

Implementeren en beheren van Business Process Automation-toepassingen op Amazon EKS: een praktische gids

Inhoud

Samenvatting

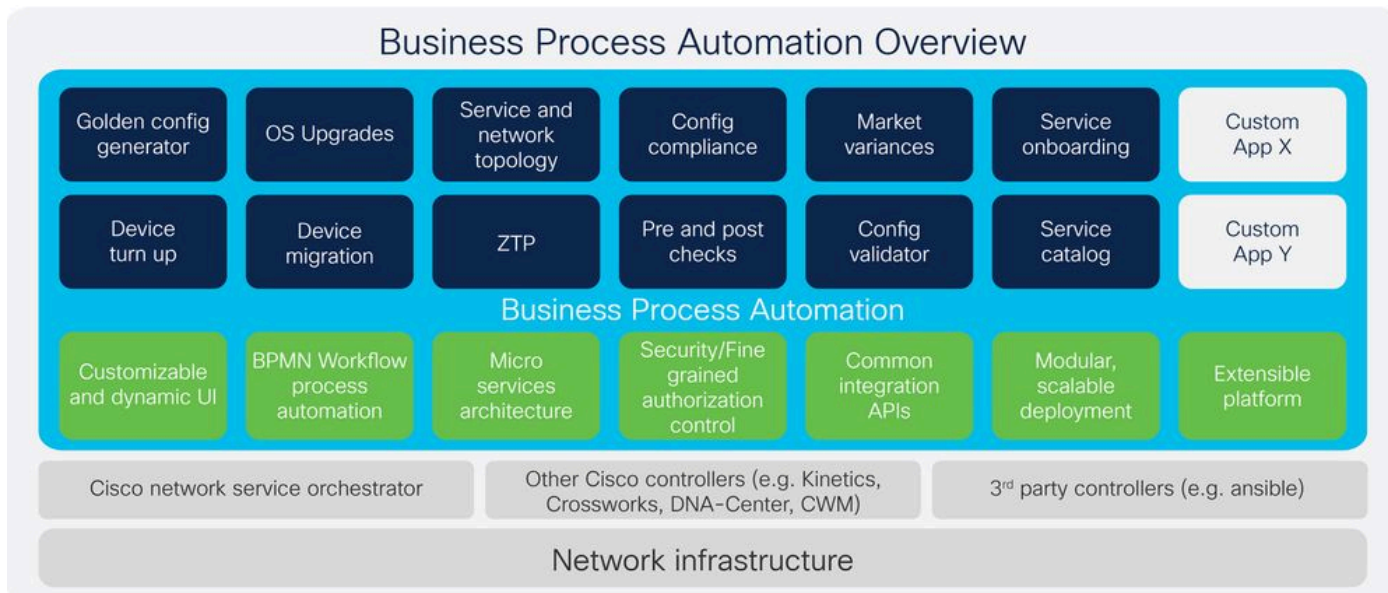
Dit artikel bevat een uitgebreide handleiding over de implementatie en het beheer van Business Process Automation (BPA) applicaties met behulp van Amazon Elastic Kubernetes Service (EKS). Het schetst de voorwaarden, benadrukt de voordelen van het gebruik van EKS, en verstrekt stap-voor-stap instructies voor het opzetten van een EKS-cluster, Amazon RDS-database, en MongoDB Atlas. Daarnaast wordt in het artikel aandacht besteed aan de implementatiearchitectuur en worden de omgevingsvereisten gespecificeerd, zodat organisaties die op zoek zijn naar een optimale benutting van de EKS voor hun containergebonden BPA-toepassingen, over een degelijke bron beschikken.

Trefwoorden

Amazon EKS, Kubernetes, AWS, RDS, MongoDB Atlas, DevOps, Cloud Computing, Business Process Automation.

Inleiding

BPA



In het huidige digitale tijdperk proberen bedrijven complexe bedrijfsprocessen te stroomlijnen en te automatiseren in een gevarieerde reeks IT-omgevingen. Business Process Automation (BPA) is uitgegroeid tot een cruciale technologie die organisaties in staat stelt de operationele efficiëntie te verbeteren, fouten te verminderen en de dienstverlening te verbeteren. BPA introduceert verschillende belangrijke innovaties en verbeteringen gericht op het bevorderen van workflow automatisering, service provisioning en off-the-shelf automatiseringstoepassingen.

Het BPA-platform is de host voor zakelijke en IT/operationele gebruikscases en toepassingen, zoals upgrades van het besturingssysteem, serviceprovisioning en integratie met orkestratiemotoren. Klanten hebben toegang tot een levenscyclus van services en BPA-functies, inclusief advies, implementatie, bedrijfskritieke services en oplossingsondersteuning die worden geleverd door Cisco-experts, best practices en beproefde technieken en methodologieën die helpen hun bedrijfsprocessen te automatiseren en het risico van hun systemen te verminderen.

Deze levenscyclusmogelijkheden kunnen op abonnement worden gebaseerd of aan individuele behoeften worden aangepast. Implementatieservices helpen bij het definiëren, integreren en implementeren van tools en processen om automatisering te versnellen. Cisco-experts voeren een formeel proces uit voor het verzamelen van vereisten, ontwerpen en ontwikkelen gebruikersverhalen op basis van flexibele processen en CI/CD-tools (Continuous Integration and Continuous Delivery) en implementeren flexibele services met geautomatiseerde tests van nieuwe of bestaande werkstromen, apparaten en services. Dankzij de ondersteuning van de oplossing krijgen klanten 24 uur per dag en 7 dagen per week toegang tot gecentraliseerde ondersteuning met de nadruk op softwarecentrische problemen in combinatie met ondersteuning van meerdere leveranciers en open bronnen via het gelaagde softwaremodel van Cisco. Cisco-experts voor oplossingsondersteuning helpen uw case te beheren vanaf de eerste oproep tot de definitieve oplossing en fungeren als het belangrijkste contactpunt wanneer u met meerdere leveranciers tegelijk werkt. U kunt tot 44 procent minder problemen ervaren bij het werken met experts op oplossingsniveau, waardoor u bedrijfscontinuïteit kunt behouden en sneller rendement krijgt op uw BPA-investering.

De belangrijkste technische kenmerken, zoals ondersteuning voor FMC en Ansible-managed devices,

parallele executies met behulp van het Advanced Queuing Framework (AQF), en uitgebreide configuratie compliance voor NDFC- en FMC-apparaten, plaatsen BPA als een uitgebreide oplossing voor grootschalige bedrijfsautomatisering. Met extra mogelijkheden in SD-WAN beheer, device onboarding, en beheer van firewallbeleid, richt de release zich op kritische aspecten van netwerkbeveiliging en automatisering, gericht op de eisen van grootschalige omgevingen met meerdere leveranciers.

