipeline:
  source:
    pipeline:
      name: "entry-pipeline"
  processor:
    - aggregate:
        # Pick the required identification keys
        identification_keys: ["serviceName"]
        action:
          histogram:
            # Pick the appropriate values for each of the following fields
            key: "durationInNanos"
            record_minmax: true
            units: "seconds"
            buckets: [0, 10000000, 50000000, 100000000]
        # Specify an aggregation period
        group_duration: "30s"
  sink:
    - opensearch:
        ...
        index: "metrics_for_traces"
```

Para ver outro exemplo de pipeline, consulte o esquema de pipeline de rastreamento de anomalia métrica. Para obter mais informações sobre esquemas, consulte the section called “Usar esquemas para criar um pipeline”.

Detecção de anomalias com a Ingestão do Amazon OpenSearch

Você pode usar a Ingestão do Amazon OpenSearch para treinar modelos e gerar anomalias quase em tempo real em eventos agregados de séries temporais. Você pode gerar anomalias em eventos gerados no pipeline ou em outros que chegam diretamente ao pipeline, como métricas do OpenTelemetry.

Você pode alimentar esses eventos de séries temporais agregados com janelas rotativas ao processador Anomaly detector (Detector de anomalias), que treina um modelo e gera anomalias com

uma pontuação. Em seguida, grave as anomalias em um índice separado para criar monitores de documentos e acionar alertas rápidos.

Além desses exemplos, você também pode usar os esquemas de log no pipeline de anomalias métricas e no pipeline de rastreamento de anomalia métrica. Para obter mais informações sobre esquemas, consulte the section called “Usar esquemas para criar um pipeline”.

Tópicos

Métricas dos logs

O pipeline a seguir recebe logs por meio de uma fonte HTTP como FluentBit, extrai valores importantes dos logs comparando o valor na chave `log` com o padrão de log comum do Grok no Apache e, em seguida, encaminha os logs do Grokd para o subpipeline `log-to-metrics-pipeline`, bem como para um índice do OpenSearch chamado `logs`.

O subpipeline `log-to-metrics-pipeline` recebe os logs agrupados do subpipeline `apache-log-pipeline-with-metrics`, os agrega e deriva as métricas do histograma com base nos valores nas chaves `clientip` e `request`. Em seguida, ele envia as métricas do histograma para um índice do OpenSearch chamado `histogram_metrics`, bem como para o subpipeline `log-to-metrics-anomaly-detector`.

O subpipeline `log-to-metrics-anomaly-detector-pipeline` recebe as métricas agregadas do histograma do subpipeline `log-to-metrics-pipeline` e as envia ao processador Anomaly detector para detectar anomalias usando o algoritmo Random Cut Forest. Se detectar anomalias, ele as envia para um índice do OpenSearch chamado `log-metric-anomalies`.

```
version: "2"
apache-log-pipeline-with-metrics:
  source:
    http:
      # Provide the path for ingestion. ${pipelineName} will be replaced with pipeline
 name configured for this pipeline.
      # In this case it would be "/apache-log-pipeline-with-metrics/logs". This will be
 the FluentBit output URI value.
      path: "/${pipelineName}/logs"
```

```
  processor:
    - grok:
        match:
          log: [ "%{COMMONAPACHELOG_DATATYPED}" ]
  sink:
    - opensearch:
        ...
        index: "logs"
    - pipeline:
        name: "log-to-metrics-pipeline"

log-to-metrics-pipeline:
  source:
    pipeline:
      name: "apache-log-pipeline-with-metrics"
  processor:
    - aggregate:
        # Specify the required identification keys
        identification_keys: ["clientip", "request"]
        action:
          histogram:
            # Specify the appropriate values for each the following fields
            key: "bytes"
            record_minmax: true
            units: "bytes"
            buckets: [0, 25000000, 50000000, 75000000, 100000000]
        # Pick the required aggregation period
        group_duration: "30s"
  sink:
    - opensearch:
        ...
        index: "histogram_metrics"
    - pipeline:
        name: "log-to-metrics-anomaly-detector-pipeline"

log-to-metrics-anomaly-detector-pipeline:
  source:
    pipeline:
      name: "log-to-metrics-pipeline"
  processor:
    - anomaly_detector:
        # Specify the key on which to run anomaly detection
        keys: [ "bytes" ]
        mode:
```

```
          random_cut_forest:
  sink:
    - opensearch:
        ...
        index: "log-metric-anomalies"
```

Métricas de rastreamento

Você pode derivar métricas de rastreamento e encontrar anomalias nas métricas geradas. Neste exemplo, o subpipeline `entry-pipeline` recebe dados de rastreamento do OpenTelemetry Collector e os encaminha para os seguintes subpipelines:

- `span-pipeline`: extrai os trechos brutos dos rastreamentos. Ele envia as extensões brutas para qualquer índice com o prefixo do OpenSearch `otel-v1-apm-span`.
- `service-map-pipeline`: agrega e analisa os dados para criar documentos que representam conexões entre serviços. Ele envia esses documentos para um índice do OpenSearch chamado `otel-v1-apm-service-map`. Em seguida, você pode ver uma visualização do mapa do serviço por meio do plug-in Trace Analytics para o OpenSearch Dashboards.
- `trace-to-metrics-pipeline`: agrega e deriva as métricas do histograma sobre os rastreamentos com base no valor do `serviceName`. Em seguida, ele envia as métricas derivadas para um índice do OpenSearch chamado `metrics_for_traces`, bem como para o subpipeline `trace-to-metrics-anomaly-detector-pipeline`.

O subpipeline `trace-to-metrics-anomaly-detector-pipeline` recebe as métricas agregadas do histograma do `trace-to-metrics-pipeline` e as envia ao processador do detector Anomaly para detectar anomalias usando o algoritmo Random Cut Forest. Se detectar quaisquer anomalias, ele as envia para um índice do OpenSearch chamado `trace-metric-anomalies`.

```
version: "2"
entry-pipeline:
  source:
    otel_trace_source:
      # Provide the path for ingestion. ${pipelineName} will be replaced with pipeline
 name configured for this pipeline.
      # In this case it would be "/entry-pipeline/v1/traces". This will be endpoint URI
 path in OpenTelemetry Exporter
      # configuration.
      # path: "/${pipelineName}/v1/traces"
```

```
  processor:
    - trace_peer_forwarder:
  sink:
    - pipeline:
        name: "span-pipeline"
    - pipeline:
        name: "service-map-pipeline"
    - pipeline:
        name: "trace-to-metrics-pipeline"

span-pipeline:
  source:
    pipeline:
      name: "entry-pipeline"
  processor:
    - otel_trace_raw:
  sink:
    - opensearch:
        ...
        index_type: "trace-analytics-raw"

service-map-pipeline:
  source:
    pipeline:
      name: "entry-pipeline"
  processor:
    - service_map:
  sink:
    - opensearch:
        ...
        index_type: "trace-analytics-service-map"

trace-to-metrics-pipeline:
  source:
    pipeline:
      name: "entry-pipeline"
  processor:
    - aggregate:
        # Pick the required identification keys
        identification_keys: ["serviceName"]
        action:
          histogram:
            # Pick the appropriate values for each the following fields
            key: "durationInNanos"
```

```
            record_minmax: true
            units: "seconds"
            buckets: [0, 10000000, 50000000, 100000000]
        # Pick the required aggregation period
        group_duration: "30s"
  sink:
    - opensearch:
        ...
        index: "metrics_for_traces"
    - pipeline:
        name: "trace-to-metrics-anomaly-detector-pipeline"

trace-to-metrics-anomaly-detector-pipeline:
  source:
    pipeline:
      name: "trace-to-metrics-pipeline"
  processor:
    - anomaly_detector:
        # Below Key will find anomalies in the max value of histogram generated for
 durationInNanos.
        keys: [ "max" ]
        mode:
          random_cut_forest:
  sink:
    - opensearch:
        ...
        index: "trace-metric-anomalies"
```

Métricas do OpenTelemetry

Você pode criar um pipeline que receba e detecte anomalias nas métricas do OpenTelemetry. Neste exemplo, `entry-pipeline` recebe dados de métricas do OpenTelemetry Collector. Se uma métrica for do tipo `GAUGE` e o nome da métrica for `totalApiBytesSent`, o processador a enviará para o subpipeline `ad-pipeline`.

O subpipeline `ad-pipeline` recebe os dados de métricas do pipeline de entrada e realiza a detecção de anomalias no valor da métrica usando o processador Anomaly detector.

```
entry-pipeline:
  source:
    otel_metrics_source:
  processor:
```

```
    - otel_metrics:
  route:
    - gauge_route: '/kind = "GAUGE" and /name = "totalApiBytesSent"'
  sink:
    - pipeline:
        name: "ad-pipeline"
        routes:
          - gauge_route
    - opensearch:
        ...
        index: "otel-metrics"

ad-pipeline:
  source:
    pipeline:
      name: "entry-pipeline"
    processor:
      - anomaly_detector:
        # Use "value" as the key on which anomaly detector needs to be run
        keys: [ "value" ]
        mode:
          random_cut_forest:
    sink:
      - opensearch:
        ...
        index: otel-metrics-anomalies
```

Além deste exemplo, você também pode usar o esquema de pipeline de rastreamento de anomalia métrica. Para obter mais informações sobre esquemas, consulte the section called “Usar esquemas para criar um pipeline”.

Amostragem com Ingestão do Amazon OpenSearch

A Ingestão do Amazon OpenSearch fornece os seguintes recursos de amostragem. Além desses exemplos, você também pode usar o esquema de amostragem de log do Apache. Para obter mais informações sobre esquemas, consulte the section called “Usar esquemas para criar um pipeline”.

Tópicos

- Amostragem de tempo
- Amostragem percentual
- Amostragem final

Amostragem de tempo

Você pode usar a ação `rate_limiter` no processador Aggregate para limitar o número de eventos que podem ser processados por segundo. Você pode optar por descartar eventos em excesso ou transferi-los para o próximo período.

Neste exemplo, somente 100 eventos por segundo com um código de status de `200` são enviados para o coletor a partir de um determinado endereço IP. Ele remove todos os eventos em excesso da janela de tempo configurada.

```
...
  processor:
   - aggregate:

        identification_keys: ["clientip"]

        action:

          rate_limiter:

            events_per_second: 100

            when_exceeds: drop
        when: "/status == 200"
...
```

Se, em vez disso, você definir a opção `when_exceeds` como `block`, o processador processará eventos em excesso no próximo período de tempo.

Amostragem percentual

Use a ação `percent_sampler` no processador Aggregate para limitar o número de eventos enviados para um coletor. Todos os eventos excedentes serão descartados.

Neste exemplo, somente 20% dos eventos com um código de status de `200` são enviados para o coletor a partir de um determinado endereço IP:

```
...
  processor:
  - aggregate:

        identification_keys: ["clientip"]
```

```
        duration :

        action:

          percent_sampler:

            percent: 20

        when: "/status == 200"
...
```

Amostragem final

Use a ação `tail_sampler` no processador Aggregate para obter amostras de eventos com base em um conjunto de políticas definidas. Essa ação aguarda a conclusão de uma agregação em diferentes períodos de agregação com base no período de espera configurado. Quando uma agregação é concluída e se ela corresponder à condição de erro específica, ela é enviada para o coletor. Caso contrário, somente uma porcentagem configurada de eventos será enviada para o coletor.

O exemplo de pipeline a seguir envia todos os rastreamentos do OpenTelemetry com um status de condição de erro 2 para o coletor. Ele envia apenas 20% dos rastreamentos que não correspondem a essa condição de erro para o coletor.

```
...
  processor:
   - aggregate:

        identification_keys: ["traceId"]

        action:

          tail_sampler:

            percent: 20

            wait_period: "10s"

            condition: "/status == 2"


...
```

Se você definir a condição de erro como `false` ou não incluí-la, somente a porcentagem configurada de eventos poderá passar, determinada por um resultado probabilístico.

Como é difícil determinar exatamente quando a amostragem da cauda deve ocorrer, você pode usar a opção `wait_period` para medir o tempo de inatividade após o recebimento do último evento.

Download seletivo com Ingestão do Amazon OpenSearch

Se seu pipeline usa uma fonte do S3, será possível usar expressões SQL para realizar filtragens e cálculos no conteúdo dos objetos do S3 antes de ingeri-los em um pipeline.

A opção `s3_select` oferece suporte a objetos no formato Parquet. Ela também funciona com objetos compactados com GZIP ou BZIP2 (somente para objetos CSV e JSON) e suporta compactação em colunas para Parquet usando GZIP e Snappy.

O exemplo de pipeline a seguir baixa dados em objetos recebidos para o S3, codificados no formato Parquet:

```
pipeline:
  source:
    s3:
      s3_select:
        expression: "select * from s3object s"
        input_serialization: parquet
      notification_type: "sqs"
...
```

O exemplo a seguir baixa somente os primeiros 10.000 registros nos objetos:

```
pipeline:
  source:
    s3:
      s3_select:
        expression: "select * from s3object s LIMIT 10000"
        input_serialization: parquet
      notification_type: "sqs"
...
```

O exemplo a seguir verifica o valor mínimo e máximo de `data_value` antes de ingerir eventos no pipeline:

```
pipeline:
  source:
    s3:
      s3_select:
        expression: "select s.* from s3object s where s.data_value > 200 and
 s.data_value < 500 "
        input_serialization: parquet
      notification_type: "sqs"
...
```

Além desses exemplos, você também pode usar o esquema do pipeline selecionado do S3. Para obter mais informações sobre esquemas, consulte the section called “Usar esquemas para criar um pipeline”.

Para obter mais informações, consulte os seguintes recursos do :

- Filtragem e recuperação de dados usando o Amazon S3 Select
- Referência SQL para o Amazon S3 Select

Segurança na Ingestão do Amazon OpenSearch

A segurança para com a nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se contará com um datacenter e uma arquitetura de rede criados para atender aos requisitos das organizações com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos programas de conformidade da AWS.
- Segurança na nuvem: sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar a Ingestão do OpenSearch. Os tópicos a seguir mostram como configurar a Ingestão

do OpenSearch para atender aos seus objetivos de segurança e conformidade. Saiba também como usar outros serviços da AWS que ajudam a monitorar e proteger os recursos de Ingestão do OpenSearch.

Tópicos

Protegendo os pipelines OpenSearch de ingestão da Amazon em uma VPC

Você pode lançar pipelines OpenSearch de ingestão da Amazon em uma nuvem privada virtual (VPC). Uma VPC é uma rede virtual dedicada à sua Conta da AWS. É logicamente isolado de outras redes virtuais na AWS nuvem. A colocação de um pipeline em uma VPC permite a comunicação segura entre o OpenSearch Inestion e outros serviços dentro da VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS

O uso de uma VPC permite impor o fluxo de dados por meio de seus pipelines de OpenSearch ingestão dentro dos limites da VPC, e não pela Internet pública. Pipelines que não estão em uma VPC enviam e recebem dados por endpoints públicos e pela Internet.

Para obter instruções sobre como provisionar um pipeline em uma VPC, consulte the section called “Como criar pipelines”.

Tópicos

Considerações

Considere o seguinte ao configurar o acesso à VPC para um pipeline.

- Um pipeline público pode gravar em um domínio VPC. Da mesma forma, um pipeline de VPC pode gravar em um domínio público.
- Um pipeline não precisa estar na mesma VPC que seu coletor de domínio. Você também não precisa estabelecer uma conexão entre as duas VPCs. OpenSearch A ingestão se encarrega de conectá-los para você.
- Você só pode especificar uma VPC para o pipeline.
- Ao contrário dos pipelines públicos, um pipeline de VPC deve estar na mesma Região da AWS do domínio em que está gravando.
- Você pode optar por implantar um pipeline em uma, duas ou três sub-redes da VPC. As sub-redes são distribuídas nas mesmas zonas de disponibilidade nas quais suas unidades de OpenSearch computação de ingestão (OCUs) estão implantadas.
- Se você implantar apenas um pipeline em uma sub-rede e a Zona de disponibilidade ficar inativa, você não conseguirá ingerir dados. Para garantir a alta disponibilidade, recomendamos que você configure pipelines com duas ou três sub-redes.
- A especificação de um grupo de segurança é opcional. Se você não fornecer um grupo de segurança, nós usamos o grupo de segurança que está especificado na VPC.

Limitações

Pipelines em uma VPC têm as seguintes limitações.

- Não é possível alterar a configuração de rede de um pipeline depois de criá-la. Se você iniciar um pipeline em uma VPC, não poderá alterá-lo posteriormente para um endpoint público e vice-versa.
- Você pode iniciar o pipeline de uma VPC ou usar um endpoint público, mas não pode fazer ambos. Você deve escolher uma opção ou outra ao criar um pipeline.
- Após provisionar um pipeline dentro de uma VPC, não será possível movê-lo para uma VPC diferente e você não pode mudar as sub-redes e as configurações do grupo de segurança.
- Se seu pipeline grava em um coletor de domínio VPC, você não pode voltar mais tarde e alterar o coletor para um domínio diferente (VPC ou público) após a criação do pipeline. Você deve excluir e recriar o pipeline com um novo coletor. Você ainda pode mudar um coletor de um domínio público para um domínio VPC.
- Você não pode fornecer acesso de ingestão entre contas aos pipelines de VPC.

Pré-requisitos

Antes de poder provisionar um pipeline em uma VPC, você deve fazer o seguinte:

- Criar uma VPC

  Para criar sua VPC, você pode usar o console Amazon VPC, a AWS CLI ou um dos SDKs. AWS Para obter mais informações, consulte Como trabalhar com VPCs compartilhadas no Manual do usuário da Amazon VPC. Se você já tiver uma VPC, ignore esta etapa.

- Reservar endereços IP

  OpenSearch A ingestão coloca uma interface de rede elástica em cada sub-rede que você especifica durante a criação do pipeline. Cada interface de rede está associada a um endereço IP. Você deve reservar um endereço IP por sub-rede para as interfaces de rede.

Como configurar o acesso à VPC para um pipeline

Você pode habilitar o acesso à VPC para um pipeline dentro do console OpenSearch de serviço ou usando o. AWS CLI

Console

Você configura o acesso à VPC durante a criação do pipeline. Em Rede, escolha Acesso à VPC e defina as seguintes configurações:

Configuração	Descrição
VPC	Escolha o ID da nuvem privada virtual (VPC) que deseja usar. A VPC e o pipeline devem estar na mesma Região da AWS.
Subredes	Escolha uma ou mais sub-redes. OpenSearch O serviço colocará um endpoint VPC e interfaces de rede elástica nas sub-redes.
Grupos de segurança	Escolha um ou mais grupos de segurança de VPC que permitam que o aplicativo necessário alcance o pipeline de OpenSearch ingestão nas portas (80 ou 443) e protocolos (HTTP ou HTTPs) expostos pelo pipeline.

CLI

Para configurar o acesso à VPC usando o AWS CLI, especifique o `--vpc-options` parâmetro:

```
aws osis create-pipeline \
  --pipeline-name vpc-pipeline \
  --min-units 4 \
  --max-units 10 \
  --vpc-options
 SecurityGroupIds={sg-12345678,sg-9012345},SubnetIds=subnet-1212234567834asdf \
  --pipeline-configuration-body "file://pipeline-config.yaml"
```

Função vinculada ao serviço para acesso à VPC

Uma função vinculada ao serviço é um tipo exclusivo de função do IAM que delega permissões para um serviço de forma que ele possa criar e gerenciar recursos em seu nome. OpenSearch A ingestão requer uma função vinculada a serviços chamada AWSServiceRoleForAmazonOpenSearchIngestionpara acessar sua VPC, criar o endpoint do pipeline e colocar interfaces de rede em uma sub-rede da sua VPC. Para obter mais informações sobre as permissões dessa função e como excluí-la, consulte the section called “Perfil de criação de pipeline”.

OpenSearch A ingestão cria automaticamente a função quando você cria um pipeline de ingestão. Para que essa criação automática seja bem-sucedida, o usuário que cria o primeiro pipeline em uma conta precisa ter permissões para a ação `iam:CreateServiceLinkedRole`. Para saber mais, consulte Permissões de funções vinculadas ao serviço no Manual do usuário do IAM. Você pode ver a função no console AWS Identity and Access Management (IAM) depois de criada.

Gerenciamento de identidade e acesso na Ingestão do Amazon OpenSearch

O AWS Identity and Access Management (IAM) é um serviço da AWS service (Serviço da AWS) que ajuda a controlar o acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (ter permissões) a usar os recursos da Ingestão do OpenSearch. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

Tópicos

- Exemplos de políticas baseadas em identidade para a Ingestão do OpenSearch

- Ações de políticas para a Ingestão do OpenSearch
- Recursos de políticas para a Ingestão do OpenSearch
- Chaves de condição da política de Ingestão do Amazon OpenSearch
- ABAC com a Ingestão do OpenSearch
- Uso de credenciais temporárias com a Ingestão do OpenSearch
- Funções vinculadas ao serviço da Ingestão do OpenSearch
- Exemplos de políticas baseadas em identidade para o OpenSearch Sem Servidor

Exemplos de políticas baseadas em identidade para a Ingestão do OpenSearch

É compatível com políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou função à qual ela está anexado. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos de política JSON do IAM no Guia do usuário do IAM.

Exemplos de políticas baseadas em identidade para o OpenSearch Sem Servidor

Para exibir exemplos de políticas baseadas em identidade do OpenSearch Sem Servidor, consulte the section called “Exemplos de políticas baseadas em identidade”.

Ações de políticas para a Ingestão do OpenSearch

Oferece suporte a ações de políticas	Sim

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome que a operação de API da AWS associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Inclua ações em uma política para conceder permissões para executar a operação associada.

As ações de políticas na Ingestão do OpenSearch usam o seguinte prefixo antes da ação:

```
osis
```

Para especificar várias ações em uma única declaração, separe-as com vírgulas.

```
"Action": [
      "osis:action1",
      "osis:action2"
         ]
```

É possível especificar várias ações usando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `List`, inclua a seguinte ação:

```
"Action": "osis:List*"
```

Para exibir exemplos de políticas baseadas em identidade do OpenSearch Sem Servidor, consulte Exemplos de políticas baseadas em identidade para o OpenSearch Sem Servidor.

Recursos de políticas para a Ingestão do OpenSearch

Oferece suporte a recursos de políticas	Sim

Os administradores podem usar AWS as políticas JSON da para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Resource` de política JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um recurso usando seu Nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem suporte a um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Chaves de condição da política de Ingestão do Amazon OpenSearch

Compatível com chaves de condição de política específicas do serviço	Não

Os administradores podem usar AWS as políticas JSON da para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou bloco de `Condition`) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único elemento `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica `OR`. Todas as condições devem ser atendidas para que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos de política do IAM: variáveis e tags no Guia do usuário do IAM.

A AWS oferece suporte a chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição globais da AWS, consulte Chaves de contexto de condição globais da AWS no Guia do usuário do IAM.

Para exibir uma lista de chaves de condição de Ingestão do OpenSearch, consulte Chaves de condição de Ingestão do Amazon OpenSearch na Referência de autorização do serviço. Para saber com quais ações e recursos é possível usar a chave de condição, consulte Ações definidas pela Ingestão do Amazon OpenSearch.

ABAC com a Ingestão do OpenSearch

Oferece suporte a ABAC (tags em políticas)	Sim

O controle de acesso baseado em atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Na AWS, esses atributos são chamados de tags. É possível anexar tags a entidades do IAM (usuários ou funções) e a muitos recursos da AWS. A marcação de entidades e recursos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela está tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys` chaves de condição.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial.

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Para obter mais informações sobre aplicação de tags em recursos de Ingestão do OpenSearch, consulte the section called “Uso de tags com pipelines”.

Uso de credenciais temporárias com a Ingestão do OpenSearch

Oferece suporte a credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Você está usando credenciais temporárias se faz login no AWS Management Console usando qualquer método, exceto um nome de usuário e uma senha. Por exemplo, quando você acessa a AWS usando o link de autenticação única (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna funções. Para obter mais informações sobre como alternar funções, consulte Alternar para uma função (console) no Guia do usuário do IAM.

Você pode criar credenciais temporárias manualmente usando a AWS CLI ou a API da AWS. Em seguida, você pode usar essas credenciais temporárias para acessar a AWS. A AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Funções vinculadas ao serviço da Ingestão do OpenSearch

Oferece suporte a funções vinculadas ao serviço	Sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode assumir a função de executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas ao serviço.

A Ingestão do OpenSearch usa uma função vinculada ao serviço denominada `AWSServiceRoleForAmazonOpenSearchIngestion`. Para obter detalhes sobre como criar e gerenciar funções vinculadas ao serviço de Ingestão do OpenSearch, consulte the section called “Perfil de criação de pipeline”.

Exemplos de políticas baseadas em identidade para o OpenSearch Sem Servidor

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos de Ingestão do OpenSearch. Eles também não podem executar tarefas usando o AWS Management Console, a AWS Command Line Interface (AWS CLI) ou a AWS API. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a perfis, e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pela Ingestão do Amazon OpenSearch, inclusive o formato dos ARNs para cada um dos tipos de recurso, consulte Ações, recursos e chaves de condição da Ingestão do Amazon OpenSearch na Referência de autorização do serviço.

Tópicos

- Práticas recomendadas de políticas
- Usar Ingestão do OpenSearch no console
- Administrando pipelines na Ingestão do OpenSearch
- Ingestão de dados em um pipeline da Ingestão do OpenSearch

Práticas recomendadas de políticas

As políticas baseadas em identidade são muito eficientes. Elas determinam se alguém pode criar, acessar ou excluir recursos de Ingestão do OpenSearch na sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos de Ingestão do OpenSearch na sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo: para começar a conceder permissões a seus usuários e workloads, use as políticas gerenciadas pela AWS que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis na sua Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.

- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um AWS service (Serviço da AWS) específico, como o AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: Condition no Manual do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM.
- Exigir autenticação multifator (MFA): se houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Usar Ingestão do OpenSearch no console

Para acessar a Ingestão do OpenSearch no console do OpenSearch Service, é necessário ter um conjunto mínimo de permissões. Essas permissões dão autorização para que você liste e exiba detalhes sobre os recursos de Ingestão do OpenSearch na sua conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (como perfis do IAM) com essa política.

Não é necessário conceder permissões mínimas do console para usuários que fazem chamadas somente à AWS CLI ou à API do AWS. Em vez disso, permita o acesso somente às ações que correspondem à operação da API que você está tentando executar.

A política a seguir permite que um usuário acesse a Ingestão do OpenSearch no console do OpenSearch Service:

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "osis:ListPipelines",
                "osis:GetPipeline",
                "osis:ListPipelineBlueprints",
                "osis:GetPipelineBlueprint",
                "osis:GetPipelineChangeProgress"
            ]
        }
    ]
}
```

Como alternativa, você pode usar a política gerenciada the section called "AmazonOpenSearchIngestionReadOnlyAccess", da AWS, que concede acesso somente leitura a todos os recursos da Ingestão do OpenSearch para um. Conta da AWS

Administrando pipelines na Ingestão do OpenSearch

Esta política é um exemplo de política de "administração de pipeline" que permite que um usuário gerencie e administre pipelines da Ingestão do Amazon OpenSearch. O usuário pode criar, exibir e excluir pipelines.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "arn:aws:osis:region:123456789012:pipeline/*",
            "Action": [
                "osis:CreatePipeline",
                "osis:DeletePipeline",
                "osis:UpdatePipeline",
                "osis:ValidatePipeline",
                "osis:StartPipeline",
                "osis:StopPipeline"
            ],
            "Effect": "Allow"
        },
        {
            "Resource": "*",
```

```
            "Action": [
                "osis:ListPipelines",
                "osis:GetPipeline",
                "osis:ListPipelineBlueprints",
                "osis:GetPipelineBlueprint",
                "osis:GetPipelineChangeProgress"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Ingestão de dados em um pipeline da Ingestão do OpenSearch

Este exemplo de política permite que um usuário ou outra entidade consuma dados em um pipeline da Ingestão do Amazon OpenSearch em sua conta. O usuário não pode modificar os pipelines.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "arn:aws:osis:region:123456789012:pipeline/*",
            "Action": [
                "osis:Ingest"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Registro em log de chamadas da API de Ingestão de Amazon OpenSearch usando AWS CloudTrail

A Ingestão do Amazon OpenSearch é integrada ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, por uma função ou por um serviço da AWS na Ingestão do OpenSearch.

O CloudTrail captura todas as chamadas de API para a Ingestão do OpenSearch como eventos. As chamadas capturadas incluem chamadas da seção de Ingestão do console do OpenSearch Service e chamadas de código para as operações da API de Ingestão do OpenSearch.

Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para a Ingestão do OpenSearch. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Histórico de eventos.

Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para a Ingestão do OpenSearch, o endereço IP no qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, além de detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Informações do OpenSearch Injestion no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando ocorre uma atividade na Ingestão do OpenSearch, essa atividade é registrada em um evento do CloudTrail com outros eventos de serviço da AWS no Histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Como visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro contínuo de eventos da sua Conta da AWS, incluindo aqueles da Ingestão do OpenSearch, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS.

A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços da AWS para analisar mais ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e Receber arquivos de log do CloudTrail de várias contas

Todas as ações de Ingestão do OpenSearch são registradas em log pelo CloudTrail e estão documentadas na Referência da API de Ingestão do OpenSearch. Por exemplo, as chamadas para

as APIs `CreateCollection`, `ListCollections` e `DeleteCollection` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

Noções básicas das entradas do arquivo de log da Ingestão do OpenSearch

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log.

Um evento representa uma solicitação única de qualquer fonte. Isso inclui informações sobre a ação solicitada, a data e hora da ação, os parâmetros de solicitação, e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `DeletePipeline`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/test-user",
        "accountId": "123456789012",
        "accessKeyId": "access-key",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
```

```
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-04-21T16:48:33Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-04-21T16:49:22Z",
    "eventSource": "osis.amazonaws.com",
    "eventName": "UpdatePipeline",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "123.456.789.012",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36",
    "requestParameters": {
        "pipelineName": "my-pipeline",
        "pipelineConfigurationBody": "version: \"2\"\nlog-pipeline:\n  source:\n
 http:\n        path: \"/test/logs\"\n  processor:\n    - grok:\n        match:\n
        log: [ '%{COMMONAPACHELOG}' ]\n    - date:\n        from_time_received: true
\n        destination: \"@timestamp\"\n  sink:\n    - opensearch:\n        hosts:
 [ \"https://search-b5zd22mwxhggheqpj5ftslgyle.us-west-2.es.amazonaws.com\" ]\n
  index: \"apache_logs2\"\n        aws_sts_role_arn: \"arn:aws:iam::709387180454:role/
canary-bootstrap-OsisRole-J1BARLD26QKN\"\n        aws_region: \"us-west-2\"\n
 aws_sigv4: true\n"
    },
    "responseElements": {
        "pipeline": {
            "pipelineName": "my-pipeline",sourceIPAddress
            "pipelineArn": "arn:aws:osis:us-west-2:123456789012:pipeline/my-pipeline",
            "minUnits": 1,
            "maxUnits": 1,
            "status": "UPDATING",
            "statusReason": {
                "description": "An update was triggered for the pipeline. It is still
 available to ingest data."
            },
            "pipelineConfigurationBody": "version: \"2\"\nlog-pipeline:\n  source:\n
    http:\n        path: \"/test/logs\"\n  processor:\n    - grok:\n        match:
\n          log: [ '%{COMMONAPACHELOG}' ]\n    - date:\n        from_time_received:
 true\n        destination: \"@timestamp\"\n  sink:\n    - opensearch:\n        hosts:
 [ \"https://search-b5zd22mwxhggheqpj5ftslgyle.us-west-2.es.amazonaws.com\" ]\n
  index: \"apache_logs2\"\n        aws_sts_role_arn: \"arn:aws:iam::709387180454:role/
```

```
canary-bootstrap-OsisRole-J1BARLD26QKN\"\n        aws_region: \"us-west-2\"\n
 aws_sigv4: true\n",
            "createdAt": "Mar 29, 2023 1:03:44 PM",
            "lastUpdatedAt": "Apr 21, 2023 9:49:21 AM",
            "ingestEndpointUrls": [
                "my-pipeline-tu33ldsgdltgv7x7tjqiudvf7m.us-west-2.osis.amazonaws.com"
            ]
        }
    },
    "requestID": "12345678-1234-1234-1234-987654321098",
    "eventID": "12345678-1234-1234-1234-987654321098",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "709387180454",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "osis.us-west-2.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

Uso de tags nos pipelines de Ingestão do Amazon OpenSearch

As tags permitem atribuir informações arbitrárias a um pipeline de Ingestão do Amazon OpenSearch para que você possa categorizar e filtrar por essas informações. Uma tag é um rótulo de metadados que você ou a AWS atribui a um recurso da AWS. Cada tag consiste em uma chave e um valor. Para tags atribuídas por você, é possível definir a chave e o valor. Por exemplo, talvez você defina a chave como `stage` e o valor de recurso como `test`.

As tags ajudam você a fazer o seguinte:

- Identificar e organizar seus recursos da AWS. Muitos serviços da AWS oferecem suporte à marcação para que você possa atribuir a mesma tag a recursos de diferentes serviços para indicar que os recursos estão relacionados. Por exemplo, é possível atribuir a mesma tag a um pipeline de Ingestão do OpenSearch que você atribui a um domínio do Amazon OpenSearch Service.
- Monitorar seus custos da AWS. Você pode ativar essas tags no painel do AWS Billing and Cost Management. A AWS usa as tags para categorizar seus custos e entregar um relatório mensal de

alocação de custos para você. Para obter mais informações, consulte Usar tags de alocação de custos no Guia do usuário do AWS Billing.

- Restrinja o acesso aos pipelines usando controle de acesso baseado em atributos. Para obter mais informações, consulte Controlar o acesso baseado em chaves de tag no Guia do Usuário do IAM.

Na Ingestão do OpenSearch, o principal recurso é um pipeline. Você pode usar o console do OpenSearch Service, o CLI AWS, APIs de Ingestão do OpenSearch ou os SDKs da AWS para adicionar, gerenciar e remover tags de um pipeline.

Tópicos

Permissões obrigatórias

A Ingestão do OpenSearch usa as seguintes permissões do (IAM) AWS Identity and Access Management Access Analyzer para aplicar tags em pipelines:

- `osis:TagResource`
- `osis:ListTagsForResource`
- `osis:UntagResource`

Para mais informações sobre cada permissão, consulte Ações, recursos e chaves de condição para a Ingestão do OpenSearch na Referência de autorização do serviço.

Uso de tags (console)

O console é a maneira mais simples marcar um pipeline com tags.

Como criar uma tag

1. Faça login no console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. No painel de navegação à esquerda, escolha Ingestão.

3. Selecione o pipeline ao qual você deseja adicionar tags e vá para guia Tags.
4. Escolha Gerenciar e Adicionar nova tag.
5. Insira uma chave de tag e um valor opcional.
6. Escolha Salvar.

Para excluir uma tag, siga as mesmas etapas e escolha Remover na página Gerenciar tags.

Para obter mais informações sobre como usar o console para trabalhar com tags, consulte Editor de tags no Guia de conceitos básicos do Console de GerenciamentoAWS.

Uso de tags (AWS CLI)

Para marcar um pipeline usando a AWS CLI, envie uma solicitação `TagResource`:

```
aws osis tag-resource
  --arn arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline
  --tags Key=service,Value=osis Key=source,Value=otel
```

Remova as tags de um pipeline usando o comando `UntagResource`:

```
aws osis untag-resource
  --arn arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline
  --tag-keys service
```

É possível exibir as tags existentes para um pipeline com o comando `ListTagsForResource`:

```
aws osis list-tags-for-resource
  --arn arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline
```

Log e monitoramento da Ingestão do Amazon OpenSearch com o Amazon CloudWatch

A Ingestão do Amazon OpenSearch publica métricas e logs no Amazon CloudWatch.

Tópicos

- Monitoramento dos logs de pipeline
- Métricas do pipeline de monitoramento

Monitoramento dos logs de pipeline

Você pode habilitar o log dos pipelines de Ingestão do Amazon OpenSearch para expor mensagens de erro e aviso geradas durante as operações do pipeline e a atividade de ingestão. A Ingestão do OpenSearch publica todos os logs no Amazon CloudWatch Logs. O CloudWatch Logs pode monitorar informações nos arquivos de log e notificar você quando determinados limites forem atingidos. Você também pode arquivar seus dados de log em armazenamento resiliente. Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch Logs.

Os logs da Ingestão do OpenSearch podem indicar falhas no processamento de solicitações, erros de autenticação da origem até o coletor e outros avisos que podem ser úteis para a solução de problemas. Para seus logs, a Ingestão do OpenSearch usa os níveis de log de `INFO`, `WARN`, `ERROR` e `FATAL`. Recomendamos habilitar a publicação de logs para todos os pipelines.

Permissões obrigatórias

Para habilitar a Ingestão do OpenSearch para enviar logs para o CloudWatch Logs, você deve estar registrado como um usuário com certas permissões do IAM.

Você precisa das seguintes permissões do CloudWatch Logs para criar e atualizar os recursos de entrega de logs:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Resource": "*",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:PutResourcePolicy",
                "logs:UpdateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:DescribeResourcePolicies",
                "logs:GetLogDelivery",
                "logs:ListLogDeliveries"
            ]
        }
    ]
}
```

Habilitar publicação de logs

Você pode ativar a publicação de logs em pipelines existentes ou ao criar um pipeline. Para ver as etapas para habilitar a publicação de logs durante a criação do pipeline, consulte the section called “Como criar pipelines”.

Console

Para habilitar a publicação de logs em um pipeline existente

1. Faça login no console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. Escolha Ingestão no painel de navegação esquerdo e selecione o pipeline para o qual você deseja habilitar logs.
3. Escolha Editar opções de publicação de logs.
4. Selecione Publicar no CloudWatch Logs.
5. Crie um novo grupo de logs ou selecione um existente. Recomendamos que você formate o nome como um caminho, como `/aws/vendedlogs/OpenSearchIngestion/pipeline-name/audit-logs`. Esse formato facilita a aplicação de uma política de acesso do CloudWatch que concede permissões a todos os grupos de log em um caminho específico, como. `/aws/vendedlogs/OpenSearchService/OpenSearchIngestion`

   > **Important**
   >
   > Você deve incluir o prefixo `vendedlogs` no nome do grupo de logs, caso contrário, a criação falhará.

6. Escolha Salvar.

CLI

Para habilitar a publicação de logs usando o AWS CLI, envie a seguinte solicitação:

```
aws osis update-pipeline \
  --pipeline-name my-pipeline \
  --log-publishing-options  IsLoggingEnabled=true,CloudWatchLogDestination={LogGroup="/aws/vendedlogs/OpenSearchIngestion/pipeline-name"}
```

Métricas do pipeline de monitoramento

Você pode monitorar os pipelines de Ingestão do Amazon OpenSearch usando o Amazon CloudWatch, que coleta dados brutos e os processa em métricas legíveis quase em tempo real. Essas estatísticas são mantidas por 15 meses, de maneira que você possa acessar informações históricas e ter uma perspectiva melhor de como o aplicativo web ou o serviço está se saindo. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch.

O console da Ingestão do OpenSearch exibe uma série de gráficos com base nos dados brutos do CloudWatch na guia Desempenho de cada pipeline.

A Ingestão do OpenSearch relata métricas da maioria dos plug-ins compatíveis. Se certos plug-ins não tiverem sua própria tabela abaixo, isso significa que eles não tiveram nenhuma métrica específica do plug-in reportada. As métricas de pipeline estão publicadas no namespace `AWS/OSIS`.

Tópicos

- Métricas do sistema e de medição

Métricas comuns

As métricas a seguir são comuns a todos os processadores e coletores.

Cada métrica é prefixada pelo nome do subpipeline e pelo nome do plug-in, no formato <*sub_pipeline_name*><*plugin*><*metric_name*>. Por exemplo, o nome completo da métrica `recordsIn.count` de um subpipeline chamado `my-pipeline` e o processador date seriam `my-pipeline.date.recordsIn.count`.

Sufixo métrico	Descrição
`recordsIn.count`	A entrada de registros em um componente do pipeline. Essa métrica se aplica a processadores e coletores. Estatísticas relevantes: soma Dimensão:`PipelineName`
`recordsOut.count`	A saída de registros em um componente do pipeline. Essa métrica se aplica a processadores e origens. Estatísticas relevantes: soma Dimensão:`PipelineName`
`timeElapsed.count`	Uma contagem de pontos de dados registrados durante a execução de um componente do pipeline. Essa métrica se aplica a processadores e coletores. Estatísticas relevantes: soma Dimensão:`PipelineName`
`timeElapsed.sum`	O tempo total decorrido durante a execução de um componente do pipeline. Essa métrica se aplica a processadores e coletores, em milissegundos. Estatísticas relevantes: soma

Sufixo métrico	Descrição
	Dimensão:`PipelineName`
`timeElapsed.max`	O tempo máximo decorrido durante a execução de um componente do pipeline. Essa métrica se aplica a processadores e coletores, em milissegundos. Estatísticas relevantes: máx. Dimensão:`PipelineName`

Métricas do buffer

As métricas a seguir se aplicam ao buffer de bloqueio limitado padrão que a Ingestão do OpenSearch configura automaticamente para todos os pipelines.

Cada métrica é prefixada pelo nome do subpipeline e pelo nome do buffer, no formato <*sub_pipeline_name*><*buffer_name*><*metric_name*>. Por exemplo, o nome completo da métrica `recordsWritten.count` de um subpipeline chamado `my-pipeline` seria `my-pipeline.BlockingBuffer.recordsWritten.count`.

Sufixo métrico	Descrição
`recordsWritten.count`	O número de registros gravados em um buffer. Estatísticas relevantes: soma Dimensão:`PipelineName`
`recordsRead.count`	O número de registros lidos de um buffer. Estatísticas relevantes: soma Dimensão:`PipelineName`
`recordsInFlight.value`	O número de registros não verificados lidos de um buffer. Estatística relevante: média

Sufixo métrico	Descrição
	Dimensão:`PipelineName`
`recordsInBuffer.value`	O número de registros atualmente em um buffer. Estatística relevante: média Dimensão:`PipelineName`
`recordsProcessed.count`	O número de registros lidos de um buffer e processados por um pipeline. Estatísticas relevantes: soma Dimensão:`PipelineName`
`recordsWriteFailed.count`	O número de registros que o pipeline não conseguiu gravar no coletor. Estatísticas relevantes: soma Dimensão:`PipelineName`
`writeTimeElapsed.count`	Uma contagem de pontos de dados registrados durante a gravação em um buffer. Estatísticas relevantes: soma Dimensão:`PipelineName`
`writeTimeElapsed.sum`	O tempo total decorrido durante a gravação em um buffer, em milissegundos. Estatísticas relevantes: soma Dimensão:`PipelineName`

Sufixo métrico	Descrição
`writeTimeElapsed.max`	O tempo máximo decorrido durante a gravação em um buffer, em milissegundos. Estatísticas relevantes: máx. Dimensão:`PipelineName`
`writeTimeouts.count`	A contagem dos tempos limite de gravação em um buffer. Estatísticas relevantes: soma Dimensão:`PipelineName`
`readTimeElapsed.count`	Uma contagem de pontos de dados registrados durante a leitura de um buffer. Estatísticas relevantes: soma Dimensão:`PipelineName`
`readTimeElapsed.sum`	O tempo total decorrido durante a leitura de um buffer, em milissegundos. Estatísticas relevantes: soma Dimensão:`PipelineName`
`readTimeElapsed.max`	O tempo máximo decorrido durante a leitura de um buffer, em milissegundos. Estatísticas relevantes: máx. Dimensão:`PipelineName`
`checkpointTimeElapsed.count`	Uma contagem de pontos de dados registrados durante o checkpoint. Estatísticas relevantes: soma Dimensão:`PipelineName`

Sufixo métrico	Descrição
`checkpointTimeElapsed.sum`	O tempo total decorrido durante o checkpoint, em milissegundos. Estatísticas relevantes: soma Dimensão:`PipelineName`
`checkpointTimeElapsed.max`	O tempo máximo decorrido durante o checkpoint, em milissegundos. Estatísticas relevantes: máx. Dimensão:`PipelineName`

Métricas do Signature V4

As métricas a seguir se aplicam ao endpoint de ingestão de um pipeline e estão associadas aos plug-ins de origem (`http`, `otel_trace` e `otel_metrics`). Todas as solicitações para o endpoint de ingestão devem ser assinadas usando o Signature Version 4. Essas métricas podem ajudar você a identificar problemas de autorização ao se conectar ao seu pipeline ou confirmar que você está autenticando com sucesso.

Cada métrica é prefixada pelo nome do subpipeline e `osis_sigv4_auth`. Por exemplo, *`sub_pipeline_name`*`.osis_sigv4_auth.httpAuthSuccess.count`.

Sufixo métrico	Descrição
`httpAuthSuccess.count`	O número de solicitações bem-sucedidas do Signature V4 para o pipeline. Estatísticas relevantes: soma Dimensão:`PipelineName`
`httpAuthFailure.count`	O número de solicitações do Signature V4 que falharam no pipeline. Estatísticas relevantes: soma

Sufixo métrico	Descrição
	Dimensão:`PipelineName`
`httpAuthServerError.count`	O número de solicitações do Signature V4 ao pipeline que retornaram erros do servidor. Estatísticas relevantes: soma Dimensão:`PipelineName`

Métricas de buffer de bloqueio limitado

As métricas a seguir se aplicam ao buffer de bloqueio limitado. Cada métrica é prefixada pelo nome do subpipeline e `BlockingBuffer`. Por exemplo, *`sub_pipeline_name`*`.BlockingBuffer.bufferUsage.value`.

Sufixo métrico	Descrição
`bufferUsage.value`	Porcentagem de uso do `buffer_size` com base no número de registros no buffer. `buffer_size` represent a o número máximo de registros gravados no buffer, bem como registros em ação que não foram verificados. Estatística relevante: média Dimensão:`PipelineName`

Métricas da fonte de rastreamento OTel

As métricas a seguir se aplicam à fonte do OTel trace (Rastreamento do OTel). Cada métrica é prefixada pelo nome do subpipeline e `otel_trace_source`. Por exemplo, *`sub_pipeline_name`*`.otel_trace_source.requestTimeouts.count`.

Sufixo métrico	Descrição
`requestTimeouts.count`	O número de solicitações que atingiram o tempo limite.

Sufixo métrico	Descrição
	Estatísticas relevantes: soma Dimensão:`PipelineName`
`requestsReceived.count`	O número de solicitações recebidas pelo plug-in. Estatísticas relevantes: soma Dimensão:`PipelineName`
`successRequests.count`	O número de solicitações que foram processadas com êxito pelo plugin. Estatísticas relevantes: soma Dimensão:`PipelineName`
`badRequests.count`	O número de solicitações com um formato inválido que foram processadas pelo plug-in. Estatísticas relevantes: soma Dimensão:`PipelineName`
`requestsTooLarge.count`	O número de solicitações cujas extensões no conteúdo são maiores do que a capacidade do buffer. Estatísticas relevantes: soma Dimensão:`PipelineName`
`internalServerError.count`	O número de solicitações processadas pelo plug-in com um tipo de exceção personalizado. Estatísticas relevantes: soma Dimensão:`PipelineName`

Sufixo métrico	Descrição
`requestProcessDuration.count`	Uma contagem de pontos de dados registrados durante o processamento de solicitações pelo plug-in. Estatísticas relevantes: soma Dimensão:`PipelineName`
`requestProcessDuration.sum`	A latência total das solicitações processadas pelo plug-in, em milissegundos. Estatísticas relevantes: soma Dimensão:`PipelineName`
`requestProcessDuration.max`	A latência máxima das solicitações processadas pelo plug-in, em milissegundos. Estatísticas relevantes: máx. Dimensão:`PipelineName`
`payloadSize.count`	Uma contagem da distribuição dos tamanhos de carga das solicitações recebidas, em bytes. Estatísticas relevantes: soma Dimensão:`PipelineName`
`payloadSize.sum`	A distribuição total dos tamanhos da carga útil das solicitações recebidas, em bytes. Estatísticas relevantes: soma Dimensão:`PipelineName`

Sufixo métrico	Descrição
`payloadSize.max`	A distribuição máxima dos tamanhos de carga das solicitações recebidas, em bytes. Estatísticas relevantes: máx. Dimensão:`PipelineName`

Métricas do OTel: métricas de origem

As métricas a seguir se aplicam à fonte de métricas do OTel. Cada métrica é prefixada pelo nome do subpipeline e `otel_metrics_source`. Por exemplo, *`sub_pipeline_name`*`.otel_metrics_source.requestTimeouts.count`.

Sufixo métrico	Descrição
`requestTimeouts.count`	O número total de solicitações do plug-in que expiraram. Estatísticas relevantes: soma Dimensão:`PipelineName`
`requestsReceived.count`	O número total de solicitações recebidas pelo plug-in. Estatísticas relevantes: soma Dimensão:`PipelineName`
`successRequests.count`	O número de solicitações processadas com sucesso (código de status de 200 respostas) pelo plug-in. Estatísticas relevantes: soma Dimensão:`PipelineName`
`requestProcessDuration.count`	Uma contagem da latência das solicitações processadas pelo plug-in, em segundos. Estatísticas relevantes: soma

Sufixo métrico	Descrição
	Dimensão:`PipelineName`
`requestProcessDuration.sum`	A latência total das solicitações processadas pelo plug-in, em milissegundos. Estatísticas relevantes: soma Dimensão:`PipelineName`
`requestProcessDuration.max`	A latência máxima das solicitações processadas pelo plug-in, em milissegundos. Estatísticas relevantes: máx. Dimensão:`PipelineName`
`payloadSize.count`	Uma contagem da distribuição dos tamanhos de carga das solicitações recebidas, em bytes. Estatísticas relevantes: soma Dimensão:`PipelineName`
`payloadSize.sum`	A distribuição total dos tamanhos da carga útil das solicitações recebidas, em bytes. Estatísticas relevantes: soma Dimensão:`PipelineName`
`payloadSize.max`	A distribuição máxima dos tamanhos de carga das solicitações recebidas, em bytes. Estatísticas relevantes: máx. Dimensão:`PipelineName`

Métricas HTTP

As métricas a seguir se aplicam à fonte HTTP. Cada métrica é prefixada pelo nome do subpipeline e `http`. Por exemplo, *`sub_pipeline_name`*`.http.requestsReceived.count`.

Sufixo métrico	Descrição
`requestsReceived.count`	O número de solicitações recebido pelo endpoint do `/log/ingest` . Estatísticas relevantes: soma Dimensão:`PipelineName`
`requestsRejected.count`	O número de solicitações rejeitadas pelo plug-in (código de status de resposta 429). Estatísticas relevantes: soma Dimensão:`PipelineName`
`successRequests.count`	O número de solicitações processadas com sucesso (código de status de 200 respostas) pelo plug-in. Estatísticas relevantes: soma Dimensão:`PipelineName`
`badRequests.count`	O número de solicitações com tipo ou formato de conteúdo inválido processadas pelo plug-in (código de status de 400 respostas). Estatísticas relevantes: soma Dimensão:`PipelineName`
`requestTimeouts.count`	O número de solicitações que atingem o tempo limite no servidor de origem HTTP (código de status de resposta 415). Estatísticas relevantes: soma

Sufixo métrico	Descrição
	Dimensão:`PipelineName`
`requestsTooLarge.count`	O número de solicitações cujo tamanho dos eventos no conteúdo é maior que a capacidade do buffer (código de status de resposta 413). Estatísticas relevantes: soma Dimensão:`PipelineName`
`internalServerError.count`	O número de solicitações processadas pelo plug-in com um tipo de exceção personalizado (código de status de 500 respostas). Estatísticas relevantes: soma Dimensão:`PipelineName`
`requestProcessDuration.count`	Uma contagem da latência das solicitações processadas pelo plug-in, em segundos. Estatísticas relevantes: soma Dimensão:`PipelineName`
`requestProcessDuration.sum`	A latência total das solicitações processadas pelo plug-in, em milissegundos. Estatísticas relevantes: soma Dimensão:`PipelineName`
`requestProcessDuration.max`	A latência máxima das solicitações processadas pelo plug-in, em milissegundos. Estatísticas relevantes: máx. Dimensão:`PipelineName`

Sufixo métrico	Descrição
`payloadSize.count`	Uma contagem da distribuição dos tamanhos de carga das solicitações recebidas, em bytes. Estatísticas relevantes: soma Dimensão:`PipelineName`
`payloadSize.sum`	A distribuição total dos tamanhos da carga útil das solicitaç ões recebidas, em bytes. Estatísticas relevantes: soma Dimensão:`PipelineName`
`payloadSize.max`	A distribuição máxima dos tamanhos de carga das solicitações recebidas, em bytes. Estatísticas relevantes: máx. Dimensão:`PipelineName`

Métricas do S3

As métricas a seguir se aplicam à fonte do S3. Cada métrica é prefixada pelo nome do subpipeline e `s3`. Por exemplo, *`sub_pipeline_name`*`.s3.s3ObjectsFailed.count`.

Sufixo métrico	Descrição
`s3ObjectsFailed.count`	O número total de objetos do S3 que o plug-in não conseguiu ler. Estatísticas relevantes: soma Dimensão:`PipelineName`
`s3ObjectsNotFound.count`	O número de objetos do S3 que o plug-in não conseguiu ler devido a um erro de `Not Found` do S3. Essas métricas também contam para a métrica `s3ObjectsFailed` .

Sufixo métrico	Descrição
	Estatísticas relevantes: soma Dimensão:`PipelineName`
`s3ObjectsAccessDenied.count`	O número de objetos do S3 que o plug-in não conseguiu ler devido a um erro de `Access Denied` ou `Forbidden` do S3. Essas métricas também contam para a métrica `s3ObjectsFailed` . Estatísticas relevantes: soma Dimensão:`PipelineName`
`s3ObjectReadTimeElapsed.count`	A quantidade de tempo que o plug-in leva para realizar uma solicitação GET para um objeto do S3, analisá-lo e gravar eventos no buffer. Estatísticas relevantes: soma Dimensão:`PipelineName`
`s3ObjectReadTimeElapsed.sum`	O tempo total que o plug-in leva para realizar uma solicitação GET para um objeto do S3, analisá-lo e gravar eventos no buffer, em milissegundos. Estatísticas relevantes: soma Dimensão:`PipelineName`
`s3ObjectReadTimeElapsed.max`	O tempo máximo que o plug-in leva para realizar uma solicitação GET para um objeto do S3, analisá-lo e gravar eventos no buffer, em milissegundos. Estatísticas relevantes: máx. Dimensão:`PipelineName`

Sufixo métrico	Descrição
`s3ObjectSizeBytes.count`	A contagem da distribuição dos tamanhos dos objetos do S3, em bytes. Estatísticas relevantes: soma Dimensão:`PipelineName`
`s3ObjectSizeBytes.sum`	A distribuição total dos tamanhos dos objetos do S3, em bytes. Estatísticas relevantes: soma Dimensão:`PipelineName`
`s3ObjectSizeBytes.max`	A distribuição máxima dos tamanhos de objetos do S3, em bytes. Estatísticas relevantes: máx. Dimensão:`PipelineName`
`s3ObjectProcessedBytes.count`	A contagem da distribuição dos objetos do S3 processados pelo plug-in, em bytes. Estatísticas relevantes: soma Dimensão:`PipelineName`
`s3ObjectProcessedBytes.sum`	A distribuição total dos objetos do S3 processados pelo plug-in, em bytes. Estatísticas relevantes: soma Dimensão:`PipelineName`

Sufixo métrico	Descrição
`s3ObjectProcessedBytes.max`	A distribuição máxima dos objetos do S3 processados pelo plug-in, em bytes. Estatísticas relevantes: máx. Dimensão:`PipelineName`
`s3ObjectsEvents.count`	A contagem da distribuição dos eventos do S3 recebidos pelo plug-in. Estatísticas relevantes: soma Dimensão:`PipelineName`
`s3ObjectsEvents.sum`	A distribuição total dos eventos do S3 recebidos pelo plug-in. Estatísticas relevantes: soma Dimensão:`PipelineName`
`s3ObjectsEvents.max`	A distribuição máxima dos eventos do S3 recebidos pelo plug-in. Estatísticas relevantes: máx. Dimensão:`PipelineName`
`sqsMessageDelay.count`	Uma contagem de pontos de dados registrados desde quando o S3 registra um horário de evento para a criação de um objeto até quando ele é totalmente analisado. Estatísticas relevantes: soma Dimensão:`PipelineName`

Sufixo métrico	Descrição
`sqsMessageDelay.sum`	O tempo total entre o momento em que o S3 registra o horário de um evento para a criação de um objeto e o momento em que ele é totalmente analisado, em milissegundos. Estatísticas relevantes: soma Dimensão:`PipelineName`
`sqsMessageDelay.max`	O tempo máximo entre o momento em que o S3 grava um evento para a criação de um objeto e o momento em que ele é totalmente analisado, em milissegundos. Estatísticas relevantes: máx. Dimensão:`PipelineName`
`s3ObjectsSucceeded.count`	O número de objetos do S3 que o plug-in leu com sucesso. Estatísticas relevantes: soma Dimensão:`PipelineName`
`sqsMessagesReceived.count`	O número de mensagens do Amazon SQS recebidas da fila pelo plug-in. Estatísticas relevantes: soma Dimensão:`PipelineName`
`sqsMessagesDeleted.count`	O número de mensagens do Amazon SQS excluídas da fila pelo plugin. Estatísticas relevantes: soma Dimensão:`PipelineName`

Sufixo métrico	Descrição
`sqsMessagesFailed.count`	O número de mensagens do Amazon SQS que o plug-in não conseguiu analisar. Estatísticas relevantes: soma Dimensão:`PipelineName`

Métricas agregadas

As métricas a seguir se aplicam ao processador Aggregate (Agregar). Cada métrica é prefixada pelo nome do subpipeline e `aggregate`. Por exemplo, *`sub_pipeline_name`*`.aggregate.actionHandleEventsOut.count`.

Sufixo métrico	Descrição
`actionHandleEvents Out.count`	O número de eventos que foram retornados da chamada `handleEvent` para a ação configurada. Estatísticas relevantes: soma Dimensão:`PipelineName`
`actionHandleEvents Dropped.count`	O número de eventos que foram retornados da chamada `handleEvent` para a ação configurada. Estatísticas relevantes: soma Dimensão:`PipelineName`
`actionHandleEvents ProcessingErrors.count`	O número de chamadas feitas para `handleEvent` para a ação configurada que resultaram em erro. Estatísticas relevantes: soma Dimensão:`PipelineName`
`actionConcludeGrou pEventsOut.count`	O número de eventos que foram retornados da chamada `concludeGroup` para a ação configurada.

Sufixo métrico	Descrição
	Estatísticas relevantes: soma Dimensão:`PipelineName`
`actionConcludeGrou pEventsDropped.count`	O número de eventos que não foram retornados da chamada `condludeGroup` para a ação configurada. Estatísticas relevantes: soma Dimensão:`PipelineName`
`actionConcludeGrou pEventsProcessingE rrors.count`	O número de chamadas feitas para `concludeGroup` para a ação configurada que resultaram em erro. Estatísticas relevantes: soma Dimensão:`PipelineName`
`currentAggregateGr oups.value`	O número atual de grupos. Esse indicador diminui quando os grupos são concluídos e aumenta quando um evento inicia a criação de um novo grupo. Estatística relevante: média Dimensão:`PipelineName`

Métricas de data

As métricas a seguir se aplicam ao processador de Date (Data). Cada métrica é prefixada pelo nome do subpipeline e `date`. Por exemplo, *`sub_pipeline_name`*`.date.dateProcessingMatchSuccess.count`.

Sufixo métrico	Descrição
`dateProcessingMatc hSuccess.count`	O número de registros que correspondem a pelo menos um dos padrões especificados na opção de configuração `match`.

Sufixo métrico	Descrição
	Estatísticas relevantes: soma Dimensão:`PipelineName`
`dateProcessingMatchFailure.count`	O número de registros que não corresponderam a nenhum dos padrões especificados na opção de configuração `match`. Estatísticas relevantes: soma Dimensão:`PipelineName`

Métricas do Grok

As métricas a seguir se aplicam ao processador Grok. Cada métrica é prefixada pelo nome do subpipeline e `grok`. Por exemplo, *`sub_pipeline_name`*`.grok.grokProcessingMatch.count`.

Sufixo métrico	Descrição
`grokProcessingMatch.count`	O número de registros que encontraram pelo menos uma correspondência de padrão na opção de configuração `match`. Estatísticas relevantes: soma Dimensão:`PipelineName`
`grokProcessingMismatch.count`	O número de registros que não corresponderam a nenhum dos padrões especificados na opção de configuração `match`. Estatísticas relevantes: soma Dimensão:`PipelineName`
`grokProcessingErrors.count`	O número de erros de processamento de registros. Estatísticas relevantes: soma

Sufixo métrico	Descrição
	Dimensão:`PipelineName`
`grokProcessingTimeouts.count`	O número de registros que atingiram o tempo limite durante a correspondência. Estatísticas relevantes: soma Dimensão:`PipelineName`
`grokProcessingTime.count`	Uma contagem de pontos de dados registrados enquanto um registro individual correspondia aos padrões da opção de configuração `match`. Estatísticas relevantes: soma Dimensão:`PipelineName`
`grokProcessingTime.sum`	O tempo total que cada registro individual leva para corresponder aos padrões da opção de configuração `match`, em milissegundos. Estatísticas relevantes: soma Dimensão:`PipelineName`
`grokProcessingTime.max`	O tempo máximo que cada registro individual leva para corresponder aos padrões da opção de configuração `match`, em milissegundos. Estatísticas relevantes: máx. Dimensão:`PipelineName`

Métricas brutas do OTel trace

As métricas a seguir se aplicam ao processador bruto de rastreamento OTel trace.
Cada métrica é prefixada pelo nome do subpipeline e `otel_trace_raw`. Por exemplo, *`sub_pipeline_name`*`.otel_trace_raw.traceGroupCacheCount.value`.

Sufixo métrico	Descrição
`traceGroupCacheCount.value`	O número de grupos de rastreamento no cache do grupo de rastreamento. Estatísticas relevantes: soma Dimensão:`PipelineName`
`spanSetCount.value`	O número de conjuntos de períodos na coleção de conjuntos de períodos. Estatísticas relevantes: soma Dimensão:`PipelineName`

Métricas de grupo de monitoramento do OTel

As métricas a seguir se aplicam ao processador de grupos de rastreamento OTel. Cada métrica é prefixada pelo nome do subpipeline e `otel_trace_group`. Por exemplo, *`sub_pipeline_name`*`.otel_trace_group.recordsInMissingTraceGroup.count`.

Sufixo métrico	Descrição
`recordsInMissingTraceGroup.count`	O número de registros de entrada sem os campos do grupo de rastreamento. Estatísticas relevantes: soma Dimensão:`PipelineName`
`recordsOutFixedTraceGroup.count`	O número de registros de saída com os campos do grupo de rastreamento preenchidos com sucesso. Estatísticas relevantes: soma Dimensão:`PipelineName`

Sufixo métrico	Descrição
`recordsOutMissingTraceGroup.count`	O número de registros de saída sem os campos do grupo de rastreamento. Estatísticas relevantes: soma Dimensão:`PipelineName`

Métricas do mapa de serviço

As métricas a seguir se aplicam ao processador Service-map stateful (Mapa de serviço com estado). Cada métrica é prefixada pelo nome do subpipeline e `service-map-stateful`. Por exemplo, *`sub_pipeline_name`*`.service-map-stateful.spansDbSize.count`.

Sufixo métrico	Descrição
`spansDbSize.value`	Os tamanhos de bytes na memória das extensões no MapDB nas durações da janela atual e anterior. Estatística relevante: média Dimensão:`PipelineName`
`traceGroupDbSize.value`	Os tamanhos de bytes na memória dos grupos de rastreamento no MapDB nas durações da janela atual e anterior. Estatística relevante: média Dimensão:`PipelineName`
`spansDbCount.value`	A contagem de intervalos das extensões no MapDB nas durações da janela atual e anterior. Estatísticas relevantes: soma Dimensão:`PipelineName`

Sufixo métrico	Descrição
`traceGroupDbCount.value`	A contagem de grupos de rastreamento das extensões no MapDB nas durações da janela atual e anterior. Estatísticas relevantes: soma Dimensão:`PipelineName`
`relationshipCount.value`	A contagem de relacionamentos armazenados nas durações da janela atual e anterior. Estatísticas relevantes: soma Dimensão:`PipelineName`

Métricas do OpenSearch

As métricas a seguir se aplicam ao coletor do OpenSearch. Cada métrica é prefixada pelo nome do subpipeline e `opensearch`. Por exemplo, *`sub_pipeline_name`*`.opensearch.bulkRequestErrors.count`.

Sufixo métrico	Descrição
`bulkRequestErrors.count`	O número total de erros encontrados ao enviar solicitações em massa. Estatísticas relevantes: soma Dimensão:`PipelineName`
`documentsSuccess.count`	O número de documentos enviados com sucesso para o OpenSearch Service por solicitação em massa, incluindo novas tentativas. Estatísticas relevantes: soma Dimensão:`PipelineName`

Sufixo métrico	Descrição
`documentsSuccessFirstAttempt.count`	O número de documentos enviados com sucesso ao OpenSearch Service por solicitação em massa na primeira tentativa. Estatísticas relevantes: soma Dimensão:`PipelineName`
`documentErrors.count`	O número de documentos que não foram enviados por solicitações em massa. Estatísticas relevantes: soma Dimensão:`PipelineName`
`bulkRequestFailed.count`	O número de solicitações em massa que falharam. Estatísticas relevantes: soma Dimensão:`PipelineName`
`bulkRequestNumberOfRetries.count`	O número de novas tentativas de solicitações em massa com falha Estatísticas relevantes: soma Dimensão:`PipelineName`
`bulkBadRequestErrors.count`	O número de `Bad Request` erros encontrados ao enviar solicitações em massa. Estatísticas relevantes: soma Dimensão:`PipelineName`

Sufixo métrico	Descrição
`bulkRequestNotAllowedErrors.count`	O número de `Request Not Allowed` erros encontrados ao enviar solicitações em massa. Estatísticas relevantes: soma Dimensão:`PipelineName`
`bulkRequestInvalidInputErrors.count`	O número de `Invalid Input` erros encontrados ao enviar solicitações em massa. Estatísticas relevantes: soma Dimensão:`PipelineName`
`bulkRequestNotFoundErrors.count`	O número de `Request Not Found` erros encontrados ao enviar solicitações em massa. Estatísticas relevantes: soma Dimensão:`PipelineName`
`bulkRequestTimeoutErrors.count`	O número de `Request Timeout` erros encontrados ao enviar solicitações em massa. Estatísticas relevantes: soma Dimensão:`PipelineName`
`bulkRequestServerErrors.count`	O número de `Server Error` erros encontrados ao enviar solicitações em massa. Estatísticas relevantes: soma Dimensão:`PipelineName`

Sufixo métrico	Descrição
`bulkRequestSizeBytes.count`	Uma contagem da distribuição dos tamanhos de pacote das solicitações em massa, em bytes. Estatísticas relevantes: soma Dimensão:`PipelineName`
`bulkRequestSizeBytes.sum`	A distribuição total dos tamanhos de pacote das solicitações em massa, em bytes. Estatísticas relevantes: soma Dimensão:`PipelineName`
`bulkRequestSizeBytes.max`	A distribuição máxima dos tamanhos de pacote das solicitações em massa, em bytes. Estatísticas relevantes: máx. Dimensão:`PipelineName`
`bulkRequestLatency.count`	Uma contagem de pontos de dados registrados enquanto as solicitações são enviadas ao plug-in, incluindo novas tentativas. Estatísticas relevantes: soma Dimensão:`PipelineName`
`bulkRequestLatency.sum`	A latência total das solicitações enviadas ao plug-in, incluindo novas tentativas, em milissegundos. Estatísticas relevantes: soma Dimensão:`PipelineName`

Sufixo métrico	Descrição
`bulkRequestLatency.max`	A latência máxima das solicitações enviadas ao plug-in, incluindo novas tentativas, em milissegundos. Estatísticas relevantes: máx. Dimensão:`PipelineName`
`s3.dlqS3RecordsSuccess.count`	O número de registros enviados com sucesso para a fila de mensagens não entregues do S3. Estatísticas relevantes: soma Dimensão:`PipelineName`
`s3.dlqS3RecordsFailed.count`	O número de registros que não foram enviados para a fila de mensagens não entregues do S3. Estatísticas relevantes: soma Dimensão:`PipelineName`
`s3.dlqS3RequestSuccess.count`	O número de solicitações bem-sucedidas para a fila de mensagens não entregues do S3. Estatísticas relevantes: soma Dimensão:`PipelineName`
`s3.dlqS3RequestFailed.count`	O número de solicitações com falha na fila de mensagens não entregues do S3. Estatísticas relevantes: soma Dimensão:`PipelineName`

Sufixo métrico	Descrição
`s3.dlqS3RequestLatency.count`	Uma contagem de pontos de dados registrados enquanto as solicitações são enviadas para a fila de mensagens não entregues do S3, incluindo novas tentativas. Estatísticas relevantes: soma Dimensão:`PipelineName`
`s3.dlqS3RequestLatency.sum`	A latência total das solicitações enviadas para a fila de mensagens não entregues do S3, incluindo novas tentativas, em milissegundos. Estatísticas relevantes: soma Dimensão:`PipelineName`
`s3.dlqS3RequestLatency.max`	A latência máxima das solicitações enviadas para a fila de mensagens não entregues do S3, incluindo novas tentativas, em milissegundos. Estatísticas relevantes: máx. Dimensão:`PipelineName`
`s3.dlqS3RequestSizeBytes.count`	Uma contagem da distribuição dos tamanhos de carga das solicitações para a fila de mensagens não entregues do S3, em bytes. Estatísticas relevantes: soma Dimensão:`PipelineName`
`s3.dlqS3RequestSizeBytes.sum`	A distribuição total dos tamanhos de carga das solicitações para a fila de mensagens não entregues do S3, em bytes. Estatísticas relevantes: soma Dimensão:`PipelineName`

Sufixo métrico	Descrição
`s3.dlqS3RequestSizeBytes.max`	A distribuição máxima dos tamanhos de carga das solicitações para a fila de mensagens não entregues do S3, em bytes. Estatísticas relevantes: máx. Dimensão:`PipelineName`

Métricas do sistema e de medição

As métricas a seguir se aplicam ao sistema geral da Ingestão do OpenSearch. Essas métricas não são prefixadas.

Métrica	Descrição
`system.cpu.usage.value`	A porcentagem de uso da CPU disponível para todos os nós de dados. Estatística relevante: média Dimensão: `PipelineName` , `area`, `id`
`system.cpu.count.value`	A quantidade total de uso da CPU para todos os nós de dados. Estatística relevante: média Dimensão: `PipelineName` , `area`, `id`
`jvm.memory.max.value`	A quantidade máxima de memória que pode ser usada para gerenciamento de memória, em bytes. Estatística relevante: média Dimensão: `PipelineName` , `area`, `id`
`jvm.memory.used.value`	A quantidade total de memória usada em bytes.

Métrica	Descrição
	Estatística relevante: média Dimensão: `PipelineName` , `area`, `idsinal`
`jvm.memory.committed.value`	A quantidade de memória comprometida para uso pela máquina virtual Java (JVM), em bytes. Estatística relevante: média Dimensão: `PipelineName` , `area`, `id`
`computeUnits`	O número de unidades computacionais da Ingestão do OpenSearch (OCUs de ingestão) em uso por um pipeline. Estatísticas relevantes: máximo, soma, média Dimensão:`PipelineName`

Práticas recomendadas para Ingestão do Amazon OpenSearch

Este tópico fornece algumas das práticas recomendadas para a criação e gestão de pipelines de Ingestão do Amazon OpenSearch e contém diretrizes gerais que se aplicam a muitos casos de uso. Cada workload é única e tem características particulares, portanto, nenhuma recomendação genérica é exatamente certa para cada caso de uso.

Tópicos

Práticas recomendadas gerais

As práticas recomendadas gerais a seguir se aplicam à criação e gerenciamento de pipelines.

- Para garantir a alta disponibilidade, configure pipelines de VPC com duas ou três sub-redes. Se você implantar apenas um pipeline em uma sub-rede e a Zona de disponibilidade ficar inativa, você não conseguirá ingerir dados.

- Em cada pipeline, recomendamos limitar o número de subpipelines a 5 ou menos.
- Se você estiver usando o plug-in de origem do S3, use arquivos do S3 de tamanho uniforme para obter um desempenho ideal.
- Se estiver usando o plug-in de origem do S3, adicione 30 segundos de tempo limite de visibilidade adicional para cada 0,25 GB de tamanho de arquivo no bucket do S3 para obter um desempenho ideal.
- Inclua uma fila de mensagens não entregues (DLQ – fila de mensagens não entregues) na configuração do pipeline para que você possa descarregar eventos com falha e torná-los acessíveis para análise. Se seus coletores rejeitarem dados devido a mapeamentos incorretos ou outros problemas, você poderá rotear os dados para o DLQ para avaliar e corrigir o problema.

Alarmes do CloudWatch recomendados

Os alarmes do CloudWatch executam uma ação quando uma métrica do CloudWatch excede um valor especificado por algum período. Por exemplo, o AWS pode enviar um e-mail se o status de integridade do cluster permanecer `red` por mais do que um minuto. Esta seção inclui alguns alarmes recomendados para a Ingestão do Amazon OpenSearch e como responder a eles.

Para obter mais informações sobre configuração de alarmes, consulte Criação de alarmes do Amazon CloudWatch no Manual do usuário do Amazon CloudWatch.

Alarme	Problema
O `computeUnits` máximo é = o `maxUnits` configurado para 15 minutos, 3 vezes consecutivas	O pipeline atingiu a capacidade máxima e pode precisar de uma atualização de `maxUnits`. Aumente a capacidade máxima do seu pipeline
Soma de `opensearch.documentErrors.count` é = soma de *`{sub_pipeline_name}`* `.opensear`	O pipeline não consegue gravar no coletor do OpenSearch. Verifique as permissões do pipeline e confirme se o domínio ou a coleção estão íntegros. Você também pode verificar se há eventos com falha na fila de mensagens não entregues (DLQ), se ela estiver configurada.

Alarme	Problema
`ch.record sIn.count` por 1 minuto, 1 vez consecutiva	
`bulkReque stLatency.max` máximo é >= x por 1 minuto, 1 vez consecutiva	O pipeline está passando por alta latência enviando dados para o coletor do OpenSearch. Provavelmente, isso se deve ao fato de a pia estar subdimensionada ou a uma estratégia de fragmentação deficient e, que está fazendo com que o coletor deixe a desejar. A alta latência sustentada pode afetar o desempenho do pipeline e provavelmente causará uma contrapressão nos clientes.
`httpAuthF ailure.count` soma >= 1 por 1 minuto, 1 vez consecutiva	As solicitações de ingestão não estão sendo autenticadas. Confirme se todos os clientes têm a autenticação Signature versão 4 ativada corretamente.
Média de `system.cp u.usage.value` >= 80% por 15 minutos, 3 vezes consecutivas	A utilização elevada e sustentada da CPU pode ser problemática. Considere aumentar a capacidade máxima do pipeline.
Média de `bufferUsa ge.value` >= 80% por 15 minutos, 3 vezes consecutivas	O uso sustentado de alta bufferização pode ser problemático. Considere aumentar a capacidade máxima do pipeline.

Outros alarmes que você pode considerar

Avalie a possibilidade de configurar os seguintes alarmes, dependendo de quais recursos de Ingestão do Amazon OpenSearch você usa regularmente.

Alarme	Problema
`dynamodb.exportJobFailure.count` soma 1	A tentativa de acionar uma exportação para o Amazon S3 falhou.
Média de `opensearch.EndtoEndLatency.avg` > X por 15 minutos, 4 vezes consecutivas	`EndtoEndLatency` é maior do que o desejado para leitura de fluxos do DynamoDB. Isso pode ser causado por um cluster do OpenSearch subdimensionado ou por uma capacidade máxima de OCUs de pipeline muito baixa para a throughput da WCU na tabela do DynamoDB. `EndtoEndLatency` será maior após uma exportação, mas deve diminuir com o tempo à medida que alcança os fluxos mais recentes do DynamoDB.
`dyanmodb.changeEventsProcessed.count` soma == 0 por X minutos	Nenhum registro está sendo coletado dos fluxos do DynamoDB. Isso pode ser causado por falta de atividade na tabela ou por um problema no acesso aos fluxos do DynamoDB.
soma `opensearch.s3.dlqS3RecordsSuccess.count` >= soma `opensearch.documentSuccess.count` por 1 minuto, 1 vez consecutiva	Um número maior de registros está sendo enviado para o DLQ do que para o coletor do OpenSearch. Analise as métricas do plug-in de coletor do OpenSearch para investigar e determinar a causa raiz.
`grok.grokProcessingTimeouts.count` é = soma de recordsIn.count por 1 minuto, 5 vezes consecutivas	Todos os dados atingem o tempo limite enquanto o processador Grok está tentando combinar padrões. Isso provavelmente está afetando o desempenho e diminuindo a velocidade do seu pipeline. Considere ajustar seus padrões para reduzir os tempos limite.

Alarme	Problema
Soma de `grok.grokProcessingErrors.count` é >= 1 por 1 minuto, 1 vez consecutiva	O processador Grok não está conseguindo combinar os padrões com os dados no pipeline, resultando em erros. Revise seus dados e as configurações do plug-in do Grok para garantir que a correspondência de padrões seja a esperada.
`grok.grokProcessingMismatch.count` é = soma de recordsIn.count por 1 minuto, 5 vezes consecutivas	O processador Grok não consegue combinar padrões com os dados no pipeline. Revise seus dados e as configurações do plug-in do Grok para garantir que a correspondência de padrões seja a esperada.
Soma de `date.dateProcessingMatchFailure.count` = soma de recordsIn.count por 1 minuto, 5 vezes consecutivas	O processador de data não consegue combinar nenhum padrão com os dados no pipeline. Revise seus dados e as configurações do plug-in de data para garantir que o padrão seja o esperado.
`s3.s3ObjectsFailed.count` soma >= 1 por 1 minuto, 1 vez consecutiva	Esse problema está ocorrendo porque o objeto S3 não existe ou porque o pipeline não tem privilégios suficientes. Analise as métricas de `s3ObjectsNotFound.count` e `s3ObjectsAccessDenied.count` para determinar a causa raiz. Confirme se o objeto S3 existe e/ou atualize as permissões.
`s3.sqsMessagesFailed.count` soma >= 1 por 1 minuto, 1 vez consecutiva	O plug-in do S3 falhou ao processar uma mensagem do Amazon SQS. Se você tiver um DLQ habilitado em sua fila do SQS, revise a mensagem de falha. A fila pode estar recebendo dados inválidos que o pipeline está tentando processar.

Alarme	Problema
Soma de `http.badRequests.count` >= 1 por 1 minuto, 1 vez consecutiva	O cliente está enviando uma solicitação incorreta. Confirme se todos os clientes estão enviando a carga útil adequada.
`http.requestsTooLarge.count` soma >= 1 por 1 minuto, 1 vez consecutiva	As solicitações do plug-in HTTP de origem contêm muitos dados, excedendo a capacidade do buffer. Ajuste o tamanho do lote para seus clientes.
Soma de `http.internalServerError.count` >=0 por 1 minuto, 1 vez consecutiva	O plug-in HTTP de origem está tendo problemas para receber eventos.
Soma de `http.requestTimeouts.count` >=0 por 1 minuto, 1 vez consecutiva	Os tempos limite de origem provavelmente são o resultado do subprovisionamento do pipeline. Considere aumentar o pipeline `maxUnits` para lidar com o workload (carga de trabalho) adicional.
`otel_trace.badRequests.count` soma >= 1 por 1 minuto, 1 vez consecutiva	O cliente está enviando uma solicitação incorreta. Confirme se todos os clientes estão enviando a carga útil adequada.
`otel_trace.requestsTooLarge.count` soma >= 1 por 1 minuto, 1 vez consecutiva	As solicitações do plug-in de origem do OTel Trace contêm muitos dados, excedendo a capacidade do buffer. Ajuste o tamanho do lote para seus clientes.

Alarme	Problema
Soma de `otel_trace.internalServerError.count` >=0 por 1 minuto, 1 vez consecutiva	O plug-in de origem do OTel Trace está tendo problemas para receber eventos.
Soma de `otel_trace.requestTimeouts.count` >=0 por 1 minuto, 1 vez consecutiva	Os tempos limite de origem provavelmente são o resultado do subprovisionamento do pipeline. Considere aumentar o pipeline `maxUnits` para lidar com o workload (carga de trabalho) adicional.
Soma de `otel_metrics.requestTimeouts.count` >=0 por 1 minuto, 1 vez consecutiva	Os tempos limite de origem provavelmente são o resultado do subprovisionamento do pipeline. Considere aumentar o pipeline `maxUnits` para lidar com o workload (carga de trabalho) adicional.

Amazon sem OpenSearch servidor

O Amazon OpenSearch Serverless é uma configuração sob demanda e de auto-escalabilidade para o Amazon Service. OpenSearch Uma coleção OpenSearch sem servidor é um OpenSearch cluster que dimensiona a capacidade computacional com base nas necessidades do seu aplicativo. Isso contrasta com os OpenSearch domínios provisionados por OpenSearch serviços, para os quais você gerencia manualmente a capacidade.

OpenSearch O Serverless fornece uma opção simples e econômica para cargas de trabalho pouco frequentes, intermitentes ou imprevisíveis. Ele é econômico porque escala automaticamente a capacidade computacional para corresponder ao uso da sua aplicação.

OpenSearch As coleções sem servidor têm o mesmo tipo de volume de armazenamento de alta capacidade, distribuído e altamente disponível que é usado pelos domínios de serviços OpenSearch provisionados.

OpenSearch As coleções sem servidor são sempre criptografadas. É possível escolher a chave de criptografia, mas não é possível desabilitar a criptografia. Para ter mais informações, consulte the section called “Criptografia”.

Tópicos

Benefícios

OpenSearch O Serverless tem os seguintes benefícios:

- Mais simples do que provisionado — o OpenSearch Serverless remove grande parte da complexidade do gerenciamento de clusters e da capacidade. OpenSearch Ele dimensiona e ajusta automaticamente seus clusters e cuida do gerenciamento do ciclo de vida de fragmentos e índices. Ele também gerencia atualizações de software de serviço e upgrades de OpenSearch versão. Todas as atualizações e upgrades não causam interrupções.
- Econômico — Ao usar o OpenSearch Serverless, você paga apenas pelos recursos que consome. Isso elimina a necessidade de provisionamento inicial e superprovisionamento para workloads de pico.
- Altamente disponível — o OpenSearch Serverless suporta cargas de trabalho de produção com redundância para proteger contra interrupções na Zona de Disponibilidade e falhas na infraestrutura.
- Escalável — O OpenSearch Serverless dimensiona automaticamente os recursos para manter taxas de ingestão de dados e tempos de resposta de consultas consistentemente rápidos.

O que é Amazon OpenSearch Serverless?

O Amazon OpenSearch Serverless é uma configuração sem servidor sob demanda para o Amazon Service. OpenSearch O Serverless remove as complexidades operacionais de provisionamento, configuração e ajuste de seus clusters. OpenSearch É uma boa opção para organizações que não querem autogerenciar seus OpenSearch clusters ou organizações que não têm os recursos ou a experiência dedicados para operar grandes clusters. Com o OpenSearch Serverless, você pode pesquisar e analisar facilmente um grande volume de dados sem precisar se preocupar com a infraestrutura subjacente e o gerenciamento de dados.

Uma coleção OpenSearch sem servidor é um grupo de OpenSearch índices que trabalham juntos para dar suporte a uma carga de trabalho ou caso de uso específico. As coleções são mais fáceis de usar do que os OpenSearch clusters autogerenciados, que exigem provisionamento manual.

As coleções têm o mesmo tipo de volume de armazenamento de alta capacidade, distribuído e altamente disponível usado pelos domínios de OpenSearch serviços provisionados, mas eliminam mais complexidade porque não exigem configuração e ajuste manuais. Os dados são criptografados em trânsito em uma coleção. OpenSearch O Serverless também oferece suporte a OpenSearch painéis, que fornecem uma interface intuitiva para análise de dados.

Atualmente, as coleções sem servidor executam a OpenSearch versão 2.0.x. À medida que novas versões são lançadas, o OpenSearch Serverless atualizará automaticamente suas coleções para consumir novos recursos, correções de bugs e melhorias de desempenho.

Tópicos

Casos de uso do OpenSearch Serverless

OpenSearch O Serverless oferece suporte a dois casos de uso principais:

- Análise de logs: o segmento de análise de logs se concentra na análise de grandes volumes de dados de séries temporais, semiestruturados e gerados por máquina para obter informações operacionais e de comportamento do usuário.
- Pesquisa de texto completo: o segmento de pesquisa de texto completo alimenta aplicações em suas redes internas (sistemas de gerenciamento de conteúdo, documentos legais) e aplicações voltadas para a Internet, como a pesquisa de conteúdo de sites de comércio eletrônico.

Ao criar uma coleção, escolha um desses casos de uso. Para ter mais informações, consulte the section called “Escolha de um tipo de coleção”.

Conceitos básicos

Para começar a usar o OpenSearch Serverless, crie uma ou mais coleções usando o console OpenSearch de serviço AWS CLI, o ou um dos AWS SDKs. Para assistir a um tutorial que pode ser útil para ajudar a colocar uma coleção em funcionamento rapidamente, consulte the section called “Introdução ao OpenSearch Serverless”.

OpenSearch O Serverless suporta as mesmas operações de API de ingestão e consulta do pacote de código OpenSearch aberto, para que você possa continuar usando seus clientes e aplicativos existentes. Seus clientes devem ser compatíveis com OpenSearch 2.x para trabalhar com o

OpenSearch Serverless. Para ter mais informações, consulte the section called “Ingestão de dados em coleções”.

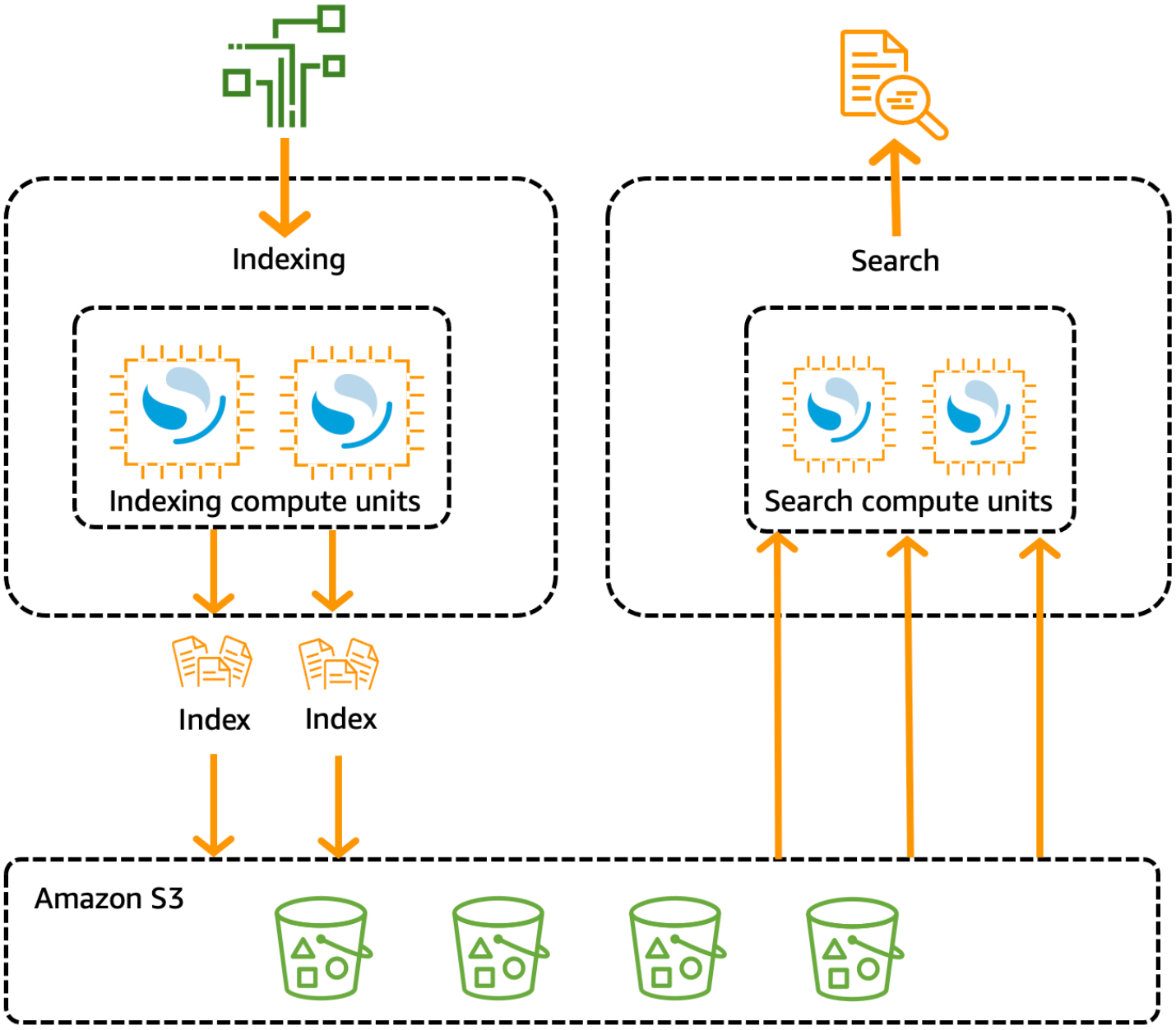
Como funciona

OpenSearch Os clusters tradicionais têm um único conjunto de instâncias que realizam operações de indexação e pesquisa, e o armazenamento de índices está estreitamente associado à capacidade computacional. Por outro lado, o OpenSearch Serverless usa uma arquitetura nativa da nuvem que separa os componentes de indexação (ingestão) dos componentes de pesquisa (consulta), com o Amazon S3 como principal armazenamento de dados para índices.

Essa arquitetura desacoplada permite escalar as funções de pesquisa e indexação de forma independente uma da outra e independentemente dos dados indexados no S3. A arquitetura também fornece isolamento para operações de ingestão e consulta para que elas possam ser executadas simultaneamente, sem contenção de recursos.

Quando você grava dados em uma coleção, o OpenSearch Serverless os distribui para as unidades computacionais de indexação. As unidades computacionais de indexação ingerem os dados recebidos e movem os índices para S3. Quando você realiza uma pesquisa nos dados da coleta, o OpenSearch Serverless encaminha as solicitações para as unidades computacionais de pesquisa que contêm os dados que estão sendo consultados. As unidades computacionais de pesquisa baixam os dados indexados diretamente do S3 (se ainda não estiverem armazenados em cache localmente), executam operações de pesquisa e realizam agregações.

A imagem a seguir ilustra essa arquitetura desacoplada:



OpenSearch A capacidade computacional sem servidor para ingestão, pesquisa e consulta de dados é medida em unidades de OpenSearch computação (OCUs). Cada OCU é uma combinação de 6 GiB de memória e CPU virtual (vCPU) correspondente e cria um pipeline de dados para o Amazon S3. Cada OCU inclui armazenamento efêmero de atividade muito alta que é suficiente para 120 GiB de dados de indexação.

Quando você cria sua primeira coleção, o OpenSearch Serverless instancia dois OCUs: um para indexação e outro para pesquisa. Para garantir alta disponibilidade, ele também lança um conjunto de nós em espera em outra zona de disponibilidade. Para fins de desenvolvimento e teste, você pode desativar a configuração Ativar redundância para uma coleção, que elimina as duas réplicas

em espera e instancia apenas duas OCUs. Réplicas ativas redundantes estão habilitadas por padrão, o que significa que um total de quatro OCUs são instanciadas para a primeira coleção em uma conta.

Essas OCUs existem mesmo quando não há atividade em nenhum dos endpoints da coleção. Todas as coleções subsequentes compartilham essas OCUs. Quando você cria coleções adicionais na mesma conta, o OpenSearch Serverless adiciona apenas OCUs adicionais para pesquisa e ingestão, conforme necessário, para dar suporte às coleções, de acordo com os limites de capacidade que você especificar. A capacidade é reduzida novamente à medida que o uso da computação diminui.

Para obter informações sobre como você é cobrado por essas OCUs, consulte the section called "Preços do OpenSearch Serverless".

Escolha de um tipo de coleção

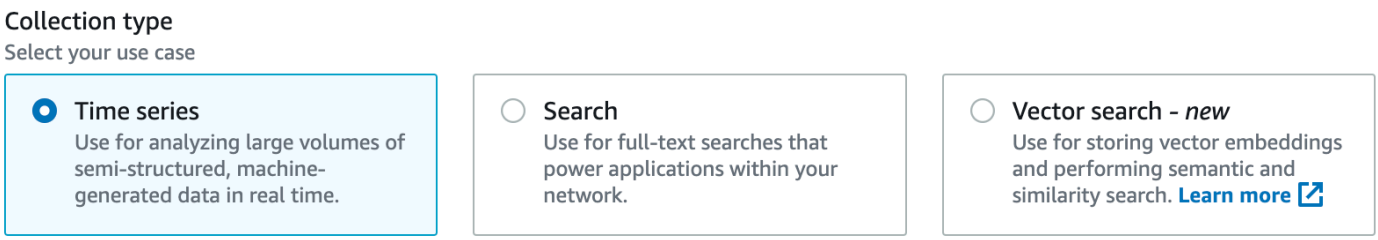
OpenSearch O Serverless oferece suporte a três tipos principais de coleção:

Séries temporais: o segmento de análise de logs se concentra na análise de grandes volumes de dados de séries temporais, semiestruturados e gerados por máquina em tempo real, para obter percepções operacionais, de segurança, de comportamento do usuário e comerciais.

Pesquisa: pesquisa de texto completo que capacita as aplicações em suas redes internas (sistemas de gerenciamento de conteúdo, documentos legais) e aplicações voltadas para a Internet, como a pesquisa de sites de comércio eletrônico e de conteúdo.

Pesquisa vetorial: pesquisa semântica em incorporações vetoriais que simplifica o gerenciamento de dados vetoriais e potencializa experiências de pesquisa aumentada de machine learning (ML) e aplicativos de IA generativa, como chatbots, assistentes pessoais e detecção de fraudes.

Você escolhe um tipo de coleção ao criar uma coleção pela primeira vez:



O tipo de coleção que você escolhe depende do tipo dos dados que planeja ingerir na coleção e de como você planeja consultá-los. Não é possível alterar o tipo da coleção depois de criá-la.

Os tipos de coleção têm as seguintes diferenças notáveis:

- Para coleções de pesquisa e pesquisa vetorial, todos os dados são armazenados no armazenamento a quente para garantir tempos de resposta rápidos às consultas. As coleções de séries temporais usam uma combinação de armazenamento de atividade alta e muito alta, em que os dados mais recentes são mantidos em armazenamento de atividade muito alta para otimizar os tempos de resposta da consulta para dados acessados com mais frequência.
- Para coleções de séries temporais e pesquisa vetorial, não é possível indexar por ID de documento personalizado nem atualizar por solicitações de upsert. Essa operação é reservada para casos de uso de pesquisa. Em vez disso, você pode atualizar por ID do documento. Para ter mais informações, consulte the section called “Operações e permissões de OpenSearch API suportadas”.
- Para pesquisas e coleções de séries temporais, você não pode usar índices do tipo k-NN.

Preços do OpenSearch Serverless

No OpenSearch Serverless, você é cobrado pelos seguintes componentes:

- Computação de ingestão de dados
- Computação de pesquisa e consulta
- Armazenamento retido no Amazon S3

As OCUs são cobradas por hora, com granularidade por segundo. No extrato da sua conta, você verá uma entrada para computação em horas de trabalho com um rótulo para ingestão de dados e um rótulo para pesquisa. Você também é cobrado mensalmente por dados armazenados no Amazon S3. Você não é cobrado pelo uso de OpenSearch painéis.

É cobrado um mínimo de quatro OCUs que são alocadas para suas workloads quando você cria uma coleção e habilita réplicas ativas redundantes. Será cobrado um mínimo de duas OCUs para a primeira coleção da sua conta se você desabilitar réplicas ativas redundantes. Todas as coleções subsequentes podem compartilhar essas OCUs.

OpenSearch O Serverless adiciona OCUs adicionais com base na computação necessária para dar suporte às suas coleções. Se sua workload usar uma OCU fracionária, o preço será proporcional. É possível configurar um número máximo de OCUs para sua conta para controlar os custos.

> **Note**
>
> Coleções com itens exclusivos não AWS KMS keys podem compartilhar OCUs com outras coleções.

OpenSearch O servidor tenta usar os recursos mínimos necessários para contabilizar as mudanças nas cargas de trabalho. O número de OCUs provisionadas a qualquer momento pode variar e não é exato. Com o tempo, o algoritmo usado pelo OpenSearch Serverless continuará melhorando para minimizar melhor o uso do sistema.

Para obter detalhes completos sobre preços, consulte os preços OpenSearch do Amazon Service.

Suportado Regiões da AWS

OpenSearch O Serverless está disponível em um subconjunto Regiões da AWS desse OpenSearch Serviço disponível em. Para obter uma lista das regiões suportadas, consulte os endpoints e cotas do Amazon OpenSearch Service no. Referência geral da AWS

Limitações

OpenSearch O Serverless tem as seguintes limitações:

- Algumas operações de OpenSearch API não são suportadas. Consulte the section called “Operações e permissões de OpenSearch API suportadas”.
- Alguns OpenSearch plug-ins não são compatíveis. Consulte the section called “ OpenSearch Plugins compatíveis”.
- Atualmente, não há como migrar automaticamente seus dados de um domínio de OpenSearch serviço gerenciado para uma coleção sem servidor. É necessário reindexar seus dados de um domínio para uma coleção.
- Não há suporte para acesso entre contas a coleções. Não é possível incluir coleções de outras contas em suas políticas de criptografia ou acesso a dados.
- Não há suporte para OpenSearch plug-ins personalizados.
- Você não pode tirar nem restaurar instantâneos de coleções sem OpenSearch servidor.
- Não há suporte para pesquisa e replicação entre regiões.
- Há limites no número de recursos de tecnologia sem servidor possíveis em uma única conta e região. Consulte Cotas OpenSearch sem servidor.

- O intervalo de atualização dos índices na pesquisa vetorial e nas coleções de séries temporais é de aproximadamente 60 segundos. O intervalo de atualização dos índices nas coletas de procura é de aproximadamente 10 segundos.
- O número de fragmentos, o número de intervalos e o intervalo de atualização não são modificáveis e são gerenciados pelo Serverless. OpenSearch A estratégia de fragmentação é baseada no tipo de coleta e no tráfego. Por exemplo, uma coleção de séries temporais dimensiona os fragmentos primários com base nos gargalos do tráfego de gravação.
- Os recursos geoespaciais disponíveis nas OpenSearch versões até 2.1 são suportados.

Comparando OpenSearch serviços e sem OpenSearch servidor

No OpenSearch Serverless, alguns conceitos e recursos são diferentes dos recursos correspondentes para um domínio de serviço provisionado OpenSearch . Por exemplo, uma diferença importante é que o OpenSearch Serverless não tem o conceito de cluster ou nó.

A tabela a seguir descreve como os recursos e conceitos importantes do OpenSearch Serverless diferem do recurso equivalente em um domínio de serviço provisionado OpenSearch .

Atributo	OpenSearch Serviço	OpenSearch Sem servidor
Domínios versus coleções	Os índices são mantidos em domínios, que são clusters OpenSearch pré-provi sionados. Para ter mais informações, consulte Criação e gerenciam ento de domínios.	Os índices são mantidos em coleções, que são agrupamentos lógicos de índices que representam uma workload ou um caso de uso específico. Para ter mais informações, consulte the section called “Criação, listagem e exclusão de coleções”.
Tipos de nós e gerenciam ento de capacidade	Você cria um cluster com tipos de nós que atendem às suas especificações de custo e performance. É necessári o calcular seus próprios requisitos de armazenamento e escolher um tipo de instância para seu domínio.	OpenSearch O Serverless dimensiona e provisiona automaticamente unidades de computação adicionais para sua conta com base no uso da capacidade. Para ter mais informações, consulte the section called “Gerenciamento de limites de capacidade”.

Atributo	OpenSearch Serviço	OpenSearch Sem servidor
	Para ter mais informaçõ es, consulte the section called “Dimensionamento de domínios”.	
Faturamento	Você paga por hora de uso de uma instância do EC2 e pelo tamanho cumulativo de todos os volumes de armazenam ento do EBS anexados às suas instâncias. Para ter mais informaçõ es, consulte the section called “Preços do Amazon OpenSearch Service”.	Você é cobrado em horas de OCU pela computação para ingestão de dados, computação para pesquisa e consulta e armazenamento retido no S3. Para ter mais informações, consulte the section called “Preços do OpenSearch Serverless”.
Criptografia	A criptografia em repouso é opcional para domínios. Para ter mais informações, consulte the section called “Criptografia inativa”.	A criptografia em repouso é obrigatória para coleções. Para ter mais informações, consulte the section called “Criptografia”.
Controle de acesso a dados	O acesso aos dados nos domínios é determinado pelas políticas do IAM e pelo controle de acesso minucioso.	O acesso aos dados nas coleções é determina do pelas políticas de acesso a dados.
OpenSearc hOperações suportadas	OpenSearch O serviço oferece suporte a um subconjunto de todas as operações da OpenSearch API. Para ter mais informações, consulte the section called “Operações compatíveis”.	OpenSearch O Serverless oferece suporte a um subconjunto diferente de operações de OpenSearch API. Para ter mais informações, consulte the section called “Operações e plug-ins com suporte”.

Atributo	OpenSearch Serviço	OpenSearch Sem servidor
Login no Dashboards	Faça login com um nome de usuário e senha. Para ter mais informações, consulte the section called “Acessando OpenSearch painéis como usuário principal”.	Se você estiver conectado ao AWS console e navegar até a URL do seu painel, você fará login automaticamente. Para ter mais informações, consulte the section called “Acessando OpenSearch painéis”.
APIs	Interaja programaticamente com o OpenSearch Serviço usando as operações da API do OpenSearch Serviço.	Interaja programaticamente com o OpenSearch Serverless usando as operações da API Serverless. OpenSearch
Acesso à rede	As configurações de rede de um domínio se aplicam ao endpoint do domínio, bem como ao endpoint do OpenSearch Dashboards. O acesso à rede para ambos está fortemente acoplado.	As configurações de rede do endpoint do domínio e do endpoint do OpenSearch Dashboards são dissociadas. Você pode optar por não configurar o acesso à rede para OpenSearch painéis. Para ter mais informações, consulte the section called “Acesso à rede”.
Assinatura de solicitações	Use os clientes REST de OpenSearch alto e baixo nível para assinar solicitações. Especifique o nome do serviço como `es`.	No momento, o OpenSearch Serverless oferece suporte a um subconjunto de clientes aos quais o Service oferece suporte. OpenSearch Ao assinar solicitações, especifique o nome do serviço como `aoss`. O cabeçalho `x-amz-content-sha256` é obrigatório. Para ter mais informações, consulte the section called “Assinar solicitações HTTP com outros clientes”.

Atributo	OpenSearch Serviço	OpenSearch Sem servidor
OpenSearch atualizações de versão	Você atualiza manualmente seus domínios à medida que novas versões do são OpenSearch disponibilizadas. Você é responsável por garantir que seu domínio atenda aos requisitos de atualização e que tenha resolvido quaisquer alterações importantes.	OpenSearch O Serverless atualiza automaticamente suas coleções para novas versões. OpenSearch As atualizações não acontecem necessariamente assim que uma nova versão é disponibilizada.
Atualizações de software de serviço	Você aplica manualmente as atualizações do software de serviço ao seu domínio assim que elas se tornam disponíveis.	OpenSearch O Serverless atualiza automaticamente suas coleções para consumir as últimas correções de bugs, recursos e melhorias de desempenho.
Acesso por VPC	É possível provisionar seu domínio em uma VPC. Você também pode criar endpoints OpenSearch VPC gerenciados por serviços adicionais para acessar o domínio.	Você cria um ou mais VPC endpoints OpenSearch gerenciados sem servidor para sua conta. Em seguida, você inclui esses endpoints nas políticas de rede.
Autenticação SAML	Você habilita a autenticação SAML por domínio. Para ter mais informações, consulte the section called “Autenticação SAML para painéis OpenSearch ”.	Você configura um ou mais provedores de SAML no nível da conta e, em seguida, inclui os IDs de usuário e grupo associados nas políticas de acesso a dados. Para ter mais informações, consulte the section called “Autenticação SAML”.

Atributo	OpenSearch Serviço	OpenSearch Sem servidor
Camada de segurança de transporte (TSL)	OpenSearch O serviço oferece suporte ao TLS 1.2, mas é recomendável usar o TLS 1.3.	OpenSearch O Serverless oferece suporte ao TLS 1.2, mas é recomendável usar o TLS 1.3.

Comece a usar o Amazon OpenSearch Serverless

Este tutorial mostra as etapas básicas para colocar uma coleção de pesquisa Amazon OpenSearch Serverless em funcionamento rapidamente. Uma coleção de pesquisas permite que você alimente aplicativos em suas redes internas e aplicativos voltados para a Internet, como a pesquisa de sites de comércio eletrônico e de conteúdo.

Para saber como usar uma coleção de pesquisa vetorial, consulte the section called “Trabalho com coleções de pesquisa vetorial”. Para obter informações detalhadas sobre o uso das coleções, consulte the section called “Criação, listagem e exclusão de coleções” e outros tópicos nesta aba.

Você concluirá as seguintes etapas neste tutorial:

1. Configurar permissões
2. Criar uma coleção
3. Transferir e pesquisar dados
4. Excluir a coleção

Etapa 1: configurar permissões

Para concluir este tutorial e usar o OpenSearch Serverless em geral, você deve ter as permissões corretas do IAM. Neste tutorial, você criará uma coleção, transferirá e pesquisará dados e, em seguida, excluirá a coleção.

Seu usuário ou função deve ter uma política baseada em identidade anexada com as seguintes permissões mínimas:

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Action": [
        "aoss:CreateCollection",
        "aoss:ListCollections",
        "aoss:BatchGetCollection",
        "aoss:DeleteCollection",
        "aoss:CreateAccessPolicy",
        "aoss:ListAccessPolicies",
        "aoss:UpdateAccessPolicy",
        "aoss:CreateSecurityPolicy",
        "aoss:GetSecurityPolicy",
        "aoss:UpdateSecurityPolicy",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Para obter mais informações sobre as permissões do IAM OpenSearch sem servidor, consulte. the section called “Identity and Access Management”

Etapa 2: criar uma coleção

Uma coleção é um grupo de OpenSearch índices que trabalham juntos para dar suporte a uma carga de trabalho ou caso de uso específico.

Para criar uma coleção OpenSearch sem servidor

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. Escolha Coleções no painel de navegação à esquerda e escolha Criar coleção.
3. Dê à coleção o nome de movies (filmes).
4. Para o tipo de coleção, escolha Pesquisar. Para obter mais informações, consulte Choosing a network type (Escolher um tipo de rede).
5. Em Segurança, escolha Criação padrão.
6. Em Criptografia, selecione Usar Chave pertencente à AWS. Isso é o AWS KMS key que o OpenSearch Serverless usará para criptografar seus dados.

7. Em Rede, configure o acesso à rede para a coleção.

   - Para o tipo de acesso, selecione Público.
   - Para o tipo de recurso, escolha Habilitar acesso a OpenSearch endpoints e Habilitar acesso a OpenSearch painéis. Como você fará o upload e pesquisará dados usando OpenSearch painéis, precisará habilitar ambos.
8. Escolha Próximo.
9. Em Configurar acesso aos dados, defina as configurações de acesso para a coleção. As políticas de acesso a dados permitem que usuários e funções acessem os dados em uma coleção. Neste tutorial, forneceremos a um único usuário as permissões necessárias para indexar e pesquisar dados na coleção movies (filmes).

   Crie uma única regra que forneça acesso à coleção de filmes. Nomeie a regra de Acesso à coleção de filmes.
10. Escolha Adicionar diretores, usuários e funções do IAM e selecione o usuário ou a função que você usará para fazer login nos OpenSearch painéis e indexar dados. Escolha Salvar.
11. Em Permissões de índices, selecione todas as permissões.
12. Escolha Próximo.
13. Para as configurações da política de acesso, escolha Criar uma nova política de acesso a dados e nomeie os filmes da política.
14. Escolha Próximo.
15. Reveja suas configurações da coleção e escolha Enviar. Aguarde alguns minutos até que o status da coleção mude para `Active`.

Etapa 3: Transferir e pesquisar dados

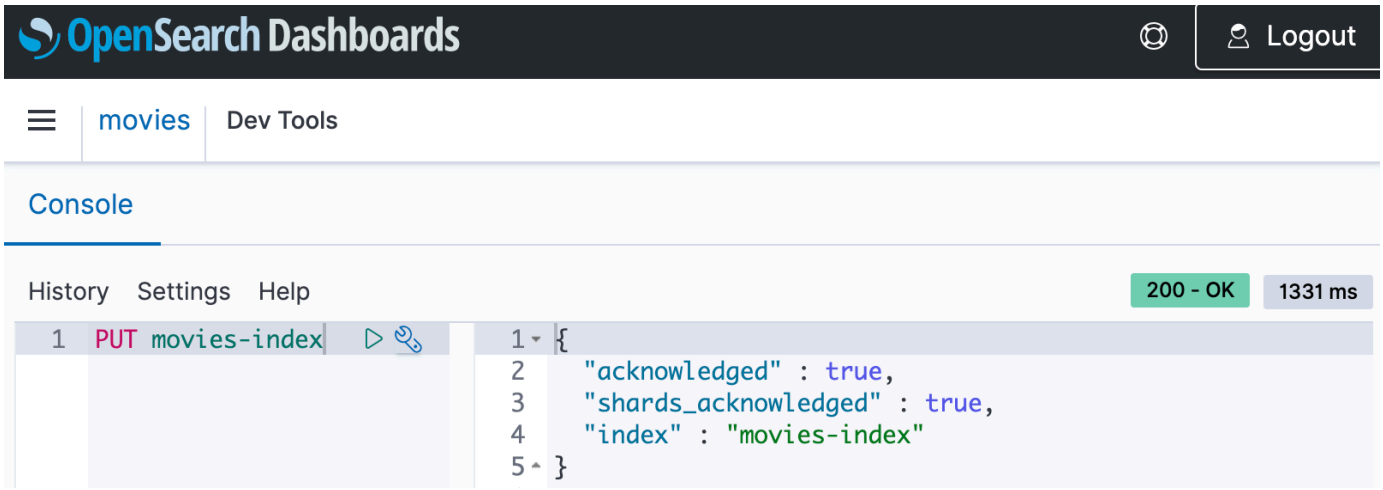
Você pode carregar dados para uma coleção OpenSearch sem servidor usando Postman ou cURL. Para resumir, esses exemplos usam Dev Tools no console OpenSearch Dashboards.

Para indexar e pesquisar dados na coleção de filmes

1. Escolha Coleções no painel de navegação à esquerda e escolha a coleção movies (filmes) para abrir sua página de detalhes.
2. Escolha o URL dos OpenSearch painéis para a coleção. O URL assume o formato `https://dashboards.{region}.aoss.amazonaws.com/_login/?collectionId={collection-id}`.

3. Em OpenSearch Painéis, abra o painel de navegação esquerdo e escolha Ferramentas de desenvolvimento.
4. Para criar um único índice chamado movies-index, envie a seguinte solicitação:

```
PUT movies-index
```



5. Para indexar um único documento em movies-index, envie a seguinte solicitação:

```
PUT movies-index/_doc/1
{
  "title": "Shawshank Redemption",
  "genre": "Drama",
  "year": 1994
}
```

6. Para pesquisar dados em OpenSearch painéis, você precisa configurar pelo menos um padrão de índice. OpenSearch usa esses padrões para identificar quais índices você deseja analisar. Abra o painel de navegação à esquerda, escolha Gerenciamento de pilhas, Padrões de índice e, em seguida, escolha Criar padrão de índice. Para este tutorial, insira movies.
7. Escolha Próxima etapa e, em seguida, Criar padrão de índice. Depois que o padrão é criado, você pode visualizar os vários campos do documento, como `title` e `genre`.
8. Para começar a pesquisar seus dados, abra novamente o painel de navegação à esquerda e escolha Descobrir, ou use a API de pesquisa nas Ferramentas de desenvolvimento.

Etapa 4: Excluir a coleção

Como a coleção movies (filmes) é usada apenas para fins de teste, você deverá excluí-la quando terminar os testes.

Para excluir uma coleção OpenSearch sem servidor

1. Volte para o console do Amazon OpenSearch Service.
2. Escolha Coleções no painel de navegação à esquerda e selecione a coleção movies (filmes).
3. Escolha Excluir e confirme a exclusão.

Próximas etapas

Agora que você sabe como criar uma coleção e indexar dados, talvez você queira tentar alguns dos seguintes exercícios:

- Veja opções mais avançadas para a criação de uma coleção. Para ter mais informações, consulte the section called “Criação, listagem e exclusão de coleções”.
- Saiba como configurar políticas de segurança para gerenciar a segurança da coleção em escala. Para ter mais informações, consulte the section called “Segurança sem OpenSearch servidor”.
- Descubra outras formas de indexar dados em coleções. Para ter mais informações, consulte the section called “Ingestão de dados em coleções”.

Criação e gerenciamento de coleções do Amazon OpenSearch Sem Servidor

É possível criar coleções do Amazon OpenSearch Sem Servidor usando o console, a AWS CLI e a API, os SDKs da AWS e o AWS CloudFormation.

Tópicos

- Criação, listagem e exclusão de coleções Amazon OpenSearch Serverless
- Trabalho com coleções de pesquisa vetorial
- Como usar as políticas de ciclo de vida dos dados com o Amazon OpenSearch Sem Servidor
- Uso de SDKs da AWS para interagir com o Amazon OpenSearch Sem Servidor
- Uso de AWS CloudFormation para a criação de coleções do Amazon OpenSearch Sem Servidor

Criação, listagem e exclusão de coleções Amazon OpenSearch Serverless

Uma coleção no Amazon OpenSearch Serverless é um agrupamento lógico de um ou mais índices que representam uma carga de trabalho de análise. OpenSearch O serviço gerencia e ajusta automaticamente a coleção, exigindo o mínimo de entrada manual.

Tópicos

Permissões obrigatórias

OpenSearch O Serverless usa as seguintes permissões AWS Identity and Access Management (IAM) para criar e gerenciar coleções. É possível especificar as condições do IAM para restringir os usuários a coleções específicas.

- `aoss:CreateCollection`: cria uma coleção.
- `aoss:ListCollections`: lista coleções na conta atual.
- `aoss:BatchGetCollection`: obtém detalhes sobre uma ou mais coleções.
- `aoss:UpdateCollection`: modifica uma coleção.
- `aoss:DeleteCollection`: exclui uma coleção.

O exemplo de política de acesso baseada em identidade a seguir fornece as permissões mínimas necessárias para que um usuário gerencie uma única coleção de nome `Logs`:

```
[
   {
      "Sid":"Allows managing logs collections",
      "Effect":"Allow",
      "Action":[
         "aoss:CreateCollection",
         "aoss:ListCollections",
```

```
            "aoss:BatchGetCollection",
            "aoss:UpdateCollection",
            "aoss:DeleteCollection",
            "aoss:CreateAccessPolicy",
            "aoss:CreateSecurityPolicy"
        ],
        "Resource":"*",
        "Condition":{
            "StringEquals":{
                "aoss:collection":"Logs"
            }
        }
    }
]
```

`aoss:CreateAccessPolicy` e `aoss:CreateSecurityPolicy` estão incluídos porque as políticas de criptografia, de rede e de acesso a dados são necessárias para que uma coleção funcione adequadamente. Para ter mais informações, consulte the section called “Identity and Access Management”.

> **Note**
>
> Se você estiver criando a primeira coleção em sua conta, também precisará da permissão `iam:CreateServiceLinkedRole`. Para ter mais informações, consulte the section called “Função de criação de coleção”.

Criação de coleções

Você pode usar o console ou o AWS CLI para criar uma coleção sem servidor. Essas etapas abordam como criar uma pesquisa ou uma coleção de séries temporais. Para criar uma coleção de pesquisa vetorial, consultethe section called “Trabalho com coleções de pesquisa vetorial”.

Criação de uma coleção (console)

Para criar uma coleção usando o console

1. Navegue até o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home/.
2. Expanda Sem Servidor no painel de navegação à esquerda e escolha Coleções.

3. Escolha Criar coleção.
4. Forneça um nome e uma descrição para a coleção. O nome deve atender aos seguintes critérios:

   - É exclusivo para sua conta e Região da AWS
   - Iniciar com letra minúscula.
   - Contém de 3 a 32 caracteres
   - Contém apenas letras minúsculas a-z, números de 0 a 9 e hífens (-).
5. Escolha um tipo de coleção:

   - Pesquisa: pesquisa de texto completo que alimenta aplicações em suas redes internas e aplicações voltadas para a Internet. Todos os dados de pesquisa são armazenados em um armazenamento de atividade muito alta para garantir tempos de resposta rápidos às consultas.
   - Séries temporais: segmento de análise de logs que se concentra na análise de grandes volumes de dados semiestruturados gerados por máquina. Pelo menos 24 horas de dados são armazenadas em índices ativos, e o restante permanece no armazenamento ativo.
   - Pesquisa vetorial: pesquisa semântica em incorporações vetoriais que simplifica o gerenciamento de dados vetoriais. Potencializa experiências de pesquisa aumentada de machine learning (ML) e aplicações de IA generativa, como chatbots, assistentes pessoais e detecção de fraudes.

   Para ter mais informações, consulte the section called “Escolha de um tipo de coleção”.
6. Em Tipo de implantação, escolha a configuração de redundância para sua coleção. Por padrão, cada coleção é criada com redundância, o que significa que as unidades de OpenSearch computação (OCUs) de indexação e pesquisa têm suas próprias réplicas em espera em uma zona de disponibilidade diferente. Para fins de desenvolvimento e teste, você pode optar por desativar a redundância, o que reduz o número de OCUs em sua coleção para duas. Para ter mais informações, consulte the section called “Como funciona”.
7. Em Criptografia, escolha uma AWS KMS chave com a qual criptografar seus dados. OpenSearch O Serverless notifica você se o nome da coleção que você inseriu corresponder a um padrão definido em uma política de criptografia. É possível optar por manter essa correspondência ou substituí-la por configurações de criptografia exclusivas. Para ter mais informações, consulte the section called “Criptografia”.
8. Em Configurações de acesso à rede, configure o acesso à rede para a coleção.

- Em Tipo de acesso, selecione público ou privado. Em seguida, especifique quais endpoints de VPC Serviços da AWS podem acessar a coleção.
  - VPC endpoints para acesso — especifique um ou mais endpoints VPC para permitir o acesso. Para criar um VPC da endpoint, consulte the section called “Endpoints da VPC”.
  - AWS service (Serviço da AWS) acesso privado — Selecione um ou mais serviços compatíveis aos quais permitir o acesso.
- Em Tipo de recurso, selecione se a coleção será acessível por meio de seu OpenSearchendpoint (para fazer chamadas de API por meio de curl, Postman e assim por diante), por meio do endpoint OpenSearch Dashboards (para trabalhar com visualizações e fazer chamadas de API por meio do console) ou por meio de ambos.

> **Note**
>
> AWS service (Serviço da AWS) o acesso privado se aplica somente ao OpenSearch endpoint, não ao endpoint do OpenSearch Dashboards.

OpenSearch O Serverless notifica você se o nome da coleção inserido corresponder a um padrão definido em uma política de rede. É possível optar por manter essa correspondência ou substituí-la por configurações de rede personalizadas. Para ter mais informações, consulte the section called “Acesso à rede”.

9. (Opcional) Adicione uma ou mais tags à coleção. Para ter mais informações, consulte the section called “Aplicação de tags nas coleções”.
10. Escolha Próximo.
11. Configure regras de acesso aos dados para a coleção, que definem quem pode acessar os dados dentro da coleção. Para cada regra que você criar, execute as seguintes etapas:
    - Escolha Adicionar entidades principais e selecione um ou mais perfis do IAM, ou usuários e grupos de SAML aos quais fornecer acesso aos dados.
    - Em Conceder permissões, selecione o alias, o modelo e as permissões de índice para conceder aos principais associados. Para obter uma lista completa de permissões e o acesso que elas permitem, consulte the section called “Operações e permissões de OpenSearch API suportadas”.

OpenSearch O Serverless notifica você se o nome da coleção inserido corresponder a um padrão definido em uma política de acesso a dados. É possível optar por manter essa correspondência ou substituí-la por configurações de acesso a dados exclusivas. Para ter mais informações, consulte the section called “Controle de acesso a dados”.

12. Escolha Próximo.
13. Em Configurações da política de acesso a dados, escolha o que fazer com as regras que você acabou de criar. É possível usá-las para criar uma nova política de acesso a dados ou adicioná-los a uma política existente.
14. Reveja sua configuração da coleção e escolha Enviar.

O status da coleção muda para `Creating` quando o OpenSearch Serverless cria a coleção.

Criação de uma coleção (CLI)

Antes de criar uma coleção usando o AWS CLI, você deve ter uma política de criptografia com um padrão de recurso que corresponda ao nome pretendido da coleção. Por exemplo, se você planeja nomear sua coleção como logs-application, é possível criar uma política de criptografia como esta:

```
aws opensearchserverless create-security-policy \
  --name logs-policy \
  --type encryption --policy "{\"Rules\":[{\"ResourceType\":\"collection\",\"Resource
\":[\"collection\/logs-application\"]}],\"AWSOwnedKey\":true}"
```

Se você planeja usar a política para cobranças adicionais, é possível tornar a regra mais ampla, como `collection/logs*` ou `collection/*`.

Você também precisa definir as configurações de rede para a coleção na forma de uma política de rede. Usando o exemplo anterior de logs-application, é possível criar a seguinte política de rede:

```
aws opensearchserverless create-security-policy \
  --name logs-policy \
  --type network --policy "[{\"Description\":\"Public access for logs collection
\",\"Rules\":[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection\/logs-
application\"]},{\"ResourceType\":\"collection\",\"Resource\":[\"collection\/logs-
application\"]}],\"AllowFromPublic\":true}]"
```

> **Note**
>
> É possível criar políticas de rede depois de criar uma coleção, mas recomendamos fazer isso previamente.

Para criar uma coleção, envie uma CreateCollectionsolicitação:

```
aws opensearchserverless create-collection --name "logs-application" --type SEARCH --
description "A collection for storing log data"
```

Para o `type`, especifique `SEARCH` ou `TIMESERIES`. Para ter mais informações, consulte the section called “Escolha de um tipo de coleção”.

Exemplo de resposta

```
{
    "createCollectionDetail": {
        "id": "07tjusf2h91cunochc",
        "name": "books",
        "description":"A collection for storing log data",
        "status": "CREATING",
        "type": "SEARCH",
        "kmsKeyArn": "auto",
        "arn": "arn:aws:aoss:us-east-1:123456789012:collection/07tjusf2h91cunochc",
        "createdDate": 1665952577473
    }
}
```

Se você não especificar um tipo de coleção na solicitação, ela assumirá o padrão `TIMESERIES`. Se sua coleção estiver criptografada com uma Chave pertencente à AWS, o `kmsKeyArn` será `auto` em vez de um ARN.

> **Important**
>
> Depois de criar uma coleção, você não poderá acessá-la, a menos que ela corresponda a uma política de acesso a dados. Para obter instruções sobre como criar políticas de acesso a dados, consulte the section called “Controle de acesso a dados”.

Acessando OpenSearch painéis

Depois de criar uma coleção com o AWS Management Console, você pode navegar até a URL dos OpenSearch painéis da coleção. Você pode encontrar o URL dos Painéis escolhendo Coleções no painel de navegação esquerdo e selecionando a coleção para abrir a página de detalhes. O URL assume o formato `https://dashboards.us-east-1.aoss.amazonaws.com/_login/?collectionId=07tjusf2h91cunochc`. Depois de navegar até o URL, você fará login no Dashboards automaticamente.

Se você já tiver o URL dos OpenSearch painéis disponível, mas não estiver no AWS Management Console, chamar o URL dos painéis pelo navegador será redirecionado para o console. Depois de inserir suas AWS credenciais, você fará login automaticamente nos painéis. Para obter informações sobre como acessar coleções para SAML, consulte Acessando OpenSearch painéis com SAML.

O tempo limite do console do OpenSearch Dashboards é de uma hora e não é configurável.

> **Note**
>
> Em 10 de maio de 2023, OpenSearch introduziu um endpoint global comum para OpenSearch painéis. Agora você pode navegar até OpenSearch Painéis no navegador com uma URL que assume o formato`https://dashboards.us-east-1.aoss.amazonaws.com/_login/?collectionId=07tjusf2h91cunochc`. Para garantir a compatibilidade com versões anteriores, continuaremos oferecendo suporte aos endpoints de OpenSearch painéis específicos da coleção existente com o formato. `https://07tjusf2h91cunochc.us-east-1.aoss.amazonaws.com/_dashboards`

Exibição das coleções

Você pode visualizar as coleções existentes Conta da AWS na sua guia Coleções do console do Amazon OpenSearch Service.

Para listar coleções junto com suas IDs, envie uma ListCollectionssolicitação.

```
aws opensearchserverless list-collections
```

Exemplo de resposta

```
{
```

```
   "collectionSummaries":[
      {
         "arn":"arn:aws:aoss:us-east-1:123456789012:collection/07tjusf2h91cunochc",
         "id":"07tjusf2h91cunochc",
         "name":"my-collection",
         "status":"CREATING"
      }
   ]
}
```

Para limitar os resultados da pesquisa, use filtros de coleções. Esta solicitação filtra a resposta para coleções no estado `ACTIVE`:

```
aws opensearchserverless list-collections --collection-filters '{ "status": "ACTIVE" }'
```

Para obter informações mais detalhadas sobre uma ou mais coleções, incluindo o OpenSearch endpoint e o endpoint do OpenSearch Dashboards, envie uma solicitação: BatchGetCollection

```
aws opensearchserverless batch-get-collection --ids ["07tjusf2h91cunochc",
 "1iu5usc4rame"]
```

> **Note**
>
> É possível incluir `--names` ou `--ids` na solicitação, mas não os dois.

Exemplo de resposta

```
{
   "collectionDetails":[
      {
         "id": "07tjusf2h91cunochc",
         "name": "my-collection",
         "status": "ACTIVE",
         "type": "SEARCH",
         "description": "",
         "arn": "arn:aws:aoss:us-east-1:123456789012:collection/07tjusf2h91cunochc",
         "kmsKeyArn": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab",
         "createdDate": 1667446262828,
         "lastModifiedDate": 1667446300769,
```

```
         "collectionEndpoint": "https://07tjusf2h91cunochc.us-
east-1.aoss.amazonaws.com",
         "dashboardEndpoint": "https://07tjusf2h91cunochc.us-east-1.aoss.amazonaws.com/
_dashboards"
      },
      {
         "id": "178ukvtg3i82dvopdid",
         "name": "another-collection",
         "status": "ACTIVE",
         "type": "TIMESERIES",
         "description": "",
         "arn": "arn:aws:aoss:us-east-1:123456789012:collection/178ukvtg3i82dvopdid",
         "kmsKeyArn": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab",
         "createdDate": 1667446262828,
         "lastModifiedDate": 1667446300769,
         "collectionEndpoint": "https://178ukvtg3i82dvopdid.us-
east-1.aoss.amazonaws.com",
         "dashboardEndpoint": "https://178ukvtg3i82dvopdid.us-
east-1.aoss.amazonaws.com/_dashboards"
      }
   ],
   "collectionErrorDetails":[]
}
```

Exclusão de coleções

A exclusão de uma coleção exclui todos os dados e índices da coleção. Você não poderá recuperar coleções depois de excluí-las.

Para excluir uma coleção usando o console

1. No painel Coleções do console do Amazon OpenSearch Service, selecione a coleção que você deseja excluir.
2. Escolha Excluir e confirme a exclusão.

Para excluir uma coleção usando o AWS CLI, envie uma DeleteCollectionsolicitação:

```
aws opensearchserverless delete-collection --id 07tjusf2h91cunochc
```

Exemplo de resposta

```
{
   "deleteCollectionDetail":{
      "id":"07tjusf2h91cunochc",
      "name":"my-collection",
      "status":"DELETING"
   }
}
```

Trabalho com coleções de pesquisa vetorial

O tipo de coleta de pesquisa vetorial no OpenSearch Serverless fornece um recurso de pesquisa por similaridade que é escalável e de alto desempenho. Isso facilita a criação de experiências modernas de pesquisa aumentada de machine learning (ML) e aplicativos de inteligência artificial generativa (IA) sem precisar gerenciar a infraestrutura subjacente do banco de dados de vetores.

Os casos de uso de coleções de pesquisa vetorial incluem pesquisas de imagens, pesquisas de documentos, recuperação de músicas, recomendações de produtos, pesquisas de vídeo, pesquisas baseadas em localização, detecção de fraudes e detecção de anomalias.

Como o mecanismo vetorial do OpenSearch Serverless é alimentado pelo recurso de pesquisa k-Nearest Neighbor (k-NN) OpenSearch, você obtém a mesma funcionalidade com a simplicidade de um ambiente sem servidor. O mecanismo suporta as operações da OpenSearch API k-NN. Com essas operações, você pode aproveitar pesquisas em texto completo, filtragem avançada, agregações, consultas geoespaciais, consultas aninhadas para uma recuperação mais rápida dos dados e resultados de pesquisa aprimorados.

O mecanismo vetorial fornece métricas de distância, como distância euclidiana, similaridade de cosseno, similaridade de produtos escalares, e também pode acomodar 16.000 dimensões. Você pode armazenar campos com vários tipos de dados para metadados, como números, booleanos, datas, palavras-chave e pontos geográficos. Também é possível armazenar campos com texto para obter informações descritivas e adicionar mais contexto aos vetores armazenados. A colocalização conjunta dos tipos de dados reduz a complexidade, aumenta a capacidade de manutenção e evita a duplicação de dados, desafios de compatibilidade de versões e problemas de licenciamento.

Conceitos básicos de coleções de pesquisa de vetores

Neste tutorial, você conclui as etapas a seguir para armazenar, pesquisar e recuperar incorporações vetoriais em tempo real:

1. Configurar permissões

2. Criar uma coleção
3. Transferir e pesquisar dados
4. Excluir a coleção

Etapa 1: configurar permissões

Para concluir este tutorial (e usar o OpenSearch Serverless em geral), você deve ter as permissões corretas AWS Identity and Access Management (IAM). Neste tutorial, você criará uma coleção, carregará e pesquisará dados e, em seguida, excluirá a coleção.

Seu usuário ou função deve ter uma política baseada em identidade anexada com as seguintes permissões mínimas:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aoss:CreateCollection",
        "aoss:ListCollections",
        "aoss:BatchGetCollection",
        "aoss:DeleteCollection",
        "aoss:CreateAccessPolicy",
        "aoss:ListAccessPolicies",
        "aoss:UpdateAccessPolicy",
        "aoss:CreateSecurityPolicy",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Para obter mais informações sobre as permissões do IAM OpenSearch sem servidor, consulte. the section called “Identity and Access Management”

Etapa 2: criar uma coleção

Uma coleção é um grupo de OpenSearch índices que trabalham juntos para dar suporte a uma carga de trabalho ou caso de uso específico.

Para criar uma coleção OpenSearch sem servidor

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. Escolha Coleções no painel de navegação à esquerda e escolha Criar coleção.
3. Nomeie o armazenamento da coleção.
4. Para o tipo de coleção, escolha Pesquisa vetorial. Para ter mais informações, consulte the section called “Escolha de um tipo de coleção”.
5. Em Tipo de implantação, desmarque Habilitar redundância (réplicas ativas). Isso cria uma coleção no modo de desenvolvimento ou teste e reduz o número de unidades de OpenSearch computação (OCUs) em sua coleção para duas. Se quiser criar um ambiente de produção neste tutorial, deixe a caixa de seleção marcada.
6. Em Segurança, selecione Criação fácil para simplificar sua configuração de segurança. Por padrão, todos os dados no mecanismo vetorial são criptografados em trânsito e em repouso. O mecanismo vetorial oferece suporte a permissões refinadas do IAM para que você possa definir quem pode criar, atualizar e excluir criptografias, redes, coleções e índices.
7. Escolha Próximo.
8. Reveja suas configurações da coleção e escolha Enviar. Aguarde alguns minutos até que o status da coleção mude para `Active`.

Etapa 3: Transferir e pesquisar dados

Um índice é uma coleção de documentos com um esquema de dados comum que fornece uma maneira de armazenar, pesquisar e recuperar suas incorporações vetoriais e outros campos. Você pode criar e carregar dados para índices em uma coleção OpenSearch sem servidor usando o console Dev Tools em OpenSearch painéis ou uma ferramenta HTTP, como Postman ou awscurl. Este tutorial usa Dev Tools.

Para indexar e pesquisar dados na coleção de filmes

1. Para criar um único índice para sua nova coleção, envie a seguinte solicitação no console do Dev Tools. Por padrão, isso cria um índice com um `nmslib` mecanismo e uma distância euclidiana.

```
PUT housing-index
{
   "settings": {
      "index.knn": true
   },
   "mappings": {
      "properties": {
         "housing-vector": {
            "type": "knn_vector",
            "dimension": 3
         },
         "title": {
            "type": "text"
         },
         "price": {
            "type": "long"
         },
         "location": {
            "type": "geo_point"
         }
      }
   }
}
```

2. Para indexar um único documento em housing-index, envie a seguinte solicitação:

```
POST housing-index/_doc
{
  "housing-vector": [
    10,
    20,
    30
  ],
  "title": "2 bedroom in downtown Seattle",
  "price": "2800",
  "location": "47.71, 122.00"
}
```

3. Para pesquisar propriedades semelhantes às do seu índice, envie a seguinte consulta:

```
GET housing-index/_search
{
```

```
    "size": 5,
    "query": {
        "knn": {
            "housing-vector": {
                "vector": [
                    10,
                    20,
                    30
                ],
                "k": 5
            }
        }
    }
}
```

Etapa 4: Excluir a coleção

Como a coleção habitação é usada apenas para fins de teste, você deverá excluí-la quando terminar os testes.

Para excluir uma coleção OpenSearch sem servidor

1. Volte para o console do Amazon OpenSearch Service.
2. Escolha Coleções no painel de navegação à esquerda e selecione a coleção propriedades.
3. Selecione Excluir para confirmar a exclusão.

Pesquisa com filtro

Você pode usar filtros para refinar os resultados da pesquisa semântica. Para criar um índice e realizar uma pesquisa com filtro nos seus documentos, substitua Carregar e pesquisar dados no tutorial anterior pelas instruções a seguir. As outras etapas permanecem as mesmas. Para obter mais informações sobre os filtros, consulte pesquisa k-NN com filtros.

Para indexar e pesquisar dados na coleção de filmes

1. Para criar um único índice para sua coleção, envie a seguinte solicitação no console do Dev Tools:

```
PUT housing-index-filtered
{
```

```
  "settings": {
    "index.knn": true
  },
  "mappings": {
    "properties": {
      "housing-vector": {
        "type": "knn_vector",
        "dimension": 3,
        "method": {
          "engine": "faiss",
          "name": "hnsw"
        }
      },
      "title": {
        "type": "text"
      },
      "price": {
        "type": "long"
      },
      "location": {
        "type": "geo_point"
      }
    }
  }
}
```

2. Para indexar um único documento em housing-index-filtered, envie a seguinte solicitação:

```
POST housing-index-filtered/_doc
{
  "housing-vector": [
    10,
    20,
    30
  ],
  "title": "2 bedroom in downtown Seattle",
  "price": "2800",
  "location": "47.71, 122.00"
}
```

3. Para pesquisar seus dados em busca de um apartamento em Seattle por um preço específico e dentro de uma determinada distância de um ponto geográfico, envie a seguinte solicitação:

```
GET housing-index-filtered/_search
{
  "size": 5,
  "query": {
    "knn": {
      "housing-vector": {
        "vector": [
          0.1,
          0.2,
          0.3
        ],
        "k": 5,
        "filter": {
          "bool": {
            "must": [
              {
                "query_string": {
                  "query": "Find me 2 bedroom apartment in Seattle under $3000 ",
                  "fields": [
                    "title"
                  ]
                }
              },
              {
                "range": {
                  "price": {
                    "lte": 3000
                  }
                }
              },
              {
                "geo_distance": {
                  "distance": "100miles",
                  "location": {
                    "lat": 48,
                    "lon": 121
                  }
                }
              }
            ]
          }
        }
      }
```

```
    }
  }
}
```

Workloads em escala de bilhões

Coleções de pesquisa vetorial oferecem suporte a workloads com bilhões de vetores. Você não precisa reindexar para fins de ajuste de escala, pois o ajuste de escala automático faz isso por você. Se você tiver milhões de vetores (ou mais) com um grande número de dimensões e precisar de mais de 200 OCUs, entre em contato com o AWS Support para aumentar o número máximo de Unidades de OpenSearch Computação (OCUs) para sua conta.

Limitações

As coleções de pesquisa vetorial têm as seguintes limitações:

- As coleções de pesquisa vetorial não são compatíveis com o mecanismo Apache Lucene ANN.
- As coleções de pesquisa vetorial são compatíveis apenas com o algoritmo HNSW com Faiss e não são compatíveis com FIV e IVFQ.
- As coleções de pesquisa vetorial não são compatíveis com as operações de API de aquecimento, estatísticas e treinamento de modelo.
- As coleções de pesquisa vetorial não oferecem suporte a scripts embutidos ou armazenados.
- As informações de contagem de índices não estão disponíveis nas coleções AWS Management Console de pesquisa vetorial.
- O intervalo de atualização dos índices nas coleções de pesquisa vetorial é de 60 segundos.

Próximas etapas

Agora que você sabe como criar uma coleção de pesquisa vetorial e indexar os dados, talvez você queira testar alguns dos seguintes exercícios:

- Use o cliente OpenSearch Python para trabalhar com coleções de pesquisa vetorial. Veja este tutorial em GitHub.
- Use o cliente OpenSearch Java para trabalhar com coleções de pesquisa vetorial. Veja este tutorial em GitHub.

- Configure LangChain para usar OpenSearch como um repositório de vetores. LangChain é uma estrutura de código aberto para o desenvolvimento de aplicativos alimentados por modelos de linguagem. Para obter mais informações, consulte a LangChain documentação.

Como usar as políticas de ciclo de vida dos dados com o Amazon OpenSearch Sem Servidor

Uma política de ciclo de vida dos dados para uma coleção de séries temporais do Amazon OpenSearch Sem Servidor determina a vida útil dos dados nessa coleção. A tecnologia sem servidor do OpenSearch retém os dados pelo período de tempo que você escolhe.

Você pode configurar uma política de ciclo de vida de dados separada para cada índice de cada coleção de séries temporais na sua Conta da AWS A com tecnologia sem servidor do OpenSearch retém documentos em índices durante um período de retenção mínimo configurado na política. Em seguida, ele os exclui automaticamente com base no melhor esforço, normalmente dentro de 48 horas ou 10% do período de retenção, o que for maior.

Somente coleções de séries temporais oferecem suporte às políticas de ciclo de vida dos dados. Elas não são suportadas por coleções de pesquisa ou pesquisa vetorial.

Tópicos

Políticas de ciclo de vida dos dados

Em uma política de ciclo de vida dos dados, você especifica uma série de regras. A política de ciclo de vida de dados permite gerenciar o período de retenção de dados associados a índices ou coleções que correspondam a essas regras. Essas regras definem o período de retenção dos dados

em um índice ou grupo de índices. Cada regra consiste em um tipo de recurso (`index`), um período de retenção e uma lista de recursos (índices) aos quais o período de retenção se aplica.

Você define o período de retenção com um dos seguintes formatos:

- `"MinIndexRetention": "24h"` – a tecnologia sem servidor do OpenSearch retém dados de índice para o período especificado em horas ou dias. Você pode definir esse período para `24h` a `3650d`.
- `"NoMinIndexRetention": true` – a tecnologia sem servidor do OpenSearch retém os dados do índice indefinidamente.

No exemplo de política a seguir, a primeira regra especifica um período de retenção de 15 dias para todos os índices da coleção `marketing`. A segunda regra especifica que todos os nomes de índice que começam com `log` na coleção `finance` não têm período de retenção definido e serão mantidos indefinidamente.

```
{
   "lifeCyclePolicyDetail": {
      "type": "retention",
      "name": "my-policy",
      "policyVersion": "MTY4ODI0NTM2OTk1N18x",
      "policy": {
         "Rules": [
            {
            "ResourceType":"index",
            "Resource":[
               "index/marketing/*"
            ],
            "MinIndexRetention": "15d"
         },
         {
            "ResourceType":"index",
            "Resource":[
               "index/finance/log*"
            ],
            "NoMinIndexRetention": true
         }
         ]
      },
      "createdDate": 1688245369957,
      "lastModifiedDate": 1688245369957
```

```
   }
}
```

No exemplo de regra de política a seguir, a tecnologia sem servidor do OpenSearch retém indefinidamente os dados em todos os índices de todas as coleções da conta.

```
{
   "Rules": [
      {
         "ResourceType": "index",
         "Resource": [
            "index/*/*"
         ]
      }
   ],
   "NoMinIndexRetention": true
}
```

Permissões obrigatórias

As políticas de ciclo de vida da tecnologia sem servidor do OpenSearch usam as permissões do AWS Identity and Access Management (IAM) a seguir. Você pode especificar as condições do IAM para restringir os usuários a políticas de ciclo de vida dos dados associadas a coleções e índices específicos.

- `aoss:CreateLifecyclePolicy` – criar uma política de ciclo de vida dos dados.
- `aoss:ListLifecyclePolicies` – listar todas as políticas de ciclo de vida dos dados na conta atual.
- `aoss:BatchGetLifecyclePolicy`: visualize uma política de ciclo de vida de dados associada a um nome de conta ou política.
- `aoss:BatchGetEffectiveLifecyclePolicy`: visualize uma política de ciclo de vida de dados para um determinado recurso (`index` é o único recurso compatível).
- `aoss:UpdateLifecyclePolicy`: modifique uma determinada política de ciclo de vida de dados e altere sua configuração ou recurso de retenção.
- `aoss:DeleteLifecyclePolicy` – excluir uma política de ciclo de vida dos dados.

A política de acesso baseada em identidade a seguir permite que um usuário exiba todas as políticas de ciclo de vida dos dados e atualize as políticas com o padrão de recursos `collection/application-logs`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aoss:UpdateLifecyclePolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:collection": "application-logs"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "aoss:ListLifecyclePolicies",
                "aoss:BatchGetLifecyclePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Precedência das políticas

Pode haver situações em que as regras das políticas de ciclo de vida se sobreponham, dentro ou entre as políticas. Quando isso acontece, uma regra com um nome de recurso ou padrão mais específico para um índice substitui uma regra com um nome de recurso ou padrão mais geral para qualquer índice que seja comum às duas regras.

Por exemplo, na política a seguir, duas regras se aplicam a um índice `index/sales/logstash`. Nessa situação, a segunda regra tem precedência porque `index/sales/log*` é a correspondência mais longa para `index/sales/logstash`. Portanto, a tecnologia sem servidor do OpenSearch não define um período de retenção para o índice.

```
{
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/sales/*",
            ],
            "MinIndexRetention": "15d"
         },
         {
            "ResourceType":"index",
            "Resource":[
               "index/sales/log*",
            ],
            "NoMinIndexRetention": true
         }
      ]
   }
```

Sintaxe da política

Forneça uma ou mais regras. Essas regras definem as configurações do ciclo de vida dos dados para seus índices tecnologia sem servidor do OpenSearch.

Cada regra contém os seguintes elementos: Você pode fornecer `MinIndexRetention` ou `NoMinIndexRetention` em cada regra, mas não em ambas.

Elemento	Descrição
Tipo de recurso	O tipo de recurso ao qual a regra se aplica. A única opção compatível com políticas de ciclo de vida de dados é `index`
Recurso	Uma lista de nomes e/ou padrões de recursos. Os padrões consistem em um prefixo seguidos por um curinga (*), que permitem que as permissões associada s sejam aplicadas a vários recursos. Por exemplo, `index/<collection-name|pattern> /<index-name|pattern>` .

Elemento	Descrição
MinIndexRetention	O período limitado, em dias (d) ou horas (h), para manter o documento no índice. O limite mínimo é `24h` e o máximo é `3650d`.
NoMinIndexRetention	Se `true`, a tecnologia sem servidor do OpenSearch retém documentos indefinid amente.

Veja os seguintes exemplos:

```
{
  "Rules": [
    {
      "ResourceType": "index",
      "Resource": [
        "index/autoparts-inventory/*"
      ],
      "MinIndexRetention": "20d"
    },
    {
      "ResourceType": "index",
      "Resource": [
        "index/auto*/gear"
      ],
      "MinIndexRetention": "24h"
    },
    {
      "ResourceType": "index",
      "Resource": [
        "index/autoparts-inventory/tires"
      ],
      "NoMinIndexRetention": true
    }
  ]
}
```

Criação de políticas de ciclo de vida de dados (AWS CLI)

Para criar uma política de ciclo de vida dos dados usando as operações de API da tecnologia sem servidor do OpenSearch, use o comando CreateLifecyclePolicy. O comando aceita tanto políticas em linha quanto arquivos .json. As políticas em linha devem ser codificadas como uma string JSON com escape.

A solicitação a seguir cria uma política de ciclo de vida dos dados:

```
aws opensearchserverless create-lifecycle-policy \
    --name my-policy \
    --type retention \
    --policy "{\"Rules\":[{\"ResourceType\":\"index\",\"Resource\":[\"index/autoparts-
inventory/*\"],\"MinIndexRetention\": \"81d\"},{\"ResourceType\":\"index\",\"Resource
\":[\"index/sales/orders*\"],\"NoMinIndexRetention\":true}]}"
```

Para fornecer a política em um arquivo JSON, use o formato `--policy file://my-policy.json`

Visualizar políticas de ciclo de vida de dados

Antes de criar uma coleção, talvez você queira pré-visualizar as políticas de ciclo de vida dos dados existentes na sua conta para ver qual delas tem um padrão de recurso que corresponda ao nome da coleção. A solicitação ListLifecyclePolicies a seguir lista todas as políticas de ciclo de vida dos dados da sua conta:

```
aws opensearchserverless list-lifecycle-policies --type retention
```

A solicitação retorna informações sobre todas as políticas de ciclo de vida dos dados configuradas. Para visualizar as regras de padrões definidas em uma política específica, encontre as informações sobre políticas no conteúdo do elemento `lifecyclePolicySummaries` na resposta. Observe o `name` e `type` e use essas propriedades em uma solicitação BatchGetLifecyclePolicy para receber uma resposta com os seguintes detalhes da política:

```
{
    "lifecyclePolicySummaries": [
        {
            "type": "retention",
            "name": "my-policy",
```

```
            "policyVersion": "MTY2MzY5MTY1MDA3Ml8x",
            "createdDate": 1663691650072,
            "lastModifiedDate": 1663691650072
        }
    ]
}
```

Para limitar os resultados às políticas que contenham coleções ou índices específicos, você pode incluir filtros de recursos:

```
aws opensearchserverless list-lifecycle-policies --type retention --resources
 "index/autoparts-inventory/*"
```

Para exibir informações detalhadas sobre uma política específica, use o comando BatchGetLifecyclePolicy.

Atualização de políticas de ciclo de vida de dados

Quando você modifica uma política de ciclo de vida dos dados, todas as coleções associadas são afetadas. Para atualizar uma política de ciclo de vida dos dados no console da tecnologia sem servidor do OpenSearch, expanda Políticas de ciclo de vida dos dados, selecione a política a ser modificada e escolha Editar. Faça suas alterações e escolha Salvar.

Para atualizar uma política de ciclo de vida dos dados usando a API da tecnologia sem servidor do OpenSearch, use o comando UpdateLifecyclePolicy. É necessário incluir uma versão da política na solicitação. É possível recuperar a versão da política usando os comandos `ListLifecyclePolicies` ou `BatchGetLifecyclePolicy`. A inclusão da versão mais recente da política garante que você não anule inadvertidamente uma alteração feita por outra pessoa.

A solicitação a seguir atualiza uma política de ciclo de vida dos dados com um novo documento JSON de política:

```
aws opensearchserverless update-lifecycle-policy \
    --name my-policy \
    --type retention \
    --policy-version MTY2MzY5MTY1MDA3Ml8x \
    --policy file://my-new-policy.json
```

Pode haver alguns minutos de atraso entre a atualização da política e o momento em que os novos períodos de retenção são aplicados.

Como excluir políticas de ciclo de vida dos dados

Quando você exclui uma política de ciclo de vida de dados, ela não se aplica mais a nenhum índice correspondente. Para excluir uma política no console do OpenSearch Sem Servidor, selecione a política e escolha Excluir.

Você também pode usar o comando DeleteLifecyclePolicy:

```
aws opensearchserverless delete-lifecycle-policy --name my-policy --type retention
```

Uso de SDKs da AWS para interagir com o Amazon OpenSearch Sem Servidor

Esta seção inclui exemplos de como usar os SDKs da AWS para interagir com o Amazon OpenSearch Sem Servidor. Esses exemplos de códigos mostram como criar políticas e coleções de segurança, e como consultar coleções.

> **Note**
>
> No momento, estamos criando esses exemplos de código. Se você quiser contribuir com uma amostra de código (Java, Go etc.), abra uma solicitação pull diretamente no repositório do GitHub.

Tópicos

- Python
- JavaScript

Python

O script de exemplo a seguir usa o AWS SDK for Python (Boto3), assim como o cliente opensearch-py para Python, para criar políticas de criptografia, rede e acesso a dados, criar uma coleção correspondente e indexar alguns dados de exemplo.

Execute os comandos a seguir para instalar as dependências necessárias:

```
pip install opensearch-py
pip install boto3
pip install botocore
```

```
pip install requests-aws4auth
```

No script, é necessário substituir o elemento `Principal` pelo o nome do recurso da Amazon (ARN) do usuário ou da função do usuário que está assinando a solicitação. Você também pode, opcionalmente, modificar a `region`.

```
from opensearchpy import OpenSearch, RequestsHttpConnection
from requests_aws4auth import AWS4Auth
import boto3
import botocore
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

client = boto3.client('opensearchserverless')
service = 'aoss'
region = 'us-east-1'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key,
                   region, service, session_token=credentials.token)


def createEncryptionPolicy(client):
    """Creates an encryption policy that matches all collections beginning with tv-"""
    try:
        response = client.create_security_policy(
            description='Encryption policy for TV collections',
            name='tv-policy',
            policy="""
                {
                    \"Rules\":[
                        {
                            \"ResourceType\":\"collection\",
                            \"Resource\":[
                                \"collection\/tv-*\"
                            ]
                        }
                    ],
                    \"AWSOwnedKey\":true
                }
                """,
```

```
            type='encryption'
        )
        print('\nEncryption policy created:')
        print(response)
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] The policy name or rules conflict with an existing
 policy.')
        else:
            raise error


def createNetworkPolicy(client):
    """Creates a network policy that matches all collections beginning with tv-"""
    try:
        response = client.create_security_policy(
            description='Network policy for TV collections',
            name='tv-policy',
            policy="""
                [{
                    \"Description\":\"Public access for TV collection\",
                    \"Rules\":[
                        {
                            \"ResourceType\":\"dashboard\",
                            \"Resource\":[\"collection\/tv-*\"]
                        },
                        {
                            \"ResourceType\":\"collection\",
                            \"Resource\":[\"collection\/tv-*\"]
                        }
                    ],
                    \"AllowFromPublic\":true
                }]
                """,
            type='network'
        )
        print('\nNetwork policy created:')
        print(response)
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] A network policy with this name already exists.')
        else:
```

```
            raise error


def createAccessPolicy(client):
    """Creates a data access policy that matches all collections beginning with tv-"""
    try:
        response = client.create_access_policy(
            description='Data access policy for TV collections',
            name='tv-policy',
            policy="""
                [{
                    \"Rules\":[
                        {
                            \"Resource\":[
                                \"index\/tv-*\/*\"
                            ],
                            \"Permission\":[
                                \"aoss:CreateIndex\",
                                \"aoss:DeleteIndex\",
                                \"aoss:UpdateIndex\",
                                \"aoss:DescribeIndex\",
                                \"aoss:ReadDocument\",
                                \"aoss:WriteDocument\"
                            ],
                            \"ResourceType\": \"index\"
                        },
                        {
                            \"Resource\":[
                                \"collection\/tv-*\"
                            ],
                            \"Permission\":[
                                \"aoss:CreateCollectionItems\"
                            ],
                            \"ResourceType\": \"collection\"
                        }
                    ],
                    \"Principal\":[
                        \"arn:aws:iam::123456789012:role\/Admin\"
                    ]
                }]
                """,
            type='data'
        )
        print('\nAccess policy created:')
```

```
        print(response)
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] An access policy with this name already exists.')
        else:
            raise error


def createCollection(client):
    """Creates a collection"""
    try:
        response = client.create_collection(
            name='tv-sitcoms',
            type='SEARCH'
        )
        return(response)
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] A collection with this name already exists. Try
 another name.')
        else:
            raise error


def waitForCollectionCreation(client):
    """Waits for the collection to become active"""
    response = client.batch_get_collection(
        names=['tv-sitcoms'])
    # Periodically check collection status
    while (response['collectionDetails'][0]['status']) == 'CREATING':
        print('Creating collection...')
        time.sleep(30)
        response = client.batch_get_collection(
            names=['tv-sitcoms'])
    print('\nCollection successfully created:')
    print(response["collectionDetails"])
    # Extract the collection endpoint from the response
    host = (response['collectionDetails'][0]['collectionEndpoint'])
    final_host = host.replace("https://", "")
    indexData(final_host)
```

```
def indexData(host):
    """Create an index and add some sample data"""
    # Build the OpenSearch client
    client = OpenSearch(
        hosts=[{'host': host, 'port': 443}],
        http_auth=awsauth,
        use_ssl=True,
        verify_certs=True,
        connection_class=RequestsHttpConnection,
        timeout=300
    )
    # It can take up to a minute for data access rules to be enforced
    time.sleep(45)

    # Create index
    response = client.indices.create('sitcoms-eighties')
    print('\nCreating index:')
    print(response)

    # Add a document to the index.
    response = client.index(
        index='sitcoms-eighties',
        body={
            'title': 'Seinfeld',
            'creator': 'Larry David',
            'year': 1989
        },
        id='1',
    )
    print('\nDocument added:')
    print(response)


def main():
    createEncryptionPolicy(client)
    createNetworkPolicy(client)
    createAccessPolicy(client)
    createCollection(client)
    waitForCollectionCreation(client)


if __name__ == "__main__":
    main()
```

JavaScript

O script de exemplo a seguir usa o SDK para JavaScript no Node.js, assim como o cliente opensearch-py para JavaScript, para criar políticas de criptografia, rede e acesso a dados, criar uma coleção correspondente, criar um índice e indexar alguns dados de exemplo.

Execute os comandos a seguir para instalar as dependências necessárias:

```
npm i aws-sdk
npm i aws4
npm i @opensearch-project/opensearch
```

No script, é necessário substituir o elemento `Principal` pelo o nome do recurso da Amazon (ARN) do usuário ou da função do usuário que está assinando a solicitação. Você também pode, opcionalmente, modificar a `region`.

```
var AWS = require('aws-sdk');
var aws4 = require('aws4');
var {
    Client,
    Connection
} = require("@opensearch-project/opensearch");
var {
    OpenSearchServerlessClient,
    CreateSecurityPolicyCommand,
    CreateAccessPolicyCommand,
    CreateCollectionCommand,
    BatchGetCollectionCommand
} = require("@aws-sdk/client-opensearchserverless");
var client = new OpenSearchServerlessClient();

async function execute() {
    await createEncryptionPolicy(client)
    await createNetworkPolicy(client)
    await createAccessPolicy(client)
    await createCollection(client)
    await waitForCollectionCreation(client)
}

async function createEncryptionPolicy(client) {
    // Creates an encryption policy that matches all collections beginning with 'tv-'
    try {
```

```
        var command = new CreateSecurityPolicyCommand({
            description: 'Encryption policy for TV collections',
            name: 'tv-policy',
            type: 'encryption',
            policy: " \
        { \
            \"Rules\":[ \
                { \
                    \"ResourceType\":\"collection\", \
                    \"Resource\":[ \
                        \"collection\/tv-*\" \
                    ] \
                } \
            ], \
            \"AWSOwnedKey\":true \
        }"
        });
        const response = await client.send(command);
        console.log("Encryption policy created:");
        console.log(response['securityPolicyDetail']);
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] The policy name or rules conflict with an
 existing policy.');
        } else
            console.error(error);
    };
}

async function createNetworkPolicy(client) {
    // Creates a network policy that matches all collections beginning with 'tv-'
    try {
        var command = new CreateSecurityPolicyCommand({
            description: 'Network policy for TV collections',
            name: 'tv-policy',
            type: 'network',
            policy: " \
            [{ \
                \"Description\":\"Public access for television collection\", \
                \"Rules\":[ \
                    { \
                        \"ResourceType\":\"dashboard\", \
                        \"Resource\":[\"collection\/tv-*\"] \
                    }, \
```

```
                    { \
                        \"ResourceType\":\"collection\", \
                        \"Resource\":[\"collection\/tv-*\"] \
                    } \
                ], \
                \"AllowFromPublic\":true \
            }]"
        });
        const response = await client.send(command);
        console.log("Network policy created:");
        console.log(response['securityPolicyDetail']);
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] A network policy with that name already
 exists.');
        } else
            console.error(error);
    };
}

async function createAccessPolicy(client) {
    // Creates a data access policy that matches all collections beginning with 'tv-'
    try {
        var command = new CreateAccessPolicyCommand({
            description: 'Data access policy for TV collections',
            name: 'tv-policy',
            type: 'data',
            policy: " \
            [{ \
                \"Rules\":[ \
                    { \
                        \"Resource\":[ \
                            \"index\/tv-*\/*\" \
                        ], \
                        \"Permission\":[ \
                            \"aoss:CreateIndex\", \
                            \"aoss:DeleteIndex\", \
                            \"aoss:UpdateIndex\", \
                            \"aoss:DescribeIndex\", \
                            \"aoss:ReadDocument\", \
                            \"aoss:WriteDocument\" \
                        ], \
                        \"ResourceType\": \"index\" \
                    }, \
```

```
                    { \
                        \"Resource\":[ \
                            \"collection\/tv-*\" \
                        ], \
                        \"Permission\":[ \
                            \"aoss:CreateCollectionItems\" \
                        ], \
                        \"ResourceType\": \"collection\" \
                    } \
                ], \
                \"Principal\":[ \
                    \"arn:aws:iam::123456789012:role\/Admin\" \
                ] \
            }]"
        });
        const response = await client.send(command);
        console.log("Access policy created:");
        console.log(response['accessPolicyDetail']);
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] An access policy with that name already
 exists.');
        } else
            console.error(error);
    };
}

async function createCollection(client) {
    // Creates a collection to hold TV sitcoms indexes
    try {
        var command = new CreateCollectionCommand({
            name: 'tv-sitcoms',
            type: 'SEARCH'
        });
        const response = await client.send(command);
        return (response)
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] A collection with this name already
 exists. Try another name.');
        } else
            console.error(error);
    };
}
```

```
async function waitForCollectionCreation(client) {
    // Waits for the collection to become active
    try {
        var command = new BatchGetCollectionCommand({
            names: ['tv-sitcoms']
        });
        var response = await client.send(command);
        while (response.collectionDetails[0]['status'] == 'CREATING') {
            console.log('Creating collection...')
            await sleep(30000) // Wait for 30 seconds, then check the status again
            function sleep(ms) {
                return new Promise((resolve) => {
                    setTimeout(resolve, ms);
                });
            }
            var response = await client.send(command);
        }
        console.log('Collection successfully created:');
        console.log(response['collectionDetails']);
        // Extract the collection endpoint from the response
        var host = (response.collectionDetails[0]['collectionEndpoint'])
        // Pass collection endpoint to index document request
        indexDocument(host)
    } catch (error) {
        console.error(error);
    };
}

async function indexDocument(host) {

    var client = new Client({
        node: host,
        Connection: class extends Connection {
            buildRequestObject(params) {
                var request = super.buildRequestObject(params)
                request.service = 'aoss';
                request.region = 'us-east-1'; // e.g. us-east-1
                var body = request.body;
                request.body = undefined;
                delete request.headers['content-length'];
                request.headers['x-amz-content-sha256'] = 'UNSIGNED-PAYLOAD';
                request = aws4.sign(request, AWS.config.credentials);
                request.body = body;
```

```
                return request
            }
        }
    });

    // Create an index
    try {
        var index_name = "sitcoms-eighties";

        var response = await client.indices.create({
            index: index_name
        });

        console.log("Creating index:");
        console.log(response.body);

        // Add a document to the index
        var document = "{ \"title\": \"Seinfeld\", \"creator\": \"Larry David\", \"year
\": \"1989\" }\n";

        var response = await client.index({
            index: index_name,
            body: document
        });

        console.log("Adding document:");
        console.log(response.body);
    } catch (error) {
        console.error(error);
    };
}

execute()
```

Uso de AWS CloudFormation para a criação de coleções do Amazon OpenSearch Sem Servidor

É possível usar AWS CloudFormation para criar recursos do Amazon OpenSearch Sem Servidor, como coleções, políticas de segurança e endpoints da VPC. Para obter a referência abrangente do OpenSearch Sem Servidor CloudFormation, consulte Amazon OpenSearch Sem Servidor no Guia do usuário do AWS CloudFormation.

O modelo de exemplo do CloudFormation a seguir cria uma política simples de acesso a dados, política de rede e política de segurança, bem como uma coleção correspondente. É uma boa maneira de começar a trabalhar rapidamente com o Amazon OpenSearch Sem Servidor e provisionar os elementos necessários para criar e usar uma coleção.

> **Important**
>
> Este exemplo usa o acesso à rede pública, o que não é recomendado para workloads de produção. Recomendamos usar o acesso pela VPC para proteger suas coleções. Para obter mais informações, consulte AWS::OpenSearchServerless::VpcEndpoint e the section called "Endpoints da VPC".

```
AWSTemplateFormatVersion: 2010-09-09
Description: 'Amazon OpenSearch Serverless template to create an IAM user, encryption
 policy, data access policy and collection'
Resources:
  IAMUSer:
    Type: 'AWS::IAM::User'
    Properties:
      UserName:  aossadmin
  DataAccessPolicy:
    Type: 'AWS::OpenSearchServerless::AccessPolicy'
    Properties:
      Name: quickstart-access-policy
      Type: data
      Description: Access policy for quickstart collection
      Policy: !Sub >-
        [{"Description":"Access for cfn user","Rules":
[{"ResourceType":"index","Resource":["index/*/*"],"Permission":["aoss:*"]},
        {"ResourceType":"collection","Resource":["collection/quickstart"],"Permission":
["aoss:*"]}],
        "Principal":["arn:aws:iam::${AWS::AccountId}:user/aossadmin"]}]
  NetworkPolicy:
    Type: 'AWS::OpenSearchServerless::SecurityPolicy'
    Properties:
      Name: quickstart-network-policy
      Type: network
      Description: Network policy for quickstart collection
      Policy: >-
```

```
        [{"Rules":[{"ResourceType":"collection","Resource":["collection/
quickstart"]}, {"ResourceType":"dashboard","Resource":["collection/
quickstart"]}],"AllowFromPublic":true}]
  EncryptionPolicy:
    Type: 'AWS::OpenSearchServerless::SecurityPolicy'
    Properties:
      Name: quickstart-security-policy
      Type: encryption
      Description: Encryption policy for quickstart collection
      Policy: >-
        {"Rules":[{"ResourceType":"collection","Resource":["collection/
quickstart"]}],"AWSOwnedKey":true}
  Collection:
    Type: 'AWS::OpenSearchServerless::Collection'
    Properties:
      Name: quickstart
      Type: TIMESERIES
      Description: Collection to holds timeseries data
    DependsOn: EncryptionPolicy
Outputs:
  IAMUser:
    Value: !Ref IAMUSer
  DashboardURL:
    Value: !GetAtt Collection.DashboardEndpoint
  CollectionARN:
    Value: !GetAtt Collection.Arn
```

Gerenciamento de limites de capacidade para o Amazon OpenSearch Sem Servidor

Com o Amazon OpenSearch Sem Servidor, você não precisa gerenciar capacidades por conta própria. O OpenSearch Sem Servidor escala automaticamente a capacidade de computação da sua conta com base na workload atual. A capacidade de computação com tecnologia sem servidor é medida em unidades de computação do OpenSearch (OCUs). Cada OCU é uma combinação de 6 GiB de memória e CPU virtual (vCPU) correspondente e cria um pipeline de dados para o Amazon S3. Para obter mais informações sobre a arquitetura desacoplada no OpenSearch Sem Servidor, consulte the section called “Como funciona”.

Quando você cria sua primeira coleção, o OpenSearch Sem Servidor instancia um total de quatro OCUs (duas para indexação e duas para pesquisa). Essas OCUs sempre existem, mesmo

quando não há atividade de indexação ou de pesquisa. Todas as coleções subsequentes poderão compartilhar essas OCUs (exceto as coleções com chaves do AWS KMS exclusivas, que instanciam seu próprio conjunto de quatro OCUs). Se necessário, o OpenSearch Sem Servidor aumenta a escala horizontalmente de maneira automática e adiciona mais OCUs à medida que seu uso de indexação e pesquisa aumenta. Quando o tráfego no seu endpoint de coleta diminuir, a capacidade retornará para o número mínimo de OCUs necessário para o tamanho dos seus dados. Ele será reduzido para no máximo 2 OCUs para indexação e 2 OCUs para pesquisa.

Para coleções de pesquisa e pesquisa vetorial, todos os dados são armazenados em índices de alta atividade para garantir tempos de resposta rápidos às consultas. Coleções de séries temporais usam uma combinação de armazenamento de atividade alta e muito alta, mantendo os dados mais recentes em armazenamento de atividade muito alta para otimizar os tempos de resposta da consulta para dados acessados com mais frequência. Para obter mais informações, consulte the section called “Escolha de um tipo de coleção”.

Para gerenciar a capacidade de suas coleções e controlar os custos, é possível especificar a capacidade máxima geral de indexação e pesquisa para a conta atual e a região, e o OpenSearch Sem Servidor aumentará a escala de seus recursos de coleção horizontalmente de maneira automática com base nessas especificações.

Como a capacidade de indexação e de pesquisa são escaladas separadamente, você especifica limites no nível de conta para cada uma:

- Capacidade máxima de indexação: o OpenSearch Sem Servidor pode aumentar a capacidade de indexação até esse número de OCUs.
- Capacidade máxima de pesquisa: o OpenSearch Sem Servidor pode aumentar a capacidade de pesquisa até esse número de OCUs.

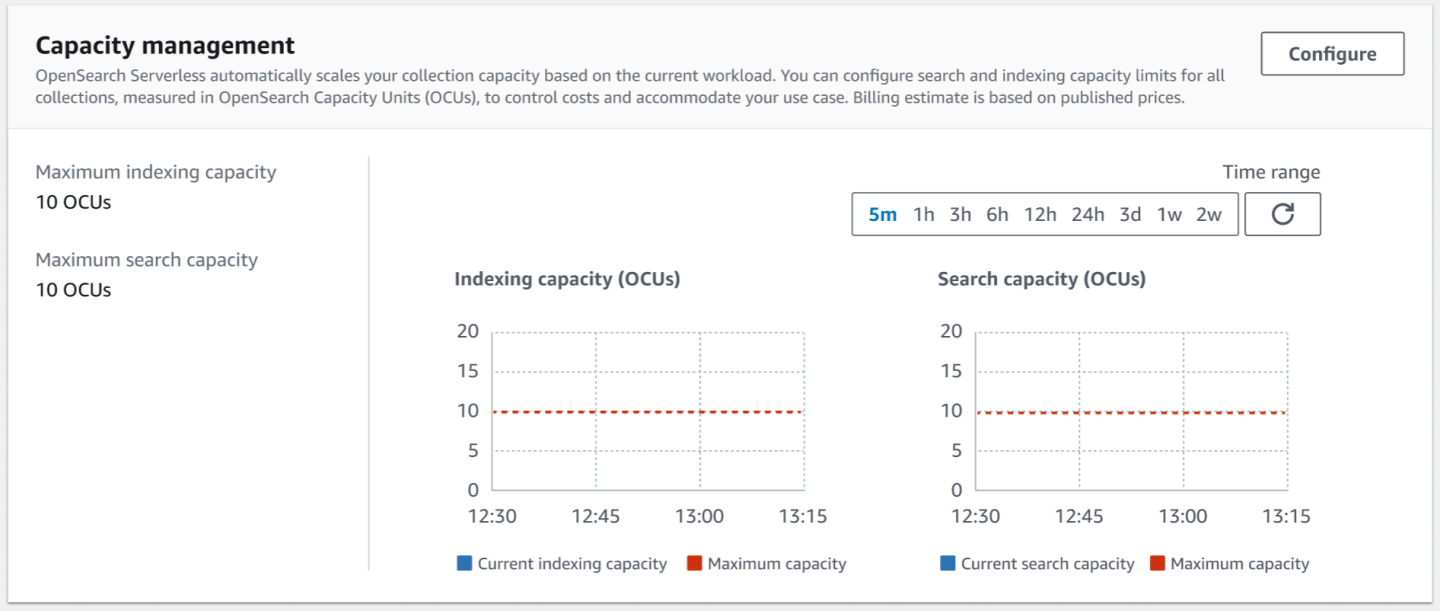
> **Note**
>
> No momento, as configurações de capacidade só se aplicam ao nível da conta. Você não pode configurar limites de capacidade por coleção.

Sua meta deve ser garantir que a capacidade máxima seja alta o suficiente para lidar com picos de workload. Com base nas suas configurações, o OpenSearch Sem Servidor aumentará a escala horizontalmente do número de OCUs das suas coleções de maneira automática para processar a workload de indexação e pesquisa.

Tópicos

Definição de configurações de capacidade

Para definir as configurações de capacidade no console do OpenSearch Sem Servidor, expanda Sem Servidor no painel de navegação à esquerda e selecione Painel. Especifique a capacidade máxima de indexação e pesquisa em Gerenciamento de capacidade:



Para configurar a capacidade usando a AWS CLI, envie uma solicitação UpdateAccountSettings:

```
aws opensearchserverless update-account-settings \
    --capacity-limits '{ "maxIndexingCapacityInOCU": 8,"maxSearchCapacityInOCU": 9 }'
```

Limites máximos de capacidade

Para todos os três tipos de coleções, a capacidade máxima padrão é 10 OCUs para indexação e 10 OCUs para pesquisa. A capacidade mínima permitida para uma conta é de 2 OCUs para indexação e 2 OCUs para pesquisa. Para todas as coleções, a capacidade máxima permitida é de 200 OCUs para indexação e 200 OCUs para pesquisa. Você pode configurar a contagem de OCUs para ser qualquer número de 2 até a capacidade máxima permitida, em múltiplos de 2.

Cada OCU inclui armazenamento efêmero de atividade muito alta que é suficiente para 120 GiB de dados de indexação. O OpenSearch sem Servidor aceita até 1 TiB de dados por índice em coleções de pesquisa e pesquisa vetorial e 10 TiB de dados de alta atividade por índice em uma coleção de séries temporais. Para coletas de séries temporais, você pode ingerir mais dados, que podem ser armazenados como dados quentes no S3.

Para obter uma lista de todas as cotas, consulte as cotas do OpenSearch Sem Servidor.

Monitoramento do uso da capacidade

É possível monitorar as métricas `Search0CU` e `Indexing0CU` do CloudWatch em nível de conta para entender como suas coleções estão sendo escaladas. É recomendável definir alarmes para notificação caso sua conta se aproxime de um limite das métricas relacionadas à capacidade, para que você possa ajustar as configurações de capacidade de acordo.

Você também pode usar essas métricas para determinar se as configurações de capacidade máxima são apropriadas ou se você precisa ajustá-las. Analise essas métricas para concentrar seus esforços para otimizar a eficiência de suas coleções. Para obter mais informações sobre as métricas que o OpenSearch Sem Servidor envia ao CloudWatch, consulte the section called “Monitoramento OpenSearch sem servidor”.

Ingestão de dados em coleções Amazon OpenSearch Serverless

Essas seções fornecem detalhes sobre os pipelines de ingestão compatíveis para ingestão de dados em coleções Amazon OpenSearch Serverless. Eles também abrangem alguns dos clientes que você pode usar para interagir com as operações da OpenSearch API. Seus clientes devem ser compatíveis com OpenSearch 2.x para se integrarem ao OpenSearch Serverless.

Tópicos

- Permissões mínimas necessárias
- OpenSearch Ingestão
- Fluent Bit
- Amazon Data Firehose
- Fluentd
- Go
- Java

- JavaScript
- Logstash
- Python
- Ruby
- Assinar solicitações HTTP com outros clientes

Permissões mínimas necessárias

Para ingerir dados em uma coleção OpenSearch sem servidor, o diretor que está gravando os dados deve ter as seguintes permissões mínimas atribuídas em uma política de acesso a dados:

```
[
   {
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/target-collection/logs"
            ],
            "Permission":[
               "aoss:CreateIndex",
               "aoss:WriteDocument",
               "aoss:UpdateIndex"
            ]
         }
      ],
      "Principal":[
         "arn:aws:iam::123456789012:user/my-user"
      ]
   }
]
```

As permissões podem ser mais amplas se você planejar gravar em índices adicionais. Por exemplo, em vez de especificar um único índice de destino, é possível atribuir permissão a todos os índices (índice/*coleção-de-destino*/*) ou a um subconjunto de índices (índice/*coleção-de-destino*/*logs**).

Para obter uma referência de todas as operações de OpenSearch API disponíveis e suas permissões associadas, consultethe section called “Operações e plug-ins com suporte”.

OpenSearch Ingestão

Em vez de usar um cliente terceirizado para enviar dados diretamente para uma coleção OpenSearch sem servidor, você pode usar o Amazon OpenSearch Ingestion. Você configura seus produtores de dados para enviar dados para OpenSearch Ingestão, e ele entrega automaticamente os dados para a coleção que você especificar. Você também pode configurar a OpenSearch ingestão para transformar seus dados antes de entregá-los. Para ter mais informações, consulte OpenSearch Ingestão da Amazon.

Um pipeline OpenSearch de ingestão precisa de permissão para gravar em uma coleção OpenSearch Serverless configurada como coletor. Essas permissões incluem a capacidade de descrever a coleção e enviar solicitações HTTP para ela.

Primeiro, crie um perfil do IAM que tenha as permissões `aoss:BatchGetCollection` e `aoss:APIAccessAll` em todos os recursos (`*`). Em seguida, inclua esse perfil em uma política de acesso a dados e forneça permissões para criar índices, atualizar índices, descrever índices e escrever documentos na coleção. Por fim, especifique o ARN do perfil como o valor da opção sts_role_arn na configuração do pipeline.

Para obter instruções sobre como concluir cada uma dessas etapas, consulte the section called “Concedendo aos oleodutos acesso às coleções”.

Para começar a usar o OpenSearch Ingestion, consultethe section called “Tutorial: Ingestão de dados em uma coleção”.

Fluent Bit

Você pode usarAWS a imagem Fluent Bit e o plug-in OpenSearch de saída para ingerir dados em coleções sem OpenSearch servidor.

> **Note**
>
> Você deve ter a versão 2.30.0 ou posterior da imagem AWS for Fluent Bit para fazer a integração com o Serverless. OpenSearch

Exemplo de configuração:

Este exemplo de seção de saída do arquivo de configuração mostra como usar uma coleção OpenSearch Serverless como destino. A adição importante é o parâmetro `AWS_Service_Name`, que é `aoss`. `Host` é o endpoint da coleção.

```
[OUTPUT]
    Name  opensearch
    Match *
    Host  collection-endpoint.us-west-2.aoss.amazonaws.com
    Port  443
    Index  my_index
    Trace_Error On
    Trace_Output On
    AWS_Auth On
    AWS_Region <region>
    AWS_Service_Name aoss
    tls     On
    Suppress_Type_Name On
```

Amazon Data Firehose

O Firehose oferece suporte ao OpenSearch Serverless como destino de entrega. Para obter instruções sobre como enviar dados para o OpenSearch Serverless, consulte Criação de um stream de entrega do Kinesis Data Firehose e OpenSearch Escolha sem servidor para seu destino no Guia do desenvolvedor do Amazon Data Firehose.

A função do IAM que você fornece ao Firehose para entrega deve ser especificada em uma política de acesso a dados com a permissão `aoss:WriteDocument` mínima para a coleção de destino, e você deve ter um índice preexistente para o qual enviar dados. Para ter mais informações, consulte the section called “Permissões mínimas necessárias”.

Antes de enviar dados para o OpenSearch Serverless, talvez seja necessário realizar transformações nos dados. Para saber mais sobre como usar funções do Lambda para executar essa tarefa, consulte Transformação de dados do Amazon Kinesis Data Firehose no mesmo guia.

Fluentd

Você pode usar o OpenSearch plug-in Fluentd para coletar dados de sua infraestrutura, contêineres e dispositivos de rede e enviá-los para coleções sem OpenSearch servidor. A Calyptia mantém uma distribuição do Fluentd que contém todas as dependências posteriores do Ruby e do SSL.

Para usar o Fluentd para enviar dados para o Serverless OpenSearch

1. Baixe a versão 1.4.2 ou posterior do Calyptia Fluentd de https://www.fluentd.org/download. Esta versão inclui o OpenSearch plug-in por padrão, que suporta OpenSearch Serverless.
2. Instale o pacote . Siga as instruções na documentação do Fluentd com base em seu sistema operacional:

   - Red Hat Enterprise Linux / CentOS / Amazon Linux
   - Debian / Ubuntu
   - Windows
   - MacOSX
3. Adicione uma configuração que envie dados para o OpenSearch Serverless. Essa configuração de exemplo envia a mensagem "teste" para uma única coleção. Não deixe de fazer o seguinte:

   - Para `host`, especifique o endpoint da sua coleção OpenSearch Serverless.
   - Em `aws_service_name`, especifique `aoss`.

   ```
   <source>
   @type sample
   tag test
   test {"hello":"world"}
   </source>

   <match test>
   @type opensearch
   host https://collection-endpoint.us-east-1.aoss.amazonaws.com
   port 443
   index_name fluentd
   aws_service_name aoss
   </match>
   ```
4. Execute o Calyptia Fluentd para começar a enviar dados para a coleção. Por exemplo, no Mac, é possível executar o seguinte comando:

   ```
   sudo launchctl load /Library/LaunchDaemons/calyptia-fluentd.plist
   ```

Go

O código de exemplo a seguir usa o cliente opensearch-go para Go para estabelecer uma conexão segura com a coleção OpenSearch Serverless especificada e criar um único índice. Você deve fornecer valores para `region` e `host`.

```
package main

import (
  "context"
  "log"
  "strings"
  "github.com/aws/aws-sdk-go-v2/aws"
  "github.com/aws/aws-sdk-go-v2/config"
  opensearch "github.com/opensearch-project/opensearch-go/v2"
  opensearchapi "github.com/opensearch-project/opensearch-go/v2/opensearchapi"
  requestsigner "github.com/opensearch-project/opensearch-go/v2/signer/awsv2"
)

const endpoint = "" // serverless collection endpoint

func main() {
 ctx := context.Background()

 awsCfg, err := config.LoadDefaultConfig(ctx,
  config.WithRegion("<AWS_REGION>"),
  config.WithCredentialsProvider(
   getCredentialProvider("<AWS_ACCESS_KEY>", "<AWS_SECRET_ACCESS_KEY>",
 "<AWS_SESSION_TOKEN>"),
  ),
 )
 if err != nil {
  log.Fatal(err) // don't log.fatal in a production-ready app
 }

 // create an AWS request Signer and load AWS configuration using default config folder
 or env vars.
 signer, err := requestsigner.NewSignerWithService(awsCfg, "aoss") // "aoss" for Amazon
 OpenSearch Serverless
 if err != nil {
  log.Fatal(err) // don't log.fatal in a production-ready app
 }
```

```
// create an opensearch client and use the request-signer
client, err := opensearch.NewClient(opensearch.Config{
 Addresses: []string{endpoint},
 Signer:    signer,
})
if err != nil {
 log.Fatal("client creation err", err)
}

indexName := "go-test-index"

 // define index mapping
mapping := strings.NewReader(`{
 "settings": {
   "index": {
        "number_of_shards": 4
        }
      }
 }`)

// create an index
createIndex := opensearchapi.IndicesCreateRequest{
 Index: indexName,
   Body: mapping,
}
createIndexResponse, err := createIndex.Do(context.Background(), client)
if err != nil {
 log.Println("Error ", err.Error())
 log.Println("failed to create index ", err)
 log.Fatal("create response body read err", err)
}
log.Println(createIndexResponse)

// delete the index
deleteIndex := opensearchapi.IndicesDeleteRequest{
 Index: []string{indexName},
}

deleteIndexResponse, err := deleteIndex.Do(context.Background(), client)
if err != nil {
 log.Println("failed to delete index ", err)
 log.Fatal("delete index response body read err", err)
}
log.Println("deleting index", deleteIndexResponse)
```

```
}

func getCredentialProvider(accessKey, secretAccessKey, token string)
 aws.CredentialsProviderFunc {
 return func(ctx context.Context) (aws.Credentials, error) {
  c := &aws.Credentials{
   AccessKeyID:     accessKey,
   SecretAccessKey: secretAccessKey,
   SessionToken:    token,
  }
  return *c, nil
 }
}
```

Java

O código de exemplo a seguir usa o cliente opensearch-java para Java para estabelecer uma conexão segura com a coleção OpenSearch Serverless especificada e criar um único índice. Você deve fornecer valores para `region` e `host`.

A diferença importante em relação aos domínios OpenSearch de serviço é o nome do serviço (`aoss` em vez de `es`).

```
// import OpenSearchClient to establish connection to OpenSearch Serverless collection
import org.opensearch.client.opensearch.OpenSearchClient;

SdkHttpClient httpClient = ApacheHttpClient.builder().build();

// create an opensearch client and use the request-signer
OpenSearchClient client = new OpenSearchClient(
    new AwsSdk2Transport(
        httpClient,
        "...us-west-2.aoss.amazonaws.com", // serverless collection endpoint
        "aoss" // signing service name
        Region.US_WEST_2, // signing service region
        AwsSdk2TransportOptions.builder().build()
    )
);

String index = "sample-index";

// create an index
```

```
CreateIndexRequest createIndexRequest = new
 CreateIndexRequest.Builder().index(index).build();
CreateIndexResponse createIndexResponse = client.indices().create(createIndexRequest);
System.out.println("Create index reponse: " + createIndexResponse);

// delete the index
DeleteIndexRequest deleteIndexRequest = new
 DeleteIndexRequest.Builder().index(index).build();
DeleteIndexResponse deleteIndexResponse = client.indices().delete(deleteIndexRequest);
System.out.println("Delete index reponse: " + deleteIndexResponse);

httpClient.close();
```

JavaScript

O código de exemplo a seguir usa o cliente opensearch-js JavaScript para estabelecer uma conexão segura com a coleção OpenSearch Serverless especificada, criar um único índice, adicionar um documento e excluir o índice. Você deve fornecer valores para `node` e `region`.

A diferença importante em relação aos domínios OpenSearch de serviço é o nome do serviço (`aoss`em vez de`es`).

Version 3

Este exemplo usa a versão 3 do SDK para JavaScript Node.js.

```
const { defaultProvider } = require('@aws-sdk/credential-provider-node');
const { Client } = require('@opensearch-project/opensearch');
const { AwsSigv4Signer } = require('@opensearch-project/opensearch/aws');

async function main() {
    // create an opensearch client and use the request-signer
    const client = new Client({
        ...AwsSigv4Signer({
            region: 'us-west-2',
            service: 'aoss',
            getCredentials: () => {
                const credentialsProvider = defaultProvider();
                return credentialsProvider();
            },
        }),
        node: '' # // serverless collection endpoint
    });
```

```
    const index = 'movies';

    // create index if it doesn't already exist
    if (!(await client.indices.exists({ index })).body) {
        console.log((await client.indices.create({ index })).body);
    }

    // add a document to the index
    const document = { foo: 'bar' };
    const response = await client.index({
        id: '1',
        index: index,
        body: document,
    });
    console.log(response.body);

    // delete the index
    console.log((await client.indices.delete({ index })).body);
}

main();
```

Version 2

Este exemplo usa a versão 2 do SDK para JavaScript Node.js.

```
const AWS = require('aws-sdk');
const { Client } = require('@opensearch-project/opensearch');
const { AwsSigv4Signer } = require('@opensearch-project/opensearch/aws');

async function main() {
    // create an opensearch client and use the request-signer
    const client = new Client({
        ...AwsSigv4Signer({
            region: 'us-west-2',
            service: 'aoss',
            getCredentials: () =>
                new Promise((resolve, reject) => {
                    AWS.config.getCredentials((err, credentials) => {
                        if (err) {
                            reject(err);
                        } else {
                            resolve(credentials);
```

```
                        }
                    });
                }),
        }),
        node: '' # // serverless collection endpoint
    });

    const index = 'movies';

    // create index if it doesn't already exist
    if (!(await client.indices.exists({ index })).body) {
        console.log((await client.indices.create({
            index
        })).body);
    }

    // add a document to the index
    const document = {
        foo: 'bar'
    };
    const response = await client.index({
        id: '1',
        index: index,
        body: document,
    });
    console.log(response.body);

    // delete the index
    console.log((await client.indices.delete({ index })).body);
}

main();
```

Logstash

Você pode usar o OpenSearch plug-in Logstash para publicar registros em coleções sem OpenSearch servidor.

Para usar o Logstash para enviar dados para o Serverless OpenSearch

1. Instale a versão 2.0.0 ou posterior do logstash-output-opensearchplug-in usando Docker ou Linux.

Docker

O Docker hospeda o software Logstash OSS com o plug-in de OpenSearch saída pré-instalado: opensearchproject/ -output-plugin. logstash-oss-with-opensearch É possível puxar a imagem como qualquer outra imagem:

```
docker pull opensearchproject/logstash-oss-with-opensearch-output-plugin:latest
```

Linux

Primeiro, instale a versão mais recente do Logstash, caso ainda não a tenha. Em seguida, instale a versão 2.0.0 do plug-in de saída:

```
cd logstash-8.5.0/
bin/logstash-plugin install --version 2.0.0 logstash-output-opensearch
```

Se o plug-in já estiver instalado, atualize-o para a versão mais recente:

```
bin/logstash-plugin update logstash-output-opensearch
```

A partir da versão 2.0.0 do plug-in, o AWS SDK usa a versão 3. Se você estiver usando uma versão do Logstash anterior à 8.4.0, deverá remover todos os plug-ins pré-instalados e instalar o AWS plug-in: `logstash-integration-aws`

```
/usr/share/logstash/bin/logstash-plugin remove logstash-input-s3
/usr/share/logstash/bin/logstash-plugin remove logstash-input-sqs
/usr/share/logstash/bin/logstash-plugin remove logstash-output-s3
/usr/share/logstash/bin/logstash-plugin remove logstash-output-sns
/usr/share/logstash/bin/logstash-plugin remove logstash-output-sqs
/usr/share/logstash/bin/logstash-plugin remove logstash-output-cloudwatch

/usr/share/logstash/bin/logstash-plugin install --version 0.1.0.pre logstash-
integration-aws
```

2. Para que o plug-in OpenSearch de saída funcione com o OpenSearch Serverless, você deve fazer as seguintes modificações na seção de `opensearch` saída do logstash.conf:

   - Especifique `aoss` como o `service_name` em `auth_type`.
   - Especifique seu endpoint de coleção para `hosts`.

- Adicione os parâmetros `default_server_major_version` e `legacy_template`. Esses parâmetros são necessários para que o plug-in funcione com o OpenSearch Serverless.

```
output {
  opensearch {
    hosts => "collection-endpoint:443"
    auth_type => {
      ...
      service_name => 'aoss'
    }
    default_server_major_version => 2
    legacy_template => false
  }
}
```

Esse exemplo de arquivo de configuração obtém sua entrada de arquivos em um bucket do S3 e os envia para uma coleção OpenSearch Serverless:

```
input {
  s3  {
    bucket => "my-s3-bucket"
    region => "us-east-1"
  }
}

output {
  opensearch {
    ecs_compatibility => disabled
    hosts => "https://my-collection-endpoint.us-east-1.aoss.amazonaws.com:443"
    index => my-index
    auth_type => {
      type => 'aws_iam'
      aws_access_key_id => 'your-access-key'
      aws_secret_access_key => 'your-secret-key'
      region => 'us-east-1'
      service_name => 'aoss'
    }
    default_server_major_version => 2
    legacy_template => false
  }
}
```

3. Em seguida, execute o Logstash com a nova configuração para testar o plug-in:

```
bin/logstash -f config/test-plugin.conf
```

Python

O código de exemplo a seguir usa o cliente opensearch-py para Python para estabelecer uma conexão segura com a coleção OpenSearch Serverless especificada, criar um único índice e pesquisar esse índice. Você deve fornecer valores para `region` e `host`.

A diferença importante em relação aos domínios OpenSearch de serviço é o nome do serviço (`aoss`em vez de`es`).

