

# تاي لمعلا ةتمتأ تاقيبطت ةرادإو رشن ي لمع ليلد: Amazon EKS عقوم يلع ةيراجتلا

## تايوتحملا

### درجم

اهترادإو (BPA) لامعلا تاي لمع ةتمتأ تاقيبطت رشن لوح الماش اليلد ةقرولا هذه مدقت زربي و، ةيساسأل تابلطتملا ددحي وهو. Amazon Flexible Kubernetes (EKS) ةمدخ مادختساب ةوطخ تاداشرا رفوي و، ةينورتكلال تاجتنم لل يئيبل مبيقتلا جذومن مادختسا دئاوف تانايب ةدعاق و، ةينورتكلال تاجتنم لل يئيبل مبيقتلا جذومن ةومجم ءاشنإل ةوطخب MongoDB سلسلطاو، Amazon ي ف دعب نع رشنل تانايب تانايب تانايب تانايب تانايب رفوي امم، ةيئيبل تابلطتملا ددحتو رشنل ةينب ي ف ةقرولا لخادتت، كلذ يلى ةفاضل اب و ةزعملا ةيتحتلا ةينبلا تامدخ نم ةدافتسالا يلى فدهت يتلا تاسسؤم لل الماش ادروم اهب ةصاخلا ةاوحمل BPA تاقيبطتلا

### ةيساسأل تاملكلا

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

## ةمدقملا

### هيأ ي ب ي ب



امم، FMC و NDFC ؤزهجأب صاخلا نيوكتلل عسوملا قفاوتلاو، (AQF) "ةمدقتملا راطتال انانكإل لضفب. عساو قاطن ىلع تاسسؤملا ليغشتلل الماش الح BPA لعجي رادصالا لوانتي، ؤيامل رادج ؤسايس ؤرادو ؤزهجال ماضو SD-WAN ؤكبش ؤرادا يف ؤيفاضال عساو تائيبلا تابلطتم يبل يامب، يئاقللل اهليغشتو ؤكبشلا نامأل ؤيويحل بناوچلا نيدرولم ؤددعتم و قاطنلا.

سكأ

تامدخ اهرفوتو لمالكلا اب اهترادا متت Kubernetes ؤمدخ يه Amazon Flexible Kubernetes (EKS) ؤمدخ 2018 ماع يف هقالطامت يذلا (EKS) أطخلل احيحصت ماظن طسب ي. Amazon (AWS) نم بيولا ؤصنم يه و، Kubernetes مادختساب اهؤاوتحامت يتلا تاقيبطتل ريوطتو ؤرادو رشن ؤيولمع حمسي امم، Kubernetes عاطق ؤرادا تاديقت عت EKS صخلي. رصملا ؤحوتفم تايواحل قيسننتل ؤينبل عم لماعتلا ىل ؤجالحا نود تاقيبطتل ليغشتو ؤانب ىلع زيكرتلاب نيروطملل ؤيساسال ؤتحتلا.

