

Déployer et gérer des applications d'automatisation des processus d'entreprise sur Amazon EKS : un guide pratique

Table des matières

Résumé

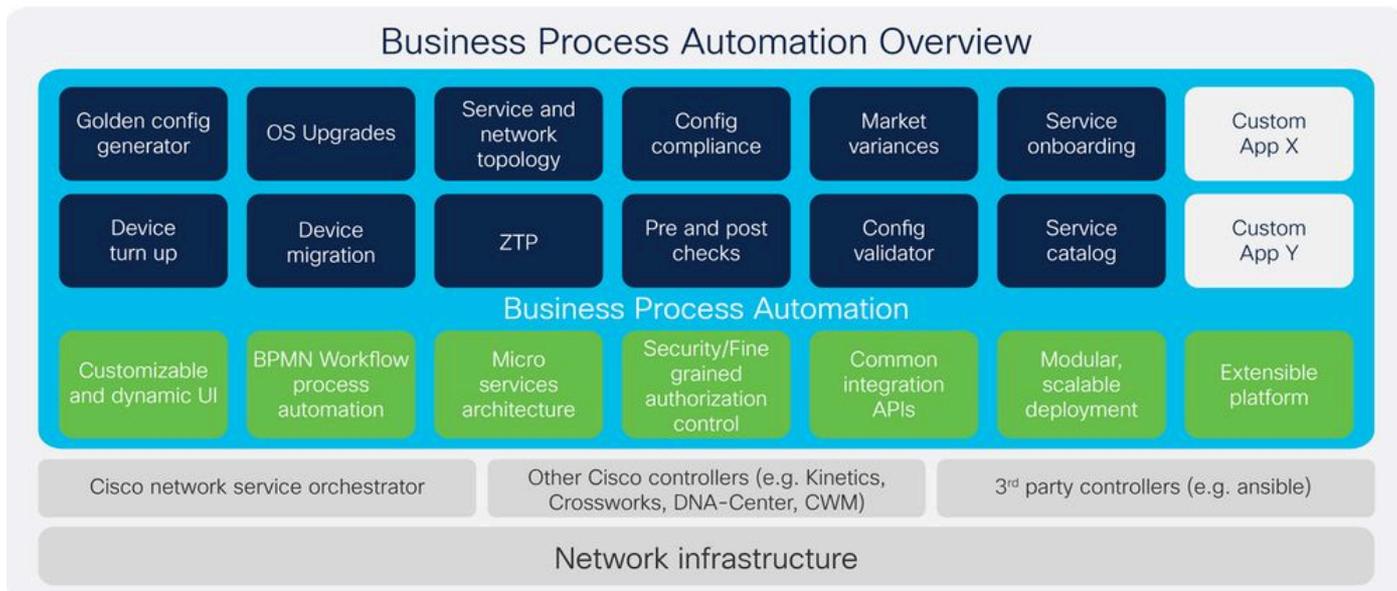
Ce document présente un guide complet sur le déploiement et la gestion des applications Business Process Automation (BPA) à l'aide d'Amazon Elastic Kubernetes Service (EKS). Il décrit les conditions préalables, souligne les avantages de l'utilisation d'EKS et fournit des instructions détaillées pour la mise en place d'un cluster EKS, d'une base de données Amazon RDS et de l'Atlas MongoDB. En outre, le document se penche sur l'architecture de déploiement et spécifie les exigences de l'environnement, offrant une ressource complète pour les organisations visant à tirer parti d'EKS pour leurs applications BPA conteneurisées.

Mots clés

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

Introduction

BPA



Dans l'ère numérique actuelle, les entreprises cherchent à rationaliser et à automatiser des processus métier complexes dans divers environnements informatiques. L'automatisation des processus d'entreprise (BPA) est devenue une technologie essentielle qui permet aux entreprises d'améliorer l'efficacité opérationnelle, de réduire les erreurs et d'améliorer la prestation de services. BPA introduit plusieurs innovations et améliorations clés visant à faire progresser l'automatisation du workflow, le provisionnement de services et les applications d'automatisation prêtes à l'emploi.

La plate-forme BPA héberge des applications et des cas d'utilisation professionnels et informatiques/opérationnels, tels que les mises à niveau du système d'exploitation, le provisionnement de services et l'intégration aux moteurs d'orchestration. Les clients ont accès à un cycle de vie de services et de fonctionnalités BPA, notamment des services de conseil, de mise en oeuvre, de services critiques et d'assistance pour les solutions, fournis par des experts Cisco, des meilleures pratiques, des techniques et des méthodologies éprouvées qui aident à automatiser leurs processus métier et à éliminer les risques liés à leurs systèmes.

Ces fonctionnalités de cycle de vie peuvent être basées sur un abonnement ou personnalisées en fonction des besoins individuels. Les services de mise en oeuvre aident à définir, intégrer et déployer des outils et des processus pour accélérer l'automatisation. Les experts Cisco organisent un processus formel de collecte des exigences, conçoivent et développent des témoignages d'utilisateurs basés sur des processus agiles et des outils CI/CD (Continuous Integration and Continuous Delivery), et mettent en oeuvre des services flexibles avec des tests automatisés de flux de travail, de périphériques et de services nouveaux ou existants. Grâce à l'assistance pour les solutions, les clients bénéficient d'une assistance centralisée 24 heures sur 24, 7 jours sur 7, axée sur les problèmes logiciels, associée à une assistance multifournisseur et open source proposée par le modèle logiciel hiérarchisé de Cisco. Les experts de l'assistance pour les solutions Cisco vous aident à gérer votre dossier, du premier appel à la résolution finale, et à agir en tant que point de contact principal en travaillant avec plusieurs fournisseurs simultanément. Vous pourriez rencontrer jusqu'à 44 % de problèmes en moins en travaillant avec des experts de niveau solution, ce qui vous aiderait à maintenir la continuité de l'activité et à obtenir un retour sur votre investissement BPA plus rapide.

