在Amazon EKS上部署和管理業務流程自動化應用程式：實用指南

目錄

摘要

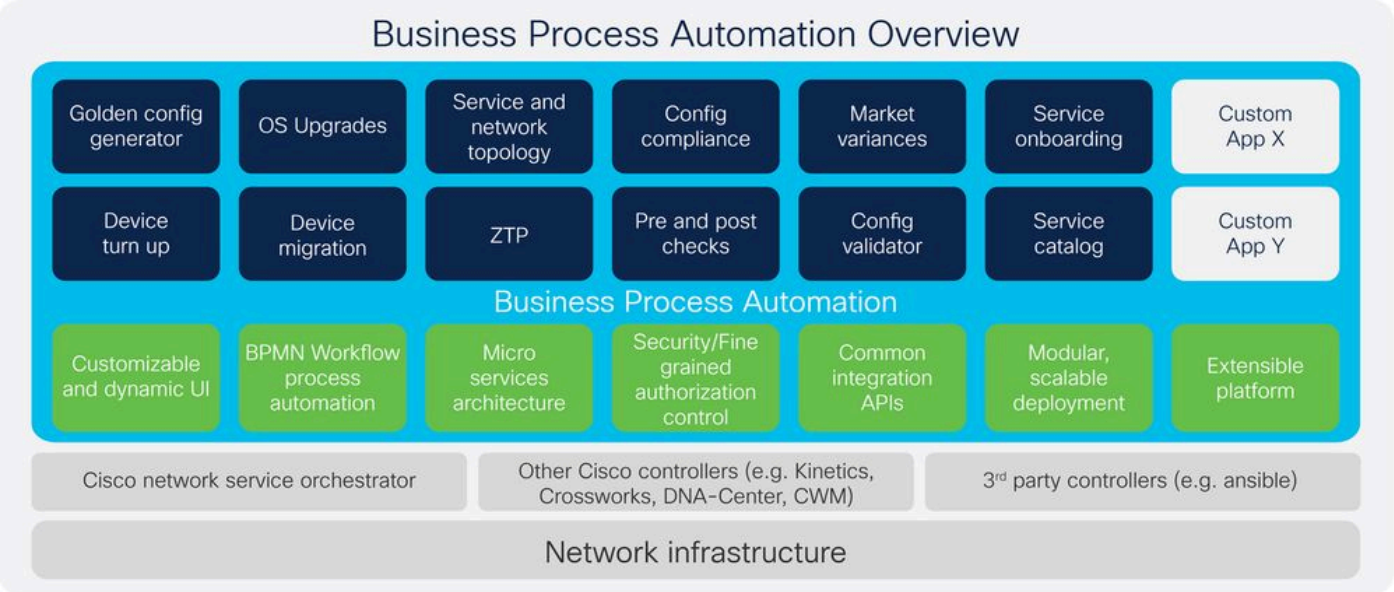
本文提供使用Amazon Elastic Kubernetes Service (EKS)部署和管理業務流程自動化(BPA)應用程式的綜合指南。它概述了前提條件，重點說明了利用EKS的好處，並提供了設定EKS集群、Amazon RDS資料庫和MongoDB Atlas的分步說明。此外，本文檔還深入探討了部署架構並明確了環境要求，為旨在將EKS用於其容器化BPA應用的組織提供了全面的資源。

關鍵字

Amazon EKS、Kubernetes、AWS、RDS、MongoDB Atlas、DevOps、雲端計算、業務流程自動化。

簡介

BPA



在當今的數位化時代，企業尋求跨多種IT環境最佳化和自動化複雜的業務流程。業務流程自動化

(BPA)已成為一項關鍵技術，使組織能夠提高運營效率、減少錯誤和改進服務交付。BPA引進了幾項重要的創新與增強功能，旨在推進工作流程自動化、服務布建與現成自動化應用程式。

BPA平台託管業務和IT/運營使用案例和應用，例如作業系統升級、服務調配以及到協調引擎的整合。客戶可以訪問一系列服務和BPA功能，包括諮詢、實施、業務關鍵型服務和解決方案支援，這些服務透過思科專家提供，還有最佳實踐、久經考驗的技術和方法，可幫助實現業務流程的自動化並降低系統風險。

這些生命週期功能可基於訂用或根據個人需求定製。實施服務可幫助定義、整合和部署工具和流程，從而加快自動化速度。思科專家會根據靈活流程和持續整合和持續交付(CICD)工具，執行收集需求的正式流程、設計和開發使用者案例，並透過自動測試新工作流程、裝置和服務來實施靈活服務。透過解決方案支援，客戶可以全天候獲得集中式支援，重點關注以軟體為中心的問題，同時還可以透過思科分層軟體模型提供多供應商和開源支援。思科解決方案支援專家可幫助管理您的案例，從首次致電到最終解決，並充當與多個供應商同時合作的主要聯絡人。與解決方案級專家合作，您可以減少多達44%的問題，幫助您保持業務連續性，並更快地實現BPA投資回報。

關鍵的技術功能，例如對FMC和Ansible-Managed裝置的支援、使用高級排隊架構(AQF)的並行執行，以及NDFC和FMC裝置的擴展配置合規性，將BPA定位為大規模企業自動化的全面解決方案。該版本在SD-WAN管理、裝置自註冊和防火牆策略管理方面增加了更多功能，解決了網路安全和自動化的關鍵方面，滿足了大規模、多供應商環境的需求。

EKS

Amazon Elastic Kubernetes Service (EKS)是由Amazon Web Services (AWS)提供的完全託管Kubernetes服務。2018年推出的EKS使用開源容器協調平台Kubernetes簡化了容器化應用的部署、管理和擴展過程。EKS將Kubernetes群集管理的複雜性抽象化，允許開發人員專注於構建和運行應用程式，而無需處理底層基礎設施。

使用Amazon EKS進行應用程式部署的優勢

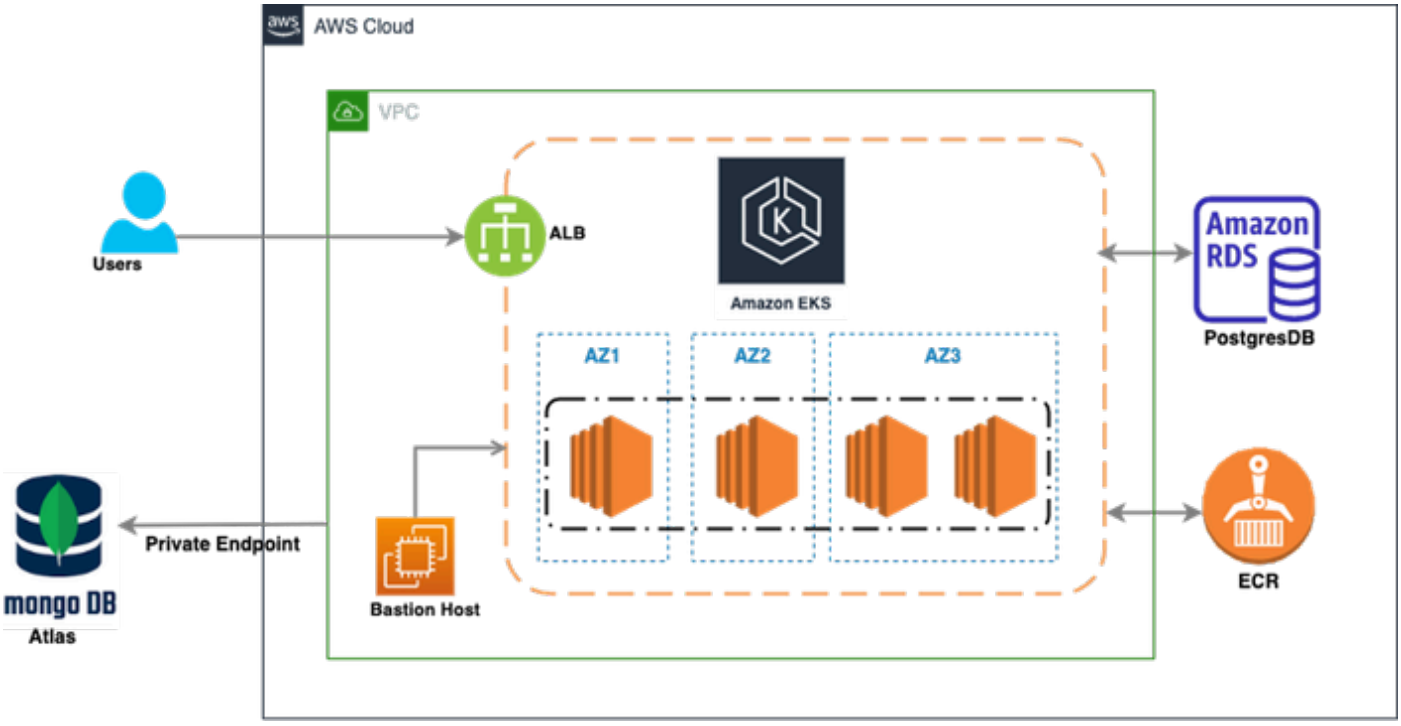
Amazon EKS為應用部署提供了多種優勢，使其成為利用容器化應用和微服務的組織的熱門選擇。