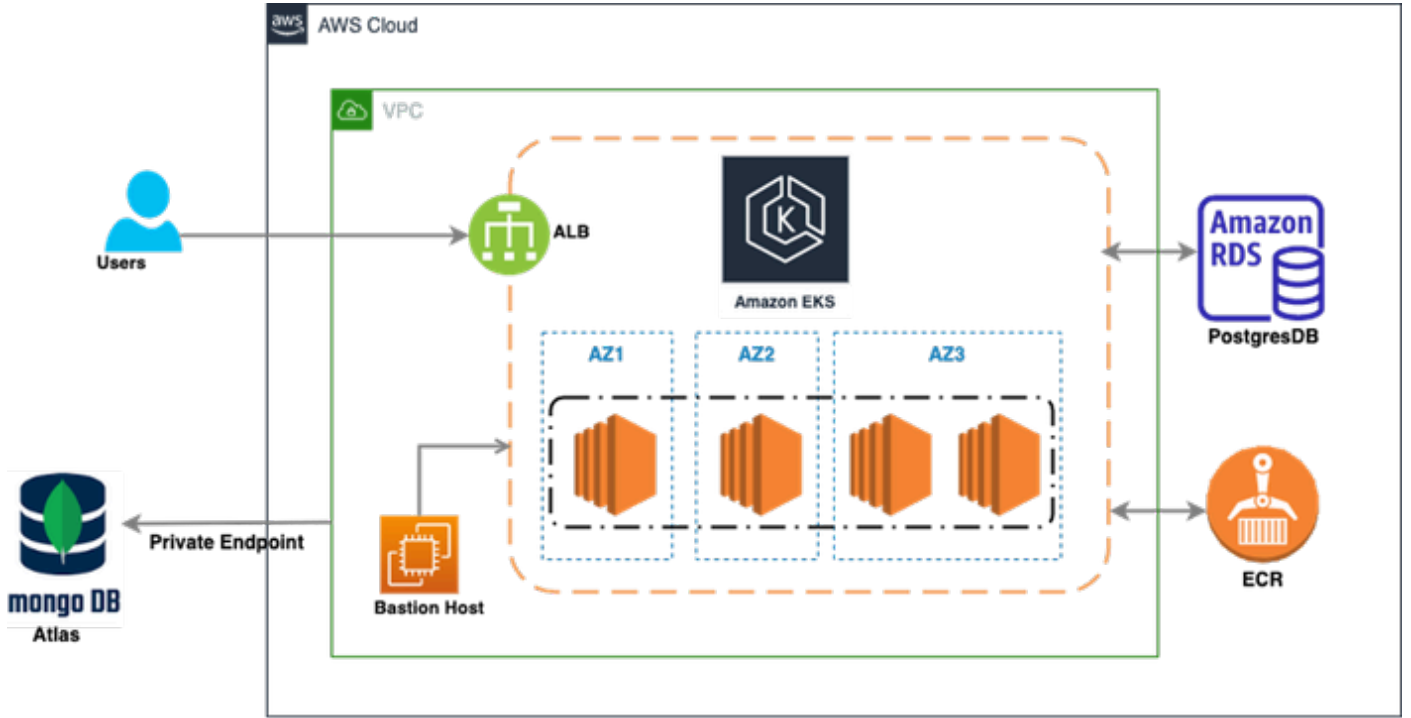
تاقيبطتل رشنل Amazon EKS ؤزهجأ مادختسا دئواف

اعئاش ارايتخا هل عجي امم، تاقيبطتل رشنل دئوافل نم ديدعل Amazon EKS ماظن رفوي ؤيقدلا تامدخالو تايواحل ىلع يوتحت يتلا تاقيبطتل نم ديفتست يتلا تاسسؤملا

يولي ام ؤيس يئرلا ايازمل نمضتتو

- Kubernetes يف مكحتلا يوتسم رشن EKS جلاعي: رادمل Kubernetes يف مكحتلا يوتسم ليغشتلا عبع نم للقي امم، هتئايسو هميسقتو.
- ؤيداصتقالا بناوچلاب ينعمل اربخال قيرف موقبي: تئايبلا تاعومجم ؤطسبملا ؤرادال ستيانربوك تاعومجم ؤرادو ؤاشن تاديقت ديجتبا.
- باعيتسال ؤمات ؤلوهسب تاعومجم ريوطت ؤينانكم EKS ماظن حيتي: ريوطتلا ؤيلباق ؤديازتملا لمعلال امحأ.
- لمعي امم، ؤددعتم رفاوتلا قطانم يف رشنل تايولمع EKS ماظن معددي: يلاعال رفاوتلا لاطعال ؤهجاوم و رفاوتلا نيسحت ىلع.
- AWS تامدخ فلتخم عم ؤسالسب EKS جمدم تي: AWS تامدخ عم لمالكلا.
- جمدلا (EKS) نسحمل ي نورتكلال ليغشتلا ماظن معددي: DevOps ل يئاقللل ليغشتلا ليغشتلا ؤاوتحمل تاقيبطتل (CI/CD) رمتسمل رشنل او رمتسمل.

