

Bereitstellung und Management von Anwendungen zur Automatisierung von Geschäftsprozessen auf Amazon EKS: ein praktischer Leitfaden

Inhalt

Zusammenfassung

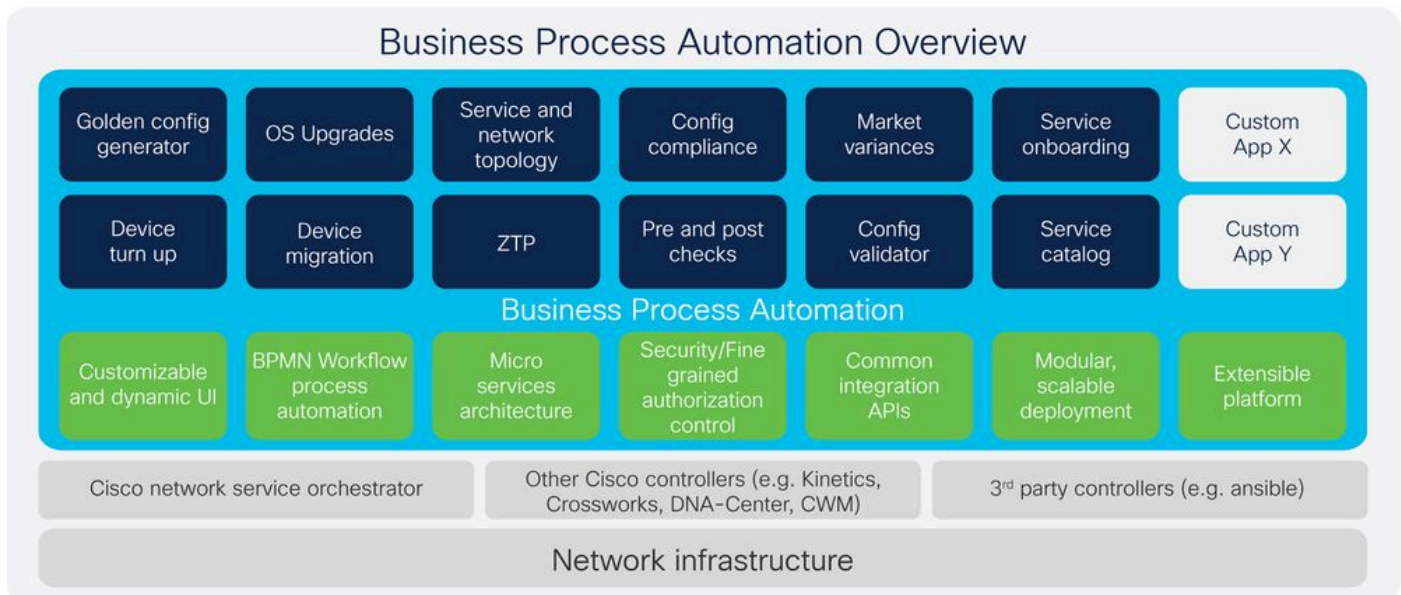
Dieses Dokument enthält einen umfassenden Leitfaden zur Bereitstellung und Verwaltung von Business Process Automation (BPA)-Anwendungen mit Amazon Elastic Kubernetes Service (EKS). Es beschreibt die Voraussetzungen, hebt die Vorteile der Verwendung von EKS hervor und liefert Schritt-für-Schritt-Anleitungen für die Einrichtung eines EKS-Clusters, einer Amazon RDS-Datenbank und von MongoDB Atlas. Darüber hinaus wird in diesem Dokument die Bereitstellungsarchitektur näher beschrieben und auf die Anforderungen der Umgebung eingegangen. Unternehmen, die EKS für ihre containerisierten BPA-Anwendungen nutzen möchten, erhalten dadurch eine umfassende Ressource.

Schlüsselwörter

Amazon EKS, Kubernetes, AWS, RDS, MongoDB Atlas, DevOps, Cloud Computing, Automatisierung von Geschäftsprozessen

Einleitung

BPA



Im heutigen digitalen Zeitalter streben Unternehmen die Optimierung und Automatisierung komplexer Geschäftsprozesse in einer Vielzahl unterschiedlicher IT-Umgebungen an. Die Automatisierung von Geschäftsprozessen (Business Process Automation, BPA) hat sich zu einer zentralen Technologie entwickelt, die es Unternehmen ermöglicht, die Betriebseffizienz zu verbessern, Fehler zu reduzieren und die Servicebereitstellung zu verbessern. BPA führt eine Reihe wichtiger Innovationen und Verbesserungen ein, die auf die Weiterentwicklung von Anwendungen zur Workflow-Automatisierung, Servicebereitstellung und Standardautomatisierung abzielen.

Die BPA-Plattform hostet geschäftliche und IT-/betriebliche Anwendungsfälle und Anwendungen wie Betriebssystem-Upgrades, Servicebereitstellung und die Integration in Orchestrierungs-Engines. Kunden haben Zugriff auf einen Lebenszyklus von Services und BPA-Funktionen, einschließlich Beratung, Implementierung, geschäftskritische Services und Lösungssupport, die von Cisco Experten, Best Practices und bewährten Techniken und Methoden bereitgestellt werden, die sie bei der Automatisierung ihrer Geschäftsprozesse und der Risikobeseitigung ihrer Systeme unterstützen.

Diese Lebenszyklusfunktionen können abonnementbasiert oder an individuelle Anforderungen angepasst werden. Implementierungsservices unterstützen bei der Definition, Integration und Bereitstellung von Tools und Prozessen, um die Automatisierung zu beschleunigen. Die Experten von Cisco führen einen formellen Prozess für die Ermittlung der Anforderungen durch, entwerfen und entwickeln Benutzerberichte auf der Grundlage flexibler Prozesse und CI/CD-Tools (Continuous Integration and Continuous Delivery) und implementieren flexible Services mit automatisierten Tests neuer oder bestehender Workflows, Geräte und Services. Mit dem Solution Support erhalten Kunden rund um die Uhr Zugang zu zentralisiertem Support, der sich auf softwarebasierte Probleme konzentriert, kombiniert mit Support durch mehrere Anbieter und Open-Source-Ressourcen über das mehrstufige Software-Modell von Cisco. Die Experten des Cisco Solution Support unterstützen Sie beim Management Ihres Tickets vom ersten Anruf bis zur endgültigen Lösung und fungieren als Hauptansprechpartner für die Zusammenarbeit mit mehreren Anbietern gleichzeitig. Bei der Zusammenarbeit mit Experten auf Lösungsebene können Sie bis zu 44 Prozent weniger Probleme feststellen. So können Sie die Geschäftskontinuität aufrechterhalten und eine schnellere Rendite für Ihre BPA-Investition erzielen.

