Implante e gerencie aplicativos de automação de processos empresariais no Amazon EKS: um guia prático

Contents

Resumo

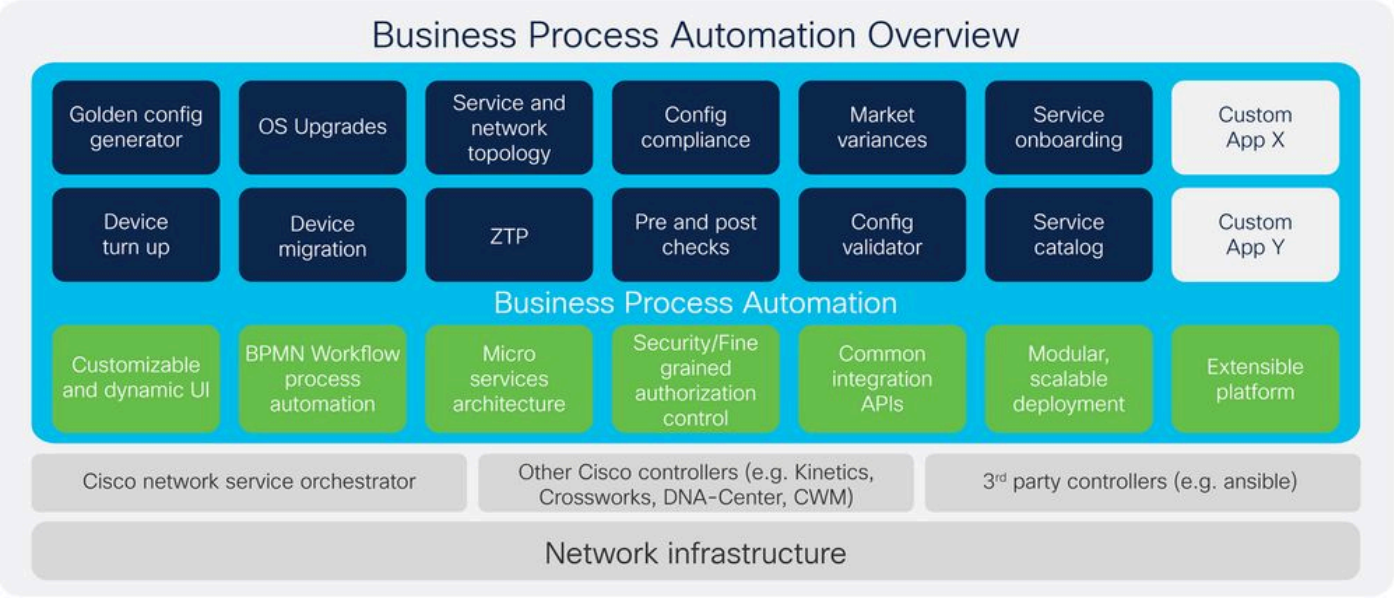
Este documento apresenta um guia abrangente sobre a implantação e o gerenciamento de aplicativos BPA (Business Process Automation, automação de processos de negócios) usando o Amazon EKS (Elastic Kubernetes Service). Ele descreve os pré-requisitos, destaca os benefícios da utilização do EKS e fornece instruções passo a passo para a configuração de um cluster EKS, da base de dados do Amazon RDS e do MongoDB Atlas. Além disso, o documento analisa a arquitetura de implantação e especifica os requisitos do ambiente, oferecendo um recurso completo para as empresas que desejam aproveitar o EKS para seus aplicativos BPA em contêineres.

Palavras-chave

Amazon EKS, Kubernetes, AWS, RDS, MongoDB Atlas, DevOps, computação em nuvem, automação de processos empresariais.

Introdução

BPA



Na era digital de hoje, as empresas buscam simplificar e automatizar processos comerciais complexos em uma variedade diversificada de ambientes de TI. O BPA (Business Process Automation, automação de processos de negócios) surgiu como uma tecnologia essencial, permitindo que as empresas melhorem a eficiência operacional, reduzam erros e melhorem a prestação de serviços. O BPA apresenta várias inovações e aprimoramentos importantes destinados a promover a automação do fluxo de trabalho, o provisionamento de serviços e os aplicativos de automação prontos para uso.

A plataforma BPA hospeda aplicativos e casos de uso operacionais e de TI e de negócios, como atualizações de SO, provisionamento de serviços e integração com mecanismos de orquestração. Os clientes têm acesso a um ciclo de vida de serviços e recursos de BPA, incluindo consultoria, implementação, serviços essenciais aos negócios e suporte a soluções fornecidos por especialistas da Cisco, práticas recomendadas e técnicas e metodologias comprovadas que ajudam a automatizar seus processos de negócios e a eliminar os riscos de seus sistemas.

Esses recursos de ciclo de vida podem ser baseados em assinatura ou personalizados para necessidades individuais. Os serviços de implementação ajudam a definir, integrar e implantar ferramentas e processos para acelerar a automação. Os especialistas da Cisco conduzem um processo formal para reunir requisitos, projetar e desenvolver histórias de usuários com base em processos ágeis e ferramentas de CICD (Continuous Integration and Continuous Delivery, integração contínua e fornecimento contínuo), e implementam serviços flexíveis com testes automatizados de fluxos de trabalho, dispositivos e serviços novos ou existentes. Com o Suporte às soluções, os clientes obtêm acesso ao suporte centralizado 24 horas por dia, 7 dias por semana, com foco em problemas centralizados em software, juntamente com suporte de vários fornecedores e código aberto oferecido através do modelo de software em camadas da Cisco. Os especialistas em suporte às soluções da Cisco ajudam a gerenciar seu caso desde a primeira chamada até a resolução final e atuam como o principal ponto de contato ao trabalhar com vários fornecedores simultaneamente. Você poderia enfrentar até 44% menos problemas trabalhando com especialistas em soluções, ajudando a manter a continuidade dos negócios e obter um retorno mais rápido do seu investimento em BPA.

Recursos técnicos importantes, como suporte para dispositivos gerenciados por FMC e Ansible, execuções

paralelas usando o Advanced Queuing Framework (AQF) e conformidade de configuração expandida para dispositivos NDFC e FMC, posicionam o BPA como uma solução abrangente para automação corporativa de grande escala. Com recursos adicionais em gerenciamento de SD-WAN, integração de dispositivos e controle de políticas de firewall, a versão aborda aspectos críticos de segurança e automação de rede, atendendo às demandas de ambientes de grande escala de vários fornecedores.

EKS

O Amazon Elastic Kubernetes Service (EKS) é um serviço Kubernetes totalmente gerenciado fornecido pela Amazon Web Services (AWS). Lançado em 2018, o EKS simplifica o processo de implantação, gerenciamento e dimensionamento de aplicativos em contêineres usando Kubernetes, uma plataforma de orquestração de contêineres de código aberto. O EKS abstrai as complexidades do gerenciamento de cluster Kubernetes, permitindo que os desenvolvedores se concentrem na construção e execução de aplicativos sem a necessidade de manipular a infraestrutura subjacente.

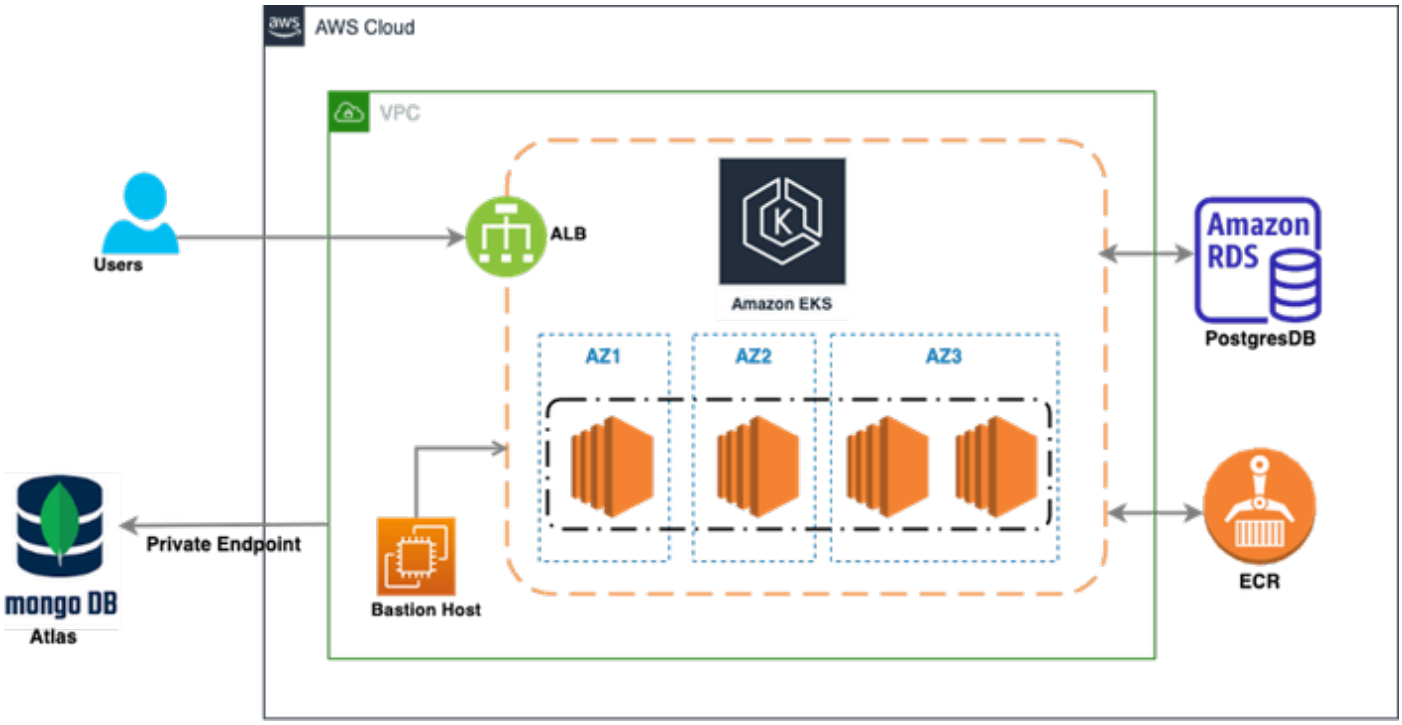
Benefícios do uso do Amazon EKS para implantação de aplicativos

O Amazon EKS oferece vários benefícios para a implantação de aplicativos, tornando-o uma escolha popular para empresas que utilizam aplicativos e microsserviços em contêineres.