BPA رشن ؤينب



اهرشن متي ةباحسلا لى دن تست ةي ساسا ةي نبل يوت سمل ةي لى ةي نبل ةر وصال هذه لثمت طخ م ل ل في نصت ي لى امي فو . ةي ساسا ل تان وكم ل نم ديدع ل مادخت ساب ، AWS لى

1. **EKS نم Amazon** (Kubernetes ةنرمل ةمدخل) **Amazon EKS** رشن متي ، طخ م ل بلق ي ف اذهو . ةقطنم لك لخاد Kubernetes لامع ل دقع عم ، (AZ1، AZ2، AZ3) رفوت قطنم ثالث ربع قطنم ربع لامع ل امحأ عيزوت متي شيح ، لاطع ل ل ل باقو رفوت لى لى داع لى لى ريشي ةددعتم رفوت .
2. **ALB** (ق ي ب ط ت ل ل م ح ن ز اوم) رورم ة ك رح ل ب ق ت س ي شيح ، ي م ا م ا ل ا ع ز ج ل ي ف اذهو عضو متي : (ق ي ب ط ت ل ل م ح ن ز اوم) . تاق ي ب ط ت ل ل م ل م ا م ا ل ا ع ل م ل EKS ةو م ج م ربع اهو ع ز و ي و ن ي م د خ ت س م ل م ت ا ن ا ي ب ل س ا ي ق ل ل ا ع ل م ه ن ك م ي و ي و ا س ت ل ا ب ا ه ع ي ز و ت م ت ي ت ا ب ل ل ط ل ا ن ا ل ي م ح ت ل ل ن ز اوم ن م ض ي رورم ل ا ع ل م ل ط ي ل ع ا ن ب .
3. **Amazon RDS** - PostgreSQL (ةي طاب ت ر ا ل ا ت ا ن ا ي ب ل ا ة د ع ا ق ة م د خ) ، طخ م ل م ن م ي ا ل ا ب ن ا ج ل لى ع ، هذه تان ا ي ب ل ا ة د ع ا ق لى لى ل و ص و ل ن ك م ي . PostgreSQL ل غ ش ي ي ذ ل ا Amazon RDS ل ي ث م د ج و ي EKS ةو م ج م ن م ض ل م ع ت ي ت ل ا تاق ي ب ط ت ل ل ل ا ل م .
4. **ECR** (نرمل ةي و ا ح ل ل ي ج س ت) اساس رال ا ةي و ا ح ر و ص ن ي ز خ ت ه ي ف م ت ي ي ذ ل ا ن ا ك م ل و ه اذهو : (نرمل ةي و ا ح ل ل ي ج س ت) . ل م ع ل ل ا م ا ل ل ي غ ش ت ل Amazon EKS ة ز ه ا ي ف ل ك ل ذ د ع ب ا ه ر ش ن م ت ي ي ت ل و ، ا ه ا ت ر ا د ا و .
5. **MongoDB** س ل ط ا م ا ظ ن ج م د م ت ي ، ر س ي ا ل ا ب ن ا ج ل لى ع ، ن م ةي ن ب ل ا ي ف MongoDB س ل ط ا م ا ظ ن ج م د م ت ي ، ر س ي ا ل ا ب ن ا ج ل لى ع . ة ف ا ض ت س م NoSQL تان ا ي ب ل ا ة د ع ا ق ة م د خ ن ع ر ا ب ع MongoDB Atlas . ة ص ا خ ةي ا ه ن ة ط ق ن ل ل ا ل م ة د ن ت س م ل ا تان ا ي ب ل ا ة د ع ا ق ت ا ب ل ل ط ت م ة ج ل م ل ا ن ه ا م ا د خ ت س ل م ت ي ، ة ب ا ح س ل ا ة ط س ا و ب ل ي ث م ن ي ب ص ا خ ل ل و ن م ا ل ل ا ص ت ا ل ا ة ص ا خ ل ا ةي ا ه ن ل ا ة ط ق ن ن م ض ت . ت ا د ن ت س م ل ا لى لى ر خ ا ل AWS تان و ك م و MongoDB Atlas .
6. **Bastion** ف ي ض م ر ف و ي ، (ةي ره ا ظ ل ا ة ص ا خ ل ا ة ك ب ش ل ل) VPC ز ا ه ج ل خ ا د ه د و ج و ل ا ر ط ن ، ن و د VPC ز ا ه ج ل خ ا د د ر ا و م ل لى لى ل و ص و ل ل ن ي ل و و س م ل ل ن م ا ل و خ د ة ط ق ن BaseTion . ت ن ر ت ن ا ل لى لى ة ر ش ا ب م م ه ص ي ر ع ت .