```
from opensearchpy import OpenSearch, RequestsHttpConnection, AWSV4SignerAuth
import boto3

host = ''  # serverless collection endpoint, without https://
region = ''  # e.g. us-east-1

service = 'aoss'
credentials = boto3.Session().get_credentials()
auth = AWSV4SignerAuth(credentials, region, service)

# create an opensearch client and use the request-signer
client = OpenSearch(
    hosts=[{'host': host, 'port': 443}],
    http_auth=auth,
    use_ssl=True,
    verify_certs=True,
    connection_class=RequestsHttpConnection,
    pool_maxsize=20,
)

# create an index
index_name = "books-index"
create_response = client.indices.create(
    index_name
)

print('\nCreating index:')
print(create_response)
```

```
# index a document
document = {
  'title': 'The Green Mile,
  'director': 'Stephen King',
  'year': '1996'
}

response = client.index(
    index = 'books-index',
    body = document,
    id = '1'
)


# delete the index
delete_response = client.indices.delete(
    index_name
)

print('\nDeleting index:')
print(delete_response)
```

Ruby

A `opensearch-aws-sigv4` gema fornece acesso ao OpenSearch Serverless, junto com o OpenSearch Service, pronto para uso. Ele tem todos os recursos do cliente opensearch-ruby porque é uma dependência desse gem.

Ao instanciar o signatário do Sigv4, especifique `aoss` como nome do serviço:

```
require 'opensearch-aws-sigv4'
require 'aws-sigv4'

signer = Aws::Sigv4::Signer.new(service: 'aoss',
                                region: 'us-west-2',
                                access_key_id: 'key_id',
                                secret_access_key: 'secret')

# create an opensearch client and use the request-signer
client = OpenSearch::Aws::Sigv4Client.new(
  { host: 'https://your.amz-opensearch-serverless.endpoint',
    log: true },
```

```
  signer)

# create an index
index = 'prime'
client.indices.create(index: index)

# insert data
client.index(index: index, id: '1', body: { name: 'Amazon Echo',
                                            msrp: '5999',
                                            year: 2011 })

# query the index
client.search(body: { query: { match: { name: 'Echo' } } })

# delete index entry
client.delete(index: index, id: '1')

# delete the index
client.indices.delete(index: index)
```

Assinar solicitações HTTP com outros clientes

Os requisitos a seguir se aplicam ao assinar solicitações em coleções OpenSearch sem servidor quando você cria solicitações HTTP com outros clientes.

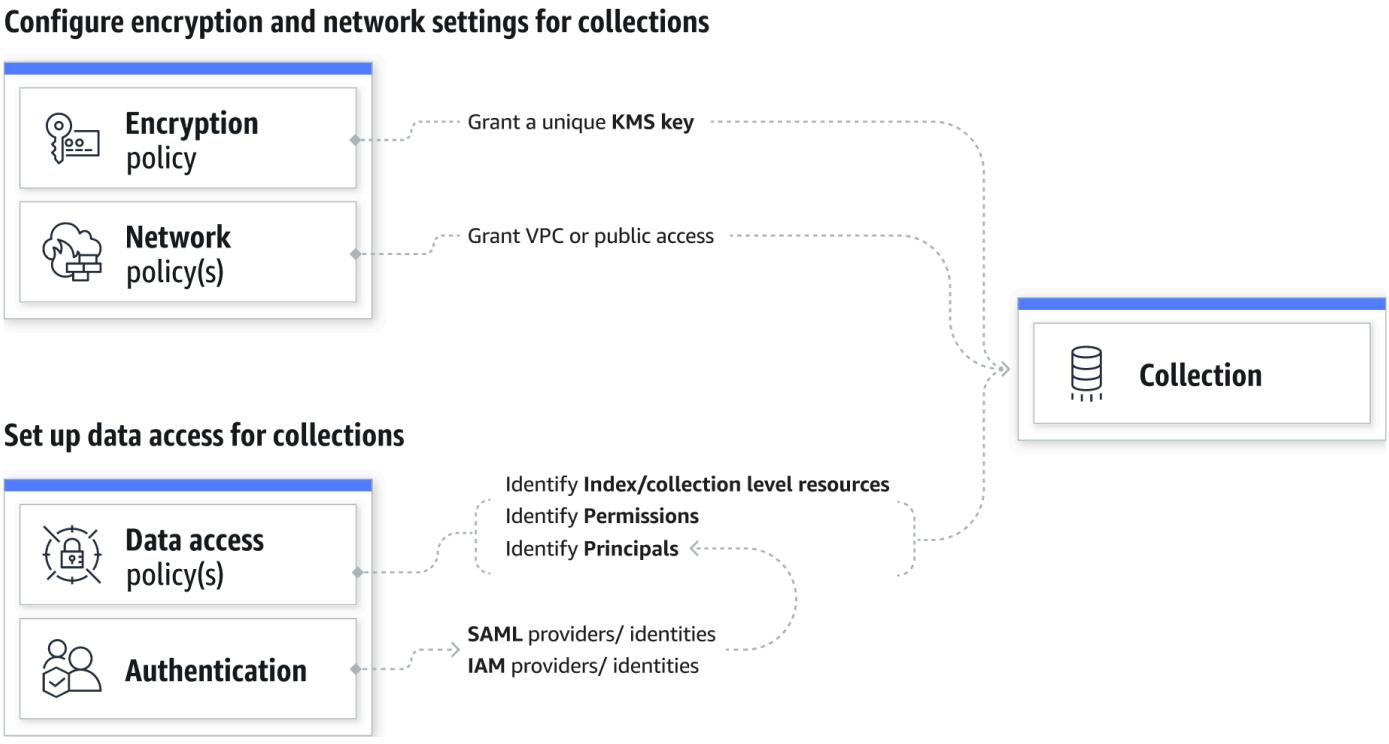
- O nome do serviço deve ser especificado como `aoss`.
- O cabeçalho `x-amz-content-sha256` é obrigatório para todas as solicitações do AWS Signature Version 4. Ele fornece um hash da carga da solicitação. Se houver uma carga de solicitação, defina o valor como seu hash criptográfico (SHA256) do Secure Hash Algorithm (SHA). Se não houver carga de solicitação, defina o valor como `e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`, que é o hash de uma string vazia.

Visão geral da segurança no Amazon OpenSearch Serverless

A segurança no Amazon OpenSearch Serverless difere fundamentalmente da segurança no Amazon OpenSearch Service das seguintes maneiras:

Atributo	OpenSearch Serviço	OpenSearch Sem servidor
Controle de acesso a dados	O acesso aos dados é determinado por políticas do IAM e por controle de acesso minucioso.	O acesso aos dados é determinado por políticas de acesso a dados.
Criptografia em repouso	A criptografia em repouso é opcional para domínios.	A criptografia em repouso é obrigatória para coleções.
Configuração e administração da segurança	Você deve configurar a rede, a criptografia e o acesso aos dados individualmente para cada domínio.	É possível usar políticas de segurança para gerenciar as configurações de segurança de várias coleções em escala.

O diagrama a seguir ilustra os componentes de segurança que compõem uma coleção funcional. Uma coleção deve ter uma chave de criptografia atribuída, configurações de acesso à rede e uma política de acesso a dados correspondente que conceda permissão aos seus recursos.



Tópicos

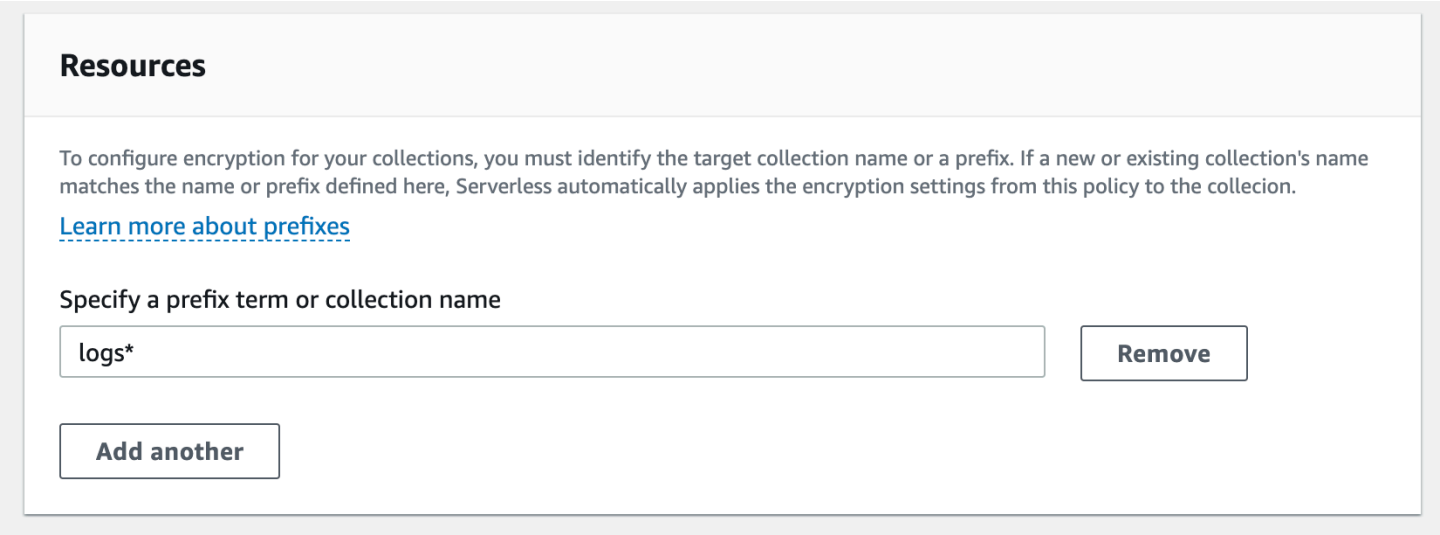
- Políticas de criptografia

- Políticas de rede
- Políticas de acesso a dados
- Autenticação SAML e IAM
- Segurança da infraestrutura
- Introdução à segurança no Amazon OpenSearch Serverless
- Gerenciamento de identidade e acesso no Amazon OpenSearch Sem Servidor
- Criptografia no Amazon OpenSearch Sem Servidor
- Acesso à rede para Amazon OpenSearch Serverless
- Controle de acesso a dados do Amazon OpenSearch Sem Servidor
- Acesse o Amazon OpenSearch Serverless usando um endpoint de interface () AWS PrivateLink
- Autenticação SAML para Amazon Serverless OpenSearch
- Validação de compatibilidade do Amazon OpenSearch Sem Servidor

Políticas de criptografia

As políticas de criptografia definem se suas coleções são criptografadas com uma chave gerenciada pelo cliente Chave pertencente à AWS ou com uma chave gerenciada pelo cliente. As políticas de criptografia consistem em dois componentes: um padrão de recursos e uma chave de criptografia. O padrão de recursos define a qual coleção ou coleções a política se aplica. A chave de criptografia determina como as coleções associadas serão protegidas.

Para aplicar uma política a várias coleções, inclua um curinga (*) na regra da política. Por exemplo, a política a seguir se aplica a todas as coleções com nomes que começam com “logs”.

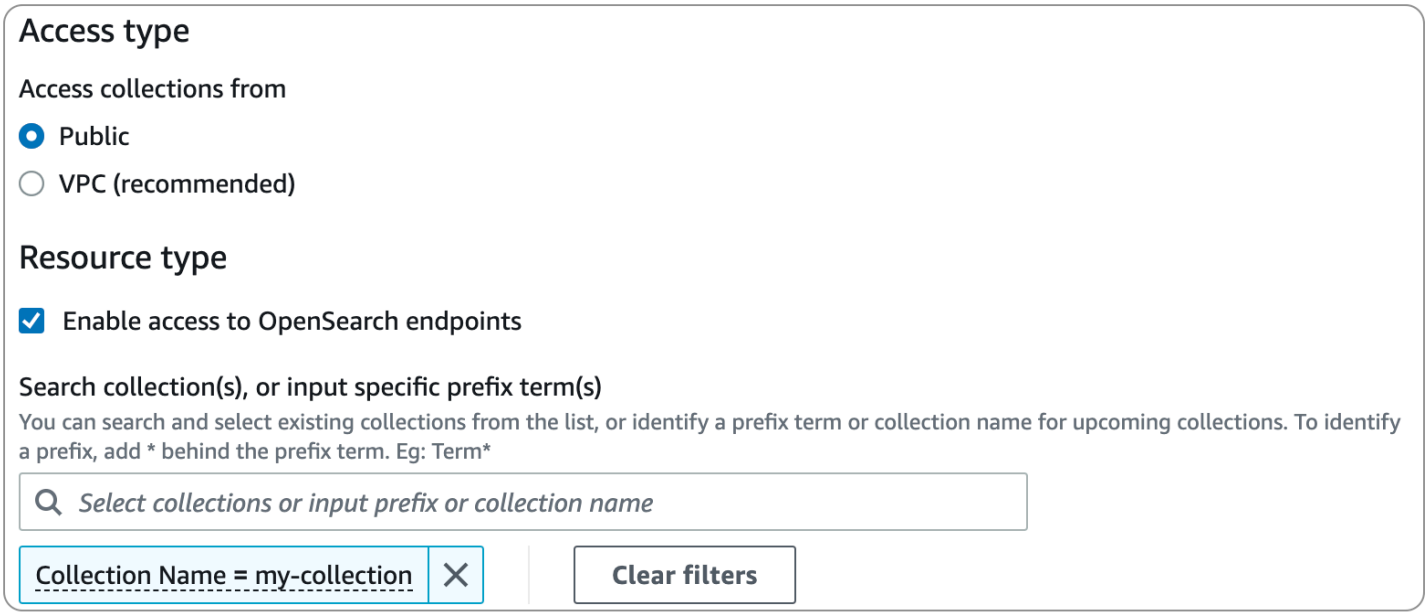


As políticas de criptografia simplificam o processo de criação e gerenciamento de coleções, especialmente quando isso é feito de forma programática. É possível criar uma coleção simplesmente especificando um nome, e uma chave de criptografia será automaticamente atribuída a ela na criação.

Políticas de rede

As políticas de rede definem se suas coleções podem ser acessadas de forma privada ou pela Internet a partir de redes públicas. As coleções particulares podem ser acessadas por meio de endpoints VPC OpenSearch gerenciados sem servidor ou por pontos específicos, Serviços da AWS como o Amazon Bedrock, usando acesso privado.AWS service (Serviço da AWS) Assim como as políticas de criptografia, as políticas de rede podem ser aplicadas a várias coleções, o que permite gerenciar o acesso à rede para muitas coleções em grande escala.

As políticas de rede consistem em dois componentes: um tipo de acesso e um tipo de recurso. O tipo de acesso pode ser público ou privado. O tipo de recurso determina se o acesso escolhido se aplica ao endpoint da coleção, ao endpoint do OpenSearch Dashboards ou a ambos.



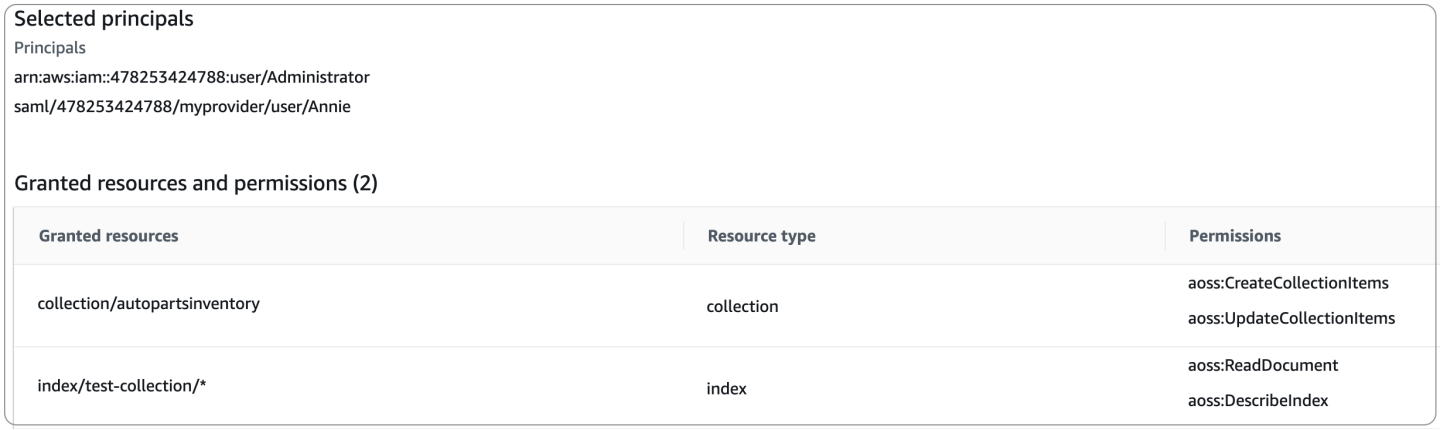
Se você planeja configurar o acesso à VPC dentro de uma política de rede, primeiro deve criar um ou mais VPC endpoints gerenciados OpenSearch sem servidor. Esses endpoints permitem que você acesse o OpenSearch Serverless como se estivesse em sua VPC, sem o uso de um gateway de internet, dispositivo NAT, conexão VPN ou conexão. AWS Direct Connect

O acesso privado ao só Serviços da AWS pode ser aplicado ao endpoint da coleção, não ao OpenSearch endpoint do OpenSearch Dashboards. Serviços da AWS não pode ter acesso aos OpenSearch painéis.

Políticas de acesso a dados

As políticas de acesso a dados definem como seus usuários acessam os dados em suas coleções. As políticas de acesso a dados ajudam você a gerenciar coleções em grande escala atribuindo automaticamente permissões de acesso a coleções e índices que correspondam a um padrão específico. Várias políticas podem ser aplicadas a um único recurso.

As políticas de acesso a dados consistem em um conjunto de regras, cada uma com três componentes: um tipo de recurso, recursos concedidos e um conjunto de permissões. O tipo de recurso pode ser uma coleção ou um índice. Os recursos concedidos podem ser nomes de coleções/índices ou padrões com um caractere curinga (*). A lista de permissões especifica a quais operações de OpenSearch API a política concede acesso. Além disso, a política contém uma lista de entidades principais, que especificam os perfis e usuários do IAM e as identidades SAML aos quais conceder acesso.



Para obter mais informações sobre o formato de uma política de acesso a dados, consulte a sintaxe da política.

Antes de criar uma política de acesso a dados, é necessário ter um ou mais usuários ou perfis do IAM, ou identidades SAML, aos quais fornecer acesso na política. Consulte a próxima seção para obter detalhes.

Autenticação SAML e IAM

As entidades principais do IAM e as identidades do SAML são um dos alicerces de uma política de acesso a dados. Na declaração `principal` de uma política de acesso, é possível incluir usuários e

perfis do IAM e identidades SAML. Em seguida, essas entidades principais recebem as permissões que você especifica nas regras de política associadas.

```
[
   {
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/marketing/orders*"
            ],
            "Permission":[
               "aoss:*"
            ]
         }
      ],
      "Principal":[
         "arn:aws:iam::123456789012:user/Dale",
         "arn:aws:iam::123456789012:role/RegulatoryCompliance",
         "saml/123456789012/myprovider/user/Annie"
      ]
   }
]
```

Você configura a autenticação SAML diretamente no OpenSearch Serverless. Para ter mais informações, consulte the section called “Autenticação SAML”.

Segurança da infraestrutura

O Amazon OpenSearch Serverless é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o Amazon OpenSearch Serverless pela rede. Os clientes devem suportar o Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3. Para obter uma lista das cifras compatíveis com o TLS 1.3, consulte Protocolos e cifras TLS na documentação do Elastic Load Balancing.

Além disso, você deve assinar solicitações usando um ID de chave de acesso e uma chave de acesso secreta associada a um principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Introdução à segurança no Amazon OpenSearch Serverless

Os tutoriais a seguir ajudam você a começar a usar o Amazon OpenSearch Serverless. Ambos os tutoriais realizam as mesmas etapas básicas, mas um usa o console enquanto o outro usa a AWS CLI.

Observe que os casos de uso nestes tutoriais são simplificados. As políticas de rede e segurança são bastante abertas. Nas workloads de produção, recomendamos que você configure recursos de segurança mais robustos, como autenticação SAML, acesso por VPC e políticas de acesso a dados restritivas.

Tópicos

- Tutorial: Introdução à segurança no Amazon OpenSearch Serverless (console)
- Tutorial: Introdução à segurança no Amazon OpenSearch Serverless (CLI)

Tutorial: Introdução à segurança no Amazon OpenSearch Serverless (console)

Este tutorial mostra as etapas básicas para criar e gerenciar políticas de segurança usando o console Amazon OpenSearch Serverless.

Você concluirá as seguintes etapas neste tutorial:

1. Configurar permissões
2. Criar uma política de criptografia
3. Criar uma política de rede
4. Configurar uma política de acesso a dados
5. Criar uma coleção
6. Transferir e pesquisar dados

Este tutorial orienta você ao longo da configuração de uma coleção usando o AWS Management Console. Para obter as mesmas etapas usando a AWS CLI, consulte the section called “Tutorial: Conceitos básicos de segurança (CLI)”.

Etapa 1: configurar permissões

> **Note**
>
> É possível pular esta etapa se já estiver usando uma política baseada em identidade mais ampla, como `Action":"aoss:*"` ou `Action":"*"`. Em ambientes de produção, no entanto, recomendamos que você siga o princípio do privilégio mínimo e atribua somente as permissões mínimas necessárias para concluir uma tarefa.

Para concluir este tutorial, você deve ter as permissões corretas do IAM. Seu usuário ou função deve ter uma política baseada em identidade anexada com as seguintes permissões mínimas:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aoss:ListCollections",
        "aoss:BatchGetCollection",
        "aoss:CreateCollection",
        "aoss:CreateSecurityPolicy",
        "aoss:GetSecurityPolicy",
        "aoss:ListSecurityPolicies",
        "aoss:CreateAccessPolicy",
        "aoss:GetAccessPolicy",
        "aoss:ListAccessPolicies"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Para obter uma lista completa das permissões OpenSearch sem servidor, consulte. the section called “Identity and Access Management”

Etapa 2: criar uma política de criptografia

As políticas de criptografia especificam a AWS KMS chave que o OpenSearch Serverless usará para criptografar a coleção. É possível criptografar coleções com uma Chave gerenciada pela AWS

ou uma chave diferente. Por simplicidade, neste tutorial, criptografaremos nossa coleção com uma Chave gerenciada pela AWS.

Para criar uma política de criptografia

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. No painel de navegação à esquerda, expanda Sem Servidor e escolha Políticas de criptografia.
3. Escolha Criar política de criptografia.
4. Nomeie a política como books-policy. Para a descrição, insira Política de criptografia para coleção de livros.
5. Em Recursos, insira livros, que é como você chamará sua coleção. Se você quiser ser mais amplo, inclua um asterisco (`books*`) para que a política se aplique a todas as coleções que comecem com a palavra “books” (livros).
6. Em Criptografia, mantenha a opção Usar chave própria da AWS selecionada.
7. Escolha Criar.

Etapa 3: criar uma política de rede

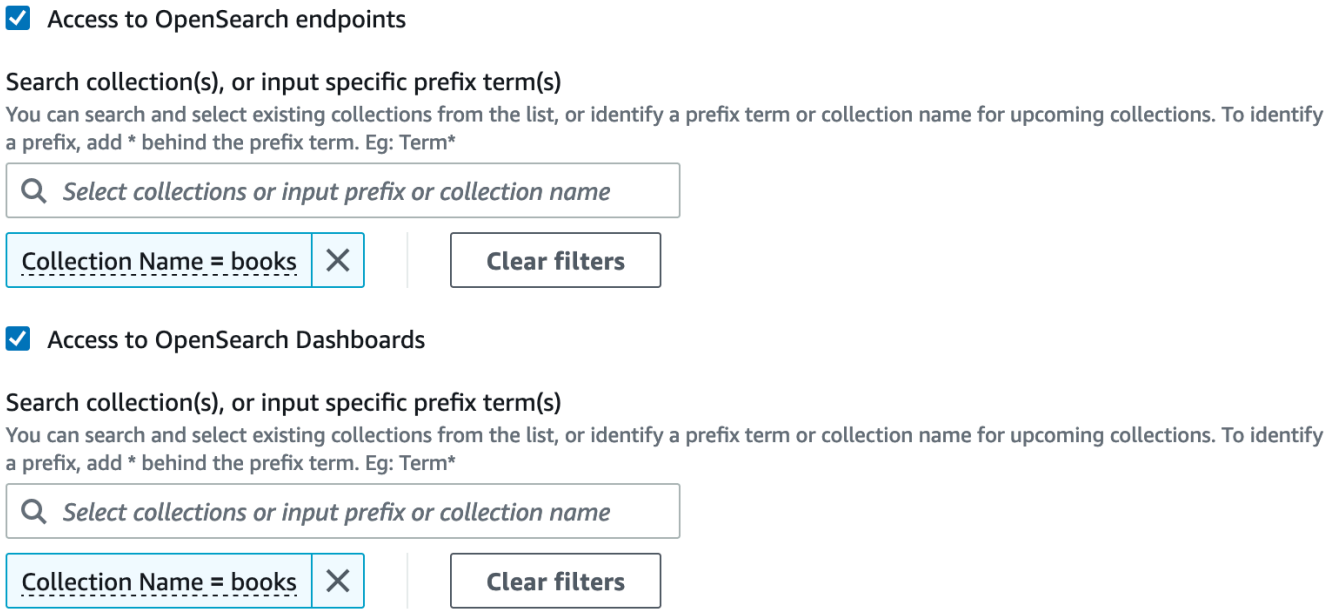
As políticas de rede determinam se sua coleção pode ser acessada pela Internet a partir de redes públicas ou se ela deve ser acessada por meio de VPC endpoints OpenSearch gerenciados sem servidor. Neste tutorial, configuraremos o acesso público.

Para criar uma política de rede

1. Escolha Políticas de rede no painel de navegação à esquerda, e escolha Criar política de rede.
2. Nomeie a política como books-policy. Para a descrição, insira Política de rede para coleção de livros.
3. Na Regra 1, nomeie a regra como Acesso público para coleção de livros .
4. Para simplificar, neste tutorial, configuraremos o acesso público para a coleção livros. Para o tipo de acesso, selecione Público.
5. Vamos acessar a coleção a partir dos OpenSearch painéis. Para fazer isso, você precisa configurar o acesso à rede para painéis e o OpenSearch endpoint, caso contrário, os painéis não funcionarão.

   Para o tipo de recurso, habilite o acesso aos OpenSearch endpoints e o acesso aos OpenSearch painéis.

6. Em ambas as caixas de entrada, insira Nome da coleção = livros. Essa configuração reduz o escopo da política para que ela se aplique somente a uma única coleção (`books`). Sua regra deve ser semelhante a esta:



7. Escolha Criar.

Etapa 4: Criar uma política de acesso a dados

Os dados da sua coleção não estarão acessíveis até que você configure o acesso aos dados. As políticas de acesso a dados são separadas da política baseada em identidade do IAM que você configurou na etapa 1. Elas permitem que os usuários acessem os dados reais de uma coleção.

Neste tutorial, forneceremos a um único usuário as permissões necessárias para indexar dados na coleção livros.

Para criar uma política de acesso a dados

1. No painel de navegação à esquerda, escolha Políticas de acesso a dados e, em seguida, Criar política de acesso.
2. Nomeie a política como books-policy. Para a descrição, insira Política de acesso a dados para coleção de livros.
3. Selecione JSON para o método de definição de política e cole a seguinte política no editor JSON.

Substitua o ARN principal pelo ARN da conta que você usará para fazer login nos OpenSearch painéis e indexar dados.

```
[
   {
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/books/*"
            ],
            "Permission":[
               "aoss:CreateIndex",
               "aoss:DescribeIndex",
               "aoss:ReadDocument",
               "aoss:WriteDocument",
               "aoss:UpdateIndex",
               "aoss:DeleteIndex"
            ]
         }
      ],
      "Principal":[
         "arn:aws:iam::123456789012:user/my-user"
      ]
   }
]
```

Esta política fornece a um único usuário as permissões mínimas necessárias para criar um índice na coleção livros, indexar alguns dados e pesquisá-los.

4. Escolha Criar.

Etapa 5: Criar uma coleção

Agora que você configurou as políticas de criptografia e rede, será possível criar uma coleção correspondente e as configurações de segurança serão aplicadas automaticamente a ela.

Para criar uma coleção OpenSearch sem servidor

1. Escolha Coleções no painel de navegação à esquerda e escolha Criar coleção.
2. Dê o nome de livros à coleção.

3. Para o tipo de coleção, escolha Pesquisar.
4. Em Criptografia, OpenSearch Serverless informa que o nome da coleção corresponde à política de criptografia. `books-policy`
5. Em Configurações de acesso à rede, o OpenSearch Serverless informa que o nome da coleção corresponde à `books-policy` política de rede.
6. Escolha Próximo.
7. Em Opções de política de acesso a dados, o OpenSearch Serverless informa que o nome da coleção corresponde à política de acesso a `books-policy` dados.
8. Escolha Próximo.
9. Reveja a configuração da coleção e escolha Enviar. Normalmente, as coleções levam menos de um minuto para serem inicializadas.

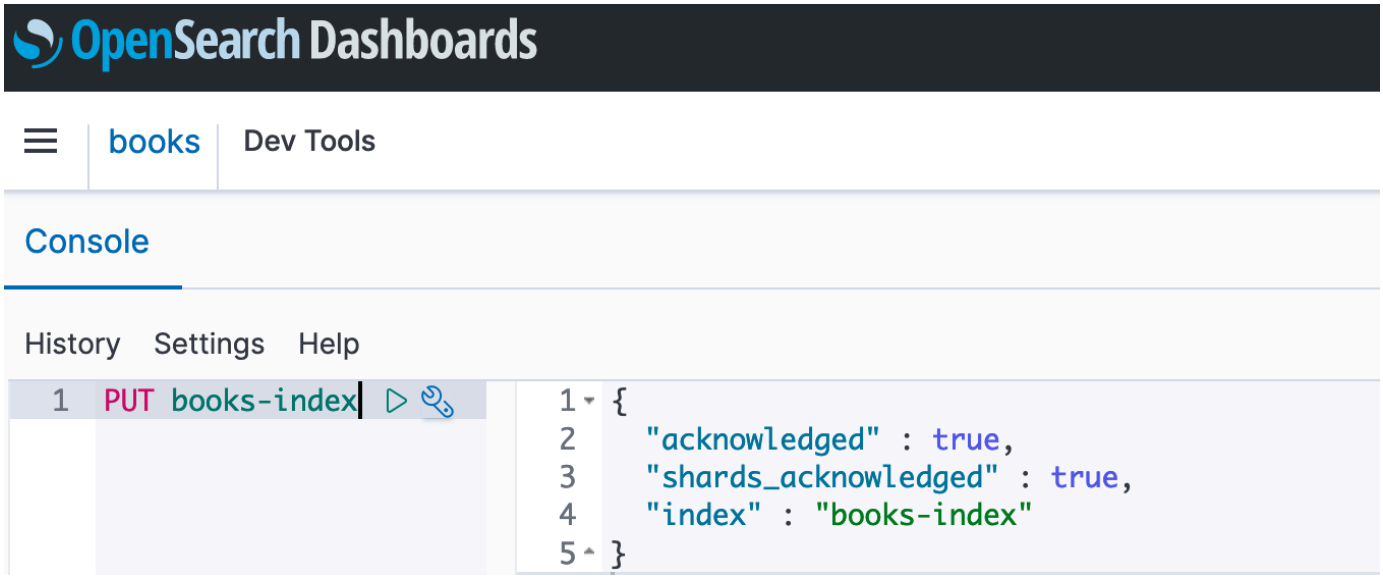
Etapa 6: transferir e pesquisar dados

Você pode carregar dados para uma coleção OpenSearch sem servidor usando Postman ou curl. Para resumir, esses exemplos usam Dev Tools no console OpenSearch Dashboards.

Para indexar e pesquisar dados em uma coleção

1. Escolha Coleções no painel de navegação à esquerda e escolha a coleção livros para abrir sua página de detalhes.
2. Escolha o URL dos OpenSearch painéis para a coleção. O URL assume o formato `https://collection-id.us-east-1.aoss.amazonaws.com/_dashboards`.
3. Faça login nos OpenSearch painéis usando as chaves de AWS acesso e secretas do principal que você especificou em sua política de acesso a dados.
4. Em OpenSearch Painéis, abra o menu de navegação à esquerda e escolha Ferramentas de desenvolvimento.
5. Para criar um único índice chamado books-index, execute o seguinte comando:

```
PUT books-index
```



6. Para indexar um único documento em books-index, execute o seguinte comando:

```
PUT books-index/_doc/1
{
  "title": "The Shining",
  "author": "Stephen King",
  "year": 1977
}
```

7. Para pesquisar dados em OpenSearch painéis, você precisa configurar pelo menos um padrão de índice. OpenSearch usa esses padrões para identificar quais índices você deseja analisar. Abra o menu principal do Dashboards, escolha Gerenciamento de pilhas, escolha Padrões de índice e, em seguida, escolha Criar padrão de índice. Para este tutorial, insira books-index.
8. Escolha Próxima etapa e, em seguida, Criar padrão de índice. Depois que o padrão é criado, você pode visualizar os vários campos do documento, como `author` e `title`.
9. Para começar a pesquisar seus dados, abra o menu principal novamente e escolha Descobrir, ou use a API de pesquisa.

Tutorial: Introdução à segurança no Amazon OpenSearch Serverless (CLI)

Este tutorial orienta você pelas etapas descritas no tutorial de introdução do console sobre segurança, mas usa o console AWS CLI em vez do OpenSearch Service console.

Você concluirá as seguintes etapas neste tutorial:

1. Crie uma política do IAM.
2. Anexar a política do IAM ao perfil do IAM
3. Criar uma política de criptografia
4. Criar uma política de rede
5. Criar uma coleção
6. Configurar uma política de acesso a dados
7. Recupere o endpoint da coleta
8. Faça upload de dados para sua conexão
9. Pesquise dados em sua coleção

O objetivo deste tutorial é configurar uma única coleção OpenSearch Serverless com configurações bastante simples de criptografia, rede e acesso a dados. Por exemplo, configuraremos o acesso pela rede pública, uma Chave gerenciada pela AWS para criptografia e uma política simplificada de acesso a dados que concede permissões mínimas a um único usuário.

Em um cenário de produção, considere implementar uma configuração mais robusta, incluindo autenticação SAML, uma chave de criptografia personalizada e acesso pela VPC.

Para começar a usar as políticas de segurança no OpenSearch Serverless

1. **Note**

   É possível pular esta etapa se já estiver usando uma política baseada em identidade mais ampla, como `Action":"aoss:*"` ou `Action":"*"`. Em ambientes de produção, no entanto, recomendamos que você siga o princípio do privilégio mínimo e atribua somente as permissões mínimas necessárias para concluir uma tarefa.

   Para iniciar, crie uma política AWS Identity and Access Management com as permissões mínimas necessárias para executar as etapas deste tutorial. Daremos o nome de `TutorialPolicy` à política:

   ```
   aws iam create-policy \
     --policy-name TutorialPolicy \
     --policy-document "{\"Version\": \"2012-10-17\",\"Statement\":
    [{\"Action\": [\"aoss:ListCollections\",\"aoss:BatchGetCollection\",
   ```

```
\"aoss:CreateCollection\",\"aoss:CreateSecurityPolicy\",\"aoss:GetSecurityPolicy\",
\"aoss:ListSecurityPolicies\",\"aoss:CreateAccessPolicy\",\"aoss:GetAccessPolicy\",
\"aoss:ListAccessPolicies\"],\"Effect\": \"Allow\",\"Resource\": \"*\"}]}"
```

Exemplo de resposta

```
{
    "Policy": {
        "PolicyName": "TutorialPolicy",
        "PolicyId": "ANPAW6WRAECKG6QJWUV7U",
        "Arn": "arn:aws:iam::123456789012:policy/TutorialPolicy",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 0,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "CreateDate": "2022-10-16T20:57:18+00:00",
        "UpdateDate": "2022-10-16T20:57:18+00:00"
    }
}
```

2. Anexe `TutorialPolicy` ao perfil do IAM que indexará e pesquisará dados na coleção. Daremos o nome de `TutorialRole` ao usuário:

```
aws iam attach-role-policy \
  --role-name TutorialRole \
  --policy-arn arn:aws:iam::123456789012:policy/TutorialPolicy
```

3. Antes de criar uma coleção, você precisa criar uma política de criptografia que atribua uma Chave pertencente à AWS à coleção livros que você criará em uma etapa posterior.

   Envie a seguinte solicitação para criar uma política de criptografia para a coleção livros:

```
aws opensearchserverless create-security-policy \
  --name books-policy \
  --type encryption --policy "{\"Rules\":[{\"ResourceType\":\"collection\",
\"Resource\":[\"collection\/books\"]}],\"AWSOwnedKey\":true}"
```

   Exemplo de resposta

```
{
```

```
    "securityPolicyDetail": {
        "type": "encryption",
        "name": "books-policy",
        "policyVersion": "MTY2OTI0MDAwNTk5MF8x",
        "policy": {
            "Rules": [
                {
                    "Resource": [
                        "collection/books"
                    ],
                    "ResourceType": "collection"
                }
            ],
            "AWSOwnedKey": true
        },
        "createdDate": 1669240005990,
        "lastModifiedDate": 1669240005990
    }
}
```

4. Crie uma política de rede que forneça acesso público à coleção livros:

```
aws opensearchserverless create-security-policy --name books-policy --type network
 \
  --policy "[{\"Description\":\"Public access for books collection\",\"Rules
\":[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection\/books\"]},
{\"ResourceType\":\"collection\",\"Resource\":[\"collection\/books\"]}],
\"AllowFromPublic\":true}]"
```

Exemplo de resposta

```
{
    "securityPolicyDetail": {
        "type": "network",
        "name": "books-policy",
        "policyVersion": "MTY2OTI0MDI1Njk1NV8x",
        "policy": [
            {
                "Rules": [
                    {
                        "Resource": [
                            "collection/books"
                        ],
```

```
                        "ResourceType": "dashboard"
                    },
                    {
                        "Resource": [
                            "collection/books"
                        ],
                        "ResourceType": "collection"
                    }
                ],
                "AllowFromPublic": true,
                "Description": "Public access for books collection"
            }
        ],
        "createdDate": 1669240256955,
        "lastModifiedDate": 1669240256955
    }
}
```

5. Crie a coleção livros:

```
aws opensearchserverless create-collection --name books --type SEARCH
```

Exemplo de resposta

```
{
    "createCollectionDetail": {
        "id": "8kw362bpwg4gx9b2f6e0",
        "name": "books",
        "status": "CREATING",
        "type": "SEARCH",
        "arn": "arn:aws:aoss:us-
east-1:123456789012:collection/8kw362bpwg4gx9b2f6e0",
        "kmsKeyArn": "auto",
        "createdDate": 1669240325037,
        "lastModifiedDate": 1669240325037
    }
}
```

6. Crie uma política de acesso a dados que forneça as permissões mínimas para indexar e pesquisar dados na coleção livros. Substitua o ARN da entidade principal pelo ARN do `TutorialRole` da etapa 1:

```
aws opensearchserverless create-access-policy \
  --name books-policy \
  --type data \
  --policy "[{\"Rules\":[{\"ResourceType\":\"index\",\"Resource\":
[\"index\/books\/books-index\"],\"Permission\":[\"aoss:CreateIndex
\",\"aoss:DescribeIndex\",\"aoss:ReadDocument\",\"aoss:WriteDocument
\",\"aoss:UpdateIndex\",\"aoss:DeleteIndex\"]}],\"Principal\":
[\"arn:aws:iam::123456789012:role\/TutorialRole\"]}]"
```

Exemplo de resposta

```
{
    "accessPolicyDetail": {
        "type": "data",
        "name": "books-policy",
        "policyVersion": "MTY2OTI0MDM5NDY1M18x",
        "policy": [
            {
                "Rules": [
                    {
                        "Resource": [
                            "index/books/books-index"
                        ],
                        "Permission": [
                            "aoss:CreateIndex",
                            "aoss:DescribeIndex",
                            "aoss:ReadDocument",
                            "aoss:WriteDocument",
                            "aoss:UpdateDocument",
                            "aoss:DeleteDocument"
                        ],
                        "ResourceType": "index"
                    }
                ],
                "Principal": [
                    "arn:aws:iam::123456789012:role/TutorialRole"
                ]
            }
        ],
        "createdDate": 1669240394653,
        "lastModifiedDate": 1669240394653
    }
```

```
}
```

O `TutorialRole` agora deve ser capaz de indexar e pesquisar documentos na coleção livros.

7. Para fazer chamadas para a OpenSearch API, você precisa do endpoint da coleção. Envie a seguinte solicitação para recuperar o parâmetro `collectionEndpoint`:

```
aws opensearchserverless batch-get-collection --names books
```

Exemplo de resposta

```
{
    "collectionDetails": [
        {
            "id": "8kw362bpwg4gx9b2f6e0",
            "name": "books",
            "status": "ACTIVE",
            "type": "SEARCH",
            "description": "",
            "arn": "arn:aws:aoss:us-
east-1:123456789012:collection/8kw362bpwg4gx9b2f6e0",
            "createdDate": 1665765327107,
            "collectionEndpoint": "https://8kw362bpwg4gx9b2f6e0.us-
east-1.aoss.amazonaws.com",
            "dashboardEndpoint": "https://8kw362bpwg4gx9b2f6e0.us-
east-1.aoss.amazonaws.com/_dashboards"
        }
    ],
    "collectionErrorDetails": []
}
```

> **Note**
>
> Não será possível ver o endpoint da coleção até que o status da coleção mude para `ACTIVE`. Talvez seja necessário fazer várias chamadas para verificar o status até que a coleção seja criada com êxito.

8. Use uma ferramenta HTTP, como o Postman ou curl, para indexar dados na coleção livros. Criaremos um índice chamado books-index e adicionaremos um único documento.

Envie a solicitação a seguir para o endpoint da coleção que você recuperou na etapa anterior, usando as credenciais do `TutorialRole`.

```
PUT https://8kw362bpwg4gx9b2f6e0.us-east-1.aoss.amazonaws.com/books-index/_doc/1
{
  "title": "The Shining",
  "author": "Stephen King",
  "year": 1977
}
```

Exemplo de resposta

```
{
  "_index" : "books-index",
  "_id" : "1",
  "_version" : 1,
  "result" : "created",
  "_shards" : {
    "total" : 0,
    "successful" : 0,
    "failed" : 0
  },
  "_seq_no" : 0,
  "_primary_term" : 0
}
```

9. Para começar a pesquisar dados em sua coleção, use a API de pesquisa. A consulta a seguir executa uma pesquisa básica:

```
GET https://8kw362bpwg4gx9b2f6e0.us-east-1.aoss.amazonaws.com/books-index/_search
```

Exemplo de resposta

```
{
    "took": 405,
    "timed_out": false,
    "_shards": {
        "total": 6,
        "successful": 6,
        "skipped": 0,
```

```
        "failed": 0
    },
    "hits": {
        "total": {
            "value": 2,
            "relation": "eq"
        },
        "max_score": 1.0,
        "hits": [
            {
                "_index": "books-index:0::3xJq14MBUaOS0wL26UU9:0",
                "_id": "F_bt4oMBLle5pYmm5q4T",
                "_score": 1.0,
                "_source": {
                    "title": "The Shining",
                    "author": "Stephen King",
                    "year": 1977
                }
            }
        ]
    }
}
```


Gerenciamento de identidade e acesso no Amazon OpenSearch Sem Servidor

O AWS Identity and Access Management (IAM) é um AWS service (Serviço da AWS) que ajuda o administrador a controlar o acesso aos recursos da AWS de forma segura. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (ter permissões) a usar os recursos do OpenSearch Sem Servidor. O IAM é um AWS service (Serviço da AWS) que pode ser usado sem custo adicional.

Tópicos

- Políticas baseadas em identidade para o OpenSearch Sem Servidor
- Ações de políticas para o OpenSearch Sem Servidor
- Recursos de políticas para o OpenSearch Sem Servidor
- Chaves de condição de política do Amazon OpenSearch Sem Servidor
- ABAC com o OpenSearch Sem Servidor

- Uso de credenciais temporárias com o OpenSearch Sem Servidor
- Funções vinculadas ao serviço do OpenSearch Sem Servidor
- Exemplos de políticas baseadas em identidade para o OpenSearch Sem Servidor

Políticas baseadas em identidade para o OpenSearch Sem Servidor

Suporta políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou atributos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou função à qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade para o OpenSearch Sem Servidor

Para exibir exemplos de políticas baseadas em identidade do OpenSearch Sem Servidor, consulte the section called “Exemplos de políticas baseadas em identidade”.

Ações de políticas para o OpenSearch Sem Servidor

Oferece suporte a ações de políticas	Sim

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome que a operação de API da AWS associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

As ações de políticas no OpenSearch Sem Servidor usam o seguinte prefixo antes da ação:

```
aoss
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
      "aoss:action1",
      "aoss:action2"
         ]
```

É possível especificar várias ações usando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Describe`, inclua a seguinte ação:

```
"Action": "aoss:List*"
```

Para exibir exemplos de políticas baseadas em identidade do OpenSearch Sem Servidor, consulte Exemplos de políticas baseadas em identidade para o OpenSearch Sem Servidor.

Recursos de políticas para o OpenSearch Sem Servidor

Oferece suporte a atributos de políticas	Sim

Os administradores podem usar as políticas de JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política `Resource` JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um atributo usando seu Nome do atributo da Amazon (ARN). Isso pode ser feito para ações que oferecem suporte a um tipo de atributo específico, conhecido como permissões em nível de atributo.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um caractere curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Chaves de condição de política do Amazon OpenSearch Sem Servidor

Suporta chaves de condição de política específicas de serviço	Sim

Os administradores podem usar as políticas de JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou `Condition` bloco de) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica `OR`. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode utilizar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos de política do IAM: variáveis e tags no Guia do usuário do IAM.

A AWS oferece suporte a chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as AWS chaves de condição globais da , consulte AWSChaves de contexto de condição globais da no Guia do usuário do IAM.

Além do controle de acesso por atributo (ABAC), o OpenSearch Sem Servidor oferece suporte às seguintes chaves de condição:

- `aoss:collection`
- `aoss:CollectionId`
- `aoss:index`

É possível usar essas chaves de condição mesmo ao fornecer permissões para políticas de acesso e políticas de segurança. Por exemplo:

```
[
   {
      "Effect":"Allow",
      "Action":[
         "aoss:CreateAccessPolicy",
         "aoss:CreateSecurityPolicy"
      ],
      "Resource":"*",
      "Condition":{
         "StringLike":{
            "aoss:collection":"log"
         }
      }
   }
]
```

Neste exemplo, a condição se aplica às políticas que contenham regras que correspondam a um nome ou padrão de coleção. As condições têm o seguinte comportamento:

- `StringEquals`: aplica-se a políticas com regras que contenham a string de recurso "log" exata (ou seja, `collection/log`).
- `StringLike`: aplica-se a políticas com regras que contenham uma string de recurso que inclua a string "log" (ou seja, `collection/log`, mas também `collection/logs-application` ou `collection/applogs123`).

> **Note**
>
> As chaves de condição coleção não se aplicam ao nível do índice. Por exemplo, na política acima, a condição não se aplicaria a uma política de acesso ou segurança contendo a string de recurso `index/logs-application/*`.

Para exibir uma lista de chaves de condição do OpenSearch Sem Servidor, consulte Chaves de condição do Amazon OpenSearch Sem Servidor na Referência de autorização do serviço. Para saber com quais ações e recursos é possível usar a chave de condição, consulte Ações definidas pelo Amazon OpenSearch Sem Servidor.

ABAC com o OpenSearch Sem Servidor

Oferece suporte a ABAC (tags em políticas)	Sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Na AWS, esses atributos são chamados de tags. É possível anexar tags a entidades do IAM (usuários ou perfis) e a muitos atributos da AWS. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do atributo que ela está tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys` chaves de condição.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial.

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Para obter mais informações sobre aplicação de tags em recursos do OpenSearch Sem Servidor, consulte the section called “Aplicação de tags nas coleções”.

Uso de credenciais temporárias com o OpenSearch Sem Servidor

Oferece suporte a credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Você está usando credenciais temporárias se faz login no AWS Management Console usando qualquer método, exceto um nome de usuário e uma senha. Por exemplo, quando você acessa a AWS usando o link de autenticação única (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar perfis, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

Você pode criar credenciais temporárias manualmente usando a AWS CLI ou a API da AWS. Em seguida, você pode usar essas credenciais temporárias para acessar aAWS .AWS A recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias no IAM.

Funções vinculadas ao serviço do OpenSearch Sem Servidor

Oferece suporte a perfis vinculados ao serviço	Sim

Um perfil vinculado ao serviço é um tipo de perfil de serviço vinculado a um AWS service (Serviço da AWS). O serviço pode presumir a função de executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode exibir, mas não pode editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar e gerenciar funções vinculadas ao serviço do OpenSearch Sem Servidor, consulte the section called “Função de criação de coleção”.

Exemplos de políticas baseadas em identidade para o OpenSearch Sem Servidor

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do OpenSearch Sem Servidor. Eles também não podem executar tarefas usando o AWS Management Console, a AWS Command Line Interface (AWS CLI) ou a API AWS. Para conceder aos usuários permissão para executar ações nos recursos de que precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis, e os usuários podem assumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo Amazon OpenSearch Sem Servidor, inclusive o formato dos ARNs para cada um dos tipos de recurso, consulte Ações, recursos

e chaves de condição do Amazon OpenSearch Sem Servidor na Referência de autorização do serviço.

Tópicos

- Melhores práticas de políticas
- Uso do OpenSearch Sem Servidor no console
- Administração de coleções do OpenSearch Sem Servidor
- Exibição de coleções do OpenSearch Sem Servidor
- Usar operações de API do OpenSearch

Melhores práticas de políticas

As políticas baseadas em identidade são muito eficientes. Elas determinam se alguém pode criar, acessar ou excluir recursos do OpenSearch Sem Servidor em sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do OpenSearch Sem Servidor na sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com AWS as políticas gerenciadas pela e avance para as permissões de privilégio mínimo: para começar a conceder permissões a seus usuários e workloads, use as AWS políticas gerenciadas pela que concedem permissões para muitos casos de uso comuns. Elas estão disponíveis na sua Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para perfis de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e atributos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando

SSL. Você também pode usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um AWS service (Serviço da AWS) específico, como o AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: Condition no Guia do usuário do IAM.

- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM.
- Exigir autenticação multifator (MFA): se houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

Uso do OpenSearch Sem Servidor no console

Para acessar o OpenSearch Sem Servidor no console do OpenSearch Service, é necessário ter um conjunto mínimo de permissões. Essas permissões dão autorização para que você liste e exiba detalhes sobre os recursos do OpenSearch Sem Servidor na sua conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (como perfis do IAM) com essa política.

Não é necessário conceder permissões mínimas do console para usuários que fazem chamadas somente à AWS CLI ou à API do AWS. Em vez disso, permita o acesso somente às ações que corresponderem a operação da API que você estiver tentando executar.

A política a seguir permite que um usuário acesse o OpenSearch Sem Servidor no console do OpenSearch Service:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
```

```
            "Effect": "Allow",
            "Action": [
                "aoss:ListCollections",
                "aoss:BatchGetCollection",
                "aoss:ListAccessPolicies",
                "aoss:ListSecurityConfigs",
                "aoss:ListSecurityPolicies",
                "aoss:ListTagsForResource",
                "aoss:ListVpcEndpoints",
                "aoss:GetAccessPolicy",
                "aoss:GetAccountSettings",
                "aoss:GetSecurityConfig",
                "aoss:GetSecurityPolicy"
            ]
        }
    ]
}
```

Administração de coleções do OpenSearch Sem Servidor

Esta política é um exemplo de política de “administração de coleções” que permite que um usuário gerencie e administre coleções do Amazon OpenSearch Sem Servidor. O usuário pode criar, exibir e excluir coleções.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "arn:aws:aoss:region:123456789012:collection/*",
            "Action": [
                "aoss:CreateCollection",
                "aoss:DeleteCollection",
                "aoss:UpdateCollection"
            ],
            "Effect": "Allow"
        },
        {
            "Resource": "*",
            "Action": [
                "aoss:BatchGetCollection",
                "aoss:ListCollections",
                "aoss:CreateAccessPolicy",
                "aoss:CreateSecurityPolicy"
```

```
            ],
            "Effect": "Allow"
        }
    ]
}
```

Exibição de coleções do OpenSearch Sem Servidor

Este exemplo de política permite que um usuário exiba detalhes de todas as coleções do Amazon OpenSearch Sem Servidor em sua conta. O usuário não pode modificar as coleções nem as políticas de segurança associadas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
            "Action": [
                "aoss:ListAccessPolicies",
                "aoss:ListCollections",
                "aoss:ListSecurityPolicies",
                "aoss:ListTagsForResource",
                "aoss:BatchGetCollection"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Usar operações de API do OpenSearch

As operações de API do plano de dados consistem nas funções que você usa no OpenSearch sem Servidor para obter valor em tempo real do serviço. As operações da API do plano de controle consistem nas funções que você usa para configurar o ambiente.

Para acessar as APIs do plano de dados do Amazon OpenSearch Sem Servidor e do OpenSearch Dashboards no navegador, você precisa adicionar duas permissões do IAM para recursos de coleções. Essas permissões são `aoss:APIAccessAll` e `aoss:DashboardsAccessAll`.

> **Note**
>
> A partir de 10 de maio de 2023, a tecnologia sem servidor do OpenSearch exige essas duas novas permissões do IAM para recursos de coleções. A `aoss:APIAccessAll` permissão permite o acesso ao plano de dados e a `aoss:DashboardsAccessAll` permissão permite o OpenSearch Dashboards a partir do navegador. A falha na adição das duas novas permissões do IAM resulta em um erro 403.

Este exemplo de política permite que um usuário acesse APIs do plano de dados de uma coleção específica em sua conta e acesse OpenSearch Dashboards para todas as coleções na sua conta.

```
{
    "Version": "2012-10-17",
    "Statement": [
         {
            "Effect": "Allow",
            "Action": "aoss:APIAccessAll",
            "Resource": "arn:aws:aoss:region:account-id:collection/collection-id"
        },
        {
            "Effect": "Allow",
            "Action": "aoss:DashboardsAccessAll",
            "Resource": "arn:aws:aoss:region:account-id:dashboards/default"
        }
    ]
}
```

Tanto `aoss:APIAccessAll` quanto `aoss:DashboardsAccessAll` fornecem permissão total do IAM aos recursos da coleção, enquanto a permissão para o Dashboards também fornece acesso ao OpenSearch Dashboards. Cada permissão funciona de forma independente, portanto, uma negação explícita de `aoss:APIAccessAll` não bloqueia o acesso aos recursos de `aoss:DashboardsAccessAll`, incluindo as Ferramentas de desenvolvimento. O mesmo vale para uma negativa de `aoss:DashboardsAccessAll`.

O tecnologia sem servidor do OpenSearch suporta apenas o endereço IP de origem na configuração de condição na política do IAM da entidade principal para chamadas de plano de dados:

```
"Condition": {
    "IpAddress": {
```

```
            "aws:SourceIp": "52.95.4.14"
        }
}
```

Criptografia no Amazon OpenSearch Sem Servidor

Criptografia em repouso

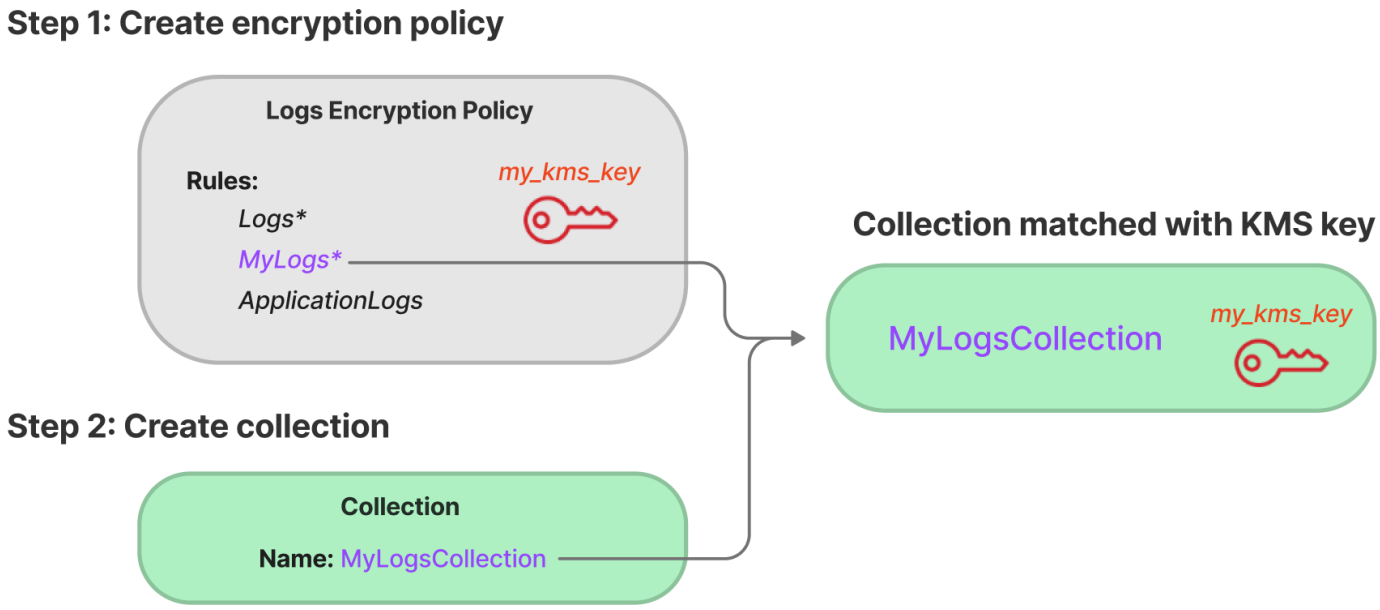
Cada coleção do Amazon OpenSearch Sem Servidor que você cria é protegida com criptografia de dados em repouso, um recurso de segurança que ajuda a impedir o acesso não autorizado aos seus dados. A criptografia em repouso usa AWS Key Management Service (AWS KMS) para armazenar e gerenciar suas chaves de criptografia. Ela usa o algoritmo Advanced Encryption Standard com chaves de 256 bits (AES-256) para executar a criptografia.

Tópicos

Políticas de criptografia

Com as políticas de criptografia, é possível gerenciar várias coleções em grande escala atribuindo automaticamente uma chave de criptografia às coleções recém-criadas que correspondam a um nome ou padrão específico.

Ao criar uma política de criptografia, é possível especificar um prefixo, que é uma regra de correspondência baseada em curingas, como `MyCollection*`, ou inserir um único nome de coleção. Em seguida, quando você criar uma coleção que corresponda a esse padrão de nome ou prefixo, a política e a chave do KMS correspondente serão automaticamente atribuídas a ela.



As políticas de criptografia contêm os seguintes elementos:

- `Rules`: uma ou mais regras de correspondência de coleções, cada uma com os seguintes subelementos:
  - `ResourceType`: no momento, a única opção é “collection” (coleção). As políticas de criptografia se aplicam somente aos recursos de coleção.
  - `Resource`: um ou mais nomes ou padrões de coleção aos quais a política será aplicada, no formato `collection/<collection name|pattern>`.
- `AWSOwnedKey`: opção de uso de uma Chave pertencente à AWS.
- `KmsARN`: se você definir `AWSOwnedKey` como falso, especifique o nome do recurso da Amazon (ARN) da chave do KMS com a qual criptografar as coleções associadas. Se você incluir esse parâmetro, o OpenSearch Sem Servidor ignorará o parâmetro `AWSOwnedKey`.

O exemplo de política a seguir atribuirá uma chave gerenciada pelo cliente a qualquer coleção futura denominada `autopartsinventory`, bem como às coleções que comecem com o termo “sales” (vendas):

```
{
   "Rules":[
      {
         "ResourceType":"collection",
         "Resource":[
```

```
            "collection/autopartsinventory",
            "collection/sales*"
         ]
      }
   ],
   "AWSOwnedKey":false,
   "KmsARN":"arn:aws:encryption:us-east-1:123456789012:key/93fd6da4-a317-4c17-
bfe9-382b5d988b36"
}
```

Mesmo que uma política corresponda a um nome de coleção, é possível optar por substituir essa atribuição automática durante a criação da coleção se o padrão do recurso contiver um caractere curinga (*). Se você optar por substituir a atribuição automática de chaves, o OpenSearch Sem Servidor criará uma política de criptografia para você chamada auto-**<*nome-da-coleção*>** e a anexará à coleção. Inicialmente, a política só se aplica a uma única coleção, mas é possível modificá-la para incluir coleções adicionais.

Se você modificar as regras de política para que não correspondam mais a uma coleção, a chave do KMS associada não terá a atribuição a essa coleção cancelada. A coleção permanece sempre criptografada com sua chave de criptografia inicial. Se você desejar alterar a chave de criptografia de uma coleção, deverá recriar a coleção.

Se as regras de várias políticas corresponderem a uma coleção, a regra mais específica será usada. Por exemplo, se uma política contiver uma regra para `collection/log*` e outra para `collection/logSpecial`, a chave de criptografia da segunda política será usada porque é mais específica.

Você não pode usar um nome ou um prefixo em uma política se ele já existir em outra política. O OpenSearch Sem Servidor exibirá um erro se você tentar configurar padrões de recursos idênticos em políticas de criptografia diferentes.

Considerações

Considere o seguinte ao configurar a criptografia de suas coleções:

- A criptografia em repouso é obrigatória para todas as coleções do Sem Servidor.
- Você tem a opção de usar uma chave gerenciada pelo cliente ou uma Chave pertencente à AWS. Se você escolher uma chave gerenciada pelo cliente, recomendamos habilitar a rotação automática de chaves.

- Não é possível alterar a chave de criptografia de uma coleção depois que a coleção é criada. Escolha com cuidado qual AWS KMS usar na primeira vez que configurar uma coleção.
- Uma coleção só pode corresponder a uma única política de criptografia.
- Coleções com chaves do KMS exclusivas não podem compartilhar unidades de computação (OCUs) do OpenSearch com outras coleções. Cada coleção com uma chave exclusiva requer suas próprias 4 OCUs.
- Se você atualizar a chave do KMS em uma política de criptografia, a alteração não afetará as coleções correspondentes existentes com as chaves do KMS já atribuídas.
- O OpenSearch Sem Servidor não verifica explicitamente as permissões do usuário nas chaves gerenciadas pelo cliente. Se um usuário tiver permissões para acessar uma coleção por meio de uma política de acesso a dados, ele poderá ingerir e consultar os dados criptografados com a chave associada.

Permissões obrigatórias

A criptografia em repouso do OpenSearch Sem Servidor usa as seguintes permissões do AWS Identity and Access Management (IAM). É possível especificar as condições do IAM para restringir os usuários a coleções específicas.

- `aoss:CreateSecurityPolicy`: cria uma política de criptografia.
- `aoss:ListSecurityPolicies`: lista todas as políticas e coleções de criptografia às quais elas estão vinculadas.
- `aoss:GetSecurityPolicy`: exibe os detalhes de uma política de criptografia específica.
- `aoss:UpdateSecurityPolicy`: modifica uma política de criptografia.
- `aoss:DeleteSecurityPolicy`: exclui uma política de criptografia.

O exemplo a seguir de política de acesso baseada em identidade fornece as permissões mínimas necessárias para que um usuário gerencie políticas de criptografia com o padrão de recursos `collection/application-logs`.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
```

```
            "aoss:CreateSecurityPolicy",
            "aoss:UpdateSecurityPolicy",
            "aoss:DeleteSecurityPolicy",
            "aoss:GetSecurityPolicy"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aoss:collection":"application-logs"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "aoss:ListSecurityPolicies"
         ],
         "Resource":"*"
      }
   ]
}
```

Política de chaves para uma chave gerenciada pelo cliente

Se você selecionar uma chave gerenciada pelo cliente para proteger uma coleção, o OpenSearch Sem Servidor obterá permissão para usar a chave do KMS em nome da entidade principal que fizer a seleção. Essa entidade principal, um usuário ou um perfil, deve ter as permissões em uma chave do KMS solicitada pelo OpenSearch Sem Servidor. É possível fornecer essas permissões em uma política de chaves ou em uma política do IAM.

No mínimo, oOpenSearch Sem Servidor exige as seguintes permissões em uma chave gerenciada pelo cliente:

- kms:DescribeKey
- kms:CreateGrant
- kms:ListKeys

Por exemplo:

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:ListKeys"
      ],
      "Resource": "*"
    },
{
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:CreateGrant"
      ],
      "Resource": "{kms-key-arn}"
    }
  ]
}
```

O OpenSearch Sem Servidor cria uma concessão com as permissões kms:GenerateDataKey e kms:Decrypt.

Se você quiser manter sua chave exclusiva no OpenSearch Sem Servidor, poderá adicionar a condição kms:ViaService à política principal:

```
"Condition": {
  "StringEquals": {
    "kms:ViaService": "aoss.us-east-1.amazonaws.com"
  },
  "Bool": {
    "kms:GrantIsForAWSResource": "true"
  }
}
```

Para obter mais informações, consulte Uso de políticas de chaves no AWS KMS no Guia do desenvolvedor do AWS Key Management Service.

Como o OpenSearch Sem Servidor usa concessões no AWS KMS

O OpenSearch Sem Servidor exige uma concessão para usar uma chave gerenciada pelo cliente.

Quando você cria uma política de criptografia em sua conta com uma nova chave, o OpenSearch Sem Servidor cria uma concessão em seu nome enviando uma solicitação CreateGrant para AWS

KMS. As concessões no AWS KMS são usadas para dar ao OpenSearch Sem Servidor acesso a uma chave do KMS em uma conta de cliente.

O OpenSearch Sem Servidor exige a concessão para usar sua chave gerenciada pelo cliente para as seguintes operações internas:

- Enviar solicitações DescribeKey para AWS KMS para verificar se o ID de chave simétrico gerenciado pelo cliente fornecido é válido.
- Enviar solicitações GenerateDataKey para a chave do KMS para criar chaves de dados com as quais criptografar objetos.
- Enviar solicitações Decrypt para AWS KMS para descriptografar as chaves de dados criptografadas para que elas possam ser usadas para criptografar seus dados.

É possível revogar o acesso à concessão, ou remover o acesso do serviço à chave gerenciada pelo cliente a qualquer momento. Se você fizer isso, o OpenSearch Sem Servidor não poderá acessar nenhum dos dados criptografados pela chave gerenciada pelo cliente, o que afetará todas as operações que dependam desses dados, causando erros `AccessDeniedException` e falhas nos fluxos de trabalho assíncronos.

O OpenSearch Sem Servidor retira concessões em um fluxo de trabalho assíncrono quando uma determinada chave gerenciada pelo cliente não está associada a nenhuma política ou coleção de segurança.

Criação de políticas de criptografia (console)

Em uma política de criptografia, você especifica uma chave do KMS e uma série de padrões de coleção aos quais a política se aplicará. Qualquer nova coleção que corresponda a um dos padrões definidos na política receberá a chave do KMS correspondente quando você criar a coleção. Recomendamos que você crie políticas de criptografia antes de começar a criar coleções.

Para criar uma política de criptografia do OpenSearch Sem Servidor

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. No painel de navegação à esquerda, expanda Sem Servidor e escolha Políticas de criptografia.
3. Escolha Criar política de criptografia.
4. Forneça um nome e uma descrição para a política.
5. Em Recursos, insira um ou mais padrões de recursos para essa política de criptografia. Todas as coleções recém-criadas na Conta da AWS e região atual que correspondam a um

dos padrões serão automaticamente atribuídas a essa política. Por exemplo, se você inserir `ApplicationLogs` (sem nenhum curinga) e depois criar uma coleção com esse nome, a política e a chave do KMS correspondente serão atribuídas a essa coleção.

Você também pode fornecer um prefixo como `Logs*`, que atribuirá a política a qualquer nova coleção com nomes começando com `Logs`. Usando curingas, é possível gerenciar as configurações de criptografia para várias coleções em grande escala.

6. Em Criptografia, escolha uma chave do KMS para usar.
7. Escolha Criar.

Próxima etapa: criar coleções

Depois de configurar uma ou mais políticas de criptografia, será possível começar a criar coleções que correspondam às regras definidas nessas políticas. Para obter instruções, consulte the section called “Criação de coleções”.

Na etapa Criptografias da criação da coleção, o OpenSearch Sem Servidor informa que o nome inserido corresponde ao padrão definido em uma política de criptografia e atribui automaticamente a chave do KMS correspondente à coleção. Se o padrão do recurso contiver um curinga (*), será possível optar por substituir a correspondência e selecionar sua própria chave.

Criação de políticas de criptografia (AWS CLI)

Para criar uma política de criptografia usando as operações da API do OpenSearch Sem Servidor, você especifica padrões de recursos e uma chave de criptografia no formato JSON. A solicitação CreateSecurityPolicy aceita tanto políticas em linha quanto arquivos .json.

As políticas de criptografia têm o formato a seguir. Esse arquivo `my-policy.json` de exemplo corresponde a qualquer coleção futura denominada `autopartsinventory`, bem como a qualquer coleção com nomes iniciando por `sales`.

```
{
   "Rules":[
      {
         "ResourceType":"collection",
         "Resource":[
            "collection/autopartsinventory",
            "collection/sales*"
         ]
```

```
      }
   ],
   "AWSOwnedKey":false,
   "KmsARN":"arn:aws:encryption:us-east-1:123456789012:key/93fd6da4-a317-4c17-
bfe9-382b5d988b36"
}
```

Para usar uma chave de propriedade do serviço, defina `AWSOwnedKey` como `true`:

```
{
   "Rules":[
      {
         "ResourceType":"collection",
         "Resource":[
            "collection/autopartsinventory",
            "collection/sales*"
         ]
      }
   ],
   "AWSOwnedKey":true
}
```

A solicitação a seguir cria a política de criptografia:

```
aws opensearchserverless create-security-policy \
    --name sales-inventory \
    --type encryption \
    --policy file://my-policy.json
```

Em seguida, use a operação da API CreateCollection para criar uma ou mais coleções que correspondam a um dos padrões de recursos.

Exibição de políticas de criptografia

Antes de criar uma coleção, talvez você queira pré-visualizar as políticas de criptografia existentes em sua conta para ver qual delas tem um padrão de recurso que corresponda ao nome da sua coleção. A solicitação ListSecurityPolicies a seguir lista todas as políticas de criptografia em sua conta:

```
aws opensearchserverless list-security-policies --type encryption
```

A solicitação retorna informações sobre todas as políticas de criptografia configuradas. Use o conteúdo do elemento `policy` para visualizar as regras de padrões definidas na política:

```
{
   "securityPolicyDetails": [
      {
         "createdDate": 1663693217826,
         "description": "Sample encryption policy",
         "lastModifiedDate": 1663693217826,
         "name": "my-policy",
         "policy": "{\"Rules\":[{\"ResourceType\":\"collection\",\"Resource\":
[\"collection/autopartsinventory\",\"collection/sales*\"]}],\"AWSOwnedKey\":true}",
         "policyVersion": "MTY2MzY5MzIxNzgyNl8x",
         "type": "encryption"
      }
   ]
}
```

Para exibir informações detalhadas sobre uma política específica, incluindo a chave do KMS, use o comando GetSecurityPolicy.

Atualização de políticas de criptografia

Se você atualizar a chave do KMS em uma política de criptografia, a alteração só se aplicará às coleções recém-criadas que correspondam ao nome ou padrão configurado. Isso não afeta as coleções existentes que já tenham chaves do KMS atribuídas.

O mesmo se aplica às regras de correspondência das políticas. Se você adicionar, modificar ou excluir uma regra, a alteração só se aplicará às coleções recém-criadas. As coleções existentes não perdem suas chaves do KMS atribuídas se você modificar as regras de uma política para que ela não corresponda mais ao nome de uma coleção.

Para atualizar uma política de criptografia no console do OpenSearch Sem Servidor, escolha Políticas de criptografia, selecione a política a ser modificada e escolha Editar. Faça suas alterações e escolha Salvar.

Para atualizar uma política de criptografia usando a API do OpenSearch Sem Servidor, use a operação UpdateSecurityPolicy. A solicitação a seguir atualiza uma política de criptografia com um novo documento JSON de política:

```
aws opensearchserverless update-security-policy \
```

```
    --name sales-inventory \
    --type encryption \
    --policy-version 2 \
    --policy file://my-new-policy.json
```

Exclusão de políticas de criptografia

Quando você exclui uma política de criptografia, todas as coleções que estiverem usando a chave do KMS definida na política não são afetadas. Para excluir uma política no console da tecnologia sem servidor do OpenSearch, selecione a política e escolha Excluir.

Você também pode usar a operação DeleteSecurityPolicy:

```
aws opensearchserverless delete-security-policy --name my-policy --type encryption
```

Criptografia em trânsito

Na tecnologia sem servidor do OpenSearch, todos os caminhos em uma coleção são criptografados em trânsito usando o Transport Layer Security 1.2 (TLS) com uma cifra AES-256 padrão do setor. O acesso a todas as APIs e OpenSearch Dashboards também é feito por meio do TLS 1.2. O TLS é um conjunto de protocolos criptográficos padrão do setor usados para criptografar informações que são trocadas pela rede.

Acesso à rede para Amazon OpenSearch Serverless

As configurações de rede de uma coleção Amazon OpenSearch Serverless determinam se a coleção pode ser acessada pela Internet a partir de redes públicas ou se deve ser acessada de forma privada.

O acesso privado pode ser aplicado a um ou aos dois itens a seguir:

- OpenSearch VPC endpoints gerenciados sem servidor
- Compatível Serviços da AWS , como Amazon Bedrock

Você pode configurar o acesso à rede separadamente para o endpoint de uma coleção e o OpenSearchendpoint correspondente do OpenSearch Dashboards.

O acesso à rede é o mecanismo de isolamento para permitir o acesso de diferentes redes de origem. Por exemplo, se o endpoint de OpenSearch painéis de uma coleção estiver acessível publicamente,

mas o endpoint da OpenSearch API não, um usuário poderá acessar os dados da coleção somente por meio de painéis ao se conectar a partir de uma rede pública. Se eles tentarem chamar as OpenSearch APIs diretamente de uma rede pública, eles serão bloqueados. As configurações de rede podem ser usadas para essas permutações de origem para tipo de recurso.

Tópicos

Políticas de rede

As políticas de rede permitem que você gerencie várias coleções em escala, atribuindo automaticamente configurações de acesso à rede a coleções que correspondam às regras definidas na política.

Em uma política de rede, você especifica uma série de regras. Essas regras definem as permissões de acesso aos endpoints da coleção e aos endpoints do OpenSearch Dashboards. Cada regra consiste em um tipo de acesso (público ou privado) e um tipo de recurso (coleção e/ou endpoint de OpenSearch painéis). Para cada tipo de recurso (`collection` e `dashboard`), você especifica uma série de regras que definem a quais coleções a política se aplicará.

Neste exemplo de política, a primeira regra especifica o acesso do VPC endpoint ao endpoint da coleção e ao endpoint do Dashboards para todas as coleções que começam com o termo. `marketing*` Também especifica o acesso ao Amazon Bedrock.

> **Note**
>
> O acesso privado Serviços da AWS , como o Amazon Bedrock, só se aplica ao endpoint da coleção, não ao OpenSearch endpoint do OpenSearch Dashboards. Mesmo que

`ResourceType` sejadashboard, Serviços da AWS não é possível conceder acesso aos OpenSearch painéis.

A segunda regra especifica o acesso público à coleção `finance`, mas somente para o endpoint da coleção (sem acesso ao Dashboards).

```
[
   {
      "Description":"Marketing access",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/marketing*"
            ]
         },
         {
            "ResourceType":"dashboard",
            "Resource":[
               "collection/marketing*"
            ]
         }
      ],
      "AllowFromPublic":false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ],
      "SourceServices":[
         "bedrock.amazonaws.com"
      ],
   },
   {
      "Description":"Sales access",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":true
```

```
    }
]
```

Essa política fornece acesso público somente aos OpenSearch painéis para coleções que começam com “finanças”. Qualquer tentativa de acessar diretamente a OpenSearch API falhará.

```
[
  {
    "Description": "Dashboards access",
    "Rules": [
      {
        "ResourceType": "dashboard",
        "Resource": [
          "collection/finance*"
        ]
      }
    ],
    "AllowFromPublic": true
  }
]
```

As políticas de rede podem ser aplicadas tanto às coleções existentes quanto às futuras. Por exemplo, é possível criar uma coleção e depois criar uma política de rede com uma regra que corresponda ao nome da coleção. Não é necessário criar políticas de rede para criar coleções.

Considerações

Considere o seguinte ao configurar o acesso de rede para suas coleções:

- Se você planeja configurar o acesso ao VPC endpoint para uma coleção, primeiro deve criar pelo menos um VPC endpoint gerenciado sem servidorOpenSearch .
- O acesso privado Serviços da AWS só se aplica ao endpoint da coleção, não ao OpenSearch endpoint do OpenSearch Dashboards. Mesmo que `ResourceType` sejadashboard, Serviços da AWS não é possível conceder acesso aos OpenSearch painéis.
- Se uma coleção for acessível a partir de redes públicas, ela também poderá ser acessada por todos os VPC endpoints OpenSearch gerenciados sem servidor e tudo mais. Serviços da AWS
- Várias políticas de rede podem ser aplicadas a uma única coleção. Para ter mais informações, consulte the section called “Precedência das políticas”.

Permissões obrigatórias

O acesso à rede para OpenSearch Serverless usa as seguintes permissões AWS Identity and Access Management (IAM). É possível especificar as condições do IAM para restringir os usuários a políticas de rede associadas a coleções específicas.

- `aoss:CreateSecurityPolicy`: crie uma política de acesso à rede.
- `aoss:ListSecurityPolicies`: lista todas as políticas de rede na conta atual.
- `aoss:GetSecurityPolicy`: exibe uma especificação de política de acesso à rede.
- `aoss:UpdateSecurityPolicy`: modifica uma determinada política de acesso à rede e altera o ID da VPC ou a designação de acesso público.
- `aoss:DeleteSecurityPolicy`: exclui uma política de acesso à rede (depois que ela for separada de todas as coleções).

A política de acesso baseada em identidade a seguir permite que um usuário exiba todas as políticas de rede e atualize as políticas com o padrão de recursos `collection/application-logs`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aoss:UpdateSecurityPolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:collection": "application-logs"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "aoss:ListSecurityPolicies",
                "aoss:GetSecurityPolicy"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Precedência das políticas

Pode haver situações em que as regras das políticas de rede se sobreponham, dentro ou entre as políticas. Quando isso acontece, uma regra que especifica o acesso público substitui uma regra que especifica o acesso privado para qualquer coleção que seja comum às duas regras.

Por exemplo, na política a seguir, ambas as regras atribuem acesso de rede à coleção `finance`, mas uma regra especifica o acesso por VPC enquanto a outra especifica o acesso público. Nessa situação, o acesso público substitui o acesso por VPC somente para a coleção finance (porque ele existe em ambas as regras), de modo que a coleção finance será acessível a partir de redes públicas. A coleção de vendas terá acesso por VPC a partir do endpoint especificado.

```
[
   {
      "Description":"Rule 1",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/sales",
               "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ]
   },
   {
      "Description":"Rule 2",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/finance"
            ]
         }
      ],
```

```
      "AllowFromPublic":true
   }
]
```

Se vários endpoints da VPC de regras diferentes se aplicarem a uma coleção, as regras serão aditivas e a coleção poderá ser acessada de todos os endpoints especificados. Se você definir `AllowFromPublictrue`, mas também fornecer um ou mais `SourceVPCEs` ou`SourceServices`, o OpenSearch Serverless ignorará os endpoints de VPC e os identificadores de serviço, e as coleções associadas terão acesso público.

Criação de políticas de rede (console)

As políticas de rede podem ser aplicadas tanto às políticas existentes quanto às políticas futuras. Recomendamos que você crie políticas de rede antes de começar a criar coleções.

Para criar uma política de rede OpenSearch sem servidor

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. No painel de navegação à esquerda, expanda Sem Servidor e escolha Políticas de rede.
3. Escolha Criar política de rede.
4. Forneça um nome e uma descrição para a política.
5. Forneça uma ou mais regras. Essas regras definem permissões de acesso para suas coleções OpenSearch sem servidor e seus endpoints de OpenSearch painéis.

   Cada regra contém os seguintes elementos:

Elemento	Descrição
Nome da regra	Um nome que descreve o conteúdo da regra. Por exemplo, “Acesso por VPC para a equipe de marketing”.
Tipo de acesso	Escolha entre acesso público ou privado. Em seguida, selecione uma ou as duas opções a seguir: • VPC endpoints para acesso — especifiq ue um ou mais VPC endpoints gerenciad

Elemento	Descrição
	os sem servidor — OpenSearch VPC endpoints gerenciados. • AWS service (Serviço da AWS) acesso privado — Selecione um ou mais compatíveis Serviços da AWS.
Tipo de atributo	Selecione se deseja fornecer acesso aos OpenSearch endpoints (o que permite fazer chamadas para a OpenSearch API), aos OpenSearch painéis (que permitem o acesso às visualizações e à interface do usuário para OpenSearch plug-ins) ou ambos. **Note** AWS service (Serviço da AWS) o acesso privado só se aplica ao endpoint da coleção, não ao OpenSearch endpoint do OpenSearch Dashboards. Mesmo se você selecionar OpenSearch Painéis, só Serviços da AWS poderá receber acesso ao endpoint.

Para cada tipo de recurso selecionado, é possível escolher coleções existentes para aplicar as configurações de política e/ou criar um ou mais padrões de recursos. Os padrões de recursos consistem em um prefixo e um caractere curinga (*), e definem a quais coleções as configurações de política se aplicarão.

Por exemplo, se você incluir um padrão chamado `Marketing*`, qualquer coleção nova ou existente cujos nomes comecem com “Marketing” terá as configurações de rede desta política aplicadas automaticamente a elas. Um único caractere curinga (`*`) aplica a política a todas as coleções atuais e futuras.

Além disso, você pode especificar o nome de uma coleção futura sem um caractere curinga, como`Finance`. OpenSearch O Serverless aplicará as configurações de política a qualquer coleção recém-criada com esse nome exato.

6. Quando estiver satisfeito com sua configuração de política, escolha Criar.

Criação de políticas de rede (AWS CLI)

Para criar uma política de rede usando as operações da API OpenSearch Serverless, você especifica regras no formato JSON. A CreateSecurityPolicysolicitação aceita políticas embutidas e arquivos.json. Todas as coleções e padrões devem assumir o formato `collection/<collection name|pattern>`.

> **Note**
>
> O tipo de recurso `dashboards` só permite a permissão para OpenSearch painéis, mas para que os OpenSearch painéis funcionem, você também deve permitir o acesso à coleção das mesmas fontes. Veja a segunda política a seguir como um exemplo.

Para especificar o acesso privado, inclua um ou os dois elementos a seguir:

- `SourceVPCEs`— Especifique um ou mais VPC endpoints OpenSearch gerenciados sem servidor.
- `SourceServices`— Especifique o identificador de um ou mais compatíveis Serviços da AWS. Atualmente, os seguintes identificadores de serviço são compatíveis:
  - `bedrock.amazonaws.com`— Amazon Bedrock

O exemplo de política de rede a seguir fornece acesso privado, a um VPC endpoint e ao Amazon Bedrock, a endpoints de coleta somente para coleções que começam com o prefixo. `log*` Usuários autenticados não podem entrar nos OpenSearch painéis; eles só podem acessar o endpoint de coleta de forma programática.

```
[
   {
      "Description":"Private access for log collections",
      "Rules":[
         {
            "ResourceType":"collection",
```

```
            "Resource":[
               "collection/log*"
            ]
         }
      ],
      "AllowFromPublic":false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ],
      "SourceServices":[
         "bedrock.amazonaws.com"
      ],
   }
]
```

A política a seguir fornece acesso público ao OpenSearch endpoint e aos OpenSearch painéis para uma única coleção chamada. `finance` Se a coleção não existir, as configurações de rede serão aplicadas à coleção se e quando ela for criada.

```
[
   {
      "Description":"Public access for finance collection",
      "Rules":[
         {
            "ResourceType":"dashboard",
            "Resource":[
               "collection/finance"
            ]
         },
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":true
   }
]
```

A solicitação a seguir cria a política de rede acima:

```
aws opensearchserverless create-security-policy \
```

```
    --name sales-inventory \
    --type network \
    --policy "[{\"Description\":\"Public access for finance collection\",\"Rules
\":[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection\/finance\"]},
{\"ResourceType\":\"collection\",\"Resource\":[\"collection\/finance\"]}],
\"AllowFromPublic\":true}]"
```

Para fornecer a política em um arquivo JSON, use o formato `--policy file://my-policy.json`

Exibição de políticas de rede

Antes de criar uma coleção, talvez você queira pré-visualizar as políticas de rede existentes em sua conta para ver qual delas tem um padrão de recurso que corresponda ao nome da sua coleção. A ListSecurityPoliciessolicitação a seguir lista todas as políticas de rede em sua conta:

```
aws opensearchserverless list-security-policies --type network
```

A solicitação retorna informações sobre todas as políticas de rede configuradas. Para visualizar as regras de padrões definidas em uma política específica, encontre as informações sobre políticas no conteúdo do elemento `securityPolicySummaries` na resposta. Observe o `name` final `type` desta política e use essas propriedades em uma GetSecurityPolicysolicitação para receber uma resposta com os seguintes detalhes da política:

```
{
    "securityPolicyDetail": [
        {
            "type": "network",
            "name": "my-policy",
            "policyVersion": "MTY2MzY5MTY1MDA3Ml8x",
            "policy": "[{\"Description\":\"My network policy rule\",\"Rules\":
[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection/*\"]}],\"AllowFromPublic
\":true}]",
            "createdDate": 1663691650072,
            "lastModifiedDate": 1663691650072
        }
    ]
}
```

Para ver informações detalhadas sobre uma política específica, use o GetSecurityPolicycomando.

Atualização de políticas de rede

Quando você modifica os endpoints da VPC ou a designação de acesso público para uma rede, todas as coleções associadas são afetadas. Para atualizar uma política de rede no console OpenSearch sem servidor, expanda Políticas de rede, selecione a política a ser modificada e escolha Editar. Faça suas alterações e escolha Salvar.

Para atualizar uma política de rede usando a API OpenSearch Serverless, use o UpdateSecurityPolicycomando. É necessário incluir uma versão da política na solicitação. É possível recuperar a versão da política usando os comandos `ListSecurityPolicies` ou `GetSecurityPolicy`. A inclusão da versão mais recente da política garante que você não anule inadvertidamente uma alteração feita por outra pessoa.

A solicitação a seguir atualiza uma política de rede com um novo documento JSON de política:

```
aws opensearchserverless update-security-policy \
    --name sales-inventory \
    --type network \
    --policy-version MTY2MzY5MTY1MDA3Ml8x \
    --policy file://my-new-policy.json
```

Exclusão de políticas de rede

Antes de ser possível excluir uma política de rede, é preciso desvinculá-la de todas as coleções. Para excluir uma política no console OpenSearch sem servidor, selecione a política e escolha Excluir.

Você também pode usar o DeleteSecurityPolicycomando:

```
aws opensearchserverless delete-security-policy --name my-policy --type network
```

Controle de acesso a dados do Amazon OpenSearch Sem Servidor

Com o controle de acesso a dados no Amazon OpenSearch Sem Servidor, é possível permitir que os usuários acessem coleções e índices, independentemente do mecanismo de acesso ou da origem de rede. É possível fornecer acesso a perfis do IAM e identidades de SAML.

Você gerencia as permissões de acesso por meio de políticas de acesso a dados que se aplicam às coleções e aos recursos de índice. As políticas de acesso a dados ajudam você a gerenciar coleções em grande escala atribuindo automaticamente permissões de acesso a coleções e índices que

correspondam a um padrão específico. Várias políticas de acesso a dados podem ser aplicadas a um único recurso. Observe que você deve ter uma política de acesso a dados para sua coleção para acessar o URL do OpenSearch Dashboards.

Tópicos

Políticas de acesso a dados versus políticas do IAM

As políticas de acesso a dados são logicamente separadas das políticas do AWS Identity and Access Management (IAM). As permissões do IAM controlam o acesso às operações da API do Sem Servidor, como `CreateCollection` e `ListAccessPolicies`. As políticas de acesso a dados controlam o acesso às operações do OpenSearch com suporte pelo OpenSearch Sem Servidor, como PUT `<index>` ou `GET _cat/indices`.

As permissões do IAM que controlam o acesso às operações da API da política de acesso a dados, como `aoss:CreateAccessPolicy` e `aoss:GetAccessPolicy` (descritas na próxima seção), não afetam a permissão especificada em uma política de acesso a dados.

Por exemplo, suponha que uma política do IAM impeça que um usuário crie políticas de acesso a dados para `collection-a`, mas permita que ele crie políticas de acesso a dados para todas as coleções (*):

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
```

```
            "Action": [
                "aoss:CreateAccessPolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aoss:collection": "collection-a"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "aoss:CreateAccessPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Se o usuário criar uma política de acesso a dados que permita certa permissão para todas as coleções (`collection/*` ou `index/*/*`), a política será aplicada a todas as coleções, incluindo a coleção A.

> **Important**
>
> Receber permissões em uma política de acesso a dados não é suficiente para acessar dados na sua coleção do OpenSearch sem Servidor. Uma entidade principal associada também deve ter acesso às permissões do IAM `aoss:APIAccessAll` e `aoss:DashboardAccessAll`. Ambas as permissões concedem acesso total aos recursos da coleção, enquanto a permissão do Dashboards também fornece acesso ao OpenSearch Dashboards. Se uma entidade principal não tiver essas duas permissões do IAM, receberá erros 403 ao tentar enviar solicitações para a coleção. Para obter mais informações, consulte the section called “Usar operações de API do OpenSearch”.

Permissões do IAM necessárias

O controle de acesso a dados para o OpenSearch Sem Servidor usa as permissões do IAM a seguir. É possível especificar condições do IAM para restringir os usuários a nomes de políticas de acesso específicas.

- `aoss:CreateAccessPolicy`: criar uma política de acesso.
- `aoss:ListAccessPolicies`: listar todas as políticas de acesso.
- `aoss:GetAccessPolicy`: exibir detalhes sobre uma política de acesso específica.
- `aoss:UpdateAccessPolicy`: modificar uma política de acesso.
- `aoss:DeleteAccessPolicy`: excluir uma política de acesso.

A seguinte política de acesso baseada em identidade permite que um usuário exiba todas as políticas de acesso e atualize as políticas que contenham o padrão de recursos `collection/logs`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aoss:ListAccessPolicies",
                "aoss:GetAccessPolicy"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "aoss:UpdateAccessPolicy"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:collection": [
                        "logs"
                    ]
                }
            }
        }
    ]
}
```

Sintaxe da política

Uma política de acesso a dados inclui um conjunto de regras, cada uma com os seguintes elementos:

Elemento	Descrição
`ResourceType`	O tipo de recurso (coleção ou índice) ao qual as permissões se aplicam. As permissões de alias e modelo estão no nível da coleção, enquanto as permissões para criar, modificar e pesquisar dados estão no nível do índice. Para obter mais informações, consulte Permissões de políticas com suporte.
`Resource`	Uma lista de nomes e/ou padrões de recursos. Os padrões são prefixos seguidos por um curinga (*), que permitem que as permissões associadas sejam aplicadas a vários recursos. • As coleções assumem o formato `collection/` *`<name|pattern>`* . • Os índices assumem o formato `index/`*`<collection-name|pattern>`* `/`*`<index-name|pattern/>`* .
`Permission`	Uma lista de permissões a serem concedidas para os recursos especificados Para obter uma lista completa de permissões e as operações da API que elas permitem, consulte the section called “Operações e permissões de OpenSearch API suportadas”.
`Principal`	Uma lista de uma ou mais entidades principais às quais conceder acesso. Entidades principais podem ser ARNs de perfis do IAM ou identidades SAML. Essas entidades principais devem estar dentro da Conta da AWS atual. Não há suporte para o acesso entre contas.

O exemplo de política a seguir concede permissões de alias e modelo à coleção chamada `autopartsinventory`, bem como a quaisquer coleções iniciadas pelo prefixo `sales*`. Ele também concede permissões de leitura e gravação a todos os índices da coleção `autopartsinventory` e a todos os índices da coleção `salesorders` iniciados pelo prefixo `orders*`.

```
[
   {
```

```
      "Description": "Rule 1",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/autopartsinventory",
               "collection/sales*"
            ],
            "Permission":[
               "aoss:CreateCollectionItems",
               "aoss:UpdateCollectionItems",
               "aoss:DescribeCollectionItems"
            ]
         },
         {
            "ResourceType":"index",
            "Resource":[
               "index/autopartsinventory/*",
               "index/salesorders/orders*"
            ],
            "Permission":[
               "aoss:*"
            ]
         }
      ],
      "Principal":[
         "arn:aws:iam::123456789012:user/Dale",
         "arn:aws:iam::123456789012:role/RegulatoryCompliance",
         "saml/123456789012/myprovider/user/Annie",
         "saml/123456789012/anotherprovider/group/Accounting"
      ]
   }
]
```

Você não pode negar explicitamente o acesso em uma política. Dessa forma, todas as permissões de política são aditivas. Por exemplo, se uma política conceder a um usuário `aoss:ReadDocument` e outra conceder `aoss:WriteDocument`, o usuário terá ambas as permissões. Se uma terceira política conceder ao mesmo usuário `aoss:*`, o usuário poderá realizar todas as ações no índice associado; permissões mais restritivas não substituem as menos restritivas.

Permissões de políticas com suporte

Há suporte para as permissões a seguir nas políticas de acesso a dados. Para as operações da API do OpenSearch que cada permissão permite, consulte the section called “Operações e permissões de OpenSearch API suportadas”.

Permissões de coleção

- `aoss:CreateCollectionItems`
- `aoss:DeleteCollectionItems`
- `aoss:UpdateCollectionItems`
- `aoss:DescribeCollectionItems`
- `aoss:*`

Permissões de índice

- `aoss:ReadDocument`
- `aoss:WriteDocument`
- `aoss:CreateIndex`
- `aoss:DeleteIndex`
- `aoss:UpdateIndex`
- `aoss:DescribeIndex`
- `aoss:*`

Exemplos de conjuntos de dados no OpenSearch Dashboards

O OpenSearch Dashboards fornece conjuntos de dados de amostra que vêm com visualizações, painéis e outras ferramentas para ajudar você a explorar o Dashboards antes de adicionar seus próprios dados. Para criar índices a partir desses dados de amostra, você precisa de uma política de acesso a dados que forneça permissões para o conjunto de dados com o qual você deseja trabalhar. A política a seguir usa um caractere curinga (*) para fornecer permissões aos três conjuntos de dados de amostra.

```
[
  {
    "Rules": [
```

```
      {
        "Resource": [
          "index/<collection-name>/opensearch_dashboards_sample_data_*"
        ],
        "Permission": [
          "aoss:CreateIndex",
          "aoss:DescribeIndex",
          "aoss:ReadDocument"
        ],
        "ResourceType": "index"
      }
    ],
    "Principal": [
      "arn:aws:iam::<account-id>:user/<user>"
    ]
  }
]
```

Criação de políticas de acesso a dados (console)

É possível criar uma política de acesso a dados usando o editor visual, ou no formato JSON. Qualquer nova coleção que corresponda a um dos padrões definidos na política receberá as permissões correspondentes quando você criar a coleção.

Para criar uma política de acesso a dados do OpenSearch Sem Servidor

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. No painel de navegação à esquerda, expanda Sem Servidor e escolha Controle de acesso a dados.
3. Selecione Criar política de acesso.
4. Forneça um nome e uma descrição para a política.
5. Forneça um nome para a primeira regra em sua política. Por exemplo, “Acesso à coleção de logs”.
6. Escolha Adicionar entidades principais e selecione um ou mais perfis do IAM, ou usuários e grupos de SAML aos quais fornecer acesso aos dados.

> **Note**
>
> Para selecionar entidades principais nos menus suspensos, é necessário ter as permissões `iam:ListUsers` e `iam:ListRoles` (para entidades principais do IAM) e a permissão `aoss:ListSecurityConfigs` (para identidades de SAML).

7. Escolha Conceder e selecione o alias, o modelo e as permissões de índice para conceder às entidades principais associadas. Para obter uma lista completa de permissões e o acesso que elas permitem, consulte the section called “Operações e permissões de OpenSearch API suportadas”.
8. (Opcional) Configure regras adicionais para a política.
9. Escolha Criar. Pode haver cerca de um minuto de atraso entre a criação da política e o momento em que as permissões são aplicadas. Se demorar mais de 5 minutos, entre em contato com o AWS Support.

> **Important**
>
> Se sua política incluir apenas permissões de indexação (e nenhuma permissão de coleção), talvez você ainda veja uma mensagem sobre coleções correspondentes informando o seguinte: `Collection cannot be accessed yet. Configure data access policies so that users can access the data within this collection.` Você pode ignorar esse aviso. As entidades principais autorizadas ainda podem realizar suas operações relacionadas ao índice atribuídas na coleção.

Criação de políticas de acesso a dados (AWS CLI)

Para criar uma política de acesso a dados usando a API do OpenSearch Sem Servidor, use o comando `CreateAccessPolicy`. O comando aceita tanto políticas em linha quanto arquivos .json. As políticas em linha devem ser codificadas como uma string JSON com escape.

A solicitação a seguir cria uma política de acesso a dados:

```
aws opensearchserverless create-access-policy \
    --name marketing \
    --type data \
```

```
    --policy "[{\"Rules\":[{\"ResourceType\":\"collection\",\"Resource\":
[\"collection/autopartsinventory\",\"collection/sales*\"],\"Permission\":
[\"aoss:UpdateCollectionItems\"]},{\"ResourceType\":\"index\",\"Resource\":
[\"index/autopartsinventory/*\",\"index/salesorders/orders*\"],\"Permission
\":[\"aoss:ReadDocument\",\"aoss:DescribeIndex\"]}],\"Principal\":
[\"arn:aws:iam::123456789012:user/Shaheen\"]}]"
```

Para fornecer a política em um arquivo .json, use o formato `--policy file://my-policy.json`.

As entidades principais incluídas na política agora podem usar as operações do OpenSearch às quais tiverem acesso concedido.

Exibição de políticas de acesso a dados

Antes de criar uma coleção, talvez você queira pré-visualizar as políticas de acesso a dados existentes em sua conta para ver qual delas tem um padrão de recurso que corresponda ao nome da sua coleção. A solicitação ListAccessPolicies a seguir lista todas as políticas de acesso a dados em sua conta:

```
aws opensearchserverless list-access-policies --type data
```

A solicitação retorna informações sobre todas as políticas de acesso a dados configuradas. Para visualizar as regras de padrões definidas em uma política específica, encontre as informações sobre políticas no conteúdo do elemento `accessPolicySummaries` na resposta. Observe os `name` e `type` dessa política e use essas propriedades em uma solicitação getAccessPolicy para receber uma resposta com os seguintes detalhes da política:

```
{
    "accessPolicyDetails": [
        {
            "type": "data",
            "name": "my-policy",
            "policyVersion": "MTY2NDA1NDE4MDg1OF8x",
            "description": "My policy",
            "policy": "[{\"Rules\":[{\"ResourceType\":\"collection\",
\"Resource\":[\"collection/autopartsinventory\",\"collection/sales*\"],
\"Permission\":[\"aoss:UpdateCollectionItems\"]},{\"ResourceType\":\"index\",
\"Resource\":[\"index/autopartsinventory/*\",\"index/salesorders/orders*\"],
\"Permission\":[\"aoss:ReadDocument\",\"aoss:DescribeIndex\"]}],\"Principal\":
[\"arn:aws:iam::123456789012:user/Shaheen\"]}]",
            "createdDate": 1664054180858,
            "lastModifiedDate": 1664054180858
```

```
        }
    ]
}
```

É possível incluir filtros de recursos para limitar os resultados às políticas que contenham coleções ou índices específicos:

```
aws opensearchserverless list-access-policies --type data --resource
 "index/autopartsinventory/*"
```

Para exibir detalhes sobre uma política específica, use o comando GetAccessPolicy.

Atualização de políticas de acesso a dados

Quando você atualiza uma política de acesso a dados, todas as coleções associadas são afetadas. Para atualizar uma política de acesso a dados no console do OpenSearch Sem Servidor, escolha Controle de acesso a dados, selecione a política a ser modificada e escolha Editar. Faça suas alterações e escolha Salvar.

Para atualizar uma política de acesso a dados usando a API do OpenSearch Sem Servidor, envie uma solicitação `UpdateAccessPolicy`. É necessário incluir uma versão da política, que pode ser recuperada usando os comandos `ListAccessPolicies` ou `GetAccessPolicy`. A inclusão da versão mais recente da política garante que você não anule inadvertidamente uma alteração feita por outra pessoa.

A solicitação UpdateAccessPolicy a seguir atualiza uma política de acesso a dados com um novo documento JSON de política:

```
aws opensearchserverless update-access-policy \
    --name sales-inventory \
    --type data \
    --policy-version MTY2NDA1NDE4MDg1OF8x \
    --policy file://my-new-policy.json
```

Pode haver alguns minutos de atraso entre a atualização da política e o momento em que as novas permissões são aplicadas.

Exclusão de políticas de acesso a dados

Quando você exclui uma política de acesso a dados, todas as coleções associadas perdem o acesso definido na política. Certifique-se de que seus usuários do IAM e do SAML tenham o

acesso apropriado à coleção antes de excluir uma política. Para excluir uma política no console do OpenSearch Sem Servidor, selecione a política e escolha Excluir.

Também é possível usar o comando DeleteAccessPolicy:

```
aws opensearchserverless delete-access-policy --name my-policy --type data
```

Acesse o Amazon OpenSearch Serverless usando um endpoint de interface () AWS PrivateLink

Você pode usar AWS PrivateLink para criar uma conexão privada entre sua VPC e o Amazon OpenSearch Serverless. Você pode acessar o OpenSearch Serverless como se estivesse em sua VPC, sem o uso de um gateway de internet, dispositivo NAT, conexão VPN ou conexão. AWS Direct Connect As instâncias em sua VPC não precisam de endereços IP públicos para acessar OpenSearch o Serverless.

Você estabelece essa conexão privada criando um endpoint de interface, alimentado pelo AWS PrivateLink. Criamos uma interface de rede de endpoint em cada sub-rede que você habilitar para o endpoint de interface. Essas são interfaces de rede gerenciadas pelo solicitante que servem como ponto de entrada para o tráfego destinado ao Serverless. OpenSearch

Para obter mais informações, consulte Acessar os Serviços da AWS pelo AWS PrivateLink no Guia do AWS PrivateLink.

Tópicos

Resolução de DNS dos endpoints de coleta

Quando você cria um endpoint da VPC, o serviço cria uma nova zona hospedada privada Amazon Route 53 e a anexa à VPC. Essa zona hospedada privada consiste em um registro

para resolver o registro DNS curinga para coleções OpenSearch sem servidor (`*.aoss.us-east-1.amazonaws.com`) para os endereços de interface usados para o endpoint. Você só precisa de um OpenSearch VPC endpoint sem servidor em uma VPC para acessar todas e quaisquer coleções e painéis em cada uma. Região da AWS Cada VPC com um endpoint para OpenSearch Serverless tem sua própria zona hospedada privada anexada.

OpenSearch O Serverless também cria um registro DNS curinga público do Route 53 para todas as coleções na região. O nome DNS é resolvido para os endereços IP OpenSearch públicos sem servidor. Clientes em VPCs que não têm um endpoint VPC OpenSearch sem servidor ou clientes em redes públicas podem usar o resolvedor público do Route 53 e acessar as coleções e os painéis com esses endereços IP.

O endereço do resolvedor DNS de uma determinada VPC é o segundo endereço IP do CIDR da VPC. Qualquer cliente na VPC precisa usar esse resolvedor para obter o endereço do endpoint da VPC para qualquer coleção. O resolvedor usa uma zona hospedada privada criada pelo OpenSearch Serverless. É suficiente usar esse resolvedor para todas as coleções em qualquer conta. Também é possível usar o resolvedor da VPC para alguns endpoints de coleção e o resolvedor público para outros, embora isso normalmente não seja necessário.

VPCs e políticas de acesso à rede

Para conceder permissão de rede às OpenSearch APIs e painéis de suas coleções, você pode usar políticas de acesso à rede OpenSearch sem servidor. Você pode controlar esse acesso à rede a partir dos seus endpoints da VPC ou de Internet pública. Como sua política de rede controla apenas as permissões de tráfego, você também deve configurar uma política de acesso a dados que especifique a permissão para operar com os dados em uma coleção e seus índices. Pense em um endpoint OpenSearch VPC sem servidor como um ponto de acesso ao serviço, uma política de acesso à rede como o ponto de acesso em nível de rede para coleções e painéis e uma política de acesso a dados como o ponto de acesso para controle de acesso refinado para qualquer operação com dados na coleção.

Como você pode especificar vários IDs de endpoint da VPC em uma política de rede, recomendamos criar um endpoint da VPC para cada VPC que precise acessar uma coleção. Essas VPCs podem pertencer a AWS contas diferentes da conta proprietária da coleção e da política de OpenSearch rede Serverless. Não recomendamos que você crie um emparelhamento de VPC para VPC ou outra solução de proxy entre duas contas para que a VPC de uma conta possa usar o endpoint de outra. Isso é menos seguro e econômico do que cada VPC ter seu próprio endpoint. A primeira VPC não será facilmente visível para o administrador da outra VPC, que configurou o acesso ao endpoint da VPC na política de rede.

Políticas de VPCs e endpoint

O Amazon OpenSearch Serverless oferece suporte a políticas de endpoint para VPCs. Uma política de endpoint é uma política do IAM baseada em recurso que pode ser anexada a um endpoint da VPC para controlar quais entidades principais da AWS podem usar o endpoint para acessar seu serviço da AWS. Para obter mais informações, consulte Controlar o acesso a endpoints de VPC usando políticas de endpoint.

Para usar uma política de endpoint, primeiro você deve criar um endpoint de interface. Você pode criar um endpoint de interface usando o console OpenSearch Serverless ou a API Serverless. OpenSearch Depois de criar seu endpoint de interface, você precisará adicionar a política de endpoint a esse endpoint. Para obter mais informações, consulte Acesse o Amazon OpenSearch Serverless usando um endpoint de interface (). AWS PrivateLink

> **Note**
>
> Você não pode definir uma política de endpoint diretamente no console OpenSearch de serviço.

Uma política de endpoint não substitui políticas baseadas em recursos, políticas de rede nem políticas de acesso a dados que você possa ter configurado. Para obter informações sobre como atualizar sua política de endpoint de VPC, consulte Controlar o acesso a endpoints da VPC usando políticas de endpoint.

Por padrão, uma política de endpoint concede acesso total ao seu endpoint de VPC.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Embora a política padrão de endpoint de VPC conceda acesso total ao endpoint, você pode configurar uma política de endpoint de VPC para permitir acesso a perfis e usuários específicos. Para fazer isso, veja o exemplo a seguir:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "123456789012",
                    "987654321098"
                ]
            },
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Você pode especificar uma coleção OpenSearch Serverless para ser incluída como um elemento condicional na sua política de VPC endpoint. Para fazer isso, veja o exemplo a seguir:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:CollectionName": [
                        "coll-abc"
                    ]
                }
            }
        }
    ]
}
```

Você pode usar identidades SAML em sua política de endpoint de VPC para determinar o acesso ao endpoint de VPC. Você deve usar um caractere curinga (*) na seção principal da sua política de endpoint de VPC. Para fazer isso, veja o exemplo a seguir:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:SamlGroups": [
                        "saml/123456789012/idp123/group/football",
                        "saml/123456789012/idp123/group/soccer",
                        "saml/123456789012/idp123/group/cricket"
                    ]
                }
            }
        }
    ]
}
```

Além disso, você pode configurar sua política de endpoint para incluir uma política de entidade principal de SAML específica. Para isso, veja o seguinte:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SamlPrincipal": [
                        "saml/123456789012/idp123/user/user1234"]
                    }
                }
```

```
            }
        ]
    }
```

Para obter mais informações sobre o uso da autenticação SAML com o Amazon OpenSearch Serverless, consulte Autenticação SAML para Amazon Serverless. OpenSearch

Você também pode incluir usuários do IAM e do SAML na mesma política de endpoint de VPC. Para fazer isso, veja o exemplo a seguir:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:SamlGroups": [
                        "saml/123456789012/idp123/group/football",
                        "saml/123456789012/idp123/group/soccer",
                        "saml/123456789012/idp123/group/cricket"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            },
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Considerações

Antes de configurar um endpoint de interface para OpenSearch Serverless, considere o seguinte:

- OpenSearch O Serverless oferece suporte para fazer chamadas para todas as operações de OpenSearch API suportadas (não operações de API de configuração) por meio do endpoint da interface.
- Depois de criar um endpoint de interface para OpenSearch Serverless, você ainda precisa incluí-lo nas políticas de acesso à rede para que ele acesse coleções sem servidor.
- Por padrão, o acesso total ao OpenSearch Serverless é permitido por meio do endpoint da interface. Você pode associar um grupo de segurança às interfaces de rede do endpoint para controlar o tráfego para o OpenSearch Serverless por meio do endpoint da interface.
- Um único Conta da AWS pode ter no máximo 50 endpoints OpenSearch VPC sem servidor.
- Se você habilitar o acesso público à API ou aos painéis da sua coleção em uma política de rede, sua coleção pode ser acessada por qualquer VPC e pela internet pública.
- Se você estiver no local e fora da VPC, não poderá usar um resolvedor de DNS diretamente para a resolução do endpoint da VPC OpenSearch sem servidor. Se você precisar de acesso à VPN, a VPC precisará de um resolvedor de proxy DNS para ser usado por clientes externos. O Route 53 fornece uma opção de endpoint de entrada que você pode usar para resolver consultas ao DNS à VPC, originadas na rede no local (on-premises) ou em outra VPC.
- Para outras considerações, consulte Considerações no Guia do AWS PrivateLink.

Permissões obrigatórias

O acesso à VPC para OpenSearch Serverless usa as seguintes permissões AWS Identity and Access Management (IAM). É possível especificar as condições do IAM para restringir os usuários a coleções específicas.

- `aoss:CreateVpcEndpoint`: criar um endpoint da VPC.
- `aoss:ListVpcEndpoints`: listar todos os endpoints da VPC.
- `aoss:BatchGetVpcEndpoint`: veja detalhes sobre um subconjunto de endpoints da VPC.
- `aoss:UpdateVpcEndpoint`: modificar um endpoint da VPC.
- `aoss:DeleteVpcEndpoint`: excluir um endpoint da VPC.

Além disso, as seguintes permissões do Amazon EC2 e do Route 53 são necessárias para criar um endpoint de VPC.

- `ec2:CreateTags`
- `ec2:CreateVpcEndpoint`
- `ec2:DeleteVpcEndPoints`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `ec2:ModifyVpcEndPoint`
- `route53:AssociateVPCWithHostedZone`
- `route53:ChangeResourceRecordSets`
- `route53:CreateHostedZone`
- `route53:DeleteHostedZone`
- `route53:GetChange`
- `route53:GetHostedZone`
- `route53:ListHostedZonesByName`
- `route53:ListHostedZonesByVPC`
- `route53:ListResourceRecordSets`

Crie um endpoint de interface para Serverless OpenSearch

Você pode criar um endpoint de interface para OpenSearch Serverless usando o console ou a OpenSearch API Serverless.

Para criar um endpoint de interface para uma coleção sem OpenSearch servidor

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. Expanda Sem Servidor no painel de navegação à esquerda e escolha Endpoints da VPC.
3. Escolha Criar endpoint da VPC.
4. Forneça um nome para o endpoint.

5. Para VPC, selecione a VPC a partir da qual você acessará o Serverless. OpenSearch
6. Em Sub-redes, selecione uma sub-rede a partir da qual você OpenSearch acessará o Serverless.
7. Em Grupos de segurança, selecione os grupos de segurança para associar às interfaces de rede do endpoint. Essa é uma etapa crítica na qual você limita as portas, os protocolos e as origens para o tráfego de entrada que você está autorizando para o seu endpoint. Certifique-se de que as regras do grupo de segurança permitam que os recursos que usarão o VPC endpoint se comuniquem com o OpenSearch Serverless se comuniquem com a interface de rede do endpoint.
8. Escolha Criar endpoint.

Para criar um VPC endpoint usando a API OpenSearch Serverless, use o comando. `CreateVpcEndpoint`

> **Note**
>
> Depois de criar um endpoint, anote seu ID (por exemplo, `vpce-050f79086ee71ac05`. Para fornecer ao endpoint acesso às suas coleções, será necessário incluir esse ID em uma ou mais políticas de acesso à rede.

Próxima etapa: conceder ao endpoint acesso a uma coleção

Depois de criar um endpoint da interface, você deverá fornecer a ele acesso às coleções por meio de políticas de acesso à rede. Para ter mais informações, consulte the section called “Acesso à rede”.

Autenticação SAML para Amazon Serverless OpenSearch

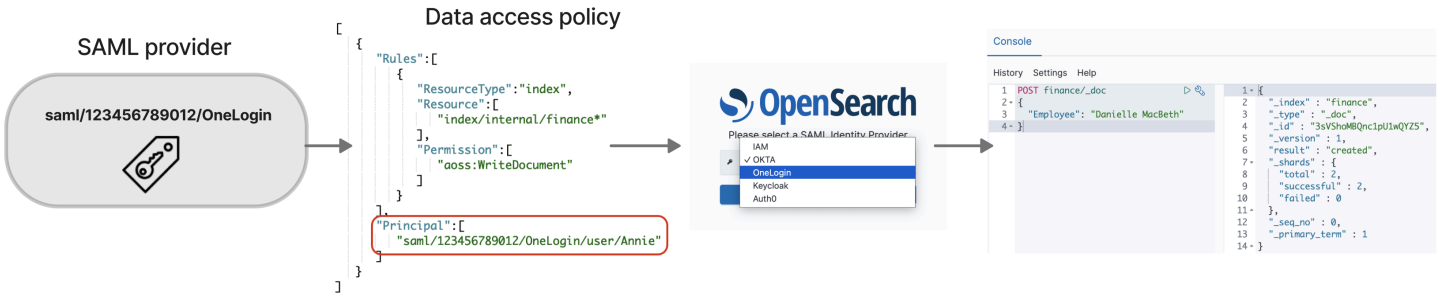
Com a autenticação SAML para Amazon OpenSearch Serverless, você pode usar seu provedor de identidade existente para oferecer login único (SSO) para os endpoints do Dashboards de coleções sem servidor. OpenSearch

A autenticação SAML permite que você use provedores de identidade terceirizados para entrar nos OpenSearch painéis para indexar e pesquisar dados. OpenSearch O Serverless oferece suporte a provedores que usam o padrão SAML 2.0, como IAM Identity Center, Okta, Keycloak, Active Directory Federation Services (AD FS) e Auth0. Você pode configurar o IAM Identity Center para

sincronizar usuários e grupos de outras fontes de identidade OneLogin, como Okta e Microsoft Entra ID. Para obter uma lista das fontes de identidade suportadas pelo IAM Identity Center e as etapas para configurá-las, consulte os tutoriais de introdução no Guia do usuário do IAM Identity Center.

> **Note**
>
> A autenticação SAML serve apenas para acessar OpenSearch painéis por meio de um navegador da web. Usuários autenticados só podem fazer solicitações às operações da OpenSearch API por meio de ferramentas de desenvolvimento em OpenSearch painéis. Suas credenciais SAML não permitem que você faça solicitações HTTP diretas para as operações da OpenSearch API.

Para configurar a autenticação SAML, primeiro é necessário configurar um provedor de identidade (IdP) SAML. Em seguida, você inclui um ou mais usuários desse IdP em uma política de acesso a dados. Essa política concede certas permissões para coleções e/ou índices. Em seguida, um usuário pode entrar nos OpenSearch painéis e realizar as ações permitidas na política de acesso a dados.



Tópicos

- Considerações
- Permissões obrigatórias
- Criação de provedores de SAML (console)
- Acessando OpenSearch painéis
- Concessão de acesso de identidades do SAML a dados de coleções
- Criação de provedores de SAML (AWS CLI)
- Exibição de provedores de SAML
- Atualização de provedores de SAML
- Exclusão de provedores de SAML

Considerações

Considere o seguinte ao configurar a autenticação SAML:

- Não há suporte para solicitações assinadas e criptografadas.
- Não há suporte para declarações criptografadas.
- Não há suporte para autenticação e desconexão iniciadas pelo IdP.

Permissões obrigatórias

A autenticação SAML para OpenSearch Serverless usa as seguintes permissões AWS Identity and Access Management (IAM):

- `aoss:CreateSecurityConfig`: criar um provedor de SAML.
- `aoss:ListSecurityConfig`: listar todos os provedores de SAML na conta atual.
- `aoss:GetSecurityConfig`: exibir as informações do provedor de SAML.
- `aoss:UpdateSecurityConfig`: modificar uma determinada configuração do provedor de SAML, incluindo os metadados XML.
- `aoss:DeleteSecurityConfig`: excluir um provedor de SAML.

A seguinte política de acesso baseada em identidade permite que um usuário gerencie todas as configurações do IdP:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aoss:CreateSecurityConfig",
                "aoss:DeleteSecurityConfig",
                "aoss:GetSecurityConfig",
                "aoss:UpdateSecurityConfig",
                "aoss:ListSecurityConfigs"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

```
}
```

Observe que o elemento `Resource` deve ser um caractere curinga.

Criação de provedores de SAML (console)

Estas etapas explicam como criar provedores de SAML. Isso permite a autenticação SAML com a autenticação iniciada pelo provedor de serviços (SP) para OpenSearch painéis. Não há suporte para autenticação iniciada pelo IdP.

Para habilitar a autenticação SAML para painéis OpenSearch

1. Faça login no console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. No painel de navegação à esquerda, expanda Sem Servidor e escolha Autenticação SAML.
3. Escolha Adicionar provedor de SAML.
4. Forneça um nome e uma descrição para o provedor.

   > **Note**
   >
   > O nome que você especificar pode ser acessado publicamente e aparecerá em um menu suspenso quando os usuários entrarem OpenSearch nos Painéis. Certifique-se de que o nome seja facilmente reconhecível e não revele informações confidenciais sobre seu provedor de identidade.

5. Em Configurar seu IdP, copie o URL do Assertion Consumer Service (ACS).
6. Use o URL do ACS que você acabou de copiar para configurar seu provedor de identidade. A terminologia e as etapas variam de acordo com o provedor. Consulte a documentação do seu provedor.

   No Okta, por exemplo, você cria uma “aplicação Web SAML 2.0” e especifica o URL do ACS como URL de login único, URL do destinatário e URL de destino. Para Auth0, especifique em URLs de retorno de chamada permitidos.
7. Forneça a restrição de público se seu IdP possuir um campo para isso. A restrição de público é um valor dentro da declaração do SAML que especifica a quem a declaração se destina. Para OpenSearch Serverless, especifique. `aws:opensearch:<aws account id>` Por exemplo, `aws:opensearch:123456789012`.

O nome do campo de restrição de público varia de acordo com o provedor. Para o Okta, é URI do público, ID de entidade do SP. Para o IAM Identity Center, é Público de SAML da aplicação.

8. Se você estiver usando o IAM Identity Center, você também precisará especificar o seguinte mapeamento de atributos: `Subject=${user:name}`, com um formato `unspecified`.
9. Aopis você configurar o provedor de identidade, ele gera um arquivo de metadados IdP. Esse arquivo XML contém informações sobre o provedor, como um certificado TLS, endpoints de acesso único e o ID de entidade do provedor de identidade.

   Copie o texto no arquivo de metadados do IdP e cole-o no campo Fornecer metadados do seu IdP. Alternativamente, escolha Importar de arquivo XML e carregue o arquivo. O arquivo de metadados deve ser semelhante ao seguinte:

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="entity-id"
 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>tls-certificate</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>s
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</
md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</
md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST" Location="idp-sso-url"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="idp-sso-url"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

10. Mantenha o campo Atributo de ID do usuário personalizado vazio para usar o elemento `NameID` da declaração do SAML para o nome do usuário. Se sua asserção não usar este elemento padrão e, em vez disso, incluir o nome de usuário como um atributo personalizado, especifique esse atributo aqui. Os atributos diferenciam maiúsculas de minúsculas. Só há suporte para um único atributo de usuário.

O exemplo a seguir mostra um atributo de substituição para `NameID` na declaração do SAML:

```
<saml2:Attribute Name="UserId" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
  <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="xs:string">annie</saml2:AttributeValue>
</saml2:Attribute>
```

11. (Opcional) Especifique um atributo personalizado no campo Atributo do grupo, como `role` ou `group`. Só há suporte para um único atributo de grupo. Não há atributo de grupo padrão. Se você não especificar uma, suas políticas de acesso a dados só poderão conter entidades principais de usuários.

    O exemplo a seguir mostra um atributo de grupo na declaração do SAML:

    ```
    <saml2:Attribute Name="department"
     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:type="xs:string">finance</saml2:AttributeValue>
    </saml2:Attribute>
    ```

12. Por padrão, os OpenSearch painéis desconectam os usuários após 24 horas. Você pode configurar esse valor para qualquer número entre 1 e 12 horas (15 e 720 minutos) especificando o tempo limite dos OpenSearch painéis. Se você tentar definir um tempo limite igual ou inferior a 15 minutos, sua sessão será redefinida para uma hora.
13. Escolha Criar provedor de SAML.

Acessando OpenSearch painéis

Depois de configurar um provedor SAML, todos os usuários e grupos associados a esse provedor podem navegar até o endpoint do OpenSearch Dashboards. O URL do Dashboards tem o formato *`collection-endpoint`*`/_dashboards/` para todas as coleções.

Se você tiver o SAML ativado, selecionar o link no AWS Management Console direcionará você para a página de seleção do IdP, na qual você poderá fazer login usando suas credenciais do SAML. Primeiro, use o menu suspenso para selecionar um provedor de identidade:

Em seguida, faça login usando suas credenciais do IdP.

Se você não tiver o SAML ativado, selecionar o link no AWS Management Console direcionará você a fazer login como usuário ou função do IAM, sem opção para SAML.

Concessão de acesso de identidades do SAML a dados de coleções

Depois de criar um provedor de SAML, você ainda precisa conceder aos usuários e grupos subjacentes acesso aos dados em suas coleções. Você concede acesso por meio de políticas de acesso a dados. Até que você forneça acesso aos usuários, eles não poderão ler, gravar ou excluir nenhum dado de suas coleções.

Para conceder acesso, crie uma política de acesso a dados e especifique seus IDs de usuário e/ou grupo do SAML na declaração `Principal`:

```
[
```

```
   {
      "Rules":[
       ...
      ],
      "Principal":[
         "saml/987654321098/myprovider/user/Shaheen",
         "saml/987654321098/myprovider/group/finance"
      ]
   }
]
```

É possível conceder acesso a coleções, índices ou ambos. Se você quiser que usuários diferentes tenham permissões diferentes, crie várias regras. Para obter uma lista das permissões disponíveis, consulte Permissões de políticas com suporte. Para obter informações sobre como formatar uma política de acesso, consulte Sintaxe das políticas.

Criação de provedores de SAML (AWS CLI)

Para criar um provedor SAML usando a API OpenSearch Serverless, envie uma solicitação: CreateSecurityConfig

```
aws opensearchserverless create-security-config \
    --name myprovider \
    --type saml \
    --saml-options file://saml-auth0.json
```

Especifique `saml-options`, incluindo o XML de metadados, como um mapa de chave-valor em um arquivo .json. O XML de metadados deve ser codificado como uma string de escape JSON.

```
{
   "sessionTimeout": 70,
   "groupAttribute": "department",
   "userAttribute": "userid",
   "metadata": "<EntityDescriptor xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata
\" ... ... ... IDPSSODescriptor>\r\n<\/EntityDescriptor>"
}
```

Exibição de provedores de SAML

A ListSecurityConfigssolicitação a seguir lista todos os provedores de SAML em sua conta:

```
aws opensearchserverless list-security-configs --type saml
```

A solicitação retorna informações sobre todos os provedores de SAML existentes, incluindo os metadados completos do IdP que seu provedor de identidade gera:

```
{
   "securityConfigDetails": [
      {
         "configVersion": "MTY2NDA1MjY4NDQ5M18x",
         "createdDate": 1664054180858,
         "description": "Example SAML provider",
         "id": "saml/123456789012/myprovider",
         "lastModifiedDate": 1664054180858,
         "samlOptions": {
            "groupAttribute": "department",
            "metadata": "<EntityDescriptor xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata
\" ... ... ... IDPSSODescriptor>\r\n<\/EntityDescriptor>",
            "sessionTimeout": 120,
            "userAttribute": "userid"
         }
      }
   ]
}
```

Para exibir detalhes sobre um provedor específico, inclusive a `configVersion` para futuras atualizações, envie uma solicitação `GetSecurityConfig`.

Atualização de provedores de SAML

Para atualizar um provedor SAML usando o console OpenSearch Serverless, escolha a autenticação SAML, selecione seu provedor de identidade e escolha Editar. É possível modificar todos os campos, incluindo os metadados e os atributos personalizados.

Para atualizar um provedor por meio da API OpenSearch Serverless, envie uma UpdateSecurityConfigsolicitação e inclua o identificador da política a ser atualizada. Também é necessário incluir uma versão da configuração, que pode ser recuperada usando os comandos `ListSecurityConfigs` ou `GetSecurityConfig`. A inclusão da versão mais recente garante que você não anule inadvertidamente uma alteração feita por outra pessoa.

A solicitação a seguir atualiza as opções do SAML para um provedor:

```
aws opensearchserverless update-security-config \
    --id saml/123456789012/myprovider \
    --type saml \
    --saml-options file://saml-auth0.json \
    --config-version MTY2NDA1MjY4NDQ5M18x
```

Especifique suas opções de configuração do SAML como um mapa de chave-valor em um arquivo .json.

> **Important**
>
> As atualizações nas opções do SAML não são incrementais. Se você não especificar um valor para um parâmetro no objeto `SAMLOptions` ao fazer uma atualização, os valores existentes serão substituídos por valores vazios. Por exemplo, se a configuração atual contiver um valor para `userAttribute`, e você fizer uma atualização em seguida e não incluir esse valor, o valor será removido da configuração. Certifique-se de saber quais são os valores existentes antes de fazer uma atualização chamando a operação `GetSecurityConfig`.

Exclusão de provedores de SAML

Quando você exclui um provedor de SAML, quaisquer referências a usuários e grupos associados em suas políticas de acesso a dados não funcionam mais. Para evitar confusão, sugerimos que você remova todas as referências ao endpoint em suas políticas de acesso antes de excluir o endpoint.

Para excluir um provedor SAML usando o console OpenSearch Serverless, escolha Autenticação, selecione o provedor e escolha Excluir.

Para excluir um provedor por meio da API OpenSearch Serverless, envie uma DeleteSecurityConfigsolicitação:

```
aws opensearchserverless delete-security-config --id saml/123456789012/myprovider
```

Validação de compatibilidade do Amazon OpenSearch Sem Servidor

Auditores externos avaliam a segurança e a conformidade do Amazon OpenSearch Sem Servidor como parte de vários programas de compatibilidade da AWS. Esses programas incluem SOC, PCI e HIPAA.

Para saber se um AWS service (Serviço da AWS) está no escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo por programa de conformidade em que você está interessado. Para obter informações gerais, consulteAWS Programas de conformidade.

É possível fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Downloading Reports inAWS Artifact.

Sua responsabilidade de conformidade ao usar o Serviços da AWS é determinada pela confidencialidade dos seus dados, pelos objetivos de conformidade da sua empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes atributos para ajudar com a conformidade:

- Guias de referência rápida de conformidade e segurança - estes guias de implantação discutem considerações sobre arquitetura e fornecem as etapas para a implantação de ambientes de linha de base focados em segurança e conformidade na AWS.
- Architecting for HIPAA Security and Compliance on Amazon Web Services (Arquitetura para segurança e conformidade com HIPAA no Amazon Web Services): esse estudo técnico descreve como as empresas podem usar a AWS para criar aplicações adequadas aos padrões HIPAA.

  > **Note**
  >
  > Nem todos os Serviços da AWS estão qualificados pela HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- atributos de conformidade da AWS: essa coleção de manuais e guias pode ser aplicada a seu setor e local.
- Guias de conformidade do cliente da AWS: entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as práticas recomendadas para proteção de Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliar atributos com regras no AWS Config Guia do desenvolvedor: o serviço AWS Config avalia como as configurações de atributos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub: este AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança na AWS. O Security Hub usa controles de segurança para avaliar os

atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.

- AWS Audit Manager – Esse AWS service (Serviço da AWS) ajuda a auditar continuamente seu uso da AWS para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

Aplicação de tags nas coleções do Amazon OpenSearch Sem Servidor

As tags permitem atribuir informações arbitrárias a um domínio do Amazon OpenSearch Sem Servidor para que você possa categorizar e filtrar por essas informações. Uma tag é um rótulo de metadados que você ou a AWS atribui a um recurso da AWS.

Cada tag consiste em uma chave e um valor. Para tags atribuídas por você, é possível definir a chave e o valor. Por exemplo, talvez você defina a chave como `stage` e o valor de recurso como `test`.

Com as tags, é possível fazer o seguinte:

- Identificar e organizar seus recursos da AWS. Muitos serviços da AWS oferecem suporte à marcação para que você possa atribuir a mesma tag a recursos de diferentes serviços para indicar que os recursos estão relacionados. Por exemplo, é possível atribuir a mesma tag a uma coleção do OpenSearch Sem Servidor que você atribui a um domínio do Amazon OpenSearch Service.
- Monitorar seus custos da AWS. Você pode ativar essas tags no painel do AWS Billing and Cost Management. A AWS usa as tags para categorizar seus custos e entregar um relatório mensal de alocação de custos para você. Para obter mais informações, consulte Usar tags de alocação de custos no Guia do usuário do AWS Billing.

No OpenSearch Sem Servidor, o recurso principal é uma coleção. É possível usar o console do OpenSearch Service, a AWS CLI, as operações da API do OpenSearch Sem Servidor ou os SDKs da AWS para adicionar, gerenciar e remover tags de uma coleção.

Permissões obrigatórias

O OpenSearch Sem Servidor usa as seguintes permissões do AWS Identity and Access Management Access Analyzer (IAM) para aplicar tags nas coleções:

- `aoss:TagResource`
- `aoss:ListTagsForResource`
- `aoss:UntagResource`

Uso de tags (console)

O console é a maneira mais simples de aplicar tags em uma coleção.

Para criar uma tag (console)

1. Faça login no console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. Expanda Serverless (Sem Servidor) no painel de navegação à esquerda e escolha Collections (Coleções).
3. Selecione a coleção na qual você deseja aplicar tags e vá para guia Tags.
4. Escolha Manage (Gerenciar) e Add new tag (Adicionar nova tag).
5. Insira uma chave de tag e um valor opcional.
6. Escolha Save (Salvar).

Para excluir uma tag, siga as mesmas etapas e escolha Remove (Remover) na página Manage tags (Gerenciar tags).

Para obter mais informações sobre como usar o console para trabalhar com tags, consulte Editor de tags no Guia de conceitos básicos do Console de GerenciamentoAWS.

Uso de tags (AWS CLI)

Para aplicar tags a uma coleção usando a AWS CLI, envie uma solicitação TagResource:

```
aws opensearchserverless tag-resource
  --resource-arn arn:aws:aoss:us-east-1:123456789012:collection/my-collection
  --tags Key=service,Value=aoss Key=source,Value=logs
```

É possível exibir as tags existentes para uma coleção com o comando ListTagsForResource:

```
aws opensearchserverless list-tags-for-resource
  --resource-arn arn:aws:aoss:us-east-1:123456789012:collection/my-collection
```

Remova as tags de uma coleção usando o comando UntagResource:

```
aws opensearchserverless untag-resource
  --resource-arn arn:aws:aoss:us-east-1:123456789012:collection/my-collection
  --tag-keys service
```

Operações e plug-ins compatíveis no Amazon OpenSearch Serverless

O Amazon OpenSearch Serverless oferece suporte a uma variedade de OpenSearch plug-ins, bem como a um subconjunto das operações de API de indexação, pesquisa e metadados disponíveis em. OpenSearch É possível incluir as permissões na coluna à esquerda da tabela nas políticas de acesso a dados para limitar o acesso a determinadas operações.

Tópicos

- Operações e permissões de OpenSearch API suportadas
- OpenSearch Plugins compatíveis

Operações e permissões de OpenSearch API suportadas

A tabela a seguir lista as operações de API compatíveis com o OpenSearch Serverless, junto com as permissões correspondentes do IAM:

Permissão da política de acesso a dados	OpenSearch Operações de API	Descrição e ressalvas
`aoss:CreateIndex`	PUT <index>	Criar índices. Para obter mais informações, consulte Criar índices. **Note** Essa permissão também se aplica à criação de índices com os dados

Permissão da política de acesso a dados	OpenSearch Operações de API	Descrição e ressalvas
		de amostra nos OpenSearch painéis.
`aoss:DescribeIndex`	• GET <index> • GET <index>/_mapping • GET <index>/_mappings • GET <index>/_setting • GET <index>/_setting/<setting> • GET <index>/_settings • GET <index>/_settings/<setting> • GET _cat/indices • GET _mapping • GET _mappings • GET _resolve/index/<index>	Descreve índices. Para obter mais informações, consulte os seguintes recursos do : • Obter índice • Obter um mapeamento • Obter configurações • Índices CAT (a resposta não inclui `health status` campos.)

Permissão da política de acesso a dados	OpenSearch Operações de API	Descrição e ressalvas
`aoss:WriteDocument`	• EXCLUIR <index>/_doc/ <id> • POST <index>/_bulk • POST <index>/_create/<id> (somente para tipos de coleção de pesquisa) • POST <index>/_doc • POST <index>/_update/ <id> • POST _bulk • PUT <index>/_create/<id> (somente para tipos de coleção de pesquisa) • PUT <index>/_doc/<id> (somente para tipos de coleção de pesquisa)	Escreve e atualiza documentos. Para obter mais informações, consulte os seguintes recursos do : • Em massa • Dados de índice **Note** Algumas operações só são permitidas para coleções do tipo SEARCH. Para ter mais informaçõ es, consulte the section called “Escolha de um tipo de coleção”.

Permissão da política de acesso a dados	OpenSearch Operações de API	Descrição e ressalvas
`aoss:ReadDocument`	• GET <index>/_analyze • GET <index>/_doc/<id> • GET <index>/_explain/<id> • GET <index>/_mget • GET <index>/_source/<id> • GET <index>/_count • GET <index>/_field_caps • GET <index>/_msearch • GET <index>/_rank_eval • GET <index>/_search • GET <index>/_validate/<query> • GET _analyze • GET _field_caps • GET _mget • GET _search • HEAD <index>/_doc/<id> • HEAD <index>/_source/<id> • POST <index>/_analyze • POST <index>/_explain/<id> • POST <index>/_count • POST <index>/_field_caps • POST <index>/_rank_eval • POST <index>/_search • POST _analyze • POST _field_caps • POST _search	Lê documentos. Para obter mais informações, consulte os seguintes recursos do : • Realizar análise de texto • Obter documento • Contagem • Consultar DSL • Avaliação de classific ação • API de análise • Explicar

Permissão da política de acesso a dados	OpenSearch Operações de API	Descrição e ressalvas
`aoss:DeleteIndex`	DELETE <target>	Excluir índices. Para obter mais informações, consulte Excluir índice.
`aoss:UpdateIndex`	• POST _mapping • POST <index>/_mapping/ • POST <index>/_mappings/ • POST <index>/_setting • POST <index>/_settings • POST _setting • POST _settings • PUT _mapping • PUT <index>/_mapping • PUT <index>/_mappings/ • PUT <index>/_setting • PUT <index>/_settings • PUT _setting • PUT _settings	Atualizar configurações de índice. Para obter mais informações, consulte os seguintes recursos do : • Mapeamento • Atualizar configurações
`aoss:CreateCollectionItems`	POST _aliases	Criar aliases de índice. Para obter mais informaçõ es, consulte Criar aliases.

Permissão da política de acesso a dados	OpenSearch Operações de API	Descrição e ressalvas
`aoss:DescribeCollectionItems`	• GET <index>/_alias/<alias> • GET _alias • GET _alias/<alias> • GET _cat/aliases • GET _cat/templates • GET _cat/templates/<template_name> • GET _component_template • GET _component_template/<component-template> • GET _index_template • GET _index_template/<index-template> • HEAD _alias/<alias> • HEAD _component_template/<component-template> • HEAD _index_template/<name> • HEAD <index>/_alias/<alias>	Descreva aliases e modelos de índices. Para obter mais informações, consulte os seguintes recursos do : • Gerenciar aliases • Modelos de índices

Permissão da política de acesso a dados	OpenSearch Operações de API	Descrição e ressalvas
`aoss:UpdateCollectionItems`	• POST <index>/_alias/<alias> • POST <index>/_aliases/<alias> • POST _component_template/<component-template> • POST _index_template/<index-template> • PUT <index>/_alias/<alias> • PUT <index>/_aliases/<alias> • PUT _component_template/<component-template> • PUT _index_template/<index-template>	Atualizar aliases e modelos de índices. Para obter mais informações, consulte os seguintes recursos do : • Aliases de índice • Modelos de índices
`aoss:DeleteCollectionItems`	• DELETE <index>/_alias/<alias> • DELETE _component_template/<component-template> • DELETE _index_template/<index-template> • DELETE <index>/_aliases/<alias>	Excluir aliases e modelos de índices. Para obter mais informações, consulte os seguintes recursos do : • Excluir aliases • Excluir um modelo

OpenSearch Plugins compatíveis

OpenSearch As coleções sem servidor vêm pré-embaladas com os seguintes plug-ins da comunidade. OpenSearch O Serverless (Sem Servidor) implanta e gerencia automaticamente os plug-ins para você.

Plug-ins de análise

- ICU Analysis
- Japanese (kuromoji) Analysis
- Análise de coreano (Nori)

- Phonetic Analysis
- Smart Chinese Analysis
- Stempel Polish Analysis
- Ukrainian Analysis

Plug-ins do Mapper

- Mapper Size
- Mapper Murmur3
- Texto anotado do Mapper

Plug-ins de script

- Painless
- Expressão
- Mustache

Além disso, o OpenSearch Serverless inclui todos os plug-ins fornecidos como módulos.

Monitorando o Amazon OpenSearch Serverless

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do Amazon OpenSearch Serverless e de suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para monitorar o OpenSearch Serverless, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos nos quais você executa AWS em tempo real. É possível coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido.

  Por exemplo, você pode CloudWatch rastrear o uso da CPU ou outras métricas de suas instâncias do Amazon EC2 e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

- AWS CloudTrail captura chamadas de API e eventos relacionados realizados pela conta da Conta da AWSou em nome dela. Ele disponibiliza os arquivos de log para um bucket do Amazon S3 especificado por você. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o AWS CloudTrail Guia do Usuário.
- A Amazon EventBridge fornece um fluxo quase em tempo real de eventos do sistema que descrevem as mudanças em seus domínios OpenSearch de serviço. Você pode criar regras que observem determinados eventos e acionem ações automatizadas em outros Serviços da AWS quando esses eventos ocorrerem. Para obter mais informações, consulte o Guia EventBridge do usuário da Amazon.

Monitoramento OpenSearch sem servidor com a Amazon CloudWatch

Você pode monitorar o Amazon OpenSearch Serverless usando CloudWatch, que coleta dados brutos e os processa em métricas legíveis, quase em tempo real. Essas estatísticas são mantidas por 15 meses, de maneira que você possa acessar informações históricas e ter uma perspectiva melhor de como o aplicativo web ou o serviço está se saindo.

Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

OpenSearch O Serverless relata as seguintes métricas no namespace. `AWS/AOSS`

Métrica	Descrição
`ActiveCollection`	Indica se uma coleção está ativa. Um valor de 1 significa que a coleção está em um estado `ACTIVE`. Esse valor é emitido após a criação com êxito de uma coleção, e permanece como 1 até que você exclua a coleção. A métrica não pode ter um valor de 0. Estatísticas relevantes: máx. Dimensões: `ClientId`, `CollectionId` , `CollectionName` Frequência: 60 segundos

Métrica	Descrição
`DeletedDocuments`	O número total de documentos excluídos. Estatísticas relevantes: média, soma Dimensões: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frequência: 60 segundos
`IndexingOCU`	O número de unidades OpenSearch computacionais (OCUs) usadas para ingerir dados de coleta. Esta métrica aplica-se no nível da conta. Estatísticas relevantes: soma Dimensões: `ClientId` Frequência: 60 segundos
`IngestionDataRate`	A taxa de indexação em GiB por segundo para uma coleção ou índice. Esta métrica aplica-se apenas às solicitações de indexação em massa. Estatísticas relevantes: soma Dimensões: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frequência: 60 segundos

Métrica	Descrição
`IngestionDocumentErrors`	O número total de erros de documentos durante a ingestão de uma coleção ou índice. Depois de uma solicitação de indexação em massa com êxito, os gravadores processam a solicitação e emitem erros para todos os documentos que falharam na solicitação. Estatísticas relevantes: soma Dimensões: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frequência: 60 segundos
`IngestionDocumentRate`	A taxa por segundo na qual os documentos estão sendo ingeridos em uma coleção ou índice. Esta métrica aplica-se apenas às solicitações de indexação em massa. Estatísticas relevantes: soma Dimensões: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frequência: 60 segundos
`IngestionRequestErrors`	O número total de erros de solicitação de indexação em massa para uma coleção. OpenSearch O Serverless emite essa métrica quando uma solicitação de indexação em massa falha por qualquer motivo, como um problema de autenticação ou disponibilidade. Estatísticas relevantes: soma Dimensões: `ClientId`, `CollectionId` , `CollectionName` Frequência: 60 segundos

Métrica	Descrição
`IngestionRequestLatency`	A latência, em segundos, para operações de gravação em massa em uma coleção. Estatísticas relevantes: mínimo, máximo, média Dimensões: `ClientId`, `CollectionId` , `CollectionName` Frequência: 60 segundos
`IngestionRequestRate`	O número total de operações de gravação em massa recebidas por uma coleção. Estatísticas relevantes: mínimo, máximo, média Dimensões: `ClientId`, `CollectionId` , `CollectionName` Frequência: 60 segundos
`IngestionRequestSuccess`	O número total de operações de indexação para uma coleção. Estatísticas relevantes: soma Dimensões: `ClientId`, `CollectionId` , `CollectionName` Frequência: 60 segundos
`SearchableDocuments`	O número total de documentos pesquisáveis em uma coleção ou no índice. Estatísticas relevantes: soma Dimensões: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frequência: 60 segundos

Métrica	Descrição
`SearchRequestErrors`	O número total de erros de consulta por minuto para uma coleção. Estatísticas relevantes: soma Dimensões: `ClientId`, `CollectionId` , `CollectionName` Frequência: 60 segundos
`SearchRequestLatency`	O tempo médio necessário, em milissegundos, para que uma operação de pesquisa seja concluída em uma coleção. Estatísticas relevantes: mínimo, máximo, média Dimensões: `ClientId`, `CollectionId` , `CollectionName` Frequência: 60 segundos
`SearchOCU`	O número de unidades OpenSearch computacionais (OCUs) usadas para pesquisar dados de coleta. Esta métrica aplica-se no nível da conta. Estatísticas relevantes: soma Dimensões: `ClientId` Frequência: 60 segundos

Métrica	Descrição
SearchRequestRate	O número total de solicitações de pesquisa por minuto para uma coleção. Estatísticas relevantes: média, máximo, soma Dimensões: ClientId, CollectionId , CollectionName Frequência: 60 segundos
StorageUsedInS3	A quantidade, em bytes, do armazenamento do Amazon S3 usado. OpenSearch O Serverless armazena dados indexados no Amazon S3. Você deve selecionar o período em um minuto para receber um valor preciso. Estatísticas relevantes: soma Dimensões: ClientId, CollectionId , CollectionName , IndexId, IndexName Frequência: 60 segundos
2xx, 3xx, 4xx, 5xx	O número de solicitações para a coleção que resultaram no determinado código de resposta HTTP (2xx, 3xx, 4xx, 5xx). Estatísticas relevantes: soma Dimensões: ClientId, CollectionId , CollectionName Frequência: 60 segundos

Registrando OpenSearch chamadas de API sem servidor usando AWS CloudTrail

O Amazon OpenSearch Serverless é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Serverless.

CloudTrail captura todas as chamadas de API para OpenSearch Serverless como eventos. As chamadas capturadas incluem chamadas da seção Serverless do console de OpenSearch serviço e chamadas de código para as operações da API OpenSearch Serverless.

Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para OpenSearch Serverless. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos.

Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita à OpenSearch Serverless, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o GuiaAWS CloudTrail do usuário.

OpenSearch Informações sem servidor em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no OpenSearch Serverless, essa atividade é registrada em um CloudTrail evento junto com outros eventos de AWS serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em seu Conta da AWS, incluindo eventos para OpenSearch Serverless, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS.

A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para mais informações, consulte:

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados

- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas as ações OpenSearch sem servidor são registradas CloudTrail e documentadas na referência da API sem OpenSearch servidor. Por exemplo, chamadas para as `DeleteCollection` ações `CreateCollectionListCollections`, e geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Entendendo as entradas do arquivo de log OpenSearch sem servidor

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log.

Um evento representa uma solicitação única de qualquer fonte. Ele inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `CreateCollection` ação.

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"AssumedRole",
      "principalId":"AIDACKCEVSQ6C2EXAMPLE",
      "arn":"arn:aws:iam::123456789012:user/test-user",
```

```
      "accountId":"123456789012",
      "accessKeyId":"access-key",
      "sessionContext":{
         "sessionIssuer":{
            "type":"Role",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:role/Admin",
            "accountId":"123456789012",
            "userName":"Admin"
         },
         "webIdFederationData":{

         },
         "attributes":{
            "creationDate":"2022-04-08T14:11:34Z",
            "mfaAuthenticated":"false"
         }
      }
   },
   "eventTime":"2022-04-08T14:11:49Z",
   "eventSource":"aoss.amazonaws.com",
   "eventName":"CreateCollection",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"AWS Internal",
   "userAgent":"aws-cli/2.1.30 Python/3.8.8 Linux/5.4.176-103.347.amzn2int.x86_64 exe/
x86_64.amzn.2 prompt/off command/aoss.create-collection",
   "errorCode":"HttpFailureException",
   "errorMessage":"An unknown error occurred",
   "requestParameters":{
      "accountId":"123456789012",
      "name":"test-collection",
      "description":"A sample collection",
      "clientToken":"d3a227d2-a2a7-49a6-8fb2-e5c8303c0718"
   },
   "responseElements": null,
   "requestID":"12345678-1234-1234-1234-987654321098",
   "eventID":"12345678-1234-1234-1234-987654321098",
   "readOnly":false,
   "eventType":"AwsApiCall",
   "managementEvent":true,
   "recipientAccountId":"123456789012",
   "eventCategory":"Management",
   "tlsDetails":{
      "clientProvidedHostHeader":"user.aoss-sample.us-east-1.amazonaws.com"
```

```
    }
}
```

Monitoramento de eventos OpenSearch sem servidor usando a Amazon EventBridge

O Amazon OpenSearch Service se integra EventBridge à Amazon para notificá-lo sobre determinados eventos que afetam seus domínios. Os eventos dos AWS serviços são entregues quase EventBridge em tempo real. Os mesmos eventos também são enviados para a Amazon CloudWatch Events, a antecessora da Amazon EventBridge. Você pode escrever regras para indicar quais eventos são do seu interesse, e as ações automatizadas a serem tomadas quando um evento corresponder à regra. Exemplos de ações que você pode ativar automaticamente incluem o seguinte:

- Invocando uma função AWS Lambda
- Invocação de um Run Command do Amazon EC2
- Transmitir o evento Amazon Kinesis Data Streams
- Ativando uma máquina de estado AWS Step Functions
- Notificação de um tópico do Amazon SNS ou de uma fila do Amazon SQS

Para obter mais informações, consulte Comece a usar a Amazon EventBridge no Guia EventBridge do usuário da Amazon.

Configuração de notificações

Você pode usar as NotificaçõesAWS do usuário para receber notificações quando ocorrer um evento OpenSearch sem servidor. Um evento é um indicador de uma mudança no ambiente OpenSearch sem servidor, como quando você atinge o limite máximo de uso da OCU. Amazon EventBridge recebe o evento e encaminha uma notificação para a Central de AWS Management Console Notificações e os canais de entrega escolhidos. Você recebe uma notificação quando um evento corresponde a uma regra especificada.

OpenSearch Eventos de unidades de computação (OCU)

OpenSearch O Serverless envia eventos para EventBridge quando um dos seguintes eventos relacionados à OCU ocorrer.

OCU usage approaching maximum limit (Uso de OCU próximo do limite máximo)

OpenSearch O Serverless envia esse evento quando o uso da OCU de pesquisa ou indexação atinge 75% do seu limite de capacidade. O uso de OCU é calculado com base no limite de capacidade configurado e no consumo atual de OCU.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Approaching Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your search OCU usage is at 75% and is approaching the configured
 maximum limit."
  }
}
```

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Approaching Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your indexing OCU usage is at 75% and is approaching the configured
 maximum limit."
  }
```

OCU usage reached maximum limit (O uso de OCU atingiu o limite máximo)

OpenSearch O Serverless envia esse evento quando o uso da OCU de pesquisa ou indexação atinge 100% do seu limite de capacidade. O uso de OCU é calculado com base no limite de capacidade configurado e no consumo atual de OCU.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Reached Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your search OCU usage has reached the configured maximum limit."
  }
}
```

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Reached Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your indexing OCU usage has reached the configured maximum limit."
  }
}
```

Criação e gerenciamento de domínios OpenSearch do Amazon Service

Este capítulo descreve como criar e gerenciar domínios do Amazon OpenSearch Service. Um domínio OpenSearch de serviço é sinônimo de um OpenSearch cluster. Domínios são clusters com configurações, tipos de instância, contagens de instâncias e recursos de armazenamento especificados por você.

Diferentemente das breves instruções apresentadas no Tutorial de introdução, este capítulo descreve todas as opções e fornece informações de referência relevantes. Você pode concluir cada procedimento usando instruções para o console OpenSearch de serviço, o AWS Command Line Interface (AWS CLI) ou os AWS SDKs.

Criação OpenSearch de domínios de serviço

Esta seção descreve como criar domínios OpenSearch de serviço usando o console OpenSearch de serviços ou usando o AWS CLI com o `create-domain` comando.

Criação OpenSearch de domínios de serviço (console)

Use o procedimento a seguir para criar um domínio de OpenSearch serviço usando o console.

Para criar um domínio OpenSearch de serviço (console)

1. Acesse http://aws.amazon.com e escolha Fazer login no console.
2. Em Analytics, escolha Amazon OpenSearch Service.
3. Escolha Criar domínio.
4. Em Nome de domínio, insira um nome de domínio O nome deve atender aos seguintes critérios:
   - Exclusivo para sua conta e Região da AWS
   - Iniciar com letra minúscula.
   - Conter de 3 a 28 caracteres.
   - Conter apenas letras minúsculas a-z, números de 0-9 e hífen (-).
5. Como método de criação de domínio, escolha Criação padrão.
6. Em Modelos, escolha a opção que melhor corresponde à finalidade do seu domínio:

- Domínios de produção para workload que precisam de alta disponibilidade e desempenho. Os domínios usam Multi-AZ (com ou sem standby) e nós principais dedicados para uma maior disponibilidade.
- Dev/test para desenvolvimento ou teste. Esses domínios podem usar Multi-AZ (com ou sem modo de espera) ou uma única zona de disponibilidade.

> **Important**
>
> Diferentes tipos de implantação apresentam diferentes opções em páginas subsequentes. Essas etapas incluem todas as opções.

7. Para Opções de implantação, escolha Domínio com modo de espera para configurar um domínio 3-AZ, com os nós em uma das zonas reservados como modo de espera. Essa opção aplica várias práticas recomendadas, como contagem especificada de nós de dados, contagem de nós principais, tipo de instância, contagem de réplicas e configurações de atualização de software.
8. Em Versão, escolha a versão OpenSearch ou o Elasticsearch OSS legado a ser usado. Recomendamos que você escolha a versão mais recente do OpenSearch. Para ter mais informações, consulte the section called “Versões compatíveis do OpenSearch e do Elasticsearch.”.

   (Opcional) Se você escolher uma OpenSearch versão para seu domínio, selecione Ativar modo de compatibilidade para OpenSearch reportar sua versão como 7.10, o que permite que determinados clientes e plug-ins do Elasticsearch OSS que verificam a versão antes de se conectar continuem trabalhando com o serviço.
9. Em Tipo de instância escolha um tipo de instância para os nós de dados. Para ter mais informações, consulte the section called “Tipos de instâncias compatíveis”.

   > **Note**
   >
   > Nem todas as zonas de disponibilidade são compatíveis com todos os tipos de instância. Se você escolher Multi-AZ com ou sem standby, é recomendável selecionar tipos de instância da geração atual, como R5 ou I3.
10. Em Número de nós, selecione o número de nós de dados.

Para valores máximos, consulte Cotas OpenSearch de domínio e instância do serviço. Os clusters de nó único são excelentes para desenvolvimento e testes, mas não devem ser usados para workloads de produção. Para obter mais orientações, consulte the section called "Dimensionamento de domínios" e the section called "Configuração de um domínio Multi-AZ".

11. Em Tipo de armazenamento, selecione Amazon EBS. Os tipos de volume disponíveis na lista dependem do tipo de instância escolhido. Para obter orientações sobre a criação de domínios especialmente grandes, consulte the section called "Escala de petabytes".
12. Em armazenamento EBS, configure as opções a seguir. A depender do tipo de volume escolhido, algumas configurações poderão não aparecer.

Configuração	Descrição
Tipo de volume do EBS	Escolha entre Finalidade geral (SSD) - gp3 e Finalidade geral (SSD) - gp2 ou IOPS provisionadas (SSD) e Magnético (padrão) da geração anterior.
Tamanho de armazenamento do EBS por nó	Insira o tamanho do volume do EBS que você deseja anexar a cada nó de dados. EBS volume size é por nó. Você pode calcular o tamanho total do cluster para o domínio OpenSearch Service multiplicando o número de nós de dados pelo tamanho do volume do EBS. O tamanho mínimo e máximo de um volume do EBS depende tanto do tipo de volume do EBS especificado quanto do tipo da instância à qual ele está anexado. Para saber mais, consulte Limites de tamanhos de volume do EBS.
IOPS provisionadas	Se você selecionou um tipo de volume SSD de IOPS provisionadas, insira o número de operações de E/S por segundo (IOPS) que o volume pode suportar.

13. (Opcional) Se você selecionou um tipo de volume gp3, amplie Configurações avançadas e especifique as IOPS (até 1.000 MiB/s) para cada 3 TiB de tamanho de volume provisionado por nó de dado) e o throughput (até 16.000 para cada 3 TiB de tamanho de volume provisionado por nó de dado) adicionais a serem provisionados para cada nó, além do que está incluído no preço do armazenamento, por um custo adicional. Para obter mais informações, consulte os preços do Amazon OpenSearch Service.

14. (Opcional) Para ativar o UltraWarm armazenamento, escolha Ativar nós UltraWarm de dados. Cada tipo de instância tem uma quantidade máxima de armazenamento que ele pode processar. Multiplique essa quantidade pelo número de nós de dados de alta atividade pelo total de armazenamento de alta atividade endereçável.
15. (Opcional) Para habilitar o armazenamento de baixa atividade, escolha Habilitar armazenamento de baixa atividade. Você deve habilitar UltraWarm para habilitar o armazenamento a frio.
16. Se você usa o multi-AZ com modo de espera, três nós principais dedicados já estão habilitados. Escolha o tipo de nós principais que você deseja. Se você escolheu um domínio Multi-AZ sem modo de espera, selecione Habilitar nós principais dedicados e escolha o tipo e o número de nós principais que você deseja. Os nós principais dedicados aumentam a estabilidade do cluster e são necessários para domínios com contagem de instâncias superior a 10. Recomendamos três nós principais dedicados para domínios de produção.

> **Note**
>
> Você pode escolher diferentes tipos de instâncias para seus nós principais dedicados e nós de dados. Por exemplo, você pode selecionar instâncias de uso geral ou de armazenamento otimizado para os nós de dados e instâncias otimizadas para computação para os nós principais dedicados.

17. (Opcional) Para domínios que executam o Elasticsearch OpenSearch 5.3 e versões posteriores, a configuração do Snapshot é irrelevante. Para obter mais informações sobre snapshots automatizados, consulte the section called “Criação de snapshots de índices”.
18. Se você quiser usar um endpoint personalizado em vez do padrão `https://search-`*`mydomain-1a2a3a4a5a6a7a8a9a0a9a8a7a`*`.`*`us-east-1`*`.es.amazonaws.com`, escolha Habilitar endpoints personalizados e forneça um nome e um certificado. Para ter mais informações, consulte the section called “Criar um endpoint personalizado”.
19. Na seção Rede, escolha Acesso via VPC ou Acesso público. Se você selecionar Acesso público, vá para a próxima etapa. Se escolher Acesso à VPC, certifique-se de atender aos pré-requisitos e defina as seguintes configurações:

Configuração	Descrição
VPC	Escolha o ID da nuvem privada virtual (VPC) que deseja usar. A VPC e o domínio devem estar no mesmo lugar Região da AWS, e você deve selecionar uma VPC com a locação definida como Padrão. OpenSearc

Configuração	Descrição
	h O serviço ainda não oferece suporte a VPCs que usam locação dedicada.
Sub-rede	Escolha uma sub-rede. Se você ativou o Multi-AZ, deverá escolher duas ou três sub-redes. OpenSearch O serviço colocará um endpoint VPC e interfaces de rede elástica nas sub-redes. Você deve reservar endereços IP suficientes para as interfaces de rede em toda sub-rede. Para obter mais informações, consulte Reserva de endereços IP em uma sub-rede da VPC.
Grupos de segurança	Escolha um ou mais grupos de segurança de VPC que permitam que seu aplicativo necessário alcance o domínio do OpenSearch Serviço nas portas (80 ou 443) e protocolos (HTTP ou HTTPS) expostos pelo domínio. Para ter mais informações, consulte the section called “Suporte à VPC”.
IAM Role	Mantenha a função padrão. OpenSearch O serviço usa essa função predefinida (também conhecida como função vinculada ao serviço) para acessar sua VPC e colocar um endpoint de VPC e interfaces de rede na sub-rede da VPC. Para obter mais informações, consulte Função vinculada ao serviço para acesso à VPC.
Tipo de endereço IP	Escolha pilha dupla ou IPv4 como seu tipo de endereço IP. Pilhas duplas permitem que você compartilhe recursos de domínio entre os tipos de endereço IPv4 e IPv6 e é a opção recomendada. Se você definir o tipo de endereço IP como pilha dupla, não poderá alterar o tipo de endereço posteriormente.

20. Habilite ou desabilite controle de acesso refinado:

    - Se você quiser usar o IAM para o gerenciamento de usuários, escolha Definir ARN do IAM como usuário primário e especifique o ARN para uma função do IAM.
    - Se quiser usar o banco de dados de usuário interno, escolha Criar usuário primário e especifique um nome de usuário e senha.

Qualquer que seja a opção escolhida, o usuário principal pode acessar todos os índices no cluster e todas as APIs. OpenSearch Para obter orientações sobre qual opção escolher, consulte the section called “Principais conceitos”.

Se você desabilitar o controle de acesso refinado, ainda assim poderá controlar o acesso ao seu domínio, colocando-o em uma VPC, aplicando uma política de acesso restritiva ou ambos. Você deve habilitar a node-to-node criptografia e a criptografia em repouso para usar um controle de acesso refinado.

> **Note**
>
> Recomendamos enfaticamente habilitar o controle de acesso refinado para proteger os dados do seu domínio. O controle de acesso refinado fornece segurança nos níveis de cluster, índice, documento e campo.

21. (Opcional) Se você quiser usar a autenticação SAML para OpenSearch painéis, escolha Habilitar autenticação SAML e configure as opções de SAML para o domínio. Para obter instruções, consulte the section called “Autenticação SAML para painéis OpenSearch ”.
22. (Opcional) Se você quiser usar a autenticação do Amazon Cognito para OpenSearch painéis, escolha Habilitar a autenticação do Amazon Cognito. Em seguida, escolha o grupo de usuários e o grupo de identidades do Amazon Cognito que você deseja usar para autenticação de OpenSearch painéis. Para obter orientações sobre a criação desses recursos, consulte the section called “Autenticação do Amazon Cognito para OpenSearch Dashboards”.
23. Para Política de acesso, escolha uma política de acesso ou configure uma das suas próprias políticas. Se você optar por criar uma política personalizada, poderá configurá-la você mesmo ou importar uma política de outro domínio. Para ter mais informações, consulte the section called “Identity and Access Management”.

> **Note**
>
> Se você ativou o acesso à VPC, não poderá usar políticas baseadas em IP. Em vez disso, você poderá usar grupos de segurança para controlar quais endereços IP poderão acessar o domínio. Para ter mais informações, consulte the section called “Sobre políticas de acesso em domínios da VPC”.

24. (Opcional) Para exigir que todas as solicitações ao domínio sejam recebidas por HTTPS, selecione Exigir HTTPS para todo o tráfego do domínio. Para ativar a node-to-node criptografia, selecione ode-to-nodeCriptografia N. Para ter mais informações, consulte the section called "ode-to-node Criptografia N". Para habilitar criptografia de dados em repouso, selecione Ativar criptografia em repouso. Essas opções são pré-selecionadas se você escolher a opção de implantação multi-AZ com modo de espera.
25. (Opcional) Selecione AWS Usar chave própria para que o OpenSearch Serviço crie uma chave de AWS KMS criptografia em seu nome (ou use a que já foi criada). Caso contrário, escolha sua própria chave do KMS. Para ter mais informações, consulte the section called "Criptografia inativa".
26. Para a Janela fora do horário de pico, selecione um horário de início para agendar atualizações do software de serviço e otimizações do Auto-Tune que exijam uma implantação azul/verde. As atualizações fora do horário de pico ajudam a minimizar a sobrecarga nos nós principais dedicados de um cluster durante períodos de tráfego intenso.
27. Para o Auto-Tune, escolha se deseja permitir que o OpenSearch Serviço sugira alterações de configuração relacionadas à memória para seu domínio para melhorar a velocidade e a estabilidade. Para ter mais informações, consulte the section called "Auto-Tune".

    (Opcional) Selecione Janela fora do horário de pico para agendar uma janela recorrente durante a qual o Auto-Tune atualizará o domínio.
28. (Opcional) Selecione Atualização automática de software para habilitar atualizações automáticas de software.
29. (Opcional) Adicione tags para descrever seu domínio para que você possa categorizar e filtrar essas informações. Para ter mais informações, consulte the section called "Marcação de domínios".
30. (Opcional) Expanda e defina as Configurações avançadas de cluster. Para obter um resumo dessas opções, consulte the section called "Configurações avançadas do cluster".
31. Escolha Criar.

Criação OpenSearch de domínios de serviço ()AWS CLI

Em vez de criar um domínio de OpenSearch serviço usando o console, você pode usar AWS CLI o. Para obter a sintaxe, consulte Amazon OpenSearch Service na referência de comandos da AWS CLI a.

Exemplos de comando

Este primeiro exemplo demonstra a seguinte configuração do domínio OpenSearch de serviço:

- Cria um domínio OpenSearch de serviço chamado mylogs com a OpenSearch versão 1.2
- Preenche o domínio com duas instâncias do tipo `r6g.large.search`
- Utilização de um volume gp3 de Finalidade geral (SSD) do EBS de 100 GiB como armazenamento para cada nó de dados
- Permite acesso anônimo, mas apenas de endereço IP único: 192.0.2.0/32.

```
aws opensearch create-domain \
    --domain-name mylogs \
    --engine-version OpenSearch_1.2 \
    --cluster-config  InstanceType=r6g.large.search,InstanceCount=2 \
    --ebs-options
 EBSEnabled=true,VolumeType=gp3,VolumeSize=100,Iops=3500,Throughput=125 \
    --access-policies '{"Version": "2012-10-17", "Statement": [{"Action": "es:*",
 "Principal":"*","Effect": "Allow", "Condition": {"IpAddress":{"aws:SourceIp":
["192.0.2.0/32"]}}}]}'
```

O próximo exemplo demonstra a seguinte configuração do domínio OpenSearch de serviço:

- Cria um domínio OpenSearch de serviço chamado mylogs com a versão 7.10 do Elasticsearch
- Preenche o domínio com seis instâncias do tipo `r6g.large.search`
- Utilização de um volume gp2 de Finalidade geral (SSD) do EBS de 100 GiB como armazenamento para cada nó de dados
- Restringe o acesso ao serviço a um único usuário, identificado pelo Conta da AWS ID do usuário: 555555555555
- Distribui as instâncias em três zonas de disponibilidade

```
aws opensearch create-domain \
    --domain-name mylogs \
    --engine-version Elasticsearch_7.10 \
    --cluster-config
 InstanceType=r6g.large.search,InstanceCount=6,ZoneAwarenessEnabled=true,ZoneAwarenessConfig={A
 \
```

```
    --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=100 \
    --access-policies '{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
"Principal": {"AWS": "arn:aws:iam::555555555555:root" }, "Action":"es:*", "Resource":
"arn:aws:es:us-east-1:555555555555:domain/mylogs/*" } ] }'
```

O próximo exemplo demonstra a seguinte configuração do domínio OpenSearch de serviço:

- Cria um domínio OpenSearch de serviço chamado mylogs com a OpenSearch versão 1.0
- Preenche o domínio com 10 instâncias do tipo `r6g.xlarge.search`
- Preenche o domínio com três instâncias do tipo `r6g.large.search` para funcionar como nós principais dedicados
- Usa um volume de EBS de IOPS provisionadas de 100 GiB como armazenamento, configurado com performance de referência de 1.000 IOPS para cada nó de dados.
- Restringe o acesso a um único usuário e a um único sub-recurso, a API `_search`

```
aws opensearch create-domain \
    --domain-name mylogs \
    --engine-version OpenSearch_1.0 \
    --cluster-config
 InstanceType=r6g.xlarge.search,InstanceCount=10,DedicatedMasterEnabled=true,DedicatedMasterTyp
 \
    --ebs-options EBSEnabled=true,VolumeType=io1,VolumeSize=100,Iops=1000 \
    --access-policies '{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
 "Principal": { "AWS": "arn:aws:iam::555555555555:root" }, "Action": "es:*",
 "Resource": "arn:aws:es:us-east-1:555555555555:domain/mylogs/_search" } ] }'
```

> **Note**
>
> Se você tentar criar um domínio OpenSearch de serviço e já existir um domínio com o mesmo nome, a CLI não relatará um erro. Em vez disso, ela retornará detalhes do domínio existente.

Criação OpenSearch de domínios de serviço (AWS SDKs)

Os AWS SDKs (exceto os SDKs para Android e iOS) oferecem suporte a todas as ações definidas na Amazon OpenSearch Service API Reference, inclusive. `CreateDomain` Para obter o código de

exemplo, consulte the section called “Uso de AWS SDKs”. Para obter mais informações sobre como instalar e usar os AWS SDKs, consulte Kits AWS de desenvolvimento de software.

Criação OpenSearch de domínios de serviço ()AWS CloudFormation

OpenSearch O serviço é integrado com AWS CloudFormation, um serviço que ajuda você a modelar e configurar seus AWS recursos para que você possa gastar menos tempo criando e gerenciando seus recursos e infraestrutura. Você cria um modelo que descreve o OpenSearch domínio que você deseja criar e CloudFormation provisiona e configura o domínio para você. Para obter mais informações, incluindo exemplos de modelos JSON e YAML para OpenSearch domínios, consulte a referência do tipo de recurso do Amazon OpenSearch Service no Guia do AWS CloudFormation usuário.

Configuração de políticas de acesso

O Amazon OpenSearch Service oferece várias maneiras de configurar o acesso aos seus domínios do OpenSearch Serviço. Para ter mais informações, consulte the section called “Identity and Access Management” e the section called “Controle de acesso refinado”.

O console fornece políticas de acesso pré-configuradas que você pode personalizar de acordo com as necessidades específicas de seu domínio. Você também pode importar políticas de acesso de outros domínios do OpenSearch Serviço. Para obter informações sobre como essas políticas de acesso interagem com o acesso à VPC, consulte the section called “Sobre políticas de acesso em domínios da VPC”.

Para configurar políticas de acesso (console)

1. Vá para https://aws.amazon.com e escolha Fazer login no console.
2. Em Analytics, escolha Amazon OpenSearch Service.
3. No painel de navegação, em Domínios, escolha o domínio que deseja atualizar.
4. Escolha Ações e Editar configuração de segurança.
5. Edite a política de acesso JSON ou importe uma opção pré-configurada.
6. Escolha Salvar alterações.

Configurações avançadas do cluster

Use as opções avançadas para configurar o seguinte:

Índices em corpos de solicitações

Especifica se são permitidas referências explícitas aos índices dentro do corpo das solicitações HTTP. A definição dessa propriedade como `false` impede que os usuários ignorem o controle de acesso para sub-recursos. Por padrão, o valor é `true`. Para ter mais informações, consulte the section called “Opções avançadas e considerações sobre a API”.

Alocação de cache de dados de campo

Especifica a porcentagem de espaço do heap do Java alocada a dados de campo. Por padrão, essa configuração é 20% do heap JVM.

> **Note**
>
> Muitos clientes consultam índices alternados diariamente. Recomenda-se começar a realizar um teste de comparação com `indices.fielddata.cache.size` configurado como 40% do heap de JVM para a maioria desses casos de uso. Para índices muito grandes, talvez um cache de dados de campo grande seja necessário.

Contagem máxima de cláusulas

Especifica o número máximo de cláusulas permitidas em uma consulta booliana no Lucene. O padrão é 1.024. Consultas que ultrapassam o número permitido de cláusulas geram o erro `TooManyClauses`. Para obter mais informações, consulte a documentação do Lucene.

Fazendo alterações de configuração no Amazon OpenSearch Service

O Amazon OpenSearch Service usa um processo de implantação azul/verde ao atualizar domínios. Uma implantação azul/verde cria um ambiente livre para atualizações de domínio que copia o ambiente de produção e direciona usuários para o novo ambiente assim que essas atualizações são concluídas. Em uma implantação azul/verde, o ambiente azul é o ambiente de produção atual. O ambiente verde é o ambiente inativo.

Os dados são migrados do ambiente azul para o ambiente verde. Quando o novo ambiente estiver pronto, o OpenSearch Serviço alterna os ambientes para promover o ambiente verde como o novo ambiente de produção. A transição ocorre sem perda de dados. Essa prática minimiza o tempo de inatividade e mantém o ambiente original caso a implantação no novo ambiente resulte em erro.

Tópicos

Alterações que normalmente causam implantações azuis/verdes

As seguintes operações causam implementações azuis/verdes:

- Alterar o tipo de instância
- Habilitar o controle de acesso detalhado
- Atualizações de software de serviço
- Alterar a contagem de instâncias de dados, caso o seu domínio não tenha nós principais dedicados
- Habilitar ou desabilitar os nós principais dedicados
- Ativar ou desativar o Multi-AZ sem modo de espera
- Alterar o tipo de armazenamento, o tipo do volume ou o tamanho do volume
- Escolher diferentes sub-redes da VPC
- Adicionar ou remover os grupos de segurança da VPC
- Ativar ou desativar a autenticação do Amazon Cognito para painéis OpenSearch
- Escolha de outro grupo de usuários ou grupo de identidades do Amazon Cognito
- Modificar configurações avançadas
- Atualização para uma nova OpenSearch versão (os OpenSearch painéis podem estar indisponíveis durante parte ou toda a atualização)
- Habilitando a criptografia de dados em repouso ou node-to-node criptografia
- Ativando ou desativando nosso UltraWarm armazenamento a frio

- Desabilitação do Auto-Tune e reversão de suas alterações
- Associar um plug-in opcional a um domínio e dissociar um plug-in opcional de um domínio
- Aumento da contagem de nós principais dedicados para domínios com dois nós principais dedicados e reconhecimento de zona ativado
- Diminuindo o tamanho do volume do EBS
- Alteração do tamanho do volume, IOPS ou taxa de transferência do EBS, se a última alteração feita estiver em andamento ou tiver ocorrido há menos de 6 horas
- Habilitando a publicação de registros de auditoria para CloudWatch.

Para domínios multi-AZ com modo de espera, você só pode fazer uma solicitação de alteração por vez. Se uma alteração já estiver em andamento, a nova solicitação será rejeitada. Você pode verificar o status da alteração atual com a API da `DescribeDomainChangeProgress`.

Alterações que normalmente não causam implantações azuis/verdes

Na maioria dos casos, as seguintes operações não causam implantações azuis/verdes:

- Alterar política de acesso
- Como modificar o endpoint personalizado
- Alterar política do Transport Layer Security (TLS)
- Alterar o horário do snapshot automatizado
- Habilitar ou desabilitar a opção Exigir HTTPS
- Habilitação do Auto-Tune ou desabilitação sem reverter suas alterações
- Se o seu domínio tiver nós mestres dedicados ou estiver alterando a contagem de UltraWarm nós
- Alterando a contagem de nós de dados
- Se seu domínio tiver nós principais dedicados, altere o tipo de instância principal dedicada ou a contagem de nós (exceto para domínios com dois mestres dedicados e reconhecimento de zona ativado)
- Ativar ou desativar a publicação de registros de erros ou registros lentos no CloudWatch
- Desabilitando a publicação de registros de auditoria no. CloudWatch
- Aumento do tamanho do volume, alteração do tipo de volume, IOPS e taxa de transferência para até 3 TiB por tamanho de volume do nó de dados

- Adicionar ou remover tags

> **Note**
>
> Há algumas exceções, dependendo da versão do software de serviço. Se você quiser ter certeza absoluta de que uma alteração não causará uma implantação azul/verde, execute uma execução seca antes de atualizar seu domínio, se essa opção estiver disponível. Algumas mudanças não oferecem a opção de funcionamento a seco. Geralmente, recomendamos que você faça alterações em seu cluster fora dos horários de pico de tráfego.

Determinar se uma alteração causará uma implantação azul/verde

Você pode testar alguns tipos de alterações de configuração planejadas para determinar se elas causarão uma implantação azul/verde, sem precisar se comprometer com essas alterações. Antes de iniciar uma alteração de configuração, use o console ou uma API para executar uma verificação de validação para garantir que o seu domínio seja qualificação para uma atualização.

Console

Para validar uma alteração na configuração

1. Navegue até o console do Amazon OpenSearch Service emhttps://console.aws.amazon.com/aos/.
2. No painel de navegação à esquerda, escolha Domínios.
3. Selecione o domínio para o qual deseja fazer uma alteração de configuração. Isso abre a página de detalhes do domínio. Selecione o menu suspenso Ações e escolha Editar configuração do cluster.
4. Na página Editar configuração do cluster, é possível fazer alterações no tipo de instância, no número de nós e em qualquer outra configuração. Depois de confirmar as suas alterações no painel de resumo, escolha Executar .
5. Quando a simulação estiver concluída, os resultados serão exibidos automaticamente no final da página, junto com um ID de simulação. Esses resultados notificam em qual categoria sua alteração se enquadra:

   - Inicia uma implantação azul/verde
   - Não exige uma implantação azul/verde

- Contém erros de validação que precisam ser resolvidos antes de salvar as alterações

Cada simulação substitui a anterior. Para consultar os detalhes de cada operação a seco posteriormente, salve seu ID de simulação. Cada simulação está disponível por 90 dias ou até que você faça uma atualização de configuração.

6. Para continuar com a atualização de configuração, escolha Salvar alterações. Caso contrário, escolha Cancelar. Qualquer uma das opções levará você de volta à guia Configuração do cluster . Nessa guia, você pode escolher Detalhes da simulação para ver os detalhes da última simulação. Essa página também inclui uma side-by-side comparação entre a configuração antes da operação a seco e a configuração da operação a seco.

API

Você pode executar uma validação de simulação por meio da API de configuração. Para testar suas alterações com a API, defina `DryRun ´`como `true` e `DryRunMode` como `Verbose`. O modo detalhado executa uma verificação de validação, além de determinar se a alteração iniciará uma implantação azul/verde. Por exemplo, essa UpdateDomainConfigsolicitação testa o tipo de implantação resultante da ativação UltraWarm:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/
config
{
   "ClusterConfig": {
    "WarmCount": 3,
    "WarmEnabled": true,
    "WarmType": "ultrawarm1.large.search"
   },
   "DryRun": true,
   "DryRunMode": "Verbose"
}
```

A solicitação executa uma verificação de validação e retorna o tipo de implantação que a alteração causará, mas na verdade não executa a atualização:

```
{
   "ClusterConfig": {
     ...
    },
   "DryRunResults": {
```

```
      "DeploymentType": "Blue/Green",
      "Message": "This change will require a blue/green deployment."
    }
}
```

Os possíveis tipos de implantação são:

- `Blue/Green`: a alteração causará uma implantação azul/verde.
- `DynamicUpdate`: a alteração não causará uma implantação azul/verde.
- `Undetermined`: o domínio ainda está em um estado de processamento, portanto, não é possível determinar o tipo de implantação.
- `None`: nenhuma alteração de configuração.

Se a validação falhar, ela retornará uma lista de falhas de validação.

```
{
   "ClusterConfig":{
      "..."
   },
   "DryRunProgressStatus":{
      "CreationDate":"2023-01-12T01:14:33.847Z",
      "DryRunId":"db00ca39-48b2-4774-bbd3-252cf094d205",
      "DryRunStatus":"failed",
      "UpdateDate":"2023-01-12T01:14:33.847Z",
      "ValidationFailures":[
         {
            "Code":"Cluster.Index.WriteBlock",
            "Message":"Cluster has index write blocks."
         }
      ]
   }
}
```

Se o status persistir`pending`, você poderá usar o ID de execução seca em sua UpdateDomainConfig resposta em DescribeDryRunProgresschamadas subsequentes para verificar o status da validação.

```
GET https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/
dryRun?dryRunId=my-dry-run-id
{
```

```
    "DryRunConfig": null,
    "DryRunProgressStatus": {
        "CreationDate": "2023-01-12T01:14:42.998Z",
        "DryRunId": "db00ca39-48b2-4774-bbd3-252cf094d205",
        "DryRunStatus": "succeeded",
        "UpdateDate": "2023-01-12T01:14:49.334Z",
        "ValidationFailures": null
    },
    "DryRunResults": {
        "DeploymentType": "Blue/Green",
        "Message": "This change will require a blue/green deployment."
    }
}
```

Para executar uma análise de simulação sem uma verificação de validação, defina `DryRunMode` como `Basic` quando usar a API de configuração.

Python

O código Python a seguir usa a UpdateDomainConfigAPI para realizar uma verificação de validação de execução seca e, se a verificação for bem-sucedida, chama a mesma API sem uma execução seca para iniciar a atualização. Se a verificação falhar, o script imprimirá o erro e será interrompido.