EKS

Amazon Elastic Kubernetes Service (EKS) is een volledig beheerde Kubernetes-service van Amazon Web Services (AWS). De in 2018 gelanceerde EKS vereenvoudigt het proces van het implementeren, beheren en schalen van containertoepassingen met behulp van Kubernetes, een open-source containerorkestratieplatform. EKS vat de complexiteit van het clusterbeheer van Kubernetes samen, waardoor ontwikkelaars zich op de bouw en het runnen van toepassingen kunnen concentreren zonder de onderliggende infrastructuur te moeten behandelen.

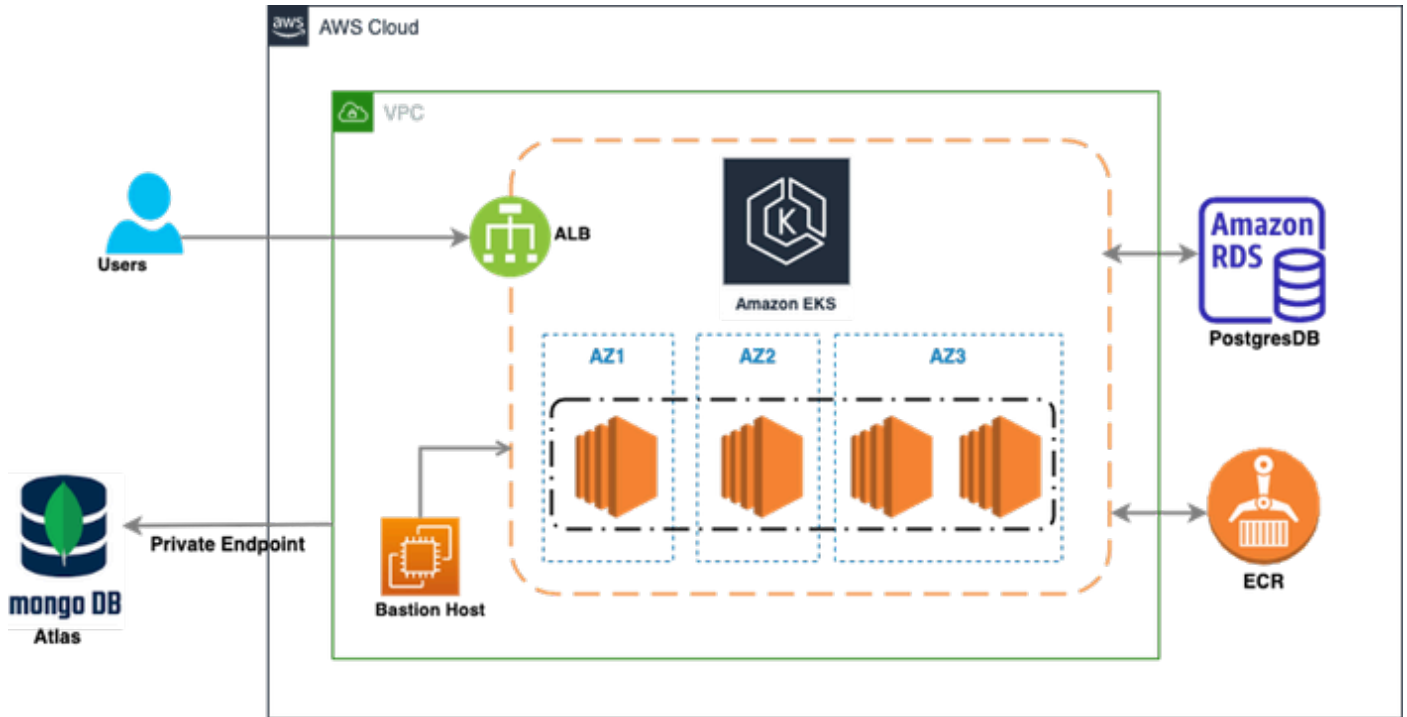
Voordelen van het gebruik van Amazon EKS voor de implementatie van toepassingen

Amazon EKS biedt verschillende voordelen voor de implementatie van applicaties, waardoor het een populaire keuze is voor organisaties die gebruik maken van containertoepassingen en microservices.

Belangrijkste voordelen:

- **Beheerde Kubernetes Control Plane:** EKS beheert de inzet, schaling en het onderhoud van het Kubernetes control plane, waardoor de operationele belasting wordt verminderd.
- **Vereenvoudigd clusterbeheer:** EKS maakt een samenvatting van de complexiteit van het opzetten en beheren van Kubernetes-clusters.
- **Schaalbaarheid:** EKS maakt het mogelijk om clusters gemakkelijk te schalen om de toenemende werkbelasting aan te kunnen.
- **Hoge beschikbaarheid:** EKS ondersteunt multi-Availability Zone implementaties, waardoor de beschikbaarheid en de fouttolerantie worden verbeterd.
- **Integratie met AWS Services:** EKS integreert naadloos met diverse AWS services.
- **DevOps Automation:** EKS ondersteunt continue integratie en continue inzet (CI/CD) voor containertoepassingen.

BPA-implementatiearchitectuur



Dit beeld vertegenwoordigt een overkoepelende architectuur van een cloudgebaseerde infrastructuur die op **AWS** is geïmplementeerd met behulp van verschillende belangrijke componenten. Hier is een uitsplitsing van het diagram:

1. **Amazon EKS (Elastic Kubernetes Service):** In de kern van het diagram wordt Amazon EKS ingezet in drie beschikbaarheidszones (AZ1, AZ2, AZ3), met Kubernetes-werkknooppunten binnen elke zone. Dit wijst op een hoogst beschikbare en fout-verdraagzame opstelling, aangezien de werkbelasting over veelvoudige beschikbaarheidszones wordt uitgespreid.
2. **ALB (Application Load Balancer):** Dit is aan de voorkant geplaatst, ontvangt verkeer van gebruikers en distribueert het over het EKS-cluster voor de verwerking van toepassingswerkbelastingen. De load balancer zorgt ervoor dat de aanvragen gelijkmatig verdeeld zijn en kan schalen op basis van de vraag naar verkeer aan.
3. **Amazon RDS (Relational Database Service) - PostgreSQL:** Aan de rechterkant van het diagram is een Amazon RDS-instantie aanwezig die PostgreSQL uitvoert. Deze database kan worden benaderd door applicaties die binnen het EKS-cluster draaien.
4. **ECR (Elastic Container Registry):** Hier worden Docker containerafbeeldingen opgeslagen en beheerd, die vervolgens worden ingezet in Amazon EKS voor het uitvoeren van de werkbelasting.
5. **MongoDB Atlas:** Aan de linkerkant is MongoDB Atlas geïntegreerd in de architectuur via een eigen eindpunt. MongoDB Atlas is een cloudgehoste NoSQL database service, hier gebruikt om documentgebaseerde database vereisten te verwerken. Het privé-eindpunt zorgt voor veilige, privé communicatie tussen de MongoDB Atlas instantie en andere AWS componenten.
6. **Bastion Host:** In de VPC (Virtual Private Cloud) is een Bastion Host een veilig toegangspunt voor beheerders om toegang te krijgen tot resources binnen de VPC zonder ze rechtstreeks bloot te stellen aan het internet.