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](#).

PostgreSQL "PostgreSQL" و اذہ نإف، انتلأح یفو. PostgreSQL نم رادصإ شدحأ ددح، قل دس نملأ قمئ اقل مادختساب 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.

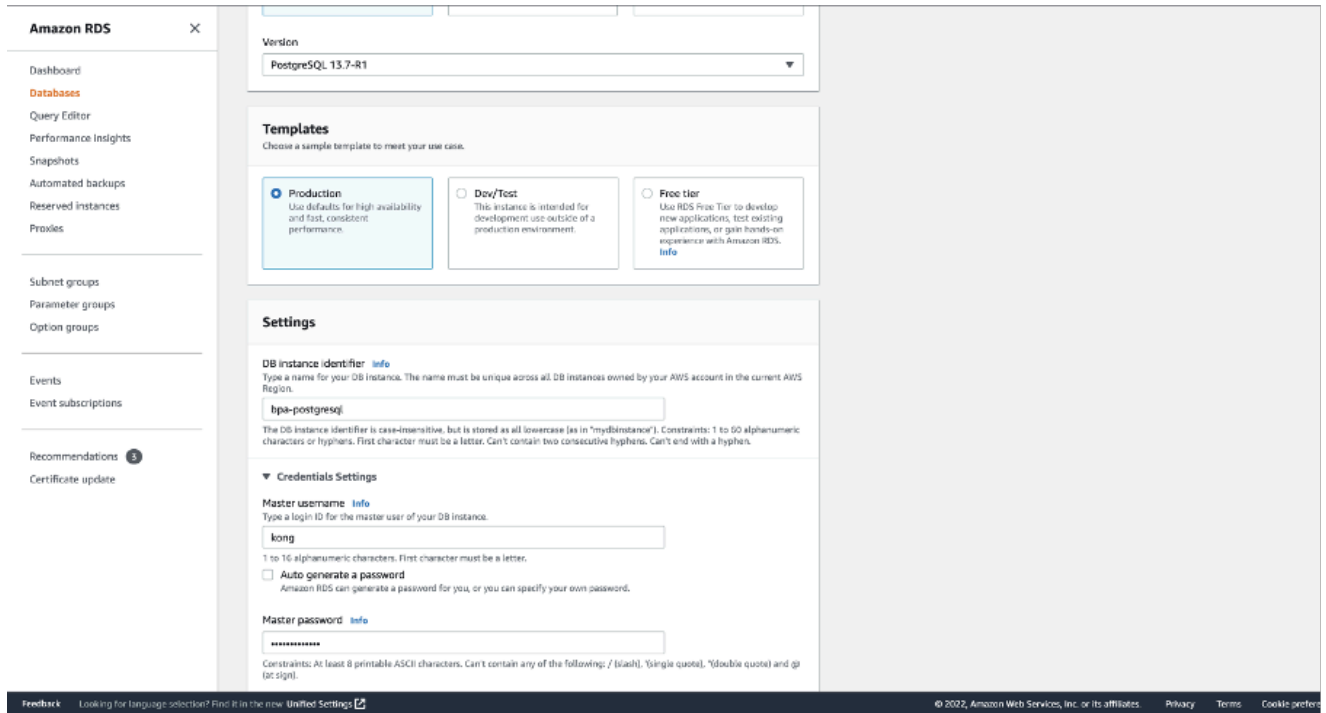
**Master password** [Info](#)