```
import time
import boto3

client = boto3.client('opensearch')

response = client.UpdateDomainConfig(
    ClusterConfig={
        'WarmCount': 3,
        'WarmEnabled': True,
        'WarmCount': 123,
    },
    DomainName='test-domain',
    DryRun=True,
    DryRunMode='Verbose'
)

dry_run_id = response.DryRunProgressStatus.DryRunId

retry_count = 0
```

```
while True:

    if retry_count == 5:
        print('An error occured')
        break

    dry_run_progress_response = client.DescribeDryRunProgress('test-domain',
 dry_run_id)
    dry_run_status = dry_run_progress_response.DryRunProgressStatus.DryRunStatus

    if dry_run_status == 'succeeded':
        client.UpdateDomainConfig(
            ClusterConfig={
            'WarmCount': 3,
            'WarmEnabled': True,
            'WarmCount': 123,
        })
        break

    elif dry_run_status == 'failed':
        validation_failures_list =
 dry_run_progress_response.DryRunProgressStatus.ValidationFailures
        for item in validation_failures_list:
            print(f"Code: {item['Code']}, Message: {item['Message']}")
        break

    retry_count += 1
    time.sleep(30)
```

Iniciando e rastreando uma alteração na configuração

> **Note**
>
> Você pode solicitar uma alteração de configuração por vez. Você também pode agrupar várias alterações de configuração em uma única solicitação. Aguarde até que o status do seu domínio se torne `Active` antes de solicitar qualquer alteração adicional na configuração.

Você pode visualizar os campos Domain Processing Status e Config Change Status no console do Amazon OpenSearch Service para rastrear alterações de domínio e configuração. Você também

pode acompanhar alterações de domínio e configuração por meio dos `ConfigChangeStatus` parâmetros `DomainProcessingStatus` e nas respostas da API. Para obter mais informações, consulte o tipo de DomainStatusdados na referência da API de OpenSearch serviço.

Visibilidade do status de processamento do domínio: você pode determinar facilmente o status da configuração de um domínio examinando o campo Status de processamento do domínio no console. Da mesma forma, o parâmetro `DomainProcessingStatus` da API pode ser usado para identificar o status. Os valores a seguir são status de processamento de um domínio:

- `Active`: Nenhuma alteração na configuração está em andamento. Você pode enviar uma nova solicitação de alteração de configuração.
- `Creating`: O domínio está sendo criado.
- `Modifying`: mudanças na configuração, como a adição de novos nós de dados, EBS, gp3, provisionamento de IOPS ou configuração de chaves KMS, estão em andamento.

> **Note**
>
> Você pode ver o status como `Modifying` em situações em que um domínio exige movimentação de fragmentos para concluir as alterações de configuração. Para compatibilidade com versões anteriores, o comportamento do `Processing` parâmetro é mantido inalterado nas respostas da API e definido como falso assim que as alterações da configuração principal são concluídas, sem esperar pela conclusão da movimentação do fragmento.

- `Upgrading Engine Version`: Uma atualização da versão do motor está em andamento.
- `Updating Service Software`: Uma atualização do software de serviço está em andamento.
- `Deleting`: O domínio está sendo excluído.
- `Isolated`: O domínio está suspenso.

Visibilidade do status da configuração: as alterações na configuração podem ser iniciadas pelo operador (por exemplo, adição de novo nó de dados, alteração do tipo de instância) ou pelo serviço (por exemplo, ajuste automático e atualizações fora do horário de pico). Você pode encontrar o status dos detalhes mais recentes da alteração de configuração no campo Status da alteração da configuração do console do Amazon OpenSearch Service e na resposta da `ConfigChangeStatus` API. Os valores a seguir indicam o status da configuração de um domínio:

- `Pending`: uma solicitação de alteração de configuração foi enviada.

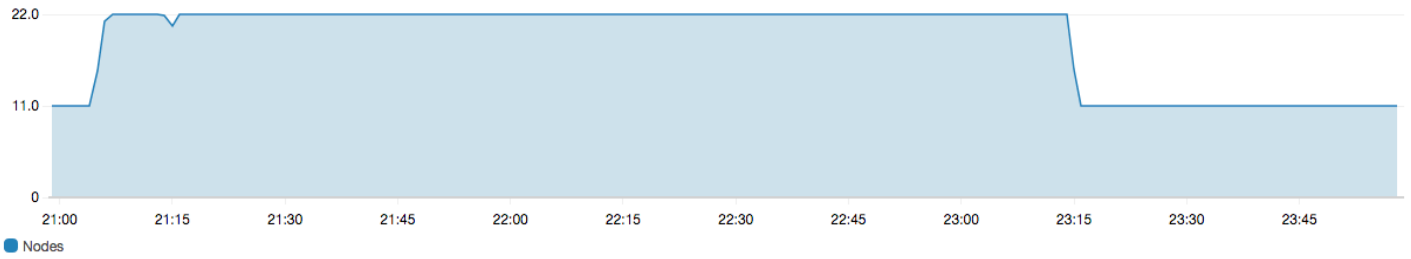
- `Initializing`: o serviço está inicializando uma solicitação de alteração de configuração.
- `Validating`: o serviço está validando as alterações solicitadas e os recursos necessários.
- `Awaiting user inputs`: se aplica quando o operador espera que algumas alterações na configuração, como a alteração do tipo de instância, prossigam. Você pode editar as alterações de configuração.
- `Applying changes`: O serviço está aplicando as alterações de configuração solicitadas.
- `Cancelled`: A alteração na configuração foi cancelada. Se você receber o status de falha na validação, poderá clicar em Cancelar no console ou chamar a operação da `CancelDomainConfigChange` API. Se você fizer isso, todas as alterações aplicadas serão revertidas.
- `Completed`: as alterações de configuração solicitadas foram concluídas com sucesso.
- `Validation Failed`: Falha na validação das alterações solicitadas. Nenhuma alteração de configuração é aplicada.

> **Note**
>
> Falhas de validação podem ser o resultado de índices vermelhos presentes em seu domínio, indisponibilidade de um tipo de instância escolhido ou pouco espaço em disco. Para obter uma lista de erros de validação, consultethe section called “Solução de problemas de erros de validação”. Durante um evento de falha na validação, você pode cancelar, tentar novamente ou editar alterações na configuração.

Resumo da API: você pode usar as operações `DescribeDomainDescribeDomainChangeProgress`, e `DescribeDomainConfig` da API para obter status detalhados de atualização de configuração. Além disso, você pode usar `CancelDomainConfigChange` para cancelar as atualizações em caso de falhas na validação. Para obter mais informações, consulte a documentação da API OpenSearch Service

Quando as alterações de configuração são concluídas, o estado do domínio volta para. `Active`

Você pode analisar a integridade do cluster e CloudWatch as métricas da Amazon e ver que o número de nós no cluster aumenta temporariamente, geralmente dobrando, enquanto a atualização do domínio ocorre. No exemplo a seguir, você pode ver o número de nós que dobram de 11 para 22 durante uma alteração de configuração e que retornam para 11 quando a atualização é concluída.



Esse aumento temporário pode sobrecarregar os nós principais dedicados do cluster, que repentinamente poderão ter muito mais nós para gerenciar. Também pode aumentar as latências de pesquisa e indexação à medida que o OpenSearch Service copia dados do cluster antigo para o novo. É importante manter capacidade suficiente no cluster para lidar com a sobrecarga associada a essas implantações azuis/verdes.

> **Important**
>
> Não há nenhuma cobrança adicional nas alterações de configuração e na manutenção do serviço. Você será cobrado apenas pelo número de nós que solicitar para seu cluster. Para obter detalhes, consulte the section called “Cobranças para alterações de configuração”.

Para evitar a sobrecarga de nós principais dedicados, você pode monitorar o uso com as CloudWatch métricas da Amazon. Para obter os valores máximos recomendados, consulte the section called “ CloudWatch Alarmes recomendados”.

Etapas de uma alteração de configuração

Depois de iniciar uma alteração na configuração, o OpenSearch Service passa por uma série de etapas para atualizar seu domínio. Você pode ver o progresso da alteração de configuração em Status de alteração de configuração no console. As etapas exatas para a realização de uma atualização depende do tipo de alteração que você está fazendo. Você também pode monitorar uma alteração na configuração usando a operação DescribeDomainChangeProgressda API.

A seguir, estão as possíveis etapas de uma atualização durante uma alteração de configuração:

Nome da etapa	Descrição
Validação	Validação se o domínio

Nome da etapa	Descrição
	está qualificado para uma atualização e identificação de problemas de validação, se necessário.
Criação de um novo ambiente	Cumprimento dos pré-requisitos exigidos e criação dos recursos necessários para iniciar a implantação azul/verde.
Provisionamento de novos nós	Criando um novo conjunto de instâncias no novo ambiente.
Roteamento de tráfego em novos nós	Redirecionamento do tráfego para os nós de dados recém-criados.
Roteamento de tráfego em nós antigos	Desabilitação tráfego em nós de dados antigos.

Nome da etapa	Descrição
Preparação dos nós para remoção	Preparação para a remoção de nós. Esta etapa só ocorre quando você reduz a escala do seu domínio (por exemplo, de 8 nós para 6 nós).
Cópia de fragmentos para novos nós	Transferência de fragmentos dos nós antigos para os novos nós.
Encerramento de nós	Encerramento e exclusão de nós antigos após a remoção dos fragmentos.
Exclusão de recursos mais antigos	Exclusão de recursos associados ao ambiente antigo (por exemplo, o balanceador de carga).

Nome da etapa	Descrição
Atualização dinâmica	Eles serão exibidos quando a atualização não exigir uma implantação azul/verde e eles forem aplicáveis dinamicam ente.
Aplicando alterações dedicadas relacionadas à entidade principal	Exibido quando o tipo ou a contagem de instância s principais dedicadas são alterados.
Aplicar alterações relacionadas ao volume	Exibido quando o tamanho, o tipo, o IOPS e o throughput do volume são alterados.

Cobranças para alterações de configuração

Se você alterar a configuração de um domínio, o OpenSearch Service criará um novo cluster conforme descrito emthe section called “Alterações de configuração”. Durante a migração do antigo para o novo, você é cobrado pelos seguintes encargos:

- Se você alterar o tipo de instância, será cobrado por ambos os clusters para a primeira hora. Após a primeira hora, você será cobrado apenas pelo novo cluster. Os volumes do EBS não são cobrados duas vezes porque fazem parte do cluster. Portanto, o faturamento segue o faturamento da instância.

  Exemplo: Você altera a configuração de três instâncias `m3.xlarge` para quatro instâncias `m4.large`. Na primeira hora, você é cobrado por ambos os clusters (3 * `m3.xlarge` + 4 * `m4.large`). Após a primeira hora, você será cobrado apenas pelo novo cluster (4 * `m4.large`).
- Se você não alterar o tipo de instância, será cobrado apenas pelo cluster maior para a primeira hora. Após a primeira hora, você será cobrado apenas pelo novo cluster.

  Exemplo: Você altera a configuração de seis instâncias `m3.xlarge` para três instâncias `m3.xlarge`. Para a primeira hora, você será cobrado pelo cluster maior (6 * `m3.xlarge`). Após a primeira hora, você será cobrado apenas pelo novo cluster (3 * `m3.xlarge`).

Solução de problemas de erros de validação

Quando você inicia uma alteração na configuração ou realiza uma OpenSearch atualização de versão do Elasticsearch, o OpenSearch Service primeiro executa uma série de verificações de validação para garantir que seu domínio esteja qualificado para uma atualização. Se alguma dessas verificações falhar, você receberá uma notificação no console contendo os problemas específicos que deverão ser corrigidos antes da atualização do domínio. A tabela a seguir lista os possíveis problemas de domínio que o OpenSearch Serviço pode surgir e as etapas para resolvê-los.

Problema	Código de erro	Etapas de solução de problemas
Grupo de segurança não encontrado	`SecurityGroupNotFound`	O grupo de segurança associado ao seu domínio de OpenSearch serviço não existe. Para resolver esse problema, crie um grupo de segurança com o nome especificado.
Sub-rede não encontrada	`SubnetNotFound`	A sub-rede associada ao seu domínio OpenSearch de serviço não existe. Para resolver esse problema, crie uma sub-rede na sua VPC.

Problema	Código de erro	Etapas de solução de problemas
Função vinculada ao serviço não configurada	`SLRNotConfigured`	A função vinculada ao OpenSearch serviço para Serviço não está configurada. A função vinculada ao serviço é predefinida pelo OpenSearch Serviço e inclui todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome. Se a função não existir, talvez seja necessário criá-la manualmente.
Não há endereços IP suficientes	`InsufficientFreeIPsForSubnets`	Uma ou mais sub-redes da VPC não têm endereços IP suficientes para atualizar seu domínio. Para calcular quantos endereços IP são necessários, consulte the section called “Reserva de endereços IP em uma sub-rede da VPC”.
O grupo de usuários do Cognito não existe	`CognitoUserPoolNotFound`	OpenSearch O serviço não consegue encontrar o grupo de usuários do Amazon Cognito. Confirme se você criou um e se tem o ID correto. Para encontrar o ID, você pode usar o console do Amazon Cognito ou o seguinte comando da AWS CLI : `aws cognito-idp list-user-pools --max-results 60 --region us-east-1`
O grupo de identidades do Cognito não existe	`CognitoIdentityPoolNotFound`	OpenSearch O serviço não consegue encontrar o pool de identidade do Cognito. Confirme se você criou um e se tem o ID correto. Para encontrar o ID, você pode usar o console do Amazon Cognito ou o seguinte comando da AWS CLI : `aws cognito-identity list-identity-pools --max-results 60 --region us-east-1`

Problema	Código de erro	Etapas de solução de problemas
Domínio do Cognito não encontrado para grupo de usuários	`CognitoDomainNotFound`	O grupo de usuários não tem um nome de domínio. Você pode configurar um usando o console do Amazon Cognito ou o seguinte comando: AWS CLI `aws cognito-idp create-user-pool-domain --domain my-domain --user-pool-id id`
Função do Cognito não configurada	`CognitoRoleNotConfigured`	A função do IAM que OpenSearch concede permissão ao Serviço para configurar os grupos de usuários e identidades do Amazon Cognito e usá-los para autenticação não está configurada. Configure a função com um conjunto de permissões e uma relação de confiança apropriados. Você pode usar o console, que cria a CognitoAccessForAmazonOpenSearchfunção padrão para você, ou pode configurar manualmente uma função usando o AWS CLI ou o AWS SDK.
Não é possível descrever o grupo de usuários	`UserPoolNotDescribable`	A função especificada do Amazon Cognito não tem permissão para descrever o grupo de usuários associado ao seu domínio. Verifique se a política de permissões da função permite a ação `cognito-identity:DescribeUserPool` . Consulte the section called “Sobre a função CognitoAccessForAmazonOpenSearch” para ver a política de permissões completa.
Não é possível descrever o grupo de identidades	`IdentityPoolNotDescribable`	A função especificada do Amazon Cognito não tem permissão para descrever o grupo de identidades associado ao seu domínio. Verifique se a política de permissões da função permite a ação `cognito-identity:DescribeIdentityPool` . Consulte the section called “Sobre a função CognitoAccessForAmazonOpenSearch” para ver a política de permissões completa.

Problema	Código de erro	Etapas de solução de problemas
Não é possível descrever os grupos usuários e de identidades	`CognitoPoolsNotDescribable`	A função especificada do Amazon Cognito não tem permissão para descrever os grupos de usuários e de identidades associados ao seu domínio. Verifique se a política de permissões da função permite as ações `cognito-identity:DescribeIdentityPool` e `cognito-identity:DescribeUserPool` . Consulte the section called “Sobre a função CognitoAccessForAmazonOpenSearch” para ver a política de permissões completa.
A chave do KMS não está habilitada	`KMSKeyNotEnabled`	A chave AWS Key Management Service (AWS KMS) usada para criptografar seu domínio está desativada. Reative a chave imediatamente.
O certificado personalizado não está no estado ISSUED (EMITIDO)	`InvalidCertificate`	Se seu domínio usa um endpoint personalizado, você o protege gerando um certificado SSL no AWS Certificate Manager (ACM) ou importando um de sua preferência. O status do certificado deve ser Emitido. Ao receber esse erro, verifique o status do certificado no console do ACM. Se o status for Expired (Expirado), Failed (Com falha), Inactive (Inativo) ou Pending validation (Validação pendente), consulte a documentação de solução de problemas do ACM para resolver o problema.
Capacidade insuficiente para iniciar o tipo de instância escolhido	`InsufficientInstanceCapacity`	A capacidade do tipo de instância solicitada não está disponível. Por exemplo, você pode ter solicitado cinco `i3.16xlarge.search` nós, mas o OpenSearch Serviço não tem `i3.16xlarge.search` hosts suficientes disponíveis, então a solicitação não pode ser atendida. Verifique os tipos de instância compatíveis em OpenSearch Service e escolha um tipo de instância diferente.

Problema	Código de erro	Etapas de solução de problemas
Índices vermelhos no cluster	`RedCluster`	Um ou mais índices em seu cluster têm um status vermelho, o que leva a um status geral de cluster vermelho. Para solucionar e corrigir esse problema, consulte the section called “Status de cluster vermelho”.
Disjuntor de memória, excesso de solicitações	`TooManyRequests`	Há muitas solicitações de pesquisa e gravação em seu domínio, então o OpenSearch Serviço não pode atualizar sua configuração. É possível reduzir o número de solicitações, aumentar instâncias na vertical até 64 GiB de RAM ou aumentar a escala na horizontal adicionando instâncias.
A nova configuração não pode acomodar os dados (pouco espaço em disco)	`InsufficientStorageCapacity`	O tamanho de armazenamento configurado não é capaz de acomodar todos os dados no seu domínio. Para resolver esse problema, escolha um volume maior, exclua índices não utilizados ou aumente o número de nós no cluster para liberar espaço em disco imediatamente.

Problema	Código de erro	Etapas de solução de problemas

Fragmentos fixados em nós específicos	`ShardMovementBlocked`	Um ou mais índices em seu domínio estão anexados a nós específicos e não podem ser reatribuídos. Isso provavelmente aconteceu porque você configurou a filtragem de alocação de fragmentos, que permite especificar quais nós têm permissão para hospedar os fragmentos de um índice específico.
		
		Para resolver esse problema, remova os filtros de alocação de fragmentos de todos os índices afetados:
		
		`PUT my-index/_settings`
		`{`
		`  "settings": {`
		`  "index.routing.allocation.require._name": null`
		`  }`
		`}`

A nova configuração não pode conter todos os fragmentos (contagem de fragmentos)	`TooManyShards`	A contagem de fragmentos em seu domínio é muito alta, o que impede que o OpenSearch Serviço os mova para a nova configuração. Para resolver esse problema, dimensione seu domínio horizontalmente adicionando nós do mesmo tipo de configuração que os nós de cluster atuais. Observe que o tamanho máximo do volume do EBS depende do tipo de instância do nó. Para evitar esse problema no futuro, consulte the section called “Como escolher o número de fragmentos” e defina uma estratégia de fragmentação que seja apropriada para o seu caso de uso.

Problema	Código de erro	Etapas de solução de problemas
A sub-rede associada ao seu domínio não oferece suporte a endereços IPv4	`ResultCodeIPv4BlockNotExists`	Para resolver esse problema, crie uma sub-rede ou atualize a sub-rede existente na sua VPC, de acordo com o tipo de endereço IP configurado do domínio. Se o domínio usa um tipo de endereço somente IPv4, use uma sub-rede somente IPv4. Se o domínio usa o modo de pilha dupla, use uma sub-rede de pilha dupla.
A sub-rede associada ao seu domínio não oferece suporte a endereços IPv6	`ResultCodeIPv6BlockNotExists`	Para resolver esse problema, crie uma sub-rede ou atualize a sub-rede existente na sua VPC, de acordo com o tipo de endereço IP configurado do domínio. Se o domínio usa um tipo de endereço somente IPv4, use uma sub-rede somente IPv4. Se o domínio usa o modo de pilha dupla, use uma sub-rede de pilha dupla.

Atualizações do software de serviço no Amazon OpenSearch Service

> **Note**
>
> Consulte as notas de versão para obter explicações sobre as alterações e adições feitas em cada atualização principal do software do serviço (sem patch).

O Amazon OpenSearch Service lança regularmente atualizações de software de serviços que adicionam recursos ou melhoram seus domínios. O painel Notificações no console é a maneira mais fácil de ver se uma atualização está disponível ou verificar o status de uma atualização. Cada

notificação inclui detalhes sobre a atualização do software de serviço. Todas as atualizações de software de serviço usam implantações azul/verde para minimizar o tempo de inatividade.

As atualizações do software de serviço são diferentes das atualizações de OpenSearch versão. Para obter informações sobre a atualização para uma versão posterior do OpenSearch, consultethe section called “Atualização de domínios”.

Tópicos

Atualizações opcionais x obrigatórias

OpenSearch O serviço tem duas grandes categorias de atualizações de software de serviço:

Atualizações opcionais

As atualizações opcionais do software de serviço geralmente incluem aprimoramentos e suporte para novos atributos ou funcionalidades. As atualizações opcionais não são aplicadas aos seus domínios e não há um prazo fixo para instalá-las. A disponibilidade da atualização é comunicada por e-mail e uma notificação no console. Você pode optar por aplicar a atualização imediatamente ou reagendá-la para uma data e hora mais convenientes. Você também pode programá-la durante a janela fora do horário de pico do domínio. A maioria das atualizações de software é opcional.

Independentemente de você agendar ou não uma atualização, se você fizer uma alteração no domínio que cause uma implantação azul/verde, o OpenSearch Service atualizará automaticamente o software do serviço para você.

Você pode configurar seu domínio para aplicar automaticamente atualizações opcionais fora do horário de pico. Quando essa opção está ativada, o OpenSearch Serviço espera pelo menos 13 dias a partir do momento em que uma atualização opcional está disponível e, em seguida, agenda a

atualização após 72 horas (três dias). Você recebe uma notificação do console quando a atualização é agendada e pode optar por reagendá-la para uma data posterior.

Para ativar as atualizações automáticas de software, selecione Habilitar atualização automática de software ao criar ou atualizar seu domínio. Para definir a mesma configuração usando o AWS CLI, `--software-update-options` defina como `true` quando você cria ou atualiza seu domínio.

Atualizações necessárias

As atualizações obrigatórias de software de serviço geralmente incluem correções críticas de segurança ou outras atualizações indispensáveis para garantir a integridade e a funcionalidade contínuas do seu domínio. Exemplos de atualizações necessárias são vulnerabilidades e exposições comuns do Log4j (CVEs) e a aplicação do Instance Metadata Service Version 2 (IMDSv2). O número de atualizações obrigatórias em um ano geralmente é menor que três.

OpenSearch O serviço agenda automaticamente essas atualizações e notifica você 72 horas (três dias) antes da atualização agendada por e-mail e uma notificação do console. Você pode optar por aplicar a atualização imediatamente ou reprogramá-la para uma data e hora mais convenientes dentro do prazo permitido. Você também pode programá-la durante a próxima janela fora do horário de pico do domínio. Se você não realizar nenhuma ação em relação à atualização necessária e não fizer nenhuma alteração no domínio que cause uma implantação azul/verde, o OpenSearch Serviço poderá iniciar a atualização a qualquer momento além do prazo especificado (normalmente 14 dias a partir da disponibilidade), dentro da janela fora do pico do domínio.

Independentemente de quando a atualização está agendada, se você fizer uma alteração no domínio que cause uma implantação azul/verde, o OpenSearch Service atualizará automaticamente seu domínio para você.

Atualizações de patch

As versões de software de serviço que terminam em “-P” e um número, como R20211203-*P4*, são lançamentos de patches. É provável que os patches incluam melhorias de performance, pequenas correções de bugs e correções de segurança ou melhorias de postura. As versões de patch não incluem novos atributos ou alterações significativas e geralmente não têm um impacto direto ou perceptível para os usuários. A notificação do software de serviço informa se a versão de um patch é opcional ou obrigatória.

Considerações

Considere o seguinte ao decidir se deseja atualizar seu domínio:

- A atualização manual do seu domínio permite aproveitar os novos recursos mais rapidamente. Quando você escolhe Atualizar, o OpenSearch Serviço coloca a solicitação em uma fila e inicia a atualização quando tiver tempo.
- Quando você inicia uma atualização do software do OpenSearch serviço, o Serviço envia uma notificação quando a atualização é iniciada e concluída.
- As atualizações de software usam implantações azul/verde para minimizar o tempo de inatividade. As atualizações podem sobrecarregar temporariamente os nós principais dedicados de um cluster. Por isso, certifique-se de manter capacidade suficiente para lidar com a sobrecarga associada.
- Normalmente, as atualizações são concluídas em minutos, mas também podem levar várias horas ou até dias se o sistema estiver lidando com muita carga. Considere atualizar seu domínio durante a janela fora do horário de pico para evitar longos períodos de atualização.

Iniciar uma atualização do software de serviço

Você pode solicitar uma atualização do software de serviço por meio do console de OpenSearch serviço AWS CLI, do ou de um dos SDKs.

Console

Solicitar uma atualização de software de serviço

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. Selecione o nome do domínio para abrir a configuração.
3. Escolha Ações, Atualizar e selecione uma das seguintes opções:
   - Aplicar a atualização agora: programa a ação para acontecer imediatamente, se houver capacidade disponível. Se a capacidade não estiver disponível, outros slots de horários disponíveis serão sugeridos.
   - Agendar fora do horário de pico: disponível somente se a janela fora do horário de pico estiver ativada para o domínio. Agenda a atualização para ocorrer durante a janela fora do horário de pico configurada do domínio. Não há garantia de que a atualização ocorrerá durante a próxima janela imediata. Dependendo da capacidade, isso pode acontecer nos dias subsequentes. Para ter mais informações, consulte the section called “Janelas fora do horário de pico”.

- Agendar para data e hora específicas agenda a atualização para ocorrer em uma data e hora específicas. Se o horário especificado não estiver disponível por motivos de capacidade, você poderá selecionar um slot de horário diferente.

Se você agendar a atualização para uma data posterior (dentro ou fora da janela de horário de pico do domínio), poderá reagendá-la a qualquer momento. Para obter instruções, consulte the section called “Ações de reagendamento”.

4. Selecione a opção Confirmar.

AWS CLI

Envie uma start-service-software-update AWS CLI solicitação para iniciar uma atualização do software de serviço. Este exemplo adiciona a atualização à fila imediatamente:

```
aws opensearch start-service-software-update \
  --domain-name my-domain \
  --schedule-at "NOW"
```

Resposta:

```
{
    "ServiceSoftwareOptions": {
        "CurrentVersion": "R20220928-P1",
        "NewVersion": "R20220928-P2",
        "UpdateAvailable": true,
        "Cancellable": true,
        "UpdateStatus": "PENDING_UPDATE",
        "Description": "",
        "AutomatedUpdateDate": "1969-12-31T16:00:00-08:00",
        "OptionalDeployment": true
    }
}
```

Tip

Depois de solicitar uma atualização, você tem um período de tempo limitado para cancelá-la. A duração desse `PENDING_UPDATE` estado pode variar muito e depende de você Região da AWS e do número de atualizações simultâneas que o OpenSearch Serviço está executando.

Para cancelar uma atualização, use o console ou o `cancel-service-software-update` AWS CLI comando.

Se a solicitação falhar com uma `BaseException`, isso significa que o horário especificado não está disponível por motivos de capacidade e você deve especificar um horário diferente. OpenSearch O serviço fornece sugestões alternativas de slots disponíveis na resposta.

AWS SDKs

Esse exemplo de script Python usa os métodos describe_domain e start_service_software_update do AWS SDK for Python (Boto3) para verificar se um domínio está qualificado para uma atualização do software de serviço e, em caso afirmativo, inicia a atualização. Você deve fornecer um valor para `domain_name`:

```
import boto3
from botocore.config import Config
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a Region other than your default.
    region_name='us-east-1'
)

domain_name = ''  # The name of the domain to check and update

client = boto3.client('opensearch', config=my_config)


def getUpdateStatus(client):
    """Determines whether the domain is eligible for an update"""
    response = client.describe_domain(
        DomainName=domain_name
    )
    sso = response['DomainStatus']['ServiceSoftwareOptions']
    if sso['UpdateStatus'] == 'ELIGIBLE':
        print('Domain [' + domain_name + '] is eligible for a service software update
 from version ' +
```

```
                sso['CurrentVersion'] + ' to version ' + sso['NewVersion'])
        updateDomain(client)
    else:
        print('Domain is not eligible for an update at this time.')


def updateDomain(client):
    """Starts a service software update for the eligible domain"""
    response = client.start_service_software_update(
        DomainName=domain_name
    )
    print('Updating domain [' + domain_name + '] to version ' +
          response['ServiceSoftwareOptions']['NewVersion'] + '...')
    waitForUpdate(client)


def waitForUpdate(client):
    """Waits for the domain to finish updating"""
    response = client.describe_domain(
        DomainName=domain_name
    )
    status = response['DomainStatus']['ServiceSoftwareOptions']['UpdateStatus']
    if status == 'PENDING_UPDATE' or status == 'IN_PROGRESS':
        time.sleep(30)
        waitForUpdate(client)
    elif status == 'COMPLETED':
        print('Domain [' + domain_name +
              '] successfully updated to the latest software version')
    else:
        print('Domain is not currently being updated.')

def main():
    getUpdateStatus(client)
```

Agendamento de atualizações do software fora do horário de pico

Cada domínio do OpenSearch Serviço criado após 16 de fevereiro de 2023 tem uma janela diária de 10 horas entre 22h e 8h, horário local, que consideramos a janela fora de pico. OpenSearch O serviço usa essa janela para agendar atualizações do software do serviço para o domínio. As atualizações fora do pico ajudam a minimizar a sobrecarga nos nós principais dedicados de um cluster durante períodos de maior tráfego. OpenSearch O serviço não pode iniciar atualizações fora dessa janela de 10 horas sem o seu consentimento.

- Para atualizações opcionais, o OpenSearch Serviço notifica você sobre a disponibilidade da atualização e solicita que você agende a atualização durante um próximo período fora de pico.
- Para as atualizações necessárias, o OpenSearch Serviço agenda automaticamente a atualização durante uma próxima janela fora de pico e notifica você com três dias de antecedência. Você pode reagendar a atualização (dentro ou fora da janela de pico), mas somente dentro do prazo necessário para que a atualização seja concluída.

Para cada domínio, você pode optar por substituir o horário de início padrão das 22h por um horário personalizado. Para obter instruções, consulte the section called “Configurar uma janela personalizada fora do horário de pico”.

Console

Como agendar uma atualização durante uma próxima janela fora do horário de pico

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. Selecione o nome do domínio para abrir a configuração.
3. Escolha Ações, Atualizar.
4. Selecione Agendar em uma janela fora do horário de pico.
5. Selecione a opção Confirmar.

Você pode visualizar a ação agendada na guia Janela fora do horário de pico e reagendá-la a qualquer momento. Consulte the section called “Exibir ações programadas”.

CLI

Para agendar uma atualização durante uma próxima janela fora de pico usando o AWS CLI, envie uma StartServiceSoftwareUpdatesolicitação e especifique `OFF_PEAK_WINDOW` o `--schedule-at` parâmetro:

```
aws opensearch start-service-software-update \
  --domain-name my-domain \
  --schedule-at "OFF_PEAK_WINDOW"
```

Monitoramento das atualizações de software de serviço

OpenSearch O serviço envia uma notificação quando uma atualização do software do serviço está disponível, é necessária, iniciada, concluída ou falha. Você pode ver essas notificações no painel

Notificações do console OpenSearch de serviço. A gravidade da notificação será `Informational` se a atualização for opcional e `High` se ela for necessária.

OpenSearch O serviço também envia eventos de software de serviço para a Amazon EventBridge. Você pode usar EventBridge para configurar regras que enviam um e-mail ou executam uma ação específica quando um evento é recebido. Para ver uma demonstração de exemplo, consulte the section called “Tutorial: Envio de alertas do SNS para atualizações disponíveis”.

Para ver o formato de cada evento de software de serviço enviado para a Amazon EventBridge, consultethe section called “Eventos de atualização de software de serviço”.

Quando os domínios não são elegíveis para uma atualização

Seu domínio poderá ser inelegível para um serviço de atualização de software se ele estiver em qualquer um dos seguintes estados:

Estado	Descrição
Domínio no processamento	O domínio está no meio de uma mudança de configuração. Verifique a qualificação da atualização após a conclusão da operação.
Status de cluster vermelho	Um ou mais índices no cluster estão vermelhos. Para obter etapas sobre a solução de problemas, consulte the section called “Status de cluster vermelho”.
Alta taxa de erros	O OpenSearch cluster está retornando um grande número de 5 erros xx ao tentar processar solicitações. Geralmente, esse problema é resultado de muitas solicitações de leitura ou gravação simultâneas. Considere reduzir o tráfego para o cluster ou dimensionar seu domínio.
Cérebro dividido	Cérebro dividido significa que seu OpenSearch cluster tem mais de um nó principal e se dividiu em dois clusters que nunca se reunirão sozinhos. Você pode evitar dividir o cérebro usando o número recomendado de nós principais dedicados. Para ajudar na recuperação do cérebro dividido, entre em contato com AWS Support.
Problema de integração do Amazon Cognito	Seu domínio usa autenticação para OpenSearch painéis, e o OpenSearch Service não consegue encontrar um ou mais recursos do Amazon Cognito. Este problema normalmente ocorre quando o grupo de usuários

Estado	Descrição
	do Amazon Cognito está ausente. Para corrigir o problema, recrie o recurso ausente e configure o domínio do OpenSearch serviço para usá-lo.
Outro problema de serviço do	Problemas com o OpenSearch serviço em si podem fazer com que seu domínio seja exibido como inelegível para uma atualização. Se nenhuma das condições anteriores se aplicar ao seu domínio e o problema persistir por mais de um dia, entre em contato com o AWS Support.

Definindo períodos fora de pico para o Amazon Service OpenSearch

Ao criar um domínio do Amazon OpenSearch Service, você define uma janela diária de 10 horas que é considerada fora do horário de pico. OpenSearch O serviço usa essa janela para agendar atualizações de software de serviço e otimizações de ajuste automático que exigem uma implantação azul/verde durante períodos de tráfego comparativamente mais baixos, sempre que possível. Azul/verde refere-se ao processo de criar um novo ambiente para atualizações de domínio e rotear usuários para o novo ambiente assim que essas atualizações são concluídas.

Embora as implantações azul/verde não causem interrupções, para minimizar qualquer impacto potencial no desempenho enquanto os recursos estão sendo consumidos por uma implantação azul/verde, recomendamos que você agende essas implantações durante a janela fora do horário de pico configurada para o domínio. Atualizações como substituições de nós ou que precisem ser implantadas no domínio imediatamente não usam a janela fora do horário de pico.

Você pode modificar a hora de início da janela fora do horário de pico, mas não pode modificar o comprimento da janela.

> **Note**
>
> As janelas fora do horário de pico foram introduzidas em 16 de fevereiro de 2023. Todos os domínios criados antes dessa data têm a janela fora do horário de pico desativada por padrão. Você deve ativar e configurar manualmente a janela fora do horário de pico para esses domínios. Todos os domínios criados após essa data terão a janela fora do horário

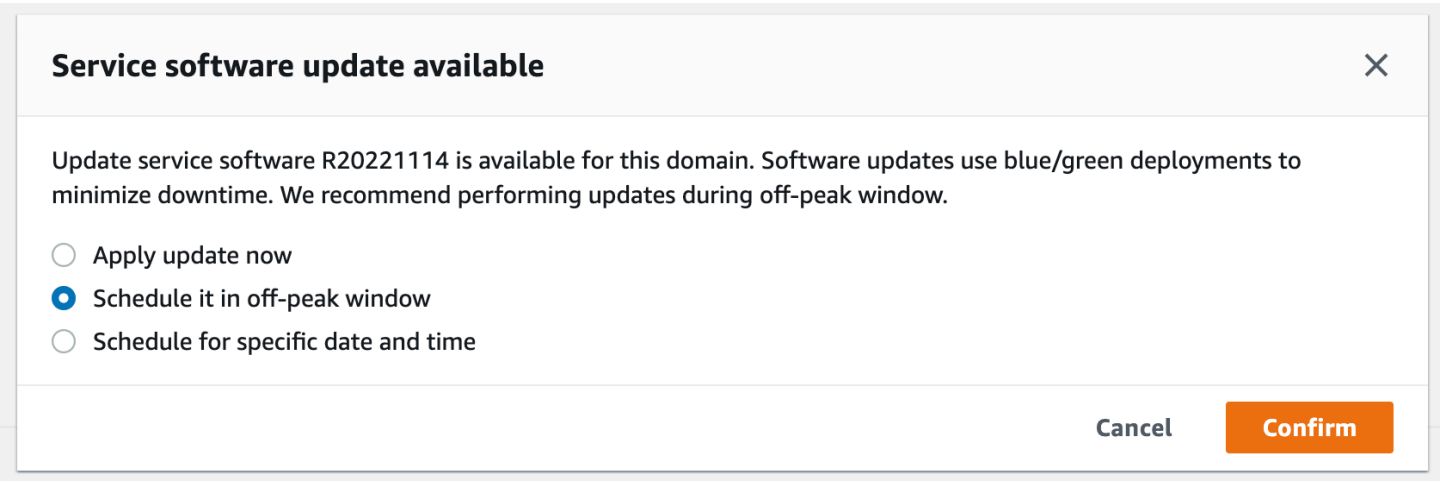
de pico ativada por padrão. Você não pode desativar a janela fora do horário de pico de um domínio depois que ela for ativada.

Tópicos

Atualizações de software de serviço fora do horário de pico

OpenSearch O serviço tem duas grandes categorias de atualizações de software de serviço — opcionais e obrigatórias. Ambos os tipos exigem implantações azul/verde. As atualizações opcionais não são aplicadas em seus domínios, enquanto as atualizações obrigatórias são instaladas automaticamente se você não realizar nenhuma ação antes do prazo especificado (normalmente duas semanas após a disponibilidade). Para ter mais informações, consulte the section called "Atualizações opcionais x obrigatórias".

Ao iniciar uma atualização opcional, você tem a opção de aplicá-la imediatamente, programá-la para uma janela subsequente fora do horário de pico ou especificar uma data e hora personalizadas.



Para as atualizações necessárias, o OpenSearch Serviço agenda automaticamente uma data e hora fora do horário de pico para realizar a atualização. Você recebe uma notificação três dias antes da atualização agendada e pode optar por reagendá-la para uma data e hora posteriores dentro do período de implantação necessário. Para obter instruções, consulte the section called “Ações de reagendamento”.

Otimizações do Auto-Tune fora do horário de pico

Anteriormente, o Auto-Tune usava janelas de manutenção para programar mudanças que exigiam uma implantação azul/verde. Os domínios que já tinham o ajuste automático e as janelas de manutenção ativadas antes da introdução das janelas fora do horário de pico continuarão usando janelas de manutenção para essas atualizações, a menos que você os migre para usar a janela fora do horário de pico.

Recomendamos que você migre seus domínios para usar a janela fora do horário de pico, pois ela é usada para agendar outras atividades no domínio, como atualizações de software de serviço. Para obter instruções, consulte the section called “Migração das janelas de manutenção do Auto-Tune”. Você não pode voltar a usar as janelas de manutenção depois de migrar seu domínio para a janela fora do horário de pico.

Todos os domínios criados após 16 de fevereiro de 2023 usarão a janela fora do horário de pico, em vez das janelas de manutenção, para realizar implantações azul/verdes. Você não pode desativar a janela fora do horário de pico de um domínio. Para obter uma lista de otimizações do Auto-Tune que exigem implantações azul/verde, consulte the section called “Tipos de alterações”.

Ativar a janela fora do horário de pico

Todos os domínios criados antes de 16 de fevereiro de 2023 (quando os períodos fora do horário de pico foram introduzidos) têm o atributo desativado por padrão. Você deve habilitá-lo manualmente para esses domínios. Você não pode desativar a janela fora do horário de pico depois de ativada.

Console

Para ativar a janela fora do horário de pico de um domínio

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. Selecione o nome do domínio para abrir a configuração.
3. Navegue até a guia Janela fora do horário de pico e escolha Editar.

4. Especifique o horário de início customizado em Tempo Universal Coordenado (UTC). Por exemplo, para configurar um horário de início às 23h30 na região Oeste dos EUA (Oregon), especifique 07h30
5. Escolha Salvar alterações.

CLI

Para modificar a janela fora do pico usando oAWS CLI, envie uma UpdateDomainConfigsolicitação:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --off-peak-window-options 'Enabled=true,
 OffPeakWindow={WindowStartTime={Hours=02,Minutes=00}}'
```

Se você não especificar um horário de início de janela personalizado, o padrão será 0h UTC.

Configurar uma janela personalizada fora do horário de pico

Você especifica uma janela personalizada fora do horário de pico para o domínio de acordo com o fuso horário UTC (Tempo Universal Coordenado). Por exemplo, se você quiser que o período comece às 23h para um domínio na região leste dos EUA (Norte da Virgínia), você deverá especificar às 04h UTC.

Console

Para modificar a janela fora do horário de pico de um domínio

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. Selecione o nome do domínio para abrir a configuração.
3. Navegue até a guia Janela fora do horário de pico. Você pode ver a janela fora do horário de pico configurada, além de uma lista das próximas ações agendadas para o domínio.
4. Escolha Editar e especifique um novo horário de início em UTC. Por exemplo, para configurar um horário de início às 21h na região leste dos EUA (Norte da Virginia), especifique 02h UCT.
5. Escolha Salvar alterações.

CLI

Para configurar uma janela personalizada fora do horário de pico usando oAWS CLI, envie uma UpdateDomainConfigsolicitação e especifique a hora e o minuto no formato de 24 horas.

Por exemplo, a solicitação a seguir altera o horário de início da janela para 2h da manhã UTC:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --off-peak-window-options 'OffPeakWindow={WindowStartTime={Hours=02,Minutes=00}}'
```

Se você não especificar o horário de início da janela, o padrão é 22h, horário local, na Região da AWS aonde o domínio foi criado.

Exibir ações programadas

Você pode ver todas as ações agendadas, em andamento ou pendentes atualmente para cada um dos seus domínios. As ações podem ter uma severidade de `HIGH`, `MEDIUM` e `LOW`.

As ações podem ter os seguintes status:

- `Pending update`: a ação está na fila para ser processada.
- `In progress`: a ação está em andamento.
- `Failed` – a operação não foi concluída.
- `Completed` – a ação foi concluída com êxito.
- `Not eligible`: somente para atualizações de software de serviço. A atualização não pode ser continuada porque o cluster não está íntegro.
- `Eligible`: somente para atualizações de software de serviço. O domínio está qualificado para uma atualização.

Console

O console OpenSearch de serviço exibe todas as ações agendadas na configuração do domínio, junto com a gravidade e o status atual de cada ação.

Como ver ações programadas para um domínio

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.

2. Selecione o nome do domínio para abrir a configuração.
3. Navegue até a guia Janela fora do horário de pico.
4. Em Ações agendadas, visualize todas as ações atualmente agendadas, em andamento ou pendentes no domínio.

CLI

Para ver as ações agendadas usando oAWS CLI, envie uma ListScheduledActionssolicitação:

```
aws opensearch list-scheduled-actions \
  --domain-name my-domain
```

Resposta:

```
{
    "ScheduledActions": [
        {
            "Cancellable": true,
            "Description": "The Deployment type is : BLUE_GREEN.",
            "ID": "R20220721-P13",
            "Mandatory": false,
            "Severity": "HIGH",
            "ScheduledBy": "CUSTOMER",
            "ScheduledTime": 1.673871601E9,
            "Status": "PENDING_UPDATE",
            "Type": "SERVICE_SOFTWARE_UPDATE",
        },
        {
            "Cancellable": true,
            "Description": "Amazon Opensearch will adjust the young generation JVM
 arguments on your domain to improve performance",
            "ID": "Auto-Tune",
            "Mandatory": true,
            "Severity": "MEDIUM",
            "ScheduledBy": "SYSTEM",
            "ScheduledTime": 1.673871601E9,
            "Status": "PENDING_UPDATE",
            "Type": "JVM_HEAP_SIZE_TUNING",
        }
    ]
}
```

Ações de reagendamento

OpenSearch O serviço notifica você sobre atualizações programadas do software de serviço e otimizações do Auto-Tune. Você pode optar por aplicar a alteração imediatamente ou reprogramá-la para uma data e hora posteriores.

> **Note**
>
> OpenSearch O serviço pode agendar a ação dentro de uma hora a partir do horário selecionado. Por exemplo, se você optar por aplicar uma atualização às 17h, ela poderá acontecer entre 17h e 18h.

Console

Como reprogramar uma ação

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. Selecione o nome do domínio para abrir a configuração.
3. Navegue até a guia Janela fora do horário de pico.
4. Selecione Ações programadas, escolha a ação e, depois, escola Reagendar.
5. Escolha uma das seguintes opções:

   - Aplicar a atualização agora: programa a ação para acontecer imediatamente, se houver capacidade disponível. Se a capacidade não estiver disponível, outros slots de horários disponíveis serão sugeridos.
   - Programar para fora do horário de pico: agenda a ação para ser iniciada durante uma próxima janela fora do horário de pico. Não há garantia de que a alteração será implementada imediatamente na próxima janela. Dependendo da capacidade, isso pode acontecer nos dias subsequentes.
   - Reagendar esta atualização: permite especificar uma data e hora personalizadas para aplicar a alteração. Se o horário especificado não estiver disponível por motivos de capacidade, você poderá selecionar um slot de horário diferente.
   - Cancelar atualização agendada: cancela a atualização. Essa opção só estará disponível para atualizações opcionais de software de serviço. Ela não está disponível para ações de ajuste automático ou atualizações obrigatórias de software.
6. Escolha Salvar alterações.

CLI

Para reagendar uma ação usando oAWS CLI, envie uma solicitação. UpdateScheduledAction Para recuperar o ID da ação, envie uma solicitação `ListScheduledActions`.

A solicitação a seguir reprograma uma atualização do software de serviço para uma data e hora específicas:

```
aws opensearch update-scheduled-action \
  --domain-name my-domain \
  --action-id R20220721-P13 \
  --action-type "SERVICE_SOFTWARE_UPDATE" \
  --desired-start-time 1677348395000 \
  --schedule-at TIMESTAMP
```

Resposta:

```
{
   "ScheduledAction": {
      "Cancellable": true,
      "Description": "Cluster status is updated.",
      "Id": "R20220721-P13",
      "Mandatory": false,
      "ScheduledBy": "CUSTOMER",
      "ScheduledTime": 1677348395000,
      "Severity": "HIGH",
      "Status": "PENDING_UPDATE",
      "Type": "SERVICE_SOFTWARE_UPDATE"
   }
}
```

Se a solicitação falhar com uma `SlotNotAvailableException`, isso significa que o horário especificado não está disponível por motivos de capacidade e você deve especificar um horário diferente. OpenSearch O serviço fornece sugestões alternativas de slots disponíveis na resposta.

Migração das janelas de manutenção do Auto-Tune

Se um domínio tiver sido criado antes de 16 de fevereiro de 2023, ele poderia usar janelas de manutenção para agendar otimizações de ajuste automático que exigem uma implantação azul/verde. Em vez disso, você pode migrar seus domínios do Auto-Tune existentes para usar a janela fora do horário de pico.

> **Note**
>
> Você não pode voltar a usar janelas de manutenção depois de migrar seu domínio para usar janelas fora do horário de pico.

Console

Como migrar um domínio para usar a janela fora do horário de pico

1. No console do Amazon OpenSearch Service, selecione o nome do domínio para abrir sua configuração.
2. Vá até a guia Auto-Tune e escolha Editar.
3. Selecione Migrar para a janela fora do horário de pico.
4. Em Hora de início (UTC), forneça uma hora de início diária para a janela fora do horário de pico de acordo com o Horário Universal Coordenado (UTC).
5. Escolha Salvar alterações.

CLI

Para migrar de uma janela de manutenção do Auto-Tune para a janela fora de pico usando oAWS CLI, envie uma solicitação: UpdateDomainConfig

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --auto-tune-options
 DesiredState=ENABLED,UseOffPeakWindow=true,MaintenanceSchedules=[]
```

A janela fora do horário de pico deve estar ativada para que você possa migrar um domínio da janela de manutenção do Auto-Tune para a janela fora do horário de pico. Você pode ativar a janela fora do horário de pico em uma solicitação separada ou na mesma solicitação. Para obter instruções, consulte the section called “Ativar a janela fora do horário de pico”.

Notificações no Amazon OpenSearch Service

As notificações no Amazon OpenSearch Service contêm informações importantes sobre o desempenho e a integridade de seus domínios. OpenSearch O serviço notifica você sobre

atualizações de software de serviço, aprimoramentos do Auto-Tune, eventos de integridade do cluster e erros de domínio. As notificações estão disponíveis para todas as versões do OpenSearch Elasticsearch OSS.

Você pode ver as notificações no painel Notificações do console OpenSearch de serviço. Todas as notificações do OpenSearch Serviço também são exibidas na Amazon EventBridge. Para obter uma lista completa de notificações e exemplos de eventos, consulte the section called “Eventos de monitoramento”.

Tópicos

- Conceitos básicos das notificações
- Gravidades das notificações
- Exemplo de EventBridge evento

Conceitos básicos das notificações

As notificações são ativadas automaticamente quando você cria um domínio. Acesse o painel Notificações do console de OpenSearch serviço para monitorar e reconhecer as notificações. Cada notificação inclui informações como a hora em que foi publicada, o domínio ao qual se relaciona, um nível de gravidade e status e uma breve explicação. Você pode exibir notificações históricas por até 90 dias no console.

Depois de acessar o painel Notifications (Notificações) ou confirmar uma notificação, você pode receber uma mensagem de erro sobre não ter permissões para executar `es:ListNotifications` ou `es:UpdateNotificationStatus`. Para resolver esse problema, dê ao usuário ou função as seguintes permissões no IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "es:UpdateNotificationStatus",
      "es:ListNotifications"
    ],
    "Resource": "arn:aws:es:*:123456789012:domain/*"
  }]
}
```

O console do IAM gera um erro (“O IAM não reconhece uma ou mais ações.”) que você pode ignorar com segurança. Você também pode restringir a ação `es:UpdateNotificationStatus` a determinados domínios. Para saber mais, consulte the section called “Referência de elementos da política”.

Gravidades das notificações

As notificações no OpenSearch Serviço podem ser informativas, relacionadas a qualquer ação que você já tenha realizado ou às operações do seu domínio, ou acionáveis, que exigem que você execute ações específicas, como a aplicação de um patch de segurança obrigatório. Cada notificação tem uma gravidade associada a ela, que pode ser `Informational`, `Low`, `Medium`, `High` ou `Critical`. A tabela a seguir resume cada gravidade:

Gravidade	Descrição	Exemplos
`Informational`	Informações relacionadas à operação do seu domínio.	• Atualização do software de serviço disponível • Auto-Tune iniciado
`Low`	Uma ação recomendada, mas que não tem impacto negativo na disponibilidade ou na performance do domínio se nenhuma ação for tomada.	• Auto-Tune cancelado • Aviso de alta contagem de fragmentos
`Medium`	Poderá haver um impacto se a ação recomendada não for executada, mas oferece uma janela de tempo estendida para que a ação seja executada.	• Falha na atualização do software de serviço • Limite de contagem de fragmentos excedido
`High`	Uma ação urgente é necessária para evitar impactos adversos.	• Atualização do software de serviço necessária • Chave do KMS inacessível

Gravidade	Descrição	Exemplos
`Critical`	Uma ação imediata é necessária para evitar impactos adversos ou se recuperar deles.	Nenhum disponível no momento

Exemplo de EventBridge evento

O exemplo a seguir mostra um evento OpenSearch de notificação de serviço enviado para a Amazon EventBridge. A notificação tem gravidade de `Informational` porque a atualização é opcional:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Available",
    "severity": "Informational",
    "description": "Service software update [R20200330-p1] available."
  }
}
```

Configuração de um domínio Multi-AZ no Amazon OpenSearch Service

Para evitar perda de dados e minimizar o tempo de inatividade do cluster do Amazon OpenSearch Service no caso de uma interrupção do serviço, você pode distribuir os nós em duas ou três zonas de disponibilidade na mesma região, uma configuração conhecida como Multi-AZ. As zonas de disponibilidade são vários locais isolados dentro de cada região da AWS.

Para domínios que executam workloads de produção, recomendamos a opção de implantação multi-AZ com modo de espera, que cria a seguinte configuração:

- Domínio implementado em três zonas.
- Tipos de instância da geração atual para os nós principais dedicados e nós de dados.
- Três nós principais dedicados e três (ou um múltiplo de três) nós de dados.
- Pelo menos duas réplicas para cada índice no seu domínio ou um múltiplo de três cópias de dados (incluindo nós primários e réplicas).

O restante desta seção fornece explicações e contexto para estas configurações.

Multi-AZ com modo de espera

O multi-AZ com modo de espera é uma opção de implantação para domínios do Amazon OpenSearch Service que oferece disponibilidade de 99,99%, desempenho consistente para cargas de trabalho de produção e configuração e gerenciamento simplificados de domínios. Quando você usa o multi-AZ com modo de espera, os domínios são resilientes a falhas de infraestrutura, sem impacto no desempenho ou na disponibilidade. Essa opção de implantação atinge esse padrão ao exigir várias práticas recomendadas, como uma contagem especificada de nós de dados, contagem de nós principais, tipo de instância, contagem de réplicas, configurações de atualização de software e ajuste automático ativado.

Quando você usa o multi-AZ com modo de espera, o OpenSearch Service cria um domínio em três zonas de disponibilidade, com cada zona contendo uma cópia completa dos dados e com os dados distribuídos igualmente em cada uma das zonas. Seu domínio reserva nós em uma dessas zonas como modo de espera, o que significa que eles não atendem a solicitações de pesquisa. Quando o OpenSearch Service detecta uma falha na infraestrutura subjacente, ele ativa automaticamente os nós em espera em menos de um minuto. O domínio continua atendendo às solicitações de indexação e pesquisa, e qualquer impacto é limitado ao tempo necessário para realizar o failover. Não há redistribuição de dados ou recursos, o que resulta em desempenho inalterado do cluster e sem risco de redução da disponibilidade. O multi-AZ com modo de espera está disponível sem custo adicional.

Você tem duas opções para criar um domínio com modo de espera no AWS Management Console. Primeiro, você pode criar um domínio com o método de criação Criação rápida , e o OpenSearch Service usará automaticamente uma configuração predeterminada, que inclui o seguinte:

- Três zonas de disponibilidade, com uma atuando como reserva

- Três nós principais e nós de dados dedicados
- Ajuste automático ativado no domínio
- Armazenamento GP3 para os nós de dados

Você também pode escolher o método Criação padrão e selecionar Domínio com modo de espera como sua opção de implantação. Isso permite que você personalize seu domínio e, ao mesmo tempo, exija os principais atributos do modo de espera, como três zonas e três nós principais. Recomendamos escolher uma contagem de nós de dados que seja múltipla de três (o número de zonas de disponibilidade).

Depois de criar seu domínio, você pode navegar até as páginas de detalhes do domínio e, na guia Configuração do cluster, confirmar se 3-AZ com espera aparece em Zona(s) de Disponibilidade.

Se você tiver problemas ao migrar um domínio existente para o multi-AZ com modo de espera, consulte Erro ao migrar para o multi-AZ com modo de espera no guia de solução de problemas.

Limitações

Ao configurar um domínio com multi-AZ com modo de espera, considere as seguintes limitações:

- O número total de fragmentos em um nó não pode exceder 1.000, o número total de fragmentos em um cluster não pode exceder 75.000 e o tamanho de um único fragmento não pode exceder 65 GB.
- O multi-AZ com modo de espera funciona somente com os tipos de instância `m5`, `c5`, `r5`, `r6g`, `c6g`, `m6g`, `r6gd` e `i3`. Para obter mais informações sobre instâncias compatíveis, consulte Tipos de instância compatíveis.
- Você só pode usar SSD de IOPs provisionadas, SSD de uso geral (GP3) ou armazenamento baseado em instância com modo de espera.

Multi-AZ sem modo de espera

O OpenSearch Service ainda oferece suporte ao Multi-AZ sem modo de espera, o que oferece 99,9% de disponibilidade. Os nós são distribuídos em zonas de disponibilidade, e a disponibilidade depende do número de zonas de disponibilidade e cópias dos dados. Enquanto no modo de espera você precisa configurar seu domínio com as melhores práticas, sem o modo de espera você pode escolher seu próprio número de zonas de disponibilidade, nós e réplicas. Não recomendamos essa

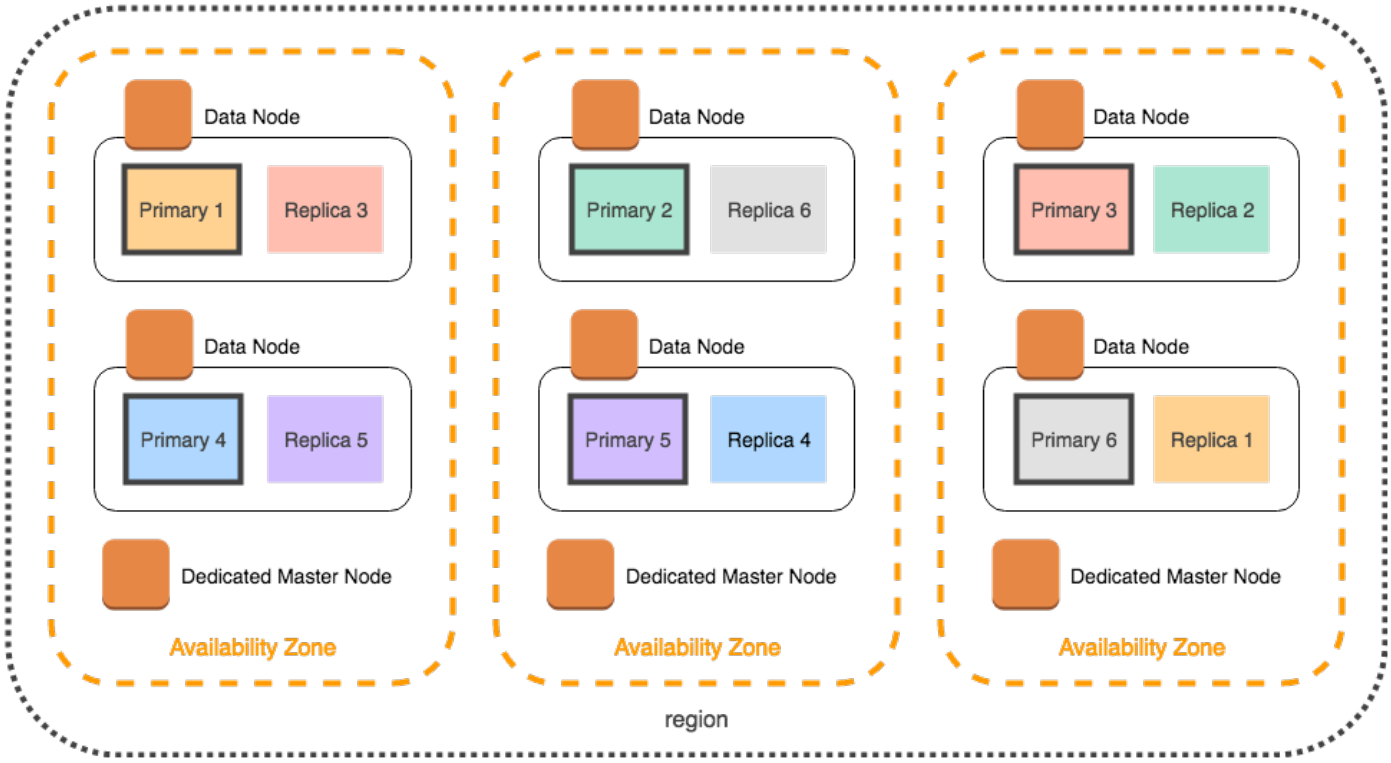
opção, a menos que você tenha fluxos de trabalho existentes que seriam interrompidos pela criação de domínios em espera.

Se você escolher essa opção, ainda recomendamos que você selecione três zonas de disponibilidade para permanecer resiliente a falhas de nó, disco e single-AZ. Quando ocorre uma falha, o cluster redistribui os dados pelos recursos restantes para manter a disponibilidade e a redundância. Essa movimentação de dados aumenta o uso de recursos no cluster e pode ter um impacto no desempenho. Se o cluster não for dimensionado adequadamente, ele poderá ter uma disponibilidade reduzida, o que, em grande parte, anula o propósito do multi-AZ.

A única maneira de configurar um domínio sem modo de espera no AWS Management Console é escolher o método Criação padrão e selecionar Domínio sem modo de espera como sua opção de implantação.

Distribuição de fragmentos

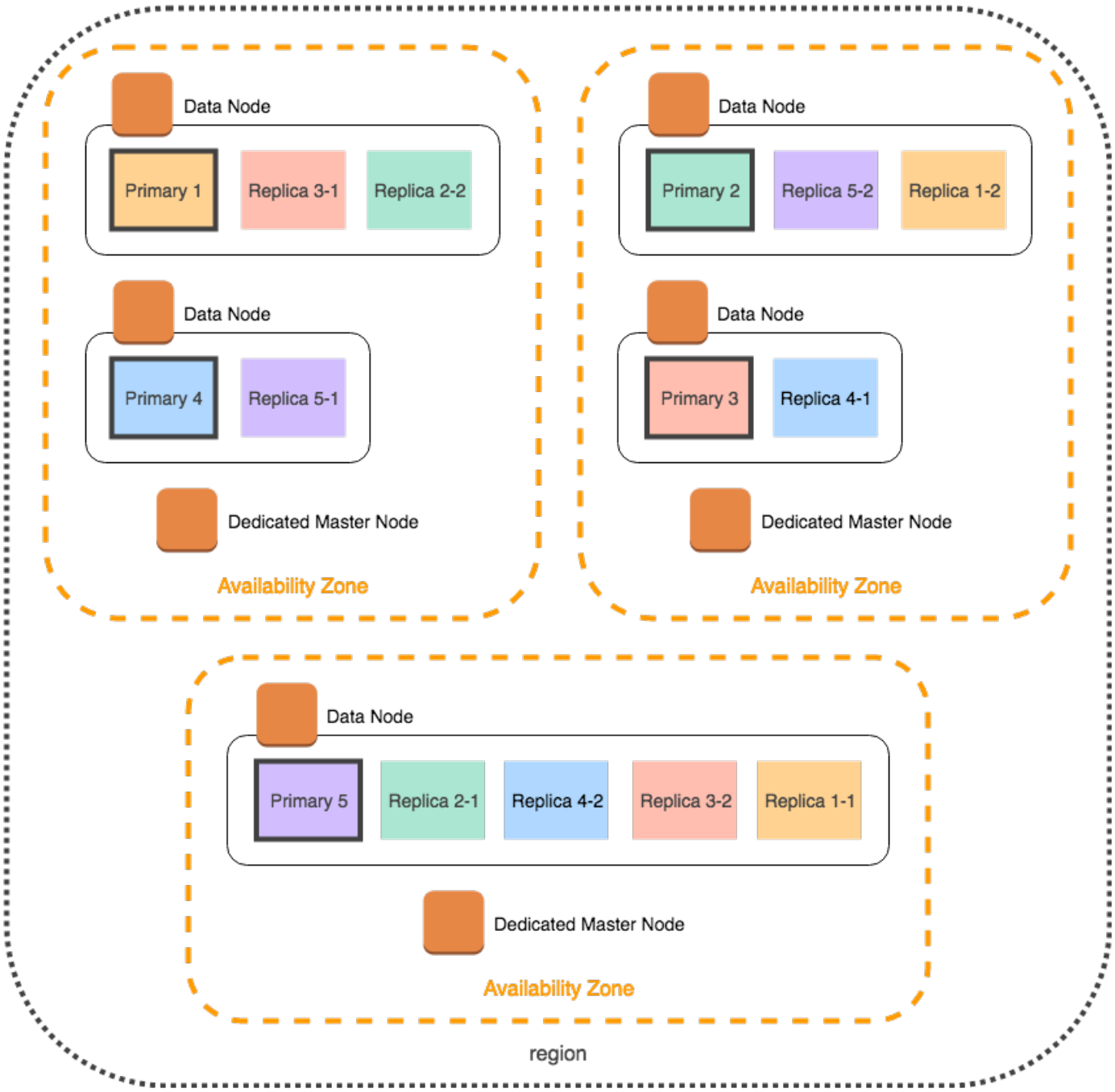
Se habilitar Multi-AZ sem standby, você deverá ter pelo menos uma réplica para cada índice no cluster. Sem réplicas, o OpenSearch Service não pode distribuir cópias de seus dados para outras Zonas de disponibilidade. Felizmente, a configuração padrão para qualquer índice é uma contagem de réplica de 1. Como mostrado no diagrama a seguir, o OpenSearch Service faz um melhor esforço para distribuir fragmentos primários e seus fragmentos de réplica correspondentes para diferentes zonas.



Além de distribuir os fragmentos por zona de disponibilidade, o OpenSearch Service os distribui por nós. Ainda assim, determinadas configurações de domínio podem resultar em contagens de fragmentos desequilibradas. Considere o seguinte domínio:

- 5 nós de dados
- 5 fragmentos principais
- 2 réplicas
- 3 zonas de disponibilidade

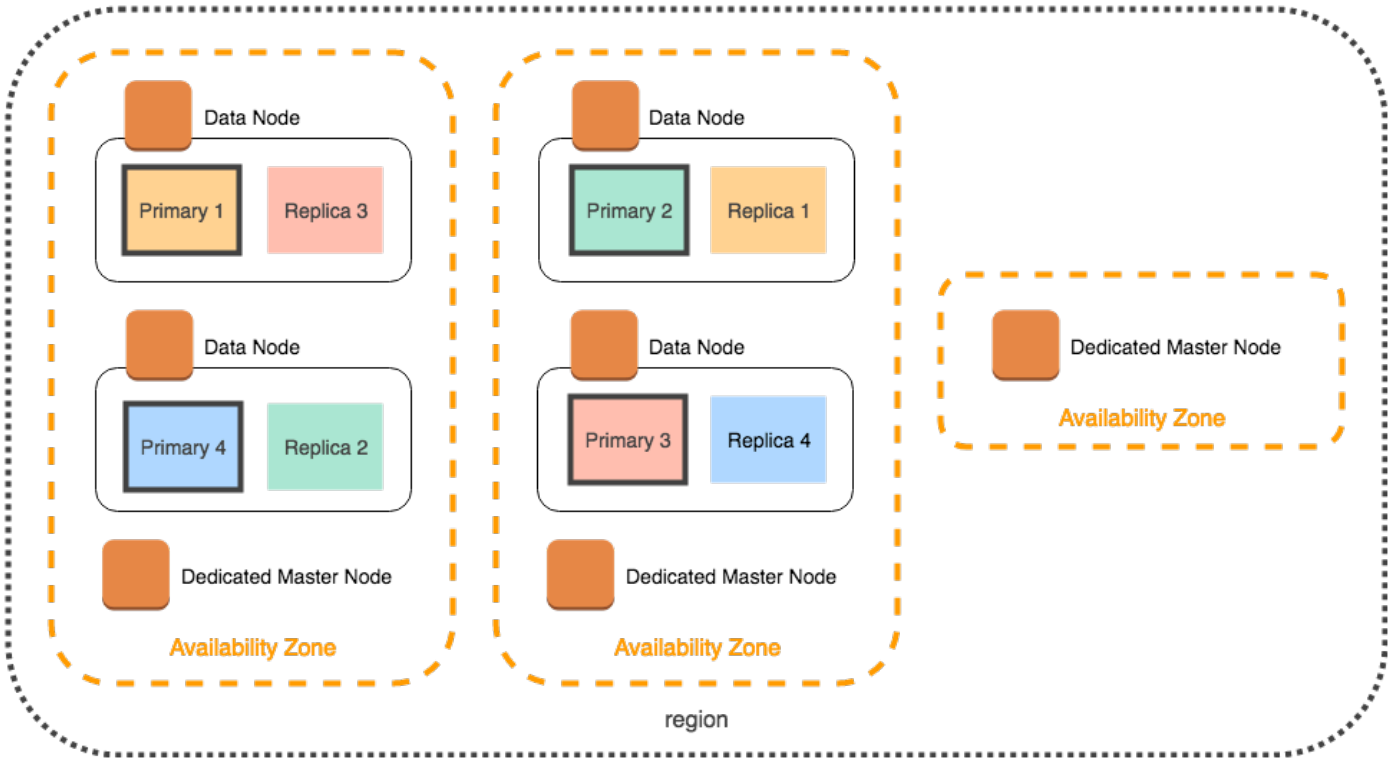
Nessa situação, o OpenSearch Service tem que sobrecarregar um nó para distribuir os fragmentos principais e de réplica entre as zonas, como mostrado no diagrama a seguir.



Para evitar esses tipos de situações, que podem sobrecarregar nós individuais e afetar a performance, recomendamos selecionar multi-AZ com modo de espera ou uma contagem de instâncias que seja um múltiplo de três quando você planejar ter duas ou mais réplicas por índice.

Distribuição de nó principal dedicado

Mesmo se você selecionar duas zonas de disponibilidade ao configurar seu domínio, o OpenSearch Service distribuirá automaticamente os nós principais dedicados em três zonas de disponibilidade. Essa distribuição ajuda a evitar tempo de inatividade do cluster se uma zona sofrer uma interrupção de serviço. Se você usar os três nós principais dedicados recomendados e uma zona de disponibilidade ficar inativa, seu cluster ainda terá um quorum (2) de nós principais dedicados e poderá selecionar um novo principal. O diagrama a seguir demonstra essa configuração.



Se você escolher um tipo de instância de gerações anteriores que não esteja disponível nas três zonas de disponibilidade, os seguintes cenários se aplicam:

- Se você escolher três zonas de disponibilidade para o domínio, o OpenSearch Service lançará um erro. Escolha um tipo de instância diferente e tente novamente.
- Se você escolher duas zonas de disponibilidade para o domínio, o OpenSearch Service distribuirá os nós principais dedicados em duas zonas.

Interrupções na zona de disponibilidade

As interrupções na zona de disponibilidade são raras, mas ocorrem. A tabela a seguir relaciona diferentes configurações de Multi-AZ e comportamentos durante uma interrupção. A última linha na tabela se aplica ao multi-AZ com modo de espera, enquanto todas as outras linhas têm configurações que se aplicam somente ao multi-AZ sem modo de espera.

Número de zonas de disponibilidade em uma região	Número de zonas de disponibilidade que você escolheu	Número de nós principais dedicados	Comportamento se uma zona de disponibilidade apresentar uma interrupção
2 ou mais	2	0	Tempo de inatividade. Seu cluster perde metade dos seus nós de dados e deve substituir pelo menos um na zona de disponibilidade restante antes que possa escolher um principal.
2	2	3	50% de chance de tempo de inatividade. O OpenSearch Service distribui dois nós principais dedicados em uma zona de disponibilidade e um na outra: • Se a zona de disponibilidade com um nó principal dedicado tiver uma interrupção, os dois nós principais dedicados na zona de disponibilidade restante podem escolher um principal. • Se a zona de disponibilidade com dois nós principais dedicados apresentar uma interrupção, o cluster permanecerá indisponível até que a zona de disponibilidade se recupere.
3 ou mais	2	3	Sem tempo de inatividade. O OpenSearch Service distribui automaticamente os nós principais dedicados em três zonas de

Número de zonas de disponibilidade em uma região	Número de zonas de disponibilidade que você escolheu	Número de nós principais dedicados	Comportamento se uma zona de disponibilidade apresentar uma interrupção
			disponibilidade para que os dois nós principais dedicados restantes possam escolher um principal.
3 ou mais	3	0	Sem tempo de inatividade. Aproximadamente, dois terços dos seus nós de dados ainda estão disponíveis para escolher um principal.
3 ou mais	3	3	Sem tempo de inatividade. Os dois nós principais dedicados restantes podem escolher um principal.

Em todas as configurações, independentemente da causa, as falhas de nó podem fazer com que os nós de dados restantes do cluster passem por um período de aumento de carga enquanto o OpenSearch Service configura automaticamente novos nós para substituir os agora ausentes.

Por exemplo, no caso de uma falha na zona de disponibilidade em uma configuração de três zonas, dois terços dos nós de dados terão que processar várias solicitações para o cluster. Conforme eles processam essas solicitações, os nós restantes também estão replicando fragmentos para novos nós à medida que ficam online, o que pode afetar ainda mais a performance. Se a disponibilidade for essencial para sua workload, considere a adição de recursos ao seu cluster para diminuir essa preocupação.

> **Note**
>
> O OpenSearch Service gerencia domínios Multi-AZ de forma transparente para que não seja possível simular manualmente interrupções da zona de disponibilidade.

Lançamento de seus domínios OpenSearch do Amazon Service em uma VPC

Você pode lançar AWS recursos, como domínios do Amazon OpenSearch Service, em uma nuvem privada virtual (VPC). Uma VPC é uma rede virtual dedicada à sua. Conta da AWSEla é isolada de maneira lógica das outras redes virtuais na Nuvem AWS . A colocação OpenSearch de um domínio de serviço em uma VPC permite a comunicação segura entre o OpenSearch serviço e outros serviços dentro da VPC sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS

> **Note**
>
> Se você colocar seu domínio OpenSearch de serviço em uma VPC, seu computador deverá ser capaz de se conectar à VPC. Essa conexão geralmente assume a forma de VPN, gateway de transito, rede gerenciada ou servidor de proxy. Você não pode acessar seus domínios diretamente de fora da VPC.

Tópicos

VPC versus domínios públicos

A seguir estão algumas das maneiras pelas quais os domínios da VPC diferem dos domínios públicos. Cada diferença é descrita posteriormente em mais detalhes.

- Devido ao seu isolamento lógico, os domínios que residem em uma VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos.
- Embora os domínios públicos sejam acessíveis a partir de qualquer dispositivo conectado à Internet, os domínios da VPC exigem alguma forma de VPN ou proxy.
- Em comparação com domínios públicos, domínios VPC exibem menos informações no console do . Especificamente, a guia Cluster health (Integridade do cluster) não inclui informações de fragmentos, e a guia Indexes (Índices) não está presente.

- Os endpoits de domínio assumem formas diferentes (`https://search-domain-name` vs. `https://vpc-domain-name`).
- Não é possível aplicar políticas de acesso baseadas em IP aos domínios que residem em uma VPC porque o grupo de segurança já impõe políticas de acesso baseadas em IP.

Limitações

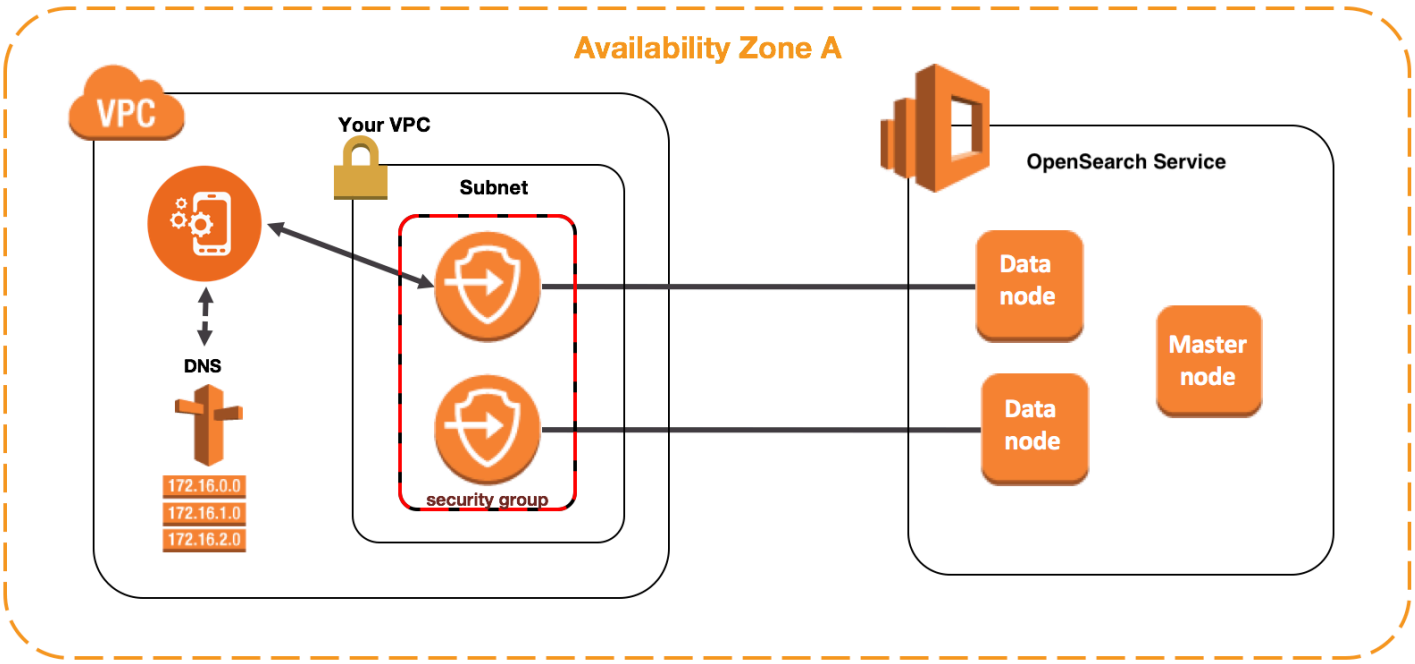
Operar um domínio de OpenSearch serviço em uma VPC tem as seguintes limitações:

- Se você executar um novo domínio de uma VPC, não será possível alternar posteriormente para um endpoint público. O inverso também é verdadeiro: se você criar um domínio com um endpoint público, não será possível colocá-lo em uma VPC. Em vez disso, você deve criar um novo domínio e migrar seus dados.
- Você pode iniciar seu domínio de uma VPC ou usar um endpoint público, mas não pode fazer ambos. Você deve escolher uma opção ou outra ao criar seu domínio.
- Você não pode iniciar seu domínio em uma VPC que usa locação dedicada. É necessário usar uma VPC com locação definida como Padrão.
- Após colocar um domínio dentro de uma VPC, não será possível movê-lo para uma VPC diferente, mas será possível alterar as sub-redes e as configurações do grupo de segurança.
- Para acessar a instalação padrão dos OpenSearch painéis para um domínio que reside em uma VPC, os usuários devem ter acesso à VPC. Esse processo varia de acordo com a configuração de rede, mas geralmente envolve a conexão a uma VPN ou rede gerenciada ou o uso de um servidor de proxy ou gateway de trânsito. Para saber mais, consulte the section called “Sobre políticas de acesso em domínios da VPC”, o Manual do usuário da Amazon VPC e o the section called “Controle do acesso aos OpenSearch painéis”.

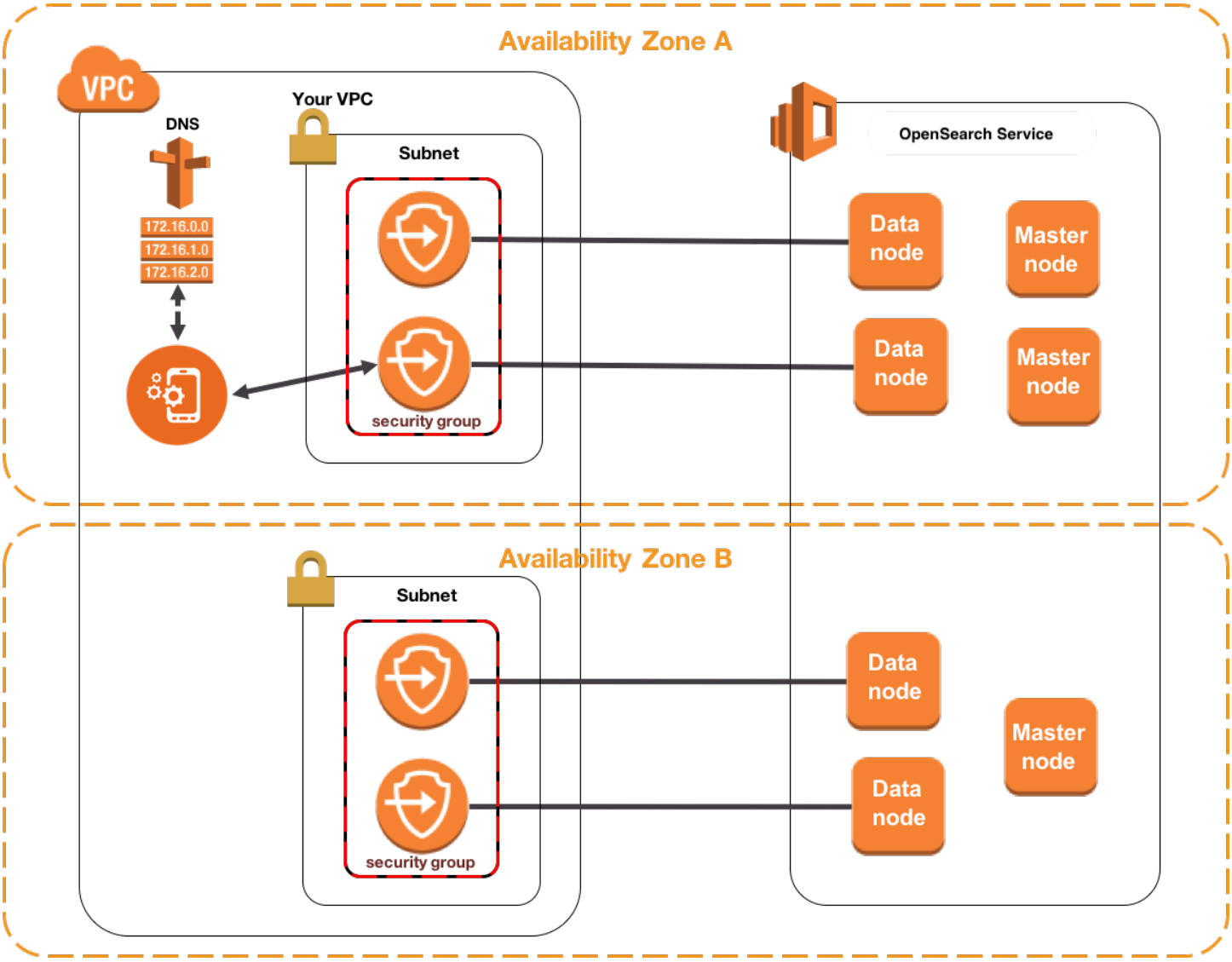
Arquitetura

Para oferecer suporte a VPCs, o OpenSearch Service coloca um endpoint em uma, duas ou três sub-redes da sua VPC. Se você habilitar várias zonas de disponibilidade para seu domínio, cada sub-rede deverá estar em uma zona de disponibilidade diferente na mesma região. Se você usar apenas uma zona de disponibilidade, o OpenSearch Service colocará um endpoint em apenas uma sub-rede.

A ilustração a seguir mostra a arquitetura da VPC para uma zona de disponibilidade:



A ilustração a seguir mostra a arquitetura da VPC para duas zonas de disponibilidade:



OpenSearch O serviço também coloca uma interface de rede elástica (ENI) na VPC para cada um dos seus nós de dados. OpenSearch O serviço atribui a cada ENI um endereço IP privado do intervalo de endereços IPv4 da sua sub-rede. O serviço também atribui um nome de host DNS público (que é o endpoint de domínio) aos endereços IP. Você deve usar um serviço de DNS público para resolver o endpoint (que é um nome de host DNS) para os endereços IP apropriados dos nós de dados:

- Se sua VPC usar o servidor DNS fornecido pela Amazon definindo a `enableDnsSupport` opção como `true` (o valor padrão), a resolução para o endpoint do OpenSearch serviço será bem-sucedida.

- Se sua VPC usa um servidor DNS privado e o servidor pode acessar os servidores DNS públicos autoritativos para resolver nomes de host DNS, a resolução para o endpoint de serviço também será bem-sucedida. OpenSearch

Como os endereços IP podem mudar, você deve resolver o endpoint do domínio periodicamente para que sempre possa acessar os nós de dados corretos. Recomendamos que você defina o intervalo de resolução do DNS para um minuto. Se você estiver usando um cliente, também deve garantir que o cache do DNS no cliente seja limpo.

Migração do acesso público para o acesso via VPC

Ao criar um domínio, você especifica se deve haver um endpoint público ou residir em uma VPC. Após ter sido criado, você não poderá mudar de um para o outro. Em vez disso, você deve criar um novo domínio e reindexar ou migrar manualmente seus dados. Os snapshots representam uma maneira conveniente de migração de dados. Para obter informações sobre a realização e restauração de snapshots, consulte the section called “Criação de snapshots de índices”.

Sobre políticas de acesso em domínios da VPC

Colocar seu domínio de OpenSearch serviço em uma VPC fornece uma camada de segurança forte e inerente. Quando você cria um domínio com acesso público, o endpoint é composto da seguinte forma:

```
https://search-domain-name-identifier.region.es.amazonaws.com
```

Como o rótulo "público" sugere, esse endpoint é acessível de qualquer dispositivo conectado à Internet, embora você possa (e deva) controlar o acesso a ele. Se você acessar o endpoint em um navegador da Web, poderá receber uma mensagem `Not Authorized`, mas a solicitação atingirá o domínio.

Quando você cria um domínio com acesso à VPC, o endpoint se assemelha a um endpoint público:

```
https://vpc-domain-name-identifier.region.es.amazonaws.com
```

Se você tentar acessar o endpoint em um navegador da Web, no entanto, poderá descobrir que a solicitação está ultrapassando o tempo limite. Para executar até mesmo solicitações `GET` básicas, seu computador deve ser capaz de se conectar à VPC. Essa conexão geralmente assume a forma

de VPN, gateway de transito, rede gerenciada ou servidor de proxy. Para obter detalhes sobre as várias formas que podem ser apresentadas, consulte Exemplos de VPC no Manual do usuário da Amazon VPC. Para obter um exemplo focalizado em desenvolvimento, consulte the section called "Teste dos domínios da VPC".

Além deste requisito de conectividade, as VPCs permitem que você gerencie o acesso ao domínio por meio de grupos de segurança. Para muitos casos de uso, essa combinação de recursos de segurança é suficiente e pode ser conveniente aplicar uma política de acesso aberta ao domínio.

Operar com uma política de acesso aberto não significa que qualquer pessoa na Internet possa acessar o domínio do OpenSearch Serviço. Em vez disso, significa que, se uma solicitação chegar ao domínio do OpenSearch Serviço e os grupos de segurança associados permitirem, o domínio aceitará a solicitação. A única exceção é no caso de você estar usando o controle de acesso refinado ou uma política de acesso que especifique perfis do IAM. Nessas situações, para que o domínio aceite uma solicitação, os grupos de segurança devem permiti-la e assiná-la com credenciais válidas.

> **Note**
>
> Como os grupos de segurança já aplicam políticas de acesso baseadas em IP, você não pode aplicar políticas de acesso baseadas em IP aos domínios de OpenSearch serviço que residem em uma VPC. Se você usa o acesso público, as políticas baseadas em IP ainda estão disponíveis.

Antes de começar: pré-requisitos de acesso à VPC

Antes de habilitar uma conexão entre uma VPC e seu novo domínio de OpenSearch serviço, você deve fazer o seguinte:

- Criar uma VPC

  Para criar sua VPC, você pode usar o console Amazon VPC, a AWS CLI ou um dos SDKs. AWS Para obter mais informações, consulte Como trabalhar com VPCs compartilhadas no Manual do usuário da Amazon VPC. Se você já tiver uma VPC, ignore esta etapa.
- Reservar endereços IP

  OpenSearch O serviço permite a conexão de uma VPC a um domínio colocando interfaces de rede em uma sub-rede da VPC. Cada interface de rede está associada a um endereço IP. Você deve

reservar um número suficiente de endereços IP na sub-rede para as interfaces de rede. Para obter mais informações, consulte Reserva de endereços IP em uma sub-rede da VPC.

Teste dos domínios da VPC

A segurança avançada de uma VPC pode tornar a conexão com seu domínio e a execução de testes básicos um desafio. Se você já tem um domínio OpenSearch Service VPC e prefere não criar um servidor VPN, tente o seguinte processo:

1. Para a política de acesso do domínio, escolha Only use fine-grained access control (Use somente o controle de acesso refinado). Sempre é possível atualizar essa configuração depois de concluir o teste.
2. Crie uma instância Amazon Linux Amazon EC2 na mesma VPC, sub-rede e grupo de segurança do seu domínio de serviço. OpenSearch

   Como essa instância é para fins de teste e precisa fazer muito pouco trabalho, escolha um tipo de instância de custo reduzido, como o `t2.micro`. Atribua um endereço IP público à instância e crie um novo par de chaves ou escolha um existente. Se você criar uma nova chave, faça download dela em seu diretório `~/.ssh`.

   Para saber mais sobre a criação de instâncias, consulte Conceitos básicos de instâncias do Amazon EC2 Linux.
3. Adicione um gateway da Internet à VPC.
4. Na tabela de rotas da VPC, adicione uma nova rota. Em Destination (Destino), especifique um bloco CIDR que contém o endereço IP público do computador. Em Target (Destino), especifique o gateway da Internet que você acabou de criar.

   Por exemplo, você pode especificar `123.123.123.123/32` somente para seu computador ou `123.123.123.0/24` para vários computadores.
5. Para o grupo de segurança, especifique duas regras de entrada:

Tipo	Protocolo	Port Range (Intervalo de portas)	Origem
SSH (22)	TCP (6)	22	*your-cidr-block*

Tipo	Protocolo	Port Range (Intervalo de portas)	Origem
HTTPS (443)	TCP (6)	443	*your-security-group-id*

A primeira regra permite que você use SSH em sua instância do EC2. A segunda permite que a instância do EC2 se comunique com o domínio do OpenSearch serviço por HTTPS.

6. No terminal, execute o comando a seguir:

```
ssh -i ~/.ssh/your-key.pem ec2-user@your-ec2-instance-public-ip -N -L
 9200:vpc-domain-name.region.es.amazonaws.com:443
```

Esse comando cria um túnel SSH que encaminha solicitações para https://localhost:9200 para seu domínio de OpenSearch serviço por meio da instância EC2. Especificar a porta 9200 no comando simula uma OpenSearch instalação local, mas use a porta que você quiser. OpenSearch O serviço só aceita conexões pela porta 80 (HTTP) ou 443 (HTTPS).

O comando não fornece comentários e é executado indefinidamente. Para interrompê-lo, pressione `Ctrl + C`.

7. Navegue até https://localhost:9200/_dashboards/ em seu navegador da web. Talvez você precise confirmar uma exceção de segurança.

Como alternativa, você pode enviar solicitações para https://localhost:9200 usando curl, Postman ou a linguagem de programação de sua preferência.

> **Tip**
>
> Se você encontrar erros de curl devido a uma incompatibilidade de certificado, tente o sinalizador `--insecure`.

Reserva de endereços IP em uma sub-rede da VPC

OpenSearch O serviço conecta um domínio a uma VPC colocando interfaces de rede em uma sub-rede da VPC (ou em várias sub-redes da VPC se você habilitar várias zonas de disponibilidade). Cada interface de rede está associada a um endereço IP. Antes de criar seu domínio OpenSearch

de serviço, você deve ter um número suficiente de endereços IP disponíveis em cada sub-rede para acomodar as interfaces de rede.

Aqui está a fórmula básica: o número de endereços IP que o OpenSearch serviço reserva em cada sub-rede é três vezes o número de nós de dados, dividido pelo número de zonas de disponibilidade.

Exemplos

- Se um domínio tiver nove nós de dados por três zonas de disponibilidade, a quantidade de IPs por sub-rede será 9 * 3 / 3 = 9.
- Se um domínio tiver oito nós de dados por duas zonas de disponibilidade, a quantidade de IPs por sub-rede será 8 * 3 / 2 = 12.
- Se um domínio tiver seis nós de dados por uma zona de disponibilidade, a quantidade de IPs por sub-rede será 6 * 3 / 1 = 18.

Quando você cria o domínio, o OpenSearch Serviço reserva os endereços IP, usa alguns para o domínio e reserva o restante para implantações azul/verde. Você pode ver as interfaces de rede e seus endereços IP associados na seção Network Interfaces (Interfaces de rede) do console do Amazon EC2. A coluna Descrição mostra a qual domínio OpenSearch de serviço a interface de rede está associada.

> **Tip**
>
> Recomendamos que você crie sub-redes dedicadas para os endereços IP reservados do OpenSearch Serviço. Ao usar sub-redes dedicadas, você evita a sobreposição com outros aplicativos e serviços e garante a possibilidade de reservar endereços IP adicionais se precisar escalar seu cluster no futuro. Para saber mais, consulte Criação de uma sub-rede na VPC.

Função vinculada ao serviço para acesso à VPC

Uma função vinculada ao serviço é um tipo exclusivo de função do IAM que delega permissões a um serviço para que ele possa criar e gerenciar recursos em seu nome. OpenSearch O serviço requer uma função vinculada ao serviço para acessar sua VPC, criar o endpoint de domínio e colocar interfaces de rede em uma sub-rede da sua VPC.

OpenSearch O Service cria automaticamente a função quando você usa o console do OpenSearch Service para criar um domínio em uma VPC. Para que essa criação automática seja bem-sucedida, você precisa ter permissões para a ação `iam:CreateServiceLinkedRole`. Para saber mais, consulte Permissões de funções vinculadas ao serviço no Manual do usuário do IAM.

Depois que o OpenSearch Service criar a função, você poderá visualizá-la (`AWSServiceRoleForAmazonOpenSearchService`) usando o console do IAM.

Para obter mais informações sobre as permissões dessa função e como excluí-la, consulte the section called “Usar funções vinculadas ao serviço”.

Criação de instantâneos de índice no Amazon Service OpenSearch

Os snapshots no Amazon OpenSearch Service são backups dos índices e do estado de um cluster. O estado inclui configurações do cluster, informações de nó, configurações de índice e alocação de fragmentos.

OpenSearch Os instantâneos do serviço vêm nas seguintes formas:

- Os snapshots automatizados são apenas para recuperação de cluster. Você pode usá-los para restaurar seu domínio em caso de status de cluster vermelho ou perda de dados. Para obter mais informações, consulte Restauração de instantâneos abaixo. OpenSearch O serviço armazena instantâneos automatizados em um bucket pré-configurado do Amazon S3 sem custo adicional.
- Os snapshots manuais são usados na recuperação de clusters ou na movimentação de dados de um cluster para outro. Você precisa iniciar os snapshots manuais. Esses snapshots são armazenados no seu próprio bucket do Amazon S3, e cobranças padrão do S3 são aplicáveis. Se você tiver um instantâneo de um OpenSearch cluster autogerenciado, poderá usar esse instantâneo para migrar para um domínio de serviço. OpenSearch Para obter mais informações, consulte Migração para o Amazon OpenSearch Service.

Todos os domínios OpenSearch de serviço tiram instantâneos automatizados, mas a frequência é diferente das seguintes formas:

- Para domínios que executam o Elasticsearch OpenSearch 5.3 e versões posteriores, o OpenSearch Service tira instantâneos automatizados de hora em hora e retém até 336 deles por 14 dias. Os snapshots por hora são menos disruptivos em função de sua natureza incremental. Eles também fornecem um ponto de recuperação mais recente, caso haja problemas em domínios.

- Para domínios que executam o Elasticsearch 5.1 e versões anteriores, o OpenSearch Service tira instantâneos automatizados diariamente durante a hora especificada, retém até 14 deles e não retém nenhum dado instantâneo por mais de 30 dias.

Se o cluster entrar no status vermelho, todos os snapshots automatizados falharão enquanto o status do cluster persistir. Se você não corrigir o problema em até duas semanas, poderá perder permanentemente os dados do cluster. Para obter etapas sobre a solução de problemas, consulte the section called “Status de cluster vermelho”.

Tópicos

Pré-requisitos

Para criar os snapshots manualmente, é necessário trabalhar com o IAM e o Amazon S3. Verifique se você atende aos seguintes pré-requisitos antes de tentar criar um snapshot:

Pré-requisito	Descrição
Bucket do S3	Crie um bucket S3 para armazenar instantâneos manuais para seu domínio de OpenSearch serviço. Para obter mais informações, consulte Criar um bucket no Manual do usuário do Amazon Simple Storage Service. Lembre-se do nome do bucket para usá-lo nos seguintes locais: • Na instrução `Resource` da política do IAM que está anexada à função do IAM

Pré-requisito	Descrição
	• O cliente Python usado para registrar um repositório de snapshots (se você usa esse método) **Important** Não aplique uma regra de ciclo de vida do S3 Glacier a esse bucket. Os snapshots manuais não são compatíveis com a classe de armazenamento do S3 Glacier.

Pré-requisito	Descrição

IAM role (Perfil do IAM)	Crie uma função do IAM para delegar permissões ao OpenSearch Serviço. Para obter instruções, consulte Criação de funções do IAM (console) no Manual do usuário do IAM. O restante deste capítulo se refere a essa função como `TheSnapshotRole` .
	
	Anexar uma política do IAM
	
	Anexe a política a seguir ao `TheSnapshotRole` para permitir acesso ao bucket do S3:
	
	`{`
	`  "Version": "2012-10-17",`
	`  "Statement": [{`
	`  "Action": [`
	`  "s3:ListBucket"`
	`  ],`
	`  "Effect": "Allow",`
	`  "Resource": [`
	`  "arn:aws:s3::: s3-bucket-name "`
	`  ]`
	`  },`
	`  {`
	`  "Action": [`
	`  "s3:GetObject",`
	`  "s3:PutObject",`
	`  "s3:DeleteObject"`
	`  ],`
	`  "Effect": "Allow",`
	`  "Resource": [`
	`  "arn:aws:s3::: s3-bucket-name /*"`
	`  ]`
	`  }`
	`  ]`
	`}`
	
	Para obter instruções de como associar uma política gerenciada a uma função, consulte Adição de permissões de identidade do IAM no Manual do usuário do IAM.

Pré-requisito	Descrição
	Editar a relação de confiança Edite a relação de confiança de `TheSnapshotRole` para especificar o OpenSearch Serviço na `Principal` declaração, conforme mostrado no exemplo a seguir: `{ "Version": "2012-10-17", "Statement": [{ "Sid": "", "Effect": "Allow", "Principal": { "Service": "es.amazonaws.com" }, "Action": "sts:AssumeRole" }] }` Para obter instruções de como editar a relação de confiança, consulte Modificação da política de confiança de uma função no Manual do usuário do IAM.

Pré-requisito	Descrição

Permissões	Para registrar o repositório de instantâneos, você precisa ser capaz de passar `TheSnapshotRole` para OpenSearch o Serviço. Você também precisa de acesso à ação `es:ESHttpPut`. Para conceder ambas as permissões, anexe a seguinte política ao perfil do IAM cujas credenciais estão sendo usadas para assinar a solicitação:
	
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "iam:PassRole", "Resource": "arn:aws:iam:: 123456789012 :role/TheSnapshotRole " }, { "Effect": "Allow", "Action": "es:ESHttpPut", "Resource": "arn:aws:es: region:123456789012 :domain/domain-name /*" } ] }`
	
	Se seu usuário ou função não tiver permissões `iam:PassRole` para passar `TheSnapshotRole`, talvez você encontre o seguinte erro comum ao tentar registrar um repositório na próxima etapa:
	
	`$ python register-repo.py {"Message":"User: arn:aws:iam:: 123456789012 :user/MyUserAccount is not authorized to perform: iam:PassRole on resource: arn:aws:iam:: 123456789012 :role/TheSnapshotRole "}`

Registro de um repositório de snapshots manuais

Você precisa registrar um repositório de instantâneos no OpenSearch Service antes de poder tirar instantâneos de índice manuais. Essa operação única exige que você assine sua AWS solicitação

com credenciais de acesso permitidoTheSnapshotRole, conforme descrito em. the section called "Pré-requisitos"

Etapa 1: mapear a função de instantâneo nos OpenSearch painéis (se estiver usando controle de acesso refinado)

O controle de acesso refinado introduz uma etapa adicional ao registrar um repositório. Mesmo que você use a autenticação básica HTTP para todos os outros fins, será necessário mapear o perfil `manage_snapshots` para o seu perfil do IAM que tem permissões `iam:PassRole` para passar `TheSnapshotRole`.

1. Navegue até o plug-in OpenSearch Dashboards do seu domínio OpenSearch de serviço. Você pode encontrar o endpoint Dashboards no painel do seu domínio no console de OpenSearch serviços.
2. No menu principal, escolha Segurança, Funções e selecione a função manage_snapshots.
3. Escolha Usuários mapeados e Gerenciar mapeamento.
4. Adicione o ARN do perfil que tenha permissões para aprovar `TheSnapshotRole`. Coloque ARNs de perfil em Perfis de backend.

   ```
   arn:aws:iam::123456789123:role/role-name
   ```

5. Selecione Mapa e confirme se o usuário ou função aparece em Usuários mapeados.

Etapa 2: Registrar um repositório

A guia Snapshots a seguir demonstra como registrar um diretório de snapshots. Para opções específicas para criptografar e registrar um snapshot manual após a migração para um novo domínio, consulte as guias relevantes.

Snapshots

Para registrar um repositório de snapshots, envie uma solicitação PUT para o endpoint do domínio OpenSearch Service. Você pode usar o curl, o cliente do Python de exemplo, Postman ou outro método para enviar uma solicitação assinada a fim de registrar o repositório de snapshot. Observe que você não pode usar uma solicitação PUT no console OpenSearch Dashboards para registrar o repositório.

O cabeçalho assume o seguinte formato:

```
PUT domain-endpoint/_snapshot/my-snapshot-repo-name
{
  "type": "s3",
  "settings": {
    "bucket": "s3-bucket-name",
    "base_path": "my/snapshot/directory",
    "region": "region",
    "role_arn": "arn:aws:iam::123456789012:role/TheSnapshotRole"
  }
}
```

> **Note**
>
> Os nomes dos repositórios não podem começar com “cs-”. Além disso, você não deve gravar no mesmo repositório a partir de vários domínios. Apenas um domínio deve ter acesso de gravação ao repositório.

Se o domínio residir em uma nuvem privada virtual (VPC), o computador deverá estar conectado à VPC para que a solicitação registre o repositório de snapshots com êxito. O acesso a uma VPC varia de acordo com a configuração de rede, mas geralmente requer uma conexão com VPN ou rede corporativa. Para verificar se você pode acessar o domínio do OpenSearch Serviço, navegue até `https://your-vpc-domain.region.es.amazonaws.com` em um navegador da Web e verifique se você recebeu a resposta JSON padrão.

Quando seu bucket do Amazon S3 estiver em outro lugar Região da AWS que não seja seu OpenSearch domínio, adicione o parâmetro `"endpoint": "s3.amazonaws.com"` à solicitação.

Encrypted snapshots

Atualmente, você não pode usar chaves AWS Key Management Service (KMS) para criptografar instantâneos manuais, mas pode protegê-los usando criptografia do lado do servidor (SSE).

Para ativar a SSE com chaves gerenciadas pelo S3 para o bucket que você usa como repositório de snapshots, adicione `"server_side_encryption": true` ao bloco `"settings"` da solicitação PUT. Para obter mais informações, consulte Proteção de dados usando criptografia no lado do servidor com chaves de criptografia gerenciadas pelo Amazon S3 no Manual do usuário do Amazon Simple Storage Service.

Como alternativa, você pode usar AWS KMS chaves para criptografia do lado do servidor no bucket do S3 que você usa como repositório de instantâneos. Se você usar essa abordagem, certifique-se de fornecer `TheSnapshotRole` permissão para a AWS KMS chave usada para criptografar o bucket do S3. Para obter mais informações, consulte Usar políticas de chaves no AWS KMS.

Domain migration

O registro de um repositório de snapshots é uma operação única. No entanto, para migrar de um domínio para outro, é necessário registrar o repositório de snapshots no domínio antigo e no novo. O nome do repositório é arbitrário.

Considere as seguintes diretrizes ao migrar para um novo domínio ou registrar o mesmo repositório com vários domínios:

- Ao registrar o repositório no novo domínio, adicione `"readonly": true` para o bloco `"settings"` da solicitação PUT. Essa configuração impede que você sobrescreva acidentalmente dados do domínio antigo. Apenas um domínio deve ter acesso de gravação ao repositório.
- Se estiver migrando dados para um domínio em uma Região da AWS diferente (por exemplo, de um domínio antigo e um bucket localizado em us-east-2 para um novo domínio em us-west-2), substitua `"region": "region"` por `"endpoint": "s3.amazonaws.com"` na instrução de PUT e tente novamente a solicitação.

Uso do cliente Python de exemplo

O cliente Python é mais fácil de automatizar do que uma simples solicitação HTTP, além de ser mais fácil reutilizá-lo. Se você optar por usar esse método para registrar um repositório de snapshots, salve o seguinte código de exemplo Python como um arquivo Python. Por exemplo, `register-repo.py`. O cliente exige os pacotes AWS SDK for Python (Boto3), requests e requests-aws4auth. O cliente contém exemplos comentados para outras operações de snapshot.

Atualize as seguintes variáveis no código de exemplo: `host`, `region`, `path` e `payload`.

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

host = '' # domain endpoint
region = '' # e.g. us-west-1
```

```
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

# Register repository

path = '/_snapshot/my-snapshot-repo-name' # the OpenSearch API endpoint
url = host + path

payload = {
  "type": "s3",
  "settings": {
    "bucket": "s3-bucket-name",
    "base_path": "my/snapshot/directory",
    "region": "us-west-1",
    "role_arn": "arn:aws:iam::123456789012:role/snapshot-role"
  }
}

headers = {"Content-Type": "application/json"}

r = requests.put(url, auth=awsauth, json=payload, headers=headers)

print(r.status_code)
print(r.text)

# # Take snapshot
#
# path = '_snapshot/my-snapshot-repo-name/my-snapshot'
# url = host + path
#
# r = requests.put(url, auth=awsauth)
#
# print(r.text)
#
# # Delete index
#
# path = 'my-index'
# url = host + path
#
# r = requests.delete(url, auth=awsauth)
#
# print(r.text)
```

```
#
# # Restore snapshot (all indexes except Dashboards and fine-grained access control)
#
# path = '_snapshot/my-snapshot-repo-name/my-snapshot/_restore'
# url = host + path
#
# payload = {
#   "indices": "-.kibana*,-.opendistro_security,-.opendistro-*",
#   "include_global_state": False
# }
#
# headers = {"Content-Type": "application/json"}
#
# r = requests.post(url, auth=awsauth, json=payload, headers=headers)
#
# print(r.text)
#
# # Restore snapshot (one index)
#
# path = '_snapshot/my-snapshot-repo-name/my-snapshot/_restore'
# url = host + path
#
# payload = {"indices": "my-index"}
#
# headers = {"Content-Type": "application/json"}
#
# r = requests.post(url, auth=awsauth, json=payload, headers=headers)
#
# print(r.text)
```

Obtenção manual de snapshots

Os snapshots não são instantâneos. Eles demoram para serem concluídos e não representam uma point-in-time visão perfeita do cluster. Enquanto um snapshot está em andamento, você ainda pode indexar documentos e fazer outras solicitações ao cluster, mas novos documentos e atualizações em documentos existentes geralmente não são incluídos no snapshot. O instantâneo inclui fragmentos primários conforme existiam quando o instantâneo OpenSearch foi iniciado. Dependendo do tamanho do grupo de threads de snapshot, diferentes fragmentos podem ser incluídos no snapshot em momentos um pouco diferentes. Para ver as práticas recomendadas de snapshots, consulte the section called “Melhore a performance do snapshot”.

Armazenamento e performance de snapshots

OpenSearch os instantâneos são incrementais, o que significa que eles armazenam somente os dados que foram alterados desde o último instantâneo bem-sucedido. Essa natureza incremental significa que a diferença no uso de disco entre snapshots frequentes e infrequentes normalmente é mínima. Ou seja, criar snapshots por hora por uma semana (em um total de 168 snapshots) pode não usar muito mais espaço em disco do que criar um único snapshot no final da semana. Além disso, quanto maior a frequência da criação de snapshots, menos tempo eles demoram para serem concluídos. Por exemplo, snapshots diários podem levar de 20 a 30 minutos para serem concluídos, enquanto os snapshots por hora podem ser concluídos em poucos minutos. Alguns OpenSearch usuários tiram fotos a cada meia hora.

Faça um snapshot

Ao criar um snapshot, você especifica as seguintes informações:

- O nome do repositório de snapshots
- Um nome para o snapshot

Os exemplos neste capítulo usam curl, um cliente HTTP comum, por conveniência e brevidade. Para passar um nome de usuário e uma senha para sua solicitação de curl, consulte o Tutorial de introdução.

Se as políticas de acesso especificarem usuários ou perfis, você deverá assinar suas solicitações de snapshot. Para o curl, você pode usar a opção `--aws-sigv4` com a versão 7.75.0 ou posterior. Você também pode usar os exemplos comentados no exemplo de cliente Python para fazer solicitações HTTP assinadas para os mesmos endpoints usados pelos comandos curl.

Para obter um snapshot manual, faça o seguinte:

1. Você não poderá obter um snapshot se houver um em andamento no momento. Para verificar, execute o seguinte comando:

   ```
   curl -XGET 'domain-endpoint/_snapshot/_status'
   ```

2. Execute o comando a seguir para obter um snapshot manual:

   ```
   curl -XPUT 'domain-endpoint/_snapshot/repository-name/snapshot-name'
   ```

Para incluir ou excluir determinados índices e especificar outras configurações, adicione um corpo de solicitação. Para a estrutura da solicitação, consulte Tirar instantâneos na OpenSearch documentação.

> **Note**
>
> O tempo necessário para tirar um instantâneo aumenta com o tamanho do domínio do OpenSearch Serviço. As operações de snapshot de longa duração, às vezes, encontram o seguinte erro: `504 GATEWAY_TIMEOUT`. Normalmente, você pode ignorar esses erros e esperar até que a operação seja concluída com êxito. Execute o comando a seguir para verificar o estado de todos os snapshots de seu domínio:
>
> ```
> curl -XGET 'domain-endpoint/_snapshot/repository-name/_all?pretty'
> ```

Restauração de snapshots

Antes de restaurar um snapshot, certifique-se de que o domínio de destino não use Multi-AZ com modo de espera. Ter o modo de espera habilitado faz com que a operação de restauração falhe.

> **Warning**
>
> Se você usar aliases de índice, você deve interromper as solicitações de gravação para um alias ou mudar o alias para outro índice antes de excluir seu índice. Parar as solicitações de gravação ajuda a evitar o seguinte cenário:
>
> 1. Você exclui um índice, que também exclui seu alias.
> 2. Uma solicitação de gravação com erro para o alias recém-excluído cria um novo índice com o mesmo nome do alias.
> 3. Você não pode mais usar o alias devido a um conflito de nomes com o novo índice. Se você alternou o alias para outro índice, especifique `"include_aliases": false` ao restaurar a partir de um snapshot.

Para restaurar um snapshot

1. Identifique o snapshot que deseja restaurar. Assegure-se de que todas as configurações desse índice, como pacotes de análise personalizados ou configurações de requisitos de alocação, sejam compatíveis com o domínio. Para ver todos os repositórios de snapshots, execute o comando a seguir:

   ```
   curl -XGET 'domain-endpoint/_snapshot?pretty'
   ```

   Após identificar o repositório, execute o comando a seguir para ver todos os snapshots:

   ```
   curl -XGET 'domain-endpoint/_snapshot/repository-name/_all?pretty'
   ```

   > **Note**
   >
   > A maioria dos snapshots automatizados é armazenada no repositório `cs-automated`. Se o seu domínio criptografa dados em repouso, eles são armazenados no repositório `cs-automated-enc`. Se não encontrar o repositório de snapshots manuais que estava buscando, confirme se você o registrou no domínio.

2. (Opcional) Exclua ou renomeie um ou mais índices no domínio OpenSearch Service se você tiver conflitos de nomenclatura entre os índices no cluster e os índices no snapshot. Você não pode restaurar um snapshot dos seus índices em um OpenSearch cluster que já contém índices com os mesmos nomes.

   Você terá as seguintes opções em caso de conflitos de nomenclatura de índice:

   - Exclua os índices no domínio de OpenSearch serviço existente e, em seguida, restaure o snapshot.
   - Renomeie os índices à medida que os restaura no snapshot e reindexe-os mais tarde.
   - Restaure o instantâneo em um domínio OpenSearch de serviço diferente (possível somente com instantâneos manuais).

   O seguinte comando exclui todos os índices existentes em um domínio:

   ```
   curl -XDELETE 'domain-endpoint/_all'
   ```

   No entanto, se você não planeja restaurar todos os índices, pode simplesmente excluir um:

```
curl -XDELETE 'domain-endpoint/index-name'
```

3. Para restaurar um snapshot, execute o seguinte comando:

```
curl -XPOST 'domain-endpoint/_snapshot/repository-name/snapshot-name/_restore'
```

Devido às permissões especiais nos OpenSearch painéis e aos índices de controle de acesso refinados, as tentativas de restaurar todos os índices podem falhar, especialmente se você tentar restaurar a partir de um instantâneo automatizado. O exemplo a seguir restaura apenas um índice `my-index` de `2020-snapshot` no repositório de snapshots `cs-automated`:

```
curl -XPOST 'domain-endpoint/_snapshot/cs-automated/2020-snapshot/_restore' \
-d '{"indices": "my-index"}' \
-H 'Content-Type: application/json'
```

Como alternativa, é possível restaurar todos os índices, exceto os índices de controle de acesso refinado e o Dashboards:

```
curl -XPOST 'domain-endpoint/_snapshot/cs-automated/2020-snapshot/_restore' \
-d '{"indices": "-.kibana*,-.opendistro*"}' \
-H 'Content-Type: application/json'
```

Você pode restaurar um snapshot sem excluir seus dados usando os parâmetros `rename_pattern` e `rename_replacement`. Para obter mais informações sobre esses parâmetros, consulte os campos de solicitação da API Restore Snapshot e o exemplo de solicitação na OpenSearch documentação.

> **Note**
>
> Se nem todos os fragmentos principais estiverem disponíveis para os índices envolvidos, o `state` do snapshot poderá ser `PARTIAL`. Esse valor indica que os dados de pelo menos um fragmento não foram armazenados com êxito. Mesmo assim é possível restaurar por meio de um snapshot parcial, mas pode ser necessário usar snapshots mais antigos para restaurar índices ausentes.

Excluir snapshots manuais

Para excluir um snapshot manual, execute o seguinte comando:

```
DELETE _snapshot/repository-name/snapshot-name
```

Automação de snapshots com o Snapshot Management

Você pode configurar uma política de gerenciamento de instantâneos (SM) nos OpenSearch painéis para automatizar a criação e a exclusão periódicas de instantâneos. O SM pode capturar um snapshot de um grupo de índices, enquanto o Index State Management só pode tirar um snapshot por índice. Para usar o SM in OpenSearch Service, você precisa registrar seu próprio repositório Amazon S3. Para obter instruções sobre como registrar seu repositório, consulte Registrar um repositório manual de snapshots.

Antes do SM, o OpenSearch Service oferecia um recurso de captura instantânea gratuito e automatizado que ainda está ativado por padrão. Esse atributo envia snapshots para o repositório mantido pelo serviço `cs-*`. Para desativar o atributo, entre em contato com o AWS Support.

Para obter mais informações sobre o recurso SM, consulte Gerenciamento de instantâneos na OpenSearch documentação.

Atualmente, o SM não oferece suporte à criação de snapshots em vários tipos de índice. Por exemplo, se você tentar criar um snapshot em vários índices `*` e alguns índices estiverem na camada de maior atividade, a criação do snapshot falhará. Se você precisar que seu snapshot contenha vários tipos de índice, use a ação de snapshot do ISM até que o SM ofereça suporte a essa opção.

Configurar permissões do

Se você estiver atualizando para 2.5 de uma versão anterior do domínio OpenSearch de serviço, as permissões de segurança do gerenciamento de instantâneos podem não estar definidas no domínio. Os usuários não administradores deverão ser mapeados nessa função para usar o gerenciamento de snapshot usando o controle de aceso detalhado. Para criar manualmente o perfil de gerenciamento de snapshot, faça o seguinte:

1. Em OpenSearch Painéis, acesse Segurança e escolha Permissões.
2. Escolha Criar grupo de ações e configure os seguintes grupos:

Group name	Permissões
`snapshot_management_full_access`	• `cluster:admin/opensearch/snapshot_management/*` • `cluster:admin/opensearch/notifications/feature/publish` • `cluster:admin/repository/*` • `cluster:admin/snapshot/*`
`snapshot_management_read_access`	• `cluster:admin/opensearch/snapshot_management/policy/get` • `cluster:admin/opensearch/snapshot_management/policy/search` • `cluster:admin/opensearch/snapshot_management/policy/explain` • `cluster:admin/repository/get` • `cluster:admin/snapshot/get`

3. Escolha Funções e, em seguida, Criar função.
4. Nomeie o perfil snapshot_management_role.
5. Para Permissões de cluster, selecione `snapshot_management_full_access` ou `snapshot_management_read_access`.
6. Escolha Criar.
7. Depois de criar a função, mapeie-a em qualquer função de usuário ou de back-end que gerencie snapshots.

Considerações

Considere o seguinte ao configurar o gerenciamento de snapshots:

- É permitida uma política por repositório.
- São permitidos até 400 snapshots para uma política.
- Esse atributo não será executado se seu domínio tiver um status vermelho, estiver sob alta pressão da JVM (85% ou mais) ou tiver uma função de captura instantânea bloqueada. Quando

o desempenho geral de indexação e pesquisa do seu cluster é afetado, o SM também pode ser afetado.

- Uma operação de snapshot só é iniciada após a conclusão da operação anterior, de forma que nenhuma operação simultânea de snapshot seja ativada por uma política.
- Várias políticas com o mesmo cronograma podem causar um pico de recursos. Se os índices de captura instantânea das políticas se sobrepõem, as operações de captura instantânea em nível de fragmento só podem ser executadas sequencialmente, o que pode causar um problema de desempenho em cascata. Se as políticas compartilharem um repositório, haverá um pico de operações de gravação nesse repositório.
- Recomendamos que você agende a automação das operações de snapshot para não mais do que uma vez por hora, a menos que tenha um caso de uso especial.

Automação de snapshots com o Gerenciamento de estados de índices

Você pode usar a operação `snapshot` do Gerenciamento de estados de índices (ISM) para acionar automaticamente instantâneos de índices com base em alterações em sua idade, tamanho ou número de documentos. O ISM é melhor quando você precisa de um snapshot por índice. Se você precisar capturar um snapshot de um grupo de índices, consulte Automação de snapshots com o Snapshot Management.

Para usar o SM in OpenSearch Service, você precisa registrar seu próprio repositório Amazon S3. Para obter um exemplo de política do ISM usando a operação `snapshot`, consulte Políticas de exemplo.

Uso do Curator para snapshots

Se o ISM não funcionar para o gerenciamento de índices e snapshots, você poderá usar o Curator. Ele oferece funcionalidade de filtragem avançada que pode ajudar a simplificar tarefas de gerenciamento em clusters complexos. Use o pip para instalar o Curator:

```
pip install elasticsearch-curator
```

Você pode usar o Curator como uma interface de linha de comando (CLI) ou API do Python. Se você usar a API do Python, deverá usar a versão 7.13.4 ou anterior do cliente elasticsearch-py herdado. Ele não oferece suporte a um cliente opensearch-py.

Se você usar a CLI, exporte suas credenciais na linha de comando e configure o `curator.yml` da seguinte maneira:

```
client:
  hosts: search-my-domain.us-west-1.es.amazonaws.com
  port: 443
  use_ssl: True
  aws_region: us-west-1
  aws_sign_request: True
  ssl_no_validate: False
  timeout: 60

logging:
  loglevel: INFO
```

Atualizando domínios do Amazon OpenSearch Service

> **Note**
>
> OpenSearch e as atualizações de versão do Elasticsearch diferem das atualizações do software de serviço. Para obter informações sobre como atualizar o software de serviço para seu domínio OpenSearch de serviço, consultethe section called “Atualizações de software de serviço”.

O Amazon OpenSearch Service oferece atualizações no local para domínios que executam OpenSearch 1.0 ou posterior, ou Elasticsearch 5.1 ou posterior. Se você usa serviços como Amazon Data Firehose ou Amazon CloudWatch Logs para transmitir dados para o OpenSearch Service, verifique se esses serviços são compatíveis com a versão mais recente do antes de OpenSearch migrar.

Tópicos

- Caminhos de atualização com suporte
- Iniciar uma atualização (console)
- Iniciar uma atualização (CLI)
- Iniciar uma atualização (SDK)
- Solução de problemas de falha de validação

- Solução de problemas em uma atualização
- Como usar um snapshot para migrar dados

Caminhos de atualização com suporte

Atualmente, o OpenSearch Service oferece suporte aos seguintes caminhos de atualização:

Da versão	Para a versão
OpenSearch 1.3 ou 2. x	OpenSearch 2. x A versão 2.3 tem as seguintes alterações importantes: • O `type` parâmetro foi removido de todos os endpoints OpenSearch da API na versão 2.0. Para obter mais informações, consulte alterações que podem causar interrupções. • Se seu domínio contiver algum índice (quente ou frio) que tenha sido originalm ente criado no Elasticsearch 6.8, esses índices não são compatíveis com 2.3. UltraWarm OpenSearch Antes de atualizar para a versão 2.3, será necessário reindexar os índices incompatíveis. Para índices incompatíveis UltraWarm ou frios, migre-os para o armazenamento ativo, reindexe os dados e, em seguida, migre-os de volta para o armazenamento quente ou frio. Também é possível excluir os índices quando eles não são mais necessários. Se você, acidentalmente, atualizar seu domínio para a versão 2.3 sem executar essas etapas primeiro, não poderá migrar os índices incompatíveis do nível de armazenamento atual. Sua única opção será excluí-los.
OpenSearch 1. x	OpenSearch 1. x
Elasticsearch 7.x	Elasticsearch 7. x ou OpenSearch 1. x

Da versão	Para a versão
	Important OpenSearch 1. x introduz várias mudanças significativas. Para obter detalhes, consulte Renomeação do Amazon OpenSearch Service.
Elasticsearch 6.8	Elasticsearch 7. x ou OpenSearch 1. x **Important** O Elasticsearch 7.0 e OpenSearch 1.0 incluem várias mudanças importantes. Antes de iniciar uma atualização local, recomendamos tirar um instantâneo manual do 6. domínio x, restaurando-o em um teste 7. x ou OpenSearch 1. domínio x e usando esse domínio de teste para identificar possíveis problemas de atualização. Para alterações significa tivas na OpenSearch versão 1.0, consulteRenomeação do Amazon OpenSearch Service. Assim como o Elasticsearch 6.x, os índices só podem conter um tipo de mapeamento, mas esse tipo agora deve ser chamado de `_doc`. Como resultado, determinadas APIs não exigem mais um tipo de mapeamento no corpo da solicitação (como a API `_bulk`). Para novos índices, o Elasticsearch 7 auto-hospedado. x e OpenSearc h 1. x têm uma contagem de fragmentos padrão de um. OpenSearch Domínios de serviço no Elasticsearch 7. x e posteriores mantêm o padrão anterior de cinco.
Elasticsearch 6.x	Elasticsearch 6.x

Da versão	Para a versão
Elasticsearch 5.6	Elasticsearch 6.x **Important** Os índices criados na versão 6.x não são mais compatíveis com vários tipos de mapeamento. Índices criados na versão 5.x ainda são compatíve is com vários tipos de mapeamento quando restaurados em um cluster 6.x. Verifique se o seu código de cliente cria apenas um único tipo de mapeamento por índice. Para minimizar o tempo de inatividade durante a atualização do Elasticsearch 5.6 para 6. x, o OpenSearch serviço reindexa o `.kibana` índice`.kibana-6` , exclui`.kibana`, cria um alias chamado `.kibana` e mapeia o novo índice para o novo alias.
Elasticsearch 5.x	Elasticsearch 5.x

O processo de atualização consiste em três etapas:

1. Verificações de pré-atualização — O OpenSearch serviço verifica se há problemas que podem bloquear uma atualização e não prossegue para a próxima etapa, a menos que essas verificações sejam bem-sucedidas.
2. Snapshot — O OpenSearch serviço tira um snapshot do cluster OpenSearch ou do Elasticsearch e não passa para a próxima etapa, a menos que o snapshot seja bem-sucedido. Se a atualização falhar, o OpenSearch Service usará esse snapshot para restaurar o cluster ao estado original. Para obter mais informações, consulte the section called “Não é possível reverter para a versão anterior após a atualização.”.
3. Atualização — O OpenSearch serviço inicia a atualização, que pode levar de 15 minutos a várias horas para ser concluída. OpenSearch Os painéis podem estar indisponíveis durante parte ou toda a atualização.

Iniciar uma atualização (console)

O processo de atualização é irreversível e não pode ser pausado nem cancelado. Durante uma atualização, não é possível fazer alterações de configuração no domínio. Antes de iniciar uma atualização, verifique novamente se deseja prosseguir. Você pode usar essas mesmas etapas para executar a verificação de pré-atualização sem realmente iniciar uma atualização.

Se o cluster tiver nós principais dedicados, as OpenSearch atualizações serão concluídas sem tempo de inatividade. Caso contrário, o cluster poderá não responder durante vários segundos após a atualização enquanto elege um nó principal.

Para atualizar um domínio para uma versão posterior do OpenSearch ou Elasticsearch

1. Crie um snapshot manual do seu domínio. Esse instantâneo serve como um backup que você pode restaurar em um novo domínio se quiser voltar a usar a OpenSearch versão anterior.
2. Acesse http://aws.amazon.com e escolha Fazer login no console.
3. Em Analytics, escolha Amazon OpenSearch Service.
4. No painel de navegação, em Domínios, escolha o domínio que deseja atualizar.
5. Escolha Ações e Atualizar.
6. Selecione a versão para a qual deseja atualizar. Se você estiver atualizando para uma OpenSearch versão, a opção Ativar modo de compatibilidade será exibida. Se você habilitar essa configuração, OpenSearch reporta sua versão como 7.10 para permitir que clientes e plug-ins do Elasticsearch OSS, como o Logstash, continuem trabalhando com o Amazon Service. OpenSearch Você poderá desabilitar essa configuração posteriormente.
7. Escolha Atualizar.
8. Marque Status no painel do domínio para monitorar o status da atualização.

Iniciar uma atualização (CLI)

Você pode usar as seguintes operações para identificar a versão correta do OpenSearch ou do Elasticsearch para seu domínio, iniciar uma atualização no local, realizar a verificação de pré-atualização e ver o progresso:

- `get-compatible-versions` (`GetCompatibleVersions`)
- `upgrade-domain` (`UpgradeDomain`)

- `get-upgrade-status` (`GetUpgradeStatus`)
- `get-upgrade-history` (`GetUpgradeHistory`)

Para obter mais informações, consulte a referência de comandos daAWS CLI e a Referência da API do Amazon OpenSearch Service.

Iniciar uma atualização (SDK)

Este exemplo usa o cliente Python de OpenSearchServicebaixo nível AWS SDK for Python (Boto) do para verificar se um domínio está qualificado para atualização para uma versão específica, atualizá-lo e verificar continuamente o status do upgrade.

```
import boto3
from botocore.config import Config
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default Region.

DOMAIN_NAME = ''  # The name of the domain to upgrade
TARGET_VERSION = ''  # The version you want to upgrade the domain to. For example,
 OpenSearch_1.1

my_config = Config(
    # Optionally lets you specify a Region other than your default.
    region_name='us-east-1'
)
client = boto3.client('opensearch', config=my_config)


def check_versions():
    """Determine whether domain is eligible for upgrade"""
    response = client.get_compatible_versions(
        DomainName=DOMAIN_NAME
    )
    compatible_versions = response['CompatibleVersions']
    for i in range(len(compatible_versions)):
        if TARGET_VERSION in compatible_versions[i]["TargetVersions"]:
            print('Domain is eligible for upgrade to ' + TARGET_VERSION)
            upgrade_domain()
            print(response)
```

```
        else:
            print('Domain not eligible for upgrade to ' + TARGET_VERSION)


def upgrade_domain():
    """Upgrades the domain"""
    response = client.upgrade_domain(
        DomainName=DOMAIN_NAME,
        TargetVersion=TARGET_VERSION
    )
    print('Upgrading domain to ' + TARGET_VERSION + '...' + response)
    time.sleep(5)
    wait_for_upgrade()


def wait_for_upgrade():
    """Get the status of the upgrade"""
    response = client.get_upgrade_status(
        DomainName=DOMAIN_NAME
    )
    if (response['UpgradeStep']) == 'UPGRADE' and (response['StepStatus']) ==
 'SUCCEEDED':
        print('Domain successfully upgraded to ' + TARGET_VERSION)
    elif (response['StepStatus']) == 'FAILED':
        print('Upgrade failed. Please try again.')
    elif (response['StepStatus']) == 'SUCCEEDED_WITH_ISSUES':
        print('Upgrade succeeded with issues')
    elif (response['StepStatus']) == 'IN_PROGRESS':
        time.sleep(30)
        wait_for_upgrade()


def main():
    check_versions()


if __name__ == "__main__":
    main()
```

Solução de problemas de falha de validação

Quando você inicia uma atualização da versão OpenSearch ou do Elasticsearch, o OpenSearch Service primeiro executa uma série de verificações de validação para garantir que seu domínio

esteja qualificado para uma atualização. Se alguma dessas verificações falhar, você receberá uma notificação no console contendo os problemas específicos que deverão ser corrigidos antes da atualização do domínio. Para obter uma lista de possíveis problemas e as etapas para resolvê-los, consulte the section called “Solução de problemas de erros de validação”.

Solução de problemas em uma atualização

As atualizações do no local exigem domínios íntegros. Seu domínio pode não estar qualificado para uma atualização ou não ser atualizado por vários motivos. A tabela a seguir mostra os problemas mais comuns.

Problema	Descrição
Plug-in opcional não compatível	Quando você atualiza um domínio com plug-ins opcionais, o OpenSearch Service também atualiza automaticamente os plug-ins. Portanto, a versão de destino do seu domínio também deve oferecer suporte a esses plug-ins opcionais. Se o domínio tiver um plug-in opcional instalado que não esteja disponível para a versão de destino, a solicitação de upgrade falhará.
Muitos fragmentos por nó	OpenSearch, bem como 7. As versões x do Elasticsearch têm uma configuração padrão de no máximo 1.000 fragmentos por nó. Se um nó em seu cluster atual exceder essa configuração, o OpenSearch Serviço não permitirá que você faça o upgrade. Consulte the section called “Limite máximo de fragmentos excedido” para obter opções de solução de problemas.
Domínio no processamento	O domínio está no meio de uma mudança de configuração. Verifique a qualificação da atualização após a conclusão da operação.
Status de cluster vermelho	Um ou mais índices no cluster estão vermelhos. Para obter etapas sobre a solução de problemas, consulte the section called “Status de cluster vermelho”.
Alta taxa de erros	O cluster está retornando um grande número de erros 5xx ao tentar processar solicitações. Geralmente, esse problema é resultado de muitas solicitações de leitura ou gravação simultâneas. Considere reduzir o tráfego para o cluster ou dimensionar seu domínio.

Problema	Descrição
Cérebro dividido	Cérebro dividido significa que o cluster tem mais de um nó principal e foi dividido em dois clusters que nunca se juntarão por conta própria. Você pode evitar dividir o cérebro usando o número recomendado de nós principais dedicados. Para ajudar na recuperação do cérebro dividido, entre em contato com AWS Support.
Nó principal não encontrado	OpenSearch O serviço não consegue encontrar o nó principal do cluster. Se o domínio usa multi-AZ, uma falha da zona de disponibilidade pode ter causado a perda de quorum do cluster e a incapacidade de escolher um novo nó principal. Se o problema não se resolver, entre em contato com AWS Support.
Muitas tarefas pendentes	O nó principal está sob carga pesada e tem muitas tarefas pendentes. Considere reduzir o tráfego para o cluster ou dimensionar seu domínio.
Volume de armazenamento prejudicado	O volume de disco de um ou mais nós não está funcionando corretame nte. Esse problema geralmente ocorre junto com outros problemas , como uma alta taxa de erros ou muitas tarefas pendentes. Se o problema ocorrer isoladamente e não se resolver, entre em contato com AWS Support.
Problema de chave do KMS	A chave do KMS usada para criptografar o domínio está inacessível ou ausente. Para ter mais informações, consulte the section called “Monitoramento de domínios que criptografam dados em repouso”.
Snapshot em andamento	O domínio está tirando um snapshot no momento. Verifique a qualifica ção da atualização após a conclusão do snapshot. Além disso, verifique se é possível listar repositórios de snapshots manuais, listar snapshots nesses repositórios e obter snapshots manuais. Se o OpenSearch Serviço não conseguir verificar se um snapshot está em andamento, as atualizações podem falhar.
Tempo limite ou falha de snapshot	O snapshot de pré-atualização demorou muito para ser concluído ou falhou. Verifique o status do cluster e tente novamente. Se o problema continuar, entre em contato com o AWS Support.

Problema	Descrição
Índices incompatíveis	Um ou mais índices são incompatíveis com a versão de destino. Esse problema pode ocorrer se você migrou os índices de uma versão mais antiga do Elasticsearch OpenSearch . Reindexe os índices e tente novamente.
Uso elevado do disco	O uso de disco para o cluster está acima de 90%. Exclua os dados ou dimensione o domínio e tente novamente.
Uso elevado do JVM	A pressão de memória JVM está acima de 75%. Reduza o tráfego para o cluster ou dimensione o domínio e tente novamente.
OpenSearch Problema de alias de painéis	`.dashboards` já está configurado como um alias e mapeia para um índice incompatível, provavelmente de uma versão anterior do Dashboards. OpenSearch Reindexe e tente novamente.
Status de painéis vermelhos	OpenSearch O status dos painéis é vermelho. Tente usar o Dashboard s quando a atualização for concluída. Se o status vermelho persistir, resolva-o manualmente e tente novamente.
Compatibilidade entre clusters	Você só pode atualizar se a compatibilidade entre clusters for mantida entre os domínios de origem e de destino após a atualização. Durante o processo de atualização, todas as conexões incompatíveis são identific adas. Para prosseguir, atualize o domínio remoto ou excluir as conexões incompatíveis. Observe que, se a replicação estiver ativa no domínio, você não poderá retomá-la depois de excluir a conexão.
Outro problema de OpenSearch serviço	Problemas com o OpenSearch serviço em si podem fazer com que seu domínio seja exibido como inelegível para um upgrade. Se nenhuma das condições anteriores se aplicar ao seu domínio e o problema persistir por mais de um dia, entre em contato com AWS Support.

Como usar um snapshot para migrar dados

As atualizações no local são a maneira mais fácil, rápida e confiável de atualizar um domínio para uma versão posterior OpenSearch ou do Elasticsearch. Os snapshots são uma boa opção se você

precisa migrar de uma versão anterior a 5.1 do Elasticsearch ou deseja migrar para um cluster totalmente novo.

A tabela a seguir mostra como usar snapshots para migrar dados para um domínio que usa uma versão diferente OpenSearch ou uma versão do Elasticsearch. Para obter mais informações sobre a criação e a restauração de snapshots, consulte the section called “Criação de snapshots de índices”.

Da versão	Para a versão	Processo de migração

OpenSearch 1.3 ou 2. x	OpenSearch 2. x	1. Analise as alterações mais recentes da versão OpenSearch 2.3 para ver se você precisa fazer ajustes em seus índices ou aplicativos.
		2. Crie um snapshot manual do domínio 1.3 ou 2.x.
		3. Crie um domínio 2.x que seja uma versão superior ao seu domínio 1.3 ou 2.x original.
		4. Restaure o snapshot do domínio original para o domínio 2.x. Durante a operação, talvez seja necessári o restaurar o índice do `.opensearch` com um novo nome:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".opensearch",`
		`  "rename_replacement": ".backup-opensearc h"`
		`}`
		Em seguida, você pode reindexar o `.backup-o pensearch` no novo domínio e definir `.opensear ch` como seu alias. Observe que a chamada REST `_restore` não inclui `include_global_state` porque a entrada padrão `_restore` é falsa. Como resultado, o domínio de teste não incluirá nenhum modelo de índice e não terá o estado completo do backup.

Da versão	Para a versão	Processo de migração
		5. Se você não precisar mais do domínio original, exclua-o. Do contrário, você continuará a ser cobrado pelo domínio.

OpenSearch 1. x	OpenSearch 1. x	1. Crie um snapshot manual do domínio 1.x.
		2. Crie um domínio 1.x que seja uma versão superior ao seu domínio 1.x original.
		3. Restaure o snapshot do domínio original para o domínio 1.x. Durante a operação, talvez seja necessário restaurar o índice do `.opensearch` com um novo nome:
		
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".opensearch",`
		`  "rename_replacement": ".backup-opensearch"`
		`}`
		
		Em seguida, você pode reindexar o `.backup-opensearch` no novo domínio e definir `.opensearch` como seu alias. Observe que a chamada REST `_restore` não inclui `include_global_state` porque a entrada padrão `_restore` é falsa. Como resultado, o domínio de teste não incluirá nenhum modelo de índice e não terá o estado completo do backup.
		4. Se você não precisar mais do domínio original, exclua-o. Do contrário, você continuará a ser cobrado pelo domínio.

Da versão	Para a versão	Processo de migração

Elasticsearch 6.x ou 7.x	OpenSearch 1. x	1. Analise as alterações mais recentes da OpenSearch versão 1.0 para ver se você precisa fazer ajustes em seus índices ou aplicativos.
		2. Crie um snapshot manual do domínio do Elasticsearch 7.x ou 6.x.
		3. Crie um OpenSearch 1. domínio x.
		4. Restaure o snapshot do domínio Elasticsearch para o domínio. OpenSearch Durante a operação, talvez seja necessário restaurar o índice do `.elasticsearch` com um novo nome:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".elasticsearch",`
		`  "rename_replacement": ".backup-opensearch"`
		`}`
		Em seguida, você pode reindexar o `.backup-opensearch` no novo domínio e definir `.elasticsearch` como seu alias. Observe que a chamada REST `_restore` não inclui `include_global_state` porque a entrada padrão `_restore` é falsa. Como resultado, o domínio de teste não incluirá nenhum modelo de índice e não terá o estado completo do backup.
		5. Se você não precisar mais do domínio original, exclua-o. Do contrário, você continuará a ser cobrado pelo domínio.

Da versão	Para a versão	Processo de migração

Elasticsearch 6.x	Elasticsearch 7.x	1. Revise as alterações que podem causar falhas na versão 7.0 para verificar se é necessário ajustar os índices ou as aplicações.
		2. Crie um snapshot manual do domínio 6.x.
		3. Crie um domínio 7.x.
		4. Restaure o snapshot do domínio original para o domínio 7.x. Durante a operação, você provavelmente precisará restaurar o índice do `.opensearch` com um novo nome:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".elasticsearch",`
		`  "rename_replacement": ".backup-elasticsearch"`
		`}`
		Em seguida, você pode reindexar o `.backup-elasticsearch` no novo domínio e definir `.elasticsearch` como seu alias. Observe que a chamada REST `_restore` não inclui `include_global_state` porque a entrada padrão `_restore` é falsa. Como resultado, o domínio de teste não incluirá nenhum modelo de índice e não terá o estado completo do backup.
		5. Se você não precisar mais do domínio original, exclua-o. Do contrário, você continuará a ser cobrado pelo domínio.

Da versão	Para a versão	Processo de migração
Elasticsearch 6.x	Elasticsearch 6.8	1. Crie um snapshot manual do domínio 6.x. 2. Crie um domínio 6.8. 3. Restaure o snapshot do domínio original para o domínio 6.8. 4. Se você não precisar mais do domínio original, exclua-o. Do contrário, você continuará a ser cobrado pelo domínio.
Elasticsearch 5.x	Elasticsearch 6.x	1. Revise as alterações que podem causar interrupções na versão 6.0 para verificar se você precisa fazer ajustes em seus índices ou aplicações. 2. Crie um snapshot manual do domínio 5.x. 3. Crie um domínio 6.x. 4. Restaure o snapshot do domínio original para o domínio 6.x. 5. Se você não precisar mais do domínio 5.x, exclua-o. Do contrário, você continuará a ser cobrado pelo domínio.
Elasticsearch 5.x	Elasticsearch 5.6	1. Crie um snapshot manual do domínio 5.x. 2. Crie um domínio 5.6. 3. Restaure o snapshot do domínio original para o domínio 5.6. 4. Se você não precisar mais do domínio original, exclua-o. Do contrário, você continuará a ser cobrado pelo domínio.

Da versão	Para a versão	Processo de migração
Elasticsearch 2.3	Elasticsearch 6.x	Os snapshots do Elasticsearch 2.3 não são compatíveis com o 6.x. Para migrar os dados diretamente da versão 2.3 para a 6.x, você terá que recriar manualmente os índices no novo domínio. Como alternativa, você pode executar as etapas da atualização da versão 2.3 para a 5.x nesta tabela, executar operações de `_reindex` no novo domínio da 5.x para converter os índices da 2.3 em índices da 5.x e, por fim, seguir as etapas da atualização da versão 5.x para a 6.x.
Elasticsearch 2.3	Elasticsearch 5.x	1. Revise as alterações que podem causar falhas na versão 5.0 para verificar se é necessário ajustar os índices ou as aplicações. 2. Crie um snapshot manual do domínio 2.3. 3. Crie um domínio 5.x. 4. Restaure o snapshot do domínio 2.3 para o 5.x. 5. Se você não precisar mais do domínio 2.3, exclua-o. Do contrário, você continuará a ser cobrado pelo domínio.

Da versão	Para a versão	Processo de migração
Elasticsearch 1.5	Elasticsearch 5.x	Os snapshots do Elasticsearch 1.5 não são compatíveis com o 5.x. Para migrar os dados da versão 1.5 para a 5.x, você terá que recriar manualmente os índices no novo domínio. **Important** Os instantâneos 1.5 são compatíveis com 2.3, mas os domínios do OpenSearch Service 2.3 não suportam a `_reindex` operação. Como você não pode reindexá-los, os índices originados em um domínio da versão 1.5 ainda não podem ser restaurados de snapshots da 2.3 para domínios da 5.x.
Elasticsearch 1.5	Elasticsearch 2.3	1. Use o plug-in de migração para descobrir se é possível atualizar diretamente para a versão 2.3. Talvez você precise alterar seus dados antes de migrar. a. Em um navegador da web, abra `http://`*`domain-endpoint`*` /_plugin/migration/` . b. Escolha Run checks now. c. Analise os resultados e, se necessário, siga as instruções para fazer alterações em seus dados. 2. Crie um snapshot manual do domínio 1.5. 3. Crie um domínio 2.3. 4. Restaure o snapshot do domínio 1.5 para o 2.3. 5. Se você não precisar mais do domínio 1.5, exclua-o. Do contrário, você continuará a ser cobrado pelo domínio.

Criação de um endpoint personalizado para o Amazon OpenSearch Service

A criação de um endpoint personalizado para o domínio do Amazon OpenSearch Service facilita a referência aos URLs do OpenSearch e do OpenSearch Dashboards. Você pode incluir a identidade visual da sua empresa ou simplesmente usar um endpoint mais curto e mais fácil de lembrar do que o padrão.

Se você precisar alternar para um novo domínio, bastará atualizar seu DNS para apontar para o novo URL e continuar usando o mesmo endpoint de antes.

Você protege os endpoints personalizados gerando um certificado no AWS Certificate Manager (ACM) ou importando um dos seus próprios certificados.

Endpoints personalizados para novos domínios

Você pode habilitar um endpoint personalizado para um novo domínio do OpenSearch Service usando o console do OpenSearch Service, a AWS CLI ou a API de configuração.

Para personalizar o endpoint (console)

1. No console do OpenSearch Service, escolha Criar domínio.
2. Em Endpoint personalizado, selecione Habilitar endpoint personalizado.
3. Em Nome de host personalizado, insira o nome de host do endpoint personalizado preferido. O nome de host deve ser um nome de domínio totalmente qualificado (FQDN), como www.seudomínio.com ou exemplo.seudomínio.com.

   > **Note**
   >
   > Caso não tenha um certificado curinga, você deverá obter um novo certificado para seus subdomínios de endpoint personalizados.

4. Em Certificado AWS , escolha o certificado SSL que deseja usar para o domínio. Se nenhum certificado estiver disponível, você poderá importar um para o ACM ou usar o ACM para provisionar um. Para obter mais informações, consulte Emissão e gerenciamento de certificados no Manual do usuário do AWS Certificate Manager.

> **Note**
>
> O certificado deve ter o nome de endpoint personalizado e estar na mesma conta do domínio do OpenSearch Service. O status do certificado deve ser ISSUED (EMITIDO).

- Siga o restante das etapas para criar seu domínio e escolha Criar.
- Selecione o domínio quando terminar o processamento para visualizar seu endpoint personalizado.

Para usar a CLI ou API de configuração, use as operações `CreateDomain` e `UpdateDomainConfig`. Para mais informações, leia Referência de comandos da AWS CLI e Referências de API do Amazon OpenSearch Service.

Endpoints personalizados para domínios existentes

Para adicionar um endpoint personalizado a um domínio existente do OpenSearch Service, escolha Editar e execute as etapas de 2 a 4, acima.

Próximas etapas

Depois de habilitar um endpoint personalizado para seu domínio do OpenSearch Service, você deverá criar um mapeamento CNAME no Amazon Route 53 (ou seu provedor de serviços DNS preferido). Você faz isso para rotear o tráfego para o endpoint personalizado e seus subdomínios. Sem esse mapeamento, seu endpoint personalizado não funcionará. Para ver as etapas necessárias para criar esse mapeamento no Route 53, consulte Configuração do roteamento de DNS para um novo domínio e Criação de uma zona hospedada para um subdomínio. Para outros provedores, consulte a respectiva documentação.

Crie o registro CNAME apontando o endpoint personalizado para o endpoint de domínio gerado automaticamente. Se seu domínio for de pilha dupla, você poderá apontar seu registro CNAME para qualquer um dos dois endpoints gerados pelo serviço. A capacidade de pilha dupla do endpoint personalizado depende do endpoint gerado pelo serviço para o qual você direciona o registro CNAME. O nome de host do endpoint personalizado é o nome do registro CNAME, e o nome de host do endpoint do domínio é o valor do registro CNAME.

Se você usar a Autenticação SAML para OpenSearch Dashboards, será necessário atualizar seu IdP com o novo URL do SSO.

Auto-Tune para Amazon OpenSearch Service

O Auto-Tune no Amazon OpenSearch Service usa métricas de performance e uso do cluster do OpenSearch para sugerir alterações de configuração relacionadas à memória, incluindo tamanhos de fila e cache e configurações de máquina virtual Java (JVM) em seus nós. Essas alterações opcionais melhoram a velocidade e a estabilidade do cluster.

Algumas alterações são implantadas imediatamente, enquanto outras são agendadas durante o período fora do horário de pico do seu domínio. Você pode reverter para as configurações padrão do OpenSearch Service a qualquer momento. À medida que o Auto-Tune reúne e analisa métricas de performance para o seu domínio, você pode visualizar suas recomendações no console do OpenSearch Service na página Notificações.

O Auto-Tune está disponível em Regiões da AWS comerciais em domínios que executam qualquer versão do OpenSearch, ou Elasticsearch 6.7 ou posterior, com um tipo de instância compatível.

Tópicos

- Tipos de alterações
- Habilitação ou desabilitação do Auto-Tune
- Agendamento de melhorias no Auto-Tune
- Monitoramento de alterações no Auto-Tune

Tipos de alterações

O Auto-Tune tem duas categorias de alterações amplas:

- Alterações sem interrupções aplicadas à medida em que o cluster é executado.
- Alterações que exigem uma implantação azul/verde, que se aplicam durante a janela fora do horário de pico do domínio.

Com base nas métricas de performance do seu domínio, o Auto-Tune pode sugerir ajustes nas seguintes configurações:

Alterar tipo	Categoria	Descrição
Tamanho do heap do JVM	Azul/verde	Por padrão, o OpenSearch Service usa 50% da RAM de uma instância para o heap do JVM, com um tamanho de heap de 32 até GiB. Aumentar essa porcentagem garante mais memória para o OpenSearch, mas menos para o sistema operacional e outros processos. Valores maiores podem diminuir o número de pausas de coleta de resíduos, mas aumentar o comprimento dessas pausas.
Configurações de geração jovem do JVM	Azul/verde	As configurações de “geração jovem” do JVM afetam a frequência de coletas de resíduos secundárias. Coleções secundárias mais frequentes podem diminuir o número de coleções principais e pausas.
Tamanho da fila	Sem interrupções	Por padrão, o tamanho da fila de pesquisa é `1000` e o tamanho da fila de gravação é `10000`. O Auto-Tune dimensiona automaticamente as filas de pesquisa e gravação quando há heap adicional disponível para lidar com solicitações.
Tamanho do cache	Sem interrupções	O cache de campo monitora estruturas de dados no heap. Por isso, é importante monitorar o uso do cache. O Auto-Tune dimensiona o tamanho do cache de dados de campo para evitar problemas de falta de memória e interruptores de circuito. O cache de solicitação de fragmento é gerenciado em nível de nó e tem um tamanho máximo padrão de 1% do heap. O Auto-Tune dimensiona o tamanho do cache de solicitação de fragmentos para aceitar mais solicitações de pesquisa e índice do que o cluster configurado é capaz de manipular.
Dimensão da solicitação	Sem interrupções	Por padrão, quando a dimensão agregada das solicitações em trânsito ultrapassar 10% do total da JVM (2% para tipos de instância `t2` e 1% para `t3.small`), o OpenSearch fará o controle

Alterar tipo	Categoria	Descrição
		de utilização de todas as novas solicitações `_search` e `_bulk` até que as solicitações existentes sejam concluídas. O Auto-Tune ajusta esse limite de forma automática, que costuma ser entre 5 e 15%, de acordo com a quantidade da JVM ocupada atualmente no sistema. Por exemplo, se a pressão de memória da JVM estiver alta, o Auto-Tune poderá reduzir o limite para 5%. Se for o caso, talvez você veja mais rejeições até o cluster se estabiliz ar e o limite aumentar.

Habilitação ou desabilitação do Auto-Tune

O OpenSearch Service habilita o Auto-Tune por padrão em domínios novos. Para habilitar ou desabilitar o Auto-Tune em domínios existentes, recomendamos utilizar o console, o que simplifica o processo. Habilitar o Auto-Tune não causa uma implantação azul/verde.

No momento, não é possível habilitar ou desabilitar o Ajuste automático usando o AWS CloudFormation.

Console

Como habilitar o Auto-Tune em um domínio existente

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. No painel de navegação, em Domínios, escolha o nome do domínio para abrir a configuração do cluster.
3. Escolha Ativar se o Auto-Tune ainda não estiver ativado.
4. Opcionalmente, selecione Janela fora do horário de pico para agendar otimizações que exijam uma implantação azul/verde durante a janela fora do horário de pico configurada para o domínio. Para obter mais informações, consulte the section called “Agendamento de melhorias no Auto-Tune”.
5. Escolha Salvar alterações.

CLI

Para ativar o Auto-Tune usando o AWS CLI, envie uma solicitação UpdateDomainConfig:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --auto-tune-options DesiredState=ENABLED
```

Agendamento de melhorias no Auto-Tune

Antes de 16 de fevereiro de 2023, o Auto-Tune usava janelas de manutenção para programar mudanças que exigiam uma implantação azul/verde. As janelas de manutenção agora estão obsoletas em favor da janela fora do horário de pico, que é um período diário de 10 horas durante o qual seu domínio normalmente tem pouco tráfego. Você pode modificar a hora de início padrão para a janela fora do horário de pico, mas não pode alterar a duração dela.

Todos os domínios do Auto-Tune que tinham as janelas de manutenção ativadas antes da introdução das janelas fora do horário de pico em 16 de fevereiro de 2023 podem continuar usando as janelas de manutenção antigas, sem interrupção. No entanto, recomendamos a migração dos seus domínios existentes para usar a janela fora do horário de pico para a manutenção do domínio. Para obter instruções, consulte the section called “Migração das janelas de manutenção do Auto-Tune”.

Console

Como agendar ações do Auto-Tune na janela fora do horário de pico

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. No painel de navegação, em Domínios, escolha o nome do domínio para abrir a configuração do cluster.
3. Vá até a guia Auto-Tune e escolha Editar.
4. Escolha Ativar se o Auto-Tune ainda não estiver ativado.
5. Em Programar otimizações durante a janela fora do pico, selecione Janela fora do horário de pico.
6. Escolha Salvar alterações.

CLI

Para configurar seu domínio para agendar ações de ajuste automático durante a janela fora do horário de pico configurada, inclua `UseOffPeakWindow` na solicitação UpdateDomainConfig:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --auto-tune-options
 DesiredState=ENABLED,UseOffPeakWindow=true,MaintenanceSchedules=null
```

Monitoramento de alterações no Auto-Tune

Você pode monitorar as estatísticas do Auto-Tune em Amazon CloudWatch. Para obter uma lista completa de métricas, consulte the section called “Métricas do Auto-Tune”.

O OpenSearch Service envia eventos do Auto-Tune ao Amazon EventBridge. É possível usar o EventBridge para configurar regras que enviem um email ou realizem uma ação específica quando um evento for recebido. Para ver o formato de cada evento do Auto-Tune enviado ao EventBridge, consulte the section called “Auto-Tune de eventos”.

Marcação de domínios do Amazon OpenSearch Service

As tags permitem que você atribua informações arbitrárias a um domínio do Amazon OpenSearch Service para que você possa categorizar e filtrar essas informações. Uma tag é um par de valores-chave que você define e associa a um domínio de OpenSearch serviço. Você pode usar essas tags para rastrear custos agrupando despesas para recursos com tags semelhantes. AWS não aplica nenhum significado semântico às suas tags. Tags são interpretadas estritamente como sequências de caracteres. Todas as tags têm os elementos a seguir:

Elemento da tag	Descrição	Obrigatório
Chave de tag	A chave de tags é o nome da tag. A chave deve ser exclusiva para o domínio do OpenSearch serviço ao qual ela está vinculada. Para obter uma lista de restrições básicas a chaves e valores de tag, consulte Restrições a tags definidas pelo usuário.	Sim
Valor da tag	O valor da tag é o valor da string da tag. Os valores de tag podem ser `null` e não precisam ser exclusivos em um conjunto de tags. Por	Não

Elemento da tag	Descrição	Obrigatório
	exemplo, você pode ter um par de chave-valor em um conjunto de tags definido como projeto/Trinity e centro-custos/Trinity. Para obter uma lista de restrições básicas a chaves e valores de tag, consulte Restrições a tags definidas pelo usuário.	

Cada domínio OpenSearch de serviço tem um conjunto de tags, que contém todas as tags atribuídas a esse domínio OpenSearch de serviço. AWS não atribui automaticamente nenhuma tag aos domínios OpenSearch de serviço. Um conjunto de tags pode conter entre 0 e 50 tags. Se você adicionar uma tag a um domínio que tenha a mesma chave que uma tag existente, o novo valor sobrescreverá o antigo.

Exemplos de marcação com tags

Você pode usar uma chave para definir uma categoria, e o valor da tag pode ser um item nessa categoria. Por exemplo, você pode definir uma chave de tag de `project` e um valor de tag de`Salix`, indicando que o domínio do OpenSearch serviço está atribuído ao projeto Salix. Você também pode usar tags para designar domínios de OpenSearch serviço como sendo usados para teste ou produção usando uma chave como `environment=test` ou. `environment=production` Tente usar um conjunto consistente de chaves de tag para facilitar o rastreamento de metadados associados aos domínios OpenSearch de serviço.

Você também pode usar etiquetas para organizar sua AWS fatura de forma a refletir sua própria estrutura de custos. Para fazer isso, inscreva-se para receber sua Conta da AWS fatura com os valores-chave da etiqueta incluídos. Organize então suas informações de faturamento de acordo com recursos com os mesmos valores de chave de tag para ver o custo de recursos combinados. Por exemplo, você pode marcar vários domínios de OpenSearch serviço com pares de valores-chave e, em seguida, organizar suas informações de cobrança para ver o custo total de cada domínio em vários serviços. Para obter mais informações, consulte Como usar tags de alocação de custos na documentação do AWS Billing and Cost Management.

> **Note**
>
> As tags são armazenados em cache para finalidade de autorização. Por esse motivo, as adições e atualizações de tags nos domínios OpenSearch de serviço podem levar alguns minutos até serem disponibilizadas.

Uso de tags (console)

O console é a maneira mais simples marcar um domínio com tags.

Para criar uma tag (console)

1. Vá para https://aws.amazon.com e escolha Fazer login no console.
2. Em Analytics, escolha Amazon OpenSearch Service.
3. Selecione o domínio ao qual você deseja adicionar tags e vá para guia Tags (Etiquetas).
4. Escolha Manage (Gerenciar) e Add new tag (Adicionar nova tag).
5. Insira uma chave de tag e um valor opcional.
6. Escolha Salvar.

Para excluir uma tag, siga as mesmas etapas e escolha Remover na página Gerenciar tags.

Para obter mais informações sobre como usar o console para trabalhar com tags, consulte Editor de tags no Guia de conceitos básicos do Console de GerenciamentoAWS .

Uso de tags (AWS CLI)

Você pode criar tags de recursos usando o --add-tags comando AWS CLI with the.

Sintaxe

```
add-tags --arn=<domain_arn> --tag-list Key=<key>,Value=<value>
```

Parâmetro	Descrição
`--arn`	Nome do recurso da Amazon para o domínio do OpenSearch serviço ao qual a tag está anexada.

Parâmetro	Descrição
`--tag-list`	Conjunto de pares de chave/valor separados por espaço no seguinte formato: `Key=<key>,Value=<value>`

Exemplo

O exemplo a seguir cria duas tags para o domínio logs:

```
aws opensearch add-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs --tag-list
 Key=service,Value=OpenSearch Key=instances,Value=m3.2xlarge
```

Você pode remover tags de um domínio OpenSearch de serviço usando o --remove-tags comando.

Sintaxe

```
remove-tags --arn=<domain_arn> --tag-keys Key=<key>,Value=<value>
```

Parâmetro	Descrição
`--arn`	Nome de recurso da Amazon (ARN) para o domínio do OpenSearch serviço ao qual a tag está anexada.
`--tag-keys`	Conjunto de pares de valores-chave separados por espaço que você deseja remover do domínio do Serviço. OpenSearch

Exemplo

O exemplo a seguir remove duas tags do domínio logs que foram criadas no exemplo anterior:

```
aws opensearch remove-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs --tag-
keys service instances
```

Você pode visualizar as tags existentes para um domínio OpenSearch de serviço com o --list-tags comando:

Sintaxe

```
list-tags --arn=<domain_arn>
```

Parâmetro	Descrição
`--arn`	Nome de recurso da Amazon (ARN) para o domínio do OpenSearch serviço ao qual as tags estão anexadas.

Exemplo

O exemplo a seguir lista todas as tags de recurso para o domínio logs:

```
aws opensearch list-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs
```

Trabalhando com tags (AWS SDKs)

Os AWS SDKs (exceto os SDKs para Android e iOS) oferecem suporte a todas as ações definidas na Amazon OpenSearch Service API Reference, incluindo as `AddTags` operações`ListTags`, e. `RemoveTags` Para obter mais informações sobre como instalar e usar os AWS SDKs, consulte KitsAWS de desenvolvimento de software.

Python

Este exemplo usa o cliente Python de OpenSearchServicebaixo nível do AWS SDK para Python (Boto) para adicionar uma tag a um domínio, listar a tag anexada ao domínio e remover uma tag do domínio. É necessário fornecer valores para `DOMAIN_ARN`, `TAG_KEY` e `TAG_VALUE`.

```
import boto3
from botocore.config import Config  # import configuration

DOMAIN_ARN = ''  # ARN for the domain. i.e "arn:aws:es:us-east-1:123456789012:domain/
my-domain
TAG_KEY = ''  # The name of the tag key. i.e 'Smileyface'
TAG_VALUE = ''  # The value assigned to the tag. i.e 'Practicetag'

# defines the configurations parameters such as region

my_config = Config(region_name='us-east-1')
client = boto3.client('opensearch', config=my_config)
```

```
# defines the client variable

def addTags():
    """Adds tags to the domain"""

    response = client.add_tags(ARN=DOMAIN_ARN,
                               TagList=[{'Key': TAG_KEY,
                                         'Value': TAG_VALUE}])

    print(response)


def listTags():
    """List tags that have been added to the domain"""

    response = client.list_tags(ARN=DOMAIN_ARN)
    print(response)


def removeTags():
    """Remove tags that have been added to the domain"""

    response = client.remove_tags(ARN=DOMAIN_ARN, TagKeys=[TAG_KEY])

    print('Tag removed')
    return response
```

Execução de ações administrativas em domínios OpenSearch do Amazon Service

O Amazon OpenSearch Service oferece várias opções administrativas que fornecem controle granular se você precisar solucionar problemas com seu domínio. Essas opções incluem a capacidade de reiniciar o OpenSearch processo em um nó de dados e a capacidade de reiniciar um nó de dados.

OpenSearch O serviço monitora os parâmetros de integridade do nó e, quando há anomalias, toma ações corretivas para manter os domínios estáveis. Com as opções administrativas para reiniciar o OpenSearch processo em um nó e reiniciar o próprio nó, você tem controle sobre algumas dessas ações de mitigação.

Você pode usar o AWS Management Console, a AWS CLI ou o SDK da AWS para realizar essas ações. As seções a seguir abordam como realizar essas ações com o console.

Reinicie o OpenSearch processo em um nó

Para reiniciar o OpenSearch processo em um nó

1. Navegue até o console OpenSearch de serviço emhttps://console.aws.amazon.com/aos/.
2. No painel de navegação à esquerda, escolha Domínios. Escolha o nome do domínio que você deseja atualizar.
3. Depois que a página de detalhes do domínio for aberta, navegue até a guia Integridade da instância.
4. Em Nós de dados, selecione o botão ao lado do nó no qual você deseja reiniciar o processo.
5. Selecione o menu suspenso Ações e escolha Reiniciar o processo OpenSearch /Elasticsearch.
6. Escolha Confirmar no modal.
7. Para ver o status da ação que você iniciou, selecione o nome do nó. Depois que a página de detalhes do nó for aberta, escolha a guia Eventos abaixo do nome do nó para ver uma lista de eventos associados a esse nó.

Reinicializar um nó de dados

Como reinicializar um nó de dados

1. Navegue até o console OpenSearch de serviço emhttps://console.aws.amazon.com/aos/.
2. No painel de navegação à esquerda, escolha Domínios. Escolha o nome do domínio que você deseja atualizar.
3. Depois que a página de detalhes do domínio for aberta, navegue até a guia Integridade da instância.
4. Em Nós de dados, selecione o botão ao lado do nó no qual você deseja reiniciar o processo.
5. Selecione o menu suspenso Ações e escolha Nó de reinicialização.
6. Escolha Confirmar no modal.
7. Para ver o status da ação que você iniciou, selecione o nome do nó. Depois que a página de detalhes do nó for aberta, escolha a guia Eventos abaixo do nome do nó para ver uma lista de eventos associados a esse nó.

Reinicie o processo do Dashboard ou Kibana em um nó

Como reiniciar o processo Dashboard ou Kibana em um nó

1. Navegue até o console OpenSearch de serviço emhttps://console.aws.amazon.com/aos/.
2. No painel de navegação à esquerda, escolha Domínios. Escolha o nome do domínio que você deseja atualizar.
3. Depois que a página de detalhes do domínio for aberta, navegue até a guia Integridade da instância.
4. Em Nós de dados, selecione o botão ao lado do nó no qual você deseja reiniciar o processo.
5. Selecione o menu suspenso Ações e escolha Reiniciar o processo do Dashboard/Kibana.
6. Escolha Confirmar no modal.
7. Para ver o status da ação que você iniciou, selecione o nome do nó. Depois que a página de detalhes do nó for aberta, escolha a guia Eventos abaixo do nome do nó para ver uma lista de eventos associados a esse nó.

Limitações

As opções administrativas têm as seguintes limitações:

- As opções administrativas são suportadas nas versões 7.x e superiores do Elasticsearch.
- As opções administrativas não oferecem suporte a domínios com Multi-AZ com modo de espera ativado.
- A reinicialização do processo OpenSearch e do Elasticsearch é suportada em domínios com três ou mais nós de dados.
- O suporte ao processo do Dashboards e Kibana é suportado em domínios com dois ou mais nós de dados.
- Para reiniciar o OpenSearch processo em um nó ou reinicializar um nó, o domínio não deve estar no estado vermelho e todos os índices devem ter réplicas configuradas.

Trabalhando com consultas diretas do Amazon OpenSearch Service com o Amazon S3 (versão prévia)

⚠ Esta é a documentação de pré-lançamento para consultas diretas do Amazon OpenSearch Service com o Amazon S3, que está em versão prévia. A documentação e o atributo estão sujeitos a alterações. Recomendamos o uso desse atributo somente em ambientes de teste, e não em ambientes de produção. Para conferir os termos e condições da pré-visualização, consulte Betas e pré-visualizações nos Termos de serviços daAWS.

Você pode usar as consultas diretas do Amazon OpenSearch Service para consultar dados no Amazon S3. O Amazon OpenSearch Service fornece uma integração direta de consultas com o Amazon S3 como uma forma de analisar registros operacionais no Amazon S3 e lagos de dados baseados no Amazon S3 sem precisar alternar entre os serviços. Agora você pode analisar dados em armazenamentos de objetos na nuvem e, simultaneamente, usar a análise operacional e as visualizações do Serviço. OpenSearch

Com consultas diretas com o Amazon S3, você não precisa mais criar pipelines de ETL complexos nem incorrer nas despesas de duplicação de dados no Service OpenSearch e no armazenamento do Amazon S3. Também é possível instalar integrações de modelos populares de tipo de log que incluem painéis predefinidos e configurar acelerações de dados personalizadas para esse tipo de log. Os modelos incluem Logs de fluxo de VPC, Logs doAWS CloudTrail e logs do Amazon S3. As acelerações incluem pular índices, visões materializadas e índices cobertos.

Tópicos

Definição de preço

Você paga pelos recursos existentes do OpenSearch Serviço e do Amazon S3 que são usados para criar e processar consultas diretas. As consultas enviadas ao Amazon S3 usam computação faturável e aparecem OpenSearch como unidades computacionais (OCUs) por hora.

Consultas diretas com o Amazon S3 são de dois tipos: manutenção interativa e de índice. Consultas interativas fazem análises nos seus dados no Amazon S3. Quando você executa uma nova consulta, o OpenSearch Service inicia uma nova sessão que dura no mínimo dez minutos. OpenSearch O serviço mantém a sessão ativa para garantir que as consultas subsequentes sejam executadas rapidamente. As consultas de manutenção de índices usam computação para manter índices no Serviço. OpenSearch Essas consultas geralmente demoram mais porque ingerem uma quantidade configurável de dados no OpenSearch Service para acelerar a execução das consultas interativas.

Para obter mais informações, consulte Amazon OpenSearch Service Pricing.

Limitações

As seguintes limitações se aplicam às consultas diretas do OpenSearch Service com o Amazon S3.

- Seu OpenSearch domínio deve ser da versão 2.11 ou posterior para oferecer suporte às consultas diretas do OpenSearch Service.
- OpenSearch As consultas diretas de serviço com o Amazon S3 só oferecem suporte a tabelas Spark dentro do. AWS Glue Data CatalogTabelas do Hive não oferecem suporte a streaming do Spark, que é necessário para manter os índices atualizados.
- Alguns tipos de dados não compatíveis. Os tipos de dados compatíveis estão limitados a Parquet, CSV e JSON.
- AWS CloudFormation os modelos não são compatíveis com a versão prévia das consultas diretas.
- Seu OpenSearch domínio e AWS Glue Data Catalog deve estar no mesmo Conta da AWS. As tabelas do Amazon S3 podem estar em uma conta diferente, mas devem estar na mesma Região da AWS do domínio.
- Não há suporte para estruturas do Spark aninhadas. Se os seus dados de origem usarem estruturas aninhadas, será necessário explodi-las em linhas.
- Não há suporte para tabelas criadas no Athena.
- Colunas ausentes podem exigir o uso da função SQL `COALESCE` para retornarem resultados.
- Não disponível no OpenSearch Serverless

- Os dados devem ser nivelados antes da consulta ou você deve usar o SQL in OpenSearch Service para transformar suas colunas aninhadas em colunas dedicadas.

Cotas

Sua conta tem as seguintes cotas relacionadas às consultas diretas OpenSearch de serviço com o Amazon S3. Sempre que você inicia uma consulta, o OpenSearch Service abre uma sessão e a mantém ativa por pelo menos dez minutos. Isso reduz a latência da consulta, removendo o tempo de inicialização da sessão nas consultas subsequentes.

Descrição	Máximo
Conexões por domínio	20
Fontes de dados por domínio	20
Índices por domínio	50
Sessões simultâneas por fonte de dados	100

Regiões compatíveis

As seguintes regiões estão disponíveis para consultas diretas de OpenSearch serviço com o Amazon S3: Ásia-Pacífico (Tóquio), Europa (Frankfurt), Europa (Irlanda), Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio) e Oeste dos EUA (Oregon).

Criação de integrações de fontes de dados do Amazon OpenSearch Service com o Amazon S3

⚠ Esta é a documentação de pré-lançamento para consultas diretas do Amazon OpenSearch Service com o Amazon S3, que está em versão prévia. A documentação e o atributo estão sujeitos a alterações. Recomendamos o uso desse atributo somente em ambientes de teste, e não em ambientes de produção. Para conferir os termos e condições da pré-visualização, consulte Betas e pré-visualizações nos Termos de serviços daAWS.

Você pode criar uma nova fonte de dados de consulta direta do Amazon S3 para o OpenSearch Serviço por meio da ou da AWS Management Console API. Cada nova fonte de dados usa o AWS Glue Data Catalog para gerenciar tabelas que representam os buckets do Amazon S3.

Tópicos

Pré-requisitos

Antes de criar uma fonte de dados, é preciso ter o seguinte:

- Um OpenSearch domínio com a versão 2.11 ou posterior

Para obter instruções sobre como configurá-los, consulte the section called “ Criação OpenSearch de domínios de serviço” e Conceitos básicos do AWS Glue Data Catalog.

Permissões obrigatórias

Para criar uma fonte de dados, seu usuário ou perfil deve ter uma política baseada em identidade anexada com as permissões apropriadas do IAM. O exemplo de política a seguir demonstra as permissões de privilégio mínimo necessárias para criar e gerenciar uma fonte de dados. Observe que, se você tiver permissões mais amplas, como `s3:*` ou a política `AdministratorAccess`, essas permissões abrangem as permissões de privilégio mínimo na política de amostra.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "es:ESHttp*",
                "es:AddDataSource",
                "es:DeleteDataSource",
                "es:GetDataSource",
                "es:ListDataSource",
```

```
                "es:UpdateDataSource",
                "s3:Get*",
                "s3:List*",
                "s3:Put*",
                "s3:Describe*",
                "glue:*"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*",
                "arn:aws:glue:us-east-1:{aws-account-id}:database/*"
            ]
        },
        {
            "Sid": "GlueCreateAndReadDataCatalog",
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:CreateDatabase",
                "glue:GetDatabases",
                "glue:CreateTable",
                "glue:GetTable",
                "glue:UpdateTable",
                "glue:DeleteTable",
                "glue:GetTables",
                "glue:GetPartition",
                "glue:GetPartitions",
                "glue:CreatePartition",
                "glue:BatchCreatePartition",
                "glue:GetUserDefinedFunctions"
            ],
            "Resource": "*"
        }
    ]
}
```

O perfil também deve ter a seguinte política de confiança, que especifica o ID de destino.

```
{
    "Version":"2012-10-17",
    "Statement":[
       {
```

```
          "Effect":"Allow",
          "Principal":{
             "Service": "directquery.opensearchservice.amazonaws.com"
          },
          "Action":"sts:AssumeRole"
       }
     ]
}
```

Para obter instruções sobre como criar o perfil, consulte Criar um perfil usando políticas de confiança personalizadas.

Se você tiver um controle de acesso refinado ativado, uma nova função de controle de acesso OpenSearch refinado será criada automaticamente para sua fonte de dados. <name of data source>O nome da nova função de controle de acesso refinada será _. AWSOpenSearchDirectQuery

Por padrão, a função tem acesso somente aos índices da fonte de dados de consulta direta. Embora você possa configurar a função para limitar ou conceder acesso à sua fonte de dados, é recomendável não ajustar o acesso dessa função. Se você excluir a fonte de dados, essa função será excluída. Isso removerá o acesso de outros usuários se eles estiverem mapeados para a função.

Mapeie a AWS Glue Data Catalog função (se o controle de acesso refinado for ativado após a criação da fonte de dados)

Se você ativou o controle de acesso refinado após criar uma fonte de dados, deverá mapear usuários não administradores para uma função do IAM com AWS Glue Data Catalog acesso para executar consultas diretas. Para criar manualmente um perfil `glue_access` de back-end que possa ser mapeado para o perfil do IAM, faça o seguinte:

> **Note**
>
> Índices são usados para qualquer consulta na fonte de dados. Um usuário com acesso para leitura ao índice de solicitações de uma determinada fonte de dados pode ler todas as consultas nessa fonte. Um usuário com acesso para leitura ao índice de resultados pode ler os resultados de todas as consultas nessa fonte de dados.

1. No menu principal em OpenSearch Painéis, escolha Segurança, Funções e Criar funções.

2. Chame o perfil de glue_access.
3. Para Permissões de cluster, selecione `indices:data/write/bulk*`, `indices:data/read/scroll`, `indices:data/read/scroll/clear`.
4. Em Índice, insira os seguintes índices aos quais você deseja conceder acesso ao usuário com o perfil:
   - `.query_execution_request_<name of data source>`
   - `query_execution_result_<name of data source>`
   - `flint_*`
5. Para Permissões de índice, selecione `indices_all`.
6. Escolha Criar.
7. Escolha Usuários mapeados e Gerenciar mapeamento.
8. Em Perfis de back-end, adicione o ARN do perfil do AWS Glue que precisa de permissão para chamar seu domínio.

   ```
   arn:aws:iam::account-id:role/role-name
   ```
9. Selecione Mapa e confirme se o perfil aparece em Usuários mapeados.

Para obter mais informações sobre o mapeamento de perfis, consulte the section called “Mapear funções em usuários”.

Configurar uma nova fonte de dados de consultas diretas

Você pode configurar uma fonte de dados de consulta direta em um domínio com a API AWS Management Console ou a OpenSearch Service API.

AWS Management Console

1. Navegue até o console do Amazon OpenSearch Service emhttps://console.aws.amazon.com/aos/.
2. No painel de navegação à esquerda, escolha Domínios.
3. Selecione o domínio para o qual configurar uma nova fonte de dados. Isso abre a página de detalhes do domínio. Escolha a guia Conexões abaixo dos detalhes gerais do domínio e localize a seção Consulta direta.
4. Escolha Criar.

5. Na página de criação da fonte de dados, insira um nome para a nova fonte de dados. Em Tipo de fonte de dados, escolha Amazon S3. Escolha uma função do IAM existente que tenha limitações para o que pode ser acessado no Amazon S3 AWS Glue Data Catalog e no Amazon S3.
6. Escolha Criar. Isso abre a tela de detalhes da fonte de dados com uma URL dos OpenSearch painéis. Navegue até esse URL para concluir as próximas etapas.

OpenSearch API de serviço

Use a operação AddDataSourceda API para criar uma nova fonte de dados em seu domínio.

```
POST https://es.region.amazonaws.com/2021-01-01/opensearch/domain/domain-name/
dataSource

{
   "DataSourceType": {
        "s3GlueDataCatalog": {
            "RoleArn": "arn:aws:iam::account-id:role/Admin"
        }
    }
   "Description": "data-source-description",
   "Name": "my-data-source"
}
```

Próximas etapas

Depois de criar uma fonte de dados, o OpenSearch Service fornece uma URL de OpenSearch painéis. Use-o para configurar o controle de acesso, definir tabelas, configurar painéis baseados em tipos de log para tipos de log populares e consultar seus dados.

Configurando sua fonte de dados em painéis OpenSearch

⚠ Esta é a documentação de pré-lançamento para consultas diretas do Amazon OpenSearch Service com o Amazon S3, que está em versão prévia. A documentação e o atributo estão sujeitos a alterações. Recomendamos o uso desse atributo somente em ambientes de teste, e não em ambientes de produção. Para conferir os termos e condições da pré-visualização, consulte Betas e pré-visualizações nos Termos de serviços daAWS.

Depois de criou a fonte de dados, é possível definir configurações de segurança, suas tabelas do Amazon S3 ou a indexação acelerada de dados. Esta seção mostra vários casos de uso com sua fonte de dados em OpenSearch painéis antes de você consultar seus dados.

Para configurar as seções a seguir, primeiro você deve navegar até sua fonte de dados em OpenSearch Painéis. Na navegação à esquerda, em Gerenciamento, selecione Fontes de dados. Em Gerenciar fontes de dados, selecione o nome da fonte de dados criada no console.

Configurar o controle de acesso

Na página de detalhes da fonte de dados, encontre a seção Controles de acesso e escolha Editar. Se o plug-in de segurança estiver instalado, escolha Restrito e selecione para quais grupos baseados em perfil você deseja fornecer acesso à nova fonte de dados. Também é possível escolher Somente administrador para que somente o administrador tenha acesso à fonte de dados.

> **Important**
>
> Observe que, como índices são usados para qualquer consulta na fonte de dados, um usuário com acesso para leitura ao índice de solicitações de uma determinada fonte de dados pode ler todas as consultas nessa fonte de dados, enquanto um usuário com acesso para leitura ao índice de resultados pode ler os resultados de todas as consultas nessa fonte de dados.

Definir AWS Glue Data Catalog tabelas

As consultas diretas do OpenSearch Service para o Amazon S3 usam tabelas Spark dentro do. AWS Glue Data CatalogVocê pode usar um Crawler do AWS Glue para rastrear seus dados, o que criará uma tabela para você. Como alternativa, é possível criar tabelas manualmente no Query Workbench.

Para gerenciar bancos de dados e tabelas existentes na sua fonte de dados, ou para criar novas tabelas nas quais usar consultas diretas, escolha a opção Definir tabelas na página de detalhes da fonte de dados. Você acessará a página do plug-in Query Workbench.

Para configurar uma tabela com dados de amostra que é possível explorar e usar para acelerações na seção a seguir, execute a seguinte consulta:

```
CREATE EXTERNAL TABLE IF NOT EXISTS datasourcename.gluedatabasename.gluetablename (
   `@timestamp` TIMESTAMP,
```

```
    clientip STRING,
    request STRING,
    status INT,
    size INT,
    year INT,
    month INT,
    day INT)
USING json PARTITIONED BY(year, month, day) OPTIONS (path 's3://my-bucket/data/
http_log', compression 'bzip2')
```

Depois de criar a tabela, execute a consulta a seguir para garantir que ela seja compatível com consultas diretas:

```
MSCK REPAIR TABLE datasourcename.databasename.tablename
```

Acelerar suas consultas

Na página de detalhes da fonte de dados, escolha a opção Acelerar performance. Para garantir uma experiência rápida com seus dados no Amazon S3, há três tipos diferentes de acelerações que você pode configurar para indexar dados no OpenSearch serviço: ignorando índices, visualizações materializadas e cobrindo índices.

Índices de salto

Com um índice de salto, é possível indexar somente os metadados dos dados armazenados no Amazon S3. Quando uma tabela com um índice de salto é consultada, o planejador de consultas faz referência ao índice e reescreve a consulta para localizar os dados com eficiência, em vez de verificar todas as partições e arquivos. Isso permite que o índice de salto restrinja rapidamente a localização específica dos dados armazenados.

Quando você configura as tabelas do Spark que você usará no AWS Glue Data Catalog, o OpenSearch Dashboards pergunta se você deseja criar índices ignorantes em suas tabelas. É possível criar um índice de salto lá ou criar um com o caso de uso em Acelerar performance depois de concluir a configuração da tabela.

```
CREATE SKIPPING INDEX
ON datasourcename.gluedatabasename.gluetablename
(
    year PARTITION,
    month PARTITION,
```

```
    day PARTITION,
    hour PARTITION
)
```

Visualizações materializadas

Com visões materializadas, é possível usar consultas complexas, como agregações, para potencializar as visualizações do Dashboard. As visualizações materializadas ingerem uma pequena quantidade de seus dados no armazenamento do OpenSearch Serviço. OpenSearch Em seguida, o serviço forma um índice a partir dos dados ingeridos que você pode usar para visualizações. Você pode gerenciar o índice de visualização materializada comthe section called “Gerenciamento de estados de índice”, assim como com qualquer outro OpenSearch índice.

Use a consulta a seguir para criar uma nova visão materializada para a tabela `http_logs` criada em the section called “Definir AWS Glue Data Catalog tabelas”:

```
CREATE MATERIALIZED VIEW datasourcename.gluedatabasename.viewname_view
AS
  SELECT
    window.start AS `start.time`,
    COUNT(*) AS count
  FROM datasourcename.gluedatabasename.gluetablename
  WHERE status != 200
  GROUP BY TUMBLE(`@timestamp`, '1 Minutes')
WITH (
  auto_refresh = true,
  refresh_interval = '1 Minutes',
  checkpoint_location = 's3://my-bucket/data/http_log/checkpoint_http_count_view',
  watermark_delay = '10 Minutes'
);
```

Índices de abrangência

Com um índice de abrangência, é possível ingerir dados de uma coluna especificada em uma tabela. Este é o mais eficiente dos três tipos de indexação. Como o OpenSearch Service ingere todos os dados da coluna desejada, você obtém melhor desempenho e pode realizar análises avançadas.

Assim como nas visualizações materializadas, o OpenSearch Service cria um novo índice a partir dos dados do índice de cobertura. Você pode usar esse novo índice para visualizações do Dashboard e outras funcionalidades do OpenSearch Serviço, como detecção de anomalias ou

recursos geoespaciais. Você pode gerenciar o índice de visualização de cobertura comthe section called “Gerenciamento de estados de índice”, assim como com qualquer outro OpenSearch índice.

Use a consulta a seguir para criar um novo índice de abrangência para a tabela `http_logs` criada em the section called “Definir AWS Glue Data Catalog tabelas”:

```
CREATE INDEX status_clientip_and_day
ON datasourcename.gluedatabasename.gluetablename ( status, day, clientip )
WITH (
  auto_refresh = true,
  refresh_interval = '5 minute',
  checkpoint_location = 's3://my-bucket/data/http_log/checkpoint_status_and_day'
)
```

Consultando dados em painéis OpenSearch

> ⚠ Esta é a documentação de pré-lançamento para consultas diretas do Amazon OpenSearch Service com o Amazon S3, que está em versão prévia. A documentação e o atributo estão sujeitos a alterações. Recomendamos o uso desse atributo somente em ambientes de teste, e não em ambientes de produção. Para conferir os termos e condições da pré-visualização, consulte Betas e pré-visualizações nos Termos de serviços daAWS.

Depois de configurar tabelas e a aceleração de consulta opcional desejada, agora é possível começar a fazer análises nos dados. Para consultar seus dados, selecione a fonte de dados no menu suspenso na página Descobrir ou na página Observabilidade em Painéis. OpenSearch

Se estiver usando um índice de salto ou não tiver criado um índice, você poderá usar o SQL ou o PPL (Piped Processing Language) para consultar seus dados. Se configurou uma visão materializada ou um índice de abrangência, você já tem um índice e pode usar a Dashboards Query Language (DQL) no Dashboards. Você também pode usar o PPL com o plug-in Observability e o SQL com o plug-in Query Workbench. Atualmente, somente os plug-ins Observability e Query Workbench oferecem suporte para PPL e SQL.

SQL

Use a consulta a seguir para executar uma amostra de consulta SQL para a tabela `http_logs` criada em the section called “Definir AWS Glue Data Catalog tabelas”:

```
SELECT
    FIRST(day) AS day,
    status,
    COUNT(status) AS status_count_by_day
FROM datasourcename.gluedatabasename.gluetablename
WHERE status >= 400
GROUP BY day, status
ORDER BY day, status
LIMIT 20;
```

PPL

Use a consulta a seguir para executar uma amostra de consulta PPL para a tabela `http_logs` criada em the section called “Definir AWS Glue Data Catalog tabelas”:

```
source = datasourcename.gluedatabasename.gluetablename |
where status = 500 | sort - clientip, @timestamp | head 20
```

Excluindo uma fonte de dados do Amazon OpenSearch Service com o Amazon S3

> ⚠ Esta é a documentação de pré-lançamento para consultas diretas do Amazon OpenSearch Service com o Amazon S3, que está em versão prévia. A documentação e o atributo estão sujeitos a alterações. Recomendamos o uso desse atributo somente em ambientes de teste, e não em ambientes de produção. Para conferir os termos e condições da pré-visualização, consulte Betas e pré-visualizações nos Termos de serviços daAWS.

Quando você exclui uma fonte de dados, o Amazon OpenSearch Service a remove do seu domínio. OpenSearch O serviço também remove índices associados à fonte de dados. Seus dados transacionais não são excluídos do Amazon S3, mas o Amazon S3 não envia novos dados para o Serviço. OpenSearch

Você pode excluir uma integração de fonte de dados usando a API AWS Management Console ou a OpenSearch Service API.

AWS Management Console

Como excluir uma fonte de dados

1. Navegue até o console do Amazon OpenSearch Service emhttps://console.aws.amazon.com/aos/.
2. No painel de navegação à esquerda, escolha Domínios.
3. Selecione o domínio cuja fonte de dados você deseja excluir. Isso abre a página de detalhes do domínio. Escolha a guia Conexões abaixo das informações gerais e localize a seção Consulta direta.
4. Selecione a fonte de dados que você deseja excluir, escolha Excluir e confirme a exclusão.

OpenSearch API de serviço

Use a operação DeleteDataSourceda API para excluir uma fonte de dados existente em seu domínio.

```
POST https://es.region.amazonaws.com/2021-01-01/opensearch/domain/domain-name/
dataSource/data-source-name
```

Monitoramento de domínios do Amazon OpenSearch Service

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e a performance do Amazon OpenSearch Service e das outras soluções da AWS. A AWS fornece as seguintes ferramentas para monitorar o OpenSearch Service, relatar problemas e realizar ações automaticamente quando apropriado:

Amazon CloudWatch

O Amazon CloudWatch monitora os recursos do OpenSearch Service em tempo real. É possível coletar e rastrear métricas, criar painéis personalizados e definir alarmes que notificam você ou realizam ações quando uma métrica atinge um determinado limite. Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch.

Amazon CloudWatch Logs

O Amazon CloudWatch Logs permite a você monitorar, armazenar e acessar seus arquivos de log do OpenSearch. O CloudWatch Logs monitora as informações nos arquivos de log e pode notificar você quando determinados limites forem atingidos. Para obter mais informações, consulte o Manual do usuário do Amazon CloudWatch Logs.

Amazon EventBridge

O Amazon EventBridge fornece um fluxo quase em tempo real dos eventos do sistema que descrevem alterações em seus domínios do OpenSearch Service. Você pode criar regras que observam certos eventos e acionam ações automatizadas em outros serviços da AWS quando esses eventos ocorrem. Para obter mais informações, consulte o Guia do usuário do Amazon EventBridge.

AWS CloudTrail

O AWS CloudTrail captura chamadas de API de configuração feitas para o OpenSearch Service como eventos. Ele pode enviar esses eventos para um bucket do Amazon S3 especificado por você. Usando essas informações, você pode identificar quais usuários e contas fizeram solicitações, o endereço IP de origem de onde as solicitações foram feitas e quando elas ocorreram. Para obter mais informações, consulte o Manual do usuário do AWS CloudTrail.

Tópicos

- Monitorar métricas de cluster do OpenSearch com o Amazon CloudWatch
- Monitoramento de logs do OpenSearch com o Amazon CloudWatch Logs
- Monitorando registros de auditoria no Amazon OpenSearch Service
- Eventos do OpenSearch Serviço de Monitoramento com a Amazon EventBridge
- Monitoramento de chamadas de API do Amazon OpenSearch Service com o AWS CloudTrail

Monitorar métricas de cluster do OpenSearch com o Amazon CloudWatch

O Amazon OpenSearch Service publica dados de seus domínios no Amazon CloudWatch. O CloudWatch permite recuperar estatísticas sobre esses pontos de dados como um conjunto ordenado de dados de séries temporais, conhecidos como métricas. O OpenSearch Service envia a maioria das métricas ao CloudWatch em intervalos de 60 segundos. Se você usar volumes magnéticos do EBS ou de uso geral, as métricas do volume do EBS serão atualizadas somente a cada cinco minutos. Para obter mais informações sobre o Amazon CloudWatch, consulte o Manual do usuário do Amazon CloudWatch.

O console do OpenSearch Service exibe uma série de gráficos com base nos dados brutos do CloudWatch. Dependendo das suas necessidades, talvez você prefira visualizar dados do cluster no CloudWatch em vez de gráficos no console. O serviço mantém as métricas arquivadas por duas semanas e depois as descarta. As métricas são fornecidas sem custo adicional, mas o CloudWatch ainda cobra pela criação de painéis e alarmes. Para obter mais informações, consulte Preço do Amazon CloudWatch.

O OpenSearch Service publica as seguintes métricas no CloudWatch:

- the section called “Métricas de cluster”
- the section called “Métricas de nó principal dedicado”
- the section called “Métricas de volume do EBS”
- the section called “Métricas de instância”
- the section called “Métricas do UltraWarm”
- the section called “Métricas de armazenamento de baixa atividade”
- the section called “Métricas de alerta”
- the section called “Métricas de detecção de anomalias”

- the section called “Métricas de pesquisa assíncrona”
- the section called “Métricas de SQL”
- the section called “Métricas de k-NN”
- the section called “Métricas de pesquisa entre clusters”
- the section called “Métricas de replicação entre clusters”
- the section called “Métricas de Learning to Rank”
- the section called “Métricas da Piped Processing Language”

Visualização de métricas com o CloudWatch

As métricas do CloudWatch são agrupadas primeiro pelo namespace do serviço e, em seguida, por várias combinações de dimensão dentro de cada namespace.

Para visualizar indicadores usando o console do CloudWatch

1. Abra o console do CloudWatch em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação à esquerda, localize Métricas e escolha Todas as métricas. Selecione o namespace ES/OpenSearchService.
3. Escolha uma dimensão para visualizar as métricas correspondentes. As métricas para nós individuais estão na dimensão `ClientId, DomainName, NodeId`. As métricas de cluster estão na dimensão `Per-Domain, Per-Client Metrics`. Algumas métricas de nó são agregadas no nível do cluster e, portanto, incluídas em ambas as dimensões. As métricas de fragmentos estão na dimensão `ClientId, DomainName, NodeId, ShardRole`.

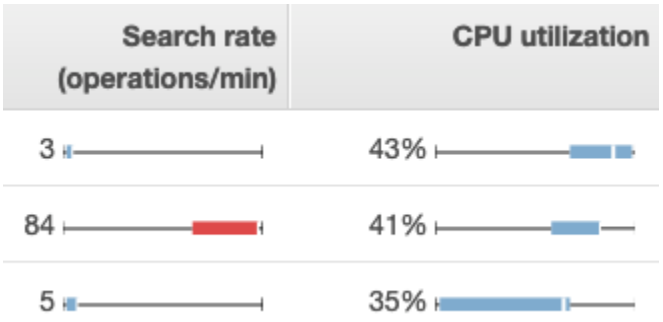
Visualizar uma lista de métricas usando o AWS CLI

Execute o seguinte comando:

```
aws cloudwatch list-metrics --namespace "AWS/ES"
```

Interpretação de gráficos de integridade no OpenSearch Service

Para exibir métricas no OpenSearch Service, use as guias Integridade do cluster e Integridade da instância. A guia Integridade da instância usa gráficos de caixa para fornecer uma visão imediata da integridade de cada nó do OpenSearch.



- Cada caixa colorida mostra a faixa de valores do nó ao longo do período de tempo especificado.
- As caixas azuis representam valores que são consistentes com outros nós. As caixas vermelhas representam exceções.
- A linha branca dentro de cada caixa de seleção mostra o valor atual do nó.
- As "caixas estreitas" em cada lado de cada caixa mostram os valores mínimo e máximo de todos os nós ao longo do período de tempo.

Se você fizer alterações de configuração para seu domínio, a lista de instâncias individuais nas guias Integridade do cluster e Integridade da instância geralmente duplicarão de tamanho por um breve período antes de retornar para o número correto. Para obter uma explicação sobre esse comportamento, consulte the section called “Alterações de configuração”.

Métricas de cluster

O Amazon OpenSearch Service fornece as métricas a seguir para clusters.

Métrica	Descrição
`ClusterStatus.green`	Um valor 1 indica que todos os fragmentos de índice estão alocados a nós no cluster. Estatística relevante: máximo
`ClusterStatus.yellow`	Um valor 1 indica que os fragmentos principais de todos os índices estão alocados a nós no cluster, mas os fragmentos de réplica de pelo menos um índice não estão. Para obter mais informações, consulte the section called “Status de cluster amarelo”. Estatística relevante: máximo

Métrica	Descrição
`ClusterStatus.red`	Um valor 1 indica que os fragmentos principais e de réplica de pelo menos um índice não estão alocados a nós no cluster. Para obter mais informações, consulte the section called “Status de cluster vermelho”. Estatística relevante: máximo
`Shards.active`	O número total de fragmentos ativos primários e de réplica. Estatística relevante: máximo, soma
`Shards.unassigned`	O número de fragmentos que não estão alocados a nós no cluster. Estatística relevante: máximo, soma
`Shards.delayedUnassigned`	O número de fragmentos cuja alocação de nó foi atrasada pelas configurações de tempo limite. Estatística relevante: máximo, soma
`Shards.activePrimary`	O número de fragmentos primários ativos. Estatística relevante: máximo, soma
`Shards.initializing`	O número de fragmentos que estão em inicialização. Estatísticas relevantes: soma
`Shards.relocating`	O número de fragmentos que estão em relocação. Estatísticas relevantes: soma
`Nodes`	O número de nós no cluster do OpenSearch Service, inclusive nós principais dedicados e nós UltraWarm. Para obter mais informações, consulte the section called “Alterações de configuração”. Estatística relevante: máximo

Métrica	Descrição
`SearchableDocuments`	O número total de documentos pesquisáveis em todos os nós de dados no cluster. Estatísticas relevantes: mínimo, máximo, média
`DeletedDocuments`	O número total de documentos marcados para exclusão em todos os nós de dados no cluster. Esses documentos não aparecem mais nos resultados de pesquisa, mas o OpenSearch elimina somente os documentos excluídos de disco durante fusões de segmento. Essa métrica aumenta após solicitações e diminuições de exclusão após fusões de segmento. Estatísticas relevantes: mínimo, máximo, média
`CPUUtilization`	A porcentagem de utilização da CPU para nós de dados no cluster. Maximum (Máximo) mostra o nó com a maior utilização da CPU. Average (Médio) representa todos os nós no cluster. Esta métrica também está disponível para nós individuais. Estatísticas relevantes: máximo, média

Métrica	Descrição
`FreeStorageSpace`	O espaço livre para nós de dados no cluster. `Sum` mostra o espaço livre total para o cluster, mas é necessário deixar o período em um minuto para obter um valor exato. `Minimum` e `Maximum` mostram os nós com o menor e o maior espaço livre, respectivamente. Esta métrica também está disponível para nós individuais. O serviço OpenSearch emite um `ClusterBlockException` quando essa métrica atinge`0`. Para recuperar, você deve excluir índices, adicionar instâncias maiores ou adicionar armazenamento EBS às instâncias existentes. Para saber mais, consulte the section called “Falta de espaço de armazenamento disponível”. O console do OpenSearch Service exibe esse valor em GiB. O console do Amazon CloudWatch exibe-o em MiB. **Note** `FreeStorageSpace` será sempre menor do que os valores fornecidos pelas APIs `_cluster/stats` e `_cat/allocation` do OpenSearch. O OpenSearch Service reserva uma porcentagem de espaço de armazenamento em cada instância para operações internas. Para obter mais informações, consulte Cálculo de requisitos de armazenamento. Estatísticas relevantes: mínima, máxima, média, soma
`ClusterUsedSpace`	O total de espaço usado para o cluster. Você deve deixar o período em um minuto para receber um valor preciso. O console do OpenSearch Service exibe esse valor em GiB. O console do Amazon CloudWatch exibe-o em MiB. Estatísticas relevantes: mínimo, máximo

Métrica	Descrição
`ClusterIndexWritesBlocked`	Indica se o cluster está aceitando ou bloqueando solicitações de gravação recebidas. Um valor de 0 significa que o cluster está aceitando solicitações. Um valor de 1 significa que ele está bloqueando solicitações. Alguns fatores comuns são: `FreeStorageSpace` é muito baixo ou `JVMMemoryPressure` é muito alto. Para aliviar esse problema, considere adicionar mais espaço em disco ou escalonar o cluster. Estatística relevante: máximo
`JVMMemoryPressure`	A porcentagem máxima do heap Java usada para todos os nós de dados no cluster. O OpenSearch Service usa metade da RAM de uma instância para o heap do Java, com um tamanho de heap de 32 GiB. Você pode dimensionar instâncias verticalmente até 64 GiB de RAM, sendo que nesse ponto você poderá dimension ar horizontalmente adicionando instâncias. Consulte the section called “ CloudWatch Alarmes recomendados”. Estatística relevante: máximo **Note** A lógica dessa métrica foi alterada no software de serviço R20220323. Para obter mais informações, consulte as notas de lançamento.
`OldGenJVMMemoryPressure`	A porcentagem máxima do heap do Java usada para a "geração antiga" em todos os nós de dados no cluster. Essa métrica também está disponível a nível de nós. Estatística relevante: máximo

Métrica	Descrição
AutomatedSnapshotFailure	O número de snapshots automatizados com falha para o cluster. Um valor de 1 indica que nenhum snapshot automatizado foi feito para o domínio nas últimas 36 horas. Estatísticas relevantes: mínimo, máximo
CPUCreditBalance	Os créditos de CPU ainda disponíveis para nós de dados no cluster. Um crédito de CPU oferece a performance de um núcleo de CPU completo por um minuto. Para obter mais informações, consulte Créditos de CPU no Guia do desenvolvedor do Amazon EC2. Essa métrica está disponível somente para os tipos de instância T2 Estatísticas relevantes: mínimo
OpenSearchDashboardsHealthyNodes	Uma verificação de integridade para o OpenSearch Dashboards. Se mínimo, máximo e média forem todos iguais a 1, o Dashboards está se comportando normalmente. Se você tiver 10 nós com máximo de 1, mínimo de 0 e média de 0,7, isso significa que 7 nós (70%) são íntegros e 3 nós (30%) não são íntegros. Estatísticas relevantes: mínimo, máximo, média
OpensearchDashboardsReportingFailedRequestSysErrCount	O número de solicitações para gerar relatórios do OpenSearch Dashboards que falharam devido a problemas de servidor ou limitações de recursos. Estatísticas relevantes: soma
OpensearchDashboardsReportingFailedRequestUserErrCount	O número de solicitações para gerar relatórios do OpenSearch Dashboards que falharam devido a problemas de cliente. Estatísticas relevantes: soma

Métrica	Descrição
`OpensearchDashboardsReportingRequestCount`	O número total de solicitações para gerar relatórios do OpenSearch Dashboards. Estatísticas relevantes: soma
`OpensearchDashboardsReportingSuccessCount`	O número de solicitações para gerar relatórios do OpenSearch Dashboards bem-sucedidas. Estatísticas relevantes: soma
`KMSKeyError`	Um valor 1 indica que a chave do AWS KMS usada para criptografar dados em repouso foi desabilitada. Para restaurar o domínio de operações normais, reabilite a chave. O console exibe essa métrica somente para domínios que criptografam dados em repouso. Estatísticas relevantes: mínimo, máximo
`KMSKeyInaccessible`	Um valor 1 indica que a chave do AWS KMS usada para criptografar dados em repouso foi excluída teve suas concessões para o OpenSearch Service revogadas. Você não pode recuperar os domínios que estejam nesse estado. Mas, se tiver um snapshot manual, você poderá usá-lo para migrar os dados do domínio para um novo domínio. O console exibe essa métrica somente para domínios que criptografam dados em repouso. Estatísticas relevantes: mínimo, máximo

Métrica	Descrição
`InvalidHostHeaderRequests`	O número de solicitações HTTP feitas para o cluster do OpenSearch que incluíram um cabeçalho de host inválido (ou ausente). As solicitações válidas incluem o nome do host do domínio como o valor do cabeçalho do host. O OpenSearch Service rejeita as solicitações inválidas para domínios de acesso público que não têm uma política de acesso restritiva. Recomendamos aplicar uma política de acesso restritiva a todos os domínios. Se você visualizar grandes valores para esta métrica, confirme se os clientes do OpenSearch incluem o nome de host do domínio (e não, por exemplo, seu endereço IP) em suas solicitações. Estatísticas relevantes: soma
`OpenSearchRequests (previously ElasticsearchRequests)`	O número de solicitações feitas ao cluster do OpenSearch. Estatísticas relevantes: soma
`2xx, 3xx, 4xx, 5xx`	O número de solicitações a um domínio que resultaram no determinado código de resposta HTTP (2xx, 3xx, 4xx, 5xx). Estatísticas relevantes: soma

Métrica	Descrição
`ThroughputThrottle`	Indica se os discos estão sob controle de utilização ou não. O controle de utilização ocorre quando o throughput combinado de `ReadThroughputMicroBursting` e `WriteThroughputMicroBursting` é maior que o throughput máximo de `MaxProvisionedThroughput`. `MaxProvisionedThroughput` é o valor mais baixo do throughput da instância ou do throughput do volume provisionado. Um valor de 1 indica que os discos estão sob controle de utilização. Um valor de 0 indica comportamento normal. Para obter informações sobre o throughput de instâncias, consulte Instâncias otimizadas para Amazon EBS. Para obter informações sobre o throughput de volume, consulte os tipos de volume do Amazon EBS. Estatísticas relevantes: mínimo, máximo

Métricas de nó principal dedicado

O Amazon OpenSearch Service fornece as métricas a seguir para nós principais dedicados.

Métrica	Descrição
`MasterCPUUtilization`	A porcentagem máxima de recursos da CPU usados pelos nós principais dedicados. Recomendamos aumentar o tamanho do tipo de instância quando essa métrica atingir 60%. Estatística relevante: máximo
`MasterFreeStorageSpace`	Essa métrica não é relevante e pode ser ignorada. O serviço não usa nós principais como nós de dados.
`MasterJVMMemoryPressure`	A porcentagem máxima do heap Java usada para todos os nós principais dedicados no cluster. Recomendamos a mudança para um tipo de instância maior quando essa métrica atingir 85%.

Métrica	Descrição
	Estatística relevante: máximo **Note** A lógica dessa métrica foi alterada no software de serviço R20220323. Para obter mais informações, consulte as notas de lançamento.
`MasterOldGenJVMMemoryPressure`	A porcentagem máxima do heap do Java usada para a “geração antiga” por nó principal. Estatística relevante: máximo
`MasterCPUCreditBalance`	Os créditos de CPU ainda disponíveis para nós principais dedicados no cluster. Um crédito de CPU oferece a performance de um núcleo de CPU completo por um minuto. Para obter mais informações, consulte Créditos de CPU no Guia do desenvolvedor do Amazon EC2. Essa métrica está disponível somente para os tipos de instância T2 Estatísticas relevantes: mínimo
`MasterReachableFromNode`	Uma verificação de integridade exceções `MasterNotDiscovered` . Um valor de 1 indica comportamento normal. Um valor de 0 indica que `/_cluster/health/` está falhando. Falhas significam que o nó principal está inacessível a partir do nó de origem. Elas normalmente são o resultado de um problema de conectividade da rede ou de dependência da AWS. Estatística relevante: máximo
`MasterSysMemoryUtilization`	O percentual de memória do nó principal que está em uso. Estatística relevante: máximo

Métricas de volume do EBS

O Amazon OpenSearch Service fornece as métricas a seguir para volumes do EBS.