Wichtige technische Funktionen wie Unterstützung für FMC- und Ansible-verwaltete Geräte, parallele Ausführung mit dem Advanced Queuing Framework (AQF) und erweiterte Konfigurationskonformität für NDFC- und FMC-Geräte positionieren BPA als umfassende Lösung für die Automatisierung großer Unternehmen. Mit zusätzlichen Funktionen für das SD-WAN-Management, die Geräteintegration und die Firewall-Richtlinien-Governance adressiert die Version wichtige Aspekte der Netzwerksicherheit und -automatisierung und erfüllt so die Anforderungen großer Umgebungen mit Komponenten mehrerer Hersteller.

EKS

Amazon Elastic Kubernetes Service (EKS) ist ein vollständig verwalteter Kubernetes-Service, der von Amazon Web Services (AWS) bereitgestellt wird. EKS wurde 2018 ins Leben gerufen und vereinfacht die Bereitstellung, Verwaltung und Skalierung von containerisierten Anwendungen mithilfe von Kubernetes, einer Open-Source-Plattform für die Containerorchestrierung. EKS abstrahiert die Komplexität des Cluster-Managements von Kubernetes und ermöglicht es Entwicklern, sich auf die Entwicklung und Ausführung von Anwendungen zu konzentrieren, ohne die zugrunde liegende Infrastruktur handhaben zu müssen.

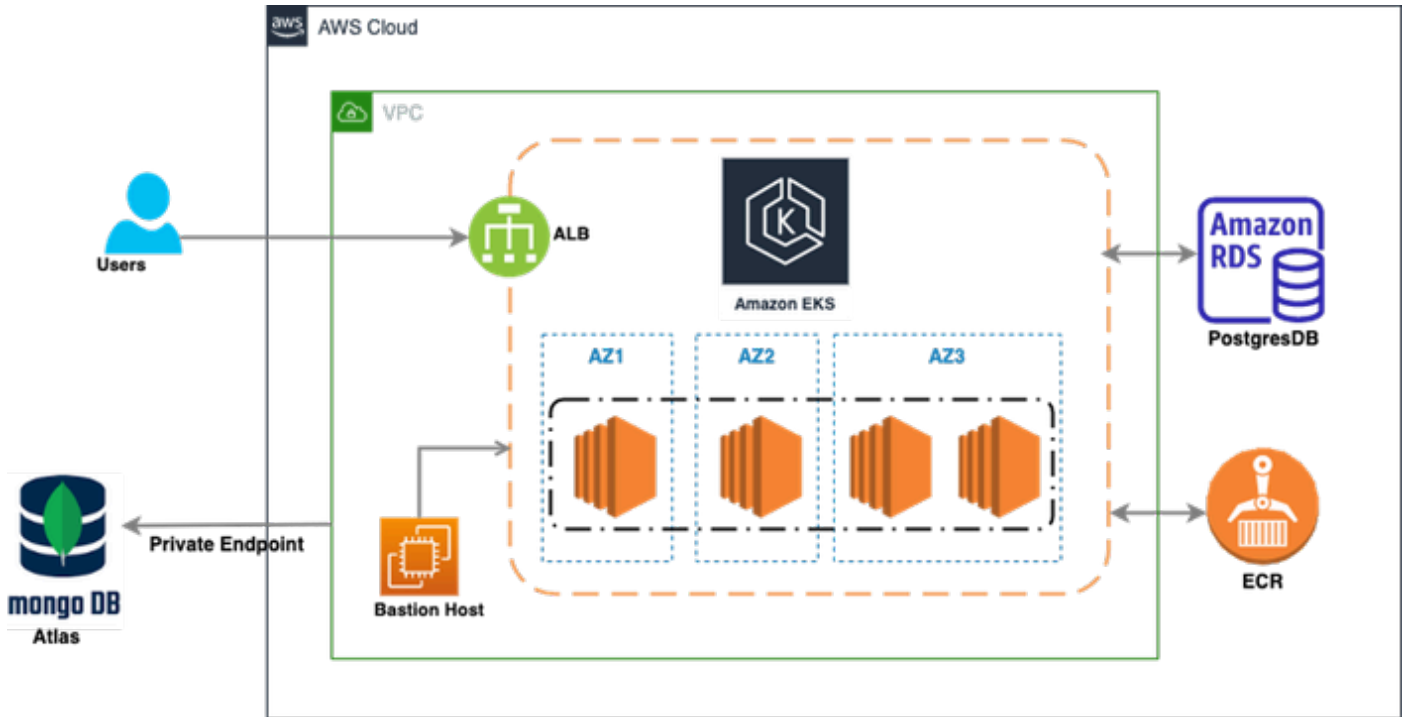
Vorteile von Amazon EKS für die Anwendungsbereitstellung

Amazon EKS bietet verschiedene Vorteile für die Anwendungsbereitstellung und ist damit eine beliebte Wahl für Unternehmen, die containerisierte Anwendungen und Mikroservices nutzen.

Zu den wichtigsten Vorteilen zählen:

- **Verwaltete Kubernetes-Kontrollebene:** EKS übernimmt die Bereitstellung, Skalierung und Wartung der Kubernetes-Kontrollebene, wodurch der Betriebsaufwand verringert wird.
- **Vereinfachtes Cluster-Management:** EKS abstrahiert die Komplexität bei der Einrichtung und Verwaltung von Kubernetes-Clustern.
- **Skalierbarkeit:** EKS ermöglicht eine einfache Skalierung von Clustern, um wachsenden Workloads gerecht zu werden.
- **Hohe Verfügbarkeit:** EKS unterstützt Bereitstellungen mit mehreren Verfügbarkeitszonen, wodurch die Verfügbarkeit und Fehlertoleranz verbessert werden.
- **Integration mit AWS Services:** EKS lässt sich nahtlos in verschiedene AWS Services integrieren.
- **DevOps-Automatisierung:** EKS unterstützt die kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) für containerisierte Anwendungen.