主要優勢包括：

- **託管Kubernetes控制平面**：EKS處理Kubernetes控制平面的部署、擴展和維護，減少運營負擔。
- **簡化的群集管理**：EKS將設定和管理Kubernetes群集的複雜性抽象化。
- **可擴充性**：EKS允許輕鬆擴展群集，以適應不斷成長的工作負載。
- **高可用性**：EKS支援多可用性區域部署，提高了可用性和容錯能力。
- **與AWS服務整合**：EKS與各種AWS服務無縫整合。

- **DevOps自動化**：EKS支援容器化應用的持續整合和持續部署(CI/CD)。

BPA部署架構



此影象表示在**AWS**上部署的基於雲的基礎設施的高級架構，使用多個關鍵元件。以下是圖表明細：

1. **Amazon EKS (Elastic Kubernetes Service)**：在圖表的核心處，Amazon EKS跨三個可用區域(AZ1、AZ2、AZ3)部署，每個區域內有Kubernetes工作節點。這表示高可用性和容錯設定，因為工作負載分佈在多個可用性區域。

2. **ALB （應用程式負載平衡器）**：它位於前方，接收來自使用者的流量，並將流量分配到EKS叢集，以處理應用程式工作負載。負載均衡器確保請求均勻分佈，並能夠根據流量需求處理擴展。

3. **Amazon RDS （關聯式資料庫服務）** - PostgreSQL：在圖表的右側，存在運行PostgreSQL的Amazon RDS例項。在EKS叢集中執行的應用程式可以存取此資料庫。

4. **ECR (Elastic Container Registry)**：這是儲存和管理Docker容器映像的位置，然後將其部署到Amazon EKS以運行工作負載。

5. **MongoDB Atlas**：在左側，MongoDB Atlas透過私有端點整合到架構中。MongoDB Atlas是一種雲託管的NoSQL資料庫服務，用於處理基於文檔的資料庫需求。專用終端確保MongoDB Atlas例項與其他AWS元件之間的安全、專用通訊。

6. **Bastion Host**：Bastion Host位於VPC（虛擬私有雲）內，可為管理員提供安全的入口點來訪問VPC內的資源，而無需直接將其暴露於網際網路。

整體而言，此架構為使用Amazon EKS部署和管理容器化應用提供了一個高度可用、可擴展且安全的解決方案，同時支援關係(PostgreSQL)和NoSQL (MongoDB)資料庫。

- **EKS群集設定**
  要使用AWS CLI建立Amazon EKS集群，可以使用`eksctl`命令列實用程式。以下是命令範例：

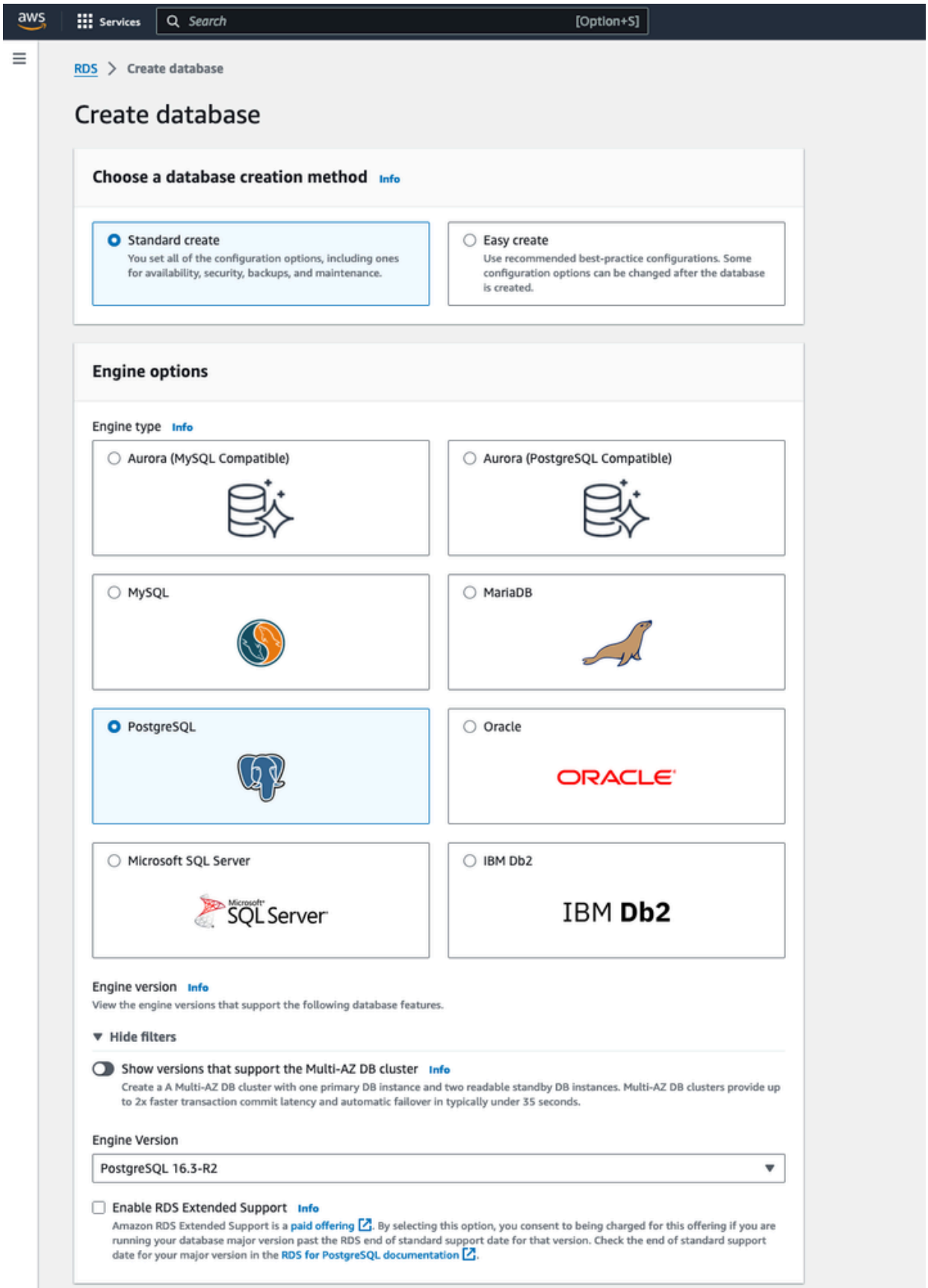
```
eksctl create cluster \
  --name
```