Les fonctionnalités techniques clés, telles que la prise en charge des périphériques gérés par FMC et

Ansible, les exécutions parallèles à l'aide de l'Advanced Queuing Framework (AQF) et la conformité de configuration étendue pour les périphériques NDFC et FMC, positionnent BPA comme une solution complète pour l'automatisation d'entreprise à grande échelle. Avec des fonctionnalités supplémentaires de gestion SD-WAN, d'intégration des périphériques et de gouvernance des politiques de pare-feu, la version répond aux aspects critiques de la sécurité et de l'automatisation du réseau, en répondant aux exigences des environnements multifournisseurs à grande échelle.

EKS

Amazon Elastic Kubernetes Service (EKS) est un service Kubernetes entièrement géré fourni par Amazon Web Services (AWS). Lancé en 2018, EKS simplifie le processus de déploiement, de gestion et de mise à l'échelle des applications conteneurisées à l'aide de Kubernetes, une plate-forme d'orchestration de conteneurs open source. EKS simplifie la gestion des clusters Kubernetes, ce qui permet aux développeurs de se concentrer sur la création et l'exécution d'applications sans avoir à gérer l'infrastructure sous-jacente.

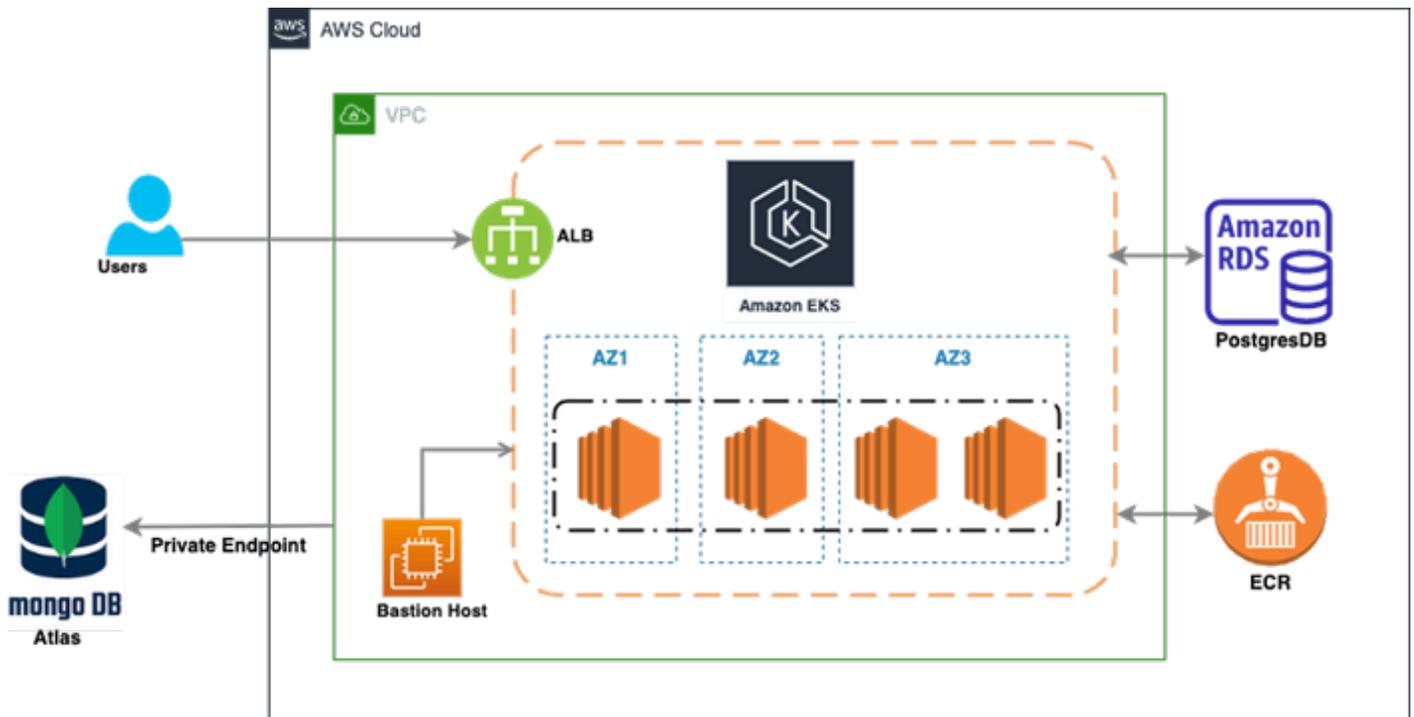
Avantages de l'utilisation d'Amazon EKS pour le déploiement des applications

Amazon EKS offre plusieurs avantages pour le déploiement d'applications, ce qui en fait un choix populaire pour les entreprises qui exploitent des applications et des microservices conteneurisés.

Principaux avantages :

- **Plan de contrôle Kubernetes géré :** EKS gère le déploiement, l'évolutivité et la maintenance du plan de contrôle Kubernetes, réduisant ainsi la charge opérationnelle.
- **Gestion simplifiée des clusters :** EKS simplifie la configuration et la gestion des clusters Kubernetes.
- **Évolutivité :** EKS permet d'adapter facilement les clusters aux charges de travail croissantes.
- **Haute disponibilité :** EKS prend en charge les déploiements de zones de disponibilité multiples, améliorant ainsi la disponibilité et la tolérance aux pannes.
- **Intégration avec les services AWS :** EKS s'intègre en toute transparence à divers services AWS.
- **DevOps Automation :** EKS prend en charge l'intégration et le déploiement continu (CI/CD) pour les applications conteneurisées.