As principais vantagens incluem:

- **Plano de controle gerenciado do Kubernetes**: o EKS lida com a implantação, dimensionamento e manutenção do plano de controle do Kubernetes, reduzindo a carga operacional.
- **Gerenciamento de cluster simplificado**: o EKS abstrai as complexidades de configurar e gerenciar clusters Kubernetes.
- **Escalabilidade**: o EKS permite o fácil dimensionamento de clusters para acomodar cargas de trabalho cada vez maiores.
- **Alta disponibilidade**: o EKS oferece suporte a implantações de várias zonas de disponibilidade, aumentando a disponibilidade e a tolerância a falhas.
- **Integração com serviços AWS**: o EKS se integra perfeitamente a vários serviços AWS.
- **Automação de DevOps**: o EKS oferece suporte à integração contínua e à implantação contínua (CI/CD) para aplicativos em contêineres.

Arquitetura de implantação de BPA



Essa imagem representa uma arquitetura de alto nível de uma infraestrutura baseada em nuvem implantada no **AWS** , usando vários componentes importantes. Aqui está uma divisão do diagrama:

1. **Amazon EKS (Elastic Kubernetes Service)**: No núcleo do diagrama, o Amazon EKS é implantado em três zonas de disponibilidade (AZ1, AZ2, AZ3), com nós de trabalho Kubernetes dentro de cada zona. Isso indica uma configuração altamente disponível e tolerante a falhas, pois as cargas de trabalho são distribuídas em várias zonas de disponibilidade.

2. **ALB (Application Load Balancer)**: Este é posicionado na frente, recebendo o tráfego dos usuários e distribuindo-o através do cluster EKS para lidar com cargas de trabalho de aplicativos. O balanceador de carga garante que as solicitações sejam distribuídas uniformemente e possam lidar com o escalonamento com base na demanda de tráfego.

3. **Amazon RDS (Relational Database Service)** - PostgreSQL: no lado direito do diagrama, uma instância do Amazon RDS que executa PostgreSQL está presente. Este banco de dados pode ser acessado por aplicativos executados no cluster EKS.

4. **ECR (Elastic Container Registry)**: É aqui que as imagens do contêiner do Docker são armazenadas e gerenciadas, que são implantadas no Amazon EKS para executar as cargas de trabalho.

5. **MongoDB Atlas**: No lado esquerdo, o MongoDB Atlas é integrado na arquitetura através de um endpoint privado. O MongoDB Atlas é um serviço de banco de dados NoSQL hospedado na nuvem, usado aqui para lidar com requisitos de banco de dados baseados em documentos. O endpoint privado garante comunicação segura e privada entre a instância do Atlas MongoDB e outros componentes do AWS.

6. **Bastion Host**: posicionado dentro do VPC (Virtual Private Cloud), um Bastion Host fornece um ponto de entrada seguro para administradores acessarem recursos dentro do VPC sem expor diretamente à Internet.

No geral, essa arquitetura oferece uma solução altamente disponível, escalável e segura para implantar e gerenciar aplicativos em contêineres usando o Amazon EKS, com suporte para bancos de dados relacionais (PostgreSQL) e NoSQL (MongoDB).

- **Configuração de cluster EKS**
  Para criar um cluster do Amazon EKS usando a CLI do AWS, o utilitário de linha de comando `eksctl` pode ser usado. Este é um exemplo de comando:

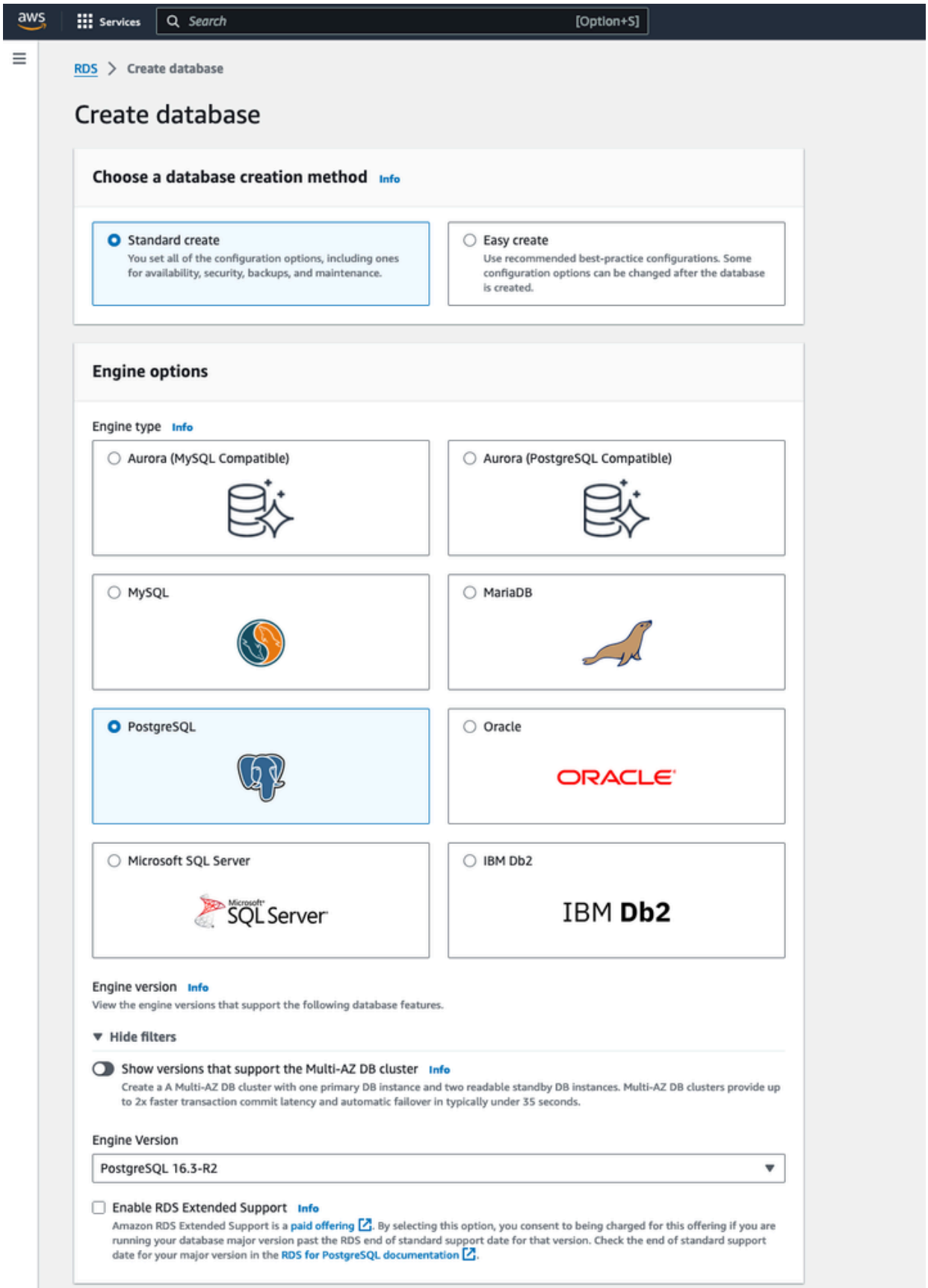
```
eksctl create cluster \
  --name
```

```
\ --region us-west-2 \ --nodegroup-name standard-workers \ --node-type t3.medium \ --node
```

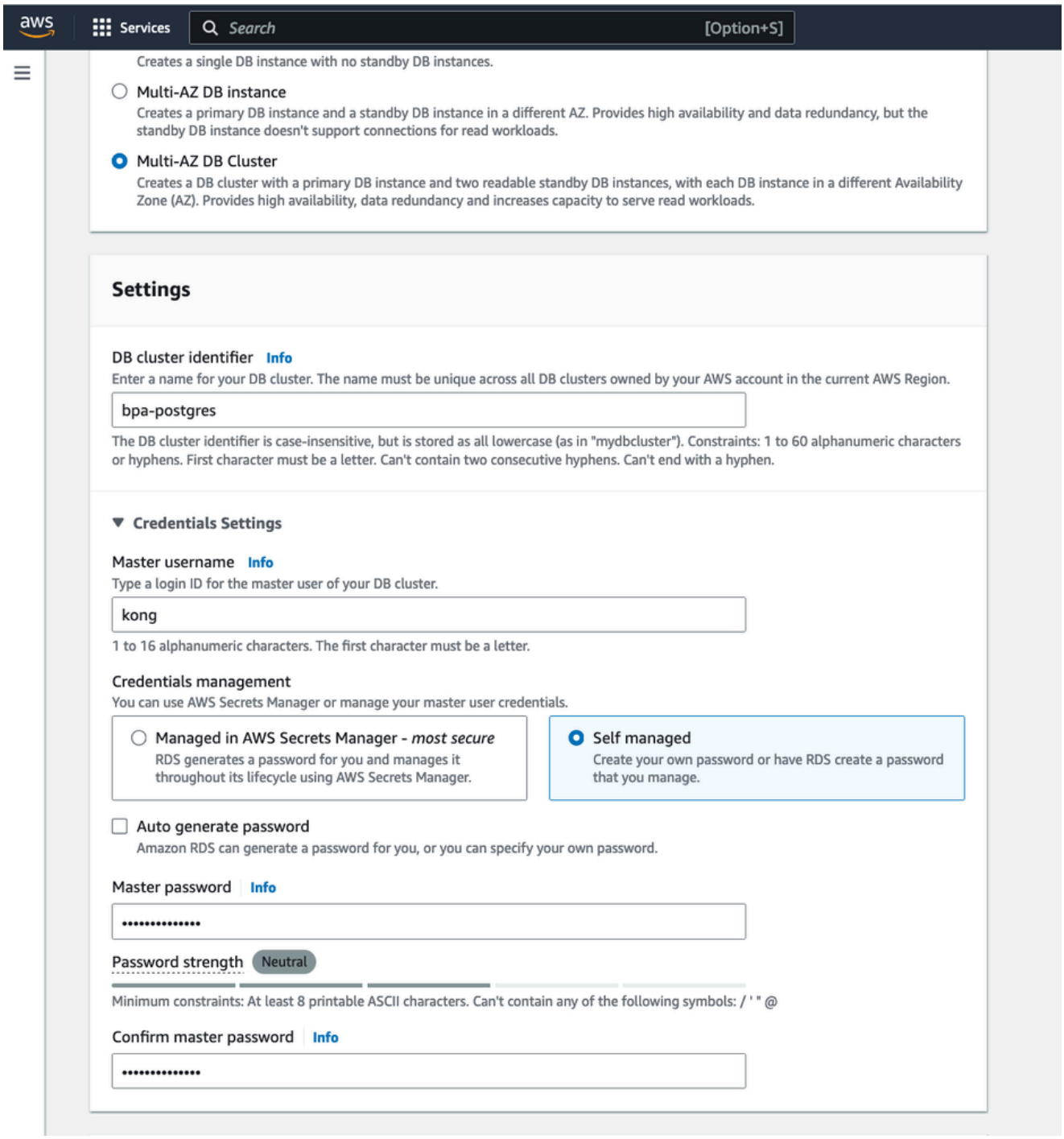
- **Configuração do Banco de Dados RDS**

