在Amazon EKS上部署和管理业务流程自动化应用程序：实用指南

目录

摘要

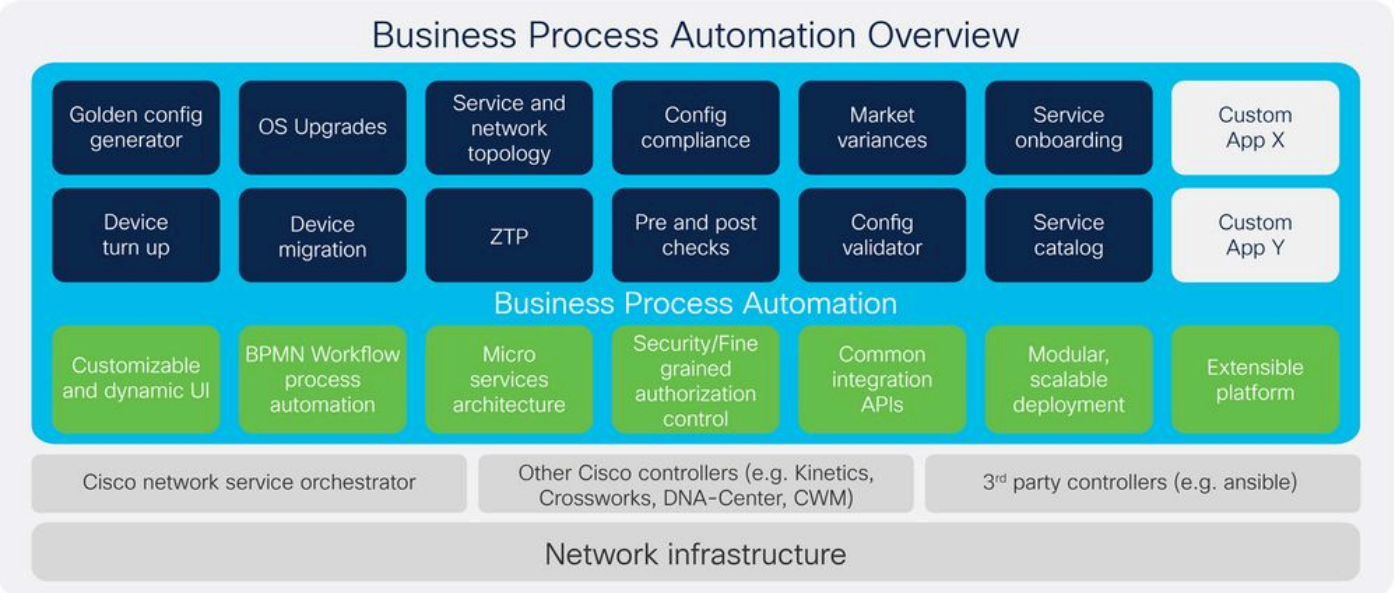
本文为使用Amazon Elastic Kubernetes Service (EKS)部署和管理业务流程自动化(BPA)应用提供了综合指南。它概述了前提条件，强调了利用EKS的优势，并提供了设置EKS集群、Amazon RDS数据库和MongoDB Atlas的分步说明。此外，本文还深入探讨了部署架构并明确了环境要求，为旨在将EKS用于其容器化BPA应用的组织提供了全面的资源。

关键字

Amazon EKS、Kubernetes、AWS、RDS、MongoDB Atlas、DevOps、云计算、业务流程自动化。

简介

BPA



在当今的数字时代，企业寻求简化和自动化各种IT环境中的复杂业务流程。业务流程自动化(BPA)已成为一项关键技术，使组织能够提高运营效率、减少错误并改进服务交付。BPA引入了多项关键创新和增强功能，旨在推进工作流程自动化、服务调配和现成自动化应用。

BPA平台托管业务和IT/运营使用案例和应用，例如操作系统升级、服务调配以及与协调引擎的集成。客户可以获得服务生命周期和BPA功能，包括通过思科专家提供的咨询、实施、关键业务服务和解决方案支持、最佳实践，以及有助于自动化业务流程和降低系统风险的经验证的技术和方法。

这些生命周期功能可以基于订用，也可以根据个人需求进行定制。实施服务有助于定义、集成和部署工具和流程，从而加速自动化。思科专家会执行收集需求的正式流程，基于灵活的流程和持续集成与持续交付(CICD)工具设计和开发用户案例，并通过自动测试新的或现有的工作流程、设备和服务来实施灵活的服务。借助解决方案支持，客户可获得全天候的集中式支持（专注于以软件为中心的问题），以及通过思科分层软件模型提供的多供应商和开源支持。思科解决方案支持专家帮助管理您的问题，从首次致电到最终解决，并充当同时与多个供应商进行沟通的主要联系人。与解决方案级专家合作，您可以减少多达44%的问题，从而帮助您保持业务连续性并更快实现BPA投资回报。

关键的技术功能，例如支持FMC和Ansible管理的设备、使用高级排队框架(AQF)的并行执行，以及NDFC和FMC设备的扩展配置合规性，将BPA定位为大规模企业自动化的全面解决方案。该版本增加了在SD-WAN管理、设备自注册和防火墙策略监管方面的功能，解决了网络安全和自动化的关键方面，满足了大规模、多供应商环境的需求。

EKS

Amazon Elastic Kubernetes Service (EKS)是由Amazon Web Services (AWS)提供的完全托管的Kubernetes服务。EKS于2018年推出，它使用开源容器协调平台Kubernetes简化容器化应用的部署、管理和扩展流程。EKS将Kubernetes群集管理的复杂性抽象化，使开发人员能够专注于构建和运行应用程序，而无需处理底层基础设施。

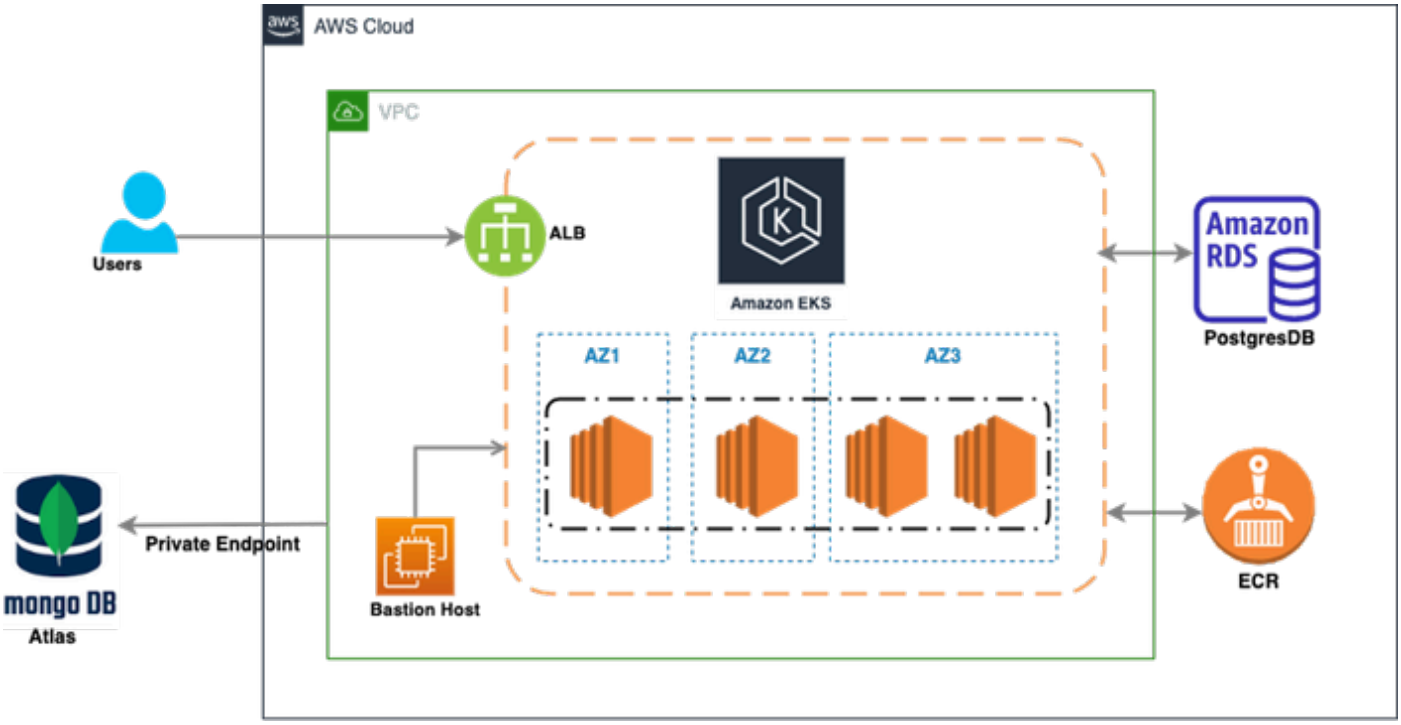
使用Amazon EKS进行应用程序部署的优势

Amazon EKS提供多种应用程序部署优势，使其成为利用容器化应用程序和微服务的组织的热门选择。

主要优势包括：

- **托管Kubernetes控制平面**：EKS处理Kubernetes控制平面的部署、扩展和维护，减少运营负担。
- 简化的集群管理：EKS将设置和管理Kubernetes集群的复杂性抽象化。
- **可扩展性**：EKS允许轻松扩展集群，以适应不断增长的工作负载。
- **高可用性**：EKS支持多可用性区域部署，从而增强可用性和容错能力。
- 与**AWS服务集成**：EKS与各种AWS服务无缝集成。
- **DevOps自动化**：EKS支持容器化应用的持续集成和持续部署(CI/CD)。