Architecture de déploiement BPA



Cette image représente une architecture de haut niveau d'une infrastructure cloud déployée sur **AWS**, en utilisant plusieurs composants clés. Voici une répartition du schéma :

1. **Amazon EKS (Elastic Kubernetes Service)** : au coeur du schéma, Amazon EKS est déployé sur trois zones de disponibilité (AZ1, AZ2, AZ3), avec des noeuds travailleurs Kubernetes à l'intérieur de chaque zone. Cela indique une configuration à haute disponibilité et à tolérance de panne, car les charges de travail sont réparties sur plusieurs zones de disponibilité.
2. **ALB (Application Load Balancer)** : il est positionné à l'avant, reçoit le trafic des utilisateurs et le distribue à travers le cluster EKS pour gérer les charges de travail des applications. L'équilibreur de charge garantit que les demandes sont distribuées de manière uniforme et peut gérer l'évolutivité en fonction de la demande de trafic.
3. **Amazon RDS (Relational Database Service) - PostgreSQL** : sur le côté droit du schéma, une instance d'Amazon RDS exécutant PostgreSQL est présente. Cette base de données est accessible aux applications exécutées dans le cluster EKS.
4. **ECR (Elastic Container Registry)** : emplacement où les images de conteneur Docker sont stockées et gérées, puis déployées sur Amazon EKS pour exécuter les charges de travail.
5. **MongoDB Atlas** : sur le côté gauche, MongoDB Atlas est intégré à l'architecture via un terminal privé. MongoDB Atlas est un service de base de données NoSQL hébergé dans le cloud, utilisé ici pour gérer les exigences de base de données basées sur des documents. Le terminal privé assure une communication privée et sécurisée entre l'instance Atlas MongoDB et les autres composants AWS.
6. **Hôte Bastion** : positionné dans le VPC (cloud privé virtuel), un hôte Bastion fournit un point d'entrée sécurisé permettant aux administrateurs d'accéder aux ressources à l'intérieur du VPC sans les exposer directement à Internet.

Dans l'ensemble, cette architecture fournit une solution hautement disponible, évolutive et sécurisée pour le déploiement et la gestion d'applications conteneurisées à l'aide d'Amazon EKS, avec la prise en charge des bases de données relationnelles (PostgreSQL) et NoSQL (MongoDB).

- **Configuration du cluster EKS**

Pour créer un cluster Amazon EKS à l'aide de l'interface de ligne de commande AWS, vous pouvez utiliser l'utilitaire de ligne de commande `eksctl`. Voici un exemple de commande :

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

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

- **Configuration de la base de données RDS**

Le déploiement d'une base de données relationnelle sur Amazon RDS comprend les étapes suivantes :

- Accédez à la console de gestion AWS et accédez au service Amazon RDS.
- Créez une nouvelle instance de base de données avec les spécifications souhaitées.
- Configurez le groupe de sécurité pour autoriser les connexions entrantes à partir de votre cluster Amazon EKS.

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](#).

Dans le menu déroulant, sélectionnez la version la plus récente de PostgreSQL. Dans notre cas, il s'agit de « 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.

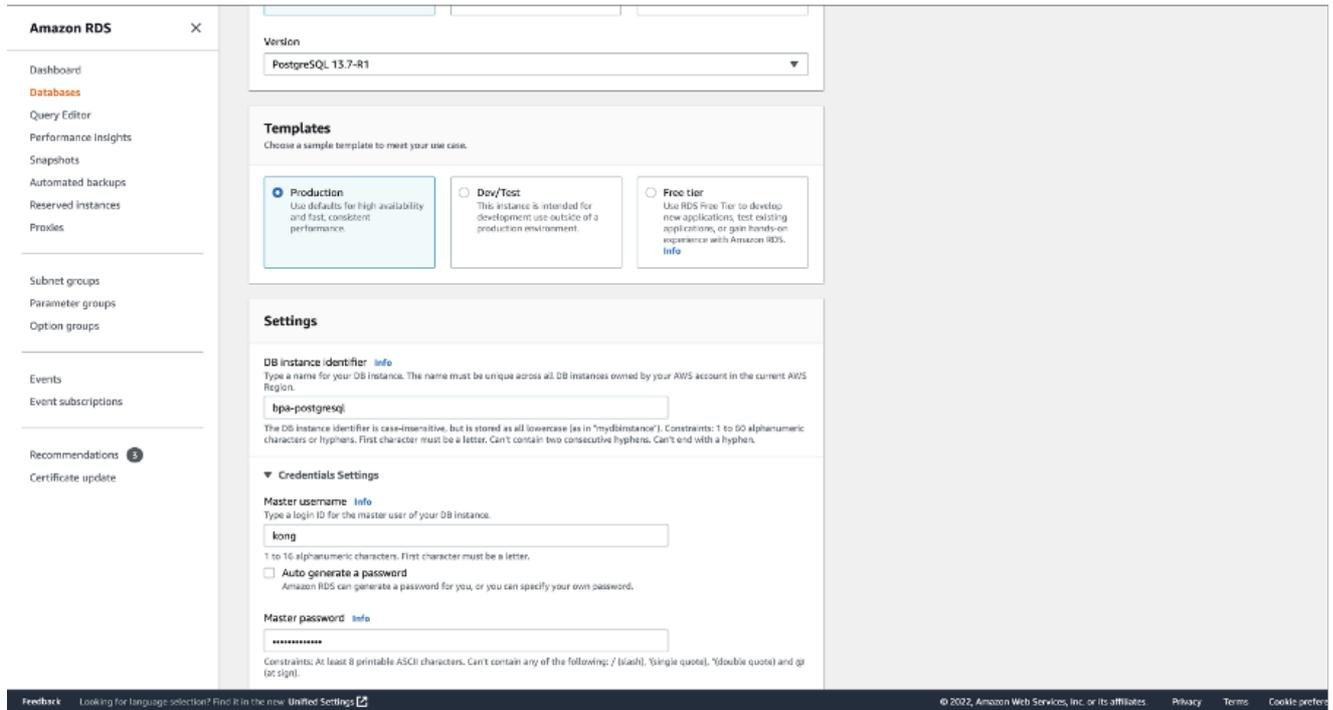
Master password [Info](#)

Password strength Neutral

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

Confirm master password [Info](#)

Pour cela, donnez un nom à l'instance de base de données et créez un nom d'utilisateur et un mot de passe.