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

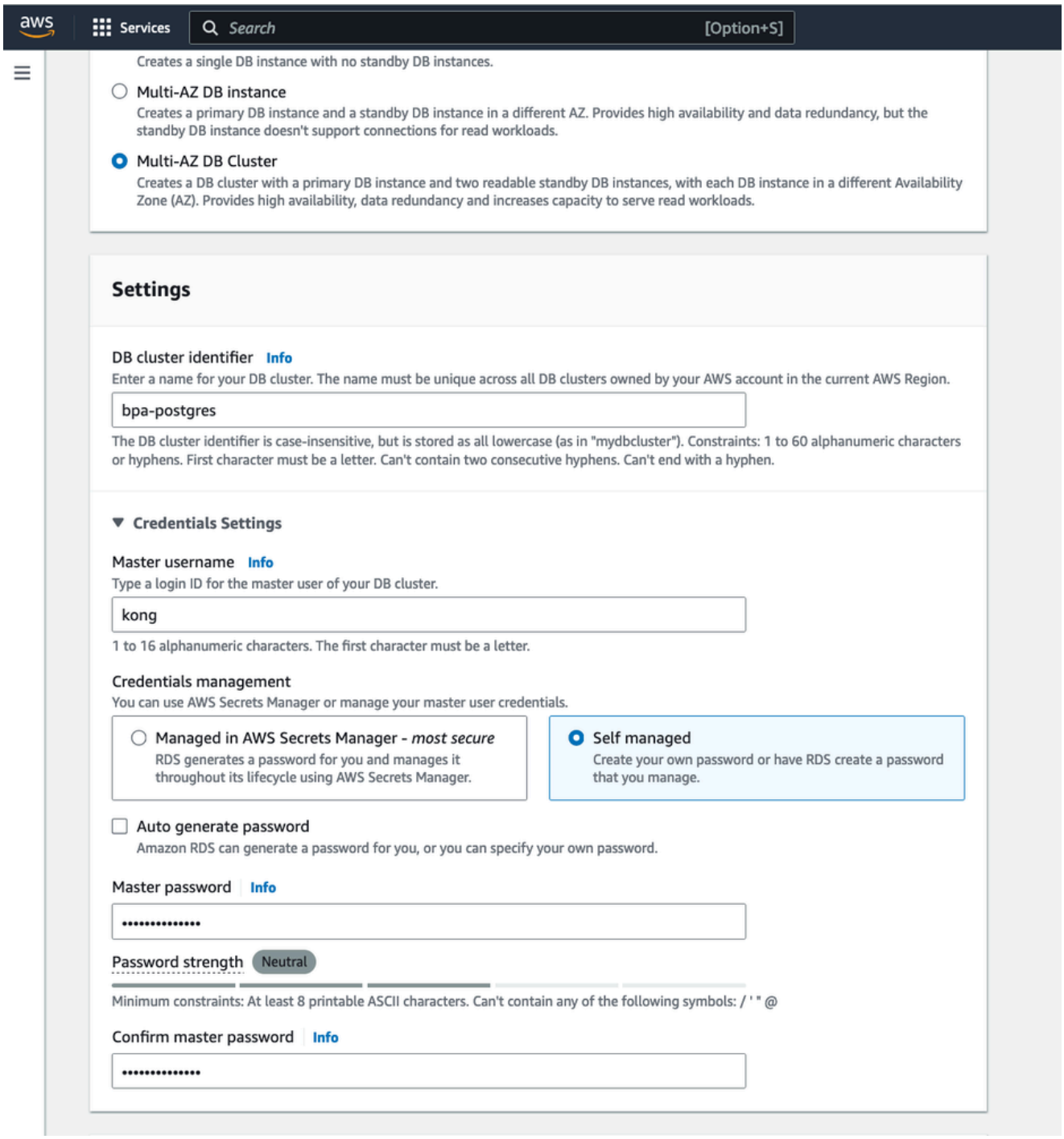
- **RDS資料庫設定**

  在Amazon RDS上部署關聯式資料庫涉及以下步驟：

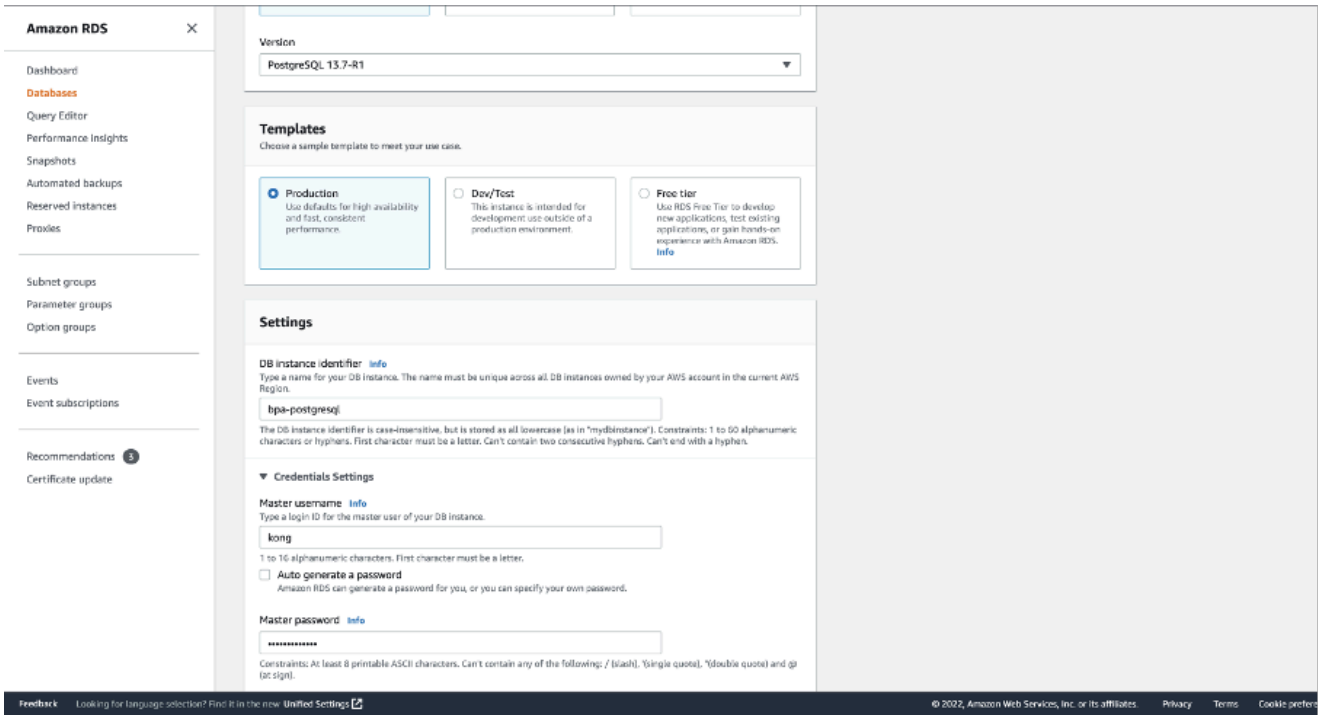
  - 訪問AWS管理控制檯並導航至Amazon RDS服務。
  - 建立具有所需規格的新資料庫執行處理。
  - 配置安全組以允許從Amazon EKS集群傳入連線。