BPA部署架构



此图像表示在**AWS**上部署的基于云的基础设施的高级架构，使用几个关键组件。下面是图表的细分：

1. **Amazon EKS (Elastic Kubernetes Service)**：在图示的核心，Amazon EKS跨三个可用区域(AZ1、AZ2、AZ3)部署，每个区域内有Kubernetes工作节点。这表示高可用性和容错设置，因为工作负载分布在多个可用性区域。

2. **ALB（应用负载均衡器）**：此模块位于前端，从用户接收流量并将其分配到EKS集群以处理应用工作负载。负载均衡器可确保均匀分配请求，并可处理基于流量需求的扩展。

3. **Amazon RDS (Relational Database Service)** - PostgreSQL：在图表的右侧，存在运行PostgreSQL的Amazon RDS实例。在EKS群集中运行的应用程序可以访问此数据库。

4. **ECR(Elastic Container Registry)**：这是Docker容器映像的存储和管理位置，然后将其部署到Amazon EKS以运行工作负载。

5. **MongoDB Atlas**：在左侧，MongoDB Atlas通过专用终端集成到架构中。MongoDB Atlas是云托管的NoSQL数据库服务，在此处用于处理基于文档的数据库要求。专用终端可确保MongoDB Atlas实例与其他AWS组件之间的安全专用通信。

6. **Bastion Host**：位于VPC（虚拟私有云）内，可为管理员提供安全的入口点以访问VPC内的资源，而无需直接将其暴露于互联网。

总体而言，此架构为使用Amazon EKS部署和管理容器化应用提供了高度可用、可扩展且安全的解决方案，同时支持关系(PostgreSQL)和NoSQL (MongoDB)数据库。

- **EKS集群设置**

要使用AWS CLI创建Amazon EKS集群，可使用`eksctl`命令行实用程序。以下是命令示例：

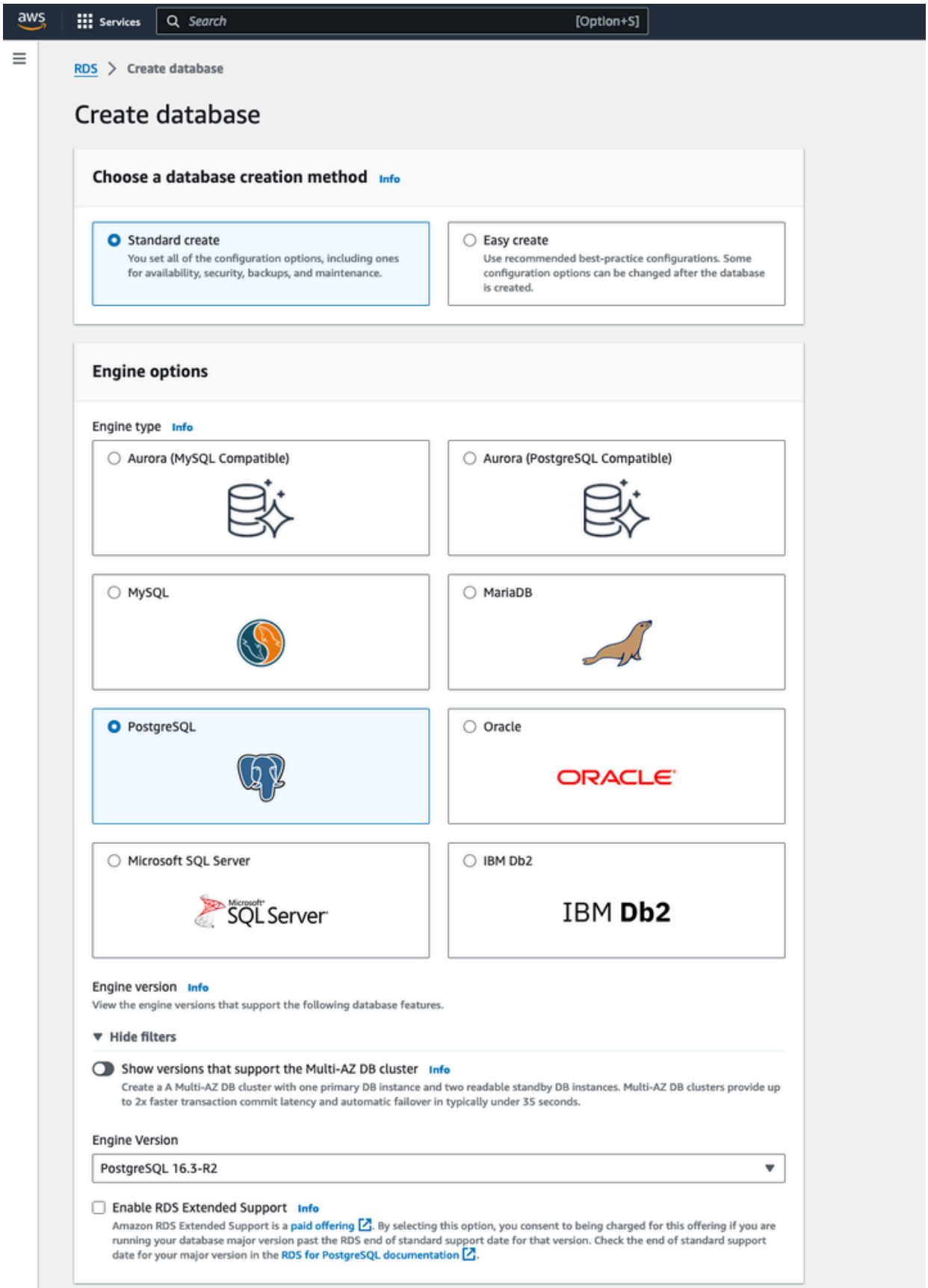
```
eksctl create cluster \
  --name
```