Métrica	Descrição
`ReadLatency`	A latência, em segundos, para operações de leitura em volumes do EBS. Esta métrica também está disponível para nós individuais. Estatísticas relevantes: mínimo, máximo, média
`WriteLatency`	A latência, em segundos, para operações de gravação em volumes do EBS. Esta métrica também está disponível para nós individuais. Estatísticas relevantes: mínimo, máximo, média
`ReadThroughput`	O throughput, em bytes por segundo, para operações de leitura em volumes do EBS. Esta métrica também está disponível para nós individuais. Estatísticas relevantes: mínimo, máximo, média
`ReadThroughputMicroBursting`	O throughput, em bytes por segundo, para operações de leitura em volumes do EBS quando a microintermitência é levada em consideração. Esta métrica também está disponível para nós individuais. A microintermitência ocorre quando um volume do EBS aumenta o IOPS ou a taxa de throughput por períodos de tempo significativamente mais curtos (menos de um minuto). Estatísticas relevantes: mínimo, máximo, média
`WriteThroughput`	O throughput, em bytes por segundo, para operações de gravação em volumes do EBS. Esta métrica também está disponível para nós individuais. Estatísticas relevantes: mínimo, máximo, média
`WriteThroughputMicroBursting`	O throughput, em bytes por segundo, para operações de gravação em volumes do EBS quando a microintermitência é levada em consideração. Esta métrica também está disponível para nós individuais. A microinte

Métrica	Descrição
	rmitência ocorre quando um volume do EBS aumenta o IOPS ou a taxa de throughput por períodos de tempo significativamente mais curtos (menos de um minuto). Estatísticas relevantes: mínimo, máximo, média
`DiskQueueDepth`	O número de solicitações pendentes de entrada e saída (E/S) de um volume do EBS. Estatísticas relevantes: mínimo, máximo, média
`ReadIOPS`	O número de operações de entrada e saída (E/S) por segundo para operações de leitura em volumes do EBS. Esta métrica também está disponível para nós individuais. Estatísticas relevantes: mínimo, máximo, média
`ReadIOPSM icroBursting`	O número de operações de entrada e saída (E/S) por segundo para operações de leitura em volumes do EBS quando a microintermitência é levando em consideração. Esta métrica também está disponível para nós individuais. A microintermitência ocorre quando um volume do EBS aumenta o IOPS ou a taxa de throughput por períodos de tempo significa tivamente mais curtos (menos de um minuto). Estatísticas relevantes: mínimo, máximo, média
`WriteIOPS`	O número de operações de entrada e saída (E/S) por segundo para operações de gravação em volumes do EBS. Esta métrica também está disponível para nós individuais. Estatísticas relevantes: mínimo, máximo, média

Métrica	Descrição
`WriteIOPS MicroBursting`	O número de operações de entrada e saída (E/S) por segundo para operações de gravação em volumes do EBS quando a microintermitência é levando em consideração. Esta métrica também está disponível para nós individuais. A microintermitência ocorre quando um volume do EBS aumenta o IOPS ou a taxa de throughput por períodos de tempo significativamente mais curtos (menos de um minuto). Estatísticas relevantes: mínimo, máximo, média
`BurstBalance`	A porcentagem de créditos de entrada e saída (E/S) restantes no bucket de intermitência para um volume do EBS. Um valor de 100 significa que o volume acumulou o número máximo de créditos. Se essa porcentagem cair abaixo de 70%, consulte the section called “O saldo de intermitência do EBS está baixo”. O saldo intermitente permanece em 0 para domínios com tipos de volume gp3 e domínios com volume gp2 cujo tamanho de volume seja superior a 1000 GiB. Estatísticas relevantes: mínimo, máximo, média

Métricas de instância

O Amazon OpenSearch Service fornece as métricas a seguir para cada instância em um domínio. O OpenSearch Service também agrega essas métricas de instâncias para fornecer um insight da integridade geral do cluster. Você pode verificar esse comportamento usando a estatística Contagem de amostras no console. Cada métrica na tabela a seguir tem estatísticas relevantes para o nó e o cluster.

> **Important**
>
> Versões diferentes do Elasticsearch usam grupos de threads diferentes para processar chamadas para a API `_index`. As versões 1.5 e 2.3 do Elasticsearch usam o grupo de threads de índice. As versões 5.x, 6.0 e 6.2 do Elasticsearch usam o grupo de threads em massa. O OpenSearch e a versão 6.3 ou superior do Elasticsearch usam o grupo de threads de gravação. No momento, o console do OpenSearch Service não inclui um gráfico para o grupo de threads em massa.

Use `GET _cluster/settings?include_defaults=true` para verificar o grupo de threads e os tamanhos de fila para seu cluster.

Métrica	Descrição
`IndexingLatency`	A diferença no tempo total, em milissegundos, obtida por todas as operações de indexação em um nó entre o minuto N e o minuto (N-1). Estatísticas do nó relevante: média Estatísticas do cluster relevante: média, máximo
`IndexingRate`	O número de operações de indexação por minuto. Uma única chamada para a API `_bulk` que adiciona dois documentos e atualiza duas contagens tem quatro operações, que podem ser espalhadas entre um ou mais nós. Se esse índice tem uma ou mais réplicas, outros nós no cluster também registram um total de quatro operações de índice. Exclusões de documento não são consideradas para essa métrica. Estatísticas do nó relevante: média Estatísticas do cluster relevante: média, máxima, soma
`SearchLatency`	A diferença no tempo total, em milissegundos, obtida por todas as pesquisas em um nó entre o minuto N e o minuto (N-1). Estatísticas do nó relevante: média Estatísticas do cluster relevante: média, máximo
`SearchRate`	O número total de solicitações de pesquisa por minuto para todos os fragmentos em um nó de dados. Uma única chamada para a API `_search` pode retornar resultados de muitos fragmentos diferentes. Se cinco desses fragmentos estiverem em um nó, o nó reportará 5 para essa métrica, mesmo se o cliente só fizer uma solicitação.

Métrica	Descrição
	Estatísticas do nó relevante: média Estatísticas do cluster relevante: média, máxima, soma
`SegmentCount`	O número de segmentos em um nó de dados. Quanto mais segmentos você tiver, mais tempo cada pesquisa demorará. O OpenSearch ocasionalmente mescla segmentos menores em um maior. Estatísticas de nós relevantes: máximo, média Estatísticas do cluster relevante: soma, máximo, média
`SysMemoryUtilization`	O percentual de memória da instância que está em uso. Valores altos para essa métrica são normais e geralmente não represent am um problema com seu cluster. Para obter um melhor indicador de possíveis problemas de performance e estabilidade, consulte a métrica `JVMMemoryPressure` . Estatísticas do nó relevante: mínimo, máximo, média Estatísticas relevantes de cluster: mínimo, máximo, média, soma
`JVMGCYoungCollectionCount`	O número de vezes que a coleta de lixo “nova geração” foi executada. Um grande número de execuções crescente é uma parte normal das operações do cluster. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma, máximo, média
`JVMGCYoungCollectionTime`	A quantidade de tempo, em milissegundos, que o cluster gastou executando a coleta de lixo "nova geração". Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma, máximo, média

Métrica	Descrição
JVMGCOldCollectionCount	O número de vezes que a coleta de lixo “geração antiga” foi executada. Em um cluster com recursos suficientes, esse número deve permanecer pequeno e com crescimento com pouca frequência. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma, máximo, média
JVMGCOldCollectionTime	A quantidade de tempo, em milissegundos, que o cluster gastou executando a coleta de lixo “geração antiga”. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma, máximo, média
OpenSearchDashboardsConcurrentConnections	O número de conexões simultâneas ativas para o OpenSearch Dashboards. Se esse número continuar a crescer, considere escalar seu cluster. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma, máximo, média
OpenSearchDashboardsHealthyNode	Uma verificação de integridade para o nó individual do OpenSearch Dashboards. Um valor de 1 indica comportamento normal. Um valor de 0 indica que Dashboards está inacessível. Estatísticas do nó relevante: mínimo Estatísticas relevantes de cluster: mínimo, máximo, média, soma
OpenSearchDashboardsHeapTotal	A quantidade de memória de heap alocada para o OpenSearch Dashboards em MiB. Diferentes tipos de instância do EC2 podem afetar a alocação exata de memória. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma, máximo, média

Métrica	Descrição
OpenSearchDashboardsHeapUsed	A quantidade absoluta de memória de heap usada pelo OpenSearch Dashboards em MiB. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma, máximo, média
OpenSearchDashboardsHeapUtilization	A porcentagem máxima de memória de heap disponível usada pelo OpenSearch Dashboards. Se esse valor aumentar acima de 80%, considere escalar seu cluster. Estatísticas do nó relevante: máximo Estatísticas relevantes de cluster: mínimo, máximo, média, soma
OpenSearchDashboardsOS1MinuteLoad	A média de carga da CPU em um minuto para o OpenSearch Dashboards. A carga da CPU deve, idealmente, permanecer abaixo de 1,00. Embora picos temporários não sejam um problema, recomendamos aumentar o tamanho do tipo de instância se essa métrica estiver consistentemente acima de 1,00. Estatísticas do nó relevante: média Estatísticas do cluster relevante: média, máximo
OpenSearchDashboardsRequestTotal	A contagem total de solicitações HTTP feitas ao OpenSearch Dashboards. Se o sistema estiver lento ou você observar números elevados de solicitações de painéis, considere aumentar o tamanho do tipo de instância. Estatísticas de nós relevantes: soma Estatísticas do cluster relevante: soma

Métrica	Descrição
`OpenSearchDashboardsResponseTimesMaxInMillis`	O tempo máximo, em milissegundos, necessário para o OpenSearch Dashboards responder a uma solicitação. Se as solicitações demorarem consistentemente muito tempo para retornar resultados, considere aumentar o tamanho do tipo de instância. Estatísticas do nó relevante: máximo Estatísticas de cluster relevantes máximo, média
`SearchTaskCancelled`	O número de cancelamentos do nó coordenador. Estatísticas de nós relevantes: soma Estatísticas do cluster relevante: soma
`SearchShardTaskCancelled`	O número de cancelamentos de nós de dados. Estatísticas de nós relevantes: soma Estatísticas do cluster relevante: soma,
`ThreadpoolForce_mergeQueue`	O número de tarefas na fila no grupo de thread de união de força. Se o tamanho da fila é consistentemente alto, considere escalonar seu cluster. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma, máximo, média
`ThreadpoolForce_mergeRejected`	O número de tarefas rejeitadas no grupo de thread de união de força. Se esse número continuar a crescer, considere escalonar seu cluster. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma

Métrica	Descrição
`ThreadpoolForce_mergeThreads`	O tamanho do grupo de threads de união de força. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: média, soma
`ThreadpoolIndexQueue`	O número de tarefas na fila no grupo de thread de índice. Se o tamanho da fila é consistentemente alto, considere escalonar seu cluster. O tamanho máximo da fila de índice é de 200. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma, máximo, média
`ThreadpoolIndexRejected`	O número de tarefas rejeitadas no grupo de thread de índice. Se esse número continuar a crescer, considere escalonar seu cluster. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma
`ThreadpoolIndexThreads`	O tamanho do grupo de threads de índice. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: média, soma
`ThreadpoolSearchQueue`	O número de tarefas na fila no grupo de thread de pesquisa. Se o tamanho da fila é consistentemente alto, considere escalonar seu cluster. O tamanho da fila de pesquisa máximo é 1.000. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma, máximo, média

Métrica	Descrição
`ThreadpoolSearchRejected`	O número de tarefas rejeitadas no grupo de thread de pesquisa. Se esse número continuar a crescer, considere escalonar seu cluster. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma
`ThreadpoolSearchThreads`	O tamanho do grupo de threads de pesquisa. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: média, soma
`Threadpoolsql-workerQueue`	O número de tarefas na fila no grupo de threads de pesquisa SQL. Se o tamanho da fila é consistentemente alto, considere escalonar seu cluster. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma, máximo, média
`Threadpoolsql-workerRejected`	O número de tarefas rejeitadas no grupo de threads de pesquisa SQL. Se esse número continuar a crescer, considere escalonar seu cluster. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma
`Threadpoolsql-workerThreads`	O tamanho do grupo de threads de pesquisa SQL. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: média, soma

Métrica	Descrição
ThreadpoolBulkQueue	O número de tarefas na fila no grupo de thread em massa. Se o tamanho da fila é consistentemente alto, considere escalonar seu cluster. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma, máximo, média
ThreadpoolBulkRejected	O número de tarefas rejeitadas no grupo de thread em massa. Se esse número continuar a crescer, considere escalonar seu cluster. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma
ThreadpoolBulkThreads	O tamanho do grupo de threads em massa. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: média, soma
ThreadpoolWriteThreads	O tamanho do grupo de threads de gravação. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: média, soma
ThreadpoolWriteQueue	O número de tarefas na fila no grupo de threads de gravação. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: média, soma

Métrica	Descrição
`ThreadpoolWriteRejected`	O número de tarefas rejeitadas no grupo de threads de gravação. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: média, soma **Note** Como o tamanho padrão da fila de gravação foi aumentado de 200 para 10.000 na versão 7.1, essa métrica não é mais o único indicador de rejeições do OpenSearch Service. Use as métricas `CoordinatingWriteRejected`, `PrimaryWriteRejected` e `ReplicaWriteRejected` para monitorar rejeições nas versões 7.1 e posteriores.
`CoordinatingWriteRejected`	O número total de rejeições que ocorreram no nó de coordenação devido à pressão de indexação desde a última inicialização de processo do OpenSearch Service. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: média, soma Esta métrica está disponível na versão 7.1 e posteriores.
`PrimaryWriteRejected`	O número total de rejeições que ocorreram nos fragmentos primários devido à pressão de indexação desde a última inicialização de processo do OpenSearch Service. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: média, soma Esta métrica está disponível na versão 7.1 e posteriores.

Métrica	Descrição
`ReplicaWriteRejected`	O número total de rejeições que ocorreram nos fragmentos de réplica devido à pressão de indexação desde a última inicialização de processo do OpenSearch Service. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: média, soma Esta métrica está disponível na versão 7.1 e posteriores.

Métricas do UltraWarm

O Amazon OpenSearch Service fornece as métricas a seguir para nós UltraWarm.

Métrica	Descrição
`WarmCPUUtilization`	A porcentagem de utilização da CPU para nós UltraWarm no cluster. Maximum (Máximo) mostra o nó com a maior utilização da CPU. Average (Médio) representa todos os nós UltraWarm no cluster. Esta métrica também está disponível para nós UltraWarm individuais. Estatísticas relevantes: máximo, média
`WarmFreeStorageSpace`	A quantidade de espaço de armazenamento de alta atividade livre em MiB. Como o UltraWarm usa o Amazon S3, em vez de discos conectados, `Sum` é a única estatística relevante. Você deve deixar o período em um minuto para receber um valor preciso. Estatísticas relevantes: soma
`WarmSearchableDocuments`	O número total de documentos pesquisáveis em todos os índices warm no cluster. Você deve deixar o período em um minuto para receber um valor preciso. Estatísticas relevantes: soma

Métrica	Descrição
`WarmSearchLatency`	A diferença no tempo total, em milissegundos, obtida por todas as pesquisas em um UltraWarm entre o minuto N e o minuto (N-1). Estatísticas do nó relevante: média Estatísticas do cluster relevante: média, máximo
`WarmSearchRate`	O número total de solicitações de pesquisa por minuto para todos os fragmentos em um nó UltraWarm. Uma única chamada para a API `_search` pode retornar resultados de muitos fragmentos diferentes. Se cinco desses fragmentos estiverem em um nó, o nó reportará 5 para essa métrica, mesmo se o cliente só fizer uma solicitação. Estatísticas do nó relevante: média Estatísticas do cluster relevante: média, máxima, soma
`WarmStorageSpaceUtilization`	A quantidade total de espaço de armazenamento de alta atividade, em MiB, que o cluster está usando. Estatística relevante: máximo
`HotStorageSpaceUtilization`	A quantidade total de espaço de armazenamento de atividade muito alta que o cluster está usando. Estatística relevante: máximo
`WarmSysMemoryUtilization`	A porcentagem de memória do nó de alta atividade que está em uso. Estatística relevante: máximo
`HotToWarmMigrationQueueSize`	O número de índices aguardando no momento para a migração do armazenamento quente para o armazenamento warm. Estatística relevante: máximo

Métrica	Descrição
`WarmToHot Migration QueueSize`	O número de índices aguardando no momento para a migração do armazenamento warm para o armazenamento quente. Estatística relevante: máximo
`HotToWarm Migration FailureCount`	O número total de migrações de atividade muito alta para alta atividade que falharam. Estatísticas relevantes: soma
`HotToWarm Migration ForceMerg eLatency`	A latência média da etapa de forçar mesclagem do processo de migração. Se este estágio demorar muito de forma consisten te, considere aumentar `index.ultrawarm.migration.f orce_merge.max_num_segments` . Estatística relevante: média
`HotToWarm Migration SnapshotL atency`	A latência média da etapa de snapshot do processo de migração. Se esse estágio demorar muito de forma consistente, certifique-se de que os fragmentos estejam adequadamente dimensionados e distribuídos por todo o cluster. Estatística relevante: média
`HotToWarm Migration Processin gLatency`	A latência média de migrações de atividade muito alta para alta atividade bem-sucedidas, nãoincluindo tempo gasto na fila. Esse valor é a soma do tempo necessário para concluir os estágios de forçar mesclagem, snapshot e realocação de fragmentos do processo de migração. Estatística relevante: média
`HotToWarm Migration SuccessCount`	O número total de migrações de atividade muito alta para alta atividade bem-sucedidas. Estatísticas relevantes: soma

Métrica	Descrição
`HotToWarmMigrationSuccessLatency`	A latência média de migrações de atividade muito alta para alta atividade bem-sucedidas, incluindo tempo gasto na fila. Estatística relevante: média
`WarmThreadpoolSearchThreads`	O tamanho do grupo de threads de pesquisa UltraWarm. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: média, soma
`WarmThreadpoolSearchRejected`	O número de tarefas rejeitadas no grupo de threads de pesquisa UltraWarm. Se esse número continuar a crescer, considere adicionar mais nós UltraWarm. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma
`WarmThreadpoolSearchQueue`	O número de tarefas na fila no grupo de threads de pesquisa UltraWarm. Se o tamanho da fila for consistentemente alto, considere adicionar mais nós UltraWarm. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma, máximo, média
`WarmJVMMemoryPressure`	A porcentagem máxima do heap Java usada para os nós do UltraWarm. Estatística relevante: máximo **Note** A lógica dessa métrica foi alterada no software de serviço R20220323. Para obter mais informações, consulte as notas de lançamento.

Métrica	Descrição
`WarmOldGenJVMMemoryPressure`	A porcentagem máxima do heap do Java usada para a "geração antiga" por nó UltraWarm. Estatística relevante: máximo
`WarmJVMGCYoungCollectionCount`	O número de vezes que a coleta de residuos da “nova geração” foi executada em nós UltraWarm. Um grande número de execuções crescente é uma parte normal das operações do cluster. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma, máximo, média
`WarmJVMGCYoungCollectionTime`	A quantidade de tempo, em milissegundos, que o cluster gastou executando a coleta de lixo “nova geração” em nós UltraWarm. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma, máximo, média
`WarmJVMGCOldCollectionCount`	O número de vezes que a coleta de residuos da “antiga geração” foi executada em nós UltraWarm. Em um cluster com recursos suficientes, esse número deve permanecer pequeno e com crescimento com pouca frequência. Estatísticas do nó relevante: máximo Estatísticas do cluster relevante: soma, máximo, média

Métricas de armazenamento de baixa atividade

O Amazon OpenSearch Service fornece as métricas a seguir para armazenamento de baixa atividade.

Métrica	Descrição
`ColdStorageSpaceUtilization`	A quantidade total de espaço de armazenamento de baixa atividade, em MiB, que o cluster está usando. Estatísticas relevantes: máx.
`ColdToWarmMigrationFailureCount`	O número total de migrações de baixa atividade para alta atividade que falharam. Estatísticas relevantes: soma
`ColdToWarmMigrationLatency`	A quantidade de tempo necessária para que as migrações de baixa atividade para alta atividade sejam concluídas. Estatística relevante: média
`ColdToWarmMigrationQueueSize`	O número de índices aguardando no momento para a migração do armazenamento frio para o armazenamento warm. Estatística relevante: máximo
`ColdToWarmMigrationSuccessCount`	O número total de migrações de baixa atividade para alta atividade bem-sucedidas. Estatísticas relevantes: soma
`WarmToColdMigrationFailureCount`	O número total de migrações de alta atividade para baixa atividade que falharam. Estatísticas relevantes: soma
`WarmToColdMigrationLatency`	A quantidade de tempo necessária para que as migrações de alta atividade para baixa atividade sejam concluídas. Estatística relevante: média
`WarmToColdMigrationQueueSize`	O número de índices aguardando atualmente para migrar do armazenamento warm para o armazenamento frio. Estatística relevante: máximo

Métrica	Descrição
`WarmToColdMigrationSuccessCount`	O número total de migrações de alta atividade para baixa atividade bem-sucedidas. Estatísticas relevantes: soma

Métricas de OR1

O Amazon OpenSearch Service fornece as métricas a seguir para instâncias OR1.

Métrica	Descrição
`RemoteStorageUsedSpace`	A quantidade total de espaço do Amazon S3, em MiB, que o cluster está usando. Estatísticas relevantes: soma
`RemoteStorageWriteRejected`	O número total de solicitações rejeitadas nos fragmentos primários devido à pressão de armazenamento e replicação remotos. Isso é calculado a partir da última inicialização do processo do OpenSearch Service. Estatísticas relevantes: soma

Métricas de alerta

O Amazon OpenSearch Service fornece as métricas a seguir para alertas.

Métrica	Descrição
`AlertingDegraded`	Um valor de 1 significa que o índice de alerta é vermelho ou um ou mais nós não estão na programação. Um valor de 0 indica comportamento normal. Estatística relevante: máximo

Métrica	Descrição
`AlertingIndexExists`	Um valor de 1 significa que o índice `.opensearch-alerting-config` existe. Um valor de 0 significa que não. Até que você use o recurso de alerta pela primeira vez, esse valor permanecerá como 0. Estatística relevante: máximo
`AlertingIndexStatus.green`	A integridade do índice. Um valor de 1 significa verde. Um valor de 0 significa que o índice não existe ou não está verde. Estatística relevante: máximo
`AlertingIndexStatus.red`	A integridade do índice. Um valor de 1 significa vermelho. Um valor de 0 significa que o índice não existe ou não está vermelho. Estatística relevante: máximo
`AlertingIndexStatus.yellow`	A integridade do índice. Um valor de 1 significa amarelo. Um valor de 0 significa que o índice não existe ou não está amarelo. Estatística relevante: máximo
`AlertingNodesNotOnSchedule`	Um valor de 1 significa que alguns trabalhos não estão sendo executados de acordo com a programação. Um valor de 0 significa que todos os trabalhos de alerta estão sendo executados de acordo com a programação (ou que não existem trabalhos de alerta). Verifique o console do OpenSearch Service ou faça uma solicitação `_nodes/stats` para ver se algum nó mostra uso elevado de recursos. Estatística relevante: máximo
`AlertingNodesOnSchedule`	Um valor de 1 significa que todos os trabalhos de alerta estão em execução de acordo com a programação (ou que não existem trabalhos de alerta). Um valor de 0 significa que alguns trabalhos não estão sendo executados de acordo com a programação. Estatística relevante: máximo

Métrica	Descrição
`AlertingScheduledJobEnabled`	Um valor de 1 significa que a configuração do cluster `opensearch.scheduled_jobs.enabled` é verdadeira. Um valor de 0 significa que é falsa e os trabalhos programados estão desabilitados. Estatística relevante: máximo

Métricas de detecção de anomalias

O Amazon OpenSearch Service fornece as métricas a seguir para detecção de anomalias.

Métrica	Descrição
`ADPluginUnhealthy`	Um valor de 1 significa que o plugin de detecção de anomalias não está funcionando corretamente, seja por causa de um alto número de falhas, seja porque um dos índices que ele usa é vermelho. Um valor de 0 indica que o plugin está funcionando conforme esperado. Estatística relevante: máximo
`ADExecuteRequestCount`	O número de solicitações para detectar anomalias. Estatísticas relevantes: soma
`ADExecuteFailureCount`	O número de solicitações com falha para detecção de anomalias. Estatísticas relevantes: soma
`ADHCExecuteFailureCount`	O número de solicitações de detecção de anomalias para detectores de alta cardinalidade que falharam. Estatísticas relevantes: soma
`ADHCExecuteRequestCount`	O número de solicitações de detecção de anomalias para detectores de alta cardinalidade. Estatísticas relevantes: soma

Métrica	Descrição
`ADAnomalyResultsIndexStatusIndexExists`	Um valor de 1 significa que o índice para o qual o alias `.opensearch-anomaly-results` aponta existe. Até que o recurso de detecção de anomalias seja usado pela primeira vez, esse valor permanecerá 0. Estatística relevante: máximo
`ADAnomalyResultsIndexStatus.red`	Um valor de 1 significa que o índice para o qual o alias `.opensearch-anomaly-results` aponta é vermelho. Um valor de 0 significa que não é. Até que o recurso de detecção de anomalias seja usado pela primeira vez, esse valor permanecerá 0. Estatística relevante: máximo
`ADAnomalyDetectorsIndexStatusIndexExists`	Um valor de 1 significa que o índice `.opensearch-anomaly-detectors` existe. Um valor de 0 significa que não. Até que o recurso de detecção de anomalias seja usado pela primeira vez, esse valor permanecerá 0. Estatística relevante: máximo
`ADAnomalyDetectorsIndexStatus.red`	Um valor de 1 significa que o índice `.opensearch-anomaly-detectors` é vermelho. Um valor de 0 significa que não é. Até que o recurso de detecção de anomalias seja usado pela primeira vez, esse valor permanecerá 0. Estatística relevante: máximo
`ADModelsCheckpointIndexStatusIndexExists`	Um valor de 1 significa que o índice `.opensearch-anomaly-checkpoints` existe. Um valor de 0 significa que não. Até que o recurso de detecção de anomalias seja usado pela primeira vez, esse valor permanecerá 0. Estatística relevante: máximo

Métrica	Descrição
`ADModelsCheckpointIndexStatus.red`	Um valor de 1 significa que o índice `.opensearch-anomaly-checkpoints` é vermelho. Um valor de 0 significa que não é. Até que o recurso de detecção de anomalias seja usado pela primeira vez, esse valor permanecerá 0. Estatística relevante: máximo

Métricas de pesquisa assíncrona

O Amazon OpenSearch Service fornece as métricas a seguir para pesquisa assíncrona.

Estatísticas de nó coordenador de pesquisa assíncrona (por nó coordenador)

Métrica	Descrição
`AsynchronousSearchSubmissionRate`	O número de pesquisas assíncronas enviadas no último minuto.
`AsynchronousSearchInitializedRate`	O número de pesquisas assíncronas inicializadas no último minuto.
`AsynchronousSearchRunningCurrent`	O número de pesquisas assíncronas atualmente em execução.
`AsynchronousSearchCompletionRate`	O número de pesquisas assíncronas concluídas com êxito no último minuto.
`AsynchronousSearchFailureRate`	O número de pesquisas assíncronas que foram concluídas e falharam no último minuto.

Métrica	Descrição
`AsynchronousSearchPersistRate`	O número de pesquisas assíncronas que persistiram no último minuto.
`AsynchronousSearchPersistFailedRate`	O número de pesquisas assíncronas que falharam ao persistir no último minuto.
`AsynchronousSearchRejected`	O número total de pesquisas assíncronas rejeitadas desde o momento de ativação do nó.
`AsynchronousSearchCancelled`	O número total de pesquisas assíncronas canceladas desde o momento de ativação do nó.
`AsynchronousSearchMaxRunningTime`	A duração da pesquisa assíncrona de execução mais longa em um nó no último minuto.

Estatísticas de cluster de pesquisa assíncrona

Métrica	Descrição
`AsynchronousSearchStoreHealth`	A integridade do armazenamento no índice persistido (vermelho/não vermelho) no último minuto.
`AsynchronousSearchStoreSize`	O tamanho do índice do sistema em todos os fragmentos no último minuto.
`AsynchronousSearch`	O número de respostas armazenadas no índice do sistema no último minuto.

Métrica	Descrição
StoredResponseCount	

Métricas do Auto-Tune

O Amazon OpenSearch Service fornece as métricas a seguir para Auto-Tune.

Métrica	Descrição
AutoTuneChangesHistoryHeapSize	O histórico de alterações em MiB para valores de ajuste do tamanho da pilha.
AutoTuneChangesHistoryJVMYoungGenArgs	O histórico de alterações dos argumentos do JVM YongGen.
AutoTuneFailed	Um booleano que indica se a alteração do Auto-Tune falhou.
AutoTuneSucceeded	Um booleano que indica se a alteração do Auto-Tune foi bem-sucedida.
AutoTuneValue	O histórico de alterações da fila (contagem) e o histórico de alterações dos ajustes do cache (em MiB) para alterações sem interrupções.

Métricas do multi-AZ com modo de espera

O Amazon OpenSearch Service fornece as métricas a seguir para multi-AZ com modo de espera.

Métricas em nível de nó para nós de dados em zonas de disponibilidade ativas

Métrica	Descrição
CPUUtilization	A porcentagem de utilização da CPU para nós de dados no cluster. Maximum (Máximo) mostra o nó com a maior utilização da CPU.

Métrica	Descrição
	Average (Médio) representa todos os nós no cluster. Esta métrica também está disponível para nós individuais.
`FreeStorageSpace`	O espaço livre para nós de dados no cluster. `Sum` mostra o espaço livre total para o cluster, mas é necessário deixar o período em um minuto para obter um valor exato. `Minimum` e `Maximum` mostram os nós com o menor e o maior espaço livre, respectivamente. Esta métrica também está disponível para nós individuais. O serviço OpenSearch emite um `ClusterBlockException` quando essa métrica atinge`0`. Para recuperar, você deve excluir índices, adicionar instâncias maiores ou adicionar armazenamento EBS às instâncias existentes. Para saber mais, consulte the section called “Falta de espaço de armazenamento disponível”. O console do OpenSearch Service exibe esse valor em GiB. O console do Amazon CloudWatch exibe-o em MiB.
`JVMMemoryPressure`	A porcentagem máxima do heap Java usada para todos os nós de dados no cluster. O OpenSearch Service usa metade da RAM de uma instância para o heap do Java, com um tamanho de heap de 32 GiB. Você pode dimensionar instâncias verticalmente até 64 GiB de RAM, sendo que nesse ponto você poderá dimensionar horizontalmente adicionando instâncias. Consulte the section called “ CloudWatch Alarmes recomendados”.
`SysMemoryUtilization`	O percentual de memória da instância que está em uso. Valores altos para essa métrica são normais e geralmente não representam um problema com seu cluster. Para obter um melhor indicador de possíveis problemas de performance e estabilidade, consulte a métrica `JVMMemoryPressure` .
`IndexingLatency`	A diferença no tempo total, em milissegundos, obtida por todas as operações de indexação em um nó entre o minuto N e o minuto (N-1).
`IndexingRate`	O número de operações de indexação por minuto.

Métrica	Descrição
SearchLatency	A diferença no tempo total, em milissegundos, obtida por todas as pesquisas em um nó entre o minuto N e o minuto (N-1).
SearchRate	O número total de solicitações de pesquisa por minuto para todos os fragmentos em um nó de dados.
ThreadpoolSearchQueue	O número de tarefas na fila no grupo de thread de pesquisa. Se o tamanho da fila é consistentemente alto, considere escalonar seu cluster. O tamanho da fila de pesquisa máximo é 1.000.
ThreadpoolWriteQueue	O número de tarefas na fila no grupo de threads de gravação.
ThreadpoolSearchRejected	O número de tarefas rejeitadas no grupo de thread de pesquisa. Se esse número continuar a crescer, considere escalonar seu cluster.
ThreadpoolWriteRejected	O número de tarefas rejeitadas no grupo de threads de gravação.

Métricas no nível do cluster para clusters em zonas de disponibilidade ativas

Métrica	Descrição
DataNodes	O número total de fragmentos ativos e em espera.
DataNodesShards.active	O número total de fragmentos ativos primários e de réplica.
DataNodesShards.unassigned	O número de fragmentos que não estão alocados a nós no cluster.
DataNodesShards.initializing	O número de fragmentos que estão em inicialização.

Métrica	Descrição
`DataNodes Shards.relocating`	O número de fragmentos que estão em relocação.

Métricas de alternação da zona de disponibilidade

Se `ActiveReads.`*`Availability-Zone`* `= 1`, então a zona está ativa. Se `ActiveReads.`*`Availability-Zone`* `= 0`, então a zona está em modo de espera.

Métricas pontuais

O Amazon OpenSearch Service fornece as métricas a seguir para pesquisas de ponto de tempo (PIT).

Estatísticas de nó coordenador de PIT (por nó coordenador)

Métrica	Descrição
`CurrentPointInTime`	O número de contextos de pesquisa PIT ativos no nó.
`TotalPointInTime`	O número de contextos de pesquisa de PIT expirados desde o momento de ativação do nó.
`AvgPointInTimeAliveTime`	A média de manutenção ativa dos contextos de pesquisa de PIT desde o momento de ativação do nó.
`HasActivePointInTime`	Um valor de 1 indica que há contextos PIT ativos nos nós desde o tempo de atividade do nó. Um valor de zero significa que não há.
`HasUsedPointInTime`	Um valor de 1 indica que há contextos PIT ativos nos nós desde o tempo de atividade do nó. Um valor de zero significa que não há.

Métricas de SQL

O Amazon OpenSearch Service fornece as métricas a seguir para suporte a SQL.

Métrica	Descrição
`SQLFailedRequestCountByCusErr`	O número de solicitações com falha para a API `_sql` devido a um problema do cliente. Por exemplo, uma solicitação pode retornar o código de status HTTP 400 devido a um `IndexNotFoundException` . Estatísticas relevantes: soma
`SQLFailedRequestCountBySysErr`	O número de solicitações com falha para a API `_sql` devido a um problema de servidor ou limitação de recurso. Por exemplo, uma solicitação pode retornar o código de status HTTP 503 devido a um `VerificationException` . Estatísticas relevantes: soma
`SQLRequestCount`	O número de solicitações para a API `_sql`. Estatísticas relevantes: soma
`SQLDefaultCursorRequestCount`	Semelhante a `SQLRequestCount` , mas conta apenas solicitações de paginação. Estatísticas relevantes: soma
`SQLUnhealthy`	Um valor 1 indica que, em resposta a determinadas solicitações, o plugin do SQL está retornando códigos de resposta 5xx ou passando DSL de consulta inválida para o OpenSearch. Outras solicitações devem continuar a ter êxito. Um valor de 0 indica que não há falhas recentes. Se você vir um valor sustentado de 1, solucione o problema das solicitações que seus clientes estão fazendo ao plugin. Estatística relevante: máximo

Métricas de k-NN

O Amazon OpenSearch Service inclui as métricas a seguir para o plugin de k-vizinhos mais próximos (k-NN).

Métrica	Descrição
KNNCacheCapacityReached	Métrica por nó para determinar se a capacidade do cache foi atingida. Essa métrica só é relevante para pesquisas k-NN aproximadas. Estatística relevante: máximo
KNNCircuitBreakerTriggered	Métrica por cluster para determinar se o disjuntor foi acionado. Se algum nó retornar um valor 1 para KNNCacheCapacityReached , esse valor também retornará 1. Essa métrica só é relevante para pesquisas k-NN aproximadas. Estatística relevante: máximo
KNNEvictionCount	Métrica por nó para o número de gráficos que foram removidos do cache devido a restrições de memória ou tempo ocioso. Remoções explícitas que ocorrem devido à exclusão do índice não são contadas. Essa métrica só é relevante para pesquisas k-NN aproximadas. Estatísticas relevantes: soma
KNNGraphIndexErrors	Métrica por nó para o número de solicitações para adicionar o campo knn_vector de um documento a um gráfico que produziram erros. Estatísticas relevantes: soma
KNNGraphIndexRequests	Métrica por nó para o número de solicitações para adicionar o campo knn_vector de um documento a um gráfico. Estatísticas relevantes: soma
KNNGraphMemoryUsage	Métrica por nó para o tamanho do cache atual (tamanho total de todos os gráficos na memória) em kilobytes. Essa métrica só é relevante para pesquisas k-NN aproximadas. Estatística relevante: média

Métrica	Descrição
KNNGraphQueryErrors	Métrica por nó para o número de consultas de gráfico que produziram erros. Estatísticas relevantes: soma
KNNGraphQueryRequests	Métrica por nó para o número de consultas de gráfico. Estatísticas relevantes: soma
KNNHitCount	Métrica por nó para o número de acertos de cache. Um acerto de cache ocorre quando um usuário consulta um gráfico que já está carregado na memória. Essa métrica só é relevante para pesquisas k-NN aproximadas. Estatísticas relevantes: soma
KNNLoadExceptionCount	Métrica por nó para o número de vezes que uma exceção ocorreu ao tentar carregar um gráfico no cache. Essa métrica só é relevante para pesquisas k-NN aproximadas. Estatísticas relevantes: soma
KNNLoadSuccessCount	Métrica por nó para o número de vezes que o plugin carregou com êxito um gráfico no cache. Essa métrica só é relevante para pesquisas k-NN aproximadas. Estatísticas relevantes: soma
KNNMissCount	Métrica por nó para o número de perdas do cache. Uma perda de cache ocorre quando um usuário consulta um gráfico que ainda não está carregado na memória. Essa métrica só é relevante para pesquisas k-NN aproximadas. Estatísticas relevantes: soma

Métrica	Descrição
KNNQueryRequests	Métrica por nó para o número de solicitações de consulta recebidas pelo plugin k-NN. Estatísticas relevantes: soma
KNNScriptCompilationErrors	Métrica por nó para o número de erros durante a compilação de scripts. Essa estatística só é relevante para a pesquisa de scripts de pontuação k-NN. Estatísticas relevantes: soma
KNNScriptCompilations	Métrica por nó para o número de vezes que o script k-NN foi compilado. Esse valor normalmente deve ser 1 ou 0, mas se o cache que contém os scripts compilados estiver preenchido, o script k-NN poderá ser recompilado. Essa estatística só é relevante para a pesquisa de scripts de pontuação k-NN. Estatísticas relevantes: soma
KNNScriptQueryErrors	Métrica por nó para o número de erros durante consultas de scripts. Essa estatística só é relevante para a pesquisa de scripts de pontuação k-NN. Estatísticas relevantes: soma
KNNScriptQueryRequests	Métrica por nó para o número total de consultas de scripts. Essa estatística só é relevante para a pesquisa de scripts de pontuação k-NN. Estatísticas relevantes: soma
KNNTotalLoadTime	O tempo em nanossegundos que o algoritmo k-NN demorou para carregar gráficos no cache. Essa métrica só é relevante para pesquisas k-NN aproximadas. Estatísticas relevantes: soma

Métricas de pesquisa entre clusters

O Amazon OpenSearch Service fornece as métricas a seguir para pesquisa entre clusters.

Métricas de domínio de origem

Métrica	Dimensão	Descrição
`CrossClusterOutboundConnections`	`ConnectionId`	Número de nós conectados. Se sua resposta incluir um ou mais domínios ignorados, use essa métrica para rastrear quaisquer conexões não íntegras. Se esse número cair para 0, a conexão não estará íntegra.
`CrossClusterOutboundRequests`	`ConnectionId`	Número de solicitações de pesquisa enviadas para o domínio de destino. Use para verificar se a carga de solicitações de pesquisa entre clusters está sobrecarregando o domínio, correlacione qualquer pico nessa métrica com qualquer pico de JVM/CPU.

Métrica de domínio de destino

Métrica	Dimensão	Descrição
`CrossClusterInboundRequests`	`ConnectionId`	Número de solicitações de conexão de entrada recebidas do domínio de origem.

Adicione um alarme do CloudWatch caso você perca uma conexão inesperadamente. Para obter as etapas para criação de um alarme, consulte Criar um alarme do CloudWatch com base em limite estático.

Métricas de replicação entre clusters

O Amazon OpenSearch Service fornece as métricas a seguir para replicação entre clusters.

Métrica	Descrição
`ReplicationRate`	A taxa média de operações de replicação por segundo. Essa métrica é semelhante à métrica do `IndexingRate` .
`LeaderCheckPoint`	Para uma conexão específica, a soma dos valores do ponto de verificação líder em todos os índices de replicação. Você pode usar essa métrica para medir a latência de replicação.
`FollowerCheckPoint`	Para uma conexão específica, a soma dos valores do ponto de verificação seguidor em todos os índices de replicação. Você pode usar essa métrica para medir a latência de replicação.
`ReplicationNumSyncingIndices`	O número de índices que têm um status de replicação de `SYNCING`.
`ReplicationNumBootstrappingIndices`	O número de índices que têm um status de replicação de `BOOTSTRAPPING` .
`ReplicationNumPausedIndices`	O número de índices que têm um status de replicação de `PAUSED`.
`ReplicationNumFailedIndices`	O número de índices que têm um status de replicação de `FAILED`.
`CrossClusterOutboundReplicationRequests`	O número de solicitações de transporte de replicação no domínio seguidor. Solicitações de transporte são internas e ocorrem sempre que uma operação de API de replicação é chamada. Também ocorrem quando as pesquisas do domínio do seguidor mudam do domínio líder.
`CrossClusterInboun`	O número de solicitações de transporte de replicação no domínio líder. Solicitações de transporte são internas e ocorrem sempre que uma operação de API de replicação é chamada.

Métrica	Descrição
dReplicationRequests	
AutoFollowNumSuccessStartReplication	O número de índices seguidores que foram criados com êxito por uma regra de replicação para uma conexão específica.
AutoFollowNumFailedStartReplication	O número de índices seguidores que falharam ao serem criados por uma regra de replicação quando havia um padrão de correspondência. Esse problema pode surgir devido a um problema de rede no cluster remoto ou devido a um problema de segurança (ou seja, a função associada não tem permissão para iniciar a replicação).
AutoFollowLeaderCallFailure	Se houve alguma consulta com falha entre o índice seguidor e o índice líder para extrair novos dados. Um valor de 1 significa que houve uma ou mais chamadas com falha no último minuto.

Métricas de Learning to Rank

O Amazon OpenSearch Service fornece as métricas a seguir para Learning to Rank.

Métrica	Descrição
LTRRequestTotalCount	Contagem total de solicitações de classificação.
LTRRequestErrorCount	Contagem total de solicitações malsucedidas.
LTRStatus.red	Rastreia se um dos índices necessários para executar o plugin é vermelho.
LTRMemoryUsage	Memória total usada pelo plugin.

Métrica	Descrição
`LTRFeatureMemoryUsageInBytes`	A quantidade de memória, em bytes, usada pelos campos de recursos do Learning to Rank.
`LTRFeaturesetMemoryUsageInBytes`	A quantidade de memória, em bytes, usada por todos os conjuntos de recursos do Learning to Rank.
`LTRModelMemoryUsageInBytes`	A quantidade de memória, em bytes, usada por todos os modelos do Learning to Rank.

Métricas da Piped Processing Language

O Amazon OpenSearch Service fornece as métricas a seguir para a Piped Processing Language.

Métrica	Descrição
`PPLFailedRequestCountByCusErr`	O número de solicitações com falha para a API `_ppl` devido a um problema do cliente. Por exemplo, uma solicitação pode retornar o código de status HTTP 400 devido a um `IndexNotFoundException` .
`PPLFailedRequestCountBySysErr`	O número de solicitações com falha para a API `_ppl` devido a um problema de servidor ou limitação de recurso. Por exemplo, uma solicitação pode retornar o código de status HTTP 503 devido a um `VerificationException` .
`PPLRequestCount`	O número de solicitações para a API `_ppl`.

Monitoramento de logs do OpenSearch com o Amazon CloudWatch Logs

O Amazon OpenSearch Service expõe os seguintes logs do OpenSearch via Amazon CloudWatch Logs:

- Logs de erro
- Logs lentos
- Logs de auditoria

Os logs lentos de pesquisa, logs lentos de indexação e logs de erros são úteis para solucionar problemas de performance e estabilidade. Os logs de auditoria rastreiam a atividade do usuário para fins de conformidade Por padrão, todos os logs são desabilitados. Se habilitados, os preços padrão do CloudWatch são aplicáveis.

> **Note**
>
> Os logs de erros estão disponíveis apenas para o OpenSearch e o Elasticsearch versões 5.1 e posteriores. Os logs lentos estão disponíveis para todas as versões do OpenSearch e do Elasticsearch.

Para os próprios logs, o OpenSearch usa o Apache Log4j 2 e seus níveis de log integrados (do menos para o mais severo) de `TRACE`, `DEBUG`, `INFO`, `WARN`, `ERROR` e `FATAL`.

Se você habilitar os logs de erros, o OpenSearch Service publicará as linhas de logs de `WARN`, `ERROR` e `FATAL` no CloudWatch. O OpenSearch Service também publica várias exceções do nível `DEBUG`, incluindo as seguintes:

- `org.opensearch.index.mapper.MapperParsingException`
- `org.opensearch.index.query.QueryShardException`
- `org.opensearch.action.search.SearchPhaseExecutionException`
- `org.opensearch.common.util.concurrent.OpenSearchRejectedExecutionException`
- `java.lang.IllegalArgumentException`

Os logs de erros podem ajudar a solucionar problemas em muitas situações, incluindo:

- Problemas de compilação de script Painless
- Consultas inválidas
- Indexação de problemas
- Falhas de snapshots
- Falhas de migração do Index State Management

Tópicos

Habilitação da publicação de logs (console)

O console do OpenSearch Service é a maneira mais simples de habilitar a publicação de logs no CloudWatch.

Para habilitar a publicação de logs no CloudWatch (console)

1. Vá para https://aws.amazon.com e escolha Fazer login no console.
2. Em Análise, escolha Amazon OpenSearch Service.
3. Selecione o domínio que deseja atualizar.
4. Na guia Logs, selecione um tipo de log e escolha Habilitar.
5. Crie um novo grupo de logs do CloudWatch ou escolha um já existente.

> **Note**
>
> Se você planejar habilitar vários logs, recomendamos publicar cada um em seu próprio grupo de logs. Essa separação torna os logs mais fáceis de serem encontrados.

6. Escolha uma política de acesso que contenha as permissões apropriadas ou crie uma política usando o JSON fornecido pelo console:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "es.amazonaws.com"
      },
      "Action": [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Resource": "cw_log_group_arn:*"
    }
  ]
}
```

Recomendamos que você adicione as chaves de condição `aws:SourceAccount` e `aws:SourceArn` na política para se proteger contra o problema confused deputy. A conta de origem é o proprietário do domínio e o ARN de origem é o ARN do domínio. Para adicionar essas chaves de condição, o seu domínio deve estar no software de serviço R20211203 ou superior.

Por exemplo, você poderia adicionar o bloco de condições a seguir na política:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

Important

O CloudWatch Logs oferece suporte a 10 políticas baseadas em recurso por região. Se você planejar habilitar os logs para vários domínios do OpenSearch Service, crie e reutilize uma política mais abrangente que inclua vários grupos de logs para evitar atingir

esse limite. Para obter as etapas sobre como atualizar a política, consulte the section called “Habilitação da publicação de logs (AWS CLI)”.

7. Escolha Habilitar.

   O status de seu domínio muda de Active para Processing. O status deve retornar para Ativo antes que a publicação de logs seja habilitada. Essa alteração geralmente leva 30 minutos, mas pode demorar mais, dependendo da configuração do domínio.

Se você tiver habilitado um dos logs lentos, consulte the section called “Configuração dos limites de logs do OpenSearch para logs lentos”. Se você habilitou os logs de auditoria, consulte the section called “Etapa 2: ativar os registros de auditoria nos OpenSearch painéis”. Se tiver habilitado apenas logs de erros, você não precisará executar nenhuma etapa de configuração adicional.

Habilitação da publicação de logs (AWS CLI)

Antes de habilitar a publicação de logs, você precisa de um grupo de logs do CloudWatch. Se você ainda não tem, pode criar um usando o seguinte comando:

```
aws logs create-log-group --log-group-name my-log-group
```

Digite o comando seguinte para localizar o ARN do grupo de log e anote-o:

```
aws logs describe-log-groups --log-group-name my-log-group
```

Agora você pode conceder permissões ao OpenSearch Service para gravar o grupo de log. Você deve fornecer o ARN do grupo de log quase no final do comando:

```
aws logs put-resource-policy \
  --policy-name my-policy \
  --policy-document '{ "Version": "2012-10-17", "Statement": [{ "Sid": "",
 "Effect": "Allow", "Principal": { "Service": "es.amazonaws.com"}, "Action":
[ "logs:PutLogEvents","logs:CreateLogStream"],"Resource": "cw_log_group_arn:*"}]}'
```

> **Important**
>
> O CloudWatch Logs oferece suporte a 10 políticas baseadas em recurso por região. Se você planejar habilitar os logs lentos para vários domínios do OpenSearch Service, crie e reutilize uma política mais abrangente que inclua vários grupos de logs para evitar atingir esse limite.

Se você precisar revisar essa política posteriormente, use o comando `aws logs describe-resource-policies`. Para atualizar a política, emita o mesmo comando `aws logs put-resource-policy` com um novo documento de política.

Por fim, você pode usar a `--log-publishing-options` opção de habilitar a publicação. A sintaxe para essa opção é a mesma para os comandos `create-domain` e `update-domain-config`.

Parâmetro	Valores válidos
`--log-publishing-options`	`SEARCH_SLOW_LOGS={CloudWatchLogsLogGroupArn=` *`cw_log_group_arn`* `,Enabled=true|false}`
	`INDEX_SLOW_LOGS={CloudWatchLogsLogGroupArn=` *`cw_log_group_arn`* `,Enabled=true|false}`
	`ES_APPLICATION_LOGS={CloudWatchLogsLogGroupArn=` *`cw_log_group_arn`* `,Enabled=true|false}`
	`AUDIT_LOGS={CloudWatchLogsLogGroupArn=` *`cw_log_group_arn`* `,Enabled=true|false}`

> **Note**
>
> Se você planejar habilitar vários logs, recomendamos publicar cada um em seu próprio grupo de logs. Essa separação torna os logs mais fáceis de serem encontrados.

Exemplo

O exemplo a seguir habilita a publicação de pesquisa e logs lentos de indexação no domínio especificado:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --log-publishing-options
 "SEARCH_SLOW_LOGS={CloudWatchLogsLogGroupArn=arn:aws:logs:us-east-1:123456789012:log-group:my-log-
group,Enabled=true},INDEX_SLOW_LOGS={CloudWatchLogsLogGroupArn=arn:aws:logs:us-east-1:123456789012:log-group:my-other-log-group,Enabled=true}"
```

Para desabilitar a publicação no CloudWatch, execute o mesmo comando com `Enabled=false`.

Se você tiver habilitado um dos logs lentos, consulte the section called “Configuração dos limites de logs do OpenSearch para logs lentos”. Se você habilitou os logs de auditoria, consulte the section called “Etapa 2: ativar os registros de auditoria nos OpenSearch painéis”. Se tiver habilitado apenas logs de erros, você não precisará executar nenhuma etapa de configuração adicional.

Habilitação da publicação de logs (AWS SDKs)

Para poder habilitar a publicação de logs, você deve primeiro criar um grupo de logs do CloudWatch, obter seu ARN e fornecer ao OpenSearch Service permissões para gravar nele. As operações relevantes estão documentadas na Referência da API do Amazon CloudWatch Logs:

- `CreateLogGroup`
- `DescribeLogGroup`
- `PutResourcePolicy`

Você pode acessar essas operações usando os AWS SDKs.

Os SDKs da AWS (exceto os SDKs para Android e iOS) são compatíveis com todas as operações definidas na Amazon OpenSearch Service API Reference (Referência da API do Amazon OpenSearch Service), incluindo a opção `--log-publishing-options` para `CreateDomain` e `UpdateDomainConfig`.

Se você tiver habilitado um dos logs lentos, consulte the section called “Configuração dos limites de logs do OpenSearch para logs lentos”. Se tiver habilitado apenas logs de erros, você não precisará executar nenhuma etapa de configuração adicional.

Habilitação da publicação de logs (CloudFormation)

Neste exemplo, usamos o CloudFormation para criar um grupo de logs chamado `opensearch-logs`, atribuímos as permissões adequadas e criamos um domínio com a publicação de log habilitada para logs de aplicações, logs lentos de pesquisa e logs lentos de indexação.

Antes que você possa habilitar a publicação de logs, é necessário criar um grupo de logs do CloudWatch:

```
Resources:
  OpenSearchLogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: opensearch-logs
Outputs:
  Arn:
    Value:
      'Fn::GetAtt':
        - OpenSearchLogGroup
        - Arn
```

O modelo gera o ARN do grupo de logs. Neste caso, o ARN é `arn:aws:logs:us-east-1:123456789012:log-group:opensearch-logs`.

Usando o ARN, crie uma política de recursos que conceda ao OpenSearch Service permissões para gravar no grupo de logs:

```
Resources:
 OpenSearchLogPolicy:
   Type: AWS::Logs::ResourcePolicy
   Properties:
     PolicyName: my-policy
     PolicyDocument: "{ \"Version\": \"2012-10-17\", \"Statement\": [{ \"Sid\": \"\",
 \"Effect\": \"Allow\", \"Principal\": { \"Service\": \"es.amazonaws.com\"}, \"Action
\":[ \"logs:PutLogEvents\",\"logs:CreateLogStream\"],\"Resource\": \"arn:aws:logs:us-
east-1:123456789012:log-group:opensearch-logs:*\"}]}"
```

Por fim, crie a seguinte pilha CloudFormation, que gera um domínio OpenSearch Service com publicação de log. A política de acesso permite que o usuário do Conta da AWS faça todas as solicitações HTTP ao domínio.

```
Resources:
  OpenSearchServiceDomain:
    Type: "AWS::OpenSearchService::Domain"
    Properties:
      DomainName: my-domain
      EngineVersion: "OpenSearch_1.0"
      ClusterConfig:
        InstanceCount: 2
        InstanceType: "r6g.xlarge.search"
        DedicatedMasterEnabled: true
        DedicatedMasterCount: 3
        DedicatedMasterType: "r6g.xlarge.search"
      EBSOptions:
        EBSEnabled: true
        VolumeSize: 10
        VolumeType: "gp2"
      AccessPolicies:
        Version: "2012-10-17"
        Statement:
            Effect: "Allow"
            Principal:
                AWS: "arn:aws:iam::123456789012:user/es-user"
            Action: "es:*"
            Resource: "arn:aws:es:us-east-1:123456789012:domain/my-domain/*"
      LogPublishingOptions:
        ES_APPLICATION_LOGS:
          CloudWatchLogsLogGroupArn: "arn:aws:logs:us-east-1:123456789012:log-
group:opensearch-logs"
          Enabled: true
        SEARCH_SLOW_LOGS:
          CloudWatchLogsLogGroupArn: "arn:aws:logs:us-east-1:123456789012:log-
group:opensearch-logs"
          Enabled: true
        INDEX_SLOW_LOGS:
          CloudWatchLogsLogGroupArn: "arn:aws:logs:us-east-1:123456789012:log-
group:opensearch-logs"
          Enabled: true
```

Para obter informações detalhadas sobre sintaxe, consulte as opções de publicação de logs no Manual do usuário do AWS CloudFormation.

Configuração dos limites de logs do OpenSearch para logs lentos

O OpenSearch desabilita os logs lentos por padrão. Depois de habilitar a publicação de logs lentos para o CloudWatch, você ainda deve especificar os limites de log para cada índice do OpenSearch. Esses limites definem exatamente o que deve ser registrado e em que nível de log.

Você especifica essas configurações por meio da API REST do OpenSearch:

```
PUT domain-endpoint/index/_settings
{
  "index.search.slowlog.threshold.query.warn": "5s",
  "index.search.slowlog.threshold.query.info": "2s"
}
```

Para testar se os logs lentos estão sendo publicados com êxito, comece com valores bem baixos para verificar se os logs aparecem no CloudWatch e, em seguida, aumente os limites para níveis mais úteis.

Se os logs não aparecerem, verifique o seguinte:

- O grupo de log do CloudWatch existe? Verifique o console do CloudWatch.
- O OpenSearch Service tem permissões para gravar no grupo de log? Verifique o console do OpenSearch Service.
- O domínio do OpenSearch Service está configurado para publicar no grupo de logs? Verifique o console do OpenSearch Service use a opção `describe-domain-config` da AWS CLI ou chame `DescribeDomainConfig` usando um dos SDKs.
- Os limites de log do OpenSearch são baixos a ponto de suas solicitações excedê-los? Para revisar seus limites para um índice, use o seguinte comando:

  ```
  GET domain-endpoint/index/_settings?pretty
  ```

Se você quer desabilitar logs lentos para um índice, redefina todos os limites que você mudou para os valores padrão de `-1`.

Desabilitar a publicação para o CloudWatch usando o console do OpenSearch Service ou a AWS CLI não impede que o OpenSearch Service gere logs, apenas interrompe a publicação desses logs. Verifique as configurações de índice se você não precisar mais de logs lentos.

Visualizar logs do

Visualizar a aplicação e os logs lentos no CloudWatch é igual a qualquer outra visualização de log do CloudWatch. Para obter mais informações, consulte Visualizar dados de log no Manual do usuário do Amazon CloudWatch Logs.

Algumas considerações sobre a visualização de logs:

- O OpenSearch Service publica apenas os primeiros 255.000 caracteres de cada linha no CloudWatch. O conteúdo restante ficará truncado. Para logs de auditoria, o limite é de 10.000 caracteres por mensagem.
- No CloudWatch, os nomes dos fluxos de log têm os sufixos `-index-slow-logs`, `-search-slow-logs`, `-application-logs` e `-audit-logs` para ajudar a identificar seu conteúdo.

Monitorando registros de auditoria no Amazon OpenSearch Service

Se o seu domínio do Amazon OpenSearch Service usa controle de acesso refinado, você pode habilitar registros de auditoria para seus dados. Os registros de auditoria são altamente personalizáveis e permitem que você acompanhe a atividade do usuário em seus OpenSearch clusters, incluindo sucesso e falhas de autenticação, solicitações OpenSearch, alterações de índice e consultas de pesquisa recebidas. A configuração padrão monitora um conjunto popular de ações do usuário, mas recomendamos adaptar as configurações às suas necessidades exatas.

Assim como os registros de OpenSearch aplicativos e os registros lentos, o OpenSearch Service publica registros de auditoria no CloudWatch Logs. Se ativado, o CloudWatch preço padrão se aplica.

> **Note**
>
> Para ativar os registros de auditoria, sua função de usuário deve ser mapeada para a `security_manager` função, o que lhe dá acesso à API OpenSearch `plugins/_security` REST. Para saber mais, consulte the section called “Modificação do usuário primário”.

Tópicos

- Limitações
- Habilitação dos logs de auditoria

- Ative o registro de auditoria usando o AWS CLI
- Habilitar o registro de auditoria em log usando a API de configuração
- Camadas e categorias do log de auditoria
- Configurações do log de auditoria
- Exemplo de log de auditoria
- Configuração de logs de auditoria usando a API REST

Limitações

Os logs de auditoria têm as seguintes limitações:

- Os logs de auditoria não incluem solicitações de pesquisa entre clusters que foram rejeitadas pela política de acesso ao domínio do destino.
- O tamanho máximo de cada mensagem do log de auditoria é 10.000 caracteres. A mensagem do log de auditoria será truncada se exceder esse limite.

Habilitação dos logs de auditoria

A habilitação dos logs de auditoria é um processo em duas etapas. Primeiro, você configura seu domínio para publicar registros de auditoria no CloudWatch Logs. Em seguida, você ativa os registros de auditoria nos OpenSearch painéis e os configura para atender às suas necessidades.

> **Important**
>
> Se você encontrar um erro ao seguir essas etapas, consulte the section called “Não é possível habilitar logs de auditoria” para obter informações de solução de problemas.

Etapa 1: ativar registros de log e configurar uma política de acesso

Estas etapas descrevem como habilitar logs de auditoria usando o console. Você também pode habilitá-los usando o AWS CLI, ou a API OpenSearch de serviço.

Para habilitar registros de auditoria para um domínio OpenSearch de serviço (console)

1. Escolha o domínio para abrir sua configuração e, em seguida, acesse a guia Logs.

2. Selecione Logs de auditoria e, em seguida, Habilitar.
3. Crie um grupo de CloudWatch registros ou escolha um existente.
4. Escolha uma política de acesso que contenha as permissões apropriadas ou crie uma política usando o JSON fornecido pelo console:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "es.amazonaws.com"
      },
      "Action": [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Resource": "cw_log_group_arn"
    }
  ]
}
```

Recomendamos que você adicione as chaves de condição `aws:SourceAccount` e `aws:SourceArn` na política para se proteger contra o problema confused deputy. A conta de origem é o proprietário do domínio e o ARN de origem é o ARN do domínio. Para adicionar essas chaves de condição, o seu domínio deve estar no software de serviço R20211203 ou superior.

Por exemplo, você poderia adicionar o bloco de condições a seguir na política:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

5. Escolha Habilitar.

Etapa 2: ativar os registros de auditoria nos OpenSearch painéis

Depois de habilitar os registros de auditoria no console de OpenSearch serviços, você também deve habilitá-los nos OpenSearch painéis e configurá-los para atender às suas necessidades.

1. Abra OpenSearch Painéis e escolha Segurança no menu do lado esquerdo.
2. Escolha Logs de auditoria.
3. Escolha Habilitar log de auditoria.

A interface do usuário do Dashboars oferece controle total das configurações do log de auditoria emConfigurações gerais e Configurações de compatibilidade. Para obter uma descrição de todas as opções de configuração, consulte Configurações de log de auditoria.

Ative o registro de auditoria usando o AWS CLI

O AWS CLI comando a seguir ativa registros de auditoria em um domínio existente:

```
aws opensearch update-domain-config --domain-name my-domain --log-publishing-options
 "AUDIT_LOGS={CloudWatchLogsLogGroupArn=arn:aws:logs:us-east-1:123456789012:log-
group:my-log-group,Enabled=true}"
```

Você também pode habilitar os logs de auditoria ao criar um domínio. Para obter mais informações, consulte a Referência de comandos daAWS CLI.

Habilitar o registro de auditoria em log usando a API de configuração

A seguinte solicitação para a API de configuração habilita os logs de auditoria em um domínio existente:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/config
{
  "LogPublishingOptions": {
    "AUDIT_LOGS": {
      "CloudWatchLogsLogGroupArn":"arn:aws:logs:us-east-1:123456789012:log-
group1:sample-domain",
      "Enabled":true
    }
  }
```

```
}
```

Para obter mais informações, consulte a referência da Amazon OpenSearch Service API.

Camadas e categorias do log de auditoria

A comunicação do cluster ocorre em duas camadas separadas: a camada REST e a camada de transporte.

- A camada REST abrange a comunicação com clientes HTTP, como curl, Logstash, OpenSearch Dashboards, o cliente REST de alto nível Java, a biblioteca Python Requests — todas as solicitações HTTP que chegam ao cluster.
- A camada de transporte cobre a comunicação entre nós. Por exemplo, depois que uma solicitação de pesquisa chega ao cluster (sobre a camada REST), o nó de coordenação que atende à solicitação envia a consulta para outros nós, recebe suas respostas, coleta os documentos necessários e os reúne na resposta final. Operações como alocação de fragmentos e rebalanceamento também ocorrem sobre a camada de transporte.

Você pode habilitar ou desabilitar logs de auditoria para camadas inteiras, bem como categorias de auditoria individuais para uma camada. A tabela a seguir contém um resumo das categorias de auditoria e das camadas para as quais elas estão disponíveis.

Categoria	Descrição	Disponível para REST	Disponível para transporte
FAILED_LOGIN	Uma solicitação continha credenciais inválidas, e a autenticação falhou.	Sim	Sim
MISSING_PRIVILEGES	Um usuário não tinha os privilégios necessários para fazer a solicitação.	Sim	Sim
GRANTED_PRIVILEGES	Um usuário tinha os privilégios necessários para fazer a solicitação.	Sim	Sim

Categoria	Descrição	Disponível para REST	Disponível para transporte
OPENSEARCH_SECURITY_INDEX_ATTEMPT	Uma solicitação tentou modificar o índice `.opendistro_security` .	Não	Sim
AUTHENTICATED	Uma solicitação continha credenciais válidas e a autenticação foi bem-sucedida.	Sim	Sim
INDEX_EVENT	Uma solicitação executou uma operação administrativa em um índice, como criar um, definir um alias ou executar uma mesclagem forçada. A lista completa de `indices:admin/` ações que essa categoria inclui está disponível na OpenSearch documentação.	Não	Sim

Além dessas categorias padrão, o controle de acesso refinado oferece várias categorias adicionais projetadas para atender aos requisitos de conformidade de dados.

Categoria	Descrição
COMPLIANCE_DOC_READ	Uma solicitação executou um evento de leitura em um documento em um índice.

Categoria	Descrição
COMPLIANCE_DOC_WRITE	Uma solicitação executou um evento de gravação em um documento em um índice.
COMPLIANCE_INTERNAL_CONFIG_READ	Uma solicitação executou um evento de leitura no índice `.opendistro_security` .
COMPLIANCE_INTERNAL_CONFIG_WRITE	Uma solicitação executou um evento de gravação no índice `.opendistro_security` .

Você pode ter qualquer combinação de categorias e atributos de mensagem. Por exemplo, se você enviar uma solicitação REST para indexar um documento, poderá ver as seguintes linhas nos logs de auditoria:

- AUTHENTICATED na camada REST (autenticação)
- GRANTED_PRIVILEGE na camada de transporte (autorização)
- COMPLIANCE_DOC_WRITE (documento gravado em um índice)

Configurações do log de auditoria

Há várias opções de configuração para os logs de auditoria.

Configurações gerais

As configurações gerais permitem habilitar ou desabilitar categorias individuais ou camadas inteiras. Recomendamos enfaticamente manter GRANTED_PRIVILEGES e AUTHENTICATED como categorias excluídas. Caso contrário, essas categorias serão registradas para cada solicitação válida para o cluster.

Nome	Configuração de backend	Descrição
Camada REST	enable_rest	Habilite ou desabilite eventos que ocorrem na camada REST.

Nome	Configuração de backend	Descrição
Categorias desabilitadas de REST	disabled_rest_categories	Especifique categorias de auditoria a serem ignoradas na camada REST. Modificar essas categorias pode aumentar drasticamente o tamanho dos logs de auditoria.
Transport Layer	enable_transport	Habilite ou desabilite eventos que acontecem na camada de transporte.
Categorias desabilitadas de transporte	disabled_transport_categories	Especifique categorias de auditoria que devem ser ignoradas na camada de transporte. Modificar essas categorias pode aumentar drasticamente o tamanho dos logs de auditoria.

As configurações de atributo permitem personalizar a quantidade de detalhes em cada linha de log.

Nome	Configuração de backend	Descrição
Solicitações em massa	resolve_bulk_requests	Habilitar essa configuração gera um log para cada documento em uma solicitação em massa, o que pode aumentar drasticamente o tamanho dos logs de auditoria.
Corpo da solicitação	log_request_body	Inclua o corpo da solicitação das solicitações.
Resolver índices	resolve_índices	Resolva aliases em índices.

Use as configurações de ignorar para excluir um conjunto de usuários ou caminhos de API:

Nome	Configuração de backend	Descrição
Usuários ignorados	ignore_users	Especifique os usuários que não deseja incluir.
Solicitações ignoradas	ignore_requests	Especifique padrões de solicitação que não deseja incluir.

Configurações de conformidade

As configurações de conformidade permitem ajustar o acesso ao índice, ao documento ou ao nível de campo.

Nome	Configuração de backend	Descrição
Log de compatibilidade	enable_compliance	Habilite ou desabilite o log de compatibilidade

Você pode especificar as configurações a seguir para o log de eventos de leitura e gravação.

Nome	Configuração de backend	Descrição
Log de configuração interno	internal_config	Habilite ou desabilite o log de eventos no índice `.opendistro_security` .

Você pode especificar as configurações a seguir para eventos de leitura.

Nome	Configuração de backend	Descrição
Ler metadados	read_metadata_only	Incluir apenas metadados para eventos de leitura. Não inclua campos de documento.
Usuários ignorados	read_ignore_users	Não inclua determinados usuários para eventos de leitura.
Campos observados	read_watched_fields	Especifique os índices e campos a serem observados para eventos de leitura. A adição de campos observados gera um log por acesso ao documento, o que pode aumentar drasticamente o tamanho dos logs de auditoria. Os campos observados oferecem suporte a padrões de índice e padrões de campo: `{ "index-name-pattern": [ "field-name-pattern" ], "logs*": [ "message" ], "twitter": [ "id", "user*" ] }`

Você pode especificar as configurações a seguir para eventos de gravação.

Nome	Configuração de backend	Descrição
Metadados de gravação	write_metadata_only	Inclua metadados somente para eventos de gravação. Não inclua campos de documento.

Nome	Configuração de backend	Descrição
Diferenças de log	write_log_diffs	Se write_metadata_only for false (falso), inclua somente as diferenças entre eventos de gravação.
Usuários ignorados	write_ignore_users	Não inclua determinados usuários para eventos de gravação.
Observar índices	write_watched_índices	Especifique os índices ou padrões de índice para observar eventos de gravação. A adição de campos observados gera um log por acesso ao documento, o que pode aumentar drasticamente o tamanho dos logs de auditoria.

Exemplo de log de auditoria

Esta seção inclui um exemplo de configuração, solicitação de pesquisa e o log de auditoria resultante para todos os eventos de leitura e gravação de um índice.

Etapa 1: Configurar logs de auditoria

Depois de habilitar a publicação de registros de auditoria em um grupo de CloudWatch registros, navegue até a página de registro de auditoria de OpenSearch painéis e escolha Habilitar registro de auditoria.

1. Em Configurações gerais, escolha Configurar e certifique-se de que a opção Camada REST esteja habilitada.
2. Em Configurações de compatibilidade, escolha Configurar.
3. Em Gravação, em Campos observados, adicione `accounts` para todos os eventos de gravação neste índice.
4. Em Leitura, na seção Campos observados, adicione os campos `ssn` e `id-` do índice `accounts`:

```
{
  "accounts-": [
    "ssn",
    "id-"
  ]
}
```

Etapa 2: Executar eventos de leitura e gravação

1. Navegue até OpenSearch Painéis, escolha Dev Tools e indexe um documento de amostra:

```
PUT accounts/_doc/0
{
  "ssn": "123",
  "id-": "456"
}
```

2. Para testar um evento de leitura, envie a seguinte solicitação:

```
GET accounts/_search
{
  "query": {
    "match_all": {}
  }
}
```

Etapa 3: Observar os logs

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Grupos de logs.
3. Escolha o grupo de logs que você especificou ao habilitar os logs de auditoria. Dentro do grupo de registros, o OpenSearch Service cria um fluxo de registros para cada nó em seu domínio.
4. Em Fluxos de log, escolha Pesquisar tudo.
5. Para os eventos de leitura e gravação, consulte os logs correspondentes. Um atraso de 5 segundos antes do log ser exibido é normal.

   Exemplo de gravação de log de auditoria

```
{
  "audit_compliance_operation": "CREATE",
  "audit_cluster_name": "824471164578:audit-test",
  "audit_node_name": "be217225a0b77c2bd76147d3ed3ff83c",
  "audit_category": "COMPLIANCE_DOC_WRITE",
  "audit_request_origin": "REST",
  "audit_compliance_doc_version": 1,
  "audit_node_id": "3xNJhm4XS_yTzEgDWcGRjA",
```

```
  "@timestamp": "2020-08-23T05:28:02.285+00:00",
  "audit_format_version": 4,
  "audit_request_remote_address": "3.236.145.227",
  "audit_trace_doc_id": "lxnJGXQBqZSlDB91r_uZ",
  "audit_request_effective_user": "admin",
  "audit_trace_shard_id": 8,
  "audit_trace_indices": [
    "accounts"
  ],
  "audit_trace_resolved_indices": [
    "accounts"
  ]
}
```

Exemplo de leitura de log de auditoria

```
{
  "audit_cluster_name": "824471164578:audit-docs",
  "audit_node_name": "806f6050cb45437e2401b07534a1452f",
  "audit_category": "COMPLIANCE_DOC_READ",
  "audit_request_origin": "REST",
  "audit_node_id": "saSevm9ASte0-pjAtYi2UA",
  "@timestamp": "2020-08-31T17:57:05.015+00:00",
  "audit_format_version": 4,
  "audit_request_remote_address": "54.240.197.228",
  "audit_trace_doc_id": "config:7.7.0",
  "audit_request_effective_user": "admin",
  "audit_trace_shard_id": 0,
  "audit_trace_indices": [
    "accounts"
  ],
  "audit_trace_resolved_indices": [
    "accounts"
  ]
}
```

Para incluir o corpo da solicitação, retorne às configurações de conformidade nos OpenSearch painéis e desative a opção Gravar metadados. Para excluir eventos por um usuário específico, adicione o usuário a Usuários Ignorados.

Para obter uma descrição de cada campo do log de auditoria, consulte Referência de campos do log de auditoria. Para obter informações sobre como pesquisar e analisar seus dados de registro de auditoria, consulte Análise de dados de log com o CloudWatch Logs Insights no Guia do usuário do Amazon CloudWatch Logs.

Configuração de logs de auditoria usando a API REST

Recomendamos o uso de OpenSearch painéis para configurar registros de auditoria, mas você também pode usar a API REST de controle de acesso refinada. Esta seção contém uma solicitação de exemplo. A documentação completa sobre a API REST está disponível na OpenSearchdocumentação.

```
PUT _plugins/_security/api/audit/config
{
  "enabled": true,
  "audit": {
    "enable_rest": true,
    "disabled_rest_categories": [
      "GRANTED_PRIVILEGES",
      "AUTHENTICATED"
    ],
    "enable_transport": true,
    "disabled_transport_categories": [
      "GRANTED_PRIVILEGES",
      "AUTHENTICATED"
    ],
    "resolve_bulk_requests": true,
    "log_request_body": true,
    "resolve_indices": true,
    "exclude_sensitive_headers": true,
    "ignore_users": [
      "kibanaserver"
    ],
    "ignore_requests": [
      "SearchRequest",
      "indices:data/read/*",
      "/_cluster/health"
    ]
  },
  "compliance": {
    "enabled": true,
    "internal_config": true,
```

```
    "external_config": false,
    "read_metadata_only": true,
    "read_watched_fields": {
      "read-index-1": [
        "field-1",
        "field-2"
      ],
      "read-index-2": [
        "field-3"
      ]
    },
    "read_ignore_users": [
      "read-ignore-1"
    ],
    "write_metadata_only": true,
    "write_log_diffs": false,
    "write_watched_indices": [
      "write-index-1",
      "write-index-2",
      "log-*",
      "*"
    ],
    "write_ignore_users": [
      "write-ignore-1"
    ]
  }
}
```

Eventos do OpenSearch Serviço de Monitoramento com a Amazon EventBridge

O Amazon OpenSearch Service se integra EventBridge à Amazon para notificá-lo sobre determinados eventos que afetam seus domínios. Os eventos dos AWS serviços são entregues quase EventBridge em tempo real. Os mesmos eventos também são enviados para a Amazon CloudWatch Events, a antecessora da Amazon EventBridge. Você pode escrever regras simples para indicar quais eventos são do seu interesse, e as ações automatizadas a serem tomadas quando um evento corresponder à regra. Ações que podem ser automaticamente acionadas incluem:

- Invocando uma função AWS Lambda
- Invocação de um Run Command do Amazon EC2

- Transmitir o evento Amazon Kinesis Data Streams
- Ativando uma máquina de estado AWS Step Functions
- Notificar um tópico do Amazon SNS ou uma fila do Amazon SQS

Para obter mais informações, consulte Comece a usar a Amazon EventBridge no Guia EventBridge do usuário da Amazon.

Tópicos

Eventos de atualização de software de serviço

OpenSearch O serviço envia eventos para EventBridge quando ocorre um dos seguintes eventos de atualização do software de serviço.

Atualização do software de serviço disponível

OpenSearch O serviço envia esse evento quando uma atualização do software do serviço está disponível.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
```

```
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Available",
    "severity": "Informational",
    "description": "Service software update R20220928 available. Service Software
 Deployment Mechanism:
                   Blue/Green. For more information on deployment configuration,
 please
                   see: https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/managedomains-configuration-changes.html"
  }
}
```

Atualização de software de serviço agendada

OpenSearch O serviço envia esse evento quando uma atualização do software do serviço é agendada. Para atualizações opcionais, você recebe a notificação na data agendada e tem a opção de reagendar a qualquer momento. Para as atualizações obrigatórias, você recebe a notificação três dias antes da data agendada e tem a opção de reagendar dentro da janela obrigatória.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Scheduled",
    "severity": "High",
    "description": "A new service software update [R20200330-p1] has been scheduled at
 [21st May 2023 12:40 GMT].
```

```
                    Please see documentation for more information on scheduling
 software updates:
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/service-software.html."
  }
}
```

Atualização do software de serviço reagendada

OpenSearch O serviço envia esse evento quando uma atualização opcional do software do serviço é reagendada. Para ter mais informações, consulte the section called “Atualizações opcionais x obrigatórias”.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Rescheduled",
    "severity": "High",
    "description": "The service software update [R20200330-p1], which was originally
 scheduled for
                    [21st May 2023 12:40 GMT], has been rescheduled to [23rd May 2023
 12:40 GMT].
                    Please see documentation for more information on scheduling
 software updates:
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/service-software.html."
  }
}
```

Atualização do software de serviço iniciada

OpenSearch O serviço envia esse evento quando uma atualização do software do serviço é iniciada.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Started",
    "severity": "Informational",
    "description": "Service software update [R20200330-p1] started.
  }
}
```

Atualização do software de serviço concluída

OpenSearch O serviço envia esse evento quando uma atualização do software do serviço é concluída.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
```

```
  "detail": {
    "event": "Service Software Update",
    "status": "Completed",
    "severity": "Informational",
    "description": "Service software update [R20200330-p1] completed."
  }
}
```

Atualização de software de serviço cancelada

OpenSearch O serviço envia esse evento quando uma atualização do software do serviço é cancelada.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Cancelled",
    "severity": "Informational",
    "description": "The scheduled service software update [R20200330-p1] has been
 cancelled as a
                    newer update is available. Please schedule the latest update."
  }
}
```

Atualização do software de serviço agendada cancelada

OpenSearch O serviço envia esse evento quando uma atualização do software do serviço que estava agendada anteriormente para o domínio é cancelada.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Cancelled",
    "severity": "Informational",
    "description": "The scheduled service software update [R20200330-p1] has been
 cancelled."
  }
}
```

Atualização de software de serviço não executada

OpenSearch O serviço envia esse evento quando não consegue iniciar uma atualização do software do serviço.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Unexecuted",
    "severity": "Informational",
```

```
    "description": "The scheduled service software update [R20200330-p1] cannot be
 started. Reason: [reason]"
  }
}
```

Falha na atualização do software de serviço

OpenSearch O serviço envia esse evento quando uma atualização do software do serviço falha.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Failed",
    "severity": "High",
    "description": "Installation of service software update [R20200330-p1] failed.
 [reason].
  }
}
```

Atualização do software de serviço necessária

OpenSearch O serviço envia esse evento quando é necessária uma atualização do software do serviço. Para ter mais informações, consulte the section called “Atualizações opcionais x obrigatórias”.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
```

```
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Required",
    "severity": "High",
    "description": "Service software update [R20200330-p1] available. Update
                    will be automatically installed after [21st May 2023] if no
                    action is taken. Service Software Deployment Mechanism: Blue/Green.
                    For more information on deployment configuration, please see:
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/managedomains-configuration-changes.html"
  }
}
```

Auto-Tune de eventos

OpenSearch O serviço envia eventos para EventBridge quando um dos seguintes eventos de ajuste automático ocorrer.

Auto-Tune pendente

OpenSearch O serviço envia esse evento quando o Auto-Tune identifica recomendações de ajuste para melhorar o desempenho e a disponibilidade do cluster. Você verá esse evento somente para domínios com o Auto-Tune desabilitado.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
```

```
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Pending",
    "description": "Auto-Tune recommends the following new settings for your
 domain: { JVM Heap size : 60%}. Enable Auto-Tune to improve cluster stability and
 performance.",
    "scheduleTime": "{iso8601-timestamp}"
  }
}
```

Auto-Tune iniciado

OpenSearch O serviço envia esse evento quando o Auto-Tune começa a aplicar novas configurações ao seu domínio.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Started",
    "scheduleTime": "{iso8601-timestamp}",
    "startTime": "{iso8601-timestamp}",
    "description" : "Auto-Tune is applying the following settings to your domain: { JVM
 Heap size : 60%}."
  }
}
```

O Auto-Tune requer uma implantação azul/verde agendada

OpenSearch O serviço envia esse evento quando o Auto-Tune identifica recomendações de ajuste que exigem uma implantação programada em azul/verde.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Low",
    "status": "Pending",
    "startTime": "{iso8601-timestamp}",
    "description": "Auto-Tune has identified the following settings for your domain
 that require a blue/green deployment: { JVM Heap size : 60%}.
                    You can schedule the deployment for your preferred time."
  }
}
```

Auto-Tune cancelado

OpenSearch O serviço envia esse evento quando a programação do Auto-Tune é cancelada porque não há recomendações de ajuste pendentes.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
```

```
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Low",
    "status": "Cancelled",
    "scheduleTime": "{iso8601-timestamp}",
    "description": "Auto-Tune has cancelled the upcoming blue/green deployment."
  }
}
```

Auto-Tune concluído

OpenSearch O serviço envia esse evento quando o Auto-Tune conclui a implantação azul/verde e o cluster está operacional com as novas configurações de JVM em vigor.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Completed",
    "completionTime": "{iso8601-timestamp}",
    "description": "Auto-Tune has completed the blue/green deployment and successfully
 applied the following settings: { JVM Heap size : 60%}."
  }
}
```

Auto-Tune desabilitado e alterações revertidas

OpenSearch O serviço envia esse evento quando o Auto-Tune é desativado e as alterações aplicadas são revertidas.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": [ "arn:aws:es:us-east-1:123456789012:domain/test-domain" ],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Completed",
    "description": "Auto-Tune is now disabled. All settings have been reverted. Auto-
Tune will continue to evaluate
                    cluster performance and provide recommendations.",
    "completionTime": "{iso8601-timestamp}"
  }
}
```

Auto-Tune desabilitado e alterações mantidas

OpenSearch O serviço envia esse evento quando o Auto-Tune é desativado e as alterações aplicadas são mantidas.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
```

```
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Completed",
    "description": "Auto-Tune is now disabled. The most-recent settings by Auto-Tune
 have been retained.
                   Auto-Tune will continue to evaluate cluster performance and provide
 recommendations.",
    "completionTime": "{iso8601-timestamp}"
  }
}
```

Eventos de integridade do cluster

OpenSearch O serviço envia determinados eventos para EventBridge quando a integridade do seu cluster está comprometida.

Recuperação de cluster vermelho iniciada

OpenSearch O serviço envia esse evento após o status do cluster ficar vermelho continuamente por mais de uma hora. Tenta restaurar automaticamente um ou mais índices vermelhos de um snapshot para corrigir o status do cluster.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
```

```
   ],
   "detail":{
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Started",
      "severity":"High",
      "description":"Your cluster status is red. We have started automatic snapshot
 restore for the red indices.
                    No action is needed from your side. Red indices [red-index-0, red-
index-1]"
   }
}
```

Recuperação de cluster vermelho parcialmente concluída

OpenSearch O serviço envia esse evento quando só conseguiu restaurar um subconjunto de índices vermelhos de um snapshot ao tentar corrigir o status de um cluster vermelho.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Partially Restored",
      "severity":"High",
      "description":"Your cluster status is red. We were able to restore the following
 Red indices from
                   snapshot: [red-index-0]. Indices not restored: [red-index-1].
 Please refer https://docs.aws.amazon.com/opensearch-service/latest/developerguide/
handling-errors.html#handling-errors-red-cluster-status for troubleshooting steps."
   }
}
```

Falha na recuperação de cluster vermelho

OpenSearch O serviço envia esse evento quando não consegue restaurar nenhum índice ao tentar corrigir o status de um cluster vermelho.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Failed",
      "severity":"High",
      "description":"Your cluster status is red. We were unable to restore the Red
 indices automatically.
                    Indices not restored: [red-index-0, red-index-1]. Please refer
 https://docs.aws.amazon.com/opensearch-service/latest/developerguide/handling-
errors.html#handling-errors-red-cluster-status for troubleshooting steps."
   }
}
```

Fragmentos a serem excluídos

OpenSearch O serviço envia esse evento quando tenta corrigir automaticamente o status do cluster vermelho depois de ficar vermelho continuamente por 14 dias, mas um ou mais índices permanecem vermelhos. Depois de mais 7 dias (21 dias no total em vermelho contínuo), o OpenSearch Serviço continua excluindo fragmentos não atribuídos em todos os índices vermelhos.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2022-04-09T10:36:48Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "severity":"Medium",
      "description":"Your cluster status is red. Please fix the red indices as soon as
 possible.
                    If not fixed by 2022-04-12 01:51:47+00:00, we will delete all
 unassigned shards,
                    the unit of storage and compute, for these red indices to recover
 your domain and make it green.
                    Please refer to https://docs.aws.amazon.com/opensearch-service/
latest/developerguide/handling-errors.html#handling-errors-red-cluster-status for
 troubleshooting steps.
                    test_data, test_data1",
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Shard(s) to be deleted"
   }
}
```

Fragmentos excluídos

OpenSearch O serviço envia esse evento após o status do cluster ficar vermelho continuamente por 21 dias. Continua excluindo os fragmentos não atribuídos (armazenamento e computação) em todos os índices vermelhos. Para obter detalhes, consulte the section called “Correção automática de clusters vermelhos”.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
```

```
   "source":"aws.es",
   "account":"123456789012",
   "time":"2022-04-09T10:54:48Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "severity":"High",
      "description":"We have deleted unassinged shards, the unit of storage and
 compute, in
                    red indices: index-1, index-2 because these indices were red for
 more than
                    21 days and could not be restored with the automated restore
 process.
                    Please refer to https://docs.aws.amazon.com/opensearch-service/
latest/developerguide/handling-errors.html#handling-errors-red-cluster-status for
 troubleshooting steps.",
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Shard(s) deleted"
   }
}
```

Aviso de alta contagem de fragmentos

OpenSearch O serviço envia esse evento quando a contagem média de fragmentos em seus nós de dados ativos excede 90% do limite padrão recomendado de 1.000. Embora as versões posteriores do Elasticsearch OpenSearch suportem um limite máximo configurável de fragmentos por nó, recomendamos que você não tenha mais do que 1.000 fragmentos por nó. Consulte Como escolher o número de fragmentos.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2016-11-01T13:12:22Z",
  "region":"us-east-1",
```

```
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"High Shard Count",
     "status":"Warning",
     "severity":"Low",
     "description":"One or more data nodes have close to 1000 shards. To ensure optimum
 performance and stability of your
                   cluster, please refer to the best practice guidelines - https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/sizing-domains.html#bp-
sharding."
  }
}
```

Limite de contagem de fragmentos excedido

OpenSearch O serviço envia esse evento quando a contagem média de fragmentos em seus nós de dados ativos excede o limite padrão recomendado de 1.000. Embora as versões posteriores do Elasticsearch OpenSearch suportem um limite máximo configurável de fragmentos por nó, recomendamos que você não tenha mais do que 1.000 fragmentos por nó. Consulte Como escolher o número de fragmentos.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2016-11-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"High Shard Count",
     "status":"Warning",
     "severity":"Medium",
     "description":"One or more data nodes have more than 1000 shards. To ensure
 optimum performance and stability of your
                   cluster, please refer to the best practice guidelines - https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/sizing-domains.html#bp-
sharding."
```

```
  }
}
```

Pouco espaço em disco

OpenSearch O serviço envia esse evento quando um ou mais nós em seu cluster têm menos de 25% do espaço de armazenamento disponível ou menos de 25 GB.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Low Disk Space",
     "status":"Warning",
     "severity":"Medium",
     "description":"One or more data nodes in your cluster has less than 25% of storage
 space or less than 25GB.
                  Your cluster will be blocked for writes at 20% or 20GB. Please refer
 to the documentation for more information - https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/handling-errors.html#troubleshooting-cluster-block"
  }
}
```

Violação de marca d'água de baixo disco

OpenSearch O serviço envia esse evento quando todos os nós em seu cluster têm menos de 10% do espaço de armazenamento disponível ou menos de 10 GB. Quando todos os nós violarem a marca d’água de disco embaixo, qualquer novo índice resultará em um cluster amarelo e, quando todos os nós ficarem abaixo da marca d'água do disco no alto, resultará em um cluster vermelho.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Low Disk Watermark Breach",
     "status":"Warning",
     "severity":"Medium",
     "description":"Low Disk Watermark threshold is about to be breached. Once the
 threshold is breached, new index creation will be blocked on all
                    nodes to prevent the cluster status from turning red. Please
 increase disk size to suit your storage needs. For more information,
                    see https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/handling-errors.html#troubleshooting-cluster-block".
  }
}
```

Saldo de intermitência do EBS abaixo de 70%

OpenSearch O serviço envia esse evento quando o saldo de estouro do EBS em um ou mais nós de dados fica abaixo de 70%. O esgotamento do saldo de intermitência do EBS pode causar indisponibilidade generalizada do cluster e do controle de utilização de solicitações de E/S, o que pode levar a altas latências e tempos limites em solicitações de indexação e pesquisa. Para obter as etapas de correção para esse problema, consulte the section called “O saldo de intermitência do EBS está baixo”.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
```

```
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"EBS Burst Balance",
     "status":"Warning",
     "severity":"Medium",
     "description":"EBS burst balance on one or more data nodes is below 70%.
                    Follow https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/handling-errors.html#handling-errors-low-ebs-burst
                    to fix this issue."
  }
}
```

Saldo de intermitência do EBS abaixo de 20%

OpenSearch O serviço envia esse evento quando o saldo de estouro do EBS em um ou mais nós de dados fica abaixo de 20%. O esgotamento do saldo de intermitência do EBS pode causar indisponibilidade generalizada do cluster e do controle de utilização de solicitações de E/S, o que pode levar a altas latências e tempos limites em solicitações de indexação e pesquisa. Para obter as etapas de correção para esse problema, consulte the section called “O saldo de intermitência do EBS está baixo”.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"EBS Burst Balance",
     "status":"Warning",
     "severity":"High",
     "description":"EBS burst balance on one or more data nodes is below 20%.
                    Follow https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/handling-errors.html#handling-errors-low-ebs-burst
```

```
                    to fix this issue.
  }
}
```

Controle de utilização do throughput do disco

OpenSearch O serviço envia esse evento quando as solicitações de leitura e gravação para seu domínio estão sendo limitadas devido às limitações de taxa de transferência dos volumes do EBS ou da instância EC2. Se você receber essa notificação, considere escalar seus volumes ou instâncias seguindo as melhores práticas AWS recomendadas. Se o seu tipo de volume for gp2, aumente o tamanho do volume. Se o seu tipo de volume for gp3, forneça mais throughput. Você também pode verificar se a base da instância e a taxa máxima de throughput do EBS são maiores ou iguais à taxa de throughput do volume provisionado e se pode aumentar a escala verticalmente.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Disk Throughput Throttle",
     "status":"Warning",
     "severity":"Medium",
     "description":"Your domain is experiencing throttling due to instance or volume
 throughput limitations.
                    Please consider scaling your domain to suit your throughput needs.
 In July 2023, we improved
                    the accuracy of throughput throttle calculation by replacing ‘Max
 volume throughput’ with
                    ‘Provisioned volume throughput’. Please refer to the documentation
 for more information."
   }
}
```

Tamanho de fragmento grande

OpenSearch O serviço envia esse evento quando um ou mais fragmentos em seu cluster excedem 50 GiB ou 65 GiB. Para garantir o desempenho e a estabilidade ideais do cluster, reduza o tamanho dos fragmentos.

Para obter mais informações, consulte as melhores práticas de fragmentação.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Large Shard Size",
     "status":"Warning",
     "severity":"Medium",
     "description":"One or more shards are larger than 65GiB. To ensure optimum cluster
 performance and stability, reduce shard sizes.
                    For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-large-shard-
size."
  }
}
```

Uso elevado do JVM

OpenSearch O serviço envia esse evento quando a `JVMMemoryPressure` métrica do seu domínio ultrapassa 80%. Se exceder 92% por 30 minutos, todas as operações de gravação em seu cluster serão bloqueadas. Para garantir a estabilidade ideal do cluster, reduza o tráfego para o cluster ou escale seu domínio para fornecer memória suficiente para sua workload.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"High JVM Usage",
     "status":"Warning",
     "severity":"High",
     "description":"JVM memory pressure has exceeded 80%. If it exceeds 92% for 30
 minutes, all write operations to your cluster
                   will be blocked. To ensure optimum cluster stability, reduce
 traffic to the cluster or use larger instance types.
                   For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-high-jvm."
  }
}
```

GC insuficiente

OpenSearch O serviço envia esse evento quando a JVM máxima está acima de 70% e a diferença entre a máxima e a mínima é menor que 30%. Isso pode indicar que a JVM não consegue recuperar memória suficiente durante os ciclos de coleta de resíduos para sua workload. Isso pode levar a respostas cada vez mais lentas e latências mais altas; e, em alguns casos, até mesmo a queda de nós devido a verificações de integridade expiradas. Para garantir a estabilidade ideal do cluster, reduza o tráfego para o cluster ou escale seu domínio para fornecer memória suficiente para sua workload.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
```

```
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Insufficient GC",
     "status":"Warning",
     "severity":"Medium",
     "description":"Maximum JVM is above 70% and JVM range is less than 30%. This may
 indicate insufficient garbage collection for your workload.
                   For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-insufficient-
gc."
  }
}
```

Aviso de roteamento de índice personalizado

OpenSearch O serviço envia esse evento quando seu domínio está em estado de processamento e contém índices com configurações personalizadas de index.routing.allocation que podem fazer com que as implantações azul-esverdeadas parem. Verifique se as configurações foram aplicadas corretamente.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Custom Index Routing Warning",
     "status":"Warning",
     "severity":"Medium",
     "description":"Your domain is in processing state and contains indice(s) with
 custom index.routing.allocation
```

```
                    settings which can cause blue-green deployments to get stuck.
 Verify settings are applied properly.
                    For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-index-routing."
  }
}
```

Falha no bloqueio de fragmentos

OpenSearch O serviço envia esse evento quando seu domínio não está íntegro devido a fragmentos não atribuídos com. `[ShardLockObtainFailedException]` Para obter mais informações, consulte Como resolvo a exceção de bloqueio por fragmentos na memória no Amazon OpenSearch Service?

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Failed Shard Lock",
     "status":"Warning",
     "severity":"Medium",
     "description":"Your domain is unhealthy due to unassigned shards with
 [ShardLockObtainFailedException]. For more information,
                    see https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/monitoring-events.html#monitoring-events-failed-shard-lock."
}
```

Eventos de endpoint da VPC

OpenSearch O serviço envia determinados eventos EventBridge relacionados aos endpoints AWS PrivateLink da interface.

Falha na criação de endpoint da VPC

OpenSearch O serviço envia esse evento quando não consegue criar um VPC endpoint solicitado. Esse erro pode ocorrer porque você atingiu o limite do número de endpoints da VPC permitido em uma região. Você também verá esse erro se uma sub-rede ou grupo de segurança especificado não existir.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service VPC Endpoint Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"VPC Endpoint Create Validation",
      "status":"Failed",
      "severity":"High",
      "description":"Unable to create VPC endpoint aos-0d4c74c0342343 for domain
                     arn:aws:es:eu-south-1:123456789012:domain/my-domain due to the
 following validation failures: You've reached the limit on the
                     number of VPC endpoints that you can create in the AWS Region."
   }
}
```

Falha na atualização de endpoint da VPC

OpenSearch O serviço envia esse evento quando não consegue excluir um VPC endpoint solicitado.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
   "version":"0",
```

```
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service VPC Endpoint Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"VPC Endpoint Update Validation",
      "status":"Failed",
      "severity":"High",
      "description":"Unable to update VPC endpoint aos-0d4c74c0342343 for domain
                    arn:aws:es:eu-south-1:123456789012:domain/my-domain due to the
 following validation failures: <failure message>."
    }
}
```

Falha na exclusão de endpoint da VPC

OpenSearch O serviço envia esse evento quando não consegue excluir um VPC endpoint solicitado.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service VPC Endpoint Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"VPC Endpoint Delete Validation",
      "status":"Failed",
      "severity":"High",
      "description":"Unable to delete VPC endpoint aos-0d4c74c0342343 for domain
```

```
                    arn:aws:es:eu-south-1:123456789012:domain/my-domain due to the
 following validation failures: Specified subnet doesn't exist."
   }
}
```

Eventos de desativação do nó

OpenSearch O serviço envia eventos para EventBridge quando ocorrer um dos seguintes eventos de desativação do nó.

Desativação do nó agendada

OpenSearch O serviço envia esse evento quando a desativação de um nó é agendada.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2023-04-07T10:07:33Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Node Retirement Notification",
    "status": "Scheduled",
    "severity": "Medium",
    "description": "An automated action to retire and replace a node has been scheduled
 on your domain.
                    The node will be replaced in the next off-peak window. For more
 information, see
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/monitoring-events.html."
  }
}
```

Desativação do nó concluída

OpenSearch O serviço envia esse evento quando a desativação do nó é concluída.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2023-04-07T10:07:33Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Node Retirement Notification",
    "status": "Completed",
    "severity": "Medium",
    "description": "The node has been retired and replaced with a new node."
  }
}
```

Falha na desativação do nó

OpenSearch O serviço envia esse evento quando a desativação de um nó falha.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2023-04-07T10:07:33Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Node Retirement Notification",
    "status": "Failed",
    "severity": "Medium",
```

```
    "description": "Node retirement failed. No actions are required from your end. We
 will automatically
                    retry replacing the node."
  }
}
```

Eventos de erro de domínio

OpenSearch O serviço envia eventos para EventBridge quando ocorrer um dos seguintes erros de domínio.

Falha na validação da atualização do domínio

OpenSearch O serviço envia esse evento se encontrar uma ou mais falhas de validação ao tentar atualizar ou realizar uma alteração na configuração em um domínio. Para obter ajuda para resolver essas falhas, consulte the section called “Solução de problemas de erros de validação”.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Domain Update Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"Domain Update Validation",
      "status":"Failed",
      "severity":"High",
      "description":"Unable to perform updates to your domain due to the following
 validation failures: <failures>
                    Please see the documentation for more information https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/managedomains-
configuration-changes.html#validation"
```

```
    }
}
```

Chave do KMS inacessível

OpenSearch O serviço envia esse evento quando não consegue acessar sua AWS KMS chave.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Domain Error Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2016-11-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"KMS Key Inaccessible",
     "status":"Error",
     "severity":"High",
     "description":"The KMS key associated with this domain is inaccessible. You are at
 risk of losing access to your domain.
                    For more information, please refer to https://docs.aws.amazon.com/
opensearch-service/latest/developerguide/encryption-at-rest.html#disabled-key."
  }
}
```

Isolamento de domínios

OpenSearch O serviço envia esse evento quando seu domínio fica isolado e não consegue receber, ler ou gravar solicitações porque não pode ser acessado pela rede.

Exemplo

O exemplo a seguir mostra um evento desse tipo.

```
{
```

```
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2023-11-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Domain Isolation Notification",
     "status":"Error",
     "severity":"High",
     "description":"Your OpenSearch Service domain has been isolated. An isolated
 domain is unreachable by network and cannot receive, read, or write requests. For more
 information and assistance, please contact AWS Support at https://docs.aws.amazon.com/
opensearch-service/latest/developerguide/encryption-at-rest.html#disabled-key."
  }
}
```


Tutorial: Ouvindo EventBridge eventos do Amazon OpenSearch Service

Neste tutorial, você configura uma AWS Lambda função simples que escuta os eventos do Amazon OpenSearch Service e os grava em um stream de CloudWatch logs do Logs.

Pré-requisitos

Este tutorial pressupõe que você tenha um domínio de OpenSearch serviço existente. Se você ainda não criou um domínio, siga as etapas em Criação e gerenciamento de domínios para criar um.

Etapa 1: Criar a função do Lambda

Neste procedimento, você cria uma função Lambda simples para servir como destino para mensagens de eventos OpenSearch de serviço.

Para criar uma função Lambda de destino

1. Abra o AWS Lambda console em https://console.aws.amazon.com/lambda/.
2. Escolha Criar função e Criar desde o início.
3. Em Nome da função, insira event-handler.
4. ParaRuntime, escolha Python 3.8.

5. Escolha Criar Função.
6. Na seção Function code, edite o código de exemplo de acordo com o exemplo a seguir.

```
import json

def lambda_handler(event, context):
    if event["source"] != "aws.es":
        raise ValueError("Function only supports input from events with a source
 type of: aws.es")

    print(json.dumps(event))
```

   Essa é uma função simples do Python 3.8 que imprime os eventos enviados pelo Service. OpenSearch Se tudo estiver configurado corretamente, no final deste tutorial, os detalhes do evento aparecerão no stream de CloudWatch registros de registros associado a essa função Lambda.
7. Escolha Implantar.

Etapa 2: registrar uma regra de evento

Nesta etapa, você cria uma EventBridge regra que captura eventos dos seus domínios de OpenSearch serviço. Essa regra captura todos os eventos na conta em que ela está definida. As mensagens de eventos em si contêm informações sobre a fonte do evento, inclusive o domínio do qual ele se originou. Você pode usar essas informações para filtrar e classificar eventos de forma programática.

Para criar uma EventBridge regra

1. Abra o EventBridge console em https://console.aws.amazon.com/events/.
2. Escolha Criar regra.
3. Nomeie a regra como event-rule.
4. Escolha Próximo.
5. Para o padrão do evento, selecione AWS services, Amazon OpenSearch Service e All Events. Esse padrão se aplica a todos os seus domínios de OpenSearch serviço e a todos os eventos OpenSearch de serviço. Como alternativa, você pode criar um padrão mais específico para filtrar alguns resultados.
6. Pressione Próximo.

7. Em Target (Destino), escolha Função do Lambda. No menu suspenso de função, escolha manipulador de eventos.
8. Pressione Próximo.
9. Ignore as tags e pressione Próximo novamente.
10. Revise a configuração e selecione Criar regra.

Etapa 3: Testar sua configuração

Na próxima vez que você receber uma notificação na seção Notificações do console de OpenSearch serviço, se tudo estiver configurado corretamente, sua função Lambda será acionada e gravará os dados do evento em um fluxo de log de CloudWatch registros da função.

Para testar sua configuração

1. Abra o CloudWatch console em https://console.aws.amazon.com/cloudwatch/.
2. No painel de navegação, escolha Logs e selecione o grupo de logs para sua função do Lambda (por exemplo, /aws/lambda/event-handler).
3. Selecione um fluxo de log para visualizar os dados do evento.

Tutorial: Envio de alertas do Amazon SNS para atualizações de software disponíveis

Neste tutorial, você configura uma regra de EventBridge evento da Amazon que captura notificações de atualizações de software de serviço disponíveis no Amazon OpenSearch Service e envia uma notificação por e-mail por meio do Amazon Simple Notification Service (Amazon SNS).

Pré-requisitos

Este tutorial pressupõe que você tenha um domínio de OpenSearch serviço existente. Se você ainda não criou um domínio, siga as etapas em Criação e gerenciamento de domínios para criar um.

Etapa 1: Criar e se inscrever em um tópico do Amazon SNS

Configure um tópico do Amazon SNS para funcionar como um destino de evento para a nova regra de evento.

Para criar um destino do Amazon SNS

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Escolha Tópicos e Criar tópico.
3. Para o tipo de trabalho, escolhaPadrão e nomeie o trabalho como software-update.
4. Escolha Criar tópico.
5. Após o tópico ser criado, escolha Criar assinatura.
6. Em Protocolo, escolha Email. Em Endpoint, insira um endereço de e-mail ao qual tenha acesso e escolha Criar assinatura.
7. Verifique sua conta de e-mail e espere para receber uma mensagem de e-mail de confirmação de assinatura. Quando você recebê-la, escolha Confirmar assinatura.

Etapa 2: Registrar uma regra de evento

Em seguida, registre uma regra de eventos que captura apenas eventos de atualização de software de serviço.

Para criar uma regra de evento

1. Abra o EventBridge console em https://console.aws.amazon.com/events/.
2. Escolha Criar regra.
3. Nomeie a regra como softwareupdate-rule.
4. Escolha Próximo.
5. Para o padrão do evento, selecione AWS serviços, Amazon OpenSearch Service e Amazon OpenSearch Service Software Update Notification. Esse padrão corresponde a qualquer evento de atualização de software de OpenSearch serviço do Service. Para obter mais informações sobre padrões de eventos, consulte os padrões de EventBridge eventos da Amazon no Guia EventBridge do usuário da Amazon.
6. Opcionalmente, você pode filtrar apenas por gravidades específicas. Para as gravidades de cada evento, consulte the section called “Eventos de atualização de software de serviço”.
7. Escolha Próximo.
8. Em Target (Destino), escolha Tópico do SNS e selecione software-update.
9. Escolha Próximo.
10. Ignore as tags e selecione Próximo.
11. Revise a configuração da regra e selecione Criar regra.

Na próxima vez que você receber uma notificação do OpenSearch Serviço sobre uma atualização de software de serviço disponível, se tudo estiver configurado corretamente, o Amazon SNS deverá enviar um alerta por e-mail sobre a atualização.

Monitoramento de chamadas de API do Amazon OpenSearch Service com o AWS CloudTrail

O Amazon OpenSearch Service é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, por uma função ou por um serviço da AWS no OpenSearch Service. O CloudTrail captura todas as chamadas de API de configuração para o OpenSearch Service como eventos.

> **Note**
>
> O CloudTrail captura apenas chamadas para a API de configuração, por exemplo, `CreateDomain` e `GetUpgradeStatus`. O CloudTrail não captura chamadas para as APIs do OpenSearch, por exemplo, `_search` e `_bulk`. Para essas chamadas, consulte the section called “Monitoramento de logs de auditoria”.

As chamadas capturadas incluem as chamadas do console do OpenSearch Service, da AWS CLI ou de um AWS SDK. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o OpenSearch Service. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para o OpenSearch Service, o endereço IP no qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, além de detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Informações do Amazon OpenSearch Service no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando uma atividade ocorre no OpenSearch Service, essa atividade é registrada em um evento do CloudTrail com outros eventos de serviço da AWS no Event history (Histórico de eventos). Você pode visualizar, pesquisar e baixar eventos recentes em sua conta da Conta da AWS. Para obter mais informações, consulte Visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro contínuo de eventos da sua conta da Conta da AWS, incluindo aqueles do OpenSearch Service, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços da AWS para analisar mais ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- Criar uma trilha para a sua Conta da AWS
- Integrações de serviços da AWS com logs do CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e Receber arquivos de log do CloudTrail de várias contas

Todas as ações de API de configuração do OpenSearch Service são registradas em log pelo CloudTrail e estão documentadas na Amazon OpenSearch Service API Reference (Referência da API do Amazon OpenSearch Service).

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do AWS Identity and Access Management (IAM)
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado
- Se a solicitação foi feita por outro serviço da AWS

Para obter mais informações, consulte o Elemento userIdentity do CloudTrail.

Entradas do arquivo de log do Amazon OpenSearch Service

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O seguinte exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a operação `CreateDomain`:


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/test-user",
    "accountId": "123456789012",
    "accessKeyId": "access-key",
    "userName": "test-user",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-08-21T21:59:11Z"
      }
    },
    "invokedBy": "signin.amazonaws.com"
  },
  "eventTime": "2018-08-21T22:00:05Z",
  "eventSource": "es.amazonaws.com",
  "eventName": "CreateDomain",
  "awsRegion": "us-west-1",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "signin.amazonaws.com",
  "requestParameters": {
    "engineVersion": "OpenSearch_1.0",
    "clusterConfig": {
      "instanceType": "m4.large.search",
      "instanceCount": 1
    },
    "snapshotOptions": {
      "automatedSnapshotStartHour": 0
    },
    "domainName": "test-domain",
    "encryptionAtRestOptions": {},
    "eBSOptions": {
      "eBSEnabled": true,
      "volumeSize": 10,
      "volumeType": "gp2"
    },
```

```
    "accessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"123456789012\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:us-west-1:123456789012:domain/test-domain/*\"}]}",
    "advancedOptions": {
      "rest.action.multi.allow_explicit_index": "true"
    }
  },
  "responseElements": {
    "domainStatus": {
      "created": true,
      "clusterConfig": {
        "zoneAwarenessEnabled": false,
        "instanceType": "m4.large.search",
        "dedicatedMasterEnabled": false,
        "instanceCount": 1
      },
      "cognitoOptions": {
        "enabled": false
      },
      "encryptionAtRestOptions": {
        "enabled": false
      },
      "advancedOptions": {
        "rest.action.multi.allow_explicit_index": "true"
      },
      "upgradeProcessing": false,
      "snapshotOptions": {
        "automatedSnapshotStartHour": 0
      },
      "eBSOptions": {
        "eBSEnabled": true,
        "volumeSize": 10,
        "volumeType": "gp2"
      },
      "engineVersion": "OpenSearch_1.0",
      "processing": true,
      "aRN": "arn:aws:es:us-west-1:123456789012:domain/test-domain",
      "domainId": "123456789012/test-domain",
      "deleted": false,
      "domainName": "test-domain",
      "accessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":\"arn:aws:iam::123456789012:root\"},\"Action\":\"es:*\",
\"Resource\":\"arn:aws:es:us-west-1:123456789012:domain/test-domain/*\"}]}"
    }
```

```
  },
  "requestID": "12345678-1234-1234-1234-987654321098",
  "eventID": "87654321-4321-4321-4321-987654321098",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Segurança no Amazon OpenSearch Service

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem.

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos compliance programs AWS. Para saber mais sobre os programas de conformidade que se aplicam ao Amazon OpenSearch Service, consulte AWS Services in Scope by Compliance Program.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o OpenSearch Serviço. Os tópicos a seguir mostram como configurar o OpenSearch Serviço para atender aos seus objetivos de segurança e conformidade. Você também aprende a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do OpenSearch Serviço.

Tópicos

- Usar perfis vinculados ao serviço com o Amazon OpenSearch Service

Proteção de dados no Amazon OpenSearch Service

O modelo de responsabilidade AWS compartilhada de se aplica à proteção de dados no Amazon OpenSearch Service. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o OpenSearch Serviço ou outro Serviços da AWS usando o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou

campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia de dados em repouso para o Amazon OpenSearch Service

OpenSearch Os domínios de serviço oferecem criptografia de dados em repouso, um recurso de segurança que ajuda a impedir o acesso não autorizado aos seus dados. O recurso usa AWS Key Management Service (AWS KMS) para armazenar e gerenciar suas chaves de criptografia e o algoritmo Advanced Encryption Standard com chaves de 256 bits (AES-256) para realizar a criptografia. Se habilitado, o recurso criptografa os seguintes aspectos de um domínio:

- Todos os índices (incluindo aqueles em UltraWarm armazenamento)
- OpenSearch troncos
- Arquivos de troca
- Todos os outros dados no diretório da aplicação
- Snapshots automatizados

Os seguintes itens não são criptografados quando você ativa a criptografia de dados em repouso, mas você pode executar etapas adicionais para protegê-los:

- Instantâneos manuais: no momento, você não pode usar AWS KMS chaves para criptografar instantâneos manuais. No entanto, você pode usar a criptografia no lado do servidor com chaves gerenciadas pelo S3 ou chaves do KMS para criptografar o bucket que você usa como repositório de snapshots. Para obter instruções, consulte the section called “Registro de um repositório de snapshots manuais”.
- Registros lentos e registros de erros: se você publicar registros e quiser criptografá-los, poderá criptografar o grupo de CloudWatch registros de registros usando a mesma AWS KMS chave do domínio de OpenSearch serviço. Para obter mais informações, consulte Criptografar dados de log em CloudWatch registros usando AWS KMS o Guia do usuário do Amazon CloudWatch Logs.

> **Note**
>
> Você não pode habilitar a criptografia em repouso em um domínio existente se UltraWarm o armazenamento a frio estiver habilitado no domínio. Primeiro, você deve desativar UltraWarm o armazenamento a frio, ativar a criptografia em repouso e, em seguida,

reativá-lo UltraWarm ou reativá-lo. Se você quiser manter os índices em UltraWarm um armazenamento refrigerado, você deve movê-los para o armazenamento a quente antes de desativar UltraWarm ou armazenar a frio.

OpenSearch O serviço suporta somente chaves KMS de criptografia simétrica, não chaves assimétricas. Para aprender a criar chaves simétricas, consulte Criação de chaves no Guia do desenvolvedor do AWS Key Management Service .

Independentemente de a criptografia em repouso estar ativada, todos os domínios criptografam automaticamente pacotes personalizados usando AES-256 e chaves gerenciadas por serviços. OpenSearch

Permissões

Para usar o console OpenSearch de serviço para configurar a criptografia de dados em repouso, você deve ter permissões de leitura AWS KMS, como a seguinte política baseada em identidade:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:List*",
        "kms:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

Se quiser usar uma chave diferente da chave AWS própria, você também deve ter permissões para criar concessões para a chave. Essas permissões normalmente assumem a forma de uma política baseada em recursos que você especifica ao criar a chave.

Se você quiser manter sua chave exclusiva para o OpenSearch Serviço, você pode adicionar a ViaService condição kms: a essa política de chaves:

```
"Condition": {
```

```
  "StringEquals": {
    "kms:ViaService": "es.us-west-1.amazonaws.com"
  },
  "Bool": {
    "kms:GrantIsForAWSResource": "true"
  }
}
```

Para obter mais informações, consulte Usando políticas de chaves no AWS KMS no Guia do AWS Key Management Service desenvolvedor.

Ativação da criptografia de dados em repouso

A criptografia de dados em repouso em novos domínios requer o Elasticsearch 5.1 OpenSearch ou posterior. Habilitá-lo em domínios existentes requer o Elasticsearch 6.7 OpenSearch ou posterior.

Para habilitar a criptografia de dados em repouso (console)

1. Abra o domínio no AWS console e escolha Ações e Editar configuração de segurança.
2. Em Criptografia, selecione Habilitar criptografia de dados em repouso.
3. Escolha uma AWS KMS chave para usar e, em seguida, escolha Salvar alterações.

Também é possível habilitar a criptografia por meio da API de configuração. A solicitação a seguir permite a criptografia de dados em repouso em um domínio existente:

```
{
   "ClusterConfig":{
      "EncryptionAtRestOptions":{
         "Enabled": true,
         "KmsKeyId":"arn:aws:kms:us-east-1:123456789012:alias/my-key"
      }
   }
}
```

A chave do KMS foi desabilitada ou excluída

Se você desabilitar ou excluir a chave usada para criptografar um domínio, o domínio ficará inacessível. OpenSearch O serviço envia uma notificação informando que não consegue acessar a chave KMS. Habilite novamente a chave imediatamente para acessar o seu domínio.

A equipe OpenSearch de serviço não poderá ajudá-lo a recuperar seus dados se sua chave for excluída. AWS KMS exclui as chaves somente após um período de espera de pelo menos sete dias. Se a exclusão da sua chave estiver pendente, cancele-a ou tire um snapshot manual do domínio para evitar a perda de dados.

Desativação da criptografia de dados em repouso

Depois de configurar um domínio para criptografar dados em repouso, você não pode desativar a configuração. Em vez disso, você pode tirar um snapshot manual do domínio existente, criar outro domínio, migrar seus dados e excluir o domínio anterior.

Monitoramento de domínios que criptografam dados em repouso

Domínios que criptografam dados em repouso têm duas métricas adicionais: `KMSKeyError` e `KMSKeyInaccessible`. Essas métricas serão exibidas somente se o domínio encontrar um problema com sua chave de criptografia. Para obter descrições completas dessas métricas, consulte the section called “Métricas de cluster”. Você pode visualizá-los usando o console do OpenSearch Service ou o CloudWatch console da Amazon.

> **Tip**
>
> Cada métrica representa um problema significativo para um domínio, por isso recomendamos que você crie CloudWatch alarmes para ambos. Para ter mais informações, consulte the section called “ CloudWatch Alarmes recomendados”.

Outras considerações

- A rotação automática de chaves preserva as propriedades de suas AWS KMS chaves, portanto, a rotação não afeta sua capacidade de acessar seus OpenSearch dados. Os domínios OpenSearch de serviço criptografados não oferecem suporte à rotação manual de chaves, o que envolve a criação de uma nova chave e a atualização de qualquer referência à chave antiga. Para saber mais, consulte Rotação de chaves no Guia do desenvolvedor do AWS Key Management Service .
- Certos tipos de instâncias não oferecem suporte à criptografia de dados em repouso. Para obter detalhes, consulte the section called “Tipos de instâncias compatíveis”.
- Domínios que criptografam dados em repouso usam outro nome de repositório para seus snapshots automatizados. Para ter mais informações, consulte the section called “Restauração de snapshots”.

- Embora seja altamente recomendável habilitar a criptografia em repouso, esse recurso pode adicionar sobrecarga adicional à CPU e acrescentar alguns milissegundos de latência. Contudo, a maioria dos casos de uso não é afetada por essas diferenças, e a magnitude do impacto depende da configuração do cluster, dos clientes e do perfil de uso.

ode-to-node Criptografia N para Amazon OpenSearch Service

A ode-to-node criptografia N fornece uma camada adicional de segurança além dos recursos padrão do Amazon OpenSearch Service.

Cada domínio OpenSearch de serviço, independentemente de usar o acesso à VPC, reside em sua própria VPC dedicada. Essa arquitetura impede que possíveis invasores interceptem o tráfego entre os OpenSearch nós e mantém o cluster seguro. Por padrão, no entanto, o tráfego na VPC não é criptografado. A ode-to-node criptografia N habilita a criptografia TLS 1.2 para todas as comunicações dentro da VPC.

Se você enviar dados para o OpenSearch Serviço via HTTPS, a node-to-node criptografia ajuda a garantir que seus dados permaneçam criptografados enquanto OpenSearch os distribuem (e redistribuem) por todo o cluster. Se os dados chegarem sem criptografia via HTTP, o OpenSearch Service os criptografará depois que chegarem ao cluster. Você pode exigir que todo o tráfego para o domínio chegue por HTTPS usando o console ou a API de configuração. AWS CLI

Nenhuma ode-to-node criptografia é necessária se você habilitar um controle de acesso refinado.

Ativando a node-to-node criptografia

A ode-to-node criptografia N em novos domínios requer qualquer versão do OpenSearch Elasticsearch 6.0 ou posterior. Habilitar a node-to-node criptografia em domínios existentes requer qualquer versão do OpenSearch Elasticsearch 6.7 ou posterior. Escolha o domínio existente no console do AWS , Ações e Editar configuração de segurança.

Como alternativa, você pode usar a API de configuração AWS CLI ou. Para obter mais informações, consulte a Referência de AWS CLI comandos e a referência da API de OpenSearch serviços.

Desativando a criptografia node-to-node

Depois de configurar um domínio para usar node-to-node criptografia, você não pode desativar a configuração. Em vez disso, você pode tirar um snapshot manual do domínio criptografado, criar outro domínio, migrar seus dados e excluir o domínio anterior.

Identity and Access Management no Amazon OpenSearch Service

O Amazon OpenSearch Service oferece várias maneiras de controlar o acesso aos seus domínios. Esta seção aborda os diversos tipos de políticas, como elass interagem entre si e como você pode criar suas próprias políticas personalizadas.

> **Important**
>
> O suporte à VPC introduz algumas considerações adicionais sobre o controle de acesso ao OpenSearch serviço. Para ter mais informações, consulte the section called “Sobre políticas de acesso em domínios da VPC”.

Tipos de políticas

OpenSearch O serviço oferece suporte a três tipos de políticas de acesso:

- the section called “Políticas baseadas em recursos”
- the section called “Políticas baseadas em identidade”
- the section called “Políticas baseadas em IP”

Políticas baseadas em recursos

Quando um domínio é criado, uma política baseada em recurso é adicionada, muitas vezes chamada de política de acesso ao domínio. Essas políticas especificam que ações uma entidade principal pode executar nos sub-recursos do domínio (com exceção da pesquisa entre clusters). Os sub-recursos incluem OpenSearch índices e APIs. O elemento Principal especifica as contas, os usuários ou as funções com acesso permitido. O elemento Resource especifica quais sub-recursos essas entidades principais podem acessar.

Por exemplo, a política baseada em recurso a seguir concede ao `test-user` (`es:*`) acesso total aos sub-recursos em `test-domain`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": [
        "es:*"
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
    }
  ]
}
```

Duas considerações importantes se aplicam a essa política:

- Esses privilégios se aplicam apenas a esse domínio. A menos que você crie políticas semelhantes em outros domínios, `test-user` só poderá acessar `test-domain`.
- O terminador `/*` no elemento `Resource` é significativo e indica que as políticas baseadas em recursos só se aplicam aos sub-recursos do domínio, e não ao próprio domínio. Em políticas baseadas em recursos, a ação `es:*` é equivalente a `es:ESHttp*`.

  Por exemplo, o `test-user` pode fazer solicitações em relação a um índice (`GET https://search-test-domain.us-west-1.es.amazonaws.com/test-index`), mas não pode atualizar a configuração do domínio (`POST https://es.us-west-1.amazonaws.com/2021-01-01/opensearch/domain/test-domain/config`). Observe a diferença entre os dois endpoints. O acesso à API de configuração requer uma política baseada em identidade.

Você pode especificar um nome de índice parcial adicionando um curinga. Este exemplo identifica todos os índices que começam com `commerce`:

```
arn:aws:es:us-west-1:987654321098:domain/test-domain/commerce*
```

Nesse caso, o curinga significa que o `test-user` pode fazer solicitações para índices em `test-domain` que tenham nomes que comecem com `commerce`.

Para restringir ainda mais o `test-user`, você pode aplicar a seguinte política:

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": [
        "es:ESHttpGet"
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/commerce-data/
_search"
    }
  ]
}
```

Agora, o `test-user` só pode executar uma operação: pesquisar no índice `commerce-data`. Todos os outros índices no domínio estão inacessíveis, e sem permissões para usar as ações `es:ESHttpPut` ou `es:ESHttpPost`, o `test-user` não pode adicionar ou modificar documentos.

Em seguida, você pode optar por configurar uma função para usuários avançados. Esta política oferece acesso `power-user-role` aos métodos HTTP GET e PUT para todos os URIs no índice:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:role/power-user-role"
        ]
      },
      "Action": [
        "es:ESHttpGet",
        "es:ESHttpPut"
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/commerce-data/
*"
    }
  ]
```

```
}
```

Se o seu domínio estiver em uma VPC ou usar controle de acesso refinado, você poderá usar uma política de acesso a domínios abertos. Caso contrário, sua diretiva de acesso ao domínio deverá conter alguma restrição, seja por endereço IP ou principal.

Para obter informações sobre todas as ações disponíveis, consulte the section called “Referência de elementos da política”. Para obter um controle muito mais granular sobre seus dados, use uma política de acesso a domínio aberto com controle de acesso refinado.

Políticas baseadas em identidade

Ao contrário das políticas baseadas em recursos, que fazem parte de cada domínio de OpenSearch serviço, você anexa políticas baseadas em identidade a usuários ou funções usando o serviço AWS Identity and Access Management (IAM). Assim como nas políticas baseadas em recursos, as políticas baseadas em identidade especificam quem pode acessar um serviço, quais ações podem ser executadas e, se aplicável, em quais recursos essas ações podem ser executadas.

As políticas baseadas em identidade tendem a ser mais genéricas, embora não exista essa exigência. Elas geralmente controlam somente as ações de API de configuração que um usuário pode realizar. Depois de implementar essas políticas, você pode usar políticas baseadas em recursos (ou controle de acesso refinado) no OpenSearch Service para oferecer aos usuários acesso a índices e APIs. OpenSearch

> **Note**
>
> Os usuários com a `AmazonOpenSearchServiceReadOnlyAccess` política AWS gerenciada não conseguem ver o status de integridade do cluster no console. Para permitir que eles vejam o status de integridade do cluster (e outros OpenSearch dados), adicione a `es:ESHttpGet` ação a uma política de acesso e anexe-a às suas contas ou funções.

Como as políticas baseadas em identidade são anexadas a usuários ou funções (principais), o JSON não especifica um principal. A política a seguir concede acesso a ações que começam com `Describe` e `List`. Essa combinação de ações fornece acesso somente leitura a configurações de domínio, mas não aos dados armazenados no próprio domínio:

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "es:Describe*",
        "es:List*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Um administrador pode ter acesso total ao OpenSearch Serviço e a todos os dados armazenados em todos os domínios:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "es:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

As políticas baseadas em identidade permitem que você use tags para controlar o acesso à API de configuração. A seguinte política, por exemplo, permitirá que os principais anexados visualizem e atualizem a configuração de um domínio se o domínio tiver a tag `team:devops`:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "es:UpdateDomainConfig",
      "es:DescribeDomain",
      "es:DescribeDomainConfig"
    ],
    "Effect": "Allow",
```

```
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:ResourceTag/team": [
          "devops"
        ]
      }
    }
  }]
}
```

Você também pode usar tags para controlar o acesso à OpenSearch API. As políticas baseadas em tags para a OpenSearch API se aplicam somente aos métodos HTTP. Por exemplo, a política a seguir permite que os diretores anexados enviem solicitações GET e PUT para a OpenSearch API se o domínio tiver a `environment:production` tag:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "es:ESHttpGet",
      "es:ESHttpPut"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:ResourceTag/environment": [
          "production"
        ]
      }
    }
  }]
}
```

Para um controle mais granular da OpenSearch API, considere usar um controle de acesso refinado.

> **Note**
>
> Depois de adicionar uma ou mais OpenSearch APIs a qualquer política baseada em tags, você deve realizar uma única operação de tag (como adicionar, remover ou modificar uma tag) para que as alterações entrem em vigor em um domínio. Você deve usar o software

de serviço R20211203 ou posterior para incluir operações de OpenSearch API em políticas baseadas em tags.

OpenSearch O serviço oferece suporte às chaves de condição `TagKeys` globais `RequestTag` e da API de configuração, não da OpenSearch API. Essas condições aplicam-se somente a chamadas de API que incluem tags dentro da solicitação, como `CreateDomain`, `AddTags` e `RemoveTags`. A política a seguir permite que os principais anexados criem domínios, mas somente se incluírem a tag `team:it` na solicitação:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "es:CreateDomain",
      "es:AddTags"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/team": [
          "it"
        ]
      }
    }
  }
}
```

Para obter mais detalhes sobre o uso de tags para controle de acesso e as diferenças entre as políticas baseadas em recursos e as baseadas em identidade, consulte o Manual do usuário do IAM.

Políticas baseadas em IP

As políticas baseadas em IP restringem o acesso a um domínio para um ou mais endereços IP ou blocos CIDR. Tecnicamente, as políticas baseadas em IP não são um tipo de política diferente. Na verdade, elas são apenas políticas baseadas em recursos que especificam uma entidade principal anônima e incluem um elemento Condition especial.

O principal atrativo das políticas baseadas em IP é que elas permitem solicitações não assinadas a um domínio de OpenSearch serviço, o que permite usar clientes como curl e OpenSearch painéis

ou acessar o domínio por meio de um servidor proxy. Para saber mais, consulte the section called "Usando um proxy para acessar o OpenSearch serviço a partir de OpenSearch painéis".

> **Note**
>
> Se você ativou o acesso à VPC para seu domínio, não poderá configurar uma política baseada em IP. Em vez disso, você poderá usar grupos de segurança para controlar quais endereços IP poderão acessar o domínio. Para ter mais informações, consulte the section called "Sobre políticas de acesso em domínios da VPC".

A política a seguir concede a todas as solicitações HTTP que se originam no intervalo de IP especificado acesso ao `test-domain`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24"
          ]
        }
      },
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
    }
  ]
}
```

Se o seu domínio tiver um endpoint público e não usar controle de acesso refinado, recomendamos combinar principais do IAM e endereços IP. Esta política concederá acesso HTTP ao `test-user` somente se a solicitação se originar do intervalo de IP especificado:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::987654321098:user/test-user"
      ]
    },
    "Action": [
      "es:ESHttp*"
    ],
    "Condition": {
      "IpAddress": {
        "aws:SourceIp": [
          "192.0.2.0/24"
        ]
      }
    },
    "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
  }]
}
```

Fazendo e assinando solicitações OpenSearch de serviço

Mesmo se você configurar uma política de acesso totalmente aberta baseada em recursos, todas as solicitações para a API de configuração do OpenSearch serviço devem ser assinadas. Se suas políticas especificarem funções ou usuários do IAM, as solicitações para as OpenSearch APIs também precisarão ser assinadas usando o AWS Signature versão 4. O método de assinatura é diferente dependendo da API:

- Para fazer chamadas para a API OpenSearch de configuração do serviço, recomendamos que você use um dos AWS SDKs. Os SDKs simplificam muito o processo e podem economizar uma quantidade significativa de tempo em comparação com a criação e assinatura das suas próprias solicitações. Os endpoints da API de configuração usam o formato a seguir:

  ```
  es.region.amazonaws.com/2021-01-01/
  ```

  Por exemplo, a seguinte solicitação faz uma alteração de configuração no domínio `movies`, mas é necessário que você a assine (não recomendado):

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/movies/config
{
  "ClusterConfig": {
    "InstanceType": "c5.xlarge.search"
  }
}
```

Se você usar um dos SDKs, como Boto 3, o SDK gerencia automaticamente a assinatura de solicitações:

```
import boto3

client = boto3.client(es)
response = client.update_domain_config(
  DomainName='movies',
  ClusterConfig={
    'InstanceType': 'c5.xlarge.search'
  }
)
```

Para obter um código de exemplo Java, consulte the section called “Uso de AWS SDKs”.

- Para fazer chamadas para as OpenSearch APIs, você deve assinar suas próprias solicitações. As OpenSearch APIs usam o seguinte formato:

```
domain-id.region.es.amazonaws.com
```

Por exemplo, a seguinte solicitação procura o índice `movies` para thor:

```
GET https://my-domain.us-east-1.es.amazonaws.com/movies/_search?q=thor
```

> **Note**
>
> O serviço ignora parâmetros passados em URLs para solicitações HTTP POST assinadas com o Signature versão 4.

Quando há colisão de políticas

Quando as políticas discordam entre si ou não fazem nenhuma referência explícita a um usuário, surgem complexidades. Como o IAM funciona no Manual do usuário do IAM fornece um breve resumo da lógica de avaliação de políticas:

- Por padrão, todas as solicitações são negadas.
- Uma permissão explícita substitui esse padrão.
- Uma deny (negar) explícito substitui todas as permissões.

Por exemplo, se uma política baseada em recursos conceder acesso a um sub-recurso de domínio (um OpenSearch índice ou API), mas uma política baseada em identidade negar seu acesso, você terá acesso negado. Se uma política baseada em identidade concede acesso e uma política baseada em recursos não especifica se você deve ou não ter acesso, esse acesso é concedido. Consulte a tabela a seguir com o cruzamento de políticas para obter um resumo completo dos resultados para sub-recursos de domínios.

	Permitido na política baseada em recursos	Negado na política baseada em recursos	Nem permitido nem negado na política baseada em recursos
Allowed in identity-based policy	Permitir	Deny	Allow
Denied in identity-based policy	Deny	Deny	Deny
Neither allowed nor denied in identity-based policy	Allow	Deny	Deny

Referência de elementos da política

OpenSearch O serviço oferece suporte à maioria dos elementos de política na Referência de elementos de política do IAM, com exceção de`NotPrincipal`. A tabela a seguir mostra os elementos mais comuns.

Elemento da política de JSON	Resumo
`Version`	Versão atual da linguagem de política é `2012-10-17` . Todas as políticas de acesso devem especificar esse valor.
`Effect`	Esse elemento especifica se a declaração permite ou nega o acesso às ações especificadas. Os valores válidos são `Allow` ou `Deny`.
`Principal`	Esse elemento especifica a função Conta da AWS ou o usuário do IAM que tem acesso permitido ou negado a um recurso e pode assumir várias formas: • AWS contas: `"Principal":{"AWS": ["123456789012"]}` ou `"Principal":{"AWS": ["arn:aws:iam::123456789012:root"]}` • Usuários do IAM: `"Principal":{"AWS": ["arn:aws:iam::123456789012:user/test-user"]}` • Funções do IAM: `"Principal":{"AWS": ["arn:aws:iam::123456789012:role/test-role"]}` **Important** Especificar o curinga * permite o acesso anônimo ao domínio, o que não recomendamos, a menos que você adicione uma condição baseada em IP, use o suporte à VPC ou habilite o controle de acesso refinado. Além disso, inspecione cuidadosa mente as seguintes políticas para confirmar se elas não concedem amplo acesso: • Políticas baseadas em identidade vinculadas aos AWS diret ores associados (por exemplo, funções do IAM) • Políticas baseadas em recursos anexadas aos AWS recur sos associados (por exemplo, chaves AWS Key Management Service KMS)

Elemento da política de JSON	Resumo

`Action`	OpenSearch O serviço usa `ESHttp*` ações para métodos OpenSearch HTTP. O resto das ações se aplicam à API de configuração.
	
	Determinadas ações `es:` dão suporte a permissões no nível do recurso. Por exemplo, você pode conceder a um usuário permissões para excluir um determinado domínio sem conceder a esse usuário permissões para excluir qualquer domínio. Outras ações se aplicam apenas ao serviço em si. Por exemplo, `es:ListDomainNames` não faz sentido no contexto de um único domínio e, portanto, requer um curinga.
	
	Para obter uma lista de todas as ações disponíveis e se elas se aplicam aos sub-recursos do domínio (`test-domain/*`), à configuração do domínio (`test-domain`) ou somente ao serviço (`*`), consulte Ações, recursos e chaves de condição do Amazon OpenSearch Service na Referência de Autorização de Serviço
	Políticas baseadas em recursos são diferentes das permissões no nível do recurso. As políticas baseadas em recursos são políticas JSON completas anexadas aos domínios. As permissões no nível do recurso tornam possível a restrição de ações em domínios específicos ou sub-recursos. Na prática, você pode pensar na permissão no nível do recurso como uma seção opcional de um recurso ou uma política baseada em identidade.
	
	Embora as permissões no nível de recurso para `es:CreateDomain` possam parecer não intuitivas — afinal de contas, por que conceder permissões a um usuário para criar um domínio que já existe? —, o uso de um curinga permite aplicar um esquema de nomenclatura simples aos seus domínios, como `"Resource": "arn:aws:es:us-west-1:987654321098:domain/my-team-name-*"` .
	
	Naturalmente, nada impede que você inclua ações juntamente com elementos de recursos menos restritivos, como estes:
	
	`{`
	`"Version": "2012-10-17",`

Elemento da política de JSON	Resumo

	<pre>"Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "es:ESHttpGet",
	  "es:DescribeDomain"
	  ],
	  "Resource": "*"
	  }
	  ]
	}</pre>
	Para saber mais sobre o emparelhamento de ações e recursos, consulte o elemento `Resource` nesta tabela.

`Condition`	OpenSearch O serviço é compatível com a maioria das condições descritas nas chaves de contexto de condição AWS global no Guia do usuário do IAM. Exceções notáveis incluem a `aws:PrincipalTag` chave, que o OpenSearch Serviço não suporta.
	
	Ao configurar uma política baseada em IP, você especifica os endereços IP ou bloco CIDR como uma condição, como esta:
	
	<pre>"Condition": {
	  "IpAddress": {
	  "aws:SourceIp": [
	  "192.0.2.0/32"
	  ]
	  }
	}</pre>
	Conforme observado emthe section called “Políticas baseadas em identidade”, as chaves de `aws:TagKeys` condição `aws:Resou rceTag` `aws:RequestTag` , e se aplicam à API de configuração e às OpenSearch APIs.

Elemento da política de JSON	Resumo

`Resource`	OpenSearch O serviço usa `Resource` elementos de três maneiras básicas:
	
	• Para ações que se aplicam ao próprio OpenSearch Serviço, como`es:ListDomainNames` , ou para permitir acesso total, use a seguinte sintaxe:
	
	`"Resource": "*"`
	
	• Para as ações que envolvem uma configuração de domínio, como `es:DescribeDomain` , você pode usar a seguinte sintaxe:
	
	`"Resource": "arn:aws:es:` *region*`:`*aws-account-id*`:domain/`*domain-name*`"`
	
	• Para as ações que se aplicam a um sub-recurso de domínio, como `es:ESHttpGet` , você pode usar a seguinte sintaxe:
	
	`"Resource": "arn:aws:es:` *region*`:`*aws-account-id*`:domain/`*domain-name*`/*"`
	
	Você não precisa usar um curinga. OpenSearch O serviço permite que você defina uma política de acesso diferente para cada OpenSearch índice ou API. Por exemplo, você pode limitar as permissões de um usuário para o índice `test-index` :
	
	`"Resource": "arn:aws:es:` *region*`:`*aws-account-id*`:domain/`*domain-name*`/test-index"`
	
	Em vez de acesso total ao `test-index` , você pode preferir limitar a política somente à API de pesquisa:
	
	`"Resource": "arn:aws:es:` *region*`:`*aws-account-id*`:domain/`*domain-name*`/test-index/_search"`

Elemento da política de JSON	Resumo
	Você pode até mesmo controlar o acesso a documentos individuais: `"Resource": "arn:aws:es:  region:aws-account-id:domain/domain-name /test-index/test-type/1"` Essencialmente, se OpenSearch expressar o sub-recurso como um URI, você pode controlar o acesso a ele usando uma política de acesso. Para ter ainda mais controle sobre quais recursos um usuário pode acessar, consulte the section called “Controle de acesso refinado”. Para obter detalhes sobre quais ações dão suporte a permissões no nível do recurso, consulte o elemento `Action` nesta tabela.

Opções avançadas e considerações sobre a API

OpenSearch O serviço tem várias opções avançadas, uma das quais tem implicações de controle de acesso:`rest.action.multi.allow_explicit_index`. Como sua configuração padrão é verdadeiro, ela permite que os usuários ignorem as permissões de sub-recursos em determinadas circunstâncias.

Por exemplo, considere a seguinte política baseada em recurso:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": [
        "es:ESHttp*"
```

```
      ],
      "Resource": [
        "arn:aws:es:us-west-1:987654321098:domain/test-domain/test-index/*",
        "arn:aws:es:us-west-1:987654321098:domain/test-domain/_bulk"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": [
        "es:ESHttpGet"
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/restricted-
index/*"
    }
  ]
}
```

Essa política concede acesso `test-user` total `test-index` e à API OpenSearch em massa. Ela também permite solicitações `GET` ao `restricted-index`.

A seguinte solicitação de indexação, como você pode esperar, falha devido a um erro de permissão:

```
PUT https://search-test-domain.us-west-1.es.amazonaws.com/restricted-index/movie/1
{
  "title": "Your Name",
  "director": "Makoto Shinkai",
  "year": "2016"
}
```

Ao contrário da API de índice, a API em massa permite criar, atualizar e excluir vários documentos em uma única chamada. Contudo, normalmente você especifica essas operações no corpo da solicitação, em vez de na URL da solicitação. Como o OpenSearch Service usa URLs para controlar o acesso aos sub-recursos do domínio, `test-user` pode, na verdade, usar a API em massa para fazer alterações em. `restricted-index` Embora o usuário não tenha permissões `POST` no índice, a seguinte solicitação é bem-sucedida:

```
POST https://search-test-domain.us-west-1.es.amazonaws.com/_bulk
```

```
{ "index" : { "_index": "restricted-index", "_type" : "movie", "_id" : "1" } }
{ "title": "Your Name", "director": "Makoto Shinkai", "year": "2016" }
```

Nesta situação, a política de acesso não consegue cumprir o que pretendia. Para evitar que os usuários ignorem esses tipos de restrições, você pode alterar o `rest.action.multi.allow_explicit_index` para o valor falso. Se esse valor for falso, todas as chamadas para as APIs em massa, mget e msearch, que especificam nomes de índice no corpo da solicitação irão parar de funcionar. Em outras palavras, as chamadas para `_bulk` não funcionam mais, mas as chamadas para o `test-index/_bulk` funcionam. Este segundo endpoint contém um nome de índice, portanto, você não precisa especificar um no corpo da solicitação.

OpenSearch Os painéis dependem muito de mget e msearch, portanto, é improvável que funcionem corretamente após essa alteração. Para correção parcial, você pode deixar o `rest.action.multi.allow_explicit_index` como verdadeiro e negar o acesso a determinados usuários para uma ou mais dessas APIs.

Para obter informações sobre como alterar essa configuração, consulte the section called “Configurações avançadas do cluster”.

Da mesma forma, a seguinte política baseada em recursos contém dois problemas sutis:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/test-user"
      },
      "Action": "es:ESHttp*",
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
    },
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/test-user"
      },
      "Action": "es:ESHttp*",
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/restricted-
index/*"
    }
```

```
  ]
}
```

- Apesar da negação explícita, o `test-user` ainda pode fazer chamadas, como `GET https://search-test-domain.us-west-1.es.amazonaws.com/_all/_search` e `GET https://search-test-domain.us-west-1.es.amazonaws.com/*/_search` para acessar os documentos no `restricted-index`.
- Como o elemento `Resource` faz referência ao `restricted-index/*`, o `test-user` não tem permissões para acessar diretamente os documentos do índice. O usuário, no entanto, tem permissões para excluir todo o índice. Para evitar o acesso e a exclusão, a política deve especificar `restricted-index*`.

Em vez de misturar permissões amplas e negações focadas, a abordagem mais segura é seguir o princípio do privilégio mínimo e conceder apenas as permissões necessárias para executar uma tarefa. Para obter mais informações sobre como controlar o acesso a índices ou OpenSearch operações individuais, consultethe section called “Controle de acesso refinado”.

> **Important**
>
> Especificar o caractere curinga * permite acesso anônimo ao seu domínio. Não é recomendável usar o caractere curinga. Além disso, inspecione cuidadosamente as seguintes políticas para confirmar se elas não concedem amplo acesso:
>
> - Políticas baseadas em identidade vinculadas aos AWS diretores associados (por exemplo, funções do IAM)
> - Políticas baseadas em recursos anexadas aos AWS recursos associados (por exemplo, chaves AWS Key Management Service KMS)

Configuração de políticas de acesso

- Para obter instruções sobre como criar ou modificar políticas baseadas em recursos e IP no OpenSearch Service, consulte. the section called “Configuração de políticas de acesso”
- Para obter instruções sobre como criar ou modificar políticas baseadas em identidade no IAM, consulte Criação de políticas do IAM no Manual do usuário do IAM.

Exemplos adicionais de políticas

Embora este capítulo inclua muitos exemplos de políticas, o controle de AWS acesso é um assunto complexo que é melhor compreendido por meio de exemplos. Para obter mais informações, consulte Exemplo de políticas baseadas em identidade do IAM noManual do usuário do IAM.

Referência de permissões da Amazon OpenSearch Service API

Ao configurar o controle de acesso, você escreve políticas de permissão que podem ser anexadas a uma identidade do IAM (políticas baseadas em identidade). Para obter informações de referência detalhadas, consulte os seguintes tópicos na Referência de autorização do serviço:

- Ações, recursos e chaves de condição para o OpenSearch Serviço.
- Ações, recursos e chaves de condição para OpenSearch ingestão.

Essa referência contém informações sobre quais operações de API do podem ser usadas em uma política do IAM. Também inclui o AWS recurso para o qual você pode conceder as permissões e as chaves de condição que você pode incluir para um controle de acesso refinado.

Você especifica as ações no campo `Action` da política, o valor de recurso no campo `Resource` da política e as condições no campo `Condition` da política. Para especificar uma ação para o OpenSearch Serviço, use o `es:` prefixo seguido pelo nome da operação da API (por exemplo,`es:CreateDomain`). Para especificar uma ação para OpenSearch ingestão, use o `osis:` prefixo seguido pela operação da API (por exemplo,`osis:CreatePipeline`).

AWS políticas gerenciadas para o Amazon OpenSearch Service

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que

atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) for lançada ou novas operações de API forem disponibilizadas para serviços existentes.

Para mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

AmazonOpenSearchServiceFullAccess

Concede acesso total às operações e recursos da API de configuração de OpenSearch serviços para um Conta da AWS.

Você pode encontrar a AmazonOpenSearchServiceFullAccesspolítica no console do IAM.

AmazonOpenSearchServiceReadOnlyAccess

Concede acesso somente de leitura a todos os recursos do OpenSearch Serviço para um. Conta da AWS

Você pode encontrar a AmazonOpenSearchServiceReadOnlyAccesspolítica no console do IAM.

AmazonOpenSearchServiceRolePolicy

Não é possível anexar `AmazonOpenSearchServiceRolePolicy` às entidades do IAM. Essa política está vinculada a uma função vinculada ao serviço que permite que o OpenSearch Serviço acesse os recursos da conta. Para ter mais informações, consulte the section called “Permissões”.

Você pode encontrar a AmazonOpenSearchServiceRolePolicypolítica no console do IAM.

AmazonOpenSearchServiceCognitoAccess

Fornece as permissões mínimas do Amazon Cognito necessárias para ativar a autenticação Cognito.

Você pode encontrar a AmazonOpenSearchServiceCognitoAccesspolítica no console do IAM.

AmazonOpenSearchIngestionServiceRolePolicy

Não é possível anexar `AmazonOpenSearchIngestionServiceRolePolicy` às entidades do IAM. Essa política está vinculada a uma função vinculada ao serviço que permite que a OpenSearch ingestão habilite o acesso à VPC para pipelines de ingestão, crie tags e publique métricas relacionadas à ingestão em sua conta. CloudWatch Para ter mais informações, consulte the section called “Usar funções vinculadas ao serviço”.

Você pode encontrar a AmazonOpenSearchIngestionServiceRolePolicypolítica no console do IAM.

AmazonOpenSearchIngestionFullAccess

Concede acesso total às operações e aos recursos da API de OpenSearch ingestão para um Conta da AWS.

Você pode encontrar a AmazonOpenSearchIngestionFullAccesspolítica no console do IAM.

AmazonOpenSearchIngestionReadOnlyAccess

Concede acesso somente de leitura a todos os recursos OpenSearch de ingestão para um. Conta da AWS

Você pode encontrar a AmazonOpenSearchIngestionReadOnlyAccesspolítica no console do IAM.

AmazonOpenSearchServerlessServiceRolePolicy

Fornece as Amazon CloudWatch permissões mínimas necessárias para enviar dados métricos OpenSearch sem servidor para o. CloudWatch

Você pode encontrar a AmazonOpenSearchServerlessServiceRolePolicypolítica no console do IAM.

OpenSearch Atualizações de serviços para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do OpenSearch Serviço desde que esse serviço começou a monitorar as alterações.

Alteração	Descrição	Data
Atualização do `AmazonOpenSearchServiceRolePolicy` e do `AmazonElasticsearchServiceRolePolicy` .	Foram adicionadas as permissões necessárias para que a função vinculada ao serviço atribua e cancele a atribuição de endereços IPv6. A política obsoleta do Elasticsearch também foi atualizada para garantir a compatibilidade com versões anteriores.	18 de outubro de 2023

Alteração	Descrição	Data
Adicionado `AmazonOpenSearchIngestionServiceRolePolicy`	Uma nova política que permite que a OpenSearch ingestão habilite o acesso à VPC para pipelines de ingestão, crie tags e publique métricas relacionadas à CloudWatch ingestão em sua conta. Para ver a política JSON, consulte o console do IAM.	26 de abril de 2023
Adicionado `AmazonOpenSearchIngestionFullAccess`	Uma nova política que concede acesso total às operações e aos recursos da API de OpenSearch ingestão para um Conta da AWS. Para ver a política JSON, consulte o console do IAM.	26 de abril de 2023
Adicionado `AmazonOpenSearchIngestionReadOnlyAccess`	Uma nova política que concede acesso somente de leitura a todos os recursos de OpenSearch ingestão para um. Conta da AWS Para ver a política JSON, consulte o console do IAM.	26 de abril de 2023

Alteração	Descrição	Data
Adicionado `AmazonOpenSearchServerlessServiceRolePolicy`	Uma nova política que fornece as permissões mínimas necessárias para enviar dados métricos OpenSearch sem servidor para o. Amazon CloudWatch Para ver a política JSON, consulte o console do IAM.	29 de novembro de 2022
Atualização do `AmazonOpenSearchServiceRolePolicy` e do `AmazonElasticsearchServiceRolePolicy` .	Foram adicionadas as permissões necessárias para que a função vinculada ao serviço crie VPC endpoints OpenSearch gerenciados por serviços. Algumas ações só podem ser executadas quando a solicitação contém a tag `OpenSearchManaged=true` . A política obsoleta do Elasticsearch também foi atualizada para garantir a compatibilidade com versões anteriores.	7 de novembro de 2022

Alteração	Descrição	Data
Atualização do `AmazonOpenSearchServiceRolePolicy` e do `AmazonElasticsearchServiceRolePolicy` .	Foi adicionado suporte para a `PutMetricData` ação, que é necessário para publicar métricas de OpenSearch cluster na Amazon CloudWatch. A política obsoleta do Elasticsearch também foi atualizada para garantir a compatibilidade com versões anteriores. Para ver a política JSON, consulte o console do IAM.	12 de setembro de 2022
Atualização do `AmazonOpenSearchServiceRolePolicy` e do `AmazonElasticsearchServiceRolePolicy` .	Adicionado suporte ao tipo de recurso `acm`. A política fornece a permissão mínima AWS Certificate Manager (ACM) somente leitura necessária para que a função vinculada ao serviço verifique e valide os recursos do ACM a fim de criar e atualizar domínios personalizados habilitados para endpoints. A política obsoleta do Elasticsearch também foi atualizada para garantir a compatibilidade com versões anteriores.	28 de julho de 2022

Alteração	Descrição	Data
Atualização do `AmazonOpenSearchServiceCognitoAccess` e do `AmazonESCognitoAccess` .	Foi adicionado suporte para a `UpdateUserPoolClient` ação, que é necessário para definir a configuração do grupo de usuários do Cognito durante a atualização do Elasticsearch para o. OpenSearch Permissões corrigidas para a ação `SetIdentityPoolRoles` para permitir o acesso a todos os recursos. A política obsoleta do Elasticsearch também foi atualizada para garantir a compatibilidade com versões anteriores.	20 de dezembro de 2021
Atualização do `AmazonOpenSearchServiceRolePolicy`	Adicionado suporte ao tipo de recurso `security-group` . A política fornece as permissões mínimas do Amazon EC2 e do Elastic Load Balancing necessárias para a função vinculada ao serviço habilitar o acesso à VPC.	9 de setembro de 2021

Alteração	Descrição	Data
• Adicionado `AmazonOpenSearchServiceFullAccess` • Defasada `AmazonESFullAccess`	Esta nova política destina-se a substituir a política antiga. Ambas as políticas fornecem acesso total à API OpenSearch de configuração do serviço e a todos os métodos HTTP das OpenSearch APIs. O controle de acesso refinado e as políticas baseadas em recursos ainda podem restringir o acesso.	7 de setembro de 2021
• Adicionado `AmazonOpenSearchServiceReadOnlyAccess` • Defasada `AmazonESReadOnlyAccess`	Esta nova política destina-se a substituir a política antiga. Ambas as políticas fornecem acesso somente de leitura à API OpenSearch de configuração do serviço (`es:Describe* es:List*`, `ees:Get*`) e nenhum acesso aos métodos HTTP das APIs. OpenSearch	7 de setembro de 2021
• Adicionado `AmazonOpenSearchServiceCognitoAccess` • Defasada `AmazonESCognitoAccess`	Esta nova política destina-se a substituir a política antiga. Ambas as políticas fornecem as permissões mínimas do Amazon Cognito necessárias para ativar a autenticação Cognito.	7 de setembro de 2021

Alteração	Descrição	Data
• Adicionado AmazonOpenSearchServiceRolePolicy • Defasada `AmazonElasticsearchServiceRolePolicy`	Esta nova política destina-se a substituir a política antiga. Ambas as políticas fornecem as permissões mínimas do Amazon EC2 e do Elastic Load Balancing necessárias para a função vinculada ao serviço habilitar o acesso à VPC.	7 de setembro de 2021
Início do rastreamento das alterações	O Amazon OpenSearch Service agora rastreia alterações nas políticas AWS gerenciadas.	7 de setembro de 2021

Prevenção contra o ataque “Confused deputy” em todos os serviços

O problema ‘confused deputy’ é um problema de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Em AWS, a personificação entre serviços pode resultar no problema do ‘confused deputy’. A personificação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado de modo a usar suas permissões para atuar nos recursos de outro cliente de uma forma na qual ele não deveria ter permissão para acessar. Para evitar isso, o AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com entidades principais de serviço que receberam acesso aos recursos em sua conta.

Recomendamos o uso das chaves de contexto de condição global `aws:SourceArn` e `aws:SourceAccount` em políticas de recursos para limitar as permissões que o Amazon OpenSearch Service concede para o recurso a outro serviço. Se o valor de `aws:SourceArn` não contiver o ID da conta, como um ARN de bucket do Amazon S3, você deverá usar ambas as chaves de contexto de condição global para limitar as permissões. Se você utilizar ambas as chaves de contexto de condição global, e o valor `aws:SourceArn` contiver o ID da conta, o valor

`aws:SourceAccount` e a conta no valor `aws:SourceArn` deverão utilizar o mesmo ID de conta quando utilizados na mesma declaração da política. Use `aws:SourceArn` se quiser que apenas um recurso seja associado ao acesso entre serviços. Use `aws:SourceAccount` se quiser permitir que qualquer recurso nessa conta seja associado ao uso entre serviços.

O valor de `aws:SourceArn` deve ser o ARN do domínio do OpenSearch Service.

A maneira mais eficaz de se proteger do problema 'confused deputy' é usar a chave de contexto de condição global `aws:SourceArn` com o ARN completo do recurso. Se você não souber o ARN completo do recurso ou se estiver especificando vários recursos, use a chave de condição de contexto global `aws:SourceArn` com curingas (*) para as partes desconhecidas do ARN. Por exemplo, `arn:aws:es:*:123456789012:*`.

O exemplo a seguir mostra como é possível usar as chaves de contexto de condição globais `aws:SourceArn` e `aws:SourceAccount` no OpenSearch Service para evitar o problema de "confused deputy".

```
{
   "Version":"2012-10-17",
   "Statement":{
      "Sid":"ConfusedDeputyPreventionExamplePolicy",
      "Effect":"Allow",
      "Principal":{
         "Service":"es.amazonaws.com"
      },
      "Action":"sts:AssumeRole",
      "Condition":{
         "StringEquals":{
            "aws:SourceAccount":"123456789012"
         },
         "ArnLike":{
            "aws:SourceArn":"arn:aws:es:region:123456789012:domain/my-domain"
         }
      }
   }
}
```

Controle de acesso refinado no Amazon Service OpenSearch

O controle de acesso refinado oferece formas adicionais de controlar o acesso aos seus dados no Amazon Service. OpenSearch Por exemplo, dependendo de quem faz a solicitação, você pode

querer que uma pesquisa retorne resultados de somente um índice. Talvez você queira ocultar determinados campos em seus documentos ou excluir determinados documentos completamente.

O controle de acesso refinado oferece os seguintes recursos:

- Controle de acesso com base em função
- Segurança no nível de índice, documento e campo
- OpenSearch Multilocação de painéis
- Autenticação básica HTTP para OpenSearch OpenSearch painéis

Tópicos

Visão geral: controle de acesso refinado e segurança de serviços OpenSearch

A segurança OpenSearch do Amazon Service tem três camadas principais:

Rede

A primeira camada de segurança é a rede, que determina se as solicitações chegam a um domínio OpenSearch de serviço. Se você escolher Acesso público ao criar um domínio, as solicitações de qualquer cliente conectado à Internet poderão chegar ao endpoint do domínio. Se você escolher o Acesso à VPC, os clientes devem se conectar à VPC (e os grupos de segurança associados devem permitir) para que uma solicitação chegue ao endpoint. Para ter mais informações, consulte the section called “Suporte à VPC”.

Política de acesso ao domínio

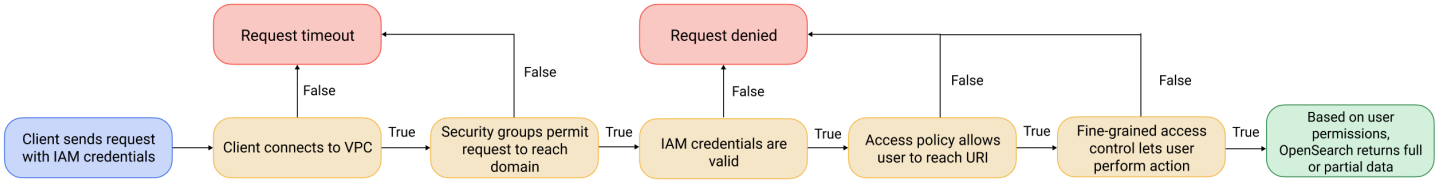
A segunda camada de segurança é a política de acesso ao domínio. Depois que uma solicitação chega a um endpoint do domínio, a política de acesso baseada em recursos permite ou nega o acesso da solicitação a um determinado URI. A política de acesso aceita ou rejeita solicitações na "borda" do domínio, antes que elas cheguem ao OpenSearch.

Controle de acesso refinado

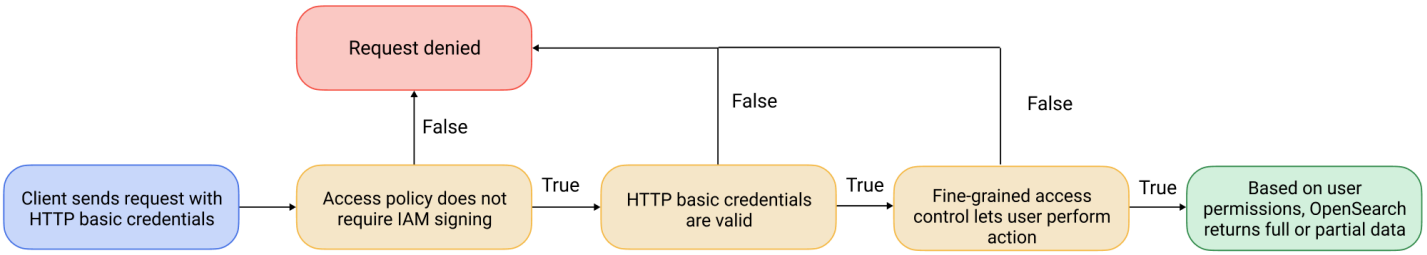
A terceira e última camada de segurança é o controle de acesso refinado. Depois que uma política de acesso baseada em recursos permitir que uma solicitação chegue a um endpoint do domínio, o controle de acesso refinado avaliará as credenciais do usuário e autenticará o usuário ou negará a solicitação. Se o controle de acesso refinado autenticar o usuário, ele obterá todas as funções mapeadas para esse usuário e usará o conjunto completo de permissões para determinar como lidar com a solicitação.

> **Note**
>
> Se uma política de acesso baseada em recursos contiver funções ou usuários do IAM, os clientes devem enviar solicitações assinadas usando o AWS Signature versão 4. Como tal, as políticas de acesso podem entrar em conflito com o controle de acesso refinado, especialmente se você usar o banco de dados interno de usuários e a autenticação básica HTTP. Não é possível assinar uma solicitação com um nome de usuário e senha e credenciais do IAM. Em geral, se você habilitar o controle de acesso refinado, recomendamos usar uma política de acesso ao domínio que não exija solicitações assinadas.

O diagrama a seguir ilustra uma configuração comum: um domínio de acesso da VPC com controle de acesso refinado habilitado, uma política de acesso baseada no IAM e um usuário primário do IAM.



O diagrama ilustra a seguir outra configuração comum: um domínio de acesso público com controle de acesso refinado habilitado, uma política de acesso que não usa os principais do IAM e um usuário primário no banco de dados de usuários interno.



Exemplo

Considere uma solicitação de `GET` para `movies/_search?q=thor`. O usuário tem permissões para pesquisar o índice `movies`? Em caso afirmativo, o usuário tem as permissões para exibir todos os documentos dentro dele? A resposta deve omitir ou tornar algum campo anônimo? Para o usuário primário, a resposta pode ser semelhante a esta:

```
{
  "hits": {
    "total": 7,
    "max_score": 8.772789,
    "hits": [{
        "_index": "movies",
        "_type": "_doc",
        "_id": "tt0800369",
        "_score": 8.772789,
        "_source": {
          "directors": [
            "Kenneth Branagh",
            "Joss Whedon"
          ],
          "release_date": "2011-04-21T00:00:00Z",
          "genres": [
```

```
            "Action",
            "Adventure",
            "Fantasy"
          ],
          "plot": "The powerful but arrogant god Thor is cast out of Asgard to
 live amongst humans in Midgard (Earth), where he soon becomes one of their finest
 defenders.",
          "title": "Thor",
          "actors": [
            "Chris Hemsworth",
            "Anthony Hopkins",
            "Natalie Portman"
          ],
          "year": 2011
        }
      },
      ...
    ]
  }
}
```

Se um usuário com permissões mais limitadas emitir exatamente a mesmo solicitação, a resposta pode ser semelhante a esta:

```
{
  "hits": {
    "total": 2,
    "max_score": 8.772789,
    "hits": [{
        "_index": "movies",
        "_type": "_doc",
        "_id": "tt0800369",
        "_score": 8.772789,
        "_source": {
          "year": 2011,
          "release_date":
 "3812a72c6dd23eef3c750c2d99e205cbd260389461e19d610406847397ecb357",
          "plot": "The powerful but arrogant god Thor is cast out of Asgard to
 live amongst humans in Midgard (Earth), where he soon becomes one of their finest
 defenders.",
          "title": "Thor"
        }
      },
```

```
      ...
    ]
  }
}
```

A resposta tem menos ocorrências e menos campos para cada ocorrência. Além disso, o campo `release_date` torna-se anônimo. Se um usuário sem permissões fizer a mesma solicitação, o cluster retornará um erro:

```
{
  "error": {
    "root_cause": [{
      "type": "security_exception",
      "reason": "no permissions for [indices:data/read/search] and User [name=limited-
user, roles=[], requestedTenant=null]"
    }],
    "type": "security_exception",
    "reason": "no permissions for [indices:data/read/search] and User [name=limited-
user, roles=[], requestedTenant=null]"
  },
  "status": 403
}
```

Se um usuário fornecer credenciais inválidas, o cluster retornará uma exceção `Unauthorized`.

Principais conceitos

Ao começar a usar o controle de acesso refinado, considere os seguintes conceitos:

- Funções — A principal forma de usar o controle de acesso refinado. Nesse caso, as funções são distintas das funções do IAM. As funções contêm qualquer combinação de permissões: nível de cluster, específica de índice, nível de documento e nível de campo.
- Mapeamento — Depois de configurar uma função, você a mapeia para um ou mais usuários. Por exemplo, é possível mapear três funções para um único usuário: uma função que fornece acesso ao Dashboards, uma que fornece acesso somente leitura ao `index1` e uma que fornece acesso de gravação ao `index2`. Ou, é possível incluir todas essas permissões em uma única função.
- Usuários — Pessoas ou aplicativos que fazem solicitações ao OpenSearch cluster. Os usuários têm credenciais, sejam chaves de acesso do IAM ou um nome de usuário e senha, que eles especificam quando fazem solicitações.

Sobre o usuário principal

O usuário principal no OpenSearch Service é uma combinação de nome de usuário e senha, ou um principal do IAM, que tem permissões completas para o OpenSearch cluster subjacente. Um usuário é considerado usuário principal se tiver todo o acesso ao OpenSearch cluster junto com a capacidade de criar usuários internos, funções e mapeamentos de funções nos OpenSearch painéis.

Um usuário mestre criado no console de OpenSearch serviço ou por meio da CLI é mapeado automaticamente para duas funções predefinidas:

- `all_access`— fornece acesso total a todas as operações em todo o cluster, permissão para gravar em todos os índices do cluster e permissão para gravar em todos os locatários.
- `security_manager`— Fornece acesso ao plug-in de segurança e gerenciamento de usuários e permissões.

Com essas duas funções, o usuário obtém acesso à guia Segurança nos OpenSearch painéis, onde pode gerenciar usuários e permissões. Se você criar outro usuário interno e mapeá-lo apenas para a `all_access` função, o usuário não terá acesso à guia Segurança. Você pode criar usuários mestres adicionais mapeando-os explicitamente para as `security_manager` funções `all_access` e. Para obter instruções, consulte the section called “Usuários primários adicionais”.

Ao criar um usuário mestre para seu domínio, você pode especificar um principal do IAM existente ou criar um usuário principal no banco de dados interno do usuário. Considere o seguinte ao decidir qual usar:

- IAM principal — Se você escolher um IAM principal para seu usuário principal, todas as solicitações para o cluster devem ser assinadas usando o AWS Signature Version 4.

  OpenSearch O serviço não leva em consideração nenhuma das permissões do diretor do IAM. O usuário ou a função do IAM serve apenas para autenticação. As políticas desse usuário ou função não têm relação com a autorização do usuário principal. A autorização é feita por meio de várias permissões no plug-in de OpenSearch segurança.

  Por exemplo, você pode atribuir zero permissões do IAM a um principal do IAM e, desde que a máquina ou pessoa possa se autenticar para esse usuário ou função, ela terá o poder do usuário mestre no OpenSearch Serviço.

Recomendamos o IAM se você quiser usar os mesmos usuários em vários clusters, se quiser usar o Amazon Cognito para acessar painéis ou se tiver OpenSearch clientes que ofereçam suporte à assinatura do Signature versão 4.

- Banco de dados interno do usuário — Se você criar um mestre no banco de dados interno do usuário (com uma combinação de nome de usuário e senha), poderá usar a autenticação básica HTTP (bem como as credenciais do IAM) para fazer solicitações ao cluster. A maioria dos clientes oferece suporte à autenticação básica, incluindo curl, que também oferece suporte à AWS Signature versão 4 com a opção --aws-sigv4. O banco de dados interno do usuário é armazenado em um OpenSearch índice, então você não pode compartilhá-lo com outros clusters.

  Recomendamos o banco de dados interno de usuários se você não precisar reutilizar usuários em vários clusters, se quiser usar a autenticação básica HTTP para acessar o Dashboards (em vez do Amazon Cognito) ou se você tiver clientes que oferecem suporte somente à autenticação básica. O banco de dados interno do usuário é a maneira mais simples de começar a usar o OpenSearch Service.

Habilitar o controle de acesso detalhado

Ative o controle de acesso refinado usando o console ou a API de AWS CLIconfiguração. Para obter as etapas, consulte Criação e gerenciamento de domínios.

O controle de acesso refinado requer o Elasticsearch OpenSearch 6.7 ou posterior. Também requer HTTPS para todo o tráfego para o domínio, criptografia de dados em repouso e node-to-node criptografia. Dependendo de como você configura os atributos avançados do controle de acesso detalhado, o processamento adicional de suas solicitações pode exigir atributos de computação e memória em nós de dados individuais. Depois que habilitar o controle de acesso refinado, não será possível desabilitá-lo.

Habilitação do controle de acesso refinado em domínios existentes

Você pode habilitar um controle de acesso refinado em domínios existentes em execução no Elasticsearch 6.7 OpenSearch ou posterior.

Para habilitar o controle de acesso refinado em um domínio existente (console)

1. Selecione o seu domínio e escolha Ações e, depois, Editar configurações de segurança.
2. Selecione Habilitar o controle de acesso refinado.

3. Escolha como criar o usuário primário:

   - Se você quiser usar o IAM para o gerenciamento de usuários, escolha Definir ARN do IAM como usuário primário e especifique o ARN para uma função do IAM.
   - Se quiser usar o banco de dados de usuário interno, escolha Criar usuário primário e especifique um nome de usuário e senha.

4. (Opcional) Selecione Habilitar o período de migração para política de acesso aberto/baseado em IP. Essa configuração viabiliza um período de transição de 30 dias durante o qual os usuários existentes podem continuar acessando o domínio sem interrupções e as políticas de acesso baseado em IP e aberto existentes continuarão funcionando com o seu domínio. Durante esse período de migração, recomendamos que os administradores criem as funções necessárias e as mapeiem para os usuários para o domínio. Se você usar políticas baseadas em identidade, em vez de uma política de acesso aberto ou baseado em IP, será possível desabilitar essa configuração.

   Você também precisa atualizar os seus clientes para trabalhar com controle de acesso refinado durante o período de migração. Por exemplo, se você mapear funções do IAM com controle de acesso refinado, você deve atualizar seus clientes para começar a assinar solicitações com o AWS Signature versão 4. Se você configurar a autenticação básica de HTTP com controle de acesso refinado, deverá atualizar os seus clientes para fornecer as credenciais de autenticação básicas apropriadas nas solicitações.

   Durante o período de migração, os usuários que acessarem o endpoint do OpenSearch Dashboards do domínio acessarão diretamente a página Discover em vez da página de login. Os administradores e usuários primários podem escolher Login para fazer login com credenciais de administrador e configurar mapeamentos de funções.

   > **Important**
   >
   > OpenSearch O serviço desativa automaticamente o período de migração após 30 dias. Recomendamos encerrá-lo assim que você criar as funções necessárias e mapeá-las para os usuários. Após o término do período de migração, não será possível habilitá-lo novamente.

5. Escolha Salvar alterações.

A alteração aciona uma implantação azul-verde durante a qual a integridade do cluster fica vermelha, mas todas as operações do cluster permanecem inalteradas.

Para habilitar o controle de acesso refinado em um domínio existente (CLI)

Configure `AnonymousAuthEnabled` como `true` para habilitar o período de migração com controle de acesso refinado:

```
aws opensearch update-domain-config --domain-name test-domain --region us-east-1 \
      --advanced-security-options '{ "Enabled": true,
 "InternalUserDatabaseEnabled":true, "MasterUserOptions": {"MasterUserName":"master-
username","MasterUserPassword":"master-password"},"AnonymousAuthEnabled": true}'
```

Sobre o default_role

O controle de acesso refinado exige o mapeamento de funções. Se seu domínio usa políticas de acesso baseadas em identidade, o OpenSearch Service mapeia automaticamente seus usuários para uma nova função chamada default_role para ajudá-lo a migrar adequadamente os usuários existentes. Esse mapeamento temporário garante que os seus usuários ainda possam enviar com êxito solicitações GET e PUT assinadas pelo IAM até que você crie seus próprios mapeamentos de função.

A função não adiciona nenhuma vulnerabilidade ou falha de segurança ao seu domínio do OpenSearch Serviço. Recomendamos excluir a função padrão assim que você configurar suas próprias funções e mapeá-las adequadamente.

Cenários de migração

A tabela a seguir descreve o comportamento de cada método de autenticação antes e depois de habilitar o controle de acesso refinado em um domínio existente, assim como as etapas que os administradores devem seguir para mapear corretamente seus usuários para funções:

Método de autenticação	Antes de habilitar o controle de acesso refinado	Depois de habilitar o controle de acesso refinado	Tarefas do administrador
Políticas baseadas em identidade	Todos os usuários que cumprem a política do IAM podem acessar o domínio.	Não é necessário habilitar o período de migração. OpenSearch O serviço mapeia automaticamente todos os usuários que atendem à política do IAM para o default_role para que eles possam continuar acessando o domínio.	1. Crie mapeamentos de função personalizados no domínio. 2. Exclua a default_role.
Políticas baseadas em IP	Todos os usuários dos endereços IP ou blocos CIDR permitidos podem acessar o domínio.	Durante o período de migração de 30 dias, todos os usuários dos endereços IP ou blocos CIDR permitidos poderão continuar acessando o domínio.	1. Crie mapeamentos de função personalizados no domínio. 2. Atualize os seus clientes para fornecer credenciais de autenticação básicas ou credenciais do IAM, dependendo da sua configuração de mapeamento de função. 3. Encerre o período de migração. Os usuários dos endereços IP ou blocos CIDR permitidos enviando solicitações sem autenticação básica ou credenciais do IAM perderão o acesso ao domínio.
Políticas de acesso aberto	Todos os usuários na Internet	Durante o período de migração de 30 dias, todos os usuários	1. Crie mapeamentos de função no domínio.

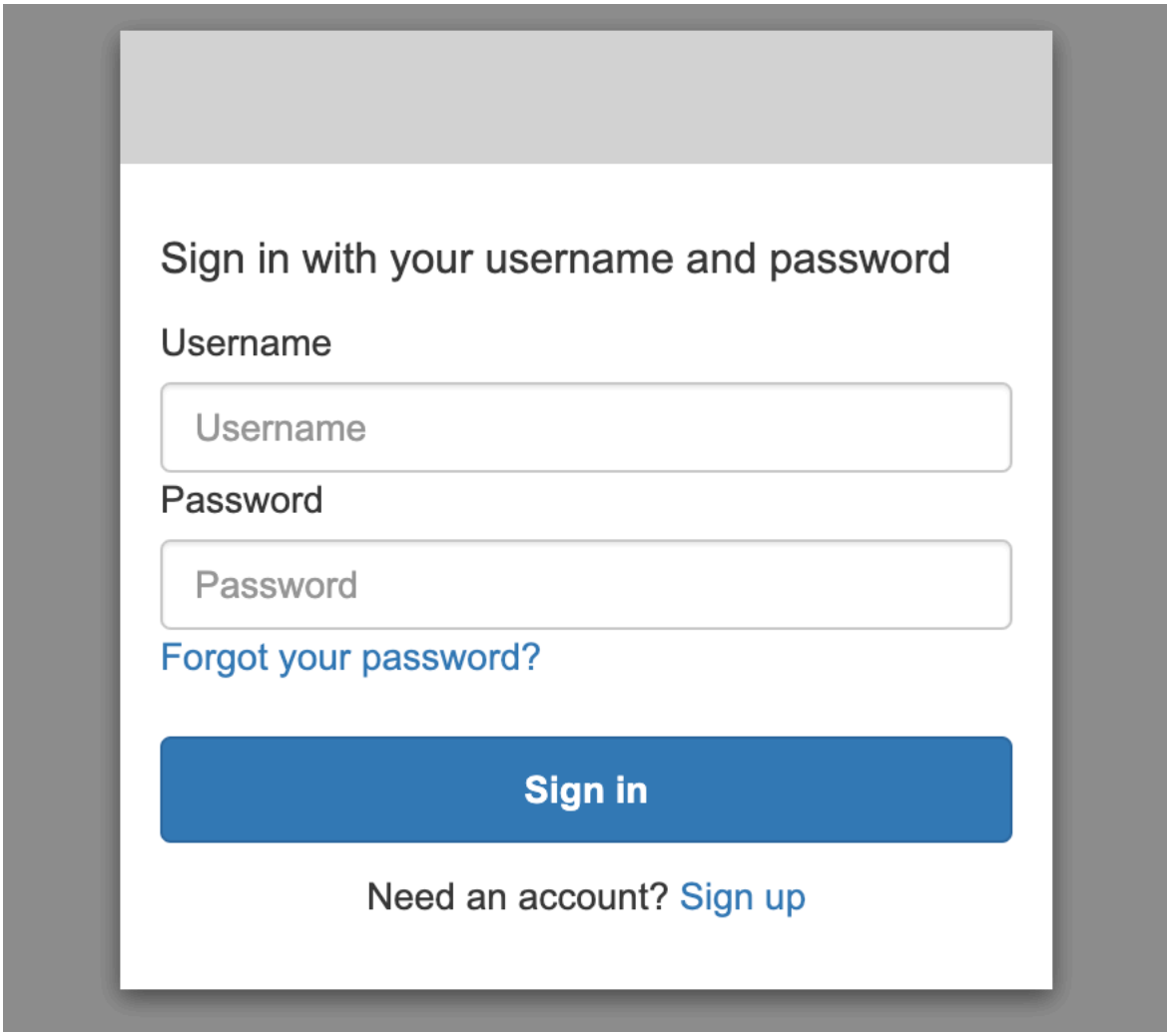
Método de autenticação	Antes de habilitar o controle de acesso refinado	Depois de habilitar o controle de acesso refinado	Tarefas do administrador
	podem acessar o domínio.	na Internet podem continuar acessando o domínio.	2. Atualize os seus clientes para fornecer credenciais de autentica ção básicas ou credenciais do IAM, dependendo da sua configuração de mapeamento de função. 3. Encerre o período de migração. Os usuários que enviarem solicitaç ões sem autenticação básica ou credenciais do IAM perderão o acesso ao domínio.

Acessando OpenSearch painéis como usuário principal

O controle de acesso refinado tem um plug-in de OpenSearch painéis que simplifica as tarefas de gerenciamento. Você pode usar o Dashboard para gerenciar usuários, funções, mapeamentos, grupos de ação e locatários. No entanto, a página de login do OpenSearch Dashboards e o método de autenticação subjacente diferem, dependendo de como você gerencia os usuários e configura seu domínio.

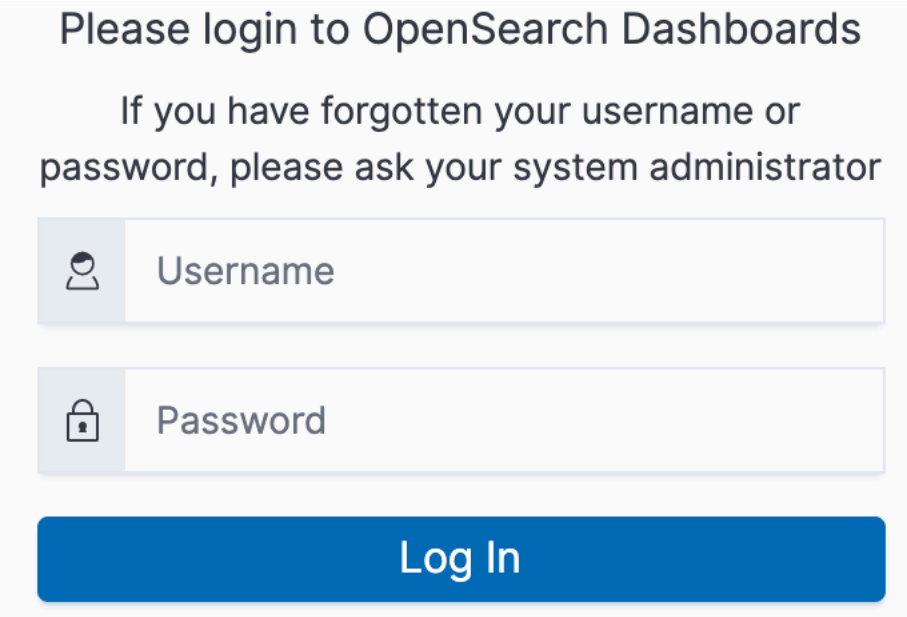
- Se desejar usar o IAM para o gerenciamento de usuários, use the section called “Autenticação do Amazon Cognito para OpenSearch Dashboards” para acessar o Dashboards. Caso contrário, o Dashboards exibirá uma página de login não funcional. Consulte the section called “Limitações”.

  Com a autenticação do Amazon Cognito, uma das funções assumidas do grupo de identidades deve corresponder à função do IAM especificada para o usuário primário. Para obter mais informações sobre essa configuração, consulte the section called “(Opcional) Configuração de acesso granular” e the section called “Tutorial: Controle de acesso minucioso com autenticação Cognito”.



- Se você escolher usar o banco de dados de usuário interno, você pode fazer login no Painéis com seu nome de usuário principal e senha. Você deverá acessar o Dashboards via HTTPS. O Amazon Cognito e a autenticação SAML para Dashboards substituem essa tela de login.

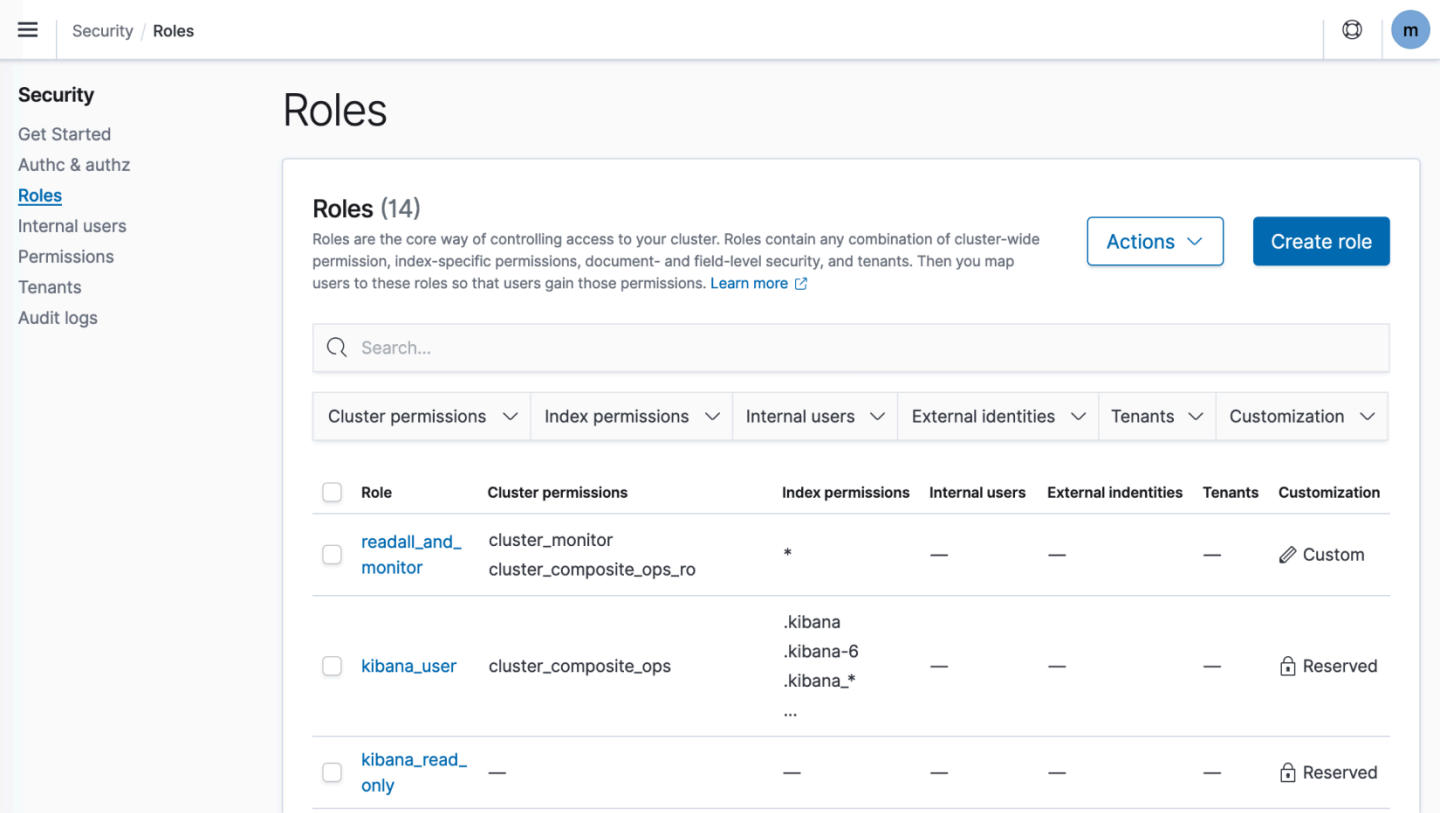
  Para obter mais informações sobre essa configuração, consulte the section called “Tutorial: Banco de dados interno de usuários com autenticação básica”.



- Se você optar por usar a autenticação SAML, poderá entrar usando credenciais de um provedor de identidade externo. Para ter mais informações, consulte the section called “Autenticação SAML para painéis OpenSearch ”.

Gerenciar permissões

Conforme observado em the section called “Principais conceitos”, você gerencia permissões de controle de acesso refinado usando funções, usuários e mapeamentos. Esta seção descreve como criar e aplicar esses recursos. Recomendamos fazer login no Dashboards como o usuário primário para executar essas operações.



> **Note**
>
> As permissões que você escolhe conceder aos usuários variam amplamente com base no caso de uso. Não podemos cobrir todos os cenários nesta documentação. Ao determinar quais permissões conceder aos seus usuários, faça referência às permissões de OpenSearch cluster e índice mencionadas nas seções a seguir e sempre siga o princípio do privilégio mínimo.

Criar funções

Você pode criar novas funções para um controle de acesso refinado usando OpenSearch painéis ou a `_plugins/_security` operação na API REST. Para obter mais informações, consulte Criar funções.

O controle de acesso refinado também inclui várias funções predefinidas. Clientes como OpenSearch Dashboards e Logstash fazem uma grande variedade de solicitações OpenSearch, o que pode dificultar a criação manual de funções com o conjunto mínimo de permissões. Por exemplo, a função `opensearch_dashboards_user` inclui as permissões de que um usuário precisa para

criar padrões de índice, visualizações, painéis e locatários. Recomendamos mapeá-la em qualquer função de usuário ou de backend que acesse o Dashboards, juntamente com funções adicionais que permitam o acesso a outros índices.

O Amazon OpenSearch Service não oferece as seguintes OpenSearch funções:

- `observability_full_access`
- `observability_read_access`
- `reports_read_access`
- `reports_full_access`

O Amazon OpenSearch Service oferece várias funções que não estão disponíveis com OpenSearch:

- `ultrawarm_manager`
- `ml_full_access`
- `cold_manager`
- `notifications_full_access`
- `notifications_read_access`

Segurança em nível de cluster

As permissões em nível de cluster incluem a capacidade de realizar solicitações amplas, como `_mget`, `_msearch` e `_bulk`, monitorar a integridade, obter snapshots e muito mais. Gerencie essas permissões usando a seção Permissões do cluster ao criar uma função. Para obter a lista completa das permissões no nível do cluster, consulte Permissões de cluster.

Em vez de usar permissões individuais, muitas vezes você pode alcançar a postura de segurança desejada usando uma combinação dos grupos de ação padrão. Para obter uma lista de grupos de ação no nível do cluster, consulte Nível do cluster.

Segurança em nível de índice

As permissões no nível do índice incluem a capacidade de criar novos índices, pesquisar índices, ler e escrever documentos, excluir documentos, gerenciar aliases e muito mais. Gerencie essas permissões usando a seção Permissões do índice ao criar uma função. Para obter a lista completa das permissões no nível do índice, consulte Permissões de índice.

Em vez de usar permissões individuais, muitas vezes você pode alcançar a postura de segurança desejada usando uma combinação dos grupos de ação padrão. Para obter uma lista de grupos de ação no nível do índice, consulte Nível do índice.

Segurança em nível de documento

A segurança no nível do documento permite restringir quais documentos em um índice um usuário pode ver. Ao criar uma função, especifique um padrão de índice e uma OpenSearch consulta. Qualquer usuário mapeado para essa função poderá ver somente os documentos que correspondam à consulta. A segurança no nível do documento afeta o número de ocorrências que você recebe ao pesquisar.

Para obter mais informações, consulte Segurança em nível de documento.

Segurança em nível de campo

A segurança no nível do campo permite controlar quais campos de documento um usuário pode ver. Ao criar uma função, adicione uma lista de campos a serem incluídos ou excluídos. Se você incluir campos, os usuários que você mapear para essa função poderão ver somente esses campos. Se você excluir campos, eles poderão ver todos os campos exceto os excluídos. A segurança no nível do campo afeta o número de campos incluídos em ocorrências ao pesquisar.

Para obter mais informações, consulte Segurança em nível de campo.

Mascaramento de campo

O mascaramento de campo é uma alternativa à segurança no nível do campo que permite que você torne os dados anônimos em um campo em vez de removê-los completamente. Ao criar uma função, adicione uma lista de campos a serem mascarados. O mascaramento de campo afeta a possibilidade de ver o conteúdo de um campo ao pesquisar.

> **Tip**
>
> Se você aplicar o mascaramento padrão a um campo, o OpenSearch Service usará um hash seguro e aleatório que pode causar resultados de agregação imprecisos. Para executar agregações em campos mascarados, use o mascaramento baseado em padrões.

Criar usuários

Se você ativou o banco de dados interno do usuário, poderá criar usuários usando OpenSearch painéis ou a `_plugins/_security` operação na API REST. Para obter mais informações, consulte Criar usuários.

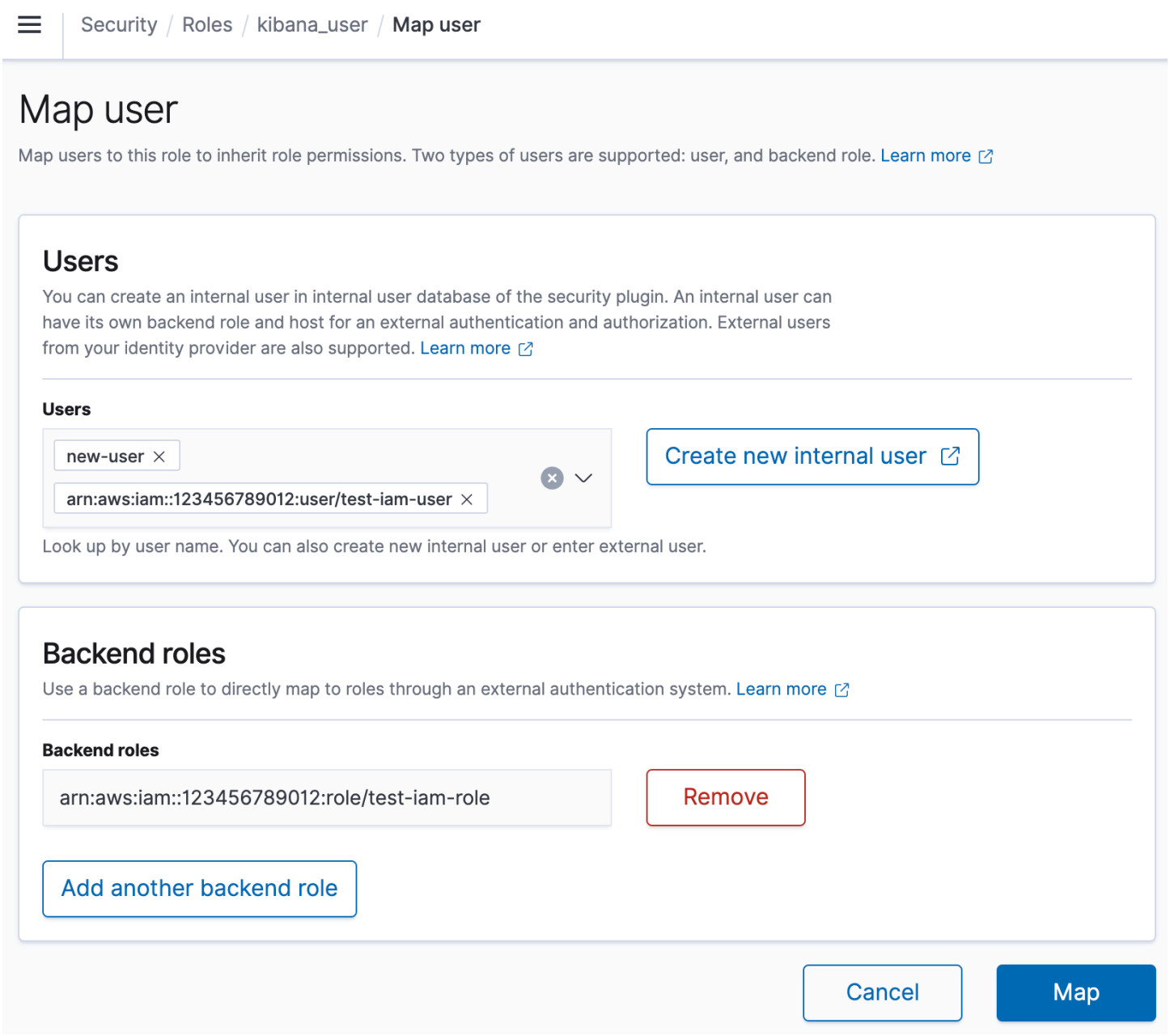
Se você escolheu o IAM para seu usuário primário, ignore esta parte do Dashboards. Crie perfis do IAM. Para obter mais informações, consulte o Manual do usuário do IAM.

Mapear funções em usuários

O mapeamento de função é o aspecto mais crítico do controle de acesso refinado. O controle de acesso refinado tem algumas funções predefinidas para ajudar a começar, mas a menos que você mapeie funções para os usuários, cada solicitação ao cluster terminará em um erro de permissões.

As funções de back-end podem ajudar a simplificar o processo de mapeamento de funções. Em vez de mapear a mesma perfil para 100 usuários individuais, é possível mapear a perfil para uma única perfil de backend. Todos os 100 usuários compartilham. As funções de backend podem ser funções do IAM ou strings arbitrárias.

- Especifique usuários, ARNs de usuário e strings de usuário do Amazon Cognito na seção Usuários. As strings de usuário do Cognito assumem a forma de `Cognito/`*`user-pool-id`*`/`*`username`*.
- Especifique funções de backend e ARNs de função do IAM na seção Funções de backend.



Você pode mapear funções para usuários usando OpenSearch painéis ou a `_plugins/_security` operação na API REST. Para obter mais informações sobre as funções de usuário, consulte Mapear usuários em funções.

Criação de grupos de ação

Grupos de ação são conjuntos de permissões que podem ser reutilizados em diferentes recursos. Você pode criar novos grupos de ação usando OpenSearch painéis ou a `_plugins/_security` operação na API REST, embora os grupos de ação padrão sejam suficientes para a maioria dos

casos de uso. Para obter mais informações sobre os grupos de ação padrão, consulte Grupos de ação padrão.

OpenSearch Multilocação de painéis

Locatários são espaços para salvar padrões de índice, visualizações, painéis e outros objetos do Dashboards. A locação múltipla dos Painéis permite que você compartilhe seu trabalho de forma segura com outros usuários dos Painéis (ou mantenha-o privado) e configure as locações dinamicamente. É possível controlar quais funções têm acesso a um locatário e se essas funções têm acesso de leitura ou gravação. O inquilino global é o padrão. Para saber mais, consulte Multilocação de OpenSearch painéis.

Como visualizar o locatário atual ou alterar locatários

1. Navegue até OpenSearch Painéis e faça login.
2. Selecione o ícone de usuário no canto superior direito e escolha Alternar locatários.
3. Verifique seu locatário antes de criar visualizações ou painéis. Se você deseja compartilhar seu trabalho com todos os outros usuários do Dashboards, escolha Global. Para compartilhar seu trabalho com um subconjunto de usuários do Dashboards, escolha um locatário compartilhado diferente. Caso contrário, escolha Privado.

> **Note**
>
> OpenSearch Os painéis mantêm um índice separado para cada inquilino e criam um modelo de índice chamado. `tenant_template` Não exclua nem modifique o `tenant_template` índice, pois isso pode causar mau funcionamento dos OpenSearch painéis se o mapeamento do índice do inquilino estiver configurado incorretamente.

Configurações recomendadas

Devido à forma como o controle de acesso refinadointerage com outros recursos de segurança, recomendamos várias configurações de controle de acesso refinado que funcionam bem na maioria dos casos de uso.

Descrição	Usuário primário	Política de acesso ao domínio
Use as credenciais do IAM para chamadas para as OpenSearch APIs e use a autenticação SAML para acessar os painéis. Gerencie funções de controle de acesso detalhado usando o Dashboards ou a API REST.	Usuário ou perfil do IAM	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "*" }, "Action": "es:ESHttp*", "Resource": " domain-arn /*" } ] }`
Use credenciais do IAM ou autenticação básica para chamadas para as OpenSearch APIs. Gerencie funções de controle de acesso detalhado usando o Dashboards ou a API REST. Essa configuração oferece muita flexibilidade, especialmente se você tiver OpenSearch clientes que oferecem suporte apenas à autenticação básica. Se você tiver um provedor de identidade existente, use a Autenticação	Nome de usuário e senha	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "*" }, "Action": "es:ESHttp*", "Resource": " domain-arn /*" } ] }`

Descrição	Usuário primário	Política de acesso ao domínio
do SAML para acessar o Dashboards. Caso contrário, gerencie usuários do Dashboard s no banco de dados interno de usuários.		
Use as credenciais do IAM para chamadas para as OpenSearch APIs e use o Amazon Cognito para acessar painéis. Gerencie funções de controle de acesso detalhado usando o Dashboards ou a API REST.	Usuário ou perfil do IAM	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "*" }, "Action": "es:ESHttp*", "Resource": " domain-arn /*" } ] }`

Descrição	Usuário primário	Política de acesso ao domínio

Use as credenciais do IAM para chamadas para as OpenSearch APIs e bloqueie a maior parte do acesso aos painéis. Gerencie funções de controle de acesso refinado usando a API REST.	Usuário ou perfil do IAM	{
		"Version": "2012-10-17",
		"Statement": [
		{
		"Effect": "Allow",
		"Principal": {
		"AWS": "*"
		},
		"Action": "es:ESHttp*",
		"Resource": " *domain-arn* /*"
		},
		{
		"Effect": "Deny",
		"Principal": {
		"AWS": "*"
		},
		"Action": "es:ESHttp*",
		"Resource": " *domain-arn* /_dashboards*"
		}
		]
		}

Limitações

O controle de acesso refinado tem várias limitações importantes:

- O aspecto `hosts` dos mapeamentos de função, que mapeia funções para os nomes de host ou endereços IP, não funcionará se o domínio estiver dentro de uma VPC. Ainda assim, é possível mapear funções para usuários e funções de backend.
- Se você escolher o IAM para o usuário primário e não habilitar a autenticação do Amazon Cognito ou SAML, o Dashboards exibirá uma página de login não funcional.
- Se você escolher o IAM para o usuário primário, ainda poderá criar usuários no banco de dados interno de usuários. No entanto, como a autenticação básica HTTP não está habilitada nesta configuração, quaisquer pedidos assinados com essas credenciais de utilizador serão rejeitados.

- Se utilizar o SQL para consultar um índice ao qual você não tenha acesso, receberá um erro "sem permissões". Se o índice não existir, você receberá um erro "Índice não existe". Essa diferença nas mensagens de erro significa que você pode confirmar a existência de um índice se adivinhar seu nome.

  Para minimizar o problema, não inclua informações confidenciais em nomes de índice. Para negar todo o acesso ao SQL, adicione o seguinte elemento à sua política de acesso ao domínio:

```
{
  "Effect": "Deny",
  "Principal": {
    "AWS": [
      "*"
    ]
  },
  "Action": [
    "es:*"
  ],
  "Resource": "arn:aws:es:us-east-1:123456789012:domain/my-domain/_plugins/_sql"
}
```

- Se a versão do seu domínio for 2.3 ou superior e você tiver um controle de acesso detalhado ativado, `max_clause_count` a configuração como 1 causará problemas com seu domínio. Recomendamos definir essa conta para um número maior.
- Se você estiver habilitando o controle de acesso refinado em um domínio em que o controle de acesso refinado não está configurado, para fontes de dados criadas para consulta direta, você mesmo precisará configurar funções de controle de acesso refinadas. Para obter mais informações sobre como configurar funções de acesso refinadas, consulte Criação de integrações de fontes de dados do Amazon OpenSearch Service com o Amazon S3.

Modificação do usuário primário

Se você esquecer os detalhes do usuário primário, poderá reconfigurá-lo usando o console, a AWS CLIou a API de configuração.

Como modificar o usuário primário (console)

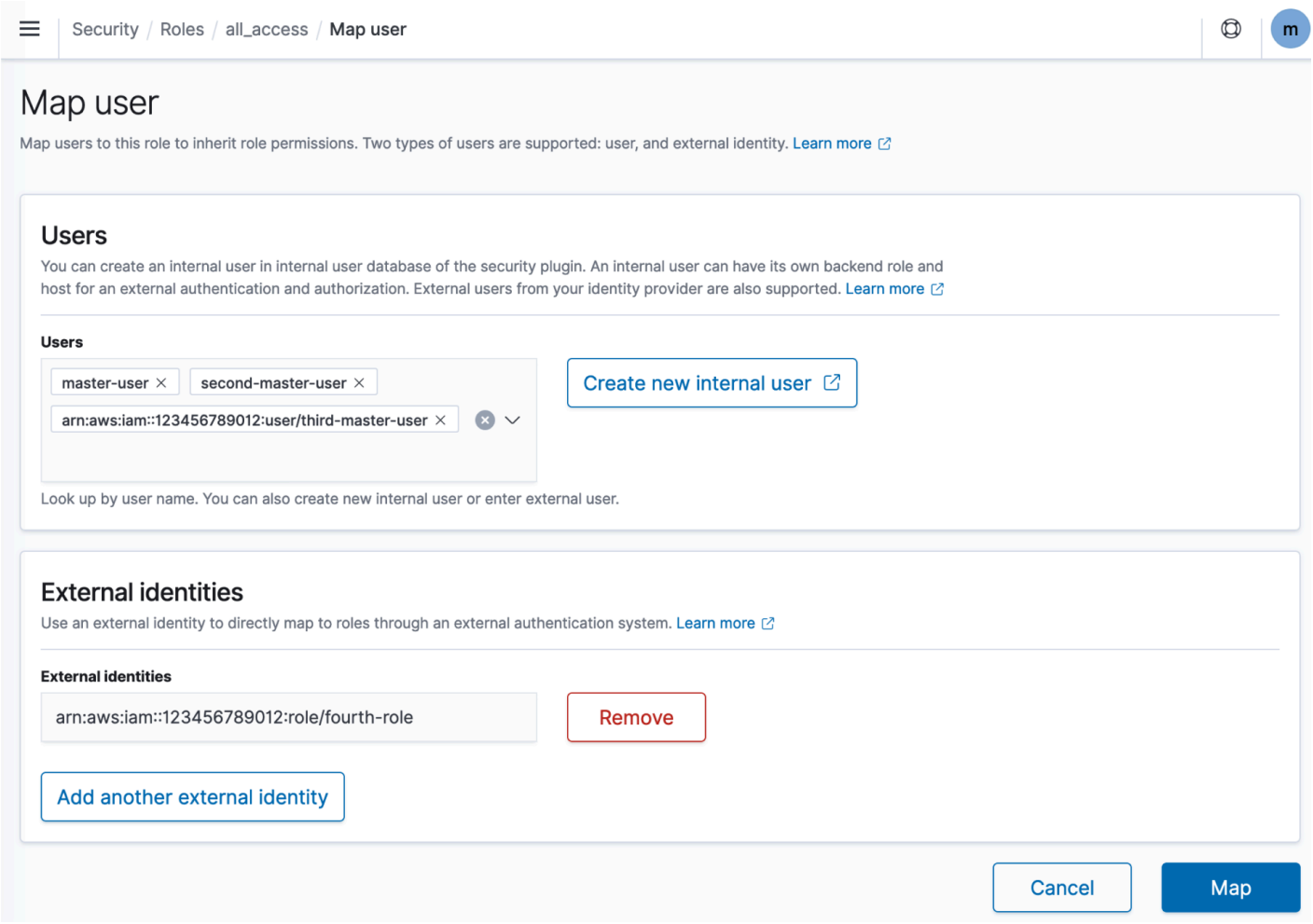
1. Navegue até o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home/.

2. Escolha o seu domínio e escolha Ações, Editar configurações de segurança.
3. Escolha Definir ARN do IAM como usuário primário ou Criar novo usuário primário.
   - Se você usou anteriormente um usuário primário do IAM, o controle de acesso refinado mapeará novamente a função `all_access` para o novo ARN do IAM especificado.
   - Se você usou anteriormente o banco de dados interno de usuários, o controle de acesso refinado criará um novo usuário primário. É possível usar o novo usuário primário para excluir o antigo.
   - A mudança do banco de dados de usuário interno para um usuário primário do IAM não exclui os usuários do banco de dados interno de usuários. Em vez disso, ela apenas desabilita a autenticação básica HTTP. Exclua manualmente os usuários do banco de dados interno do usuário ou mantenha-os para o caso de precisar reativar a autenticação básica HTTP.
4. Escolha Salvar alterações.

Usuários primários adicionais

Você designa um usuário primário ao criar um domínio, mas, se desejar, pode usar esse usuário primário para criar usuários primários adicionais. Você tem duas opções: OpenSearch painéis ou a API REST.

- No Dashboards, escolha Segurança, Funções e mapeie o novo usuário primário nas funções `all_access` e `security_manager`.



- Para usar a API REST, envie as seguintes solicitações:

```
PUT _plugins/_security/api/rolesmapping/all_access
{
  "backend_roles": [
    "arn:aws:iam::123456789012:role/fourth-master-user"
  ],
  "hosts": [],
  "users": [
    "master-user",
    "second-master-user",
    "arn:aws:iam::123456789012:user/third-master-user"
  ]
}
```

```
PUT _plugins/_security/api/rolesmapping/security_manager
{
```

```
  "backend_roles": [
    "arn:aws:iam::123456789012:role/fourth-master-user"
  ],
  "hosts": [],
  "users": [
    "master-user",
    "second-master-user",
    "arn:aws:iam::123456789012:user/third-master-user"
  ]
}
```

Essas solicitações substituem os mapeamentos de função atuais, portanto, execute as solicitações `GET` primeiro para que você possa incluir todas as funções atuais nas solicitações `PUT`. A API REST será especialmente útil se você não conseguir acessar o Dashboards e quiser mapear uma função do IAM do Amazon Cognito na função `all_access`.

Snapshots manuais

O controle de acesso refinado apresenta algumas complicações adicionais quando são tirados snapshots manuais. Para registrar um repositório de snapshots, mesmo que use a autenticação básica HTTP para todos os outros fins, você deve mapear a função `manage_snapshots` em uma função do IAM que tenha permissões `iam:PassRole` para assumir `TheSnapshotRole`, conforme definido nos the section called “Pré-requisitos”.

Depois, use essa função do IAM para enviar uma solicitação assinada ao domínio, conforme descrito em the section called “Registro de um repositório de snapshots manuais”.

Integrações

Se você usa outros AWS serviços com o OpenSearch Service, deve fornecer as funções do IAM para esses serviços com as permissões apropriadas. Por exemplo, os streams de entrega do Firehose geralmente usam uma função do IAM chamada. `firehose_delivery_role` No Dashboards, crie uma função para o controle de acesso refinado e mapeie a função do IAM nela. Nesse caso, a nova função precisará das seguintes permissões:

```
{
  "cluster_permissions": [
    "cluster_composite_ops",
    "cluster_monitor"
```

```
  ],
  "index_permissions": [{
    "index_patterns": [
      "firehose-index*"
    ],
    "allowed_actions": [
      "create_index",
      "manage",
      "crud"
    ]
  }]
}
```

As permissões variam de acordo com as ações que cada serviço executa. Uma AWS IoT regra ou AWS Lambda função que indexa dados provavelmente precisa de permissões semelhantes às do Firehose, enquanto uma função Lambda que só realiza pesquisas pode usar um conjunto mais limitado.

Diferenças de API REST

A API REST de controle de acesso refinada difere um pouco dependendo da sua OpenSearch versão /Elasticsearch. Antes de fazer uma solicitação PUT, faça uma solicitação GET para verificar o corpo da solicitação esperada. Por exemplo, uma solicitação GET para `_plugins/_security/api/user` retornar todos os usuários, que poderá ser modificada e usada para fazer solicitações PUT válidas.

No Elasticsearch 6.x, as solicitações para criar usuários são semelhantes a:

```
PUT _opendistro/_security/api/user/new-user
{
  "password": "some-password",
  "roles": ["new-backend-role"]
}
```

No OpenSearch Elasticsearch 7.x, as solicitações têm a seguinte aparência (altere `_plugins` para `_opendistro` se estiver usando o Elasticsearch):

```
PUT _plugins/_security/api/user/new-user
{
  "password": "some-password",
  "backend_roles": ["new-backend-role"]
```

```
}
```

Além disso, os locatários são propriedades de funções no Elasticsearch 6.x:

```
GET _opendistro/_security/api/roles/all_access

{
  "all_access": {
    "cluster": ["UNLIMITED"],
    "tenants": {
      "admin_tenant": "RW"
    },
    "indices": {
      "*": {
        "*": ["UNLIMITED"]
      }
    },
    "readonly": "true"
  }
}
```

No OpenSearch Elasticsearch 7.x, eles são objetos com seu próprio URI (altere `_plugins` para `_opendistro` se estiver usando o Elasticsearch)::

```
GET _plugins/_security/api/tenants

{
  "global_tenant": {
    "reserved": true,
    "hidden": false,
    "description": "Global tenant",
    "static": false
  }
}
```

Para obter a documentação sobre a API OpenSearch REST, consulte a referência da API do plug-in de segurança.

> **Tip**
>
> Se usar o banco de dados de usuário interno, você poderá usar curl para fazer solicitações e testar seu domínio. Teste os seguintes comandos de exemplo:

```
curl -XGET -u 'master-user:master-user-password' 'domain-endpoint/_search'
curl -XGET -u 'master-user:master-user-password' 'domain-endpoint/_plugins/
_security/api/user'
```

Tutorial: Configuração de um domínio com um usuário primário do IAM e autenticação do Amazon Cognito

Este tutorial aborda um caso de uso popular do Amazon OpenSearch Service para controle de acesso refinado: um usuário mestre do IAM com autenticação do Amazon Cognito para painéis. OpenSearch

No tutorial, configuraremos um perfil do IAM principal e um perfil do IAM limitado, que depois associaremos aos usuários no Amazon Cognito. O usuário principal pode então entrar nos OpenSearch painéis, mapear o usuário limitado para uma função e usar um controle de acesso refinado para limitar as permissões do usuário.

Embora essas etapas usem o grupo de usuários do Amazon Cognito para a autenticação, esse mesmo processo básico funciona para qualquer provedor de autenticação do Cognito que permita atribuir diferentes funções do IAM a usuários diferentes.

Você concluirá as seguintes etapas neste tutorial:

1. Criar perfis do IAM principais e limitado
2. Criar um domínio com a autenticação Cognito
3. Configurar um grupo de usuários e um banco de identidades do Cognito
4. Mapeie funções em OpenSearch painéis
5. Testas as permissões

Etapa 1: Criar perfis do IAM principal e limitado

Navegue até o console AWS Identity and Access Management (IAM) e crie duas funções separadas:

- `MasterUserRole`: o usuário principal, que terá permissões completas para o cluster e gerencia funções e mapeamentos de função.
- `LimitedUserRole`: um perfil mais restrito, à qual você concederá acesso limitado como usuário principal.

Para obter instruções sobre como criar os perfis, consulte Criação de um perfil usando políticas de confiança personalizadas.

Ambos os perfis devem ter a política de confiança a seguir, que permite que seu grupo de identidades do Cognito assuma os perfis:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Federated": "cognito-identity.amazonaws.com"
    },
    "Action": "sts:AssumeRoleWithWebIdentity",
    "Condition": {
      "StringEquals": {
        "cognito-identity.amazonaws.com:aud": "{identity-pool-id}"
      },
      "ForAnyValue:StringLike": {
        "cognito-identity.amazonaws.com:amr": "authenticated"
      }
    }
  }]
}
```

> **Note**
>
> Substitua `identity-pool-id` pelo identificador exclusivo do seu grupo de identidades do Amazon Cognito. Por exemplo, `us-east-1:0c6cdba7-3c3c-443b-a958-fb9feb207aa6`.