BPA-Bereitstellungsarchitektur



Dieses Image stellt eine High-Level-Architektur einer Cloud-basierten Infrastruktur dar, die auf **AWS** bereitgestellt wird und verschiedene Schlüsselkomponenten verwendet. Hier ist eine Aufschlüsselung des Diagramms:

1. **Amazon EKS (Elastic Kubernetes Service):** Im Kern des Diagramms wird Amazon EKS in drei Verfügbarkeitszonen (AZ1, AZ2, AZ3) bereitgestellt, wobei sich in jeder Zone Kubernetes-Mitarbeiterknoten befinden. Dies deutet auf eine hochverfügbare und fehlertolerante Konfiguration hin, da die Workloads über mehrere Verfügbarkeitszonen verteilt sind.
2. **ALB (Application Load Balancer):** Dieser befindet sich an der Vorderseite, empfängt Datenverkehr von Benutzern und verteilt diesen zur Bewältigung von Anwendungs-Workloads über das EKS-Cluster. Der Load Balancer stellt sicher, dass die Anforderungen gleichmäßig verteilt sind und eine Skalierung entsprechend der Datenverkehrsnachfrage verarbeiten können.
3. **Amazon RDS (Relational Database Service) - PostgreSQL:** Auf der rechten Seite des Diagramms ist eine Amazon RDS-Instanz vorhanden, auf der PostgreSQL ausgeführt wird. Auf diese Datenbank kann von Anwendungen zugegriffen werden, die im EKS-Cluster ausgeführt werden.
4. **ECR (Elastic Container Registry):** Hier werden Docker-Containerbilder gespeichert und verwaltet, die dann zum Ausführen der Workloads auf Amazon EKS bereitgestellt werden.
5. **MongoDB Atlas:** Auf der linken Seite ist MongoDB Atlas über ein privates Endgerät in die Architektur integriert. MongoDB Atlas ist ein in der Cloud gehosteter NoSQL-Datenbankdienst, der hier verwendet wird, um dokumentbasierte Datenbankanforderungen zu erfüllen. Der private Endpunkt sorgt für eine sichere, private Kommunikation zwischen der MongoDB Atlas Instanz und anderen AWS Komponenten.
6. **Bastion Host:** Ein Bastion Host, der innerhalb der VPC (Virtual Private Cloud) positioniert ist, bietet einen sicheren Einstiegspunkt für Administratoren, um auf Ressourcen innerhalb der VPC

zuzugreifen, ohne sie direkt dem Internet auszusetzen.

Insgesamt bietet diese Architektur eine hochverfügbare, skalierbare und sichere Lösung für die Bereitstellung und Verwaltung containerisierter Anwendungen mit Amazon EKS, die sowohl relationale (PostgreSQL) als auch NoSQL (MongoDB) Datenbanken unterstützt.

- **Einrichtung des EKS-Clusters**

Zum Erstellen eines Amazon EKS-Clusters mithilfe der AWS-CLI kann das Befehlszeilendienstprogramm `eksctl` verwendet werden. Dies ist ein Beispielbefehl:

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

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

- **RDS-Datenbankeinrichtung**

Die Bereitstellung einer relationalen Datenbank auf Amazon RDS umfasst folgende Schritte:

- Rufen Sie die AWS Management Console auf, und navigieren Sie zum Amazon RDS-Service.
- Erstellen Sie eine neue Datenbankinstanz mit den gewünschten Spezifikationen.
- Konfigurieren Sie die Sicherheitsgruppe so, dass eingehende Verbindungen von Ihrem Amazon EKS-Cluster zugelassen werden.

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](#).

Wählen Sie aus dem Dropdown-Menü die aktuelle Version von PostgreSQL aus. In unserem Fall ist es "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.

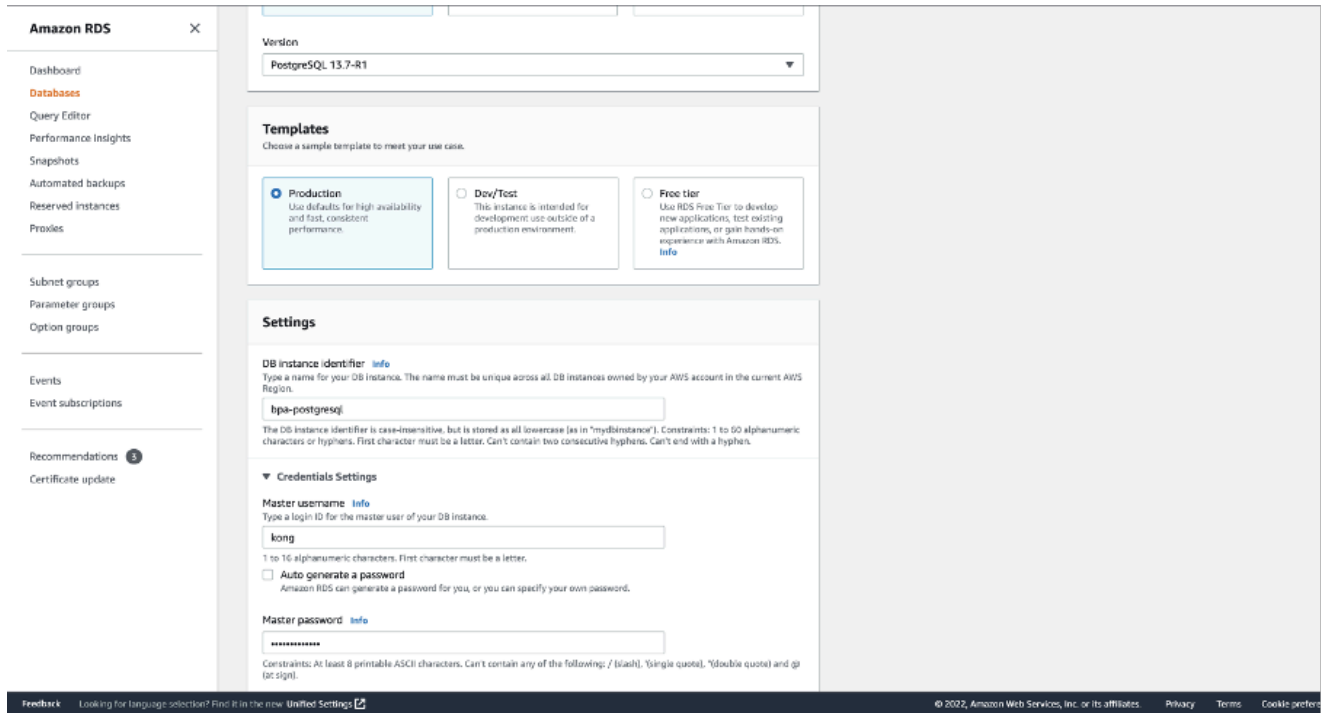
Master password [Info](#)

Password strength Neutral

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

Confirm master password [Info](#)

Geben Sie der Datenbankinstanz einen Namen und erstellen Sie einen Benutzernamen und ein Kennwort.