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

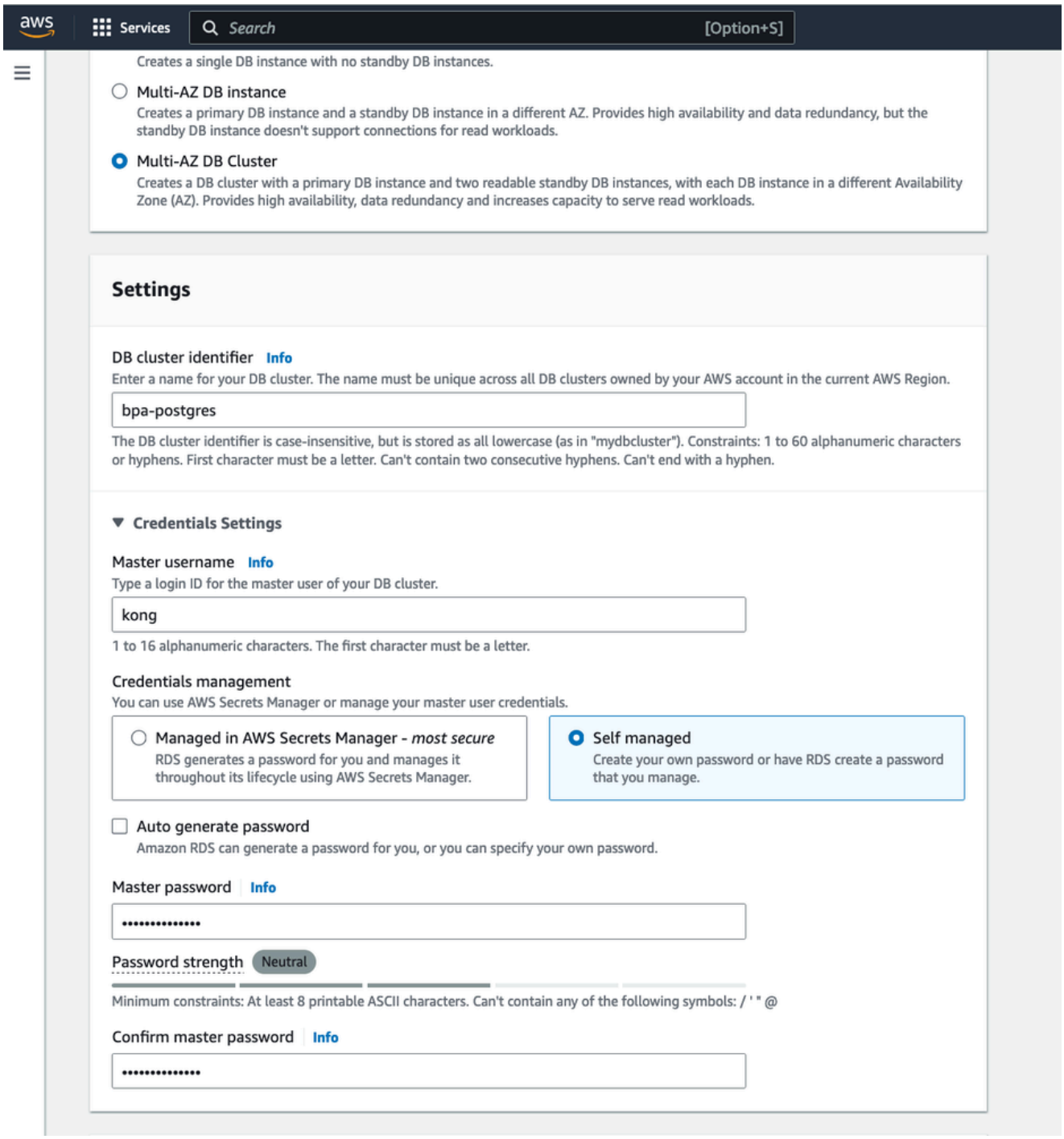
- **RDS数据库设置**

  在Amazon RDS上部署关系数据库涉及以下步骤：

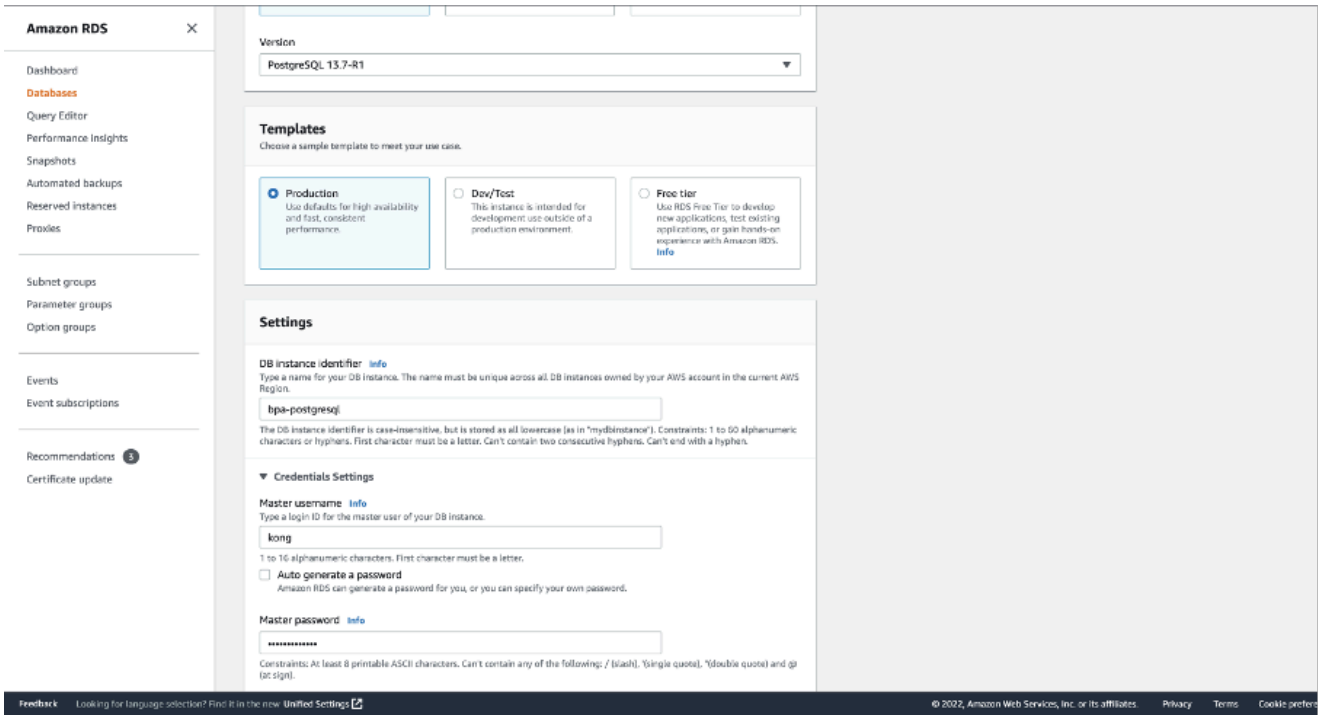
  - 访问AWS管理控制台并导航至Amazon RDS服务。
  - 按照所需的规格创建新的数据库实例。
  - 配置安全组以允许来自Amazon EKS集群的传入连接。