Etapa 2: Criar um domínio com a autenticação Cognito

Navegue até o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home/ e crie um domínio com as seguintes configurações:

- OpenSearch 1.0 ou posterior, ou Elasticsearch 7.8 ou posterior
- Acesso público
- Controle de acesso minucioso habilitado com `MasterUserRole` como usuário principal (criado na etapa anterior)
- Autenticação do Amazon Cognito habilitada para painéis OpenSearch . Para obter instruções para habilitar a autenticação do Cognito e selecionar um usuário e um grupo de identidades, consulte the section called “Configuração de um domínio para uso da autenticação do Amazon Cognito”.
- A seguinte política de acesso ao domínio:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::{account-id}:role/*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:{region}:{account-id}:domain/{domain-name}/*"
    }
  ]
}
```

- HTTPS necessário para todo o tráfego para o domínio
- ode-to-node Criptografia N
- Criptografia de dados em repouso

Etapa 3: Configurar usuários do Cognito

Enquanto seu domínio estiver sendo criado, configure os usuários principal e limitado no Amazon Cognito seguindo Criar um grupo de usuários no Guia do desenvolvedor do Amazon Cognito. Por fim, configure seu banco de identidades seguindo as etapas em Criar um grupo de identidades no Amazon Cognito. Os grupos de usuários e identidades devem estar na mesma Região da AWS.

Etapa 4: mapear funções em OpenSearch painéis

Agora que seus usuários estão configurados, você pode entrar no OpenSearch Dashboards como usuário principal e mapear usuários para funções.

1. Volte para o console OpenSearch de serviços e navegue até a URL dos OpenSearch painéis do domínio que você criou. O URL segue este formato: *domain-endpoint*`/_dashboards/`.
2. Faça login com as credenciais `master-user`.
3. Escolha Adicionar dados de amostras e adicione os dados de voo de amostra.
4. No painel de navegação à esquerda, escolha Segurança, Funções, Criar função.
5. Nomeie a função `new-role`.
6. Em Índice, especifique `opensearch_dashboards_sample_data_fli*` (`kibana_sample_data_fli*` nos domínios do Elasticsearch).
7. Em Permissões de índice, escolha ler.
8. Em Segurança em nível de documento, especifique a seguinte consulta:

```
{
  "match": {
    "FlightDelay": true
  }
}
```

9. Para segurança em nível de campo, escolha Excluir e especifique `FlightNum`.
10. Em Anonimização, especifique `Dest`.
11. Escolha Criar.
12. Escolha Usuários mapeados e Gerenciar mapeamento. Adicione o nome do recurso da Amazon (ARN) para `LimitedUserRole` como uma identidade externa e escolha Mapa.
13. Retorne à lista de funções e escolha opensearch_dashboards_user. Escolha Usuários mapeados e Gerenciar mapeamento. Adicione o ARN para `LimitedUserRole` como uma função de backend e escolha Mapa.

Etapa 5: Testar as permissões

Quando suas funções estiverem mapeadas corretamente, é possível fazer login como o usuário limitado e testá-las.

1. Em uma nova janela privada do navegador, navegue até o URL dos OpenSearch painéis do domínio, faça login usando `limited-user` as credenciais e escolha Explorar sozinho.
2. Escolha Ferramentas de desenvolvimento e execute a pesquisa padrão:

   ```
   GET _search
   {
     "query": {
       "match_all": {}
     }
   }
   ```

   Observe o erro de permissões. `limited-user` não tem permissões para executar pesquisas em todo o cluster.
3. Execute outra pesquisa:

   ```
   GET opensearch_dashboards_sample_data_flights/_search
   {
     "query": {
       "match_all": {}
     }
   }
   ```

   Observe que todos os documentos correspondentes têm um campo `FlightDelay` de `true`, um campo anônimo `Dest` e nenhum campo `FlightNum`.
4. Na janela original do navegador, conectado como `master-user`, escolha Ferramentas de desenvolvimento e execute as mesmas pesquisas. Observe a diferença nas permissões, número de ocorrências, documentos correspondentes e campos incluídos.

Tutorial: Configuração de um domínio com o banco de dados interno do usuário e a autenticação básica HTTP

Este tutorial aborda outro caso de uso de controle de acesso refinado e popular: um usuário principal no banco de dados de usuários interno e autenticação básica HTTP para painéis. OpenSearch

O usuário principal pode então entrar nos OpenSearch painéis, criar um usuário interno, mapear o usuário para uma função e usar um controle de acesso refinado para limitar as permissões do usuário.

Você concluirá as seguintes etapas neste tutorial:

1. Crie um domínio com um usuário principal
2. Configurar um usuário interno nos OpenSearch painéis
3. Mapeie funções em OpenSearch painéis
4. Testas as permissões

Etapa 1: Criar um domínio

Navegue até o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home/ e crie um domínio com as seguintes configurações:

- OpenSearch 1.0 ou posterior, ou Elasticsearch 7.9 ou posterior
- Acesso público
- Controle de acesso refinado com um usuário primário no banco de dados interno de usuários (`TheMasterUser` para o restante deste tutorial)
- Autenticação do Amazon Cognito para Dashboards desabilitada
- A seguinte política de acesso:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::{account-id}:user/*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:{region}:{account-id}:domain/{domain-name}/*"
    }
  ]
```

```
}
```

- HTTPS necessário para todo o tráfego para o domínio
- ode-to-node Criptografia N
- Criptografia de dados em repouso

Etapa 2: criar um usuário interno nos OpenSearch painéis

Agora que você tem um domínio, pode entrar no OpenSearch Dashboards e criar um usuário interno.

1. Volte para o console OpenSearch de serviços e navegue até a URL dos OpenSearch painéis do domínio que você criou. O URL segue este formato: *domain-endpoint*`/_dashboards/`.
2. Faça login com o `TheMasterUser`.
3. Escolha Adicionar dados de amostras e adicione os dados de voo de amostra.
4. No painel de navegação à esquerda, escolha Segurança, Usuários internos, Criar usuário interno.
5. Nomeie o usuário `new-user` e especifique uma senha. Em seguida, selecione Criar.

Etapa 3: mapear funções em OpenSearch painéis

Agora que seu usuário está configurado, você pode mapeá-lo para uma perfil.

1. Fique na seção Segurança dos OpenSearch Painéis e escolha Funções, Criar função.
2. Nomeie a função `new-role`.
3. Em Índice, especifique `opensearch_dashboards_sample_data_fli*`(`kibana_sample_data_fli*` nos domínios do Elasticsearch) para o padrão de índice.
4. Para o grupo de ações, escolha leitura.
5. Em Segurança em nível de documento, especifique a seguinte consulta:

```
{
  "match": {
    "FlightDelay": true
  }
}
```

6. Para segurança em nível de campo, escolha Excluir e especifique `FlightNum`.

7. Em Anonimização, especifique `Dest`.
8. Escolha Criar.
9. Escolha Usuários mapeados e Gerenciar mapeamento. Em seguida, adicione `new-user` a Usuários e escolha Mapa.
10. Retorne à lista de funções e escolha opensearch_dashboards_user. Escolha Usuários mapeados e Gerenciar mapeamento. Em seguida, adicione `new-user` a Usuários e escolha Mapa.

Etapa 4: Testar as permissões

Quando suas funções estiverem mapeadas corretamente, é possível fazer login como o usuário limitado e testá-las.

1. Em uma nova janela privada do navegador, navegue até o URL dos OpenSearch painéis do domínio, faça login usando `new-user` as credenciais e escolha Explorar sozinho.
2. Escolha Ferramentas de desenvolvimento e execute a pesquisa padrão:

   ```
   GET _search
   {
     "query": {
       "match_all": {}
     }
   }
   ```

   Observe o erro de permissões. `new-user` não tem permissões para executar pesquisas em todo o cluster.
3. Execute outra pesquisa:

   ```
   GET dashboards_sample_data_flights/_search
   {
     "query": {
       "match_all": {}
     }
   }
   ```

   Observe que todos os documentos correspondentes têm um campo `FlightDelay` de `true`, um campo anônimo `Dest` e nenhum campo `FlightNum`.

4. Na janela original do navegador, conectado como `TheMasterUser`, escolha Ferramentas de desenvolvimento e execute as mesmas pesquisas. Observe a diferença nas permissões, número de ocorrências, documentos correspondentes e campos incluídos.

Validação de conformidade para o Amazon OpenSearch Service

Auditores terceirizados avaliam a segurança e a conformidade do Amazon OpenSearch Service como parte de vários programas de AWS conformidade. Esses programas incluem SOC, PCI e HIPAA.

Se você tiver requisitos de conformidade, considere usar qualquer versão do Elasticsearch 6.0 OpenSearch ou posterior. As versões anteriores do Elasticsearch não oferecem uma combinação de criptografia de dados em repouso e node-to-node criptografia e é improvável que atendam às suas necessidades. Você também pode considerar usar qualquer versão do Elasticsearch 6.7 OpenSearch ou posterior se o controle de acesso refinado for importante para seu caso de uso. Independentemente disso, escolher uma versão específica OpenSearch ou do Elasticsearch ao criar um domínio não garante a conformidade.

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

> **Note**
>
> Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência no Amazon OpenSearch Service

A infraestrutura global da AWS se baseia em Regiões da AWS e zonas de disponibilidade. A Regiões da AWS oferece várias zonas de disponibilidade separadas e isoladas fisicamente que são conectadas com baixa latência, altas taxas de throughput e em redes altamente redundantes. Com as zonas de disponibilidade, você pode projetar e operar aplicações e bancos de dados que executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura globalAWS.

Além da infraestrutura global da AWS, o OpenSearch Service oferece vários recursos para ajudar a oferecer suporte às suas necessidades de backup e resiliência de dados:

- Domínios e estilhaços de réplica Multi-AZ
- Snapshots automatizados e manuais

Segurança da infraestrutura no Amazon OpenSearch Service

Como um serviço gerenciado, o Amazon OpenSearch Service é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o OpenSearch Serviço pela rede. Os clientes precisam oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com sigilo de encaminhamento perfeito (perfect forward secrecy, ou PFS) como DHE (Ephemeral Diffie-Hellman, ou Efêmero Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman, ou Curva elíptica efêmera Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas utilizando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Você usa chamadas de API AWS publicadas para acessar a API OpenSearch de configuração do serviço por meio da rede. Para configurar a versão mínima necessária do TLS para aceitar, especifique o valor `TLSSecurityPolicy` nas opções do endpoint do domínio:

```
aws opensearch update-domain-config --domain-name my-domain --domain-endpoint-options
 '{"TLSSecurityPolicy": "Policy-Min-TLS-1-2-2019-07"}'
```

Para obter detalhes, consulte a Referência de comandos daAWS CLI.

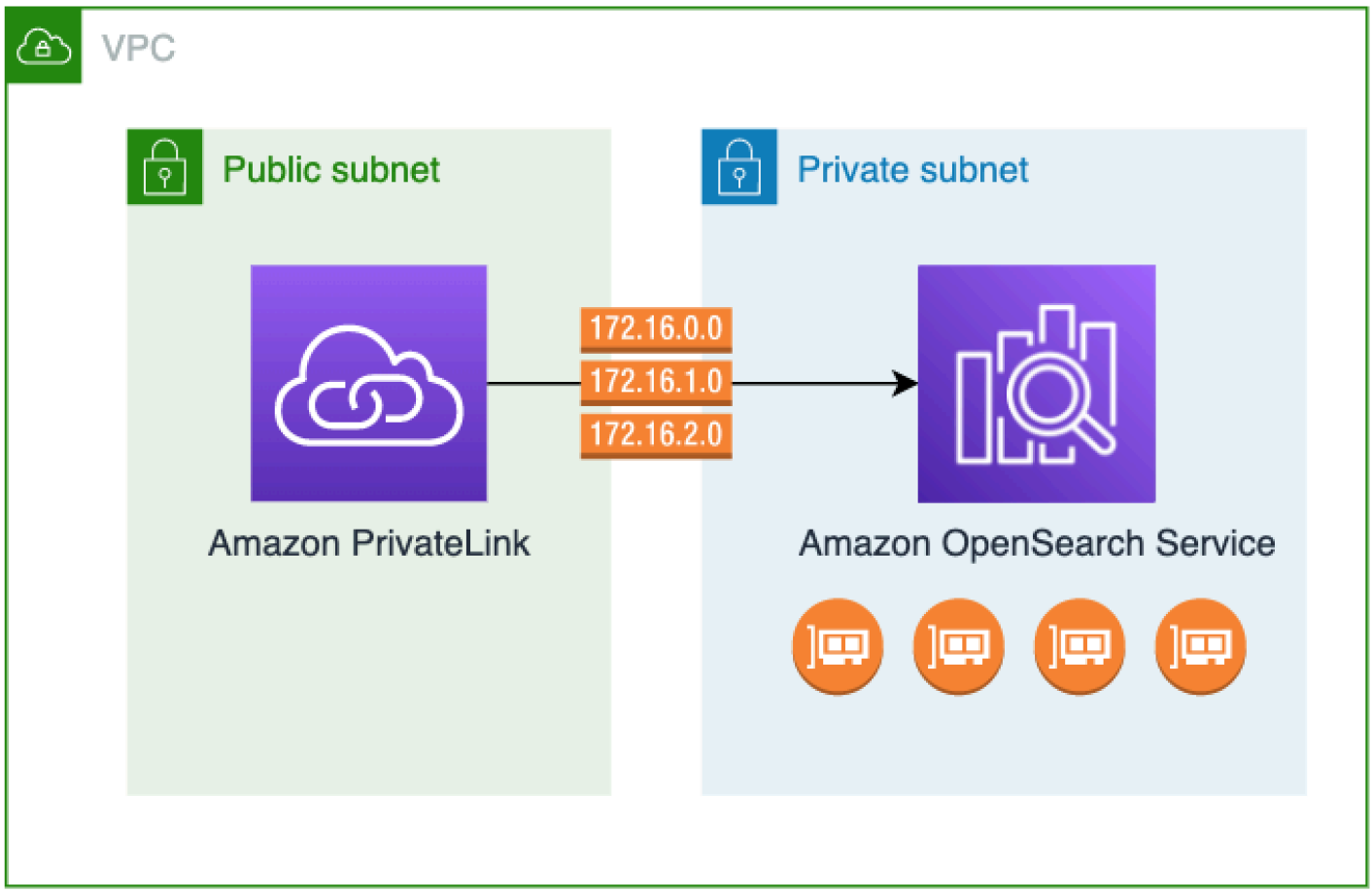
Dependendo da sua configuração de domínio, talvez você também precise assinar solicitações às APIs OpenSearch . Para ter mais informações, consulte the section called “Fazendo e assinando solicitações OpenSearch de serviço”.

OpenSearch O serviço oferece suporte a domínios de acesso público, que podem receber solicitações de qualquer dispositivo conectado à Internet, e domínios de acesso VPC, que são isolados da Internet pública.

Acesse o Amazon OpenSearch Service usando um OpenSearch VPC endpoint gerenciado por serviços ()AWS PrivateLink

Você pode acessar um domínio do Amazon OpenSearch Service configurando um OpenSearch VPC endpoint gerenciado pelo serviço (desenvolvido por). AWS PrivateLinkEsses endpoints criam uma conexão privada entre sua VPC e o Amazon OpenSearch Service. Você pode acessar os domínios do OpenSearch Service VPC como se estivessem em sua VPC, sem o uso de um gateway de internet, dispositivo NAT, conexão VPN ou conexão. AWS Direct Connect As instâncias em sua VPC não precisam de endereços IP públicos para acessar OpenSearch o Serviço.

Você pode configurar domínios OpenSearch de serviço para expor endpoints adicionais em execução em sub-redes públicas ou privadas dentro da mesma VPC, VPC diferente ou diferente. Contas da AWSIsso permite que você adicione uma camada adicional de segurança para acessar seus domínios, independentemente de onde eles sejam executados, sem nenhuma infraestrutura para gerenciar. O diagrama a seguir ilustra os endpoints de VPC OpenSearch gerenciados por serviços dentro da mesma VPC:



Você estabelece essa conexão privada criando um endpoint VPC OpenSearch de interface gerenciada por serviços, desenvolvido por. AWS PrivateLinkCriaremos uma interface de rede de endpoint em cada sub-rede que você habilitar para o endpoint da VPC de interface. Essas são interfaces de rede gerenciadas por serviços que servem como ponto de entrada para o tráfego destinado ao Serviço. OpenSearch O preço padrãoAWS PrivateLink do endpoint de interface se aplica aos endpoints VPC OpenSearch gerenciados por serviços cobrados abaixo. AWS PrivateLink

Você pode criar VPC endpoints para domínios que executam todas as versões do Elasticsearch legado e do OpenSearch Elasticsearch. Para obter mais informações, consulte Acessar os Serviços da AWS pelo AWS PrivateLink no Guia doAWS PrivateLink .

Considerações e limitações do serviço OpenSearch

Antes de configurar uma interface VPC endpoint for OpenSearch Service, analise as considerações no guia.AWS PrivateLink

Ao usar OpenSearch VPC endpoints gerenciados por serviços, considere o seguinte:

- É possível apenas usar endpoints da VPC de interface para se conectar a domínios da VPC. Não há suporte para domínios públicos.
- Os endpoints da VPC só podem se conectar a domínios dentro da mesma Região da AWS.
- O HTTPS é o único protocolo com suporte para endpoints da VPC. O HTTP não é permitido.
- OpenSearch O serviço oferece suporte para fazer chamadas para todas as operações de OpenSearch API suportadas por meio de uma interface VPC endpoint.
- É possível configurar no máximo 50 endpoints por conta, e no máximo 10 endpoints por domínio. Um único domínio pode ter no máximo 10 entidades principais autorizadas.
- No momento, você não pode usar AWS CloudFormation para criar endpoints VPC de interface.
- Você só pode criar endpoints VPC de interface por meio do console de OpenSearch serviço ou usando a OpenSearch API de serviço. Você não pode criar endpoints VPC de interface para OpenSearch serviço usando o console Amazon VPC.
- OpenSearch Os VPC endpoints gerenciados por serviços não podem ser acessados pela Internet. Um OpenSearch VPC endpoint gerenciado por serviços pode ser acessado somente na VPC em que o endpoint é provisionado ou em qualquer VPC emparelhada com a VPC em que o endpoint é provisionado, conforme permitido pelas tabelas de rotas e grupos de segurança.
- As políticas de VPC endpoint não são compatíveis com o Service. OpenSearch Você pode associar um grupo de segurança às interfaces de rede do endpoint para controlar o tráfego para o OpenSearch serviço por meio da interface VPC endpoint.
- Sua função vinculada ao serviço deve estar na mesma AWS conta que você usa para criar o VPC endpoint.
- Para criar, atualizar e excluir o endpoint OpenSearch Service VPC, você deve ter as seguintes permissões do Amazon EC2, além das permissões do Amazon Service: OpenSearch
  - `ec2:CreateVpcEndpoint`
  - `ec2:DescribeVpcEndpoints`
  - `ec2:ModifyVpcEndpoint`
  - `ec2:DeleteVpcEndpoints`
  - `ec2:CreateTags`
  - `ec2:DescribeTags`
  - `ec2:DescribeSubnets`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeVpcs`

> **Note**
>
> Atualmente, você não pode limitar a criação de VPC endpoints ao Service. OpenSearch Estamos trabalhando para tornar isso possível em uma atualização futura.

Fornecimento de acesso a um domínio

Se a VPC que você deseja acessar seu domínio estiver em outra Conta da AWS, você precisará autorizá-la na conta do proprietário antes de criar uma interface VPC endpoint.

Para permitir que uma VPC em outra Conta da AWS acesse seu domínio

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home/.
2. No painel de navegação, escolha Domínios e abra o domínio ao qual você deseja fornecer acesso.
3. Acesse a guia Endpoints da VPC, que mostra as contas e as VPCs correspondentes que têm acesso ao domínio.
4. Escolha Autorizar principal.
5. Insira o Conta da AWS ID da conta que acessará seu domínio. Essa etapa autoriza a conta especificada a criar endpoints da VPC no domínio.
6. Escolha Authorize.

Criação de uma endpoint da VPC de interface para um domínio de VPC

Você pode criar uma interface VPC endpoint para OpenSearch Service usando o console OpenSearch Service ou o AWS Command Line Interface ().AWS CLI

Para criar uma interface VPC endpoint para um domínio de serviço OpenSearch

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home/.
2. No painel de navegação à esquerda, escolha Endpoints da VPC.
3. Escolha Criar endpoint.
4. Selecione se deseja conectar um domínio no atual Conta da AWS ou em outro Conta da AWS.

5. Selecione o domínio ao qual você se conecta com esse endpoint. Se o domínio estiver no atual Conta da AWS, use o menu suspenso para escolher o domínio. Se o domínio estiver em uma conta diferente, insira o nome do recurso da Amazon (ARN) do domínio ao qual você deseja se conectar. Para escolher um domínio em uma conta diferente, o proprietário precisa fornecer acesso ao domínio.
6. Para VPC, selecione a VPC a partir da qual você acessará o Serviço. OpenSearch
7. Para Sub-redes, selecione uma ou mais sub-redes a partir das quais você acessará o Serviço. OpenSearch
8. Em Grupos de segurança, selecione os grupos de segurança para associar às interfaces de rede do endpoint. Essa é uma etapa crítica na qual você limita as portas, os protocolos e as origens para o tráfego de entrada que você está autorizando para o seu endpoint. As regras do grupo de segurança devem permitir que os recursos que usarão o VPC endpoint para se comunicar com o OpenSearch Serviço se comuniquem com a interface de rede do endpoint.
9. Escolha Criar endpoint. O endpoint deverá estar ativo em 2 a 5 minutos.

Trabalhando com endpoints OpenSearch VPC gerenciados por serviços usando a API de configuração

Use as seguintes operações de API para criar e gerenciar endpoints de OpenSearch VPC gerenciados por serviços.

- CreateVpcEndpoint
- ListVpcEndpoints
- UpdateVpcEndpoint
- DeleteVpcEndpoint

Use as seguintes operações de API para gerenciar o acesso de endpoints aos domínios da VPC:

- AuthorizeVpcEndpointAccess
- ListVpcEndpointAccess
- ListVpcEndpointsForDomain
- RevokeVpcEndpointAccess

Autenticação SAML para painéis OpenSearch

A autenticação SAML para OpenSearch painéis permite que você use seu provedor de identidade existente para oferecer login único (SSO) para painéis em domínios do Amazon OpenSearch Service executados no Elasticsearch 6.7 ou posterior. OpenSearch Para usar autenticação do SAML, é necessário habilitar o controle de acesso refinado.

Em vez de se autenticar por meio do Amazon Cognito ou do banco de dados interno de usuários, a autenticação SAML OpenSearch para painéis permite que você use provedores de identidade terceirizados para fazer login nos painéis, gerenciar o controle de acesso refinado, pesquisar seus dados e criar visualizações. OpenSearch O serviço oferece suporte a provedores que usam o padrão SAML 2.0, como Okta, Keycloak, Active Directory Federation Services (ADFS), Auth0 e. AWS IAM Identity Center

A autenticação SAML para painéis serve apenas para acessar OpenSearch painéis por meio de um navegador da web. Suas credenciais SAML não permitem que você faça solicitações HTTP diretas para as APIs OpenSearch ou Dashboards.

Visão geral da configuração do SAML

Esta documentação pressupõe que você tenha um provedor de identidade existente e alguma familiaridade com ele. Não podemos fornecer etapas de configuração detalhadas para seu provedor exato, somente para seu domínio OpenSearch de serviço.

O fluxo de login do OpenSearch Dashboards pode assumir uma das duas formas:

- Provedor de serviço (SP) iniciado: você navega até Dashboards (por exemplo, `https://my-domain.us-east-1.es.amazonaws.com/_dashboards`), a qual redireciona você para a tela de login. Após você fazer login, o provedor de identidade redirecionará você para o Dashboards.
- Provedor de identidade (IdP) iniciado: você navega até seu provedor de identidade, faz login e escolhe OpenSearch Painéis em um diretório de aplicativos.

OpenSearch O serviço fornece dois URLs de login único, iniciados pelo SP e iniciados pelo IdP, mas você só precisa daquele que corresponda ao fluxo de login do Dashboards desejado. OpenSearch

Independentemente do tipo de autenticação utilizado, o objetivo é fazer login por meio do provedor de identidade e receber uma declaração SAML que contenha seu nome de usuário (obrigatório) e quaisquer funções de backend (opcional, mas recomendado). Esta informação permite que o

controle de acesso refinado atribua permissões a usuários do SAML. Em provedores de identidade externos, as funções de backend são normalmente chamadas de "funções" ou "grupos"

Considerações

Considere o seguinte ao configurar a autenticação SAML:

- Devido ao tamanho do arquivo de metadados IdP, é altamente recomendável usar o console da AWS para configurar a autenticação SAML.
- Os domínios oferecem suporte a apenas um método de autenticação do Dashboards por vez. Se você tiver a autenticação do Amazon Cognito para OpenSearch painéis ativada, deverá desativá-la antes de habilitar a autenticação SAML.
- Se você usa um network load balancer com SAML, primeiro deve criar um endpoint personalizado. Para ter mais informações, consulte ???.

Autenticação SAML para domínios de VPC

O SAML não requer comunicação direta entre o seu provedor de identidade e seu provedor de serviços. Portanto, mesmo que seu OpenSearch domínio esteja hospedado em uma VPC privada, você ainda poderá usar o SAML, desde que seu navegador possa se comunicar com seu OpenSearch cluster e seu provedor de identidade. O seu navegador atua essencialmente como intermediário entre o seu provedor de identidade e seu provedor de serviços. Para um diagrama útil que explica o fluxo de autenticação SAML, consulte a Documentação do Okta.

Modificar a política de acesso ao domínio

Antes de configurar a autenticação SAML, é necessário atualizar a política de acesso ao domínio para permitir que os usuários de SAML acessem o domínio. Caso contrário, haverá erros de acesso negado.

Recomendamos a seguinte política de acesso ao domínio, que fornece acesso total aos sub-recursos (`/*`) no domínio:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESHttp*",
      "Resource": "domain-arn/*"
    }
  ]
}
```

Para tornar a política mais restritiva, você pode adicionar uma condição de endereço IP à política. Essa condição limita o acesso somente ao intervalo de endereços IP ou sub-rede especificado. Por exemplo, a política a seguir permite acesso somente da sub-rede 192.0.2.0/24:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24"
          ]
        }
      },
      "Resource": "domain-arn/*"
    }
  ]
}
```

> **Note**
>
> Uma política de acesso ao domínio aberto exige que um controle de acesso refinado seja ativado em seu domínio, caso contrário, você verá o seguinte erro:
> `To protect domains with public access, a restrictive policy or fine-grained access control is required.`

Se você tiver um usuário principal ou interno configurado com uma senha robusta, manter a política aberta enquanto usa um controle de acesso refinado pode ser aceitável do ponto de vista da segurança. Para ter mais informações, consulte ???.

Configurar a autenticação iniciada por SP ou IdP

Essas etapas explicam como habilitar a autenticação SAML com autenticação iniciada por SP ou IdP para painéis. OpenSearch Para visualizar a etapa extra necessária para habilitar ambos, consulte Configurar a autenticação iniciada tanto por SP quanto por IdP.

Etapa 1: Habilitar a autenticação SAML

É possível habilitar a autenticação SAML durante a criação do domínio ou escolhendo Ações, Editar configuração de segurança em um domínio existente. As etapas a seguir variam um pouco, dependendo de qual delas você escolher.

Na configuração do domínio, em Autenticação SAML para OpenSearch Dashboards/Kibana, selecione Habilitar autenticação SAML.

Etapa 2: Configurar seu provedor de identidade

Conclua as etapas a seguir, dependendo de quando você está configurando a autenticação SAML.

Se estiver criando um novo domínio

Se você estiver criando um novo domínio, o OpenSearch Service ainda não poderá gerar um ID de entidade do provedor de serviços ou URLs de SSO. Seu provedor de identidade requer esses valores para habilitar adequadamente a autenticação SAML, mas eles apenas podem ser gerados depois da criação do domínio. Para solucionar essa interdependência durante a criação do domínio, forneça valores temporários na sua configuração de IdP para gerar os metadados necessários e depois atualizá-los quando o domínio estiver ativo.

Se estiver usando um endpoint personalizado, você poderá inferir quais serão os URLs. Por exemplo, se o endpoint personalizado for `www.custom-endpoint.com`, o ID de entidade do provedor de serviços será `www.custom-endpoint.com`, o URL de SSO iniciado pelo IdP será `www.custom-endpoint.com/_dashboards/_opendistro/_security/saml/acs/idpinitiated` e o URL de SSO iniciado pelo SP será `www.custom-endpoint.com/`

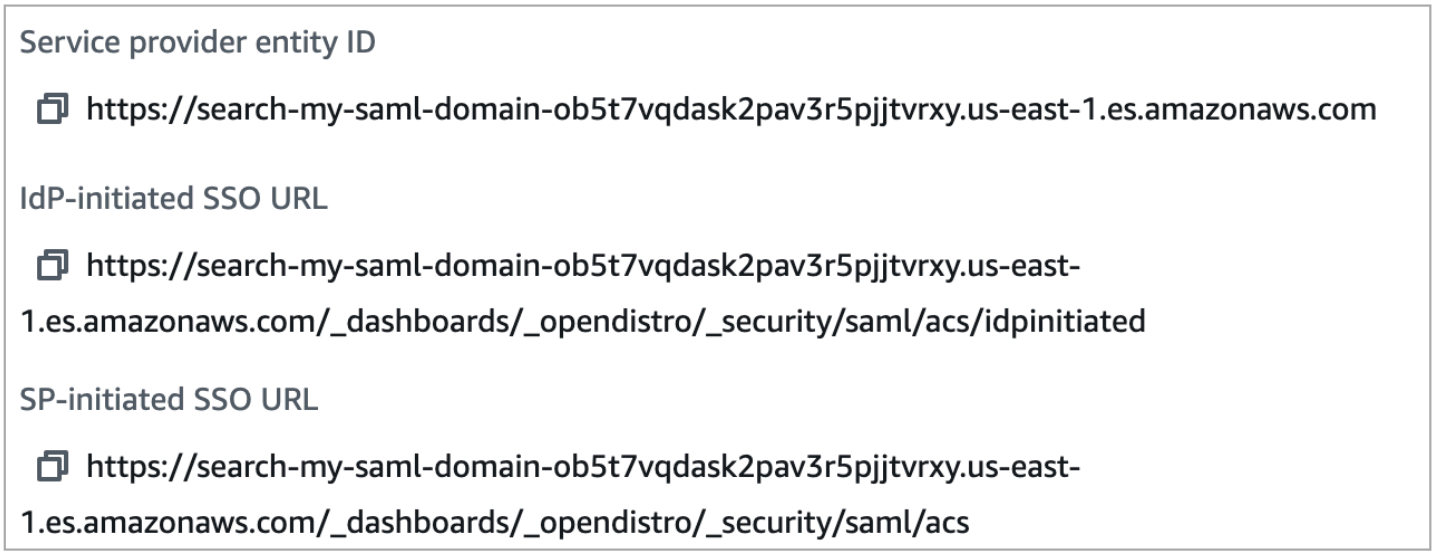
`_dashboards/_opendistro/_security/saml/acs`. É possível usar os valores para configurar seu provedor de identidade antes de criar o domínio. Consulte a próxima seção para ver exemplos.

Se você não estiver usando um endpoint personalizado, poderá inserir valores temporários no seu IdP para gerar os metadados necessários e atualizá-los posteriormente quando o domínio estiver ativo.

Por exemplo, no Okta, você pode inserir `https://temp-endpoint.amazonaws.com` nos campos URL de login único e URI do público - ID da entidade SP, o que permite gerar os metadados. Depois que o domínio estiver ativo, você poderá recuperar os valores corretos do OpenSearch Serviço e atualizá-los no Okta. Para obter instruções, consulte the section called “Etapa 6: Atualizar seus URLs de IdP”.

Se estiver editando um domínio existente

Se estiver habilitando a autenticação SAML em um domínio existente, copie o ID da entidade do provedor de serviços e um dos URLs de SSO. Para orientação sobre qual URL usar, consulte the section called “Visão geral da configuração do SAML”.



Use os valores para configurar seu provedor de identidade. Essa é a parte mais complexa do processo e, infelizmente, a terminologia e as etapas variam muito de acordo com o provedor. Consulte a documentação do seu provedor.

No Okta, por exemplo, você deve criar uma aplicação web SAML 2.0. Para URL de acesso único, especifique o URL de SSO. Para URI do público (ID da entidade do SP), especifique o ID da entidade do provedor de serviços.

Em vez de usuários e funções de backend, o Okta tem usuários e grupos. Em Instruções de atributo de grupo, recomendamos adicionar `role` ao campo Nome e a expressão regular `.+` ao campo Filtro. Esta instrução diz ao provedor de identidade do Okta para incluir todos os grupos de usuários sob o campo `role` da asserção SAML após a autenticação de um usuário.

No IAM Identity Center, você especifica o ID da entidade SP como o público do Application SAML. Você também precisa especificar o mapeamento dos seguintes atributos: `Subject=${user:name}` e `Role=${user:groups}`.

No Auth0, você cria uma aplicação Web regular e, em seguida, habilita o complemento SAML 2.0. No Keycloak, você cria um cliente.

Etapa 3: Importar metadados do IdP

Aopis você configurar o provedor de identidade, ele gera um arquivo de metadados IdP. Esse arquivo XML contém informações sobre o provedor, como um certificado TLS, endpoints de acesso único e o ID de entidade do provedor de identidade.

Copie o conteúdo do arquivo de metadados do IdP e cole-o no campo Metadados do IdP no console de serviço. OpenSearch Alternativamente, escolha Importar de arquivo XML e carregue o arquivo. O arquivo de metadados deve ser semelhante ao seguinte:

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="entity-id"
 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>tls-certificate</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</
md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</
md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="idp-sso-url"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="idp-sso-url"/>
```

```
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

Etapa 4: Configurar campos SAML

Depois de inserir seus metadados do IdP, configure os seguintes campos adicionais no OpenSearch console de serviço:

- ID da entidade do IdP: copie o valor da propriedade `entityID` do seu arquivo de metadados e cole-o nesse campo. Muitos provedores de identidade também exibem esse valor como parte de um resumo pós-configuração. Alguns provedores chamam isso de “emissor”.
- Nome de usuário principal do SAML e função de back-end principal do SAML — O usuário e/ou a função de back-end que você especifica recebe permissões completas para o cluster, equivalentes a um novo usuário mestre, mas só pode usar essas permissões nos painéis. OpenSearch

  No Okta, por exemplo, você pode ter um usuário `jdoe` que pertence ao grupo `admins`. Se você adicionar `jdoe` ao nome de usuário primário do SAML, somente esse usuário receberá permissões completas. Se você adicionar `admins` ao campo Perfil de backend primário SAML, qualquer usuário que pertença ao grupo `admins` receberá permissões completas.

  > **Note**
  >
  > O conteúdo da asserção SAML deve corresponder exatamente às strings que você usa para o nome de usuário primário do SAML e o perfil primário SAML. Alguns provedores de identidade adicionam um prefixo antes de seus nomes de usuário, o que pode causar uma hard-to-diagnose incompatibilidade. Na interface do usuário do provedor de identidade, talvez você veja `jdoe`, mas a asserção SAML poderá conter `auth0|jdoe`. Use sempre a string da asserção SAML.

Muitos provedores de identidade permitem que você visualize uma declaração de exemplo durante o processo de configuração, e ferramentas como o SAML-tracer podem ajudar a examinar e solucionar problemas de conteúdo de asserções reais. As asserções são semelhantes a:

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="id67229299299259351343340162"
 IssueInstant="2020-09-22T22:03:08.633Z" Version="2.0"
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
```

```
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">idp-issuer</
saml2:Issuer>
  <saml2:Subject>
    <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified">username</saml2:NameID>
    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml2:SubjectConfirmationData NotOnOrAfter="2020-09-22T22:08:08.816Z"
 Recipient="domain-endpoint/_dashboards/_opendistro/_security/saml/acs"/>
    </saml2:SubjectConfirmation>
  </saml2:Subject>
  <saml2:Conditions NotBefore="2020-09-22T21:58:08.816Z"
 NotOnOrAfter="2020-09-22T22:08:08.816Z">
    <saml2:AudienceRestriction>
      <saml2:Audience>domain-endpoint</saml2:Audience>
    </saml2:AudienceRestriction>
  </saml2:Conditions>
  <saml2:AuthnStatement AuthnInstant="2020-09-22T19:54:37.274Z">
    <saml2:AuthnContext>

 <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport<
saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
  <saml2:AttributeStatement>
    <saml2:Attribute Name="role" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecified">
      <saml2:AttributeValue
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="xs:string">GroupName Match Matches regex ".+" (case-sensitive)
      </saml2:AttributeValue>
    </saml2:Attribute>
  </saml2:AttributeStatement>
</saml2:Assertion>
```

Etapa 5: (Opcional) Configurar definições adicionais

Em Configurações adicionais, defina os seguintes campos opcionais:

- Chave do requerente: você pode deixar esse campo vazio para usar o elemento `NameID` da asserção SAML como nome de usuário. Se sua asserção não usar este elemento padrão e, em vez disso, incluir o nome de usuário como um atributo personalizado, especifique esse atributo aqui.

- Chave de perfis: se quiser usar funções de backend (recomendadas), especifique um atributo da afirmação nesse campo, como `role` ou `group`. Esta é outra situação em que ferramentas como o SAML tracer podem ajudar.
- Tempo de ativação da sessão — Por padrão, o OpenSearch Dashboards desconecta os usuários após 24 horas. Você pode configurar esse valor como qualquer número entre 60 e 1.440 (24 horas) especificando um novo valor.

Quando estiver satisfeito com sua configuração, salve o domínio.

Etapa 6: Atualizar seus URLs de IdP

Se tiver habilitado a autenticação SAML ao criar um domínio, você precisará especificar URLs temporários no seu IdP para gerar o arquivo de metadados XML. Quando o status do domínio for alterado para `Active`, você poderá obter os URLs corretos e modificar seu IdP.

Para recuperar os URLs, selecione o domínio e escolha Ações, Editar configuração de segurança. Em Autenticação SAML para OpenSearch dashboards/Kibana, você pode encontrar a ID da entidade do provedor de serviços e os URLs de SSO corretos. Copie esses valores e use-os para configurar seu provedor de identidade, substituindo os URLs temporários fornecidos na etapa 2.

Etapa 7: mapear usuários SAML para perfis

Quando o status do seu domínio estiver Ativo e seu IdP estiver configurado corretamente, navegue até OpenSearch Painéis.

- Se você escolheu o URL iniciado pelo SP, navegue até *`domain-endpoint`*`/_dashboards`. Para fazer login diretamente em um inquilino específico, você pode anexar `?security_tenant=`*`tenant-name`* ao URL.
- Se você escolheu o URL iniciado pelo IsP, navegue até o diretório de aplicações do provedor de identidade.

Em ambos os casos, faça login como usuário primário do SAML ou um usuário que pertence à função de backend primário do SAML. Para continuar o exemplo da etapa 7, faça login como `jdoe` ou como um membro do grupo `admins`.

Depois que os OpenSearch painéis forem carregados, escolha Segurança, Funções. Em seguida, mapeie as funções para permitir que outros usuários acessem os OpenSearch painéis.

Por exemplo, você pode mapear o seu colega confiável `jroe` nas funções `all_access` e `security_manager`. Você também pode mapear a função de backend `analysts` nas funções `readall` e `opensearch_dashboards_user`.

Se você preferir usar a API em vez de OpenSearch painéis, veja o seguinte exemplo de solicitação:

```
PATCH _plugins/_security/api/rolesmapping
[
  {
    "op": "add", "path": "/security_manager", "value": { "users": ["master-user",
 "jdoe", "jroe"], "backend_roles": ["admins"] }
  },
  {
    "op": "add", "path": "/all_access", "value": { "users": ["master-user", "jdoe",
 "jroe"], "backend_roles": ["admins"] }
  },
  {
    "op": "add", "path": "/readall", "value": { "backend_roles": ["analysts"] }
  },
  {
    "op": "add", "path": "/opensearch_dashboards_user", "value": { "backend_roles":
 ["analysts"] }
  }
]
```

Configurar a autenticação iniciada por SP ou IdP

Caso pretenda configurar a autenticação iniciada pelo SP e pelo IdP, você deverá fazê-lo via provedor de identidade. Por exemplo, no Okta, você pode executar as seguintes etapas:

1. Em sua aplicação SAML, vá para Geral, Configurações SAML.
2. Para o URL de autenticação única, forneça o URL de SSO iniciado por IdP. Por exemplo, `https://search-domain-hash/_dashboards/_opendistro/_security/saml/acs/idpinitiated`.
3. Habilite Permitir que este aplicativo solicite outros URLs de SSO.
4. Em URLs de SSO que podem ser requeridas, adicione um ou mais URLs de SSO iniciados por SP. Por exemplo, `https://search-domain-hash/_dashboards/_opendistro/_security/saml/acs`.

Configurar a autenticação SAML (AWS CLI)

O AWS CLI comando a seguir ativa a autenticação SAML para OpenSearch painéis em um domínio existente:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --advanced-security-options '{"SAMLOptions":{"Enabled":true,"MasterUserName":"my-idp-user","MasterBackendRole":"my-idp-group-or-role","Idp":{"EntityId":"entity-id","MetadataContent":"metadata-content-with-quotes-escaped"},"RolesKey":"optional-roles-key","SessionTimeoutMinutes":180,"SubjectKey":"optional-subject-key"}}'
```

Você deve “escapar” todas as aspas e caracteres de nova linha no XML de metadados. Por exemplo, use `<KeyDescriptor use=\"signing\">\n` em vez de `<KeyDescriptor use="signing">` e uma quebra de linha. Para obter informações detalhadas sobre o uso do AWS CLI, consulte a Referência de AWS CLI Comandos.

Configurar a autenticação SAML (API de configuração)

A solicitação a seguir para a API de configuração permite a autenticação SAML para OpenSearch painéis em um domínio existente:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/config
{
  "AdvancedSecurityOptions": {
    "SAMLOptions": {
      "Enabled": true,
      "MasterUserName": "my-idp-user",
      "MasterBackendRole": "my-idp-group-or-role",
      "Idp": {
        "EntityId": "entity-id",
        "MetadataContent": "metadata-content-with-quotes-escaped"
      },
      "RolesKey": "optional-roles-key",
      "SessionTimeoutMinutes": 180,
      "SubjectKey": "optional-subject-key"
    }
  }
}
```

Você deve “escapar” todas as aspas e caracteres de nova linha no XML de metadados. Por exemplo, use `<KeyDescriptor use=\"signing\">\n` em vez de `<KeyDescriptor use="signing">` e uma quebra de linha. Para obter informações detalhadas sobre como usar a API de configuração, consulte a referência da API de OpenSearch serviço.

Solução de problemas de SAML

Erro	Detalhes
Sua solicitação: “*/algum/caminho* ” não é permitida.	Verifique se você forneceu o URL de SSO correto (etapa 3) ao seu provedor de identidade.
Forneça um documento de metadados do provedor de identidades válido para habilitar o SAML.	O arquivo de metadados do IdP não atende ao padrão SAML 2.0. Verifique se há erros usando uma ferramenta de validação.
As opções de configuração do SAML não estão visíveis no console.	Atualize para o software de serviço mais recente.
Erro de configuração do SAML: algo errado ocorreu ao tentar recuperar a configuração do SAML. Verifique suas configurações.	Esse erro genérico pode ocorrer por vários motivos. • Verifique se você forneceu ao provedor de identidade o ID de entidade do provedor de serviços e o URL de SSO corretos. • Gere novamente o arquivo de metadados do IdP e verifique o ID de entidade do IdP. Adicione quaisquer metadados atualizados no console do AWS . • Verifique se sua política de acesso ao domínio permite acesso aos OpenSearch painéis e. `_plugins/_security/*` Em geral, recomenda mos uma política de acesso aberto para domínios que usam controle de acesso refinado. • Consulte a documentação do provedor de identidad e para obter as etapas de configuração do SAML.
Função ausente: nenhuma função disponível para este usuário, entre	Você autenticou com êxito, mas o nome de usuário e quaisquer funções de backend da asserção SAML

Erro	Detalhes
em contato com o administrador do sistema..	não são mapeados em nenhuma função e, portanto, não têm permissões. Esses mapeamentos diferenci am maiúsculas de minúsculas. O administrador do sistema pode verificar o conteúdo da sua declaração de SAML usando uma ferrament a como o SAML-tracer e, em seguida, verificar seu mapeamento de funções usando a seguinte solicitaç ão: `GET _plugins/_security/api/rolesmapping`
Seu navegador redireciona ou recebe continuamente erros HTTP 500 ao tentar acessar OpenSearch os painéis.	Esses erros podem ocorrer se sua asserção SAML contiver um grande número de funções totalizando aproximadamente 1.500 caracteres. Por exemplo, se você passar 80 funções com tamanho médio de 20 caracteres, o limite de tamanho para cookies em seu navegador da Web poderá ser excedido. A partir da OpenSearch versão 2.7, a asserção SAML oferece suporte a funções de até 5.000 caracteres.
Não é possível sair do ADFS.	O ADFS exige que todas as solicitações de logout sejam assinadas, o que o OpenSearch Serviço não suporta. Remova `<SingleLogoutService />` do arquivo de metadados do IdP para forçar o OpenSearch Serviço a usar seu próprio mecanismo de logout interno.
`Could not find entity descriptor for __PATH__.`	O ID da entidade do IdP fornecido nos metadados XML to OpenSearch Service é diferente daquele na resposta SAML. Para corrigir isso, verifique se eles correspondem. Ative logs de erros do aplicativo CW no seu domínio para encontrar a mensagem de erro para depurar o problema de integração do SAML.

Erro	Detalhes
`Signature validation failed. SAML response rejected.`	OpenSearch O serviço não consegue verificar a assinatura na resposta SAML usando o certificado do IdP fornecido no XML de metadados. Você pode ter cometido um erro ou seu IdP alterou o certificado. Atualize o certificado mais recente do seu IdP no XML de metadados fornecido ao OpenSearch Serviço por meio do. AWS Management Console
`__PATH__ is not a valid audience for this response.`	O campo de público na resposta do SAML não corresponde ao endpoint do domínio. Para corrigir esse erro, atualize o campo “SP audience” para corresponder ao endpoint do seu domínio. Se você ativou endpoints personalizados, o campo de público deve corresponder ao seu endpoint personalizado. Ative logs de erros do aplicativo CW no seu domínio para encontrar a mensagem de erro para depurar o problema de integração do SAML.
Seu navegador recebe um erro HTTP 400 na resposta ao `Invalid Request Id`.	Esse erro geralmente ocorre se você configurou o URL iniciado pelo IdP com o formato *<DashboardsURL>* `/_opendistro/_security/saml/acs`. Em vez disso, configure o URL com o formato *<DashboardsURL>* `/_opendistro/_security/saml/acs/idpinitiated` .

Erro	Detalhes
A resposta foi recebida às `__PATH__` em vez de `__PATH__`.	O campo de destino na resposta do SAML não corresponde a um dos seguintes formatos de URL: • *<DashboardsURL>* `/_opendistro/_security/saml/acs` • *<DashboardsURL>* `/_opendistro/_security/saml/acs/idpinitiated` . Dependendo do fluxo de login que você usa (iniciado pelo SP ou iniciado pelo IDP), insira um campo de destino que corresponda a um dos URLs. OpenSearch
A resposta tem um `InResponseTo` atributo, enquanto `InResponseTo` não era esperado.	Você está usando o URL iniciado por IdP para um fluxo de login iniciado por SP. Em vez disso, use o URL iniciado por SP.

Desabilitação da autenticação SAML

Para desativar a autenticação SAML para OpenSearch painéis (console)

1. Escolha o domínio, Ações, e Editar configuração de segurança.
2. Desmarque Habilitar autenticação SAML.
3. Escolha Salvar alterações.
4. Após o processamento do domínio, verifique o mapeamento de função de controle de acesso refinado com a seguinte solicitação:

   ```
   GET _plugins/_security/api/rolesmapping
   ```

   Desabilitar a autenticação SAML para o Dashboards não remove os mapeamentos para o nome de usuário primário do SAML e/ou a função de backend primária do SAML. Se você quiser remover esses mapeamentos, faça login no Dashboards usando o banco de dados interno de usuários (se habilitado) ou use a API para removê-los:

```
PUT _plugins/_security/api/rolesmapping/all_access
{
  "users": [
    "master-user"
  ]
}
```

Configuração da autenticação do Amazon Cognito para OpenSearch Dashboards

Você pode autenticar e proteger sua instalação padrão do Amazon OpenSearch Service do OpenSearch Dashboards usando o Amazon Cognito. A autenticação do Amazon Cognito é opcional e está disponível apenas para domínios que usam o OpenSearch ou o Elasticsearch 5.1 ou posterior. Se você não configurar a autenticação do Amazon Cognito, ainda poderá proteger o Dashboards usando uma política de acesso baseada em IP e um servidor de proxy, autenticação básica HTTP ou SAML.

Grande parte do processo de autenticação ocorre no Amazon Cognito, mas esta seção oferece diretrizes e requisitos para configurar recursos do Amazon Cognito para trabalhar com domínios do OpenSearch Service. Preços padrão aplicam-se a todos os recursos do Amazon Cognito.

> **Tip**
>
> Na primeira vez que você configurar um domínio para usar a autenticação do Amazon Cognito para o OpenSearch Dashboards, recomendamos usar o console. Os recursos do Amazon Cognito são extremamente personalizáveis, e o console pode ajudar você a identificar e compreender os recursos que são importantes para você.

Tópicos

- (Opcional) Personalização da página de login
- (Opcional) Configuração da segurança avançada
- Testes
- Cotas
- Problemas de configuração comuns
- Desabilitação da autenticação do Amazon Cognito para OpenSearch Dashboards
- Exclusão de domínios que usam a autenticação do Amazon Cognito para OpenSearch Dashboards

Pré-requisitos

Antes de configurar a autenticação do Amazon Cognito para o Kibana, você deverá atender a vários pré-requisitos. O console do OpenSearch Service ajuda a simplificar a criação desses recursos, mas compreender a finalidade de cada recurso ajuda na configuração e na solução de problemas. A autenticação do Amazon Cognito para Dashboards requer os seguintes recursos:

- Conjunto de usuários do Amazon Cognito
- Grupo de identidades do Amazon Cognito
- Função do IAM com a política `AmazonOpenSearchServiceCognitoAccess` anexada (`CognitoAccessForAmazonOpenSearch`)

> **Note**
>
> Os grupos de usuários e identidades devem estar na mesma Região da AWS. Você pode usar o mesmos grupo de usuários, grupo de identidades e função do IAM para adicionar a autenticação do Amazon Cognito para o Dashboards para vários domínios do OpenSearch Service. Para saber mais, consulte the section called “Cotas”.

Sobre o grupo de usuários

Os grupos de usuários têm dois recursos principais: criar e gerenciar um diretório de usuários e permitir que os usuários se cadastrem e façam login. Para obter instruções sobre como criar um grupo de usuários, consulte Criar um grupo de usuários no Guia do desenvolvedor do Amazon Cognito.

Ao criar um grupo de usuários para usar com o OpenSearch Service, considere o seguinte:

- O grupo de usuários do Amazon Cognito deve ter um nome de domínio. O OpenSearch Service usa esse nome de domínio para redirecionar os usuários para uma página de login para acessar o Dashboards. Além de um nome de domínio, o grupo de usuários não exige qualquer configuração não padrão.
- Você deve especificar os atributos padrão necessários do grupo, como nome, data de nascimento, endereço de e-mail e número de telefone. Você não pode alterar esses atributos depois de criar o grupo de usuários. Portanto, escolha os atributos importantes para você neste momento.
- Ao criar seu grupo de usuários, escolha se os usuários podem criar suas próprias contas, a segurança mínima da senha para contas e se deseja habilitar a autenticação multifator. Se você planeja usar um provedor de identidade externo, essas configurações são não têm qualquer consequência. Tecnicamente, você pode habilitar o grupo de usuários como um provedor de identidade e habilitar um provedor de identidade externo, mas a maioria das pessoas prefere um ou o outro.

Os IDs de grupo de usuários assumem a forma de *region*_*ID*. Se você planeja usar a AWS CLI ou um AWS SDK para configurar o OpenSearch Service, anote o ID.

Sobre o grupo de identidades

Os grupos de identidades permitem que você atribua funções temporárias e de privilégio limitado a usuários depois que eles fazem login. Para obter instruções sobre como criar um grupo de identidades, consulte Grupos de identidades no Guia do desenvolvedor do Amazon Cognito. Ao criar um grupo de identidades para usar com o OpenSearch Service, considere o seguinte:

- Se você usar o console do Amazon Cognito, deverá marcar a caixa de seleção EPermitir acesso a identidades não autenticadas para criar o grupo de identidades. Após você criar o grupo de identidades e configurar o domínio do OpenSearch Service, o Amazon Cognito desabilitará essa configuração.
- Você não precisa adicionar provedores de identidade externos ao grupo de identidades. Quando você configurar o OpenSearch Service para usar a autenticação do Amazon Cognito, ele configurará o grupo de identidades para usar o grupo de usuários que você acabou de criar.
- Depois de criar o grupo de identidades, você deve escolher as funções do IAM autenticadas e não autenticadas. Essas funções especificam as políticas de acesso que os usuários têm antes e depois de fazer login. Se você usar o console do Amazon Cognito ele poderá criar essas funções para você. Depois de criar a função autenticada, anote o nome do

recurso da Amazon (ARN), que tem o formato de `arn:aws:iam::123456789012:role/Cognito_identitypoolnameAuth_Role`.

Os IDs de grupo de identidades assumem a forma de *region*:*ID-ID-ID-ID-ID*. Se você planeja usar a AWS CLI ou um AWS SDK para configurar o OpenSearch Service, anote o ID.

Sobre a função CognitoAccessForAmazonOpenSearch

O OpenSearch Service precisa de permissões para configurar os usuários e os grupos de identidades do Amazon Cognito e usá-los para autenticação. É possível usar `AmazonOpenSearchServiceCognitoAccess`, que é uma política gerenciada pela AWS para essa finalidade. `AmazonESCognitoAccess` é uma política legada que foi substituída por `AmazonOpenSearchServiceCognitoAccess` quando o serviço foi renomeado para Amazon OpenSearch Service. Ambas as políticas fornecem as permissões mínimas do Amazon Cognito necessárias para ativar a autenticação Cognito. Para ver a política JSON, consulte o console do IAM.

Se você usar o console para criar ou configurar o domínio do OpenSearch Service, ele criará uma função do IAM para você e anexará a política da `AmazonOpenSearchServiceCognitoAccess` à função (ou à política `AmazonESCognitoAccess` se for um domínio do Elasticsearch) à função. O nome padrão desta função é `CognitoAccessForAmazonOpenSearch`.

As políticas de permissões da função `AmazonOpenSearchServiceCognitoAccess` e `AmazonESCognitoAccess` permitem que o OpenSearch Service conclua as seguintes ações em todos os grupos usuários e de identidade:

- Ação: `cognito-idp:DescribeUserPool`
- Ação: `cognito-idp:CreateUserPoolClient`
- Ação: `cognito-idp:DeleteUserPoolClient`
- Ação: `cognito-idp:UpdateUserPoolClient`
- Ação: `cognito-idp:DescribeUserPoolClient`
- Ação: `cognito-idp:AdminInitiateAuth`
- Ação: `cognito-idp:AdminUserGlobalSignOut`
- Ação: `cognito-idp:ListUserPoolClients`
- Ação: `cognito-identity:DescribeIdentityPool`
- Ação: `cognito-identity:SetIdentityPoolRoles`
- Ação: `cognito-identity:GetIdentityPoolRoles`

Se você usar a AWS CLI ou um dos AWS SDKs, deverá criar sua própria função, anexar a política e especificar o nome do recurso da Amazon (ARN) para essa função ao configurar o domínio do OpenSearch Service. A função deve ter a seguinte relação de confiança:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "opensearchservice.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Para obter instruções, consulte Criação de uma função para delegar permissões a um serviço da AWS e Anexação e desanexação de políticas do IAM no Manual do usuário do IAM.

Configuração de um domínio para uso da autenticação do Amazon Cognito

Depois de concluir os pré-requisitos, você poderá configurar um domínio do OpenSearch Service para usar o Amazon Cognito para o Dashboards.

> **Note**
>
> O Amazon Cognito não está disponível em todas as Regiões da AWS. Para obter uma lista de regiões e endpoints compatíveis, consulte Regiões da AWS e endpoints. Não é necessário usar a mesma região para o Amazon Cognito e para o OpenSearch Service.

Configuração da autenticação do Amazon Cognito (console)

Como ele cria a função CognitoAccessForAmazonOpenSearch para você, o console oferece a experiência de configuração mais simples. Além das permissões padrão do OpenSearch Service, você precisa do seguinte conjunto mínimo de permissões para usar o console para criar um domínio que usa a autenticação do Amazon Cognito para o Dashboards.

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:ListUserPools",
        "iam:CreateRole",
        "iam:AttachRolePolicy"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/service-
role/CognitoAccessForAmazonOpenSearch"
    }
  ]
}
```

Para obter instruções sobre como adicionar permissões a uma identidade (usuário, grupo de usuários ou função), consulte Adicionar permissões de identidade do IAM (console).

Se `CognitoAccessForAmazonOpenSearch` já existir, você precisará de um número menor de permissões:

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:ListUserPools"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/service-
role/CognitoAccessForAmazonOpenSearch"
    }
  ]
}
```

Para configurar a autenticação do Amazon Cognito para Dashboards (console)

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home/.
2. Em Domínios, selecione o domínio que deseja configurar.
3. Escolha Ações, Editar configuração de segurança.
4. Selecione Habilitar autenticação do Amazon Cognito.
5. Em Região, selecione a Região da AWS que contém o grupo de usuários e o grupo de identidades do Amazon Cognito.
6. Em Grupo de usuários do Cognito, selecione um grupo de usuários ou crie um. Para obter orientações, consulte the section called “Sobre o grupo de usuários”.
7. Em Grupo de identidades do Cognito, selecione um grupo de identidades ou crie um. Para obter orientações, consulte the section called “Sobre o grupo de identidades”.

   > **Note**
   >
   > Os links Criar grupo de usuários e Criar grupo de identidades direcionam você para o console do Amazon Cognito e exigem que você crie esses recursos manualmente. O processo não é automático. Para saber mais, consulte the section called “Pré-requisitos”.

8. Em Nome da função do IAM, use o valor padrão de `CognitoAccessForAmazonOpenSearch` (recomendado) ou insira um novo nome. Para saber mais sobre o propósito desta função, consulte the section called “Sobre a função CognitoAccessForAmazonOpenSearch”.
9. Escolha Salvar alterações.

Depois que o seu domínio concluir o processamento, consulte the section called “Como permitir a função autenticada” e the section called “Configuração de provedores de identidade” para ver as etapas de configuração adicionais.

Configuração da autenticação do Amazon Cognito (AWS CLI)

Use o parâmetro `--cognito-options` para configurar o domínio do OpenSearch Service. A sintaxe a seguir é usada pelos comandos `create-domain` e `update-domain-config`:

```
--cognito-options Enabled=true,UserPoolId="user-pool-id",IdentityPoolId="identity-pool-id",RoleArn="arn:aws:iam::123456789012:role/CognitoAccessForAmazonOpenSearch"
```

Exemplo

O exemplo a seguir cria um domínio na região `us-east-1` que habilita a autenticação do Amazon Cognito para o Dashboards usando a função `CognitoAccessForAmazonOpenSearch` e fornece acesso ao domínio para `Cognito_Auth_Role`:

```
aws opensearch create-domain --domain-name my-domain --region us-east-1 --access-policies '{ "Version":"2012-10-17", "Statement":[{"Effect":"Allow","Principal":{"AWS":
 ["arn:aws:iam::123456789012:role/
Cognito_Auth_Role"]},"Action":"es:ESHttp*","Resource":"arn:aws:es:us-east-1:123456789012:domain/*" }]}' --engine-version "OpenSearch_1.0"
 --cluster-config InstanceType=m4.xlarge.search,InstanceCount=1
 --ebs-options EBSEnabled=true,VolumeSize=10 --cognito-options
 Enabled=true,UserPoolId="us-east-1_123456789",IdentityPoolId="us-east-1:12345678-1234-1234-1234-123456789012",RoleArn="arn:aws:iam::123456789012:role/CognitoAccessForAmazonOpenSearch"
```

Depois que o seu domínio concluir o processamento, consulte the section called “Como permitir a função autenticada” e the section called “Configuração de provedores de identidade” para ver as etapas de configuração adicionais.

Configuração da autenticação do Amazon Cognito (AWS SDKs)

Os SDKs da AWS (exceto os SDKs para Android e iOS) são compatíveis com todas as operações definidas na Amazon OpenSearch Service API Reference (Referência da API do Amazon OpenSearch Service), incluindo o parâmetro `CognitoOptions` para as operações `CreateDomain` e `UpdateDomainConfig`. Para obter mais informações sobre instalação e uso dos AWS SDKs, consulte Kits de desenvolvimento de software da AWS.

Depois que o seu domínio concluir o processamento, consulte the section called “Como permitir a função autenticada” e the section called “Configuração de provedores de identidade” para ver as etapas de configuração adicionais.

Como permitir a função autenticada

Por padrão, a função do IAM autenticada que você configurou seguindo as diretrizes em the section called “Sobre o grupo de identidades” não tem os privilégios necessários para acessar o OpenSearch Dashboards. Você deve fornecer permissões adicionais à função.

> **Note**
>
> Se tiver configurado o controle de acesso detalhado e usar uma política de acesso “aberta” ou baseada em IP, poderá ignorar esta etapa.

É possível incluir essas permissões em uma política baseada em identidades, mas, a menos que você queira que os usuários autenticados tenham acesso a todos os domínios do OpenSearch Service, a melhor abordagem é uma política baseada em recursos anexada a um único domínio.

Para o `Principal`, especifique o ARN da função autenticada do Cognito que você configurou com as diretrizes em the section called “Sobre o grupo de identidades”.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":[
               "arn:aws:iam::123456789012:role/Cognito_identitypoolnameAuth_Role"
            ]
         },
         "Action":[
            "es:ESHttp*"
         ],
         "Resource":"arn:aws:es:region:123456789012:domain/domain-name/*"
      }
   ]
}
```

Para obter instruções sobre como adicionar uma política baseada em recursos a um domínio do OpenSearch Service, consulte the section called “Configuração de políticas de acesso”.

Configuração de provedores de identidade

Quando você configura um domínio para usar a autenticação do Amazon Cognito para o Dashboards, o OpenSearch Service adiciona um cliente da aplicação ao grupo de usuários e adiciona o grupo de usuários ao grupo de identidades como um provedor de autenticação.

> **Warning**
>
> Não renomeie nem exclua o cliente do aplicativo.

Dependendo de como você configurou o grupo de usuários, talvez precise criar contas de usuário manualmente ou os usuários podem ser capazes de criar suas próprias contas. Se essas configurações forem aceitáveis, você não precisará realizar ações adicionais. No entanto, muitas pessoas preferem usar provedores de identidade externos.

Para habilitar um provedor de identidade SAML 2.0, você deve fornecer um documento de metadados do SAML. Para habilitar provedores de identidades sociais, como o Login with Amazon, o Facebook e o Google, você deve ter um ID e um segredo do aplicativo a partir desses provedores. Você pode habilitar qualquer combinação de provedores de identidade.

A maneira mais fácil de configurar seu grupo de usuários é usar o console do Amazon Cognito. Para obter instruções, consulte Uso da federação a partir de um grupo de usuários e Especificação das configurações do provedor de identidade para sua aplicação de grupo de usuários no Guia do desenvolvedor do Amazon Cognito.

(Opcional) Configuração de acesso granular

Talvez você tenha percebido que as configurações padrão do grupo de identidades atribui todos os usuário que fazem log in na mesma função do IAM (`Cognito_identitypoolAuth_Role`). Isso significa que todos os usuários podem acessar os mesmos recursos da AWS. Para usar o controle de acesso refinado com o Amazon Cognito, por exemplo, se desejar que os analistas da sua organização tenham acesso somente leitura a vários índices, mas que os desenvolvedores tenham acesso de gravação a todos os índices, você terá duas opções:

- Criar grupos de usuários e configurar seu provedor de identidade para escolher a função do IAM com base no token de autenticação do usuário (recomendado).
- Configurar o provedor de identidade para escolher a função do IAM com base em uma ou mais regras.

Para obter um passo a passo que inclui controle de acesso refinado, consulte the section called "Tutorial: Controle de acesso minucioso com autenticação Cognito".

> **Important**
>
> Assim como a função padrão, o Amazon Cognito deve fazer parte da relação de confiança de cada função adicional. Para obter mais detalhes, consulte Criação de funções para mapeamento de função no Guia do desenvolvedor do Amazon Cognito.

Grupos de usuários e tokens

Quando você cria um grupo de usuários, escolhe uma função do IAM para os membros do grupo. Para obter informações sobre a criação de grupos, consulte Grupos de usuários no Guia do desenvolvedor do Amazon Cognito.

Depois de criar um ou mais grupos de usuários, você pode configurar o provedor de autenticação para atribuir aos usuários suas funções de grupo em vez da função padrão do grupo de identidades. Selecione Escolher função do token e, em seguida, escolha Usar função autenticada padrão ou NEGAR para especificar como o pool de identidades lidará com os usuários que não fazem parte do grupo.

Regras

As regras são essencialmente uma série de instruções `if` que o Amazon Cognito avalia em sequência. Por exemplo, se um endereço de e-mail do usuário contiver `@corporate`, o Amazon Cognito atribuirá `Role_A` a esse usuário. Se um endereço de e-mail do usuário contém `@subsidiary`, esse usuário é atribuído a `Role_B`. Caso contrário, ele atribui ao usuário a função autenticada padrão.

Para saber mais, consulte Uso do mapeamento com base em regras para atribuir funções a usuários no Guia do desenvolvedor do Amazon Cognito.

(Opcional) Personalização da página de login

Você pode usar o console do Amazon Cognito para fazer upload de um logo personalizado e fazer alterações de CSS na página de login. Para obter instruções e uma lista completa das propriedades do CSS, consulte Especificação das configurações de personalização de interface do usuário da aplicação para seu grupo de usuários no Guia do desenvolvedor do Amazon Cognito.

(Opcional) Configuração da segurança avançada

Os grupos de usuários do Amazon Cognito oferecem suporte a recursos de segurança avançada, como a autenticação multifator, a verificação de credenciais comprometidas e a autenticação adaptável. Para saber mais, consulte Gerenciamento da segurança no Guia do desenvolvedor do Amazon Cognito.

Testes

Depois que você estiver satisfeito com sua configuração, verifique se a experiência do usuário atende às suas expectativas.

Para acessar o OpenSearch Dashboards

1. Vá para `https://`*`opensearch-domain`*`/_dashboards` em um navegador da Web. Para fazer login diretamente em um inquilino específico, anexe `?security_tenant=`*`tenant-name`* ao URL.
2. Faça login usando suas credenciais preferenciais.
3. Depois que o OpenSearch Dashboards carregar, configure pelo menos um padrão de índice. O Dashboards usa esses padrões para identificar quais índices você deseja analisar. Digite `*`, escolha Próxima etapa e, em seguida, Criar padrão de índice.
4. Para pesquisar ou explorar seus dados, escolha Descobrir.

Se qualquer etapa desse processo falhar, consulte the section called “Problemas de configuração comuns” para obter informações sobre soluções de problemas.

Cotas

O Amazon Cognito tem limites flexíveis em muitos dos seus recursos. Se desejar habilitar a autenticação do Dashboards para um grande número de domínios do OpenSearch Service, revise as Cotas do Amazon Cognito e solicite aumentos de limite conforme necessário.

Cada domínio do OpenSearch Service adiciona um cliente de aplicação ao grupo de usuários, o qual adiciona um provedor de autenticação ao grupo de identidades. Se você habilitar a autenticação do OpenSearch Dashboards para mais de 10 domínios, poderá encontrar o limite "máximo de provedores do grupo de usuários do Amazon Cognito por grupo de identidades". Se você exceder um limite, qualquer domínio do OpenSearch Service que tentar configurar para usar a autenticação

do Amazon Cognito para o Dashboards poderá ficar preso em um estado de configuração de PEm processamento.

Problemas de configuração comuns

As tabelas a seguir listam os problemas de configuração comuns e as soluções.

Configuração do OpenSearch Service

Problema	Solução
`OpenSearch Service can't create the role` (console)	Você não tem as permissões corretas do IAM. Adicione as permissões especificadas em the section called "Configuração da autenticação do Amazon Cognito (console)".
`User is not authorized to perform: iam:PassRole on resource CognitoAccessForAmazonOpenSearch` (console)	Você não tem permissões `iam:PassRole` para a função CognitoAccessForAmazonOpenSearch. Anexe a política a seguir à sua conta: `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "iam:PassRole" ], "Resource": "arn:aws:iam::  123456789012:role/service-role/CognitoAccessForAmazonOpenSearch  " } ] }` Como alternativa, você pode anexar a política `IAMFullAccess` .
`User is not authorized to perform: cognito-`	Você não tem permissões de leitura para o Amazon Cognito. Anexe a política `AmazonCognitoReadOnly` à sua conta.

Problema	Solução
`identity:ListIdentityPools on resource`	
`An error occurred (ValidationException) when calling the CreateDomain operation: OpenSearch Service must be allowed to use the passed role`	O OpenSearch Service não está especificado na relação de confiança da função `CognitoAccessForAmazonOpenSearch`. Verifique se a sua função usa a relação de confiança especificada em the section called “Sobre a função CognitoAccessForAmazonOpenSearch”. Como alternativa, use o console para configurar a autenticação do Amazon Cognito. O console cria uma função para você.
`An error occurred (ValidationException) when calling the CreateDomain operation: User is not authorized to perform: cognito-idp: action on resource: user pool`	A função especificada em `--cognito-options` não tem permissões para acessar o Amazon Cognito. Verifique se a função tem a política `AmazonOpenSearchServiceCognitoAccess` gerenciada pela AWS anexada. Como alternativa, use o console para configurar a autenticação do Amazon Cognito. O console cria uma função para você.
`An error occurred (ValidationException) when calling the CreateDomain operation: User pool does not exist`	O OpenSearch Service não consegue encontrar o grupo de usuários. Confirme se você criou um e se tem o ID correto. Para encontrar o ID, você pode usar o console do Amazon Cognito ou o seguinte comando da AWS CLI: `aws cognito-idp list-user-pools --max-results 60 --region region`
`An error occurred (ValidationException) when calling the CreateDomain operation: IdentityPool not found`	O OpenSearch Service não consegue encontrar o grupo de identidades. Confirme se você criou um e se tem o ID correto. Para encontrar o ID, você pode usar o console do Amazon Cognito ou o seguinte comando da AWS CLI: `aws cognito-identity list-identity-pools --max-results 60 --region region`

Problema	Solução
`An error occurred (ValidationException) when calling the CreateDomain operation: Domain needs to be specified for user pool`	O grupo de usuários não tem um nome de domínio. Você pode configurar um usando o console do Amazon Cognito ou o seguinte comando da AWS CLI: `aws cognito-idp create-user-pool-domain --domain name --user-pool-id id`

Acesso ao OpenSearch Dashboards

Problema	Solução
A página de login não mostra meus provedores de identidade preferenciais.	Verifique se você habilitou o provedor de identidade para o cliente da aplicação do OpenSearch Service, conforme especificado em the section called “Configuração de provedores de identidade”.
A página de login não parece estar associada à minha organização.	Consulte the section called “(Opcional) Personalização da página de login”.
Minhas credenciais de login não funcionam.	Verifique se você configurou o provedor de identidade conforme especificado em the section called “Configuração de provedores de identidade”. Se você usa o grupo de usuários como seu provedor de identidade, verifique se a conta existe no console do Amazon Cognito.
O OpenSearch Dashboards não carrega ou não funciona corretamente.	A função autenticada do Amazon Cognito precisa de permissões `es:ESHttp*` para o domínio (`/*`) a fim de acessar e usar o Dashboards. Verifique se você adicionou uma política de acesso conforme especificado em the section called “Como permitir a função autenticada”.
Quando eu desconecto do OpenSearch Dashboards em uma	Quando você desconecta de uma sessão do OpenSearch Dashboards enquanto usa a autenticação do Amazon

Problema	Solução
guia, as guias restantes exibem uma mensagem informando que o token de atualização foi revogado.	Cognito, o OpenSearch Service executa uma operação AdminUserGlobalSignout, que desconecta você de todas as sessões ativas do OpenSearch Dashboards.
`Invalid identity pool configuration. Check assigned IAM roles for this pool.`	O Amazon Cognito não tem permissões para assumir a função do IAM em nome do usuário autenticado. Modifique a relação de confiança da função para incluir: `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principal": { "Federated": "cognito-identity.amazonaws.com" }, "Action": "sts:AssumeRoleWithWebIdentity", "Condition": { "StringEquals": { "cognito-identity.amazonaws.com:aud": " identity-pool-id " }, "ForAnyValue:StringLike": { "cognito-identity.amazonaws.com:amr": "authenticated" } } }] }`
`Token is not from a supported provider of this identity pool.`	Este erro incomum pode ocorrer quando você remover o cliente do aplicativo a partir do grupo de usuários. Tente abrir o Dashboards em uma nova sessão do navegador.

Desabilitação da autenticação do Amazon Cognito para OpenSearch Dashboards

Use o procedimento a seguir para desabilitar a autenticação do Amazon Cognito para Dashboards.

Para desabilitar a autenticação do Amazon Cognito para Dashboards (console)

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home/.
2. Em Domínios, escolha o domínio que deseja configurar.
3. Escolha Ações, Editar configuração de segurança.
4. Desmarque a opção Habilitar autenticação do Amazon Cognito.
5. Escolha Salvar alterações.

> **Important**
>
> Se você não precisar mais do grupo de usuários e do grupo de identidades do Amazon Cognito, exclua-os. Caso contrário, você continuará a ser cobrado.

Exclusão de domínios que usam a autenticação do Amazon Cognito para OpenSearch Dashboards

Para evitar que domínios que usem a autenticação do Amazon Cognito para Dashboards fiquem presos em um estado de configuração Em processamento , exclua domínios do OpenSearch Service antes de excluir os grupos de usuários e grupos de identidades do Amazon Cognito associados.

Usar perfis vinculados ao serviço com o Amazon OpenSearch Service

O Amazon OpenSearch Service usa funções vinculadas ao serviço do AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de perfil do (IAM) vinculado diretamente ao OpenSearch Service. As funções vinculadas a serviços são predefinidas pelo OpenSearch Service e incluem todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome.

Uma função vinculada ao serviço facilita a configuração do OpenSearch Service porque você não precisa adicionar as permissões necessárias manualmente. O OpenSearch Service define as permissões das funções vinculadas ao serviço e, exceto se definido de outra forma, somente o OpenSearch Service pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política não pode ser anexada a nenhuma outra entidade do IAM. Para atualizações das políticas de funções e permissões vinculadas ao serviço, consulte Histórico de documentação do Amazon OpenSearch Service.

Para obter informações sobre outros serviços compatíveis com funções vinculadas aos serviços, consulte serviços da AWS que funcionam com o IAM e procure os serviços que apresentam Sim na coluna Funções vinculadas aos serviços. Escolha um Sim com um link para visualizar a documentação da função vinculada a esse serviço.

Tópicos

- Uso de funções vinculadas ao serviço para criar domínios da VPC
- Uso de funções vinculadas ao serviço para criar coleções do OpenSearch Sem Servidor
- Uso de funções vinculadas ao serviço para criar pipelines de Ingestão do OpenSearch

Uso de funções vinculadas ao serviço para criar domínios da VPC

O Amazon OpenSearch Service usa funções vinculadas ao serviço do AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de perfil do (IAM) vinculado diretamente ao OpenSearch Service. As funções vinculadas a serviços são predefinidas pelo OpenSearch Service e incluem todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome.

O OpenSearch Service usa a função vinculada ao serviço denominada AWSServiceRoleForAmazonOpenSearchService, que fornece as permissões mínimas do Amazon EC2 e do Elastic Load Balancing necessárias para a função habilitar o acesso por VPC para um domínio.

Função legada do Elasticsearch

O Amazon OpenSearch Service usa uma função vinculada ao serviço denominada `AWSServiceRoleForAmazonOpenSearchService`. Suas contas também podem conter uma função vinculada ao serviço herdada chamada `AWSServiceRoleForAmazonElasticsearchService`, que funciona com os endpoints obsoletos da API Elasticsearch.

Se a função herdada do Elasticsearch não existir em sua conta, o OpenSearch Service cria automaticamente uma nova função vinculada ao serviço OpenSearch na primeira vez que você cria um domínio OpenSearch. Caso contrário, sua conta continuará usando a função Elasticsearch. Para que essa criação automática seja bem-sucedida, você precisa ter permissões para a ação `iam:CreateServiceLinkedRole`.

Permissões

A função vinculada ao serviço `AWSServiceRoleForAmazonOpenSearchService` confia nos seguintes serviços para assumir a função:

- `opensearchservice.amazonaws.com`

A política de permissões da função `AmazonOpenSearchServiceRolePolicy` permite que o OpenSearch Service conclua as seguintes ações nos recursos especificados:

- Ação: `acm:DescribeCertificate` em *
- Ação: `cloudwatch:PutMetricData` em *
- Ação: `ec2:CreateNetworkInterface` em *
- Ação: `ec2:DeleteNetworkInterface` em *
- Ação: `ec2:DescribeNetworkInterfaces` em *
- Ação: `ec2:ModifyNetworkInterfaceAttribute` em *
- Ação: `ec2:DescribeSecurityGroups` em *
- Ação: `ec2:DescribeSubnets` em *
- Ação: `ec2:DescribeVpcs` em *
- Ação: `ec2:CreateTags` em todas as interfaces de rede e endpoints da VPC
- Ação: `ec2:DescribeTags` em *
- Ação: `ec2:CreateVpcEndpoint` em todas as VPCs, grupos de segurança, sub-redes e tabelas de rotas, bem como em todos os endpoints da VPC, quando a solicitação contiver a tag `OpenSearchManaged=true`
- Ação: `ec2:ModifyVpcEndpoint` em todas as VPCs, grupos de segurança, sub-redes e tabelas de rotas, bem como em todos os endpoints da VPC, quando a solicitação contiver a tag `OpenSearchManaged=true`
- Ação: `ec2:DeleteVpcEndpoints` em todos os endpoints quando a solicitação contiver a tag `OpenSearchManaged=true`

- Ação: `ec2:AssignIpv6Addresses` em *
- Ação: `ec2:UnAssignIpv6Addresses` em *
- Ação: `elasticloadbalancing:AddListenerCertificates` em *
- Ação: `elasticloadbalancing:RemoveListenerCertificates` em *

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Permissões de função vinculada a serviços no Guia do usuário do IAM.

Criar uma função vinculada ao serviço

Não é necessário criar manualmente uma função vinculada ao serviço. Ao criar um domínio habilitado para VPC usando o AWS Management Console, o OpenSearch Service cria a função vinculada ao serviço para você. Para que essa criação automática seja bem-sucedida, você precisa ter permissões para a ação `iam:CreateServiceLinkedRole`.

Também é possível usar o console do IAM, a CLI do IAM ou a API do IAM para criar manualmente uma função vinculada ao serviço. Para obter mais informações, consulte Criação de uma função vinculada ao serviço no Manual do usuário do IAM.

Edição da função vinculada ao serviço

O OpenSearch Service não permite que você edite a função vinculada ao serviço `AWSServiceRoleForAmazonOpenSearchService`. Depois que você criar uma função vinculada a serviço, não poderá alterar o nome da função, pois várias entidades podem fazer referência à função. No entanto, você poderá editar a descrição da função usando o IAM. Para ter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço

Se você não precisar mais usar um recurso ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar sua função vinculada ao serviço para excluí-la manualmente.

Limpar a função vinculada ao serviço

Antes de você poder usar o IAM para excluir uma função vinculada ao serviço, você deve primeiro confirmar que a função não tem sessões ativas e remover quaisquer recursos usados pela função.

Para verificar se a função vinculada ao serviço tem uma sessão ativa no console do IAM

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação do console do IAM, escolha Perfis. A seguir, selecione o nome (não a caixa de seleção) da função `AWSServiceRoleForAmazonOpenSearchService`.
3. Na página Resumo para a função selecionada, escolha a guia Consultor de Acesso.
4. Na guia Consultor de Acesso, revise a atividade recente para a função vinculada ao serviço.

> **Note**
>
> Se não tiver certeza se o OpenSearch Service está usando a função `AWSServiceRoleForAmazonOpenSearchService`, você poderá tentar excluí-la. Se o serviço estiver usando a função, a exclusão falhará e você poderá visualizar os recursos usando a função. Se a função estiver sendo usada, você deverá aguardar o término da sessão antes de poder excluir a função e/ou excluir os recursos usando a função. Você não pode revogar a sessão para uma função vinculada a serviço.

Exclusão manual de uma função vinculada ao serviço

Exclua funções vinculadas ao serviço do console do IAM, da API ou da AWS CLI. Para obter instruções, consulte Exclusão de uma função vinculada ao serviço no Manual do usuário do IAM.

Uso de funções vinculadas ao serviço para criar coleções do OpenSearch Sem Servidor

O tecnologia sem servidor do OpenSearch usa perfis vinculados ao serviço do AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de perfil do (IAM) vinculado diretamente ao OpenSearch Service. As funções vinculadas a serviços são predefinidas pelo OpenSearch Service e incluem todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome.

O tecnologia sem servidor do OpenSearch usa a função vinculada ao serviço denominada AWSServiceRoleForAmazonOpenSearchServerless, que fornece as permissões necessárias para que a função publique métricas do CloudWatch relacionadas a tecnologia sem servidor em sua conta.

Permissões da função vinculada ao serviço do OpenSearch Sem Servidor

O tecnologia sem servidor do OpenSearch usa a função vinculada ao serviço denominada AWSServiceRoleForAmazonOpenSearchServerless, que permite aa tecnologia sem servidor do OpenSearch chamar serviços da AWS em seu nome.

O perfil vinculado ao serviço AWSServiceRoleForAmazonOpenSearchServerless confia nos seguintes serviços para assumir o perfil:

- `observability.aoss.amazonaws.com`

A política de permissões da função `AmazonOpenSearchServerlessServiceRolePolicy` permite que o OpenSearch Sem Servidor conclua as seguintes ações nos recursos especificados:

- Ação: `cloudwatch:PutMetricData` em todos os recursos da AWS.

> **Note**
>
> A política inclui a chave de condição `{"StringEquals": {"cloudwatch:namespace": "AWS/AOSS"}}`, o que significa que a função vinculada ao serviço só pode enviar dados métricos para o namespace do `AWS/AOSS` CloudWatch.

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Permissões de função vinculada a serviços no Guia do usuário do IAM.

Criação da função vinculada ao serviço da tecnologia sem servidor do OpenSearch

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você cria uma coleção do OpenSearch Sem Servidor no AWS Management Console, na AWS CLI ou na API da AWS, o OpenSearch Sem Servidor cria a função vinculada ao serviço para você.

> **Note**
>
> Na primeira vez que você criar uma coleção, deverá receber a atribuição de `iam:CreateServiceLinkedRole` em uma política baseada em identidade.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você poderá usar esse mesmo processo para recriar a função em sua conta. Quando você cria uma coleção do OpenSearch Sem Servidor, o OpenSearch Sem Servidor cria a função vinculada ao serviço para você novamente.

Você também pode usar o console do IAM para criar uma função vinculada ao serviço com o caso de uso do Amazon OpenSearch Sem Servidor. Na AWS CLI ou na API do AWS, crie uma função vinculada ao serviço com o nome de serviço `observability.aoss.amazonaws.com`:

```
aws iam create-service-linked-role --aws-service-name
 "observability.aoss.amazonaws.com"
```

Para obter mais informações, consulte Criação de uma função vinculada ao serviço no Manual do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

Edição de uma função vinculada ao serviço da tecnologia sem servidor do OpenSearch

O tecnologia sem servidor do OpenSearch não permite que você edite a função vinculada ao serviço AWSServiceRoleForAmazonOpenSearchServerless. Depois que você criar uma função vinculada a serviço, não poderá alterar o nome da função, pois várias entidades podem fazer referência à função. No entanto, você poderá editar a descrição da função usando o IAM. Para ter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Exclusão da função vinculada ao serviço da tecnologia sem servidor do OpenSearch

Se você não precisar mais usar um recurso ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Isso evita que você tenha uma entidade não utilizada que não seja ativamente monitorada ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de excluí-la manualmente.

Para excluir a AWSServiceRoleForAmazonOpenSearchServerless, exclua primeiro todas as coleções da tecnologia sem servidor do OpenSearch em seu Conta da AWS.

> **Note**
>
> Se o OpenSearch Sem Servidor estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Como excluir manualmente a função vinculada ao serviço usando o IAM

Use o console do IAM, a AWS CLI ou a API da AWS para excluir a função vinculada ao serviço AWSServiceRoleForAmazonOpenSearchServerless. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Regiões com suporte para funções vinculadas ao serviço do OpenSearch Sem Servidor

O tecnologia sem servidor do OpenSearch oferece suporte ao uso da função vinculada ao serviço AWSServiceRoleForAmazonOpenSearchServerless em todas as regiões em que a tecnologia sem servidor do OpenSearch estiver disponível. Para obter uma lista das regiões compatíveis, consulte Endpoints e cotas do Amazon OpenSearch Sem Servidor na Referência geral da AWS.

Uso de funções vinculadas ao serviço para criar pipelines de Ingestão do OpenSearch

A Ingestão do Amazon OpenSearch usa funções vinculadas a serviço do AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de perfil do (IAM) vinculado diretamente à Ingestão do OpenSearch. As funções vinculadas a serviços são predefinidas pela Ingestão do OpenSearch e incluem todas as permissões que o serviço requer para chamar outros serviços da AWS em seu nome.

A Ingestão do OpenSearch usa a função vinculada ao serviço chamada AWSServiceRoleForAmazonOpenSearchIngestion. A política anexada fornece as permissões necessárias para que o perfil crie uma nuvem privada virtual (VPC) entre sua conta e na Ingestão do OpenSearch e publique métricas do CloudWatch em sua conta.

Permissões

A função vinculada ao serviço `AWSServiceRoleForAmazonOpenSearchIngestion` confia nos seguintes serviços para assumir a função:

- `osis.amazon.com`

A política de permissões da função `AmazonOpenSearchIngestionServiceRolePolicy` permite que a Ingestão do OpenSearch conclua as seguintes ações nos recursos especificados:

- Ação: `ec2:DescribeSubnets` em `*`

- Ação: `ec2:DescribeSecurityGroups` em *
- Ação: `ec2:DeleteVpcEndpoints` em *
- Ação: `ec2:CreateVpcEndpoint` em *
- Ação: `ec2:DescribeVpcEndpoints` em *
- Ação: `ec2:CreateTags` em `arn:aws:ec2:*:*:network-interface/*`
- Ação: `cloudwatch:PutMetricData` em `cloudwatch:namespace": "AWS/OSIS"`

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada ao serviço. Para obter mais informações, consulte Permissões de função vinculada a serviços no Guia do usuário do IAM.

Criação de perfil vinculada ao serviço de Ingestão do OpenSearch

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você cria um pipeline de Ingestão do OpenSearch no AWS Management Console, o AWS CLI, ou a API do AWS, a Ingestão do OpenSearch cria a função vinculada ao serviço para você.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você poderá usar esse mesmo processo para recriar a função em sua conta. Quando você cria um pipeline de Ingestão do OpenSearch, a Ingestão do OpenSearch recria o perfil vinculado ao serviço para você.

Edição de perfil vinculada ao serviço de Ingestão do OpenSearch

A Ingestão do OpenSearch não permite editar a função vinculada ao serviço `AWSServiceRoleForAmazonOpenSearchIngestion`. Depois que criar uma função vinculada ao serviço, você não poderá alterar o nome da função, pois várias entidades podem fazer referência a ela. No entanto, será possível editar a descrição da função usando o IAM. Para ter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Exclusão de perfil vinculada ao serviço de Ingestão do OpenSearch

Se você não precisar mais usar um recurso ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar os recursos de sua função vinculada ao serviço antes de exclui-la manualmente.

Limpar uma função vinculada ao serviço

Antes de usar o IAM para excluir uma função vinculada ao serviço, você deverá excluir qualquer recurso usado pela função.

> **Note**
>
> Se a Ingestão do OpenSearch estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Como excluir os recursos de Ingestão do OpenSearch usados pelo **`AWSServiceRoleForAmazonOpenSearchIngestion`**

1. Navegue até o console do Amazon OpenSearch Service e escola Ingestão.
2. Exclua todos os pipelines. Para obter instruções, consulte the section called “Exclusão de pipelines”.

Exclusão de função vinculada ao serviço de Ingestão do OpenSearch

É possível usar o console da Ingestão do OpenSearch para excluir uma função vinculada a serviço.

Para excluir uma função vinculada ao serviço (console)

1. Navegue até o console do IAM.
2. Escolha Perfis e busque o perfil AWSServiceRoleForAmazonOpenSearchIngestion.
3. Selecione a função e escolha Excluir.

Código de exemplo do Amazon OpenSearch Service

Este capítulo contém um código de exemplo comum para trabalhar com o Amazon OpenSearch Service: assinatura de solicitação HTTP em diversas linguagens de programação, compactação de corpos de solicitações HTTP e uso de AWS SDKs para criar domínios.

Tópicos

Compatibilidade com clientes Elasticsearch

As versões mais recentes dos clientes Elasticsearch podem incluir verificações de licença ou versão que interrompem artificialmente a compatibilidade. A tabela a seguir inclui recomendações de quais versões desses clientes devem ser usadas para melhor compatibilidade com o OpenSearch Service.

> **Important**
>
> Essas versões do cliente estão desatualizadas e não estão atualizadas com as dependências mais recentes, incluindo o Log4j. É altamente recomendável usar as versões do OpenSearch dos clientes sempre que possível.

Cliente	Versão recomendada
Cliente REST de baixo nível Java	7.13.4
Cliente REST de alto nível Java	7.13.4
Cliente Elasticsearch Python	7.13.4
Cliente Elasticsearch Ruby	7.13.3
Cliente Elasticsearch Node.js	7.13.0

Compactação de solicitações HTTP no Amazon OpenSearch Service

Você pode compactar solicitações e respostas HTTP nos domínios do Amazon OpenSearch Service usando a compactação gzip. A compactação gzip pode ajudar a reduzir o tamanho de seus documentos e reduzir a utilização e a latência da largura de banda, levando a velocidades de transferência aprimoradas.

A compactação gzip é compatível com todos os domínios que executam o OpenSearch ou o Elasticsearch 6.0 ou posterior. Alguns clientes OpenSearch oferecem suporte interno à compactação gzip, e muitas linguagens de programação têm bibliotecas que simplificam o processo.

Habilitação da compactação gzip

Não confunda com configurações semelhantes do OpenSearch, `http_compression.enabled` é específico do OpenSearch Service e habilita ou desabilita a compactação gzip em um domínio. Domínios que executam o OpenSearch ou o Elasticsearch 7.x têm a compactação gzip habilitada por padrão, enquanto os domínios que executam o Elasticsearch 6.x têm o recurso desabilitado por padrão.

Para habilitar a compactação gzip, envie a seguinte solicitação:

```
PUT _cluster/settings
{
  "persistent" : {
    "http_compression.enabled": true
  }
}
```

As solicitações para `_cluster/settings` devem ser descompactadas, então você talvez precise usar um cliente separado ou uma solicitação HTTP padrão para atualizar as configurações do cluster.

Cabeçalhos obrigatórios

Ao incluir um corpo de solicitação compactado com gzip, mantenha o cabeçalho `Content-Type: application/json` padrão e adicione o cabeçalho `Content-Encoding: gzip`. Para aceitar uma resposta compactada por gzip, adicione o cabeçalho `Accept-Encoding: gzip` também.

Quando um cliente OpenSearch oferece suporte à compactação gzip, ele provavelmente inclui esses cabeçalhos automaticamente.

Código de exemplo (Python 3)

O exemplo a seguir usa opensearch-py para executar a compactação e enviar a solicitação. Esse código assina a solicitação usando suas credenciais do IAM.

```
from opensearchpy import OpenSearch, RequestsHttpConnection
from requests_aws4auth import AWS4Auth
import boto3

host = '' # e.g. my-test-domain.us-east-1.es.amazonaws.com
region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

# Create the client.
search = OpenSearch(
    hosts = [{'host': host, 'port': 443}],
    http_auth = awsauth,
    use_ssl = True,
    verify_certs = True,
    http_compress = True, # enables gzip compression for request bodies
    connection_class = RequestsHttpConnection
)

document = {
  "title": "Moneyball",
  "director": "Bennett Miller",
  "year": "2011"
}

# Send the request.
print(search.index(index='movies', id='1', body=document, refresh=True))

# print(search.index(index='movies', doc_type='_doc', id='1', body=document,
 refresh=True))
```

Alternativamente, você pode especificar os cabeçalhos apropriados, compactar o corpo da solicitação e usar uma biblioteca HTTP padrão como Requests. Este código assina a solicitação

usando credenciais básicas HTTP, às quais seu domínio pode oferecer suporte se você usa o controle de acesso refinado.

```
import requests
import gzip
import json

base_url = '' # The domain with https:// and a trailing slash. For example, https://my-
test-domain.us-east-1.es.amazonaws.com/
auth = ('master-user', 'master-user-password') # For testing only. Don't store
 credentials in code.

headers = {'Accept-Encoding': 'gzip', 'Content-Type': 'application/json',
           'Content-Encoding': 'gzip'}

document = {
  "title": "Moneyball",
  "director": "Bennett Miller",
  "year": "2011"
}

# Compress the document.
compressed_document = gzip.compress(json.dumps(document).encode())

# Send the request.
path = 'movies/_doc?refresh=true'
url = base_url + path
response = requests.post(url, auth=auth, headers=headers, data=compressed_document)
print(response.status_code)
print(response.text)
```

Uso de AWS SDKs para interagir com o Amazon OpenSearch Service

Esta seção inclui exemplos de como usar os AWS SDKs para interagir com a API de configuração do Amazon OpenSearch Service. Esses exemplos de códigos mostram como criar, atualizar e excluir domínios do OpenSearch Service.

Java

Esta seção inclui exemplos para as versões 1 e 2 do AWS SDK for Java.

Version 2

Este exemplo usa o construtor AmazonOpenSearchClientBuilder da versão 2 do AWS SDK for Java para criar um domínio do OpenSearch, atualizar sua configuração e excluí-lo. Remova os comentários das chamadas para `waitForDomainProcessing` (e comente as chamadas para `deleteDomain`) para permitir que o domínio fique online e seja utilizável.

```
package com.example.samples;

import java.util.concurrent.TimeUnit;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.opensearch.OpenSearchClient;
import software.amazon.awssdk.services.opensearch.model.ClusterConfig;
import software.amazon.awssdk.services.opensearch.model.EBSOptions;
import software.amazon.awssdk.services.opensearch.model.CognitoOptions;
import software.amazon.awssdk.services.opensearch.model.NodeToNodeEncryptionOptions;
import software.amazon.awssdk.services.opensearch.model.CreateDomainRequest;
import software.amazon.awssdk.services.opensearch.model.CreateDomainResponse;
import software.amazon.awssdk.services.opensearch.model.DescribeDomainRequest;
import software.amazon.awssdk.services.opensearch.model.UpdateDomainConfigRequest;
import software.amazon.awssdk.services.opensearch.model.UpdateDomainConfigResponse;
import software.amazon.awssdk.services.opensearch.model.DescribeDomainResponse;
import software.amazon.awssdk.services.opensearch.model.DeleteDomainRequest;
import software.amazon.awssdk.services.opensearch.model.DeleteDomainResponse;
import software.amazon.awssdk.services.opensearch.model.OpenSearchException;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

/**
 * Sample class demonstrating how to use the Amazon Web Services SDK for Java to
 create, update,
 * and delete Amazon OpenSearch Service domains.
 */

public class OpenSearchSample {

    public static void main(String[] args) {

     String domainName = "my-test-domain";

     // Build the client using the default credentials chain.
        // You can use the CLI and run `aws configure` to set access key, secret
        // key, and default region.
```

```
        OpenSearchClient client = OpenSearchClient.builder()
          // Unnecessary, but lets you use a region different than your default.
          .region(Region.US_EAST_1)
          // Unnecessary, but if desired, you can use a different provider chain.
          .credentialsProvider(DefaultCredentialsProvider.create())
                    .build();

        // Create a new domain, update its configuration, and delete it.
        createDomain(client, domainName);
        //waitForDomainProcessing(client, domainName);
        updateDomain(client, domainName);
        //waitForDomainProcessing(client, domainName);
        deleteDomain(client, domainName);
    }

    /**
     * Creates an Amazon OpenSearch Service domain with the specified options.
     * Some options require other Amazon Web Services resources, such as an Amazon
Cognito user pool
     * and identity pool, whereas others require just an instance type or instance
     * count.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain you want to create
     */

    public static void createDomain(OpenSearchClient client, String domainName) {

     // Create the request and set the desired configuration options

        try {

            ClusterConfig clusterConfig = ClusterConfig.builder()
                    .dedicatedMasterEnabled(true)
                    .dedicatedMasterCount(3)
                    // Small, inexpensive instance types for testing. Not
recommended for production.
                    .dedicatedMasterType("t2.small.search")
                    .instanceType("t2.small.search")
                    .instanceCount(5)
                    .build();
```

```
            // Many instance types require EBS storage.
            EBSOptions ebsOptions = EBSOptions.builder()
                    .ebsEnabled(true)
                    .volumeSize(10)
                    .volumeType("gp2")
                    .build();

            NodeToNodeEncryptionOptions encryptionOptions =
 NodeToNodeEncryptionOptions.builder()
                    .enabled(true)
                    .build();

            CreateDomainRequest createRequest = CreateDomainRequest.builder()
                    .domainName(domainName)
                    .engineVersion("OpenSearch_1.0")
                    .clusterConfig(clusterConfig)
                    .ebsOptions(ebsOptions)
                    .nodeToNodeEncryptionOptions(encryptionOptions)
                    // You can uncomment this line and add your account ID, a
 username, and the
                    // domain name to add an access policy.
                    // .accessPolicies("{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:region:123456789012:domain/domain-name/*\"}]}")
                    .build();

            // Make the request.
            System.out.println("Sending domain creation request...");
            CreateDomainResponse createResponse =
 client.createDomain(createRequest);
            System.out.println("Domain status:
 "+createResponse.domainStatus().toString());
            System.out.println("Domain ID:
 "+createResponse.domainStatus().domainId());


        } catch (OpenSearchException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }

    /**
```

```
    * Updates the configuration of an Amazon OpenSearch Service domain with the
    * specified options. Some options require other Amazon Web Services resources,
such as an
    * Amazon Cognito user pool and identity pool, whereas others require just an
    * instance type or instance count.
    *
    * @param client
    *            The client to use for the requests to Amazon OpenSearch Service
    * @param domainName
    *            The name of the domain to update
    */

   public static void updateDomain(OpenSearchClient client, String domainName) {

    // Updates the domain to use three data instances instead of five.
       // You can uncomment the Cognito line and fill in the strings to enable
Cognito
       // authentication for OpenSearch Dashboards.

       try {

           ClusterConfig clusterConfig = ClusterConfig.builder()
                   .instanceCount(5)
                   .build();

           CognitoOptions cognitoOptions = CognitoOptions.builder()
                   .enabled(true)
                   .userPoolId("user-pool-id")
                   .identityPoolId("identity-pool-id")
                   .roleArn("role-arn")
                   .build();

           UpdateDomainConfigRequest updateRequest =
UpdateDomainConfigRequest.builder()
                   .domainName(domainName)
                   .clusterConfig(clusterConfig)
                   //.cognitoOptions(cognitoOptions)
                   .build();

           System.out.println("Sending domain update request...");
           UpdateDomainConfigResponse updateResponse =
client.updateDomainConfig(updateRequest);
           System.out.println("Domain config:
"+updateResponse.domainConfig().toString());
```

```
        } catch (OpenSearchException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }

    /**
     * Deletes an Amazon OpenSearch Service domain. Deleting a domain can take
     * several minutes.
     *
     * @param client
     *             The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *             The name of the domain that you want to delete
     */

    public static void deleteDomain(OpenSearchClient client, String domainName) {

        try {

            DeleteDomainRequest deleteRequest = DeleteDomainRequest.builder()
                    .domainName(domainName)
                    .build();

            System.out.println("Sending domain deletion request...");
            DeleteDomainResponse deleteResponse =
client.deleteDomain(deleteRequest);
            System.out.println("Domain status: "+deleteResponse.toString());


        } catch (OpenSearchException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }

    /**
     * Waits for the domain to finish processing changes. New domains typically take
15-30 minutes
     * to initialize, but can take longer depending on the configuration. Most
updates to existing domains
```

```
     * take a similar amount of time. This method checks every 15 seconds and
 finishes only when
     * the domain's processing status changes to false.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain that you want to check
     */

    public static void waitForDomainProcessing(OpenSearchClient client, String
 domainName) {
        // Create a new request to check the domain status.
        DescribeDomainRequest describeRequest = DescribeDomainRequest.builder()
                .domainName(domainName)
                .build();

        // Every 15 seconds, check whether the domain is processing.
        DescribeDomainResponse describeResponse =
 client.describeDomain(describeRequest);
        while (describeResponse.domainStatus().processing()) {
            try {
                System.out.println("Domain still processing...");
                TimeUnit.SECONDS.sleep(15);
                describeResponse = client.describeDomain(describeRequest);
            } catch (InterruptedException e) {
                e.printStackTrace();
            }
        }

        // Once we exit that loop, the domain is available
        System.out.println("Amazon OpenSearch Service has finished processing
 changes for your domain.");
        System.out.println("Domain description: "+describeResponse.toString());
    }
}
```

Version 1

Este exemplo usa o construtor AWSElasticsearchClientBuilder da versão 1 do AWS SDK for Java para criar um domínio legado do Elasticsearch herdado, atualizar sua configuração e excluí-lo. Remova os comentários das chamadas para `waitForDomainProcessing` (e comente as chamadas para `deleteDomain`) para permitir que o domínio fique online e seja utilizável.

```
package com.amazonaws.samples;

import java.util.concurrent.TimeUnit;
import com.amazonaws.auth.DefaultAWSCredentialsProviderChain;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.elasticsearch.AWSElasticsearch;
import com.amazonaws.services.elasticsearch.AWSElasticsearchClientBuilder;
import com.amazonaws.services.elasticsearch.model.CreateElasticsearchDomainRequest;
import com.amazonaws.services.elasticsearch.model.CreateElasticsearchDomainResult;
import com.amazonaws.services.elasticsearch.model.DeleteElasticsearchDomainRequest;
import com.amazonaws.services.elasticsearch.model.DeleteElasticsearchDomainResult;
import
 com.amazonaws.services.elasticsearch.model.DescribeElasticsearchDomainRequest;
import com.amazonaws.services.elasticsearch.model.DescribeElasticsearchDomainResult;
import com.amazonaws.services.elasticsearch.model.EBSOptions;
import com.amazonaws.services.elasticsearch.model.ElasticsearchClusterConfig;
import com.amazonaws.services.elasticsearch.model.ResourceNotFoundException;
import
 com.amazonaws.services.elasticsearch.model.UpdateElasticsearchDomainConfigRequest;
import
 com.amazonaws.services.elasticsearch.model.UpdateElasticsearchDomainConfigResult;
import com.amazonaws.services.elasticsearch.model.VolumeType;

/**
 * Sample class demonstrating how to use the Amazon Web Services SDK for Java to
 create, update,
 * and delete Amazon OpenSearch Service domains.
 */

public class OpenSearchSample {

    public static void main(String[] args) {

        final String domainName = "my-test-domain";

        // Build the client using the default credentials chain.
        // You can use the CLI and run `aws configure` to set access key, secret
        // key, and default region.
        final AWSElasticsearch client = AWSElasticsearchClientBuilder
                .standard()
                // Unnecessary, but lets you use a region different than your
 default.
                .withRegion(Regions.US_WEST_2)
```

```
                // Unnecessary, but if desired, you can use a different provider
chain.
                .withCredentials(new DefaultAWSCredentialsProviderChain())
                .build();

        // Create a new domain, update its configuration, and delete it.
        createDomain(client, domainName);
        // waitForDomainProcessing(client, domainName);
        updateDomain(client, domainName);
        // waitForDomainProcessing(client, domainName);
        deleteDomain(client, domainName);
    }

    /**
     * Creates an Amazon OpenSearch Service domain with the specified options.
     * Some options require other Amazon Web Services resources, such as an Amazon
Cognito user pool
     * and identity pool, whereas others require just an instance type or instance
     * count.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain you want to create
     */
    private static void createDomain(final AWSElasticsearch client, final String
domainName) {

        // Create the request and set the desired configuration options
        CreateElasticsearchDomainRequest createRequest = new
CreateElasticsearchDomainRequest()
                .withDomainName(domainName)
                .withElasticsearchVersion("7.10")
                .withElasticsearchClusterConfig(new ElasticsearchClusterConfig()
                        .withDedicatedMasterEnabled(true)
                        .withDedicatedMasterCount(3)
                        // Small, inexpensive instance types for testing. Not
recommended for production
                        // domains.
                        .withDedicatedMasterType("t2.small.elasticsearch")
                        .withInstanceType("t2.small.elasticsearch")
                        .withInstanceCount(5))
                // Many instance types require EBS storage.
                .withEBSOptions(new EBSOptions()
```

```
                        .withEBSEnabled(true)
                        .withVolumeSize(10)
                        .withVolumeType(VolumeType.Gp2));
                // You can uncomment this line and add your account ID, a username,
 and the
                // domain name to add an access policy.
                // .withAccessPolicies("{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:region:123456789012:domain/domain-name/*\"}]}")


        // Make the request.
        System.out.println("Sending domain creation request...");
        CreateElasticsearchDomainResult createResponse =
 client.createElasticsearchDomain(createRequest);
        System.out.println("Domain creation response from Amazon OpenSearch
 Service:");
        System.out.println(createResponse.getDomainStatus().toString());
    }

    /**
     * Updates the configuration of an Amazon OpenSearch Service domain with the
     * specified options. Some options require other Amazon Web Services resources,
 such as an
     * Amazon Cognito user pool and identity pool, whereas others require just an
     * instance type or instance count.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain to update
     */
    private static void updateDomain(final AWSElasticsearch client, final String
 domainName) {
        try {
            // Updates the domain to use three data instances instead of five.
            // You can uncomment the Cognito lines and fill in the strings to enable
 Cognito
            // authentication for OpenSearch Dashboards.
            final UpdateElasticsearchDomainConfigRequest updateRequest = new
 UpdateElasticsearchDomainConfigRequest()
                    .withDomainName(domainName)
                    // .withCognitoOptions(new CognitoOptions()
```

```
                            // .withEnabled(true)
                            // .withUserPoolId("user-pool-id")
                            // .withIdentityPoolId("identity-pool-id")
                            // .withRoleArn("role-arn")
                    .withElasticsearchClusterConfig(new ElasticsearchClusterConfig()
                            .withInstanceCount(3));

            System.out.println("Sending domain update request...");
            final UpdateElasticsearchDomainConfigResult updateResponse = client
                    .updateElasticsearchDomainConfig(updateRequest);
            System.out.println("Domain update response from Amazon OpenSearch
Service:");
            System.out.println(updateResponse.toString());
        } catch (ResourceNotFoundException e) {
            System.out.println("Domain not found. Please check the domain name.");
        }
    }

    /**
     * Deletes an Amazon OpenSearch Service domain. Deleting a domain can take
     * several minutes.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain that you want to delete
     */
    private static void deleteDomain(final AWSElasticsearch client, final String
domainName) {
        try {
            final DeleteElasticsearchDomainRequest deleteRequest = new
DeleteElasticsearchDomainRequest()
                    .withDomainName(domainName);

            System.out.println("Sending domain deletion request...");
            final DeleteElasticsearchDomainResult deleteResponse =
client.deleteElasticsearchDomain(deleteRequest);
            System.out.println("Domain deletion response from Amazon OpenSearch
Service:");
            System.out.println(deleteResponse.toString());
        } catch (ResourceNotFoundException e) {
            System.out.println("Domain not found. Please check the domain name.");
        }
    }
```

```
   /**
    * Waits for the domain to finish processing changes. New domains typically take
15-30 minutes
    * to initialize, but can take longer depending on the configuration. Most
updates to existing domains
    * take a similar amount of time. This method checks every 15 seconds and
finishes only when
    * the domain's processing status changes to false.
    *
    * @param client
    *            The client to use for the requests to Amazon OpenSearch Service
    * @param domainName
    *            The name of the domain that you want to check
    */
   private static void waitForDomainProcessing(final AWSElasticsearch client, final
String domainName) {
       // Create a new request to check the domain status.
       final DescribeElasticsearchDomainRequest describeRequest = new
DescribeElasticsearchDomainRequest()
               .withDomainName(domainName);

       // Every 15 seconds, check whether the domain is processing.
       DescribeElasticsearchDomainResult describeResponse =
client.describeElasticsearchDomain(describeRequest);
       while (describeResponse.getDomainStatus().isProcessing()) {
           try {
               System.out.println("Domain still processing...");
               TimeUnit.SECONDS.sleep(15);
               describeResponse =
client.describeElasticsearchDomain(describeRequest);
           } catch (InterruptedException e) {
               e.printStackTrace();
           }
       }

       // Once we exit that loop, the domain is available
       System.out.println("Amazon OpenSearch Service has finished processing
changes for your domain.");
       System.out.println("Domain description response from Amazon OpenSearch
Service:");
       System.out.println(describeResponse.toString());
   }
```

```
}
```

Python

Este exemplo usa o cliente Python de baixo nível OpenSearchService do AWS SDK for Python (Boto) para criar um domínio, atualizar sua configuração e excluí-lo.

```
import boto3
import botocore
from botocore.config import Config
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a region other than your default.
    region_name='us-west-2'
)

client = boto3.client('opensearch', config=my_config)

domainName = 'my-test-domain'  # The name of the domain


def createDomain(client, domainName):
    """Creates an Amazon OpenSearch Service domain with the specified options."""
    response = client.create_domain(
        DomainName=domainName,
        EngineVersion='OpenSearch_1.0',
        ClusterConfig={
            'InstanceType': 't2.small.search',
            'InstanceCount': 5,
            'DedicatedMasterEnabled': True,
            'DedicatedMasterType': 't2.small.search',
            'DedicatedMasterCount': 3
        },
        # Many instance types require EBS storage.
        EBSOptions={
            'EBSEnabled': True,
            'VolumeType': 'gp2',
```

```
            'VolumeSize': 10
        },
        AccessPolicies="{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":
[\"es:*\"],\"Resource\":\"arn:aws:es:us-west-2:123456789012:domain/my-test-domain/*
\"}]}",
        NodeToNodeEncryptionOptions={
            'Enabled': True
        }
    )
    print("Creating domain...")
    print(response)


def updateDomain(client, domainName):
    """Updates the domain to use three data nodes instead of five."""
    try:
        response = client.update_domain_config(
            DomainName=domainName,
            ClusterConfig={
                'InstanceCount': 3
            }
        )
        print('Sending domain update request...')
        print(response)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
            print('Domain not found. Please check the domain name.')
        else:
            raise error


def deleteDomain(client, domainName):
    """Deletes an OpenSearch Service domain. Deleting a domain can take several
 minutes."""
    try:
        response = client.delete_domain(
            DomainName=domainName
        )
        print('Sending domain deletion request...')
        print(response)

    except botocore.exceptions.ClientError as error:
```

```
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
            print('Domain not found. Please check the domain name.')
        else:
            raise error


def waitForDomainProcessing(client, domainName):
    """Waits for the domain to finish processing changes."""
    try:
        response = client.describe_domain(
            DomainName=domainName
        )
        # Every 15 seconds, check whether the domain is processing.
        while response["DomainStatus"]["Processing"] == True:
            print('Domain still processing...')
            time.sleep(15)
            response = client.describe_domain(
                DomainName=domainName)

        # Once we exit the loop, the domain is available.
        print('Amazon OpenSearch Service has finished processing changes for your
 domain.')
        print('Domain description:')
        print(response)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
            print('Domain not found. Please check the domain name.')
        else:
            raise error


def main():
    """Create a new domain, update its configuration, and delete it."""
    createDomain(client, domainName)
    waitForDomainProcessing(client, domainName)
    updateDomain(client, domainName)
    waitForDomainProcessing(client, domainName)
    deleteDomain(client, domainName)
```

Nó

Este exemplo usa a versão 3 do cliente OpenSearch do SDK para JavaScript in Node.js para criar um domínio, atualizar sua configuração e excluí-lo.

```
var {
    OpenSearchClient,
    CreateDomainCommand,
    DescribeDomainCommand,
    UpdateDomainConfigCommand,
    DeleteDomainCommand
} = require("@aws-sdk/client-opensearch");
var sleep = require('sleep');

var client = new OpenSearchClient();

var domainName = 'my-test-domain'

// Create a new domain, update its configuration, and delete it.
createDomain(client, domainName)
waitForDomainProcessing(client, domainName)
updateDomain(client, domainName)
waitForDomainProcessing(client, domainName)
deleteDomain(client, domainName)

async function createDomain(client, domainName) {
    // Creates an Amazon OpenSearch Service domain with the specified options.
    var command = new CreateDomainCommand({
        DomainName: domainName,
        EngineVersion: 'OpenSearch_1.0',
        ClusterConfig: {
        'InstanceType': 't2.small.search',
        'InstanceCount': 5,
        'DedicatedMasterEnabled': 'True',
        'DedicatedMasterType': 't2.small.search',
        'DedicatedMasterCount': 3
        },
        EBSOptions:{
            'EBSEnabled': 'True',
            'VolumeType': 'gp2',
            'VolumeSize': 10
        },
```

```
        AccessPolicies: "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":
[\"es:*\"],\"Resource\":\"arn:aws:es:us-east-1:123456789012:domain/my-test-domain/*
\"}]}",
         NodeToNodeEncryptionOptions:{
            'Enabled': 'True'
        }
    });
    const response = await client.send(command);
    console.log("Creating domain...");
    console.log(response);
}

async function updateDomain(client, domainName) {
    // Updates the domain to use three data nodes instead of five.
    var command = new UpdateDomainConfigCommand({
        DomainName: domainName,
        ClusterConfig: {
        'InstanceCount': 3
        }
    });
    const response = await client.send(command);
    console.log('Sending domain update request...');
    console.log(response);
}

async function deleteDomain(client, domainName) {
    // Deletes an OpenSearch Service domain. Deleting a domain can take several
 minutes.
    var command = new DeleteDomainCommand({
        DomainName: domainName
    });
    const response = await client.send(command);
    console.log('Sending domain deletion request...');
    console.log(response);
}

async function waitForDomainProcessing(client, domainName) {
    // Waits for the domain to finish processing changes.
    try {
        var command = new DescribeDomainCommand({
            DomainName: domainName
        });
        var response = await client.send(command);
```

```
        while (response.DomainStatus.Processing == true) {
            console.log('Domain still processing...')
            await sleep(15000) // Wait for 15 seconds, then check the status again
            function sleep(ms) {
                return new Promise((resolve) => {
                    setTimeout(resolve, ms);
                });
            }
            var response = await client.send(command);
        }
        // Once we exit the loop, the domain is available.
        console.log('Amazon OpenSearch Service has finished processing changes for your
 domain.');
        console.log('Domain description:');
        console.log(response);

    } catch (error) {
        if (error.name === 'ResourceNotFoundException') {
            console.log('Domain not found. Please check the domain name.');
            }
    };
}
```

Indexação de dados no Amazon OpenSearch Service

Como o Amazon OpenSearch Service usa uma API REST, existem vários métodos para indexar documentos. Você pode usar os clientes padrão, como curl, ou qualquer linguagem de programação que possa enviar solicitações HTTP. Para simplificar ainda mais o processo de interação, o OpenSearch Service tem clientes para várias linguagens de programação. Os usuários avançados podem ir diretamente para the section called “Carregando dados de streaming no OpenSearch Serviço”.

É altamente recomendável que você use a Ingestão do Amazon OpenSearch para ingerir dados. Trata-se de um coletor de dados totalmente gerenciado criado dentro do OpenSearch Service. Para obter mais informações, consulte Ingestão do Amazon OpenSearch.

Para obter uma introdução à indexação, consulte a documentação OpenSearch.

Restrições de nomenclatura para índices

Os índices do OpenSearch Service têm as seguintes restrições de nomenclatura:

- Todas as letras devem estar em minúscula.
- Os nomes de índice não podem começar com `_` ou `-`.
- Os nomes de índice não podem conter espaços, vírgulas, `:`, `"`, `*`, `+`, `/`, `\`, `|`, `?`, `#`, `>` ou `<`.

Não inclua informações sigilosas nos nomes de índice, tipos ou IDs de documentos. O OpenSearch Service usa esses nomes em seus identificadores de recursos uniformes (URIs). Servidores e aplicativos geralmente registram solicitações de HTTP, o que poderá levar à exposição desnecessária de dados se os URIs contiverem informações confidenciais.

```
2018-10-03T23:39:43 198.51.100.14 200 "GET https://opensearch-domain/dr-jane-doe/flu-patients-2018/202-555-0100/ HTTP/1.1"
```

Mesmo se não tivesse permissões para visualizar o documento JSON associado, você poderia inferir por essa linha de log falsa que um dos pacientes do Dr. Doe cujo número de telefone é 202-555-0100 contraiu gripe em 2018.

Se o OpenSearch Service detectar um endereço IP real ou aparente em um nome de índice (por exemplo, `my-index-12.34.56.78.91`), ele vai mascarar o endereço IP. Uma chamada para `_cat/indices` produz a seguinte resposta:

```
green open my-index-x.x.x.x.91    soY19tBERoKo71WcEScidw 5 1 0 0   2kb  1kb
```

Para evitar confusões desnecessárias, evite incluir endereços IP em nomes de índices.

Redução do tamanho da resposta

As respostas das APIs `_index` e `_bulk` contêm um pouco de informações. Essas informações podem ser úteis para solução de problemas de solicitações ou para implementar a lógica de tentativas repetidas, mas pode usar consideravelmente a banda larga. Neste exemplo, indexar um documento de 32 bytes resulta em uma resposta de 339 bytes (incluindo cabeçalhos):

```
PUT opensearch-domain/more-movies/_doc/1
{"title": "Back to the Future"}
```

Resposta

```
{
  "_index": "more-movies",
  "_type": "_doc",
  "_id": "1",
  "_version": 4,
  "result": "updated",
  "_shards": {
    "total": 2,
    "successful": 2,
    "failed": 0
  },
  "_seq_no": 3,
  "_primary_term": 1
}
```

Esse tamanho de resposta pode parecer insignificante, mas se você indexar 1.000.000 documentos por dia — aproximadamente 11,5 documentos por segundo —, 339 bytes por resposta representam 10,17 GB de tráfego de download por mês.

Se os custos de transferência de dados forem uma preocupação, use o parâmetro `filter_path` para reduzir o tamanho da resposta do OpenSearch Service, mas tenha cuidado para não filtrar campos que você precisa para identificar ou realizar novas tentativas de solicitações com falha. Esses campos variam de acordo com o cliente. O parâmetro `filter_path` funciona para todas as APIs REST do OpenSearch Service, mas é especialmente útil com APIs que você chama com frequência, como as APIs `_index` e `_bulk`:

```
PUT opensearch-domain/more-movies/_doc/1?filter_path=result,_shards.total
{"title": "Back to the Future"}
```

Resposta

```
{
  "result": "updated",
  "_shards": {
    "total": 2
  }
}
```

Em vez de incluir campos, você pode excluir campos com um prefixo `-`. `filter_path` também oferece suporte a curingas:

```
POST opensearch-domain/_bulk?filter_path=-took,-items.index._*
{ "index": { "_index": "more-movies", "_id": "1" } }
{"title": "Back to the Future"}
{ "index": { "_index": "more-movies", "_id": "2" } }
{"title": "Spirited Away"}
```

Resposta

```
{
  "errors": false,
  "items": [
    {
      "index": {
        "result": "updated",
        "status": 200
      }
    },
    {
```

```
      "index": {
        "result": "updated",
        "status": 200
      }
    }
  ]
}
```

Codecs de índice

Os codecs de índice determinam como os campos armazenados em um índice são compactados e armazenados no disco. O codec de índice é controlado pela configuração estática `index.codec`, que especifica o algoritmo de compactação. Essa configuração afeta o tamanho do fragmento de índice e o desempenho da operação.

Para obter uma lista dos codecs compatíveis e suas características de desempenho, consulte Codecs suportados na documentação do OpenSearch.

Ao escolher um codec de índice, considere o seguinte:

- Para evitar os desafios de alterar a configuração do codec de um índice existente, teste uma workload representativa em um ambiente que não seja de produção antes de usar uma nova configuração de codec. Para mais informações, consulte Alterar um codec de índice.
- Você não pode usar os codecs de compressão `zstd` e `zstd_no_dict` para índices k-NN ou Security Analytics.
- A migração para instâncias UltraWarm está desativada para índices zStandard.

Carregando dados de streaming no Amazon OpenSearch Service

Você pode usar o OpenSearch Inestion para carregar diretamente dados de streaming em seu domínio do Amazon OpenSearch Service, sem precisar usar soluções de terceiros. Para enviar dados para o OpenSearch Ingestion, você configura seus produtores de dados e o serviço entrega automaticamente os dados ao domínio ou à coleção que você especificar. Para começar a usar o OpenSearch Ingestion, consultethe section called “Tutorial: Ingestão de dados em uma coleção”.

Você ainda pode usar outras fontes para carregar dados de streaming, como Amazon Data Firehose e Amazon CloudWatch Logs, que têm suporte integrado para OpenSearch o Service. Outras, como Amazon S3, Amazon Kinesis Data Streams e Amazon DynamoDB, usam funções do AWS Lambda

como manipuladores de eventos. As funções do Lambda respondem a novos dados processando e transmitindo-os para seu domínio.

> **Note**
>
> O Lambda oferece suporte a várias linguagens de programação populares e está disponível na maioria das Regiões da AWS. Para obter mais informações, consulte Conceitos básicos do Lambda na AWS Lambda Guia do desenvolvedor e AWS Endpoints de serviço na Referência geral da AWS.

Tópicos

Carregando dados de streaming do OpenSearch Ingestion

Você pode usar o Amazon OpenSearch Ingestion para carregar dados em um domínio OpenSearch de serviço. Você configura seus produtores de dados para enviar dados para OpenSearch Ingestão, e ele entrega automaticamente os dados para a coleção que você especificar. Você também pode configurar a OpenSearch ingestão para transformar seus dados antes de entregá-los. Para ter mais informações, consulte OpenSearch Ingestão da Amazon.

Carregamento de dados de transmissão do Amazon S3

Você pode usar o Lambda para enviar dados para seu domínio de OpenSearch serviço do Amazon S3. Os novos dados recebidos em um bucket do S3 acionam uma notificação de evento para o Lambda, que executa seu código personalizado para realizar a indexação.

Esse método de streaming de dados é extremamente flexível. Você pode indexar metadados de objeto, ou se o objeto for texto simples, analisar e indexar alguns elementos do corpo do objeto.

Esta seção inclui alguns códigos de exemplo Python simples que usam expressões regulares para analisar um arquivo de log e indexar as correspondências.

Pré-requisitos

Para continuar, você deve ter os recursos a seguir.

Pré-requisito	Descrição
Bucket do Amazon S3.	Para obter mais informações, consulte Criar seu primeiro bucket do S3 no Manual do usuário do Amazon Simple Storage Service. O bucket deve residir na mesma região do seu domínio OpenSearch de serviço.
OpenSearch Domínio do serviço	O destino dos dados depois que a função do Lambda os processa. Para ter mais informações, consulte the section called “ Criação OpenSearch de domínios de serviço”.

Criar o pacote de implantação do Lambda

Os pacotes de implantação são arquivos ZIP ou JAR que contêm o código e as dependências. Esta seção inclui código de exemplo Python. Para outras linguagens de programação, consulte Pacotes de implantação do Lambda no Guia do desenvolvedor doAWS Lambda .

1. Crie um diretório. Neste exemplo, usamos o nome `s3-to-opensearch`.
2. Crie um arquivo no diretório chamado `sample.py`:

```
import boto3
import re
import requests
from requests_aws4auth import AWS4Auth

region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

host = '' # the OpenSearch Service domain, e.g. https://search-mydomain.us-
west-1.es.amazonaws.com
index = 'lambda-s3-index'
```

```
datatype = '_doc'
url = host + '/' + index + '/' + datatype

headers = { "Content-Type": "application/json" }

s3 = boto3.client('s3')

# Regular expressions used to parse some simple log lines
ip_pattern = re.compile('(\d+\.\d+\.\d+\.\d+)')
time_pattern = re.compile('\[(\d+\/\w\w\w\/\d\d\d\d:\d\d:\d\d:\d\d\s-\d\d\d\d)\]')
message_pattern = re.compile('\"(.+)\"')

# Lambda execution starts here
def handler(event, context):
    for record in event['Records']:

        # Get the bucket name and key for the new file
        bucket = record['s3']['bucket']['name']
        key = record['s3']['object']['key']

        # Get, read, and split the file into lines
        obj = s3.get_object(Bucket=bucket, Key=key)
        body = obj['Body'].read()
        lines = body.splitlines()

        # Match the regular expressions to each line and index the JSON
        for line in lines:
            line = line.decode("utf-8")
            ip = ip_pattern.search(line).group(1)
            timestamp = time_pattern.search(line).group(1)
            message = message_pattern.search(line).group(1)

            document = { "ip": ip, "timestamp": timestamp, "message": message }
            r = requests.post(url, auth=awsauth, json=document, headers=headers)
```

Edite as variáveis de `region` e `host`.

3. Se ainda não o fez, instale o pip. Em seguida, instale as dependências em um novo diretório `package`:

```
cd s3-to-opensearch

pip install --target ./package requests
```

```
pip install --target ./package requests_aws4auth
```

Como todos os ambientes de execução do Lambda têm o Boto3 instalado, você não precisa incluí-lo no pacote de implantação.

4. Empacote o código do aplicativo e as dependências:

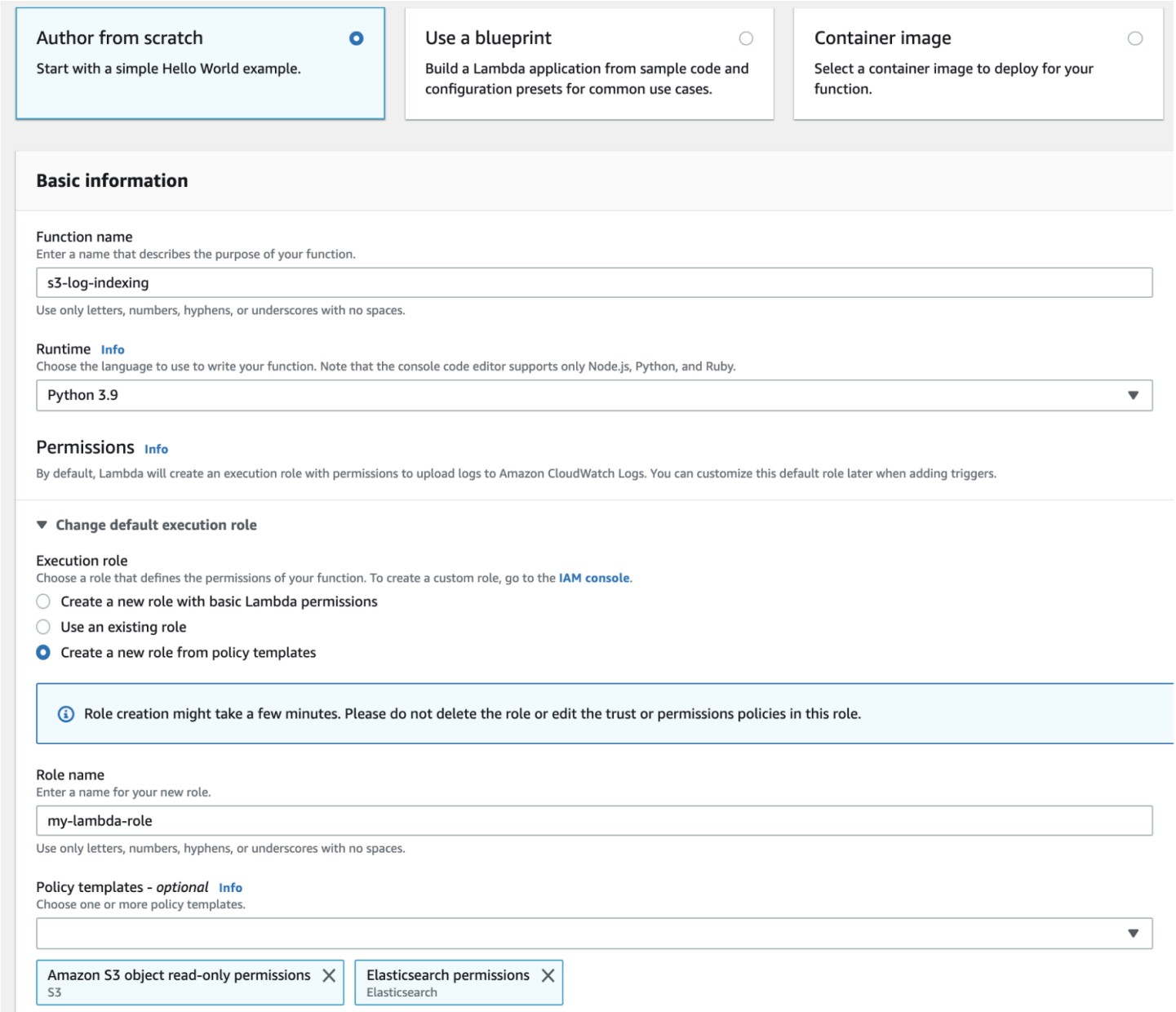
```
cd package
zip -r ../lambda.zip .

cd ..
zip -g lambda.zip sample.py
```

Criar a função do Lambda

Depois de criar o pacote de implantação, você poderá criar a função do Lambda. Ao criar uma função, escolha um nome, o tempo de execução (por exemplo, Python 3.8) e a função do IAM. A função do IAM define as permissões para a função. Para obter instruções detalhadas, consulte Criar uma função Lambda com o console no Guia do desenvolvedor doAWS Lambda .

Esse exemplo pressupõe que você está usando o console. Escolha Python 3.9 e uma função que tenha permissões de leitura do S3 e permissões de gravação do OpenSearch Serviço, conforme mostrado na captura de tela a seguir:



Depois de criar a função, você deverá adicionar um gatilho. Neste exemplo, queremos que o código seja executado sempre que um arquivo de log chegue em um bucket do S3:

1. Escolha Adicionar acionador e selecione S3.
2. Escolha o bucket.
3. Em Tipo de evento, selecione PUT.
4. Em Prefixo, digite `logs/`.
5. Em Sufixo, digite `.log`.
6. Confirme o aviso de invocação recursiva e escolha Adicionar.

Por fim, você pode carregar o pacote de implantação:

1. Escolha Carregar de e arquivo .zip e siga os avisos para carregar do pacote de implantação.
2. Depois que o carregamento terminar, edite as Configurações do tempo de execução e altere o Manipulador para `sample.handler`. Essa configuração informa ao Lambda o arquivo (`sample.py`) e o método (`handler`) que deverão ser executados depois de um acionador.

Nesse ponto, você tem um conjunto completo de recursos: um bucket para arquivos de log, uma função que é executada sempre que um arquivo de log é adicionado ao bucket, código que executa a análise e a indexação e um domínio de OpenSearch serviço para pesquisa e visualização.

Teste da função do Lambda

Após criar a função, você poderá testá-la carregando de um arquivo no bucket do Amazon S3. Crie um arquivo chamado `sample.log` usando as seguintes linhas de log de exemplo:

```
12.345.678.90 - [10/Oct/2000:13:55:36 -0700] "PUT /some-file.jpg"
12.345.678.91 - [10/Oct/2000:14:56:14 -0700] "GET /some-file.jpg"
```

Carregue o arquivo na pasta `logs` do bucket do S3. Para obter instruções, consulte Carregar um objeto para o seu bucket no Manual do usuário do Amazon Simple Storage Service.

Em seguida, use o console de OpenSearch serviço ou os OpenSearch painéis para verificar se o `lambda-s3-index` índice contém dois documentos. Você também pode fazer uma solicitação de pesquisa padrão:

```
GET https://domain-name/lambda-s3-index/_search?pretty
{
  "hits" : {
    "total" : 2,
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "lambda-s3-index",
        "_type" : "_doc",
        "_id" : "vTYXaWIBJWV_TTkEuSDg",
        "_score" : 1.0,
        "_source" : {
          "ip" : "12.345.678.91",
          "message" : "GET /some-file.jpg",
```

```
          "timestamp" : "10/Oct/2000:14:56:14 -0700"
        }
      },
      {
        "_index" : "lambda-s3-index",
        "_type" : "_doc",
        "_id" : "vjYmaWIBJWV_TTkEuCAB",
        "_score" : 1.0,
        "_source" : {
          "ip" : "12.345.678.90",
          "message" : "PUT /some-file.jpg",
          "timestamp" : "10/Oct/2000:13:55:36 -0700"
        }
      }
    ]
  }
}
```

Carregamento dados de transmissão do Amazon Kinesis Data Streams

Você pode carregar dados de streaming do Kinesis Data OpenSearch Streams para o Service. Os novos dados recebidos no fluxo de dados acionam uma notificação de evento para o Lambda, o qual executa seu código personalizado para realizar a indexação. Esta seção inclui um código de exemplo Python simples.

Pré-requisitos

Para continuar, você deve ter os recursos a seguir.

Pré-requisito	Descrição
Amazon Kinesis Data Streams	A fonte do evento para a função do Lambda. Para saber mais, consulte Kinesis Data Streams.
OpenSearch Domínio do serviço	O destino dos dados depois que a função do Lambda os processa. Para obter mais informações, consulte the section called “ Criação OpenSearch de domínios de serviço”.
Perfil do IAM	Essa função deve ter permissões básicas OpenSearch de Service, Kinesis e Lambda, como as seguintes:

Pré-requisito	Descrição

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "es:ESHttpPost",
        "es:ESHttpPut",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "kinesis:GetShardIterator",
        "kinesis:GetRecords",
        "kinesis:DescribeStream",
        "kinesis:ListStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

A função deve ter a seguinte relação de confiança:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Para saber mais, consulte Criação de funções do IAM no Manual do usuário do IAM.

Criar a função do Lambda

Siga as instruções no the section called “Criar o pacote de implantação do Lambda”, mas crie um diretório chamado `kinesis-to-opensearch` e use o seguinte código para `sample.py`:

```
import base64
import boto3
import json
import requests
from requests_aws4auth import AWS4Auth

region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

host = '' # the OpenSearch Service domain, e.g. https://search-mydomain.us-
west-1.es.amazonaws.com
index = 'lambda-kine-index'
datatype = '_doc'
url = host + '/' + index + '/' + datatype + '/'

headers = { "Content-Type": "application/json" }

def handler(event, context):
    count = 0
    for record in event['Records']:
        id = record['eventID']
        timestamp = record['kinesis']['approximateArrivalTimestamp']

        # Kinesis data is base64-encoded, so decode here
        message = base64.b64decode(record['kinesis']['data'])

        # Create the JSON document
        document = { "id": id, "timestamp": timestamp, "message": message }
        # Index the document
        r = requests.put(url + id, auth=awsauth, json=document, headers=headers)
        count += 1
    return 'Processed ' + str(count) + ' items.'
```

Edite as variáveis de `region` e `host`.

Caso ainda não tenha feito, instale o pip. Em seguida, use os seguintes comandos para instalar as dependências:

```
cd kinesis-to-opensearch

pip install --target ./package requests
pip install --target ./package requests_aws4auth
```

Depois siga as instruções em the section called “Criar a função do Lambda”, mas especifique a função do IAM por the section called “Pré-requisitos” e as seguintes configurações do gatilho:

- Fluxo do Kinesis: o fluxo do Kinesis
- Tamanho do lote: 100
- Posição inicial: redução horizontal

Para saber mais, consulte O que é o Amazon Kinesis Data Streams? no Guia do desenvolvedor do Amazon Kinesis Data Streams.

Nesse ponto, você tem um conjunto completo de recursos: um stream de dados do Kinesis, uma função que é executada depois que o stream recebe novos dados e indexa esses dados, e um domínio de OpenSearch serviço para pesquisa e visualização.

Testar a função do Lambda

Depois de criar a função, você poderá testá-la adicionando um novo registro ao streaming de dados usando a AWS CLI:

```
aws kinesis put-record --stream-name test --data "My test data." --partition-key
 partitionKey1 --region us-west-1
```

Em seguida, use o console de OpenSearch serviço ou os OpenSearch painéis para verificar se `lambda-kine-index` contém um documento. Você também pode usar a seguinte solicitação:

```
GET https://domain-name/lambda-kine-index/_search
{
  "hits" : [
    {
      "_index": "lambda-kine-index",
      "_type": "_doc",
```

```
      "_id":
 "shardId-000000000000:495835116157626994950129608214214566865294366804960870 42",
      "_score": 1,
      "_source": {
        "timestamp": 1523648740.051,
        "message": "My test data.",
        "id":
 "shardId-000000000000:495835116157626994950129608214214566865294366804960870 42"
      }
    }
  ]
}
```

Carregamento de dados de transmissão do Amazon DynamoDB

Você pode usar AWS Lambda para enviar dados para seu domínio de OpenSearch serviço do Amazon DynamoDB. Os novos dados recebidos na tabela do banco de dados acionam uma notificação de evento para o Lambda, que executa seu código personalizado para realizar a indexação.

Pré-requisitos

Para continuar, você deve ter os recursos a seguir.

Pré-requisito	Descrição
Tabela do DynamoDB	A tabela contém os dados de origem. Para obter mais informações, consulte Operações básicas nas tabelas do DynamoDB no Guia do desenvolvedor do Amazon DynamoDB. A tabela deve residir na mesma região do seu domínio OpenSearch de serviço e ter um stream definido como Nova imagem. Para saber mais, consulte Como habilitar um stream.
OpenSearch Domínio do serviço	O destino dos dados depois que a função do Lambda os processa. Para ter mais informações, consulte the section called “ Criação OpenSearch de domínios de serviço”.
IAM role (Perfil do IAM)	Essa função deve ter permissões básicas OpenSearch de execução de Service, DynamoDB e Lambda, como as seguintes:

Pré-requisito	Descrição

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "es:ESHttpPost",
        "es:ESHttpPut",
        "dynamodb:DescribeStream",
        "dynamodb:GetRecords",
        "dynamodb:GetShardIterator",
        "dynamodb:ListStreams",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

A função deve ter a seguinte relação de confiança:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Para saber mais, consulte Criação de funções do IAM no Manual do usuário do IAM.

Criar a função do Lambda

Siga as instruções no the section called “Criar o pacote de implantação do Lambda”, mas crie um diretório chamado `ddb-to-opensearch` e use o seguinte código para `sample.py`:

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

region = '' # e.g. us-east-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

host = '' # the OpenSearch Service domain, e.g. https://search-mydomain.us-
west-1.es.amazonaws.com
index = 'lambda-index'
datatype = '_doc'
url = host + '/' + index + '/' + datatype + '/'

headers = { "Content-Type": "application/json" }

def handler(event, context):
    count = 0
    for record in event['Records']:
        # Get the primary key for use as the OpenSearch ID
        id = record['dynamodb']['Keys']['id']['S']

        if record['eventName'] == 'REMOVE':
            r = requests.delete(url + id, auth=awsauth)
        else:
            document = record['dynamodb']['NewImage']
            r = requests.put(url + id, auth=awsauth, json=document, headers=headers)
        count += 1
    return str(count) + ' records processed.'
```

Edite as variáveis de `region` e `host`.

Caso ainda não tenha feito, instale o pip. Em seguida, use os seguintes comandos para instalar as dependências:

```
cd ddb-to-opensearch
```

```
pip install --target ./package requests
pip install --target ./package requests_aws4auth
```

Depois siga as instruções em the section called “Criar a função do Lambda”, mas especifique a função do IAM por the section called “Pré-requisitos” e as seguintes configurações do gatilho:

- Tabela: a tabela do DynamoDB
- Tamanho do lote: 100
- Posição inicial: redução horizontal

Para saber mais, consulte Processar novos itens com o DynamoDB Streams e o Lambda no Guia do desenvolvedor do Amazon DynamoDB.

Neste momento, você tem um conjunto completo de recursos: uma tabela do DynamoDB para seus dados de origem, um stream de alterações na tabela do DynamoDB, uma função que é executada após a alteração dos dados de origem e indexa essas alterações e um domínio de serviço para pesquisa e visualização. OpenSearch

Testar a função do Lambda

Depois de criar a função, você poderá testá-la adicionando um novo item à tabela do DynamoDB usando a AWS CLI:

```
aws dynamodb put-item --table-name test --item '{"director": {"S": "Kevin
 Costner"},"id": {"S": "00001"},"title": {"S": "The Postman"}}' --region us-west-1
```

Em seguida, use o console de OpenSearch serviço ou os OpenSearch painéis para verificar se `lambda-index` contém um documento. Você também pode usar a seguinte solicitação:

```
GET https://domain-name/lambda-index/_doc/00001
{
    "_index": "lambda-index",
    "_type": "_doc",
    "_id": "00001",
    "_version": 1,
    "found": true,
    "_source": {
        "director": {
```

```
            "S": "Kevin Costner"
        },
        "id": {
            "S": "00001"
        },
        "title": {
            "S": "The Postman"
        }
    }
}
```

Carregamento de dados de streaming do Amazon Data Firehose

O Firehose oferece suporte OpenSearch ao serviço como destino de entrega. Para obter instruções sobre como carregar dados de streaming no OpenSearch Serviço, consulte Criação de um stream de entrega do Kinesis Data Firehose OpenSearch e Escolha o serviço para seu destino no Guia do desenvolvedor do Amazon Data Firehose.

Antes de carregar dados no OpenSearch Serviço, talvez seja necessário realizar transformações nos dados. Para saber mais sobre como usar funções do Lambda para executar essa tarefa, consulte Transformação de dados do Amazon Kinesis Data Firehose no mesmo guia.

Ao configurar um stream de entrega, o Firehose apresenta uma função IAM de “um clique” que fornece o acesso aos recursos necessários para enviar dados ao OpenSearch Serviço, fazer backup de dados no Amazon S3 e transformar dados usando o Lambda. Em virtude da complexidade envolvida na criação manual de uma função como essa, é recomendável usar a função fornecida.

Carregando dados de streaming da Amazon CloudWatch

Você pode carregar dados de streaming do CloudWatch Logs para seu domínio do OpenSearch Serviço usando uma assinatura do CloudWatch Logs. Para obter informações sobre as CloudWatch assinaturas da Amazon, consulte Processamento em tempo real de dados de log com assinaturas. Para obter informações de configuração, consulte Streaming de dados de CloudWatch registros para o Amazon OpenSearch Service no Amazon CloudWatch Developer Guide.

Carregamento de dados de transmissão do AWS IoT

Você pode enviar dados AWS IoT usando regras. Para saber mais, consulte a OpenSearchação no Guia doAWS IoT desenvolvedor.

Carregamento de dados no Amazon OpenSearch Service com o Logstash

A versão de código aberto do Logstash (Logstash OSS) fornece uma maneira conveniente de usar a API em massa para carregar dados em seu domínio do Amazon OpenSearch Service. O serviço oferece suporte a todos os plugins de entrada padrão do Logstash, incluindo o plugin de entrada do Amazon S3. O OpenSearch Service oferece suporte ao plugin de saída logstash-output-opensearch, que é compatível com a autenticação básica e as credenciais do IAM. O plugin funciona com a versão 8.1 e inferior do Logstash OSS.

Configuração

A configuração do Logstash varia de acordo com o tipo de autenticação utilizada pelo seu domínio.

Não importa que método de autenticação você use, é necessário definir `ecs_compatibility`como `disabled` na seção de saída do arquivo de configuração. O Logstash 8.0 introduziu uma mudança revolucionária em que todos os plugins são executados no modo de compatibilidade com ECS por padrão. Você deve substituir o valor padrão para manter o comportamento herdado.

Configuração do controle de acesso refinado

Se seu domínio do OpenSearch Service usa o controle de acesso refinado com autenticação básica HTTP, a configuração é semelhante a qualquer outro cluster do OpenSearch. Este arquivo de configuração de exemplo obtém a entrada da versão de código aberto do Filebeat (Filebeat OSS):

```
input {
  beats  {
    port => 5044
  }
}

output {
  opensearch {
    hosts       => "https://domain-endpoint:443"
    user        => "my-username"
    password    => "my-password"
    index       => "logstash-logs-%{+YYYY.MM.dd}"
    ecs_compatibility => disabled
    ssl_certificate_verification => false
```

```
  }
}
```

A configuração varia de acordo com a aplicações Beats e o caso de uso, mas sua configuração do Filebeat OSS pode ser semelhante a esta:

```
filebeat.inputs:
- type: log
  enabled: true
  paths:
    - /path/to/logs/dir/*.log
filebeat.config.modules:
  path: ${path.config}/modules.d/*.yml
  reload.enabled: false
setup.ilm.enabled: false
setup.ilm.check_exists: false
setup.template.settings:
  index.number_of_shards: 1
output.logstash:
  hosts: ["logstash-host:5044"]
```

Configuração do IAM

Se seu domínio usa uma política de acesso a domínio baseada no IAM ou um controle de acesso refinado com um usuário mestre, é necessário assinar todas as solicitações para o OpenSearch Service usando credenciais do IAM. A política baseada em identidade a seguir concede todas as solicitações HTTP para os sub-recursos do seu domínio.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:aws-account-id:domain/domain-name/*"
    }
  ]
}
```

Para configurar o Logstash, altere o seu arquivo de configuração para usar o plug-in para a saída. Este arquivo de configuração de exemplo obtém a entrada de arquivos em um bucket do S3:

```
input {
  s3 {
    bucket => "my-s3-bucket"
    region => "us-east-1"
  }
}

output {
  opensearch {
    hosts => ["domain-endpoint:443"]
    auth_type => {
      type => 'aws_iam'
      aws_access_key_id => 'your-access-key'
      aws_secret_access_key => 'your-secret-key'
      region => 'us-east-1'
      }
      index  => "logstash-logs-%{+YYYY.MM.dd}"
      ecs_compatibility => disabled
  }
}
```

Se você não quiser fornecer as suas credenciais do IAM no arquivo de configuração, poderá exportá-las (ou executar o `aws configure`):

```
export AWS_ACCESS_KEY_ID="your-access-key"
export AWS_SECRET_ACCESS_KEY="your-secret-key"
export AWS_SESSION_TOKEN="your-session-token"
```

Se seu domínio do OpenSearch Service estiver em uma VPC, a máquina do Logstash OSS deverá poder se conectar à VPC e ter acesso ao domínio via grupos de segurança da VPC. Para obter mais informações, consulte the section called “Sobre políticas de acesso em domínios da VPC”.

Pesquisa de dados no Amazon OpenSearch Service

Existem vários métodos comuns para pesquisa de documentos no Amazon OpenSearch Service, incluindo pesquisas de URI e pesquisas de corpo da solicitação. O OpenSearch Service oferece funcionalidade adicional que melhora a experiência de pesquisa, como pacotes personalizados, suporte a SQL e pesquisa assíncrona. Para obter uma referência abrangente da API de pesquisa do OpenSearch, consulte a documentação do OpenSearch.

> **Note**
>
> As solicitações de exemplo a seguir funcionam com APIs do OpenSearch. Algumas solicitações podem não funcionar com versões mais antigas do Elasticsearch.

Tópicos

Pesquisas de URI

As pesquisas do URI (Universal Resource Identifier, Identificador de recurso universal) são a forma mais simples de pesquisa. Em uma pesquisa do URI, você especifica a consulta como um parâmetro de solicitação HTTP.

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/_search?q=house
```

Uma resposta de exemplo pode ser a seguinte:

```
{
  "took": 25,
  "timed_out": false,
  "_shards": {
    "total": 10,
    "successful": 10,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": {
      "value": 85,
      "relation": "eq",
    },
    "max_score": 6.6137657,
    "hits": [
      {
        "_index": "movies",
        "_type": "movie",
        "_id": "tt0077975",
        "_score": 6.6137657,
        "_source": {
          "directors": [
            "John Landis"
          ],
          "release_date": "1978-07-27T00:00:00Z",
          "rating": 7.5,
          "genres": [
            "Comedy",
            "Romance"
          ],
          "image_url": "http://ia.media-imdb.com/images/M/
MV5BMTY2OTQxNTc1OF5BMl5BanBnXkFtZTYwNjA3NjI5._V1_SX400_.jpg",
          "plot": "At a 1962 College, Dean Vernon Wormer is determined to expel the
 entire Delta Tau Chi Fraternity, but those troublemakers have other plans for him.",
          "title": "Animal House",
          "rank": 527,
          "running_time_secs": 6540,
          "actors": [
```

```
            "John Belushi",
            "Karen Allen",
            "Tom Hulce"
          ],
          "year": 1978,
          "id": "tt0077975"
        }
      },
      ...
    ]
  }
}
```

Por padrão, essa consulta pesquisa todos os campos de todos os índices do termo casa. Para restringir a pesquisa, especifique um índice (`movies`) e um campo de documento (`title`) no URI:

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search?q=title:house
```

Você pode incluir parâmetros adicionais na solicitação, mas os parâmetros compatíveis fornecem apenas um pequeno subconjunto das opções de pesquisa do OpenSearch. A solicitação a seguir retorna 20 resultados (em vez do padrão de 10) e classifica por ano (em vez de por `_score`):

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search?
q=title:house&size=20&sort=year:desc
```

Pesquisas de corpo da solicitação

Para realizar pesquisas mais complexas, use o corpo da solicitação HTTP e o idioma específico do domínio (DSL) do OpenSearch para realizar consultas. A consulta DSL permite especificar a gama completa de opções de pesquisa do OpenSearch.

> **Note**
>
> Você não pode incluir caracteres especiais Unicode em um valor de campo de texto, ou o valor será analisado como vários valores separados pelo caractere especial. Essa análise incorreta pode levar à filtragem não intencional de documentos e potencialmente comprometer o controle sobre seu acesso. Para obter mais informações, consulte Uma nota sobre caracteres especiais Unicode em campos de texto na documentação do OpenSearch.

A consulta `match` a seguir é semelhante ao exemplo de pesquisa final do URI:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "sort": {
    "year": {
      "order": "desc"
    }
  },
  "query": {
    "query_string": {
      "default_field": "title",
      "query": "house"
    }
  }
}
```

> **Note**
>
> A API `_search` aceita HTTP`GET` e `POST` para pesquisas de corpo de solicitação, mas nem todos os clientes HTTP suportam a adição de um corpo de solicitação a uma solicitação `GET`. `POST` é a escolha mais universal.

Em muitos casos, você pode pesquisar vários campos, mas não todos os campos. Use a consulta `multi_match`:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title", "plot", "actors", "directors"]
    }
  }
}
```

Impulsão de campos

Você pode melhorar a relevância de pesquisa "aumentando" determinados campos. Boosts são multiplicadores que ponderam os resultados em um campo maior do que os correspondentes em outros campos. No exemplo a seguir, uma correspondência para john no campo `title` influencia `_score` duas vezes mais que uma correspondência no campo `plot` e quatro vezes mais que uma correspondência nos campos `actors` ou `directors`. O resultado é que filmes como John Wick e John Carter estão próximos do topo dos resultados de busca, e filmes estrelados por John Travolta estão quase no fim.

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "john",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  }
}
```

Destaques de resultados da pesquisa

A opção `highlight` informa ao OpenSearch para retornar um objeto adicional dentro da matriz `hits` se a consulta corresponder a um ou mais campos:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  },
  "highlight": {
    "fields": {
      "plot": {}
    }
  }
}
```

Se a consulta corresponder ao conteúdo do campo `plot`, um resultado pode ser semelhante ao seguinte:

```
{
  "_index": "movies",
  "_type": "movie",
  "_id": "tt0091541",
  "_score": 11.276199,
  "_source": {
    "directors": [
      "Richard Benjamin"
    ],
    "release_date": "1986-03-26T00:00:00Z",
    "rating": 6,
    "genres": [
      "Comedy",
      "Music"
    ],
    "image_url": "http://ia.media-imdb.com/images/M/
MV5BMTIzODEzODE2OF5BMl5BanBnXkFtZTcwNjQ3ODcyMQ@@._V1_SX400_.jpg",
    "plot": "A young couple struggles to repair a hopelessly dilapidated house.",
    "title": "The Money Pit",
    "rank": 4095,
    "running_time_secs": 5460,
    "actors": [
      "Tom Hanks",
      "Shelley Long",
      "Alexander Godunov"
    ],
    "year": 1986,
    "id": "tt0091541"
  },
  "highlight": {
    "plot": [
      "A young couple struggles to repair a hopelessly dilapidated <em>house</em>."
    ]
  }
}
```

Por padrão, o OpenSearch agrupa a string correspondente em tags , fornece até 100 caracteres de contexto da correspondência e divide o conteúdo em sentenças, identificando

sinais de pontuação, espaços, tabulações e quebras de linha. Todas estas configurações são personalizáveis:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  },
  "highlight": {
    "fields": {
      "plot": {}
    },
    "pre_tags": "<strong>",
    "post_tags": "</strong>",
    "fragment_size": 200,
    "boundary_chars": ".,!? "
  }
}
```

API de contagem

Se você não estiver interessado no conteúdo de seus documentos e quiser apenas saber o número de correspondências, poderá usar a API `_count` em vez da API `_search`. A solicitação a seguir usa a consulta `query_string` para identificar comédias românticas:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_count
{
  "query": {
    "query_string": {
      "default_field": "genres",
      "query": "romance AND comedy"
    }
  }
}
```

Uma resposta de exemplo pode ser a seguinte:

```
{
```

```
  "count": 564,
  "_shards": {
    "total": 5,
    "successful": 5,
    "skipped": 0,
    "failed": 0
  }
}
```

Paginação de resultados da pesquisa

Se precisar exibir um grande número de resultados de pesquisa, você poderá implementar a paginação usando vários métodos diferentes.

Ponto de tempo

O atributo point in time (PIT – um ponto no tempo) é um tipo de pesquisa que permite executar consultas diferentes em um conjunto de dados fixo no tempo. Esse é o método de paginação preferido no OpenSearch, especialmente para paginação profunda. Você pode usar o PIT com o OpenSearch Service versão 2.5 e posterior. Para ter mais informações sobre o PIT, consulte ???.

Os parâmetros **`from`** e **`size`**.

A maneira mais simples de paginar é com os parâmetros `from` e `size`. A seguinte solicitação retorna resultados de 20 a 39 da lista indexada zero de resultados da pesquisa:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "from": 20,
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  }
}
```

Para obter mais informações sobre paginação de pesquisa, consulte Resultados de paginação na documentação do OpenSearch.

Dashboards Query Language

É possível usar a Dashboards Query Language (DQL) para pesquisar dados e visualizações no OpenSearch Dashboaords. A DQL usa quatro tipos de consulta principais:termos, boleana, data e intervalo e campo aninhado.

Consulta de termos

Uma consulta de termos exige que você especifique o termo que está procurando.

Para executar uma consulta de termos, insira o seguinte:

```
host:www.example.com
```

Consulta booleana

É possível usar os operadores booleanos `AND`, `or` e `not` para combinar várias consultas.

Para executar uma consulta booleana, cole o seguinte:

```
host.keyword:www.example.com and response.keyword:200
```

Consulta de data e intervalo

Você pode usar uma consulta de data e intervalo para encontrar uma data antes ou depois da consulta.

- > indica uma pesquisa por uma data posterior à data especificada.
- < indica uma pesquisa por uma data anterior à data especificada.

```
@timestamp > "2020-12-14T09:35:33"
```

Consulta de campo aninhado

Se você tiver um documento com campos aninhados, será necessário especificar quais partes do documento você deseja recuperar. Veja a seguir um exemplo de documento que contém campos aninhados:

```
{"NBA players":[
    {"player-name": "Lebron James",
      "player-position": "Power forward",
```

```
      "points-per-game": "30.3"
    },
    {"player-name": "Kevin Durant",
      "player-position": "Power forward",
      "points-per-game": "27.1"
    },
    {"player-name": "Anthony Davis",
      "player-position": "Power forward",
      "points-per-game": "23.2"
    },
    {"player-name": "Giannis Antetokounmpo",
      "player-position": "Power forward",
      "points-per-game":"29.9"
    }
  ]
}
```

Para recuperar um campo específico usando DQL, cole o seguinte:

```
NBA players: {player-name: Lebron James}
```

Para recuperar vários objetos do documento aninhado, cole o seguinte:

```
NBA players: {player-name: Lebron James} and NBA players: {player-name: Giannis
 Antetokounmpo}
```

Para pesquisar em um intervalo, cole o seguinte:

```
NBA players: {player-name: Lebron James} and NBA players: {player-name: Giannis
 Antetokounmpo and < 30}
```

Se o documento tiver um objeto aninhado em outro objeto, você ainda poderá recuperar dados especificando todos os níveis. Para fazer isso, cole o seguinte:

```
Top-Power-forwards.NBA players: {player-name:Lebron James}
```

Pacotes personalizados para Amazon OpenSearch Service

O Amazon OpenSearch Service permite que você faça upload de arquivos de dicionário personalizados, como palavras irrelevantes e sinônimos, e também fornece vários plug-ins opcionais

pré-empacotados que você pode associar ao seu domínio. O termo genérico para esses dois tipos de arquivos é pacotes.

Os arquivos de dicionário melhoram seus resultados de pesquisa dizendo OpenSearch para ignorar certas palavras de alta frequência ou tratar termos como “creme congelado”, “gelato” e “sorvete” como equivalentes. Eles também podem melhorar as raízes de palavras, como no plug-in de análise japonês (kuromoji).

Os plug-ins opcionais podem fornecer funcionalidades adicionais ao seu domínio. Por exemplo, você pode usar o plug-in Amazon Personalize para fornecer resultados de pesquisa personalizados. Os plug-ins opcionais usam o tipo de pacote `ZIP-PLUGIN`. Para obter mais informações sobre plug-ins opcionais, consulte the section called “Plug-ins por versão do mecanismo”.

Tópicos

Requisitos de permissões de pacotes

Usuários sem acesso de administrador exigem determinadas ações AWS Identity and Access Management (IAM) para gerenciar pacotes:

- `es:CreatePackage`- criar um pacote em uma região OpenSearch de serviço
- `es:DeletePackage`- excluir um pacote de uma região OpenSearch de serviço
- `es:AssociatePackage`: associar um pacote a um domínio
- `es:DissociatePackage`: dissociar um pacote de um domínio

Você também precisa de permissões no caminho do bucket do Amazon S3 ou no objeto em que o pacote personalizado reside.

Conceda todas as permissões no IAM, e não na política de acesso ao domínio. Para ter mais informações, consulte the section called “Identity and Access Management”.

Carregar pacotes para o Amazon S3

Esta seção aborda como carregar pacotes de dicionários personalizados, já que os pacotes de plug-ins opcionais já estão pré-instalados. Antes de associar um dicionário customizado ao seu domínio, você deverá carregá-lo em um bucket do Amazon S3. Para obter mais informações, consulte Carregar objetos no Manual do usuário do Amazon Simple Storage Service. Plug-ins compatíveis não precisam ser carregados.

Se seu dicionário contiver informações confidenciais, especifique a criptografia do lado do servidor com chaves gerenciadas pelo S3 ao fazer o upload. OpenSearch O serviço não pode acessar arquivos no S3 que você protege usando uma AWS KMS chave.

Depois de carregar o arquivo, anote o caminho do S3. O formato do caminho é `s3://bucket-name/file-path/file-name`.

Você pode usar o seguinte arquivo de sinônimos para fazer testes. Salve-o como `synonyms.txt`.

```
danish, croissant, pastry
ice cream, gelato, frozen custard
sneaker, tennis shoe, running shoe
basketball shoe, hightop
```

Certos dicionários, como dicionários Hunspell, usam vários arquivos e exigem seus próprios diretórios no sistema de arquivos. No momento, o OpenSearch Service oferece suporte apenas a dicionários de arquivo único.

Importação e associação de pacotes

O console é a maneira mais simples de importar um dicionário personalizado para o OpenSearch Service. Quando você importa um dicionário do Amazon S3, o OpenSearch Service armazena sua própria cópia do pacote e criptografa automaticamente essa cópia usando AES-256 com chaves gerenciadas pelo serviço. OpenSearch

Os plug-ins opcionais já estão pré-instalados no OpenSearch Service, então você não precisa carregá-los sozinho, mas precisa associar um plug-in a um domínio. Os plug-ins disponíveis estão listados na tela Pacotes, no console.

Importe e associe um pacote a um domínio com o AWS Management Console

1. No console do Amazon OpenSearch Service, escolha Pacotes.
2. Escolha Importar pacote.
3. Dê um nome descritivo ao dicionário personalizado.
4. Forneça o caminho do S3 até o arquivo e escolha Enviar.
5. Retorne à tela Pacotes.
6. Quando o status do pacote estiver Disponível, selecione-o. Plug-ins opcionais aparecerão com o status Disponível automaticamente.
7. Escolha Associar a um domínio.
8. Selecione um domínio e, em seguida, escolha Associar.
9. No painel de navegação, escolha o domínio vá para a guia Pacotes.
10. Se o pacote for um dicionário personalizado, anote o ID quando o pacote se tornar Disponível. Use `analyzers/id` como caminho do arquivo em solicitações para OpenSearch.

Como alternativa, use os AWS CLI SDKs ou a API de configuração para importar e associar pacotes. Para obter mais informações, consulte a Referência de AWS CLI Comandos e a Referência da API do Amazon OpenSearch Service.

Usando pacotes com OpenSearch

Esta seção aborda como usar os dois tipos de pacotes: dicionários personalizados e plug-ins opcionais.

Uso de dicionários customizados

Depois de associar um arquivo a um domínio, será possível usá-lo em parâmetros como `synonyms_path`, `stopwords_path` e `user_dictionary` ao criar tokenizers e filtros de token. O parâmetro exato varia de acordo com o objeto. Vários objetos oferecem suporte a `synonyms_path` e `stopwords_path`, mas `user_dictionary` é exclusivo para o plug-in kuromoji.

Para o plug-in de análise IK (chinês), você pode carregar um arquivo de dicionário personalizado como um pacote personalizado e associá-lo a um domínio, e o plug-in o seleciona automaticamente sem exigir um parâmetro `user_dictionary`. Se seu arquivo for um arquivo de sinônimos, use o parâmetro `synonyms_path`.

O seguinte exemplo adiciona um arquivo de sinônimo a um novo índice:

```
PUT my-index
{
  "settings": {
    "index": {
      "analysis": {
        "analyzer": {
          "my_analyzer": {
            "type": "custom",
            "tokenizer": "standard",
            "filter": ["my_filter"]
          }
        },
        "filter": {
          "my_filter": {
            "type": "synonym",
            "synonyms_path": "analyzers/F111111111",
            "updateable": true
          }
        }
      }
    }
  },
  "mappings": {
    "properties": {
      "description": {
        "type": "text",
        "analyzer": "standard",
        "search_analyzer": "my_analyzer"
      }
    }
  }
}
```

Esta solicitação cria um analisador personalizado para o índice que utiliza o tokenizer padrão e um filtro de token de sinônimo.

- Os tokenizers quebram fluxos de caracteres em tokens (normalmente palavras) de acordo com algum conjunto de regras. O exemplo mais simples é o tokenizer de espaço em branco, que divide os caracteres anteriores em um token cada vez que encontra um caractere de espaço em branco.

Um exemplo mais complexo é o tokenizer padrão, que usa um conjunto de regras com base na gramática para trabalhar em vários idiomas.

- Os filtros de token adicionam, modificam ou excluem tokens. Por exemplo, um filtro de token de sinônimo adiciona tokens quando encontra uma palavra na lista de sinônimos. O filtro de token de palavras irrelevantes remove tokens quando encontra uma palavra na lista de palavras irrelevantes.

Essa solicitação também adiciona um campo de texto (`description`) ao mapeamento e solicita OpenSearch o uso do novo analisador como analisador de pesquisa. Você pode ver que ele ainda usa o analisador padrão como seu analisador de índices.

Finalmente, observe a linha `"updateable": true` no filtro de token. Este campo aplica-se somente a analisadores de pesquisas, e não a analisadores de índices, e será crítico se você desejar atualizar o analisador de pesquisas automaticamente.

Para fazer testes, adicione alguns documentos ao índice:

```
POST _bulk
{ "index": { "_index": "my-index", "_id": "1" } }
{ "description": "ice cream" }
{ "index": { "_index": "my-index", "_id": "2" } }
{ "description": "croissant" }
{ "index": { "_index": "my-index", "_id": "3" } }
{ "description": "tennis shoe" }
{ "index": { "_index": "my-index", "_id": "4" } }
{ "description": "hightop" }
```

Depois, pesquise-os usando um sinônimo:

```
GET my-index/_search
{
  "query": {
    "match": {
      "description": "gelato"
    }
  }
}
```

Nesse caso, OpenSearch retorna a seguinte resposta:

```
{
  "hits": {
    "total": {
      "value": 1,
      "relation": "eq"
    },
    "max_score": 0.99463606,
    "hits": [{
      "_index": "my-index",
      "_type": "_doc",
      "_id": "1",
      "_score": 0.99463606,
      "_source": {
        "description": "ice cream"
      }
    }]
  }
}
```

> **Tip**
>
> Arquivos de dicionário usam espaço de heap Java proporcional ao seu tamanho. Por exemplo, um arquivo de dicionário de 2 GiB pode consumir 2 GiB de espaço de heap em um nó. Ao usar arquivos grandes, verifique se os nós têm espaço de heap suficiente para acomodá-los. Monitore a métrica `JVMMemoryPressure` e dimensione o cluster conforme necessário.

Plug-ins opcionais

OpenSearch O serviço permite que você associe OpenSearch plug-ins opcionais pré-instalados para usar com seu domínio. Um pacote de plug-in opcional é compatível com uma OpenSearch versão específica e só pode ser associado a domínios com essa versão. A lista de pacotes disponíveis para seu domínio inclui todos os plug-ins compatíveis com a versão do seu domínio. Depois de associar um plug-in a um domínio, um processo de instalação no domínio é iniciado. Em seguida, você pode referenciar e usar o plug-in ao fazer solicitações ao OpenSearch Serviço.

Associar e dissociar um plug-in requer uma implantação azul/verde. Para ter mais informações, consulte the section called “Alterações que normalmente causam implantações azuis/verdes”.

Plug-ins opcionais incluem analisadores de idioma e resultados de pesquisa personalizados. Por exemplo, o plug-in Amazon Personalize Search Ranking usa machine learning para personalizar os resultados da pesquisa para seus clientes. Para obter mais informações sobre esse plug-in, consulte Personalização dos resultados da pesquisa de OpenSearch. Para obter uma lista de todos os plug-ins compatíveis, consulte the section called “Plug-ins por versão do mecanismo”.

Plug-in Sudachi

Quando você reassocia um arquivo de dicionário do plug-in Sudachi, ele não reflete imediatamente no domínio. O dicionário é atualizado quando a próxima implantação azul/verde é executada no domínio como parte de uma alteração de configuração ou outra atualização. Como alternativa, você pode criar um novo pacote com os dados atualizados, criar um novo índice usando esse novo pacote, reindexar o índice existente no novo índice e, em seguida, excluir o índice antigo. Se preferir usar a abordagem de reindexação, use um alias de índice para que não haja interrupções no tráfego.

Além disso, o plug-in Sudachi suporta apenas dicionários binários do Sudachi, que você pode carregar com a operação da API. CreatePackage Para obter informações sobre o dicionário do sistema pré-construído e o processo para compilar dicionários do usuário, consulte a documentação do Sudachi.

O exemplo a seguir demonstra como usar os dicionários do sistema e do usuário com o tokenizador do Sudachi. Você deve carregar esses dicionários como pacotes personalizados de tipo `TXT-DICTIONARY` e fornecer seus IDs de pacote nas configurações adicionais.

```
PUT sudachi_sample
{
  "settings": {
    "index": {
      "analysis": {
        "tokenizer": {
          "sudachi_tokenizer": {
            "type": "sudachi_tokenizer",
            "additional_settings": "{\"systemDict\": \"<system-dictionary-package-
id>\",\"userDict\": [\"<user-dictionary-package-id>\"]}"
        }
        },
        "analyzer": {
          "sudachi_analyzer": {
            "filter": ["my_searchfilter"],
            "tokenizer": "sudachi_tokenizer",
            "type": "custom"
```

```
          }
        },
        "filter":{
          "my_searchfilter": {
            "type": "sudachi_split",
            "mode": "search"
          }
        }
      }
    }
  }
}
```

Atualização de pacotes

Esta seção aborda apenas como atualizar um pacote de dicionário personalizado, porque pacotes de plug-ins opcionais já são atualizados para você. O upload de uma nova versão de um dicionário para o Amazon S3 não atualiza automaticamente o pacote no Amazon OpenSearch Service. OpenSearch O serviço armazena sua própria cópia do arquivo, portanto, se você fizer upload de uma nova versão para o S3, deverá atualizá-la manualmente.

Cada um dos seus domínios associados armazena sua própria cópia do arquivo também. Para manter o comportamento de pesquisa previsível, os domínios continuarão a usar a versão atual do pacote até que você os atualize explicitamente. Para atualizar um pacote personalizado, modifique o arquivo Amazon S3 Control, atualize o pacote no OpenSearch Serviço e, em seguida, aplique a atualização.

Atualize um pacote com o AWS Management Console

1. No console de OpenSearch serviço, escolha Pacotes.
2. Escolha um pacote e, em seguida, Atualizar.
3. Forneça o caminho do S3 para o arquivo e escolha Atualizar pacote.
4. Retorne à tela Pacotes.
5. Quando o status do pacote mudar para Disponível, selecione-o. Em seguida, escolha um ou mais domínios associados, Aplicar atualização e confirme. Aguarde até que o status da associação mude para Ativo.
6. As próximas etapas variam dependendo de como você configurou seus índices:

- Se o seu domínio está executando OpenSearch o Elasticsearch 7.8 ou posterior e usa apenas analisadores de pesquisa com o campo atualizável definido como verdadeiro, você não precisa realizar nenhuma ação adicional. OpenSearch O serviço atualiza automaticamente seus índices usando a API _plugins/_refresh_search_analyzers.
- Se seu domínio estiver executando o Elasticsearch 7.7 ou anterior, usa analisadores de índice ou não usa o campo, consulte. `updateable` the section called “Atualizações manuais do índice para dicionários”

Embora o console seja o método mais simples, você também pode usar os AWS CLI SDKs ou a API de configuração para atualizar pacotes OpenSearch de serviços. Para obter mais informações, consulte a Referência de AWS CLI Comandos e a Referência da API do Amazon OpenSearch Service.

Atualizar um pacote com o AWS SDK

Em vez de atualizar manualmente um pacote no console, você pode usar os SDKs para automatizar o processo de atualização. O exemplo de script Python a seguir carrega um novo arquivo de pacote no Amazon S3, atualiza o pacote no OpenSearch Service e aplica o novo pacote ao domínio especificado. Depois de confirmar que a atualização foi bem-sucedida, ele faz uma chamada de amostra para OpenSearch demonstrar que os novos sinônimos foram aplicados.