Over het algemeen biedt deze architectuur een zeer beschikbare, schaalbare en veilige oplossing voor het implementeren en beheren van containertoepassingen met Amazon EKS, met ondersteuning voor zowel relationele (PostgreSQL) en NoSQL (MongoDB) databases.

- **EKS Cluster instellen**

Om een Amazon EKS-cluster te maken met de AWS CLI, kan de `eksctl`-opdrachtregel worden gebruikt. Dit is een voorbeeldopdracht:

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

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

- **RDS-database instellen**

Het implementeren van een relationele database op Amazon RDS omvat de volgende stappen:

- Ga naar de AWS Management Console en ga naar de Amazon RDS-service.
- Maak een nieuwe database-instantie met de gewenste specificaties.
- Configureer de beveiligingsgroep zodat inkomende verbindingen van uw Amazon EKS-cluster mogelijk zijn.

aws Services Search [Option+S]

RDS > Create database

Create database


Choose a database creation method [Info](#)


Standard create
You set all of the configuration options, including ones for availability, security, backups, and maintenance.


Easy create
Use recommended best-practice configurations. Some configuration options can be changed after the database is created.


Engine options


Engine type [Info](#)


Aurora (MySQL Compatible) 


Aurora (PostgreSQL Compatible) 


MySQL 

MariaDB 

PostgreSQL 

Oracle 

Microsoft SQL Server 

IBM Db2 

Engine version [Info](#)
View the engine versions that support the following database features.

▼ Hide filters

Show versions that support the Multi-AZ DB cluster [Info](#)
Create a Multi-AZ DB cluster with one primary DB instance and two readable standby DB instances. Multi-AZ DB clusters provide up to 2x faster transaction commit latency and automatic failover in typically under 35 seconds.

Engine Version
PostgreSQL 16.3-R2 ▼

Enable RDS Extended Support [Info](#)
Amazon RDS Extended Support is a [paid offering](#). By selecting this option, you consent to being charged for this offering if you are running your database major version past the RDS end of standard support date for that version. Check the end of standard support date for your major version in the [RDS for PostgreSQL documentation](#).

Selecteer met behulp van het vervolgkeuzemenu de meest recente versie van PostgreSQL. In ons geval is het "PostgreSQL 16.3-R1."

aws Services Search [Option+S]

Creates a single DB instance with no standby DB instances.

- Multi-AZ DB instance
Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.
- Multi-AZ DB Cluster
Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.

Settings

DB cluster identifier [Info](#)
Enter a name for your DB cluster. The name must be unique across all DB clusters owned by your AWS account in the current AWS Region.

The DB cluster identifier is case-insensitive, but is stored as all lowercase (as in "mydbcluster"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ **Credentials Settings**

Master username [Info](#)
Type a login ID for the master user of your DB cluster.

1 to 16 alphanumeric characters. The first character must be a letter.

Credentials management
You can use AWS Secrets Manager or manage your master user credentials.

- Managed in AWS Secrets Manager - most secure**
RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.
- Self managed**
Create your own password or have RDS create a password that you manage.

Auto generate password
Amazon RDS can generate a password for you, or you can specify your own password.

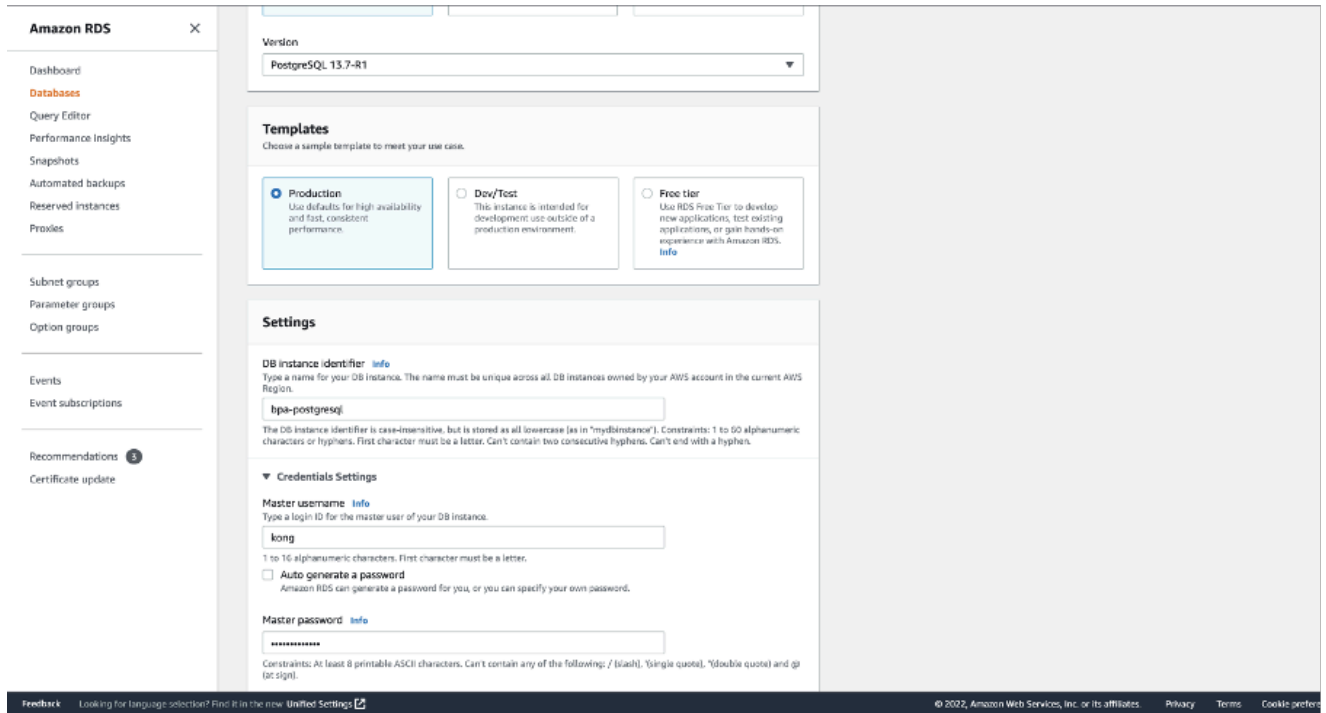
Master password [Info](#)

Password strength Neutral

Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / ' " @

Confirm master password [Info](#)

Geef de database-instantie hiervoor een naam en voer een gebruikersnaam en wachtwoord in.