使用下拉菜单，选择PostgreSQL的最新版本。在本例中，它是“PostgreSQL 16.3-R1”。



为此，请为数据库实例指定名称并创建用户名和口令。

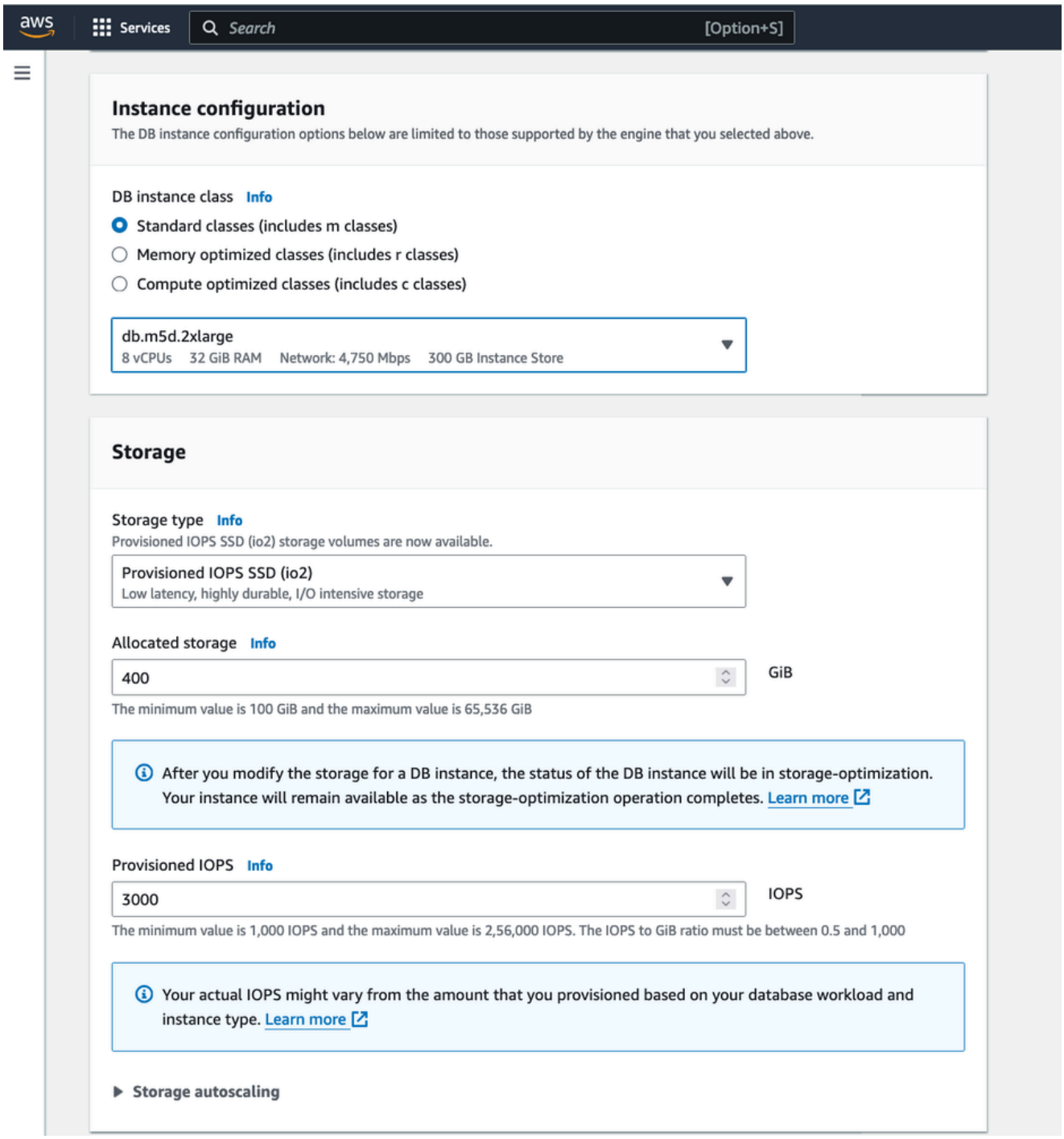


确保选中“数据库实例大小”和“存储”的默认设置。

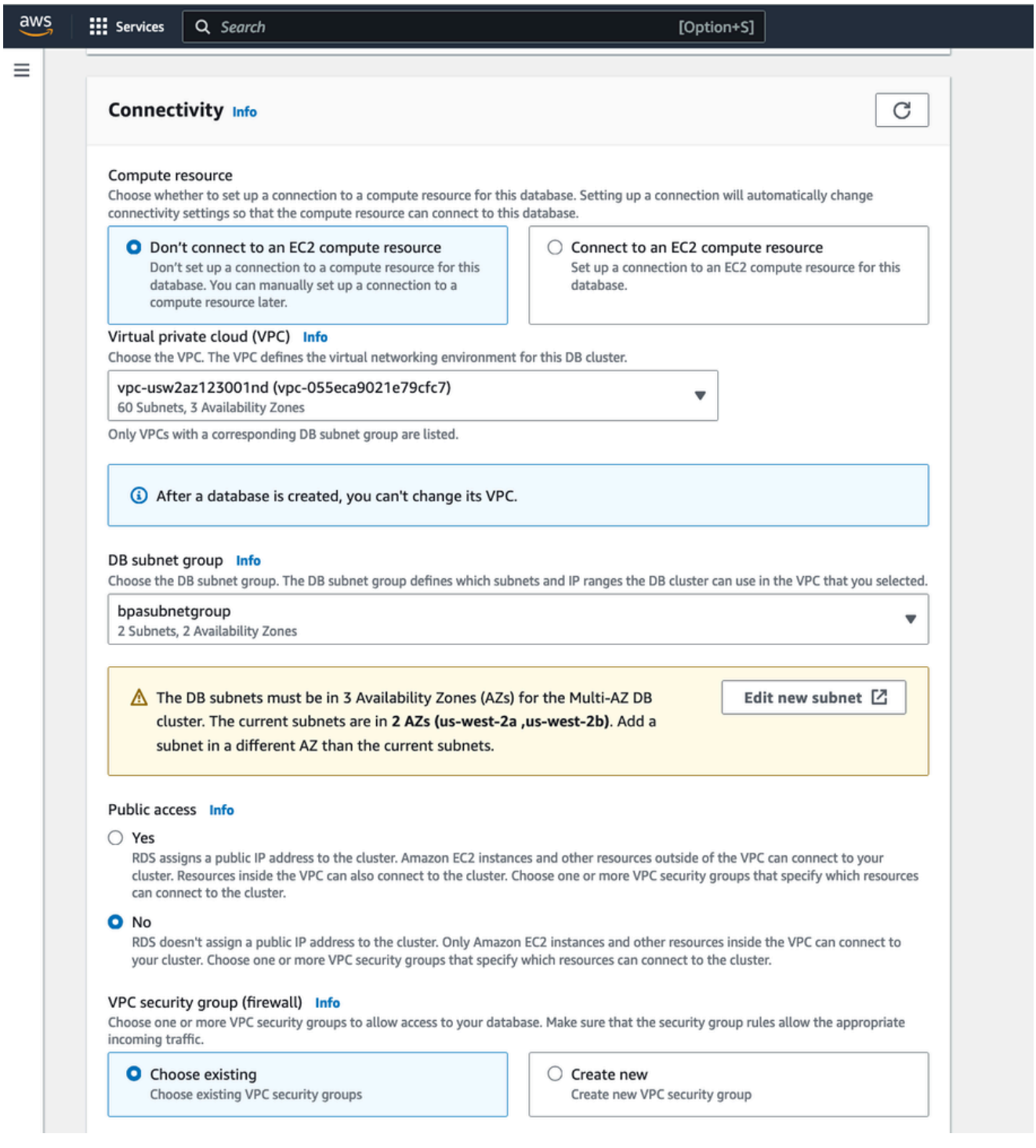
根据群集大小和数据要求，选择适当的数据库实例大小和存储类型。

根据我们的使用案例，我们选择了以下配置：

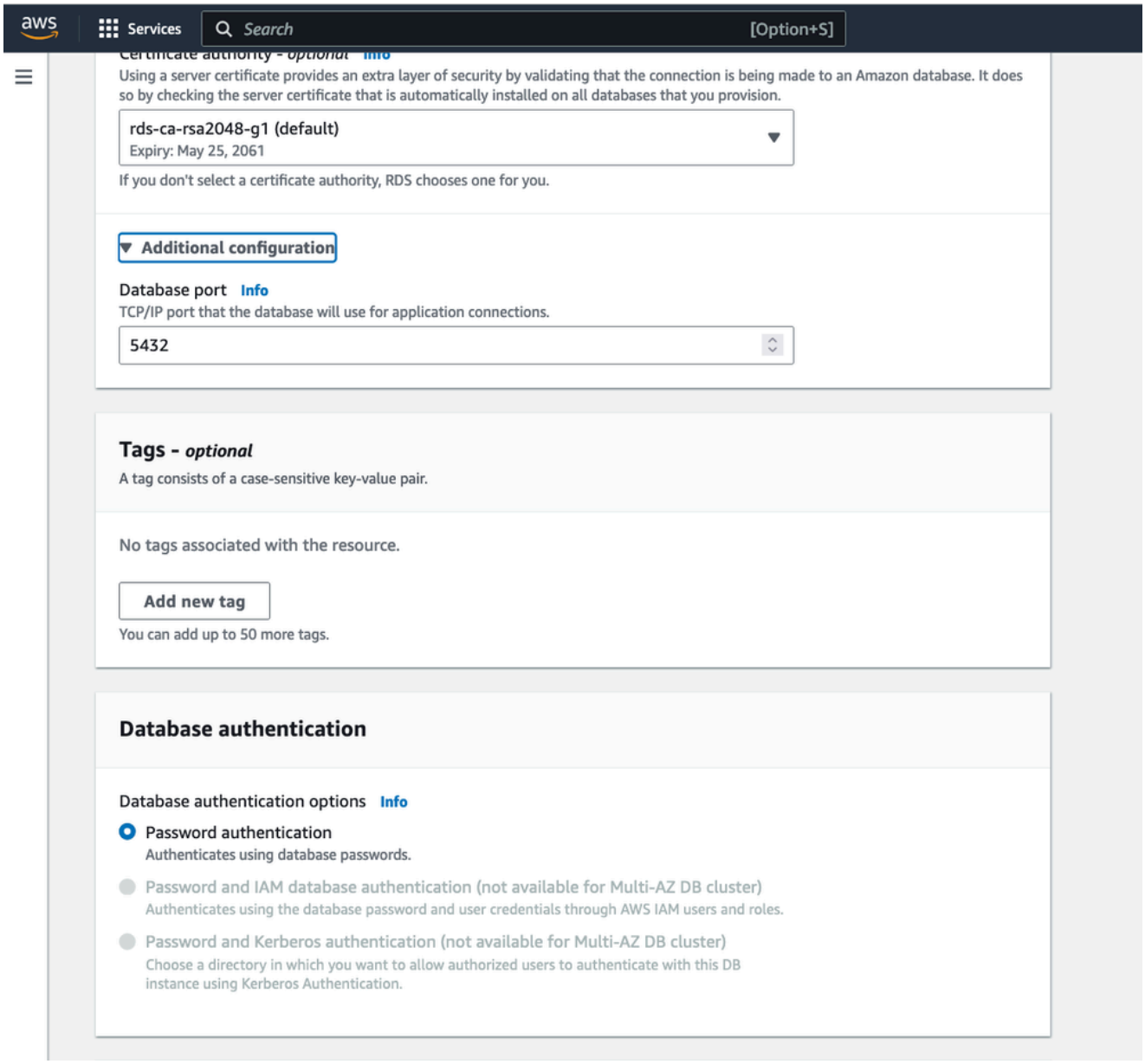
- 数据库实例大小：db.m5d.2xlarge
    - 8 个 vCPU
    - 32 GiB内存
    - 网络：4,750 Mbps
    - 300 GB实例存储