Stellen Sie sicher, dass die Standardeinstellungen für "DB Instance Size" (Datenbankinstanzgröße) und "Storage" (Speicher) ausgewählt sind.

Wählen Sie abhängig von der Clustergröße und den Datenanforderungen die entsprechende Datenbankinstanzgröße und den entsprechenden Speichertyp aus.

Je nach Anwendungsfall haben wir folgende Konfiguration ausgewählt:

- **Größe der DB-Instanz:** db.m5d.2xlarge
 - 8 vCPUs
 - 32 GiB RAM
 - Netzwerk: 4.750 Mbit/s
 - 300-GB-Instanzspeicher

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

Wählen Sie die entsprechenden Werte entsprechend Ihrem Anwendungsfall aus. Wir haben die Standardwerte ausgewählt.

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

Vergewissern Sie sich, dass Sie unter "Datenbankauthentifizierung" die Kennwortauthentifizierung ausgewählt haben. Authentifizierung mithilfe von Datenbankkennwörtern

**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:

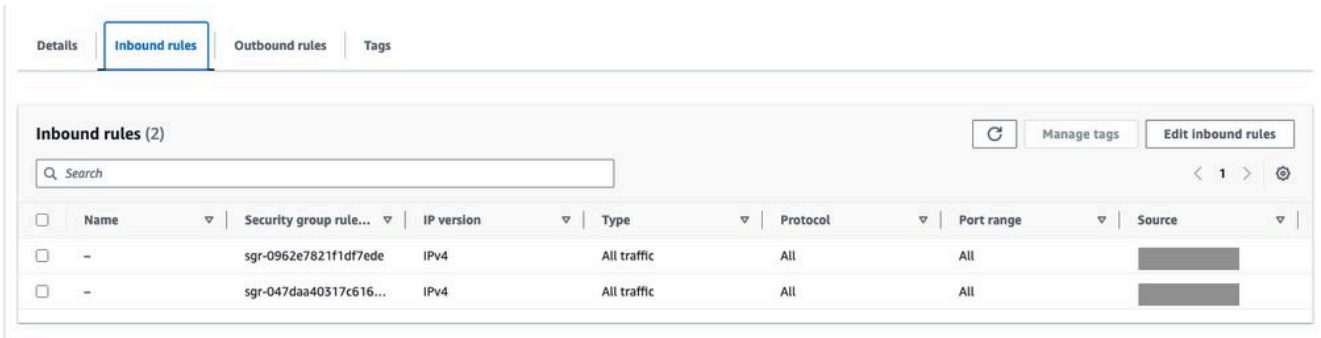
- Enable encryption:** A checked checkbox. Below it, text explains that master key IDs and aliases appear in the list after creation using the AWS Key Management Service (KMS) console. An 'Info' link is provided.
- AWS KMS key:** A dropdown menu currently showing '(default) aws/rds'.
- Account:** The account ID '193670463418' is displayed.
- KMS key ID:** The key ID '61e6c956-745e-42be-8fd1-77953104ad4f' is displayed.
- Log exports:** A section titled 'Log exports' 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 titled 'IAM role' with the instruction 'The following service-linked role is used for publishing logs to CloudWatch Logs.' A grey box below shows 'RDS service-linked role'.
- Maintenance:** A section titled 'Maintenance' with the instruction 'Auto minor version upgrade Info'. A checked checkbox 'Enable auto minor version upgrade' is present. Below it, text explains that enabling this will automatically upgrade to new minor versions as they are released during the maintenance window.
- Maintenance window:** A section titled 'Maintenance window Info' with the instruction 'Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.' Two radio buttons are present: 'Choose a window' (unchecked) and 'No preference' (checked).
- Deletion protection:** A section titled 'Deletion protection' with a checked checkbox 'Enable deletion protection'. Below it, text explains that this protects the database from being deleted accidentally.

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.' To the right of this box are two buttons: 'Cancel' and 'Create database' (which is highlighted in orange).

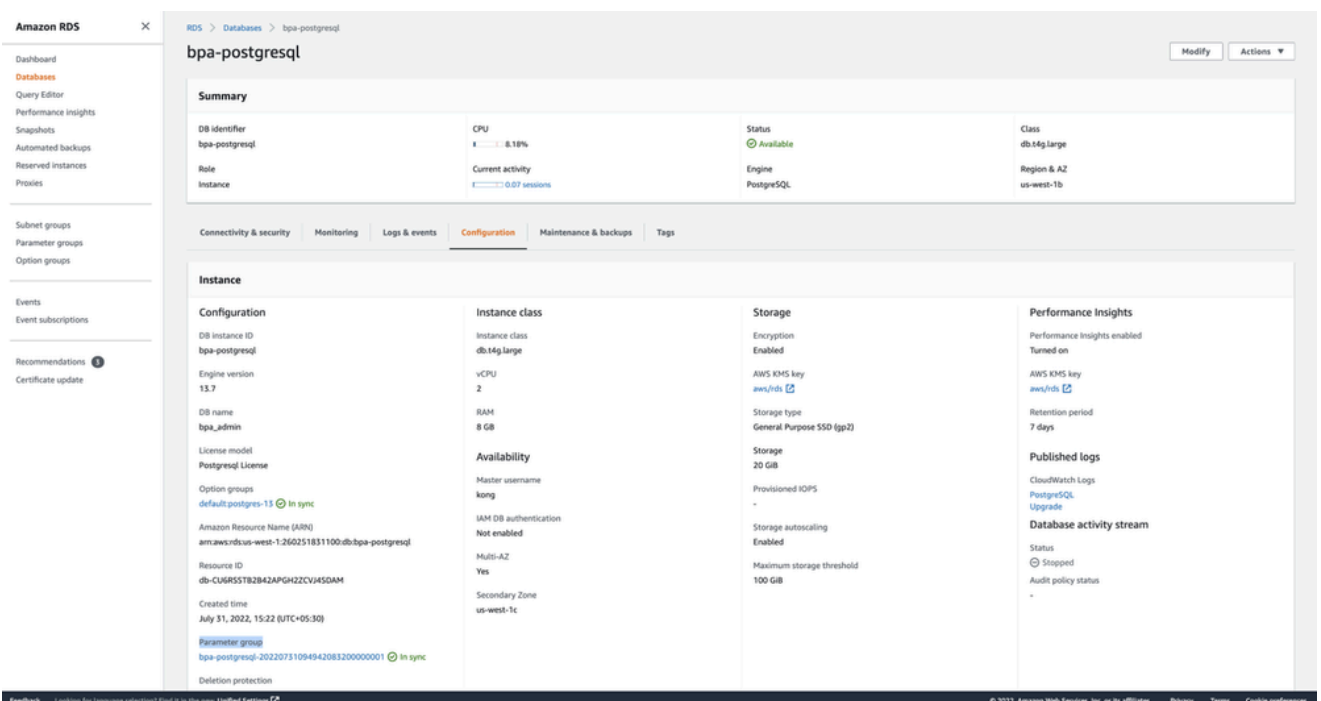
Sobald dies überprüft ist, können Sie die Datenbank erstellen. Zurück zum Amazon RDS Dashboard. Bestätigen Sie, dass die Instanz für die Verwendung verfügbar ist.