Zorg ervoor dat de standaardinstellingen voor "DB-instantiegrootte" en "Storage" zijn geselecteerd.

Afhankelijk van de clustergrootte en de gegevensvereisten, selecteer de juiste grootte van de DB-
instantie en het juiste opslagtype.

Gebaseerd op onze use case hebben we de volgende configuratie gekozen:

- **Grootte van DB-instantie:** db.m5d.2xlarge
 - 8 vCPU's
 - 32 GiB RAM
 - Netwerk: 4.750 Mbps
 - 300 GB Instance Store

aws Services Search [Option+S]

Instance configuration

The DB instance configuration options below are limited to those supported by the engine that you selected above.

DB instance class [Info](#)

- Standard classes (includes m classes)
- Memory optimized classes (includes r classes)
- Compute optimized classes (includes c classes)

db.m5d.2xlarge
8 vCPUs 32 GiB RAM Network: 4,750 Mbps 300 GB Instance Store

Storage

Storage type [Info](#)
Provisioned IOPS SSD (io2) storage volumes are now available.

Provisioned IOPS SSD (io2)
Low latency, highly durable, I/O intensive storage

Allocated storage [Info](#)
400 GiB
The minimum value is 100 GiB and the maximum value is 65,536 GiB

i After you modify the storage for a DB instance, the status of the DB instance will be in storage-optimization. Your instance will remain available as the storage-optimization operation completes. [Learn more](#)

Provisioned IOPS [Info](#)
3000 IOPS
The minimum value is 1,000 IOPS and the maximum value is 2,56,000 IOPS. The IOPS to GiB ratio must be between 0.5 and 1,000

i Your actual IOPS might vary from the amount that you provisioned based on your database workload and instance type. [Learn more](#)

► Storage autoscaling

Selecteer de gewenste waarden op basis van uw gebruikscase. We hebben de standaardwaarden geselecteerd.

aws Services Search [Option+S]

Connectivity [Info](#)

Compute resource
Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

Don't connect to an EC2 compute resource
Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

Connect to an EC2 compute resource
Set up a connection to an EC2 compute resource for this database.

Virtual private cloud (VPC) [Info](#)
Choose the VPC. The VPC defines the virtual networking environment for this DB cluster.

vpc-usw2az123001nd (vpc-055eca9021e79cfc7)
60 Subnets, 3 Availability Zones

Only VPCs with a corresponding DB subnet group are listed.

ⓘ After a database is created, you can't change its VPC.

DB subnet group [Info](#)
Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB cluster can use in the VPC that you selected.

bpasubnetgroup
2 Subnets, 2 Availability Zones

⚠ The DB subnets must be in 3 Availability Zones (AZs) for the Multi-AZ DB cluster. The current subnets are in 2 AZs (us-west-2a ,us-west-2b). Add a subnet in a different AZ than the current subnets. [Edit new subnet ↗](#)

Public access [Info](#)

Yes
RDS assigns a public IP address to the cluster. Amazon EC2 instances and other resources outside of the VPC can connect to your cluster. Resources inside the VPC can also connect to the cluster. Choose one or more VPC security groups that specify which resources can connect to the cluster.

No
RDS doesn't assign a public IP address to the cluster. Only Amazon EC2 instances and other resources inside the VPC can connect to your cluster. Choose one or more VPC security groups that specify which resources can connect to the cluster.

VPC security group (firewall) [Info](#)
Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

Choose existing
Choose existing VPC security groups

Create new
Create new VPC security group

Zorg ervoor in "Database authenticatie" hebben we Wachtwoordverificatie geselecteerd. Verificeert met behulp van database-wachtwoorden.

**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.



▼ 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

The screenshot shows the 'Encryption' configuration page in the AWS Management Console. At the top, there is a navigation bar with the AWS logo, 'Services', a search bar, and a keyboard shortcut '[Option+S]'. A hamburger menu icon is on the left. The main content area is titled 'Encryption' and contains several sections:

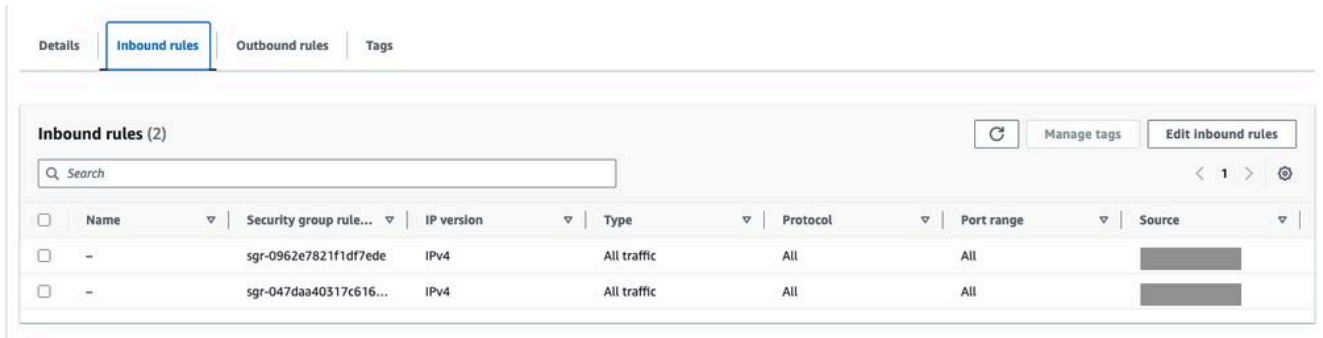
- Enable encryption:** A checked checkbox. Below it, text explains that master key IDs and aliases appear in the list after creation using the AWS Key Management Service (KMS) console. An 'Info' link is provided.
- AWS KMS key:** A dropdown menu currently showing '(default) aws/rds'.
- Account:** The account ID '193670463418' is displayed.
- KMS key ID:** The key ID '61e6c956-745e-42be-8fd1-77953104ad4f' is displayed.
- Log exports:** A section with the instruction 'Select the log types to publish to Amazon CloudWatch Logs'. Two checkboxes are present: 'PostgreSQL log' and 'Upgrade log', both of which are unchecked.
- IAM role:** A section with the instruction 'The following service-linked role is used for publishing logs to CloudWatch Logs.' Below this, a grey box displays 'RDS service-linked role'.
- Maintenance:** A section with the instruction 'Auto minor version upgrade Info'. It includes a checked checkbox for 'Enable auto minor version upgrade' and explanatory text: 'Enabling auto minor version upgrade will automatically upgrade to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the database.'
- Maintenance window:** A section with the instruction 'Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.' It has two radio button options: 'Choose a window' (unchecked) and 'No preference' (checked).
- Deletion protection:** A section with a checked checkbox for 'Enable deletion protection' and explanatory text: 'Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database cluster.'