使用下拉選單，選擇PostgreSQL的最新版本。在本例中為「PostgreSQL 16.3-R1」。



為此，請為資料庫例項指定名稱並建立使用者名稱和口令。

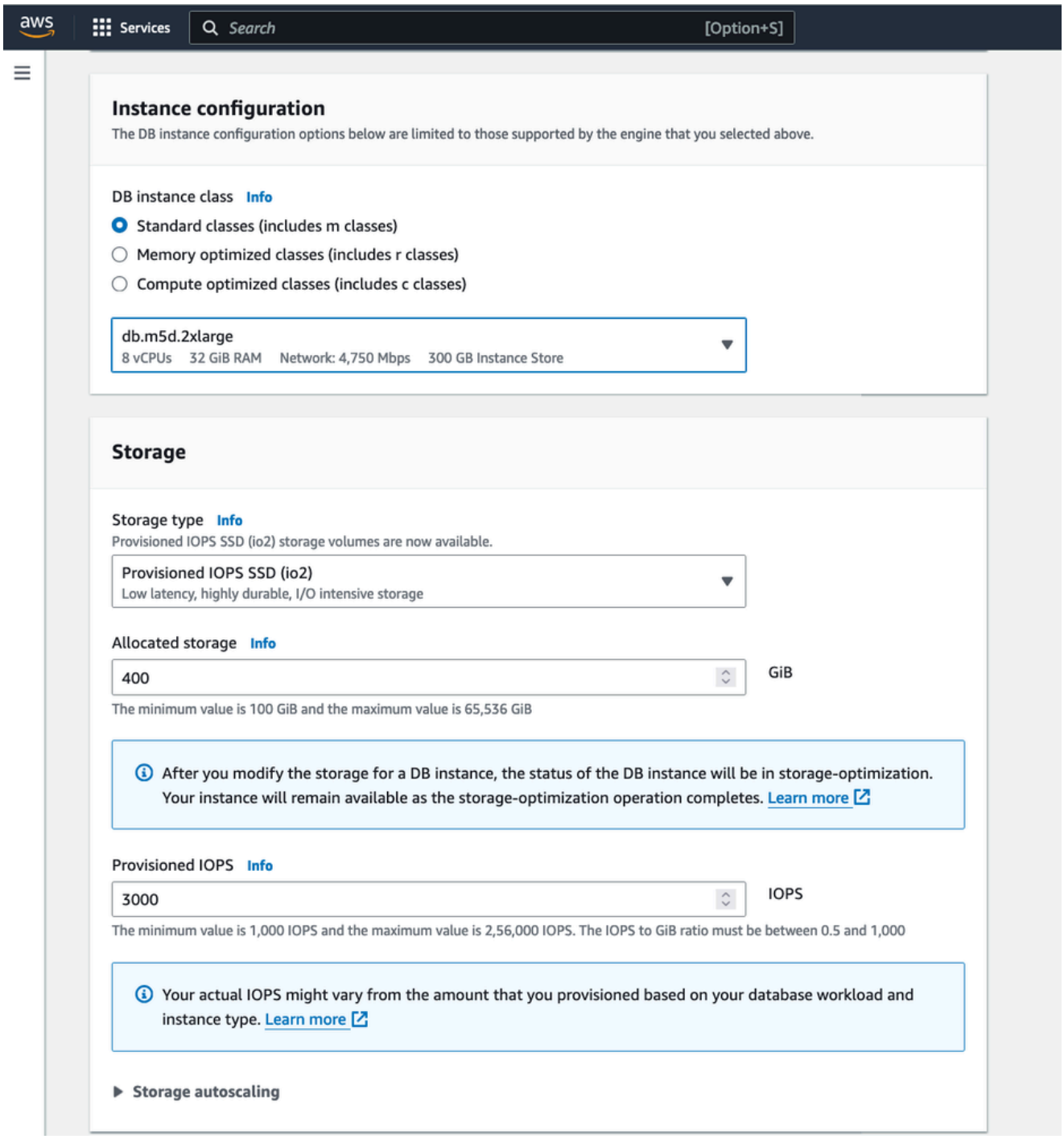


確保已選擇「資料庫例項大小」和「儲存」的預設設定。

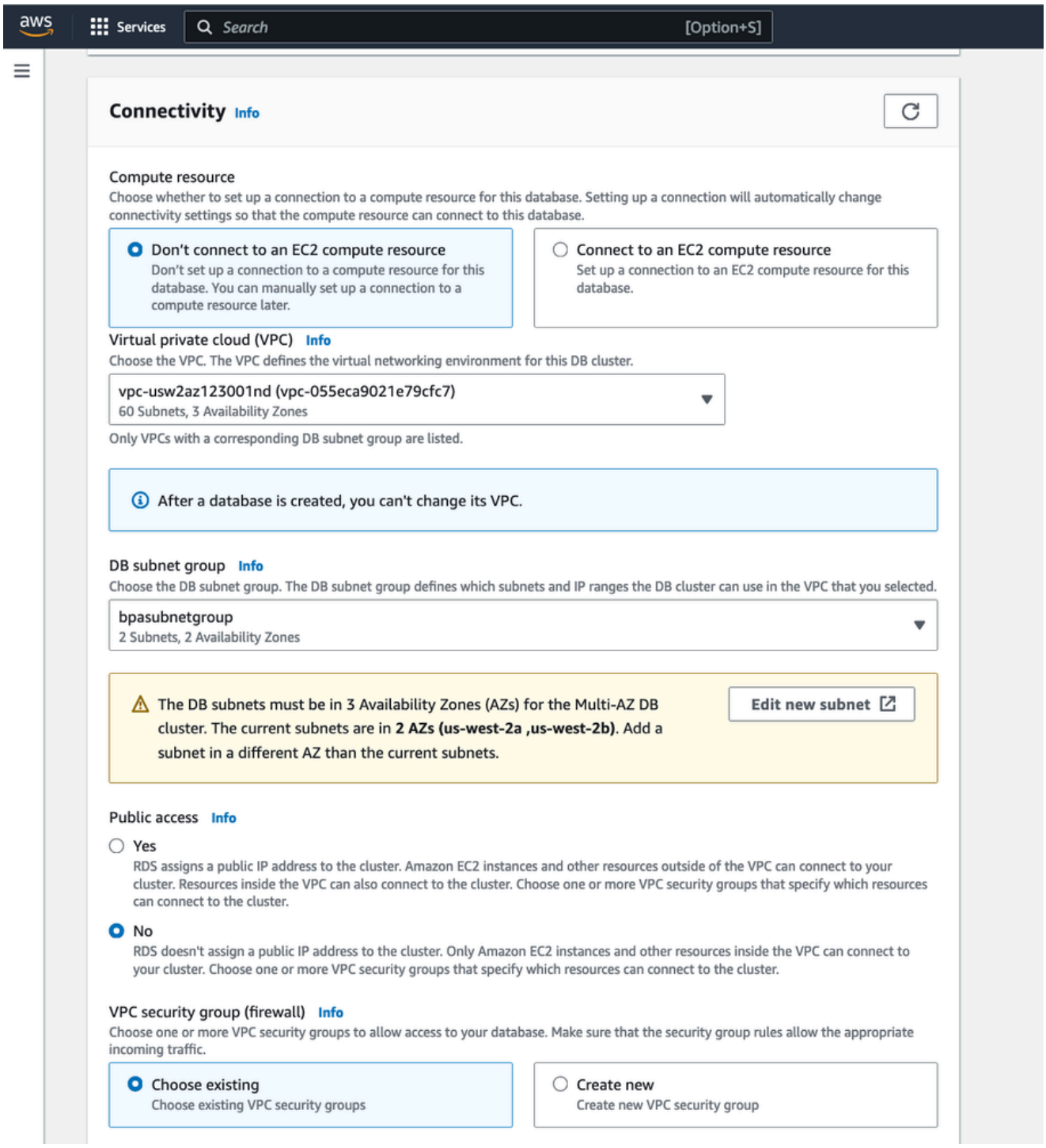
根據叢集大小和資料需求，選取適當的DB執行處理大小和儲存型別。

根據使用案例，我們選擇了以下配置：

- **資料庫例項大小**： db.m5d.2xlarge
    - 8個vCPU
    - 32 GiB記憶體
    - 網路：4,750 Mbps
    - 300 GB例項儲存