  A implantação de um banco de dados relacional no Amazon RDS envolve estas etapas:

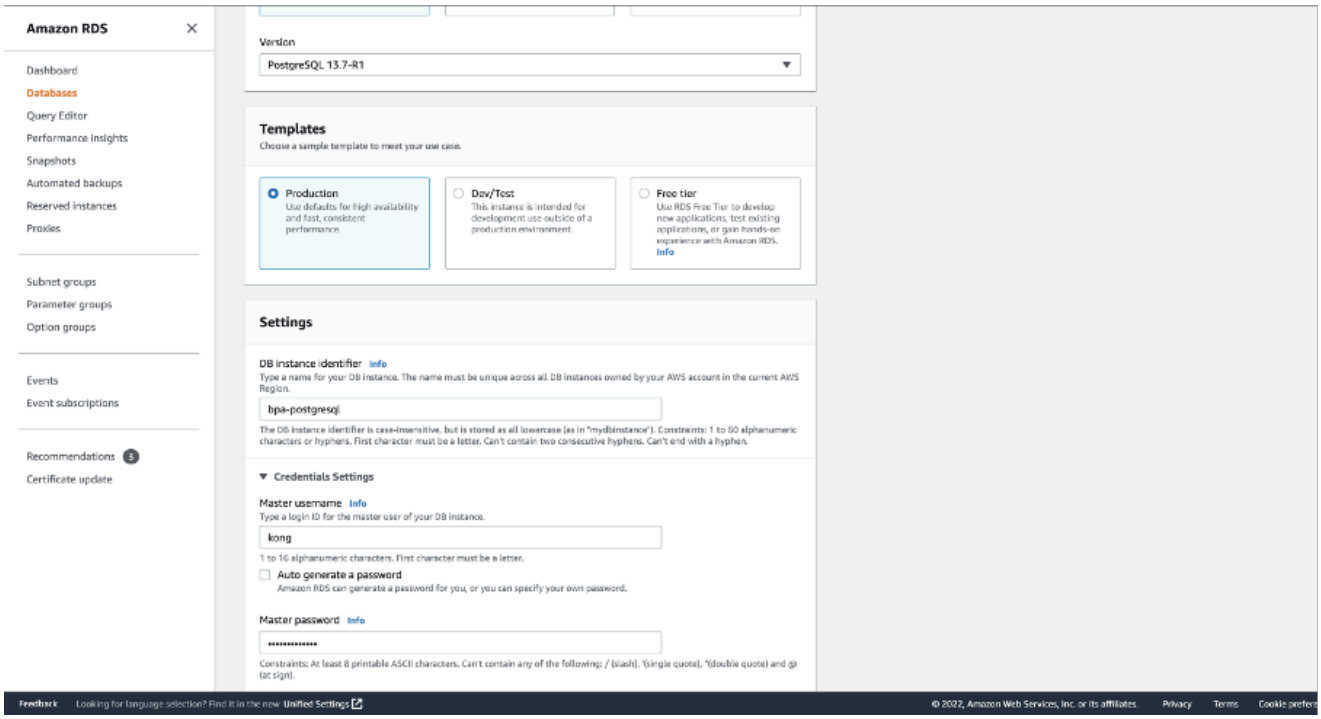
  - Acesse o AWS Management Console e navegue até o serviço Amazon RDS.
  - Crie uma nova instância de banco de dados com as especificações desejadas.
  - Configure o grupo de segurança para permitir conexões de entrada do cluster do Amazon EKS.



Usando o menu suspenso, selecione a versão mais recente do PostgreSQL. No nosso caso, é "PostgreSQL 16.3-R1."



Para isso, dê um nome à instância do banco de dados e crie um nome de usuário e uma senha.

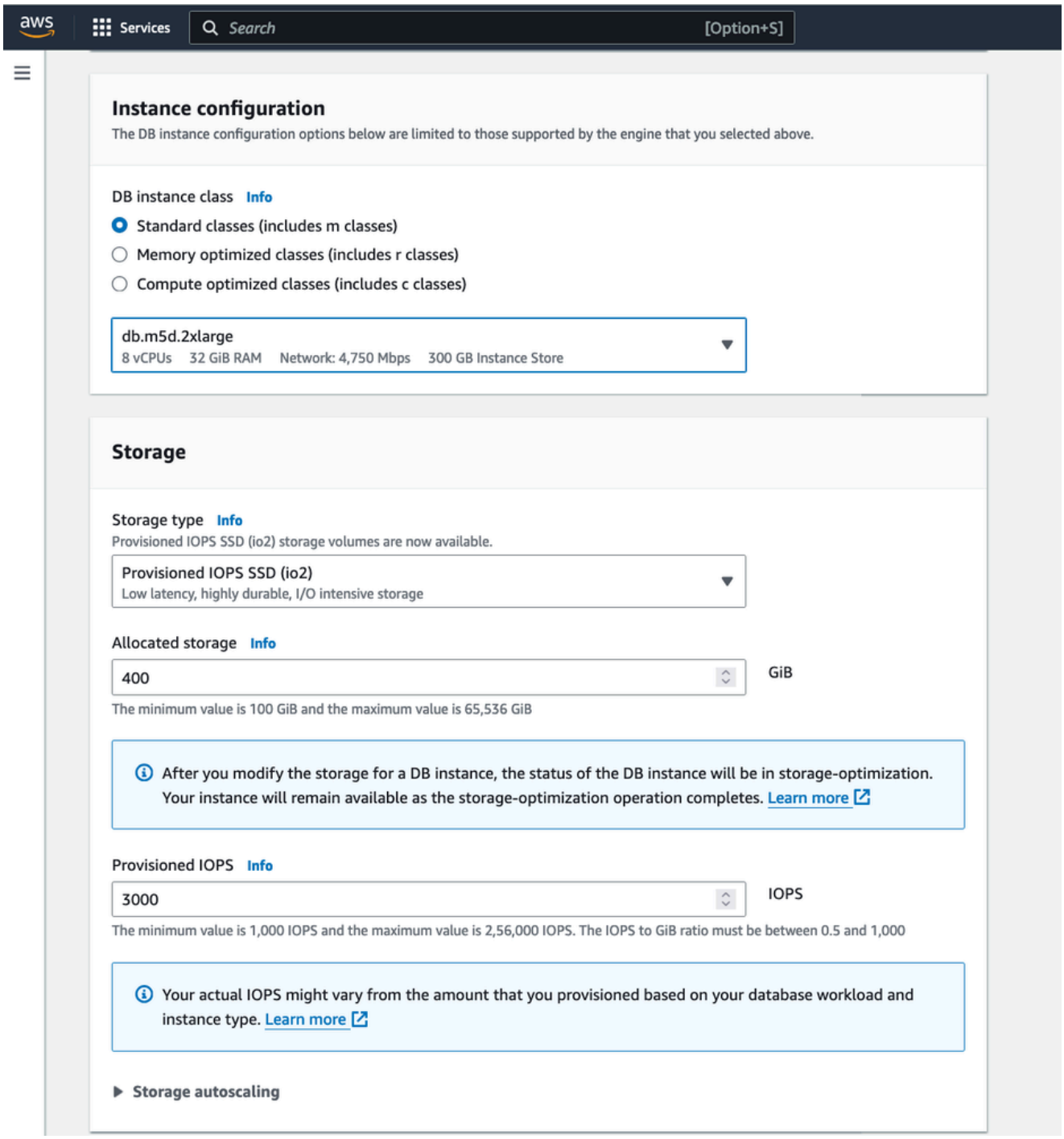


Verifique se as configurações padrão para "Tamanho da instância do banco de dados" e "Armazenamento" estão selecionadas.

