

# Implementación y gestión de aplicaciones de automatización de procesos empresariales en Amazon EKS: una guía práctica

## Contenido

---

---

### Abstracto

Este documento presenta una guía completa sobre la implementación y la gestión de aplicaciones de automatización de procesos empresariales (BPA) mediante el servicio Amazon Elastic Kubernetes Service (EKS). Describe los requisitos previos, destaca las ventajas de utilizar EKS y proporciona instrucciones paso a paso para configurar un clúster EKS, una base de datos Amazon RDS y un sistema MongoDB Atlas. Además, el documento profundiza en la arquitectura de implementación y especifica los requisitos del entorno, ofreciendo un recurso exhaustivo para las organizaciones que pretenden aprovechar EKS para sus aplicaciones BPA en contenedores.

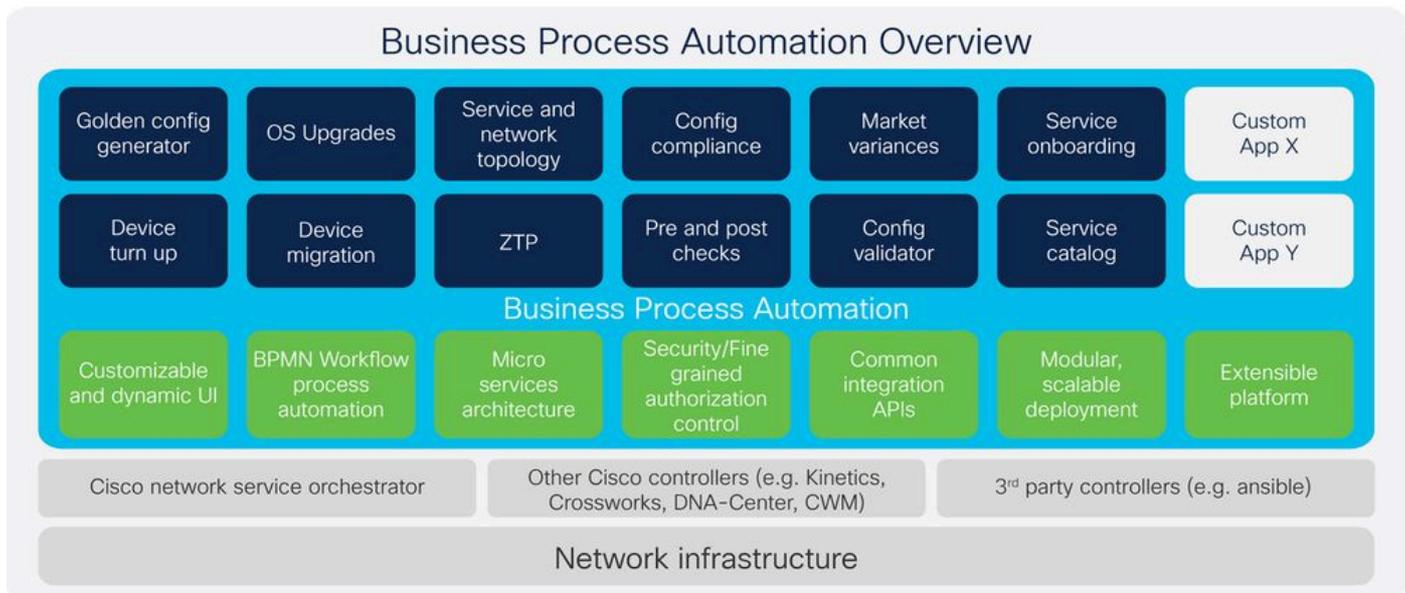
### Palabras clave

Amazon EKS, Kubernetes, AWS, RDS, MongoDB Atlas, DevOps, Cloud Computing, automatización de procesos empresariales.

---

## Introducción

### BPA



En la era digital actual, las empresas buscan agilizar y automatizar los procesos empresariales complejos en una amplia gama de entornos de TI. La automatización de procesos empresariales (BPA) se ha convertido en una tecnología fundamental que permite a las organizaciones mejorar la eficacia operativa, reducir los errores y mejorar la prestación de servicios. BPA presenta varias innovaciones y mejoras clave destinadas a avanzar en la automatización del flujo de trabajo, el aprovisionamiento de servicios y las aplicaciones de automatización estándar.

La plataforma BPA aloja aplicaciones y casos de uso operativos y de TI/empresariales, como actualizaciones de SO, aprovisionamiento de servicios e integración con motores de orquestación. Los clientes tienen acceso a un ciclo de vida de servicios y funciones de BPA que incluyen asesoría, implementación, servicios empresariales críticos y asistencia para soluciones a través de expertos de Cisco, prácticas recomendadas y técnicas y metodologías probadas que ayudan a automatizar sus procesos empresariales y a eliminar el riesgo de sus sistemas.

Estas capacidades del ciclo de vida pueden estar basadas en suscripciones o personalizarse según las necesidades individuales. Los servicios de implementación ayudan a definir, integrar e implementar herramientas y procesos para acelerar la automatización. Los expertos de Cisco llevan a cabo un proceso formal para recopilar requisitos, diseñar y desarrollar historias de usuarios basadas en procesos ágiles y herramientas de integración continua y prestación continua (CICD), e implementa servicios flexibles con pruebas automatizadas de flujos de trabajo, dispositivos y servicios nuevos o existentes. Con la Asistencia para soluciones, los clientes pueden acceder a una asistencia centralizada las 24 horas del día, los 7 días de la semana, que se centra en los problemas centrados en el software, junto con la asistencia de varios proveedores y código abierto que se ofrece a través del modelo de software por niveles de Cisco. Los expertos en asistencia para soluciones de Cisco le ayudan a gestionar su caso desde la primera llamada hasta la resolución final y actúan como el principal punto de contacto al trabajar con varios proveedores simultáneamente. Podrá experimentar hasta un 44% menos de problemas al trabajar con expertos en soluciones, lo que le ayudará a mantener la continuidad empresarial y a obtener un retorno de la inversión en BPA más rápido.