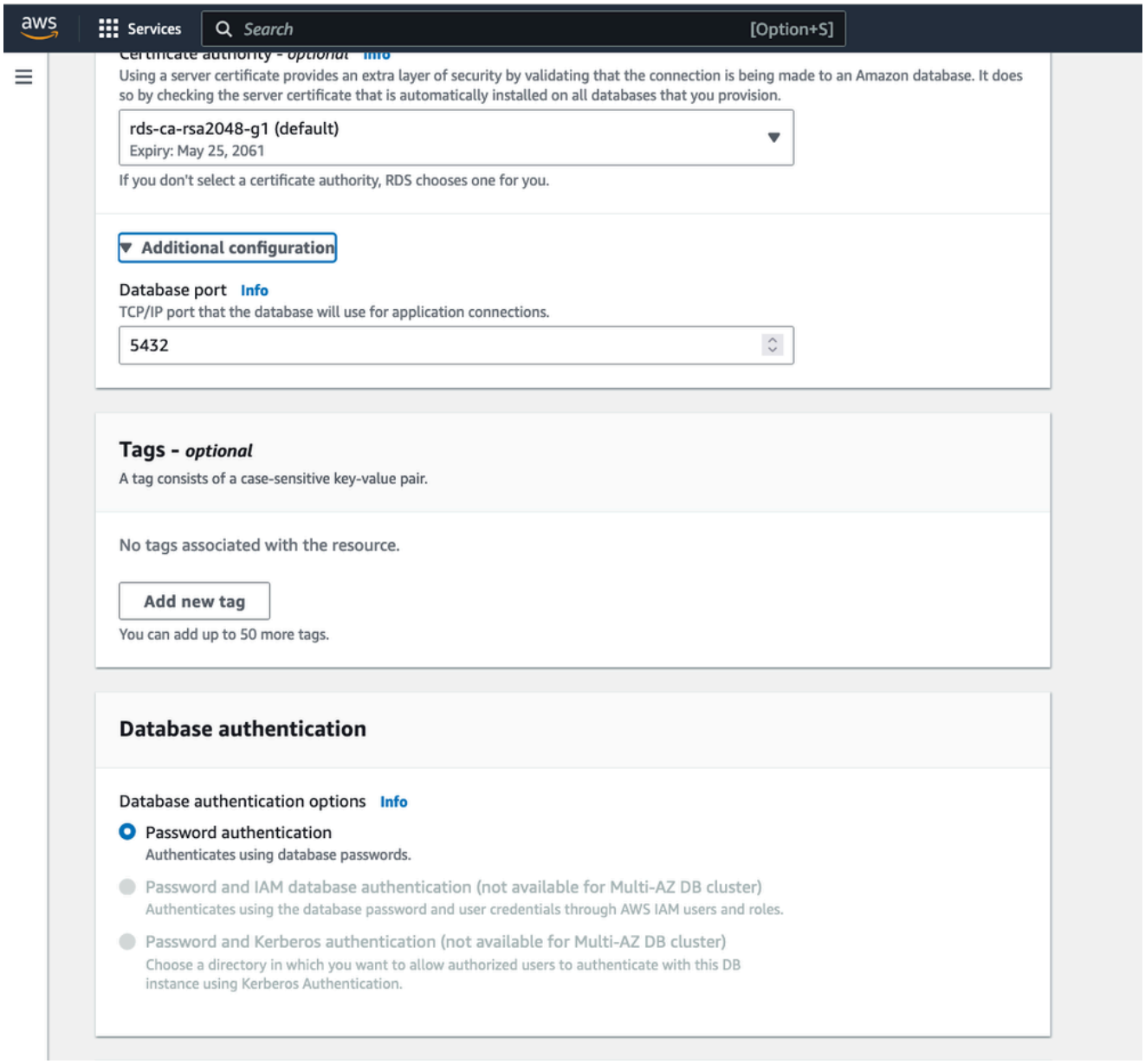


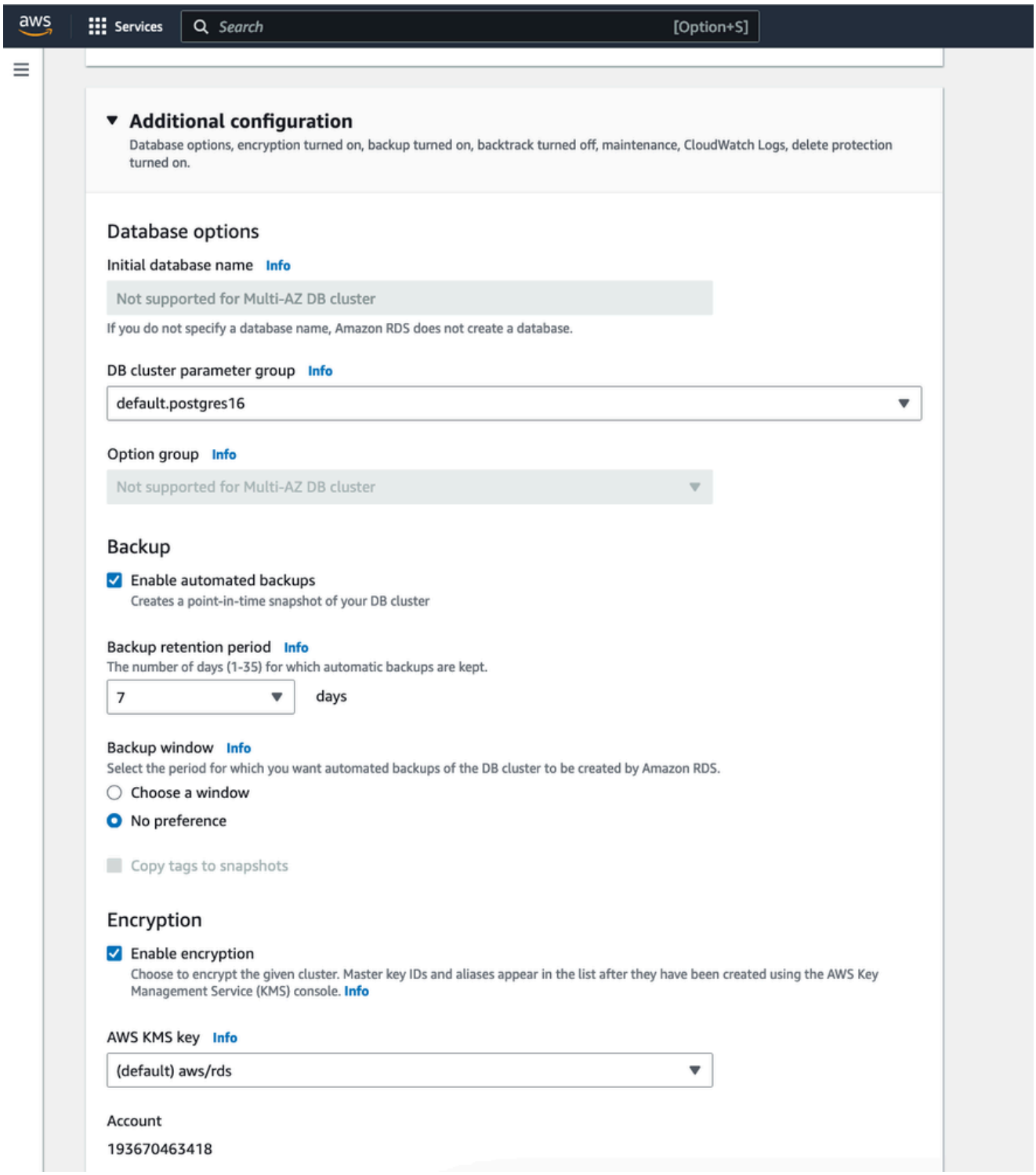
根據您的使用案例選擇適當的值。我們已選取預設值。

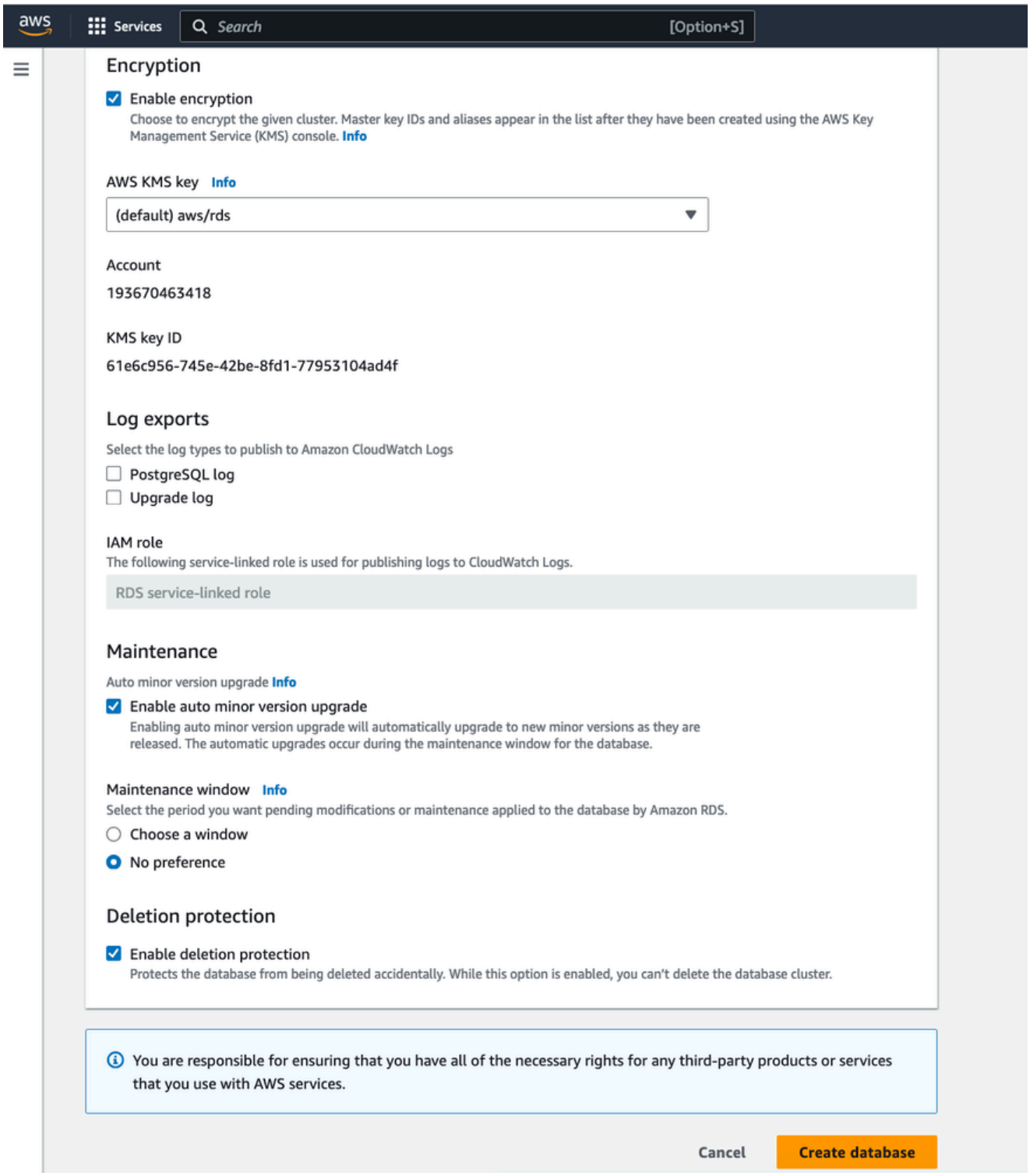


確保在「資料庫身份驗證」中，我們選擇了「密碼身份驗證」。使用資料庫密碼進行身份驗證

。


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.

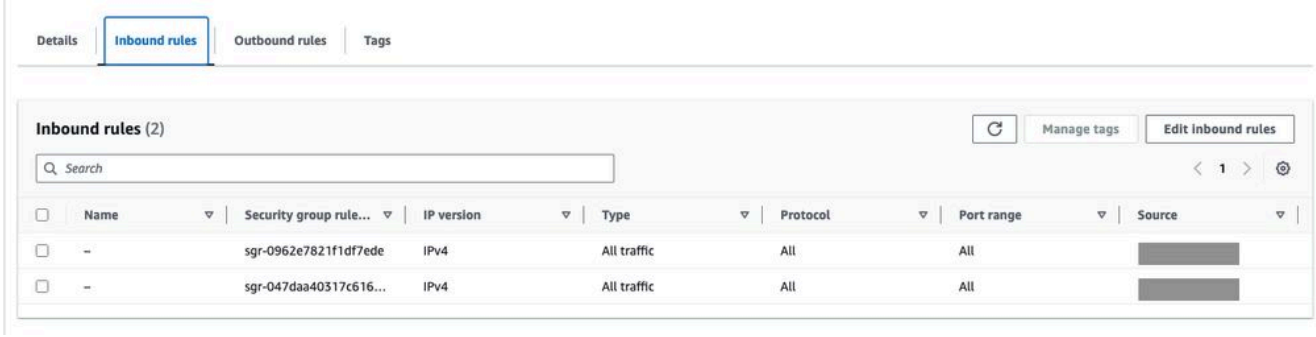

aws
Services
Search
[Option+S]
Additional configuration
Database options, encryption turned on, backup turned on, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned on.
Database options
Initial database name Info
Not supported for Multi-AZ DB cluster
If you do not specify a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