**Password strength** Neutral

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

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

رورم قملكو مدختسم مسا عاشن اب مقو امسا تان اي بل ادعاق لي شم اعطع اب مق ، اذهل



"نيزختل" و "DB ليثم مجح" ل ؤيضا رتفالا تاداد ؤل ديحت نم دكأت

(DB) تانا يبال ؤدعاق ليثم مجح دح، تانا يبال تاب ل طتمو ؤوم مجم الما ظن مجحل اقفو نيزختل ؤونو بس انم الما

للاتل نيوكتل رايتخاب انم ق، انب ؤصاخال مادختسالا ؤلح ؤل اذانتسا

- **DB ليثم مجح**: db.m5d.2xlarge
  - 8 vCPUs
  - 32 GiB RAM
  - ؤي نائل ي ف تباچ يم 4750: ؤك بشل
  - ليثم الما نيزختل تباچاچي 300 ؤعس



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

ةيضا رتفالا مي قلا انددح دقل .كب ةصاخلا مادختسالا ةل اهل اقفو ةبس انملا مي قلا ددح

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

تدعاق رورم تاملك مادختساب ققداصملا . "تانايبل اددعاق ققداصم" يف رورملا قملك ققداصم دي دحت نم دكأت تانايبل.

**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

aws Services Search [Option+S]

### 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

KMS key ID  
61e6c956-745e-42be-8fd1-77953104ad4f

### Log exports

Select the log types to publish to Amazon CloudWatch Logs

PostgreSQL log  
 Upgrade log

### IAM role

The following service-linked role is used for publishing logs to CloudWatch Logs.

RDS service-linked role

### Maintenance

Auto minor version upgrade [Info](#)

**Enable auto minor version upgrade**  
Enabling auto minor version upgrade will automatically upgrade to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the database.

Maintenance window [Info](#)  
Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.

Choose a window  
 No preference

### Deletion protection

**Enable deletion protection**  
Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database cluster.

**ⓘ 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.**

Cancel **Create database**

ةحول ىل عجرا . تاناىبلا ةءاق ءاشنإل نىءءءسم نوكن ، كلذ نم ققءءءل ءرءمبو  
مءءءءءل لىءمءل رفوء نم ءءء . Amazon فى RDS ءامولءم

نامأل ةءومءم ءءاوق

CIDR ءءقءل او Pod ب ءصءءل CIDR ءءء مءءءءءءاب ءءراول نامأل ةءومءم ءءءءءب مق

Details | **Inbound rules** | Outbound rules | Tags

Inbound rules (2)

Search

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
-	sgr-0962e7821f1df7ede	IPv4	All traffic	All	All	
-	sgr-047daa40317c616...	IPv4	All traffic	All	All	

رقن او تامل عمل اة عوم جم مسق عجر او ني وكتل ا قوف رقنا ، DB-NAME -> تان اي بلا دعوق -> RDS ي ف اهضر عل تامل عمل اة عوم جم قوف .

Amazon RDS

RDS > Databases > bpa-postgresql

bpa-postgresql

Summary

DB identifier bpa-postgresql	CPU 0.18%	Status Available	Class db.t4g.large
Role Instance	Current activity 0.07 sessions	Engine PostgreSQL	Region & AZ us-west-1b