Assurez-vous que les paramètres par défaut pour « Taille de l'instance de base de données » et « Stockage » sont sélectionnés.

En fonction de la taille du cluster et des besoins en données, sélectionnez la taille d'instance de base de données et le type de stockage appropriés.

Sur la base de notre exemple d'utilisation, nous avons choisi la configuration suivante :

- **Taille de l'instance de base de données** : db.m5d.2xlarge
 - 8 vCPUs
 - 32 Go de RAM
 - Réseau : 4 750 Mbit/s
 - Magasin d'instances 300 Go

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

Sélectionnez les valeurs appropriées en fonction de votre cas d'utilisation. Nous avons sélectionné les valeurs par défaut.

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

Assurez-vous que l'option Authentification par mot de passe est sélectionnée dans Authentification par base de données. Authentifie à l'aide de mots de passe.

**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 'Select the log types to publish to Amazon CloudWatch Logs' with two unchecked checkboxes: 'PostgreSQL log' and 'Upgrade log'.
- IAM role:** A section titled 'The following service-linked role is used for publishing logs to CloudWatch Logs.' with a highlighted box containing 'RDS service-linked role'.
- Maintenance:** A section titled 'Auto minor version upgrade' with an 'Info' link. Below it, a checked checkbox for 'Enable auto minor version upgrade' is shown, with text explaining that it automatically upgrades to new minor versions during the maintenance window.
- Maintenance window:** A section titled 'Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.' with two radio button options: 'Choose a window' (unselected) and 'No preference' (selected).
- Deletion protection:** A section with a checked checkbox for 'Enable deletion protection', with text explaining it 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.' Below this box are two buttons: 'Cancel' and 'Create database' (highlighted in orange).

Une fois cette vérification effectuée, nous sommes prêts à créer la base de données. Revenir au tableau de bord Amazon RDS. Vérifiez que l'instance est disponible.

Règles du groupe de sécurité

Mettez à jour le groupe de sécurité entrant avec le CIDR pod et le bloc CIDR de noeud.

Details **Inbound rules** Outbound rules Tags

Inbound rules (2) Manage tags Edit inbound rules

Search

<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range	Source
<input type="checkbox"/>	-	sgr-0962e7821f1df7ede	IPv4	All traffic	All	All	
<input type="checkbox"/>	-	sgr-047daa40317c616...	IPv4	All traffic	All	All	

Dans RDS -> Bases de données -> DB-NAME, cliquez sur configuration et reportez-vous à la section Groupe de paramètres, puis cliquez sur le groupe de paramètres à afficher.

Amazon RDS

RDS > Databases > bpa-postgresql

bpa-postgresql Modify Actions

Summary

DB identifier bpa-postgresql	CPU 8.18%	Status Available	Class db.t4g.large
Role Instance	Current activity 0.07 sessions	Engine PostgreSQL	Region & AZ us-west-1b

Connectivity & security | Monitoring | Logs & events | **Configuration** | Maintenance & backups | Tags

Instance

Configuration DB instance ID bpa-postgresql Engine version 13.7 DB name bpa_admin License model PostgreSQL License Option groups default:postgres-13 In sync Amazon Resource Name (ARN) arn:aws:rds-west-1:260251851100:db:bpa-postgresql Resource ID db-CU6R55TB2B4ZAPGH2ZCVJ4SDAM Created time July 31, 2022, 15:22 (UTC+05:30) Parameter group bpa-postgresql-20220731094942083200000001 In sync Deletion protection	Instance class Instance class db.t4g.large vCPU 2 RAM 8 GB Availability Master username kong IAM DB authentication Not enabled Multi-AZ Yes Secondary Zone us-west-1c	Storage Encryption Enabled AWS KMS key aws/rds Storage type General Purpose SSD (gp2) Storage 20 GiB Provisioned IOPS - Storage autoscaling Enabled Maximum storage threshold 100 GiB	Performance Insights Performance Insights enabled Turned on AWS KMS key aws/rds Retention period 7 days Published logs CloudWatch Logs PostgreSQL Upgrade Database activity stream Status Stopped Audit policy status -
---	--	--	--

Recherchez « password_encryption » et remplacez la valeur par md5 (vide/autre). Ceci est nécessaire pour que les configurations Camunda fonctionnent.

Amazon RDS

RDS > Parameter groups > bpa-postgresql-20220731094942083200000001

bpa-postgresql-20220731094942083200000001 Edit parameters

Parameters

<input type="checkbox"/>	Name	Values	Allowed values	Modifiable	Source	Apply type	Data type	Description
<input checked="" type="checkbox"/>	password_encryption	md5	md5, scram-sha-256	true	system	dynamic	string	Encrypt passwords.
<input type="checkbox"/>	rds.accepted_password_auth_method	md5+scram	md5+scram, scram	true	system	dynamic	string	Force authentication for connections with password stored locally
<input type="checkbox"/>	rds.restrict_password_commands	0, 1		true	system	static	boolean	restricts password-related commands to members of rds_password

Recent events

Filter db events

Time	System notes
No events found.	