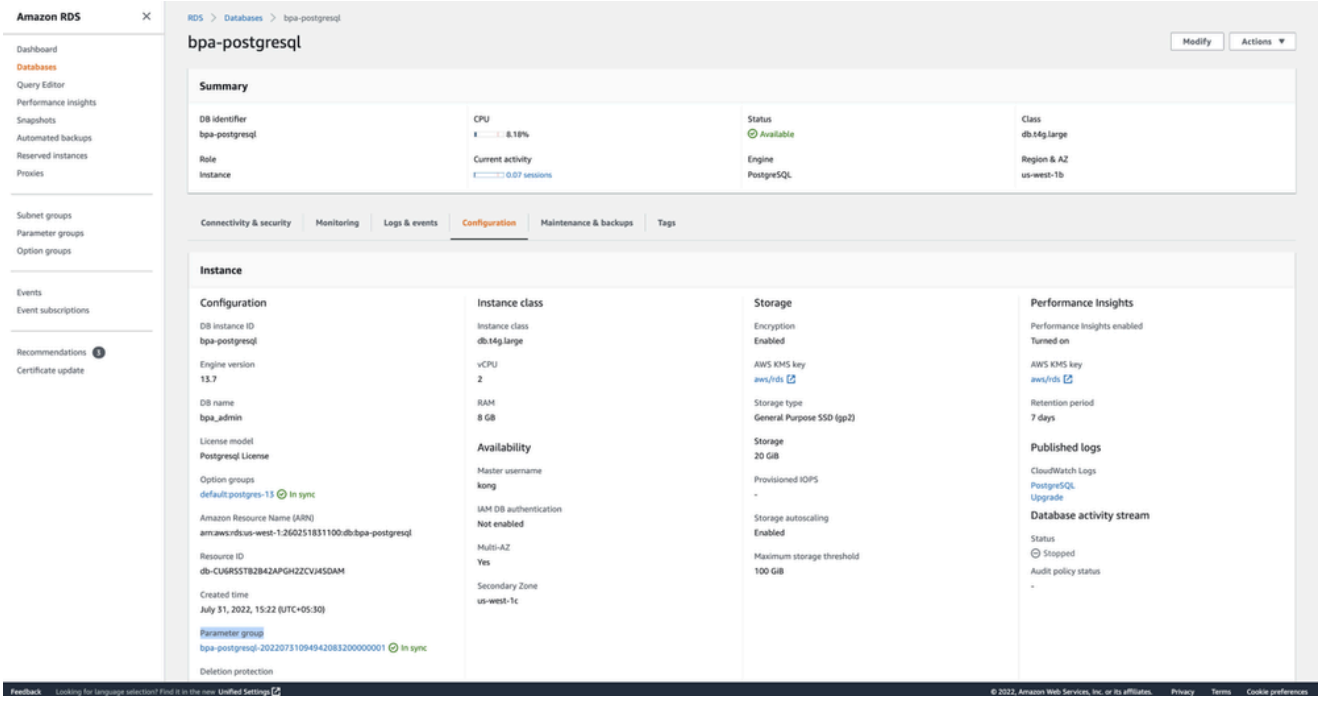
一旦確認無誤，我們便可以建立資料庫。 返回Amazon RDS控制台。確認該例項可供使用。

安全性群組規則

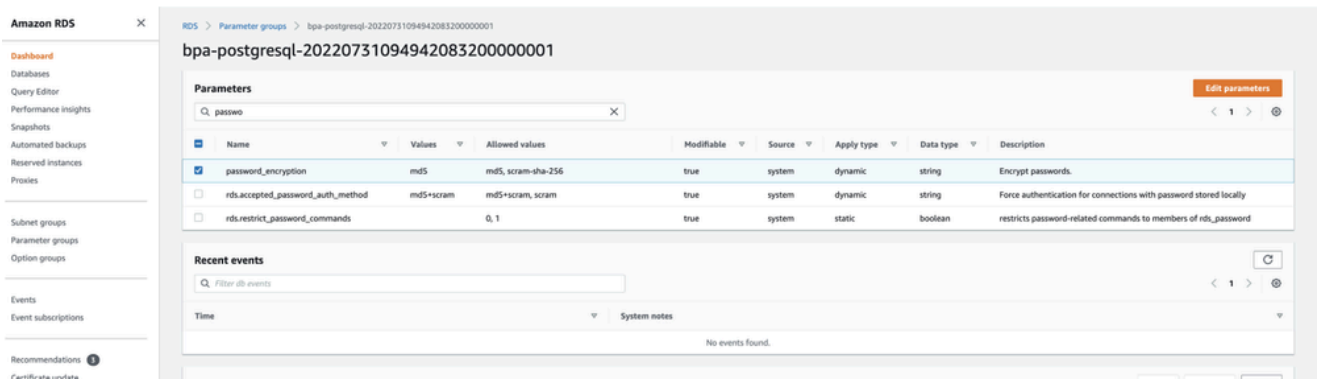
使用Pod CIDR和節點CIDR塊更新入站安全組。



在RDS -> Databases -> DB-NAME中，按一下configuration並參閱Parameter Group部分，然後按一下要檢視的參陣列。



搜尋「password_encryption」，並將值從空白/其他值變更為md5。要使camunda配置正常工作，需要執行此操作。



透過連線到RDS來建立這些資料庫以及使用者。

```
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
```

- 密碼驗證

  使用資料庫密碼進行身份驗證。

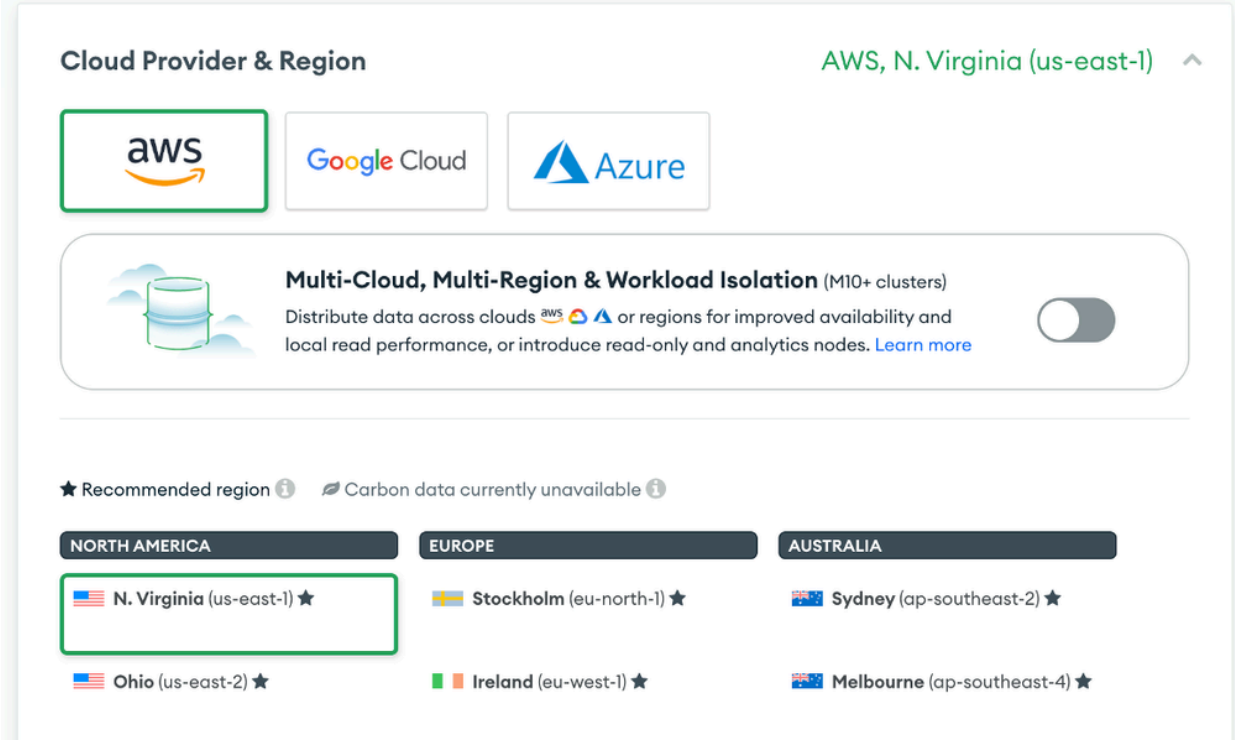
- **Atlas MongoDB設定**

  設定Atlas MongoDB涉及：

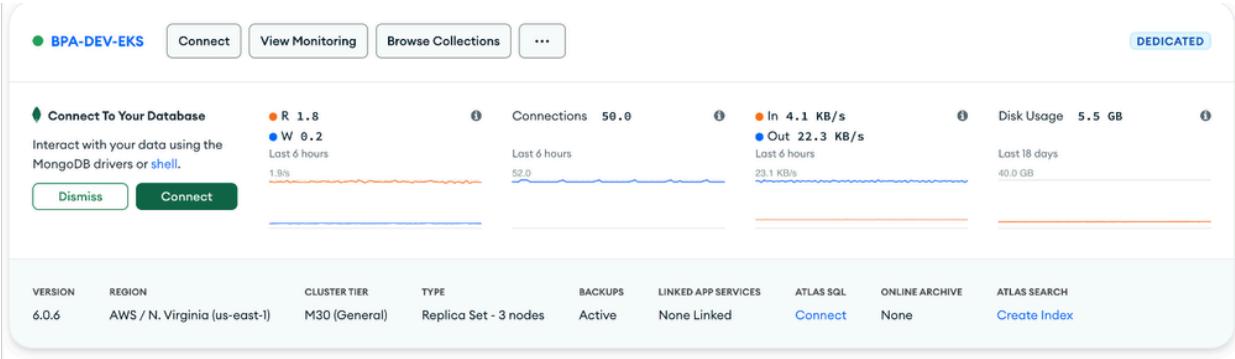
  - **登入Atlas MongoDB。**
  - **選取組織與專案。**
  - **建立具有適當規格的專用叢集。**