Você deve fornecer valores para `host`, `region`, `file_name`, `bucket_name`, `s3_key`, `package_id`, `domain_name` e `query`.

```
from requests_aws4auth import AWS4Auth
import boto3
import requests
import time
import json
import sys

host = ''  # The OpenSearch domain endpoint with https:// and a trailing slash. For
 example, https://my-test-domain.us-east-1.es.amazonaws.com/
region = ''  # For example, us-east-1
file_name = ''  # The path to the file to upload
bucket_name = ''  # The name of the S3 bucket to upload to
s3_key = ''  # The name of the S3 key (file name) to upload to
package_id = ''  # The unique identifier of the OpenSearch package to update
domain_name = ''  # The domain to associate the package with
```

```
query = ''  # A test query to confirm the package has been successfully updated

service = 'es'
credentials = boto3.Session().get_credentials()
client = boto3.client('opensearch')
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key,
                   region, service, session_token=credentials.token)


def upload_to_s3(file_name, bucket_name, s3_key):
    """Uploads file to S3"""
    s3 = boto3.client('s3')
    try:
        s3.upload_file(file_name, bucket_name, s3_key)
        print('Upload successful')
        return True
    except FileNotFoundError:
        sys.exit('File not found. Make sure you specified the correct file path.')


def update_package(package_id, bucket_name, s3_key):
    """Updates the package in OpenSearch Service"""
    print(package_id, bucket_name, s3_key)
    response = client.update_package(
        PackageID=package_id,
        PackageSource={
            'S3BucketName': bucket_name,
            'S3Key': s3_key
        }
    )
    print(response)


def associate_package(package_id, domain_name):
    """Associates the package to the domain"""
    response = client.associate_package(
        PackageID=package_id, DomainName=domain_name)
    print(response)
    print('Associating...')


def wait_for_update(domain_name, package_id):
    """Waits for the package to be updated"""
    response = client.list_packages_for_domain(DomainName=domain_name)
```

```
    package_details = response['DomainPackageDetailsList']
    for package in package_details:
        if package['PackageID'] == package_id:
            status = package['DomainPackageStatus']
            if status == 'ACTIVE':
                print('Association successful.')
                return
            elif status == 'ASSOCIATION_FAILED':
                sys.exit('Association failed. Please try again.')
            else:
                time.sleep(10)  # Wait 10 seconds before rechecking the status
                wait_for_update(domain_name, package_id)


def sample_search(query):
    """Makes a sample search call to OpenSearch"""
    path = '_search'
    params = {'q': query}
    url = host + path
    response = requests.get(url, params=params, auth=awsauth)
    print('Searching for ' + '"' + query + '"')
    print(response.text)
```

> **Note**
>
> Se você receber um erro de “pacote não encontrado” ao executar o script usando o AWS CLI, provavelmente significa que o Boto3 está usando a região especificada em ~/.aws/config, que não é a região em que seu bucket do S3 está. Execute `aws configure` e especifique a região correta ou adicione explicitamente a região ao cliente:
>
> ```
> client = boto3.client('opensearch', region_name='us-east-1')
> ```

Atualizações manuais do índice para dicionários

As atualizações manuais do índice se aplicam somente a dicionários personalizados, não a plug-ins opcionais. Para usar um dicionário atualizado, será necessário atualizar manualmente seus índices se você atender a qualquer uma das seguintes condições:

- Seu domínio executa o Elasticsearch 7.7 ou anterior.

- Você usa pacotes personalizados como analisadores de índices.
- Você usa pacotes personalizados como analisadores de pesquisas, mas não inclui o campo atualizável.

Para atualizar os analisadores com os novos arquivos de pacote, você tem duas opções:

- Feche e abra todos os índices que deseja atualizar:

```
POST my-index/_close
POST my-index/_open
```

- Reindexe os índices. Primeiro, crie um índice que use o arquivo de sinônimos atualizado (ou um arquivo inteiramente novo). Observe que apenas o UTF-8 é compatível.

```
PUT my-new-index
{
  "settings": {
    "index": {
      "analysis": {
        "analyzer": {
          "synonym_analyzer": {
            "type": "custom",
            "tokenizer": "standard",
            "filter": ["synonym_filter"]
          }
        },
        "filter": {
          "synonym_filter": {
            "type": "synonym",
            "synonyms_path": "analyzers/F222222222"
          }
        }
      }
    }
  },
  "mappings": {
    "properties": {
      "description": {
        "type": "text",
        "analyzer": "synonym_analyzer"
      }
    }
```

```
  }
}
```

Depois reindexe o índice antigo para o novo:

```
POST _reindex
{
  "source": {
    "index": "my-index"
  },
  "dest": {
    "index": "my-new-index"
  }
}
```

Se você atualiza analisadores de índices com frequência, use aliases de índices para manter um caminho consistente para o índice mais recente:

```
POST _aliases
{
  "actions": [
    {
      "remove": {
        "index": "my-index",
        "alias": "latest-index"
      }
    },
    {
      "add": {
        "index": "my-new-index",
        "alias": "latest-index"
      }
    }
  ]
}
```

Se não precisar do índice antigo, exclua-o:

```
DELETE my-index
```

Dissociação e remoção de pacotes

Dissociar um pacote (seja um dicionário personalizado ou um plug-in opcional) de um domínio significa que você não poderá mais usar esse pacote ao criar novos índices. Depois que um pacote é dissociado, os índices existentes que estavam usando o pacote não podem mais usá-lo. Você deve remover o pacote de qualquer índice antes de poder dissociá-lo, caso contrário, a dissociação falhará.

O console é a maneira mais simples de dissociar um pacote de um domínio e removê-lo do OpenSearch Serviço. Remover um pacote do OpenSearch Serviço não o remove de sua localização original no Amazon S3.

Dissociar um pacote de um domínio com AWS Management Console

1. Vá para https://aws.amazon.com e escolha Fazer login no console.
2. Em Analytics, escolha Amazon OpenSearch Service.
3. No painel de navegação, escolha o domínio e a guia Pacotes.
4. Escolha um pacote, Ações e Dissociar. Confirme sua escolha.
5. Aguarde até que o pacote desapareça da lista. Talvez seja necessário atualizar o navegador.
6. Se desejar usar o pacote com outros domínios, pare aqui. Para continuar com a remoção do pacote (se for um dicionário customizado), escolha Pacotes no painel de navegação.
7. Selecione o pacote e Excluir.

Como alternativa, use os SDKs ou a AWS CLI API de configuração para dissociar e remover pacotes. Para obter mais informações, consulte a Referência de AWS CLI Comandos e a Referência da API do Amazon OpenSearch Service.

Consulta dos dados do Amazon OpenSearch Service com SQL

Você pode usar SQL para consultar seu Amazon OpenSearch Service em vez de usar a DSL de consultas do OpenSearch baseada em JSON. Consultar com SQL é útil se você já está familiarizado com a linguagem ou se deseja integrar seu domínio a uma aplicação que usa SQL.

Use a tabela a seguir para encontrar a versão do plug-in SQL compatível com cada versão do OpenSearch e Elasticsearch.

OpenSearch

Versão do OpenSearch	Versão do plug-in SQL	Recursos notáveis
2.11.0	2.11.0.0	Adicionar suporte para linguagem e consultas PPL
2.9.0	2.9.0.0	Adicione o conector Spark e suporte à tabela e às funções PromQL
2.7.0	2.7.0.0	Adicionar API `datasource`
2.5.0	2.5.0.0	
2.3.0	2.3.0.0	Adicione funções de data e hora `maketime` e `makedate`
1.3.0	1.3.0.0	Suporta tamanho limite de consulta padrão e cláusula IN para selecionar em uma lista de valores
1.2.0	1.2.0.0	Adicionar novo protocolo para o formato de resposta de visualização
1.1.0	1.1.0.0	Ofereça suporte à função de correspondência como um filtro no SQL e PPL
1.0.0	1.0.0.0	Suporte à consulta de um fluxo de dados

Open Distro for Elasticsearch

Versão do Elasticsearch	Versão do plug-in SQL	Recursos notáveis
7.10	1.13.0	NULL FIRST e LAST para funções de janela, função CAST (), comandos SHOW e DESCRIBE
7.9	1.11.0	Funções adicionais de data/hora adicionais, palavra-c have ORDER BY
7.8	1.9.0	

Versão do Elasticsearch	Versão do plug-in SQL	Recursos notáveis
7.7	1.8.0	
7.3	1.3.0	Operadores de strings e numéricos diversos
7.1	1.1.0	

O suporte a SQL está disponível em domínios que executam o OpenSearch ou Elasticsearch 6.5 ou superior. A documentação completa do plugin SQL está disponível na documentação do OpenSearch.

Chamada de exemplo

Para consultar seus dados usando o SQL, envie solicitações HTTP para `_sql` usando o seguinte formato:

```
POST domain-endpoint/_plugins/_sql
{
  "query": "SELECT * FROM my-index LIMIT 50"
}
```

> **Note**
>
> Se o seu domínio estiver executando o Elasticsearch em vez do OpenSearch, o formato será `_opendistro/_sql`.

Notas e diferenças

As chamadas para `_plugins/_sql` incluem nomes de índice no corpo da solicitação, portanto, elas têm as mesmas considerações da política de acesso das operações bulk, mget, e msearch. Como sempre, siga o princípio do privilégio mínimo ao conceder permissões para operações de API.

Para obter considerações de segurança sobre o uso de SQL com o controle de acesso refinado, consulte the section called “Controle de acesso refinado”.

O plugin do OpenSearch SQL inclui muitas configurações ajustáveis. No OpenSearch Service, use o caminho `_cluster/settings`, e não o caminho das configurações do plugin (`_plugins/_query/settings`):

```
PUT _cluster/settings
{
  "transient" : {
    "plugins.sql.enabled" : true
  }
}
```

Para domínios herdados do Elasticsearch, substitua `plugins` por `opendistro`:

```
PUT _cluster/settings
{
  "transient" : {
    "opendistro.sql.enabled" : true
  }
}
```

SQL Workbench

O SQL Workbench é uma interface do usuário do OpenSearch Dashboards que permite executar consultas SQL sob demanda, traduzir SQL em seu equivalente REST e exibir e salvar resultados como texto, JSON, JDBC ou CSV. Para obter mais informações, consulte Query Workbench.

SQL CLI

O SQL CLI é uma aplicação Python autônoma que você pode executar com o comando `opensearchsql`. Para obter as etapas de instalação, configuração e uso, consulte SQL CLI.

Driver JDBC

O driver Java Database Connectivity (JDBC) permite integrar domínios do OpenSearch Service a suas aplicações favoritas de business intelligence (BI). Para baixar o driver, clique aqui. Para obter mais informações, consulte o repositório GitHub.

As tabelas a seguir resumem a compatibilidade de versões do driver.

OpenSearch

Versão do OpenSearch	Versão do driver JDBC
2.11	1.1.0.1
2.9	1.1.0.1
2.7	1.1.0.1
2,5	1.1.0.1
2.3	1.1.0.1
1.3	1.1.0.1
1.2	1.1.0.1
1.1	1.1.0.1
1,0	1.1.0.1

Open Distro for Elasticsearch

Versão do Elasticsearch	Versão do driver JDBC
7.10	1.13.0
7.9	1.11.0
7.8	1.9.0
7.7	1.8.0
7.4	1.4.0
7.1	1.0.0
6.8	0.9.0
6.7	0.9.0

Versão do Elasticsearch	Versão do driver JDBC
6.5	0.9.0

Driver ODBC

O driver de conectividade do banco de dados aberta (ODBC) é um driver ODBC somente leitura para Windows e macOS que permite conectar aplicativos de business intelligence e visualização de dados, como o Microsoft Excel, ao plug-in SQL.

Você pode baixar um exemplo de arquivo de driver funcional na página de artefatos do OpenSearch. Para obter informações sobre como instalar o driver, consulte o repositório de SQL no GitHub.

Pesquisa de k-vizinhos mais próximos (k-NN) no Amazon OpenSearch Service

Abreviação em inglês de seu algoritmo associado k-vizinhos mais próximos (k-nearest neighbors), o k-NN para Amazon OpenSearch Service permite procurar pontos em um espaço vetorial e encontrar os “vizinhos mais próximos” desses pontos por distância euclidiana ou similaridade de cossenos. Os casos de uso incluem recomendações (por exemplo, um recurso de “outras músicas que você pode gostar” em um aplicativo de música), reconhecimento de imagem e detecção de fraudes.

Use as tabelas a seguir para encontrar a versão do plugin k–NN em execução em seu domínio do Amazon OpenSearch Service. Cada versão do plugin k-NN corresponde a uma versão do OpenSearch ou Elasticsearch.

OpenSearch

Versão do OpenSearch	Versão do plugin k-NN	Recursos notáveis
2.11	2.11.0.0	Suporte adicionado para `ignore_unmapped` em consultas k-NN
2.9	2.9.0.0	Implementou vetores de bytes k-NN e filtragem eficiente com o mecanismo Faiss
2.7	2.7.0.0	

Versão do OpenSearch	Versão do plugin k-NN	Recursos notáveis
2,5	2.5.0.0	O SystemIndexPlugin estendido para o índice de sistema do modelo k-NN adicionou extensões de arquivo específicas do Lucene ao HybridFS principal
2.3	2.3.0.0	
1.3	1.3.0.0	
1.2	1.2.0.0	Adicionado suporte para a biblioteca Faiss
1.1	1.1.0.0	
1,0	1.0.0.0	Renomeação das APIs REST em termpos de compatibilidade com versões anteriores, renomeação do namespace de `opendistro` para `opensearch`

Elasticsearch

Versão do Elasticsearch	Versão do plugin k-NN	Recursos notáveis
7.1	1.3.0.0	Distância euclidiana
7.4	1.4.0.0	
7.7	1.8.0.0	Similaridade de cossenos
7.8	1.9.0.0	
7.9	1.11.0.0	API de Warmup, pontuação personalizada
7.10	1.13.0.0	Distância de Hamming, distância L1 Norm, desenvolvimento de scripts Painless

A documentação completa do plugin k-NN está disponível na documentação do OpenSearch. Para obter informações de contexto sobre o algoritmo k-nearest neighbors, consulte a Wikipédia.

Conceitos básicos do k-NN

Para usar o k-NN, é necessário criar um índice com a configuração `index.knn` e adicionar um ou mais campos do tipo de dados `knn_vector`.

```
PUT my-index
{
  "settings": {
    "index.knn": true
  },
  "mappings": {
    "properties": {
      "my_vector1": {
        "type": "knn_vector",
        "dimension": 2
      },
      "my_vector2": {
        "type": "knn_vector",
        "dimension": 4
      }
    }
  }
}
```

O tipo de dados `knn_vector` oferece suporte a uma única lista de até 10.000 flutuantes, com o número de flutuantes definido pelo parâmetro `dimension`. Depois de criar o índice, adicione alguns dados a ele.

```
POST _bulk
{ "index": { "_index": "my-index", "_id": "1" } }
{ "my_vector1": [1.5, 2.5], "price": 12.2 }
{ "index": { "_index": "my-index", "_id": "2" } }
{ "my_vector1": [2.5, 3.5], "price": 7.1 }
{ "index": { "_index": "my-index", "_id": "3" } }
{ "my_vector1": [3.5, 4.5], "price": 12.9 }
{ "index": { "_index": "my-index", "_id": "4" } }
{ "my_vector1": [5.5, 6.5], "price": 1.2 }
{ "index": { "_index": "my-index", "_id": "5" } }
{ "my_vector1": [4.5, 5.5], "price": 3.7 }
{ "index": { "_index": "my-index", "_id": "6" } }
{ "my_vector2": [1.5, 5.5, 4.5, 6.4], "price": 10.3 }
{ "index": { "_index": "my-index", "_id": "7" } }
```

```
{ "my_vector2": [2.5, 3.5, 5.6, 6.7], "price": 5.5 }
{ "index": { "_index": "my-index", "_id": "8" } }
{ "my_vector2": [4.5, 5.5, 6.7, 3.7], "price": 4.4 }
{ "index": { "_index": "my-index", "_id": "9" } }
{ "my_vector2": [1.5, 5.5, 4.5, 6.4], "price": 8.9 }
```

Em seguida, você poderá pesquisar os dados usando o tipo de consulta `knn`.

```
GET my-index/_search
{
  "size": 2,
  "query": {
    "knn": {
      "my_vector2": {
        "vector": [2, 3, 5, 6],
        "k": 2
      }
    }
  }
}
```

Nesse caso, `k` é o número de vizinhos a serem retornados pela consulta, mas também é necessário incluir a opção `size`. Caso contrário, você obterá `k` resultados para cada fragmento (e cada segmento) em vez de `k` resultados para toda a consulta. O k-NN oferece suporte a um valor de `k` máximo de 10.000.

Se você misturar a consulta `knn` com outras cláusulas, poderá receber menos do que `k` resultados. Neste exemplo, a cláusula `post_filter` reduz o número de resultados de 2 para 1.

```
GET my-index/_search
{
  "size": 2,
  "query": {
    "knn": {
      "my_vector2": {
        "vector": [2, 3, 5, 6],
        "k": 2
      }
    }
  },
  "post_filter": {
    "range": {
```

```
      "price": {
        "gte": 6,
        "lte": 10
      }
    }
  }
}
```

Se precisar lidar com um grande volume de consultas e, ao mesmo tempo, manter o desempenho ideal, você pode usar a API `_msearch` para criar uma pesquisa em massa com JSON e enviar uma única solicitação para realizar várias pesquisas:

```
GET _msearch
{ "index": "my-index"}
{ "query": { "knn": {"my_vector2":{"vector": [2, 3, 5, 6],"k":2 }} } }
{ "index": "my-index", "search_type": "dfs_query_then_fetch"}
{ "query": { "knn": {"my_vector1":{"vector": [2, 3],"k":2 }} } }
```

O vídeo a seguir demonstra como configurar pesquisas vetoriais em massa para consultas K-NN.

Diferenças, ajustes e limitações do k-NN

O OpenSearch permite modificar todas as configurações do k-NN com a API `_cluster/settings`. No OpenSearch Service, é possível alterar todas as configurações, exceto `knn.memory.circuit_breaker.enabled` e `knn.circuit_breaker.triggered`. As estatísticas do k-NN são incluídas como métricas do Amazon CloudWatch.

Em particular, verifique a métrica `KNNGraphMemoryUsage` em cada nó de dados em relação à estatística `knn.memory.circuit_breaker.limit` e à RAM disponível para o tipo de instância. O OpenSearch Service usa metade da RAM de uma instância para o heap do Java (com um tamanho de heap de até 32 GiB). Por padrão, o k-NN usa até 50% da metade restante, portanto, um tipo de instância com 32 GiB de RAM pode acomodar 8 GiB de gráficos (32 * 0,5 * 0,5). A performance poderá ser prejudicada se o uso da memória do gráfico exceder esse valor.

Não é possível migrar um índice de k-NN para armazenamento UltraWarm ou armazenamento de baixa atividade se o índice usar aproximação de k-NN (`"index.knn": true`). Se `index.knn` estiver definido como `false` (k-NN exato), ainda é possível mover o índice para outros níveis de armazenamento.

Pesquisa entre clusters no Amazon Service OpenSearch

A pesquisa entre clusters no Amazon OpenSearch Service permite que você realize consultas e agregações em vários domínios conectados. Muitas vezes, faz mais sentido usar vários domínios menores em vez de um único domínio grande, principalmente quando você está executando diferentes tipos de workloads.

Os domínios específicos de workloads spermitem executar as seguintes tarefas:

- Otimizar cada domínio escolhendo tipos de instância para workloads específicas.
- Estabelecer limites de isolamento de falhas entre workloads. Isso significa que, se uma de suas workloads falhar, a falha estará contida nesse domínio específico e não afetará as outras workloads.
- Dimensionar mais facilmente entre domínios.

A pesquisa entre clusters é compatível com OpenSearch painéis, para que você possa criar visualizações e painéis em todos os seus domínios. Você paga taxas padrão AWS de transferência de dados pelos resultados de pesquisa transferidos entre domínios.

Tópicos

Limitações

A pesquisa entre clusters tem várias limitações importantes:

- Você não pode conectar um domínio do Elasticsearch a um OpenSearch domínio.
- Você não pode se conectar a clusters OpenSearch autogerenciados/Elasticsearch.

- Para conectar domínios entre regiões, ambos os domínios devem estar no Elasticsearch 7.10 ou posterior ou. OpenSearch
- Um domínio pode ter um máximo de 20 conexões de saída. Da mesma forma, um domínio pode ter um máximo de 20 conexões de entrada. Em outras palavras, um domínio pode se conectar a um máximo de 20 outros domínios.
- O domínio de origem deve estar na mesma versão ou em uma versão superior à do domínio de destino. Se você configurar uma conexão bidirecional entre dois domínios e quiser atualizar um ou ambos, primeiro exclua uma das conexões.
- Não é possível usar dicionários personalizados ou o SQL com a pesquisa entre clusters.
- Você não pode usar AWS CloudFormation para conectar domínios.
- Não é possível usar a pesquisa entre clusters em instâncias M3 ou expansíveis (T2 e T3).

Pré-requisitos da pesquisa entre clusters

Antes de configurar a pesquisa entre clusters, verifique se os domínios atendem aos seguintes requisitos:

- Dois OpenSearch domínios ou domínios do Elasticsearch na versão 6.7 ou posterior
- Controle de acesso refinado habilitado
- Nenhuma ode-to-node criptografia ativada

Preços da pesquisa entre clusters

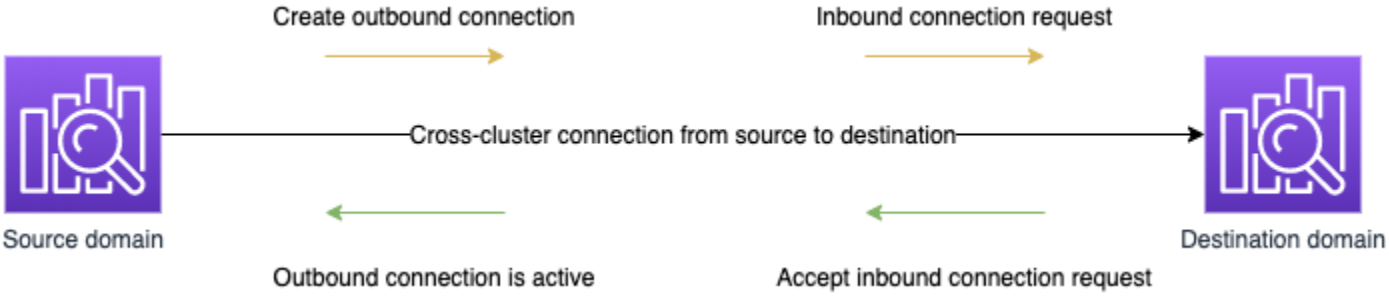
Não há custo adicional para a pesquisa entre domínios.

Configuração de uma conexão

O domínio de “origem” refere-se ao domínio no qual uma solicitação de pesquisa entre clusters se origina. Ou seja, o domínio de origem é aquele para o qual você envia a solicitação de pesquisa inicial.

O domínio de “destino” é aquele que o domínio de origem consulta.

Uma conexão entre clusters é unidirecional do domínio de origem para o domínio de destino. Isso significa que o domínio de destino não pode consultar o domínio de origem. No entanto, você pode configurar outra conexão na direção oposta.



O domínio de origem cria uma conexão de “saída” com o domínio de destino. O domínio de destino recebe uma solicitação de conexão de “entrada” do domínio de origem.

Como configurar uma conexão

1. No painel do domínio, escolha um domínio e escolha a guia Conexões.
2. Na seção Conexões de saída, escolha Solicitar.
3. Em Alias de conexão, insira um nome para a conexão.
4. Escolha entre se conectar a um domínio em sua Conta da AWS região ou em outra conta ou região.
   - Para se conectar a um cluster em sua Conta da AWS região, selecione o domínio no menu suspenso e escolha Solicitar.
   - Para se conectar a um cluster em outra região Conta da AWS ou região, selecione o ARN do domínio remoto e escolha Solicitar. Para conectar domínios entre regiões, ambos os domínios devem estar executando a versão 7.10 ou posterior do Elasticsearch ou. OpenSearch
5. Para ignorar clusters indisponíveis para consultas de cluster, selecione Ignorar indisponíveis. Essa configuração garante que suas consultas entre clusters retornem resultados parciais, apesar de falhas em um ou mais clusters remotos.
6. A pesquisa entre clusters primeiro valida a solicitação de conexão para ter certeza de que os pré-requisitos são atendidos. Se os domínios forem considerados incompatíveis, a solicitação de conexão entrará no estado `Validation failed`.
7. Depois que a solicitação de conexão é validada com êxito, ela é enviada para o domínio de destino, onde precisa ser aprovada. Até que essa aprovação aconteça, a conexão permanecerá em um estado `Pending acceptance`. Quando a solicitação de conexão é aceita no domínio de destino, o estado muda para `Active` e o domínio de destino torna-se disponível para consultas.

- A página de domínio mostra os detalhes gerais da integridade do domínio e da instância do domínio de destino. Os proprietários de domínios têm a flexibilidade de criar, visualizar, remover e monitorar conexões de saída e de entrada de seus domínios.

Depois que a conexão é estabelecida, qualquer tráfego que flua entre os nós dos domínios conectados é criptografado. Se você conectar um domínio da VPC a um domínio que não seja de VPC e o domínio de não VPC for um endpoint público que pode receber tráfego da Internet, o tráfego entre clusters entre os domínios ainda será criptografado e seguro.

Remoção de uma conexão

A remoção de uma conexão interrompe qualquer operação entre clusters em seus índices.

1. No painel do domínio, selecione a guia Conexões.
2. Selecione as conexões de domínio a serem removidas e escolha Excluir. Em seguida, confirme a exclusão.

Você pode executar essas etapas no domínio de origem ou de destino para remover a conexão. Depois que a conexão é removida, ela permanece visível com o status `Deleted` por um período de 15 dias.

Não é possível excluir um domínio com conexões ativas entre clusters. Para excluir um domínio, primeiro remova todas as conexões de entrada e saída desse domínio. Isso garante que você leve em consideração os usuários de domínio entre clusters antes de excluir o domínio.

Configuração da segurança e demonstração de exemplo

1. Envie uma solicitação de pesquisa entre clusters para o domínio de origem.
2. O domínio de origem avalia essa solicitação em relação à política de acesso ao domínio. Como a pesquisa entre clusters requer controle de acesso refinado, recomendamos uma política de acesso aberto no domínio de origem.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:account:domain/src-domain/*"
    }
  ]
}
```

> **Note**
>
> Se você incluir índices remotos no caminho, deverá codificar em URL o URI no ARN do domínio. Por exemplo, use `arn:aws:es:us-east-1:123456789012:domain/my-domain/local_index,dst%3Aremote_index` em vez de `arn:aws:es:us-east-1:123456789012:domain/my-domain/local_index,dst:remote_index`.

Se você optar por usar uma política de acesso restritiva além do controle de acesso refinado, sua política deverá permitir o acesso, no mínimo, ao `es:ESHttpGet`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": "es:ESHttpGet",
      "Resource": "arn:aws:es:region:account:domain/src-domain/*"
    }
  ]
}
```

3. O controle de acesso refinado no domínio de origem avalia a solicitação:

- A solicitação é assinada com credenciais básicas do IAM ou HTTP válidas?
- Em caso afirmativo, o usuário tem permissão para realizar a pesquisa e acessar os dados?

Se a solicitação pesquisar dados somente no domínio de destino (por exemplo, `dest-alias:dest-index/_search`), você só precisará de permissões no domínio de destino.

Se a solicitação pesquisar dados nos dois domínios (por exemplo, `source-index,dest-alias:dest-index/_search`), você precisará de permissões nos dois domínios.

No controle de acesso refinado, os usuários devem ter a permissão `indices:admin/shards/search_shards` além das permissões `read` ou `search` padrão para os índices relevantes.

4. O domínio de origem passa a solicitação para o domínio de destino. O domínio de destino avalia essa solicitação em relação à política de acesso ao domínio. Você deve incluir a permissão `es:ESCrossClusterGet` no domínio de destino:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESCrossClusterGet",
      "Resource": "arn:aws:es:region:account:domain/dst-domain"
    }
  ]
}
```

Verifique se a permissão `es:ESCrossClusterGet` é aplicada a `/dst-domain` e não a `/dst-domain/*`.

No entanto, essa política mínima só permite pesquisas entre clusters. Para executar outras operações, como indexar documentos e executar pesquisas padrão, você precisa de permissões adicionais. Recomendamos a seguinte política no domínio de destino:

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:account:domain/dst-domain/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESCrossClusterGet",
      "Resource": "arn:aws:es:region:account:domain/dst-domain"
    }
  ]
}
```

> **Note**
>
> Todas as solicitações de pesquisa entre clusters entre domínios são criptografadas em trânsito por padrão como parte da node-to-node criptografia.

5. O domínio de destino executa a pesquisa e retorna os resultados para o domínio de origem.
6. O domínio de origem combina seus próprios resultados (se houver) com os resultados do domínio de destino e os retorna para você.
7. Recomendamos o Postman para solicitações de teste:

   - No domínio de destino, indexe um documento:

```
POST https://dst-domain.us-east-1.es.amazonaws.com/books/_doc/1

{
  "Dracula": "Bram Stoker"
}
```

- Para consultar esse índice do domínio de origem, inclua o alias de conexão do domínio de destino dentro da consulta.

```
GET https://src-domain.us-east-1.es.amazonaws.com/<connection_alias>:books/
_search

{
    ...
  "hits": [
    {
      "_index": "source-destination:books",
      "_type": "_doc",
      "_id": "1",
      "_score": 1,
      "_source": {
        "Dracula": "Bram Stoker"
      }
    }
  ]
}
```

Você pode encontrar o alias de conexão na guia Conexões no painel do domínio.

- Se você configurar uma conexão entre `domain-a -> domain-b` com alias de conexão `cluster_b` e `domain-a -> domain-c` com alias de conexão `cluster_c`, `domain-a`, pesquise `domain-b` e `domain-c` da seguinte forma:

```
GET https://src-domain.us-east-1.es.amazonaws.com/
local_index,cluster_b:b_index,cluster_c:c_index/_search
{
  "query": {
    "match": {
      "user": "domino"
    }
  }
}
```

Resposta

```
{
  "took": 150,
  "timed_out": false,
```

```
  "_shards": {
    "total": 3,
    "successful": 3,
    "failed": 0,
    "skipped": 0
  },
  "_clusters": {
    "total": 3,
    "successful": 3,
    "skipped": 0
  },
  "hits": {
    "total": 3,
    "max_score": 1,
    "hits": [
      {
        "_index": "local_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 1,
        "_source": {
          "user": "domino",
          "message": "Lets unite the new mutants",
          "likes": 0
        }
      },
      {
        "_index": "cluster_b:b_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 2,
        "_source": {
          "user": "domino",
          "message": "I'm different",
          "likes": 0
        }
      },
      {
        "_index": "cluster_c:c_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 3,
        "_source": {
          "user": "domino",
```

```
          "message": "So am I",
          "likes": 0
        }
      }
    ]
  }
}
```

Se você não optou por ignorar clusters indisponíveis na sua configuração de conexão, todos os clusters de destino na sua pesquisa precisam estar disponíveis para que sua solicitação de pesquisa seja executada com êxito. Caso contrário, toda a solicitação falhará — mesmo que um dos domínios não esteja disponível, nenhum resultado da pesquisa será retornado.

OpenSearch Painéis

Você pode visualizar dados de vários domínios conectados da mesma maneira que de um único domínio, exceto que você deve acessar os índices remotos usando `connection-alias:index`. Portanto, o padrão de índice deve corresponder a `connection-alias:index`.

Learning to Rank para Amazon OpenSearch Service

O OpenSearch usa um framework de classificação probabilística chamado BM-25 para calcular pontuações de relevância. Se uma palavra-chave distintiva aparece com mais frequência em um documento, o BM-25 atribui uma pontuação de relevância maior a esse documento. Esse framework, no entanto, não leva em conta o comportamento do usuário, como dados de cliques, o que pode melhorar ainda mais a relevância.

O Learning to Rank é um plugin de código aberto que permite que você use machine learning e dados comportamentais para ajustar a relevância de documentos. Ele usa modelos das bibliotecas XGBoost e Ranklib para reclassificar os resultados da pesquisa. O plugin Elasticsearch LTR foi desenvolvido inicialmente pela OpenSource Connections, com contribuições importantes da Wikimedia Foundation, Snagajob Engineering, Bonsai e Yelp Engineering. A versão OpenSearch do plugin se deriva do plugin Elasticsearch LTR. A documentação completa, incluindo etapas detalhadas e descrições da API, está disponível na documentação do Learning to Rank.

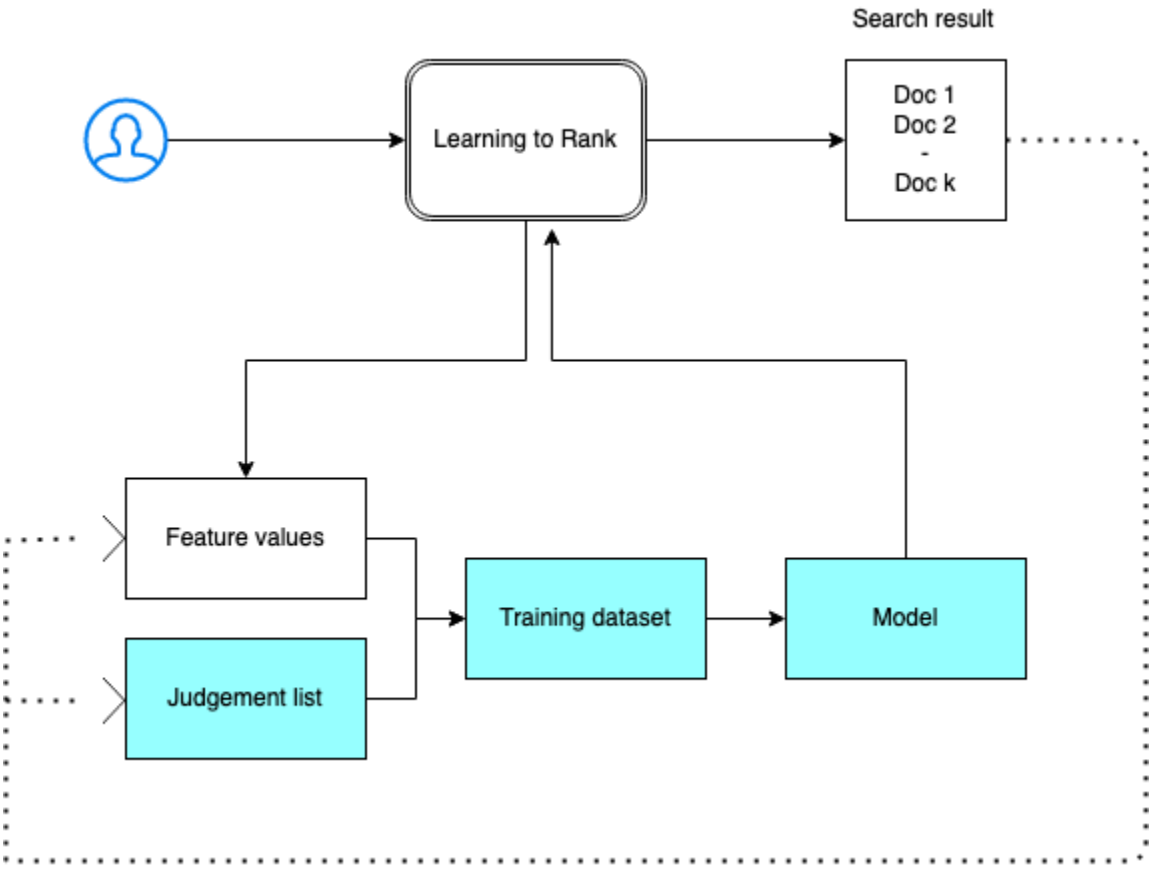
O Learning to Rank exige o OpenSearch ou Elasticsearch 7.7 ou superior

> **Note**
>
> Para usar o plugin Learning to Rank, é necessário ter permissões de administrador completas. Para saber mais, consulte the section called “Modificação do usuário primário”.

Tópicos

Conceitos básicos do Learning to Rank

Você precisa fornecer uma lista de julgamento, preparar um conjunto de dados de treinamento e treinar o modelo fora do Amazon OpenSearch Service. As partes em azul ocorrem fora do OpenSearch Service:



Etapa 1: Inicializar o plugin

Para inicializar o plugin Learning to Rank, envie a seguinte solicitação para seu domínio do OpenSearch Service:

```
PUT _ltr
```

```
{
  "acknowledged" : true,
  "shards_acknowledged" : true,
  "index" : ".ltrstore"
}
```

Este comando cria um índice `.ltrstore` oculto que armazena informações de metadados, como conjuntos de recursos e modelos.

Etapa 2: Criar uma lista de julgamento

> **Note**
>
> Esta etapa deve ser realizada fora do OpenSearch Service.

Uma lista de julgamentos é uma coleção de exemplos com os quais um modelo de machine learning aprende. Sua lista de julgamento deve incluir palavras-chave que são importantes para você e um conjunto de documentos classificados para cada palavra-chave.

Neste exemplo, temos uma lista de julgamento para um conjunto de dados de filmes. Um grau 4 indica uma combinação perfeita. Um grau 0 indica a pior correspondência.

Grau	Palavra-chave	ID do documento	Nome do filme
4	rambo	7555	Rambo
3	rambo	1370	Rambo III
3	rambo	1369	Rambo: First Blood Part II

Grau	Palavra-chave	ID do documento	Nome do filme
3	rambo	1368	First Blood

Prepare sua lista de julgamento no seguinte formato:

```
4 qid:1 # 7555 Rambo
3 qid:1 # 1370 Rambo III
3 qid:1 # 1369 Rambo: First Blood Part II
3 qid:1 # 1368 First Blood

where qid:1 represents "rambo"
```

Para um exemplo mais completo de uma lista de julgamento, consulte Julgamentos de filmes.

Você pode criar essa lista de julgamentos manualmente com a ajuda de anotadores humanos ou inferi-la programaticamente a partir de dados analíticos.

Etapa 3: Construir um conjunto de recursos

Um recurso é um campo que corresponde à relevância de um documento — por exemplo, `title`, `overview`, `popularity score`(número de visualizações) e assim por diante.

Crie um conjunto de recursos com um modelo do Mustache para cada recurso. Para obter mais informações sobre os recursos, consulte Como trabalhar com recursos.

Neste exemplo, construímos um conjunto de recursos `movie_features` com os campos `title` e `overview`:

```
POST _ltr/_featureset/movie_features
{
  "featureset" : {
      "name" : "movie_features",
      "features" : [
        {
          "name" : "1",
          "params" : [
            "keywords"
          ],
          "template_language" : "mustache",
```

```
          "template" : {
            "match" : {
              "title" : "{{keywords}}"
            }
          }
        },
        {
          "name" : "2",
          "params" : [
            "keywords"
          ],
          "template_language" : "mustache",
          "template" : {
            "match" : {
              "overview" : "{{keywords}}"
            }
          }
        }
      ]
    }
}
```

Se você consultar o índice `.ltrstore` original, obterá seu conjunto de recursos de volta:

```
GET _ltr/_featureset
```

Etapa 4: Registrar os valores dos recursos

Os valores dos recursos são as pontuações de relevância calculadas pelo BM-25 para cada recurso.

Combine o conjunto de recursos e a lista de julgamento para registrar os valores dos recursos. Para obter mais informações sobre recursos de registro em log do, consulte Pontuações de recursos de registro.

Neste exemplo, a consulta `bool` recupera os documentos classificados com o filtro e, em seguida, seleciona o conjunto de recursos com a consulta `sltr`. A consulta `ltr_log` combina os documentos e os recursos para registrar os valores dos recursos correspondentes:

```
POST tmdb/_search
{
  "_source": {
    "includes": [
```

```
      "title",
      "overview"
    ]
  },
  "query": {
    "bool": {
      "filter": [
        {
          "terms": {
            "_id": [
              "7555",
              "1370",
              "1369",
              "1368"
            ]
          }
        },
        {
          "sltr": {
            "_name": "logged_featureset",
            "featureset": "movie_features",
            "params": {
              "keywords": "rambo"
            }
          }
        }
      ]
    }
  },
  "ext": {
    "ltr_log": {
      "log_specs": {
        "name": "log_entry1",
        "named_query": "logged_featureset"
      }
    }
  }
}
```

Uma resposta de exemplo pode ser a seguinte:

```
{
  "took" : 7,
```

```
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 4,
      "relation" : "eq"
    },
    "max_score" : 0.0,
    "hits" : [
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1368",
        "_score" : 0.0,
        "_source" : {
          "overview" : "When former Green Beret John Rambo is harassed by local law
enforcement and arrested for vagrancy, the Vietnam vet snaps, runs for the hills and
rat-a-tat-tats his way into the action-movie hall of fame. Hounded by a relentless
sheriff, Rambo employs heavy-handed guerilla tactics to shake the cops off his tail.",
          "title" : "First Blood"
        },
        "fields" : {
          "_ltrlog" : [
            {
              "log_entry1" : [
                {
                  "name" : "1"
                },
                {
                  "name" : "2",
                  "value" : 10.558305
                }
              ]
            }
          ]
        },
        "matched_queries" : [
          "logged_featureset"
        ]
```

```
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "7555",
        "_score" : 0.0,
        "_source" : {
          "overview" : "When governments fail to act on behalf of captive missionaries,
ex-Green Beret John James Rambo sets aside his peaceful existence along the Salween
River in a war-torn region of Thailand to take action.  Although he's still haunted
by violent memories of his time as a U.S. soldier during the Vietnam War, Rambo can
hardly turn his back on the aid workers who so desperately need his help.",
          "title" : "Rambo"
        },
        "fields" : {
          "_ltrlog" : [
            {
              "log_entry1" : [
                {
                  "name" : "1",
                  "value" : 11.2569065
                },
                {
                  "name" : "2",
                  "value" : 9.936821
                }
              ]
            }
          ]
        },
        "matched_queries" : [
          "logged_featureset"
        ]
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1369",
        "_score" : 0.0,
        "_source" : {
          "overview" : "Col. Troutman recruits ex-Green Beret John Rambo for a highly
secret and dangerous mission. Teamed with Co Bao, Rambo goes deep into Vietnam to
rescue POWs. Deserted by his own team, he's left in a hostile jungle to fight for his
life, avenge the death of a woman and bring corrupt officials to justice.",
```

```
          "title" : "Rambo: First Blood Part II"
        },
        "fields" : {
          "_ltrlog" : [
            {
              "log_entry1" : [
                {
                  "name" : "1",
                  "value" : 6.334839
                },
                {
                  "name" : "2",
                  "value" : 10.558305
                }
              ]
            }
          ]
        },
        "matched_queries" : [
          "logged_featureset"
        ]
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1370",
        "_score" : 0.0,
        "_source" : {
          "overview" : "Combat has taken its toll on Rambo, but he's finally begun to
find inner peace in a monastery. When Rambo's friend and mentor Col. Trautman asks for
his help on a top secret mission to Afghanistan, Rambo declines but must reconsider
when Trautman is captured.",
          "title" : "Rambo III"
        },
        "fields" : {
          "_ltrlog" : [
            {
              "log_entry1" : [
                {
                  "name" : "1",
                  "value" : 9.425955
                },
                {
                  "name" : "2",
```

```
                "value" : 11.262714
              }
            ]
          }
        ]
      },
      "matched_queries" : [
        "logged_featureset"
      ]
    }
  ]
}
}
```

No exemplo anterior, o primeiro recurso não tem um valor de recurso porque a palavra-chave “rambo” não aparece no campo título do documento com um ID igual a 1368. Este é um valor de recurso ausente nos dados de treinamento.

Etapa 5: Criar um conjunto de dados de treinamento

> **Note**
>
> Esta etapa deve ser realizada fora do OpenSearch Service.

A próxima etapa é combinar a lista de julgamento e os valores de recursos para criar um conjunto de dados de treinamento. Se a lista de julgamento original é semelhante a:

```
4 qid:1 # 7555 Rambo
3 qid:1 # 1370 Rambo III
3 qid:1 # 1369 Rambo: First Blood Part II
3 qid:1 # 1368 First Blood
```

Converta-a para o conjunto de dados de treinamento final, que é semelhante a:

```
4 qid:1 1:12.318474 2:10.573917 # 7555 rambo
3 qid:1 1:10.357875 2:11.950391 # 1370 rambo
3 qid:1 1:7.010513 2:11.220095 # 1369 rambo
3 qid:1 1:0.0 2:11.220095 # 1368 rambo
```

Você pode executar esta etapa manualmente ou escrever um programa para automatizá-la.

Etapa 6: Escolher um algoritmo e construir o modelo

> **Note**
>
> Esta etapa deve ser realizada fora do OpenSearch Service.

Com o conjunto de dados de treinamento instalado, o próximo passo é usar bibliotecas XGBoost ou Ranklib para construir um modelo. As bibliotecas XGBoost e Ranklib permitem criar modelos populares como LambdaMART, Random Forests e assim por diante.

Para obter as etapas para usar as bibliotecas XGBoost e o Ranklib para construir o modelo, consulte a documentação do XGBoost e do RankLib, respectivamente. Para usar o Amazon SageMaker para criar o modelo do XGBoost, consulte Algoritmo XGBoost.

Etapa 7: Implantar o modelo

Depois de criar o modelo, implante-o no plugin Learning to Rank. Para obter mais informações sobre como implantar um modelo, consulte Upload de um modelo treinado.

Neste exemplo, construímos um modelo `my_ranklib_model` usando a biblioteca Ranklib:

```
POST _ltr/_featureset/movie_features/_createmodel?pretty
{
  "model": {
    "name": "my_ranklib_model",
    "model": {
      "type": "model/ranklib",
      "definition": """## LambdaMART
## No. of trees = 10
## No. of leaves = 10
## No. of threshold candidates = 256
## Learning rate = 0.1
## Stop early = 100

<ensemble>
   <tree id="1" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
```

```
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-2.0</output>
            </split>
            <split pos="right">
               <feature>1</feature>
               <threshold>7.010513</threshold>
               <split pos="left">
                  <output>-2.0</output>
               </split>
               <split pos="right">
                  <output>-2.0</output>
               </split>
            </split>
         </split>
         <split pos="right">
            <output>2.0</output>
         </split>
      </split>
   </tree>
   <tree id="2" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-1.67031991481781</output>
            </split>
            <split pos="right">
               <feature>1</feature>
               <threshold>7.010513</threshold>
               <split pos="left">
                  <output>-1.67031991481781</output>
               </split>
               <split pos="right">
                  <output>-1.6703200340270996</output>
               </split>
            </split>
         </split>
         <split pos="right">
            <output>1.6703201532363892</output>
         </split>
```

```
      </split>
   </tree>
   <tree id="3" weight="0.1">
      <split>
         <feature>2</feature>
         <threshold>10.573917</threshold>
         <split pos="left">
            <output>1.479954481124878</output>
         </split>
         <split pos="right">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.4799546003341675</output>
               </split>
               <split pos="right">
                  <output>-1.479954481124878</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.479954481124878</output>
            </split>
         </split>
      </split>
   </tree>
   <tree id="4" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-1.3569872379302979</output>
            </split>
            <split pos="right">
               <feature>1</feature>
               <threshold>7.010513</threshold>
               <split pos="left">
                  <output>-1.3569872379302979</output>
               </split>
```

```
            <split pos="right">
               <output>-1.3569872379302979</output>
            </split>
         </split>
         <split pos="right">
            <output>1.3569873571395874</output>
         </split>
      </split>
   </tree>
   <tree id="5" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-1.2721362113952637</output>
            </split>
            <split pos="right">
               <feature>1</feature>
               <threshold>7.010513</threshold>
               <split pos="left">
                  <output>-1.272136330604532</output>
               </split>
               <split pos="right">
                  <output>-1.272136330604532</output>
               </split>
            </split>
         </split>
         <split pos="right">
            <output>1.2721362113952637</output>
         </split>
      </split>
   </tree>
   <tree id="6" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
```

```
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-1.2110036611557007</output>
            </split>
            <split pos="right">
               <output>-1.2110036611557007</output>
            </split>
         </split>
         <split pos="right">
            <output>-1.2110037803649902</output>
         </split>
      </split>
      <split pos="right">
         <output>1.2110037803649902</output>
      </split>
   </split>
</tree>
<tree id="7" weight="0.1">
   <split>
      <feature>1</feature>
      <threshold>10.357875</threshold>
      <split pos="left">
         <feature>1</feature>
         <threshold>7.010513</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-1.165616512298584</output>
            </split>
            <split pos="right">
               <output>-1.165616512298584</output>
            </split>
         </split>
         <split pos="right">
            <output>-1.165616512298584</output>
         </split>
      </split>
      <split pos="right">
         <output>1.165616512298584</output>
      </split>
   </split>
</tree>
```

```
   <tree id="8" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.131177544593811</output>
               </split>
               <split pos="right">
                  <output>-1.131177544593811</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.131177544593811</output>
            </split>
         </split>
         <split pos="right">
            <output>1.131177544593811</output>
         </split>
      </split>
   </tree>
   <tree id="9" weight="0.1">
      <split>
         <feature>2</feature>
         <threshold>10.573917</threshold>
         <split pos="left">
            <output>1.1046180725097656</output>
         </split>
         <split pos="right">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.1046180725097656</output>
               </split>
               <split pos="right">
                  <output>-1.1046180725097656</output>
```

```
               </split>
            </split>
            <split pos="right">
               <output>-1.1046180725097656</output>
            </split>
         </split>
      </split>
   </tree>
   <tree id="10" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.0838804244995117</output>
               </split>
               <split pos="right">
                  <output>-1.0838804244995117</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.0838804244995117</output>
            </split>
         </split>
         <split pos="right">
            <output>1.0838804244995117</output>
         </split>
      </split>
   </tree>
</ensemble>
"""
    }
  }
}
```

Para ver o modelo, envie a seguinte solicitação:

```
GET _ltr/_model/my_ranklib_model
```

Etapa 8: Pesquisar com Learning to Rank

Após a implantação do modelo, você estará pronto para pesquisar.

Execute a consulta `sltr` com os recursos que você está usando e o nome do modelo que deseja executar:

```
POST tmdb/_search
{
  "_source": {
    "includes": ["title", "overview"]
  },
  "query": {
    "multi_match": {
      "query": "rambo",
      "fields": ["title", "overview"]
    }
  },
  "rescore": {
    "query": {
      "rescore_query": {
        "sltr": {
          "params": {
            "keywords": "rambo"
          },
          "model": "my_ranklib_model"
        }
      }
    }
  }
}
```

Com o Learning to Rank, você vê “Rambo” como o primeiro resultado porque nós atribuímos a ele a nota mais alta na lista de julgamento:

```
{
  "took" : 12,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
```

```
 },
 "hits" : {
   "total" : {
     "value" : 7,
     "relation" : "eq"
   },
   "max_score" : 13.096414,
   "hits" : [
     {
       "_index" : "tmdb",
       "_type" : "movie",
       "_id" : "7555",
       "_score" : 13.096414,
       "_source" : {
         "overview" : "When governments fail to act on behalf of captive missionaries,
ex-Green Beret John James Rambo sets aside his peaceful existence along the Salween
River in a war-torn region of Thailand to take action.  Although he's still haunted
by violent memories of his time as a U.S. soldier during the Vietnam War, Rambo can
hardly turn his back on the aid workers who so desperately need his help.",
         "title" : "Rambo"
       }
     },
     {
       "_index" : "tmdb",
       "_type" : "movie",
       "_id" : "1370",
       "_score" : 11.17245,
       "_source" : {
         "overview" : "Combat has taken its toll on Rambo, but he's finally begun to
find inner peace in a monastery. When Rambo's friend and mentor Col. Trautman asks for
his help on a top secret mission to Afghanistan, Rambo declines but must reconsider
when Trautman is captured.",
         "title" : "Rambo III"
       }
     },
     {
       "_index" : "tmdb",
       "_type" : "movie",
       "_id" : "1368",
       "_score" : 10.442155,
       "_source" : {
         "overview" : "When former Green Beret John Rambo is harassed by local law
enforcement and arrested for vagrancy, the Vietnam vet snaps, runs for the hills and
```

```
rat-a-tat-tats his way into the action-movie hall of fame. Hounded by a relentless
sheriff, Rambo employs heavy-handed guerilla tactics to shake the cops off his tail.",
         "title" : "First Blood"
       }
     },
     {
       "_index" : "tmdb",
       "_type" : "movie",
       "_id" : "1369",
       "_score" : 10.442155,
       "_source" : {
         "overview" : "Col. Troutman recruits ex-Green Beret John Rambo for a highly
secret and dangerous mission. Teamed with Co Bao, Rambo goes deep into Vietnam to
rescue POWs. Deserted by his own team, he's left in a hostile jungle to fight for his
life, avenge the death of a woman and bring corrupt officials to justice.",
         "title" : "Rambo: First Blood Part II"
       }
     },
     {
       "_index" : "tmdb",
       "_type" : "movie",
       "_id" : "31362",
       "_score" : 7.424202,
       "_source" : {
         "overview" : "It is 1985, and a small, tranquil Florida town is being rocked
by a wave of vicious serial murders and bank robberies. Particularly sickening to the
authorities is the gratuitous use of violence by two “Rambo” like killers who dress
themselves in military garb. Based on actual events taken from FBI files, the movie
depicts the Bureau’s efforts to track down these renegades.",
         "title" : "In the Line of Duty: The F.B.I. Murders"
       }
     },
     {
       "_index" : "tmdb",
       "_type" : "movie",
       "_id" : "13258",
       "_score" : 6.43182,
       "_source" : {
         "overview" : """Will Proudfoot (Bill Milner) is looking for an escape from
his family's stifling home life when he encounters Lee Carter (Will Poulter), the
school bully. Armed with a video camera and a copy of "Rambo: First Blood", Lee plans
to make cinematic history by filming his own action-packed video epic. Together, these
two newfound friends-turned-budding-filmmakers quickly discover that their imaginative
```

```
 – and sometimes mishap-filled – cinematic adventure has begun to take on a life of its
 own!""",
          "title" : "Son of Rambow"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "61410",
        "_score" : 3.9719706,
        "_source" : {
          "overview" : "It's South Africa 1990. Two major events are about to happen:
 The release of Nelson Mandela and, more importantly, it's Spud Milton's first year
 at an elite boys only private boarding school. John Milton is a boy from an ordinary
 background who wins a scholarship to a private school in Kwazulu-Natal, South Africa.
 Surrounded by boys with nicknames like Gecko, Rambo, Rain Man and Mad Dog, Spud has
 his hands full trying to adapt to his new home. Along the way Spud takes his first
 tentative steps along the path to manhood. (The path it seems could be a rather long
 road). Spud is an only child. He is cursed with parents from well beyond the lunatic
 fringe and a senile granny. His dad is a fervent anti-communist who is paranoid that
 the family domestic worker is running a shebeen from her room at the back of the
 family home. His mom is a free spirit and a teenager's worst nightmare, whether it's
 shopping for Spud's underwear in the local supermarket",
          "title" : "Spud"
        }
      }
    ]
  }
}
```

Se você pesquisar sem usar o plugin Learning to Rank, o OpenSearch retornará resultados diferentes:

```
POST tmdb/_search
{
  "_source": {
    "includes": ["title", "overview"]
  },
  "query": {
    "multi_match": {
      "query": "Rambo",
      "fields": ["title", "overview"]
    }
```

```
  }
}
```


```
{
  "took" : 5,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 5,
      "relation" : "eq"
    },
    "max_score" : 11.262714,
    "hits" : [
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1370",
        "_score" : 11.262714,
        "_source" : {
          "overview" : "Combat has taken its toll on Rambo, but he's finally begun to
 find inner peace in a monastery. When Rambo's friend and mentor Col. Trautman asks for
 his help on a top secret mission to Afghanistan, Rambo declines but must reconsider
 when Trautman is captured.",
          "title" : "Rambo III"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "7555",
        "_score" : 11.2569065,
        "_source" : {
          "overview" : "When governments fail to act on behalf of captive missionaries,
 ex-Green Beret John James Rambo sets aside his peaceful existence along the Salween
 River in a war-torn region of Thailand to take action.  Although he's still haunted
 by violent memories of his time as a U.S. soldier during the Vietnam War, Rambo can
 hardly turn his back on the aid workers who so desperately need his help.",
```

```
        "title" : "Rambo"
      }
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "1368",
      "_score" : 10.558305,
      "_source" : {
        "overview" : "When former Green Beret John Rambo is harassed by local law
enforcement and arrested for vagrancy, the Vietnam vet snaps, runs for the hills and
rat-a-tat-tats his way into the action-movie hall of fame. Hounded by a relentless
sheriff, Rambo employs heavy-handed guerilla tactics to shake the cops off his tail.",
        "title" : "First Blood"
      }
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "1369",
      "_score" : 10.558305,
      "_source" : {
        "overview" : "Col. Troutman recruits ex-Green Beret John Rambo for a highly
secret and dangerous mission. Teamed with Co Bao, Rambo goes deep into Vietnam to
rescue POWs. Deserted by his own team, he's left in a hostile jungle to fight for his
life, avenge the death of a woman and bring corrupt officials to justice.",
        "title" : "Rambo: First Blood Part II"
      }
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "13258",
      "_score" : 6.4600153,
      "_source" : {
        "overview" : """Will Proudfoot (Bill Milner) is looking for an escape from
his family's stifling home life when he encounters Lee Carter (Will Poulter), the
school bully. Armed with a video camera and a copy of "Rambo: First Blood", Lee plans
to make cinematic history by filming his own action-packed video epic. Together, these
two newfound friends-turned-budding-filmmakers quickly discover that their imaginative
– and sometimes mishap-filled – cinematic adventure has begun to take on a life of its
own!""",
        "title" : "Son of Rambow"
      }
```

```
      }
    ]
  }
}
```

Com base no quanto bem você acha que o modelo está funcionando, ajuste a lista de julgamento e os recursos. Em seguida, repita as etapas 2 a 8 para melhorar os resultados da classificação ao longo do tempo.

API do Learning to Rank

Use as operações do Learning to Rank para trabalhar programaticamente com conjuntos de recursos e modelos.

Criar armazenamento

Cria um índice `.ltrstore` oculto que armazena informações de metadados, como conjuntos de recursos e modelos.

```
PUT _ltr
```

Excluir armazenamento

Exclui o índice `.ltrstore` oculto e redefine o plugin.

```
DELETE _ltr
```

Criar conjunto de recursos

Cria um conjunto de recursos.

```
POST _ltr/_featureset/<name_of_features>
```

Excluir conjunto de recursos

Exclui um conjunto de recursos.

```
DELETE _ltr/_featureset/<name_of_feature_set>
```

Obter conjunto de recursos

Recupera um conjunto de recursos.

```
GET _ltr/_featureset/<name_of_feature_set>
```

Criar modelo

Cria um modelo.

```
POST _ltr/_featureset/<name_of_feature_set>/_createmodel
```

Excluir modelo

Exclui um modelo.

```
DELETE _ltr/_model/<name_of_model>
```

Obter modelo

Recupera um modelo.

```
GET _ltr/_model/<name_of_model>
```

Obter estatísticas

Fornece informações sobre como o plugin está se comportando.

```
GET _ltr/_stats
```

Também é possível usar filtros para recuperar uma única estatística:

```
GET _ltr/_stats/<stat>
```

Além disso, é possível limitar as informações a um único nó no cluster:

```
GET _ltr/_stats/<stat>/nodes/<nodeId>

{
  "_nodes" : {
    "total" : 1,
```

```
    "successful" : 1,
    "failed" : 0
  },
  "cluster_name" : "873043598401:ltr-77",
  "stores" : {
    ".ltrstore" : {
      "model_count" : 1,
      "featureset_count" : 1,
      "feature_count" : 2,
      "status" : "green"
    }
  },
  "status" : "green",
  "nodes" : {
    "DjelK-_ZSfyzstO5dhGGQA" : {
      "cache" : {
        "feature" : {
          "eviction_count" : 0,
          "miss_count" : 0,
          "entry_count" : 0,
          "memory_usage_in_bytes" : 0,
          "hit_count" : 0
        },
        "featureset" : {
          "eviction_count" : 2,
          "miss_count" : 2,
          "entry_count" : 0,
          "memory_usage_in_bytes" : 0,
          "hit_count" : 0
        },
        "model" : {
          "eviction_count" : 2,
          "miss_count" : 3,
          "entry_count" : 1,
          "memory_usage_in_bytes" : 3204,
          "hit_count" : 1
        }
      },
      "request_total_count" : 6,
      "request_error_count" : 0
    }
  }
}
```

As estatísticas são fornecidas em dois níveis, nó e cluster, conforme especificado nas seguintes tabelas:

Estatísticas em nível de nó

Nome do campo	Descrição
request_total_count	Contagem total de solicitações de classific ação.
request_error_count	Contagem total de solicitações malsucedidas.
cache	Estatísticas em todos os caches (recursos, conjuntos de recursos, modelos). Um acerto de cache ocorre quando um usuário consulta o plugin e o modelo já está carregado na memória.
cache.eviction_count	Número de remoções de cache.
cache.hit_count	Número de acertos de cache.
cache.miss_count	Número de perdas no cache. Uma perda de cache ocorre quando um usuário consulta o plugin e o modelo ainda não está carregado na memória.
cache.entry_count	Número de entradas no cache.
cache.memory_usage_in_bytes	Memória total usada em bytes.
cache.cache_capacity_reached	Indica se o limite de cache foi atingido.

Estatísticas em nível de cluster

Nome do campo	Descrição
stores	Indica onde os conjuntos de recursos e metadados de modelos são armazenados. (O padrão é “.ltrstore”. Caso contrário, é prefixado

Nome do campo	Descrição
	com “.ltrstore_”, mais um nome fornecido pelo usuário).
stores.status	O status do índice.
stores.feature_sets	Número de conjuntos de recursos.
stores.features_count	Número de recursos.
stores.model_count	Número de modelos.
status	O status do plugin baseado no status dos índices da feature store (vermelho, amarelo ou verde) e estado do disjuntor (aberto ou fechado).
cache.cache_capacity_reached	Indica se o limite de cache foi atingido.

Get cache stats (Obter estatísticas de cache)

Retorna estatísticas sobre o uso do cache e da memória.

```
GET _ltr/_cachestats

{
    "_nodes": {
        "total": 2,
        "successful": 2,
        "failed": 0
    },
    "cluster_name": "opensearch-cluster",
    "all": {
        "total": {
            "ram": 612,
            "count": 1
        },
        "features": {
            "ram": 0,
            "count": 0
```

```
        },
        "featuresets": {
            "ram": 612,
            "count": 1
        },
        "models": {
            "ram": 0,
            "count": 0
        }
    },
    "stores": {
        ".ltrstore": {
            "total": {
                "ram": 612,
                "count": 1
            },
            "features": {
                "ram": 0,
                "count": 0
            },
            "featuresets": {
                "ram": 612,
                "count": 1
            },
            "models": {
                "ram": 0,
                "count": 0
            }
        }
    },
    "nodes": {
        "ejF6uutERF20wOFNOXB61A": {
            "name": "opensearch1",
            "hostname": "172.18.0.4",
            "stats": {
                "total": {
                    "ram": 612,
                    "count": 1
                },
                "features": {
                    "ram": 0,
                    "count": 0
                },
                "featuresets": {
```

```
                    "ram": 612,
                    "count": 1
                },
                "models": {
                    "ram": 0,
                    "count": 0
                }
            }
        },
        "Z2RZNWRLSveVcz2c6lHf5A": {
            "name": "opensearch2",
            "hostname": "172.18.0.2",
            "stats": {
                ...
            }
        }
    }
}
```

Clear cache (Limpar cache)

Limpa o cache do plugin. Use esta opção para atualizar o modelo.

```
POST _ltr/_clearcache
```

Pesquisa assíncrona do Amazon OpenSearch Service

Com a pesquisa assíncrona do Amazon OpenSearch Service, você pode enviar uma consulta de pesquisa que é executada em segundo plano, monitorar o andamento da solicitação e recuperar os resultados em um estágio posterior. Você pode recuperar resultados parciais à medida que eles se tornam disponíveis antes da conclusão da pesquisa. Após a conclusão da pesquisa, salve os resultados para recuperação e análise posteriores.

A pesquisa assíncrona requer o OpenSearch 1.0 ou posterior ou o Elasticsearch 7.10 ou posterior. A documentação completa da pesquisa assíncrona, incluindo as etapas e descrições detalhadas da API, está disponível na documentação do OpenSearch.

Exemplo de chamada de pesquisa

Para executar uma pesquisa assíncrona, envie solicitações HTTP ao `_plugins/_asynchronous_search` usando o seguinte formato:

```
POST opensearch-domain/_plugins/_asynchronous_search
```

> **Note**
>
> Se você estiver usando o Elasticsearch 7.10 em vez de uma versão do OpenSearch, substitua `_plugins` por `_opendistro` em todas as solicitações de pesquisa assíncronas.

Também é possível especificar as seguintes opções de pesquisa assíncrona:

Opções	Descrição	Valor padrão	Obrigatório
`wait_for_completion_timeout`	Especifica o tempo que você planeja esperar pelos resultados. Você pode ver os resultados obtidos dentro deste tempo, assim como em uma pesquisa normal. Você pode consultar os resultados restantes com base em um ID. O valor máximo é 300 segundos.	1 segundo	Não
`keep_on_completion`	Especifica se você deseja salvar os resultados no cluster após a conclusão da pesquisa. Você poderá examinar os resultados armazenados mais tarde.	`false`	Não
`keep_alive`	Especifica por quanto tempo o resultado é salvo no cluster. Por exemplo, `2d` significa que os resultados são armazenados no cluster por 48 horas. Os resultados da pesquisa salvos serão excluídos após esse período ou se a pesquisa for cancelada. Observe que isso inclui o tempo de execução da consulta. Se a consulta ultrapassar este tempo, o processo cancelará a consulta automaticamente.	12 horas	Não

Exemplo de solicitação

```
POST _plugins/_asynchronous_search/?
pretty&size=10&wait_for_completion_timeout=1ms&keep_on_completion=true&request_cache=false
{
  "aggs": {
    "city": {
      "terms": {
        "field": "city",
        "size": 10
      }
    }
  }
}
```

> **Note**
>
> Todos os parâmetros de solicitação aplicáveis a uma consulta `_search` padrão são aceitos. Se você estiver usando o Elasticsearch 7.10 em vez de uma versão do OpenSearch, substitua `_plugins` por `_opendistro`.

Permissões da pesquisa assíncrona

A pesquisa assíncrona oferece suporte ao controle de acesso refinado. Para obter detalhes sobre combinação e correspondência de permissões para se adequar ao seu caso de uso, consulte Segurança da pesquisa assíncrona.

Para domínios com controle de acesso refinado habilitado, você precisa das seguintes permissões mínimas para uma função:

```
# Allows users to use all asynchronous search functionality
asynchronous_search_full_access:
  reserved: true
  cluster_permissions:
    - 'cluster:admin/opensearch/asynchronous-search/*'
  index_permissions:
    - index_patterns:
        - '*'
      allowed_actions:
        - 'indices:data/read/search*'

# Allows users to read stored asynchronous search results
```

```
asynchronous_search_read_access:
  reserved: true
  cluster_permissions:
    - 'cluster:admin/opensearch/asynchronous-search/get'
```

Para domínios com controle de acesso refinado desabilitado, use o acesso do IAM e a chave secreta para assinar todas as solicitações. Você pode acessar os resultados com o ID da pesquisa assíncrona.

Configurações da pesquisa assíncrona

O OpenSearch permite alterar todas as configurações da pesquisa assíncrona via API `_cluster/settings`. No OpenSearch Service, só é possível alterar as seguintes configurações:

- `plugins.asynchronous_search.node_concurrent_running_searches`
- `plugins.asynchronous_search.persist_search_failures`

Pesquisa entre clusters

Você pode executar uma pesquisa assíncrona em clusters com as seguintes limitações secundárias:

- Você pode executar uma pesquisa assíncrona somente no domínio de origem.
- Não é possível minimizar round trips de rede como parte de uma consulta de pesquisa entre clusters.

Se você configurar uma conexão entre `domain-a -> domain-b` com alias de conexão `cluster_b` e `domain-a -> domain-c` com alias de conexão `cluster_c`, `domain-a`, pesquise assincronamente `domain-b` e `domain-c` da seguinte forma:

```
POST https://src-domain.us-east-1.es.amazonaws.com/
local_index,cluster_b:b_index,cluster_c:c_index/_plugins/_asynchronous_search/?
pretty&size=10&wait_for_completion_timeout=500ms&keep_on_completion=true&request_cache=false
{
  "size": 0,
  "_source": {
    "excludes": []
  },
  "aggs": {
    "2": {
```

```
      "terms": {
        "field": "clientip",
        "size": 50,
        "order": {
          "_count": "desc"
        }
      }
    }
  },
  "stored_fields": [
    "*"
  ],
  "script_fields": {},
  "docvalue_fields": [
    "@timestamp"
  ],
  "query": {
    "bool": {
      "must": [
        {
          "query_string": {
            "query": "status:404",
            "analyze_wildcard": true,
            "default_field": "*"
          }
        },
        {
          "range": {
            "@timestamp": {
              "gte": 1483747200000,
              "lte": 1488326400000,
              "format": "epoch_millis"
            }
          }
        }
      ],
      "filter": [],
      "should": [],
      "must_not": []
    }
  }
}
```

Resposta

```
{
  "id" :
 "Fm9pYzJyVG91U19xb0hIQUJnMHJfRFEAAAAAAAAknghQ1OWVBczNZQjVEa2dMYTBXaTdEagAAAAAAAAAB",
  "state" : "RUNNING",
  "start_time_in_millis" : 1609329314796,
  "expiration_time_in_millis" : 1609761314796
}
```

Para obter mais informações, consulte the section called “Pesquisa entre clusters”.

UltraWarm

As pesquisas assíncronas com índices UltraWarm continuam funcionando. Para obter mais informações, consulte the section called “UltraWarm armazenamento”.

> **Note**
>
> Você pode monitorar estatísticas da pesquisa assíncrona no CloudWatch. Para obter uma lista completa de métricas, consulte the section called “Métricas de pesquisa assíncrona”.

Ponto de tempo no Amazon OpenSearch Service

O atributo point in time (PIT – um ponto no tempo) é um tipo de pesquisa que permite executar consultas diferentes em um conjunto de dados fixo no tempo. Normalmente, quando você executa a mesma consulta no mesmo índice em momentos diferentes, recebe resultados diferentes porque os documentos são constantemente indexados, atualizados e excluídos. Com o PIT, você pode consultar um estado constante do seu conjunto de dados.

O principal uso do atributo PIT é acoplá-lo à funcionalidade `search_after`. Esse é o método de paginação preferido no OpenSearch, especialmente para paginação profunda, porque opera em um conjunto de dados congelado no tempo, não está vinculado a uma consulta e oferece suporte à paginação consistente para frente e para trás. Você pode usar o PIT com o OpenSearch Service versão 2.5 e posterior.

Para obter mais informações sobre PIT, consulte Ponto de tempo na documentação do OpenSearch.

Considerações

Considere o seguinte ao configurar suas pesquisas com o PIT:

- Se você estiver fazendo o upgrade de um domínio 2.3 e precisar de um controle de acesso refinado nas ações do PIT, precisará adicionar essas ações e funções manualmente.
- Não há resiliência para o PIT. A reinicialização do nó, o encerramento do nó, as implantações em azul/verde e a reinicialização do processo ES fazem com que todos os dados do PIT sejam perdidos.
- Se um fragmento for realocado durante a implantação azul/verde, somente segmentos de dados ativos serão transferidos para o novo nó. Segmentos de fragmentos mantidos pelo PIT (tanto exclusivos quanto aqueles compartilhados com dados ativos) permanecem no nó antigo.
- Atualmente, as pesquisas com PIT não funcionam com a pesquisa assíncrona.

Criar um PIT

Para criar um PIT, envie solicitações HTTP para `_search/point_in_time` usando o seguinte formato:

```
POST opensearch-domain/my-index/_search/point_in_time?keep_alive=time
```

Você pode especificar as seguintes opções de PIT:

Opções	Descrição	Valor padrão	Obrigatório
`keep_alive`	A quantidade de tempo para manutenção do PIT. Toda vez que você acessa um PIT com uma solicitação de pesquisa, a vida útil do PIT é estendida pela quantidade de tempo igual ao parâmetro `keep_alive` . Esse parâmetro de consulta é obrigatório quando você cria um PIT, mas é opcional em uma solicitação de pesquisa.		Sim
`preference`	Uma string que especifica o nó ou o fragmento usado para realizar a pesquisa.	Aleatório	Não

Opções	Descrição	Valor padrão	Obrigatório
`routing`	Uma string que especifica o roteamento de solicitações de pesquisa para um fragmento específico.	O documento é `_id`	Não
`expand_wildcards`	Uma string que especifica o tipo de índice que pode corresponder ao padrão curinga. Suporta valores separados por vírgulas. Os valores válidos são os seguintes: • `all`: combine qualquer índice ou fluxo de dados, inclusive os ocultos. • `open`: combine índices abertos e não ocultos ou fluxos de dados não ocultos. • `closed`: combine índices fechados e não ocultos ou fluxos de dados não ocultos. • `hidden`: combine índices ou fluxos de dados ocultos. Deve ser combinado com aberto, fechado ou aberto e fechado. • `none`: nenhum padrão curinga é aceito.	`open`	Não
`allow_partial_pit_creation`	Um booleano que especifica se um PIT deve ser criado com falhas parciais.	`true`	Não

Exemplo de resposta

```
{
    "pit_id":
 "o463QQEPbXktaW5kZXgtMDAwMDAxFnNOWU43ckt3U3IyaFVpbGE1UWEtMncAFjFyeXBsRGJmVFM2RTB6eVg1aVVqQncAA
    "_shards": {
        "total": 1,
        "successful": 1,
        "skipped": 0,
        "failed": 0
    },
    "creation_time": 1658146050064
```

```
}
```

Ao criar um PIT, você recebe um PIT ID na resposta. Esse é o ID que você usa para realizar pesquisas com o PIT.

Permissões pontuais

O PIT é compatível com o controle de acesso detalhado. Se você estiver atualizando para um domínio 2.5 e precisar de um controle de acesso refinado, precisará criar funções manualmente com as seguintes permissões:

```
# Allows users to use all point in time search search functionality
point_in_time_full_access:
  reserved: true
  index_permissions:
    - index_patterns:
        - '*'
      allowed_actions:
        - "indices:data/read/point_in_time/create"
        - "indices:data/read/point_in_time/delete"
        - "indices:data/read/point_in_time/readall"
        - "indices:data/read/search"
        - "indices:monitor/point_in_time/segments"


# Allows users to use point in time search search functionality for specific index
# All type operations like list all PITs, delete all PITs are not supported in this
 case

point_in_time_index_access:
  reserved: true
  index_permissions:
    - index_patterns:
        - 'my-index-1'
      allowed_actions:
        - "indices:data/read/point_in_time/create"
        - "indices:data/read/point_in_time/delete"
        - "indices:data/read/search"
        - "indices:monitor/point_in_time/segments"
```

Para domínios com a versão 2.5 e superior, você pode usar a função integrada `point_in_time_full_access`. Para obter mais informações, consulte modelo de Segurança na documentação do OpenSearch.

Configurações do PIT

O OpenSearch permite alterar todas as configurações de PIT disponíveis via API `_cluster/settings`. No OpenSearch Service, atualmente não é possível modificar as configurações.

Pesquisa entre clusters

Você pode criar PITs, pesquisar com PIT IDs, listar PITs e excluir PITs em clusters com as pequenas limitações a seguir:

- Você pode listar todos e excluir todos os PITs somente no domínio de origem.
- Não é possível minimizar round trips de rede como parte de uma consulta de pesquisa entre clusters.

Para obter mais informações, consulte the section called “Pesquisa entre clusters”.

UltraWarm

O PIT faz buscas com índices UltraWarm continuam funcionando. Para obter mais informações, consulte the section called “UltraWarm armazenamento”.

> **Note**
>
> Você pode monitorar estatísticas da pesquisa PIT no CloudWatch. Para obter uma lista completa de métricas, consulte the section called “Métricas pontuais”.

Pesquisa semântica no Amazon Service OpenSearch

A partir da versão 2.9 do OpenSearch Service, você pode usar a pesquisa semântica para ajudá-lo a entender as consultas de pesquisa e melhorar a relevância da pesquisa. Você pode usar a pesquisa semântica de duas maneiras: com a pesquisa neural e com o k-NN.

Com o OpenSearch Serviço, você pode configurar conectores de IA para Serviços da AWS serviços externos. Usando o console do, você também pode criar um modelo de ML com um exemplo AWS

CloudFormation. Para ter mais informações, consulte the section called “CloudFormation integrações de modelos”.

Usando OpenSearch painéis com o Amazon Service OpenSearch

OpenSearch O Dashboards é uma ferramenta de visualização de código aberto projetada para trabalhar com. OpenSearch O Amazon OpenSearch Service fornece uma instalação de OpenSearch painéis com cada domínio do OpenSearch serviço.

Você pode encontrar um link para OpenSearch painéis no painel do seu domínio no console OpenSearch de serviços. Para domínios em execução OpenSearch, o URL é*domain-endpoint*/_dashboards/. Para domínios que executam o Elasticsearch legado, a URL é. *domain-endpoint*/_plugin/kibana

As consultas que usam essa instalação padrão do OpenSearch Dashboards têm um tempo limite de 300 segundos.

As seções a seguir abordam alguns casos de uso comuns de OpenSearch painéis:

- the section called “Controle do acesso aos OpenSearch painéis”
- the section called “Configurando OpenSearch painéis para usar um servidor de mapas WMS”
- the section called “Conectando um servidor local de painéis ao serviço OpenSearch ”

Controle do acesso aos OpenSearch painéis

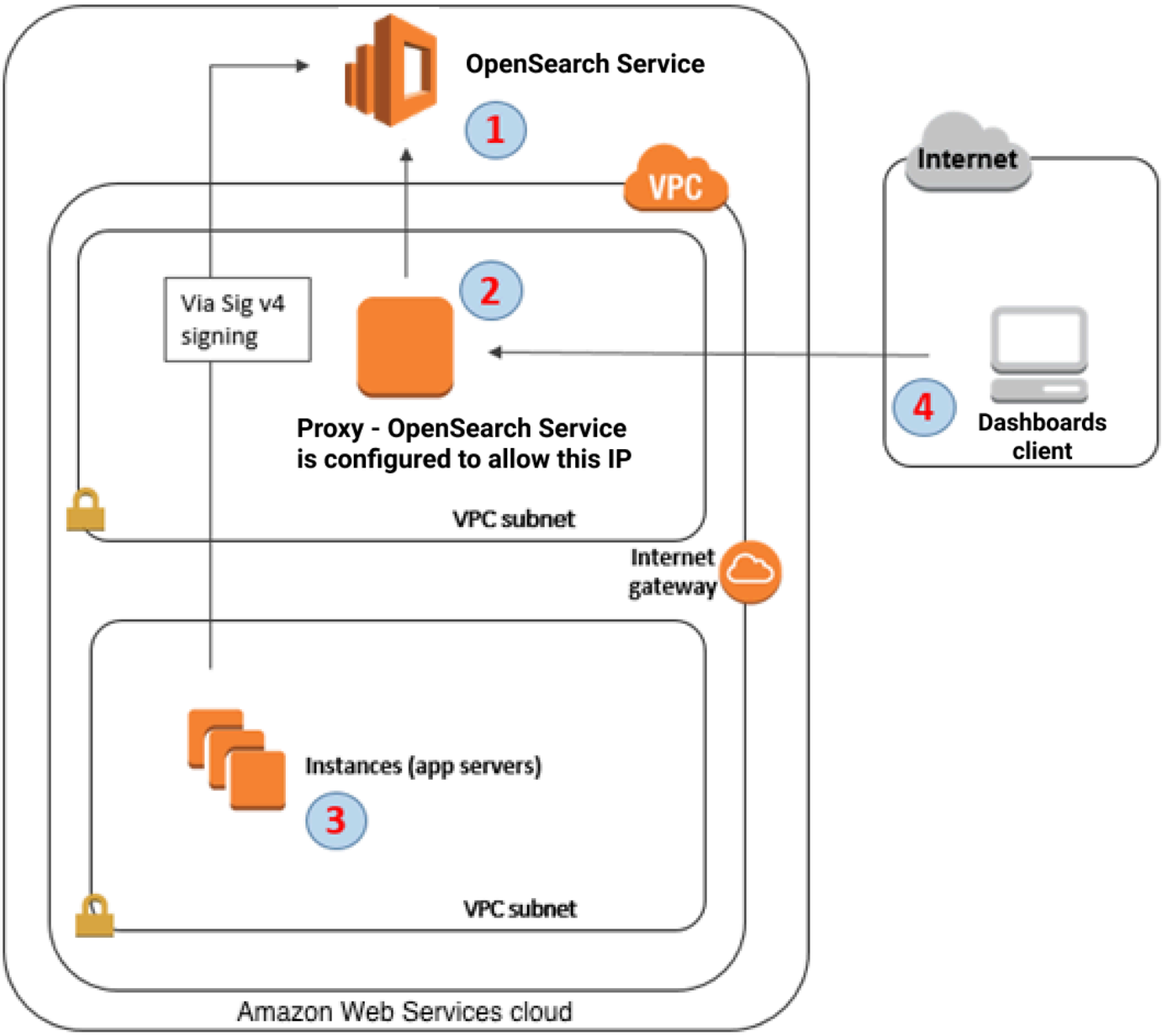
Os painéis não oferecem suporte nativo a usuários e funções do IAM, mas o OpenSearch Service oferece várias soluções para controlar o acesso aos painéis:

- Habilitar a Autenticação SAML para Dashboards.
- Usar o controle de acesso refinado com a autenticação básica HTTP.
- Configure a Autenticação do Cognito para painéis.
- Para domínios de acesso público, configure uma política de acesso baseada em IP que use ou não um servidor de proxy.
- Para domínios de acesso VPC, use uma política de acesso aberto que use ou não use um servidor de proxy e grupos de segurança para controlar o acesso. Para saber mais, consulte the section called “Sobre políticas de acesso em domínios da VPC”.

Usando um proxy para acessar o OpenSearch serviço a partir de OpenSearch painéis

> **Note**
>
> Esse processo só será aplicável se o domínio usar acesso público e você não quiser usar a autenticação do Cognito. Consulte the section called “Controle do acesso aos OpenSearch painéis”.

Como o Dashboards é um JavaScript aplicativo, as solicitações se originam do endereço IP do usuário. O controle de acesso baseado em IP pode ser impraticável devido ao grande número de endereços IP que você precisaria inserir em uma lista de permissões para que cada usuário tivesse acesso ao Dashboards. Uma solução alternativa é colocar um servidor proxy entre os OpenSearch painéis e OpenSearch o serviço. Em seguida, você pode adicionar uma política de acesso com base em IP que permite solicitações de apenas um endereço IP, o do proxy. O diagrama a seguir mostra essa configuração.



1. Esse é o seu domínio OpenSearch de serviço. O IAM fornece acesso autorizado para este domínio. Uma política de acesso adicional com base em IP fornece acesso ao servidor de proxy.
2. Este é o servidor de proxy, em execução em uma instância do Amazon EC2.
3. Outros aplicativos podem usar o processo de assinatura Signature Version 4 para enviar solicitações autenticadas ao OpenSearch Serviço.
4. OpenSearch Os clientes do Dashboards se conectam ao seu domínio OpenSearch de serviço por meio do proxy.

Para habilitar esse tipo de configuração, você precisa de uma política com base em recursos que especifica funções e endereços IP. Aqui está um exemplo de política:

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Resource": "arn:aws:es:us-west-2:111111111111:domain/my-domain/*",
      "Principal": {
        "AWS": "arn:aws:iam::111111111111:role/allowedrole1"
      },
      "Action": [
        "es:ESHttpGet"
      ],
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": [
            "123.456.789.123"
          ]
        }
      },
      "Resource": "arn:aws:es:us-west-2:111111111111:domain/my-domain/*"
    }
  ]
}
```

Recomendamos configurar a instância do EC2 executando o servidor de proxy com um endereço IP elástico. Dessa forma, você pode substituir a instância quando necessário e ainda anexar o mesmo endereço IP público. Para saber mais, consulte Endereços IP elásticos no Manual do usuário do Amazon EC2 para instâncias do Linux.

Se você usar um servidor de proxy e a autenticação do Cognito, talvez seja necessário adicionar configurações do Dashboards e do Amazon Cognito para evitar erros de `redirect_mismatch`. Veja o exemplo `nginx.conf` a seguir:

```
server {
    listen 443;
    server_name $host;
    rewrite ^/$ https://$host/_plugin/_dashboards redirect;

    ssl_certificate          /etc/nginx/cert.crt;
    ssl_certificate_key      /etc/nginx/cert.key;

    ssl on;
    ssl_session_cache  builtin:1000  shared:SSL:10m;
    ssl_protocols  TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers HIGH:!aNULL:!eNULL:!EXPORT:!CAMELLIA:!DES:!MD5:!PSK:!RC4;
    ssl_prefer_server_ciphers on;

    location /_plugin/_dashboards {
        # Forward requests to Dashboards
        proxy_pass https://$dashboards_host/_plugin/_dashboards;

        # Handle redirects to Cognito
        proxy_redirect https://$cognito_host https://$host;

        # Update cookie domain and path
        proxy_cookie_domain $dashboards_host $host;
        proxy_cookie_path / /_plugin/_dashboards/;

        # Response buffer settings
        proxy_buffer_size 128k;
        proxy_buffers 4 256k;
        proxy_busy_buffers_size 256k;
    }

    location ~ \/(log|sign|fav|forgot|change|saml|oauth2) {
        # Forward requests to Cognito
        proxy_pass https://$cognito_host;

        # Handle redirects to Dashboards
        proxy_redirect https://$dashboards_host https://$host;

        # Update cookie domain
        proxy_cookie_domain $cognito_host $host;
    }
}
```

Configurando OpenSearch painéis para usar um servidor de mapas WMS

A instalação padrão do OpenSearch Dashboards for OpenSearch Service inclui um serviço de mapas, exceto para domínios nas regiões da Índia e da China. O serviço de mapa oferece suporte a até 10 níveis de zoom.

Independentemente da sua região, é possível configurar o Dashboards para usar um servidor diferente do Web Map Service (WMS) para coordenar visualizações de mapas. As visualizações de mapa de região oferecem suporte apenas ao serviço de mapa padrão.

Para configurar o Dashboards para usar um servidor de mapas WMS:

1. Abra o Dashboards.
2. Escolha Stack Management (Gerenciamento de pilhas).
3. Escolha Advanced Settings.
4. Localize visualization:tileMap:WMSdefaults.
5. Altere `enabled` para `true` e `url` para o URL de um servidor de mapas WMS válido:

```
{
  "enabled": true,
  "url": "wms-server-url",
  "options": {
    "format": "image/png",
    "transparent": true
  }
}
```

6. Escolha Salvar alterações.

Para aplicar o novo valor padrão a visualizações, talvez seja necessário recarregar o Dashboards. Se você salvou as visualizações, selecione Opções depois de abrir a visualização. Verifique se o Servidor de mapas WMS está habilitado e se o URL do WMS contém o servidor de mapas de sua preferência e selecione Aplicar alterações.

> **Note**
>
> Os serviços de mapa costumam ter taxas ou restrições de licenciamento. Você será responsável por todos esses fatores em qualquer servidor de mapas que especificar. Você pode encontrar os serviços de mapa em U.S. Geological Survey, útil para testes.

Conectando um servidor local de painéis ao serviço OpenSearch

Se você já investiu um tempo significativo na configuração de sua própria instância de OpenSearch Dashboards, você pode usá-la em vez (ou além) da instância de Dashboards padrão que OpenSearch o Service fornece. O procedimento a seguir destina-se a domínios que usam o controle de acesso refinado com uma política de acesso aberto.

Para conectar um servidor local do OpenSearch Dashboards ao Serviço OpenSearch

1. No seu domínio OpenSearch de serviço, crie um usuário com as permissões apropriadas:
   a. No Dashboards, vá para Security (Segurança), Internal users (Usuários internos) e escolhaCreate internal user (Criar usuário interno).
   b. Forneça um nome de usuário e uma senha e escolha Create (Criar).
   c. Vá para Roles (Funções) e selecione uma função.
   d. Selecione Mapped users (Usuários mapeados) e escolha Manage mapping (Gerenciar mapeamento).
   e. Em Users (Usuários), adicione seu nome de usuário e escolha Map (Mapa).
2. Baixe e instale a versão apropriada do plug-in de OpenSearch segurança em sua instalação autogerenciada do Dashboards OSS.
3. No servidor local do Dashboards, abra o `config/opensearch_dashboards.yml` arquivo e adicione seu endpoint de OpenSearch serviço com o nome de usuário e a senha que você criou anteriormente:

   ```
   opensearch.hosts: ['https://domain-endpoint']
   opensearch.username: 'username'
   opensearch.password: 'password'
   ```

   Você pode usar seguinte arquivo `opensearch_dashboards.yml` de exemplo:

```
server.host: '0.0.0.0'

opensearch.hosts: ['https://domain-endpoint']

opensearch_dashboards.index: ".username"

opensearch.ssl.verificationMode: none # if not using HTTPS

opensearch_security.auth.type: basicauth
opensearch_security.auth.anonymous_auth_enabled: false
opensearch_security.cookie.secure: false # set to true when using HTTPS
opensearch_security.cookie.ttl: 3600000
opensearch_security.session.ttl: 3600000
opensearch_security.session.keepalive: false
opensearch_security.multitenancy.enabled: false
opensearch_security.readonly_mode.roles: ['opensearch_dashboards_read_only']
opensearch_security.auth.unauthenticated_routes: []
opensearch_security.basicauth.login.title: 'Please log in using your username and
 password'

opensearch.username: 'username'
opensearch.password: 'password'
opensearch.requestHeadersWhitelist:
[
authorization,
securitytenant,
security_tenant,
]
```

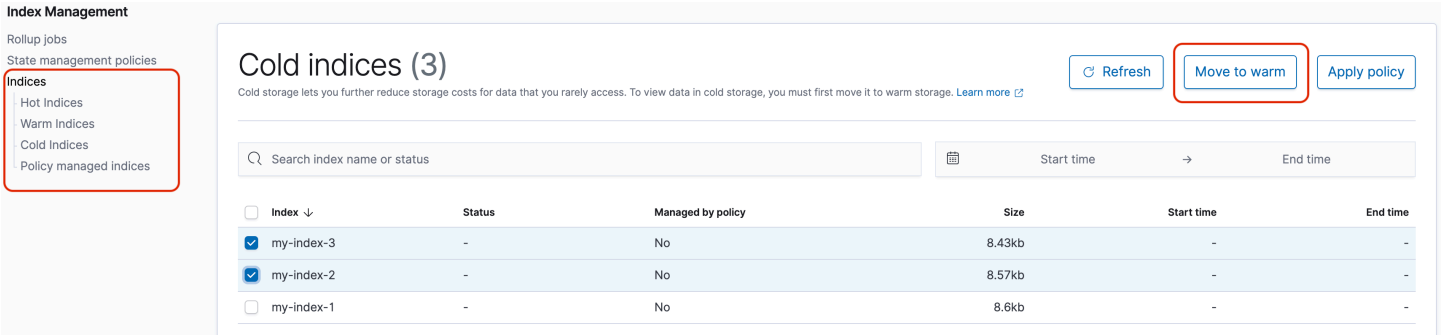
Para ver seus índices OpenSearch de serviço, inicie seu servidor local de painéis, acesse Dev Tools e execute o seguinte comando:

```
GET _cat/indices
```

Gerenciando índices em painéis OpenSearch

A instalação do OpenSearch Dashboards em seu domínio OpenSearch de serviço fornece uma interface de usuário útil para gerenciar índices em diferentes níveis de armazenamento em seu domínio. Escolha Gerenciamento de índices no menu principal dos painéis para visualizar todos

os índices em armazenamento quente e refrigerado UltraWarm, bem como os índices gerenciados pelas políticas do Index State Management (ISM). Use o gerenciamento de índices para mover índices entre os armazenamentos mornos e frios, e para monitorar migrações entre os três níveis.



Observe que você não verá as opções de índice de quente, quente e frio, a menos que tenha o armazenamento a frio UltraWarm e/ou o armazenamento a frio ativado.

Recursos adicionais

A instalação padrão do OpenSearch Dashboards em cada domínio do OpenSearch Serviço tem alguns recursos adicionais:

- Interfaces de usuário para os vários OpenSearchplug-ins
- Locatários
- Relatórios

  Use o menu Reports (Relatórios) para gerar relatórios CSV sob demanda na página Discover (Descobrir) e relatórios PDF ou PNG de painéis ou visualizações. Os relatórios CSV têm um limite de 10.000 linhas.
- Gráficos de Gantt
- Cadernos

Gerenciamento de índices no Amazon OpenSearch Service

Depois de adicionar dados ao Amazon OpenSearch Service, muitas vezes é necessário reindexar esses dados, trabalhar com aliases de índice, mover um índice para um armazenamento mais econômico ou excluí-lo completamente. Este capítulo aborda armazenamento UltraWarm, armazenamento de baixa atividade e Gerenciamento de estados de índices. Para obter informações sobre as APIs de índice do OpenSearch, consulte a documentação do OpenSearch.

Tópicos

UltraWarm armazenamento para Amazon OpenSearch Service

UltraWarm fornece uma maneira econômica de armazenar grandes quantidades de dados somente para leitura no Amazon Service. OpenSearch Os nós de dados padrão usam o armazenamento de atividade muito alta, o qual assume a forma de armazenamentos de instâncias ou volumes do Amazon EBS anexados a cada nó. O armazenamento de atividade muito alta fornece a performance mais rápida possível para indexar e pesquisar novos dados.

Em vez de armazenamento conectado, UltraWarm os nós usam o Amazon S3 e uma solução de cache sofisticada para melhorar o desempenho. Para índices nos quais você não está gravando ativamente, consultar com menos frequência e dos quais não precisa do mesmo desempenho UltraWarm oferece custos significativamente mais baixos por GiB de dados. Como os índices quentes são somente para leitura, a menos que você os devolva ao armazenamento ativo, UltraWarm é mais adequado para dados imutáveis, como registros.

Em OpenSearch, os índices quentes se comportam como qualquer outro índice. Você pode consultá-las usando as mesmas APIs ou usá-las para criar visualizações em OpenSearch painéis.

Tópicos

Pré-requisitos

UltraWarm tem alguns pré-requisitos importantes:

- UltraWarm requer o Elasticsearch 6.8 OpenSearch ou superior.
- Para usar o armazenamento de alta atividade (warm), os domínios devem ter nós principais dedicados.
- Se o domínio usar um tipo de instância T2 ou T3 para os nós de dados, não será possível usar o armazenamento de alta atividade.
- Se seu índice usa codecs de compressão Zstandard (`"index.codec": "zstd"`ou`"index.codec": "zstd_no_dict"`), você não pode movê-lo para um armazenamento de alta atividade.
- Se o índice usar aproximação de k-NN (`"index.knn": true`), você não pode movê-lo para o armazenamento de alta atividade.

- Se o domínio usa controle de acesso refinado, os usuários devem ser mapeados para a `ultrawarm_manager` função nos OpenSearch painéis para fazer chamadas de API. UltraWarm

> **Note**
>
> A `ultrawarm_manager` função pode não estar definida em alguns domínios de OpenSearch serviço preexistentes. Se você não vir a função no Dashboards, será necessário criá-la manualmente.

Configurar permissões

Se você habilitar UltraWarm em um domínio OpenSearch de serviço preexistente, a `ultrawarm_manager` função pode não estar definida no domínio. Os usuários não administradores deverão ser mapeados nessa função para poderem gerenciar índices warm usando o controle de aceso detalhado. Para criar manualmente a função `ultrawarm_manager`, faça o seguinte:

1. Em OpenSearch Painéis, acesse Segurança e escolha Permissões.
2. Escolha Criar grupo de ações e configure os seguintes grupos:

Group name	Permissões
`ultrawarm_cluster`	• `cluster:admin/ultrawarm/migration/list` • `cluster:monitor/nodes/stats`
`ultrawarm_index_read`	• `indices:admin/ultrawarm/migration/get` • `indices:admin/get`
`ultrawarm_index_write`	• `indices:admin/ultrawarm/migration/warm` • `indices:admin/ultrawarm/migration/hot` • `indices:monitor/stats` • `indices:admin/ultrawarm/migration/cancel`

3. Escolha Funções e, em seguida, Criar função.
4. Nomeie a função como ultrawarm_manager.
5. Para Permissões de cluster, selecione `ultrawarm_cluster` e `cluster_monitor`.

6. Para Índice, digite `*`.
7. Para Permissões de índice, selecione `ultrawarm_index_read`, `ultrawarm_index_write`, e `indices_monitor`.
8. Escolha Criar.
9. Depois de criar a função, mapeie-a para qualquer função de usuário ou back-end que gerenciará UltraWarm índices.

UltraWarm requisitos de armazenamento e considerações de desempenho

Conforme abordado emthe section called “Cálculo de requisitos de armazenamento”, os dados no armazenamento dinâmico geram uma sobrecarga significativa: réplicas, espaço reservado do Linux e espaço reservado do OpenSearch serviço. Por exemplo, um fragmento primário de 20 GiB com um fragmento de réplica requer aproximadamente 58 GiB de armazenamento de atividade muito alta.

Como ele usa o Amazon S3, não UltraWarm incorre em nenhuma dessas despesas gerais. Ao calcular os requisitos UltraWarm de armazenamento, você considera somente o tamanho dos fragmentos primários. A durabilidade dos dados no S3 elimina a necessidade de réplicas e o S3 abstrai qualquer consideração de sistema operacional ou de serviço. Esse mesmo fragmento de 20 GiB exige 20 GiB de armazenamento de alta atividade. Se você provisionar uma instância `ultrawarm1.large.search`, poderá usar todos os 20 TiB de seu armazenamento máximo para fragmentos primários. Consulte the section called “UltraWarm cotas de armazenamento” para obter um resumo dos tipos de instância e a quantidade máxima de armazenamento que cada um pode atender.

Com UltraWarm, ainda recomendamos um tamanho máximo de fragmento de 50 GiB. O número de núcleos de CPU e a quantidade de RAM alocada para cada tipo de UltraWarm instância dão uma ideia do número de fragmentos que eles podem pesquisar simultaneamente. Observe que, embora apenas os fragmentos primários contem para o UltraWarm armazenamento no S3, os OpenSearch painéis `_cat/indices` ainda relatam o tamanho do UltraWarm índice como o total de todos os fragmentos primários e de réplica.

Por exemplo, cada instância de `ultrawarm1.medium.search` tem dois núcleos de CPU e pode endereçar até 1,5 TiB de armazenamento no S3. Duas dessas instâncias têm uma combinação de 3 TiB de armazenamento, o que funcionará para aproximadamente 62 fragmentos se o tamanho de cada fragmento for 50 GiB. Se uma solicitação para o cluster pesquisar apenas quatro desses fragmentos, a performance poderá ser excelente. Se a solicitação for ampla e pesquisar todos os 62, os quatro núcleos da CPU poderão ter dificuldade para executar a operação. Monitore as

`WarmJVMMemoryPressure` UltraWarm métricas `WarmCPUUtilization` e para entender como as instâncias lidam com suas cargas de trabalho.

Se as suas pesquisas forem amplas ou frequentes, considere deixar os índices no armazenamento quente. Assim como qualquer outra OpenSearch carga de trabalho, a etapa mais importante para determinar se UltraWarm atende às suas necessidades é realizar testes representativos do cliente usando um conjunto de dados realista.

UltraWarm preços

Com o armazenamento de alta atividade, você paga pelo que provisiona. Algumas instâncias exigem um volume do Amazon EBS vinculado, enquanto outras incluem um armazenamento de instâncias. Se esse armazenamento estiver vazio ou cheio, você pagará o mesmo preço.

Com o UltraWarm armazenamento, você paga pelo que usa. Uma instância `ultrawarm1.large.search` pode processar até 20 TiB de armazenamento no S3, mas se você armazenar apenas 1 TiB de dados, será cobrado somente por 1 TiB de dados. Como todos os outros tipos de nós, você também paga uma taxa horária por cada UltraWarm nó. Para ter mais informações, consulte the section called “Preços do Amazon OpenSearch Service”.

Habilitando UltraWarm

O console é a maneira mais simples de criar um domínio que usa o armazenamento de alta atividade. Ao criar o domínio, escolha Habilitar nós de UltraWarm dados e o número de nós quentes que você deseja. O mesmo processo básico funciona em domínios existentes, desde que eles atendam aos pré-requisitos. Mesmo depois que o estado do domínio mudar de Processamento para Ativo, UltraWarm pode não estar disponível para uso por várias horas.

Você também pode usar a API de configuração AWS CLIou para habilitar UltraWarm, especificamente`WarmEnabled`, as `WarmType` opções`WarmCount`, e em`ClusterConfig`.

> **Note**
>
> Os domínios oferecem suporte a um número máximo de nós de alta atividade. Para obter detalhes, consulte the section called “Cotas”.

Exemplo de comando da CLI

Os seguinte comando AWS CLI cria um domínio com três nós de dados, três nós principais dedicados, seis nos de alta atividade e controle de acesso refinado habilitado:

```
aws opensearch create-domain \
  --domain-name my-domain \
  --engine-version Opensearch_1.0 \
  --cluster-config
 InstanceCount=3,InstanceType=r6g.large.search,DedicatedMasterEnabled=true,DedicatedMasterType=
 \
  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=11 \
  --node-to-node-encryption-options Enabled=true \
  --encryption-at-rest-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true,TLSSecurityPolicy=Policy-Min-
TLS-1-2-2019-07 \
  --advanced-security-options
 Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions='{MasterUserName=master-
user,MasterUserPassword=master-password}' \
  --access-policies '{"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":{"AWS":["123456789012"]},"Action":
["es:*"],"Resource":"arn:aws:es:us-west-1:123456789012:domain/my-domain/*"}]}' \
  --region us-east-1
```

Para obter mais informações, consulte a Referência de comandos da AWS CLI.

Exemplo de solicitação da API de configuração

A solicitação a seguir à API de configuração cria um domínio com três nós de dados, três nós principais dedicados e seis nós de alta atividade com o controle de acesso refinado habilitado e uma política de acesso restritiva:

```
POST https://es.us-east-2.amazonaws.com/2021-01-01/opensearch/domain
{
  "ClusterConfig": {
    "InstanceCount": 3,
    "InstanceType": "r6g.large.search",
    "DedicatedMasterEnabled": true,
    "DedicatedMasterType": "r6g.large.search",
    "DedicatedMasterCount": 3,
    "ZoneAwarenessEnabled": true,
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": 3
```

```
    },
    "WarmEnabled": true,
    "WarmCount": 6,
    "WarmType": "ultrawarm1.medium.search"
  },
  "EBSOptions": {
    "EBSEnabled": true,
    "VolumeType": "gp2",
    "VolumeSize": 11
  },
  "EncryptionAtRestOptions": {
    "Enabled": true
  },
  "NodeToNodeEncryptionOptions": {
    "Enabled": true
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": true,
    "TLSSecurityPolicy": "Policy-Min-TLS-1-2-2019-07"
  },
   "AdvancedSecurityOptions": {
    "Enabled": true,
    "InternalUserDatabaseEnabled": true,
    "MasterUserOptions": {
      "MasterUserName": "master-user",
      "MasterUserPassword": "master-password"
    }
  },
  "EngineVersion": "Opensearch_1.0",
  "DomainName": "my-domain",
  "AccessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"123456789012\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:us-east-1:123456789012:domain/my-domain/*\"}]}"
}
```

Para obter informações detalhadas, consulte a Amazon OpenSearch Service API Reference.

Migração de índices para armazenamento UltraWarm

Se você terminou de escrever em um índice e não precisa mais do desempenho de pesquisa mais rápido possível, migre-o de hot para UltraWarm:

```
POST _ultrawarm/migration/my-index/_warm
```

Depois, verifique o status da migração:

```
GET _ultrawarm/migration/my-index/_status

{
  "migration_status": {
    "index": "my-index",
    "state": "RUNNING_SHARD_RELOCATION",
    "migration_type": "HOT_TO_WARM",
    "shard_level_status": {
      "running": 0,
      "total": 5,
      "pending": 3,
      "failed": 0,
      "succeeded": 2
    }
  }
}
```

A integridade do índice deve ser verde para que seja possível executar uma migração. Se você migrar vários índices em sucessão rápida, poderá obter um resumo de todas as migrações em texto não criptografado, semelhante à API `_cat`:

```
GET _ultrawarm/migration/_status?v

index    migration_type state
my-index HOT_TO_WARM    RUNNING_SHARD_RELOCATION
```

OpenSearch O serviço migra um índice por vez para o. UltraWarm É possível ter até 200 migrações na fila. Qualquer solicitação que exceda o limite será rejeitada. Para verificar o número de migrações atual, monitore a métrica `HotToWarmMigrationQueueSize`. Os índices permanecem disponíveis durante todo o processo de migração, sem tempo de inatividade.

O processo de migração tem os seguintes estados:

```
PENDING_INCREMENTAL_SNAPSHOT
RUNNING_INCREMENTAL_SNAPSHOT
FAILED_INCREMENTAL_SNAPSHOT
PENDING_FORCE_MERGE
RUNNING_FORCE_MERGE
FAILED_FORCE_MERGE
```

```
PENDING_FULL_SNAPSHOT
RUNNING_FULL_SNAPSHOT
FAILED_FULL_SNAPSHOT
PENDING_SHARD_RELOCATION
RUNNING_SHARD_RELOCATION
FINISHED_SHARD_RELOCATION
```

Como esses estados indicam, as migrações podem falhar durante os snapshots, as realocações de fragmentos ou as uniões de força. As falhas durante os snapshots ou as realocações de fragmentos geralmente ocorrem devido a falhas de nós ou a problemas de conectividade do S3. A falta de espaço em disco geralmente é a causa subjacente das falhas de união de força.

Após o término da migração, a mesma solicitação `_status` retornará um erro. Se você verificar o índice nesse momento, verá algumas configurações exclusivas dos índices mornos:

```
GET my-index/_settings

{
  "my-index": {
    "settings": {
      "index": {
        "refresh_interval": "-1",
        "auto_expand_replicas": "false",
        "provided_name": "my-index",
        "creation_date": "1599241458998",
        "unassigned": {
          "node_left": {
            "delayed_timeout": "5m"
          }
        },
        "number_of_replicas": "1",
        "uuid": "GswyCdR0RSq0SJYmzsIpiw",
        "version": {
          "created": "7070099"
        },
        "routing": {
          "allocation": {
            "require": {
              "box_type": "warm"
            }
          }
        },
        "number_of_shards": "5",
```

```
        "merge": {
          "policy": {
            "max_merge_at_once_explicit": "50"
          }
        }
      }
    }
  }
}
```

- `number_of_replicas`, nesse caso, é o número de réplicas passivas, que não consomem espaço em disco.
- `routing.allocation.require.box_type` especifica que o índice deve usar nós de alta atividade em vez de nós de dados padrão.
- `merge.policy.max_merge_at_once_explicit` especifica o número de segmentos a serem mesclados simultaneamente durante a migração.

Os índices no armazenamento quente são somente para leitura, a menos que você os retorne ao armazenamento ativo, o que os torna UltraWarm mais adequados para dados imutáveis, como registros. Você pode consultar os índices e excluí-los, mas não pode adicionar, atualizar ou excluir documentos individuais. Se tentar, você poderá encontrar a seguinte mensagem de erro:

```
{
  "error" : {
    "root_cause" : [
      {
        "type" : "cluster_block_exception",
        "reason" : "index [indexname] blocked by: [TOO_MANY_REQUESTS/12/disk usage
 exceeded flood-stage watermark, index has read-only-allow-delete block];"
      }
    ],
    "type" : "cluster_block_exception",
    "reason" : "index [indexname] blocked by: [TOO_MANY_REQUESTS/12/disk usage exceeded
 flood-stage watermark, index has read-only-allow-delete block];"
  },
  "status" : 429
}
```

Automatização de migrações

Recomendamos usar the section called “Gerenciamento de estados de índice” para automatizar o processo de migração depois que um índice atinge uma determinada idade ou atende a outras condições. Consulte a política de exemplo que demonstra este fluxo de trabalho.

Ajuste de migrações

As migrações de índice para o UltraWarm armazenamento exigem uma mesclagem forçada. Cada OpenSearch índice é composto por um certo número de fragmentos, e cada fragmento é composto por algum número de segmentos do Lucene. A operação de forças mesclagem expurga documentos que foram marcados para exclusão e conserva espaço em disco. Por padrão, UltraWarm mescla índices em um segmento.

Você pode alterar esse valor para até 1.000 segmentos usando a configuração `index.ultrawarm.migration.force_merge.max_num_segments`. Valores mais altos aceleram o processo de migração, mas aumentam a latência de consulta para o índice de alta atividade após a conclusão da migração. Para alterar a configuração, faça a seguinte solicitação:

```
PUT my-index/_settings
{
  "index": {
    "ultrawarm": {
      "migration": {
        "force_merge": {
          "max_num_segments": 1
        }
      }
    }
  }
}
```

Para verificar a duração desse estágio do processo de migração, monitore a métrica `HotToWarmMigrationForceMergeLatency`.

Cancelamento de migrações

UltraWarm lida com migrações sequencialmente, em uma fila. Se uma migração estiver na fila, mas ainda não tiver sido iniciada, você poderá removê-la da fila usando a seguinte solicitação:

```
POST _ultrawarm/migration/_cancel/my-index
```

Se o domínio usa controle de acesso refinado, você precisará da permissão `indices:admin/ultrawarm/migration/cancel` para fazer essa solicitação.

Listagem de índices quentes e mornos

UltraWarm adiciona duas opções adicionais, semelhantes a`_all`, para ajudar a gerenciar índices quentes e quentes. Para obter uma lista de todos os índices mornos ou quentes, faça as seguintes solicitações:

```
GET _warm
GET _hot
```

Você pode usar essas opções em outras solicitações que especificam índices, como:

```
_cat/indices/_warm
_cluster/state/_all/_hot
```

Retorno de índices warm para o armazenamento quente

Se você precisar gravar em um índice novamente, migre-o de volta para o armazenamento de atividade muito alta:

```
POST _ultrawarm/migration/my-index/_hot
```

Você pode ter até 10 migrações em fila do armazenamento quente para o armazenamento quente por vez. OpenSearch O serviço processa as solicitações de migração uma de cada vez, na ordem em que foram colocadas na fila. Para verificar o número atual, monitore a `WarmToHotMigrationQueueSize` métrica.

Após a conclusão da migração, verifique as configurações de índice para garantir que atendam às suas necessidades. Os índices retornam ao armazenamento quente com uma réplica.

Restauração de índices quentes de snapshots

Além do repositório padrão para instantâneos automatizados, UltraWarm adiciona um segundo repositório para índices quentes,. `cs-ultrawarm` Cada snapshot neste repositório contém apenas

um índice. Se você excluir um índice de alta atividade, seu instantâneo permanecerá no repositório `cs-ultrawarm` por 14 dias, assim como qualquer outro snapshot automatizado.

Quando você restaura um snapshot de `cs-ultrawarm`, ele é restaurado no armazenamento de alta atividade (warm), não no armazenamento de atividade muito alta (hot). Os snapshots nos repositórios `cs-automated` e `cs-automated-enc` são restaurados no armazenamento de atividade muito alta.

Para restaurar um UltraWarm instantâneo para um armazenamento aquecido

1. Identifique o snapshot mais recente que contém o índice que você deseja restaurar:

```
GET _snapshot/cs-ultrawarm/_all?verbose=false

{
  "snapshots": [{
    "snapshot": "snapshot-name",
    "version": "1.0",
    "indices": [
      "my-index"
    ]
  }]
}
```

> **Note**
>
> Por padrão, a operação `GET _snapshot/<repo>` exibe informações detalhadas de dados, como hora de início, hora de término e duração de cada instantâneo em um repositório. A operação `GET _snapshot/<repo>` recupera informações dos arquivos de cada instantâneo contido em um repositório. Se você não precisar do horário de início, horário de término e duração e precisar apenas do nome e das informações de índice de um snapshot, recomendamos usar o parâmetro `verbose=false` ao listar snapshots para minimizar o tempo de processamento e evitar o tempo limite.

2. Se o índice já existir, exclua-o:

```
DELETE my-index
```

Se não quiser excluir o índice, devolva-o ao armazenamento de atividade muito alta e reindexe-o.

3. Restaure o snapshot:

```
POST _snapshot/cs-ultrawarm/snapshot-name/_restore
```

UltraWarm ignora todas as configurações de índice que você especificar nessa solicitação de restauração, mas você pode especificar opções como `rename_pattern` e. `rename_replacement` Para obter um resumo das opções de restauração de OpenSearch instantâneos, consulte a OpenSearch documentação.

Snapshots manuais de índices mornos

Você pode obter snapshots manuais de índices mornos, mas não recomendamos fazer isso. O repositório `cs-ultrawarm` automatizado já contém um snapshot para cada índice de alta atividade, obtido durante a migração, sem custo adicional.

Por padrão, o OpenSearch Serviço não inclui índices quentes em instantâneos manuais. Por exemplo, a chamada a seguir inclui apenas índices quentes:

```
PUT _snapshot/my-repository/my-snapshot
```

Se você optar por obter snapshots manuais de índices mornos, diversas considerações importantes serão aplicáveis.

- Você não pode misturar índices quentes e mornos. Por exemplo, a solicitação a seguir falha:

```
PUT _snapshot/my-repository/my-snapshot
{
  "indices": "warm-index-1,hot-index-1",
  "include_global_state": false
}
```

  Se eles incluírem uma mistura de índices quentes e mornos, as instruções universais (*) também falharão.
- Você só pode incluir um índice de alta atividade por snapshot. Por exemplo, a solicitação a seguir falha:

```
PUT _snapshot/my-repository/my-snapshot
{
  "indices": "warm-index-1,warm-index-2,other-warm-indices-*",
  "include_global_state": false
}
```

Esta solicitação é bem-sucedida:

```
PUT _snapshot/my-repository/my-snapshot
{
  "indices": "warm-index-1",
  "include_global_state": false
}
```

- Os snapshots manuais são sempre restaurados para o armazenamento de atividade muito alta, mesmo que tenham originalmente incluído um índice de alta atividade.

Migração de índices mornos para o armazenamento frio

Se você tiver dados UltraWarm que não consulta com frequência, considere migrá-los para o armazenamento a frio. O armazenamento de baixa atividade é destinado a dados que você acessa apenas ocasionalmente ou que não estão mais em uso ativo. Você não pode ler nem gravar em índices frios, mas pode migrá-los de volta para o armazenamento morno sem nenhum custo sempre que precisar consultá-los. Para obter instruções, consulte the section called “Migração de índices para o armazenamento frio”.

Desativando UltraWarm

O console é a maneira mais simples de desativar UltraWarm. Escolha o domínio, Ações, e Editar configuração do cluster. Desmarque a opção Ativar nós de UltraWarm dados e escolha Salvar alterações. Você também pode usar a opção `WarmEnabled` na AWS CLI e na API de configuração.

Antes de desativar UltraWarm, você deve excluir todos os índices quentes ou migrá-los de volta para o armazenamento ativo. Depois que o armazenamento quente estiver vazio, aguarde cinco minutos antes de tentar UltraWarm desativá-lo.

Armazenamento de baixa atividade para Amazon OpenSearch Service

O armazenamento de baixa atividade permite armazenar qualquer quantidade de dados históricos ou acessados com pouca frequência em seu domínio do Amazon OpenSearch Service e analisá-los sob demanda a um custo menor do que outros níveis de armazenamento. O armazenamento de baixa atividade é apropriado se você precisa fazer pesquisas periódicas ou análises forenses em seus dados mais antigos. Exemplos práticos de dados adequados para armazenamento de baixa atividade incluem logs acessados com pouca frequência, dados que devem ser preservados para atender a requisitos de compatibilidade ou registros com valor histórico.

Similar ao armazenamento UltraWarm, o armazenamento de baixa atividade é baseado no Amazon S3. Quando precisar consultar dados de baixa atividade, você poderá anexá-los seletivamente aos nós UltraWarm existentes. Você pode gerenciar a migração e o ciclo de vida de seus dados de baixa atividade manualmente ou com políticas de gerenciamento de estado de índice.

Tópicos

- Desabilitação do armazenamento de baixa atividade

Pré-requisitos

O armazenamento de baixa atividade apresenta os seguintes pré-requisitos:

- O armazenamento de baixa atividade requer o OpenSearch ou Elasticsearch versão 7.9 ou posterior.
- Para habilitar o armazenamento de baixa atividade em um domínio do OpenSearch Service, você também deve habilitar o UltraWarm no mesmo domínio.
- Para que seja possível usar o armazenamento de baixa atividade, os domínios deverão ter nós principais dedicados.
- Se o domínio usar um tipo de instância T2 ou T3 para os nós de dados, não será possível usar o armazenamento de baixa atividade .
- Se seu índice usa codecs de compressão Zstandard (`"index.codec": "zstd"` ou `"index.codec": "zstd_no_dict"`), você não pode movê-lo para um armazenamento de baixa atividade.
- Se o índice usar aproximação de k-NN (`"index.knn": true`), você não pode movê-lo para o armazenamento de baixa atividade.
- Se o domínio usar controle de acesso refinado, os usuários não administradores deverão ser mapeados na função `cold_manager` no OpenSearch Dashboards para poderem gerenciar índices de baixa atividade.

> **Note**
>
> A função `cold_manager` pode não existir em alguns domínios pré-existentes do OpenSearch Service. Se você não vir a função no Dashboards, será necessário criá-la manualmente.

Configurar permissões

Se você habilitar o armazenamento de baixa atividade em um domínio preexistente do OpenSearch Service, a função `cold_manager` não poderá ser definida no domínio. Se o domínio usar controle de acesso refinado, os usuários não administradores deverão ser mapeados nessa função para

poderem gerenciar índices de baixa atividade. Para criar manualmente a função `cold_manager`, faça o seguinte:

1. No OpenSearch Dashboards, vá para Segurança e escolha Permissões.
2. Escolha Criar grupo de ações e configure os seguintes grupos:

Group name	Permissões
`cold_cluster`	• `cluster:monitor/nodes/stats` • `cluster:admin/ultrawarm*` • `cluster:admin/cold/*`
`cold_index`	• `indices:monitor/stats` • `indices:data/read/minmax` • `indices:admin/ultrawarm/migration/get` • `indices:admin/ultrawarm/migration/cancel`

3. Escolha Funções e, em seguida, Criar função.
4. Nomeie a função como cold_manager.
5. Em Permissões de cluster, escolha o grupo `cold_cluster` que você criou.
6. Em Índice, insira `*`.
7. Em Permissões de índice, escolha o grupo `cold_index` que você criou.
8. Escolha Criar.
9. Depois de criar a função, mapeie-a em qualquer função de usuário ou backend que gerencie índices de baixa atividade.

Requisitos de armazenamento e considerações de performance do armazenamento de baixa atividade

Como o armazenamento frio usa o Simple Storage Service (Amazon S3), ele não incorre na sobrecarga do armazenamento quente, como réplicas, espaço reservado do Linux e espaço reservado do OpenSearch Service. O armazenamento de baixa atividade não tem tipos de instância específicos porque não há nenhuma capacidade computacional anexada a ele. Você pode armazenar qualquer quantidade de dados em armazenamento de baixa atividade. Monitore

a métrica `ColdStorageSpaceUtilization` no Amazon CloudWatch para ver quanto espaço de armazenamento de baixa atividade você está usando.

Preços do armazenamento de baixa atividade

Semelhante ao armazenamento UltraWarm, com o armazenamento de baixa atividade você paga apenas pelo armazenamento de dados. Não há custo de computação para dados de baixa atividade e você não será cobrado se não houver dados no armazenamento de baixa atividade.

Você não incorre em cobranças de transferência ao mover dados entre os armazenamentos de baixa e de alta atividade. Enquanto os índices estão sendo migrados entre o armazenamento warm e o frio, você continua pagando por apenas uma cópia do índice. Após a conclusão da migração, o índice é cobrado de acordo com o nível de armazenamento para o qual foi migrado. Para obter mais informações sobre o preço do armazenamento frio, consulte Preços do Amazon OpenSearch Service.

Habilitação do armazenamento de baixa atividade

O console é a maneira mais simples de criar um domínio que usa o armazenamento de baixa atividade. Ao criar o domínio, escolha Habilitar armazenamento de baixa atividade. O mesmo processo funciona em domínios existentes, desde que você atenda aos pré-requisitos. Mesmo depois que o estado do domínio mudar de Em processamento para Ativo, o UltraWarm poderá permanecer indisponível por várias horas.

Você também pode usar a AWS CLI ou a API de configuração para habilitar o armazenamento de baixa atividade.

Exemplo de comando da CLI

Os seguinte comando AWS CLI cria um domínio com três nós de dados, três nós principais dedicados, armazenamento de baixa atividade habilitado e controle de acesso refinado habilitado:

```
aws opensearch create-domain \
  --domain-name my-domain \
  --engine-version Opensearch_1.0 \
  --cluster-
config ColdStorageOptions={Enabled=true},WarmEnabled=true,WarmCount=4,WarmType=ultrawarm1.mediu
 \
  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=11 \
  --node-to-node-encryption-options Enabled=true \
  --encryption-at-rest-options Enabled=true \
```

```
  --domain-endpoint-options EnforceHTTPS=true,TLSSecurityPolicy=Policy-Min-
TLS-1-2-2019-07 \
  --advanced-security-options
 Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions='{MasterUserName=master-
user,MasterUserPassword=master-password}' \
  --region us-east-2
```

Para obter mais informações, consulte a Referência de comandos da AWS CLI.

Exemplo de solicitação da API de configuração

A seguinte solicitação à API de configuração cria um domínio com três nós de dados, três nós principais dedicados, armazenamento de baixa atividade habilitado e controle de acesso refinado habilitado:

```
POST https://es.us-east-2.amazonaws.com/2021-01-01/opensearch/domain
{
  "ClusterConfig": {
    "InstanceCount": 3,
    "InstanceType": "r6g.large.search",
    "DedicatedMasterEnabled": true,
    "DedicatedMasterType": "r6g.large.search",
    "DedicatedMasterCount": 3,
    "ZoneAwarenessEnabled": true,
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": 3
     },
    "WarmEnabled": true,
    "WarmCount": 4,
    "WarmType": "ultrawarm1.medium.search",
    "ColdStorageOptions": {
       "Enabled": true
     }
  },
  "EBSOptions": {
    "EBSEnabled": true,
    "VolumeType": "gp2",
    "VolumeSize": 11
  },
  "EncryptionAtRestOptions": {
    "Enabled": true
  },
  "NodeToNodeEncryptionOptions": {
```

```
    "Enabled": true
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": true,
    "TLSSecurityPolicy": "Policy-Min-TLS-1-2-2019-07"
  },
   "AdvancedSecurityOptions": {
    "Enabled": true,
    "InternalUserDatabaseEnabled": true,
    "MasterUserOptions": {
      "MasterUserName": "master-user",
      "MasterUserPassword": "master-password"
    }
  },
  "EngineVersion": "Opensearch_1.0",
  "DomainName": "my-domain"
}
```

Para obter informações detalhadas, consulte Referência da API do Amazon OpenSearch Service.

Gerenciamento de índices frios no OpenSearch Dashboards

Você pode gerenciar índices quentes, warm e frios com a interface do Dashboards existente em seu domínio do OpenSearch Service. O Dashboards permite que você migre índices entre armazenamentos warm e frio e monitore o status da migração do índice sem usar a CLI ou a API de configuração. Para obter mais informações, consulte Gerenciamento de índices no OpenSearch Dashboards.

Migração de índices para o armazenamento frio

Ao migrar índices para o armazenamento frio, você deve fornecer um intervalo de tempo para os dados para facilitar a descoberta. Você pode selecionar um campo de timestamp com base nos dados em seu índice, fornecer manualmente um carimbo de data/hora inicial e final ou optar por não especificar um.

Parâmetro	Valor compatível	Descrição
`timestamp_field`	O campo de data/hora do mapeamento do índice.	Os valores mínimo e máximo do campo fornecido são calculados e armazenad

Parâmetro	Valor compatível	Descrição
		os como os metadados `start_time` e `end_time` para o índice de baixa atividade.
`start_time` e `end_time`	Use um dos seguintes formatos: • strict_date_optional_time. Por exemplo: `yyyy-MM-dd'T'HH:mm:ss.SSSZ` ou `yyyy-MM-dd` • Tempo de época em milissegundos	Os valores são fornecidos como os metadados `start_time` e `end_time` para o índice de baixa atividade.

Se não quiser especificar um carimbo de data/hora, adicione `?ignore=timestamp` à solicitação em vez disso.

A seguinte solicitação migra um índice de alta atividade para o armazenamento de baixa atividade e fornece horários de início e término para os dados nesse índice:

```
POST _ultrawarm/migration/my-index/_cold
  {
    "start_time": "2020-03-09",
    "end_time": "2020-03-09T23:00:00Z"
  }
```

Depois, verifique o status da migração:

```
GET _ultrawarm/migration/my-index/_status

{
  "migration_status": {
    "index": "my-index",
    "state": "RUNNING_METADATA_RELOCATION",
    "migration_type": "WARM_TO_COLD"
  }
```

```
}
```

O OpenSearch Service migra um índice de cada vez para o armazenamento de baixa atividade. É possível ter até 100 migrações na fila. Qualquer solicitação que exceda o limite será rejeitada. Para verificar o número de migrações atual, monitore a métrica `WarmToColdMigrationQueueSize`. O processo de migração tem os seguintes estados:

```
ACCEPTED_COLD_MIGRATION - Migration request is accepted and queued.
RUNNING_METADATA_MIGRATION - The migration request was selected for execution and
 metadata is migrating to cold storage.
FAILED_METADATA_MIGRATION - The attempt to add index metadata has failed and all
 retries are exhausted.
PENDING_INDEX_DETACH - Index metadata migration to cold storage is completed. Preparing
 to detach the warm index state from the local cluster.
RUNNING_INDEX_DETACH - Local warm index state from the cluster is being removed. Upon
 success, the migration request will be completed.
FAILED_INDEX_DETACH - The index detach process failed and all retries are exhausted.
```

Automatização de migrações para o armazenamento frio

Você pode usar o Gerenciamento de estados de índices para automatizar o processo de migração depois que um índice atinge uma determinada idade ou atende a outras condições. Consulte a política de exemplo que demonstra como migrar automaticamente índices de armazenamento quente para UltraWarm para frio.

> **Note**
>
> Um `timestamp_field` explícito é necessário para mover índices para o armazenamento frio usando uma política de gerenciamento de estados de índices.

Cancelando migrações para armazenamento frio

Se uma migração para armazenamento frio estiver enfileirada ou em um estado de falha, você poderá cancelar a migração usando a seguinte solicitação:

```
POST _ultrawarm/migration/_cancel/my-index

{
```

```
  "acknowledged" : true
}
```

Se o domínio usa controle de acesso refinado, você precisará da permissão `indices:admin/ultrawarm/migration/cancel` para fazer essa solicitação.

Listagem de índices de baixa atividade

Antes de consultar, você pode listar os índices no armazenamento frio para decidir quais migrar para o UltraWarm para análise posterior. A seguinte solicitação lista todos os índices de baixa atividade classificados por nome de índice:

```
GET _cold/indices/_search
```

Exemplo de resposta

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 3,
  "indices" : [
    {
      "index" : "my-index-1",
      "index_cold_uuid" : "hjEoh26mRRCFxRIMdgvLmg",
      "size" : 10339,
      "creation_date" : "2021-06-28T20:23:31.206Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-2",
      "index_cold_uuid" : "0vIS2n-oROmOWDFmwFIgdw",
      "size" : 6068,
      "creation_date" : "2021-07-15T19:41:18.046Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-3",
      "index_cold_uuid" : "EaeXOBodTLiDYcivKsXVLQ",
      "size" : 32403,
      "creation_date" : "2021-07-08T00:12:01.523Z",
      "start_time" : "2020-03-09T00:00Z",
```

```
      "end_time" : "2020-03-09T23:00Z"
    }
  ]
}
```

Filtrando

Você pode filtrar índices frios com base em um padrão de índice baseado em prefixos e em deslocamentos de intervalo de tempo.

A seguinte solicitação lista índices que correspondem ao padrão de prefixo de `event-*`:

```
GET _cold/indices/_search
 {
   "filters":{
      "index_pattern": "event-*"
   }
 }
```

Exemplo de resposta

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 1,
  "indices" : [
    {
      "index" : "events-index",
      "index_cold_uuid" : "4eFiab7rRfSvp3slrIsIKA",
      "size" : 32263273,
      "creation_date" : "2021-08-18T18:25:31.845Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    }
  ]
}
```

A seguinte solicitação retorna índices com campos de metadados `start_time` e `end_time` entre `2019-03-01` e `2020-03-01`:

```
GET _cold/indices/_search
{
```

```
  "filters": {
    "time_range": {
      "start_time": "2019-03-01",
      "end_time": "2020-03-01"
    }
  }
}
```

Exemplo de resposta

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 1,
  "indices" : [
    {
      "index" : "my-index",
      "index_cold_uuid" : "4eFiab7rRfSvp3slrIsIKA",
      "size" : 32263273,
      "creation_date" : "2021-08-18T18:25:31.845Z",
      "start_time" : "2019-05-09T00:00Z",
      "end_time" : "2019-09-09T23:00Z"
    }
  ]
}
```

Classificar

Você pode classificar índices frios por campos de metadados, como nome ou tamanho do índice. A seguinte solicitação lista todos os índices classificados por tamanho em ordem decrescente:

```
GET _cold/indices/_search
 {
 "sort_key": "size:desc"
 }
```

Exemplo de resposta

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 5,
  "indices" : [
    {
```

```
      "index" : "my-index-6",
      "index_cold_uuid" : "4eFiab7rRfSvp3slrIsIKA",
      "size" : 32263273,
      "creation_date" : "2021-08-18T18:25:31.845Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-9",
      "index_cold_uuid" : "mbD3ZRVDRI6ONqgEOsJyUA",
      "size" : 57922,
      "creation_date" : "2021-07-07T23:41:35.640Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-5",
      "index_cold_uuid" : "EaeXOBodTLiDYcivKsXVLQ",
      "size" : 32403,
      "creation_date" : "2021-07-08T00:12:01.523Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    }
  ]
}
```

Outras chaves de classificação válidas são `start_time:asc/desc`, `end_time:asc/desc` e `index_name:asc/desc`.

Paginação

Você pode paginar uma lista de índices frios. Configure o número de índices a serem retornados por página com o parâmetro `page_size` (o padrão é 10). Cada solicitação `_search` em seus índices frios retorna um `pagination_id` que você pode usar para chamadas subsequentes.

A seguinte solicitação pagina os resultados de uma solicitação `_search` de seus índices frios e exibe os próximos 100 resultados:

```
GET _cold/indices/_search?page_size=100
{
"pagination_id": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY"
}
```

Migração de índices frios para o armazenamento warm

Depois de restringir sua lista de índices frios com os critérios de filtragem na seção anterior, migre-os de volta para UltraWarm, onde você poderá consultar os dados e usá-los para criar visualizações.

A solicitação a seguir migra dois índices frios de volta para o armazenamento warm:

```
POST _cold/migration/_warm
 {
 "indices": "my-index1,my-index2"
 }


{
  "acknowledged" : true
}
```

Para verificar o status da migração e recuperar o ID de migração, envie a seguinte solicitação:

```
GET _cold/migration/_status
```

Exemplo de resposta

```
{
  "cold_to_warm_migration_status" : [
    {
      "migration_id" : "tyLjXCA-S76zPQbPVHkOKA",
      "indices" : [
        "my-index1,my-index2"
      ],
      "state" : "RUNNING_INDEX_CREATION"
    }
  ]
}
```

Para obter informações de migração específicas do índice, inclua o nome do índice:

```
GET _cold/migration/my-index/_status
```

Em vez de especificar um índice, você pode listar os índices por seu status de migração atual. Os valores válidos são `_failed`, `_accepted` e `_all`.

O comando a seguir obtém o status de todos os índices em uma única solicitação de migração:

```
GET _cold/migration/_status?migration_id=my-migration-id
```

Recupere o ID de migração usando a solicitação de status. Para obter informações detalhadas sobre migração, adicione `&verbose=true`.

Você pode migrar índices do armazenamento frio para o armazenamento morno em lotes de 10, com, no máximo, 100 índices sendo migados simultaneamente. Qualquer solicitação que exceda o limite será rejeitada. Para verificar o número de migrações que estão ocorrendo no momento, monitore a métrica `ColdToWarmMigrationQueueSize`. O processo de migração tem os seguintes estados:

```
ACCEPTED_MIGRATION_REQUEST - Migration request is accepted and queued.
RUNNING_INDEX_CREATION - Migration request is picked up for processing and will create
 warm indexes in the cluster.
PENDING_COLD_METADATA_CLEANUP - Warm index is created and the migration service will
 attempt to clean up cold metadata.
RUNNING_COLD_METADATA_CLEANUP - Cleaning up cold metadata from the indexes migrated to
 warm storage.
FAILED_COLD_METADATA_CLEANUP - Failed to clean up metadata in the cold tier.
FAILED_INDEX_CREATION - Failed to create an index in the warm tier.
```

Restauração de índices frios de snapshots

Se precisar restaurar um índice de baixa atividade excluído, você pode restaurá-lo de volta ao nível de maior atividade seguindo as instruções the section called “Restauração de índices quentes de snapshots” e, em seguida, migrando o índice de volta para o nível de baixa atividade novamente. Você não pode restaurar um índice de baixa atividade excluído diretamente para o nível frio. O OpenSearch Service retém os índices frios por 14 dias após a sua exclusão.

Cancelamento de migrações do armazenamento de baixa atividade para o armazenamento de alta atividade

Se uma migração de índice do armazenamento de baixa atividade para o armazenamento de alta atividade estiver enfileirada ou em um estado de falha, você poderá cancelá-la com a seguinte solicitação:

```
POST _cold/migration/my-index/_cancel
```

```
{
  "acknowledged" : true
}
```

Para cancelar a migração de um lote de índices (máximo de 10 por vez), especifique o ID de migração:

```
POST _cold/migration/_cancel?migration_id=my-migration-id

{
  "acknowledged" : true
}
```

Recupere o ID de migração usando a solicitação de status.

Atualizando metadados de índice de baixa atividade

Você pode atualizar os campos `start_time` e `end_time` para um índice de baixa atividade:

```
PATCH _cold/my-index
 {
 "start_time": "2020-01-01",
 "end_time": "2020-02-01"
 }
```

Não é possível atualizar o `timestamp_field` de um índice no armazenamento de baixa atividade.

> **Note**
>
> O OpenSearch Dashboards não oferece suporte ao método PATCH. Use curl, Postman ou algum outro método para atualizar metadados de baixa atividade.

Exclusão de índices de baixa atividade

Se você não estiver usando uma política do ISM, poderá excluir índices frios manualmente. A seguinte solicitação exclui um índice de baixa atividade:

```
DELETE _cold/my-index
```

```
{
  "acknowledged" : true
}
```

Desabilitação do armazenamento de baixa atividade

O console do OpenSearch Service é a maneira mais simples de desabilitar o armazenamento de baixa atividade. Selecione o domínio e escolha Ações, Editar configuração do cluster, depois desmarque a opção Habilitar armazenamento estático.

Para usar a AWS CLI ou a API de configuração, em `ColdStorageOptions`, defina `"Enabled"="false"`.

Antes de desabilitar o armazenamento frio, você deve excluir todos os índices frios ou migrá-los de volta para o armazenamento warm, caso contrário, a ação de desabilitar falhará.

Armazenamento OR1 para Amazon Service OpenSearch

OR1 é uma família de instâncias do Amazon OpenSearch Service que fornece uma maneira econômica de armazenar grandes quantidades de dados. Um domínio com instâncias OR1 usa o Amazon Elastic Block Store (Amazon EBS) `gp3` ou `io1` volumes para armazenamento primário, com dados copiados de forma síncrona para o Amazon S3 assim que chegam. Essa estrutura de armazenamento proporciona maior throughput de indexação com alta durabilidade. A família de instâncias OR1 também oferece suporte para recuperação automática de dados em caso de falha. Para obter informações sobre as opções de tipos de instância OR1, consulte the section called “Tipos de instâncias da geração atual”.

Se você estiver indexando cargas de trabalho de análise operacional pesadas, como análise de log, observabilidade ou análise de segurança, você pode se beneficiar do desempenho aprimorado e da eficiência computacional das instâncias OR1. Além disso, a recuperação automática de dados oferecida pelas instâncias OR1 melhora a confiabilidade geral do seu domínio.

OpenSearch O serviço envia métricas OR1 relacionadas ao armazenamento para a Amazon. CloudWatch Para ver uma lista das métricas disponíveis, consulte ???.

As instâncias OR1 estão disponíveis sob demanda ou com preços de instância reservada, com uma taxa horária para as instâncias e o armazenamento provisionados no Amazon EBS e no Amazon S3.

Tópicos

- Limitações

- Como o OR1 difere do armazenamento UltraWarm
- Usar instâncias OR1

Limitações

Considere as seguintes limitações ao usar instâncias OR1 para seu domínio.

- Seu domínio deve estar executando a OpenSearch versão 2.11 ou superior.
- Seu domínio deve ter a criptografia em repouso ativada. Para ter mais informações, consulte ???.
- Seu domínio deve ser um novo domínio. Você não pode modificar um domínio existente para usar instâncias OR1.
- Se seu domínio usa nós mestres dedicados, eles devem usar instâncias do Graviton. Para obter mais informações sobre nós mestres dedicados, consulte???.
- Os tamanhos dos fragmentos nas instâncias OR1 devem ser menores que 100 GiB. Fragmentos maiores que 100 GiB podem diminuir os tempos de recuperação. Se você criar fragmentos maiores que 100 GiB em instâncias OR1 OpenSearch , o Service bloqueia solicitações de gravação no domínio. Se você ainda quiser usar fragmentos maiores que 100 GiB, AWS Supportentre em contato para solicitar um aumento de cota.
- O intervalo de atualização dos índices nas instâncias OR1 deve ser de 10 segundos ou mais. O intervalo de atualização padrão para instâncias OR1 é de 10 segundos.

Como o OR1 difere do armazenamento UltraWarm

OpenSearch O serviço fornece UltraWarm instâncias otimizadas para reduzir o custo de armazenamento de dados quentes. Tanto o OR1 quanto as UltraWarm instâncias armazenam dados localmente no Amazon EBS e remotamente no Amazon S3. No entanto, OR1 e UltraWarm instâncias diferem de várias maneiras importantes:

- As instâncias OR1 mantêm uma cópia dos dados no armazenamento local e remoto. UltraWarm instâncias, para reduzir os custos de armazenamento, mantenha os dados principalmente no armazenamento remoto. Dependendo dos padrões de uso, eles podem movê-lo para o armazenamento local.
- As instâncias OR1 estão ativas e podem aceitar operações de leitura e gravação, enquanto os dados nas UltraWarm instâncias são somente para leitura até que você os mova manualmente de volta para o armazenamento dinâmico.

- UltraWarm depende de instantâneos de índice para durabilidade dos dados. As instâncias OR1, em comparação, realizam replicação e recuperação nos bastidores. No caso de um índice vermelho, as instâncias OR1 restauram automaticamente os fragmentos ausentes do armazenamento remoto no Amazon S3. O tempo de recuperação varia de acordo com o volume de dados a serem recuperados.

Para obter mais informações sobre UltraWarm armazenamento, consulte???.

Usar instâncias OR1

Você pode selecionar instâncias OR1 para seus nós de dados ao criar um novo domínio com o AWS Management Console, o AWS Command Line Interface (AWS CLI) ou o AWS SDK. Em seguida, você pode indexar e consultar os dados usando suas ferramentas existentes.

Console

1. Navegue até o console do Amazon OpenSearch Service emhttps://console.aws.amazon.com/aos/.
2. No painel de navegação à esquerda, escolha Domínios.
3. Escolha Criar domínio.
4. Insira um nome para o domínio junto com outras opções de sua preferência. Em Família de instâncias, escolha OR1. Escolha Criar para iniciar o processo de criação do domínio.

AWS CLI

1. Navegue até seu AWS CLI terminal. Se você precisar instalar o AWS CLI, consulte Instalar ou atualizar a versão mais recente do AWS CLI.
2. Para usar o armazenamento OR1, você deve fornecer o valor do tamanho específico do tipo de instância OR1 no `InstanceType` campo ao criar um domínio. Você também deve ativar a criptografia em repouso.

   O exemplo a seguir cria um domínio com instâncias OR1 do tamanho `2xlarge`.

```
aws opensearch create-domain \
  --domain-name test-domain \
  --engine-version OpenSearch_2.11 \
```

```
  --cluster-config
 "InstanceType=or1.2xlarge.search,InstanceCount=3,DedicatedMasterEnabled=true,DedicatedMast
 \
  --ebs-options "EBSEnabled=true,VolumeType=gp3,VolumeSize=200" \
  --encryption-at-rest-options Enabled=true \
  --advanced-security-options
 "Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions={MasterUserName=test-
user,MasterUserPassword=test-password}" \
  --node-to-node-encryption-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true \
  --access-policies '{"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":
{"AWS":"*"},"Action":"es:*","Resource":"arn:aws:es:us-east-1:account-
id:domain/test-domain/*"}]}'
```

Gerenciamento de estados de índices no Amazon OpenSearch Service

O Gerenciamento de estados de índices (ISM) no Amazon OpenSearch Service permite definir políticas de gerenciamento personalizadas que automatizam tarefas de rotina e aplicá-las a índices e padrões de índices. Não é mais necessário configurar e gerenciar processos externos para executar operações de índice.

Uma política contém um estado padrão e uma lista de estados entre os quais o índice transita. Dentro de cada estado, é possível definir uma lista de ações a serem realizadas e das condições que acionam essas transições. Um caso de uso típico é excluir periodicamente índices antigos após um determinado período. Por exemplo, é possível definir uma política que mova seu índice para o estado `read_only` após 30 dias e, por fim, excluí-lo após 90 dias.

Depois de anexar uma política a um índice, o ISM cria um trabalho que é executado em intervalos de 5 a 8 minutos (ou 30 a 48 minutos para clusters pré-1.3) para executar ações de política, verificar condições e fazer a transição do índice para estados diferentes. O tempo base para que esse trabalho seja executado é a cada 5 minutos. Além disso, uma variação aleatória de 0 a 60% é adicionada a ele para garantir que não ocorra um surto de atividade de todos os seus índices ao mesmo tempo. O ISM não executa tarefas se o estado do cluster for vermelho.

O ISM exige o OpenSearch ou Elasticsearch 6.8 ou superior A documentação completa está disponível na documentação do OpenSearch.

> **Important**
>
> Você não pode mais utilizar modelos de índice para aplicar políticas de ISM a índices recém-criados. Você pode continuar gerenciando automaticamente índices recém-criados com o campo do modelo de ISM. Esta atualização introduz uma alteração que afeta os modelos existentes do CloudFormation que usam essa configuração.

Criar uma política do IAM

Para começar a usar o gerenciamento de estados de índices

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. Selecione o domínio para o qual você deseja criar uma política do ISM.
3. No painel do domínio, navegue até o URL do OpenSearch Dashboards e faça login com seu nome de usuário principal e a senha correspondente. O URL segue este formato:

   ```
   domain-endpoint/_dashboards/
   ```

4. Abra o painel de navegação esquerdo no OpenSearch Dashboards, escolha Gerenciamento de índices e Criar política.
5. Use o editor visual ou o editor JSON para criar políticas. Recomendamos que você use o editor visual, pois ele oferece uma maneira mais estruturada de definir políticas. Para obter ajuda com a criação de políticas, consulte as políticas de exemplo abaixo.
6. Depois de criar uma política, anexe-a a um ou mais índices:

   ```
   POST _plugins/_ism/add/my-index
   {
     "policy_id": "my-policy-id"
   }
   ```

   > **Note**
   >
   > Se o seu domínio estiver executando uma versão herdada do Elasticsearch, use `_opendistro` em vez de `_plugins`.

Como alternativa, selecione o índice no OpenSearch Dashboards e escolha Aplicar.

Políticas de exemplo

As políticas de exemplo a seguir demonstram como automatizar casos de uso comuns do ISM.

Armazenamento de atividade muito alta para alta atividade para baixa atividade

Este política de exemplo move um índice do armazenamento a quente para UltraWarm e, eventualmente, para o armazenamento a frio. Em seguida, ele exclui o índice.

O índice está inicialmente no estado `hot`. Após dez dias, o ISM o transfere para o estado `warm`. 80 dias depois, quando o índice tiver 90 dias, o ISM move o índice para o estado `cold`. Após um ano, o serviço envia uma notificação para uma sala do Amazon Chime informando que o índice está sendo excluído e, depois, o exclui permanentemente.

Observe que os índices frios exigem a operação `cold_delete` em vez da operação normal `delete`. Observe também que um `timestamp_field` explícito é necessário em seus dados para gerenciar índices frios com ISM.

```
{
  "policy": {
    "description": "Demonstrate a hot-warm-cold-delete workflow.",
    "default_state": "hot",
    "schema_version": 1,
    "states": [{
        "name": "hot",
        "actions": [],
        "transitions": [{
          "state_name": "warm",
          "conditions": {
            "min_index_age": "10d"
          }
        }]
      },
      {
        "name": "warm",
        "actions": [{
          "warm_migration": {},
```

```
          "retry": {
            "count": 5,
            "delay": "1h"
          }
        }],
        "transitions": [{
          "state_name": "cold",
          "conditions": {
            "min_index_age": "90d"
          }
        }]
      },
      {
        "name": "cold",
        "actions": [{
            "cold_migration": {
              "timestamp_field": "<your timestamp field>"
            }
          }
        ],
        "transitions": [{
          "state_name": "delete",
          "conditions": {
             "min_index_age": "365d"
          }
        }]
      },
      {
        "name": "delete",
        "actions": [{
          "notification": {
            "destination": {
              "chime": {
                "url": "<URL>"
              }
            },
            "message_template": {
              "source": "The index {{ctx.index}} is being deleted."
            }
          }
        },
        {
          "cold_delete": {}
        }]
```

```
      }
    ]
  }
}
```

Reduzir a contagem de réplicas

Esta política de exemplo mais simples reduz a contagem de réplicas para zero após sete dias para conservar espaço em disco e exclui o índice após 21 dias. Essa política pressupõe que seu índice não seja crítico e não receba mais solicitações de gravação. Ter réplicas zero traz algum risco de perda de dados.

```
{
  "policy": {
    "description": "Changes replica count and deletes.",
    "schema_version": 1,
    "default_state": "current",
    "states": [{
        "name": "current",
        "actions": [],
        "transitions": [{
          "state_name": "old",
          "conditions": {
            "min_index_age": "7d"
          }
        }]
      },
      {
        "name": "old",
        "actions": [{
          "replica_count": {
            "number_of_replicas": 0
          }
        }],
        "transitions": [{
          "state_name": "delete",
          "conditions": {
            "min_index_age": "21d"
          }
        }]
      },
      {
        "name": "delete",
```

```
        "actions": [{
          "delete": {}
        }],
        "transitions": []
      }
    ]
  }
}
```

Obter o snapshot de um índice

Esta política de exemplo usa a operação `snapshot` para obter um instantâneo de um índice assim que ele passa a conter pelo menos um documento. `repository` é o nome do repositório manual de snapshots que você registrou no Amazon S3. `snapshot` é o nome do snapshot. Para obter pré-requisitos para a obtenção de snapshot e etapas para registrar um repositório, consulte the section called “Criação de snapshots de índices”.

```
{
  "policy": {
    "description": "Takes an index snapshot.",
    "schema_version": 1,
    "default_state": "empty",
    "states": [{
        "name": "empty",
        "actions": [],
        "transitions": [{
          "state_name": "occupied",
          "conditions": {
            "min_doc_count": 1
          }
        }]
      },
      {
        "name": "occupied",
        "actions": [{
          "snapshot": {
            "repository": "<my-repository>",
            "snapshot": "<my-snapshot>"
            }
          }],
          "transitions": []
      }
    ]
```

```
  }
}
```

Modelos do ISM

Você pode configurar um campo `ism_template` em uma política para que, quando criar um índice que corresponda ao padrão do modelo, a política seja anexada automaticamente a esse índice. Neste exemplo, qualquer índice que você criar com um nome começando com "log" é automaticamente correspondido à política do ISM `my-policy-id`:

```
PUT _plugins/_ism/policies/my-policy-id
{
  "policy": {
    "description": "Example policy.",
    "default_state": "...",
    "states": [...],
    "ism_template": {
      "index_patterns": ["log*"],
      "priority": 100
    }
  }
}
```

Para obter um exemplo mais detalhado, consulte Exemplo de política com modelo de ISM para rolagem automática.

Diferenças

Comparado ao OpenSearch e ao Elasticsearch, o ISM para o Amazon OpenSearch Service tem várias diferenças.

Operações do ISM

- O OpenSearch Service oferece suporte a três operações do ISM exclusivas, `warm_migration`, `cold_migration` e `cold_delete`:
  - Se o seu domínio tiver o UltraWarm ativado, a ação `warm_migration` fará a transição do índice para o armazenamento de alta atividade.
  - Se o seu domínio tiver armazenamento frio habilitado, a ação `cold_migration` passará o índice para o armazenamento frio, e a ação `cold_delete` excluirá um índice do armazenamento frio.

Mesmo que uma dessas ações não seja concluída dentro do período de tempo limite definido, a migração ou exclusão dos índices ainda continuará. Definir uma error_notification para uma das ações acima vai notificar você de que a ação falhou se não tiver sido concluída em um período de tempo limite, mas a notificação é apenas para sua própria referência. A operação real não tem tempo limite inerente e continua a ser executada até que eventualmente seja bem-sucedida ou falhe.

- Se o seu domínio executa o OpenSearch ou o Elasticsearch 7.4 ou posterior, o OpenSearch Service oferece suporte às operações `open` e `close` do ISM.

- Se o seu domínio executa o OpenSearch ou o Elasticsearch 7.7 ou posterior, o OpenSearch Service oferece suporte à operação `snapshot` do ISM.

Operações ISM de armazenamento de baixa atividade

Para índices frios, você deve especificar um parâmetro `?type=_cold` ao usar as seguintes APIs do ISM:

- Adicionar política
- Remover política
- Atualizar política
- Repetir índice com falha
- Explicar índice

Essas APIs para índices frios têm as seguintes diferenças adicionais:

- Operadores curingas não são aceitos, exceto quando usados no final. Por exemplo, `_plugins/_ism/<add, remove, change_policy, retry, explain>/logstash-*` é aceito, mas `_plugins/_ism/<add, remove, change_policy, retry, explain>/iad-*-prod` não.
- Não há suporte a índices e padrões de vários índices. Por exemplo, `_plugins/_ism/<add, remove, change_policy, retry, explain>/app-logs` é aceito, mas `_plugins/_ism/<add, remove, change_policy, retry, explain>/app-logs,sample-data` não.

Configurações do ISM

O OpenSearch e o Elasticsearch permitem alterar todas as configurações do ISM disponíveis usando via API `_cluster/settings`. No Amazon OpenSearch Service, só é possível alterar as seguintes configurações do ISM:

- Configurações no nível do cluster:
  - `plugins.index_state_management.enabled`
  - `plugins.index_state_management.history.enabled`
- Configurações no nível do índice:
  - `plugins.index_state_management.rollover_alias`

Tutorial: como automatizar processos do Gerenciamento de estados de índice

Este tutorial demonstra como implementar uma política do ISM que automatiza tarefas de rotina de gerenciamento de índices e as aplica a índices e padrões de índices.

O Gerenciamento de estados de índice (ISM) no Amazon OpenSearch Service permite automatizar atividades recorrentes de gerenciamento de índices para que você possa evitar o uso de ferramentas adicionais para gerenciar ciclos de vida de índices. É possível criar uma política para automatizar essas operações com base na idade, no tamanho e em outras condições do índice, tudo de dentro do domínio do Amazon OpenSearch Service.

O OpenSearch Service oferece suporte a três camadas de armazenamento: o estado “quente” padrão para gravação ativa e análise de baixa latência, UltraWarm para dados somente leitura de até três petabytes e armazenamento de baixa atividade (frio) para arquivamento ilimitado a longo prazo.

Este tutorial apresenta um exemplo de caso de uso do tratamento de dados de séries temporais em índices diários. No tutorial, você configurará uma política que captura um instantâneo automatizado de cada índice anexado após 24 horas. Em seguida, a política migra o índice do estado quente padrão para um armazenamento UltraWarm após dois dias, para um armazenamento de baixa atividade (frio) após 30 dias e, finalmente, exclui o índice após 60 dias.

Pré-requisitos

- O domínio do OpenSearch Service deve estar executando o Elasticsearch versão 6.8 ou posterior ou qualquer versão do OpenSearch.
- O domínio deve ter o UltraWarm e o armazenamento de baixa atividade (frio) habilitados.
- É necessário registrar um repositório de snapshots manuais para seu domínio.
- Sua função de usuário precisa de permissões suficientes para acessar o console do OpenSearch Service. Se necessário, valide e configure o acesso ao seu domínio.

Etapa 1: configurar a política do ISM

Primeiro, configure uma política do ISM no OpenSearch Dashboards.

1. No painel do domínio no console do OpenSearch Service, navegue até o URL do OpenSearch Dashboards e faça login com seu nome de usuário principal e a senha. O URL segue este formato: *domain-endpoint*/_dashboards/.
2. No OpenSearch Dashboards, escolha Adicionar dados de exemplo e adicione um ou mais dos índices de amostra ao domínio.
3. Abra o painel de navegação esquerdo e escolha IGerenciamento de índices e Criar política.
4. Atribua o nome `ism-policy-example` à política.
5. Substitua a política padrão pela seguinte política:

```
{
  "policy": {
    "description": "Move indexes between storage tiers",
    "default_state": "hot",
    "states": [
      {
        "name": "hot",
        "actions": [],
        "transitions": [
          {
            "state_name": "snapshot",
            "conditions": {
              "min_index_age": "24h"
            }
          }
        ]
```

```
      },
      {
        "name": "snapshot",
        "actions": [
          {
            "retry": {
              "count": 5,
              "backoff": "exponential",
              "delay": "30m"
            },
            "snapshot": {
              "repository": "snapshot-repo",
              "snapshot": "ism-snapshot"
            }
          }
        ],
        "transitions": [
          {
            "state_name": "warm",
            "conditions": {
              "min_index_age": "2d"
            }
          }
        ]
      },
      {
        "name": "warm",
        "actions": [
          {
            "retry": {
              "count": 5,
              "backoff": "exponential",
              "delay": "1h"
            },
            "warm_migration": {}
          }
        ],
        "transitions": [
          {
            "state_name": "cold",
            "conditions": {
              "min_index_age": "30d"
            }
          }
```

```
        ]
      },
      {
        "name": "cold",
        "actions": [
          {
            "retry": {
              "count": 5,
              "backoff": "exponential",
              "delay": "1h"
            },
            "cold_migration": {
              "start_time": null,
              "end_time": null,
              "timestamp_field": "@timestamp",
              "ignore": "none"
            }
          }
        ],
        "transitions": [
          {
            "state_name": "delete",
            "conditions": {
              "min_index_age": "60d"
            }
          }
        ]
      },
      {
        "name": "delete",
        "actions": [
          {
            "cold_delete": {}
          }
        ],
        "transitions": []
      }
    ],
    "ism_template": [
      {
        "index_patterns": [
          "index-*"
        ],
        "priority": 100
```

```
      }
    ]
  }
}
```

> **Note**
>
> O campo `ism_template` anexa automaticamente a política a qualquer índice recém-criado que corresponda a um dos `index_patterns` especificados. Nesse caso, todos os índices que começam com `index-`. É possível modificar esse campo para corresponder a um formato de índice em seu ambiente. Para obter mais informações, consulte Modelos do ISM.

6. Na seção `snapshot` da política, substitua *`snapshot-repo`* pelo nome do repositório de snapshots que você registrou para o seu domínio. Se quiser, você também pode substituir *`ism-snapshot`*, que será o nome do snapshot quando ele for criado.
7. Escolha Criar. A política agora está visível na página Políticas de gerenciamento de estado.

Etapa 2: anexar a política a um ou mais índices.

Agora que você criou a política, anexe-a a um ou mais índices no cluster.

1. Vá para a guia Índices quentes e procure `opensearch_dashboards_sample`, que lista todos os índices de exemplo adicionados na etapa 1.
2. Selecione todos os índices e escolha Aplicar política. Em seguida, escolha a política ism-policy-example que você acabou de criar.
3. Escolha Aplicar.

É possível monitorar os índices à medida que eles avançam pelos vários estados na página Índices gerenciados por políticas.

Resumo dos índices no Amazon OpenSearch Service com agrupamentos de índices

As totalizações de índices no Amazon OpenSearch Service permitem reduzir os custos de armazenamento ao combinar periodicamente dados antigos em índices resumidos.

Você escolhe os campos que interessam e usa uma totalização de índices para criar um novo índice com apenas esses campos agregados em buckets de tempo menos detalhados. Você pode armazenar meses ou anos de dados históricos por uma fração do custo com a mesma performance de consulta.

As totalizações de índices exigem o OpenSearch ou Elasticsearch 7.9 ou posterior A documentação completa do recurso está disponível na documentação do OpenSearch.

Criação de um trabalho de totalização de índices

Para começar a usar, escolha Index Management (Gerenciamento de índices) no OpenSearch Dashboards. Selecione Rollup Jobs (Trabalhos de totalização) e escolha Create rollup job (Criar trabalho de totalização).

Etapa 1: Configurar índices

Configure os índices de origem e de destino. O índice de origem é aquele que você deseja totalizar. O índice de destino é onde os resultados do conjunto de índices são salvos.

Depois de criar um trabalho de totalização de índices, você não poderá alterar suas seleções de índice.

Etapa 2: Definir agregações e métricas

Selecione os atributos com as agregações (termos e histogramas) e métricas (média, soma, máximo, mínimo e contagem de valores) que deseja totalizar. Certifique-se de não adicionar muitos atributos altamente granulares, porque você não economizará muito espaço.

Etapa 3: Especificar agendamentos

Especifique um agendamento para agrupar seus índices à medida que são ingeridos. O trabalho de totalização é habilitado por padrão.

Etapa 4: Revisar e criar

Revise sua configuração e selecione Create (Criar).

Etapa 5: Pesquisar o índice de destino

Você pode usar a API `_search` padrão para pesquisar o índice de destino. Você não pode acessar a estrutura interna dos dados no índice de destino porque o plugin reescreve automaticamente a consulta em segundo plano para se adequar ao índice de destino. Isso é para garantir que você possa usar a mesma consulta para o índice de origem e de destino.

Para consultar o índice de destino, defina `size` como 0:

```
GET target_index/_search
{
  "size": 0,
  "query": {
    "match_all": {}
  },
  "aggs": {
    "avg_cpu": {
      "avg": {
        "field": "cpu_usage"
      }
    }
  }
}
```

> **Note**
>
> As versões 2.2 e posteriores do OpenSearch oferecem suporte à pesquisa de vários índices cumulativos em uma solicitação. As versões do OpenSearch anteriores à 2.2 e as versões antigas do Elasticsearch OSS oferecem suporte apenas a um índice cumulativo por pesquisa.

Transformação de índices no Amazon OpenSearch Service

Considerando que os trabalhos de recolhimento de índices permitem que você reduza a granularidade dos dados totalizando dados antigos em índices condensados, os trabalhos de

transformação permitem criar uma visualização resumida e diferente dos dados centrada em determinados campos para que você possa visualizar ou analisar os dados de diferentes maneiras.

As transformações de índice têm uma interface de usuário do OpenSearch Dashboards e uma API REST. O recurso requer o OpenSearch 1.0 ou posterior. A documentação completa está disponível na documentação do OpenSearch.

Criação de um trabalho de transformação de índice

Se você não possui nenhum dado no cluster, use os dados de voo de exemplo no OpenSearch Dashboards para testar os trabalhos de transformação. Após adicionar os dados, inicie o OpenSearch Dashboards. Em seguida, escolha Index management (Gerenciamento de índices),Transform Jobs (Trabalhos de transformação) e Create Transform Job (Criar trabalho de transformação).

Etapa 1: Escolher índices

Na seção Indexes (Índices), selecione o índice de origem e o índice de destino. Você pode selecionar um índice de destino existente, ou criar um novo inserindo um nome para ele.

Se desejar transformar apenas um subconjunto do seu índice de origem, escolha Add Data Filter (Adicionar filtro de dados) e use o DSL de consulta do OpenSearch para especificar um subconjunto do índice de origem.

Etapa 2: Escolher campos

Depois de escolher seus índices, escolha os campos que deseja usar no trabalho de transformação, bem como se deseja usar agrupamentos ou agregações.

- Você pode usar agrupamentos para colocar seus dados em buckets separados em seu índice transformado. Por exemplo, para agrupar todos os destinos de aeroporto dentro dos dados de amostra de voos, agrupe o campo `DestAirportID` em um campo de destino do campo `DestAirportID_terms`. Ao fazer isso, você poderá encontrar os IDs de aeroporto agrupados em seu índice transformado após a conclusão do trabalho de transformação.
- Por outro lado, as agregações permitem realizar cálculos simples. Por exemplo, você pode incluir uma agregação no trabalho de transformação para definir um novo campo de `sum_of_total_ticket_price` que calcula a soma de todas as passagens aéreas. Em seguida, você pode analisar os novos dados em seu índice transformado.

Etapa 3: Especificar um agendamento

Os trabalhos de transformação são habilitados por padrão e executados de acordo com agendamentos. Em Transform execution interval (Transformar intervalo de execução), especifique um intervalo em minutos, horas ou dias.

Etapa 4: Revisar e monitorar

Revise sua configuração e selecione Create (Criar). Em seguida, monitore a coluna Transform job status (Status do trabalho de transformação).

Etapa 5: Pesquisar o índice de destino

Após a conclusão do trabalho, você pode usar a API `_search` padrão para pesquisar o índice de destino.

Por exemplo, após executar um trabalho de transformação que transforma os dados de voo com base no campo `DestAirportID`, você poderá executar a seguinte solicitação para retornar todos os campos que têm um valor `SFO`:

```
GET target_index/_search
{
  "query": {
    "match": {
      "DestAirportID_terms" : "SFO"
    }
  }
}
```

Replicação entre clusters do Amazon OpenSearch Service

Com a replicação entre clusters no Amazon OpenSearch Service, você pode replicar índices de usuário, mapeamentos e metadados de um domínio do OpenSearch Service para outro. Usar a replicação entre clusters ajuda a garantir a recuperação de desastres em caso de interrupção, e permite replicar dados em datacenters geograficamente distantes para reduzir a latência. Você paga taxas de transferência de dados padrão da AWS pelos dados transferidos entre domínios.

A replicação entre clusters segue um modelo de replicação ativo-passivo em que o índice local ou seguidor extrai dados do índice remoto ou líder. O índice líder se refere à fonte dos dados ou ao

índice do qual você deseja replicar os dados. O índice de seguidores se refere ao destino dos dados ou ao índice para o qual você deseja replicar os dados.

A replicação entre clusters está disponível em domínios que executam a versão 7.10 do Elasticsearch ou 1.1 ou superior do OpenSearch. A documentação completa para replicação entre clusters está disponível na documentação do OpenSearch.

Tópicos

Limitações

A replicação entre clusters tem as seguintes limitações:

- Você não pode replicar dados entre domínios do Amazon OpenSearch Service ou clusters autogerenciados do OpenSearch ou do Elasticsearch.
- Você não pode replicar um índice de um domínio de seguidor para outro domínio de seguidor. Se você quiser replicar um índice para vários domínios de seguidores, só poderá replicá-lo a partir do único domínio líder.
- Um domínio pode ser conectado, por meio de uma combinação de conexões de entrada e saída, a um máximo de 20 outros domínios.
- Quando você configura inicialmente uma conexão entre clusters, o domínio líder deve estar na mesma versão ou em uma versão superior à do domínio seguidor.
- Você não pode usar o AWS CloudFormation para conectar domínios.
- Não é possível usar a replicação entre clusters em instâncias M3 ou expansíveis (T2 e T3).

- Você não pode replicar dados entre índices UltraWarm ou frios. Ambos os índices devem estar em um armazenamento quente.
- Quando você exclui um índice do domínio líder, o índice correspondente no domínio seguidor não é excluído automaticamente.

Pré-requisitos

Antes de configurar a replicação entre clusters, verifique se os domínios atendem aos seguintes requisitos:

- Elasticsearch 7.10 ou OpenSearch 1.1 ou superior
- Controle de acesso refinado habilitado
- Criptografia de nó para nó habilitada

Requisitos de permissão

Para iniciar a replicação, você deve incluir a permissão `es:ESCrossClusterGet` no domínio remoto (líder). Recomendamos a seguinte política do IAM no domínio remoto. Essa política também permite executar outras operações, como indexar documentos e executar pesquisas padrão:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:account:domain/leader-domain/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
```

```
      },
      "Action": "es:ESCrossClusterGet",
      "Resource": "arn:aws:es:region:account:domain/leader-domain"
    }
  ]
}
```

Verifique se a permissão `es:ESCrossClusterGet` é aplicada a `/leader-domain` e não a `/leader-domain/*`.

Para que usuários não administradores realizem atividades de replicação, também é preciso que eles sejam mapeados às permissões apropriadas. A maioria das permissões corresponde a operações de API REST específicas. Por exemplo, a permissão `indices:admin/plugins/replication/index/_resume` permite que você retome a replicação de um índice. Para obter uma lista completa de permissões, consulte Permissões de replicação na documentação do OpenSearch.

> **Note**
>
> Os comandos para iniciar a replicação e criar uma regra de replicação são casos especiais. Como eles invocam processos em segundo plano nos domínios líder e seguidor, você deve passar uma `leader_cluster_role` e uma `follower_cluster_role` pela solicitação. O OpenSearch Service usa essas funções em todas as tarefas de replicação de backend. Para obter informações sobre mapeamento e uso dessas funções, consulte Mapear as funções de cluster líder e seguidor na documentação do OpenSearch.

Configurar uma conexão entre clusters

Para replicar índices de um domínio para outro, você precisa configurar uma conexão entre clusters entre os domínios. A maneira mais fácil de conectar domínios é através da guia Conexões do painel de domínio. Você também pode usar a API de configuração ou a CLI da AWS. Como a replicação entre clusters segue um modelo “pull”, você inicia as conexões a partir do domínio seguidor.

> **Note**
>
> Se você conectou anteriormente dois domínios para executar pesquisas entre clusters, essa mesma conexão não pode ser usada para replicação. A conexão é marcada como `SEARCH_ONLY` no console. Para executar a replicação entre dois domínios conectados

anteriormente, você deve excluir a conexão e recriá-la. Assim que você tiver feito isso, a conexão estará disponível para a pesquisa entre clusters e a replicação entre clusters.

Como configurar uma conexão

1. No console do Amazon OpenSearch Service, selecione o domínio seguidor, vá para a guia Conexões e escolha Solicitar.
2. Em Alias de conexão , insira um nome para a conexão.
3. Escolha entre conectar-se a um domínio na sua Conta da AWS e região ou em outra conta ou região.
   - Para se conectar a um domínio em sua Conta da AWS e região, selecione o domínio e escolha Solicitar.
   - Para se conectar a um domínio em outra Conta da AWS ou região, especifique o ARN do domínio remoto e escolha Solicitar.

O OpenSearch Service valida a solicitação de conexão. Se os domínios forem incompatíveis, a conexão falhará. Se a validação for bem-sucedida, ela será enviada ao domínio de destino para aprovação. Quando o domínio de destino aprova a solicitação, você pode iniciar a replicação.

A replicação entre clusters oferece suporte à replicação bidirecional. Isso significa que você pode criar uma conexão de saída do domínio A para o domínio B e outra conexão de saída do domínio B para o domínio A. Você pode então configurar a replicação para que o domínio A siga um índice no domínio B e o domínio B siga um índice no domínio A.

Como iniciar a replicação

Depois de estabelecer uma conexão entre clusters, você pode começar a replicar dados. Primeiro, crie um índice no domínio líder a ser replicado:

```
PUT leader-01
```

Para replicar esse índice, envie esse comando ao domínio seguidor:

```
PUT _plugins/_replication/follower-01/_start
{
   "leader_alias": "connection-alias",
```

```
   "leader_index": "leader-01",
   "use_roles":{
      "leader_cluster_role": "all_access",
      "follower_cluster_role": "all_access"
   }
}
```

Você pode encontrar o alias de conexão na guia Conexões no painel do domínio.

Este exemplo pressupõe que um administrador esteja emitindo a solicitação e usa `all_access` para `leader_cluster_role` e `follower_cluster_role` para simplificar. Em ambientes de produção, no entanto, recomendamos que você crie usuários de replicação nos índices líder e seguidor e os mapeie de acordo. Os nomes de usuário devem ser idênticos. Para obter informações sobre essas funções e como mapeá-las, consulte Mapear as funções de cluster líder e seguidor na documentação do OpenSearch.

Confirmar replicação

Para confirmar se a replicação está acontecendo, obtenha o status da replicação:

```
GET _plugins/_replication/follower-01/_status

{
  "status" : "SYNCING",
  "reason" : "User initiated",
  "leader_alias" : "connection-alias",
  "leader_index" : "leader-01",
  "follower_index" : "follower-01",
  "syncing_details" : {
    "leader_checkpoint" : -5,
    "follower_checkpoint" : -5,
    "seq_no" : 0
  }
}
```

Os valores de ponto de verificação de líder e seguidor começam como números inteiros negativos e refletem o número de fragmentos que você tem (-1 para um fragmento, -5 para cinco fragmentos e assim por diante). Os valores aumentam para números inteiros positivos a cada alteração que você fizer. Se os valores forem os mesmos, significa que os índices estão totalmente sincronizados. Você pode usar esses valores de ponto de verificação para medir a latência de replicação em seus domínios.

Para validar ainda mais a replicação, adicione um documento ao índice líder:

```
PUT leader-01/_doc/1
{
   "Doctor Sleep":"Stephen King"
}
```

E confirme que ele aparece no índice de seguidor:

```
GET follower-01/_search

{
    ...
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "follower-01",
        "_type" : "_doc",
        "_id" : "1",
        "_score" : 1.0,
        "_source" : {
          "Doctor Sleep" : "Stephen King"
        }
      }
    ]
  }
}
```

Interromper e retomar a replicação

Você pode interromper temporariamente a replicação se precisar corrigir problemas ou reduzir a carga no domínio líder. Envie essa solicitação ao domínio seguidor. Certifique-se de incluir um corpo da solicitação vazio:

```
POST _plugins/_replication/follower-01/_pause
{}
```

Em seguida, obtenha o status para garantir que a replicação seja interrompida:

```
GET _plugins/_replication/follower-01/_status
```

```
{
  "status" : "PAUSED",
  "reason" : "User initiated",
  "leader_alias" : "connection-alias",
  "leader_index" : "leader-01",
  "follower_index" : "follower-01"
}
```

Quando terminar de fazer as alterações, retome a replicação. Envie essa solicitação ao domínio seguidor. Certifique-se de incluir um corpo da solicitação vazio:

```
POST _plugins/_replication/follower-01/_resume
{}
```

Não será possível retomar a replicação depois que ela for pausada por mais de 12 horas. Você deve interromper a replicação, excluir o índice de seguidores e reiniciar a replicação do líder.

Encerrar a replicação

Quando você encerra completamente a replicação, o índice seguidor deixa de seguir o líder e torna-se um índice padrão. Você não pode reiniciar uma replicação depois de encerrá-la.

Encerre a replicação do domínio seguidor. Certifique-se de incluir um corpo da solicitação vazio:

```
POST _plugins/_replication/follower-01/_stop
{}
```

Seguir automaticamente

Você pode definir um conjunto de regras de replicação em um único domínio líder que replica automaticamente índices correspondentes a um padrão especificado. Quando um índice no domínio líder corresponde a um dos padrões (por exemplo, `books*`), um índice de seguidor correspondente é criado no domínio seguidor. O OpenSearch Service replica quaisquer índices existentes que correspondam ao padrão, bem como novos índices que você cria. Não replica índices que já existem no domínio seguidor.

Para replicar todos os índices (com exceção dos índices criados pelo sistema e aqueles que já existem no domínio seguidor), use um padrão curinga (`*`).

Criar uma regra de replicação

Crie uma regra de replicação no domínio do seguidor e especifique o nome da conexão entre clusters:

```
POST _plugins/_replication/_autofollow
{
   "leader_alias" : "connection-alias",
   "name": "rule-name",
   "pattern": "books*",
   "use_roles":{
      "leader_cluster_role": "all_access",
      "follower_cluster_role": "all_access"
   }
}
```

Você pode encontrar o alias de conexão na guia Conexões no painel do domínio.

Este exemplo pressupõe que um administrador esteja emitindo a solicitação e usa `all_access` como as funções de domínio líder e seguidor para simplificar. Em ambientes de produção, no entanto, recomendamos que você crie usuários de replicação nos índices líder e seguidor e os mapeie de acordo. Os nomes de usuário devem ser idênticos. Para obter informações sobre essas funções e como mapeá-las, consulte Mapear as funções de cluster líder e seguidor na documentação do OpenSearch.

Para recuperar uma lista de regras de replicação existentes em um domínio, use a operação da API de estatísticas de auto-follow.

Para testar a regra, crie um índice que corresponda ao padrão no domínio líder:

```
PUT books-are-fun
```

E confira se sua réplica aparece no domínio seguidor:

```
GET _cat/indices

health status index          uuid                   pri rep docs.count docs.deleted
 store.size pri.store.size
green  open   books-are-fun  ldfHO78xYYdxRMULuiTvSQ     1   1          0            0
     208b           208b
```

Excluir uma regra de replicação

Quando você exclui uma regra de replicação, o OpenSearch Service para de replicar índices novos que correspondem ao padrão, mas continua a atividade de replicação existente até você encerrar a replicação desses índices.

Exclua regras de replicação do domínio seguidor:

```
DELETE _plugins/_replication/_autofollow
{
   "leader_alias" : "connection-alias",
   "name": "rule-name"
}
```

Atualizar domínios conectados

Para atualizar a versão do mecanismo de dois domínios que têm uma conexão entre clusters, atualize primeiro o domínio seguidor e depois o líder. Não exclua a conexão entre eles, caso contrário, a replicação será interrompida e não será possível retomá-la.

Migração de índices do Amazon OpenSearch Service usando reindexação remota

A reindexação remota permite copiar índices de um domínio do Amazon OpenSearch Service para outro. Você pode migrar índices de qualquer domínio de OpenSearch serviço ou clusters autogerenciados OpenSearch e do Elasticsearch.

Com domínio e índice remotos, se referem à fonte dos dados ou ao domínio e índice dos quais você deseja copiar os dados. Um domínio e índice local referem-se ao destino dos dados ou ao domínio e índice para os quais você deseja copiar os dados.

A reindexação remota exige OpenSearch 1.0 ou posterior, ou Elasticsearch 6.7 ou posterior, no domínio local. O domínio remoto deve ser inferior ou da mesma versão principal que o domínio local. As versões do Elasticsearch são consideradas inferiores às OpenSearch versões, o que significa que você pode reindexar dados de domínios do Elasticsearch para domínios. OpenSearch Dentro da mesma versão principal, o domínio remoto pode ser qualquer versão secundária. Por exemplo, a reindexação remota do Elasticsearch 7.10.x para 7.9 é suportada, mas OpenSearch 1.0 para o Elasticsearch 7.10.x não é suportada.

A documentação completa da `reindex` operação, incluindo etapas detalhadas e opções suportadas, está disponível na OpenSearchdocumentação.

Tópicos

Pré-requisitos

A reindexação remota tem os seguintes requisitos:

- O domínio remoto deve ser acessível pelo domínio local. Para um domínio remoto que reside em uma VPC, o domínio local deve ter acesso à VPC. Este processo varia de acordo com a configuração de rede, mas geralmente envolve a conexão a uma VPN ou rede gerenciada ou o uso a conexão de endpoint da VPC nativa. Para saber mais, consulte the section called “Suporte à VPC”.
- A solicitação deve ser autorizada pelo domínio remoto como qualquer outra solicitação REST. Se o domínio remoto tiver o controle de acesso detalhado habilitado, você deve ter permissão para executar a reindexação no domínio remoto e ler o índice no domínio local. Para obter mais considerações de segurança, consulte the section called “Controle de acesso refinado”.
- Recomendamos criar um índice com a configuração desejada no domínio local antes de iniciar o processo de reindexação.
- Se o domínio usar um tipo de instância T2 ou T3 para os nós de dados, não será possível usar a reindexação remota.

Reindexar dados entre os domínios da Internet OpenSearch do Serviço

O cenário mais básico é que o índice remoto esteja no mesmo Região da AWS que seu domínio local com um endpoint acessível ao público e você tenha assinado as credenciais do IAM.

A partir do domínio remoto, especifique o índice remoto do qual a reindexação será feita e o índice local para o qual reindexar:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443"
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

Você deve adicionar 443 no final do endpoint do domínio remoto para verificar a validade.

Para verificar se o índice foi copiado para o domínio local, envie essa solicitação para o domínio local:

```
GET local_index/_search
```

Se a reindexação remota estiver em uma região diferente do domínio local, passe seu nome de região, como nesta solicitação de exemplo:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "region": "eu-west-1"
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

No caso de regiões isoladas, como AWS GovCloud (US) regiões da China, o endpoint pode não estar acessível porque seu usuário do IAM não é reconhecido nessas regiões.

Se o domínio remoto estiver protegido com autenticação básica, especifique o nome de usuário e a senha:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "username": "username",
      "password": "password"
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

Reindexe dados entre domínios OpenSearch de serviço quando o controle remoto está em uma VPC

Cada domínio OpenSearch de serviço é composto por sua própria infraestrutura interna de nuvem privada virtual (VPC). Quando você cria um novo domínio em uma OpenSearch Service VPC existente, uma interface de rede elástica é criada para cada nó de dados na VPC.

Como a operação de reindexação remota é executada a partir do domínio de OpenSearch serviço remoto e, portanto, dentro de sua própria VPC privada, você precisa de uma forma de acessar a VPC do domínio local. Você pode fazer isso usando o recurso de conexão de endpoint VPC integrado para estabelecer uma conexão ou configurando um proxy. AWS PrivateLink

Se o seu domínio local usa a OpenSearch versão 1.0 ou posterior, você pode usar o console ou o AWS CLI para criar uma AWS PrivateLink conexão. Uma AWS PrivateLink conexão permite que os recursos na VPC local se conectem de forma privada aos recursos na VPC remota dentro da mesma. Região da AWS

Reindexe os dados com o AWS Management Console

Você pode usar a reindexação remota com o console para copiar índices entre dois domínios que compartilham uma conexão de endpoint da VPC.

1. Navegue até o console do Amazon OpenSearch Service emhttps://console.aws.amazon.com/aos/.
2. No painel de navegação à esquerda, escolha Domínios.
3. Selecione o domínio local ou o domínio para o qual você deseja copiar dados. Isso abre a página de detalhes do domínio. Selecione a guia Conexões abaixo das informações gerais e escolha Solicitar.
4. Na página Solicitar conexão, selecione Conexão de endpoint da VPC para seu modo de conexão e insira outros detalhes relevantes. Esses detalhes incluem o domínio remoto, que é o domínio do qual você deseja copiar dados. Em seguida, escolha Solicitar.
5. Navegue até a página de detalhes do domínio remoto, selecione a guia Conexões e encontre a tabela Conexões de entrada. Marque a caixa de seleção ao lado do nome do domínio do qual você acabou de criar a conexão (o domínio local). Escolha Aprovar.
6. Retorne ao domínio local, escolha a guia Conexões e encontre a tabela Conexões de saída. Depois que a conexão entre os dois domínios estiver ativa, um endpoint ficará disponível na coluna Endpoint na tabela. Copie o endpoint.
7. Abra o painel do domínio local e escolha Ferramentas de desevolvedor na barra de navegação à esquerda. Para confirmar que o índice do domínio remoto ainda não existe no seu domínio local, execute a seguinte solicitação GET. *remote-domain-index-name*Substitua pelo seu próprio nome de índice.

   ```
   GET remote-domain-index-name/_search
   {
      "query":{
         "match_all":{}
      }
   }
   ```

   Na saída, você verá um erro que indica que o índice não foi encontrado.
8. Abaixo da sua solicitação GET, crie uma solicitação POST e use seu endpoint como host remoto, da seguinte maneira.

   ```
   POST _reindex
   {
      "source":{
         "remote":{
            "host":"endpoint",
            "username":"username",
   ```

```
            "password":"password"
         },
         "index":"remote-domain-index-name"
      },
      "dest":{
         "index":"local-domain-index-name"
      }
}
```

Execute essa solicitação.

9. Execute a solicitação GET novamente. A saída agora deve indicar que o índice local existe. Você pode consultar esse índice para verificar se OpenSearch copiou todos os dados do índice remoto.

Reindexe dados com operações da API OpenSearch de serviço

Você pode usar a reindexação remota com a API para copiar índices entre dois domínios que compartilham uma conexão de endpoint da VPC.

1. Use a operação da CreateOutboundConnectionAPI para solicitar uma nova conexão do seu domínio local com seu domínio remoto.

```
POST https://es.region.amazonaws.com/2021-01-01/opensearch/cc/outboundConnection

{
   "ConnectionAlias": "remote-reindex-example",
   "ConnectionMode": "VPC_ENDPOINT",
   "LocalDomainInfo": {
      "AWSDomainInformation": {
         "DomainName": "local-domain-name",
         "OwnerId": "aws-account-id",
         "Region": "region"
      }
   },
   "RemoteDomainInfo": {
      "AWSDomainInformation": {
         "DomainName": "remote-domain-name",
         "OwnerId": "aws-account-id",
         "Region": "region"
      }
   }
```

```
}
```

Você recebe um `ConnectionId` na resposta. Salve essa ID para a próxima etapa.

2. Use a operação da AcceptInboundConnectionAPI com seu ID de conexão para aprovar a solicitação do domínio local.

```
PUT https://es.region.amazonaws.com/2021-01-01/opensearch/cc/
inboundConnection/ConnectionId/accept
```

3. Use a operação DescribeOutboundConnectionsda API para recuperar o endpoint do seu domínio remoto.

```
{
    "Connections": [
        {
            "ConnectionAlias": "remote-reindex-example",
            "ConnectionId": "connection-id",
            "ConnectionMode": "VPC_ENDPOINT",
            "ConnectionProperties": {
                "Endpoint": "connection-endpoint"
            },
            ...
        }
    ]
}
```

Salve o *endpoint de conexão* para usar na Etapa 5.

4. Para confirmar que o índice do domínio remoto ainda não existe no seu domínio local, execute a seguinte solicitação GET. *remote-domain-index-name*Substitua pelo seu próprio nome de índice.

```
GET local-domain-endpoint/remote-domain-index-name/_search
{
   "query":{
      "match_all":{}
   }
}
```

Na saída, você verá um erro que indica que o índice não foi encontrado.

5. Crie uma solicitação POST e use seu endpoint como host remoto, da seguinte maneira.

```
POST local-domain-endpoint/_reindex
{
   "source":{
      "remote":{
         "host":"connection-endpoint",
         "username":"username",
         "password":"password"
      },
      "index":"remote-domain-index-name"
   },
   "dest":{
      "index":"local-domain-index-name"
   }
}
```

   Execute essa solicitação.

6. Execute a solicitação GET novamente. A saída agora deve indicar que o índice local existe. Você pode consultar esse índice para verificar se OpenSearch copiou todos os dados do índice remoto.

Se o domínio remoto estiver hospedado em uma VPC e você não quiser usar o atributo de conexão endpoint da VPC, você deverá configurar um proxy com um endpoint acessível publicamente. Nesse caso, o OpenSearch Service exige um endpoint público porque não tem a capacidade de enviar tráfego para sua VPC.

Quando você executa um domínio no modo de VPC, um ou mais endpoints são colocados na sua VPC. No entanto, esses endpoints são apenas para tráfego que entra no domínio dentro da VPC e não permitem tráfego na própria VPC.

O comando remote reindex é executado a partir do domínio local, portanto, o tráfego de origem não consegue usar esses endpoints para acessar o domínio remoto. É por isso que um proxy é necessário nesse caso de uso. O domínio proxy deve ter um certificado assinado por uma autoridade de certificação (CA) pública. Não há suporte a certificados CA autoassinados ou privados.

Reindexe dados entre domínios que não são OpenSearch de serviço

Se o índice remoto estiver hospedado fora do OpenSearch Service, como em uma instância EC2 autogerenciada, defina o `external` parâmetro como: `true`

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "username": "username",
      "password": "password",
      "external": true
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

Nesse caso, somente a autenticação básica com nome de usuário e senha é suportada. O domínio remoto deve ter um endpoint acessível ao público (mesmo que esteja na mesma VPC do domínio de serviço OpenSearch local) e um certificado assinado por uma CA pública. Não há suporte para certificados CA autoassinados ou privados.

Reindexar conjuntos de dados grandes

A reindexação remota envia uma solicitação de rolagem para o domínio remoto com os seguintes valores padrão:

- Contexto de pesquisa de 5 minutos
- Tempo limite de soquete de 30 segundos
- Tamanho do lote 1.000

Recomendamos ajustar esses parâmetros para acomodar seus dados. Para documentos grandes, considere um tamanho de lote menor e/ou um tempo limite mais longo. Para obter mais informações sobre pesquisa, consulte Pesquisa de rolagem.

```
POST _reindex?pretty=true&scroll=10h&wait_for_completion=false
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "socket_timeout": "60m"
```

```
    },
    "size": 100,
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

Também recomendamos adicionar as seguintes configurações ao índice local para melhorar a performance:

```
PUT local_index
{
  "settings": {
    "refresh_interval": -1,
    "number_of_replicas": 0
  }
}
```

Após a conclusão do processo de reindexação, você poderá definir a contagem de réplicas desejada e remover a configuração de intervalo de atualização.

Para reindexar somente um subconjunto de documentos selecionados por meio de uma consulta, envie esta solicitação para o domínio local:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443"
    },
    "index": "remote_index",
    "query": {
      "match": {
        "field_name": "text"
      }
    }
  },
  "dest": {
    "index": "local_index"
  }
```

```
}
```

A reindexação remota não oferece suporte a fatiamento. Por isso, você não pode executar várias operações de rolagem para a mesma solicitação em paralelo.

Configurações da reindexação remota

Além das opções de reindexação padrão, o OpenSearch Service oferece suporte às seguintes opções:

Opções	Valores válidos	Descrição	Obrigatório
external	Booleano	Se o domínio remoto não for um domínio OpenSearch de serviço ou se você estiver reindexando entre dois domínios VPC, especifique como. `true`	Não
região	String	Se o domínio remoto estiver em uma região diferente, especifique o nome da região.	Não

Gerenciamento dados de séries temporais no Amazon OpenSearch Service com fluxos de dados

Um fluxo de trabalho típico para gerenciar dados de séries temporais envolve várias etapas, como criar um alias de índice de sobreposição, definir um índice de gravação e definir mapeamentos e configurações comuns para os índices de apoio.

Os fluxos de dados no Amazon OpenSearch Service ajudam a simplificar esse processo de configuração inicial. Os fluxos de dados funcionam “fora da caixa” para dados baseados em tempo, como logs de aplicações que, normalmente, são de natureza somente anexação.

Os fluxos de dados exigem o OpenSearch 1.0 ou posterior. A documentação completa do recurso está disponível na documentação do OpenSearch.

Conceitos básicos de fluxos de dados

Um fluxo de dados é composto internamente por vários índices de apoio. As solicitações de pesquisa são roteadas para todos os índices de apoio, enquanto as solicitações de indexação são roteadas para o índice de gravação mais recente.

Etapa 1: Criar um modelo de índice

Para criar um fluxo de dados, primeiro você precisa criar um modelo de índice que configura um conjunto de índices como um fluxo de dados. O objeto `data_stream` indica que ele é um fluxo de dados, e não um modelo de índice regular. O padrão de índice corresponde ao nome do fluxo de dados:

```
PUT _index_template/logs-template
{
  "index_patterns": [
    "my-data-stream",
    "logs-*"
  ],
  "data_stream": {},
  "priority": 100
}
```

Nesse caso, cada documento ingerido deve ter um campo `@timestamp`. Você também pode definir seu campo de datação personalizado como uma propriedade no objeto `data_stream`:

```
PUT _index_template/logs-template
{
  "index_patterns": "my-data-stream",
  "data_stream": {
    "timestamp_field": {
      "name": "request_time"
    }
  }
}
```

Etapa 2: Criar um stream de dados

Depois de criar um modelo de índice, você poderá começar a ingerir dados diretamente sem criar um fluxo de dados.

Porque temos um modelo de índice correspondente com um objeto `data_stream`, o OpenSearch cria automaticamente o fluxo de dados:

```
POST logs-staging/_doc
{
  "message": "login attempt failed",
  "@timestamp": "2013-03-01T00:00:00"
}
```

Etapa 3: Ingerir dados no fluxo de dados

Para ingerir dados em um fluxo de dados, você pode usar as APIs de indexação regulares. Certifique-se de que todos os documentos indexados tenham um campo de carimbo de data/hora. Se tentar ingerir um documento que não tenha um campo de carimbo de data/hora, você receberá uma mensagem de erro.

```
POST logs-redis/_doc
{
  "message": "login attempt",
  "@timestamp": "2013-03-01T00:00:00"
}
```

Etapa 4: Pesquisar um fluxo de dados

Você pode pesquisar um fluxo de dados da mesma forma que pesquisa um índice regular ou um alias de índice. A operação de pesquisa aplica-se a todos os índices de apoio (todos os dados presentes no fluxo).

```
GET logs-redis/_search
{
  "query": {
    "match": {
      "message": "login"
    }
  }
```

```
}
```

Etapa 5: Rolar um fluxo de dados

Você pode configurar um Gerenciamento de estados de índices (ISM) para automatizar o processo de rolagem para o fluxo de dados. A política do ISM é aplicada aos índices de apoio no momento da sua criação. Quando você associa uma política a um fluxo de dados, ela afeta apenas os índices de apoio futuros desse fluxo de dados. Você também não precisa fornecer a configuração `rollover_alias`, porque a política ISM infere essas informações do índice de suporte.

> **Note**
>
> Se você rolar um índice de apoio para o armazenamento a frio, o OpenSearch removerá esse índice do fluxo de dados. Mesmo se você mover o índice de volta para o UltraWarm, o índice permanecerá independente e não fará parte do fluxo de dados original. Depois que um índice for removido do fluxo de dados, a pesquisa no fluxo não retornará nenhum dado do índice.

> **Warning**
>
> O índice de gravação de um fluxo de dados não pode ser migrado para o armazenamento de baixa atividade. Se deseja migrar dados do seu fluxo de dados para o armazenamento de baixa atividade, você deve reverter o fluxo de dados antes da migração.

Etapa 6: Gerenciar fluxos de dados no OpenSearch Dashboards

Para gerenciar fluxos de dados via OpenSearch Dashboards, abra OpenSearch Dashboards, escolha Gerenciamento de índices, selecione Índices ou Índices gerenciados pela política.

Etapa 7: Excluir um fluxo de dados

A operação de exclusão primeiro exclui os índices de apoio de um fluxo de dados e, em seguida, exclui o próprio fluxo de dados.