At the bottom of the page, there is a light blue information box with an 'i' icon: 'You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.' Below this box are two buttons: 'Cancel' and 'Create database' (highlighted in orange).

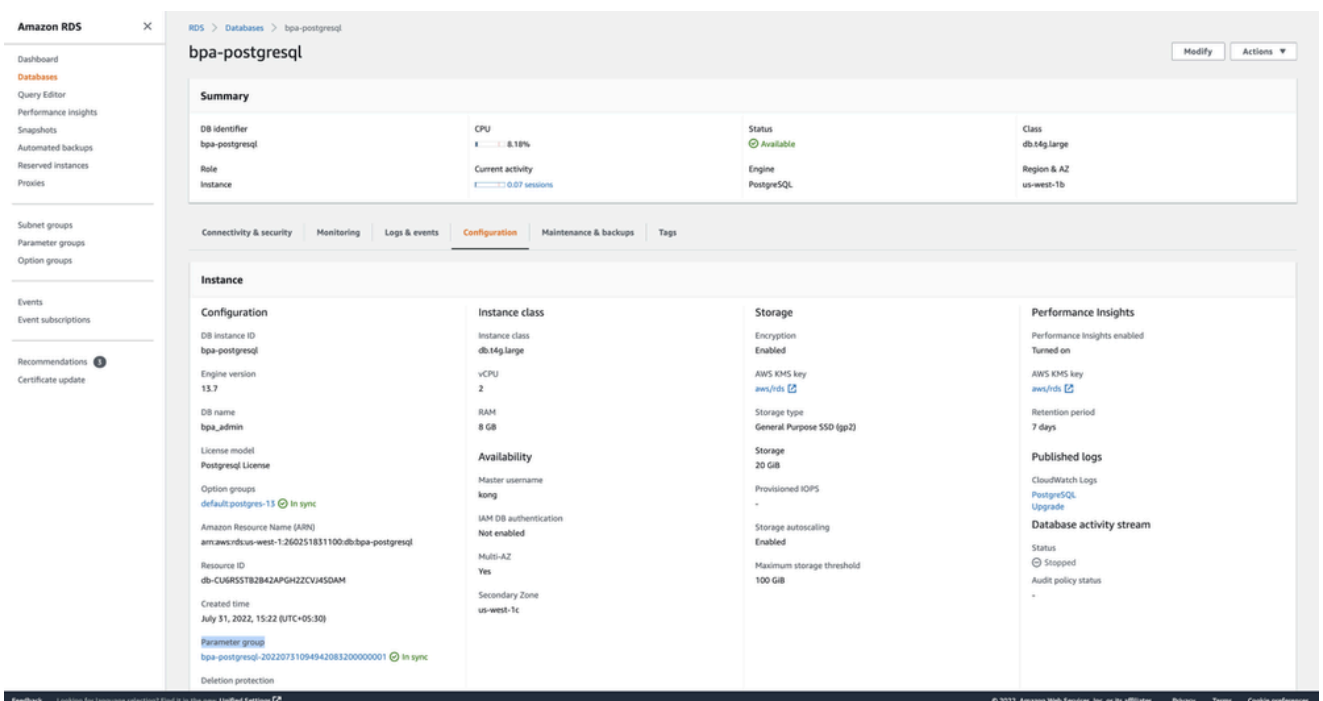
Zodra dat is geverifieerd, zijn we klaar om de database aan te maken. Ga terug naar het Amazon RDS dashboard. Bevestig dat de instantie beschikbaar is voor gebruik.

Regels voor security groepen

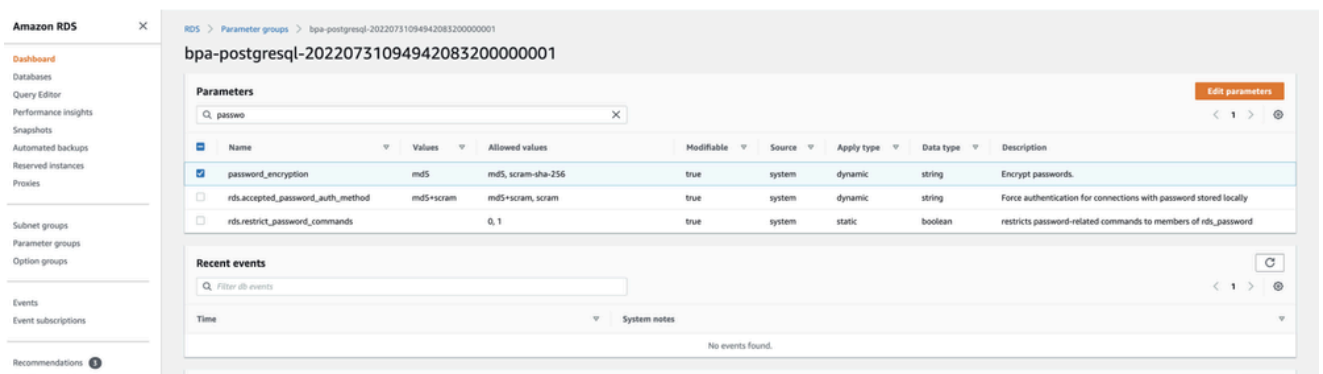
Werk de inkomende beveiligingsgroep bij met het CIDR-blok van de peul en het CIDR-blok van het knooppunt.



In RDS -> Databases -> DB-NAME, klik op Configuration, verwijfs de sectie Parameter Group en klik op de parametergroep om deze te bekijken.



Zoek naar "password_encryptie" en verander de waarde naar md5 van blank / andere waarde. Dit is nodig voor camunda configuraties om te werken.