Las características técnicas clave, como la compatibilidad con FMC y dispositivos administrados con

Ansible, las ejecuciones paralelas mediante Advanced Queuing Framework (AQF) y el cumplimiento ampliado de la configuración para los dispositivos NDFC y FMC, posicionan a BPA como una solución completa para la automatización empresarial a gran escala. Con capacidades añadidas en gestión de SD-WAN, incorporación de dispositivos y administración de políticas de firewall, la versión aborda aspectos críticos de la seguridad y la automatización de la red, satisfaciendo las demandas de entornos de varios proveedores a gran escala.

## **EKS**

Amazon Elastic Kubernetes Service (EKS) es un servicio de Kubernetes totalmente administrado proporcionado por Amazon Web Services (AWS). EKS, que se lanzó en 2018, simplifica el proceso de implementación, gestión y ampliación de aplicaciones en contenedores mediante Kubernetes, una plataforma de orquestación de contenedores de código abierto. EKS abstrae las complejidades de la gestión de clústeres de Kubernetes, lo que permite a los desarrolladores centrarse en crear y ejecutar aplicaciones sin necesidad de gestionar la infraestructura subyacente.

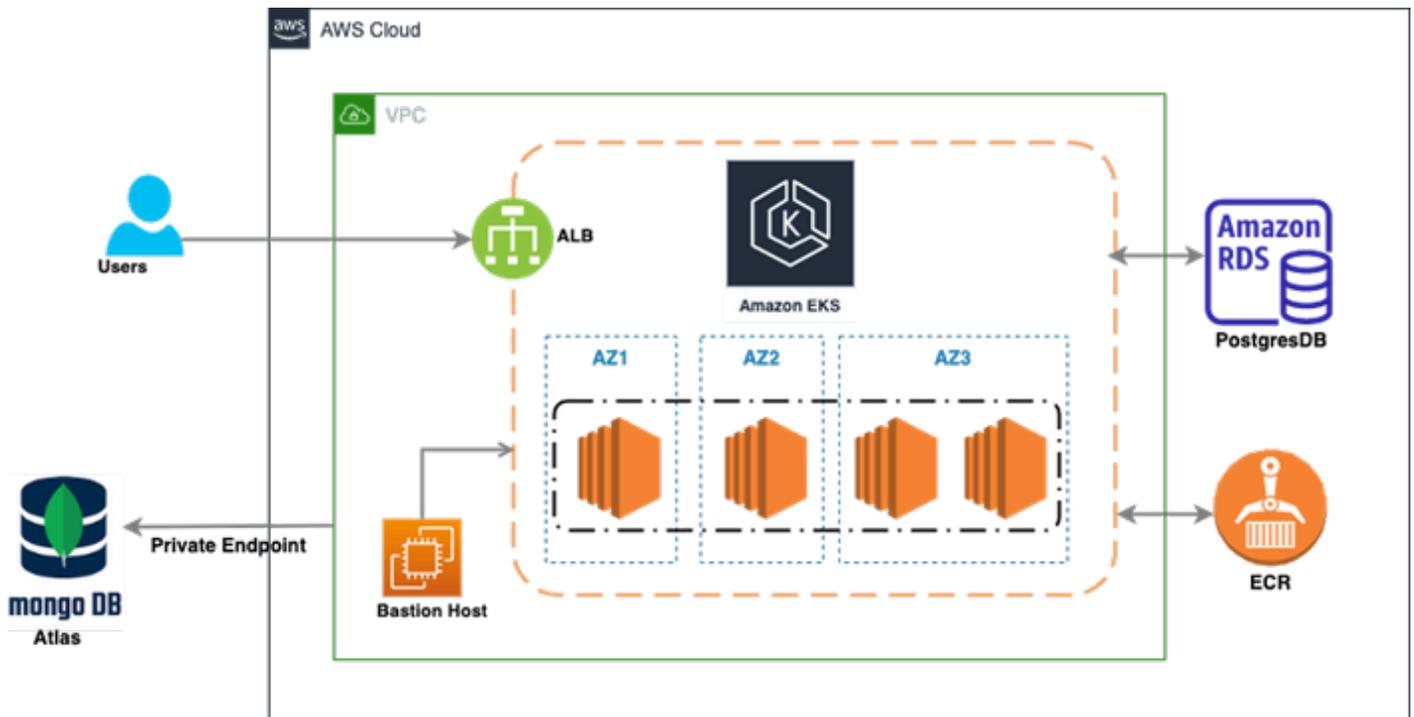
### **Ventajas del uso de Amazon EKS para la implementación de aplicaciones**

Amazon EKS ofrece varias ventajas para la implementación de aplicaciones, lo que lo convierte en una opción popular para las organizaciones que aprovechan aplicaciones y microservicios en contenedores.

#### **Entre las principales ventajas se incluyen:**

- **Plano de control de Kubernetes administrado:** EKS se encarga de la implementación, la ampliación y el mantenimiento del plano de control de Kubernetes, lo que reduce la carga operativa.
- **Gestión de clústeres simplificada:** EKS abstrae las complejidades de la configuración y gestión de clústeres de Kubernetes.
- **Escalabilidad:** EKS permite una sencilla ampliación de clústeres para adaptarse a cargas de trabajo cada vez mayores.
- **Alta disponibilidad:** EKS admite implementaciones de zonas de disponibilidad múltiple, lo que mejora la disponibilidad y la tolerancia a fallos.
- **Integración con los servicios de AWS:** EKS se integra a la perfección con varios servicios de AWS.
- **DevOps Automation:** EKS admite la integración continua y la implementación continua (CI/CD) para aplicaciones en contenedores.

### **Arquitectura de implementación de BPA**



Esta imagen representa una arquitectura de alto nivel de una infraestructura basada en la nube implementada en AWS, utilizando varios componentes clave. Aquí hay un desglose del diagrama:

1. **Amazon EKS (Elastic Kubernetes Service):** en el núcleo del diagrama, Amazon EKS se implementa en tres zonas de disponibilidad (AZ1, AZ2, AZ3), con nodos de trabajo de Kubernetes dentro de cada zona. Esto indica una configuración de alta disponibilidad y tolerante a fallos, ya que las cargas de trabajo se distribuyen en varias zonas de disponibilidad.
2. **ALB (equilibrador de carga de aplicaciones):** se sitúa en la parte frontal, recibe el tráfico de los usuarios y lo distribuye por el clúster EKS para gestionar las cargas de trabajo de las aplicaciones. El equilibrador de carga garantiza que las solicitudes se distribuyan de manera uniforme y que puedan gestionar la escalabilidad según la demanda del tráfico.
3. **Amazon RDS (Servicio de base de datos relacional) - PostgreSQL:** En el lado derecho del diagrama, hay una instancia de Amazon RDS que ejecuta PostgreSQL. A esta base de datos pueden tener acceso las aplicaciones que se ejecutan dentro del clúster EKS.
4. **ECR (Elastic Container Registry):** Aquí es donde se almacenan y administran las imágenes del contenedor Docker, que luego se implementan en Amazon EKS para ejecutar las cargas de trabajo.
5. **MongoDB Atlas:** En el lado izquierdo, MongoDB Atlas se integra en la arquitectura a través de un terminal privado. MongoDB Atlas es un servicio de base de datos NoSQL alojado en la nube, utilizado aquí para manejar los requisitos de base de datos basados en documentos. El terminal privado garantiza una comunicación segura y privada entre la instancia de MongoDB Atlas y otros componentes de AWS.
6. **Host de bastión:** ubicado en la VPC (nube privada virtual), un host de bastión proporciona un punto de entrada seguro para que los administradores accedan a los recursos dentro de la VPC sin exponerlos directamente a Internet.

En general, esta arquitectura proporciona una solución segura, escalable y de alta disponibilidad para implementar y administrar aplicaciones en contenedores mediante Amazon EKS, con compatibilidad con bases de datos relacionales (PostgreSQL) y NoSQL (MongoDB).

- **Configuración del clúster EKS**

Para crear un clúster de Amazon EKS mediante la CLI de AWS, se puede utilizar la utilidad de línea de comandos `eksctl`. Este es un ejemplo de comando:

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

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

- **Configuración de base de datos RDS**

La implementación de una base de datos relacional en Amazon RDS implica estos pasos:

- Acceda a la consola de administración de AWS y navegue hasta el servicio Amazon RDS.
- Cree una nueva instancia de base de datos con las especificaciones deseadas.
- Configure el grupo de seguridad para permitir conexiones entrantes desde el clúster de 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](#).

En el menú desplegable, seleccione la versión más reciente de PostgreSQL. En nuestro caso, 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.

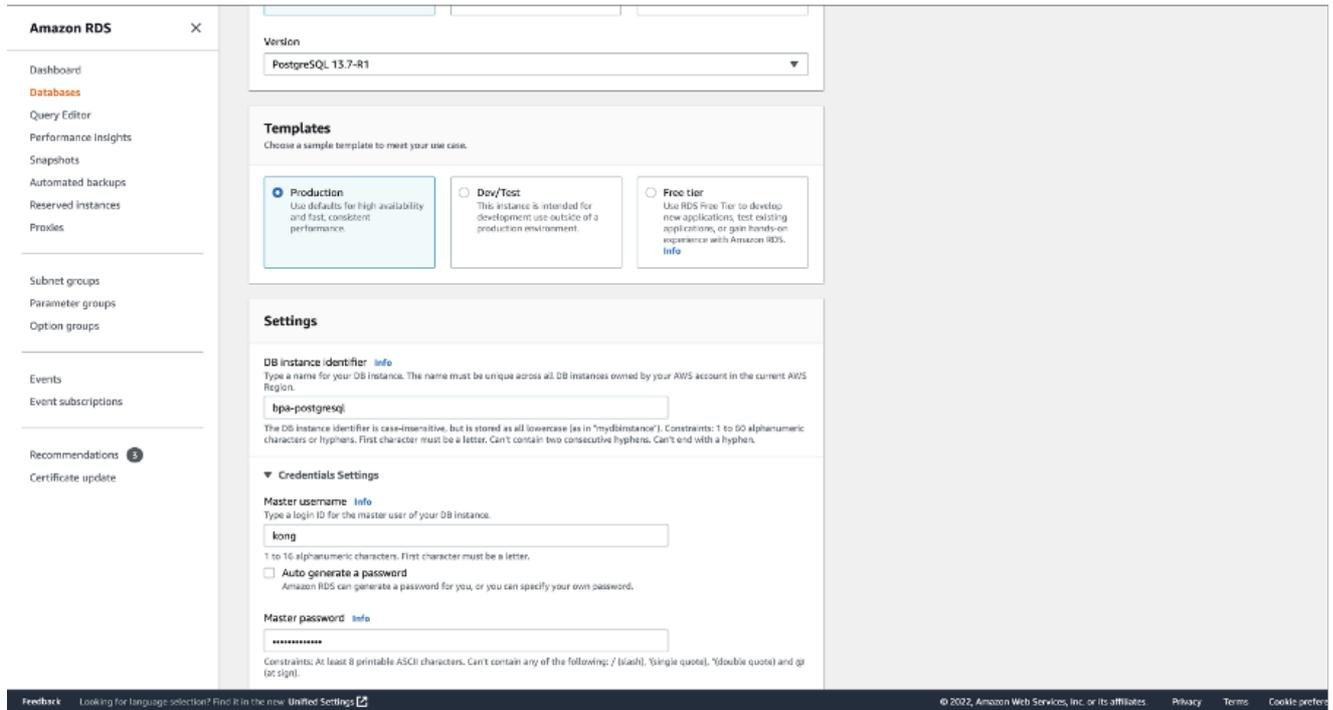
**Master password** [Info](#)

**Password strength** Neutral

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

**Confirm master password** [Info](#)

**Para ello, asigne un nombre a la instancia de base de datos y cree un nombre de usuario y una contraseña.**



Asegúrese de que la configuración predeterminada para "DB instance size" (Tamaño de instancia de base de datos) y "Storage" (Almacenamiento) esté seleccionada.

En función del tamaño del clúster y de los requisitos de datos, seleccione el tamaño de instancia de base de datos y el tipo de almacenamiento adecuados.