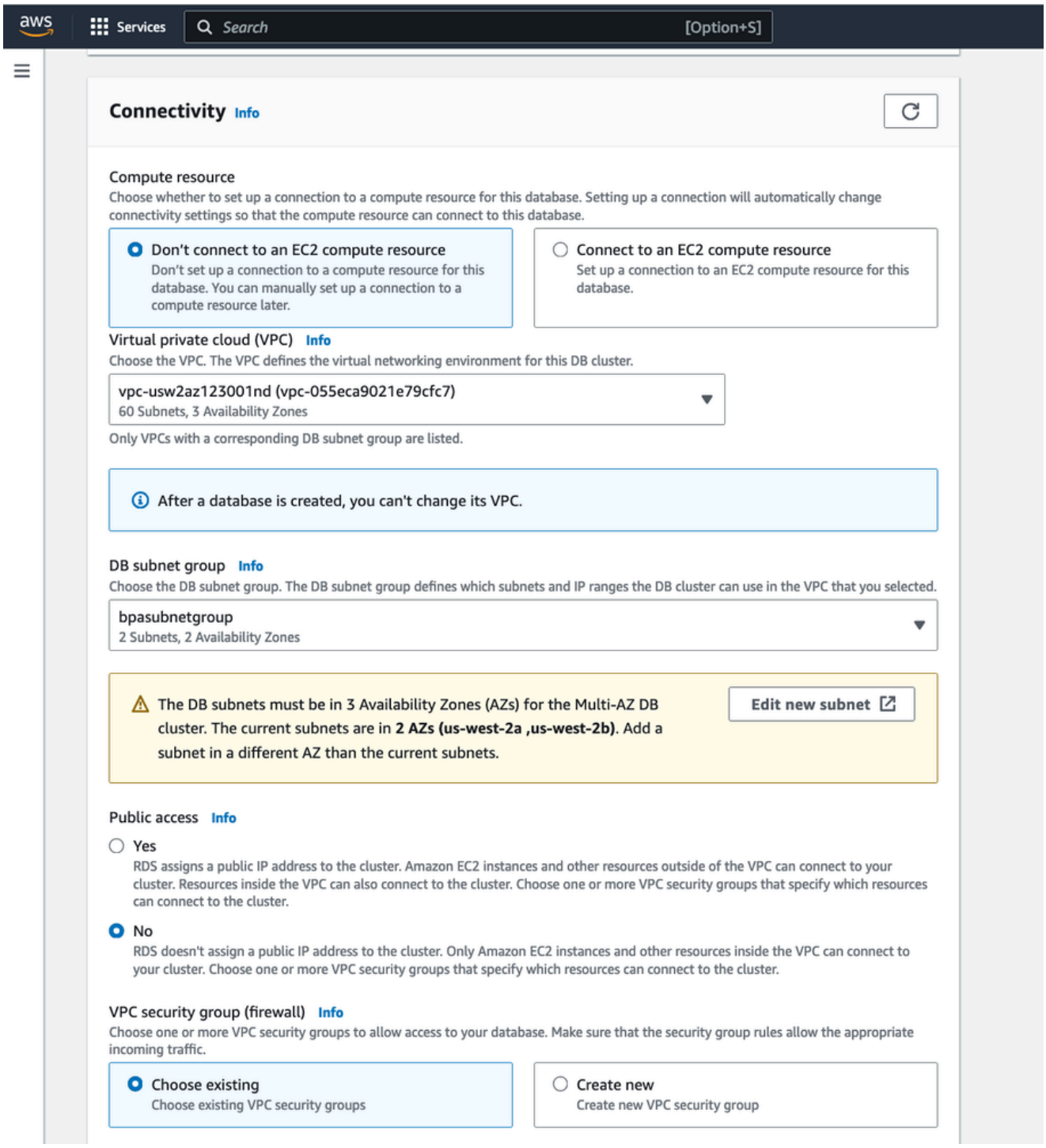
Dependendo do tamanho do cluster e dos requisitos de dados, selecione o tamanho apropriado da instância do banco de dados e o tipo de armazenamento.

Com base em nosso caso de uso, escolhemos a seguinte configuração:

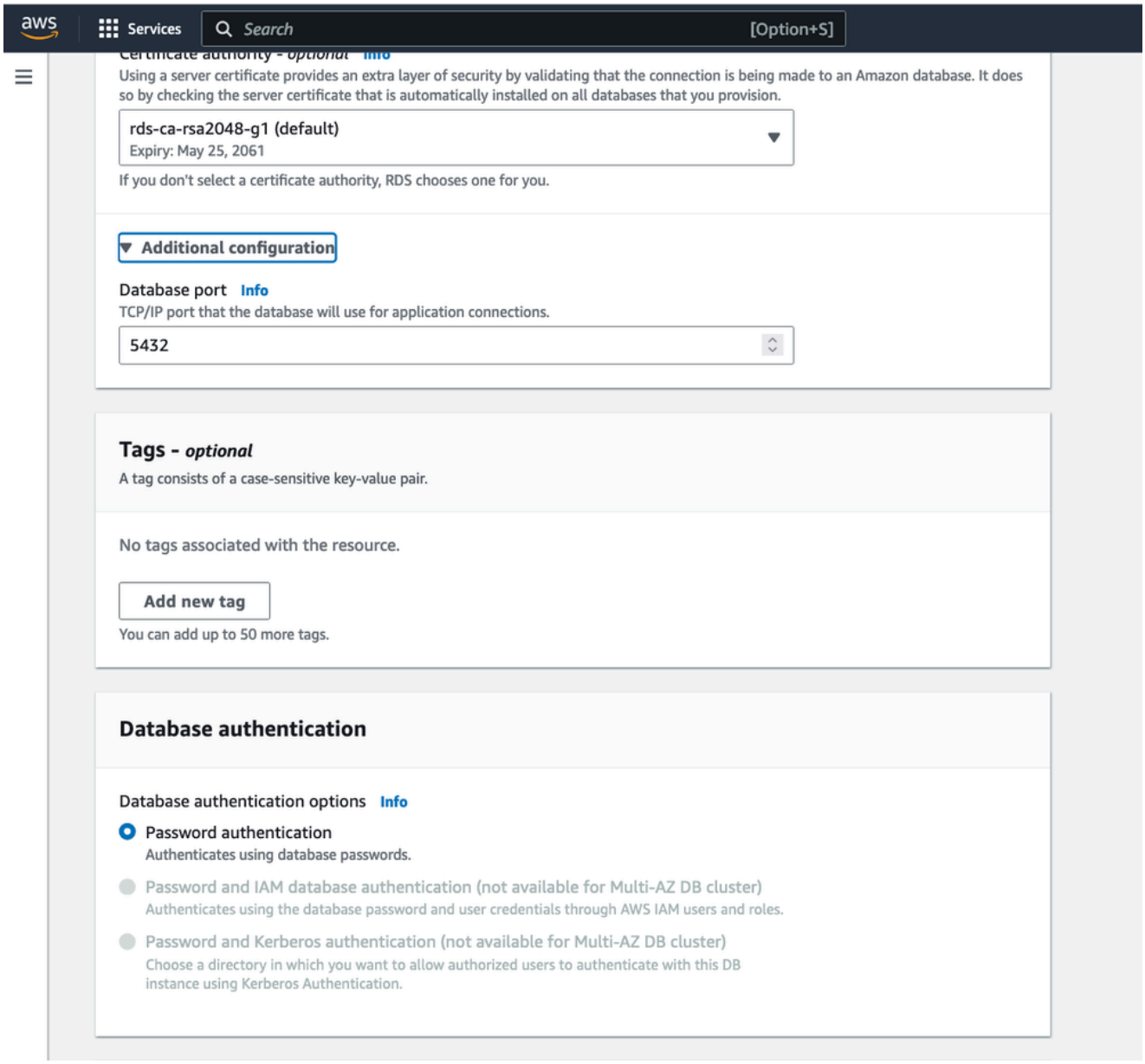
- **Tamanho da Instância do Banco de Dados**: db.m5d.2xlarge
    - 8 vCPUs
    - 32 GiB de RAM
    - Rede: 4.750 Mbps
    - Repositório de Instâncias de 300 GB