Sicherheitsgruppenregeln

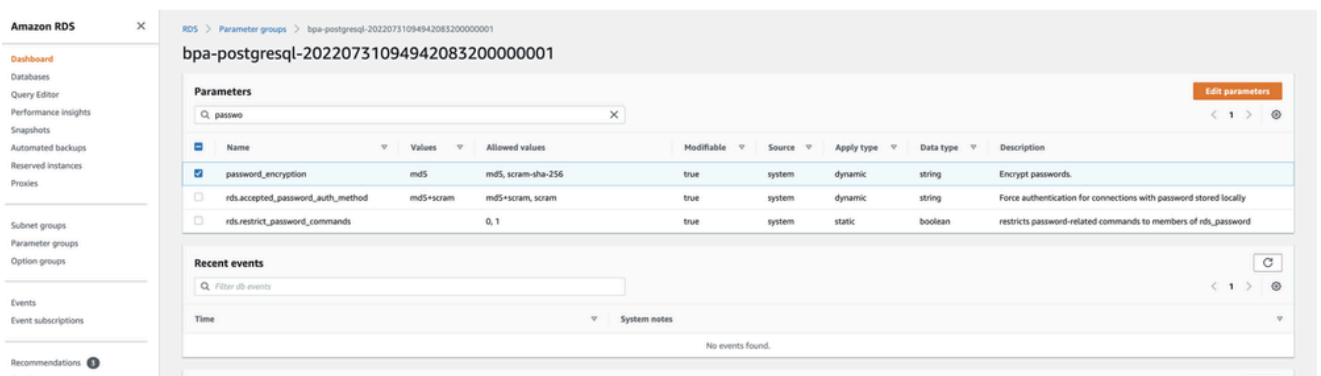
Aktualisieren Sie die eingehende Sicherheitsgruppe mit dem POD-CIDR- und dem Knoten-CIDR-Block.



Klicken Sie in RDS -> Databases -> DB-NAME auf configuration, lesen Sie den Abschnitt Parameter Group (Parametergruppe), und klicken Sie auf die anzuzeigende Parametergruppe.



Suchen Sie nach "password_encryption", und ändern Sie den Wert in md5 von leer / anderen Wert. Dies ist erforderlich, damit die Camunda-Konfigurationen funktionieren.



Erstellen Sie diese Datenbanken zusammen mit den Benutzern, indem Sie eine Verbindung mit

dem RDS herstellen.

```
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=W0rkFlo#ChangeNow  
WFE_DB_NAME=process-engine
```

- Kennwortauthentifizierung

Authentifizierung mithilfe von Datenbankkennwörtern.

- **Atlas MongoDB-Einrichtung**


Die Einrichtung von Atlas MongoDB umfasst:


- **Anmeldung bei Atlas MongoDB.**
- **Auswählen der Organisation und des Projekts.**
- **Erstellen eines dedizierten Clusters mit den entsprechenden Spezifikationen.**





- **Wählen Sie die dedizierte Ebene, den Cloud-Anbieter und die Region aus.**

Cloud Provider & Region AWS, N. Virginia (us-east-1) ^














Multi-Cloud, Multi-Region & Workload Isolation (M10+ clusters)

Distribute data across clouds    or regions for improved availability and local read performance, or introduce read-only and analytics nodes. [Learn more](#)


★ Recommended region ⓘ 🗨 Carbon data currently unavailable ⓘ


NORTH AMERICA


N. Virginia (us-east-1) ★


Ohio (us-east-2) ★

EUROPE


Stockholm (eu-north-1) ★


Ireland (eu-west-1) ★

AUSTRALIA


Sydney (ap-southeast-2) ★


Melbourne (ap-southeast-4) ★

- Wählen Sie den entsprechenden dedizierten Cluster-Tier (wir haben M30 als Tier verwendet) aus, geben Sie den entsprechenden Clusternamen an, und klicken Sie auf "Cluster erstellen". Es wird den Atlas-Monogodb-Cluster initialisieren.

● BPA-DEV-EKS

Connect
View Monitoring
Browse Collections
...

DEDICATED

Connect To Your Database


Interact with your data using the MongoDB drivers or [shell](#).