Configuration

DB instance ID bpa-postgresql	Instance class db.t4g.large	Storage Encryption Enabled	Performance Insights Performance Insights enabled Turned on
Engine version 13.7	vCPU 2	AWS KMS key aws/rds	AWS KMS key aws/rds
DB name bpa_admin	RAM 8 GB	Storage type General Purpose SSD (gp2)	Retention period 7 days
License model PostgreSQL License	Availability Master username kong	Storage 20 GiB	Published logs CloudWatch Logs PostgreSQL Upgrade
Option groups default:postgres-13	IAM DB authentication Not enabled	Provisioned IOPS -	Database activity stream Status Stopped
Amazon Resource Name (ARN) arn:aws:rds-west-1:260251831100:db:bpa-postgresql	Multi-AZ Yes	Storage autoscaling Enabled	Audit policy status -
Resource ID db-CU6R5S7B2B4ZAPGH2ZCVJ4SDAM	Secondary Zone us-west-1c	Maximum storage threshold 100 GiB	
Created time July 31, 2022, 15:22 (UTC+05:30)			

اذه . رخا / غراف ميق نم MD5 الى ميق لال ري غتب مقو "password\_encryption" نع شحبا ل. م عمل ادنوماك تان ي وكتل ي رورض .

Amazon RDS

RDS > Parameter groups > bpa-postgresql-20220731094942083200000001

bpa-postgresql-20220731094942083200000001

Parameters

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.

RDS ب لالصتال ا ق ي رظ نع ني مدختس مل ا عم هذه تان اي بلا دعوق عاشن اب مق .

```
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
```