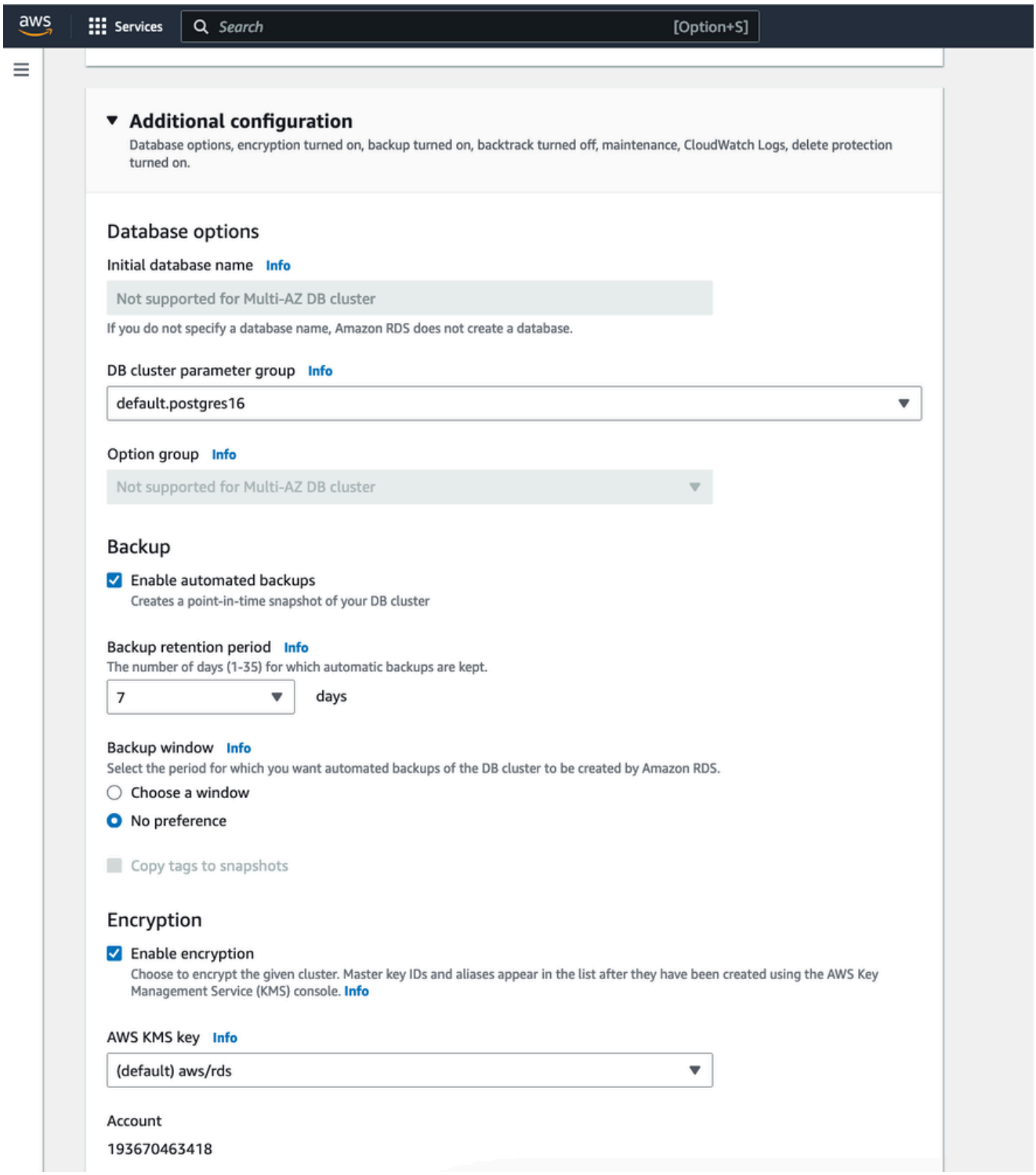


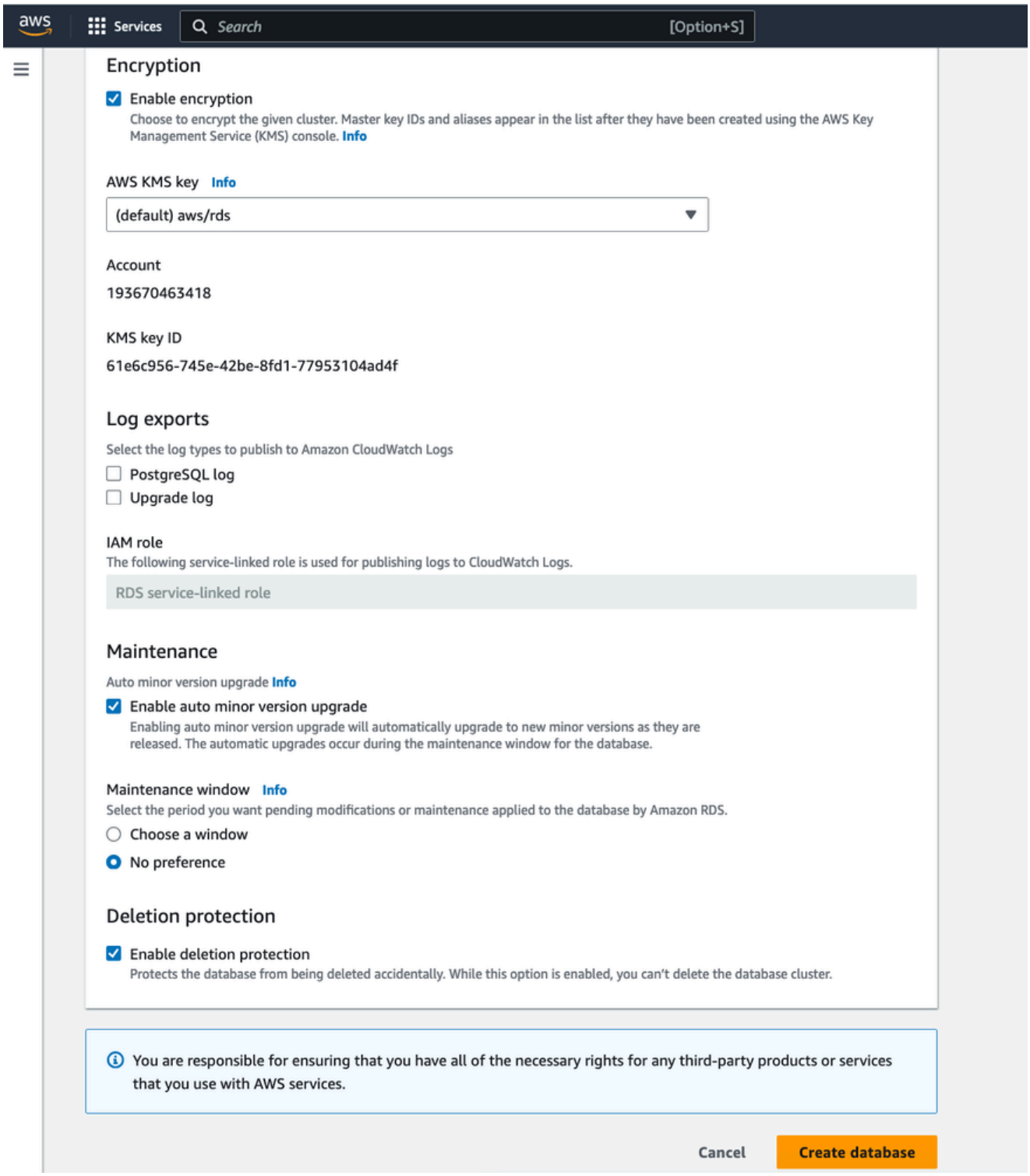
Selecione os valores apropriados de acordo com seu caso de uso. Selecionamos os valores padrão.



Verifique se em "Autenticação de banco de dados" selecionamos Autenticação de senha. Autentica usando senhas de banco de dados.


aws
Services
Search
[Option+S]
Certificate authority - optional Info
Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatically installed on all databases that you provision.
rds-ca-rsa2048-g1 (default)
Expiry: May 25, 2061
If you don't select a certificate authority, RDS chooses one for you.
Additional configuration
Database port Info
TCP/IP port that the database will use for application connections.
5432
Tags - optional
A tag consists of a case-sensitive key-value pair.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Database authentication
Database authentication options Info
Password authentication
Authenticates using database passwords.
Password and IAM database authentication (not available for Multi-AZ DB cluster)
Authenticates using the database password and user credentials through AWS IAM users and roles.
Password and Kerberos authentication (not available for Multi-AZ DB cluster)
Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

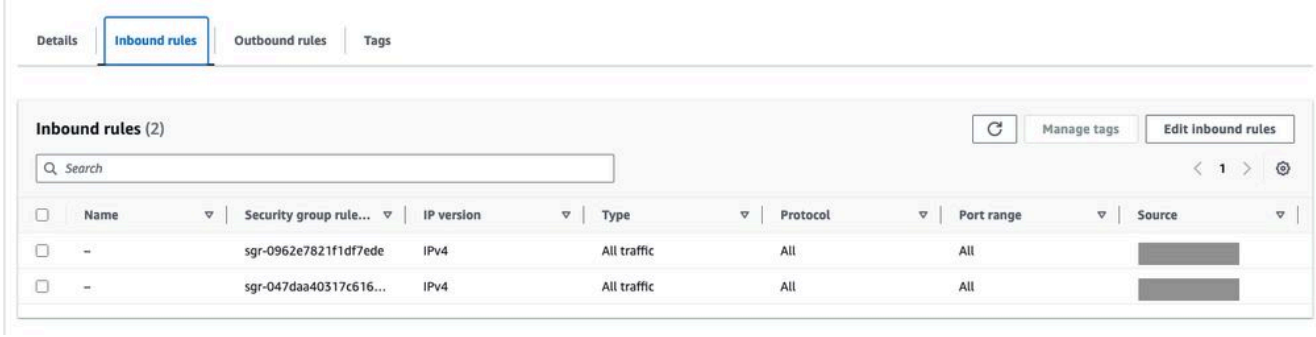

aws
Services
Search
[Option+S]
Additional configuration
Database options, encryption turned on, backup turned on, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned on.
Database options
Initial database name Info
Not supported for Multi-AZ DB cluster
If you do not specify a database name, Amazon RDS does not create a database.
DB cluster parameter group Info
default.postgres16
Option group Info
Not supported for Multi-AZ DB cluster
Backup
Enable automated backups
Creates a point-in-time snapshot of your DB cluster
Backup retention period Info
The number of days (1-35) for which automatic backups are kept.
7
days
Backup window Info
Select the period for which you want automated backups of the DB cluster to be created by Amazon RDS.
Choose a window
No preference
Copy tags to snapshots
Encryption
Enable encryption
Choose to encrypt the given cluster. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service (KMS) console. Info
AWS KMS key Info
(default) aws/rds
Account
193670463418



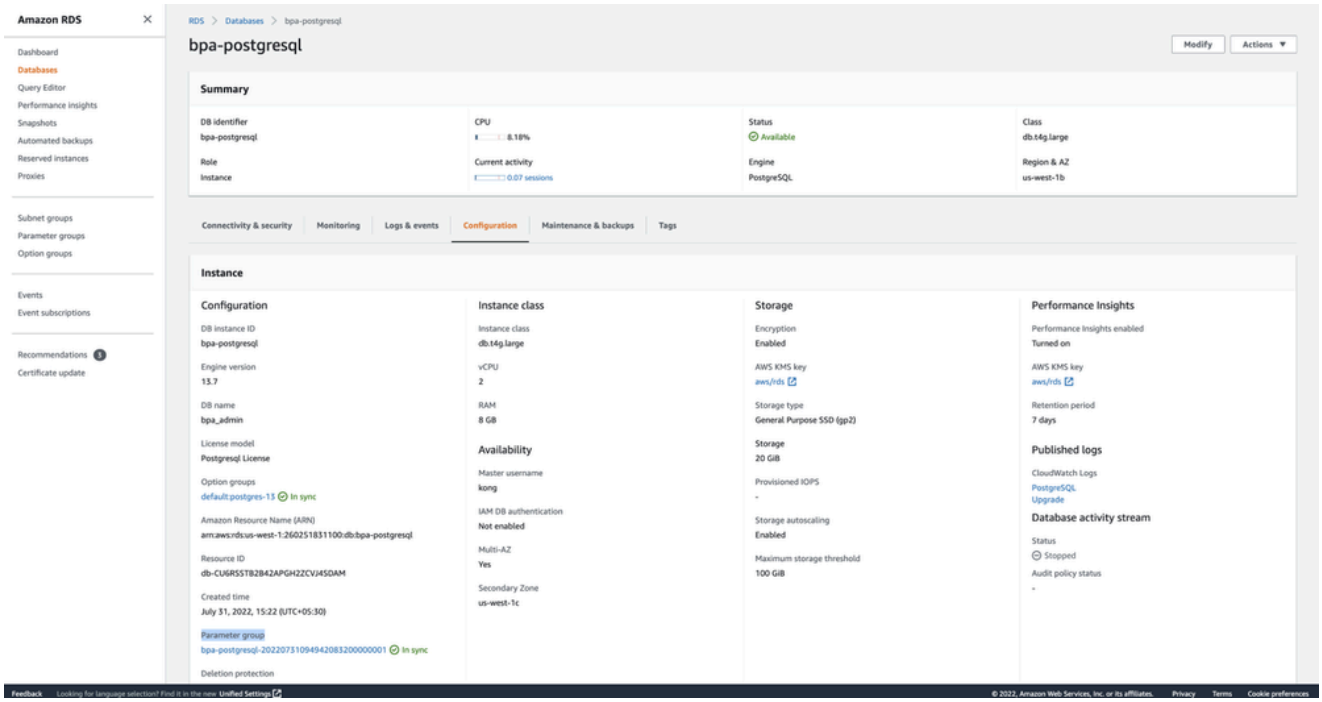
Uma vez verificado, estamos prontos para criar o banco de dados. Retorne ao painel do Amazon RDS. Confirme se a instância está disponível para uso.