En función de nuestro caso práctico, hemos elegido la siguiente configuración:

- **Tamaño de instancia de BD:** db.m5d.2xlarge
  - 8 vCPU
  - 32 GiB RAM
  - Red: 4750 Mbps
  - Almacén de instancias de 300 GB

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

**ⓘ** 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

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

► Storage autoscaling

**Seleccione los valores adecuados en función de su caso práctico. Hemos seleccionado los valores predeterminados.**

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

**Asegúrese de que en "Autenticación de base de datos" hemos seleccionado la autenticación de contraseña. Autentica mediante contraseñas de base de datos.**

**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:

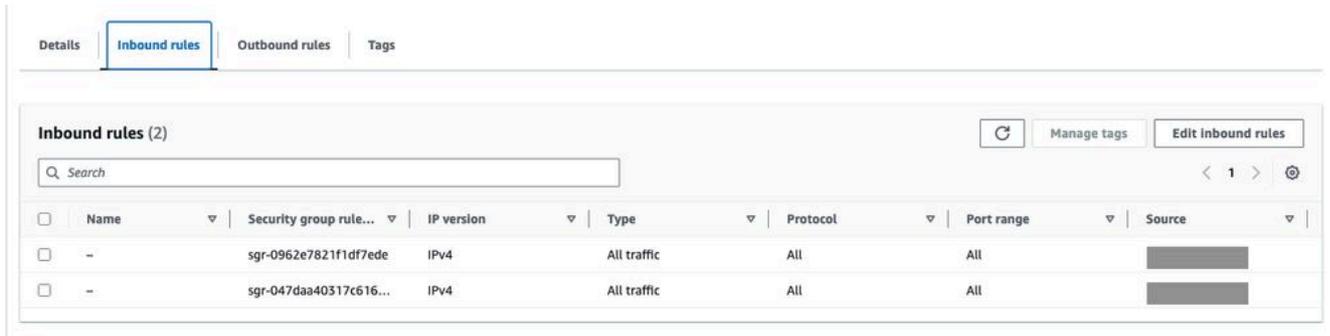
- Enable encryption:** A checked checkbox. Below it, text explains that master key IDs and aliases appear in the list after creation using the AWS Key Management Service (KMS) console. An 'Info' link is provided.
- AWS KMS key:** A dropdown menu showing '(default) aws/rds'.
- Account:** The account ID '193670463418'.
- KMS key ID:** The key ID '61e6c956-745e-42be-8fd1-77953104ad4f'.
- Log exports:** A section titled 'Log exports' with the instruction 'Select the log types to publish to Amazon CloudWatch Logs'. It includes two unchecked checkboxes: 'PostgreSQL log' and 'Upgrade log'.
- IAM role:** A section titled 'IAM role' with the instruction 'The following service-linked role is used for publishing logs to CloudWatch Logs.' Below this, a grey box contains the text 'RDS service-linked role'.
- Maintenance:** A section titled 'Maintenance' 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.' Below this, it says 'Maintenance window Info' and 'Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.' There are two radio button options: 'Choose a window' (unselected) and 'No preference' (selected).
- Deletion protection:** A section titled 'Deletion protection' 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).

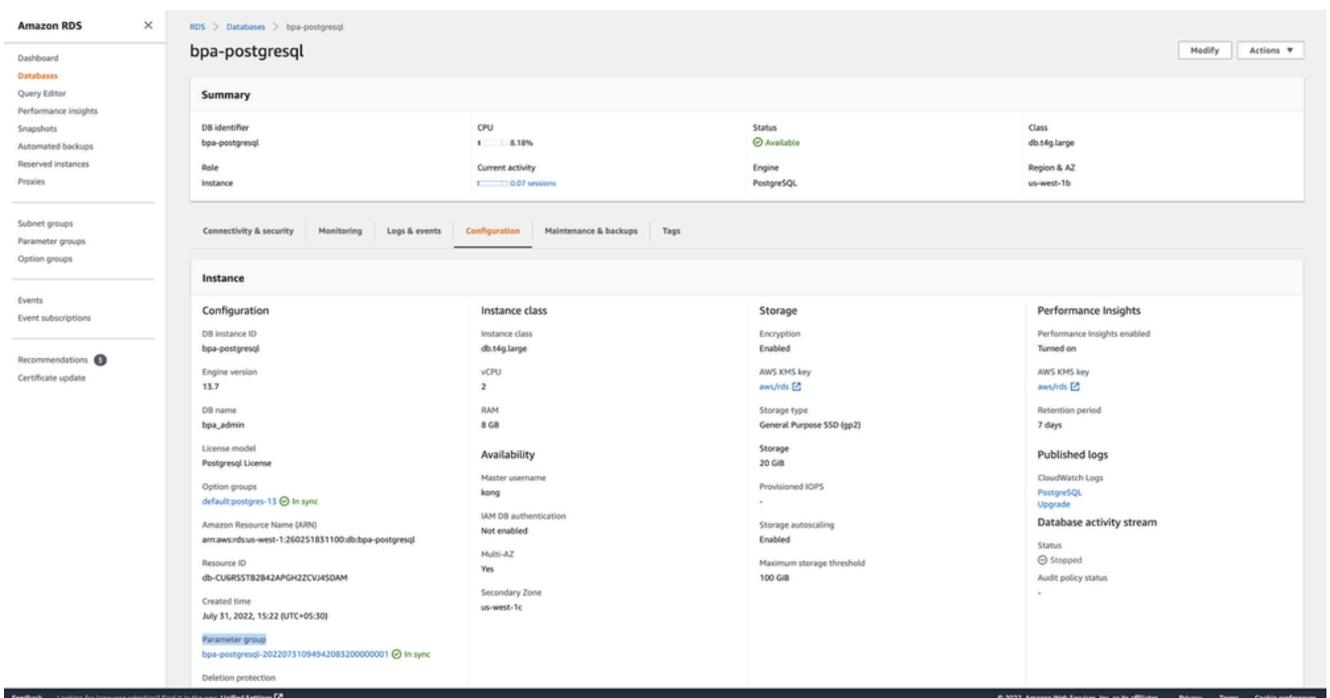
Una vez verificado, estamos listos para crear la base de datos. Vuelva al panel de Amazon RDS. Confirme que la instancia está disponible para su uso.