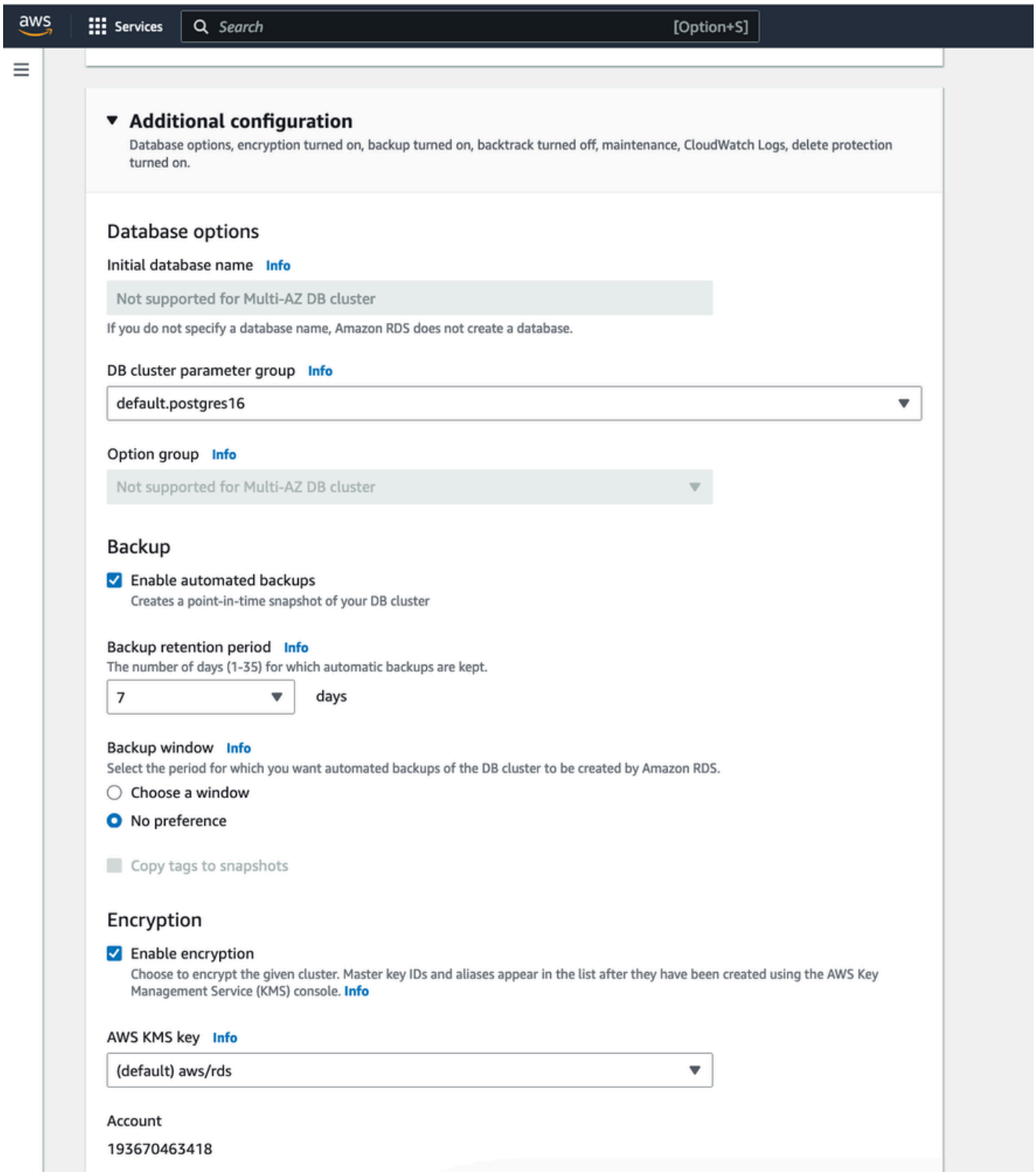


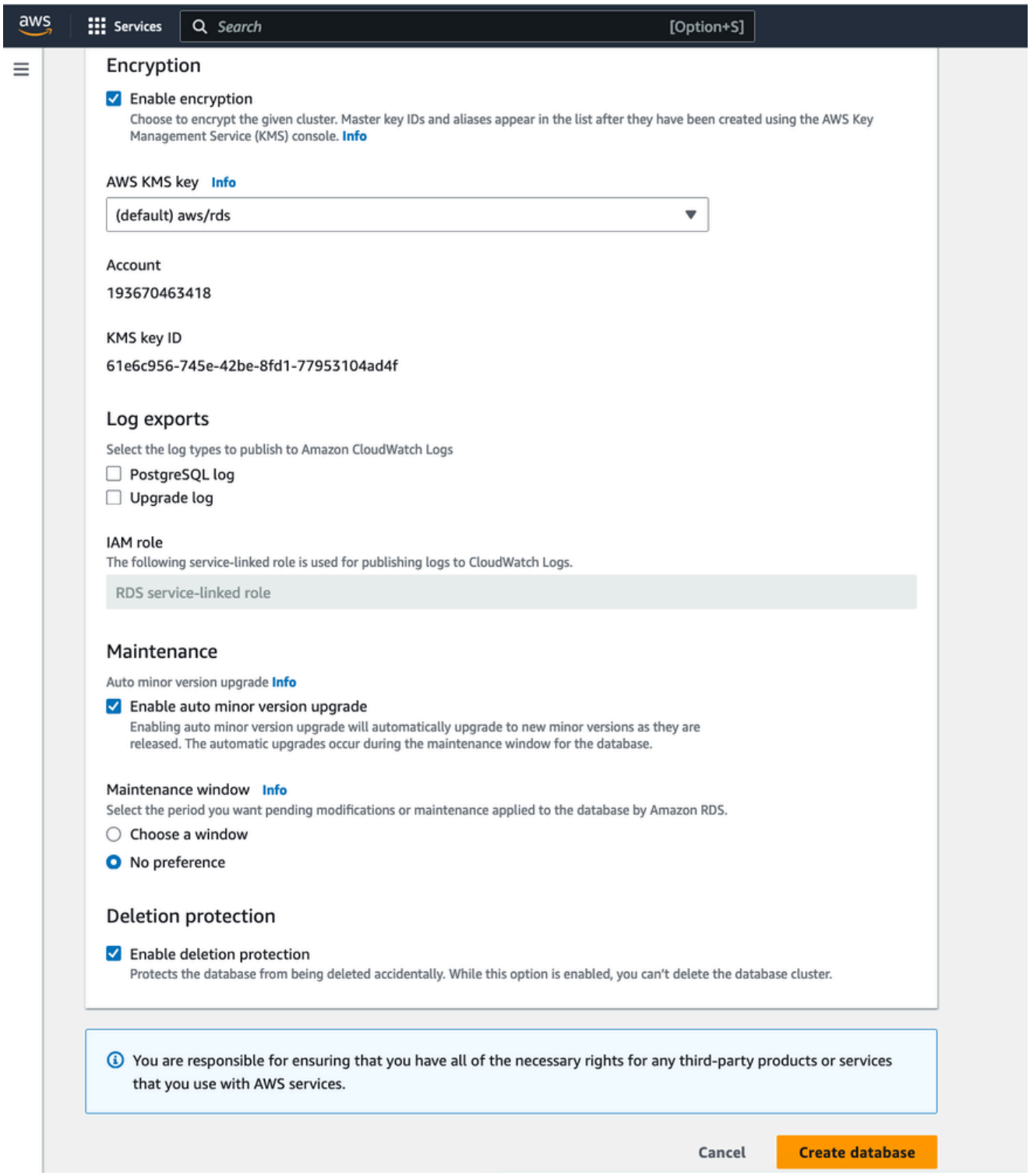
根据您的使用案例选择适当的值。我们已选择默认值。



确保在“Database authentication”中选择了“Password authentication”。使用数据库密码进行身份验证。


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.

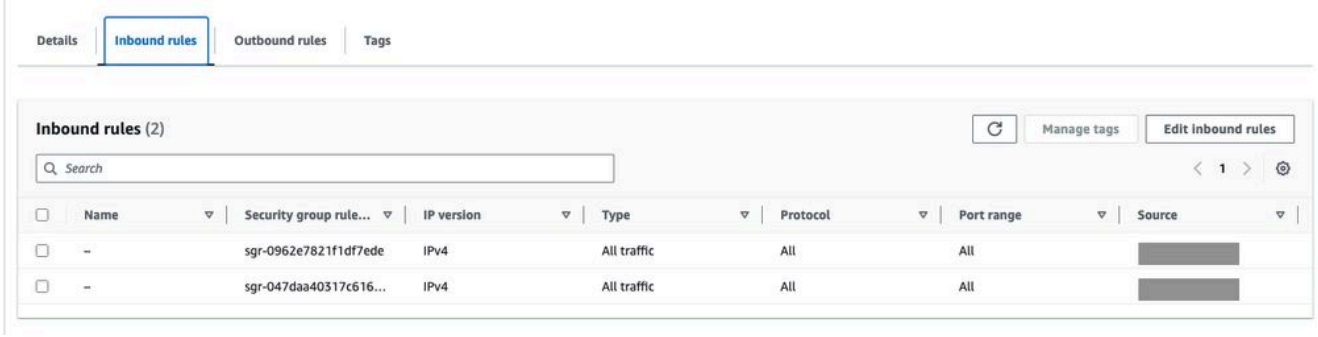

aws
Services
Search
[Option+S]
Additional configuration
Database options, encryption turned on, backup turned on, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned on.
Database options
Initial database name Info
Not supported for Multi-AZ DB cluster
If you do not specify a 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