Regras do Grupo de Segurança

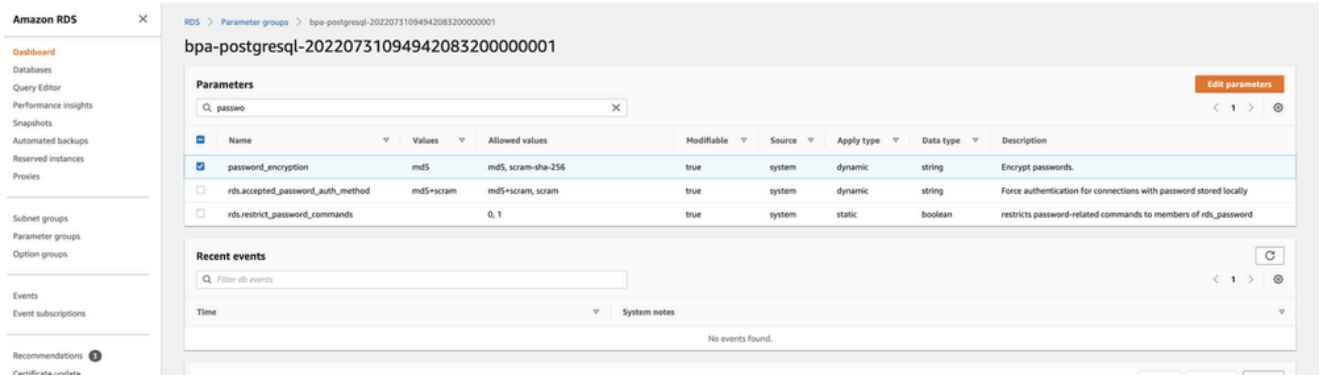
Atualize o grupo de segurança de entrada com os blocos pod CIDR e node CIDR.



Em RDS -> Bancos de dados -> DB-NAME, clique em configuração, consulte a seção Grupo de parâmetros e clique no grupo de parâmetros a ser exibido.



Procure "password_encryption" e altere o valor para md5 de branco / outro valor. Isso é necessário para que as configurações de camunda funcionem.



Crie esses Bancos de Dados junto com os usuários conectando-se ao RDS.

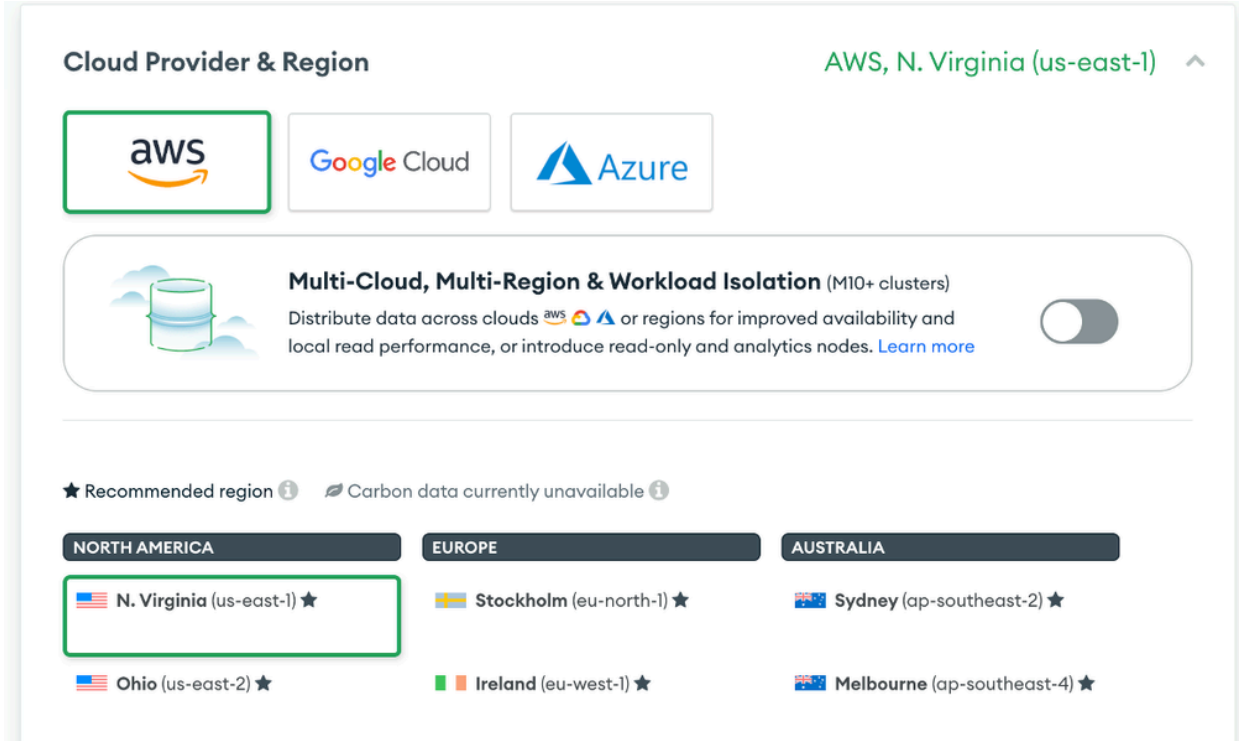
```
PG_ROOT_DATABASE=admin
PG_INITDB_ROOT_USERNAME=admin
PG_INITDB_ROOT_PASSWORD=Bp@Chang3d!
AUTH_DB_NAME=kong
AUTH_DB_USER=kong
AUTH_DB_PASSWORD=K@ngPwdCha*g3
WFE_DB_USER=camunda
WFE_DB_PASSWORD=WOrkFlo#ChangeNow
WFE_DB_NAME=process-engine
```

- Autenticação de senha

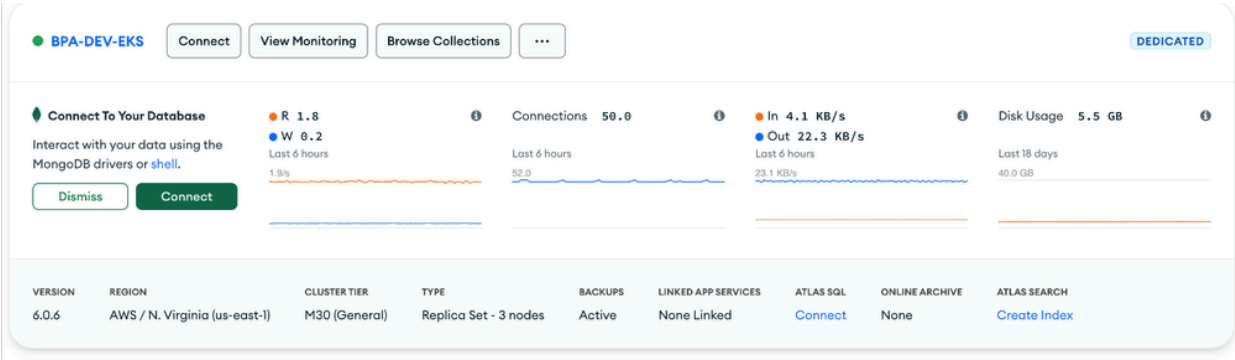
  Autentica usando senhas de banco de dados.