Maak deze databases samen met gebruikers door verbinding te maken met de 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=W0rkFl0#ChangeNow
WFE_DB_NAME=process-engine
```

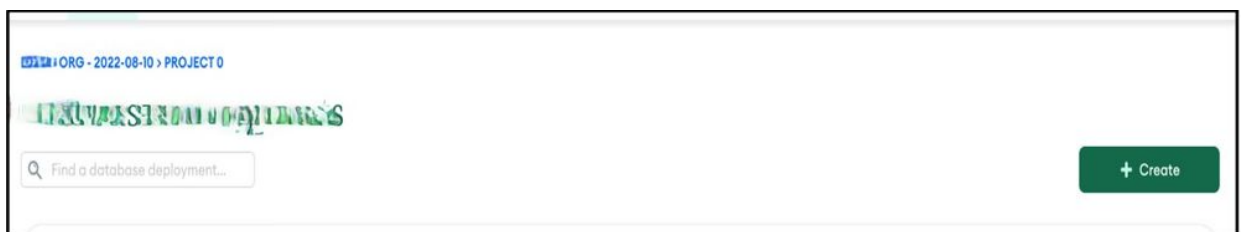
- Wachtwoordverificatie

Verifieert met behulp van database-wachtwoorden.

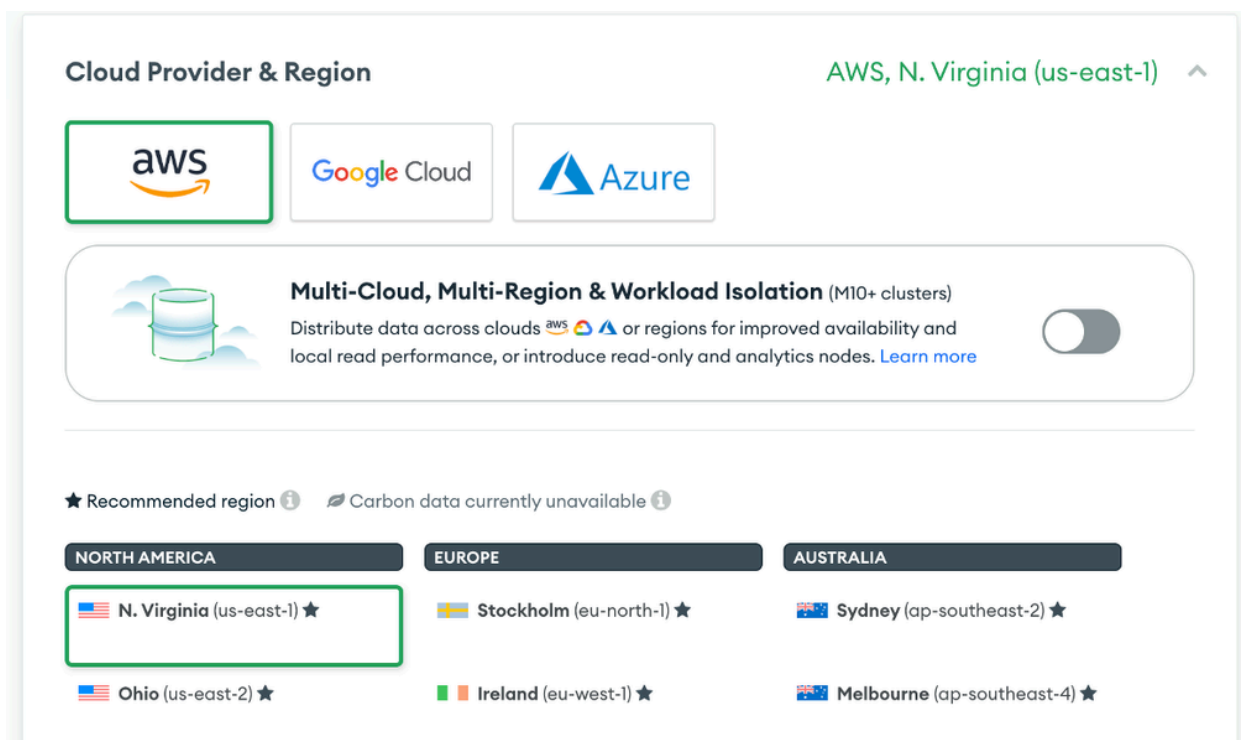
- **Atlas MongoDB instellen**

Het opzetten van Atlas MongoDB omvat:

- **Inloggen bij Atlas MongoDB.**
- **De organisatie en het project selecteren.**
- **Een specifieke cluster maken met de juiste specificaties.**



- **Selecteer de speciale laag, Cloud Provider & regio.**



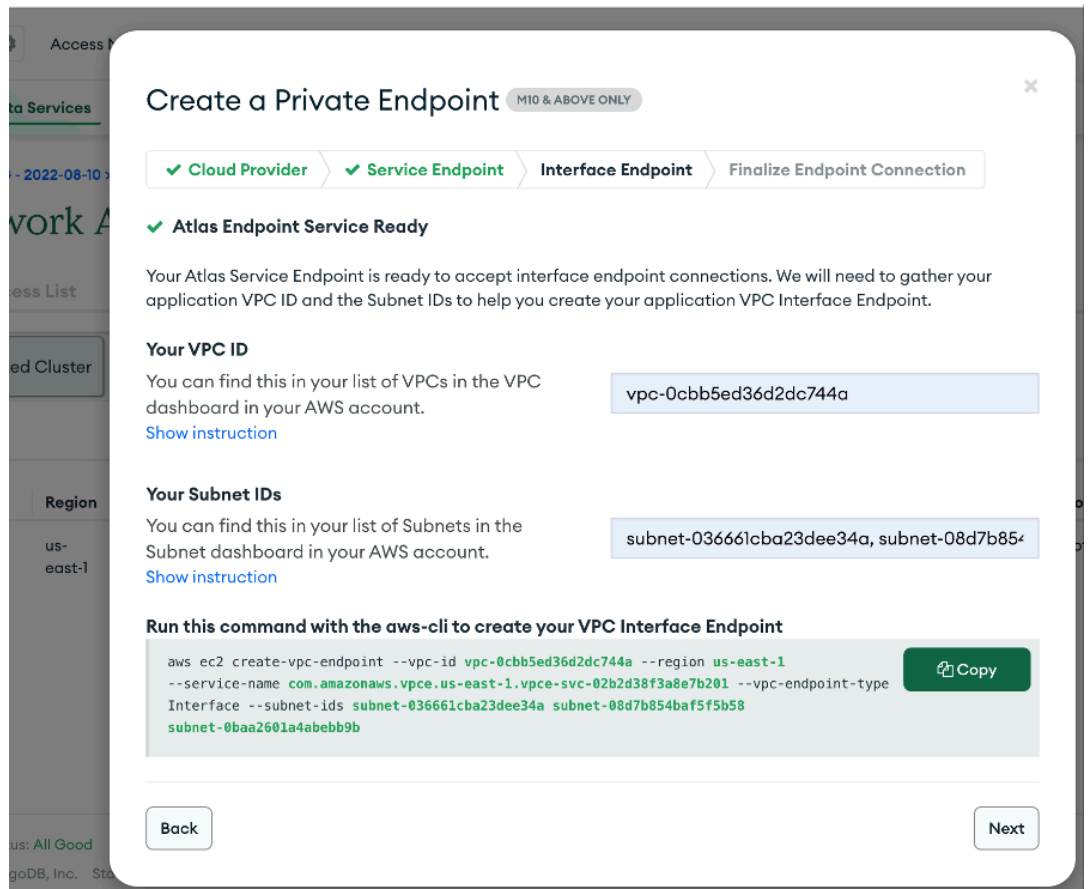
- **Selecteer de juiste laag (we hebben M30 als laag gebruikt) toegewezen cluster en geef de juiste clusternaam op en klik op Create Cluster. Het zal het Atlas monogodb-cluster initialiseren.**

VERSION	REGION	CLUSTER TIER	TYPE	BACKUPS	LINKED APP SERVICES	ATLAS SQL	ONLINE ARCHIVE	ATLAS SEARCH
6.0.6	AWS / N. Virginia (us-east-1)	M30 (General)	Replica Set - 3 nodes	Active	None Linked	Connect	None	Create Index

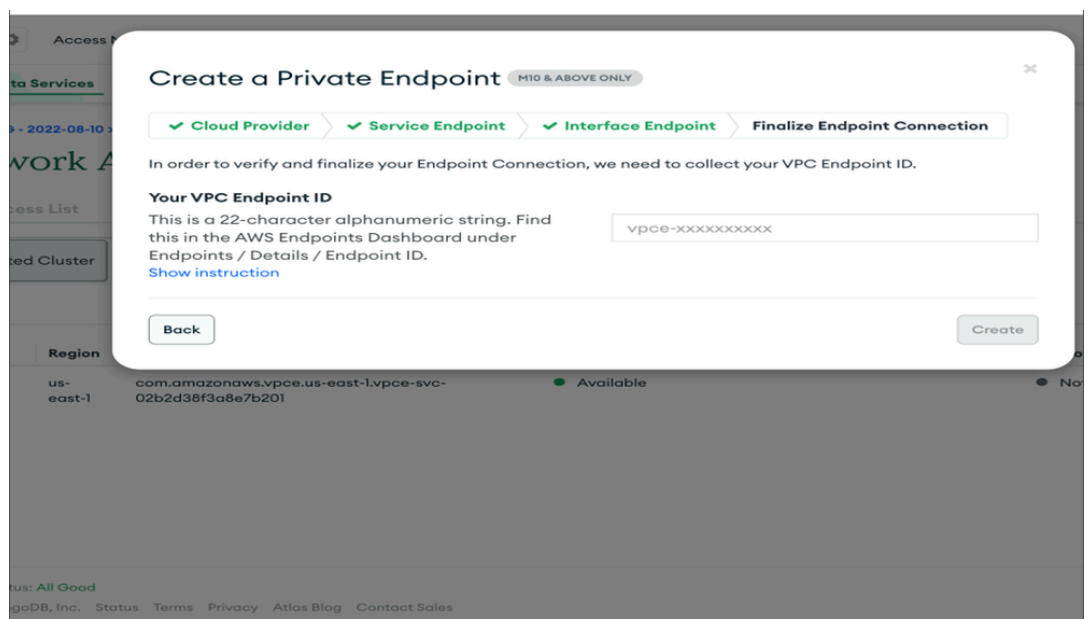
- **VPC Private endpoint instellen voor het Atlas- en K8S-cluster.**
 - **Klik op het tabblad Private Endpoint voor netwerktoegang en klik op Add Private Endpoint.**

- **Selecteer Cloud Provider als AWS, selecteer de betreffende regio en klik op Volgende.**

- **Respectieve PVC-id en subnetnummer opgeven. Zodra u de details hebt ingevoerd, kopieert u de opdracht voor het maken van de vpc-eindpunten en voert u deze uit in de webconsole. U krijgt de vpc-eindpunt-id als uitvoer.**

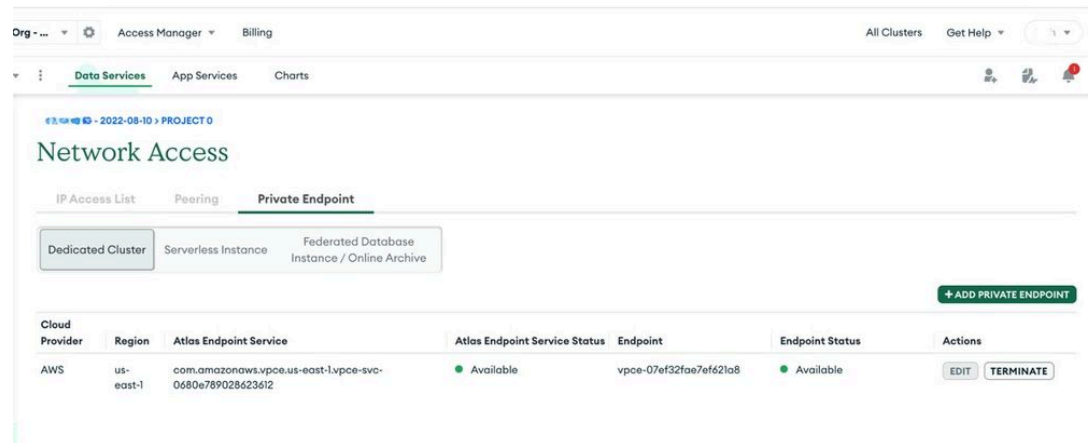


- **Klik op Next om de VPC-eindpunt-ID te plakken en klik op Create.**

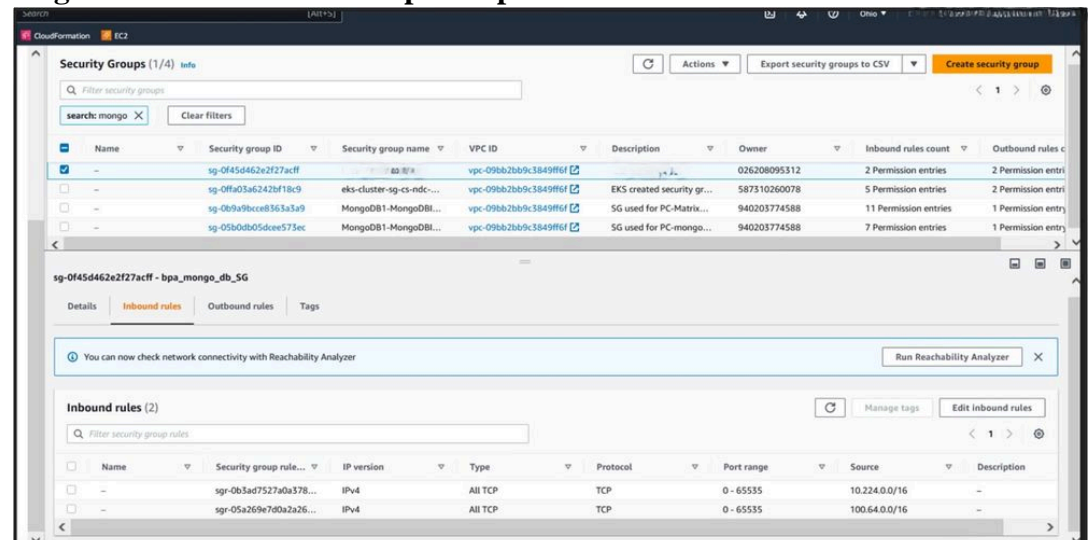


- **Zodra de eindpuntstatus met succes is gemaakt, is deze beschikbaar zoals in**