## Reglas de grupo de seguridad

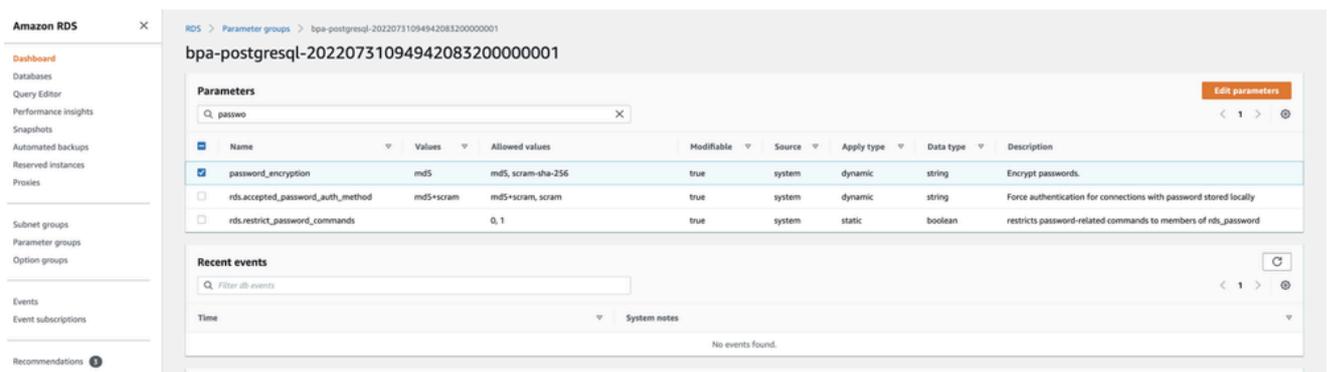
Actualice el grupo de seguridad entrante con el POD CIDR y el bloque CIDR del nodo.



**En RDS -> Databases -> DB-NAME, haga clic en configuration y consulte la sección Parameter Group y haga clic en el grupo de parámetros para ver.**



Busque "password\_encryption" y cambie el valor a md5 desde blank / other value. Esto es necesario para que las configuraciones de campus funcionen.