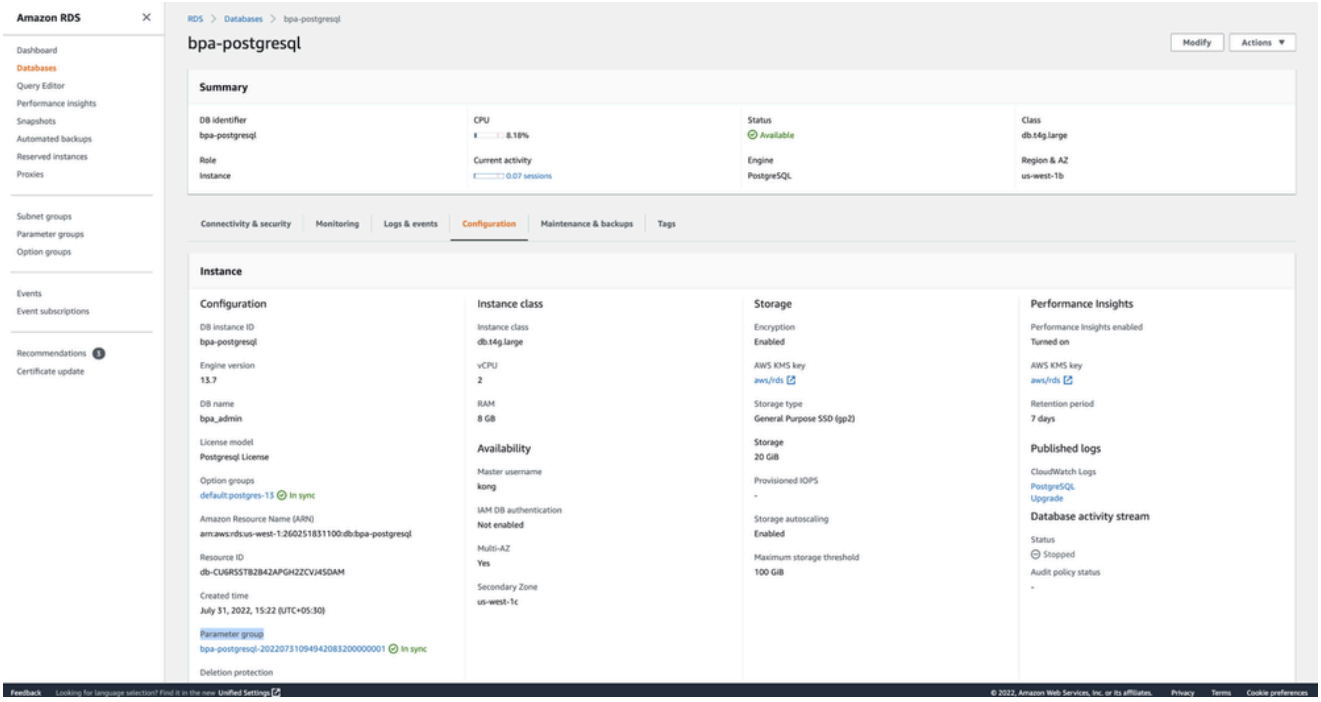
验证之后，即可创建数据库。 返回Amazon RDS控制面板。确认该实例可供使用。

安全组规则

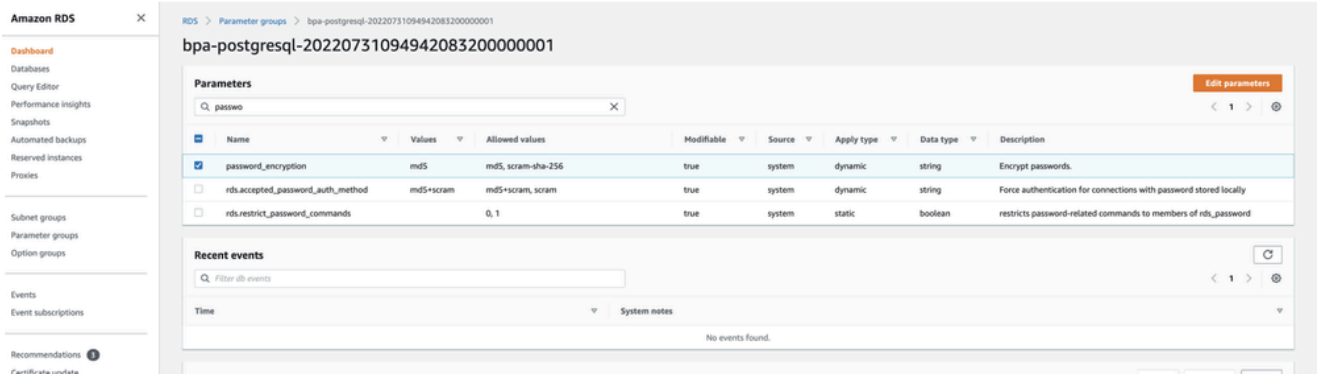
使用Pod CIDR和节点CIDR块更新入站安全组。



在RDS -> Databases -> DB-NAME中，点击configuration并参阅Parameter Group部分，然后点击要查看的参数组。



搜索“password_encryption”并将值从空白/其他值更改为md5。要使camunda配置正常工作，需要使用此命令。



通过连接到RDS与用户一起创建这些数据库。

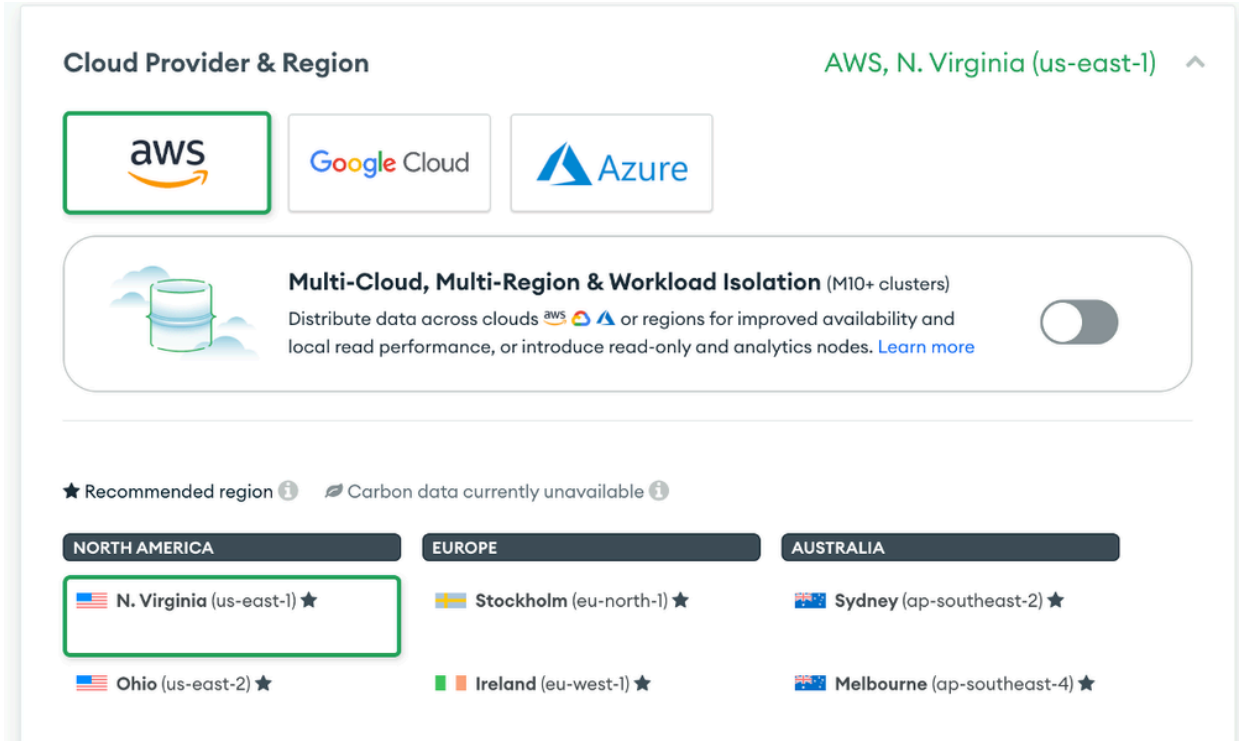
```
PG_ROOT_DATABASE=admin
PG_INITDB_ROOT_USERNAME=admin
PG_INITDB_ROOT_PASSWORD=Bp@Chang3d!
AUTH_DB_NAME=kong
AUTH_DB_USER=kong
AUTH_DB_PASSWORD=K@ngPwdCha*g3
WFE_DB_USER=camunda
WFE_DB_PASSWORD=WOrkFlo#ChangeNow
WFE_DB_NAME=process-engine
```

- 密码验证

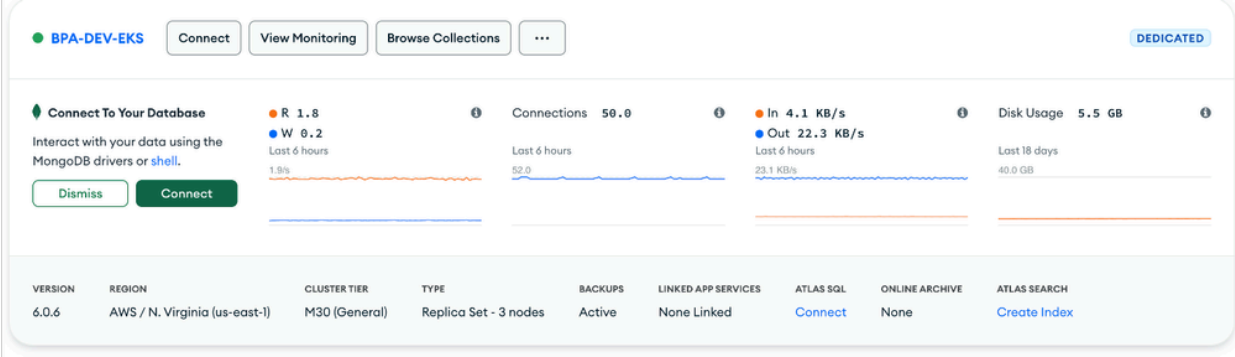
  使用数据库密码进行身份验证。

- **Atlas MongoDB设置**
  设置Atlas MongoDB涉及：
  - **登录Atlas MongoDB。**
  - 选择组织和项目。
  - 创建具有适当规格的专用集群。