de volgende afbeelding. VPC-eindpunt moet worden gemaakt voor pod cidr. In ons geval hebben we "100.64.0.0/16" gebruikt.



- Voeg inkomende regels toe aan het nieuwe VPC-eindpunt. Het vpc-eindpunt wordt in de parent-account geplaatst en een beveiligingsgroep moet worden toegewezen aan het nieuwe vpc-eindpunt.



ECR als beeldregister

Het creëren van Amazon ECR-repositories en het indrukken van Docker-afbeeldingen in deze repositories impliceert verschillende stappen. Dit zijn de stappen om een ECR-opslagplaats te maken, een Docker-afbeelding te labelen en naar de opslagplaats te duwen met de AWS CLI.

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

Vervangen:

- uw-afbeelding-naam met de gewenste naam voor uw ECR-opslagplaats.

- uw-regio met uw AWS-regio

IAM-rol voor EKS-knooppunten configureren

Zorg ervoor dat de EKS-werknemersknooppunten (EC2-instanties) de noodzakelijke IAM-rol hebben toegewezen met toestemming om beelden van ECR te halen. Het vereiste IAM-beleid is:

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

Hang dit beleid aan de IAM rol verbonden aan uw EKS-werknemersknooppunten.

BPA-implementatie

De uitrol van BPA omvat verschillende stappen, waaronder het labelen van EKS-werknemersknooppunten, het voorbereiden van directory's op knooppunten, het kopiëren van BPA-pakketten en het inzetten van BPA met Helm.

Voor onze klantimplementatie hebben we de volgende versies van software- en cloudservices gebruikt:

- **BPA:** 4,0,3-6
- **RDS (Relational Database Service):** 16.3-R2
- **MongoDB Atlas:** v5.0.29
- **EKS (Elastic Kubernetes Service):** v1.27

Deze componenten zorgen ervoor dat onze implementatie robuust, schaalbaar en in staat is om de vereiste werkbelasting efficiënt te verwerken.

- **Etikettering EKS Worker Knooppunten**