Dismiss
Connect

R 1.8


W 0.2

Last 6 hours



Connections 50.0


Last 6 hours



In 4.1 KB/s


Out 22.3 KB/s

Last 6 hours



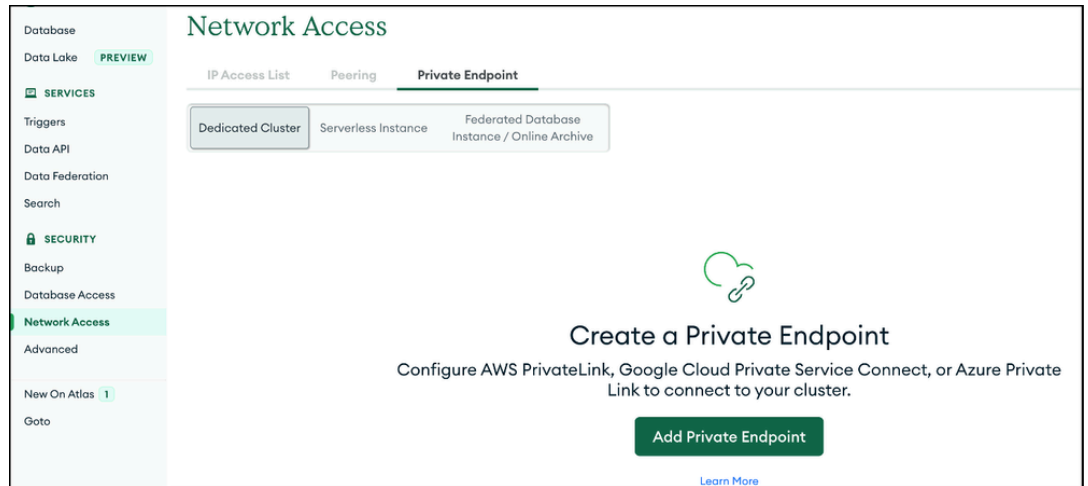
Disk Usage 5.5 GB

Last 18 days

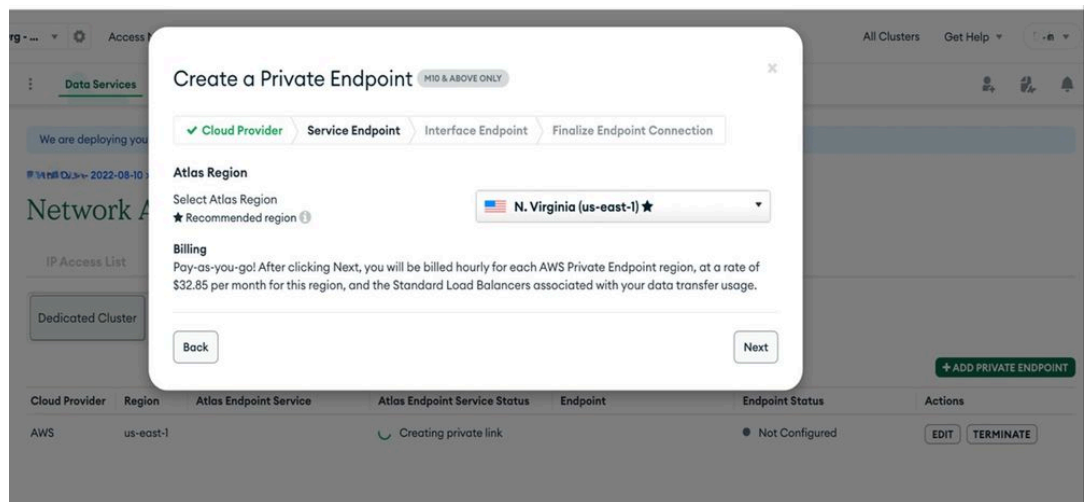


VERSION	REGION	CLUSTER TIER	TYPE	BACKUPS	LINKED APP SERVICES	ATLAS SQL	ONLINE ARCHIVE	ATLAS SEARCH
6.0.6	AWS / N. Virginia (us-east-1)	M30 (General)	Replica Set - 3 nodes	Active	None Linked	Connect	None	Create Index

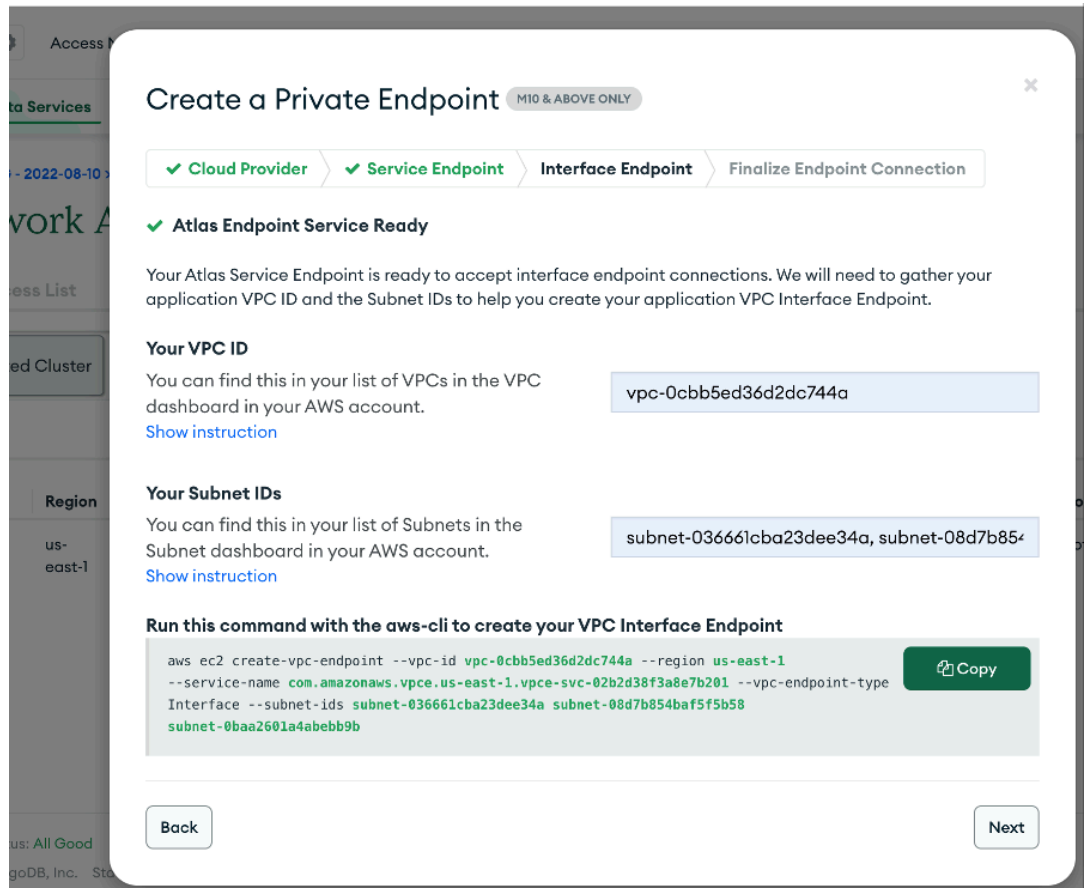
- Einrichten des privaten VPC-Endpunkts für das Atlas- und das K8S-Cluster.
 - Klicken Sie auf Network Access Select Private Endpoint, und klicken Sie dann auf Add Private Endpoint.