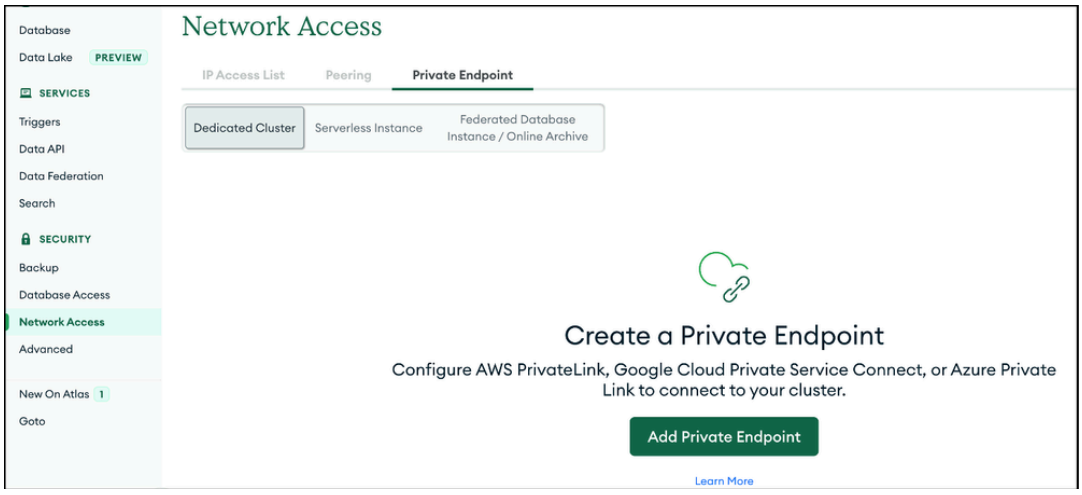
  - 选择专用层、云提供商和地区。



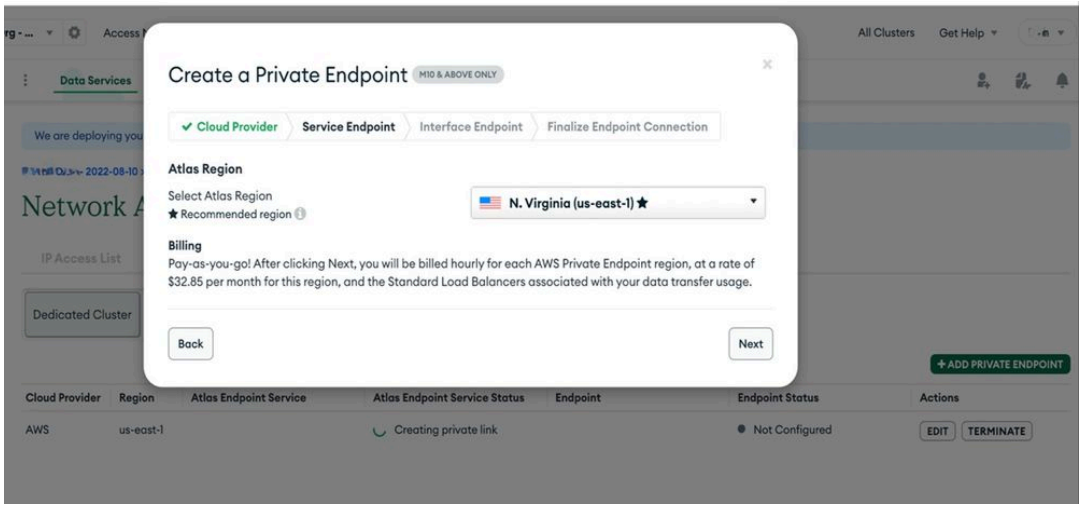
- 选择适当的层（我们使用**M30作**为层）专用集群，并提供相应的集群名称，然后点击**Create Cluster**。它将初始化**Atlas monogodb群集**。



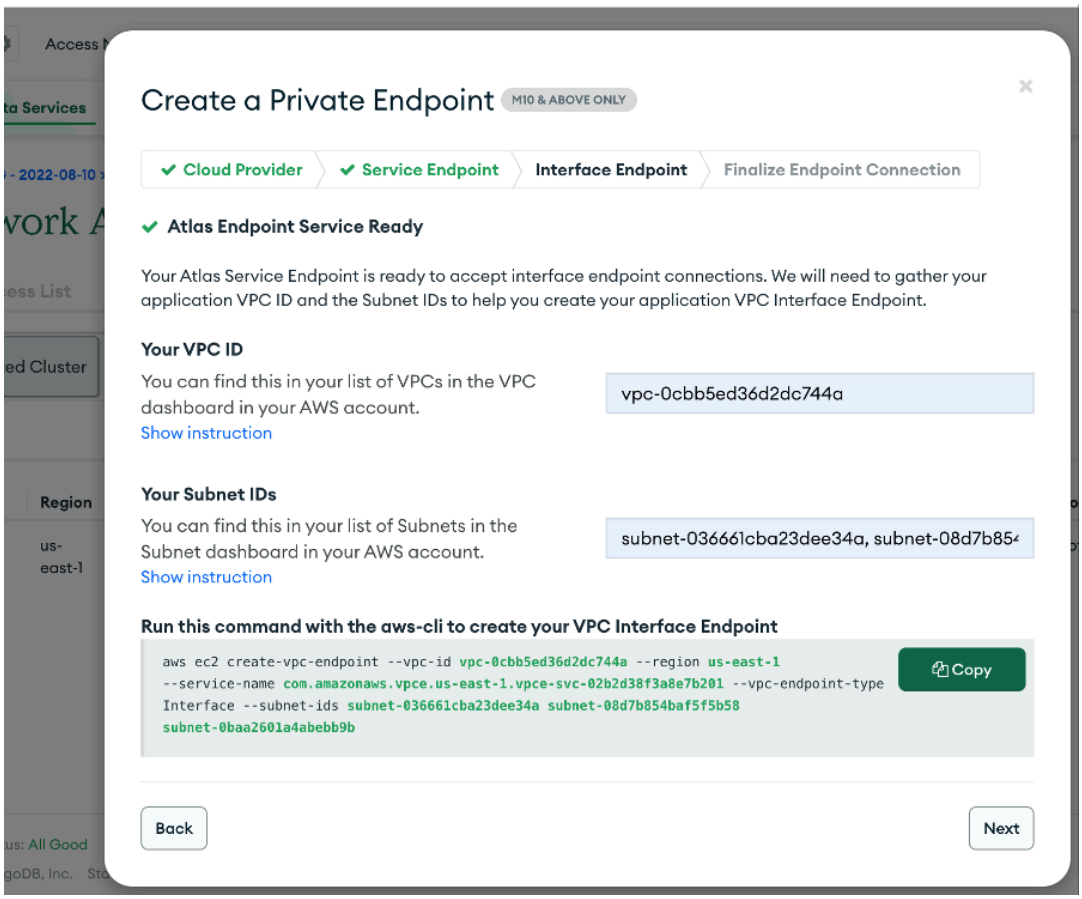
- 为**Atlas和K8S集群**设置**VPC**专用终端。
  - **点击Network Access Select Private Endpoint然后点击Add Private Endpoint**。