```
kubectl label node
```

```
name=node-1 kubect1 label node
```

```
name=node-2 kubect1 label node
```

```
name=node-3 kubect1 label node
```

```
name=node-4
```

- **Directories op knooppunten voorbereiden**

- Knooppunt 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
```

- knooppunt 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
```

knooppunt 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
```

Knooppunt 4:

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

- BPA-pakketten kopiëren

```
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/
```

- BPA implementeren met Helm

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

Instellen toegangscontrole

- **Inloop inschakelen**

Update `values.yaml`om toegang te krijgen:

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

- **Een geheim maken met BPA-certificaat**

Navigeer naar de certificaatmap en maak een geheim:

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

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

- **Ingress Controller bijwerken**

Voeg het nieuw gemaakte geheim toe in de `toegang-controller.yaml` bestand:

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

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

- **Ingress-certificaat bijwerken**

Voer Helm verwijderen en installeren om het toegangscertificaat bij te werken.

Omgevingsspecificaties

De omgevingsspecificaties omvatten eisen voor EC2-instanties, load balancers, VPC-endpoints en RDS-instanties. Belangrijkste specificaties zijn:

Eisen EC2:

Opslagvereisten: 2 TB ruimte per knooppunten. Monteer EBS volume naar /opt en voeg een vermelding toe in /etc/fstab voor alle knooppunten.

Beveiligingsgroep inkomend: 30101, 443, 0 - 65535 TCP, 22 voor SSH.

Security groep uitgaand: al het verkeer moet zijn ingeschakeld.

DNS Resolver: EC2 moet over on-prem-oplossers beschikken in /etc/resolve.conf.

Eisen voor taakverdeling:

- Listeners poorten moeten 443, 30101 zijn.
- VPC-eindpuntvereisten (Atlas MongoDB).
- VPC-eindpunten die zijn gemaakt voor de Atlas-connectiviteit zijn beschikbaar in de parent-account (aws-5g-ndc-prod). VPC Endpoint moet een beveiligingsgroep hebben die alle inkomende toegang (0-65535) biedt.

RDS-vereisten:

RDS-type: db.r5b.2xlarge

Postgres Engine versie: 13.7

Security groep: Inbound moet verkeer toestaan uit de POD CIDR-bron.

Belangrijke concepten en componenten

Het begrijpen van de basisprincipes van Kubernetes is essentieel voor het effectief inzetten en beheren van applicaties met Amazon EKS.

Conclusie

Dit artikel biedt een gedetailleerde handleiding voor het implementeren en beheren van Business Process Automation (BPA) applicaties met behulp van Amazon EKS. Door de beschreven stappen te volgen en de belangrijkste concepten te begrijpen, kunnen organisaties de voordelen van EKS gebruiken voor hun containergebonden BPA-toepassingen.

Referenties

- Amazon Web Services, "Amazon EKS Documentatie," [Online]. Beschikbaar op:<https://docs.aws.amazon.com/eks/>
- Kubernetes, "Kubernetes Documentatie," [Online]. Beschikbaar op:<https://kubernetes.io/docs/home/>
- Cisco BPA in een oogopslag <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/at-a-glance-c45-742579.html>
- BPA Operations Guide <https://www.cisco.com/c/dam/en/us/support/docs/bpa/v403/cisco-bpa-operations-guide-v403.pdf>
- BPA Developer Guide <https://www.cisco.com/c/dam/en/us/support/docs/bpa/v403/cisco-bpa-developer-guide-v403.pdf>

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.