Créez ces bases de données avec les utilisateurs en vous connectant à 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
```

- Authentification par mot de passe

Authentifie à l'aide de mots de passe.

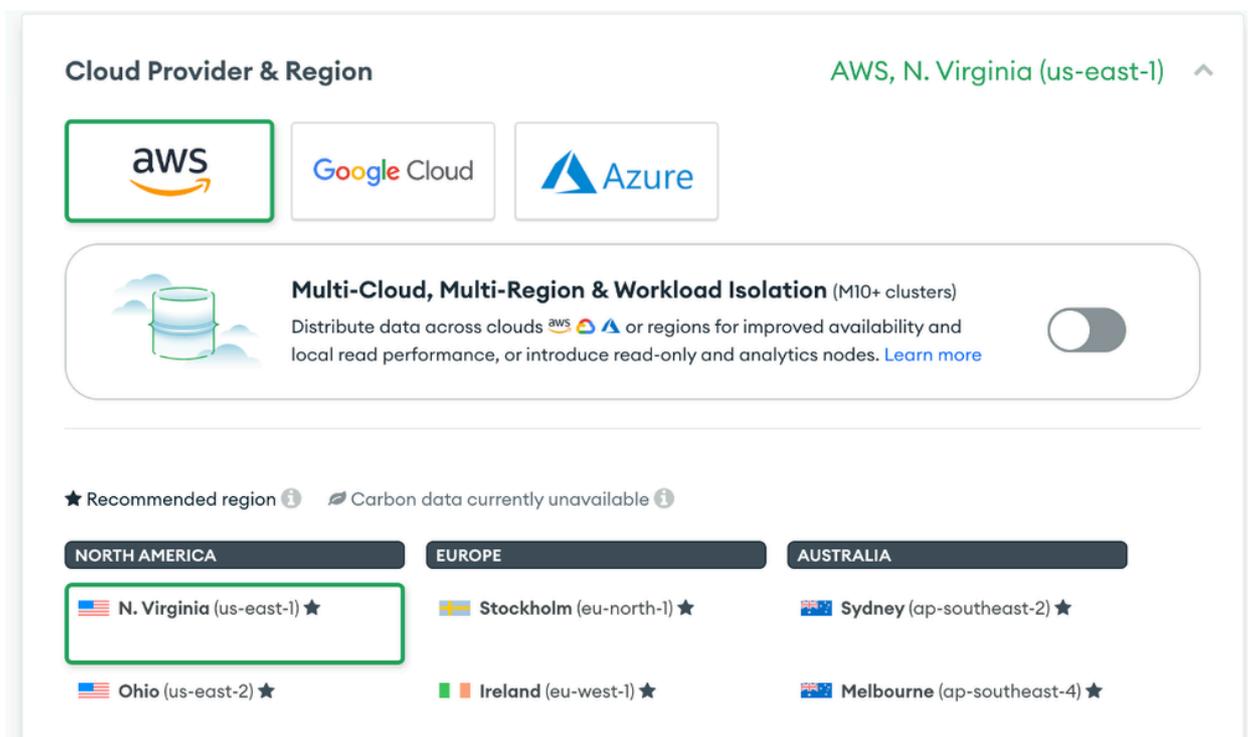
- **Configuration d'Atlas MongoDB**

La configuration d'Atlas MongoDB comprend :

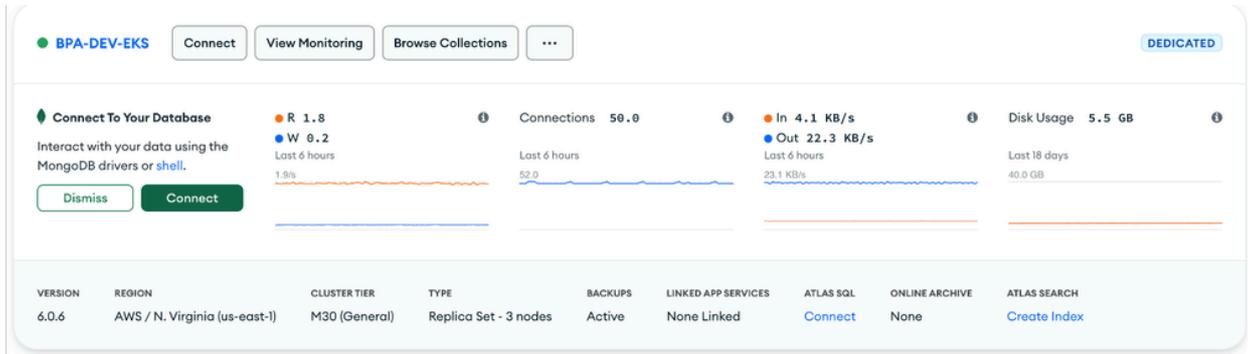
- **Connexion à Atlas MongoDB.**
- **Sélectionner l'organisation et le projet.**
- **Créer un cluster dédié avec les spécifications appropriées.**



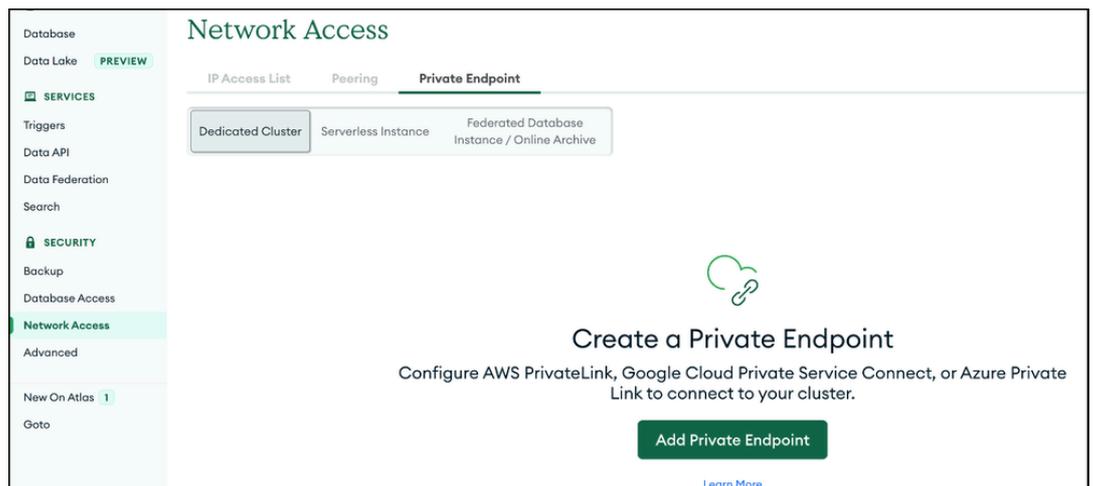
- **Sélectionnez le niveau dédié, le fournisseur de cloud et la région.**



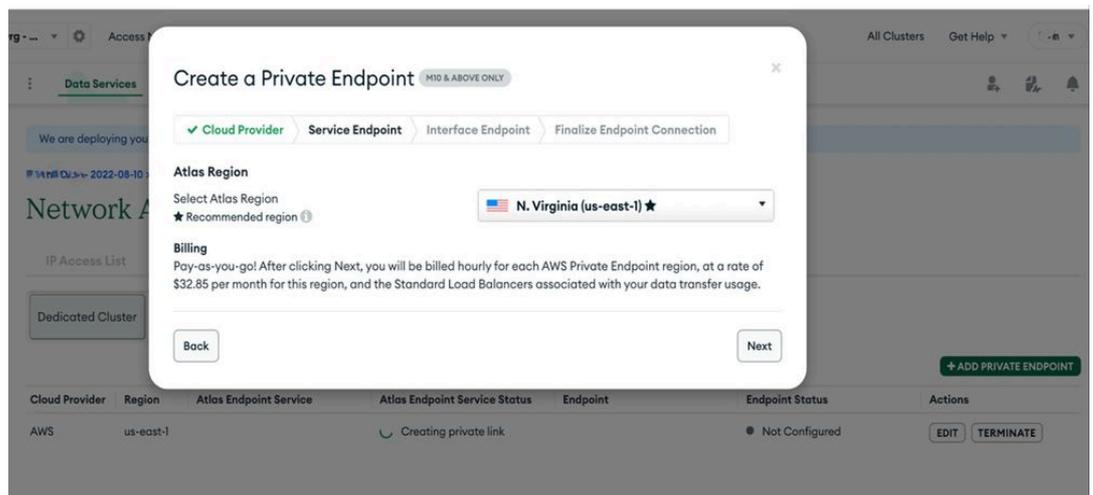
- **Sélectionnez le niveau approprié (nous avons utilisé M30 comme niveau) pour le cluster dédié, indiquez le nom de cluster approprié et cliquez sur Create Cluster (Créer un cluster). Il initialisera la grappe monogodb de l'Atlas.**



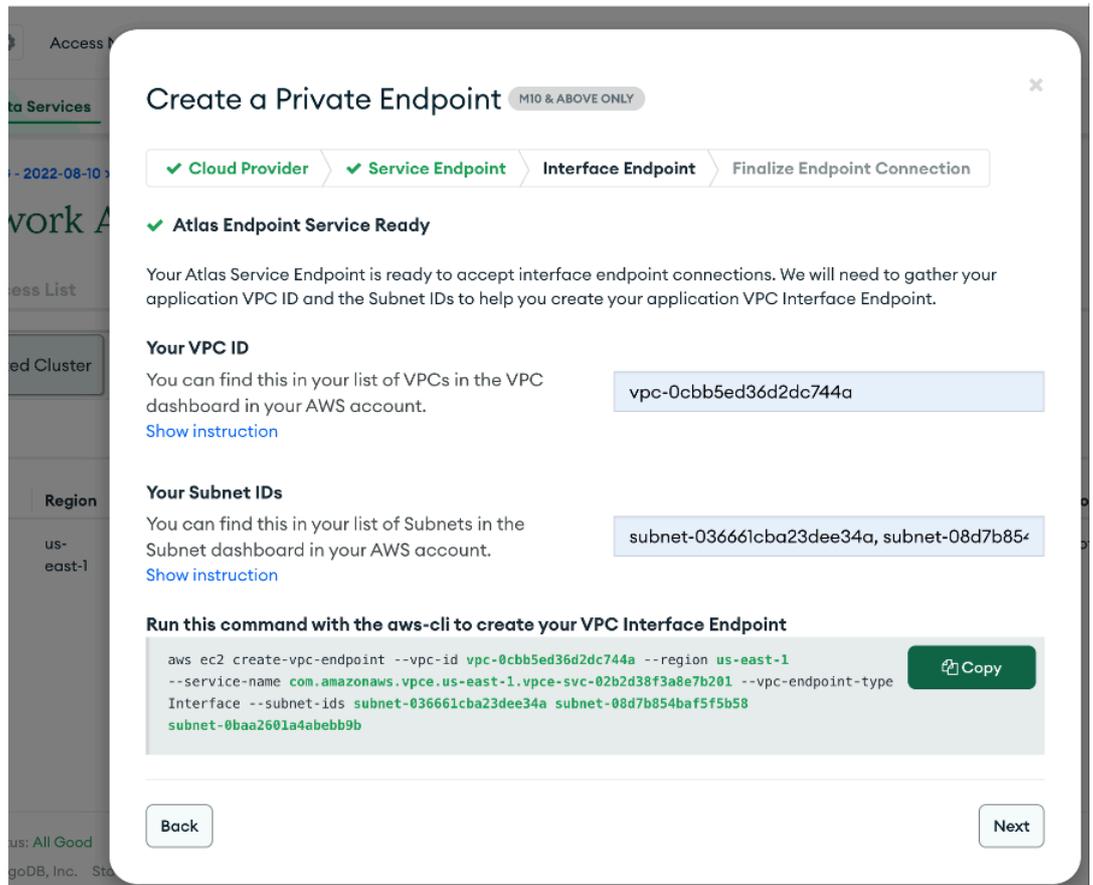
- **Configuration d'un terminal privé VPC pour le cluster Atlas et K8S.**
 - **Cliquez sur le bouton Network Access Select Private Endpoint à cliquer sur Add Private Endpoint.**



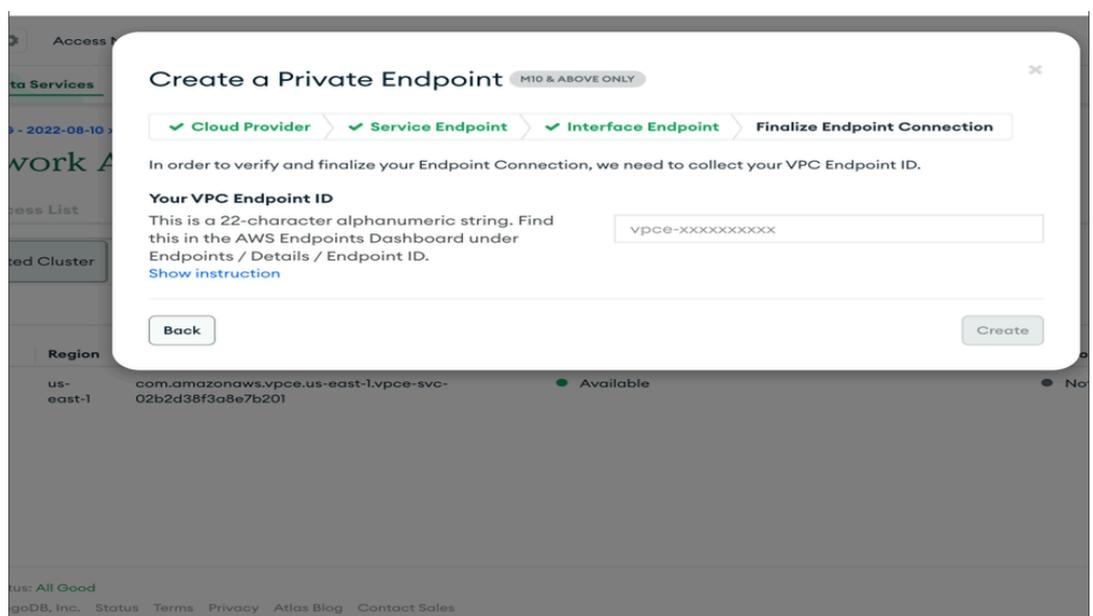