**Cree estas bases de datos junto con los usuarios conectándose a 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
```

- Autenticación de contraseña

Autentica mediante contraseñas de base de datos.

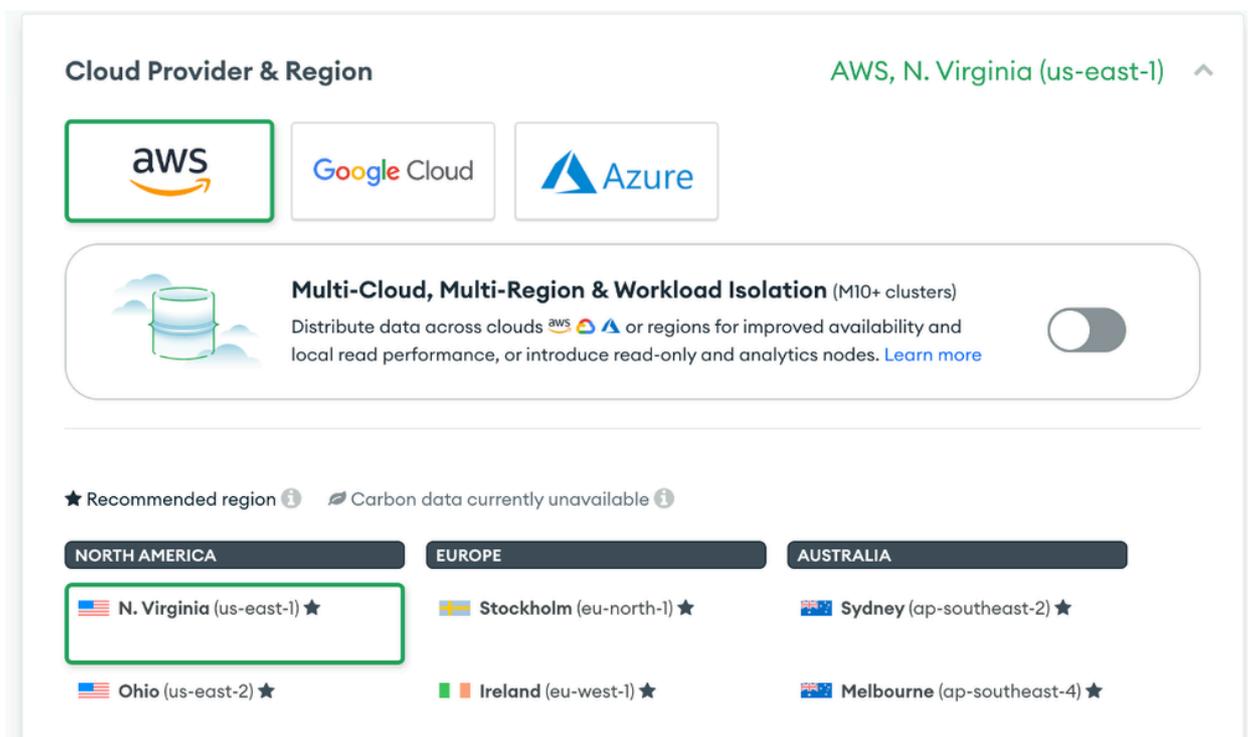
- **Configuración de Atlas MongoDB**

La configuración de Atlas MongoDB implica:

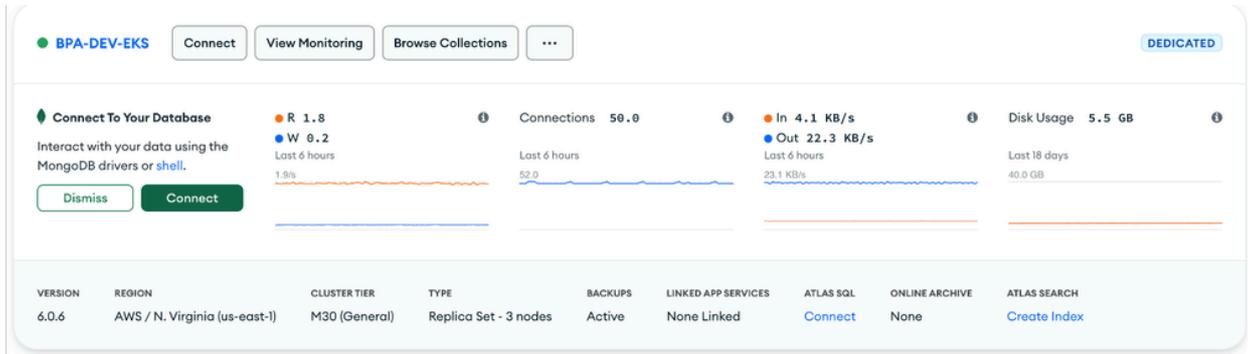
- **Inicio de sesión en Atlas MongoDB.**
- **Seleccionar la organización y el proyecto.**
- **Crear un clúster dedicado con las especificaciones adecuadas.**



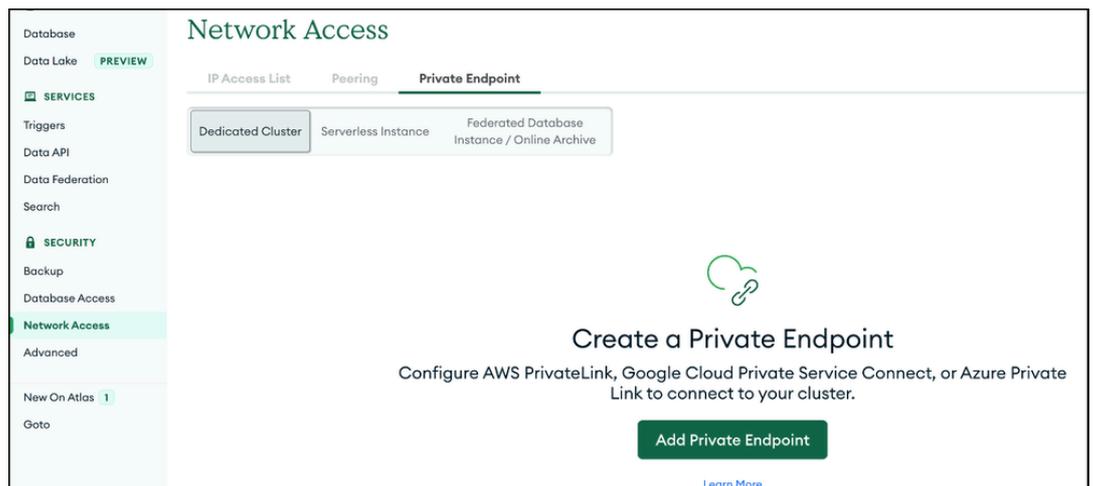
- **Seleccione el nivel dedicado, el proveedor de nube y la región.**



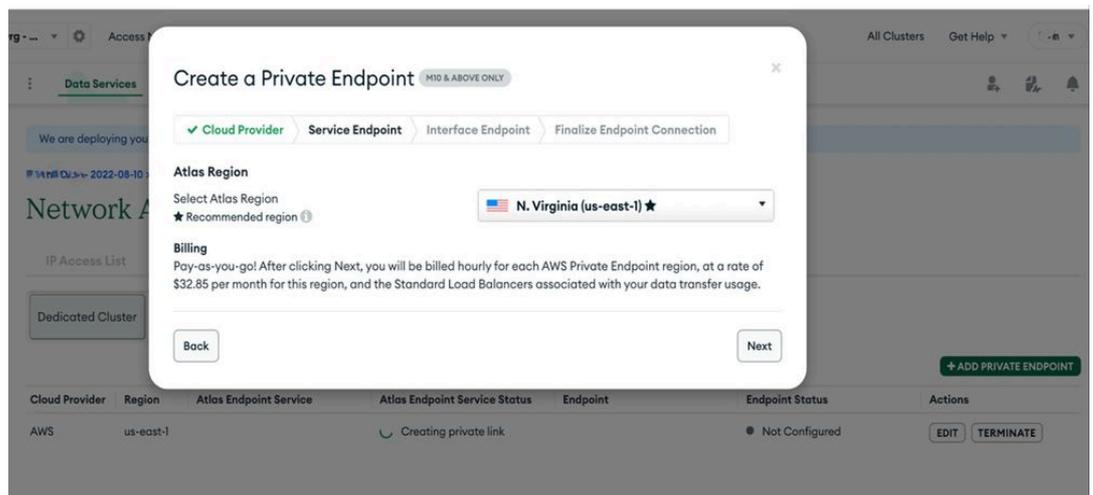
- **Seleccione el clúster dedicado del nivel adecuado (hemos utilizado M30 como nivel), proporcione el nombre del clúster adecuado y haga clic en Create Cluster (Crear clúster). Inicializará el grupo monogodb del sistema Atlas.**



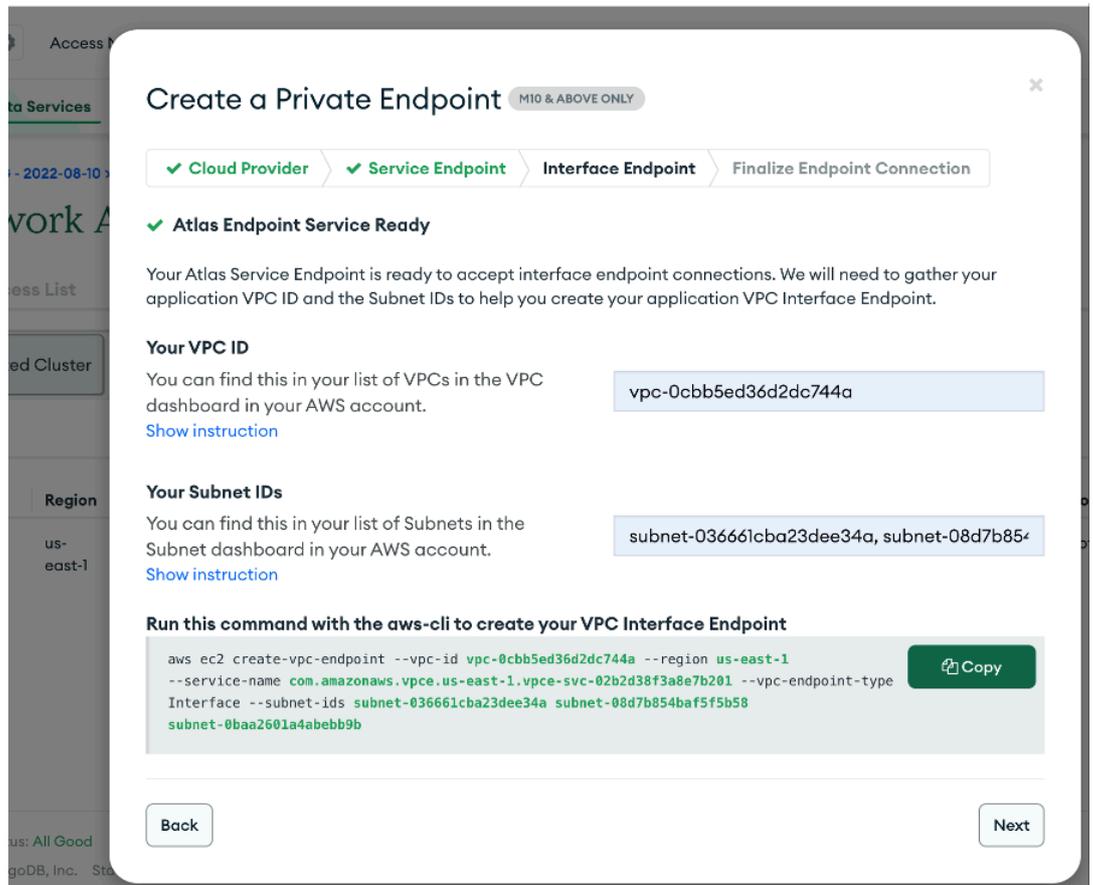
- **Configuración del terminal privado VPC para el clúster Atlas y K8S.**
  - **Haga clic en Network Access Select Private Endpoint y haga clic en Add Private Endpoint.**



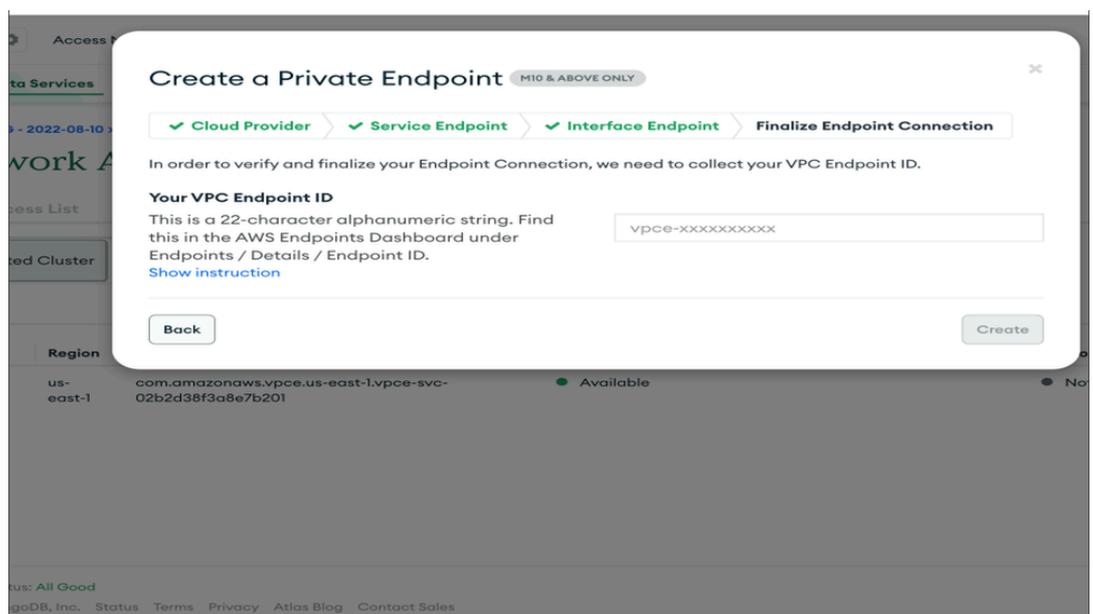
- **Seleccione Cloud Provider como AWS, seleccione la región correspondiente y haga clic en Next (Siguiente).**



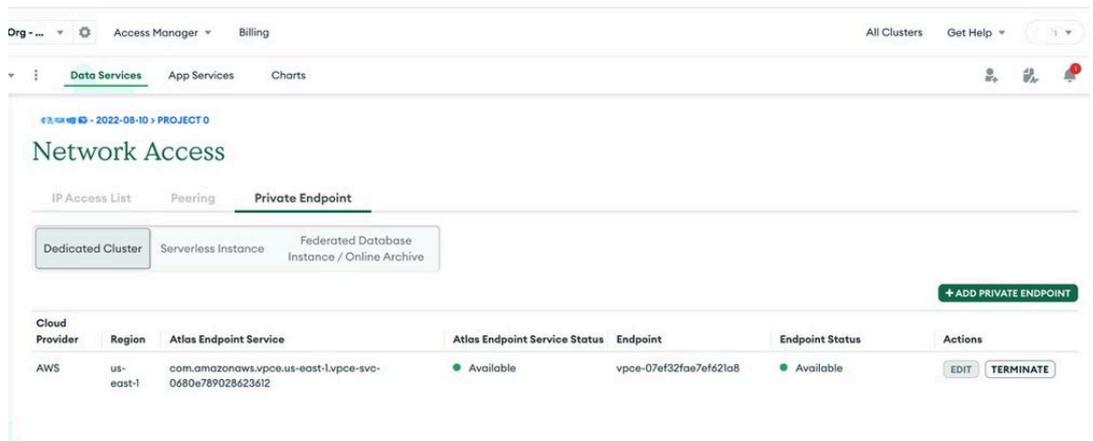
- **Proporcione el ID de PVC y los ID de subred respectivos. Una vez que ingrese los detalles, copie el comando vpc end point creation y ejecútelo en la consola de AWS. Obtendrá el ID del terminal vpc como resultado.**



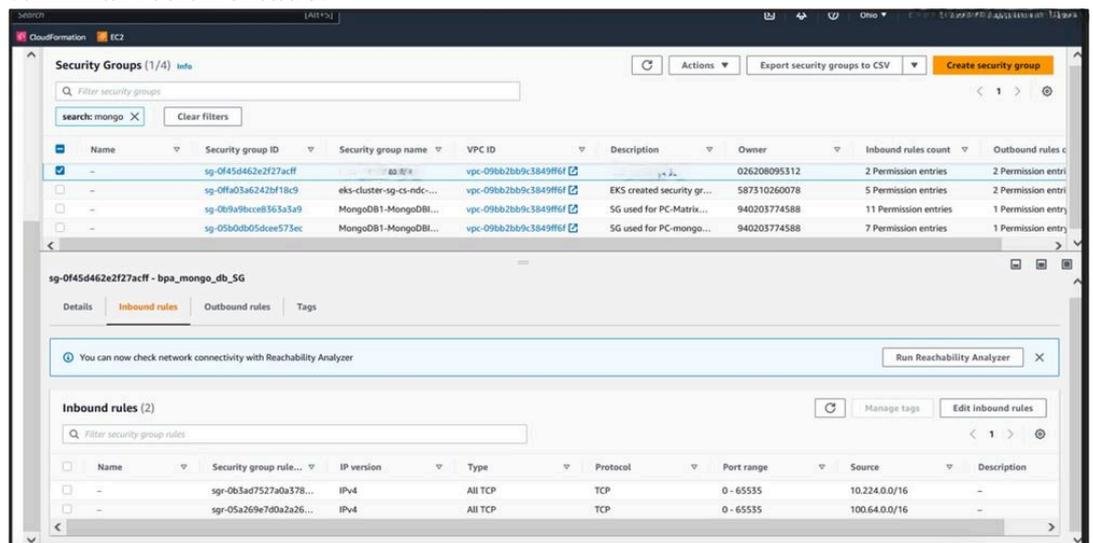
- **Haga clic en Next (Siguiete) para pegar la ID del terminal VPC y haga clic en Create (Crear).**



- Una vez que se haya creado correctamente, el estado del terminal será **Disponible**, como se muestra en la siguiente imagen. Se debe crear un punto final de VPC para POD CIDR. En nuestro caso hemos utilizado **"100.64.0.0/16"** .