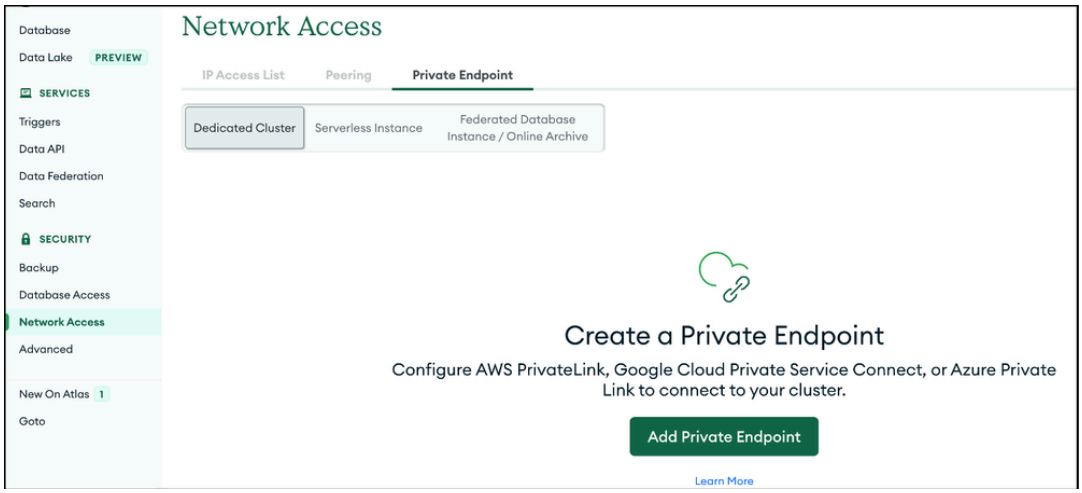
  - **選擇專用層、雲提供商和地區。**



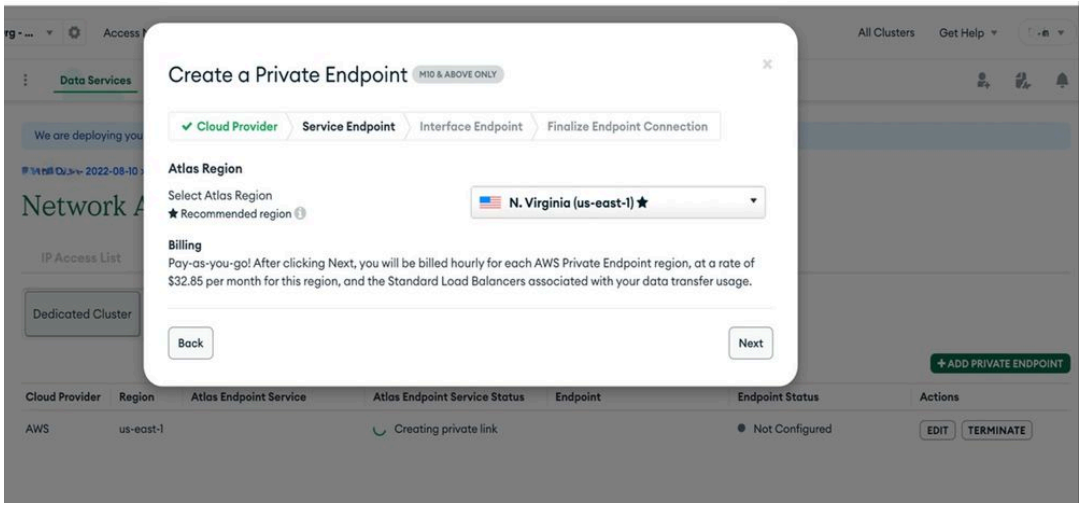
- **選取適當的層（我們使用M30作為層）專屬叢集，並提供適當的叢集名稱，然後按一下「建立叢集」。它將初始化Atlas monogodb群集。**



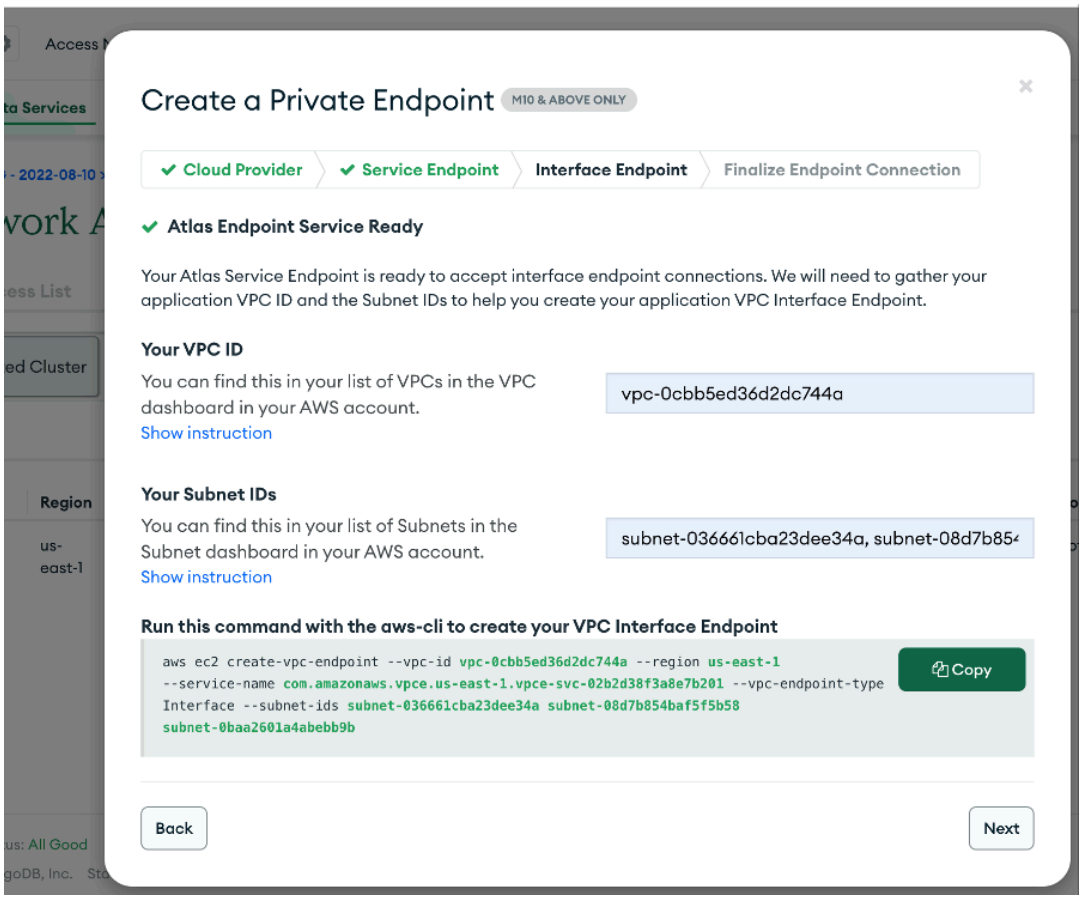
- **為Atlas和K8S集群設定VPC專用終端。**
  - **點選Network Access（網路訪問）Select Private Endpoint（選擇專用終端）或點選Add Private Endpoint（增加專用終端）。**