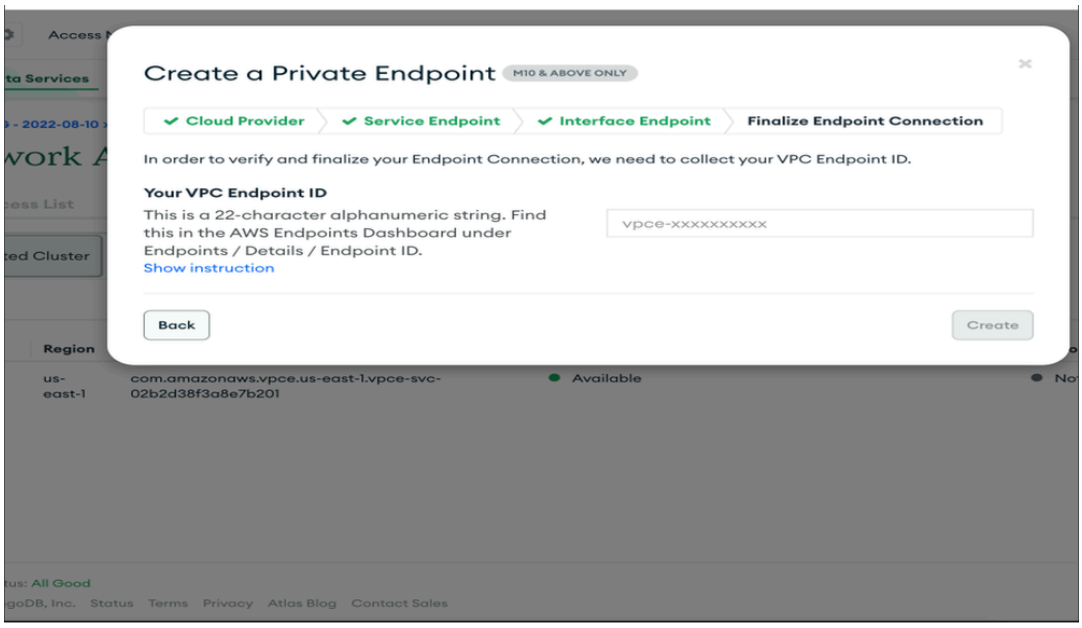
  - 选择**Cloud Provider（云提供商）作**为**AWS**，选择相应的区域，然后点击**Next（下一步）**。



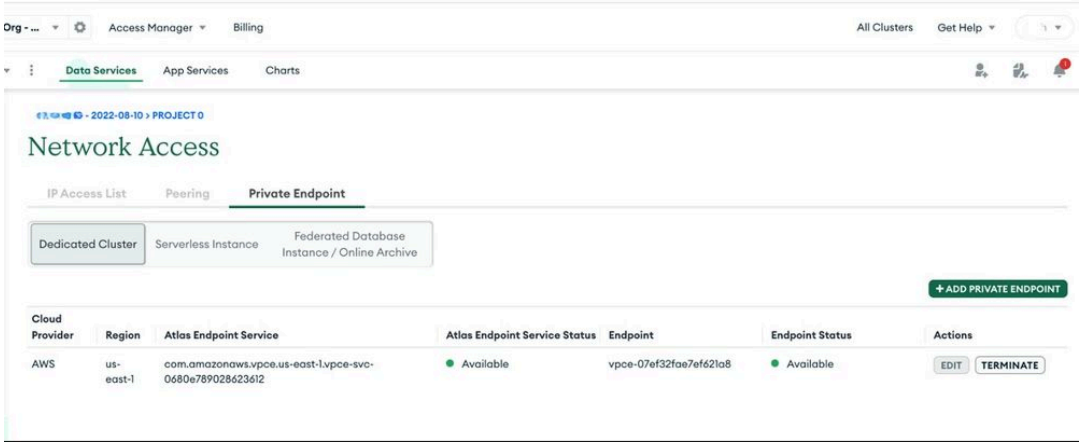
- **提供相应的PVC ID和子网ID。输入详细信息后，复制vpc终端创建命令并在aws控制台中执行。您将获得vpc终端id作为输出。**



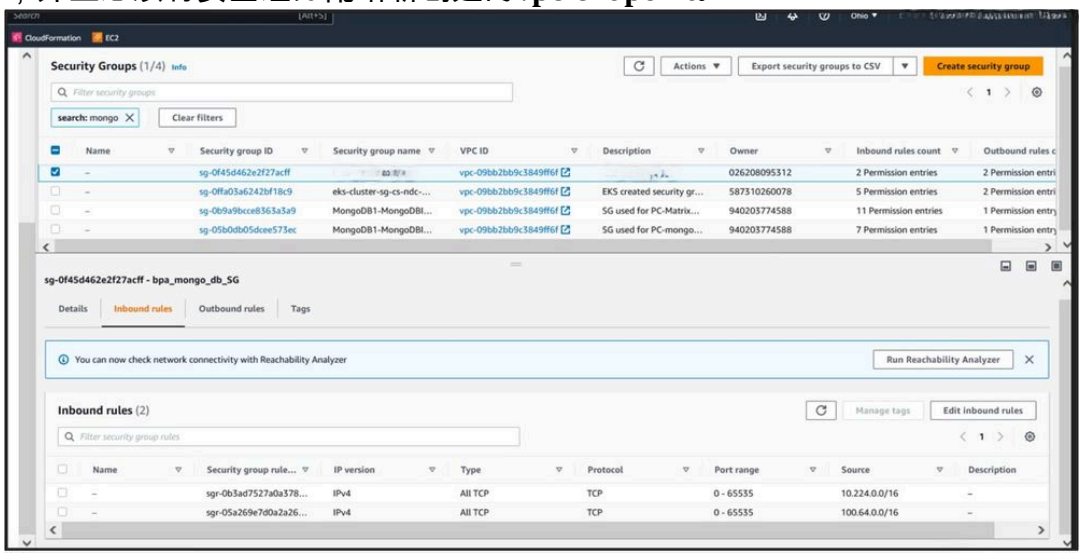
- **点击Next粘贴VPC终端ID，然后点击Create。**



- **成功创建终端后，终端状态将为“可用”，如下图所示。必须为Pod CIDR创建VPC终端。在本例中，我们使用了“100.64.0.0/16”。**



- 将入站规则添加到新创建的**vpc-endpoint**。**vpc-endpoint**将位于父帐户中，并且必须将安全组分配给新创建的**vpc-endpoint**。



ECR作为映像注册表

创建Amazon ECR存储库并将Docker映像推入其中涉及几个步骤。以下是使用AWS CLI创建ECR存储库、标记Docker映像并将其推送到存储库的步骤。

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

替换：

- **your-image-**name与ECR存储库的所需名称。
- 您的AWS区域

配置EKS节点的IAM角色

确保EKS工作节点（EC2实例）具有附加从ECR提取映像的权限的必要IAM角色。所需的IAM策略为

：

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

将此策略附加到与您的EKS工作节点相关联的IAM角色。

BPA部署

BPA的部署涉及几个步骤，包括标记EKS工作节点，在节点上准备目录，复制BPA软件包，以及使用Helm部署BPA。

在客户部署方面，我们使用了以下版本的软件和云服务：

- **BPA：**4.0.3-6
- **RDS（关系数据库服务）：**16.3-R2
- **MongoDB Atlas：** v5.0.29
- **EKS（Elastic Kubernetes服务）：**v1.27

这些组件可确保我们的部署稳健、可扩展且能够高效地处理所需的工作负载。

- 标记**EKS工作**节点

```
kubectl label node
```

```
name=node-1 kubectl label node
```

```
name=node-2 kubectl label node
```

```
name=node-3 kubectl label node
```

```
 name=node-4
```

- **准备节点上的目录**
  节点 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
```

  节点 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
```

  节点 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
```

节点 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
```

- 复制BPA包

```
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/
```

- 使用Helm部署BPA

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

入口设置

- 启用入口
  更新值。yamlto启用入口：

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

- **使用BPA**证书创建密钥
  导航到证书目录并创建密钥：

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

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

- **更新入口控制器**
  将新创建的密钥添加到 **`ingress-controller.yaml`** 文件:

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

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

- **更新入口**证书
  执行Helm删除和安装以更新入口证书。

环境规格
环境规范包括EC2实例、负载均衡器、VPC终端和RDS实例的要求。主要规格包括：

EC2要求：

存储要求：每个节点2TB的空间。将EBS卷装入/opt并在/etc/fstab中添加所有节点的条目。

Security group inbound：30101、443、0 - 65535 TCP、22 for ssh。

Security group outbound：必须启用所有流量。

DNS解析器：EC2必须在/etc/resolve.conf中具有内部解析器。

负载均衡器要求：

- 侦听程序端口必须是443、30101。
- VPC终端要求(Atlas MongoDB)。
- 为Atlas连接创建的VPC终端在父帐户(aws-5g-ndc-prod)中可用。VPC终端必须具有允许所有入站访问的安全组(0 - 65535)。

RDS要求：

RDS类型：db.r5b.2xlarge

Postgres引擎版本：13.7

安全组：入站必须允许来自POD CIDR源的流量。

关键概念和组件
了解Kubernetes基础知识对于使用Amazon EKS有效部署和管理应用至关重要。

结论
本文为使用Amazon EKS部署和管理业务流程自动化(BPA)应用程序提供了详细的指南。通过遵循概述的步骤并了解关键概念，组织可以将EKS的优势用于其容器化BPA应用。

参考

- **Amazon Web Services、“Amazon EKS文档”**[在线]。可用地址：**https://docs.aws.amazon.com/eks/**
- **Kubernetes，“Kubernetes Documentation”[在线]**。可用地址：**https://kubernetes.io/docs/home/**
- **思科BPA概览**https://www.cisco.com/c/en/us/solutions/collateral/service-provider/at-a-glance-c45-742579.html
- **BPA操作指南**https://www.cisco.com/c/dam/en/us/support/docs/bpa/v403/cisco-bpa-operations-guide-v403.pdf
- **BPA开发人员指南**https://www.cisco.com/c/dam/en/us/support/docs/bpa/v403/cisco-bpa-developer-guide-v403.pdf

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。