- **Agregue reglas de entrada al terminal de vpc recién creado. El vpc-terminal estará en la cuenta padre y se debe asignar un grupo de seguridad al vpc-terminal recién creado.**



## ECR como registro de imágenes

La creación de repositorios de Amazon ECR y la inserción de imágenes Docker en ellos implica varios pasos. Estos son los pasos para crear un repositorio ECR, etiquetar una imagen Docker y enviarla al repositorio mediante la CLI de AWS.

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

Sustituir:

- **your-image-name** con el nombre deseado para el repositorio de ECR.
- **su región con** su región de AWS

## Configuración de la función IAM para nodos EKS

Asegúrese de que los nodos de trabajo EKS (instancias EC2) tengan la función IAM necesaria asociada con permisos para extraer imágenes de ECR. La política IAM necesaria es:

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

Adjunte esta política al rol IAM asociado con sus nodos de trabajo EKS.

## Implementación de BPA

La implementación de BPA implica varios pasos, incluidos el etiquetado de nodos de trabajo EKS, la preparación de directorios en nodos, la copia de paquetes BPA y la implementación de BPA mediante Helm.

**Para la implementación de nuestros clientes, hemos utilizado las siguientes versiones de software y servicios en la nube:**

- **BPA:** 4.0.3-6
- **RDS (servicio de base de datos relacional):** 16.3-R2
- **MongoDB Atlas:** v5.0.29
- **EKS (Elastic Kubernetes Service):** v1.27

Estos componentes garantizan que nuestra implementación sea sólida, escalable y capaz de gestionar las cargas de trabajo necesarias de forma eficaz.

- **Etiquetado de nodos de trabajadores 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
```