## • رورمل ةمك ةقداصم

تانايبل ةدعاق رورم تاملك مادختساب ةقداصملا

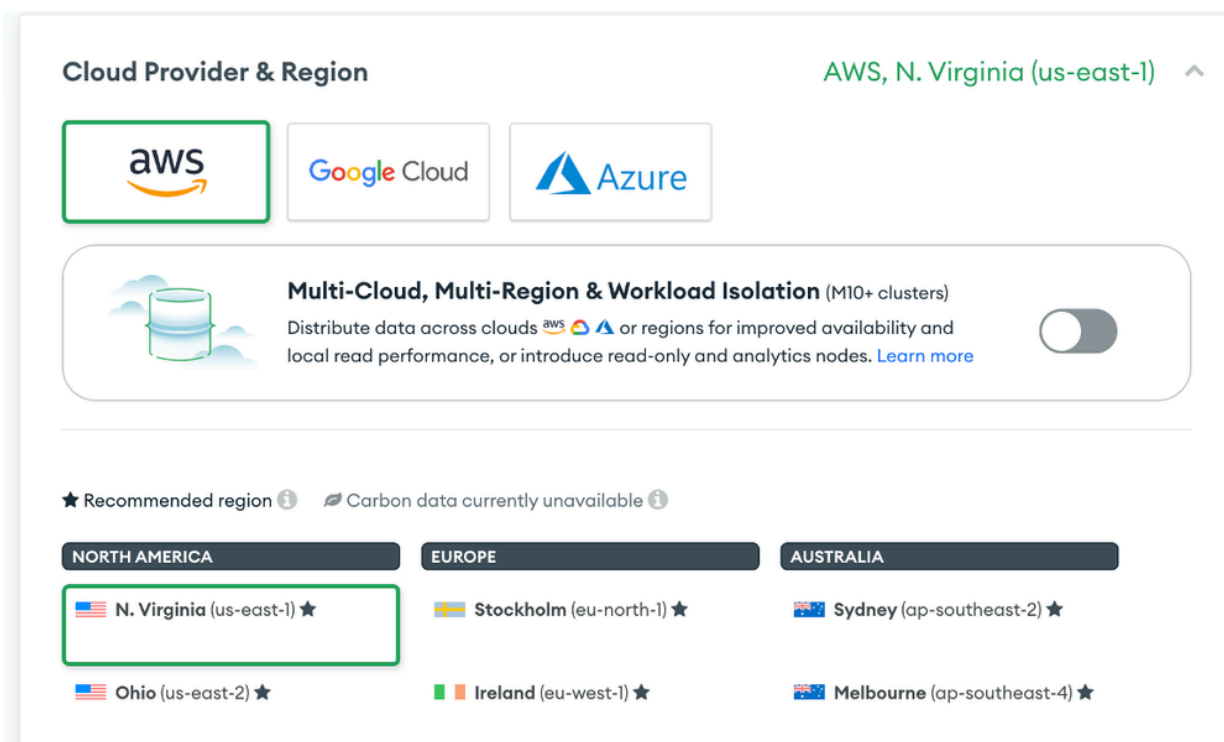
## • MongoDB س لظأ دادعإ

يلي ام MongoDB س لظأ دادعإ نمضتي

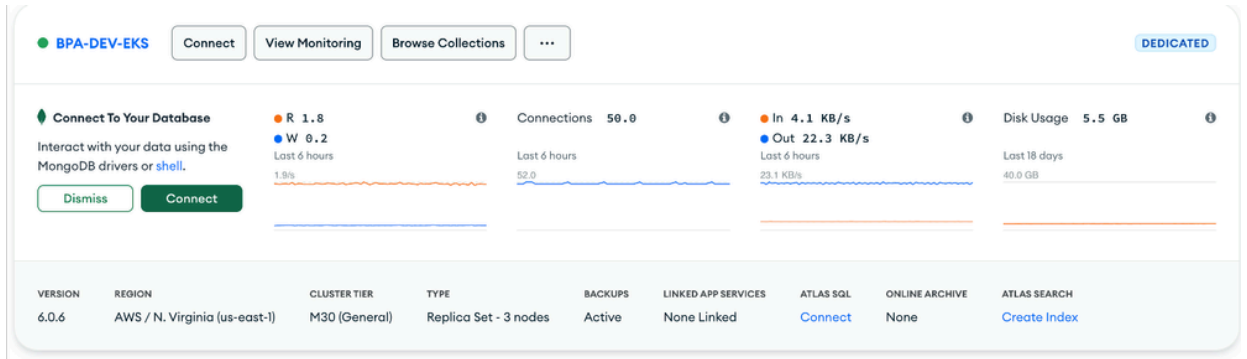
- Atlas MongoDB. لي لوخدلا لي جست
- عورشمل او ةسسؤملا دي دحت
- ةبسانملا تافصاوملا اهل ةصصخم ةعومجم ءاشنإ



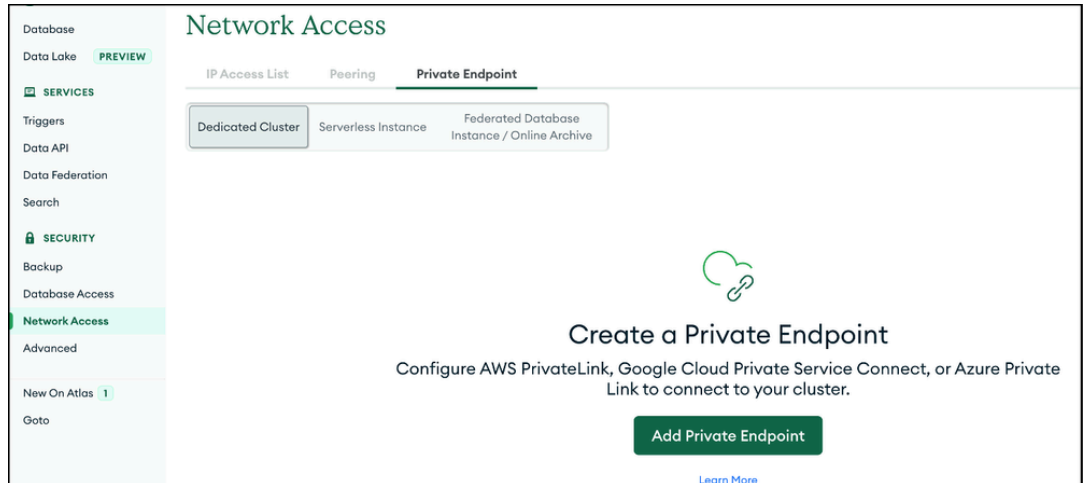
- ةقطنملا ةباحسلا رفومو ةصصخملا ةقبطلا دح