Para excluir um fluxo de dados e todos os seus índices de apoio ocultos:

```
DELETE _data_stream/name_of_data_stream
```

Monitoramento de dados no Amazon OpenSearch Service

Monitore proativamente seus dados no Amazon OpenSearch Service com alertas e detecção de anomalias. Configure alertas para receber notificações quando seus dados excederem determinados limites. A detecção de anomalias usa o machine learning para detectar automaticamente todas as discrepâncias em seus dados de streaming. Você pode emparelhar a detecção de anomalias com alertas para garantir que seja notificado assim que uma anomalia for detectada.

Tópicos

Configurando alertas no Amazon Service OpenSearch

Configure alertas no Amazon OpenSearch Service para ser notificado quando os dados de um ou mais índices atenderem a determinadas condições. Por exemplo, talvez você queira receber um e-mail se a aplicação registrar mais de cinco erros HTTP 503 em uma hora, ou talvez queira notificar um desenvolvedor caso nenhum documento novo tenha sido indexado nos últimos 20 minutos.

O alerta requer o Elasticsearch 6.2 OpenSearch ou posterior. Para ver a documentação completa, incluindo as descrições da API, consulte Alertas na OpenSearch documentação. Este tópico destaca as diferenças nos alertas no OpenSearch Service em comparação com a versão de código aberto.

Tópicos

Permissões de alertas

O recurso de alertas oferece suporte ao controle de acesso refinado. Para obter detalhes sobre como combinar e combinar permissões de acordo com seu caso de uso, consulte Segurança de alertas na OpenSearch documentação.

Para acessar a página de alertas nos OpenSearch painéis, você deve pelo menos estar mapeado para a função `alerting_read_access` predefinida ou receber permissões equivalentes. Essa função concede permissões para visualizar alertas, destinos e monitores, mas não para reconhecer alertas ou modificar destinos ou monitores.

Conceitos básicos dos alertas

Para criar um alerta, você configura um monitor, que é um trabalho executado em uma programação definida e consulta OpenSearch índices. Você também configura um ou mais acionadores, que definem as condições que geram os eventos. Finalmente, você configura ações, que é o que acontece depois que um alerta é acionado.

Para começar a usar alertas

1. Escolha Alertas no menu principal OpenSearch Painéis e escolha Criar monitor.
2. Crie um monitor por consulta, por bucket, por métrica de cluster ou por documento. Para obter instruções, consulte Criar um monitor.
3. Em Triggers (Acionadores), crie um ou mais acionadores. Para obter instruções, consulte Criação de acionadores.
4. Em Actions (Ações), configure um canal de notificação para o alerta. Escolha entre Slack, Amazon Chime, um webhook personalizado ou Amazon SNS. Como você pode imaginar, as notificações exigem conectividade com o canal. Por exemplo, seu domínio do OpenSearch Serviço deve ser capaz de se conectar à Internet para notificar um canal do Slack ou enviar um webhook personalizado para um servidor de terceiros. O webhook personalizado deve ter um endereço IP público para que um domínio OpenSearch de serviço envie alertas para ele.

   > **Tip**
   >
   > Após uma ação enviar uma mensagem com êxito, proteger o acesso a essa mensagem (por exemplo, acesso a um canal do Slack) é sua responsabilidade. Se o seu domínio contiver dados confidenciais, considere usar acionadores sem ações e verificar periodicamente o Dashboards em busca de alertas.

Notificações

O alerta se integra ao Notifications, que é um sistema unificado para OpenSearch notificações. O Notifications permite que você configure qual serviço de comunicação você deseja usar e veja

estatísticas relevantes e informações de solução de problemas. Para obter uma documentação abrangente, consulte Notificações na OpenSearch documentação.

Seu domínio deve estar executando a OpenSearch versão 2.3 ou posterior para usar as notificações.

> **Note**
>
> OpenSearch as notificações são separadas das notificações de OpenSearch serviço, que fornecem detalhes sobre atualizações do software de serviço, aprimoramentos do Auto-Tune e outras informações importantes em nível de domínio. OpenSearch as notificações são específicas do plug-in.

Os canais de notificação substituíram os destinos de alerta a partir da OpenSearch versão 2.0. Os destinos foram oficialmente descontinuados e todas as notificações de alertas serão gerenciadas por meio de canais daqui para frente.

Quando você atualiza seus domínios para a versão 2.3 ou posterior (já que o suporte do OpenSearch Service para 2.x começa com 2.3), seus destinos existentes são migrados automaticamente para os canais de notificação. Se houver falha na migração deum destino, o monitor continuará a usá-lo até que o monitor seja migrado para um canal de notificação. Para obter mais informações, consulte Perguntas sobre destinos na OpenSearch documentação.

Para começar a usar as notificações, faça login nos OpenSearch painéis e escolha Notificações, Canais e Criar canal.

Amazon Simple Notification Service (Amazon SNS) é um tipo de canal compatível com notificações. Para autenticar usuários, você precisa fornecer ao usuário acesso total ao Amazon SNS, ou permitir que ele assuma um perfil do IAM que tenha permissões para acessar o Amazon SNS. Para obter instruções, consulte Amazon SNS como um tipo de canal.

Diferenças

Em comparação com a versão de código aberto do OpenSearch, os alertas no Amazon OpenSearch Service têm algumas diferenças notáveis.

Configurações de alertas

OpenSearch O serviço permite que você modifique as seguintes configurações de alerta:

- `plugins.scheduled_jobs.enabled`
- `plugins.alerting.alert_history_enabled`
- `plugins.alerting.alert_history_max_age`
- `plugins.alerting.alert_history_max_docs`
- `plugins.alerting.alert_history_retention_period`
- `plugins.alerting.alert_history_rollover_period`
- `plugins.alerting.filter_by_backend_roles`

Todas as outras configurações usam os valores padrão que não podem ser alterados.

Para desabilitar o alerta, envie a seguinte solicitação:

```
PUT _cluster/settings
{
  "persistent" : {
    "plugins.scheduled_jobs.enabled" : false
  }
}
```

A solicitação a seguir configura o alerta para excluir automaticamente os índices de histórico após sete dias, em vez dos 30 dias padrão:

```
PUT _cluster/settings
{
  "persistent": {
    "plugins.alerting.alert_history_retention_period": "7d"
  }
}
```

Se você criou monitores anteriormente e deseja interromper a criação de índices de alertas diários, exclua todos os índices de histórico de alertas:

```
DELETE .plugins-alerting-alert-history-*
```

Para reduzir a contagem de fragmentos para índices históricos, crie um modelo de índice. A solicitação a seguir define índices de histórico para alertas em um fragmento e uma réplica:

```
PUT _index_template/template-name
```

```
{
  "index_patterns": [".opendistro-alerting-alert-history-*"],
  "template": {
    "settings": {
      "number_of_shards": 1,
      "number_of_replicas": 1
    }
  }
}
```

Dependendo da sua tolerância à perda de dados, você pode até considerar o uso de réplicas zero. Para obter mais informações sobre como criar e gerenciar modelos de índice, consulte Modelos de índice na OpenSearch documentação.

Detecção de anomalias no Amazon OpenSearch Service

O recurso de detecção de anomalias no Amazon OpenSearch Service detecta automaticamente anomalias em seus dados do OpenSearch em tempo quase real usando o algoritmo RCF (Random Cut Forest). O RCF é um algoritmo de machine learning não supervisionado que modela um esboço do fluxo de dados de entrada. O algoritmo calcula um valor de `anomaly grade` e `confidence score` para cada ponto de dados de entrada. A detecção de anomalias usa esses valores para diferenciar uma anomalia de variações normais nos dados.

Você pode emparelhar o plug-in de detecção de anomalias com o plug-in the section called “Geração de alertas” para receber uma notificação assim que for detectada uma anomalia.

A detecção de anomalias está disponível em domínios que executam qualquer versão do OpenSearch ou Elasticsearch 7.4 ou posterior. Todos os tipos de instâncias oferecem suporte à detecção de anomalias, exceto `t2.micro` e `t2.small`. A documentação completa da detecção de anomalias, incluindo as etapas e descrições detalhadas da API, está disponível na documentação do OpenSearch.

Pré-requisitos

A detecção de anomalias apresenta os seguintes pré-requisitos:

- A detecção de anomalias requer o OpenSearch ou Elasticsearch 7.4 ou posterior.
- A detecção de anomalias só oferece suporte ao controle de acesso refinado no Elasticsearch versões 7.9 e posteriores e em todas as versões do OpenSearch. Antes do Elasticsearch 7.9, somente usuários administradores podiam criar, visualizar e gerenciar detectores.

- Se seu domínio usa o controle de acesso refinado, os usuários não administradores deverão ser mapeados na função `anomaly_read_access` no OpenSearch Dashboards para poder visualizar detectores ou na função `anomaly_full_access` para poder criar e gerenciar detectores.

Conceitos básicos da detecção de anomalias

Para começar a usar, escolha Anomaly Detection (Detecção de anomalias) no OpenSearch Dashboards.

Etapa 1: Criar um detector

Um detector é uma tarefa individual de detecção de anomalias. Você pode criar vários detectores, e todos os detectores podem ser executados simultaneamente, com cada um efetuando análises de dados de diferentes fontes.

Etapa 2: Adicionar recursos ao detector

Um recurso é o campo no índice que você verifica em busca de anomalias. Um detector pode descobrir anomalias em um ou mais recursos. Você deve escolher uma das agregações a seguir para cada recurso: `average()`, `sum()`, `count()`, `min()` ou `max()`.

> **Note**
>
> O método de agregação `count()` só está disponível no OpenSearch e no Elasticsearch 7.7 ou posterior. Para o Elasticsearch 7.4, use uma expressão personalizada como a seguinte:

```
{
  "aggregation_name": {
     "value_count": {
        "field": "field_name"
     }
  }
}
```

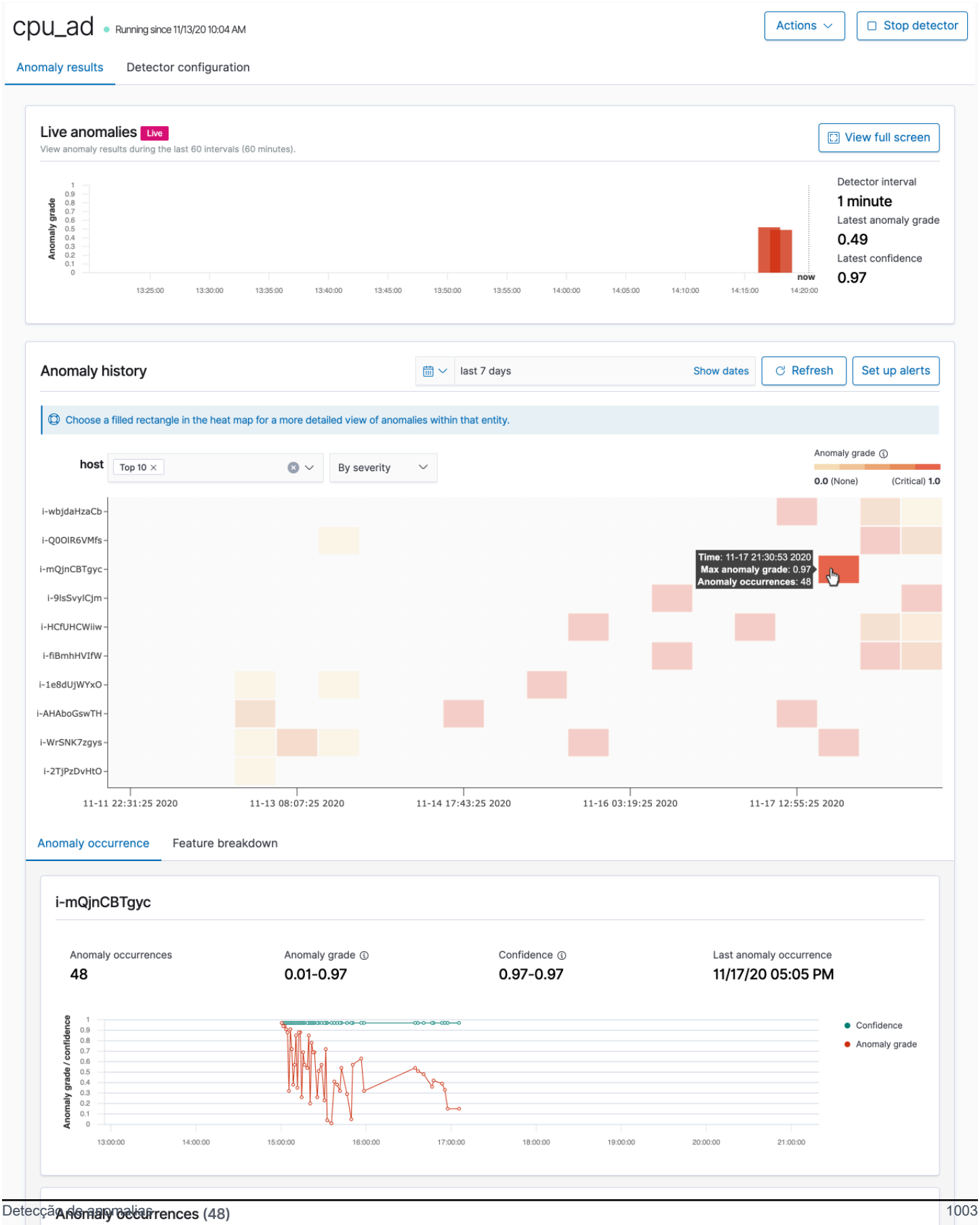
O método de agregação determina o que constitui uma anomalia. Por exemplo, se você escolher `min()`, o detector se concentrará em encontrar anomalias com base nos valores mínimos de seu recurso. Se você escolher `average()`, o detector encontrará anomalias com base nos valores médios de seu recurso. Você pode adicionar um máximo de cinco recursos por detector.

Você pode definir as seguintes configurações opcionais (disponíveis no Elasticsearch 7.7 e posterior):

- Category (Categoria): categorize ou corte seus dados com uma dimensão como endereço IP, ID do produto, código do país e assim por diante.
- Window size (Tamanho da janela): defina o número de intervalos de agregação do fluxo de dados a considerar em uma janela de detecção.

Depois de configurar seus recursos, visualize anomalias de amostra e ajuste as configurações do recurso, se necessário.

Etapa 3: Observar os resultados



- Live anomalies (Anomalias em tempo real): exibe os resultados das anomalias em tempo real dos últimos 60 intervalos. Por exemplo, se o intervalo for definido como 10, ele mostra os resultados dos últimos 600 minutos. Esse gráfico é atualizado a cada 30 segundos.
- Anomaly history (Histórico da anomalia): plota o grau da anomalia com a medida de confiança correspondente.
- Feature breakdown (Detalhamento de recurso): plota os recursos com base no método de agregação. É possível variar o intervalo de data e hora do detector.
- Anomaly occurrence (Ocorrência das anomalias) mostra os valores de `Start time`, `End time`, `Data confidence` e `Anomaly grade` para cada anomalia detectada.

  Se você definir o campo de categoria, verá um gráfico de Mapa de calor adicional que correlaciona resultados para entidades anômalas. Escolha um retângulo preenchido para obter uma visualização mais detalhada da anomalia.

Etapa 4: Configurar alertas

Para criar um monitor para enviar notificações quando qualquer anomalia for detectada, escolha Configurar alertas. O plugin redireciona você para a página Add monitor (Adicionar monitor), onde você pode configurar um alerta.

Tutorial: Detectar uso elevado da CPU com detecção de anomalias

Este tutorial demonstra como criar um detector de anomalias no Amazon OpenSearch Service para detectar uso elevado da CPU. Você usará o OpenSearch Dashboards para configurar um detector para monitorar o uso da CPU e gerar um alerta quando o uso da CPU ultrapassar um limite especificado.

> **Note**
>
> Essas etapas se aplicam à versão mais recente do OpenSearch e podem ser ligeiramente diferentes para as versões anteriores.

Pré-requisitos

- É necessário ter um domínio do OpenSearch Service executando o Elasticsearch 7.4 ou posterior ou qualquer versão do OpenSearch.

- Também é necessário estar ingerindo arquivos de log de aplicação em seu cluster que contêm dados de uso da CPU.

Etapa 1: Criar um detector

Primeiro, crie um detector que identifique anomalias nos dados de uso da CPU.

1. Abra o menu do painel esquerdo noOpenSearch Dashboards e escolha Anomaly Detection (Detecção de anomalias) e, em seguida, Create detector (Criar detector).
2. Nomeie o detector como **`high-cpu-usage`**.
3. Para sua fonte de dados, escolha o índice que contém os arquivos de log de uso da CPU em que deseja identificar anomalias.
4. Selecione o Timestamp field (Campo de identificação de data/hora) dos dados. Opcionalmente, é possível adicionar um filtro de dados. Esse filtro de dados analisa apenas um subconjunto da fonte de dados e reduz o ruído dos dados que não são relevantes.
5. Defina o Detector interval (Intervalo do detector) como 2 minutos. Esse intervalo define o tempo (por intervalo de minutos) para o detector coletar os dados.
6. Em Window delay (Atraso da janela), adicione um atraso de 1 minuto. Esse atraso adiciona tempo de processamento extra para garantir que todos os dados dentro da janela estejam presentes.
7. Escolha Next (Próximo). No painel de detecção de anomalias, embaixo do nome do detector, escolha Configure model (Configurar modelo).
8. Em Feature name (Nome do recurso), insira **`max_cpu_usage`**. Em Feature state (Estado do recurso), selecione Enable feature (Habilitar recurso).
9. Em Find anomalies based on (Encontrar anomalias com base em), escolha Field value (Valor do campo).
10. Em Aggregation method (Método de agregação), escolha **`max()`**.
11. Em Field (Campo), selecione o campo nos dados que será verificado em busca de anomalias. Por exemplo, ele pode ser chamado de `cpu_usage_percentage`.
12. Mantenha todas as outras configurações em seus valores padrão e escolha Next (Próximo).
13. Ignore a configuração de trabalhos do detector e escolha Next (Próximo).
14. Na janela pop-up, escolha quando iniciar o detector (automática ou manualmente) e escolha Confirm (Confirmar).

Agora que o detector está configurado, depois que ele inicializar, você poderá ver os resultados em tempo real de uso da CPU na seção Real-time results (Resultados em tempo real) do painel do detector. A seção Live anomalies (Anomalias ao vivo) exibe todas as anomalias que ocorrem à medida que os dados são ingeridos em tempo real.

Etapa 2: Configurar um alerta

Agora que você criou um detector, crie um monitor que invoque um alerta para enviar uma mensagem ao Slack quando ele detectar uso da CPU que atenda às condições especificadas nas configurações do detector. Você receberá notificações do Slack quando os dados de um ou mais índices atenderem às condições que invocam o alerta.

1. Abra o menu do painel esquerdo no OpenSearch Dashboards e escolha Alerting (Alertas) e, em seguida, Create monitor (Criar monitor).
2. Informe um nome para o monitor.
3. Em Monitor type (Tipo de monitor), escolha Per-query monitor (Monitor por consulta). Um monitor por consulta executa uma consulta especificada e define os acionadores.
4. Em Monitor defining method (Método de definição do monitor), escolha Anomaly detector (Detector de anomalias) e, em seguida, selecione no menu suspenso Detector o detector criado na seção anterior.
5. Para Schedule (Programação), escolha a frequência com que o monitor coleta dados e a frequência com que você recebe alertas. Para este tutorial, defina a programação para executar a cada 7minutos.
6. Na seção Triggers (Acionadores), escolha Add trigger (Adicionar acionador). Em Trigger name (Nome do acionador), insira **`High CPU usage`**. Para fins deste tutorial, em Severity level (Nível de severidade), escolha1, o nível mais elevado de severidade.
7. Em Anomaly grade threshold (Limite de grau da anomalia), escolha IS ABOVE (ESTÁ ACIMA). No menu embaixo dessa opção, escolha o limite de grau a ser aplicado. Para este tutorial, defina Anomaly grade (Grau da anomalia) como 0,7.
8. Em Anomaly confidence threshold (Limite de confiança da anomalia), escolha IS ABOVE (ESTÁ ACIMA). No menu embaixo dessa opção, escolha o mesmo número que o grau da anomalia. Para este tutorial, defina Anomaly confidence threshold (Limite de confiança da anomalia) como 0,7.
9. Na seção Actions (Ações), escolha Destination (Destino). No campo Name (Nome), escolha o nome do destino. No menu Type (Tipo), escolha Slack. No campo Webhook URL (URL do webhook), insira um URL de webhook para receber alertas. Para obter mais informações, consulte Sending messages using incoming webhooks (Enviar mensagens usando webhooks recebidos).

10 Escolha Create (Criar).

Recursos relacionados

- the section called “Geração de alertas”

- the section called “Detecção de anomalias”
- Anomaly detection API (API de detecção de anomalias)

Aprendizado de máquina para Amazon OpenSearch Service

O ML Commons é um OpenSearch plug-in que fornece um conjunto de algoritmos comuns de aprendizado de máquina (ML) por meio de chamadas de transporte e da API REST. Essas chamadas escolhem os nós e os recursos certos para cada solicitação de ML e monitoram as tarefas de ML para garantir o tempo de atividade. Isso permite que você aproveite os algoritmos de ML de código aberto existentes e reduza o esforço necessário para desenvolver novos atributos de ML. Para saber mais sobre o plug-in, consulte Aprendizado de máquina na OpenSearch documentação. Este capítulo aborda como usar o plug-in com o Amazon OpenSearch Service.

Tópicos

Conectores Amazon OpenSearch Service ML para Serviços da AWS

Ao usar conectores de aprendizado de máquina (ML) do Amazon OpenSearch Service com outros AWS service (Serviço da AWS), você precisa configurar uma função do IAM para conectar o serviço com segurança a esse OpenSearch serviço. Serviços da AWS que você pode configurar um conector para incluir Amazon SageMaker e Amazon Bedrock. Neste tutorial, abordamos como criar um conector do OpenSearch Service ao SageMaker Runtime. Para obter mais informações sobre conectores, consulte Conectores compatíveis.

Tópicos

Pré-requisitos

Para criar um conector, você deve ter um endpoint do Amazon SageMaker Domain e uma função do IAM que conceda acesso ao OpenSearch serviço.

Configurar um SageMaker domínio da Amazon

Consulte Implantar um modelo na Amazon SageMaker no Amazon SageMaker Developer Guide para implantar seu modelo de aprendizado de máquina. Observe o URL do endpoint do seu modelo, que você precisa para criar um conector de IA.

Criar um perfil do IAM

Configure uma função do IAM para delegar permissões SageMaker de tempo de execução ao OpenSearch serviço. Para criar um novo perfil, consulte Como criar um perfil do IAM (console) no Guia do usuário do IAM. Opcionalmente, você pode usar um perfil existente, desde que tenha o mesmo conjunto de privilégios. Se você criar uma nova função em vez de usar uma função AWS gerenciada, substitua `opensearch-sagemaker-role` neste tutorial pelo nome da sua própria função.

1. Anexe a seguinte política gerenciada de IAM à sua nova função para permitir que o OpenSearch Serviço acesse seu SageMaker endpoint. Para anexar uma política a uma função, consulte Adicionar permissões de identidade do IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sagemaker:InvokeEndpointAsync",
                "sagemaker:InvokeEndpoint"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

2. Siga as instruções em Modificação da política de confiança de um perfil para editar a relação de confiança do perfil. Você deve especificar OpenSearch Serviço na `Principal` declaração:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
```

```
                "sts:AssumeRole"
            ],
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "opensearchservice.amazonaws.com"
                ]
            }
        }
    ]
}
```

Recomendamos que você use as chaves de condição `aws:SourceAccount` e `aws:SourceArn` para limitar o acesso a um domínio específico. `SourceAccount`É o Conta da AWS ID que pertence ao proprietário do domínio e `SourceArn` é o ARN do domínio. Por exemplo, você pode adicionar o bloco de condições a seguir na política de confiança:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

Configurar permissões do

Para criar o conector, você precisa de permissão para passar a função do IAM para o OpenSearch Serviço. Você também precisa de acesso à ação `es:ESHttpPost`. Para conceder ambas as permissões, anexe a seguinte política ao perfil do IAM cujas credenciais estão sendo usadas para assinar a solicitação:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/opensearch-sagemaker-role"
```

```
    },
    {
      "Effect": "Allow",
      "Action": "es:ESHttpPost",
      "Resource": "arn:aws:es:region:account-id:domain/domain-name/*"
    }
  ]
}
```

Se seu usuário ou função não tiver permissões `iam:PassRole` para passar sua função, talvez você encontre o seguinte erro de autorização ao tentar registrar um repositório na próxima etapa.

Mapeie a função de ML em OpenSearch painéis (se estiver usando controle de acesso refinado)

O controle minucioso de acesso introduz uma etapa adicional ao configurar um conector. Mesmo que você use a autenticação básica HTTP para todos os outros fins, será necessário mapear o perfil `ml_full_access` para o seu perfil do IAM que tem permissões `iam:PassRole` para passar `opensearch-sagemaker-role`.

1. Navegue até o plug-in OpenSearch Dashboards do seu domínio OpenSearch de serviço. Você pode encontrar o endpoint do Dashboards no painel do seu domínio no console de OpenSearch serviços.
2. No menu principal, escolha Segurança, Funções e selecione a função ml_full_access.
3. Escolha Usuários mapeados e Gerenciar mapeamento.
4. Em Funções de backend, adicione o ARN da função que tem permissão para aprovar `opensearch-sagemaker-role`.

   ```
   arn:aws:iam::account-id:role/role-name
   ```

5. Selecione Mapa e confirme se o usuário ou função aparece em Usuários mapeados.

Crie um conector OpenSearch de serviço

Para criar um conector, envie uma `POST` solicitação para o endpoint do domínio OpenSearch Service. Você pode usar curl, o cliente Python de amostra, o Postman ou outro método para enviar uma solicitação assinada. Você não pode usar uma solicitação `POST` no console do Kibana. O cabeçalho assume o seguinte formato:

```
POST domain-endpoint/_plugins/_ml/connectors/_create
{
   "name": "sagemaker: embedding",
   "description": "Test connector for Sagemaker embedding model",
   "version": 1,
   "protocol": "aws_sigv4",
   "credential": {
      "roleArn": "arn:aws:iam::account-id:role/opensearch-sagemaker-role"
   },
   "parameters": {
      "region": "region",
      "service_name": "sagemaker"
   },
   "actions": [
      {
         "action_type": "predict",
         "method": "POST",
         "headers": {
            "content-type": "application/json"
         },
         "url": "https://runtime.sagemaker.region.amazonaws.com/endpoints/endpoint-id/
invocations",
         "request_body": "{ \"inputs\": { \"question\": \"${parameters.question}\",
 \"context\": \"${parameters.context}\" } }"
      }
   ]
}
```

Se o domínio residir em uma nuvem privada virtual (VPC), o computador deverá estar conectado à VPC para que a solicitação crie o conector de IA com êxito. O acesso a uma VPC varia de acordo com a configuração de rede, mas geralmente requer uma conexão com VPN ou rede corporativa. Para verificar se você pode acessar seu domínio OpenSearch de serviço, navegue até `https://your-vpc-domain.region.es.amazonaws.com` em um navegador da Web e verifique se você recebeu a resposta JSON padrão.

Exemplo de cliente do Python

O cliente Python é mais simples de automatizar do que uma solicitação HTTP, além de ser mais fácil reutilizá-lo. Para criar o conector AI com o cliente Python, salve o código de exemplo a seguir em um arquivo Python. O cliente requer os pacotes AWS SDK for Python (Boto3), `requests` e `requests-aws4auth`.

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

host = 'domain-endpoint/'
region = 'region'
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

# Register repository
path = '_plugins/_ml/connectors/_create'
url = host + path

payload = {
   "name": "sagemaker: embedding",
   "description": "Test connector for Sagemaker embedding model",
   "version": 1,
   "protocol": "aws_sigv4",
   "credential": {
      "roleArn": "arn:aws:iam::account-id:role/opensearch-sagemaker-role"
   },
   "parameters": {
      "region": "region",
      "service_name": "sagemaker"
   },
   "actions": [
      {
         "action_type": "predict",
         "method": "POST",
         "headers": {
            "content-type": "application/json"
         },
         "url": "https://runtime.sagemaker.region.amazonaws.com/endpoints/endpoint-id/
invocations",
         "request_body": "{ \"inputs\": { \"question\": \"${parameters.question}\",
 \"context\": \"${parameters.context}\" } }"
      }
   ]
}
headers = {"Content-Type": "application/json"}
```

```
r = requests.post(url, auth=awsauth, json=payload, headers=headers)
print(r.status_code)
print(r.text)
```

Conectores Amazon OpenSearch Service ML para plataformas de terceiros

Neste tutorial, abordamos como criar um conector do OpenSearch Service ao Cohere. Para obter mais informações sobre conectores, consulte Conectores compatíveis.

Ao usar um conector de aprendizado de máquina (ML) do Amazon OpenSearch Service com um modelo remoto externo, você precisa armazenar suas credenciais de autorização específicas em AWS Secrets Manager. Isso pode ser uma chave de API ou uma combinação de nome de usuário e senha. Isso significa que você também precisa criar uma função do IAM que permita que o OpenSearch serviço acesse a leitura do Secrets Manager.

Tópicos

Pré-requisitos

Para criar um conector para o Cohere ou qualquer provedor externo com o OpenSearch Service, você deve ter uma função do IAM que conceda acesso ao OpenSearch Service AWS Secrets Manager, onde você armazena suas credenciais. Você também deve armazenar suas credenciais no Secrets Manager.

Criar um perfil do IAM

Configure uma função do IAM para delegar permissões do Secrets Manager ao OpenSearch Service. Você também pode usar a função `SecretManagerReadWrite` existente. Para criar um novo perfil, consulte Como criar um perfil do IAM (console) no Guia do usuário do IAM. Se você criar uma nova função em vez de usar uma função AWS gerenciada, substitua `opensearch-secretmanager-role` neste tutorial pelo nome da sua própria função.

1. Anexe a seguinte política gerenciada do IAM à sua nova função para permitir que o OpenSearch Service acesse seus valores do Secrets Manager. Para anexar uma política ao perfil, consulte Como adicionar permissões de identidade do IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

2. Siga as instruções em Modificação da política de confiança de um perfil para editar a relação de confiança do perfil. Você deve especificar OpenSearch Serviço na `Principal` declaração:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "opensearchservice.amazonaws.com"
                ]
            }
        }
    ]
}
```

   Recomendamos que você use as chaves de condição `aws:SourceAccount` e `aws:SourceArn` para limitar o acesso a um domínio específico. `SourceAccount`É o Conta da AWS ID que pertence ao proprietário do domínio e `SourceArn` é o ARN do domínio. Por exemplo, você pode adicionar o bloco de condições a seguir na política de confiança:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

Configurar permissões do

Para criar o conector, você precisa de permissão para passar a função do IAM para o OpenSearch Serviço. Você também precisa de acesso à ação `es:ESHttpPost`. Para conceder ambas as permissões, anexe a seguinte política ao perfil do IAM cujas credenciais estão sendo usadas para assinar a solicitação:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/opensearch-secretmanager-role"
    },
    {
      "Effect": "Allow",
      "Action": "es:ESHttpPost",
      "Resource": "arn:aws:es:region:account-id:domain/domain-name/*"
    }
  ]
}
```

Se seu usuário ou função não tiver permissões `iam:PassRole` para passar sua função, talvez você encontre o seguinte erro de autorização ao tentar registrar um repositório na próxima etapa.

Configurar AWS Secrets Manager

Para armazenar suas credenciais de autorização no Secrets Manager, consulte Como criar um segredo AWS Secrets Manager no Guia do usuário da AWS Secrets Manager .

Depois que o Secrets Manager aceitar seu par de valores-chave como segredo, você recebe um ARN com o formato: `arn:aws:secretsmanager:us-west-2:123456789012:secret:MySecret-a1b2c3` Mantenha um registro desse ARN, conforme você o usa, e da sua chave ao criar um conector na próxima etapa.

Mapeie a função de ML em OpenSearch painéis (se estiver usando controle de acesso refinado)

O controle minucioso de acesso introduz uma etapa adicional ao configurar um conector. Mesmo que você use a autenticação básica HTTP para todos os outros fins, será necessário mapear o perfil `ml_full_access` para o seu perfil do IAM que tem permissões `iam:PassRole` para passar `opensearch-sagemaker-role`.

1. Navegue até o plug-in OpenSearch Dashboards do seu domínio OpenSearch de serviço. Você pode encontrar o endpoint do Dashboards no painel do seu domínio no console de OpenSearch serviços.
2. No menu principal, escolha Segurança, Funções e selecione a função ml_full_access.
3. Escolha Usuários mapeados e Gerenciar mapeamento.
4. Em Funções de backend, adicione o ARN da função que tem permissão para aprovar `opensearch-sagemaker-role`.

   ```
   arn:aws:iam::account-id:role/role-name
   ```

5. Selecione Mapa e confirme se o usuário ou função aparece em Usuários mapeados.

Crie um conector OpenSearch de serviço

Para criar um conector, envie uma `POST` solicitação para o endpoint do domínio OpenSearch Service. Você pode usar curl, o cliente Python de amostra, o Postman ou outro método para enviar uma solicitação assinada. Você não pode usar uma solicitação `POST` no console do Kibana. O cabeçalho assume o seguinte formato:

```
POST domain-endpoint/_plugins/_ml/connectors/_create
{
    "name": "Cohere Connector: embedding",
    "description": "The connector to cohere embedding model",
    "version": 1,
    "protocol": "http",
```

```
    "credential": {
        "secretArn": "arn:aws:secretsmanager:region:account-id:secret:cohere-key-id",
        "roleArn": "arn:aws:iam::account-id:role/opensearch-secretmanager-role"
    },
    "actions": [
        {
            "action_type": "predict",
            "method": "POST",
            "url": "https://api.cohere.ai/v1/embed",
            "headers": {
                "Authorization": "Bearer ${credential.secretArn.cohere-key-used-in-
secrets-manager}"
            },
            "request_body": "{ \"texts\": ${parameters.texts}, \"truncate\": \"END\" }"
        }
    ]
}
```

De duas maneiras, o corpo dessa solicitação é diferente do de uma solicitação de conector de código aberto. Dentro do `credential` campo, você passa o ARN para a função do IAM que permite que o OpenSearch Service leia do Secrets Manager, junto com o ARN para o segredo de quê. No campo `headers`, você se refere ao segredo usando a chave secreta e o fato de ser proveniente de um ARN.

Se o domínio residir em uma nuvem privada virtual (VPC), seu computador deverá estar conectado à VPC para que a solicitação crie o conector de IA com êxito. O acesso a uma VPC varia de acordo com a configuração de rede, mas geralmente requer uma conexão com VPN ou rede corporativa. Para verificar se você pode acessar seu domínio OpenSearch de serviço, navegue até `https://your-vpc-domain.region.es.amazonaws.com` em um navegador da Web e verifique se você recebeu a resposta JSON padrão.

Exemplo de cliente do Python

O cliente Python é mais simples de automatizar do que uma solicitação HTTP, além de ser mais fácil reutilizá-lo. Para criar o conector AI com o cliente Python, salve o código de exemplo a seguir em um arquivo Python. O cliente requer os pacotes AWS SDK for Python (Boto3), `requests` e `requests-aws4auth`.

```
import boto3
import requests
from requests_aws4auth import AWS4Auth
```

```
host = 'domain-endpoint/'
region = 'region'
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

path = '_plugins/_ml/connectors/_create'
url = host + path

payload = {
    "name": "Cohere Connector: embedding",
    "description": "The connector to cohere embedding model",
    "version": 1,
    "protocol": "http",
    "credential": {
        "secretArn": "arn:aws:secretsmanager:region:account-id:secret:cohere-key-id",
        "roleArn": "arn:aws:iam::account-id:role/opensearch-secretmanager-role"
    },
    "actions": [
        {
            "action_type": "predict",
            "method": "POST",
            "url": "https://api.cohere.ai/v1/embed",
            "headers": {
                "Authorization": "Bearer ${credential.secretArn.cohere-key-used-in-
secrets-manager}"
            },
            "request_body": "{ \"texts\": ${parameters.texts}, \"truncate\": \"END\" }"
        }
    ]
}

headers = {"Content-Type": "application/json"}

r = requests.post(url, auth=awsauth, json=payload, headers=headers)
print(r.status_code)
print(r.text)
```

Usando AWS CloudFormation para configurar a inferência remota para pesquisa semântica

A partir da OpenSearch versão 2.9, você pode usar a inferência remota com pesquisa semântica para hospedar seus próprios modelos de aprendizado de máquina (ML). A inferência remota usa o plug-in ML Commons para permitir que você hospede suas inferências de modelo remotamente em serviços de ML, como a Amazon SageMaker Amazon, e conecte-as ao Amazon BedRock OpenSearch Service com conectores de ML.

Para facilitar a configuração da inferência remota, o Amazon OpenSearch Service fornece um AWS CloudFormationmodelo no console. CloudFormation é uma AWS service (Serviço da AWS) ferramenta que permite modelar, provisionar AWS e gerenciar recursos de terceiros tratando a infraestrutura como código.

O OpenSearch CloudFormation modelo automatiza o processo de provisionamento do modelo para que você possa criar facilmente um modelo em seu domínio de OpenSearch serviço e, em seguida, usar o ID do modelo para ingerir dados e executar consultas de pesquisa neural.

Tópicos

Pré-requisitos

Para usar um CloudFormation modelo com o OpenSearch Serviço, preencha os pré-requisitos a seguir.

Configurar um domínio OpenSearch de serviço

Antes de usar um CloudFormation modelo, você deve configurar um domínio do Amazon OpenSearch Service com a versão 2.9 ou posterior e um controle de acesso refinado ativado. Crie uma função OpenSearch de back-end de serviço para dar permissão ao plug-in ML Commons para criar seu conector para você.

O CloudFormation modelo cria uma função do Lambda IAM para você com o nome padrão`LambdaInvokeOpenSearchMLCommonsRole`, que você pode substituir se quiser escolher

um nome diferente. Depois que o modelo criar essa função do IAM, você precisa dar permissão à função Lambda para chamar seu domínio de OpenSearch serviço. Para fazer isso, mapeie a função nomeada `ml_full_access` para sua função OpenSearch de back-end de serviço com as seguintes etapas:

1. Navegue até o plug-in OpenSearch Dashboards do seu domínio OpenSearch de serviço. Você pode encontrar o endpoint do Dashboards no painel do seu domínio no console de OpenSearch serviços.
2. No menu principal, escolha Segurança, Funções e selecione a função ml_full_access.
3. Escolha Usuários mapeados e Gerenciar mapeamento.
4. Em Funções de back-end, adicione o ARN da função do Lambda que precisa de permissão para chamar seu domínio.

   ```
   arn:aws:iam::account-id:role/role-name
   ```

5. Selecione Mapa e confirme se o usuário ou função aparece em Usuários mapeados.

Depois de mapear a função, navegue até a configuração de segurança do seu domínio e adicione a função Lambda IAM à OpenSearch sua política de acesso ao serviço.

Ative as permissões no seu Conta da AWS

Você Conta da AWS deve ter permissão para acessar CloudFormation o Lambda, junto com o que AWS service (Serviço da AWS) você escolher para seu modelo — Runtime SageMaker ou Amazon. BedRock

Se estiver usando o Amazon Bedrock, você também deve registrar seu modelo. Consulte Acesso aos modelos no Guia do usuário do Amazon Bedrock para registrar seu modelo.

Se você estiver usando seu próprio bucket do Amazon S3 para fornecer artefatos de modelo, deverá adicionar a função do CloudFormation IAM à sua política de acesso do S3. Para obter mais informações, consulte Adicionar e remover permissões de identidade do IAM no Guia do usuário do IAM.

Amazon SageMaker modelos

Os SageMaker CloudFormation modelos da Amazon definem vários AWS recursos para configurar o plug-in neural e a pesquisa semântica para você.

Primeiro, use a integração com modelos de incorporação de texto por meio do SageMaker modelo da Amazon para implantar um modelo de incorporação de texto no SageMaker Runtime como um servidor. Se você não fornecer um endpoint de modelo, CloudFormation cria uma função do IAM que permite ao SageMaker Runtime baixar artefatos de modelo do Amazon S3 e implantá-los no servidor. Se você fornecer um endpoint, CloudFormation cria uma função do IAM que permite que a função Lambda acesse OpenSearch o domínio do Serviço ou, se a função já existir, atualize e reutilize a função. O endpoint serve o modelo remoto usado para o conector ML com o plug-in ML Commons.

Em seguida, use o modelo Integration with Sparse Encoders por meio do Amazon Sagemaker para criar uma função Lambda que faça com que seu domínio configure conectores de inferência remotos. Depois que o conector é criado no OpenSearch Service, a inferência remota pode executar a pesquisa semântica usando o modelo remoto no SageMaker Runtime. O modelo retorna o ID do modelo em seu domínio para que você possa começar a pesquisar.

Para usar os SageMaker CloudFormation modelos da Amazon

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. No painel de navegação à esquerda, escolha Integrações.
3. Em cada um dos SageMaker modelos da Amazon, escolha Configurar domínio, Configurar domínio público.
4. Siga as instruções no CloudFormation console para provisionar sua pilha e configurar um modelo.

> **Note**
>
> OpenSearch O serviço também fornece um modelo separado para configurar o domínio VPC. Se você usar esse modelo, precisará fornecer o ID da VPC para a função do Lambda.

Modelos Amazon Bedrock

Semelhante aos SageMaker CloudFormation modelos da Amazon, o CloudFormation modelo Amazon Bedrock provisiona os AWS recursos necessários para criar conectores entre o OpenSearch Service e o Amazon Bedrock.

Primeiro, o modelo cria uma função do IAM que permite que a futura função Lambda acesse seu domínio de OpenSearch serviço. Em seguida, o modelo cria a função Lambda, que faz com que o domínio crie um conector usando o plug-in ML Commons. Depois que o OpenSearch Service cria o conector, a configuração da inferência remota é concluída e você pode executar pesquisas semânticas usando as operações da API Amazon Bedrock.

Observe que, como o Amazon Bedrock hospeda seus próprios modelos de ML, você não precisa implantar um modelo no SageMaker Runtime. Em vez disso, o modelo usa um endpoint predeterminado para o Amazon Bedrock e ignora as etapas de provisionamento do endpoint.

Para usar o modelo Amazon Bedrock CloudFormation

1. Abra o console do Amazon OpenSearch Service em https://console.aws.amazon.com/aos/home.
2. No painel de navegação à esquerda, escolha Integrações.
3. Em Integrar com o modelo Amazon Titan Text Embeddings por meio do Amazon Bedrock, escolha Configurar domínio, Configurar domínio público.
4. Siga as instruções para configurar seu modelo.

> **Note**
>
> OpenSearch O serviço também fornece um modelo separado para configurar o domínio VPC. Se você usar esse modelo, precisará fornecer o ID da VPC para a função do Lambda.

Além disso, o OpenSearch Service fornece os seguintes modelos do Amazon Bedrock para se conectar ao modelo Cohere e ao modelo de incorporação multimodal Amazon Titan:

- `Integration with Cohere Embed through Amazon Bedrock`
- `Integrate with Amazon Bedrock Titan Multi-modal`

Configurações do ML Commons não suportadas

O Amazon OpenSearch Service não suporta o uso das seguintes configurações do ML Commons:

- `plugins.ml_commons.allow_registering_model_via_url`
- `plugins.ml_commons.allow_registering_model_via_local_file`

Para obter mais informações sobre as configurações do ML Commons, consulte Configurações de cluster do ML Commons.

Análise de segurança para Amazon OpenSearch Service

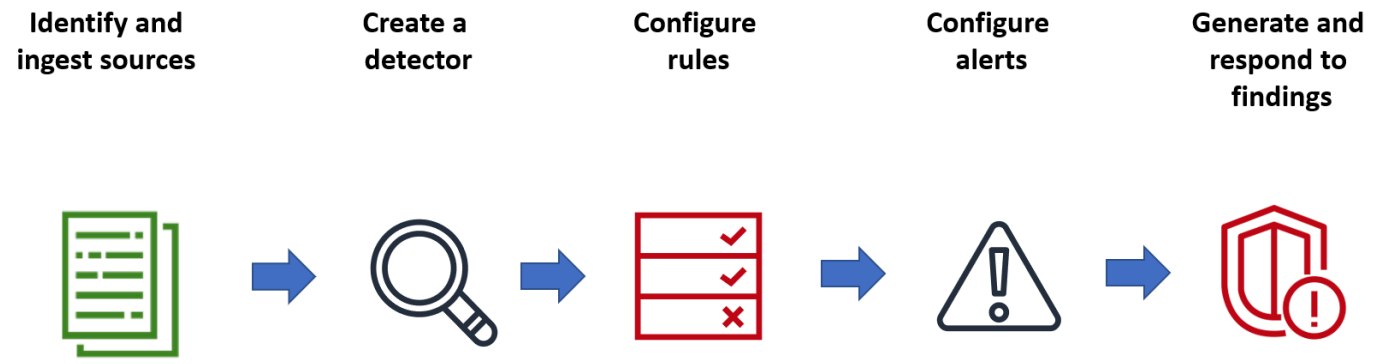
O Security Analytics é uma OpenSearch solução que fornece visibilidade da infraestrutura da sua organização, monitora atividades anômalas, detecta possíveis ameaças à segurança em tempo real e aciona alertas para destinos pré-configurados. Você pode monitorar atividades maliciosas nos seus logs de eventos de segurança avaliando continuamente as regras e revisando as descobertas de segurança geradas automaticamente. Além disso, o Security Analytics pode gerar alertas automatizados e enviá-los para um canal de notificação específico, como Slack ou e-mail.

Você pode usar o plug-in Security Analytics para detectar ameaças comuns out-of-the-box e gerar informações críticas de segurança a partir de seus registros de eventos de segurança existentes, como registros de firewall, registros do Windows e registros de auditoria de autenticação. Para usar o Security Analytics, seu domínio deve estar executando a OpenSearch versão 2.5 ou posterior.

Para obter mais informações sobre como configurar o plug-in Security Analytics, consulte Security Analytics na OpenSearch documentação.

Componentes e conceitos de Security Analytics

Várias ferramentas e atributos fornecem a base para a operação do Security Analytics. Os principais componentes que compõem o plug-in incluem detectores, tipos de log, regras, descobertas e alertas.



Tipos de log

OpenSearch suporta vários tipos de registros e fornece out-of-the-box mapeamentos para cada tipo. Você especifica o tipo de log e configura um intervalo de tempo ao criar um detector e, a partir daí, o Security Analytics ativa automaticamente um conjunto relevante de regras que são executadas nesse intervalo.

Detectores

Os detectores identificam uma variedade de ameaças à segurança cibernética para um tipo de log em seus índices de dados. Você configura seu detector para usar regras personalizadas e regras Sigma prontas para uso que avaliam eventos que ocorrem no sistema. O detector então gera descobertas de segurança a partir desses eventos. Para obter mais informações sobre detectores, consulte Criação de detectores na OpenSearch documentação.

Regras

As regras de detecção de ameaças definem as condições que os detectores aplicam aos dados de log ingeridos para identificar um evento de segurança. O Security Analytics oferece suporte à importação, criação e personalização de regras para atender às suas necessidades e também fornece regras Sigma predefinidas e de código aberto para detectar ameaças comuns em seus logs. O Security Analytics mapeia muitas regras para uma base de conhecimento cada vez maior de táticas e técnicas adversárias mantida pela organização MITRE ATT&CK. Você pode usar os OpenSearch painéis ou as APIs para criar e usar regras. Para obter mais informações sobre regras, consulte Como trabalhar com regras na OpenSearch documentação.

Descobertas

Quando um detector combina uma regra com um evento de log, ele gera uma descoberta. Cada descoberta inclui uma combinação exclusiva de regras selecionadas, um tipo de log e uma severidade da regra. As descobertas não apontam necessariamente para ameaças iminentes no sistema, mas sempre isolam um evento de interesse. Para obter mais informações sobre descobertas, consulte Trabalhando com descobertas na OpenSearch documentação.

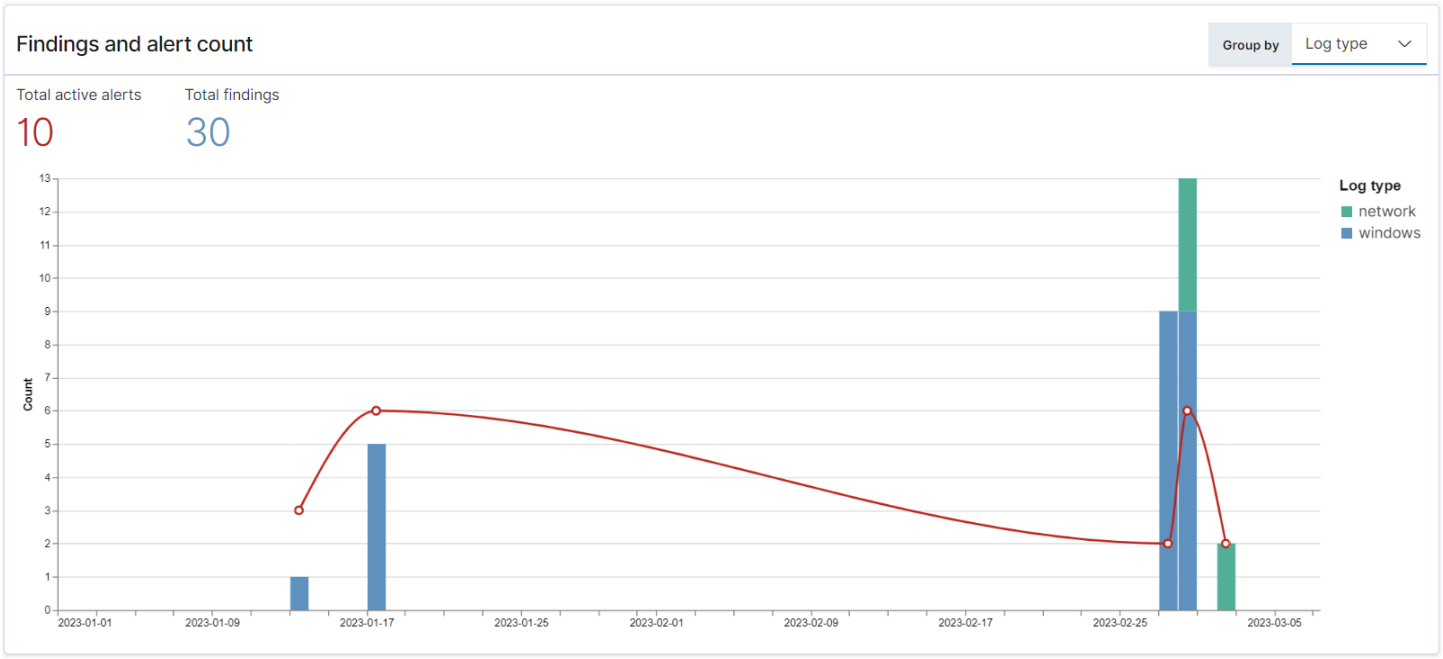
Alertas

Ao criar um detector, você pode especificar uma ou mais condições que acionam um alerta. Um alerta é uma notificação enviada para um canal preferencial, como Slack ou e-mail. Você configura o alerta para ser acionado quando o detector corresponde a uma ou várias regras e pode personalizar a mensagem de notificação. Para obter mais informações sobre alertas, consulte Como trabalhar com alertas na OpenSearch documentação.

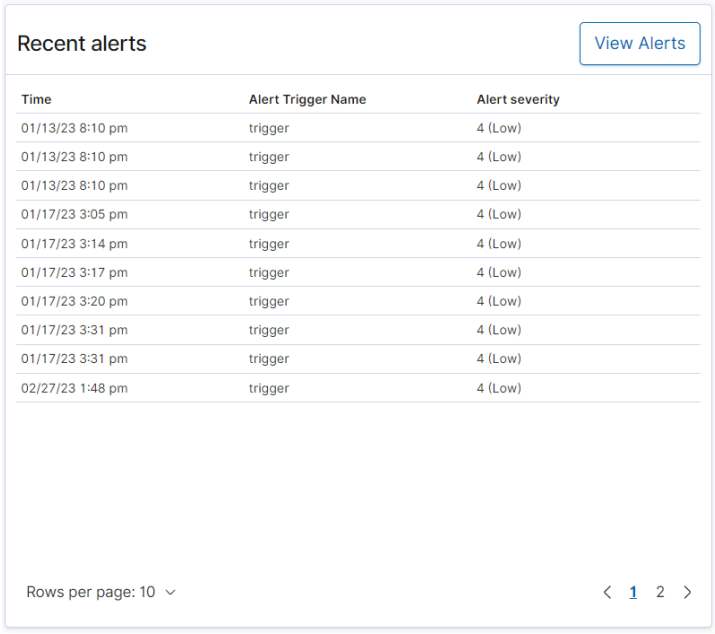
Explorando o Security Analytics

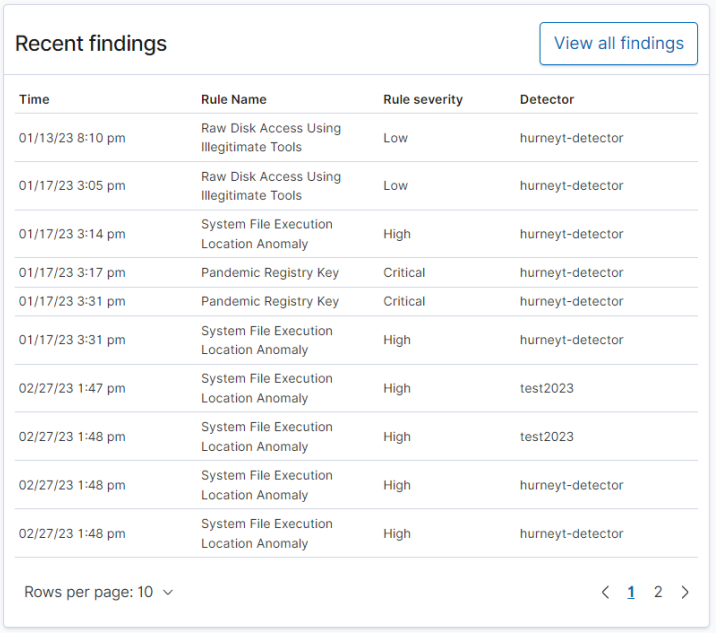
Você pode usar OpenSearch painéis para visualizar e obter informações sobre seu plug-in de análise de segurança. A visão geral fornece informações como descobertas e contagens de alertas,

descobertas e alertas recentes, regras de detecção frequentes e uma lista de seus detectores. Você pode ver uma exibição resumida composta por várias visualizações. O gráfico a seguir, por exemplo, mostra a tendência de descobertas e alertas para vários tipos de logs em um determinado período de tempo.



Mais abaixo na página, você pode revisar suas descobertas e alertas mais recentes.





Além disso, você pode ver uma distribuição das regras acionadas com mais frequência em todos os detectores ativos. Isso pode ajudar você a detectar e investigar diferentes tipos de atividades maliciosas em todos os tipos de log.

Finalmente, é possível visualizar o status dos detectores configurados. Nesse painel, você também pode navegar até o fluxo de trabalho de criação de detectores.

Para configurar sua configuração do Security Analytics, crie regras com a página Regras e use essas regras para escrever detectores na página Detectors. Para uma visão mais focada dos resultados do Security Analytics, você pode usar as páginas Descobertas e Alertas.

Configurar permissões do

Se você habilitar o Security Analytics em um domínio OpenSearch de serviço preexistente, a `security_analytics_manager` função pode não estar definida no domínio. Os usuários não administradores deverão ser mapeados nessa função para poderem gerenciar índices warm usando o controle de aceso detalhado. Para criar manualmente a função `security_analytics_manager`, faça o seguinte:

1. Em OpenSearch Painéis, acesse Segurança e escolha Permissões.

2. Escolha Criar grupo de ações e configure os seguintes grupos:

Group name	Permissões
`security_analytics_full_access`	• `cluster:admin/opensearch/securityanalytics/alerts/*` • `cluster:admin/opensearch/securityanalytics/detector/*` • `cluster:admin/opensearch/securityanalytics/findings/*` • `cluster:admin/opensearch/securityanalytics/mapping/*` • `cluster:admin/opensearch/securityanalytics/rule/*`
`security_analytics_read_access`	• `cluster:admin/opensearch/securityanalytics/alerts/get` • `cluster:admin/opensearch/securityanalytics/detector/get` • `cluster:admin/opensearch/securityanalytics/detector/search` • `cluster:admin/opensearch/securityanalytics/findings/get` • `cluster:admin/opensearch/securityanalytics/mapping/get` • `cluster:admin/opensearch/securityanalytics/mapping/view/get` • `cluster:admin/opensearch/securityanalytics/rule/get` • `cluster:admin/opensearch/securityanalytics/rule/search`

3. Escolha Funções e, em seguida, Criar função.

4. Nomeie o perfil security_analytics_manager.

5. Para Permissões de cluster, selecione `security_analytics_full_access` e `security_analytics_read_access`.
6. Para Índice, digite `*`.
7. Para Permissões de índice, selecione `indices:admin/mapping/put` e `indices:admin/mappings/get`,
8. Escolha Criar.
9. Depois de criar a função, mapeie-a em qualquer função de usuário ou de back-end que gerencie índices de Security Analytics.

Solução de problemas

Esse erro de índice não existe

Se você não tiver detectores e abrir o painel do Security Analytics, verá uma notificação no canto inferior direito que diz `[index_not_found_exception] no such index [.opensearch-sap-detectors-config]`. Você pode ignorar essa notificação, que desaparece em alguns segundos e não aparecerá novamente depois que um detector for criado.

Observabilidade no Amazon OpenSearch Service

A instalação padrão do OpenSearch Dashboards para Amazon OpenSearch Service inclui o plugin de Observabilidade, que você pode usar para visualizar eventos orientados por dados usando a Piped Processing Language (PPL) para explorar, descobrir e consultar dados armazenados no OpenSearch. O plugin requer o OpenSearch 1.2 ou mais recente.

O plugin de Observabilidade fornece uma experiência unificada para coletar e monitorar métricas, logs e rastreamentos de fontes de dados comuns. A coleta e o monitoramento de dados em um só lugar permitem a observabilidade completa de toda a sua infraestrutura. A documentação completa para o plugin de Observabilidade está na documentação do OpenSearch.

O processo de todos para explorar dados é diferente. Se for novidade para você a exploração de dados e na criação de visualizações, recomendamos tentar um fluxo de trabalho como o seguinte:

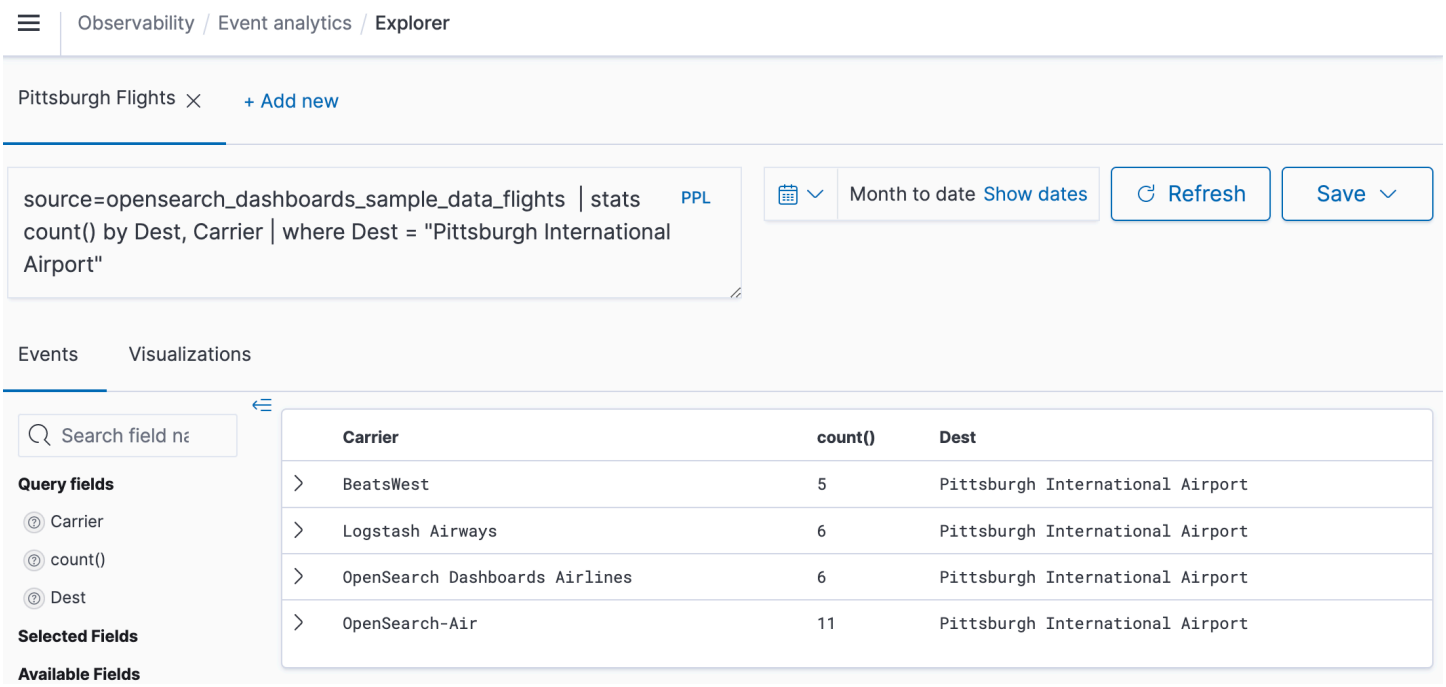
Explore seus dados com a análise de eventos

Para começar, digamos que você esteja coletando dados de voos em seu domínio do OpenSearch Service e queira descobrir qual companhia aérea teve mais voos chegando no Aeroporto Internacional de Pittsburgh no mês passado. Você grava a seguinte consulta PPL:

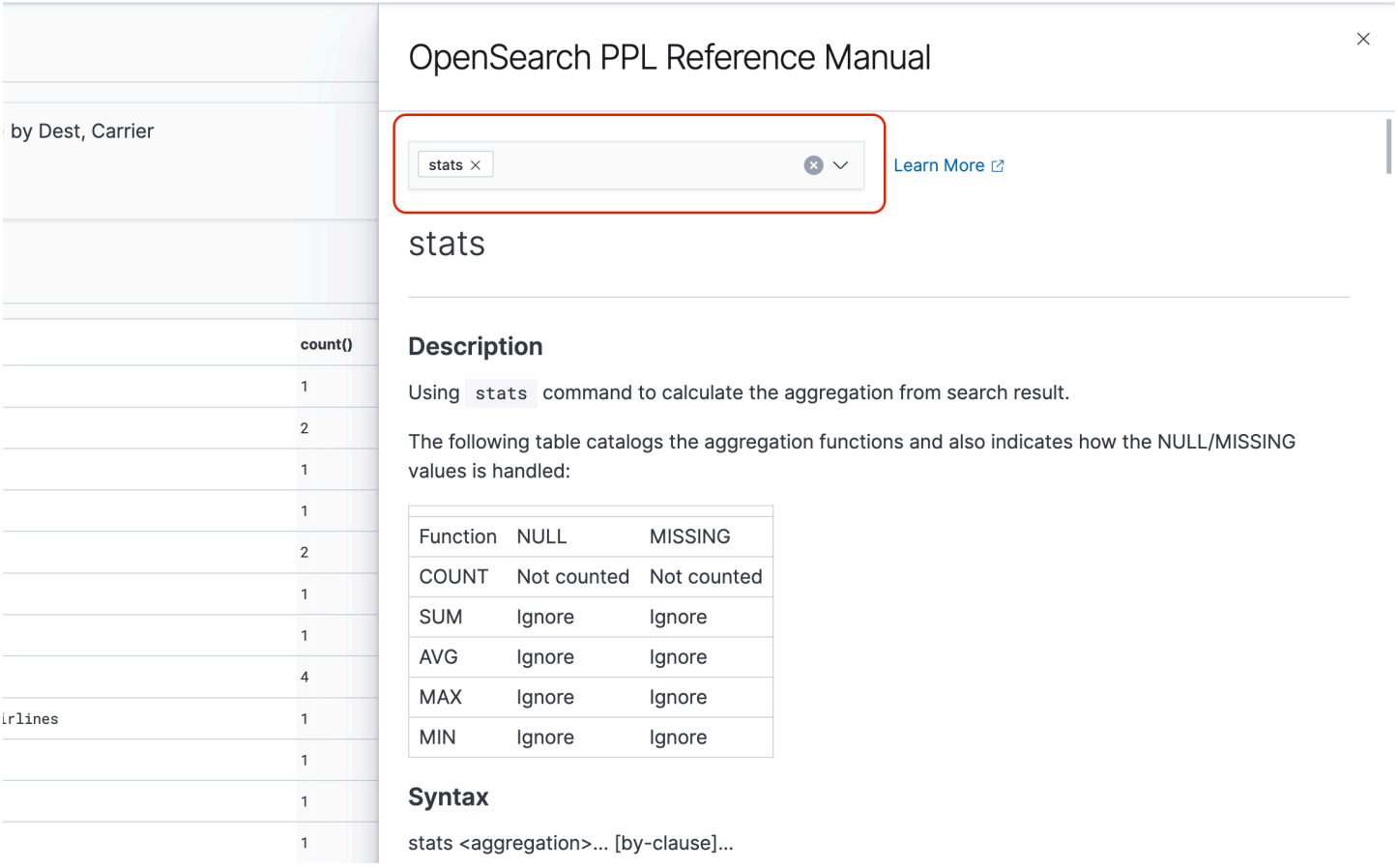
```
source=opensearch_dashboards_sample_data_flights |
    stats count() by Dest, Carrier |
    where Dest = "Pittsburgh International Airport"
```

Essa consulta extrai dados do índice chamado`opensearch_dashboards_sample_data_flights`. Em seguida, ele usa o comando `stats` para obter uma contagem total de voos e agrupá-lo de acordo com o aeroporto de destino e a transportadora. Finalmente, ele usa a cláusula `where` para filtrar os resultados para voos que chegam ao Aeroporto Internacional de Pittsburgh.

Veja como os dados se parecem quando exibidos no último mês:



Você pode escolher o botão PPL no editor de consultas para obter informações de uso e exemplos para cada comando PPL:



Vejamos um exemplo mais complexo, que consulta informações sobre atrasos de voos:

```
source=opensearch_dashboards_sample_data_flights |
    where FlightDelayMin > 0 |
    stats sum(FlightDelayMin) as minimum_delay, count() as total_delayed by Carrier,
 Dest |
    eval avg_delay=minimum_delay / total_delayed |
    sort - avg_delay
```

Cada comando na consulta afeta o resultado final:

- `source=opensearch_dashboards_sample_data_flights` - extrai dados do mesmo índice que o exemplo anterior
- `where FlightDelayMin > 0` - filtra os dados para voos que estavam atrasados
- `stats sum(FlightDelayMin) as minimum_delay, count() as total_delayed by Carrier` - para cada transportadora, obtém o tempo de atraso mínimo total e a contagem total de voos atrasados
- `eval avg_delay=minimum_delay / total_delayed` - calcula o tempo médio de atraso para cada transportadora dividindo o tempo mínimo de atraso pelo número total de voos atrasados
- `sort - avg_delay` - classifica os resultados por atraso médio em ordem decrescente

Com essa consulta, você pode determinar que a OpenSearch Dashboards Airlines tem, em média, menos atrasos.

	avg_delay	Carrier	minimum_delay	total_delayed
>	212	Logstash Airways	4470	21
>	184	OpenSearch-Air	4245	23
>	155	BeatsWest	2025	13
>	153	OpenSearch Dashboards Airlines	4305	28

Você pode encontrar mais consultas PPL de amostra em Consultas e visualizações na página Análise de eventos.

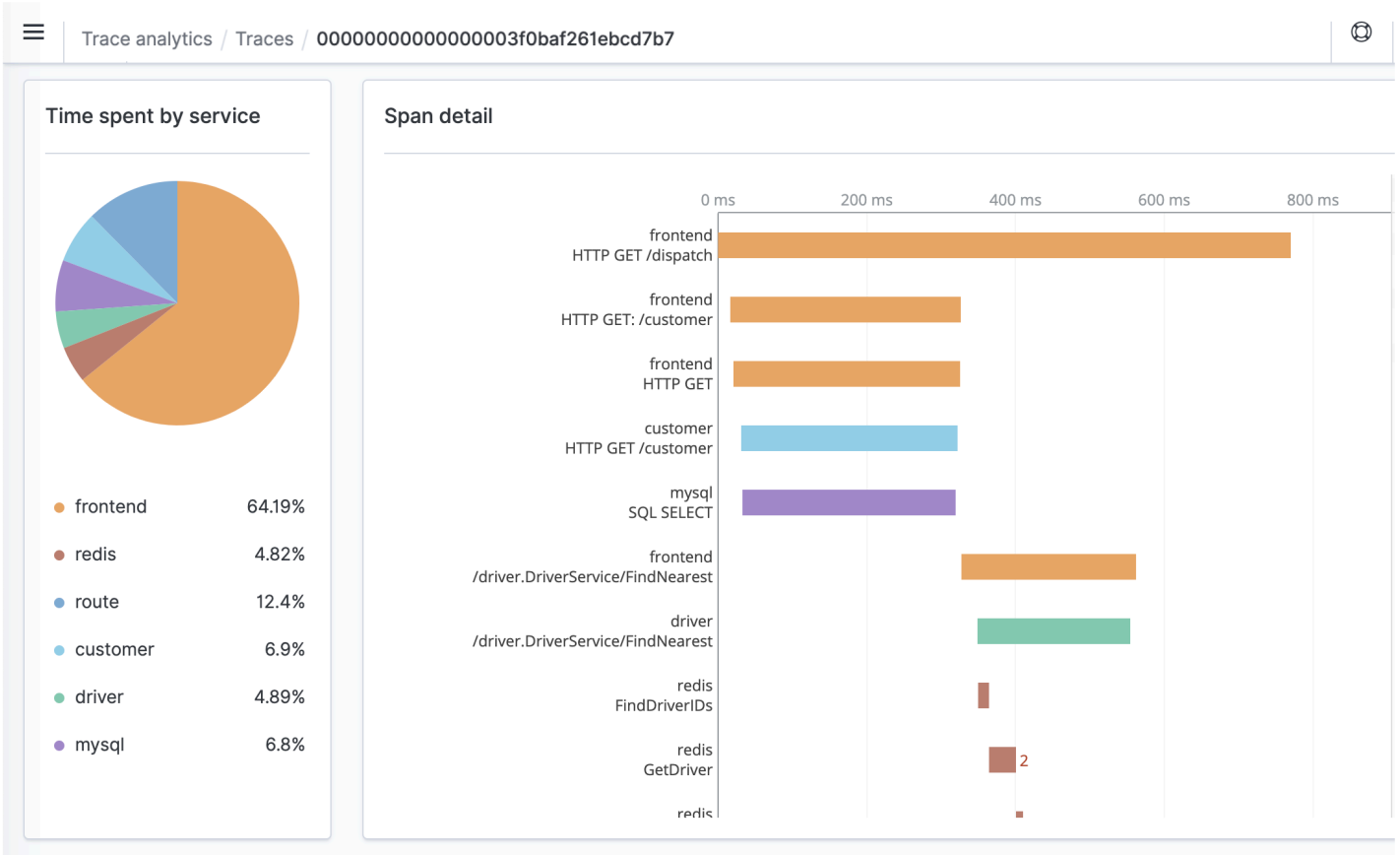
Crie visualizações

Depois de consultar corretamente os dados de seu interesse, você pode salvar essas consultas como visualizações:

Em seguida, adicione essas visualizações aos painéis operacionais para comparar diferentes partes de dados. Utilize cadernos para combinar diferentes visualizações e blocos de código que você pode compartilhar com os membros da equipe.

Aprofunde-se mais com Trace Analytics

O Trace Analytics fornece uma maneira de visualizar o fluxo de eventos em seus dados do OpenSearch para identificar e corrigir problemas de performance em aplicativos distribuídos.

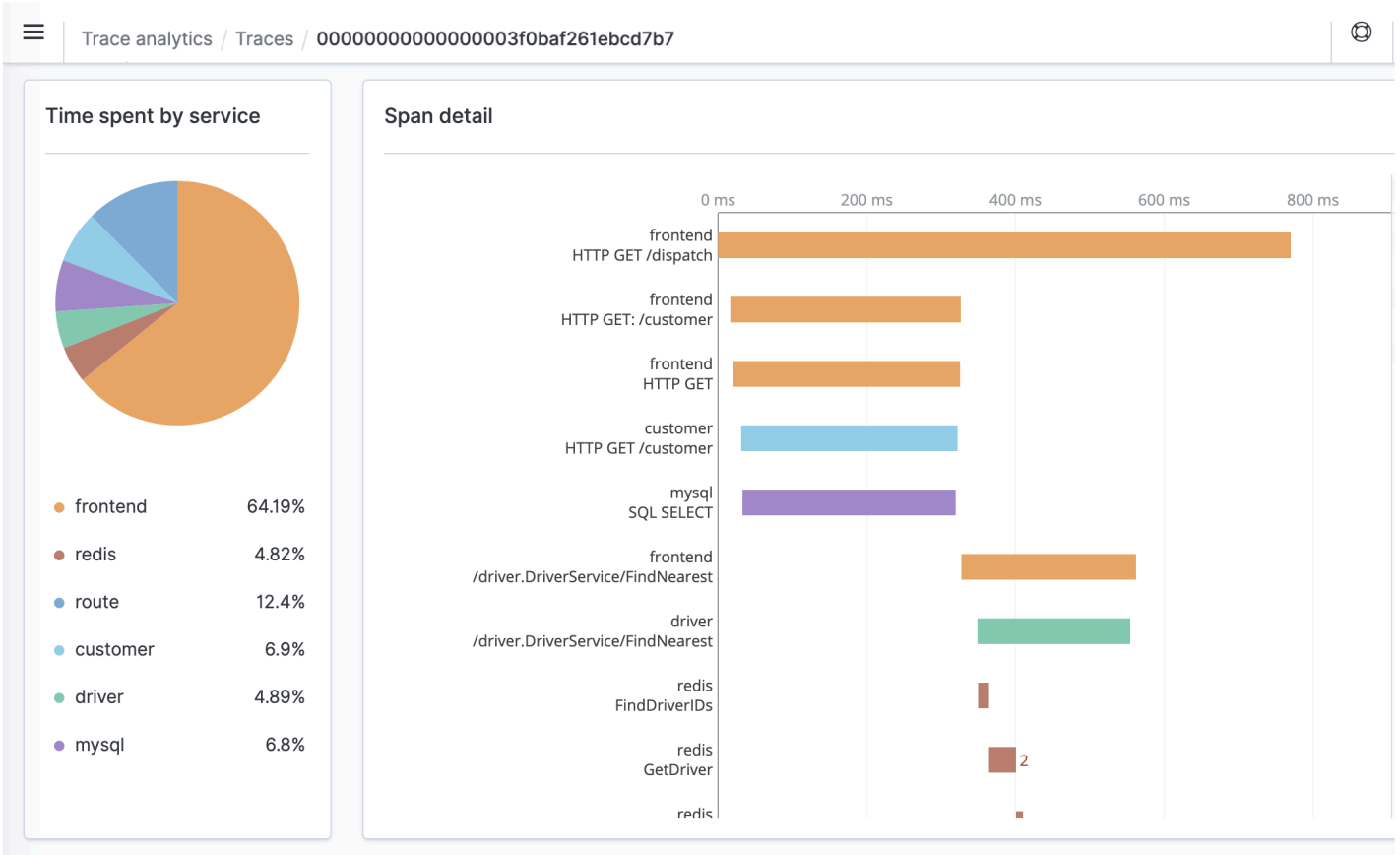


Trace Analytics para Amazon OpenSearch Service

Você pode usar o Trace Analytics, que faz parte do plug-in OpenSearch Observability, para analisar dados de rastreamento de aplicativos distribuídos. O Trace Analytics requer OpenSearch ou Elasticsearch 7.9 ou mais recente.

Em uma aplicação distribuída, uma única operação, como um usuário clicando em um botão, pode acionar uma série estendida de eventos. Por exemplo, o frontend da aplicação pode chamar um serviço de backend, que chama outro serviço, que consulta um banco de dados, que processa a consulta e retorna um resultado. Em seguida, o primeiro serviço de backend envia uma confirmação para o frontend, que atualiza a interface do usuário.

Você pode usar o Trace Analytics para ajudá-lo a visualizar esse fluxo de eventos e identificar problemas de performance.



Pré-requisitos

O Trace Analytics exige que você adicione instrumentação à sua aplicação e gere dados de rastreamento usando uma biblioteca compatível com OpenTeMetry, como Jaeger ou Zipkin. Esta etapa ocorre inteiramente fora do OpenSearch Service. A documentação do AWS Distro for OpenTeMetry contém aplicativos de exemplo para muitas linguagens de programação que podem ajudá-lo a começar, incluindo Java, Python, Go e JavaScript.

Depois de adicionar instrumentação à sua aplicação, o OpenTelemetry Connector recebe dados da aplicação e os formata como dados do OpenTelemetry. Veja a lista de receptores no GitHub. AWS O Distro for OpenTelemetry inclui um receptor para AWS X-Ray.

Finalmente, o Data Prepper, um componente independente do OpenSearch, formata esses dados do OpenTelemetry para uso com o OpenSearch. O Data Prepper é executado em uma máquina fora do cluster do OpenSearch Service, semelhante ao Logstash.

Para obter um arquivo do Docker Compose que demonstre o fluxo completo de dados, consulte a documentação do OpenSearch.

Configuração de exemplo do OpenTelemetry Collector

Para usar o Coletor do OpenTelemetry com a Ingestão do Amazon OpenSearch, teste o seguinte exemplo de configuração:

```
extensions:
  sigv4auth:
    region: "us-east-1"
    service: "osis"

receivers:
  jaeger:
    protocols:
      grpc:

exporters:
  otlphttp:
    traces_endpoint: "https://pipeline-endpoint.us-east-1.osis.amazonaws.com/
opentelemetry.proto.collector.trace.v1.TraceService/Export"
    auth:
      authenticator: sigv4auth
    compression: none

service:
  extensions: [sigv4auth]
  pipelines:
    traces:
      receivers: [jaeger]
      exporters: [otlphttp]
```

Exemplo de configuração de Ingestão do OpenSearch

Para enviar dados de rastreamento para um domínio do OpenSearch Service, teste a seguinte configuração do pipeline de exemplo de Ingestão do OpenSearch. Para obter instruções sobre como criar um pipeline, consulte Criação de pipelines de Ingestão do Amazon OpenSearch.

```
version: "2"
otel-trace-pipeline:
  source:
    otel_trace_source:
      "/${pipelineName}/ingest"
  processor:
```

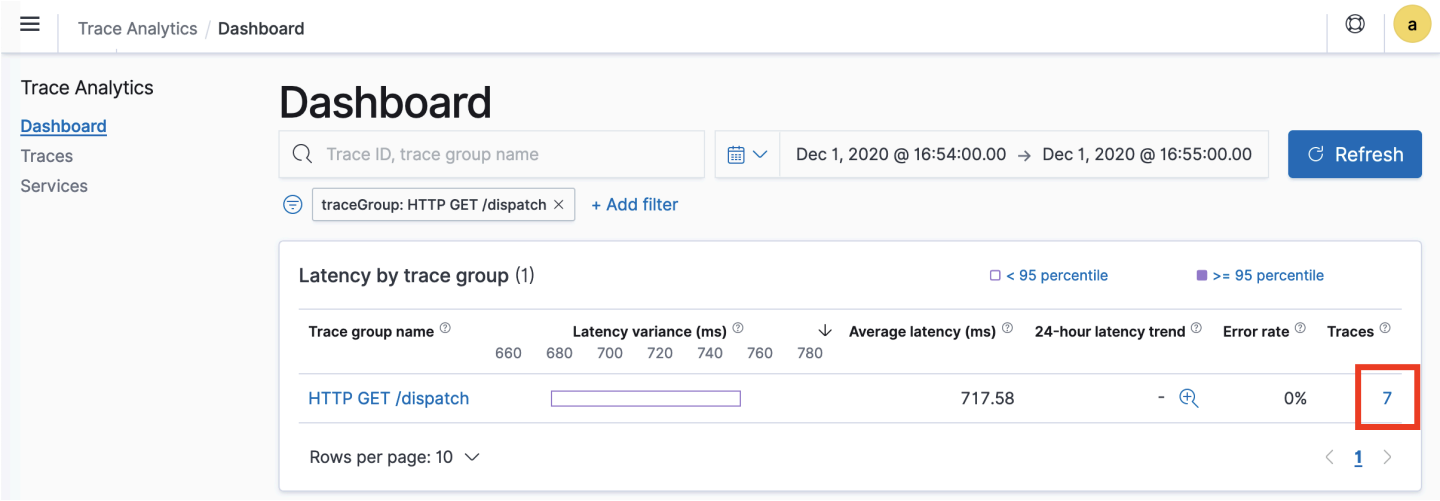
```
    - trace_peer_forwarder:
  sink:
    - pipeline:
        name: "trace_pipeline"
    - pipeline:
        name: "service_map_pipeline"
trace-pipeline:
  source:
    pipeline:
      name: "otel-trace-pipeline"
  processor:
    - otel_traces:
  sink:
    - opensearch:
        hosts: ["https://domain-endpoint"]
        index_type: trace-analytics-raw
        aws:
          # IAM role that OpenSearch Ingestion assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"

service-map-pipeline:
  source:
    pipeline:
      name: "otel-trace-pipeline"
  processor:
    - service_map:
  sink:
    - opensearch:
        hosts: ["https://domain-endpoint"]
        index_type: trace-analytics-service-map
        aws:
          # IAM role that the pipeline assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"
```

O perfil do pipeline especificado na opção `sts_role_arn` deve ter permissões de gravação para o coletor do domínio. Para obter instruções sobre como configurar permissões para o perfil de pipeline, consulte Permitir que os pipelines de Ingestão do Amazon OpenSearch gravem em domínios.

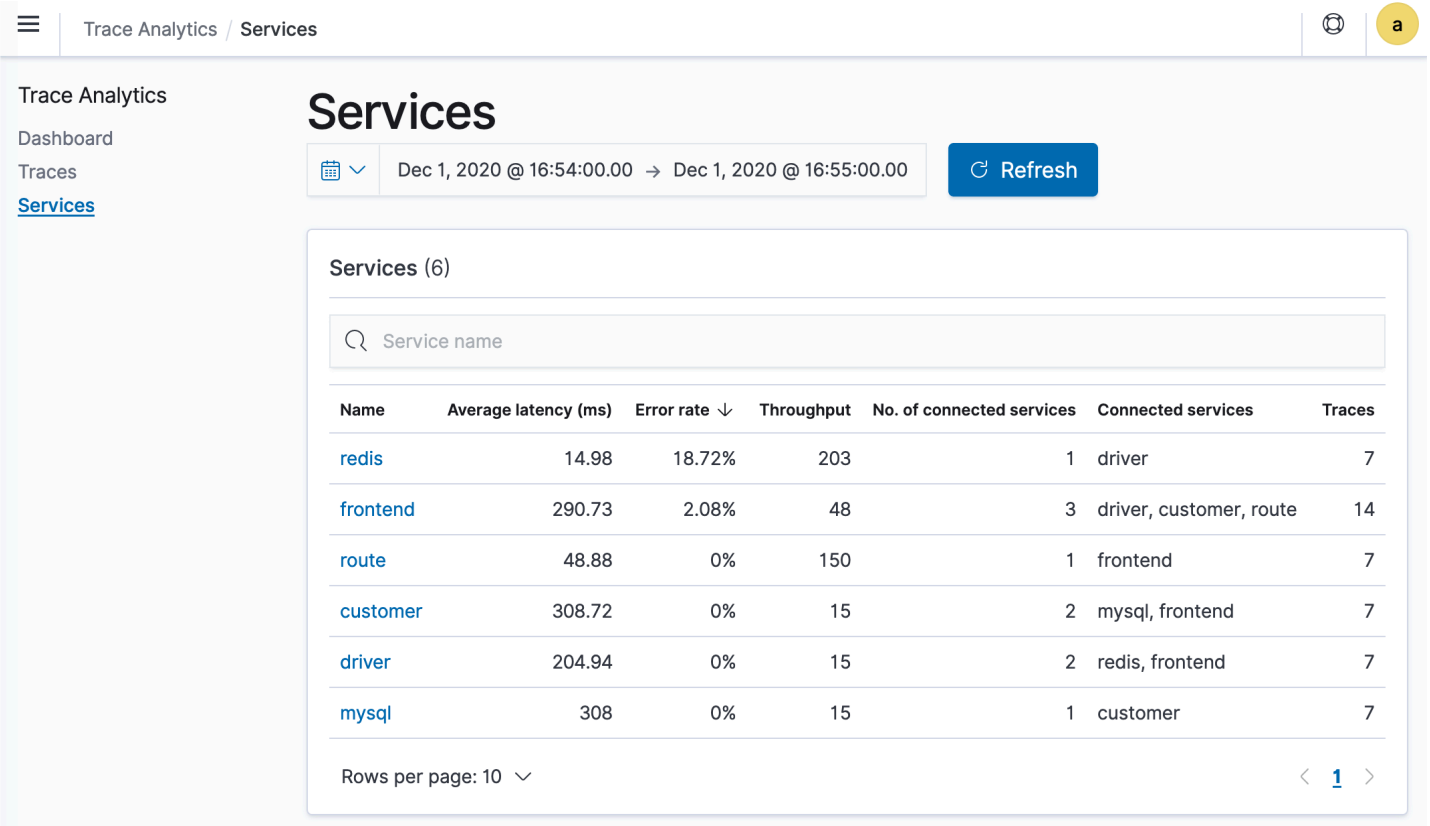
Exploração de dados de rastreamento

A visualização Painel agrupa rastreamentos por método HTTP e caminho para que você possa ver a latência média, a taxa de erros e as tendências associadas a uma operação específica. Para obter uma visualização mais focada, tente filtrar pelo nome do grupo de rastreamento.



Para fazer expandir os rastreamentos que compõem um grupo de rastreamento, escolha o número de rastreamentos na coluna à direita. Em seguida, escolha um rastreamento individual para obter um resumo detalhado.

A visualização Serviços lista todos os serviços na aplicação, além de um mapa interativo que mostra como os vários serviços se conectam uns aos outros. Em contraste com o painel (que ajuda a identificar problemas por operação), o mapa de serviço ajuda você a identificar problemas por serviço. Tente classificar por taxa de erro ou latência para ter uma noção das áreas problemáticas potenciais da sua aplicação.



Consulta de dados do Amazon OpenSearch Service usando Piped Processing Language

A Piped Processing Language é uma linguagem de consultas que permite usar a sintaxe de pipes (`|`) para consultar dados armazenados no Amazon OpenSearch Service.

A sintaxe de PPL consiste em comandos delimitados por um caractere de pipe (`|`), onde os dados fluem da esquerda para a direita através de cada pipeline. Por exemplo, a sintaxe de PPL para localizar o número de hosts com erros HTTP 403 ou 503, agregá-los por host e classificá-los em ordem de impacto é a seguinte:

```
source = dashboards_sample_data_logs | where response='403' or response='503' | stats
 count(request) as request_count by host, response | sort -request_count
```

A PPL requer o OpenSearch ou o Elasticsearch 7.9 ou posterior. Etapas detalhadas e descrições de comandos estão disponíveis no Manual de referência do OpenSearch PPL.

Para começar a usar, escolha Query Workbench no OpenSearch Dashboards e selecione PPL. Use a operação `bulk` para indexar alguns dados de amostra:

```
PUT accounts/_bulk?refresh
{"index":{"_id":"1"}}
{"account_number":1,"balance":39225,"firstname":"Amber","lastname":"Duke","age":32,"gender":"M"
 Holmes
 Lane","employer":"Pyrami","email":"amberduke@pyrami.com","city":"Brogan","state":"IL"}
{"index":{"_id":"6"}}
{"account_number":6,"balance":5686,"firstname":"Hattie","lastname":"Bond","age":36,"gender":"M"
 Bristol
 Street","employer":"Netagy","email":"hattiebond@netagy.com","city":"Dante","state":"TN"}
{"index":{"_id":"13"}}
{"account_number":13,"balance":32838,"firstname":"Nanette","lastname":"Bates","age":28,"gender"
 Mady Street","employer":"Quility","city":"Nogal","state":"VA"}
{"index":{"_id":"18"}}
{"account_number":18,"balance":4180,"firstname":"Dale","lastname":"Adams","age":33,"gender":"M"
 Hutchinson Court","email":"daleadams@boink.com","city":"Orick","state":"MD"}
```

O seguinte exemplo retorna os campos `firstname` e `lastname` para documentos em um índice de contas com `age`maior que 18:

```
search source=accounts | where age > 18 | fields firstname, lastname
```

Exemplo de resposta

ID	firstname	lastname
0	Amber	Duque
1	Hattie	Bond
2	Nanette	Bates
3	Dale	Adams

Você pode usar um conjunto completo de comandos somente leitura como `search`, `where`, `fields`, `rename`, `dedup`, `stats`, `sort`, `eval`, `head`, `top` e `rare`. Para obter descrições e exemplos de cada comando, consulte o Manual de referência do OpenSearch PPL.

O plugin de PPL oferece suporte a todas as funções SQL, incluindo operadores e expressões matemáticos, trigonométricos, data-hora, string, agregados e avançados. Para saber mais, consulte o Manual de referência do OpenSearch PPL.

Melhores práticas operacionais para o Amazon OpenSearch Service

Este capítulo fornece as melhores práticas para operar domínios do Amazon OpenSearch Service e inclui diretrizes gerais que se aplicam a muitos casos de uso. Cada workload é única e tem características particulares, portanto, nenhuma recomendação genérica é exatamente certa para cada caso de uso. A prática recomendada mais importante é implantar, testar e ajustar seus domínios em um ciclo contínuo para encontrar a configuração, a estabilidade e o custo ideais para a workload.

Tópicos

Monitoramento e alertas

As melhores práticas a seguir se aplicam ao monitoramento de seus domínios OpenSearch de serviço.

Configurar CloudWatch alarmes

OpenSearch O serviço emite métricas de desempenho para a Amazon CloudWatch. Analise regularmente as métricas do cluster e da instância e configure CloudWatch os alarmes recomendados com base no desempenho da sua carga de trabalho.

Habilitar a publicação de logs

OpenSearch O serviço expõe registros OpenSearch de erros, pesquisa registros lentos, indexação de registros lentos e registros de auditoria no Amazon CloudWatch Logs. Os logs lentos de pesquisa, logs lentos de indexação e logs de erros são úteis para solucionar problemas de performance e estabilidade. Os logs de auditoria, que estarão disponíveis apenas se você habilitar o controle de acesso detalhado para rastrear a atividade do usuário. Para obter mais informações, consulte Registros na OpenSearch documentação.

Logs lentos de pesquisa e logs lentos de indexação são ferramentas importantes para que você entenda e solucione problemas relacionados à performance de suas operações de pesquisa e indexação. Habilite a entrega de logs de lentidão de pesquisa e indexação para todos os domínios de produção. Você também deve configurar limites de registro — caso contrário, CloudWatch não capturará os registros.

Estratégia de fragmentação

Os fragmentos distribuem sua carga de trabalho pelos nós de dados em seu domínio OpenSearch de serviço. Índices configurados corretamente podem auxiliar no aumento da performance geral do domínio.

Quando você envia dados para o OpenSearch Serviço, você envia esses dados para um índice. Um índice é semelhante a uma tabela de banco de dados, com documentos como linhas e campos como colunas. Ao criar o índice, você OpenSearch informa quantos fragmentos primários deseja criar. Os fragmentos primários são partições independentes do conjunto de dados completo. OpenSearch O serviço distribui automaticamente seus dados pelos fragmentos principais em um índice. Você também pode configurar réplicas do índice. Cada fragmento de réplica compreende um conjunto completo de cópias dos fragmentos primários desse índice.

OpenSearch O serviço mapeia os fragmentos de cada índice nos nós de dados do seu cluster. Ele garante que os fragmentos primários e de réplica do índice sejam inerentes a nós de dados diferentes. A primeira réplica garante que você tenha duas cópias dos dados no índice. Você sempre deve usar pelo menos uma réplica. Réplicas adicionais fornecem redundância e capacidade de leitura adicionais.

OpenSearch envia solicitações de indexação para todos os nós de dados que contêm fragmentos que pertencem ao índice. Ele envia solicitações de indexação primeiro para nós de dados que contenham fragmentos primários e depois para nós de dados que contenham fragmentos de réplica.

As solicitações de pesquisa são encaminhadas pelo nó coordenador para um fragmento primário ou de réplica para todos os fragmentos pertencentes ao índice.

Por exemplo, para um índice com cinco fragmentos primários e uma réplica, cada solicitação de indexação toca em dez fragmentos. Por outro lado, as solicitações de pesquisa são enviadas para n fragmentos, onde n é o número de fragmentos primários. Para um índice com cinco fragmentos primários e uma réplica, cada consulta de pesquisa toca em cinco fragmentos (primários ou de réplica) desse índice.

Determinar as contagens de fragmentos e de nós de dados

Use as seguintes práticas recomendadas para determinar contagens de fragmentos e nós de dados para seu domínio.

Tamanho do fragmento: o tamanho dos dados no disco é um resultado direto do tamanho dos dados de origem e se altera à medida que você indexa mais dados. A source-to-index proporção pode variar muito, de 1:10 a 10:1 ou mais, mas geralmente é em torno de 1:1,10. Você pode usar essa proporção para prever o tamanho do índice no disco. Você pode indexar alguns dados e recuperar os tamanhos reais do índice para determinar a proporção de sua workload. Após prever um tamanho de índice, defina uma contagem de fragmentos de modo que cada fragmento tenha entre 10 e 30 GiB (para workloads de pesquisa) ou entre 30 e 50 GiB (para workloads de logs). O máximo deve ser 50 GiB; não se esqueça de planejar o crescimento.

Contagem de fragmentos: a distribuição de fragmentos para nós de dados tem um grande impacto na performance de um domínio. Quando tiver índices com vários fragmentos, tente fazer a contagem de fragmentos em um múltiplo par da contagem de nós de dados. Isso ajuda a garantir que os fragmentos sejam distribuídos uniformemente entre os nós de dados e evita os nós quentes. Por exemplo, se você tiver 12 fragmentos primários, sua contagem de nós de dados deverá ser 2, 3, 4, 6 ou 12. No entanto, a contagem de fragmentos é secundária ao tamanho do fragmento. Se você tiver 5 GiB de dados, ainda deverá usar um único fragmento.

Fragmentos por nó de dados: o número total de fragmentos que um nó pode conter é proporcional à memória heap da máquina virtual Java (JVM) do nó. Busque 25 fragmentos ou menos para cada GiB de memória heap. Por exemplo, um nó com 32 GiB de memória heap não deve conter mais de 800 fragmentos. Embora a distribuição de fragmentos possa variar de acordo com os padrões de workload, há um limite de mil fragmentos por nó. A API cat/allocation fornece uma visualização rápida do número de fragmentos e do armazenamento total de fragmentos nos nós de dados.

Proporção de fragmentos para CPU: quando um fragmento está envolvido em uma solicitação de indexação ou pesquisa, ele utiliza uma vCPU para processar a solicitação. Como prática recomendada, use um ponto de escala inicial de 1,5 vCPU por fragmento. Se o seu tipo de instância tiver 8 vCPUs, defina a contagem de nós de dados para que cada nó não tenha mais do que seis fragmentos. Observe que isso é uma aproximação. Certifique-se de testar sua workload e escalar seu cluster adequadamente.

Para obter recomendações sobre volume de armazenamento, tamanho do fragmento e tipo de instância, consulte os seguintes recursos:

- the section called “Dimensionamento de domínios”
- the section called “Escala de petabytes”

Evitar distorções de armazenamento

A distorção de armazenamento ocorre quando um ou mais nós de um cluster mantêm uma proporção maior de armazenamento para um ou mais índices do que para outros. Podem indicar distorções de armazenamento: utilização de CPU desigual, latência intermitente e desigual e enfileiramento desigual entre nós de dados. Para determinar se você tem problemas de distorção, consulte as seguintes seções de resolução de problemas:

- the section called “Distorção de armazenamento e de fragmentos do nó”
- the section called “Distorção de armazenamento e de fragmentos de índices”

Estabilidade

As melhores práticas a seguir se aplicam à manutenção de um domínio de OpenSearch serviço estável e íntegro.

Mantenha-se atualizado com OpenSearch

Atualizações de software de serviço

OpenSearch O serviço lança regularmente atualizações de software que adicionam recursos ou melhoram seus domínios. As atualizações não alteram a versão do mecanismo OpenSearch ou do Elasticsearch. Recomendamos que você agende um horário recorrente para executar a operação da DescribeDomainAPI e inicie uma atualização do software de serviço, se for o `UpdateStatus`

caso. `ELIGIBLE` Se você não atualizar seu domínio dentro de um determinado período de tempo (normalmente duas semanas), o OpenSearch Serviço executará a atualização automaticamente.

OpenSearch atualizações de versão

OpenSearch O serviço adiciona regularmente suporte para versões mantidas pela comunidade do. OpenSearch Sempre atualize para as OpenSearch versões mais recentes quando elas estiverem disponíveis.

OpenSearch O serviço atualiza simultaneamente os OpenSearch OpenSearch painéis (ou o Elasticsearch e o Kibana, se seu domínio estiver executando um mecanismo legado). Se o cluster tiver nós principais dedicados, as atualizações serão concluídas sem tempo de inatividade. Caso contrário, o cluster pode não responder por vários segundos após a atualização enquanto elege um nó principal. OpenSearch Os painéis podem estar indisponíveis durante parte ou toda a atualização.

Há duas maneiras de atualizar um domínio:

- Atualização no local: esta opção é mais fácil porque você mantém o mesmo cluster.
- Atualização de snapshot/restauração: esta opção serve para testar novas versões em um novo cluster ou realizar migrações entre clusters.

Independentemente do processo de atualização usado, recomendamos manter um domínio exclusivamente para desenvolvimento e teste e atualizá-lo para a nova versão antes de atualizar o domínio de produção. Escolha Desenvolvimento e teste como tipo de implantação ao criar o domínio de teste. Certifique-se de atualizar todos os clientes para versões compatíveis imediatamente após a atualização do domínio.

Melhore a performance do snapshot

Para evitar que seu snapshot fique preso no processamento, o tipo de instância do nó principal dedicado deve corresponder à contagem de fragmentos. Para ter mais informações, consulte the section called “Escolher tipos de instâncias para nós principais dedicados”. Além disso, cada nó não deve ter mais de 25 fragmentos recomendados por GiB de memória heap de Java. Para ter mais informações, consulte the section called “Como escolher o número de fragmentos”.

Habilite nós principais dedicados

Os nós principais dedicados melhoram a estabilidade do cluster. Um nó principal dedicado executa tarefas de gerenciamento de cluster, mas não retém dados de índice nem responde a solicitações de

clientes. Essa transferência de tarefas de gerenciamento de cluster aumenta a estabilidade de seu domínio e possibilita que algumas alterações de configuração ocorram sem tempo de inatividade.

Habilite e use três nós principais dedicados para obter estabilidade de domínio ideal em três zonas de disponibilidade. A implantação com multi-AZ com modo de espera configura três nós principais dedicados para você. Para obter recomendações sobre tipos de instâncias, consulte the section called “Escolher tipos de instâncias para nós principais dedicados”.

Implantar em diversas zonas de disponibilidade

Para evitar a perda de dados e minimizar o tempo de inatividade do cluster em caso de interrupção do serviço, você pode distribuir nós em duas ou três zonas de disponibilidade na mesma Região da AWS. A melhor prática é implantar o multi-AZ com modo de espera, que configura três zonas de disponibilidade, com duas zonas ativas e uma atuando em espera, e com dois fragmentos de réplica por índice. Essa configuração permite que o OpenSearch Service distribua fragmentos de réplica para AZs diferentes dos fragmentos primários correspondentes. Não há cobranças de transferência de dados entre AZs para comunicações de cluster entre zonas de disponibilidade.

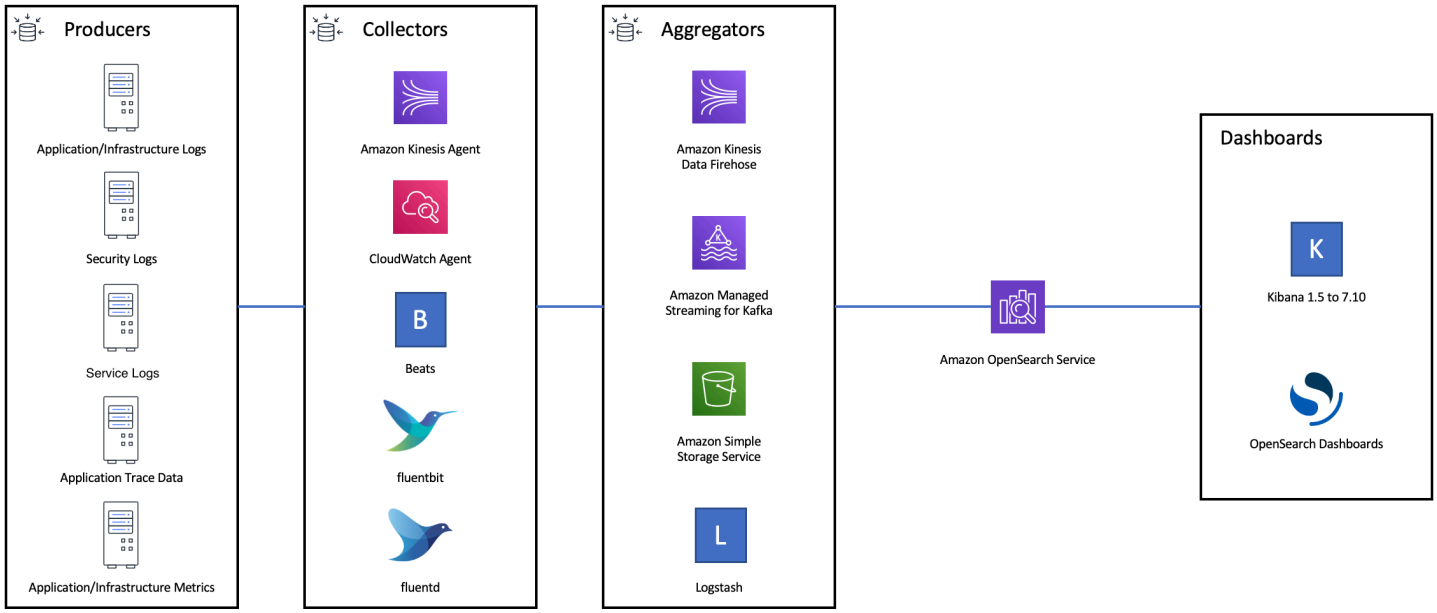
As zonas de disponibilidade são vários locais isolados dentro de cada região da . Com uma configuração de duas AZ (zonas de disponibilidade), perder uma zona de disponibilidade significa que você perde metade de toda a capacidade do domínio. A mudança para três zonas de disponibilidade reduz ainda mais o impacto da perda de uma única zona de disponibilidade.

Controlar o fluxo de ingestão e o armazenamento em buffer

Recomendamos limitar a contagem geral de solicitações usando a operação de API _bulk. É mais eficiente enviar uma solicitação `_bulk` contendo 5 mil documentos do que enviar 5 mil solicitações contendo um único documento.

Para uma estabilidade operacional ideal, às vezes é necessário limitar ou até mesmo pausar o fluxo de envio de informação de solicitações de indexação. Limitar a taxa de solicitações de indexação é um mecanismo importante para lidar com picos inesperados ou ocasionais nas solicitações que poderiam sobrecarregar o cluster. Considere a criação de um mecanismo de controle de fluxo em sua arquitetura de envio de informação.

O diagrama a seguir mostra diversas opções de componentes para uma arquitetura de ingestão de log. Configure a camada de agregação para permitir espaço suficiente para armazenar em buffer os dados de entrada para picos de tráfego repentinos e breve manutenção de domínio.



Criar mapeamentos para workloads de pesquisa

Para cargas de trabalho de pesquisa, crie mapeamentos que definam como OpenSearch armazena e indexa documentos e seus campos. Defina `dynamic` como `strict` para evitar adicionar novos campos acidentalmente.

```
PUT my-index
{
  "mappings": {
    "dynamic": "strict",
    "properties": {
      "title": { "type" : "text" },
      "author": { "type" : "integer" },
      "year": { "type" : "text" }
    }
  }
}
```

Usar modelos de índice

Você pode usar um modelo de índice como forma de saber OpenSearch como configurar um índice quando ele é criado. Configure modelos de índice antes de criar índices. Então, quando você cria um índice, ele herda as configurações e mapeamentos do modelo. É possível aplicar mais de um modelo a um único índice, assim você pode especificar configurações em um modelo e mapeamentos em

outro. Essa estratégia permite o uso de um modelo para configurações comuns em diversos índices e modelos separados para configurações e mapeamentos mais específicos.

As configurações a seguir são úteis para configurar em modelos:

- Número de fragmentos primários e de réplica
- Intervalo de atualização (com que frequência atualizar e realizar alterações recentes no índice disponível para pesquisa)
- Controle de mapeamento dinâmico
- Mapeamentos de campos explícitos

O modelo de exemplo a seguir contém cada uma destas configurações:

```
{
   "index_patterns":[
      "index-*"
   ],
   "order": 0,
   "settings": {
      "index": {
         "number_of_shards": 3,
         "number_of_replicas": 1,
         "refresh_interval": "60s"
      }
   },
   "mappings": {
      "dynamic": false,
      "properties": {
         "field_name1": {
            "type": "keyword"
         }
      }
   }
}
```

Mesmo que raramente mudem, ter configurações e mapeamentos definidos centralmente OpenSearch é mais simples de gerenciar do que atualizar vários clientes upstream.

Gerenciar índices com o Index State Management

Se você estiver gerenciando logs ou dados de séries temporais, recomendamos usar o ISM – Gerenciamento de estados de índice. O ISM permite automatizar tarefas regulares de gerenciamento do ciclo de vida do índice. Com o ISM, você pode criar políticas que invocam sobreposições de alias de índice, obter snapshots de índices, mover índices entre camadas de armazenamento e excluir índices antigos. Você pode até mesmo usar a operação de sobreposição do ISM como uma estratégia alternativa de gerenciamento do ciclo de vida dos dados para evitar distorções de fragmentos.

Primeiro, configure uma política de ISM. Por exemplo, consulte the section called “Políticas de exemplo”. Em seguida, anexe a política a um ou mais índices. Se você incluir um campo de modelo do ISM na política, o OpenSearch Service aplicará automaticamente a política a qualquer índice que corresponda ao padrão especificado.

Remover índices não utilizados

Revise regularmente os índices em seu cluster e identifique os que não estão em uso. Obtenha um snapshot desses índices para que sejam armazenados no S3 e depois exclua-os. Ao remover os índices não utilizados, você reduz a contagem de fragmentos e permite uma distribuição mais equilibrada de armazenamento e utilização de recursos entre os nós. Mesmo quando estão ociosos, os índices consomem alguns recursos durante as atividades internas de manutenção do índice.

Em vez de excluir manualmente os índices não utilizados, você pode usar o ISM para obter automaticamente um snapshot e excluir índices após um determinado período.

Usar vários domínios para alta disponibilidade

Para alcançar alta disponibilidade além de 99,9% de tempo de atividade em várias regiões, considere o uso de dois domínios. Para conjuntos de dados pequenos ou de alteração lenta, você pode configurar a replicação entre clusters para manter um modelo ativo-passivo. Nesse modelo, apenas o domínio principal é gravado, mas é possível ler qualquer domínio. Para conjuntos de dados maiores e dados de alteração rápida, configure a entrega dupla em seu pipeline de ingestão para que todos os dados sejam gravados independentemente em ambos os domínios utilizando um modelo ativo-ativo.

Projete seus aplicativos de envio e recebimento de informação com o failover em mente. Certifique-se de testar o processo de failover junto com outros processos de recuperação de desastres.

Performance

As práticas recomendadas a seguir se aplicam ao ajuste de seus domínios para obter uma performance ideal.

Otimizar o tamanho e a compactação de solicitações em massa

O dimensionamento em massa depende dos dados, da análise e da configuração do cluster, mas um bom ponto de partida é de 3 a 5 MiB por solicitação em massa.

Envie solicitações e receba respostas de seus OpenSearch domínios usando a compressão gzip para reduzir o tamanho da carga útil das solicitações e respostas. Você pode usar a compactação gzip com o cliente OpenSearch Python ou incluir os seguintes cabeçalhos do lado do cliente:

- `'Accept-Encoding': 'gzip'`
- `'Content-Encoding': 'gzip'`

Para otimizar os tamanhos das solicitações em massa, comece com um tamanho de solicitação em massa de 3 MiB. Em seguida, aumente aos poucos o tamanho da solicitação até que a performance da indexação deixe de melhorar.

> **Note**
>
> Para habilitar a compactação gzip em domínios que executam o Elasticsearch versão 6.x, você deve definir `http_compression.enabled` no nível do cluster. Essa configuração é verdadeira por padrão nas versões 7.x do Elasticsearch e em todas as versões do. OpenSearch

Reduzir o tamanho das respostas de solicitações em massa

Para reduzir o tamanho das OpenSearch respostas, exclua campos desnecessários com o `filter_path` parâmetro. Verifique se não filtrou os campos necessários para identificar ou repetir as solicitações com falha. Para ter mais informações e exemplos, consulte the section called “Redução do tamanho da resposta”.

Ajustar os intervalos de atualização

OpenSearch índices têm eventual consistência de leitura. Uma operação de atualização disponibiliza todas as atualizações executadas em um índice para pesquisa. O intervalo de atualização padrão é de um segundo, o que significa que ele OpenSearch executa uma atualização a cada segundo enquanto um índice está sendo gravado.

Quanto menor a frequência com que você atualizar um índice (maior intervalo de atualização), melhor será a performance geral da indexação. A desvantagem de aumentar o intervalo de atualização é que há um atraso maior entre uma atualização de índice e quando os novos dados estão disponíveis para pesquisa. Defina o intervalo de atualização mais alto possível para melhorar a performance geral.

Recomendamos definir o parâmetro `refresh_interval` de todos os seus índices para 30 segundos ou mais.

Habilitar o Auto-Tune

O Auto-Tune usa métricas de desempenho e uso do seu OpenSearch cluster para sugerir alterações nos tamanhos das filas, nos tamanhos do cache e nas configurações da máquina virtual Java (JVM) nos seus nós. Essas alterações opcionais melhoram a velocidade e a estabilidade do cluster. Você pode voltar às configurações padrão do OpenSearch Serviço a qualquer momento. O Auto-Tune é habilitado por padrão em novos domínios, a menos que você o desabilite explicitamente.

Recomendamos habilitar o Auto-Tune em todos os domínios e definir uma janela de manutenção recorrente ou revisar periodicamente as recomendações.

Segurança

As práticas recomendadas a seguir se aplicam à proteção de seus domínios.

Habilite o controle de acesso detalhado

O controle de acesso refinado permite que você controle quem pode acessar determinados dados em um OpenSearch domínio do Serviço. Comparado ao controle de acesso generalizado, o controle de acesso detalhado fornece a cada cluster, índice, documento e campo sua própria política de acesso especificada. Os critérios de acesso podem ser baseados em vários fatores, como o perfil da pessoa que solicita o acesso e a ação que ela pretende realizar nos dados. Por exemplo, você

pode conceder a um usuário acesso para gravar em um índice, e outro usuário pode receber acesso apenas para ler os dados no índice sem fazer alterações.

O controle de acesso detalhado permite que dados com diferentes requisitos de acesso existam no mesmo espaço de armazenamento sem problemas de segurança ou conformidade.

Recomendamos habilitar o controle de acesso detalhado em seus domínios.

Implantar domínios em uma VPC

Colocar seu domínio de OpenSearch serviço em uma nuvem privada virtual (VPC) ajuda a permitir a comunicação segura entre o OpenSearch serviço e outros serviços dentro da VPC, sem a necessidade de um gateway de internet, dispositivo NAT ou conexão VPN. Todo o tráfego permanece seguro na nuvem. AWS Devido ao seu isolamento lógico, os domínios que residem em uma VPC contam com uma camada adicional de segurança se comparados aos domínios que utilizam endpoints públicos.

Recomendamos que você crie seus domínios em uma VPC.

Aplicar uma política de acesso restritiva

Mesmo que seu domínio esteja implantado em uma VPC, uma prática recomendada é implementar a segurança em camadas. Certifique-se de verificar a configuração de suas políticas de acesso atuais.

Aplique uma política restritiva de acesso baseada em recursos aos seus domínios e siga o princípio do menor privilégio ao conceder acesso à API de configuração e às operações da API. OpenSearch Como regra geral, evite usar o código `"Principal": {"AWS": "*" }` da entidade principal do usuário anônimo em suas políticas de acesso.

No entanto, há algumas situações em que é aceitável usar uma política de acesso aberta, como quando você habilita o controle de acesso detalhado. Uma política de acesso aberta pode permitir que você acesse o domínio nos casos em que a assinatura da solicitação é difícil ou impossível, como de determinados clientes e ferramentas.

Habilite a criptografia em repouso

OpenSearch Os domínios de serviço oferecem criptografia de dados em repouso para ajudar a impedir o acesso não autorizado aos seus dados. A criptografia em repouso usa AWS Key Management Service (AWS KMS) para armazenar e gerenciar suas chaves de criptografia e o algoritmo Advanced Encryption Standard com chaves de 256 bits (AES-256) para realizar a criptografia.

Se seu domínio armazena dados confidenciais, habilite a criptografia de dados em repouso.

Ativar node-to-node criptografia

A ode-to-node criptografia N fornece uma camada adicional de segurança além dos recursos de segurança padrão do OpenSearch Serviço. Ele implementa o Transport Layer Security (TLS) para todas as comunicações entre os nós que são provisionados nele. OpenSearch Sem ode-to-node criptografia, todos os dados enviados ao seu domínio de OpenSearch serviço por HTTPS permanecem criptografados em trânsito enquanto são distribuídos e replicados entre os nós.

Se o seu domínio armazenar dados confidenciais, ative a node-to-node criptografia.

Monitor com AWS Security Hub

Monitore seu uso do OpenSearch Serviço no que se refere às melhores práticas de segurança usando AWS Security Hub. O Security Hub usa controles de segurança para avaliar configurações de recursos e padrões de segurança que ajudam você a cumprir vários frameworks de conformidade. Para obter mais informações sobre como usar o Security Hub para avaliar os recursos do OpenSearch Serviço, consulte Amazon OpenSearch Service os controles no GuiaAWS Security Hub do Usuário.

Otimização de custo

As melhores práticas a seguir se aplicam à otimização e economia em seus custos OpenSearch de serviço.

Use os tipos de instâncias de última geração

OpenSearch O serviço está sempre adotando novos tipos de instâncias do Amazon EC2 que oferecem melhor desempenho a um custo menor. Recomendamos sempre usar as instâncias de última geração.

Evite usar instâncias T2 ou `t3.small` para domínios de produção, porque elas podem se tornar instáveis sob cargas pesadas sustentadas. As instâncias `t3.medium` são uma opção para pequenas workloads de produção (tanto como nós de dados quanto como nós principais dedicados).

Usar os volumes gp3 do Amazon EBS gp3

OpenSearch os nós de dados exigem armazenamento de baixa latência e alta taxa de transferência para fornecer indexação e consulta rápidas. Ao usar os volumes gp3 do Amazon EBS, você obtém

maior desempenho básico (IOPS e throughput) a um custo 9,6% menor do que com o tipo de volume Amazon EBS gp2 oferecido anteriormente. É possível provisionar IOPS e throughput adicionais, independentemente do tamanho do volume, usando gp3. Esses volumes também são mais estáveis do que os volumes da geração anterior, pois não usam créditos intermitentes. O tipo de volume gp3 também dobra os limites de tamanho do per-data-node volume do tipo de volume gp2. Com esses volumes maiores, você pode reduzir o custo dos dados passivos, aumentando a quantidade de armazenamento por nó de dados.

Uso UltraWarm e armazenamento refrigerado para dados de registro de séries temporais

Se você estiver usando OpenSearch para análise de registros, mova seus dados para UltraWarm um armazenamento refrigerado para reduzir custos. Use o Index State Management (ISM) para migrar dados entre camadas de armazenamento e gerenciar a retenção de dados.

UltraWarmfornece uma maneira econômica de armazenar grandes quantidades de dados somente para leitura no Service. OpenSearch UltraWarm usa o Amazon S3 para armazenamento, o que significa que os dados são imutáveis e somente uma cópia é necessária. Você paga apenas pelo armazenamento que é equivalente ao tamanho dos fragmentos primários dos índices. As latências UltraWarm das consultas aumentam com a quantidade de dados do S3 necessária para atender à consulta. Depois que os dados são armazenados em cache nos nós, as consultas aos UltraWarm índices têm um desempenho semelhante às consultas aos índices ativos.

O armazenamento frio também é apoiado pelo S3. Quando precisar consultar dados frios, você pode anexá-los seletivamente aos UltraWarm nós existentes. Os dados frios incorrem no mesmo custo de armazenamento gerenciado UltraWarm, mas os objetos no armazenamento frio não consomem recursos UltraWarm do nó. Portanto, o armazenamento a frio fornece uma quantidade significativa de capacidade de armazenamento sem afetar o tamanho ou a contagem de UltraWarm nós.

UltraWarm torna-se econômico quando você tem aproximadamente 2,5 TiB de dados para migrar do armazenamento dinâmico. Monitore sua taxa de preenchimento e planeje transferir os índices para UltraWarm antes de atingir esse volume de dados.

Revisar as recomendações para instâncias reservadas

Considere comprar instâncias reservadas (RIs) depois de ter uma boa linha de base sobre sua performance e consumo de computação. Os descontos começam em torno de 30% para reservas não antecipadas de um ano e podem aumentar em até 50% para todas as reservas antecipadas de três anos.

Após observar uma operação estável por pelo menos 14 dias, revise as recomendações da instância reservada no Explorador de Custos. O título do Amazon OpenSearch Service exibe recomendações específicas de compra de RI e economias projetadas.

Dimensionamento de domínios do Amazon OpenSearch Service

Não existe um método perfeito para dimensionar os domínios do Amazon OpenSearch Service. No entanto, começando com uma compreensão de suas necessidades de armazenamento, do serviço e de OpenSearch si mesmo, você pode fazer uma estimativa inicial fundamentada sobre suas necessidades de hardware. Essa estimativa pode servir como um ponto de partida útil para a maioria dos aspectos mais importantes do dimensionamento de domínios: testá-los com workloads e monitorar sua performance.

Tópicos

- Cálculo de requisitos de armazenamento
- Como escolher o número de fragmentos
- Escolha dos tipos de instância e testes

Cálculo de requisitos de armazenamento

A maioria das OpenSearch cargas de trabalho se enquadra em uma das duas grandes categorias:

- Índice de longa duração: você escreve um código que processa dados em um ou mais OpenSearch índices e, em seguida, atualiza esses índices periodicamente à medida que os dados de origem são alterados. Alguns exemplos comuns são pesquisa de sites, documentos e comércio eletrônico.
- Índices contínuos: os dados fluem de modo contínuo para um conjunto de índices temporários, com um período de indexação e uma janela de retenção (como um conjunto de índices diários que é retido por duas semanas). Alguns exemplos comuns são análises de log, processamento de séries temporais e análise de cliques.

Para workloads de índice de longa duração, você pode examinar os dados de origem no disco e determinar facilmente a quantidade de espaço de armazenamento que eles consomem. Se os dados vierem de várias fontes, basta adicionar essas fontes.

Para índices contínuos, você pode multiplicar o volume de dados gerados durante um período representativo pelo período de retenção. Por exemplo, se você gerar 200 MiB de dados de log por hora, são 4,7 GiB por dia, que é 66 GiB de dados em um determinado momento, se você tiver um período de retenção de duas semanas.

O tamanho de seus dados de origem, no entanto, é apenas um aspecto dos seus requisitos de armazenamento. Também é necessário considerar o seguinte:

- Número de réplicas: cada réplica é uma cópia completa de um índice e precisa da mesma quantidade de espaço em disco. Por padrão, cada OpenSearch índice tem uma réplica. Recomendamos pelo menos uma para evitar a perda de dados. As réplicas também melhoram a performance da pesquisa, portanto, é aconselhável ter mais réplicas se você tiver uma workload com uso intensivo de leitura. Use `PUT /my-index/_settings` para atualizar a configuração `number_of_replicas` para o seu índice.
- OpenSearch sobrecarga de indexação: o tamanho em disco de um índice varia. O tamanho total dos dados de origem mais o índice geralmente é de 110% da origem, com o índice de até 10% dos dados de origem. Após indexar os dados, é possível usar a API `_cat/indices?v` e o valor `pri.store.size` para calcular a sobrecarga exata. `_cat/allocation?v` também fornece um resumo útil.
- Espaço reservado para o sistema operacional: por padrão, o Linux reserva 5% do sistema de arquivos para o usuário `root` para processos críticos, recuperação do sistema e para se proteger contra problemas ocasionados pela fragmentação do disco.
- OpenSearch Sobrecarga de OpenSearch serviço: o serviço reserva 20% do espaço de armazenamento de cada instância (até 20 GiB) para mesclagens de segmentos, registros e outras operações internas.

  Por causa desse máximo de 20 GiB, a quantidade total de espaço reservado pode variar muito, dependendo do número de instâncias em seu domínio. Por exemplo, um domínio pode ter três instâncias `m6g.xlarge.search`, cada uma com 500 GiB de espaço de armazenamento, para um total de 1,46 TiB. Nesse caso, o total de espaço reservado é apenas 60 GiB. Outro domínio pode ter 10 instâncias `m3.medium.search`, cada uma com 100 GiB de espaço de armazenamento, para um total de 0,98 TiB. Aqui, o total de espaço reservado é 200 GiB, embora o primeiro domínio seja 50% maior.

  Na fórmula a seguir, aplicamos uma estimativa sobre a “pior das hipóteses” para sobrecarga. Essa estimativa inclui espaço livre adicional para ajudar a minimizar o impacto das falhas nos nós e das interrupções da zona de disponibilidade.

Em resumo, se em determinado momento você tiver 66 GiB de dados e quiser uma réplica, seu requisito de armazenamento mínimo será mais próximo de 66 * 2 * 1,1 / 0,95 / 0,8 = 191 GiB. Você pode generalizar esse cálculo da seguinte maneira:

Dados de origem * (1 + número de réplicas) * (1 + sobrecarga de indexação)/(1 - espaço reservado do Linux)/(1 - sobrecarga do OpenSearch serviço) = requisito mínimo de armazenamento

Ou você pode usar esta versão simplificada:

Dados da origem * (1 + número de réplicas) * 1,45 = requisito de armazenamento mínimo

Espaço de armazenamento insuficiente é uma das causas mais comuns da instabilidade do cluster. Portanto, é necessário verificar os números ao escolher tipos de instância, as contagens de instâncias e os volumes de armazenamento.

Existem outras considerações de armazenamento:

- Se o requisito mínimo de armazenamento ultrapassar 1 PB, consulte the section called “Escala de petabytes”.
- Se você tiver índices contínuos e quiser usar uma arquitetura quente-morna, consulte the section called “UltraWarm armazenamento”.

Como escolher o número de fragmentos

Depois de entender os requisitos de armazenamento, você poderá investigar a sua estratégia de indexação. Por padrão, no OpenSearch Serviço, cada índice é dividido em cinco fragmentos principais e uma réplica (total de 10 fragmentos). Esse comportamento difere do código aberto OpenSearch, cujo padrão é um fragmento primário e uma réplica. Como você não pode alterar facilmente o número de fragmentos principais para um índice existente, decida sobre a contagem de fragmentos antes de indexar seu primeiro documento.

O objetivo geral de escolher um número de fragmentos é distribuir um índice de forma uniforme por todos os nós de dados no cluster. No entanto, esses fragmentos não devem ser muito grandes nem muito numerosos. Uma orientação geral é buscar manter o tamanho do fragmento entre 10 e 30 GiB, para workloads em que a latência de pesquisa é um dos principais objetivos de performance, e entre 30 e 50 GiB, para workloads em que há gravação intensa, como análise de log.

Fragmentos grandes podem dificultar OpenSearch a recuperação de falhas, mas como cada fragmento usa uma certa quantidade de CPU e memória, ter muitos fragmentos pequenos pode

causar problemas de desempenho e erros de falta de memória. Em outras palavras, os fragmentos devem ser pequenos o suficiente para que a instância de OpenSearch serviço subjacente possa lidar com eles, mas não tão pequenos que sobrecarreguem desnecessariamente o hardware.

Por exemplo, suponha que você tenha 66 GiB de dados. Você não espera que esse número aumente ao longo do tempo e deseja manter seus fragmentos em torno de 30 GiB cada um. Seu número de fragmentos, portanto, deve ser aproximadamente 66 * 1,1/30 = 3. Você pode generalizar esse cálculo da seguinte maneira:

(Dados da origem + espaço para crescer) * (1 + sobrecarga de indexação) / tamanho desejado do fragmento = número aproximado de fragmentos principais

Essa equação ajuda a compensar o crescimento dos dados ao longo do tempo. Se você espera que os mesmos 66 GiB de dados quadrupliquem nos próximos anos, o número aproximado de fragmentos será (66 + 198) * 1,1/30 = 10. No entanto, lembre-se de que você ainda não tem esses 198 GiB de dados extras. Verifique se essa preparação para o futuro não cria desnecessariamente fragmentos muito pequenos que consomem enormes quantidades de CPU e memória. Nesse caso, 66 * 1,1/10 fragmentos = 7,26 GiB por fragmento, o que consumirá recursos adicionais e está abaixo do intervalo de tamanho recomendado. Você pode considerar a middle-of-the-road abordagem mais ampla de seis fragmentos, o que deixa você com fragmentos de 12 GiB hoje e fragmentos de 48 GiB no futuro. Em seguida, novamente, você pode preferir começar com três fragmentos e reindexar seus dados quando os fragmentos ultrapassarem 50 GiB.

Um problema muito menos comum envolve limitar o número de fragmentos por nó. Se você dimensionar seus fragmentos adequadamente, normalmente ficará sem espaço em disco muito antes de atingir esse limite. Por exemplo, uma instância `m6g.large.search` tem um tamanho máximo de disco de 512 GiB. Se você ficar abaixo de 80% do uso do disco e dimensionar seus fragmentos em 20 GiB, ela poderá acomodar aproximadamente 20 fragmentos. Elasticsearch 7. x e versões posteriores, e todas as versões de OpenSearch, têm um limite de 1.000 fragmentos por nó. Para ajustar o máximo de fragmentos por nó, ajuste a configuração `cluster.max_shards_per_node`. Para ver um exemplo, consulte Configurações de cluster.

Se dimensionar os fragmentos adequadamente, você quase sempre se manterá abaixo desse limite, mas também é possível considerar o número de fragmentos para cada GiB de heap Java. Em um determinado nó, não tenha mais de 25 fragmentos por GiB de heap de Java. Por exemplo, uma instância `m5.large.search` tem um heap de 4 GiB, de modo que cada nó não deva ter mais de 100 fragmentos. Nessa contagem de fragmentos, cada fragmento tem aproximadamente 5 GiB de tamanho, o que está bem abaixo da nossa recomendação.

Escolha dos tipos de instância e testes

Depois de calcular os requisitos de armazenamento e escolher o número de fragmentos de que precisa, você pode começar a tomar decisões quanto ao hardware. Os requisitos de hardware variam drasticamente por workload, mas ainda podemos fazer algumas recomendações básicas.

Em geral, os limites de armazenamento para cada tipo de instância são mapeados para a quantidade de CPU e memória que pode ser necessária para workloads leves. Por exemplo, uma instância `m6g.large.search` tem um tamanho máximo de volume do EBS de 512 GiB, 2 núcleos de vCPUs e 8 GiB de memória. Se o seu cluster tiver muitos fragmentos, executar agregações desgastantes, atualizar os documentos com frequência ou processar um grande número de consultas, esses recursos poderão ser insuficientes para suas necessidades. Se o cluster estiver em uma dessas categorias, tente começar com uma configuração mais próxima de dois núcleos de vCPU e 8 GiB de memória para cada 100 GiB de seu requisito de armazenamento.

> **Tip**
>
> Para obter um resumo dos recursos de hardware que são alocados para cada tipo de instância, consulte os preços do Amazon OpenSearch Service.

No entanto, até mesmo esses recursos podem ser insuficientes. Alguns OpenSearch usuários relatam que muitas vezes precisam desses recursos para atender às suas necessidades. Para localizar o hardware certo para sua workload, é necessário fazer uma estimativa inicial embasada, testar workloads representativas, ajustar e testar novamente.

Etapa 1: Fazer uma estimativa inicial

Para começar, recomendamos um mínimo de três nós para evitar possíveis OpenSearch problemas, como um estado cerebral dividido (quando um lapso na comunicação leva a um cluster com dois nós principais). Se você tiver três nós principais dedicados, ainda recomendamos um mínimo de dois nós de dados para replicação.

Etapa 2: Calcular os requisitos de armazenamento por nó

Se você tiver um requisito de 184 GiB de armazenamento e o número mínimo recomendado for de três nós, use a equação 184/3 = 61 GiB para determinar a quantidade de armazenamento necessária para cada nó. Nesse exemplo, é possível selecionar três instâncias `m6g.large.search`, em que cada uma usa um volume de armazenamento do EBS de 90 GiB,

para que você tenha uma rede de segurança e espaço para crescimento ao longo do tempo. Essa configuração fornece 6 núcleos de vCPU e 24 GiB de memória, portanto, é adequada para workloads mais leves.

Para obter um exemplo mais substancial, considere um requisito de armazenamento de 14 TiB (14.336 GiB) e uma workload pesada. Nesse caso, você pode optar por iniciar testes com 2 * 144 = 288 núcleos de vCPU e 8 * 144 = 1.152 GiB de memória. Esses números funcionam para aproximadamente 18 instâncias do `i3.4xlarge.search`. Se você não precisar do armazenamento local rápido, também poderá testar 18 instâncias `r6g.4xlarge.search`, cada uma usando um volume de armazenamento do EBS de 1 TiB.

Se o cluster incluir centenas de terabytes de dados, consulte the section called “Escala de petabytes”.

Etapa 3: Executar o teste de representatividade

Depois de configurar o cluster, você pode adicionar seus índices usando o número de fragmentos calculados anteriormente, realizar alguns testes representativos do cliente usando um conjunto de dados realista e monitorar CloudWatch métricas para ver como o cluster lida com a carga de trabalho.

Etapa 4: Sucesso ou iteração

Se o desempenho satisfizer suas necessidades, os testes forem bem-sucedidos e CloudWatch as métricas estiverem normais, o cluster estará pronto para uso. Lembre-se de definir CloudWatch alarmes para detectar o uso insalubre de recursos.

Se a performance não for aceitável, os testes falharem ou `CPUUtilization` ou `JVMMemoryPressure` estiverem altas, poderá ser necessário escolher um tipo de instância diferente (ou adicionar instâncias) e continuar o teste. Conforme você adiciona instâncias, reequilibra OpenSearch automaticamente a distribuição dos fragmentos em todo o cluster.

Como é mais fácil medir a capacidade em excesso de um cluster sobrecarregado do que o déficit de um cluster não sobrecarregado, recomendamos começar com um cluster maior do que você imagina ser necessário. Depois, teste e reduza para um cluster eficiente que tenha os recursos adicionais a fim de garantir operações estáveis durante períodos de maior atividade.

Os clusters de produção ou os clusters com estados complexos se beneficiam de nós principais dedicados, que melhoram a performance e a confiabilidade do cluster.

Escala de petabytes no Amazon Service OpenSearch

Os domínios do Amazon OpenSearch Service oferecem armazenamento anexado de até 3 PB. Você pode configurar um domínio com 200 tipos de instância `i3.16xlarge.search`, cada um com 15 TB de armazenamento. Devido à grande diferença em escala, as recomendações para domínios desse tamanho diferem de nossas recomendações gerais. Esta seção descreve as considerações para a criação de domínios, custos, armazenamento e tamanho de fragmento.

Embora esta seção frequentemente faça referência a tipos de instância `i3.16xlarge.search`, você pode usar vários outros tipos de instância para alcançar 1 PB do total de armazenamento de domínio.

Criar domínios

Domínios desse tamanho excedem o limite padrão de 80 instâncias por domínio. Para solicitar um aumento do limite de serviço de até 200 instâncias por domínio, abra um caso no AWS Support Center.

Definição de preço

Antes de criar um domínio desse tamanho, verifique a página de preços do Amazon OpenSearch Service para garantir que os custos associados correspondam às suas expectativas. Examine the section called “UltraWarm armazenamento” para ver se uma arquitetura de atividade muito alta é adequada ao seu caso de uso.

Armazenamento

Os tipos de instância `i3` são projetados para fornecer armazenamento local e rápido de memória expressa não volátil (NVMe). Como esse armazenamento local tende a oferecer benefícios de desempenho quando comparado ao Amazon Elastic Block Store, os volumes do EBS não são uma opção quando você seleciona esses tipos de instância no OpenSearch Service. Se você preferir o armazenamento do EBS, use outro tipo de instância, como `r6.12xlarge.search`.

Tamanho e contagem de fragmentos

Uma OpenSearch diretriz comum é não exceder 50 GB por fragmento. Considerando o número de fragmentos necessários para acomodar grandes domínios e os recursos disponíveis para instâncias `i3.16xlarge.search`, recomendamos um tamanho de fragmento de 100 GB.

Por exemplo, se você tiver 450 TB de dados de origem e quiser uma réplica, seu requisito de armazenamento mínimo será mais próximo de 450 TB * 2 * 1,1/0.95 = 1.04 PB. Para obter

uma explicação sobre esse cálculo, consulte the section called “Cálculo de requisitos de armazenamento”. Embora 1,04 PB / 15 TB = 70 instâncias, você pode selecionar 90 ou mais instâncias `i3.16xlarge.search` para obter uma rede de segurança de armazenamento, lidar com falhas de nós e lidar com alguma variação na quantidade de dados ao longo do tempo. Cada instância adiciona outros 20 GiB ao seu requisito de armazenamento mínimo, ainda que para discos deste tamanho, esses 20 GiB sejam quase insignificantes.

Controlar o número de fragmentos é complicado. OpenSearch os usuários geralmente alternam os índices diariamente e retêm os dados por uma ou duas semanas. Nesta situação, pode ser útil distinguir entre fragmentos "ativos" e "inativos". fragmentos ativos estão sendo gravados ou lidos ativamente. Fragmentos inativos podem servir para uma solicitação de leitura ocasional, mas são essencialmente ociosos. Em geral, você deve manter o número de fragmentos ativos abaixo de alguns milhares. À medida que o número de fragmentos ativos se aproxima de 10.000, riscos de performance e de estabilidade consideráveis podem surgir.

Para calcular o número de fragmentos principais, use esta fórmula: 450.000 GB * 1,1/100 GB por fragmento = 4,950 fragmentos. Ao dobrar esse número para contabilizar réplicas, temos 9.900 fragmentos, o que representa uma grande preocupação se todos os fragmentos estão ativos. No entanto, se você alternar índices e apenas 1/7 ou 1/14 dos fragmentos estiver ativo em um determinado dia (1.414 ou 707 fragmentos, respectivamente), o cluster poderá funcionar normalmente. Como sempre, a etapa mais importante do dimensionamento e da configuração do domínio é executar testes de cliente representativos usando um conjunto de dados realista.

Nodes mestres dedicados no Amazon OpenSearch Service

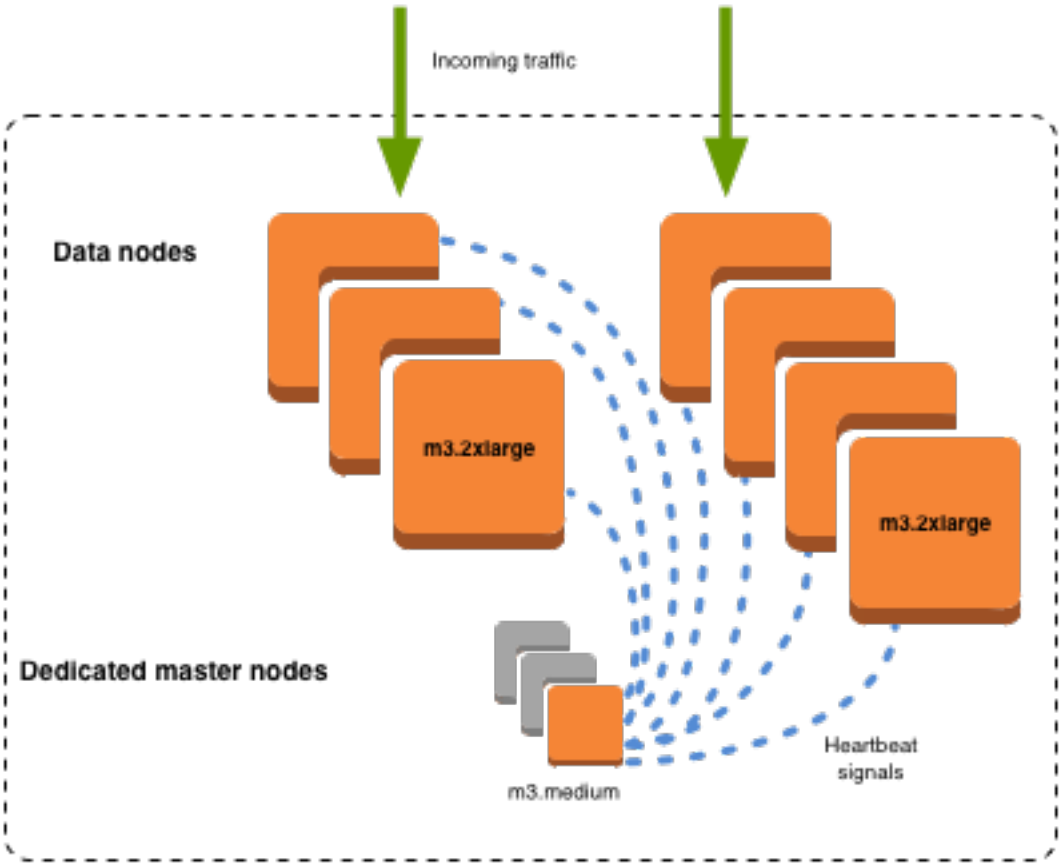
O Amazon OpenSearch Service usa nós principais dedicados para aumentar a estabilidade do cluster. Um nó principal dedicado executa tarefas de gerenciamento de cluster, mas não mantém dados nem responde a solicitações de carregamento de dados. Essa transferência de tarefas de gerenciamento de cluster aumenta a estabilidade do seu domínio. Assim como todos os outros tipos de nó, você paga uma taxa por hora para cada nó principal dedicado.

Nós principais dedicados executam as seguintes tarefas de gerenciamento de cluster:

- Rastreiam todos os nós no cluster.
- Rastreiam o número de índices no cluster.
- Rastreiam o número de fragmentos pertencentes a cada índice.
- Mantêm informações de roteamento para nós no cluster.

- Atualizam o estado do cluster após alterações de estado, como criação de um índice e adição ou remoção de nós no cluster.
- Replicam alterações no estado do cluster em todos os nós no cluster.
- Monitoram a integridade de todos os nós do cluster, enviando sinais de pulsação, sinais periódicos que monitoram a disponibilidade de nós de dados no cluster.

A ilustração a seguir mostra um domínio OpenSearch de serviço com 10 instâncias. Sete das instâncias são nós de dados e três são nós principais dedicados. Somente um dos nós principais dedicados está ativo. Os dois nós principais dedicados de cor cinza aguardam como backup em caso de falha do nó principal dedicado ativo. Todas as solicitações de carregamento de dados são atendidas por sete nós de dados, e todas as tarefas de gerenciamento de cluster são transferidas para o nó principal dedicado ativo.



Como escolher o número de nós principais dedicados

Recomendamos que você use o Multi-AZ com Standby, que adiciona três nós mestres dedicados a cada domínio do OpenSearch Serviço de produção. Se você implantar com multi-AZ sem modo de espera ou com single-AZ (uma única zona de disponibilidade), ainda recomendamos três nós principais dedicados. Nunca escolha um número par de nós principais dedicados. Considere o seguinte ao escolher o número de nós principais dedicados:

- Um nó principal dedicado é explicitamente proibido pelo OpenSearch Serviço porque você não tem backup no caso de uma falha. Você receberá uma exceção de validação se tentar criar um domínio com apenas um nó principal dedicado.
- Se você tiver dois nós principais dedicados, seu cluster não terá o quorum necessário de nós para escolher um novo nó principal em caso de falha.

  Um quorum é o número de nós principais dedicados/2+1 (arredondado para o número inteiro mais próximo). Neste caso, 2/2 + 1 = 2. Como um nó principal dedicado falhou e existe apenas um backup, o cluster não tem um quorum e não pode selecionar um novo principal.
- Três nós principais dedicados, o número recomendado, fornecem dois nós de backup em caso de falha de um nó principal e o quorum necessário (2) para selecionar um novo principal.
- Ter quatro nós principais dedicados não é melhor do que ter três, e isso poderá causar problemas se você usar várias zonas de disponibilidade.
  - Se um nó principal falhar, você tem o quorum (3) para escolher um novo principal. Se dois nós falharem, você perderá esse quorum, da mesma forma com três nós principais dedicados.
  - Em uma configuração de três zonas de disponibilidade, duas AZs têm um nó principal dedicado e uma AZ tem dois. Se essa AZ sofrer uma interrupção, as duas AZs restantes não terão o quorum necessário (3) para escolher um novo principal.
- Ter cinco nós principais dedicados funciona tão bem quanto ter três e permite que você perca dois nós enquanto mantém um quorum. No entanto, como apenas um nó principal dedicado está ativo a qualquer momento, essa configuração significa que você pagará por quatro nós ociosos. Muitos usuários acham esse nível de proteção de failover excessivo.

Se um cluster tiver um número par de nós elegíveis como mestre, OpenSearch e as versões 7 do Elasticsearch. x e posteriores ignoram um nó para que a configuração de votação seja sempre um número ímpar. Nesse caso, quatro nós principais dedicados são essencialmente equivalentes a três (e dois a um).

> **Note**
>
> Se o cluster não tiver o quorum necessário para escolher um novo nó principal, ocorrerão falhas nas solicitações de gravação e leitura para o cluster. Esse comportamento é diferente do OpenSearch padrão.

Escolher tipos de instâncias para nós principais dedicados

Embora os nós principais dedicados não processem solicitações de pesquisa e consulta, seu tamanho está amplamente correlacionado ao tamanho da instância e ao número de instâncias, índices e fragmentos que podem gerenciar. Para clusters de produção, recomendamos pelo menos os seguintes tipos de instâncias para nós principais dedicados.

Essas recomendações se baseiam em workloads usuais e podem variar de acordo com suas necessidades. Clusters com muitos fragmentos ou mapeamentos de campo podem se beneficiar de tipos de instância maiores. Monitore as métricas do nó principal dedicado para ver se será necessário usar um tipo de instância maior.

Contagem de instâncias	Tamanho da RAM do nó principal	Contagem máxima de fragmentos aceita	Mínimo recomendado de tipo de instância principal dedicada
1 – 10	8 GiB	10 mil	`m5.large.search` ou `m6g.large.search`
11 – 30	16 GiB	30 mil	`c5.2xlarge.search` ou `c6g.2xlarge.search`
37 – 75	32 GiB	40K	`r5.xlarge.search` ou `r6g.xlarge.search`

Contagem de instâncias	Tamanho da RAM do nó principal	Contagem máxima de fragmentos aceita	Mínimo recomendado de tipo de instância principal dedicada
76 – 125	64 GiB	75 mil	`r5.2xlarge.search` ou `r6g.2xlarge.search`
126 – 200	128 GiB	75 mil	`r5.4xlarge.search` ou `r6g.4xlarge.search`

- Para obter informações sobre como determinadas alterações de configuração podem afetar os nós principais dedicados, consulte the section called “Alterações de configuração”.
- Para obter esclarecimentos sobre os limites de contagem de instâncias, consulte Domínio do OpenSearch serviço e cotas de instância.
- Para obter mais informações sobre tipos específicos de instâncias, incluindo vCPU, memória e preços, consulte os preços do Amazon OpenSearch Service.

CloudWatch Alarmes recomendados para o Amazon Service OpenSearch

CloudWatch os alarmes realizam uma ação quando uma CloudWatch métrica excede um valor especificado por um determinado período de tempo. Por exemplo, talvez você queira AWS enviar um e-mail se o status de integridade do seu cluster `red` for superior a um minuto. Esta seção inclui alguns alarmes recomendados para o Amazon OpenSearch Service e como responder a eles.

Você pode implantar automaticamente esses alarmes usando AWS CloudFormation. Para ver uma pilha de amostra, consulte o GitHubrepositório relacionado.

> **Note**
>
> Se você implantar a CloudFormation pilha, os `KMSKeyInaccessible` alarmes `KMSKeyError` e existirão em um `Insufficient Data` estado porque essas métricas só aparecerão se um domínio encontrar um problema com sua chave de criptografia.

Para obter mais informações sobre a configuração de alarmes, consulte Criação de CloudWatchalarmes da Amazon no Guia do usuário da Amazon CloudWatch .

Alarme	Problema
Máximo de `ClusterStatus.red` é >= 1 por 1 minuto, 1 período consecutivo	Pelo menos um fragmento principal e suas réplicas não estão alocados para um nó. Consulte the section called “Status de cluster vermelho”.
O máximo de `ClusterStatus.yellow` é >= um por um minuto, cinco vezes consecutivas	Pelo menos um fragmento de réplica não está alocado para um nó. Consulte the section called “Status de cluster amarelo”.
Mínimo de `FreeStorageSpace` é <= 20480 por 1 minuto, 1 período consecutivo	Um nó no seu cluster tem 20 GiB de espaço de armazenamento livre. Consulte the section called “Falta de espaço de armazenamento disponível”. Esse valor é em MiB; portanto, em vez de 20.480, recomendamos defini-lo como 25% do espaço de armazenamento para cada nó.
`ClusterIndexWritesBlocked` é >= 1 por 5 minutos, 1 período consecutivo	O cluster está bloqueando solicitações de gravação. Consulte the section called “ClusterBlockException”.

Alarme	Problema
Mínimo de `Nodes` é < x por 1 dia, 1 período consecutivo	x é o número de nós em seu cluster. Esse alarme indica que pelo menos um nó no cluster permaneceu inacessível por um dia. Consulte the section called “Nós de cluster com falha”.

Máximo de `AutomatedSnapshotFailure` é >= 1 por 1 minuto, 1 período consecutivo	Ocorreu falha em um snapshot automatizado. Essa falha normalmente é o resultado de um status de integridade vermelho do cluster. Consulte the section called “Status de cluster vermelho”.
	
	Para obter um resumo de todos os snapshots automatizados e algumas informações sobre falhas, experimenteo uma das seguintes solicitaç ões:
	
	`GET domain_endpoint /_snapshot/cs-automated/_all`
	`GET domain_endpoint /_snapshot/cs-automated-enc/_all`

O máximo de `CPUUtilization` ou `WarmCPUUtilization` é >= 80% por 15 minutos, 3 períodos consecutivos	Às vezes, pode ocorrer 100% de utilização da CPU, mas o alto uso sustentado é um problema. Considere o uso de tipos de instância maiores ou a adição de instâncias.
O máximo de `JVMMemoryPressure` é >= 95% por um minuto, três vezes consecutivas	O cluster poderá apresentar erros de memória insuficiente se o uso aumentar. Considere escalar verticalmente. OpenSearch O serviço usa metade da RAM de uma instância para o heap Java, até um tamanho de heap de 32 GiB. Você pode dimensionar instâncias verticalmente até 64 GiB de RAM, sendo que nesse ponto você poderá dimensionar horizontalmente adicionando instâncias.
O máximo de `OldGenJVMMemoryPressure` é >= 80% por um minuto, três vezes consecutivas	

Alarme	Problema
O máximo de `MasterCPU Utilization` é >= 50% por 15 minutos, 3 períodos consecutivos	Considere o uso de tipos de instância maiores para os nós principais dedicados. Devido à sua função na estabilidade do cluster e implantações azuis/verdes, os nós principais dedicados devem ter um uso de CPU menor do que os nós de dados.
O máximo de `MasterJVM MemoryPressure` é >= 95% por um minuto, três vezes consecutivas	
O máximo de `MasterOld GenJVMMem oryPressure` é >= 80% por um minuto, três vezes consecuti vas	
`KMSKeyError` é >= 1 por 1 minuto, 1 período consecutivo	A chave de AWS KMS criptografia usada para criptografar dados em repouso no seu domínio está desativada. Reative-a para restaurar as operações normais. Para ter mais informações, consulte the section called “Criptografia inativa”.
`KMSKeyIna ccessible` é >= 1 por 1 minuto, 1 período consecutivo	A chave de AWS KMS criptografia usada para criptografar dados em repouso em seu domínio foi excluída ou revogou suas concessões ao OpenSearch Serviço. Você não pode recuperar os domínios que estejam nesse estado. Porém, se tiver um snapshot manual, você poderá usá-lo para migrar para um novo domínio. Para saber mais, consulte the section called “Criptografia inativa”.

Alarme	Problema
`shards.active` é >= 30.000 por 1 minuto, 1 período consecutivo	O número total de fragmentos ativos primários e de réplica é maior que 30.000. Talvez você esteja alternando seus índices com muita frequência. Considere usar o ISM para remover índices quando atingirem um período de validade específico.
Alarmes 5*xx* >= 10% de `OpenSearchRequests`	Um ou mais nós de dados podem estar sobrecarregados ou as solicitações não são concluídas dentro do período de tempo limite ocioso. Considere alternar para tipos de instância maiores ou adicionar mais nós ao cluster. Confirme se você está seguindo as práticas recomendadas para arquitetura de fragmentos e clusters.
`MasterReachableFromNode` máximo é < 1 por 5 minutos, 1 vez consecutiva	Esse alarme indica que o nó principal foi interrompido ou está fora do alcance. Essas falhas geralmente são o resultado de um problema de conectividade de rede ou de AWS dependência.
A média de `ThreadpoolWriteQueue` é >= 100 por 1 minuto, 1 período consecutivo	O cluster está passando por alta simultaneidade de indexação. Revise e controle as solicitações de indexação ou aumente os recursos do cluster.
A média de `ThreadpoolSearchQueue` é >= 500 por 1 minuto, 1 período consecutivo	O cluster está passando por alta simultaneidade de pesquisa. Avalie a possibilidade de escalar seu cluster. Você também pode aumentar o tamanho da fila de pesquisa, mas aumentá-la excessivamente pode causar erros de falta de memória.
O máximo de `ThreadpoolSearchQueue` é >= 5.000 por 1 minuto, 1 período consecutivo	

Alarme	Problema
O aumento na SOMA de `Threadpool SearchRejected` é >=1{ math expression DIFF ( )} por um minuto, um período consecutivo	Esses alarmes notificam você sobre problemas de domínio que podem afetar a performance e a estabilidade.
O aumento na SOMA de `Threadpool WriteRejected` é >=1{ math expression DIFF ( )} por um minuto, um período consecutivo	

> **Note**
>
> Se você só desejar visualizar métricas, consulte the section called “Monitoramento de métricas de cluster”.

Outros alarmes que você pode considerar

Considere configurar os seguintes alarmes, dependendo dos recursos do OpenSearch Serviço que você usa regularmente.

Alarme	Problema
O mínimo de `WarmFreeStorageSpace` é <= 10.240 por 1 minuto, 1 período consecutivo	Um UltraWarm nó em seu cluster tem menos de 10 GiB de espaço de armazenamento livre. Consulte the section called “Falta de espaço de armazenamento disponível”. Esse valor está em MiB, portanto, em vez de 10240, recomendamos configurá-lo para 10% do espaço de armazenamento de cada nó. UltraWarm

Alarme	Problema
`HotToWarmMigrationQueueSize` é >= 20 por 1 minuto, 3 períodos consecutivos	Um grande número de índices está migrando simultaneamente do sistema ativo para o UltraWarm armazenamento. Avalie a possibilidade de escalar seu cluster.
`HotToWarmMigrationSuccessLatency` é >= 1 dia, 1 período consecutivo	Configure este alarme para que você seja notificado se `HotToWarmMigrationSuccessCount` x latência for maior que 24 horas, caso você esteja tentando alterar índices diários.
O máximo de `WarmJVMMemoryPressure` é >= 95% por um minuto, três vezes consecutivas	O cluster poderá apresentar erros de memória insuficiente se o uso aumentar. Considere escalar verticalmente. OpenSearch O serviço usa metade da RAM de uma instância para o heap Java, até um tamanho de heap de 32 GiB. Você pode dimensionar instâncias verticalmente até 64 GiB de RAM, sendo que nesse ponto você poderá dimensionar horizontalmente adicionando instâncias.
O máximo de `WarmOldGenJVMMemoryPressure` é >= 80% por um minuto, três vezes consecutivas	
`WarmToColdMigrationQueueSize` é >= 20 por 1 minuto, 3 períodos consecutivos	Um grande número de índices está migrando simultaneamente UltraWarm para o armazenamento refrigerado. Avalie a possibilidade de escalar seu cluster.

Alarme	Problema
`HotToWarm Migration FailureCount` é >= 1 por 1 minuto, 1 período consecutivo	As migrações podem falhar durante os snapshots, as realocações de fragmentos ou as uniões de força. As falhas durante os snapshots ou as realocações de fragmentos geralmente ocorrem devido a falhas de nós ou a problemas de conectividade do S3. A falta de espaço em disco geralmente é a causa subjacente das falhas de união de força.
`WarmToCol dMigratio nFailureCount` é >= 1 por 1 minuto, 1 período consecutivo	As migrações geralmente falham quando as tentativas de migrar metadados de índice para o armazenamento frio falham. Também podem ocorrer falhas quando o estado do cluster de índice quente estiver sendo removido.
`WarmToCol dMigratio nLatency` é >= 1 dia, 1 período consecutivo	Configure este alarme para que você seja notificado se `WarmToCol dMigrationSuccessCount` x latência for maior que 24 horas, caso você esteja tentando alterar índices diários.
`AlertingDegraded` é >= 1 por 1 minuto, 1 período consecutivo	O índice de alerta é vermelho ou um ou mais nós não estão na programação.
`ADPluginU nhealthy` é >= 1 por 1 minuto, 1 período consecutivo	O plug-in de detecção de anomalias não está funcionando corretame nte, seja por causa de altas taxas de falhas, seja por um dos índices que está sendo usado estar vermelho.
`Asynchron ousSearch FailureRate` é >= 1 por 1 minuto, 1 período consecutivo	Pelo menos uma pesquisa assíncrona falhou no último minuto, o que provavelmente significa que o nó coordenador falhou. O ciclo de vida de uma solicitação de pesquisa assíncrona é gerenciado exclusiva mente no nó do coordenador, portanto, se o coordenador ficar inativo, a solicitação falhará.

Alarme	Problema
`AsynchronousSearchStoreHealth` é >= 1 por 1 minuto, 1 período consecutivo	A integridade do armazenamento de respostas de pesquisa assíncrona no índice persistido é vermelha. Você pode estar armazenando grandes respostas assíncronas, que podem desestabilizar um cluster. Tente limitar suas respostas de pesquisa assíncronas a 10 MB ou menos.
`SQLUnhealthy` é >= 1 por 1 minuto, 3 períodos consecutivos	O plug-in SQL está retornando 5 códigos de resposta xx ou passando uma consulta DSL inválida para. OpenSearch Solucione o problema das solicitações que os clientes estão fazendo ao plug-in.
`LTRStatus.red` é >= 1 por 1 minuto, 1 período consecutivo	Pelo menos um dos índices necessários para executar o plug-in Learning to Rank tem fragmentos primários ausentes e não está funcional.

Referência geral para Amazon OpenSearch Service

O Amazon OpenSearch Service oferece suporte a uma variedade de instâncias, operações, plug-ins e outros recursos.

Tópicos

Tipos de instância compatíveis no Amazon OpenSearch Service

O Amazon OpenSearch Service oferece suporte aos seguintes tipos de instância. Nem todas as regiões são compatíveis com todos os tipos de instância. Para obter detalhes de disponibilidade, consulte os preços OpenSearch do Amazon Service.

Para obter informações sobre qual tipo de instância é apropriado para seu caso de uso, consulte the section called “Dimensionamento de domínios”, the section called “Limites de tamanhos de volume do EBS” e the section called “Limites de rede”.

Tipos de instâncias da geração atual

Para obter o melhor desempenho, recomendamos que você use os seguintes tipos de instância ao criar novos domínios OpenSearch de serviço.

Tipo de instância	Instâncias	Restrições
OR1	`or1.medium.search`	• Os tipos de instância OR1 exigem a OpenSearch versão 2.11 ou posterior.

Tipo de instância	Instâncias	Restrições
	or1.large.search or1.xlarge.search or1.2xlarge.search or1.4xlarge.search or1.8xlarge.search or1.12xlarge.search or1.16xlarge.search	• As instâncias OR1 são compatíveis apenas com outros nós principais de tipos de instância Graviton (C6g, M6g, R6g).

Tipo de instância	Instâncias	Restrições

Im4gn	`im4gn.large.search`
	`im4gn.xlarge.search`
	`im4gn.2xlarge.search`
	`im4gn.4xlarge.search`
	`im4gn.8xlarge.search`
	`im4gn.16xlarge.search`
		• Os tipos de instância IM4gn exigem o Elasticsearch 7.9 ou posterior ou qualquer versão do OpenSearch, e não oferecem suporte aos volumes de armazenamento do EBS.
		• As instâncias Im4gn só são compatíveis com outros tipos de instância Graviton (C6g, M6g, R6g, R6gd). Você não pode combinar instâncias do Graviton e não Graviton no mesmo cluster.

Tipo de instância	Instâncias	Restrições

C5	`c5.large.search`
	`c5.xlarge.search`
	`c5.2xlarge.search`
	`c5.4xlarge.search`
	`c5.9xlarge.search`
	`c5.18xlarge.search`
		Os tipos de instância C5 exigem o Elasticsearch 5.1 ou posterior ou qualquer versão do. OpenSearch

Tipo de instância	Instâncias	Restrições

C6g	`c6g.large.search`
	`c6g.xlarge.search`
	`c6g.2xlarge.search`
	`c6g.4xlarge.search`
	`c6g.8xlarge.search`
	`c6g.12xlarge.search`
		• Os tipos de instância C6g exigem o Elasticsearch 7.9 ou posterior ou qualquer versão do. OpenSearch
		• As instâncias C6g só são compatíveis com outros tipos de instância Graviton (Im4gn, M6g, R6g, R6gd). Você não pode combinar instâncias do Graviton e não Graviton no mesmo cluster.

Tipo de instância	Instâncias	Restrições

I3	`i3.large.search`
	`i3.xlarge.search`
	`i3.2xlarge.search`
	`i3.4xlarge.search`
	`i3.8xlarge.search`
	`i3.16xlarge.search`
		Os tipos de instância I3 exigem o Elasticsearch 5.1 ou posterior ou qualquer versão do OpenSearch, e não oferecem suporte aos volumes de armazenamento do EBS.

M5	`m5.large.search`
	`m5.xlarge.search`
	`m5.2xlarge.search`
	`m5.4xlarge.search`
	`m5.12xlarge.search`
		Os tipos de instância M5 exigem o Elasticsearch 5.1 ou posterior ou qualquer versão do. OpenSearch

Tipo de instância	Instâncias	Restrições

M6g	`m6g.large.search`
	`m6g.xlarge.search`
	`m6g.2xlarge.search`
	`m6g.4xlarge.search`
	`m6g.8xlarge.search`
	`m6g.12xlarge.search`
		• Os tipos de instância M6g exigem o Elasticsearch 7.9 ou posterior ou qualquer versão do. OpenSearch
		• As instâncias M6g só são compatíveis com outros tipos de instância Graviton (Im4gn, C6g, R6g, R6gd). Você não pode combinar instâncias do Graviton e não Graviton no mesmo cluster.

Tipo de instância	Instâncias	Restrições

R5	`r5.large.search`
	`r5.xlarge.search`
	`r5.2xlarge.search`
	`r5.4xlarge.search`
	`r5.12xlarge.search`
		Os tipos de instância R5 exigem o Elasticsearch 5.1 ou posterior ou qualquer versão do. OpenSearch

Tipo de instância	Instâncias	Restrições

R6g	`r6g.large.search`
	`r6g.xlarge.search`
	`r6g.2xlarge.search`
	`r6g.4xlarge.search`
	`r6g.8xlarge.search`
	`r6g.12xlarge.search`
		• Os tipos de instância R6g exigem o Elasticsearch 7.9 ou posterior ou qualquer versão do. OpenSearch
		• As instâncias R6g só são compatíveis com outros tipos de instância Graviton (Im4gn, C6g, M6g, R6gd). Você não pode combinar instâncias do Graviton e não Graviton no mesmo cluster.

Tipo de instância	Instâncias	Restrições

R6gd	`r6gd.large.search`
	`r6gd.xlarge.search`
	`r6gd.2xlarge.search`
	`r6gd.4xlarge.search`
	`r6gd.8xlarge.search`
	`r6gd.12xlarge.search`
	`r6gd.16xlarge.search`
		• Os tipos de instância R6gd exigem o Elasticsearch 7.9 ou posterior ou qualquer versão do OpenSearch, e não oferecem suporte aos volumes de armazenamento do EBS.
		• As instâncias R6gd só são compatíveis com outros tipos de instância Graviton (Im4gn, C6g, M6g, R6g). Você não pode combinar instâncias do Graviton e não Graviton no mesmo cluster.

Tipo de instância	Instâncias	Restrições
T3	`t3.small.search` `t3.medium.search`	• Os tipos de instância T3 exigem o Elasticsearch 5.6 ou posterior ou qualquer versão do. OpenSearch • Você pode usar tipos de instância T3 somente se seu domínio for provisionado sem espera. Para ter mais informações, consulte the section called “Multi-AZ sem modo de espera”. • Você pode usar tipos de instância T3 somente se a contagem de instâncias do seu domínio for 10 ou menos. • Os tipos de instância T3 não oferecem suporte a UltraWarm armazenamento, armazenamento frio ou ajuste automático.

Tipos de instância da geração anterior

OpenSearch O serviço oferece tipos de instância da geração anterior para usuários que otimizaram seus aplicativos e ainda precisam fazer o upgrade. Recomendamos que você use os tipos de instância da geração atual para obter a melhor performance, mas continuamos a oferecer suporte aos seguintes tipos de instância da geração anterior.

Tipo de instância	Instâncias	Restrições

C4	`c4.large.search`
	`c4.xlarge.search`
	`c4.2xlarge.search`
	`c4.4xlarge.search`	

Tipo de instância	Instâncias	Restrições
	`c4.8xlarge.search`	
I2	`i2.xlarge.search` `i2.2xlarge.search`	

M3	`m3.medium.search`
	`m3.large.search`
	`m3.xlarge.search`
	`m3.2xlarge.search`
		• Os tipos de instância M3 não oferecem suporte à criptografia de dados em repouso, ao controle de acesso refinado ou à pesquisa entre clusters.
		• Os tipos de instância M3 têm restrições adicionais por OpenSearch versão. Para saber mais, consulte the section called “Tipo de instância M3 inválido”.

M4	`m4.large.search`
	`m4.xlarge.search`
	`m4.2xlarge.search`
	`m4.4xlarge.search`
	`m4.10xlarge.search`	

Tipo de instância	Instâncias	Restrições

R3	`r3.large.search`
	`r3.xlarge.search`
	`r3.2xlarge.search`
	`r3.4xlarge.search`
	`r3.8xlarge.search`
		Os tipos de instância R3 não oferecem suporte à criptografia de dados em repouso ou ao controle de acesso refinado.

R4	`r4.large.search`
	`r4.xlarge.search`
	`r4.2xlarge.search`
	`r4.4xlarge.search`
	`r4.8xlarge.search`
	`r4.16xlarge.search`	

Tipo de instância	Instâncias	Restrições

T2	`t2.micro.search`
	`t2.small.search`
	`t2.medium.search`
		• Você só poderá usar os tipos de instância T2 se a contagem de instâncias de seu domínio for 10 ou menos.
		• O tipo de instância `t2.micro.search` só oferece suporte ao Elasticsearch 1.5 e 2.3.
		• Os tipos de instância T2 não oferecem suporte à criptografia de dados em repouso, ao controle de acesso refinado, ao armazenamento, ao UltraWarm armazenamento frio, à pesquisa entre clusters ou ao Auto-Tune.

> **Tip**
>
> Muitas vezes, recomendamos usar tipos de instâncias diferentes para nós principais dedicados e nós de dados.

Recursos por versão do mecanismo no Amazon OpenSearch Service

Muitos recursos do OpenSearch Service têm um requisito mínimo de OpenSearch versão ou um requisito de versão antiga do Elasticsearch OSS. Se você atender à versão mínima de um recurso, mas o recurso não estiver disponível em seu domínio, atualize o software de serviço do seu domínio.

Atributo	OpenSearch Versão mínima exigida	Versão mínima necessária do Elasticsearch
Suporte à VPC	1.0	1,0
Exigir HTTPS para todo o		

Atributo	OpenSearch Versão mínima exigida	Versão mínima necessária do Elasticsearch
tráfego para o domínio		
Suporte Multi-AZ		
Nós principais dedicados		
Pacotes personalizados		
Endpoints personalizados		
Publicação de logs lentos		
Publicação de logs de erros	1,0	5.1
Criptografia de dados em repouso		
Autenticação Cognito para painéis OpenSearch		

Atributo	OpenSearch Versão mínima exigida	Versão mínima necessária do Elasticsearch
Atualizações no local		
Suporte ao curador	Não incluído	5.1
Snapshots automatizados por hora	1,0	5.3
ode-to-node CriptografiaN	1,0	6.0
Suporte a clientes REST de alto nível do Java		
Solicitação HTTP e compactação da resposta		
Geração de alertas	1,0	6.2
SQL	1,0	6.5
Pesquisa entre clusters	1,0	6.7

Atributo	OpenSearch Versão mínima exigida	Versão mínima necessária do Elasticsearch
Controle de acesso refinado		
Autenticação SAML para painéis OpenSearch		
Auto-Tune		
Reindexação remota		
UltraWarm	1,0	6.8
Gerenciamento de estados de índice		
k-NN por distância euclidiana	1,0	7.1
Detecção de anomalias	1,0	7.4
k-NN por similaridade de cosseno	1,0	7.7
Learning to Rank		

Atributo	OpenSearch Versão mínima exigida	Versão mínima necessária do Elasticsearch
Piped Processing Language	1,0	7.9
OpenSearch Relatórios de painéis		
OpenSearch Painéis e análises de rastreamento		
Instâncias do Graviton baseadas em ARM		
Armazenamento de baixa atividade		
Distância de Hamming, distância L1 Norm e desenvolvimento de scripts Painless para K-NN	1,0	7.10

Atributo	OpenSearch Versão mínima exigida	Versão mínima necessária do Elasticsearch
Pesquisa assíncrona		
Transformações de índices	1,0	Não incluído
Replicação entre clusters	1.1	7.10
ML Commons	1.3	Não incluído
Notificações	2.3	Não incluído
Pesquisa pontual	2,5	Não incluído
Pipelines de pesquisa	2.9	Não incluído
Conectores de Machine Learning	2.9	Não incluído
Pesquisa semântica multimodal	2.11	Não incluído
Fontes de dados de consulta direta para o Amazon S3	2.11	Não incluído

Para obter informações sobre plug-ins, que habilitam alguns desses recursos e funcionalidades adicionais, consulte the section called “Plug-ins por versão do mecanismo”. Para obter informações sobre a OpenSearch API de cada versão, consultethe section called “Operações compatíveis”.

Plugins por versão do mecanismo no Amazon OpenSearch Service

Os domínios OpenSearch do Amazon Service vêm pré-embalados com plug-ins da comunidade. OpenSearch O serviço implanta e gerencia automaticamente plug-ins para você, mas implanta plug-ins diferentes dependendo da versão OpenSearch ou do OSS Elasticsearch legado que você escolher para seu domínio.

A tabela a seguir lista os plug-ins por OpenSearch versão, bem como as versões compatíveis do Elasticsearch OSS legado. Ele inclui apenas plug-ins com os quais você pode interagir — não é abrangente. OpenSearch O serviço usa plug-ins adicionais para habilitar a funcionalidade principal do serviço, como o plug-in S3 Repository para instantâneos e o plug-in OpenSearchPerformance Analyzer para otimização e monitoramento. Para obter uma lista completa de todos os plug-ins em execução no seu domínio, faça a seguinte solicitação:

```
GET _cat/plugins?v
```

Plug-in	OpenSearch Versão mínima exigida	Versão mínima necessária do Elasticsearch
ICU Analysis	1,0	Incluído em todos os domínios
Japanese (kuromoji) Analysis		
Phonetic Analysis	1,0	2.3
Análise da Seunjeon Korean	1,0	5.1

Plug-in	OpenSearch Versão mínima exigida	Versão mínima necessária do Elasticsearch
Smart Chinese Analysis		
Stempel Polish Analysis		
Ingest Attachment Processor		
Ingest User Agent Processor		
Mapper Murmur3		
Mapper Size	1,0	5.3
Ukrainian Analysis		
OpenSearch alertando	1,0	6.2
OpenSearch SQL	1,0	6.5
OpenSearch segurança	1,0	6.7

Plug-in	OpenSearch Versão mínima exigida	Versão mínima necessária do Elasticsearch
OpenSearch Gerenciamento de estados de índice	1,0	6.8
OpenSearch k-NN	1,0	7.1
OpenSearch detecção de anomalias	1,0	7.4
Análise IK (Chinês)	1,0	7.7
Análise em vietnamita		
Análise em tailandês		
Learning to Rank		
OpenSearch pesquisa assíncrona	1,0	7.10
OpenSearch replicação entre clusters	1.1	7.10

Plug-in	OpenSearch Versão mínima exigida	Versão mínima necessária do Elasticsearch
OpenSearch observabilidade	1.2	Não suportado
Análise Nori	1.3	Não suportado
Análise Pinyin	1.3	Não suportado
ST Convert	1.3	Não suportado
Análise Sudachi	1.3	Não suportado
ML Commons	1.3	Não suportado
OpenSearch notificações	2.3	Não suportado
Security Analytics	2,5	Não suportado
Pesquisa neural	2.9	Não suportado
Ranking de pesquisa do Amazon Personalize	2.9	Não suportado

Plug-ins opcionais

Além dos plug-ins padrão que vêm pré-instalados, o Amazon OpenSearch Service oferece suporte a vários plug-ins de análise de linguagem. Esses plug-ins estão marcados como opcionais na tabela

acima. Você pode usar o AWS Management Console e AWS CLI para associar um plug-in a um domínio, desassociar um plug-in de um domínio e listar todos os plug-ins. Um pacote de plug-in opcional é compatível com uma OpenSearch versão específica e só pode ser associado a domínios com essa versão.

Observe que, quando você reassocia um arquivo de dicionário do plug-in Sudachi, ele não reflete imediatamente no domínio. O dicionário é atualizado quando a próxima implantação azul/verde é executada no domínio como parte de uma alteração de configuração ou outra atualização. Como alternativa, você pode criar um novo índice, reindexar o índice existente ao novo e, em seguida, excluir o índice antigo. Se preferir usar a abordagem de reindexação, use um alias de índice para que não haja interrupções no tráfego.

Os plug-ins opcionais usam o tipo de pacote `ZIP-PLUGIN`. Para obter mais informações sobre plug-ins opcionais, consulte the section called “Pacotes personalizados”.

Operações suportadas no Amazon OpenSearch Service

OpenSearch O serviço oferece suporte a várias versões OpenSearch e ao antigo Elasticsearch OSS. As seções a seguir mostram as operações que o OpenSearch Serviço suporta em cada versão.

Tópicos

- Elasticsearch versão 7.4
- Elasticsearch versão 7.1
- Elasticsearch versão 6.8
- Elasticsearch versão 6.7
- Elasticsearch versão 6.5
- Elasticsearch versão 6.4
- Elasticsearch versão 6.3
- Elasticsearch versão 6.2
- Elasticsearch versão 6.0
- Elasticsearch versão 5.6
- Elasticsearch versão 5.5
- Elasticsearch versão 5.3
- Elasticsearch versão 5.1
- Elasticsearch versão 2.3
- Elasticsearch versão 1.5

Diferenças notáveis de API

Configurações e estatísticas

OpenSearch O serviço só aceita solicitações PUT para a `_cluster/settings` API que usam o formulário de configurações “simples”. Ele rejeita solicitações que usam o formulário de configurações expandidas.