- **Preparación de Directorios en Nodos**

**Nodo 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
```

**Nodo 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
```

### **Nodo 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
```

### **Nodo 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
```

- Copia de paquetes 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/
```

- Implementación de BPA mediante Helm

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

## **Configuración de entrada**

- **Habilitación del ingreso**

Actualice `values.yaml` para habilitar el ingreso:

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

- **Creación de un secreto mediante un certificado BPA**

Navegue hasta el directorio de certificados y cree un secreto:

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

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

- **Actualización del controlador de ingreso**

Agregue el secreto recién creado en el `ingress-controller.yaml` archivo:

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

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

- **Actualización del certificado de ingreso**

Realice la eliminación e instalación del timón para actualizar el certificado de ingreso.

## **Especificaciones del entorno**

Las especificaciones de entorno incluyen requisitos para instancias EC2, equilibradores de carga, terminales VPC e instancias RDS. Las especificaciones clave son:

### **Requisitos de EC2:**

**Requisitos de almacenamiento:** 2 TB de espacio por nodos. Monte el volumen EBS en /opt y agregue una entrada en /etc/fstab para todos los nodos.

**Grupo de seguridad entrante:** 30101, 443, 0 - 65535 TCP, 22 para ssh.

**Grupo de seguridad saliente:** todo el tráfico debe estar habilitado.

**Resolución de DNS:** EC2 debe tener resoluciones en las instalaciones en /etc/resolve.conf.

### **Requisitos del equilibrador de carga:**

- Los puertos de receptores deben ser 443, 30101.
- Requisitos del terminal VPC (Atlas MongoDB).
- Los terminales VPC creados para la conectividad Atlas están disponibles en la cuenta principal (aws-5g-ndc-prod). El terminal VPC debe tener un grupo de seguridad que permita todo el acceso entrante (0 - 65535).

### **Requisitos de RDS:**

**Tipo de RDS:** db.r5b.2xlarge

**Versión del motor Postgres:** 13.7

**Grupo de seguridad:** el tráfico entrante debe permitir el tráfico del origen de POD CIDR.

### **Conceptos y componentes clave**

Comprender los fundamentos de Kubernetes es esencial para implementar y administrar eficazmente aplicaciones usando Amazon EKS.

---

### **Conclusión**

Este documento proporciona una guía detallada para implementar y administrar aplicaciones de automatización de procesos empresariales (BPA) mediante Amazon EKS. Siguiendo los pasos descritos y comprendiendo los conceptos clave, las organizaciones pueden aprovechar las ventajas de EKS para sus aplicaciones BPA en contenedores.

---

### **Referencias**

- Servicios web de Amazon, "Documentación de Amazon EKS", [Online].  
Disponible: <https://docs.aws.amazon.com/eks/>
- Kubernetes, "Documentación de Kubernetes" [Online].  
Disponible: <https://kubernetes.io/docs/home/>
- Guía rápida de Cisco BPA <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/at-a-glance-c45-742579.html>
- Guía de operaciones de BPA <https://www.cisco.com/c/dam/en/us/support/docs/bpa/v403/cisco-bpa-operations-guide-v403.pdf>
- Guía del desarrollador de BPA <https://www.cisco.com/c/dam/en/us/support/docs/bpa/v403/cisco-bpa-developer-guide-v403.pdf>

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).