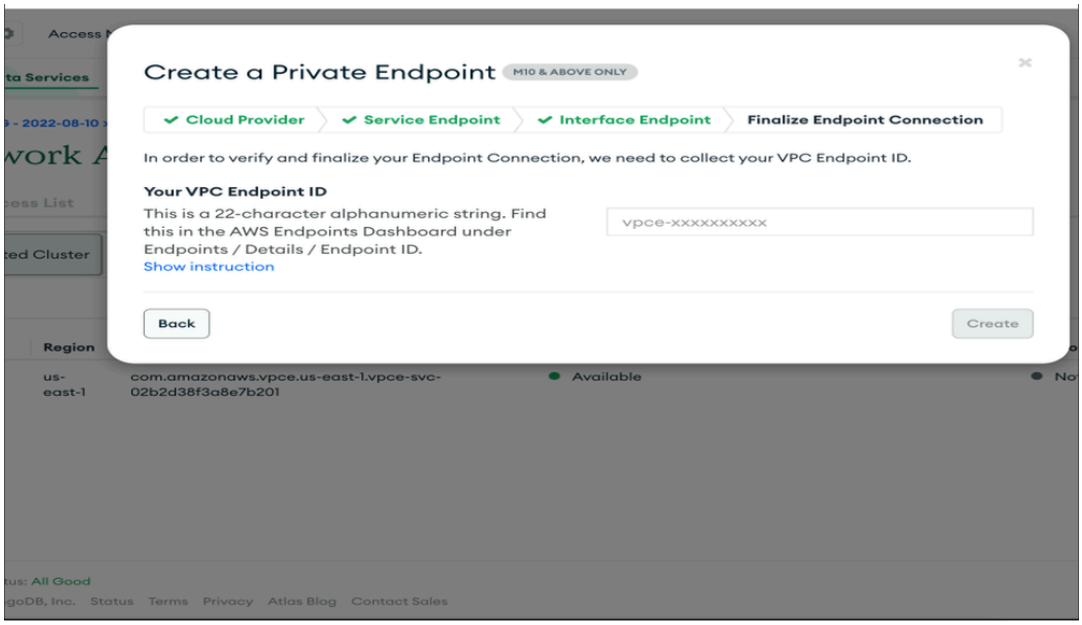
- **選擇Cloud Provider作為AWS，選擇相應的區域，然後點選Next。**



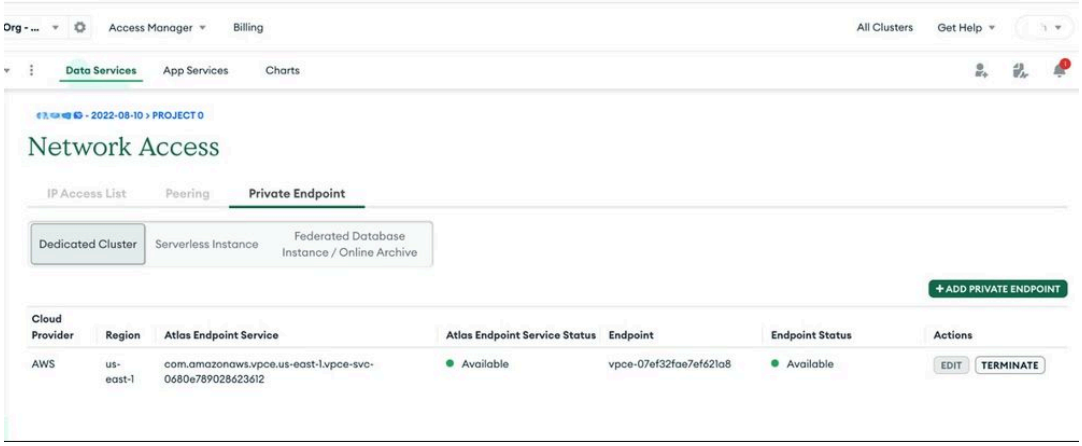
- **提供相應的PVC ID和子網ID。輸入詳細資訊後，複製vpc終端建立命令並在aws控制檯中執行它。您將獲得vpc端點id作為輸出。**



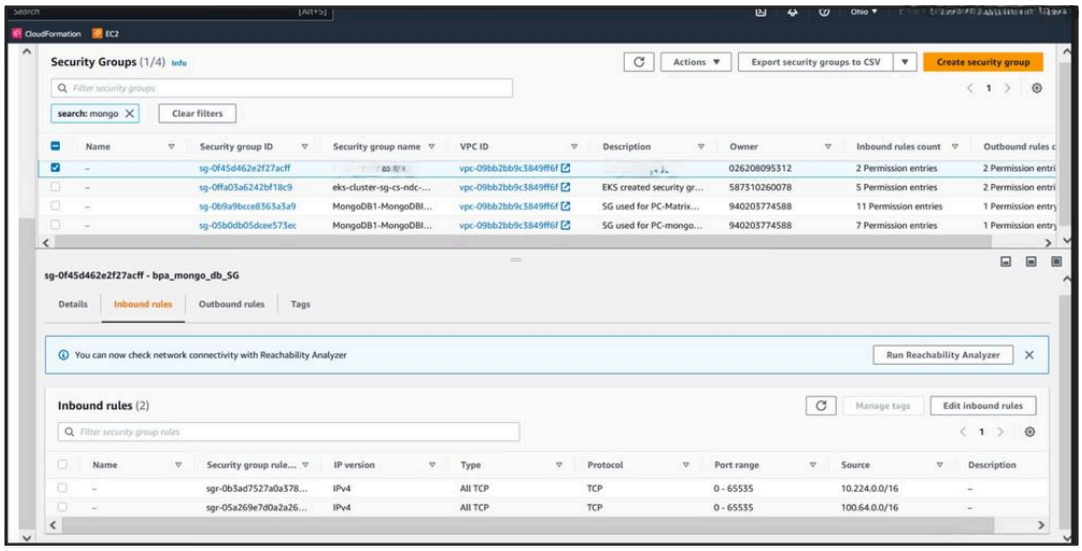
- **點選Next貼上VPC終端ID，然後點選Create。**



- **成功建立終端後，終端狀態將為「可用」，如下圖所示。必須為Pod CIDR建立VPC端點。在我們的案例中，我們使用了「100.64.0.0/16」。**



- **將入站規則增加到新建立的vpc-endpoint。vpc-endpoint將位於父帳戶中，並且必須將安全組分配給新建立的vpc-endpoint。**



ECR作為影像登入

建立Amazon ECR儲存庫和將Docker映像推入這些儲存庫涉及幾個步驟。以下是使用AWS CLI建立ECR儲存庫、標籤Docker映像並將其推送到儲存庫的步驟。

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

取代：

- **your-image**-name和ECR儲存庫的所需名稱。
- **您的**區域與AWS區域

為EKS節點配置IAM角色

確保EKS工作節點（EC2例項）具有從ECR提取映像的所需許可權的IAM角色。所需的IAM策略是：

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

將此策略附加到與您的EKS工作節點關聯的IAM角色。

BPA部署

BPA的部署包括幾個步驟，包括標籤EKS工作節點、在節點上準備目錄、複製BPA包，以及使用Helm部署BPA。

在客戶部署方面，我們使用了以下版本的軟體和雲服務：

- **BPA：**4.0.3-6
- **RDS （關聯式資料庫服務）**：16.3-R2
- **MongoDB Atlas**： v5.0.29
- **EKS（彈性庫伯內特斯服務）**：v1.27

這些元件可確保我們的部署功能強大、可擴展，並能有效處理所需的工作負載。

- **標籤EKS工作節點**

```
kubectl label node
```

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

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

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

```
name=node-4
```

- **準備節點上的目錄**

  節點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
```

  節點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
```

節點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
```

節點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
```

- 複製BPA套裝程式

```
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
```

入口設定

- 啟用入口
  更新值。yamlto enable ingress：

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

- **使用BPA證書建立金鑰**
  導航到證書目錄並建立金鑰：

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

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

- **更新入口控制器**
  將新建立的金鑰增加到 **`ingress-controller.yaml`** 檔案：

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

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

- **更新入口證書**
  執行Helm刪除和安裝以更新入口證書。

環境規格

環境規範包括EC2例項、負載平衡器、VPC終端和RDS例項的要求。主要規格包括：

EC2要求：

儲存需求：每個節點有2TB的空間。將EBS磁碟區掛載至/opt，並在/etc/fstab中新增所有節點的專案。

入站安全組：30101、443、0 - 65535 TCP、22 for ssh。

出站安全組：必須啟用所有流量。

DNS解析程式：EC2在/etc/resolve.conf中必須具有內部解析程式。

負載平衡器需求：

- 監聽器連線埠必須是443、30101。
- VPC終端要求(Atlas MongoDB)。
- 為Atlas連線建立的VPC終端在父帳戶(aws-5g-ndc-prod)中可用。VPC終端必須具有允許所有入站訪問的安全組(0 - 65535)。

RDS要求：

RDS型別：db.r5b.2xlarge

Postgres引擎版本：13.7

安全組：入站必須允許來自POD CIDR源的流量。

主要概念和元件

瞭解Kubernetes基礎知識對於使用Amazon EKS有效部署和管理應用程式至關重要。

結論

本文為使用Amazon EKS部署和管理業務流程自動化(BPA)應用程式提供詳細指南。透過遵循概述的步驟並瞭解關鍵概念，組織可以將EKS的優勢用於其容器化BPA應用程式。

參考資料

- **Amazon Web Services，「Amazon EKS Documentation」，[線上]。可參閱：https://docs.aws.amazon.com/eks/**
- **Kubernetes，「Kubernetes Documentation」，[線上]。可參閱：https://kubernetes.io/docs/home/**
- **Cisco BPA概覽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開發人員指南https://www.cisco.com/c/dam/en/us/support/docs/bpa/v403/cisco-bpa-developer-guide-v403.pdf**

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。