- **Sélectionnez Cloud Provider comme AWS, sélectionnez la région correspondante et cliquez sur Next (Suivant).**



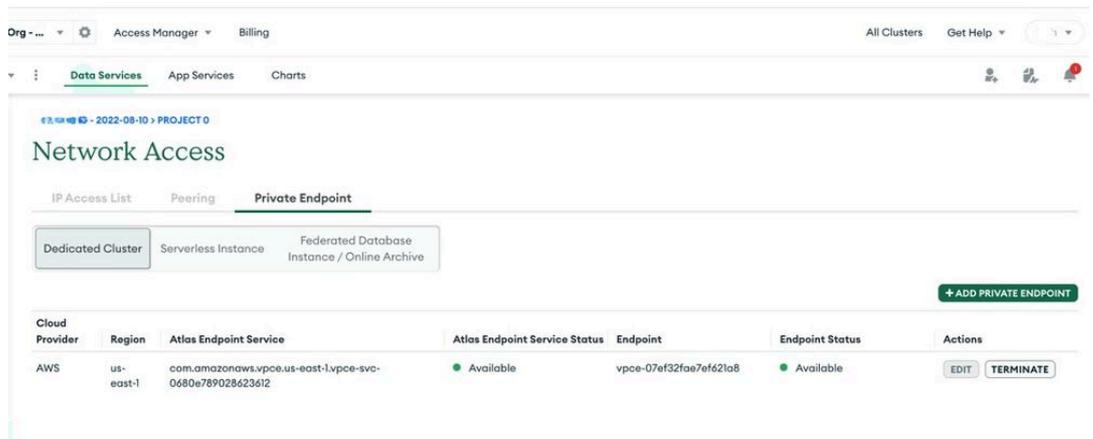
- Fournissez l'ID PVC et les ID de sous-réseau respectifs. Une fois que vous avez entré les détails, copiez la commande vpc end point creation et exécutez-la dans la console Aws. Vous obtiendrez l'ID du point de terminaison vpc comme résultat.



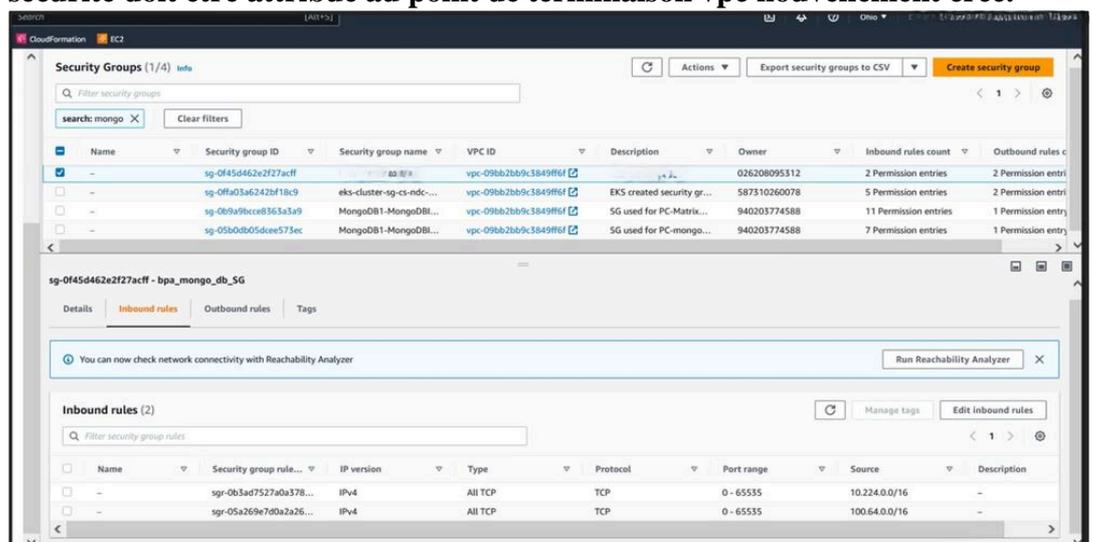
- Cliquez sur Next (Suivant) pour coller l'ID de point de terminaison VPC et cliquez sur Create (Créer).



- Une fois créé, l'état du point de terminaison est Disponible, comme illustré dans l'image suivante. Le point de terminaison VPC doit être créé pour pod cidr. Dans notre cas, nous avons utilisé "100.64.0.0/16" .



- Ajoutez des règles entrantes au point de terminaison vpc nouvellement créé. Le point de terminaison vpc sera dans le compte parent et un groupe de sécurité doit être attribué au point de terminaison vpc nouvellement créé.



ECR comme registre d'images

La création de référentiels Amazon ECR et la diffusion d'images Docker dans ceux-ci implique plusieurs étapes. Voici les étapes à suivre pour créer un référentiel ECR, marquer une image Docker et la transmettre au référentiel à l'aide de l'interface de ligne de commande AWS.

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

Remplacer :

- **your-image-name** avec le nom souhaité pour votre référentiel ECR.
- **votre région** avec votre région AWS

Configurer le rôle IAM pour les noeuds EKS

Assurez-vous que les noeuds de travail EKS (instances EC2) disposent du rôle IAM nécessaire associé avec les autorisations d'extraction d'images à partir d'ECR. La stratégie IAM requise est la suivante :

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

Associez cette stratégie au rôle IAM associé à vos noeuds de travail EKS.

Déploiement BPA

Le déploiement de BPA comprend plusieurs étapes, notamment l'étiquetage des noeuds de travail EKS, la préparation des répertoires sur les noeuds, la copie des packages BPA et le déploiement de BPA à l'aide de Helm.

Pour le déploiement de nos clients, nous avons utilisé les versions suivantes de logiciels et de services cloud :

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

Ces composants garantissent que notre déploiement est robuste, évolutif et capable de gérer efficacement les charges de travail requises.

- **Étiquetage des noeuds travailleurs EKS**