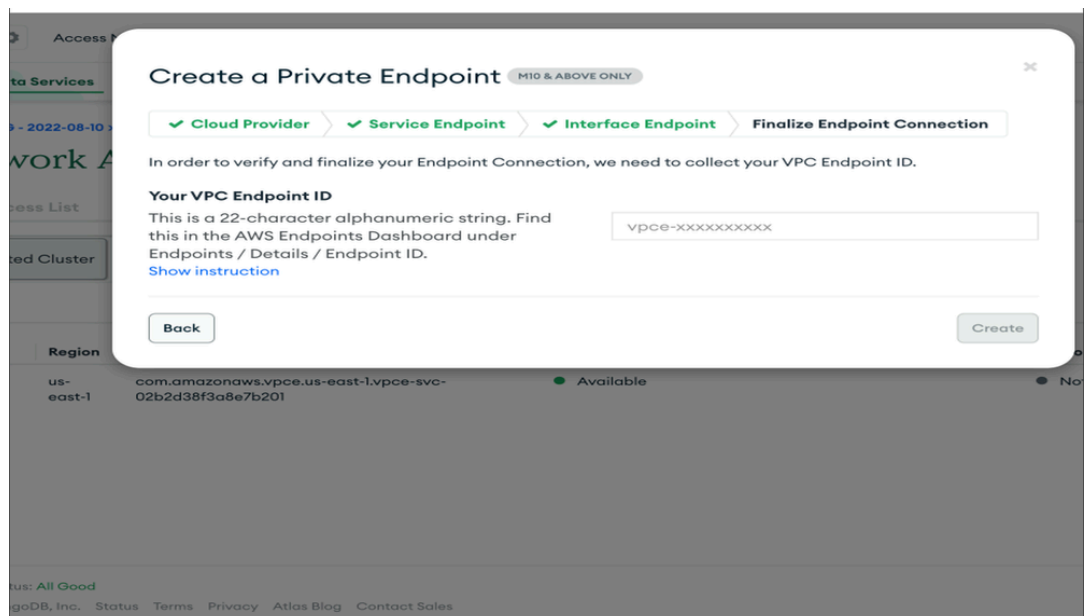
- **Wählen Sie Cloud Provider als AWS aus, wählen Sie die entsprechende Region aus, und klicken Sie auf Weiter.**



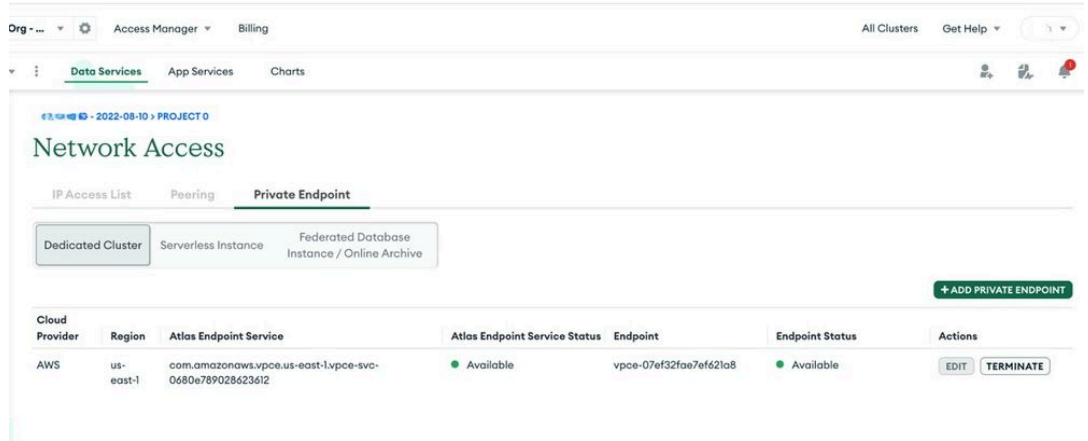
- **Geben Sie die entsprechenden PVC-IDs und Subnetz-IDs an. Wenn Sie die Details eingegeben haben, kopieren Sie den Befehl `vpc end point create`, und führen Sie ihn in der aws-Konsole aus. Sie erhalten die vPC-Endpoint-ID als Ausgabe.**



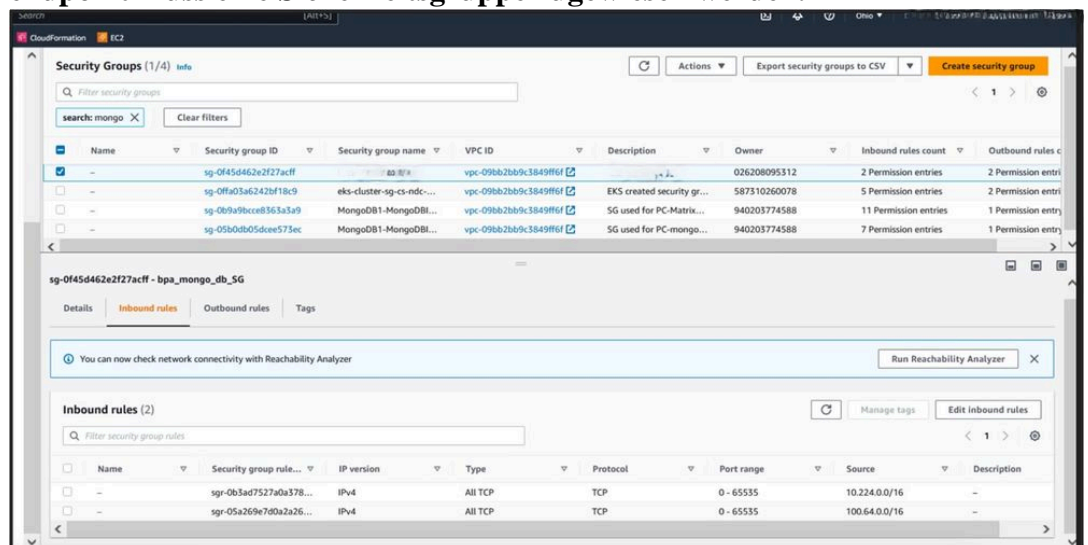
- **Klicken Sie auf Weiter, um die VPC-Endpoint-ID einzufügen, und klicken Sie auf Erstellen.**