- **Configuração do Atlas MongoDB**
  A criação da Atlas MongoDB envolve:
  - **Fazendo login no Atlas MongoDB.**
  - **Selecionando a organização e o projeto.**
  - **Criar um cluster dedicado com as especificações apropriadas.**

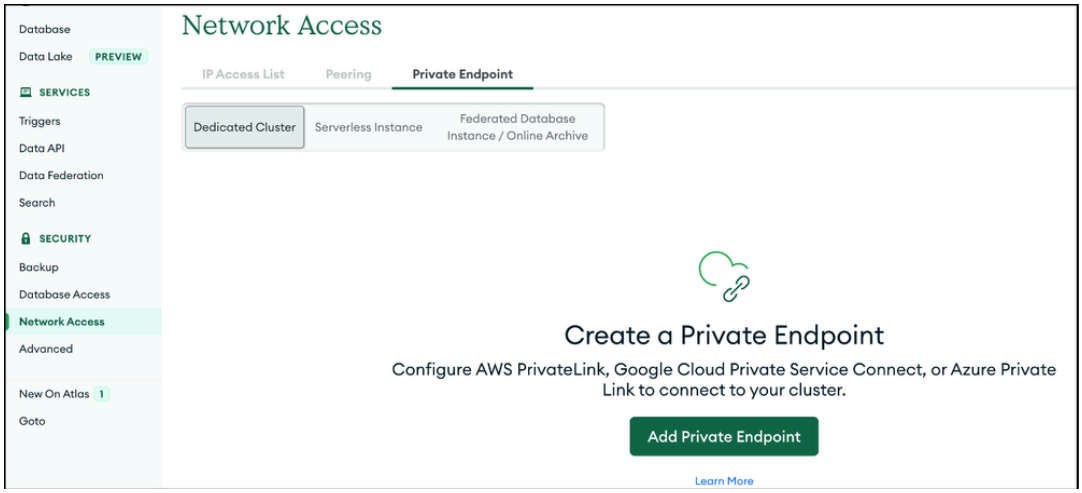
  - **Selecione a camada Dedicada, Provedor de nuvem e Região.**



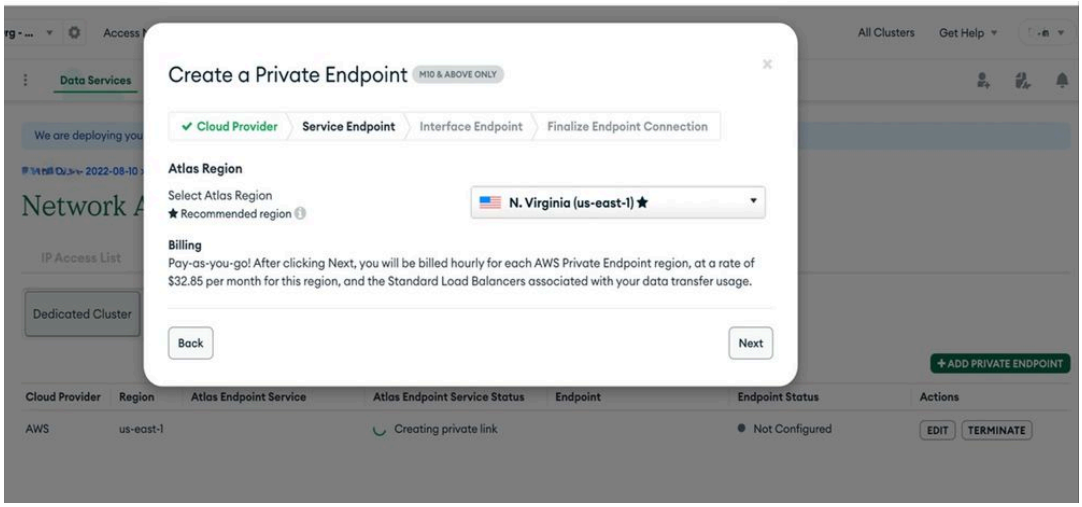
- **Selecione a camada apropriada (usamos M30 como camada) do cluster dedicado e forneça o nome do cluster apropriado e clique em Criar cluster. Inicializará o cluster monogodb Atlas.**



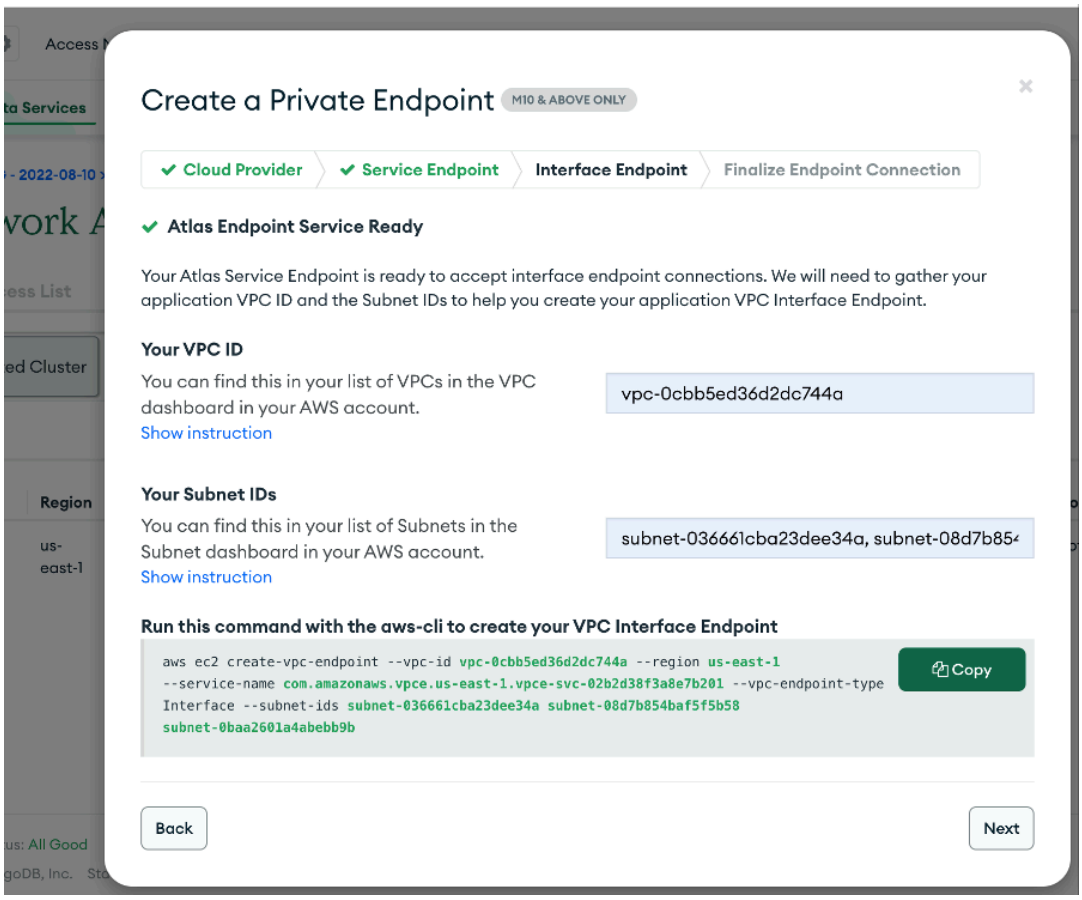
- **Configuração de endpoint privado de VPC para o cluster Atlas e K8S.**
  - **Clique em Network Access Select Private Endpoint à Clique em Add Private Endpoint.**



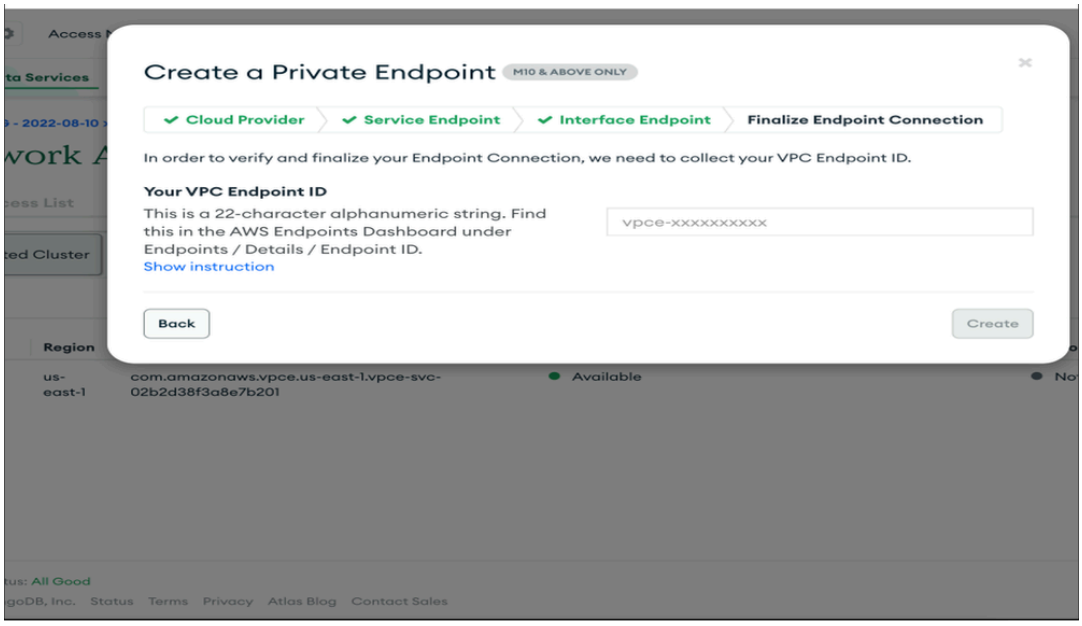
  - **Selecione Cloud Provider como AWS, selecione a respectiva região e clique em Next.**



- **Forneça o respectivo ID de PVC e ID de sub-rede. Depois de inserir os detalhes, copie o comando vpc end point creation e execute-o no console aws. Você obterá o id do ponto de extremidade do vpc como saída.**