```
kubectl label node
```

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

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

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

```
name=node-4
```

- **Préparation des répertoires sur les noeuds**

Noeud 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
```

Noeud 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
```

Noeud 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
```

Noeud 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
```

- Copie des packages BPA

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

- Déploiement de BPA via Helm

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

Configuration en entrée

- **Activation des entrées**

Mettez à jour `values.yaml` pour activer ingress :

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

- **Créer un secret à l'aide du certificat BPA**

Accédez au répertoire du certificat et créez un secret :

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

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

- **Mise à jour du contrôleur entrant**

Ajoutez le nouveau secret créé dans le `ingress-controller.yaml` fichier:

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

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

- **Mise à jour du certificat entrant**

Effectuez la suppression et l'installation Helm pour mettre à jour le certificat d'entrée.

Caractéristiques environnementales

Les spécifications d'environnement incluent les exigences relatives aux instances EC2, aux équilibreurs de charge, aux points d'extrémité VPC et aux instances RDS. Les principales spécifications sont les suivantes :

EC2 Exigences :

Besoins en stockage : 2 To d'espace par noeud. Montez le volume EBS sur /opt et ajoutez une entrée dans /etc/fstab pour tous les noeuds.

Groupe de sécurité entrant : 30101, 443, 0 - 65535 TCP, 22 pour ssh.

Groupe de sécurité sortant : tout le trafic doit être activé.

Résolveur DNS : EC2 doit disposer de résolveurs sur site dans /etc/resolve.conf.

Exigences d'équilibrage de charge :

- Les ports des écouteurs doivent être 443, 30101.
- Exigences relatives aux terminaux VPC (Atlas MongoDB).
- Les terminaux VPC créés pour la connectivité Atlas sont disponibles dans le compte parent (aws-5g-ndc-prod). Le point de terminaison VPC doit avoir un groupe de sécurité qui autorise tous les accès entrants (0 - 65535).

Exigences RDS :

Type RDS : db.r5b.2xlarge

Version du moteur Postgres : 13.7

Groupe de sécurité : le trafic entrant doit autoriser le trafic en provenance de la source CIDR POD.

Concepts et composants clés

Il est essentiel de comprendre les principes fondamentaux de Kubernetes pour déployer et gérer efficacement les applications à l'aide d'Amazon EKS.

Conclusion

Ce document fournit un guide détaillé pour le déploiement et la gestion des applications Business Process Automation (BPA) à l'aide d'Amazon EKS. En suivant les étapes décrites et en comprenant les concepts clés, les entreprises peuvent tirer parti des avantages d'EKS pour leurs applications BPA conteneurisées.

Références

- Amazon Web Services, « Amazon EKS Documentation », [en ligne]. Disponible : <https://docs.aws.amazon.com/eks/>
- Kubernetes, « Documentation Kubernetes », [En ligne]. Disponible : <https://kubernetes.io/docs/home/>
- Cisco BPA en quelques mots <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/at-a-glance-c45-742579.html>
- Guide des opérations BPA <https://www.cisco.com/c/dam/en/us/support/docs/bpa/v403/cisco-bpa-operations-guide-v403.pdf>
- Guide du développeur BPA <https://www.cisco.com/c/dam/en/us/support/docs/bpa/v403/cisco-bpa-developer-guide-v403.pdf>

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.