- **Nach der erfolgreichen Erstellung ist der Endpunktstatus "Verfügbar" (Available), wie im nächsten Bild gezeigt. Für den POD-CIDR muss ein VPC-Endpoint erstellt werden. In unserem Fall haben wir "100.64.0.0/16" benutzt.**



- **Fügen Sie dem neu erstellten vpc-endpoint eingehende Regeln hinzu. Der vpc-endpoint befindet sich im übergeordneten Konto, und dem neu erstellten vpc-endpoint muss eine Sicherheitsgruppe zugewiesen werden.**



ECR als Image-Registry

Das Erstellen von Amazon ECR-Repositories und das Einschleusen von Docker-Bildern in diese erfordert mehrere Schritte. Dies sind die Schritte, um ein ECR-Repository zu erstellen, ein Docker-Image zu kennzeichnen und es mithilfe der AWS-CLI in das Repository zu verschieben.

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

Ersetzen:

- **Ihren Image-Namen** mit dem gewünschten Namen für Ihr ECR-Repository.
- **Ihre Region** mit Ihrer AWS Region

Konfigurieren der IAM-Rolle für EKS-Knoten

Stellen Sie sicher, dass den EKS-Workerknoten (EC2-Instanzen) die erforderliche IAM-Rolle mit Berechtigungen zum Abrufen von Bildern aus ECR zugeordnet ist. Die erforderliche IAM-Richtlinie lautet:

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

Hängen Sie diese Richtlinie an die IAM-Rolle an, die Ihren EKS-Workerknoten zugeordnet ist.

BPA-Bereitstellung

Die Bereitstellung von BPA umfasst mehrere Schritte, darunter die Kennzeichnung von EKS-Workerknoten, die Vorbereitung von Verzeichnissen auf Knoten, das Kopieren von BPA-Paketen und die Bereitstellung von BPA mithilfe von Helm.

Für die Bereitstellung beim Kunden haben wir die folgenden Versionen von Software und Cloud-Services verwendet:

- **BPA:** 4.0.3-6
- **RDS (Relational Database Service):** 16.3-R2
- **MongoDB Atlas:** v5.0.29
- **EKS (Elastic Kubernetes Service):** v1.27

Diese Komponenten stellen sicher, dass unsere Bereitstellung robust, skalierbar und in der Lage ist, die erforderlichen Workloads effizient zu verarbeiten.

- **Beschriften von EKS-Workerknoten**

```
kubectl label node
```

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

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

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

```
name=node-4
```

- **Vorbereiten von Verzeichnissen auf Knoten**

Knoten 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
```

Knoten 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
```

Knoten 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
```

Knoten 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
```

- Kopieren von BPA-Paketen

```
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/
```

- Bereitstellen von BPA mithilfe von Helm

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

Eingangs-Setup

- **Aktivieren des Eingangs**

Aktualisieren Sie `values.yaml`, um den Eingang zu aktivieren:

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

- **Erstellen eines Schlüssels mit einem BPA-Zertifikat**

Navigieren Sie zum Zertifikatverzeichnis, und erstellen Sie einen Schlüssel:

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

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

- **Eingangscontroller wird aktualisiert**

Fügen Sie den neu erstellten geheimen Schlüssel im `ingress-controller.yaml` Datei:

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

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

- **Eingangszertifikat wird aktualisiert**

Helm löschen und installieren, um das Eingangszertifikat zu aktualisieren.

Umgebungsbedingungen

Die Umgebungsspezifikationen umfassen Anforderungen für EC2-Instanzen, Load Balancer, VPC-Endpunkte und RDS-Instanzen. Die wichtigsten technischen Daten sind:

EC2-Anforderungen:

Speicheranforderungen: 2 TB Speicherplatz pro Knoten. Mounten Sie das EBS-Volume nach `/opt`, und fügen Sie einen Eintrag in `/etc/fstab` für alle Knoten hinzu.

Eingehende Sicherheitsgruppe: 30101, 443, 0 - 65535 TCP, 22 für SSH

Ausgehende Sicherheitsgruppe: Der gesamte Datenverkehr muss aktiviert sein.

DNS Resolver: EC2 muss über standortbasierte Resolver in `/etc/resolve.conf` verfügen.

Anforderungen an den Load Balancer:

- Listeners-Ports müssen 443, 30101 sein.
- VPC-Endgeräteanforderungen (Atlas MongoDB).
- VPC-Endpunkte, die für Atlas-Verbindungen erstellt wurden, sind im übergeordneten Konto verfügbar (aws-5g-ndc-prod). Der VPC-Endpunkt muss über eine Sicherheitsgruppe verfügen, die den gesamten eingehenden Zugriff zulässt (0 - 65535).

RDS-Anforderungen:

RDS-Typ: db.r5b.2xlarge

Postgres-Engine-Version: 13.7

Sicherheitsgruppe: Der eingehende Verkehr muss den Datenverkehr von der POD-CIDR-Quelle zulassen.

Wichtige Konzepte und Komponenten

Ein Verständnis der Grundlagen von Kubernetes ist für die effektive Bereitstellung und Verwaltung von Anwendungen mithilfe von Amazon EKS unerlässlich.

Schlussfolgerung

Dieses Whitepaper bietet einen detaillierten Leitfaden für die Bereitstellung und Verwaltung von Business Process Automation (BPA)-Anwendungen mit Amazon EKS. Wenn Sie die beschriebenen Schritte durchführen und die wichtigsten Konzepte verstehen, können Organisationen die Vorteile von EKS für ihre containerisierten BPA-Anwendungen nutzen.

Referenzen

- Amazon Web Services, "Amazon EKS Documentation", [Online]
Verfügbar:<https://docs.aws.amazon.com/eks/>
- Kubernetes, "Kubernetes Documentation", [Online].
Verfügbar:<https://kubernetes.io/docs/home/>
- Cisco BPA auf einen Blick <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/at-a-glance-c45-742579.html>
- BPA-Betriebshandbuch <https://www.cisco.com/c/dam/en/us/support/docs/bpa/v403/cisco-bpa-operations-guide-v403.pdf>
- BPA-Entwicklerhandbuch <https://www.cisco.com/c/dam/en/us/support/docs/bpa/v403/cisco-bpa-developer-guide-v403.pdf>

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.