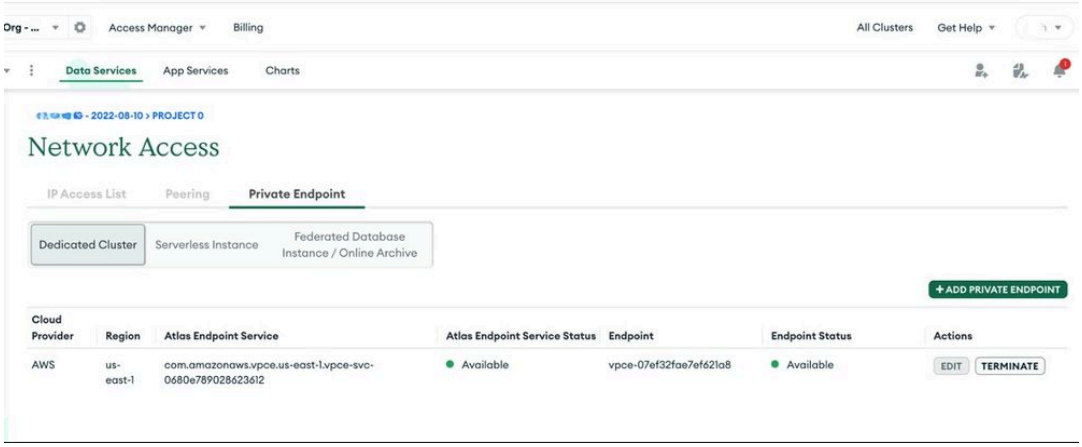


- **Clique em Avançar para colar a ID do endpoint do VPC e clique em Criar.**

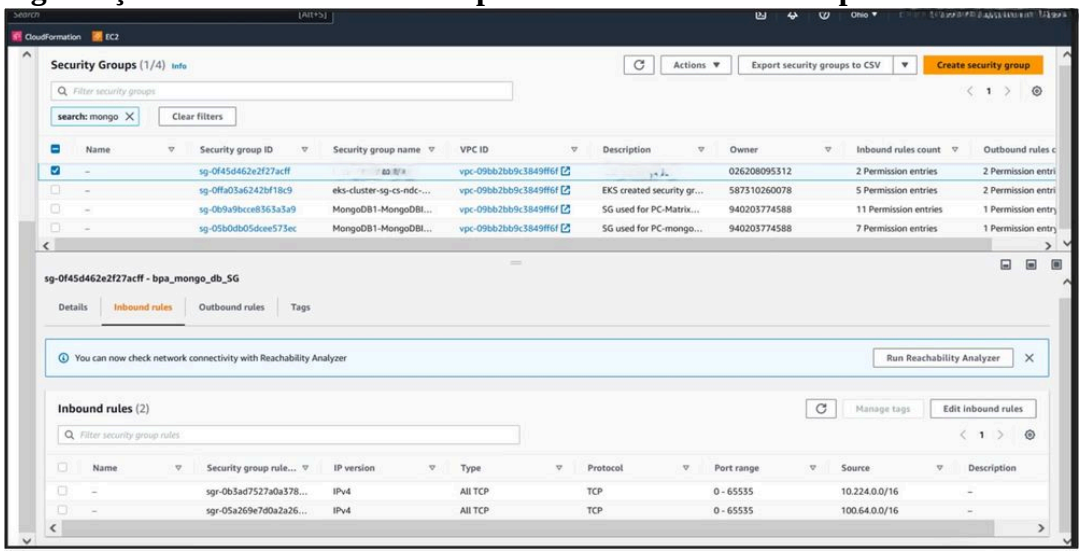


- **Depois de criado com êxito, o status do endpoint estará disponível, como**

mostrado na imagem a seguir. O ponto final do VPC deve ser criado para o pod cidr. No nosso caso, usamos "100.64.0.0/16" .



- **Adicione regras de entrada ao ponto de extremidade do vpc recém-criado. O ponto de extremidade do vpc estará na conta principal e um grupo de segurança deverá ser atribuído ao ponto de extremidade do vpc recém-criado.**



ECR como registro de imagens

Criar repositórios Amazon ECR e enviar imagens Docker para eles envolve várias etapas. Estas são as etapas para criar um repositório ECR, marcar uma imagem do Docker e enviá-la para o repositório usando a CLI do AWS.

```
aws ecr create-repository --repository-name your-image-name --region your-region
```

Substituir:

- **nome-da-imagem-**com o nome desejado para o repositório ECR.

- **your-**regioncom sua região AWS

Configurar Função IAM para Nós EKS

Certifique-se de que os nós de trabalho EKS (instâncias EC2) tenham a função IAM necessária anexada com permissões para receber imagens do ECR. A política IAM necessária é:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability"
      ],
      "Resource": "*"
    }
  ]
}
```

Anexe essa política à função IAM associada aos nós de trabalho EKS.

Implantação de BPA
A implantação do BPA envolve várias etapas, incluindo rotular os nós de trabalho EKS, preparar diretórios nos nós, copiar pacotes BPA e implantar o BPA usando Helm.

Para a implantação de nossos clientes, utilizamos as seguintes versões de software e serviços em nuvem:

- **BPA:** 4.0.3-6
- **RDS (Serviço de Banco de Dados Relacional)**: 16.3-R2
- **Atlas MongoDB**: v5.0.29
- **EKS (Elastic Kubernetes Service)**: v1.27

Esses componentes garantem que nossa implantação seja robusta, escalável e capaz de lidar com as cargas de trabalho necessárias de forma eficiente.

- **Rotulando nós de trabalho EKS**

```
kubectl label node
```

```
name=node-1 kubectl label node

name=node-2 kubectl label node

name=node-3 kubectl label node

name=node-4
```

- **Preparando Diretórios em Nós**
  Nó 1:

```
rm -rf /opt/bpa/data/
mkdir -p /opt/bpa/data/zookeeper1
mkdir -p /opt/bpa/data/zookeeper4
mkdir -p /opt/bpa/data/zookeeper5
chmod 777 /opt/bpa/data/zookeeper1
chmod 777 /opt/bpa/data/zookeeper4
chmod 777 /opt/bpa/data/zookeeper5
mkdir -p /opt/bpa/data/kafka1
chmod 777 /opt/bpa/data/kafka1
sysctl -w vm.max_map_count=262144
```

  Nó 2:

```
rm -rf /opt/bpa/data
sysctl -w vm.max_map_count=262144
mkdir -p /opt/bpa/data/kafka2
mkdir -p /opt/bpa/data/zookeeper2
mkdir -p /opt/bpa/data/zookeeper4
mkdir -p /opt/bpa/data/zookeeper5
chmod 777 /opt/bpa/data/kafka2
```

```
chmod 777 /opt/bpa/data/zookeeper2
chmod 777 /opt/bpa/data/zookeeper4
chmod 777 /opt/bpa/data/zookeeper5
```

Nó 3:

```
rm -rf /opt/bpa/data
sysctl -w vm.max_map_count=262144
mkdir -p /opt/bpa/data/kafka3
mkdir -p /opt/bpa/data/zookeeper3
mkdir -p /opt/bpa/data/zookeeper4
mkdir -p /opt/bpa/data/zookeeper5
chmod 777 /opt/bpa/data/kafka3
chmod 777 /opt/bpa/data/zookeeper3
chmod 777 /opt/bpa/data/zookeeper4
chmod 777 /opt/bpa/data/zookeeper5
```

Nó 4:

```
mkdir -p /opt/bpa/data/elk
mkdir -p /opt/bpa/data/metrices/prometheus
mkdir -p /opt/bpa/data/metrices/grafana
chmod 777 /opt/bpa/data/metrices
chmod 777 /opt/bpa/data/metrices/prometheus
chmod 777 /opt/bpa/data/metrices/grafana
sysctl -w vm.max_map_count=262144
```

- Copiando pacotes BPA

```
scp -r packages to node1:/opt/bpa/
scp -r packages to node2:/opt/bpa/
scp -r packages to node3:/opt/bpa/
scp -r packages to node4:/opt/bpa/
```

- Implantação do BPA usando Helm

```
helm install bpa-rel --create-namespace --namespace bpa-ns /opt/EKS/bpa-helm-chart
```

Configuração de ingresso

- **Ativando o ingresso**
  Atualize `values.`yamlpara habilitar o ingresso:

```
ingress_controller: {create: true}
```

- **Criando um segredo usando o certificado BPA**
  Navegue até o diretório do certificado e crie um segredo:

```
cd /opt/bpa/
```

```
/bpa/conf/common/certs/ kubectl create secret tls bpa-certificate-ingress --cert=bap-cert
```

- **Atualizando controlador de ingresso**
  Adicione o segredo recém-criado no **`ingress-controller.yaml`** arquivo:

```
cd /opt/bpa/
```

```
/templates/ vi ingress-controller.yaml "- --default-ssl-certificate=$(POD_NAMESPACE)/bpa-
```

- **Atualizando certificado de entrada**
  Execute a exclusão e instalação de Helm para atualizar o certificado de entrada.

Especificações ambientais
As especificações de ambiente incluem requisitos para instâncias EC2, balanceadores de carga, terminais de VPC e instâncias de RDS. As principais especificações são:

Requisitos CE2:

Requisitos de armazenamento:2 TB de espaço por nós. Monte o volume EBS em /opt e adicione uma entrada em /etc/fstab para todos os nós.

Entrada do grupo de segurança: 30101, 443, 0 - 65535 TCP, 22 para ssh.

Saída do grupo de segurança: todo o tráfego deve ser habilitado.

DNS Resolver: EC2 deve ter resolvedores locais em /etc/resolve.conf.

Requisitos do balanceador de carga:

- As portas de ouvintes devem ser 443, 30101.
- Requisitos para terminais VPC (Atlas MongoDB).
- Os pontos de extremidade VPC criados para a conectividade Atlas estão disponíveis na conta principal (aws-5g-ndc-prod). O Ponto de Extremidade VPC deve ter um grupo de segurança que permita todo o acesso de entrada (0 a 65535).

Requisitos do RDS:

Tipo de RDS: db.r5b.2xlarge

Versão do mecanismo Postgres: 13.7

Grupo de segurança: a entrada deve permitir o tráfego da origem CIDR do POD.

Principais conceitos e componentes
Entender os fundamentos do Kubernetes é essencial para implantar e gerenciar aplicativos com eficiência usando o Amazon EKS.

Conclusão
Este documento fornece um guia detalhado para a implantação e o gerenciamento de aplicativos BPA (Business Process Automation, automação de processos de negócios) usando o Amazon EKS. Seguindo as etapas descritas e compreendendo os conceitos principais, as empresas podem aproveitar os benefícios do EKS para seus aplicativos BPA em contêineres.

Referências

- **Amazon Web Services, "Documentação do Amazon EKS" [Online]. Disponível:https://docs.aws.amazon.com/eks/**
- **Kubernetes, "Documentação do Kubernetes," [Online]. Disponível:https://kubernetes.io/docs/home/**
- **Introdução ao Cisco BPA https://www.cisco.com/c/en/us/solutions/collateral/service-provider/at-a-glance-c45-742579.html**
- **Guia de operações do BPA https://www.cisco.com/c/dam/en/us/support/docs/bpa/v403/cisco-bpa-operations-guide-v403.pdf**
- **Guia do desenvolvedor de BPA https://www.cisco.com/c/dam/en/us/support/docs/bpa/v403/cisco-bpa-developer-guide-v403.pdf**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.