```
// Accepted
PUT _cluster/settings
{
  "persistent" : {
    "action.auto_create_index" : false
  }
}

// Rejected
PUT _cluster/settings
{
```

```
  "persistent": {
    "action": {
      "auto_create_index": false
    }
  }
}
```

O cliente Java REST de alto nível usa o formulário expandido, portanto, se for necessário enviar solicitações de configurações, use o cliente de baixo nível.

Antes do Elasticsearch 5.3, a `_cluster/settings` API em domínios de OpenSearch serviço suportava somente o `PUT` método HTTP, não o método. `GET` OpenSearch e versões posteriores do Elasticsearch oferecem suporte ao `GET` método, conforme mostrado no exemplo a seguir:

```
GET https://domain-name.region.es.amazonaws.com/_cluster/settings?pretty
```

Veja um exemplo de retorno:

```
{
  "persistent": {
    "cluster": {
      "routing": {
        "allocation": {
          "cluster_concurrent_rebalance": "2",
          "node_concurrent_recoveries": "2",
          "disk": {
            "watermark": {
              "low": "1.35gb",
              "flood_stage": "0.45gb",
              "high": "0.9gb"
            }
          },
          "node_initial_primarirecoveries": "4"
        }
      }
    },
    "indices": {
      "recovery": {
        "max_bytper_sec": "40mb"
      }
    }
  }
```

```
}
```

Se você comparar as respostas de um OpenSearch cluster de código aberto e de um OpenSearch serviço para determinadas APIs de configurações e estatísticas, poderá notar campos ausentes. OpenSearch O serviço redige determinadas informações que expõem os componentes internos do serviço, como o caminho de dados do sistema de arquivos `_nodes/stats` ou o nome e a versão do sistema operacional de. `_nodes`

Shrink

A API `_shrink` pode causar falhas em atualizações, alterações de configuração e exclusões de domínio. Não recomendamos usá-la em domínios que executam o Elasticsearch versões 5.3 ou 5.1. Essas versões têm um erro que pode causar falha na restauração de snapshots de índices reduzidos.

Se você usa a `_shrink` API em outras OpenSearch versões do Elasticsearch, faça a seguinte solicitação antes de iniciar a operação de redução:

```
PUT https://domain-name.region.es.amazonaws.com/source-index/_settings
{
  "settings": {
    "index.routing.allocation.require._name": "name-of-the-node-to-shrink-to",
    "index.blocks.read_only": true
  }
}
```

Depois, faça a seguinte solicitação após concluir a operação de redução:

```
PUT https://domain-name.region.es.amazonaws.com/source-index/_settings
{
  "settings": {
    "index.routing.allocation.require._name": null,
    "index.blocks.read_only": false
  }
}

PUT https://domain-name.region.es.amazonaws.com/shrunken-index/_settings
{
  "settings": {
    "index.routing.allocation.require._name": null,
    "index.blocks.read_only": false
  }
```

```
}
```

OpenSearch versão 2.11

Para a OpenSearch versão 2.11, o OpenSearch Service oferece suporte às seguintes operações. Para obter informações sobre a maioria das operações, consulte a referência da API OpenSearch REST ou a referência da API para o plug-in específico.

- Todas as operações no caminho do índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (exceto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para várias propriedades[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_plugins/_asynchronous_search`
- `/_plugins/_alerting`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_plugins/_ml`
- `/_plugins/_notifications`
- `/_plugins/_ppl`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search/pipeline`
- `/_search/point_in_time`
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- indices.breaker.total.limit
- cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_plugins/_security
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a string de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.
4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às OpenSearch operações genéricas que o OpenSearch Serviço suporta e não inclui operações suportadas específicas do plug-in para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

OpenSearch versão 2.9

Para a OpenSearch versão 2.9, o OpenSearch Service suporta as seguintes operações. Para obter informações sobre a maioria das operações, consulte a referência da API OpenSearch REST ou a referência da API para o plug-in específico.

- Todas as operações no caminho do índice (como */index-name* `/_forcemerge` , */index-*
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_refresh`
- `/_reindex` [1]
- `/_render`

name /update/*id* e /*index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (exceto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para várias propriedades[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search/pipeline
- /_search/point_in_time
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a string de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.
4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às OpenSearch operações genéricas que o OpenSearch Serviço suporta e não inclui operações suportadas específicas do plug-in para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

OpenSearch versão 2.7

Para OpenSearch 2.7, o OpenSearch Service suporta as seguintes operações. Para obter informações sobre a maioria das operações, consulte a referência da API OpenSearch REST ou a referência da API para o plug-in específico.

- Todas as operações no caminho do índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (exceto `/_cat/nodeattrs`)
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search/point_in_time`
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]

- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para várias propriedades[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `cluster.max_shards_per_node`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_dashboards`
- `/_plugins/_asynchronous_search`
- `/_plugins/_alerting`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_plugins/_ml`
- `/_plugins/_notifications`
- `/_plugins/_ppl`
- `/_plugins/_security`
- `/_plugins/_security_analytics`
- `/_plugins/_sm`
- `/_plugins/_sql`
- `/_percolate`
- `/_rank_eval`
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.

4. Refere-se ao método PUT. Para obter informações sobre o método GET, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às OpenSearch operações genéricas que o OpenSearch Serviço suporta e não inclui operações suportadas específicas do plug-in para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

OpenSearch versão 2.5

Para OpenSearch 2.5, o OpenSearch Service suporta as seguintes operações. Para obter informações sobre a maioria das operações, consulte a referência da API OpenSearch REST ou a referência da API para o plug-in específico.

- Todas as operações no caminho do índice (como */index-name* /_forcemerge , */index-name* /update/*id* e */index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (exceto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para várias propriedades[4]:
  - action.auto_create_index
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search/point_in_time
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.
4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às OpenSearch operações genéricas que o OpenSearch Serviço suporta e não inclui operações suportadas específicas do plug-in para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

OpenSearch versão 2.3

Para OpenSearch 2.3, o OpenSearch Service oferece suporte às seguintes operações. Para obter informações sobre a maioria das operações, consulte a referência da API OpenSearch REST ou a referência da API para o plug-in específico.

- Todas as operações no caminho do índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (exceto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para várias propriedades[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_plugins/_asynchronous_search`
- `/_plugins/_alerting`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_plugins/_ml`
- `_plugins/_notifications`
- `/_plugins/_ppl`
- `/_plugins/_security`
- `/_plugins/_sql`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- `indices.breaker.total.limit`
- `cluster.max_shards_per_node`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_dashboards`
- `/_percolate`
- `/_rank_eval`

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.
4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às OpenSearch operações genéricas que o OpenSearch Serviço suporta e não inclui operações suportadas específicas do plug-in para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

OpenSearch versão 1.3

Para OpenSearch 1.3, o OpenSearch Service oferece suporte às seguintes operações. Para obter informações sobre a maioria das operações, consulte a referência da API OpenSearch REST ou a referência da API para o plug-in específico.

- Todas as operações no caminho do índice (como */index-nam*
- `/_delete_by_query` [1]
- `/_explain`
- `/_refresh`
- `/_reindex` [1]

e /_forcemerge , /*index-name* /update/*id* e /*index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (exceto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para várias propriedades[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.
4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às OpenSearch operações genéricas que o OpenSearch Serviço suporta e não inclui operações suportadas específicas do plug-in para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

OpenSearch versão 1.2

Para OpenSearch 1.2, o OpenSearch Service oferece suporte às seguintes operações. Para obter informações sobre a maioria das operações, consulte a referência da API OpenSearch REST ou a referência da API para o plug-in específico.

- Todas as operações no caminho do índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (exceto `/_cat/nodeattrs`)
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`

- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para várias propriedades[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `cluster.max_shards_per_node`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_dashboards`
- `/_nodes`
- `/_plugins/_asynchronous_search`
- `/_plugins/_alerting`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_plugins/_ppl`
- `/_plugins/_security`
- `/_plugins/_sql`
- `/_percolate`
- `/_rank_eval`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.

4. Refere-se ao método PUT. Para obter informações sobre o método GET, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às OpenSearch operações genéricas que o OpenSearch Serviço suporta e não inclui operações suportadas específicas do plug-in para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

OpenSearch versão 1.1

Para OpenSearch 1.1, o OpenSearch Service oferece suporte às seguintes operações. Para obter informações sobre a maioria das operações, consulte a referência da API OpenSearch REST ou a referência da API para o plug-in específico.

- Todas as operações no caminho do índice (como */index-name* /_forcemerge , */index-name* /update/*id* e */index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (exceto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para várias propriedades[4]:
  - action.auto_create_index
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ppl
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_plugins/_security
- /_plugins/_sql
- /_plugins/_transforms
- /_percolate
- /_rank_eval

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.
4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às OpenSearch operações genéricas que o OpenSearch Serviço suporta e não inclui operações suportadas específicas do plug-in para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

OpenSearch versão 1.0

Para OpenSearch 1.0, o OpenSearch Service oferece suporte às seguintes operações. Para obter informações sobre a maioria das operações, consulte a referência da API OpenSearch REST ou a referência da API para o plug-in específico.

- Todas as operações no caminho do índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (exceto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para várias propriedades[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_plugins/_asynchronous_search`
- `/_plugins/_alerting`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_plugins/_ppl`
- `/_plugins/_security`
- `/_plugins/_sql`
- `/_plugins/_transforms`
- `/_percolate`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- `indices.breaker.total.limit`
- `cluster.max_shards_per_node`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_dashboards`
- `/_rank_eval`

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.
4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às OpenSearch operações genéricas que o OpenSearch Serviço suporta e não inclui operações suportadas específicas do plug-in para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

Elasticsearch versão 7.10

Para o Elasticsearch 7.10, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice (como */index-name* `/_forcemerge` , */index-*
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`

name /update/*id* e /*index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (exceto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para várias propriedades[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_flush
- /_index_template [6]
- /_ingest/pipeline
- /_index_template
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_asynchronous_search
- /_opendistro/_anomaly_detection
- /_opendistro/_ism
- /_opendistro/_ppl
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_plugins/_replication
- /_rank_eval
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template [6]
- /_update_by_query [1]
- /_validate

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.
4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às operações genéricas do Elasticsearch que o OpenSearch Service suporta e não inclui operações suportadas específicas de plug-ins para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.
6. Modelos de índice herdados (`_template`) foram substituídos por modelos que podem ser compostos (`_index_template`) começando com o Elasticsearch 7.8. Os modelos que podem ser compostos têm precedência sobre os modelos legados. Se nenhum modelo que pode ser composto corresponder a um determinado índice, um modelo legado ainda poderá corresponder e ser aplicado. A `_template` operação ainda funciona nas OpenSearch versões posteriores do Elasticsearch OSS, mas as chamadas GET para os dois tipos de modelo retornam resultados diferentes.

Elasticsearch versão 7.9

Para o Elasticsearch 7.9, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_index_template` [6]
- `/_ingest/pipeline`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]

- /_all
- /_analyze
- /_bulk
- /_cat (exceto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para várias propriedades[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_anomaly_detection
- /_opendistro/_ism
- /_opendistro/_ppl
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template [6]
- /_update_by_query [1]
- /_validate

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação /_tasks com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para /_search/scroll com um corpo de mensagem deve especificar "Content-Length" no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho

por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.

3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.
4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às OpenSearch operações genéricas que o OpenSearch Serviço suporta e não inclui operações suportadas específicas do plug-in para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.
6. Modelos de índice herdados (`_template`) foram substituídos por modelos que podem ser compostos (`_index_template`) começando com o Elasticsearch 7.8. Os modelos que podem ser compostos têm precedência sobre os modelos legados. Se nenhum modelo que pode ser composto corresponder a um determinado índice, um modelo legado ainda poderá corresponder e ser aplicado. A `_template` operação ainda funciona nas OpenSearch versões posteriores do Elasticsearch OSS, mas as chamadas GET para os dois tipos de modelo retornam resultados diferentes.

Elasticsearch versão 7.8

Para o Elasticsearch 7.8, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (exceto `/_cat/nodeattrs`)
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_index_template` [6]
- `/_ingest/pipeline`
- `/_ltr`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`

- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para várias propriedades[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `cluster.max_shards_per_node`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_anomaly_detection`
- `/_opendistro/_ism`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template` [6]
- `/_update_by_query` [1]
- `/_validate`

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.
4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às operações genéricas do Elasticsearch que o OpenSearch Service suporta e não inclui operações suportadas específicas de plug-ins para detecção de anomalias, ISM e assim por diante.

5. Consulte the section called “Shrink”.
6. Modelos de índice herdados (`_template`) foram substituídos por modelos que podem ser compostos (`_index_template`) começando com o Elasticsearch 7.8. Os modelos que podem ser compostos têm precedência sobre os modelos legados. Se nenhum modelo que pode ser composto corresponder a um determinado índice, um modelo legado ainda poderá corresponder e ser aplicado. A `_template` operação ainda funciona nas OpenSearch versões posteriores do Elasticsearch OSS, mas as chamadas GET para os dois tipos de modelo retornam resultados diferentes.

Elasticsearch versão 7.7

Para o Elasticsearch 7.7, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* e */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (exceto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para várias propriedades[4]:
  - `action.auto_create_index`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_anomaly_detection`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- `action.search.shard_count.limit`
- `indices.breaker.fielddata.limit`
- `indices.breaker.request.limit`
- `indices.breaker.total.limit`
- `cluster.max_shards_per_node`

- `/_opendistro/_ism`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.
4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às operações genéricas do Elasticsearch que o OpenSearch Service suporta e não inclui operações suportadas específicas de plug-ins para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

Elasticsearch versão 7.4

Para o Elasticsearch 7.4, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice (como */index-nam*
- `/_cluster/state`
- `/_cluster/stats`
- `/_refresh`
- `/_reindex` [1]

e /_forcemerge , /*index-name* /update/*id* e /*index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (exceto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para várias propriedades[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_anomaly_detection
- /_opendistro/_ism
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_render
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação /_tasks com essas operações para verificar se as solicitações foram concluídas com êxito.

2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.
4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às operações genéricas do Elasticsearch que o OpenSearch Service suporta e não inclui operações suportadas específicas de plug-ins para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

Elasticsearch versão 7.1

Para o Elasticsearch 7.1, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice (como */index-name* `/_forcemerge` e */index-name* `/update/`*id*) exceto */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (exceto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`

- `/_cluster/settings` para várias propriedades[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `cluster.max_shards_per_node`
- `/_opendistro/_ism`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_update_by_query` [1]
- `/_validate`

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.
4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às operações genéricas do Elasticsearch que o OpenSearch Service suporta e não inclui operações suportadas específicas de plug-ins para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

Elasticsearch versão 6.8

Para o Elasticsearch 6.8, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice (como */index-name* `/_forcemerge` e */index-name* `/update/`*id*) exceto */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (exceto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para várias propriedades[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query`[1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_ism`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_refresh`
- `/_reindex`[1]
- `/_render`
- `/_rollover`
- `/_scripts`[3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query`[1]
- `/_validate`

- `cluster.max_shards_per_node`
- `cluster.blocks.read_only`

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.
4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às operações genéricas do Elasticsearch que o OpenSearch Service suporta e não inclui operações suportadas específicas de plug-ins para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

Elasticsearch versão 6.7

Para o Elasticsearch 6.7, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice (como */index-name* `/_forcemerge` e */index-name* `/update/`*id*) exceto */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`

- `/_analyze`
- `/_bulk`
- `/_cat` (exceto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para várias propriedades[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `cluster.max_shards_per_node`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.

4. Refere-se ao método PUT. Para obter informações sobre o método GET, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às operações genéricas do Elasticsearch que o OpenSearch Service suporta e não inclui operações suportadas específicas de plug-ins para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

Elasticsearch versão 6.5

Para o Elasticsearch 6.5, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice (como */index-name* */_forcemerge* e */index-name* */update/id*) exceto */index-name* */_close*
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (exceto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para várias propriedades[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_refresh
- /_reindex [1]
- /_render
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

- indices.breaker.fielddata.limit
- indices.breaker.request.limit
- indices.breaker.total.limit

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.
4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às operações genéricas do Elasticsearch que o OpenSearch Service suporta e não inclui operações suportadas específicas de plug-ins para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

Elasticsearch versão 6.4

Para o Elasticsearch 6.4, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice (como */index-name* `/_forcemerge` e */index-name* `/update/`*id*) exceto */index-name* `/_close`
- `/_alias`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search` [2]

- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (exceto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para várias propriedades[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.

4. Refere-se ao método PUT. Para obter informações sobre o método GET, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às operações genéricas do Elasticsearch que o OpenSearch Service suporta e não inclui operações suportadas específicas de plug-ins para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

Elasticsearch versão 6.3

Para o Elasticsearch 6.3, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice (como */index-name* */_forcemerge* e */index-name* */update/id*) exceto */index-name* */_close*
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (exceto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para várias propriedades[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_refresh
- /_reindex [1]
- /_render
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

- `indices.breaker.fielddata.limit`
- `indices.breaker.request.limit`
- `indices.breaker.total.limit`

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.
4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às operações genéricas do Elasticsearch que o OpenSearch Service suporta e não inclui operações suportadas específicas de plug-ins para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

Elasticsearch versão 6.2

Para o Elasticsearch 6.2, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice (como */index-name* `/_forcemerge` e */index-name* `/update/`*id*) exceto */index-name* `/_close`
- `/_alias`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search` [2]

- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (exceto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para várias propriedades[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.

4. Refere-se ao método PUT. Para obter informações sobre o método GET, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às operações genéricas do Elasticsearch que o OpenSearch Service suporta e não inclui operações suportadas específicas de plug-ins para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

Elasticsearch versão 6.0

Para o Elasticsearch 6.0, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice (como */index-name* */_forcemerge* e */index-name* */update/id*) exceto */index-name* */_close*
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (exceto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para várias propriedades[4]:
  - action.auto_create_index
  - action.search.shard_count.limit
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_percolate
- /_plugin/kibana
- /_refresh
- /_reindex [1]
- /_render
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

- `indices.breaker.fielddata.limit`
- `indices.breaker.request.limit`
- `indices.breaker.total.limit`

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.
4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às operações genéricas do Elasticsearch que o OpenSearch Service suporta e não inclui operações suportadas específicas de plug-ins para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

Elasticsearch versão 5.6

Para o Elasticsearch 5.6, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice (como */index-name* `/_forcemerge` e */index-name* `/update/`*id*) exceto */index-name* `/_close`
- `/_alias`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search` [2]
- `/_search profile`
- `/_shard_stores`

- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (exceto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para várias propriedades[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_refresh`
- `/_reindex` [1]
- `/_shrink`[5]
- `/_snapshot`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.

4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às operações genéricas do Elasticsearch que o OpenSearch Service suporta e não inclui operações suportadas específicas de plug-ins para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

Elasticsearch versão 5.5

Para o Elasticsearch 5.5, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice (como */index-name* `/_forcemerge` e */index-name* `/update/`*id*) exceto */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (exceto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para várias propriedades[4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- `indices.breaker.fielddata.limit`
- `indices.breaker.request.limit`
- `indices.breaker.total.limit`

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Para saber as considerações sobre o uso de scripts, consulte the section called “Outros recursos compatíveis”.
4. Refere-se ao método `PUT`. Para obter informações sobre o método `GET`, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às operações genéricas do Elasticsearch que o OpenSearch Service suporta e não inclui operações suportadas específicas de plug-ins para detecção de anomalias, ISM e assim por diante.
5. Consulte the section called “Shrink”.

Elasticsearch versão 5.3

Para o Elasticsearch 5.3, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice (como */index-name* `/_forcemerge` e */index-name* `/update/`*id*) exceto */index-name* `/_close`
- `/_alias`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_render`
- `/_rollover`
- `/_search` [2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink` [4]

- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (exceto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para várias propriedades[3]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_percolate
- /_plugin/kibana
- /_refresh
- /_reindex [1]
- /_snapshot
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação /_tasks com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para /_search/scroll com um corpo de mensagem deve especificar "Content-Length" no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em scroll_id valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar scroll_id valores para o OpenSearch Serviço.
3. Refere-se ao método PUT. Para obter informações sobre o método GET, consulte the section called “Diferenças notáveis de API”. Essa lista se refere apenas às operações genéricas do

Elasticsearch que o OpenSearch Service suporta e não inclui operações suportadas específicas de plug-ins para detecção de anomalias, ISM e assim por diante.

4. Consulte the section called “Shrink”.

Elasticsearch versão 5.1

Para o Elasticsearch 5.1, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice (como */index-name* */_forcemerge* e */index-name* */update/id*) exceto */index-name* */_close*
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (exceto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para várias propriedades (somente PUT):
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_search` [2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink` [3]
- `/_snapshot`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- `indices.breaker.request.limit`
- `indices.breaker.total.limit`

1. Essas operações podem ser interrompidas por alterações na configuração de cluster. É recomendável usar a operação `/_tasks` com essas operações para verificar se as solicitações foram concluídas com êxito.
2. Solicitações de DELETE para `/_search/scroll` com um corpo de mensagem deve especificar `"Content-Length"` no cabeçalho HTTP. A maioria dos clientes adicionam esse cabeçalho por padrão. Para evitar problemas com = caracteres em `scroll_id` valores, use o corpo da solicitação, não a cadeia de caracteres de consulta, para passar `scroll_id` valores para o OpenSearch Serviço.
3. Consulte the section called “Shrink”.

Elasticsearch versão 2.3

Para o Elasticsearch 2.3, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice (como `/index-name /_forcemerge` e `/index-name /_recovery`) exceto `/index-name /_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cache/clear` (somente Índice)
- `/_cat` (exceto `/_cat/nodeattrs`)
- `/_cluster/health`
- `/_cluster/settings` para várias propriedades (somente PUT):
- `/_cluster/stats`
- `/_count`
- `/_flush`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_refresh`
- `/_render`
- `/_search`
- `/_snapshot`

  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `threadpool.get.queue_size`
  - `threadpool.bulk.queue_size`
  - `threadpool.index.queue_size`
  - `threadpool.percolate.queue_size`
  - `threadpool.search.queue_size`
  - `threadpool.suggest.queue_size`
- `/_stats`
- `/_status`
- `/_template`

Elasticsearch versão 1.5

Para o Elasticsearch 1.5, o OpenSearch Service oferece suporte às seguintes operações.

- Todas as operações no caminho do índice, como */index-name* `/_optimize` e */index-name* `/_warmer`, exceto */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat`
- `/_cluster/health`
- `/_cluster/settings` para várias propriedades (somente PUT):
  - `indices.breaker.fielddata.limit`
- `/_cluster/stats`
- `/_count`
- `/_flush`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_plugin/kibana3`
- `/_plugin/migration`
- `/_refresh`
- `/_search`
- `/_snapshot`
- `/_stats`

- indices.breaker.request.limit
- indices.breaker.total.limit
- threadpool.get.queue_size
- threadpool.bulk.queue_size
- threadpool.index.queue_size
- threadpool.percolate.queue_size
- threadpool.search.queue_size
- threadpool.suggest.queue_size
- /_status
- /_template

Cotas OpenSearch do Amazon Service

Sua AWS conta tem cotas padrão, anteriormente chamadas de limites, para cada AWS serviço. A menos que especificado de outra forma, cada cota é específica da região .

Para ver as cotas para domínios e instâncias do OpenSearch Serviço, Amazon OpenSearch Serverless e Amazon OpenSearch Ingestion, consulte as cotas do OpenSearch Amazon Service no. Referência geral da AWS

Para ver as cotas de OpenSearch serviço no AWS Management Console, abra o console Service Quotas. No painel de navegação, escolha AWS serviços e selecione Amazon OpenSearch Service. Para solicitar um aumento da cota, consulte Requesting a quota increase no Guia do usuário do Service Quotas.

Tópicos

- UltraWarm cotas de armazenamento
- Limites de tamanhos de volume do EBS
- Limites de rede
- Cotas de tamanhos de fragmentos
- Limites dos processos Java
- Limites das políticas de domínio

UltraWarm cotas de armazenamento

A tabela a seguir lista os tipos de UltraWarm instância e a quantidade máxima de armazenamento que cada tipo pode usar. Para obter mais informações sobre UltraWarm, consultethe section called "UltraWarm armazenamento".

Tipo de instância	Armazenamento máximo
`ultrawarm1.medium.search`	1,5 TiB
`ultrawarm1.large.search`	20 TiB

Limites de tamanhos de volume do EBS

A tabela a seguir mostra os tamanhos mínimo e máximo dos volumes do EBS para cada tipo de instância compatível com o OpenSearch Service. Para obter informações sobre quais tipos de instância incluem armazenamento de instâncias e detalhes adicionais de hardware, consulte os preços do Amazon OpenSearch Service.

- Se você escolher o armazenamento magnético em Tipo de volume do EBS ao criar seu domínio, o tamanho máximo do volume será de 100 GiB para todos os tipos de instância, exceto `t2.small` e `t2.medium`, e todas as instâncias Graviton (M6g, C6g, R6g e R6gd), que não são compatíveis com armazenamento magnético. Para os tamanhos máximos listados na tabela a seguir, escolha uma das opções de SSD.
- Alguns tipos de instância de gerações anteriores incluem o armazenamento de instâncias, mas também oferecem suporte ao armazenamento do EBS. Se você escolher o armazenamento do EBS para um desses tipos de instância, os volumes de armazenamento não serão aditivos. Você pode usar um volume do EBS ou o armazenamento de instâncias, mas não ambos.

Tipo de instância	Tamanho mínimo do EBS	Tamanho máximo do EBS (gp2)	Tamanho máximo do EBS (gp3)
`t2.micro.search`	10 GiB	35 GiB	N/D
`t2.small.search`	10 GiB	35 GiB	N/D

Tipo de instância	Tamanho mínimo do EBS	Tamanho máximo do EBS (gp2)	Tamanho máximo do EBS (gp3)
t2.medium.search	10 GiB	35 GiB	N/D
t3.small.search	10 GiB	100 GiB	100 GiB
t3.medium.search	10 GiB	200 GiB	200 GiB
m3.medium.search	10 GiB	100 GiB	N/D
m3.large.search	10 GiB	512 GiB	N/D
m3.xlarge.search	10 GiB	512 GiB	N/D
m3.2xlarge.search	10 GiB	512 GiB	N/D
m4.large.search	10 GiB	512 GiB	N/D
m4.xlarge.search	10 GiB	1 TiB	N/D
m4.2xlarge.search	10 GiB	1,5 TiB	N/D
m4.4xlarge.search	10 GiB	1,5 TiB	N/D
m4.10xlarge.search	10 GiB	1,5 TiB	N/D
m5.large.search	10 GiB	512 GiB	1 TiB
m5.xlarge.search	10 GiB	1 TiB	2 TiB
m5.2xlarge.search	10 GiB	1,5 TiB	3 TiB
m5.4xlarge.search	10 GiB	3 TiB	6 TiB
m5.12xlarge.search	10 GiB	9 TiB	18 TiB
m6g.large.search	10 GiB	512 GiB	1 TiB
m6g.xlarge.search	10 GiB	1 TiB	2 TiB

Tipo de instância	Tamanho mínimo do EBS	Tamanho máximo do EBS (gp2)	Tamanho máximo do EBS (gp3)
m6g.2xlarge.search	10 GiB	1,5 TiB	3 TiB
m6g.4xlarge.search	10 GiB	3 TiB	6 TiB
m6g.8xlarge.search	10 GiB	6 TiB	12 TiB
m6g.12xlarge.search	10 GiB	9 TiB	18 TiB
c4.large.search	10 GiB	100 GiB	N/D
c4.xlarge.search	10 GiB	512 GiB	N/D
c4.2xlarge.search	10 GiB	1 TiB	N/D
c4.4xlarge.search	10 GiB	1,5 TiB	N/D
c4.8xlarge.search	10 GiB	1,5 TiB	N/D
c5.large.search	10 GiB	256 GiB	256 GiB
c5.xlarge.search	10 GiB	512 GiB	512 GiB
c5.2xlarge.search	10 GiB	1 TiB	1 TiB
c5.4xlarge.search	10 GiB	1,5 TiB	1,5 TiB
c5.9xlarge.search	10 GiB	3,5 TiB	3,5 TiB
c5.18xlarge.search	10 GiB	7 TiB	7 TiB
c6g.large.search	10 GiB	256 GiB	256 GiB
c6g.xlarge.search	10 GiB	512 GiB	512 GiB
c6g.2xlarge.search	10 GiB	1 TiB	1 TiB
c6g.4xlarge.search	10 GiB	1,5 TiB	1,5 TiB

Tipo de instância	Tamanho mínimo do EBS	Tamanho máximo do EBS (gp2)	Tamanho máximo do EBS (gp3)
c6g.8xlarge.search	10 GiB	3 TiB	3 TiB
c6g.12xlarge.search	10 GiB	4,5 TiB	4,5 TiB
r3.large.search	10 GiB	512 GiB	N/D
r3.xlarge.search	10 GiB	512 GiB	N/D
r3.2xlarge.search	10 GiB	512 GiB	N/D
r3.4xlarge.search	10 GiB	512 GiB	N/D
r3.8xlarge.search	10 GiB	512 GiB	N/D
r4.large.search	10 GiB	1 TiB	N/D
r4.xlarge.search	10 GiB	1,5 TiB	N/D
r4.2xlarge.search	10 GiB	1,5 TiB	N/D
r4.4xlarge.search	10 GiB	1,5 TiB	N/D
r4.8xlarge.search	10 GiB	1,5 TiB	N/D
r4.16xlarge.search	10 GiB	1,5 TiB	N/D
r5.large.search	10 GiB	1 TiB	2 TiB
r5.xlarge.search	10 GiB	1,5 TiB	3 TiB
r5.2xlarge.search	10 GiB	3 TiB	6 TiB
r5.4xlarge.search	10 GiB	6 TiB	12 TiB
r5.12xlarge.search	10 GiB	12 TiB	24 TiB
r6g.large.search	10 GiB	1 TiB	2 TiB

Tipo de instância	Tamanho mínimo do EBS	Tamanho máximo do EBS (gp2)	Tamanho máximo do EBS (gp3)
r6g.xlarge.search	10 GiB	1,5 TiB	3 TiB
r6g.2xlarge.search	10 GiB	3 TiB	6 TiB
r6g.4xlarge.search	10 GiB	6 TiB	12 TiB
r6g.8xlarge.search	10 GiB	8 TiB	16 TiB
r6g.12xlarge.search	10 GiB	12 TiB	24 TiB
r6gd.large.search	N/D	N/D	N/D
r6gd.xlarge.search	N/D	N/D	N/D
r6gd.2xlarge.search	N/D	N/D	N/D
r6gd.4xlarge.search	N/D	N/D	N/D
r6gd.8xlarge.search	N/D	N/D	N/D
r6gd.12xlarge.search	N/D	N/D	N/D
r6gd.16xlarge.search	N/D	N/D	N/D
i2.xlarge.search	10 GiB	512 GiB	N/D
i2.2xlarge.search	10 GiB	512 GiB	N/D
i3.large.search	N/D	N/D	N/D
i3.xlarge.search	N/D	N/D	N/D
i3.2xlarge.search	N/D	N/D	N/D
i3.4xlarge.search	N/D	N/D	N/D
i3.8xlarge.search	N/D	N/D	N/D

Tipo de instância	Tamanho mínimo do EBS	Tamanho máximo do EBS (gp2)	Tamanho máximo do EBS (gp3)
i3.16xlarge.search	N/D	N/D	N/D
or1.medium.search	20 GiB	N/D	768 GiB
or1.large.search	20 GiB	N/D	1532 GiB
or1.xlarge.search	20 GiB	N/D	3 TiB
or1.2xlarge.search	20 GiB	N/D	6 TiB
or1.4xlarge.search	20 GiB	N/D	12 TiB
or1.8xlarge.search	20 GiB	N/D	16 TiB
or1.12xlarge.search	20 GiB	N/D	24 TiB
or1.16xlarge.search	20 GiB	N/D	36 TiB
im4gn.large.search	N/D	N/D	N/D
im4gn.xlarge.search	N/D	N/D	N/D
im4gn.2xlarge.search	N/D	N/D	N/D
im4gn.4xlarge.search	N/D	N/D	N/D
im4gn.8xlarge.search	N/D	N/D	N/D
im4gn.16xlarge.search	N/D	N/D	N/D

Limites de rede

A tabela a seguir mostra o tamanho máximo de cargas de solicitação HTTP.

Tipo de instância	Tamanho máximo das cargas úteis das solicitações HTTP
t2.micro.search	10 MiB
t2.small.search	10 MiB
t2.medium.search	10 MiB
t3.small.search	10 MiB
t3.medium.search	10 MiB
m3.medium.search	10 MiB
m3.large.search	10 MiB
m3.xlarge.search	100 MiB
m3.2xlarge.search	100 MiB
m4.large.search	10 MiB
m4.xlarge.search	100 MiB
m4.2xlarge.search	100 MiB
m4.4xlarge.search	100 MiB
m4.10xlarge.search	100 MiB
m5.large.search	10 MiB
m5.xlarge.search	100 MiB
m5.2xlarge.search	100 MiB
m5.4xlarge.search	100 MiB
m5.12xlarge.search	100 MiB

Tipo de instância	Tamanho máximo das cargas úteis das solicitações HTTP
m6g.large.search	10 MiB
m6g.xlarge.search	100 MiB
m6g.2xlarge.search	100 MiB
m6g.4xlarge.search	100 MiB
m6g.8xlarge.search	100 MiB
m6g.12xlarge.search	100 MiB
c4.large.search	10 MiB
c4.xlarge.search	100 MiB
c4.2xlarge.search	100 MiB
c4.4xlarge.search	100 MiB
c4.8xlarge.search	100 MiB
c5.large.search	10 MiB
c5.xlarge.search	100 MiB
c5.2xlarge.search	100 MiB
c5.4xlarge.search	100 MiB
c5.9xlarge.search	100 MiB
c5.18xlarge.search	100 MiB

Tipo de instância	Tamanho máximo das cargas úteis das solicitações HTTP
c6g.large.search	10 MiB
c6g.xlarge.search	100 MiB
c6g.2xlarge.search	100 MiB
c6g.4xlarge.search	100 MiB
c6g.8xlarge.search	100 MiB
c6g.12xlarge.search	100 MiB
r3.large.search	10 MiB
r3.xlarge.search	100 MiB
r3.2xlarge.search	100 MiB
r3.4xlarge.search	100 MiB
r3.8xlarge.search	100 MiB
r4.large.search	100 MiB
r4.xlarge.search	100 MiB
r4.2xlarge.search	100 MiB
r4.4xlarge.search	100 MiB
r4.8xlarge.search	100 MiB
r4.16xlarge.search	100 MiB

Tipo de instância	Tamanho máximo das cargas úteis das solicitações HTTP
r5.large.search	100 MiB
r5.xlarge.search	100 MiB
r5.2xlarge.search	100 MiB
r5.4xlarge.search	100 MiB
r5.12xlarge.search	100 MiB
r6g.large.search	100 MiB
r6g.xlarge.search	100 MiB
r6g.2xlarge.search	100 MiB
r6g.4xlarge.search	100 MiB
r6g.8xlarge.search	100 MiB
r6g.12xlarge.search	100 MiB
r6gd.large.search	100 MiB
r6gd.xlarge.search	100 MiB
r6gd.2xlarge.search	100 MiB
r6gd.4xlarge.search	100 MiB

Tipo de instância	Tamanho máximo das cargas úteis das solicitações HTTP
r6gd.8xlarge.search	100 MiB
r6gd.12xlarge.search	100 MiB
r6gd.16xlarge.search	100 MiB
i2.xlarge.search	100 MiB
i2.2xlarge.search	100 MiB
i3.large.search	100 MiB
i3.xlarge.search	100 MiB
i3.2xlarge.search	100 MiB
i3.4xlarge.search	100 MiB
i3.8xlarge.search	100 MiB
i3.16xlarge.search	100 MiB
or1.medium.search	10 MiB
or1.large.search	100 MiB
or1.xlarge.search	100 MiB
or1.2xlarge.search	100 MiB
or1.4xlarge.search	100 MiB

Tipo de instância	Tamanho máximo das cargas úteis das solicitações HTTP
or1.8xlarge.search	100 MiB
or1.12xlarge.search	100 MiB
or1.16xlarge.search	100 MiB
im4gn.large.search	100 MiB
im4gn.xlarge.search	100 MiB
im4gn.2xlarge.search	100 MiB
im4gn.4xlarge.search	100 MiB
im4gn.8xlarge.search	100 MiB
im4gn.16xlarge.search	100 MiB

Cotas de tamanhos de fragmentos

A seção a seguir lista os tamanhos máximos dos fragmentos para várias famílias de instâncias.

Tipo de instância	Multi-AZ sem modo de espera	Multi-AZ com modo de espera
R5, C5, M5	N/D	65 GiB
I3	N/D	65 GiB

Tipo de instância	Multi-AZ sem modo de espera	Multi-AZ com modo de espera
R6g, C6g, M6g, R6gd	N/D	65 GiB
OR1	100 GiB	65 GiB
Im4gn	N/D	65 GiB

Para solicitar um aumento na cota, entre em contato com o AWS Support.

Limites dos processos Java

OpenSearch O serviço limita os processos Java a um tamanho de pilha de 32 GiB. Os usuários avançados podem especificar a porcentagem do heap usado para dados de campo. Para ter mais informações, consulte the section called “Configurações avançadas do cluster” e the section called “OutOfMemoryError em JVM”.

Limites das políticas de domínio

OpenSearch O serviço limita as políticas de acesso em domínios a 100 KiB.

Instâncias reservadas no Amazon OpenSearch Service

As instâncias reservadas do Amazon OpenSearch Service oferecem descontos significativos em comparação com as instâncias sob demanda padrão. As instâncias propriamente ditas são idênticas; as RIs são apenas um desconto de faturamento aplicado a instâncias sob demanda na conta. Para aplicativos de longa duração com uso previsível, as RIs podem oferecer uma economia considerável ao longo do tempo.

As instâncias reservadas do OpenSearch Service exigem termos de um ou três anos e oferecem três opções de pagamento que afetam a taxa de desconto:

- Sem pagamento adiantado: você não paga adiantado. Você paga uma taxa por hora com desconto a cada hora dentro do prazo.
- Adiantamento parcial: você paga uma parte do custo inicial e paga uma taxa por hora com desconto para cada hora dentro do termo.
- Adiantamento total: você paga todos os custos iniciais. Você não paga uma taxa por hora no prazo.

De modo geral, um maior pagamento adiantado significa um desconto maior. Você não pode cancelar instâncias reservadas: ao reservá-las, você se compromete em pagar pelo termo completo, e os pagamentos adiantados não são reembolsáveis.

As instâncias reservadas não são flexíveis; elas se aplicam apenas ao tipo exato de instância que você reserva. Por exemplo, uma reserva para oito instâncias `c5.2xlarge.search` não se aplica a dezesseis instâncias `c5.xlarge.search` ou quatro instâncias `c5.4xlarge.search`. Para obter informações detalhadas sobre preços, consulte Preços do Amazon OpenSearch Service e as Perguntas frequentes.

Tópicos

Compra de instâncias reservadas (console)

O console permite que você exiba as instâncias reservadas existentes e compre novas.

Para comprar uma reserva

1. Vá para https://aws.amazon.com e escolha Sign In to the Console (Fazer login no console)
2. Em Analytics (Análise), escolha Amazon OpenSearch Service.
3. Escolha Reserved Instanace Leases (Locações de instância reservada) no painel de navegação.

   Nesta página, você pode exibir as reservas existentes. Se tiver muitas reservas, você poderá filtrá-las para identificar mais facilmente e exibir uma determinada reserva.

   > **Tip**
   >
   > Se você não encontrar o link Reserved Instance Leases (Locações de instância reservada), crie um domínio na Região da AWS.

4. Escolha Order Reserved Instance (Encomendar instância reservada).
5. Forneça um nome exclusivo e descritivo.

6. Escolha um tipo de instância e o número de instâncias. Para obter orientações, consulte the section called “Dimensionamento de domínios”.
7. Escolha um prazo e uma opção de pagamento. Examine os detalhes de pagamento atentamente.
8. Escolha Next (Próximo).
9. Examine o resumo da compra com atenção. As compras de instâncias reservadas não são reembolsáveis.
10. Escolha Order (Solicitar).

Compra de instâncias reservadas (AWS CLI)

A AWS CLI tem comandos para exibir ofertas, comprar uma reserva e exibir as reservas. O comando e a resposta de exemplo a seguir mostram as ofertas para uma determinada Região da AWS:

```
aws opensearch describe-reserved-instance-offerings --region us-east-1
{
  "ReservedInstanceOfferings": [
    {
      "FixedPrice": x,
      "ReservedInstanceOfferingId": "1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a",
      "RecurringCharges": [
        {
          "RecurringChargeAmount": y,
          "RecurringChargeFrequency": "Hourly"
        }
      ],
      "UsagePrice": 0.0,
      "PaymentOption": "PARTIAL_UPFRONT",
      "Duration": 31536000,
      "InstanceType": "m4.2xlarge.search",
      "CurrencyCode": "USD"
    }
  ]
}
```

Para obter uma explicação de cada valor de retorno, consulte a tabela a seguir.

Campo	Descrição
`FixedPrice`	O custo inicial da reserva.
`ReservedInstanceOfferingId`	O ID da oferta. Anote esse valor caso você queira reservar a oferta.
`RecurringCharges`	A taxa por hora da reserva.
`UsagePrice`	Um campo herdado. Em OpenSearch Service, esse valor é sempre 0.
`PaymentOption`	Sem adiantamento, adiantamento parcial ou adiantamento total.
`Duration`	Extensão do prazo em segundos: • 31.536.000 segundos são um ano. • 94.608.000 segundos são três anos.
`InstanceType`	O tipo de instância da reserva. Para obter informações sobre os recursos de hardware que são alocados para cada tipo de instância , consulte Preços do Amazon OpenSearch Service.
`CurrencyCode`	A moeda de `FixedPrice` e `RecurringChargeAmount` .

Este próximo exemplo compra uma reserva:

```
aws opensearch purchase-reserved-instance-offering --reserved-instance-offering-
id 1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a --reservation-name my-reservation --instance-
count 3 --region us-east-1
{
  "ReservationName": "my-reservation",
  "ReservedInstanceId": "9a8a7a6a-5a4a-3a2a-1a0a-9a8a7a6a5a4a"
}
```

Por fim, você pode listar as reservas para uma determinada Região usando o seguinte exemplo:

```
aws opensearch describe-reserved-instances --region us-east-1
{
  "ReservedInstances": [
    {
      "FixedPrice": x,
      "ReservedInstanceOfferingId": "1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a",
      "ReservationName": "my-reservation",
      "PaymentOption": "PARTIAL_UPFRONT",
      "UsagePrice": 0.0,
      "ReservedInstanceId": "9a8a7a6a-5a4a-3a2a-1a0a-9a8a7a6a5a4a",
      "RecurringCharges": [
        {
          "RecurringChargeAmount": y,
          "RecurringChargeFrequency": "Hourly"
        }
      ],
      "State": "payment-pending",
      "StartTime": 1522872571.229,
      "InstanceCount": 3,
      "Duration": 31536000,
      "InstanceType": "m4.2xlarge.search",
      "CurrencyCode": "USD"
    }
  ]
}
```

> **Note**
>
> `StartTime` é tempo epoch Unix, que é o número de segundos decorridos desde a meia-noite UTC de 1° de janeiro de 1970. Por exemplo, o tempo epoch 1522872571 20:09:31 UTC é de 4 de abril de 2018. Você pode usar conversores online.

Para saber mais sobre os comandos usados nos exemplos anteriores, consulte a Referência de comandos da AWS CLI.

Compra de instâncias reservadas (AWS SDKs)

Os SDKs da AWS (exceto os SDKs para Android e iOS) são compatíveis com todas as operações definidas na Amazon OpenSearch Service API Reference (Referência da API do Amazon OpenSearch Service), inclusive as seguintes:

- `DescribeReservedInstanceOfferings`
- `PurchaseReservedInstanceOffering`
- `DescribeReservedInstances`

Este script de exemplo usa o cliente Python OpenSearchService de baixo nível do AWS SDK for Python (Boto3) para comprar instâncias reservadas. Você deve fornecer um valor para `instance_type`:

```
import boto3
from botocore.config import Config

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a region other than your default.
    region_name='us-east-1'
)

client = boto3.client('opensearch', config=my_config)

instance_type = '' # e.g. m4.2xlarge.search


def describe_RI_offerings(client):
    """Gets the Reserved Instance offerings for this account"""

    response = client.describe_reserved_instance_offerings()
    offerings = (response['ReservedInstanceOfferings'])
    return offerings


def check_instance(offering):
    """Returns True if instance type is the one you specified above"""
```

```
    if offering['InstanceType'] == instance_type:
        return True

    return False


def get_instance_id():
    """Iterates through the available offerings to find the ID of the one you
 specified"""

    instance_type_iterator = filter(
        check_instance, describe_RI_offerings(client))
    offering = list(instance_type_iterator)
    id = offering[0]['ReservedInstanceOfferingId']
    return id


def purchase_RI_offering(client):
    """Purchase Reserved Instances"""

    response = client.purchase_reserved_instance_offering(
        ReservedInstanceOfferingId = get_instance_id(),
        ReservationName = 'my-reservation',
        InstanceCount = 1
    )
    print('Purchased reserved instance offering of type ' + instance_type)
    print(response)


def main():
    """Purchase Reserved Instances"""
    purchase_RI_offering(client)
```

Para obter mais informações sobre instalação e uso dos AWS SDKs, consulte Kits de desenvolvimento de software da AWS.

Verificação dos custos

Cost Explorer é uma ferramenta gratuita que você pode usar para exibir os dados de gastos nos últimos 13 meses. Analisar esses dados ajuda a identificar tendências e compreender se RIs se ajustam ao caso de uso. Se já tiver RIs, você poderá agrupar por Purchase Option (Opção de compra) e mostrar custos amortizados para comparar esse gasto com o gasto das instâncias sob

demanda. Você também pode definir orçamentos de uso para garantir que está aproveitando suas reservas. Para obter mais informações, consulte Análise dos custos com o Cost Explorer no Manual do usuário do AWS Billing.

Outros recursos suportados no Amazon OpenSearch Service

Este tópico descreve recursos adicionais aos quais o Amazon OpenSearch Service oferece suporte.

bootstrap.memory_lock

OpenSearch O serviço é `bootstrap.memory_lock` ativado`opensearch.yml`, o que bloqueia a memória JVM e impede que o sistema operacional a troque por disco. Isso se aplica a todos os tipos de instância compatíveis, exceto os seguintes:

- `t2.micro.search`
- `t2.small.search`
- `t2.medium.search`
- `t3.small.search`
- `t3.medium.search`

Módulo de scripting

OpenSearch O serviço oferece suporte a scripts para o Elasticsearch 5. domínios x e posteriores. Esse serviço não oferece suporte ao desenvolvimento de scripts para as versões 1.5 ou 2.3.

As opções de script compatíveis incluem as seguintes:

- Painless
- Lucene Expressions
- Mustache

Para domínios do Elasticsearch 5.5 e versões posteriores, e para todos os OpenSearch domínios, o OpenSearch Service oferece suporte a scripts armazenados usando o endpoint. `_scripts` Os domínios do Elasticsearch 5.3 e 5.1 oferecem suporte somente a scripts em linha.

Transporte com TLS

OpenSearch O serviço oferece suporte a HTTP na porta 80 e HTTPS pela porta 443, mas não oferece suporte ao transporte TLS.

Tutoriais do Amazon OpenSearch Service

Este capítulo inclui vários tutoriais completos para trabalhar com o Amazon OpenSearch Service, incluindo como migrar para o serviço, criar uma aplicação de pesquisa simples e criar uma visualização no OpenSearch Dashboards.

Tópicos

Tutorial: Criar e pesquisar documentos no Amazon OpenSearch Service

Neste tutorial, você aprenderá a criar e pesquisar um documento no Amazon OpenSearch Service. Você adiciona dados a um índice na forma de um documento JSON. O OpenSearch Service cria um índice em torno do primeiro documento que você adiciona.

Este tutorial explica como fazer solicitações HTTP para criar documentos, gerar automaticamente um ID para um documento e realizar pesquisas básicas e avançadas em seus documentos.

> **Note**
>
> Este tutorial usa um domínio com acesso aberto. Para obter o mais alto nível de segurança, recomendamos colocar o domínio em uma nuvem privada virtual (VPC).

Pré-requisitos

Este tutorial tem os seguintes pré-requisitos:

- É necessário ter uma Conta da AWS.
- É necessário ter um domínio ativo do OpenSearch Service.

Adicionar um documento a um índice

Para adicionar um documento a um índice, é possível usar qualquer ferramenta HTTP, como oPostman, o cURL ou o console do OpenSearch Dashboards. Esses exemplos supõem que você está usando o console do desenvolvedor no OpenSearch Dashboards. Se você estiver usando uma ferramenta diferente, ajuste adequadamente fornecendo o URL completo e as credenciais, se necessário.

Para adicionar um documento a um índice

1. Acesse o URL do OpenSearch Dashboards para seu domínio. O URL está disponível no painel do domínio no console do OpenSearch Service. O URL segue este formato:

   ```
   domain-endpoint/_dashboards/
   ```

2. Entre usando o nome de usuário principal e a senha.
3. Abra o painel de navegação esquerdo e escolha Ferramentas de desenvolvimento.
4. O verbo HTTP para criar um novo recurso é PUT. É ele que deve ser usado para criar um novo documento e um índice. Insira o seguinte comando no console:

   ```
   PUT fruit/_doc/1
   {
     "name":"strawberry",
     "color":"red"
   }
   ```

   A solicitação PUT cria um índice chamado fruit e adiciona um único documento ao índice com um ID de 1. Ele produz a seguinte resposta:

   ```
   {
     "_index" : "fruit",
     "_type" : "_doc",
     "_id" : "1",
     "_version" : 1,
     "result" : "created",
     "_shards" : {
       "total" : 2,
       "successful" : 2,
       "failed" : 0
     },
   ```

```
  "_seq_no" : 0,
  "_primary_term" : 1
}
```

Criar IDs gerados automaticamente

O OpenSearch Service pode gerar automaticamente um ID para seus documentos. O comando de geração de IDs usa uma solicitação POST em vez de uma solicitação PUT e não requer nenhum ID de documento (em comparação com a solicitação anterior).

Insira a seguinte solicitação no console do desenvolvedor:

```
POST veggies/_doc
{
  "name":"beet",
  "color":"red",
  "classification":"root"
}
```

Essa solicitação cria um índice chamado veggies e adiciona o documento ao índice. Ele produz a seguinte resposta:

```
{
  "_index" : "veggies",
  "_type" : "_doc",
  "_id" : "3WgyS4IB5DLqbRIvLxtF",
  "_version" : 1,
  "result" : "created",
  "_shards" : {
    "total" : 2,
    "successful" : 2,
    "failed" : 0
  },
  "_seq_no" : 0,
  "_primary_term" : 1
}
```

Observe o campo `_id` adicional na resposta, que indica que um ID foi criado automaticamente.

> **Note**
>
> Você não acrescenta nada depois de `_doc` no URL, onde o ID normalmente é adicionado. Como está criando um documento com um ID gerado, você ainda não fornece um. Isso está reservado para atualizações.

Atualizar um documento com um comando POST

Para atualizar um documento, use um comando HTTP `POST` com o número do ID.

Primeiro, crie um documento com ID `42`:

```
POST fruits/_doc/42
{
  "name":"banana",
  "color":"yellow"
}
```

Em seguida, use esse ID para atualizar o documento:

```
POST fruits/_doc/42
{
  "name":"banana",
  "color":"yellow",
  "classification":"berries"
}
```

Esse comando atualiza o documento com o novo campo `classification`. Ele produz a seguinte resposta:

```
{
  "_index" : "fruits",
  "_type" : "_doc",
  "_id" : "42",
  "_version" : 2,
  "result" : "updated",
  "_shards" : {
    "total" : 2,
    "successful" : 2,
    "failed" : 0
```

```
  },
  "_seq_no" : 1,
  "_primary_term" : 1
}
```

> **Note**
>
> Se você tentar atualizar um documento que não existe, o OpenSearch Service criará o documento.

Executar ações em massa

Você pode usar a operação da API `POST _bulk` para executar várias ações em um ou mais índices em uma solicitação. Os comandos de ação em massa têm o seguinte formato:

```
POST /_bulk
<action_meta>\n
<action_data>\n
<action_meta>\n
<action_data>\n
```

Cada ação requer duas linhas de JSON. Primeiro, é necessário fornecer a descrição ou os metadados da ação. Na próxima linha, você deve fornecer os dados. Cada parte é separada por uma nova linha (\n). Uma descrição de ação de uma inserção pode ser semelhante a esta:

```
{ "create" : { "_index" : "veggies", "_type" : "_doc", "_id" : "7" } }
```

E a próxima linha contendo os dados pode ter a seguinte aparência:

```
{ "name":"kale", "color":"green", "classification":"leafy-green" }
```

Juntos, os metadados e os dados representam uma única ação em uma operação em massa. Você pode realizar várias operações em uma solicitação, como esta:

```
POST /_bulk
{ "create" : { "_index" : "veggies", "_id" : "35" } }
{ "name":"kale", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "36" } }
```

```
{ "name":"spinach", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "37" } }
{ "name":"arugula", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "38" } }
{ "name":"endive", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "39" } }
{ "name":"lettuce", "color":"green", "classification":"leafy-green" }
{ "delete" : { "_index" : "vegetables", "_id" : "1" } }
```

Observe que a última ação é `delete`. Não há dados seguindo a ação `delete`.

Pesquisando documentos

Agora que os dados existem no seu cluster, você pode procurá-los. Por exemplo, talvez você queira pesquisar todos os tubérculos ou obter uma contagem de todas as folhas verdes ou encontrar o número de erros registrados por hora.

Pesquisas básicas

Uma pesquisa básica é semelhante a esta:

```
GET veggies/_search?q=name:l*
```

A solicitação produz uma resposta JSON que contém o documento lettuce.

Pesquisas avançadas

É possível realizar pesquisas mais avançadas fornecendo as opções de consulta como JSON no corpo da solicitação:

```
GET veggies/_search
{
  "query": {
    "term": {
      "name": "lettuce"
    }
  }
}
```

Este exemplo também produz uma resposta JSON com o documento lettuce.

Classificar

É possível executar mais desse tipo de consulta usando a classificação. Primeiro, é necessário recriar o índice, porque o mapeamento automático de campo escolheu tipos que não podem ser classificados por padrão. Envie as seguintes solicitações para excluir e recriar o índice:

```
DELETE /veggies

PUT /veggies
{
   "mappings":{
      "properties":{
         "name":{
            "type":"keyword"
         },
         "color":{
            "type":"keyword"
         },
         "classification":{
            "type":"keyword"
         }
      }
   }
}
```

Em seguida, preencha novamente o índice com dados:

```
POST /_bulk
{ "create" : { "_index" : "veggies", "_id" : "7"  } }
{ "name":"kale", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "8" } }
{ "name":"spinach", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "9" } }
{ "name":"arugula", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "10" } }
{ "name":"endive", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "11" } }
{ "name":"lettuce", "color":"green", "classification":"leafy-green" }
```

Agora você pode pesquisar com uma classificação. Esta solicitação adiciona uma classificação crescente:

```
GET veggies/_search
{
```

```
  "query" : {
    "term": { "color": "green" }
  },
  "sort" : [
      "classification"
  ]
}
```

Recursos relacionados

Para mais informações, consulte os seguintes recursos do :

- Conceitos básicos
- Indexação de dados
- Pesquisa de dados

Tutorial: migração para o Amazon OpenSearch Service

Os snapshots de índices são uma maneira popular de realizar migração de um cluster autogerenciado do OpenSearch ou obsoleto do Elasticsearch para o Amazon OpenSearch Service. Em termos gerais, o processo consiste nas seguintes etapas:

1. Faça um snapshot do cluster existente e faça upload do snapshot para um bucket do Amazon S3.
2. Crie um domínio do OpenSearch Service.
3. Conceda ao OpenSearch Service permissões para acessar o bucket e verifique se você tem permissões para trabalhar com snapshots.
4. Restaure o snapshot no domínio do OpenSearch Service.

Esta demonstração fornece etapas mais detalhadas e opções alternativas, quando aplicável.

Obter e fazer upload do snapshot

Embora você possa usar o plug-in repository-s3 para obter snapshots diretamente no S3, você precisa instalar o plug-in em cada nó, ajustar o `opensearch.yml` (ou o `elasticsearch.yml`, se estiver usando um cluster Elasticsearch), reiniciar cada nó, adicionar suas credenciais da AWS e, finalmente, obter o snapshot. O plug-in é uma ótima opção para uso contínuo ou para migrar clusters maiores.

Para clusters menores, uma abordagem única é fazer um snapshot do sistema de arquivos compartilhado e usar a AWS CLI para fazer upload para o S3. Se você já tiver um snapshot, avance para a etapa 4.

Para obter um snapshot e fazer upload no Amazon S3

1. Adicione a configuração `path.repo` ao `opensearch.yml` (ou ao `Elasticsearch.yml`) em todos os nós e, em seguida, reinicie cada nó.

```
path.repo: ["/my/shared/directory/snapshots"]
```

2. Registre um repositório de snapshots, o que é obrigatório para poder tirar um snapshot. Um repositório é apenas um local de armazenamento: um sistema de arquivos compartilhados, o Amazon S3, o Sistema de Arquivos Distribuído do Hadoop (HDFS) etc. Nesse caso, usaremos um sistema de arquivos compartilhados (“fs”):

```
PUT _snapshot/my-snapshot-repo-name
{
  "type": "fs",
  "settings": {
    "location": "/my/shared/directory/snapshots"
  }
}
```

3. Faça o snapshot:

```
PUT _snapshot/my-snapshot-repo-name/my-snapshot-name
{
  "indices": "migration-index1,migration-index2,other-indices-*",
  "include_global_state": false
}
```

4. Instale a AWS CLI, e execute `aws configure` para adicionar suas credenciais.

5. Navegue até o diretório de snapshots. Depois disso, execute os seguintes comandos para criar um novo bucket do S3 e fazer upload do conteúdo do diretório de snapshots para esse bucket:

```
aws s3 mb s3://bucket-name --region us-west-2
aws s3 sync . s3://bucket-name --sse AES256
```

Dependendo do tamanho do snapshot e da velocidade da sua conexão com a Internet, essa operação pode demorar um pouco.

Crie um domínio

Embora o console seja a maneira mais fácil de criar um domínio, nesse caso, você já tem o terminal aberto e a AWS CLI instalada. Modifique o seguinte comando para criar um domínio que atenda às suas necessidades:

```
aws opensearch create-domain \
  --domain-name migration-domain \
  --engine-version OpenSearch_1.0 \
  --cluster-config InstanceType=c5.large.search,InstanceCount=2 \
  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=100 \
  --node-to-node-encryption-options Enabled=true \
  --encryption-at-rest-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true,TLSSecurityPolicy=Policy-Min-
TLS-1-2-2019-07 \
  --advanced-security-options
 Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions='{MasterUserName=master-
user,MasterUserPassword=master-user-password}' \
  --access-policies '{"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":{"AWS":["*"]},"Action":
["es:ESHttp*"],"Resource":"arn:aws:es:us-west-2:123456789012:domain/migration-domain/
*"}]}' \
  --region us-west-2
```

Da maneira em que se encontra, o comando cria um domínio acessível à Internet com dois nós de dados, cada um com 100 GiB de armazenamento. Ele também habilita o controle de acesso refinado com autenticação básica de HTTP e todas as configurações de criptografia. Use o console do OpenSearch Service se for necessária uma configuração de segurança mais avançada, como uma VPC.

Antes de emitir o comando, altere o nome do domínio, as credenciais do usuário mestre e o número da conta. Especifique a mesma Região da AWS usada para o bucket do S3 e uma versão do OpenSearch/Elasticsearch compatível com seu snapshot.

> **Important**
>
> Os snapshots são compatíveis somente com versões posteriores e somente com uma versão principal. Por exemplo, você não pode restaurar um snapshot de um OpenSearch 1. cluster x em um Elasticsearch 7. cluster x, somente um OpenSearch 1. x ou 2. cluster x. A versão secundária também é importante. Não é possível restaurar um snapshot de um cluster 5.3.3 autogerenciado em um domínio do OpenSearch Service 5.3.2. Recomendamos escolher a versão mais recente do OpenSearch ou Elasticsearch compatível com seu snapshot. Para obter uma tabela de versões compatíveis, consulte the section called “Como usar um snapshot para migrar dados”.

Conceder permissões para o bucket do S3

No console do AWS Identity and Access Management (IAM), crie uma função com as seguintes permissões e relação de confiança. Ao criar a função, escolha S3 como o Serviço da AWS. Nomeie a função como `OpenSearchSnapshotRole` para que ela seja fácil de encontrar.

Permissões

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::bucket-name"
      ]
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::bucket-name/*"
      ]
```

```
    }
  ]
}
```

Relação de confiança

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Principal": {
        "Service": "es.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Em seguida, dê ao seu perfil do IAM pessoal permissões para assumir `OpenSearchSnapshotRole`. Crie a seguinte política e anexe-a à sua identidade:

Permissões

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/OpenSearchSnapshotRole"
    }
  ]
}
```

Mapear a função de snapshot no OpenSearch Dashboards (se estiver usando um controle de acesso refinado)

Se você habilitou o controle de acesso detalhado, mesmo se usar a autenticação básica HTTP para todos os outros fins, precisará mapear o perfil do `manage_snapshots` para o seu perfil do IAM para poder trabalhar com snapshots.

Para conceder à sua identidade permissões para trabalhar com snapshots

1. Faça login no Dashboards usando as credenciais de usuário primário especificadas ao criar o domínio do OpenSearch Service. É possível encontrar o URL do Dashboards no console do OpenSearch Service. Ele segue o formato `https://domain-endpoint/_dashboards/`.
2. No menu principal, escolha Segurança, Funções e selecione a função manage_snapshots.
3. Escolha Usuários mapeados e Gerenciar mapeamento.
4. Adicione o ARN do domínio do seu perfil do IAM pessoal no campo apropriado. O ARN assume um dos seguintes formatos:

```
arn:aws:iam::123456789123:user/user-name
```

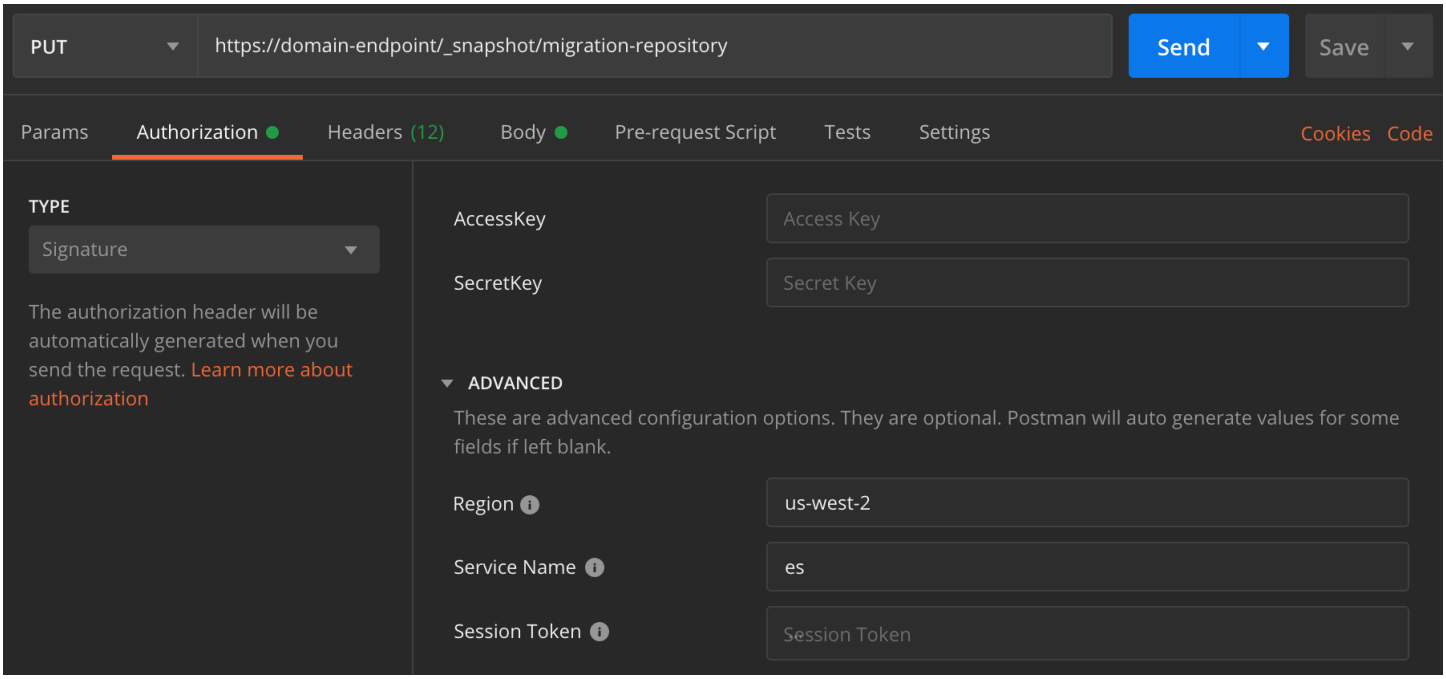
```
arn:aws:iam::123456789123:role/role-name
```

5. Selecione Mapa e confirme se o perfil aparece em Usuários mapeados.

Restaure o snapshot

Neste momento, você tem duas maneiras de acessar o domínio do OpenSearch Service: a autenticação básica HTTP com suas credenciais de usuário primário ou a autenticação da AWS usando suas credenciais do IAM. Como os snapshots usam o Amazon S3, o qual não tem um conceito de usuário primário, é necessário usar suas credenciais do IAM para registrar o repositório de snapshots com seu domínio do OpenSearch Service.

A maioria das linguagens de programação tem bibliotecas para ajudar com a assinatura de solicitações, mas a abordagem mais simples é usar uma ferramenta como o Postman e colocar suas credenciais do IAM na seção Autorização .



Como restaurar o snapshot

1. Independentemente de como você optar por assinar suas solicitações, a primeira etapa é registrar o repositório:

```
PUT _snapshot/my-snapshot-repo-name
{
  "type": "s3",
  "settings": {
    "bucket": "bucket-name",
    "region": "us-west-2",
    "role_arn": "arn:aws:iam::123456789012:role/OpenSearchSnapshotRole"
  }
}
```

2. Depois disso, liste os snapshots no repositório e encontre o que deseja restaurar. Neste momento, é possível continuar usando o Postman ou alternar para uma ferramenta como o curl.

   Abreviatura

   ```
   GET _snapshot/my-snapshot-repo-name/_all
   ```

   curl

```
curl -XGET -u 'master-user:master-user-password' https://domain-endpoint/
_snapshot/my-snapshot-repo-name/_all
```

3. Restaure o snapshot.

   Abreviatura

   ```
   POST _snapshot/my-snapshot-repo-name/my-snapshot-name/_restore
   {
     "indices": "migration-index1,migration-index2,other-indices-*",
     "include_global_state": false
   }
   ```

   curl

   ```
   curl -XPOST -u 'master-user:master-user-password' https://domain-endpoint/
   _snapshot/my-snapshot-repo-name/my-snapshot-name/_restore \
     -H 'Content-Type: application/json' \
     -d '{"indices":"migration-index1,migration-index2,other-indices-
   *","include_global_state":false}'
   ```

4. Por fim, verifique se seus índices foram restaurados conforme o esperado.

   Abreviatura

   ```
   GET _cat/indices?v
   ```

   curl

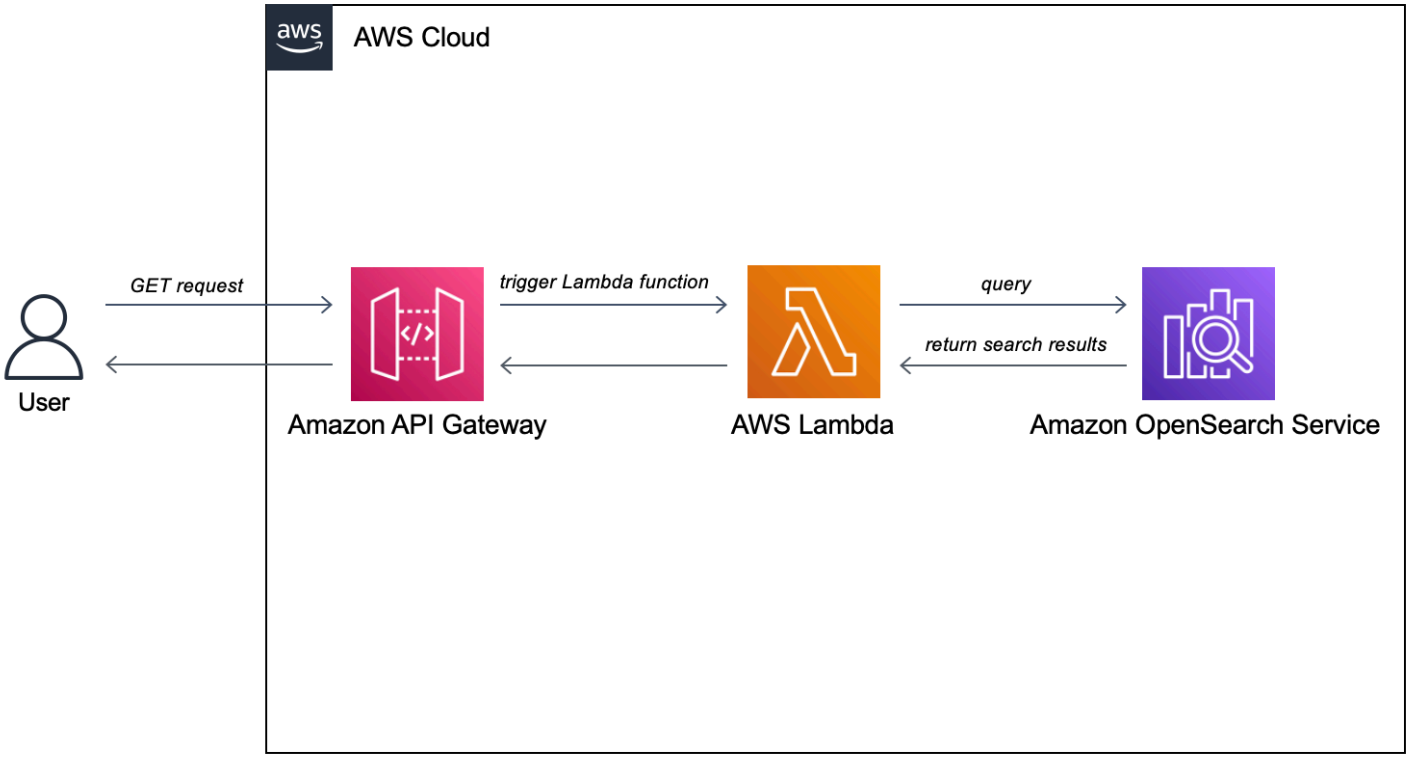
   ```
   curl -XGET -u 'master-user:master-user-password' https://domain-endpoint/_cat/
   indices?v
   ```

Neste momento, a migração está concluída. Você pode configurar seus clientes para usar o novo endpoint do OpenSearch Service, redimensionar o domínio para se adequar à sua workload, verificar a contagem de fragmentos para seus índices, alternar para um usuário primário do IAM ou começar a criar visualizações no OpenSearch Dashboards.

Tutorial: criação de uma aplicação de pesquisa com o Amazon OpenSearch Service

Uma maneira comum de criar uma aplicação de pesquisa com o Amazon OpenSearch Service é usar formulários da Web para enviar consultas do usuário a um servidor. Em seguida, você pode autorizar o servidor para chamar as APIs do OpenSearch diretamente e fazer com que o servidor envie solicitações ao OpenSearch Service. No entanto, se desejar escrever um código do lado do cliente que não dependa de um servidor, é necessário compensar os riscos de segurança e performance. Permitir o acesso público não assinado às APIs do OpenSearch não é aconselhável. Os usuários podem acessar endpoints não seguros ou afetar a performance do cluster por meio de consultas excessivamente amplas (ou muitas consultas).

Este capítulo apresenta uma solução: use o Amazon API Gateway para restringir usuários a um subconjunto das APIs do OpenSearch e o AWS Lambda para assinar solicitações do API Gateway para o OpenSearch Service.



> **Note**
>
> Os preços padrão do API Gateway e do Lambda se aplicam, mas dentro do uso limitado desse tutorial, os custos devem ser insignificantes.

Pré-requisitos

Ter um domínio do OpenSearch Service é um pré-requisito para este tutorial. Se você ainda não tem um, siga as etapas em Criar um domínio do OpenSearch Service para criá-lo.

Etapa 1: Indexar dados de exemplo

Faça download de sample-movies.zip e use a operação da API _bulk para adicionar os 5.000 documentos ao índice `movies`:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/_bulk
{ "index": { "_index": "movies", "_id": "tt1979320" } }
{"directors":["Ron
 Howard"],"release_date":"2013-09-02T00:00:00Z","rating":8.3,"genres":
["Action","Biography","Drama","Sport"],"image_url":"http://ia.media-imdb.com/images/
M/MV5BMTQyMDE0MTY0OV5BMl5BanBnXkFtZTcwMjI2OTI0OQ@@._V1_SX400_.jpg","plot":"A re-
creation of the merciless 1970s rivalry between Formula One rivals James Hunt and
 Niki Lauda.","title":"Rush","rank":2,"running_time_secs":7380,"actors":["Daniel
 Brühl","Chris Hemsworth","Olivia Wilde"],"year":2013,"id":"tt1979320","type":"add"}
{ "index": { "_index": "movies", "_id": "tt1951264" } }
{"directors":["Francis Lawrence"],"release_date":"2013-11-11T00:00:00Z","genres":
["Action","Adventure","Sci-Fi","Thriller"],"image_url":"http://ia.media-imdb.com/
images/M/
MV5BMTAyMjQ3OTAxMzNeQTJeQWpwZ15BbWU4MDU0NzA1MzAx._V1_SX400_.jpg","plot":"Katniss
 Everdeen and Peeta Mellark become targets of the Capitol after
 their victory in the 74th Hunger Games sparks a rebellion in
 the Districts of Panem.","title":"The Hunger Games: Catching
 Fire","rank":4,"running_time_secs":8760,"actors":["Jennifer Lawrence","Josh
 Hutcherson","Liam Hemsworth"],"year":2013,"id":"tt1951264","type":"add"}
...
```

Observe que o exemplo acima é um comando com um pequeno subconjunto dos dados disponíveis. Para executar a operação `_bulk`, você precisa copiar e colar todo o conteúdo do arquivo `sample-movies`. Para obter mais instruções, consulte the section called “Opção 2: Fazer upload de vários documentos”.

Também é possível usar o seguinte comando do curl para obter o mesmo resultado:

```
curl -XPOST -u 'master-user:master-user-password' 'domain-endpoint/_bulk' --data-binary
 @bulk_movies.json -H 'Content-Type: application/json'
```

Etapa 2: criar e implantar as funções do Lambda

Antes de criar sua API no API Gateway, crie a função do Lambda para a qual ela passará as solicitações.

Criar a função do Lambda

Nesta solução, o Gateway da API passa solicitações para uma função do Lambda, que consulta o OpenSearch Service e retorna resultados: Como essa função de exemplo usa bibliotecas externas, é necessário criar um pacote de implantação e fazer seu upload para o Lambda.

Para criar o pacote de implantação

1. Abra um prompt de comando e crie um diretório de projeto do `my-opensearch-function`. Por exemplo, no macOS:

   ```
   mkdir my-opensearch-function
   ```

2. Navegue até o diretório de projeto do `my-sourcecode-function`.

   ```
   cd my-opensearch-function
   ```

3. Copie o conteúdo do seguinte código Python de exemplo e salve-o em um novo arquivo chamado `opensearch-lambda.py`. Adicione sua região e o endpoint do host ao arquivo.

   ```
   import boto3
   import json
   import requests
   from requests_aws4auth import AWS4Auth

   region = '' # For example, us-west-1
   service = 'es'
   credentials = boto3.Session().get_credentials()
   awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
    session_token=credentials.token)
   ```

```
host = '' # The OpenSearch domain endpoint with https:// and without a trailing
 slash
index = 'movies'
url = host + '/' + index + '/_search'

# Lambda execution starts here
def lambda_handler(event, context):

    # Put the user query into the query DSL for more accurate search results.
    # Note that certain fields are boosted (^).
    query = {
        "size": 25,
        "query": {
            "multi_match": {
                "query": event['queryStringParameters']['q'],
                "fields": ["title^4", "plot^2", "actors", "directors"]
            }
        }
    }

    # Elasticsearch 6.x requires an explicit Content-Type header
    headers = { "Content-Type": "application/json" }

    # Make the signed HTTP request
    r = requests.get(url, auth=awsauth, headers=headers, data=json.dumps(query))

    # Create the response and add some extra content to support CORS
    response = {
        "statusCode": 200,
        "headers": {
            "Access-Control-Allow-Origin": '*'
        },
        "isBase64Encoded": False
    }

    # Add the search results to the response
    response['body'] = r.text
    return response
```

4. Instale a biblioteca externa em um novo diretório de `package`.

```
pip3 install --target ./package boto3
pip3 install --target ./package requests
```

```
pip3 install --target ./package requests_aws4auth
```

5. Crie um pacote de implantação com a biblioteca instalada na raiz. O seguinte comando gera um arquivo `my-deployment-package.zip` no diretório do projeto.

```
cd package
zip -r ../my-deployment-package.zip .
```

6. Adicione o arquivo `opensearch-lambda.py` à raiz do arquivo zip.

```
cd ..
zip my-deployment-package.zip opensearch-lambda.py
```

Para obter mais informações sobre a criação de funções do Lambda e pacotes de implantação, consulte Implantar funções do Lambda em Python com arquivos .zip no Guia do desenvolvedor do AWS Lambda e the section called “Criar o pacote de implantação do Lambda” neste guia.

Para criar sua função usando o console do Lambda

1. Navegue até o console do Lambda em https://console.aws.amazon.com/lambda/home. No painel de navegação à esquerda, escolha Funções.
2. Selecione Criar função.
3. Configure os campos a seguir.
   - Nome da função: opensearch-function
   - Runtime: Python 3.9.
   - Arquitetura: x86_64

   Mantenha todas as outras opções padrão e escolha Criar função.
4. Na seção Fonte do código da página de resumo da função, escolha Fazer upload no menu suspenso e selecione .zip. file. Localize o arquivo `my-deployment-package.zip` que você criou e escolha Salvar.
5. O manipulador é o método no código da sua função que processa eventos. Em Configurações do Runtime, escolha Editar e altere o nome do manipulador de acordo com o nome do arquivo no pacote de implantação onde a função do Lambda está localizada Como seu arquivo se chama `opensearch-lambda.py`, renomeie o manipulador para *`opensearch-`*

lambda.lambda_handler. Para obter mais informações, consulte Manipulador de função do Lambda em Python.

Etapa 3: Criar a API no Gateway da API

Usar o API Gateway permite a você criar uma API mais limitada e simplifica o processo de interação com a API _search do OpenSearch. O API Gateway também permite ativar recursos de segurança, como a autenticação do Amazon Cognito e a limitação de solicitações. Execute as seguintes etapas para criar e implantar uma API:

Criar e configurar a API

Para criar sua API usando o console do API Gateway

1. Navegue até o console do Gateway da API em https://console.aws.amazon.com/apigateway/home. No painel de navegação à esquerda, escolha APIs.
2. Localize a API REST (não privada) e escolha Compilar.
3. Na página seguinte, localize a seção Criar nova API e verifique se a opção Nova API está selecionada.
4. Configure os campos a seguir.
   - Nome da API: opensearch-api
   - Descrição: API pública para pesquisar um domínio do Amazon OpenSearch Service
   - Tipo do endpoint: Regional
5. Selecione Criar API.
6. Escolha Ações e Criar método.
7. Select GET no menu suspenso e clique na marca de seleção para confirmar.
8. Defina as seguintes configurações e escolha Salvar:

Configuração	Valor
Tipo de integração	Função do Lambda
Usar a integração de proxy do Lambda	Sim

Configuração	Valor
Região do Lambda	*us-west-1*
Função do Lambda	opensearch-lambda
Usar o tempo limite padrão	Sim

Configurar a solicitação de método

Escolha Solicitação de métodot e defina as seguintes configurações:

Configuração	Valor
Autorização	NONE
Validador da solicitação	Validar parâmetros e cabeçalhos da string de consulta
Chave da API necessária	false

Em Parâmetros da string de consulta do URL), escolha Adicionar string de consulta e configure o seguinte parâmetro:

Configuração	Valor
Nome	q
Obrigatório	Sim

Implante a API e configure um estágio

O console do API Gateway permite que você implante uma API criando uma implantação e associando-a a um estágio novo ou existente.

1. Escolha Ações e Implantar API.

2. Para Estágio da implantação), escolha Novo estágio e atribua o nome `opensearch-api-test` ao estágio.
3. Escolha Deploy (Implantar).
4. Defina as seguintes configurações no editor de estágios e, em seguida, escolha Salvar alterações:

Configuração	Valor
Habilitar controle de utilização	Sim
Rate	1000
Intermitência	500

Essas definições configuram uma API que possui apenas um método: uma solicitação `GET` para a raiz do endpoint (`https://`*`some-id`*`.execute-api.`*`us-west-1`*`.amazonaws.com/search-es-api-test`). A solicitação requer um único parâmetro (`q`), a string de consulta a ser pesquisada. Quando chamado, o método passa a solicitação para o Lambda, que executa a função `opensearch-lambda`. Para obter mais informações, consulte Criação de uma API no Amazon API Gateway e Implantação de uma API REST no Amazon API Gateway.

Etapa 4: (opcional) modificar a política de acesso ao domínio

O domínio do OpenSearch Service deve permitir que a função do Lambda faça solicitações `GET` ao índice `movies`. Se o domínio tiver uma política de acesso aberto com controle de acesso refinado habilitado, você pode deixar como está:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:*",
      "Resource": "arn:aws:es:us-west-1:123456789012:domain/domain-name/*"
    }
```

```
  ]
}
```

Ou você pode escolher tornar a política de acesso ao domínio mais granular. Por exemplo, a política mínima a seguir fornece à `opensearch-lambda-role` (criada por meio do Lambda) acesso de leitura ao índice `movies`. Para obter o nome exato da função que o Lambda cria automaticamente, vá para o console do AWS Identity and Access Management (IAM), escolha Funções e procure por "lambda".

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/service-role/opensearch-lambda-
role-1abcdefg"
      },
      "Action": "es:ESHttpGet",
      "Resource": "arn:aws:es:us-west-1:123456789012:domain/domain-name/movies/_search"
    }
  ]
}
```

> **Important**
>
> Se você tiver um controle de acesso minucioso habilitado para o domínio, será necessário mapear a função para um usuário no OpenSearch Dashboards. Caso contrário, você receberá erros de permissões.

Para obter mais informações sobre políticas de acesso, consulte the section called "Configuração de políticas de acesso".

Mapeamento da função do Lambda (se estiver usando um controle de acesso minucioso)

O controle de acesso minucioso introduz uma etapa adicional antes de testar a aplicação. Mesmo se você usar a autenticação básica do HTTP para todos os outros fins, será necessário mapear a função do Lambda para um usuário. Caso contrário, você receberá erros de permissões.

1. Navegue até o URL do OpenSearch Dashboards do domínio.
2. No menu principal, escolha Segurança, Funções e selecione o link para `all_access`, a função para a qual precisa mapear a função do Lambda.
3. Escolha Usuários mapeados e Gerenciar mapeamento.
4. Em Funções de backend, adicione o nome do recurso da Amazon (ARN) da função do Lambda. O ARN deve assumir a forma de `arn:aws:iam::`*`123456789123`*`:role/service-role/`*`opensearch-lambda-role-1abcdefg`*.
5. Selecione Mapa e confirme se o usuário ou função aparece em Usuários mapeados.

Etapa 5: Testar a aplicação Web

Para testar o aplicativo web

1. Faça download do sample-site.zip, descompacte-o e abra `scripts/search.js` em seu editor de texto de preferência.
2. Atualize a variável `apigatewayendpoint` para apontar para o endpoint do API Gateway Você pode encontrar rapidamente o endpoint no API Gateway escolhendo Estágios e selecionando o nome da API. A variável `apigatewayendpoint` deve assumir a forma de `https://`*`some-id`*`.execute-api.`*`us-west-1`*`.amazonaws.com/opensearch-api-test`.
3. Abra `index.html` e tente executar pesquisas para thor, casa e alguns outros termos.

Movie Search

thor

Found 7 results.

Thor

2011 — The powerful but arrogant god Thor is cast out of Asgard to live amongst humans in Midgard (Earth), where he soon becomes one of their finest defenders.

Thor: The Dark World

2013 — Faced with an enemy that even Odin and Asgard cannot withstand, Thor must embark on his most perilous and personal journey yet, one that will reunite him with Jane Foster and force him to sacrifice everything to save us all.

Vikingdom

2013 — A forgotten king, Eirick, is tasked with the impossible odds to defeat Thor, the God of Thunder.

Solucionar erros CORS

Mesmo que a função do Lambda inclua conteúdo na resposta para ser compatível com o CORS, você ainda pode ver o seguinte erro:

```
Access to XMLHttpRequest at '<api-gateway-endpoint>' from origin 'null' has been
 blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present in the
 requested resource.
```

Se isso acontecer, tente o seguinte:

1. Habilite o CORS no recurso GET. Em Avançado, defina Access-Control-Allow-Credentials como `'true'`.
2. Reimplante a API no API Gateway [Ações, Implantar API].
3. Exclua e torne a adicionar o acionador da função do Lambda. Adicione readicionar, escolha Adicionar acionador e crie o endpoint HTTP que invoca sua função. O acionador deve ter a seguinte configuração:

Trigger	API	Estágio de implantação	Segurança
API Gateway	opensearch-api	opensearch-api-test	Aberto

Próximas etapas

Este capítulo é apenas um ponto de partida para demonstrar um conceito. Você pode considerar as seguintes modificações:

- Adicione seus próprios dados ao domínio do OpenSearch Service.
- Adicionar métodos à API.
- Na função do Lambda, modifique a consulta de pesquisa ou incremente campos diferentes.
- Estilize os resultados de maneira diferente ou modifique `search.js` para exibir campos diferentes para o usuário.

Tutorial: visualização de chamadas de suporte ao cliente com o OpenSearch Service e o OpenSearch Dashboards

Este capítulo é uma descrição completa da seguinte situação: uma empresa recebe um determinado número de chamadas de suporte ao cliente e quer analisá-las. O que é o assunto de cada chamada? Quantas eram positivas? Quantas eram negativas? Como os gerentes podem pesquisar ou revisar as transcrições dessas chamadas?

Um fluxo de trabalho manual pode envolver funcionários ouvindo gravações, anotando o assunto de cada chamada e decidindo se a interação do cliente foi positiva.

Esse processo seria extremamente trabalhoso. Supondo um tempo médio de 10 minutos por chamada, cada funcionário escutaria apenas 48 chamadas por dia. Independentemente do viés humano, os dados que eles geram seriam altamente precisos, mas a quantidade de dados seria mínima: apenas o assunto da chamada e um booliano para saber se o cliente estava ou não satisfeito. Qualquer coisa mais complexa, como uma transcrição completa, tomaria uma quantidade imensa de tempo.

Usando o Amazon S3, Amazon Transcribe, Amazon Comprehend e Amazon OpenSearch Service, você pode automatizar um processo semelhante com muito pouco código e terminar com muito mais dados. Por exemplo, você pode obter uma transcrição completa da chamada, as palavras-chave da transcrição e um "sentimento" global da chamada (positivo, negativo, neutro ou misto). Em seguida, você pode usar o OpenSearch e o OpenSearch Dashboards para pesquisar e visualizar os dados.

Embora você possa usar esta demonstração no estado em que se encontra, a intenção é estimular ideias sobre como enriquecer seus documentos JSON antes de indexá-los no OpenSearch Service.

Custos estimados

Em geral, executar as etapas desta demonstração devem custar menos de US$ 2. A demonstração usa os seguintes recursos:

- Bucket do S3 com menos de 100 MB transferidos e armazenados

  Para saber mais, consulte Definição de preços do Amazon S3.
- Domínio do OpenSearch Service com uma instância `t2.medium` e 10 GiB de armazenamento do EBS para várias horas

  Para saber mais, consulte Preços do Amazon OpenSearch Service.

- Várias chamadas para o Amazon Transcribe

  Para saber mais, consulte Preços do Amazon Transcribe.
- Várias chamadas de processamento de linguagem natural para o Amazon Comprehend

  Para saber mais, consulte Preços do Amazon Comprehend.

Tópicos

Etapa 1: Configurar os pré-requisitos

Para continuar, você deve ter os recursos a seguir.

Pré-requisito	Descrição
Bucket do Amazon S3.	Para obter mais informações, consulte Creating a Bucket (Criar um bucket) no Manual do usuário do Amazon Simple Storage Service.
Domínio do OpenSearch Service	O destino dos dados. Para obter mais informações, consulte Criação de domínios do OpenSearch Service.

Se você ainda não tiver esses recursos, poderá criá-los usando os seguintes comandos do AWS CLI:

```
aws s3 mb s3://my-transcribe-test --region us-west-2
```

```
aws opensearch create-domain --domain-name my-transcribe-test --engine-version
 OpenSearch_1.0 --cluster-config  InstanceType=t2.medium.search,InstanceCount=1
 --ebs-options EBSEnabled=true,VolumeType=standard,VolumeSize=10 --access-
policies '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::123456789012:root"},"Action":"es:*","Resource":"arn:aws:es:us-
west-2:123456789012:domain/my-transcribe-test/*"}]}' --region us-west-2
```

> **Note**
>
> Esses comandos usam a região `us-west-2`, mas você pode usar qualquer região compatível com o Amazon Comprehend. Para saber mais, consulte o Referência geral da AWS.

Etapa 2: Copiar código de exemplo

1. Copie e cole o código de exemplo Python 3 a seguir em um novo arquivo chamado `call-center.py`:

```
import boto3
import datetime
import json
import requests
from requests_aws4auth import AWS4Auth
import time
import urllib.request

# Variables to update
audio_file_name = '' # For example, 000001.mp3
bucket_name = '' # For example, my-transcribe-test
domain = '' # For example, https://search-my-transcribe-test-12345.us-
west-2.es.amazonaws.com
index = 'support-calls'
type = '_doc'
region = 'us-west-2'

# Upload audio file to S3.
s3_client = boto3.client('s3')

audio_file = open(audio_file_name, 'rb')

print('Uploading ' + audio_file_name + '...')
response = s3_client.put_object(
    Body=audio_file,
    Bucket=bucket_name,
    Key=audio_file_name
)

# # Build the URL to the audio file on S3.
```

```
# # Only for the us-east-1 region.
# mp3_uri = 'https://' + bucket_name + '.s3.amazonaws.com/' + audio_file_name

# Get the necessary details and build the URL to the audio file on S3.
# For all other regions.
response = s3_client.get_bucket_location(
    Bucket=bucket_name
)
bucket_region = response['LocationConstraint']
mp3_uri = 'https://' + bucket_name + '.s3-' + bucket_region + '.amazonaws.com/' +
 audio_file_name

# Start transcription job.
transcribe_client = boto3.client('transcribe')

print('Starting transcription job...')
response = transcribe_client.start_transcription_job(
    TranscriptionJobName=audio_file_name,
    LanguageCode='en-US',
    MediaFormat='mp3',
    Media={
        'MediaFileUri': mp3_uri
    },
    Settings={
        'ShowSpeakerLabels': True,
        'MaxSpeakerLabels': 2 # assumes two people on a phone call
    }
)

# Wait for the transcription job to finish.
print('Waiting for job to complete...')
while True:
    response =
 transcribe_client.get_transcription_job(TranscriptionJobName=audio_file_name)
    if response['TranscriptionJob']['TranscriptionJobStatus'] in ['COMPLETED',
 'FAILED']:
        break
    else:
        print('Still waiting...')
    time.sleep(10)

transcript_uri = response['TranscriptionJob']['Transcript']['TranscriptFileUri']

# Open the JSON file, read it, and get the transcript.
```

```
response = urllib.request.urlopen(transcript_uri)
raw_json = response.read()
loaded_json = json.loads(raw_json)
transcript = loaded_json['results']['transcripts'][0]['transcript']

# Send transcript to Comprehend for key phrases and sentiment.
comprehend_client = boto3.client('comprehend')

# If necessary, trim the transcript.
# If the transcript is more than 5 KB, the Comprehend calls fail.
if len(transcript) > 5000:
    trimmed_transcript = transcript[:5000]
else:
    trimmed_transcript = transcript

print('Detecting key phrases...')
response = comprehend_client.detect_key_phrases(
    Text=trimmed_transcript,
    LanguageCode='en'
)

keywords = []
for keyword in response['KeyPhrases']:
    keywords.append(keyword['Text'])

print('Detecting sentiment...')
response = comprehend_client.detect_sentiment(
    Text=trimmed_transcript,
    LanguageCode='en'
)

sentiment = response['Sentiment']

# Build the Amazon OpenSearch Service URL.
id = audio_file_name.strip('.mp3')
url = domain + '/' + index + '/' + type + '/' + id

# Create the JSON document.
json_document = {'transcript': transcript, 'keywords': keywords, 'sentiment':
 sentiment, 'timestamp': datetime.datetime.now().isoformat()}

# Provide all details necessary to sign the indexing request.
credentials = boto3.Session().get_credentials()
```

```
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region,
 'opensearchservice', session_token=credentials.token)

# Index the document.
print('Indexing document...')
response = requests.put(url, auth=awsauth, json=json_document, headers=headers)

print(response)
print(response.json())
```

2. Atualize as primeiras seis variáveis.
3. Instale os pacotes exigidos usando os seguintes comandos:

```
pip install boto3
pip install requests
pip install requests_aws4auth
```

4. Coloque o MP3 no mesmo diretório que `call-center.py` e execute o script. Uma saída de exemplo se segue:

```
$ python call-center.py
Uploading 000001.mp3...
Starting transcription job...
Waiting for job to complete...
Still waiting...
Still waiting...
Still waiting...
Still waiting...
Still waiting...
Still waiting...
Still waiting...
Detecting key phrases...
Detecting sentiment...
Indexing document...
<Response [201]>
{u'_type': u'call', u'_seq_no': 0, u'_shards': {u'successful': 1, u'failed': 0,
 u'total': 2}, u'_index': u'support-calls4', u'_version': 1, u'_primary_term': 1,
 u'result': u'created', u'_id': u'000001'}
```

`call-center.py` executa uma série de operações:

1. O script faz upload de um arquivo de áudio (neste caso, um MP3, mas o Amazon Transcribe é compatível com vários formatos) no bucket do S3.
2. Ele envia o URL do arquivo de áudio para o Amazon Transcribe e aguarda até que o trabalho de transcrição termine.

   O tempo para concluir o trabalho de transcrição depende do tamanho do arquivo de áudio. Considere minutos, não segundos.

   > **Tip**
   >
   > Para melhorar a qualidade da transcrição, você pode configurar um vocabulário personalizado para o Amazon Transcribe.

3. Depois que o trabalho de transcrição for concluído, o script extrairá a transcrição, a deixará com 5.000 caracteres e a enviará para o Amazon Comprehend para uma análise de palavras-chave e sentimento.
4. Finalmente, o script adicionará a transcrição completa, palavras-chave, sentimentos e carimbo de data/hora atual em um documento JSON e o indexará no OpenSearch Service.

> **Tip**
>
> O LibriVox tem audiolivros de domínio público que você pode usar para testes.

(Opcional) Etapa 3: Indexar dados de exemplo

Se você não tiver várias gravações de chamadas à disposição — e quem tem? — poderá indexar os documentos de exemplo em sample-calls.zip, os quais são comparáveis àqueles produzidos pelo `call-center.py`.

1. Crie um arquivo chamado `bulk-helper.py`:

```
import boto3
from opensearchpy import OpenSearch, RequestsHttpConnection
import json
from requests_aws4auth import AWS4Auth

host = '' # For example, my-test-domain.us-west-2.es.amazonaws.com
```

```
region = '' # For example, us-west-2
service = 'es'

bulk_file = open('sample-calls.bulk', 'r').read()

credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

search = OpenSearch(
    hosts = [{'host': host, 'port': 443}],
    http_auth = awsauth,
    use_ssl = True,
    verify_certs = True,
    connection_class = RequestsHttpConnection
)

response = search.bulk(bulk_file)
print(json.dumps(response, indent=2, sort_keys=True))
```

2. Atualize as primeiras duas variáveis para `host` e `region`.
3. Instale o pacote exigido usando o seguinte comando:

```
pip install opensearch-py
```

4. Faça download e descompacte sample-calls.zip.
5. Coloque `sample-calls.bulk` no mesmo diretório que `bulk-helper.py` e execute o auxiliar. Uma saída de exemplo se segue:

```
$ python bulk-helper.py
{
  "errors": false,
  "items": [
    {
      "index": {
        "_id": "1",
        "_index": "support-calls",
        "_primary_term": 1,
        "_seq_no": 42,
        "_shards": {
          "failed": 0,
          "successful": 1,
```

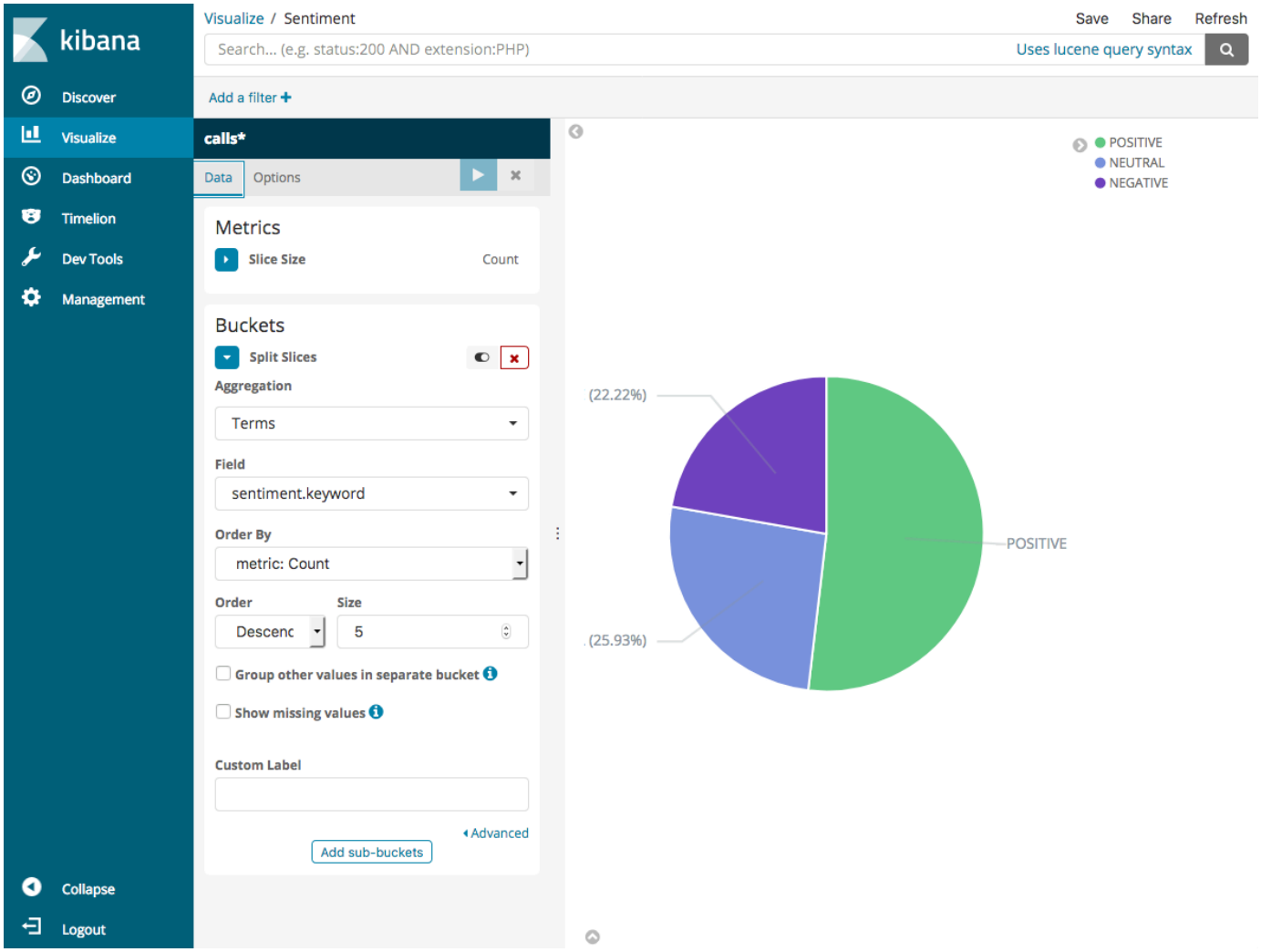
```
          "total": 2
        },
        "_type": "_doc",
        "_version": 9,
        "result": "updated",
        "status": 200
      }
    },
    ...
  ],
  "took": 27
}
```

Etapa 4: Analisar e visualizar seus dados

Agora que você tem alguns dados no OpenSearch Service, poderá visualizá-los usando o OpenSearch Dashboards.

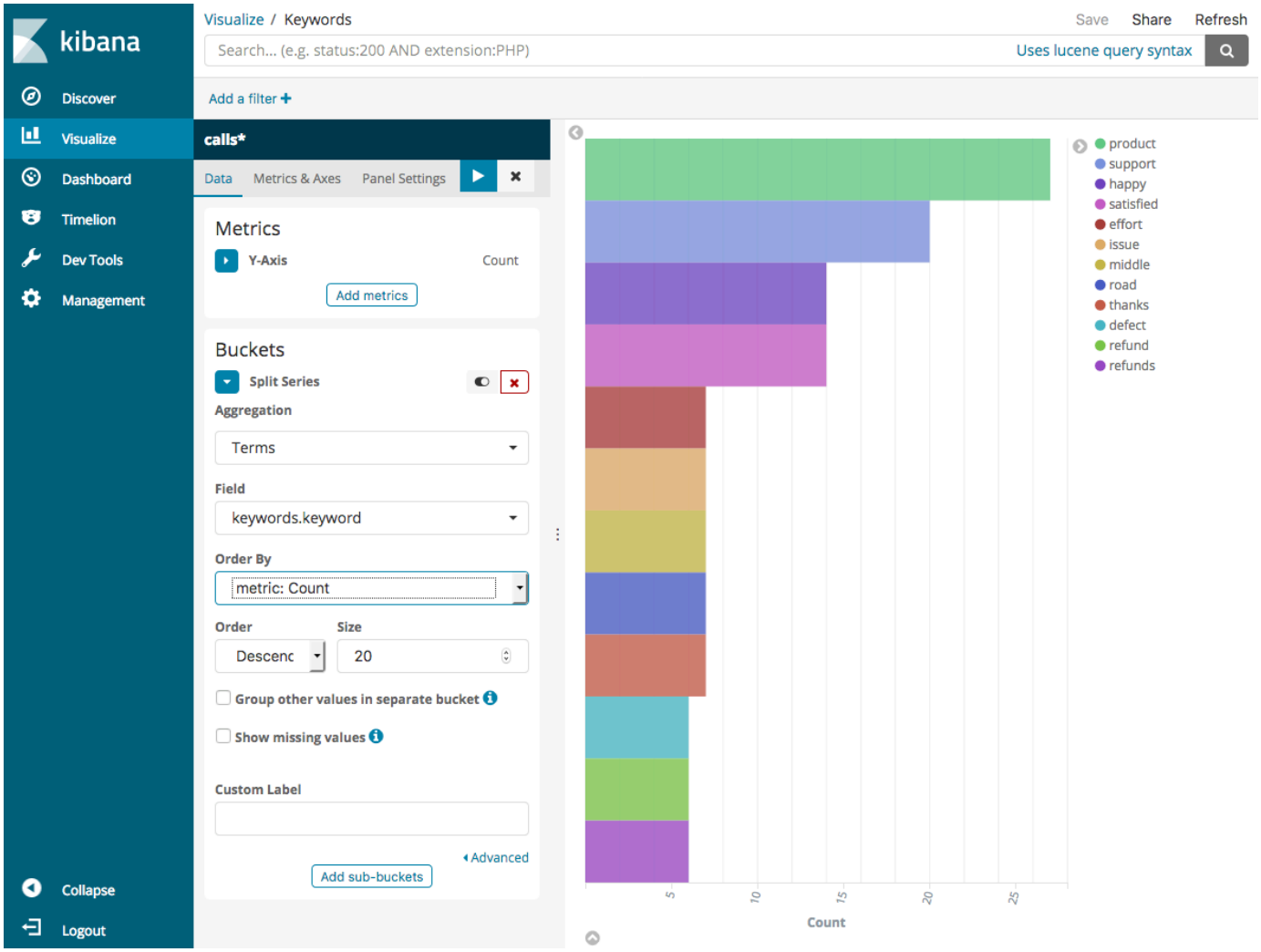
1. Navegue até `https://search-`*`domain`*`.`*`region`*`.es.amazonaws.com/_dashboards`.
2. Antes de usar o OpenSearch Dashboards, você precisará de um padrão de índice. O Dashboard usa padrões de índice para restringir sua análise a um ou mais índices. Para corresponder ao índice `support-calls` criado por `call-center.py`, vá para Stack Management (Gerenciamento de pilhas), Index Patterns (Padrões de índice) e definir um padrão de índice de `support*`. Em seguida, escolha Next step (Próxima etapa).
3. Para o nome de campo Filtro de tempo, escolha timestamp.
4. Agora, você pode começar a criar visualizações. Escolha Visualizar e, em seguida, adicione uma nova visualização.
5. Escolha o gráfico de pizza e o padrão de índice `support*`.
6. A visualização padrão é básica. Portanto, escolha Dividir fatias para criar uma visualização mais interessante.

   Em Aggregation, escolha Terms. Em Campo, escolha sentiment.keyword. Em seguida, escolha Aplicar alterações e Salvar.

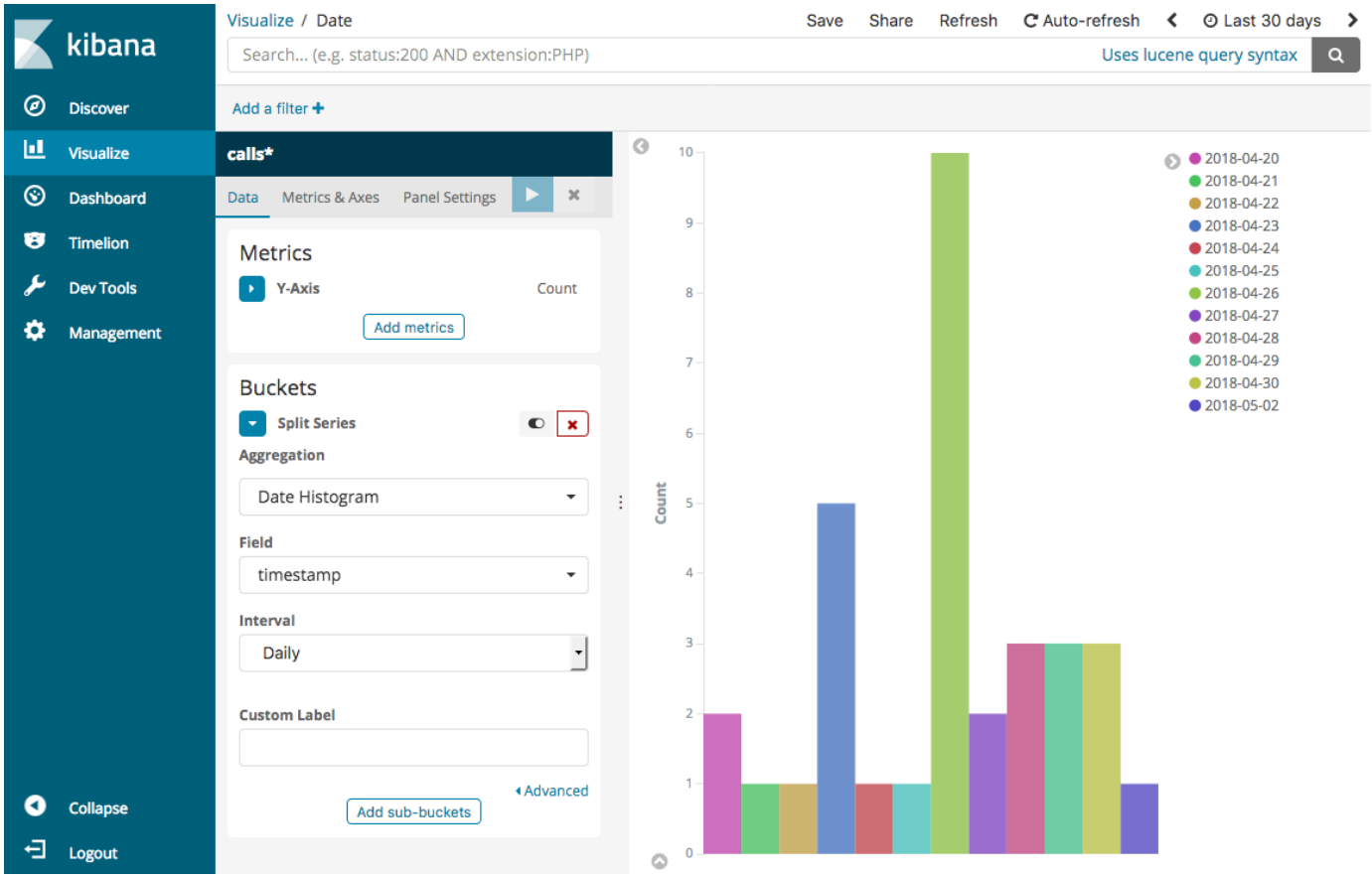


7. Volte para a página Visualizar e adicione outra visualização. Dessa vez, escolha o gráfico de barras horizontais.
8. Selecione Dividir séries.

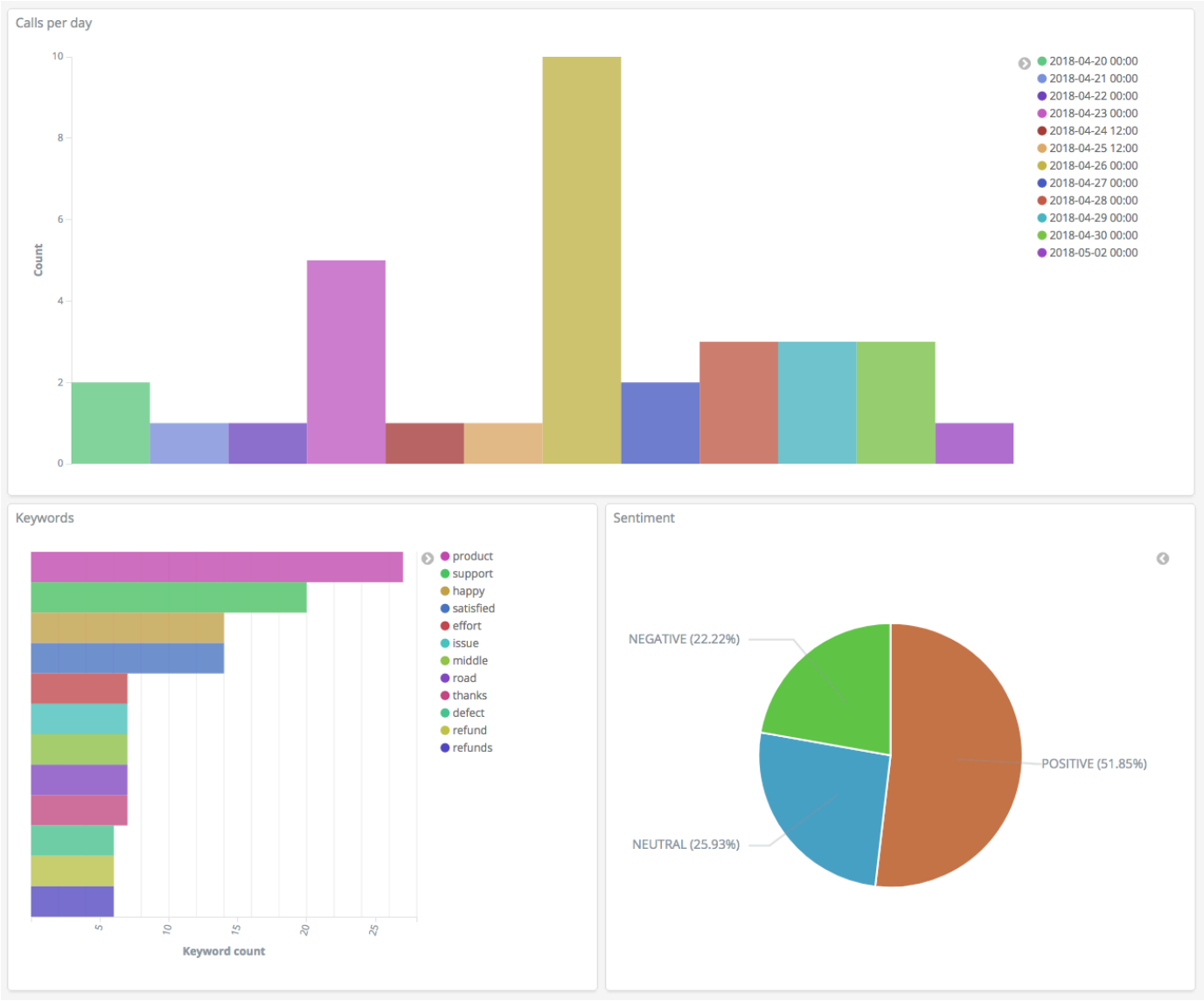
   Em Aggregation, escolha Terms. Em Campo, escolha keywords.keyword e altere Tamanho para 20. Em seguida, escolha Aplicar alterações e Salvar.



9. Volte para a página Visualizar e adicione uma visualização final, um gráfico de barras verticais.
10. Selecione Dividir séries. Em Agregação, escolha Histograma de data. Em Campo, escolha timestamp e altere Intervalo para Diariamente.
11. Escolha Métricas e eixos e altere Modo para normal.
12. Escolha Aplicar alterações e Salvar.



13. Agora que você tem três visualizações, poderá adicioná-las a uma visualização do Dashboards. Escolha Painel, crie um painel e adicione suas visualizações.



Etapa 5: Limpar recursos e próximas etapas

Para evitar cobranças desnecessárias, exclua o bucket do S3 e o domínio do OpenSearch Service. Para saber mais, consulte Delete a Bucket (Excluir um bucket) no Manual do usuário do Amazon Simple Storage Service e Delete an OpenSearch Service domain (Excluir um domínio do OpenSearch Service) nesse guia.

Transcrições exigem muito menos espaço em disco do que arquivos MP3. Você pode reduzir sua janela de retenção de MP3 — por exemplo, de três meses de gravações de chamadas para um mês —, reter anos de transcrições e ainda economizar custos de armazenamento.

Você também pode automatizar o processo de transcrição usando o AWS Step Functions e o Lambda, adicionar metadados adicionais antes de indexar ou criar visualizações mais complexas para se adequar ao seu caso de uso específico.

Renomeação do Amazon OpenSearch Service: resumo das alterações

Em 8 de setembro de 2021, nosso pacote de pesquisas e análise mudou de nome para Amazon OpenSearch Service. O OpenSearch Service oferece suporte ao OpenSearch, bem como ao antigo Elasticsearch OSS. As seções a seguir descrevem as diferentes partes do serviço que foram alteradas com a renomeação do serviço e quais ações você precisa adotar para garantir que seus domínios continuem a funcionar corretamente.

Algumas dessas alterações só se aplicam quando você atualiza seus domínios do Elasticsearch para o OpenSearch. Em outros casos, como no console de Billing and Cost Management, a experiência muda imediatamente.

Essa lista não é exaustiva. Ao mesmo tempo que outras partes do produto também mudaram, essas atualizações são as mais relevantes.

Tópicos

Nova versão de API

A nova versão da API de configuração do OpenSearch Service (2021-01-01) funciona com o OpenSearch, bem como com o antigo Elasticsearch OSS. 21 operações de API foram substituídas por nomes mais concisos e independentes do mecanismo (por exemplo,

`CreateElasticsearchDomain` alterado para `CreateDomain`), mas o OpenSearch Service continua a oferecer suporte a ambas as versões da API.

Recomendamos utilizar as novas operações de API para criar e gerenciar domínios no futuro. Observe que, ao usar as novas operações de API para criar um domínio, você precisará especificar o parâmetro `EngineVersion` no formato `Elasticsearch_X.Y` ou `OpenSearch_X.Y`, em vez de apenas o número da versão. Se você não especificar uma versão, ela assumirá por padrão a versão mais recente do OpenSearch.

Atualize seu AWS CLI para a versão 1.20.40 ou posterior para usar o `aws opensearch ...` para criar e gerenciar seus domínios. Para obter o novo formato de CLI, consulte a Referência da CLI do OpenSearch.

Tipos de instâncias renomeados

Os tipos de instâncias no Amazon OpenSearch Service agora estão no formato `<type>.<size>.search`, por exemplo, `m6g.large.search`em vez de `m6g.large.elasticsearch`. Medida a ser tomada Os domínios existentes começarão a se referir automaticamente aos novos tipos de instâncias dentro da API e no console do Billing and Cost Management.

Se você tiver instâncias reservadas, seu contrato não será afetado pela alteração. A versão antiga da API de configuração ainda é compatível com o formato de nomenclatura antigo, mas se desejar usar a nova versão da API, você precisará usar o novo formato.

Alterações na política de acesso

As seções a seguir descrevem quais ações você precisará executar para atualizar suas políticas de acesso.

Políticas do IAM

Recomendamos atualizar suas políticas do IAM para usar as operações de API renomeadas. No entanto, o OpenSearch Service continuará a respeitar as políticas existentes replicando internamente as permissões de API antigas. Por exemplo, se você tiver permissão para executar a operação `CreateElasticsearchDomain`, agora você poderá fazer chamadas tanto para `CreateElasticsearchDomain` (operação da API antiga) quanto `CreateDomain` (operação da

API nova). O mesmo se aplica às negações explícitas. Para obter uma lista das operações de API atualizadas, consulte a referência de elementos das políticas.

Políticas de SCP

As políticas de controle de serviço (SCPs) introduzem uma camada adicional de complexidade em comparação com o IAM padrão. Para evitar que suas políticas de SCP falhem, você deverá adicionar as operações de API antigas e novas a cada uma de suas políticas de SCP. Por exemplo, se um usuário tem permissões para `CreateElasticsearchDomain`, você também precisa conceder a eles permissões para `CreateDomain` para que eles possam manter a capacidade de criar domínios. O mesmo se aplica às negações explícitas.

Por exemplo:

```
"Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "es:CreateElasticsearchDomain",
        "es:CreateDomain"
         ...
      ],
    },
      "Effect": "Deny",
      "Action:" [
        "es:DeleteElasticsearchDomain",
        "es:DeleteDomain"
         ...
```

Novos tipos de recursos

O OpenSearch Service apresenta os seguintes novos tipos de recursos:

Recurso	Descrição
`AWS::OpenSearchService::Domain`	Representa um domínio do Amazon OpenSearch Service. Esse recurso existe no nível de serviço e não é específico do software em execução no domínio. Aplica-se a serviços como AWS CloudFormation e AWSResource

Recurso	Descrição
	Groups (Grupos de recursos) nos quais você cria e gerencia recursos para o serviço como um todo. Para obter instruções sobre como atualizar domínios definidos no CloudFormation do Elasticsearch para o OpenSearch, consulte as Observações no Guia do usuário do CloudFormation.
`AWS::OpenSearch::Domain`	Representa o software OpenSearch/Elastic Search em execução em um domínio. Este recurso aplica-se a serviços como AWS CloudTrail e AWS Config, os quais fazem referência ao software em execução no domínio, em vez do OpenSearch Service como um todo. Esses serviços agora contêm tipos de recursos separados para domínios que executam o Elasticsearch (`AWS::Elasticsearch::Domain`) versus domínios que executam o OpenSearch (`AWS::OpenSearch::Domain`).

> **Note**
>
> No AWS Config, você continuará a ver seus dados sob o tipo de recurso `AWS::Elasticsearch::Domain` por várias semanas, mesmo se você atualizar um ou mais domínios para o OpenSearch.

Kibana renomeado para OpenSearch Dashboards

O OpenSearch Dashboards, a alternativa do AWS ao Kibana, é uma ferramenta de visualização de código aberto projetada para funcionar com o OpenSearch. Depois de atualizar um domínio do Elasticsearch para o OpenSearch, o endpoint `/_plugin/kibana` muda para `/_dashboards`. O

OpenSearch Service redirecionará todas as solicitações para o novo endpoint, mas se você usar o endpoint do Kibana em qualquer uma das suas políticas do IAM, atualize essas políticas para incluir o novo endpoint `/_dashboards` também.

Se estiver usando the section called “Autenticação SAML para painéis OpenSearch ”, antes de atualizar seu domínio para o OpenSearch, você precisa alterar todos os URLs do Kibana configurados no seu provedor de identidade (IdP) de `/_plugin/kibana` para `/_dashboards`. Os URLs mais comuns são URLs de serviço de consumidor de asserção (ACS) e URLs de destinatário.

A função `kibana_read_only` padrão para o OpenSearch Dashboards foi renomeada para `opensearch_dashboards_read_only`, e a função `kibana_user` foi renomeada para `opensearch_dashboards_user`. A alteração se aplica a todos os domínios recém-criados do OpenSearch 1.x que executam o software de serviço R20211203 ou superior. Se você atualizar um domínio existente para o software de serviço R20211203, os nomes de funções permanecem os mesmos.

Métricas do CloudWatch renomeadas

Várias métricas do CloudWatch mudam para domínios que executam o OpenSearch. Quando você atualiza um domínio para o OpenSearch, as métricas mudam automaticamente e seus alarmes atuais do CloudWatch são interrompidos. Antes de atualizar seu cluster de uma versão do Elasticsearch para uma versão do OpenSearch, certifique-se de atualizar seus alarmes do CloudWatch para usar as novas métricas.

As seguintes métricas foram alteradas:

Nome da métrica original	Novo nome
`KibanaHealthyNodes`	`OpenSearchDashboardsHealthyNodes`
`KibanaConcurrentConnections`	`OpenSearchDashboardsConcurrentConnections`
`KibanaHeapTotal`	`OpenSearchDashboardsHeapTotal`
`KibanaHeapUsed`	`OpenSearchDashboardsHeapUsed`
`KibanaHeapUtilization`	`OpenSearchDashboardsHeapUtilization`

Nome da métrica original	Novo nome
KibanaOS1MinuteLoad	OpenSearchDashboardsOS1MinuteLoad
KibanaRequestTotal	OpenSearchDashboardsRequestTotal
KibanaResponseTimesMaxInMillis	OpenSearchDashboardsResponseTimesMaxInMillis
ESReportingFailedRequestSysErrCount	KibanaReportingFailedRequestSysErrCount
ESReportingRequestCount	KibanaReportingRequestCount
ESReportingFailedRequestUserErrCount	KibanaReportingFailedRequestUserErrCount
ESReportingSuccessCount	KibanaReportingSuccessCount
ElasticsearchRequests	OpenSearchRequests

Para obter uma lista completa das métricas que o OpenSearch Service envia para o Amazon CloudWatch, consulte the section called “Monitoramento de métricas de cluster”.

Abra o console do Billing and Cost Management.

Os dados históricos presentes no console do Billing and Cost Management e do Cost and Usage Reports continuarão a usar o nome do serviço antigo. Por isso, você precisará começar a usar filtros tanto para o Amazon OpenSearch Service, quanto para o Elasticsearch legado ao procurar dados. Se você já tiver relatórios salvos, atualize os filtros para garantir que eles também incluam o OpenSearch Service. Inicialmente, você poderá receber um alerta quando seu uso diminuir para o Elasticsearch e aumentar para o OpenSearch, mas ele desaparecerá após alguns dias.

Além do nome do serviço, os campos a seguir serão alterados para todos os relatórios, listas e operações de API de lista de preços:

Campo	Formato antigo	Formato de linha
Tipo de instância	`m5.large.elasticsearch`	`m5.large.search`
Família de produtos	Instância do Elasticsearch Volume do Elasticsearch	Instância do Amazon OpenSearch Service Volume do Amazon OpenSearch Service
Descrição dos preços	5,098 USD por hora de instância c5.18xlarge.elasticsearch (ou hora parcial), UE	5,098 USD por hora de instância c5.18xlarge.search (ou hora parcial), UE
Família de instâncias	`ultrawarm.elasticsearch`	`ultrawarm.search`

Novo formato dos eventos

O formato dos eventos que o OpenSearch Service envia para o Amazon EventBridge e o Amazon CloudWatch mudou, especificamente o campo `detail-type`. O campo de origem (`aws.es`) permanece o mesmo. Para obter o formato completo de cada tipo de evento, consulte the section called “Eventos de monitoramento”. Se você tiver regras de evento existentes que dependem do formato antigo, atualize-as para que estejam em conformidade com o novo formato.

O que não mudou?

Os seguintes recursos e funcionalidades, entre outros não listados, permanecerão os mesmos:

- Entidade principal do serviço (`es.amazonaws.com`)
- Código do fornecedor
- ARNs de domínio
- Endpoints de domínio

Comece a usar: atualize os seus domínios para a versão 1.x do OpenSearch

A versão 1.x do OpenSearch é compatível com atualizações das versões 6.8 e 7.x do Elasticsearch. Para obter instruções sobre como atualizar seu domínio, consulte the section called “Iniciar uma atualização (console)”. Se você estiver usando a AWS CLI ou a API de configuração para atualizar seu domínio, você precisará especificar o `TargetVersion` como `OpenSearch_1.x`.

A versão 1.x do OpenSearch introduz uma configuração de domínio adicional chamada Enable compatibility mode (Habilitar modo de compatibilidade). Como alguns clientes e plugins do Elasticsearch OSS verificam a versão do cluster antes de se conectarem, o modo de compatibilidade define o OpenSearch para relatar sua versão como 7.10 para que esses clientes continuem a funcionar.

Você pode habilitar o modo de compatibilidade ao criar domínios do OpenSearch pela primeira vez ou ao atualizar para o OpenSearch a partir de uma versão do Elasticsearch. Se não estiver definido, o parâmetro assumirá como padrão o valor `false` quando você criar um domínio e `true` quando você atualizar um domínio.

Para habilitar o modo de compatibilidade usando a API de configuração, defina `override_main_response_version` como `true`:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/upgradeDomain
{
  "DomainName": "domain-name",
  "TargetVersion": "OpenSearch_1.0",
  "AdvancedOptions": {
    "override_main_response_version": "true"
   }
}
```

Para habilitar ou desabilitar o modo de compatibilidade em domínios do OpenSearch existentes, é necessário usar a operação _cluster/settings da API do OpenSearch:

```
PUT /_cluster/settings
{
  "persistent" : {
    "compatibility.override_main_response_version" : true
  }
```

```
}
```

Solução de problemas do Amazon OpenSearch Service

Esta seção descreve como identificar e resolver problemas comuns do Amazon OpenSearch Service. Consulte as informações nesta seção antes de entrar em contato com o AWS Support.

Não é possível acessar o OpenSearch Dashboards

O endpoint do OpenSearch Dashboards não oferece suporte a solicitações assinadas. Se a política de controle de acesso do seu domínio apenas concede acesso a determinados perfis do IAM e, se você não tiver configurado a autenticação do Amazon Cognito, poderá receber a seguinte mensagem de erro ao tentar acessar o Dashboards:

```
"User: anonymous is not authorized to perform: es:ESHttpGet"
```

Se o domínio do OpenSearch Service usar o acesso da VPC, talvez você não receba esse erro, mas o tempo limite da solicitação poderá ser excedido. Para saber mais sobre como corrigir esse problema e as várias opções de configuração disponíveis, consulte the section called “Controle do acesso aos OpenSearch painéis”, the section called “Sobre políticas de acesso em domínios da VPC” e the section called “Identity and Access Management”.

Não é possível acessar o domínio da VPC

Consulte the section called “Sobre políticas de acesso em domínios da VPC” e the section called “Teste dos domínios da VPC”.

Cluster no estado somente leitura

Em comparação com versões anteriores do Elasticsearch, o OpenSearch e o Elasticsearch 7.xusam um sistema diferente para coordenação de clusters. Nesse novo sistema, quando o cluster perde quorum, o cluster fica indisponível até que você execute uma ação. A perda de quorum pode assumir duas formas:

- Se o cluster usar nós principais dedicados, a perda de quorum ocorrerá quando a metade ou mais estiverem indisponíveis.
- Se o cluster não usar nós principais dedicados, a perda de quorum ocorrerá quando a metade ou mais dos seus nós de dados estiverem indisponíveis.

Se ocorrer perda de quorum e seu cluster tiver mais de um nó, o OpenSearch Service restaurará o quorum e colocará o cluster em um estado somente leitura. Você tem duas opções:

- Remover o estado somente leitura e usar o cluster no estado em que se encontra.
- Restaure o cluster ou os índices individuais de um snapshot.

Se você preferir usar o cluster no estado em que se encontra, verifique se a integridade do cluster está verde usando a seguinte solicitação:

```
GET _cat/health?v
```

Se a integridade do cluster for vermelha, recomendamos restaurar o cluster a partir de um snapshot. Você também poderá consultar the section called “Status de cluster vermelho” para ver as etapas de solução de problemas. Se a integridade do cluster estiver verde, verifique se todos os índices esperados estão presentes usando a seguinte solicitação:

```
GET _cat/indices?v
```

Execute algumas pesquisas para verificar se os dados esperados estão presentes. Se estiverem, você poderá remover o estado somente leitura usando a seguinte solicitação:

```
PUT _cluster/settings
{
  "persistent": {
    "cluster.blocks.read_only": false
  }
}
```

Se houver perda de quorum e seu cluster tiver apenas um nó, o OpenSearch Service substituirá o nó e não colocará o cluster em um estado somente leitura. Caso contrário, suas opções serão as mesmas: usar o cluster no estado em que se encontra ou restaurar a partir de um snapshot.

Em ambas as situações, o OpenSearch Service envia dois eventos para seu AWS Health Dashboard. O primeiro informa sobre a perda de quorum. O segundo ocorre depois que o OpenSearch Service restaura o quorum com êxito. Para obter mais informações sobre como usar o AWS Health Dashboard, consulte o Manual do usuário do AWS Health.

Status de cluster vermelho

Um status de cluster vermelho significa que pelo menos um fragmento principal e suas réplicas não estão alocados a um nó. O OpenSearch Service continua tentando obter snapshots automatizados de todos os índices, independentemente do seu status, mas os snapshots falharão enquanto o status de cluster vermelho persistir.

As causas mais comuns do status vermelho para o cluster são nós de cluster que apresentam falha e o travamento do processamento do OpenSearch devido a uma carga contínua de processos pesados.

> **Note**
>
> O OpenSearch Service armazena snapshots automatizados por 14 dias, independentemente do status do cluster. Portanto, se o status de cluster vermelho persistir por mais de duas semanas, o último snapshot automatizado saudável será excluído e você poderá perder permanentemente os dados do seu cluster. Se o seu domínio do OpenSearch Service entrar em um status de cluster vermelho, o AWS Support poderá entrar em contato com você para perguntar se deseja resolver o problema por conta própria ou se deseja que a equipe de suporte ajude. Você também pode definir um alarme do CloudWatch para notificá-lo quando um status de cluster vermelho ocorrer.

Em última análise, fragmentos vermelhos resultam em clusters vermelhos e índices vermelhos, em fragmentos vermelhos. Para identificar os índices que estão gerando o status de cluster vermelho, o OpenSearch tem algumas APIs úteis.

- `GET /_cluster/allocation/explain` escolhe o primeiro fragmento sem atribuição que ele encontrar e explica por que ele não pode ser alocado para um nó:

```
{
    "index": "test4",
    "shard": 0,
    "primary": true,
    "current_state": "unassigned",
    "can_allocate": "no",
    "allocate_explanation": "cannot allocate because allocation is not permitted to
 any of the nodes"
}
```

- `GET /_cat/indices?v` mostra o status de integridade, o número de documentos e o uso do disco para cada índice:

```
health status index           uuid                   pri rep docs.count docs.deleted
 store.size pri.store.size
green  open   test1           30h1EiMvS5uAFr2t5CEVoQ   5   0        820            0
       14mb           14mb
green  open   test2           sdIxs_WDT56afFGu5KPbFQ   1   0          0            0
       233b           233b
green  open   test3           GGRZp_TBRZuSaZpAGk2pmw   1   1          2            0
     14.7kb          7.3kb
red    open   test4           BJxfAErbTtu5HBjIXJV_7A   1   0
green  open   test5           _8C6MIXOSxCqVYicH3jsEA   1   0          7            0
     24.3kb         24.3kb
```

A exclusão de índices vermelhos é a maneira mais rápida de corrigir um status de cluster vermelho. Dependendo do motivo para o status de cluster vermelho, você pode escalar o domínio do OpenSearch Service para usar tipos de instância maiores, um maior número de instâncias ou mais armazenamento do EBS e tentar recriar os índices problemáticos.

Se a exclusão de um índice problemático não for viável, você pode restaurar um snapshot, excluir documentos do índice, alterar as configurações de índice, reduzir o número de réplicas ou excluir outros índices para liberar espaço em disco. A etapa importante é resolver o status de cluster vermelho antes de reconfigurar o domínio do OpenSearch Service. A reconfiguração de um domínio com um status de cluster vermelho pode agravar o problema e fazer com que o domínio fique preso em um estado de configuração Em processamento até que você resolva o status.

Correção automática de clusters vermelhos

Se o status do cluster ficar continuamente vermelho por mais de uma hora, o OpenSearch Service tentará corrigi-lo automaticamente redirecionando fragmentos não alocados ou restaurando instantâneos anteriores.

Se ele não corrigir um ou mais índices vermelhos e o status do cluster permanecer vermelho por um total de 14 dias, o OpenSearch Service tomará medidas adicionais somente se o cluster atender a pelo menos um dos seguintes critérios:

- Tem apenas uma zona de disponibilidade
- Nós principais dedicados

- Contém tipos de instância intermitentes (T2 ou T3)

Neste momento, se seu cluster atender a um desses critérios, o OpenSearch Service enviará notificações diárias nos próximos 7 dias explicando que, se você não corrigir esses índices, todos os fragmentos não atribuídos serão excluídos. Se o status do cluster ainda estiver vermelho após 21 dias, o OpenSearch Service excluirá os fragmentos não atribuídos (armazenamento e computação) em todos os índices vermelhos. Você pode visualizar notificações no painel Notificações do console do OpenSearch Service. Para obter mais informações, consulte the section called “Eventos de integridade do cluster”.

Recuperação de uma carga contínua de processamento pesado

Para determinar se um status de cluster vermelho deve-se a uma carga contínua de processamento pesado em um nó de dados, monitore as métricas de cluster a seguir.

Métrica relevante	Descrição	Recuperação
JVMMemoryPressure	Especifica a porcentagem do heap do Java usada para todos os nós de dados em um cluster. Visualize a estatística Máximo para essa métrica e procure quedas ainda menores na pressão de memória enquanto o coletor de lixo Java falhar na recuperação de memória suficiente. Esse padrão provavelmente se deve a consultas complexas ou a campos de dados grandes. Os tipos de instância x86 usam o coletor de lixo Concurrent Mark Sweep (CMS), que é executado junto com os threads da aplicação para manter as pausas curtas. Se o CMS não conseguir recuperar memória suficiente durante suas coletas normais, ele acionará uma	Defina disjuntores de memória para JVM. Para obter mais informações, consulte the section called “OutOfMemoryError em JVM”. Se o problema persistir, exclua índices desnecessários, reduza o número ou a complexidade das solicitações para o domínio, adicione instâncias ou use tipos de instância maiores.

Métrica relevante	Descrição	Recuperação
	coleta de resíduos completa, o que pode levar a longas pausas na aplicação e afetar a estabilidade do cluster. Os tipos de instância Graviton baseados em ARM usam o coletor de lixo Garbage-First (G1), que é semelhante ao CMS, mas usa pausas curtas adicionais e desfragmentação de pilha para reduzir ainda mais a necessidade de coleções de lixo completas. Em ambos os casos, se o uso da memória continuar a crescer além do que o coletor de lixo pode recuperar durante as coleções de lixo completas, o OpenSearch falha com um erro de memória insuficiente. Em todos os tipos de instância, uma boa regra prática é manter o uso abaixo de 80%. A API `_nodes/stats/jvm` oferece um resumo útil das estatísticas do JVM, do uso do grupo de memórias e das informações sobre coleta de lixo: `GET domain-endpoint /_nodes/stats/jvm?pretty`	

Métrica relevante	Descrição	Recuperação
CPUUtilization	Especifica a porcentagem de recursos da CPU usados para nós de dados em um cluster. Visualize a estatística Maximum para essa métrica e procure um padrão contínuo de uso intenso.	Adicione nós de dados ou aumente o tamanho dos tipos de instância dos nós de dados existentes.
Nós	Especifica o número de nós em um cluster. Visualize a estatísti ca Mínimo para essa métrica. Esse valor oscila quando o serviço implanta uma nova frota de instância s para um cluster.	Adicione nós de dados.

Status de cluster amarelo

O status de cluster amarelo significa que os fragmentos principais de todos os índices estão alocados a nós em um cluster, mas os fragmentos de réplica de pelo menos um índice não. Os clusters de nó único sempre inicializam com um status de cluster amarelo porque não existe nenhum outro nó ao qual o OpenSearch Service possa atribuir uma réplica. Para obter o status de cluster verde, aumente a contagem de nós. Para obter mais informações, consulte the section called “Dimensionamento de domínios”.

Clusters de vários nós podem ter brevemente um status de cluster amarelo após a criação de um novo índice ou após uma falha de nó. Esse status se resolve automaticamente à medida que o OpenSearch replica dados em todo o cluster. A falta de espaço em disco também pode causar status de cluster amarelo; o cluster só poderá distribuir fragmentos de réplica se os nós tiverem espaço em disco para acomodá-los.

ClusterBlockException

Você pode receber um erro `ClusterBlockException` pelos motivos a seguir.

Falta de espaço de armazenamento disponível

Se um ou mais nós em seu cluster tiverem espaço de armazenamento inferior ao valor mínimo de 1) 20% do espaço de armazenamento disponível, ou 2) 20 GB de espaço de armazenamento, as operações básicas de gravação, como a adição de documentos e a criação de índices, poderão começar a falhar. O the section called “Cálculo de requisitos de armazenamento” fornece um resumo de como o OpenSearch Service usa o espaço em disco.

Para evitar problemas, monitore a métrica `FreeStorageSpace` no console do OpenSearch Service e crie alarmes do CloudWatch para serem acionados quando o `FreeStorageSpace` se tornar inferior a um determinado limite. O `GET /_cat/allocation?v` também fornece um resumo útil de alocação de fragmentos e do uso do disco. Para resolver problemas associados à falta de espaço de armazenamento, dimensione o domínio do OpenSearch Service para usar tipos de instância maiores, um número maior de instâncias ou mais armazenamento baseado no EBS.

Alta pressão da memória da JVM

Quando a métrica JVMMemoryPressure excede 92% por 30 minutos, o OpenSearch Service aciona um mecanismo de proteção e bloqueia todas as operações de gravação para impedir que o cluster entre no status vermelho. Quando a proteção é ativada, as operações de gravação falham devido ao erro `ClusterBlockException`, novos índices não podem ser criados e o erro `IndexCreateBlockException` é lançado.

Quando a métrica JVMMemoryPressure retorna para 88% ou menos durante cinco minutos, a proteção é desativada e as operações de gravação no cluster são desbloqueadas.

A alta pressão da memória da JVM pode ser causada por picos no número de solicitações ao cluster, alocações de fragmentos não equilibradas entre os nós, excesso de fragmentos em um cluster, explosões de mapeamento de índices ou dados de campo ou tipos de instâncias que não conseguem administrar as cargas recebidas. Também pode ser causada pelo uso de agregações, curingas ou amplos intervalos de tempo nas consultas.

Para reduzir o tráfego para o cluster e resolver problemas de alta pressão da memória da JVM, experimente uma ou mais destas opções:

- Escale o domínio para que o tamanho máximo da pilha por nó seja de 32 GB.
- Reduza o número de fragmentos excluindo índices antigos ou não utilizados.
- Limpe o cache de dados com a operação da API `POST index-name/_cache/clear?fielddata=true`. Limpar o cache poderá interromper as consultas em andamento.

Em geral, para evitar a alta pressão da memória da JVM futuramente, siga estas práticas recomendadas:

- Evite agregações em campos de texto ou altere o tipo de mapeamento de seus índices para `keyword`.
- Otimize as solicitações de pesquisa e indexação escolhendo o número correto de fragmentos.
- Configure as políticas do Index State Management (ISM) para remover regularmente os índices não utilizados.

Erro ao migrar para multi-AZ com modo de espera

Os seguintes problemas podem ocorrer quando você migra um domínio existente para o Multi-AZ com modo de espera.

Criação de um índice, modelo de índice ou política do ISM durante a migração de domínios sem espera para domínios com modo de espera

Se você criar um índice ao migrar um domínio do Multi-AZ sem modo de espera para com modo de espera e o modelo de índice ou a política do ISM não seguir as diretrizes recomendadas de cópia de dados, isso pode causar uma inconsistência de dados e a migração pode falhar. Para evitar essa situação, crie o novo índice com uma contagem de cópias de dados (incluindo nós primários e réplicas) que seja múltipla de três. Você pode verificar o progresso da migração usando a API `DescribeDomainChangeProgress`. Se você encontrar um erro de contagem de réplicas, corrija o erro e entre em contato com o Suporte da AWS para tentar a migração novamente.

Número incorreto de cópias de dados

Se você não tiver o número certo de cópias de dados em seu domínio, a migração para o multi-AZ com modo de espera falhará.

OutOfMemoryError em JVM

Normalmente, `OutOfMemoryError` em JVM significa que um dos seguintes disjuntores para JVM foi atingido.

Disjuntor	Descrição	Propriedade de configuração de cluster
Disjuntor principal	Porcentagem total de memória do heap de JVM permitida para todos os disjuntores. O valor padrão é 95%.	`indices.breaker.total.limit`
Disjuntor de dados de campo	Porcentagem de memória do heap de JVM com permissão para carregar um único campo de dados na memória. O valor padrão é 40%. Se você carregar dados com campos grandes, talvez precise aumentar esse limite.	`indices.breaker.fielddata.limit`
Disjuntor de solicitações	Porcentagem de memória do heap de JVM permitida para estruturas de dados usados para responder a uma solicitação de serviço. O valor padrão é 60%. Se suas solicitações de serviço envolverem o cálculo de agregações, recomenda-se aumentar esse limite.	`indices.breaker.request.limit`

Nós de cluster com falha

As instâncias do Amazon EC2 podem experimentar encerramentos e reinicializações inesperados. Normalmente, o OpenSearch Service reinicia os nós para você. No entanto, é possível que um ou mais nós em um cluster do OpenSearch permaneçam em uma condição de falha.

Para verificar essa condição, abra o painel do domínio no console do OpenSearch Service. Escolha a guia Integridade do cluster e, em seguida, a métrica Total de nós. Veja se o número de nós relatado é inferior ao número que você configurou para seu cluster. Se a métrica mostrar que um ou mais nós estão inativos por mais de um dia, entre em contato com o AWS Support.

Você também pode definir um alarme do CloudWatch para ser notificado quando esse problema ocorrer.

> **Note**
>
> A métrica Total de nós não é precisa durante as alterações na configuração do cluster e durante a manutenção de rotina do serviço. Esse comportamento é esperado. A métrica logo informará o número correto de nós do cluster. Para saber mais, consulte the section called "Alterações de configuração".

Para proteger seus clusters contra encerramentos e reinicializações inesperados no nó, crie pelo menos uma réplica para cada índice no domínio do OpenSearch Service.

Limite máximo de fragmentos excedido

O OpenSearch e as versões 7.x do Elasticsearch têm uma configuração padrão de até 1.000 fragmentos por nó. O OpenSearch/ElasticSearch emitirá um erro se uma solicitação, como criar um novo índice, fizer com que você exceda esse limite. Se você encontrar esse erro, terá várias opções:

- Adicionar mais nós de dados ao cluster.
- Aumentar a configuração `_cluster/settings/cluster.max_shards_per_node`.
- Usar a API _shrink para reduzir o número de fragmentos no nó.

Domínio paralisado no estado de processamento

O seu domínio do OpenSearch Service entra no estado "Processing" (Processamento) ao executar uma alteração de configuração. Quando você iniciar uma alteração de configuração, o status do domínio será alterado para "Processing" (Processamento) enquanto o OpenSearch Service cria um novo ambiente. No novo ambiente, o OpenSearch Service inicia um novo conjunto de nós aplicáveis (como dados, primário ou UltraWarm). Após a conclusão da migração, os nós mais antigos são encerrados.

O cluster pode ficar paralisado no estado “Processing” (Processamento) caso alguma destas situações ocorra:

- Um novo conjunto de nós de dados não possa ser iniciado.

- A migração de fragmentos para o novo conjunto de nós de dados não seja bem-sucedida.
- Ocorreu uma falha na verificação de validação com erros.

Para obter etapas detalhadas de resolução em cada uma dessas situações, consulte Por que o meu domínio do Amazon OpenSearch Service está paralisado no estado “Processing” (Processamento)?.

O saldo de intermitência do EBS está baixo

O OpenSearch Service enviará para você uma notificação de console quando o saldo de intermitência do EBS em um de seus volumes de Finalidade geral (SSD) estiver abaixo de 70% e uma notificação de acompanhamento se o saldo cair abaixo de 20%. Para corrigir esse problema, você pode aumentar a escala verticalmente do cluster ou reduzir as IOPS de leitura e gravação para que o saldo de intermitência possa ser creditado. O saldo intermitente permanece em 0 para domínios com tipos de volume gp3 e domínios com volume gp2 cujo tamanho de volume seja superior a 1000 GiB. Para obter mais informações, consulte Volumes de Finalidade geral (SSD) (gp2). Você pode monitorar o equilíbrio de intermitência do EBS com a métrica do `BurstBalance` CloudWatch.

Não é possível habilitar logs de auditoria

Você poderá encontrar o seguinte erro ao tentar habilitar a publicação de logs de auditoria usando o console do OpenSearch Service:

A Política de Acesso de Recursos especificada para o grupo de CloudWatch Logs não concede permissões suficientes para o Amazon OpenSearch Service criar um fluxo de registro. Verifique a Política de acesso a recursos.

Se você encontrar esse erro, verifique se o elemento `resource` da sua política inclui o ARN do grupo de logs correto. Se isso acontecer, faça o seguinte:

1. Espere vários minutos.
2. Atualize a página em seu navegador da Web.

3. Escolha Selecionar grupo existente.
4. Em Grupo de logs existente, escolha o grupo de logs que você criou antes de receber a mensagem de erro.
5. Na seção de política de acesso, escolha Selecionar política existente.
6. Em Política existente, escolha a política que você criou antes de receber a mensagem de erro.
7. Escolha Habilitar.

Se o erro persistir após o processo ser repetido várias vezes, entre em contato com o AWS Support.

Não é possível fechar o índice

O OpenSearch Service oferece suporte à API `_close` apenas para o OpenSearch e o Elasticsearch versões 7.4 e posteriores. Se você estiver usando uma versão anterior e restaurando um índice de um snapshot, poderá excluir o índice existente (antes ou depois de reindexá-lo).

Verificações de licenças do cliente

As distribuições padrão do Logstash e Beats incluem uma verificação de licença proprietária e não conseguem se conectar à versão de código aberto do OpenSearch. Certifique-se de usar as distribuições Apache 2.0 (OSS) desses clientes com o OpenSearch Service.

Controle de utilização de solicitações

Se você receber erros `403 Request throttled due to too many requests` ou `429 Too Many Requests` persistentes, considere a escalabilidade vertical. O Amazon OpenSearch Service controla a utilização de solicitações em situações em que a carga útil faz com que o uso da memória exceda o tamanho máximo do heap de Java.

Não é possível executar o SSH no nó

Não é possível usar o SSH para acessar qualquer um dos nós em seu cluster do OpenSearch nem modificar `opensearch.yml` diretamente. Em vez disso, use o console, a AWS CLI ou SDKs para configurar o domínio. Você também pode especificar algumas configurações no nível do cluster usando as APIs REST do OpenSearch. Para saber mais, consulte Referência da API do Amazon OpenSearch Service e the section called “Operações compatíveis”.

Se você precisar de mais insights sobre a performance do cluster, poderá publicar logs de erro e logs lentos no CloudWatch.

Erro de snapshot "Not Valid for the Object's Storage Class" (Inválido para a classe de armazenamento do objeto)

Os snapshots do OpenSearch Service não são compatíveis com a classe de armazenamento do S3 Glacier. Você poderá encontrar esse erro ao tentar listar os snapshots se o bucket do S3 incluir uma regra de ciclo de vida que faça a transição de objetos para a classe de armazenamento do S3 Glacier.

Se você precisar restaurar um snapshot armazenado no bucket, restaure os objetos do S3 Glacier, copie-os em um novo bucket e registre o novo bucket como um repositório de snapshots.

Cabeçalho de host inválido

O OpenSearch Service exige que os clientes especifiquem `Host` nos cabeçalhos de solicitação. Um valor `Host` válido é o endpoint do domínio sem `https://`, como:

```
Host: search-my-sample-domain-ih2lhn2ew2scurji.us-west-2.es.amazonaws.com
```

Se você receber um erro `Invalid Host Header` quando fizer uma solicitação, verifique se o seu cliente ou proxy inclui o endpoint do domínio do OpenSearch Service (e não, por exemplo, seu endereço IP) no cabeçalho do `Host`.

Tipo de instância M3 inválido

O OpenSearch Service não oferece suporte à adição ou modificação de instâncias M3 em domínios existentes que executam o OpenSearch Service ou o Elasticsearch versão 6.7 ou posterior. Você pode continuar a usar instâncias M3 com o Elasticsearch 6.5 e anteriores.

Recomendamos escolher um tipo de instância mais recente. Para domínios que executam o OpenSearch ou Elasticsearch 6.7 ou posterior, a seguinte restrição é aplicável:

- Se o domínio existente não usar instâncias M3, você não poderá mais alterar para elas.
- Se você alterar um domínio existente de um tipo de instância M3 para outro tipo de instância, não será possível alternar novamente.

Consultas de alta atividade param de funcionar após a ativação do UltraWarm

Quando você habilita o UltraWarm em um domínio, se não houver substituições preexistentes para a configuração `search.max_buckets`, o OpenSearch Service definirá automaticamente o valor como `10000` para evitar que consultas com muita memória saturem nós de alta atividade. Se suas consultas de atividade muito alta usarem mais de 10.000 buckets, elas poderão parar de funcionar quando você habilitar o UltraWarm.

Como você não pode modificar essa configuração devido à natureza gerenciada do Amazon OpenSearch Service, é necessário abrir um caso de suporte para aumentar o limite. Os aumentos de limite não exigem uma assinatura do Premium Support.

Não é possível reverter para a versão anterior após a atualização.

As atualizações no local são irreversíveis, mas se você entrar em contato com o AWS Support, eles poderão ajudar a restaurar o snapshot automático anterior à atualização em um novo domínio. Por exemplo, se você atualizar um domínio do Elasticsearch 5.6 para 6.4, o AWS Support poderá ajudar a restaurar o snapshot anterior à atualização em um novo domínio do Elasticsearch 5.6. Se você tirou um snapshot manual do domínio original, pode realizar essa etapa por conta própria.

Resumo das necessidades de domínios para todas as Regiões da AWS

O script a seguir usa o comando describe-regions da AWS CLI do Amazon EC2 para criar uma lista de todas as regiões nas quais o OpenSearch Service pode estar disponível. Depois, ele chama list-domain-names para cada região:

```
for region in `aws ec2 describe-regions --output text | cut -f4`
do
    echo "\nListing domains in region '$region':"
    aws opensearch list-domain-names --region $region --query 'DomainNames'
done
```

Você recebe a seguinte saída para cada região:

```
Listing domains in region:'us-west-2'...
[
```

```
  {
    "DomainName": "sample-domain"
  }
]
```

As regiões nas quais o OpenSearch Service não está disponível retornam "Could not connect to the endpoint URL" (Não foi possível conectar ao URL do endpoint).

Erro do navegador ao usar o OpenSearch Dashboards

Seu navegador encapsula mensagens de erro do serviço em objetos de resposta HTTP quando você usa o Dashboards para visualizar dados em seu domínio do OpenSearch Service. Você pode usar ferramentas de desenvolvedor normalmente disponíveis em navegadores da web, como Modo de Desenvolvedor no Chrome, para visualizar erros de serviço subjacentes e auxiliar suas operações de depuração.

Para visualizar erros de serviço no Chrome

1. Na barra de menu superior do Chrome, escolha Visualizar, Desenvolvedor , Ferramentas do desenvolvedor.
2. Escolha a guia Network.
3. Na coluna Status, escolha qualquer sessão HTTP com status 500.

Para visualizar erros de serviço no Firefox

1. No menu, escolha Tools, Web Developer, Network.
2. Escolha qualquer sessão HTTP com status 500.
3. Escolha a guia Response para visualizar a resposta do serviço.

Distorção de armazenamento e de fragmentos do nó

A distorção de fragmentos de nós ocorre quando um ou mais nós em um cluster têm significativamente mais fragmentos do que os outros nós. A distorção de armazenamento de nós ocorre quando um ou mais nós em um cluster têm significativamente mais armazenamento (`disk.indices`) do que os outros nós. Embora essas duas condições possam ocorrer temporariamente, como quando um domínio substituiu um nó e ainda está alocando fragmentos a ele, você deve resolvê-las se elas persistirem.

Para identificar os dois tipos de distorção, execute a operação _cat/allocation da API e compare as entradas `shards` e `disk.indices` na resposta:

```
shards    | disk.indices  | disk.used  | disk.avail   | disk.total   | disk.percent |
host     | ip       | node
   264    |      465.3mb  |   229.9mb  |      1.4tb   |      1.5tb   |            0 |
 x.x.x.x  | x.x.x.x  | node1
   115    |        7.9mb  |    83.7mb  |     49.1gb   |     49.2gb   |            0 |
x.x.x.x  | x.x.x.x  | node2
   264    |      465.3mb  |   235.3mb  |      1.4tb   |      1.5tb   |            0 |
 x.x.x.x  | x.x.x.x  | node3
   116    |        7.9mb  |    82.8mb  |     49.1gb   |     49.2gb   |            0 |
x.x.x.x  | x.x.x.x  | node4
   115    |        8.4mb  |      85mb  |     49.1gb   |     49.2gb   |            0 |
x.x.x.x  | x.x.x.x  | node5
```

Embora alguma distorção de armazenamento seja normal, qualquer coisa 10% acima da média é significativa. Quando a distribuição de fragmentos é distorcida, o uso da CPU, da rede e da largura de banda do disco também pode ficar distorcido. Como mais dados geralmente significam mais operações de indexação e pesquisa, os nós mais pesados também tendem a ser os nós com mais recursos, enquanto os nós mais leves representam capacidade subutilizada.

Correção: use contagens de fragmentos que sejam múltiplos da contagem de nós de dados para garantir que cada índice seja distribuído uniformemente entre os nós de dados.

Distorção de armazenamento e de fragmentos de índices

A distorção de fragmentos de índices ocorre quando um ou mais nós retêm mais fragmentos de um índice do que os outros nós. A distorção de armazenamento de índices ocorre quando um ou mais nós retêm uma quantidade desproporcionalmente grande do armazenamento total de um índice.

A distorção de índices é mais difícil de identificar do que a distorção de nós porque requer alguma manipulação da saída da API _cat/shards. Investigue a distorção de índices se houver alguma indicação de distorção nas métricas do cluster ou do nó. Estas são indicações comuns de distorção de índices:

- Erros HTTP 429 que ocorrem em um subconjunto de nós de dados
- Índice desigual ou enfileiramento de operações de pesquisa nos nós de dados
- Heap da JVM e/ou utilização da CPU desigual nos nós de dados

Correção: use contagens de fragmentos que sejam múltiplos da contagem de nós de dados para garantir que cada índice seja distribuído uniformemente entre os nós de dados. Se você ainda vir distorção de armazenamento ou de fragmentos de índices, talvez seja necessário realizar uma realocação de fragmentos de forma forçada, que ocorre com cada implantação azul/verde do domínio do OpenSearch Service.

Operação não autorizada após a seleção do acesso via VPC

Ao criar um novo domínio usando o console do OpenSearch Service, você tem a opção de escolher acesso via VPC ou público. Se você escolher Acesso via VPC, o OpenSearch Service realizará consultas para obter informações da VPC e falhará se você não tiver as permissões adequadas:

```
You are not authorized to perform this operation. (Service: AmazonEC2; Status Code:
 403; Error Code: UnauthorizedOperation
```

Para habilitar esta consulta, você deve ter acesso às operações `ec2:DescribeVpcs`, `ec2:DescribeSubnets` e `ec2:DescribeSecurityGroups`. Esse requisito se aplica somente ao console. Se você usar a AWS CLI para criar e configurar um domínio com um endpoint da VPC, não precisará de acesso a essas operações.

Preso no carregamento após a criação do domínio da VPC

Depois de criar um novo domínio que usa o acesso da VPC, o Estado de configuração do domínio pode ficar travado em Carregando. Se esse problema ocorrer, provavelmente o AWS Security Token Service (AWS STS) está desativado para a sua região.

Para adicionar endpoints da VPC à sua VPC, o OpenSearch Service precisa assumir a função `AWSServiceRoleForAmazonOpenSearchService`. Assim, o AWS STS deve ser ativado para criar novos domínios que usam acesso da VPC em uma determinada região. Para saber mais sobre a habilitação e a desabilitação do AWS STS, consulte o Manual do usuário do IAM.

Solicitações negadas às APIs do OpenSearch

Com a introdução do controle de acesso baseado em tags para as APIs do OpenSearch, você pode começar a ver erros de acesso negado pela primeira vez. Isso pode ocorrer porque uma ou mais de suas políticas de acesso contém `Deny` usando a condição `ResourceTag`, e essas condições agora estão sendo aplicadas.

Por exemplo, a política antigamente só negava acesso à ação `CreateDomain` da API de configuração quando o domínio tinha a tag`environment=production`. Mesmo que a lista de ações também incluísse `ESHttpPut`, a declaração de negação não se aplicava a essa ação ou a qualquer outras ações `ESHttp*`.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "es:CreateDomain",
      "es:ESHttpPut"
    ],
    "Effect": "Deny",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:ResourceTag/environment": [
          "production"
        ]
      }
    }
  }]
}
```

Com o suporte adicional de tags para métodos HTTP do OpenSearch, uma política baseada em identidade do IAM, como a acima, negará o acesso do usuário anexado à ação `ESHttpPut`. Anteriormente, na ausência de validação de tags, o usuário anexado ainda teria conseguido enviar solicitações PUT.

Se você começar a encontrar erros de acesso negado após atualizar os domínios para o software de serviço R20220323 ou posterior, verifique as políticas de acesso baseadas em identidade para ver se o caso descrito aqui está ocorrendo e atualize-as, se necessário, para permitir o acesso.

Não é possível conectar via Alpine Linux

O Alpine Linux limita o tamanho da resposta DNS a 512 bytes. Se você tentar conectar ao domínio do OpenSearch Service via Alpine Linux, versão 3.18.0 ou inferior, a resolução de DNS pode falhar se o domínio estiver em uma VPC e contiver mais de 20 nós. Se você usa uma versão Alpine Linux superior à 3.18.0, você deve ser capaz de resolver mais de 20 hosts. Para obter mais informações, consulte notas de lançamento do Alpine Linux 3.18.0.

Se seu domínio estiver em uma VPC, recomendamos usar outras distribuições Linux, como Debian, Ubuntu, CentOS, Red Hat Enterprise Linux ou Amazon Linux 2, para conectar a ele.

Muitas solicitações de pesquisa de contrapressão

O controle de admissão baseado em CPU é um mecanismo de controle que limita proativamente o número de solicitações a um nó com base em sua capacidade atual, tanto para aumentos orgânicos quanto para picos de tráfego. Solicitações excessivas retornam um código de status HTTP 429 “Muitas solicitações” após a rejeição. Esses erros indicam recursos de cluster insuficientes, solicitações de pesquisa que consomem muitos recursos ou um aumento não intencional na workload.

A contrapressão de pesquisa fornece o motivo da rejeição, o que pode ajudar a ajustar solicitações de pesquisa que consomem muitos recursos. Para picos de tráfego, recomendamos novas tentativas do lado do cliente com recuo e instabilidade exponenciais.

Erro de certificado ao usar o SDK

Como os AWS SDKs usam os certificados de CA do computador, as alterações feitas nos certificados nos servidores da AWS podem provocar falhas de conexão quando você tenta usar um SDK. As mensagens de erro variam, mas geralmente contêm o seguinte texto:

```
Failed to query OpenSearch
...
SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
```

Você pode impedir essas falhas mantendo os certificados de CA do computador e o sistema operacional atualizados. Se encontrar esse problema em um ambiente corporativo e não gerenciar seu computador, talvez tenha de pedir a um administrador para auxiliá-lo no processo de atualização.

A lista a seguir mostra as versões mínimas de sistema operacional e Java:

- As versões do Microsoft Windows que têm atualizações de janeiro de 2005 ou superiores instaladas contêm pelo menos uma das CAs necessárias em sua lista de confiança.
- O Mac OS X 10.4 com Java para Mac OS X 10.4 Release 5 (fevereiro de 2007), Mac OS X 10.5 (outubro de 2007) e versões superiores contêm pelo menos uma das CAs necessárias em sua lista de confiança.

- O Red Hat Enterprise Linux 5 (março de 2007), 6 e 7 e o CentOS 5, 6 e 7 contêm pelo menos uma das CAs necessárias em sua lista de CAs confiáveis padrão.
- Java 1.4.2_12 (maio de 2006), 5 Update 2 (março de 2005) e todas as versões mais recentes, como Java 6 (dezembro de 2006), 7 e 8, contêm pelo menos uma das CAs necessárias em sua lista de CAs confiáveis padrão.

As três autoridades de certificação são:

- Amazon Root CA 1
- Starfield Services Root Certificate Authority – G2
- Starfield Class 2 Certification Authority

Os certificados raiz das duas primeiras autoridades estão disponíveis em Amazon Trust Services, mas manter o computador atualizado é a solução mais simples. Para saber mais sobre os certificados fornecidos pelo ACM, consulte Perguntas frequentes sobre o AWS Certificate Manager.

> **Note**
>
> No momento, os domínios do OpenSearch Service na região us-east-1 usam certificados de uma autoridade diferente. Pretendemos atualizar a região para usar essas novas autoridades de certificação em um futuro próximo.

Histórico de documentos do Amazon OpenSearch Service

Este tópico descreve mudanças importantes no Amazon OpenSearch Service. As atualizações de software de serviço adicionam suporte a novos recursos, patches de segurança, correções de bugs e outras melhorias. Para usar novos recursos, talvez seja necessário atualizar o software de serviço em seu domínio. Para ter mais informações, consulte the section called “Atualizações de software de serviço”.

Os recursos do serviço são implementados de forma incremental até Regiões da AWS onde o serviço está disponível. Atualizamos esta documentação apenas para a primeira versão. Não fornecemos informações sobre a disponibilidade da região nem anunciamos lançamentos subsequentes da região. Para obter informações sobre a disponibilidade de recursos do serviço na região e para assinar notificações sobre atualizações, consulte O que há de novo em AWS?

Datas relevantes para o histórico:

- Versão atual do produto: 2021-01-01
- Última versão do produto — 1º de abril de 2024
- Última atualização da documentação — 1º de abril de 2024

Para receber notificações sobre atualizações, inscreva-se no feed RSS.

> **Note**
>
> Lançamentos de patches: versões de software de serviço que terminam em “-P” e um número, como R20211203-P4, são lançamentos de patches. É provável que os patches incluam melhorias de performance, pequenas correções de bugs e correções de segurança ou melhorias de postura. Como os patches não incluem novos recursos ou as últimas alterações, eles geralmente não têm impacto direto no usuário ou na documentação e, por isso, as especificidades de cada patch não estão incluídas neste histórico de documentos.

Alteração	Descrição	Data
Suporte da Amazon OpenSearch Ingestion para Data Prepper versão 2.7	O Amazon OpenSearch Ingestion adiciona suporte à versão 2.7 do Data Prepper.	4 de abril de 2024

	Para obter mais informações, consulte as notas de versão 2.7.	
AWS service (Serviço da AWS) acesso privado para coleções sem OpenSearch servidor	Agora você pode conceder acesso específico Serviços da AWS, como o Amazon Bedrock, às suas coleções OpenSearch sem servidor dentro de uma política de acesso à rede.	28 de março de 2024
Atualizações do EBS no local	Agora você pode fazer algumas alterações no EBS em seus domínios sem uma implantação azul/verde no Amazon Service. OpenSearch	14 de fevereiro de 2024
Visibilidade da mudança de configuração	Agora você pode acompanha r as alterações na configura ção do domínio no console do Amazon OpenSearch Service e usando a API de configura ção.	6 de fevereiro de 2024

Disponibilidade geral das coleções de pesquisa vetorial	As coleções de pesquisa vetorial do Amazon OpenSearch Serverless agora estão disponíveis ao público em geral. As melhorias a seguir foram feitas durante a fase de pré-visualização: • Coleções de pesquisa vetorial agora oferecem suporte a workloads com bilhões de vetores, cada um com até 128 dimensões. • OpenSearch Os painéis agora oferecem suporte a coleções de pesquisa vetorial.	29 de novembro de 2023
Instâncias OR1	O Amazon OpenSearch Service agora oferece suporte aos tipos de instância OR1.	29 de novembro de 2023
Consultas diretas com o Amazon S3 (demonstração)	As consultas diretas fornecem uma solução totalmente gerenciada para disponibi lizar dados transacionais no Amazon OpenSearch Service em segundos após serem gravados em um bucket do Amazon S3.	29 de novembro de 2023

Capacidade de 10 TiB para coleções de séries temporais	O Amazon OpenSearch Serverless adiciona suporte para até 10 TiB de dados de índice para coleções de séries temporais. Essa versão também é compatível com uma capacidade máxima permitida de 200 OCUs para todos os tipos de coleções e a capacidade de desabilitar réplicas em espera ao criar uma coleção.	29 de novembro de 2023
OpenSearch Suporte 2.11	O Amazon OpenSearch Service agora oferece suporte à OpenSearch versão 2.11. Essa versão inclui todos os recursos que faziam parte das versões 2.10 e 2.11. Para obter mais informações, consulte as notas de release 2.10 e 2.11.	17 de novembro de 2023
Suporte da Amazon OpenSearch Ingestion para Data Prepper versão 2.6	O Amazon OpenSearch Ingestion adiciona suporte à versão 2.6 do Data Prepper. Para obter mais informaçõ es, consulte as notas de versão 2.6. Além disso, você pode especificar o Amazon DynamoDB como uma fonte de pipeline. Para obter mais informações, consulte Uso de um pipeline de OpenSearc h ingestão com o Amazon DynamoDB.	17 de novembro de 2023

Suporte da Amazon OpenSearch Ingestion para Data Prepper versão 2.5	O Amazon OpenSearch Ingestion adiciona suporte para a versão 2.5 do Data Prepper. Para obter mais informações, consulte as notas de lançamento da versão 2.5. Além disso, agora você pode especific ar um domínio OpenSearch de serviço ou uma coleção OpenSearch sem servidor como fonte de pipeline. Para obter mais informaçõ es, consulte o plug-in de OpenSearch origem na documentação do Data Prepper.	17 de novembro de 2023
CloudFormation modelo para inferência remota	Para facilitar a configura ção da inferência remota para pesquisa semântica, o Amazon OpenSearch Service fornece um AWS CloudForm ation modelo no console que automatiza o processo de provisionamento do modelo para você.	7 de novembro de 2023

Atualizar política de função vinculada ao serviço	Adiciona as permissões necessárias para que a política de função vinculada ao serviço `AmazonOpenSearchServiceRolePolicy` atribua e cancele a atribuição de endereços IPv6. A política obsoleta do Elasticsearch `AmazonElasticsearchServiceRolePolicy` também foi atualizada para garantir a compatibilidade com versões anteriores.	26 de outubro de 2023
Políticas de ciclo de vida do Amazon OpenSearch Serverless	O Amazon OpenSearch Serverless introduz políticas de ciclo de vida de índices para simplificar o gerenciamento da retenção e exclusão de dados. Agora você pode usar APIs ou uma interface de configuração no console para definir políticas de retenção de dados para coletas de séries temporais, eliminando a necessidade de criar índices diários ou scripts para excluir dados antigos.	25 de outubro de 2023

Suporte à instância Im4gn	O Amazon OpenSearch Service agora oferece suporte aos tipos de instância IM4gn. As instâncias Im4gn são otimizadas para cargas de trabalho que gerenciam grandes conjuntos de dados e precisam de alta densidade de armazenamento por vCPU.	20 de outubro de 2023
Opções administrativas	O Amazon OpenSearch Service agora oferece várias opções administrativas que fornecem controle granular se você precisar solucionar problemas com seu domínio. Essas opções incluem a capacidade de reiniciar o OpenSearch processo em um nó de dados e a capacidade de reiniciar um nó de dados.	17 de outubro de 2023
Plug-ins opcionais	O Amazon OpenSearch Service adiciona suporte para quatro novos plug-ins de análise de linguagem: Nori (coreano), Sudachi (japonês) , Pinyin (chinês) e STConvert Analysis (chinês), bem como o plug-in Amazon Personalize Search Ranking.	16 de outubro de 2023

OpenSearch 2.9 suporte	O Amazon OpenSearch Service agora oferece suporte à OpenSearch versão 2.9. Essa versão inclui todos os recursos que faziam parte das versões 2.8 e 2.9. Para obter mais informações, consulte as notas de release 2.8 e 2.9.	2 de outubro de 2023
Conectores ML	O Amazon OpenSearch Service adiciona suporte para conectores de aprendizado de máquina (ML). Os conectores facilitam o acesso a modelos de ML hospedados em outras Serviços da AWS plataformas de aprendizado de máquina (ML) ou em plataformas de aprendizado de máquina (ML) de terceiros.	6 de setembro de 2023
Amazon OpenSearch Ingestion adiciona suporte à versão 2.4 do Data Prepper	O Amazon OpenSearch Ingestion adiciona suporte à versão 2.4 do Data Prepper. Para obter mais informaçõ es, consulte as notas de lançamento da versão 2.4. Além disso, agora você pode especificar Amazon Managed Streaming for Apache Kafka (Amazon MSK) como fonte de pipeline.	31 de agosto de 2023

Capacidade de 6 TiB para coleções de séries temporais	O Amazon OpenSearch Serverless adiciona suporte para até 6 TiB de dados de índice para coleções de séries temporais. Essa versão também é compatível com uma capacidade máxima permitida de 100 OCUs para pesquisas e coletas de séries temporais.	15 de agosto de 2023
Coleções de pesquisa vetorial	O Amazon OpenSearch Serverless adiciona a opção de criar uma coleção de pesquisa vetorial, que você pode usar para armazenar incorporações vetoriais para potencializar pesquisas semânticas e de similaridade.	26 de julho de 2023
OpenSearch Suporte 2.7	O Amazon OpenSearch Service agora oferece suporte à OpenSearch versão 2.7. Essa versão inclui todos os recursos que faziam parte das versões 2.6 e 2.7. Para obter mais informações, consulte as notas de release 2.6 e 2.7.	10 de julho de 2023

Suporte à versão 2.3 do Data Prepper	O Amazon OpenSearch Ingestion adiciona suporte ao Data Prepper versão 2.3. Para obter mais informaçõ es, consulte as notas de lançamento da versão 2.3. Além disso, agora você pode especificar o Amazon Security Lake como uma fonte de pipeline.	26 de junho de 2023
Multi-AZ com modo de espera	O Amazon OpenSearch Service adiciona a opção de implantar um domínio em três zonas de disponibilidade (AZs), com cada AZ contendo uma cópia completa dos dados e com os nós em uma dessas AZs atuando como standby. A opção de implantaç ão do multi-AZ com modo de espera fornece 99,99% de disponibilidade e desempenh o consistente no caso de uma falha na infraestrutura.	3 de maio de 2023
Nova função vinculada ao serviço	O Amazon OpenSearc h Service adiciona uma função vinculada ao serviço chamada`AWSServic eRoleForAmazonOpen SearchIngestion` , que permite que o Amazon OpenSearch Ingestion envie dados métricos para. Amazon CloudWatch	26 de abril de 2023

OpenSearch Ingestão da Amazon	O Amazon OpenSearch Ingestion é um coletor de dados totalmente gerenciado que fornece dados de log e rastreamento em tempo real para domínios de OpenSearch serviço e OpenSearch coleções sem servidor. OpenSearch A ingestão elimina a necessidade de usar soluções de terceiros, como Logstash ou Jaeger, para ingerir dados em seus domínios e coleções.	26 de abril de 2023
OpenSearch 2.5 suporte	O Amazon OpenSearch Service agora oferece suporte à OpenSearch versão 2.5. Essa versão inclui todos os recursos que faziam parte das versões 2.4 e 2.5. Para obter mais informações, consulte as notas de release 2.4 e 2.5.	13 de março de 2023

Janelas de manutenção fora do horário de pico	O Amazon OpenSearch Service adiciona janelas fora de pico, que são blocos de tempo diários de 10 horas e baixo tráfego, durante os quais ele pode agendar atualizaç ões de software do serviço e otimizações de ajuste automático que exigem uma implantação azul/verde. As atualizações fora do horário de pico ajudam a minimizar a sobrecarga nos nós principai s dedicados de um cluster durante períodos de maior tráfego. Para novos domínios criados após 16 de fevereiro, a janela fora do horário de pico é configurada automaticamente entre 22h e 8h, horário local. Para domínios existentes, você precisa habilitar a janela manualmente.	16 de fevereiro de 2023
Configurar a autenticação SAML durante a criação do domínio	O Amazon OpenSearch Service agora oferece suporte à configuração da autentica ção SAML durante a criação do domínio. Anteriormente, era necessário configurar as opções de SAML após a criação do domínio.	1° de fevereiro de 2023

Reindexação remota para domínios de VPC	O Amazon OpenSearch Service adiciona a opção de uma conexão de VPC endpoint entre dois domínios. Agora, você pode utilizar a reindexação remota para copiar índices de um domínio de VPC para outro sem um proxy reverso. Seus domínios de VPC devem estar executando o software de serviço R20221114 ou posterior para usar esse recurso.	31 de janeiro de 2023

Disponibilidade OpenSearch geral do Amazon Serverless	O Amazon OpenSearch Serverless agora está disponível ao público em geral. As melhorias a seguir foram feitas durante a fase de pré-visualização: • Agora, a capacidade pode ser reduzida para o mínimo de OCUs configurado quando há uma diminuição no tráfego no endpoint de coleta. • O máximo de OCUs permitido para indexação e pesquisa aumentou de 20 para 50. Cada OCU inclui armazenamento efêmero de atividade muito alta que é suficiente para 120 GiB de dados de indexação. • Agora, é possível definir as configurações de acesso aos dados ao criar coleções, em vez de configurá-las em um fluxo de trabalho separado.	25 de janeiro de 2023

Simulação assíncrona	O Amazon OpenSearch Service agora oferece suporte à execução seca assíncron a, que permite realizar uma verificação de validação antes de fazer uma alteração na configuração e notifica se suas alterações causarão uma implantação azul/verde.	19 de janeiro de 2023
Nova função vinculada ao serviço	O Amazon OpenSearc h Service adiciona uma função vinculada ao serviço chamada`AWSServic eRoleForAmazonOpen SearchServerless` , que permite que o OpenSearc h Serverless envie dados métricos para. Amazon CloudWatch	29 de novembro de 2022
OpenSearch Prévia do Amazon Serverless	O Amazon OpenSearch Serverless é uma configura ção sob demanda, com escalabilidade automátic a e sem servidor para o Amazon Service. OpenSearc h O Serverless remove as complexidades operacionais de provisionamento, configura ção e ajuste de seus clusters. OpenSearch	29 de novembro de 2022

OpenSearch 2.3 suporte	O Amazon OpenSearch Service agora oferece suporte à OpenSearch versão 2.3. Essa versão inclui todos os recursos que faziam parte das versões 2.0, 2.1 e 2.2. Para obter mais informações, consulte as notas de release 2.0, 2.1, 2.2 e 2.3. A versão 2.3 contém uma alteração significativa. Para obter mais informações, consulte Caminhos de atualização com suporte.	15 de novembro de 2022
Suporte ao plug-in Notifications	O Amazon OpenSearch Service agora oferece suporte ao plug-in Notifications, que oferece uma localização central para todas as notificações dos OpenSearch plug-ins. A partir da versão 2.0, os destinos de alerta foram descontinuados e substituídos por canais de notificação.	15 de novembro de 2022

Suporte ao Kibana 7.1.1	Os domínios do Amazon OpenSearch Service que executam o Elasticsearch 7.1 agora oferecem suporte à versão de patch mais recente do Kibana 7.1.1, que adiciona correções de bugs e melhora a segurança. Quando você atualiza seus domínios 7.1 para o software de serviço R20221114, o OpenSearch Service os atualizará automaticamente para esta versão de patch.	15 de novembro de 2022
Suporte ao Kibana 6.8.13	Os domínios do Amazon OpenSearch Service que executam o Elasticsearch 6.8 agora oferecem suporte à versão de patch mais recente do Kibana 6.8.13, que adiciona correções de bugs e melhora a segurança. Quando você atualiza seus domínios 6.8 para o software de serviço R20221114, o OpenSearch Service os atualizará automaticamente para esta versão de patch.	15 de novembro de 2022

Suporte ao Kibana 6.3.2	Os domínios do Amazon OpenSearch Service que executam o Elasticsearch 6.3 agora oferecem suporte à versão de patch mais recente do Kibana 6.3.2, que adiciona correções de bugs e melhora a segurança. Quando você atualiza seus domínios 6.3 para o software de serviço R20221114, o OpenSearch Service os atualizará automaticamente para esta versão de patch.	15 de novembro de 2022

AWS PrivateLink	Com os endpoints OpenSearch VPC gerenciados pelo Amazon Service, você pode se conectar diretamente aos domínios do Service OpenSearch VPC usando uma interface VPC endpoint em vez de se conectar pela Internet. Um OpenSearch VPC endpoint gerenciado por serviços pode ser acessado somente dentro da VPC em que o endpoint é provisionado ou de qualquer VPC emparelhada com a VPC em que o endpoint é provisionado, conforme permitido pelas tabelas de rotas e grupos de segurança. Seu domínio da VPC deve estar executando o software de serviço R20220928 ou posterior para se conectar a um endpoint da VPC de interface.	7 de novembro de 2022
Correções de erros e melhorias na performance	O software de serviço R20220928 inclui correções de bugs e aprimoramentos de desempenho, incluindo registro SAML aprimorado. A atualização também altera o inquilino padrão para `Global`, em vez de `Private`.	3 de outubro de 2022

Referência de API aprimorada	O Amazon OpenSearch Service oferece uma referência de API de configuração aprimorada e abrangente. As novas referências contêm todas as ações e os tipos de dados disponíveis, exemplos de sintaxe de solicitação e resposta e links para as referências de SDK correspondentes para todas as linguagens compatíveis.	13 de setembro de 2022
Validação azul/verde	O Amazon OpenSearch Service agora executa uma verificação de validação antes das implantações em azul/verde e detecta erros de validação se seu domínio não estiver qualificado para uma atualização.	16 de agosto de 2022
OpenSearch 1.3 suporte	O Amazon OpenSearch Service agora oferece suporte à OpenSearch versão 1.3. Para obter mais informações, consulte as notas de lançamento da versão 1.3.	27 de julho de 2022

Suporte ao plug-in ML Commons	O Amazon OpenSearch Service adiciona suporte ao plug-in ML Commons, que fornece um conjunto de algoritmos comuns de aprendizado de máquina por meio de transporte e chamadas de API REST. Você também pode interagir com o plug-in ML Commons por meio de comandos PPL.	27 de julho de 2022
Suporte ao volume gp3	O Amazon OpenSearch Service adiciona suporte para o tipo de volume SSD de uso geral do gp3 EBS. Você pode especificar IOPS provisionadas e throughput adicionais ao criar ou modificar o domínio.	26 de julho de 2022
Documentação aprimorada de práticas recomendadas	A documentação do Amazon OpenSearch Service fornece melhores práticas operacionais aprimoradas e recomendações gerais para criar e operar domínios OpenSearch de serviços.	6 de julho de 2022
Integração com o Service Quotas	Agora você pode visualizar as cotas do Amazon OpenSearch Service e solicitar aumentos de cotas no console Service Quotas.	29 de junho de 2022

Controle de acesso baseado em tags para a API OpenSearch	Agora você pode usar tags para controlar o acesso às OpenSearch APIs. Anteriorm ente, só era possível usar tags para controlar o acesso à API de configuração.	16 de junho de 2022
Pesquisa entre clusters e entre regiões	A pesquisa entre clusters agora é suportada Regiões da AWS desde que ambos os domínios estejam executand o a versão 7.10 ou posterior do Elasticsearch, ou qualquer versão do. OpenSearch	14 de junho de 2022
Suporte ao Kibana 5.6	O Amazon OpenSearch Service adiciona suporte para um único Kibana 5.6.16. Com o Kibana 5.6.16, é possível usar o Kibana 5.6 como front-end enquanto se conecta ao Elasticsearch versões 5.1, 5.3, 5.5 e 5.6. Para usar o Kibana 5.6, é necessário estar no software de serviço R20220323 ou superior.	4 de abril de 2022

R20220323-P1	A Amazon OpenSearch Service lançou recenteme nte a atualização de software de serviço R20220323, mas a atualização foi posterior mente revertida devido a um problema. Recomenda mos que você atualize seus domínios para o patch release R20220323-P1 ou posterior, o que corrige o problema.	4 de abril de 2022
OpenSearch 1.2 suporte	O Amazon OpenSearch Service agora oferece suporte à OpenSearch versão 1.2. Para obter mais informaçõ es, consulte as notas de lançamento da versão 1.2.	4 de abril de 2022
Observabilidade	A instalação padrão do OpenSearch Dashboards for Amazon OpenSearch Service inclui o plug-in Observabi lity, que você pode usar para visualizar eventos orientado s por dados usando a Piped Processing Language (PPL) para explorar e consultar seus dados. O plug-in requer OpenSearch 1.2 ou posterior e o software de serviço R20220323 ou posterior.	4 de abril de 2022

Suporte ao Kibana 7.7.1	Os domínios do Amazon OpenSearch Service que executam o Elasticsearch 7.7 agora oferecem suporte à versão de patch mais recente do Kibana 7.7, que adiciona correções de bugs e melhora a segurança. Quando você atualiza seus domínios 7.7 para o software de serviço R20220323 ou posterior, o OpenSearch Service os atualizará automaticamente para esta versão de patch.	4 de abril de 2022
Alterações métricas de pressão de memória JVM	O Amazon OpenSearch Service mudou a lógica das `JVMMemoryPressure` CloudWatch métricas para refletir com mais precisão a utilização da memória. Anteriormente, as métricas consideravam apenas o grupo de memória de geração antiga do heap da JVM. Com essa mudança, a métrica também considera o grupo de memória de geração jovem. Depois de atualizar seu domínio para o software de serviço R20220323, você poderá ver um aumento nas métricas `JVMMemoryPressure` , `MasterJVMMemoryPressure` e/ou `WarmJVMMemoryPressure` .	4 de abril de 2022

Dicionários personalizados com o plug-in Análise IK (Chinês)	O Amazon OpenSearch Service agora oferece suporte ao uso de dicionários personalizados com o plug-in de análise IK (chinês).	4 de abril de 2022
Replicação entre clusters em domínios existentes	O Amazon OpenSearch Service removeu a limitação de que você só pode implementar pesquisa e replicação entre clusters em domínios criados em ou após 3 de junho de 2020. Agora você pode habilitar esses recursos em todos os domínios, independentemente de quando eles foram criados. Ambos os domínios devem estar no software de serviço R20220323 ou posterior.	4 de abril de 2022
Visibilidade da implantação azul/verde	O Amazon OpenSearch Service agora oferece mais visibilidade sobre o progresso das implantações azul/verde. Você pode monitorar esses detalhes no console ou por meio da API de configuração.	27 de janeiro de 2022

Controle de acesso refinado em domínios existentes	Não é possível habilitar o controle de acesso refinado em domínios existentes. Você pode habilitar um período de migração temporária para políticas de acesso aberto/baseado em IP para garantir que os usuários possam continuar acessando o seu domínio enquanto você cria e mapeia funções. Para habilitar o controle de acesso refinado em domínios existentes, é necessário ter o software de serviço R20211203 ou superior.	6 de janeiro de 2022
Funções de OpenSearch painéis renomeadas	Com o software de serviço R20211203, a função `kibana_user` foi renomeada para `opensearch_dashboards_user` , e `kibana_read_only` foi renomeada para `opensearch_dashboards_read_only` . Essa alteração se aplica a todos os 1 recém-criados OpenSearch . domínios x. Para OpenSearch domínios existentes que você atualiza para o software de serviço R20211203, as funções permanecem as mesmas.	4 de janeiro de 2022

OpenSearch 1.1 suporte	O Amazon OpenSearch Service agora oferece suporte à OpenSearch versão 1.1. Para obter mais informaçõ es, consulte as notas de lançamento da versão 1.1.	4 de janeiro de 2022
Editor visual do ISM	A instalação padrão do OpenSearch Dashboards for Amazon OpenSearch Service agora oferece suporte ao editor visual das políticas do ISM. Esse recurso requer a OpenSearch versão 1.1 ou posterior.	4 de janeiro de 2022
Atualização da prevenção contra o problema confused deputy entre serviços	O Amazon OpenSearch Service oferece suporte ao uso das chaves de contexto de condição `aws:SourceAccount` global `aws:SourceArn` e das chaves de contexto nas políticas de recursos do IAM para evitar o problema confuso do substituto. Para usar essas chaves de condição, é necessário estar no software de serviço R20211203 ou superior.	4 de janeiro de 2022

Patch do Log4j	O software de serviço R20211203-P2 atualiza a versão do Log4j usada no Service conforme recomendado pelos avisos em CVE-2021-44228 e OpenSearch CVE-2021-45046. O patch se aplica aos domínios que executam todas as versões do Elasticsearch OpenSearch e do Elasticsearch. OpenSearch O serviço continuará atualizando várias versões do Log4j internamente e elas não estarão necessariamente restritas à versão mais recente do Log4j. A versão do Log4j em seu domínio depende da versão do software que o domínio está executando. No entanto, independentemente da versão do Log4j, desde que você esteja executando a R20211203-P2 ou posterior, seus domínios contêm a atualização do Log4j necessária para tratar o CVE-2021-44228 e o CVE-2021-45046.	15 de dezembro de 2021

Replicação entre clusters	A replicação entre clusters permite replicar índices, mapeamentos e metadados de um domínio de serviço para outro. OpenSearch A replicação entre clusters requer um domínio executando o Elasticsearch 7.10 ou 1.1 ou posterior. OpenSearch	5 de outubro de 2021
Novas AWS políticas gerenciadas	O lançamento do Amazon OpenSearch Service inclui novas políticas AWS gerenciadas e a descontinuação de políticas antigas.	8 de setembro de 2021
Suporte ao Kibana 6.4.3	Os domínios do Amazon OpenSearch Service que executam a versão 6.4 antiga do Elasticsearch agora oferecem suporte à versão de patch mais recente do Kibana 6.4, que adiciona correções de bugs e melhora a segurança. OpenSearch O serviço atualizará automaticamente os domínios para esta versão de patch.	8 de setembro de 2021

Streams de dados	O Amazon OpenSearch Service adiciona suporte para fluxos de dados, o que simplifica o processo de gerenciamento de dados de séries temporais. Seu domínio deve estar executando a OpenSearch versão 1.0 ou posterior para usar fluxos de dados.	8 de setembro de 2021
OpenSearch Serviço Amazon	AWS renomeia o Amazon OpenSearch Service para remover a marca “Elastics earch” antiga. O Amazon OpenSearch Service oferece suporte OpenSearch e lega o Elasticsearch OSS. Ao criar um cluster, você tem a opção de qual mecanismo de pesquisa usar. OpenSearc h O serviço oferece ampla compatibilidade com o Elasticsearch OSS 7.10, a versão final de código aberto do software.	8 de setembro de 2021

Armazenamento de baixa atividade	O armazenamento inativo é um novo nível de armazenamento para dados históricos ou acessados com pouca frequência. Os índices de baixa atividade ocupam apenas o armazenamento S3 e não têm computação anexada a eles. O armazenamento de baixa atividade requer um domínio executando o Elasticsearch 7.9 ou posterior e o software de serviço R20210426 ou posterior.	13 de maio de 2021
Instâncias do Graviton baseadas em ARM	O Amazon OpenSearch Service agora oferece suporte aos tipos de instância Graviton baseados em ARM (M6G, C6G, R6G e R6GD). Os tipos de instância do Graviton estão disponíveis em domínios novos e existentes executando o Elasticsearch 7.9 ou posterior e o software de serviço R20210331 ou posterior.	4 de maio de 2021

Modelos do ISM	O Amazon OpenSearch Service adiciona suporte aos modelos do ISM, que permitem anexar automatic amente uma política do ISM a um índice se o índice corresponder a um padrão definido na política. Os modelos do ISM exigem o software de serviço R20210426 ou posterior. Esta atualização também defasa a configuração `policy_id` , o que significa que você não pode mais usar modelos de índice para aplicar políticas do ISM a índices recém-cri ados. A atualização introduz uma alteração significativa nos CloudFormation modelos existentes usando essa configuração.	27 de abril de 2021
Suporte ao Elasticsearch 7.10	O Amazon OpenSearch Service agora oferece suporte ao Elasticsearch versão 7.10. Para obter mais informaçõ es, consulte as notas de lançamento da versão 7.10.	21 de abril de 2021

Pesquisa assíncrona	O Amazon OpenSearch Service agora oferece suporte à pesquisa assíncrona, que permite executar solicitaç ões de pesquisa em segundo plano. A pesquisa assíncrona requer um domínio executand o o Elasticsearch 7.10 ou posterior e o software de serviço R20210331 ou posterior.	21 de abril de 2021
Controle de acesso baseado em tags para a API de configuração	Agora você pode usar AWS tags para controlar o acesso à API de configuração do Amazon ES.	2 de março de 2021
Auto-Tune	O Amazon OpenSearch Service adiciona o Auto-Tune, que usa métricas de desempenho e uso do seu cluster para sugerir alterações nas configurações da JVM em seus nós. O Auto-Tune requer um domínio executando o Elasticsearch 6.7 ou posterior e o software de serviço R20201117 ou posterior.	24 de fevereiro de 2021

Trace Analytics	A instalação padrão do Kibana para Amazon OpenSearch Service agora inclui o plug-in de análise de rastreamento, que permite monitorar dados de rastreamento de seus aplicativos distribuídos. O plug-in requer um domínio executando o Elasticsearch 7.9 ou posterior e o software de serviço R20210201 ou posterior.	17 de fevereiro de 2021
Métricas de fragmentos	O Amazon OpenSearch Service adiciona as seguintes CloudWatch métricas para rastrear o status do fragmento:`Shards.active` ,`Shards.unassigned` ,, `Shards.delayedUnassigned` `Shards.activePrimary` `Shards.initializing` ,`Shards.relocating` . As métricas estão disponíveis em domínios que executam o software de serviço R20210201 ou superior.	17 de fevereiro de 2021

Relatórios do Kibana	A instalação padrão do Kibana para Amazon OpenSearch Service agora oferece suporte a relatórios sob demanda para as páginas Discover, Visualize e Dashboard. Esse recurso requer o Elasticsearch 7.9 ou posterior e o software de serviço R20210201 ou posterior.	17 de fevereiro de 2021
Suporte ao Kibana 5.6.16	Os domínios do Amazon OpenSearch Service que executam o Elasticsearch 5.6 agora oferecem suporte à versão de patch mais recente do Kibana 5.6, que adiciona correções de bugs e melhora a segurança. O Amazon ES atualizará automaticamente os domínios para esta versão de patch.	17 de fevereiro de 2021
Criptografia para domínios existentes	O Amazon OpenSearch Service agora oferece suporte para habilitar a criptografia de dados em repouso e a node-to-node criptografia em domínios existentes que executam o Elasticsearch 6.7 ou posterior. Após habilitar essas configurações, você não poderá desabilitá-las.	27 de janeiro de 2021

Reindexação remota	O Amazon OpenSearch Service agora oferece suporte à reindexação remota, o que permite migrar índices de domínios remotos. Esse recurso exige o software de serviço R20201117 ou posterior.	24 de novembro de 2020
Piped Processing Language	O Amazon OpenSearch Service agora oferece suporte à Piped Processing Language (PPL), uma linguagem de consulta que permite usar a sintaxe pipe (|) para consultar dados armazenados no Elasticsearch. Esse recurso exige o software de serviço R20201117 ou posterior. Para saber mais, consulte .	24 de novembro de 2020
Cadernos do Kibana	O Amazon OpenSearch Service adiciona suporte aos notebooks Kibana, o que permite combinar visualizações ao vivo e texto narrativo em uma única interface. Esse recurso exige o software de serviço R20201117 ou posterior.	24 de novembro de 2020

Gráficos de Gantt	A instalação padrão do Kibana para Amazon OpenSearch Service agora oferece suporte a um novo tipo de visualização, gráficos de Gantt. Esse recurso exige o software de serviço R20201117 ou posterior.	24 de novembro de 2020
Suporte ao Elasticsearch 7.9	O Amazon OpenSearch Service agora oferece suporte ao Elasticsearch versão 7.9. Para obter mais informações, consulte as notas de lançamento da versão 7.9.	24 de novembro de 2020
Atualizações na detecção de anomalias	A detecção de anomalias para o Amazon OpenSearch Service adiciona suporte à alta cardinalidade, o que permite categorizar anomalias com uma dimensão como endereço IP, ID do produto, código do país e assim por diante. Esse recurso exige o software de serviço R20201117 ou posterior.	24 de novembro de 2020

Atualizações do dicionário dinâmico	O Amazon OpenSearch Service agora permite que você atualize seus analisadores de pesquisa sem reindexar. Você pode atualizar os arquivos de dicionário em alguns ou todos os seus domínios, e o Amazon ES rastreia as versões do pacote ao longo do tempo para que você tenha um histórico do que mudou e quando. Esse recurso exige o software de serviço R20201019 ou posterior.	17 de novembro de 2020
Endpoints personalizados	O Amazon OpenSearch Service agora oferece suporte a endpoints personalizados, que permitem que você forneça um novo URL ao seu domínio do Amazon ES. Se você trocar de domínios, poderá manter o mesmo URL. Esse recurso exige o software de serviço R20201019 ou posterior.	5 de novembro de 2020

Novos plug-ins de idiomas	O Amazon OpenSearch Service agora oferece suporte aos plug-ins IK (chinês) Analysis, Vietnamese Analysis e Thai Analysis em domínios que executam o Elasticsearch 7.7 ou posterior com o software de serviço R20201019 ou posterior.	28 de outubro de 2020
Suporte ao Elasticsearch 7.8	O Amazon OpenSearch Service agora oferece suporte ao Elasticsearch versão 7.8. Para obter mais informações, consulte as notas de lançamento da versão 7.8.	28 de outubro de 2020
Autenticação SAML para Kibana	O Amazon OpenSearch Service agora oferece suporte à autenticação SAML para o Kibana, que permite que você use provedores de identidade terceirizados para fazer login no Kibana, gerenciar o controle de acesso refinado, pesquisar seus dados e criar visualizações. Esse recurso exige o software de serviço R20201019 ou posterior.	27 de outubro de 2020
Instâncias T3	O Amazon OpenSearch Service agora oferece suporte `t3.small` aos tipos de `t3.medium` instância e.	23 de setembro de 2020

Logs de auditoria	O Amazon OpenSearch Service agora oferece suporte a registros de auditoria para seus dados, o que permite rastrear tentativas de login malsucedidas, acesso de usuários a índices, documento s e campos e muito mais. Esse recurso exige o software de serviço R20200910 ou posterior.	16 de setembro de 2020
UltraWarm atualizações	UltraWarm for Amazon OpenSearch Service adiciona novas métricas, novas configurações, uma fila de migração maior e uma API de cancelamento. Essas atualizaç ões exigem o software de serviço R20200910 ou posterior. Para ter mais informações, consulte .	14 de setembro de 2020
Learning to Rank	O Amazon OpenSearch Service agora oferece suporte ao plug-in de código aberto Learning to Rank, que permite usar tecnologias de aprendiza do de máquina para melhorar a relevância da pesquisa. Esse recurso exige o software de serviço R20200721 ou posterior.	27 de julho de 2020

Similaridade de cosseno k-NN	O algoritmo k-vizinhos mais próximos (k-NN) agora permite procurar “vizinhos mais próximos” por similaridade de cossenos, além da distância euclidiana. Esse recurso exige o software de serviço R20200721 ou posterior.	23 de julho de 2020
Compactação gzip	O Amazon OpenSearch Service agora oferece suporte à compressão gzip para a maioria das solicitações e respostas HTTP, o que pode reduzir a latência e conservar a largura de banda. Esse recurso exige o software de serviço R20200721 ou posterior.	23 de julho de 2020
Suporte ao Elasticsearch 7.7	O Amazon OpenSearch Service agora oferece suporte ao Elasticsearch versão 7.7. Para obter mais informaçõ es, consulte as notas de lançamento da versão 7.7.	23 de julho de 2020
Serviço de mapas do Kibana	A instalação padrão do Kibana para Amazon OpenSearc h Service agora inclui um servidor de mapas WMS, exceto para domínios nas regiões da Índia e da China.	18 de junho de 2020

Melhorias em SQL	O suporte SQL para o Amazon OpenSearch Service agora oferece suporte a muitas novas operações, uma interface de usuário Kibana dedicada para exploração de dados e uma CLI interativa. Para ter mais informações, consulte .	3 de junho de 2020
Pesquisa entre clusters	O Amazon OpenSearch Service permite que você realize consultas e agregaçõe s entre clusters em vários domínios conectados.	3 de junho de 2020
Detecção de anomalias	O Amazon OpenSearch Service permite que você detecte automaticamente anomalias quase em tempo real.	3 de junho de 2020
UltraWarm	UltraWarm o armazenamento para o Amazon OpenSearch Service saiu da versão prévia pública e agora está disponíve l ao público em geral. O recurso agora oferece suporte a uma variedade maior de versões Regiões da AWS e. Para ter mais informações, consulte .	5 de maio de 2020

Dicionários personalizados	O Amazon OpenSearch Service permite que você faça upload de arquivos de dicionário personalizados para uso com seu cluster. Esses arquivos melhoram seus resultados de pesquisa instruindo o Elasticsearch a ignorar certas palavras de alta frequência ou para tratar termos como equivalentes.	21 de abril de 2020
Suporte ao Elasticsearch 7.4	O Amazon OpenSearch Service agora oferece suporte ao Elasticsearch versão 7.4. Para obter mais informações, consulte Versões compatíveis.	12 de março de 2020
k-NN	O Amazon OpenSearch Service adiciona suporte à pesquisa K-Nearest Neighbor (k-NN). O k-NN requer o software de serviço R20200302 ou posterior.	3 de março de 2020
Gerenciamento de estados de índice	O Amazon OpenSearch Service adiciona o Index State Management (ISM), que permite automatizar tarefas rotineiras, como excluir índices quando eles atingem uma certa idade. Esse recurso exige o software de serviço R20200302 ou superior.	3 de março de 2020

Suporte ao Elasticsearch 5.6.16	O Amazon OpenSearch Service agora oferece suporte à versão de patch mais recente para a versão 5.6, que adiciona correções de bugs e melhora a segurança . O Amazon ES atualizará automaticamente os domínios 5.6 para esta versão. Observe que essa versão do Elasticsearch informa incorretamente sua versão como 5.6.17.	2 de março de 2020
Controle de acesso refinado	O Amazon OpenSearch Service agora oferece suporte ao controle de acesso refinado, que oferece segurança em nível de índice, documento e campo, multilocação do Kibana e autenticação básica HTTP opcional para seu cluster.	11 de fevereiro de 2020

UltraWarm armazenamento (pré-visualização)	O Amazon OpenSearch Service adiciona UltraWarm um novo nível de armazenamento aquecido que usa o Amazon S3 e uma solução sofisticada de cache para melhorar o desempenho. Para índices nos quais você não está gravando ativamente e consultando com menos frequência, o UltraWarm armazenamento oferece custos significativamente mais baixos por GiB.	3 de dezembro de 2019
Recursos de criptografia para regiões da China	A criptografia de dados em repouso e a node-to-node criptografia agora estão disponíveis na região da `cn-north-1` China (Pequim) e na região `cn-northwest-1` da China (Ningxia).	20 de novembro de 2019
Exigir HTTPS	Agora você pode exigir que todo o tráfego para os domínios do Amazon ES seja recebido via HTTPS. Ao configurar seu domínio, marque a caixa Exigir HTTPS. Esse recurso exige o software de serviço R20190808 ou superior.	3 de outubro de 2019

Suporte ao Elasticsearch 7.1 e 6.8	O Amazon OpenSearch Service agora oferece suporte às versões 7.1 e 6.8 do Elasticsearch. Para obter mais informações, consulte Versões compatíveis.	13 de agosto de 2019
Snapshots a cada hora	Em vez de instantâneos diários, o Amazon OpenSearch Service agora tira instantâneos de hora em hora de domínios que executam o Elasticsearch 5.3 e versões posteriores, para que você tenha backups mais frequentes para restaurar seus dados.	8 de julho de 2019
Suporte ao Elasticsearch 6.7	O Amazon OpenSearch Service agora oferece suporte ao Elasticsearch versão 6.7. Para obter mais informações, consulte Versões compatíveis.	29 de maio de 2019
Suporte a SQL	O Amazon OpenSearch Service agora permite que você consulte seus dados usando SQL. O suporte a SQL exige o software de serviço R20190418 ou posterior.	15 de maio de 2019

Tipos de instâncias da série 5	O Amazon OpenSearch Service agora oferece suporte aos tipos de instância M5, C5 e R5. Em comparaçã o aos tipos de instância da geração anterior, esses novos tipos oferecem uma melhor performance a preços mais baixos. Para obter mais informações, consulte Limites.	24 de abril de 2019
Suporte ao Elasticsearch 6.5	O Amazon OpenSearch Service agora oferece suporte ao Elasticsearch versão 6.5.	8 de abril de 2019
Geração de alertas	O alerta para o Amazon OpenSearch Service notifica você quando os dados de um ou mais índices do Amazon ES atendem a determina das condições. Os alertas exigem o software de serviço R20190221 ou posterior.	25 de março de 2019
Suporte a três zonas de disponibilidade	O Amazon OpenSearch Service agora oferece suporte a três zonas de disponibi lidade em várias regiões. Essa versão também inclui uma experiência de console simplificada. Esse recurso multi-AZ exige o software de serviço R20181023 ou posterior.	7 de fevereiro de 2019

Suporte ao Elasticsearch 6.4	O Amazon OpenSearch Service agora oferece suporte ao Elasticsearch versão 6.4.	23 de janeiro de 2019
Clusters de 200 nós	O Amazon ES agora permite que você crie clusters com até 200 nós de dados para um total de 3 PB de armazenam ento.	22 de janeiro de 2019
Atualizações de software de serviço	O Amazon ES agora permite que você atualize manualmen te o software de serviço para seu domínio para se beneficia r de novos recursos mais rapidamente ou atualizar em um horário com baixo volume de tráfego. Para saber mais, consulte .	20 de novembro de 2018
Novas CloudWatch métricas	O Amazon ES agora oferece métricas em nível de nó e novas guias Integridade do cluster e Integridade da instância no console do Amazon ES.	20 de novembro de 2018
Suporte à China (Pequim)	O Amazon OpenSearch Service agora está disponíve l na região cn-north-1, onde oferece suporte aos tipos de instância M4, C4 e R4.	17 de outubro de 2018

ode-to-node Criptografia N	O Amazon OpenSearch Service agora oferece suporte à node-to-node criptografia, que mantém seus dados criptografados à medida que o Amazon ES os distribui por todo o cluster.	18 de setembro de 2018
Atualizações de versão em vigor	O Amazon OpenSearch Service agora oferece suporte a atualizações de versão no local.	14 de agosto de 2018
Suporte ao Elasticsearch 6.3 e 5.6	O Amazon OpenSearch Service agora oferece suporte às versões 6.3 e 5.6 do Elasticsearch.	14 de agosto de 2018
Logs de erro	O Amazon ES agora permite que você publique registros de erros do Elasticsearch na Amazon. CloudWatch	31 de julho de 2018
Instâncias reservadas para China (Ningxia)	O Amazon ES agora oferece Instâncias reservadas para a região da China (Ningxia).	29 de maio de 2018
Instâncias reservadas	O Amazon ES agora oferece suporte a instâncias reservadas.	7 de maio de 2018

Atualizações anteriores

A tabela a seguir descreve alterações importantes no Amazon ES antes de maio de 2018.

Alteração	Descrição	Data
Autenticação do Amazon Cognito para Kibana	O Amazon ES agora oferece proteção da página de login para o Kibana. Para saber mais, consulte the section called “Autenticação do Amazon Cognito para OpenSearch Dashboards”.	2 de abril de 2018
Suporte ao Elasticsearch 6.2	O Amazon OpenSearch Service agora oferece suporte ao Elasticsearch versão 6.2.	14 de março de 2018
Plug-in de análise coreana	O Amazon ES agora oferece suporte a uma versão otimizada para memória do plug-in de análise coreana Seunjeon.	13 de março de 2018
Atualizações instantâneas de controle de acesso	As alterações nas políticas de controle de acesso em domínios do Amazon ES agora entram em vigor instantan eamente.	7 de março de 2018
Escala de petabytes	O Amazon ES agora oferece suporte a tipos de instância I3 e armazenamento de domínio total de até 1,5 PB. Para saber mais, consulte the section called “Escala de petabytes”.	19 de dezembro de 2017
Criptografia de dados em repouso	O Amazon ES agora oferece suporte à criptografia de dados em repouso. Para saber mais, consulte the section called “Criptografia inativa”.	7 de dezembro de 2017
Suporte ao Elasticsearch 6.0	O Amazon ES agora oferece suporte ao Elasticsearch versão 6.0 Para considerações e instruções de migração, consulte the section called “Atualização de domínios”.	6 de dezembro de 2017
Suporte à VPC	O Amazon ES agora permite iniciar domínios em uma Amazon Virtual Private Cloud. O suporte a VPC fornece uma camada adicional de segurança e simplifica a comunicação entre o Amazon ES e outros serviços dentro de uma VPC. Para saber mais, consulte the section called “Suporte à VPC”.	17 de outubro de 2017

Alteração	Descrição	Data
Publicação de logs lentos	O Amazon ES agora oferece suporte à publicação de registros lentos no CloudWatch Logs. Para saber mais, consulte the section called “Monitoramento de logs”.	16 de outubro de 2017
Suporte ao Elasticsearch 5.5	O Amazon ES agora oferece suporte ao Elasticsearch versão 5.5. Agora você pode restaurar snapshots automatizados sem precisar entrar em contato com o AWS Support e armazenar scripts por meio da API `_scripts`.	7 de setembro de 2017
Suporte ao Elasticsearch 5.3	O Amazon ES adicionou suporte ao Elasticsearch versão 5.3.	1 de junho de 2017
Mais instâncias e capacidade de EBS por cluster	O Amazon ES agora oferece suporte a até 100 nós e 150 TB de capacidade de EBS por cluster.	5 de abril de 2017
Suporte no Canadá (Central) e na UE (Londres)	O Amazon ES adicionou suporte às seguintes regiões: Canadá (Central), ca-central-1 e UE (Londres), eu-west-2.	20 de março de 2017
Mais instâncias e maiores volumes de EBS	O Amazon ES adicionou suporte a mais instâncias e a volumes do EBS maiores.	21 de fevereiro de 2017
Suporte ao Elasticsearch 5.1	O Amazon ES adicionou suporte ao Elasticsearch versão 5.1.	30 de janeiro de 2017
Compatibilidade com o plug-in Phonetic Analysis	O Amazon ES agora oferece integração incorporada com o plug-in Phonetic Analysis, o qual permite a você realizar consultas "sonoras" em seus dados.	22 de dezembro de 2016
Suporte no Leste dos EUA (Ohio)	O Amazon ES adicionou suporte à seguinte região: Leste dos EUA (Ohio), us-east-2.	17 de outubro de 2016

Alteração	Descrição	Data
Nova métrica de performance	O Amazon ES adicionou uma métrica de performance, `ClusterUsedSpace` .	29 de julho de 2016
Suporte ao Elasticsearch 2.3	O Amazon ES adicionou suporte ao Elasticsearch versão 2.3.	27 de julho de 2016
Suporte na Ásia-Pacífico (Mumbai)	O Amazon ES adicionou suporte à seguinte região: Ásia-Pacífico (Mumbai), ap-south-1.	27 de junho de 2016
Mais instâncias por cluster	O Amazon ES aumentou o número máximo de instâncias (contagem de instâncias) por cluster de 10 para 20.	18 de maio de 2016
Suporte na Ásia-Pacífico (Seul)	O Amazon ES adicionou suporte à seguinte região: Ásia-Pacífico (Seul), ap-northeast-2.	28 de janeiro de 2016
Amazon ES	Versão inicial.	1 de outubro de 2015

Glossário do AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

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.