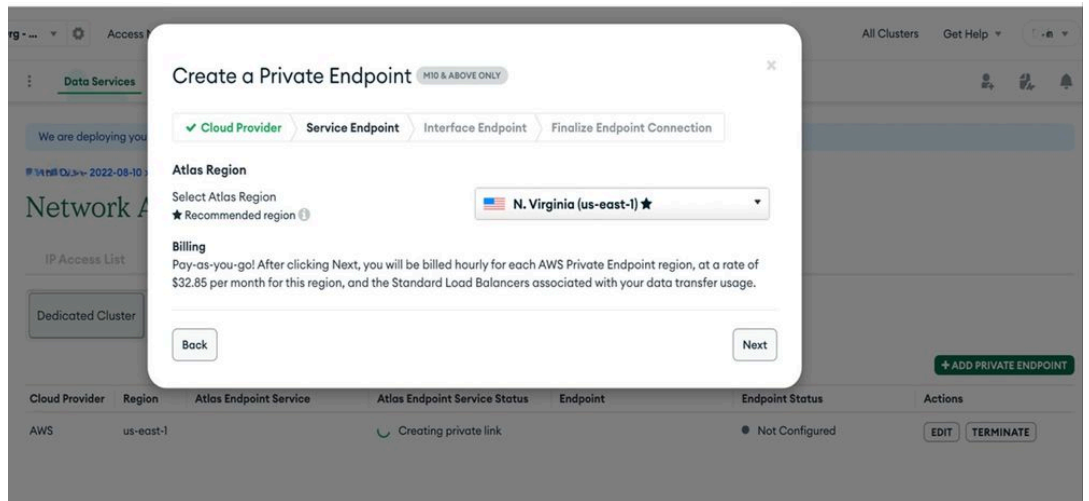
- ماظن مسا ري فوتب مقو ة عوم جمل ة ص ص خ م ل ا ( ة ق ب ط ك M30 ان م د خ ت س ا د ق ل ) ة ب س ان م ل ا ق ب ط ل ا د د ح دو غ و ل ا ة ي د ا ح ا س ل ط ا ل ا ة ع و م ج م ا د ب ت س و . ة ع و م ج م ا ظ ن ا ش ن ا ق و ف ر ق ن ا و ب س ان م ة ع و م ج م



- Atlas و K8S ة ع و م ج م ل ة ص ا خ ل ا VPC ة ي ا ه ن ة ط ق ن د ا د ع ا .
  - ( ة ص ا خ ة ي ا ه ن ة ط ق ن د ي د ح ت ) Network Access Select Private Endpoint ق و ف ر ق ن ا ة ص ا خ ة ي ا ه ن ة ط ق ن ة ف ا ض ا ق و ف ر ق ن ا .



- ي ل ا ت ل ا ق و ف ر ق ن ا و ة ل ب ا ق م ل ا ة ق ط ن م ل ا د د ح ، AWS ك ة ب ا ح س ل ا ر ف و م د د ح .



- ل ي ص ا ف ت ل ا ل ا خ د ا د ر ج م ب . ة ي ع ر ف ل ا ت ا ك ب ش ل ا ت ا ف ر ع م و ص ا خ ل ا PVC ف ر ع م ر ي ف و ت ،



زاده جلاب تصاخلا مكحتلا ءدحو يف هذي فن تيب مقو vpc end point creation رمألا خسنا جارخاك VPC ءي اهن ءطقن فرعم ىلع لصحتس.

**Create a Private Endpoint** M10 & ABOVE ONLY

✓ Cloud Provider ✓ Service Endpoint **Interface Endpoint** Finalize Endpoint Connection

✓ Atlas Endpoint Service Ready

Your Atlas Service Endpoint is ready to accept interface endpoint connections. We will need to gather your application VPC ID and the Subnet IDs to help you create your application VPC Interface Endpoint.

**Your VPC ID**  
You can find this in your list of VPCs in the VPC dashboard in your AWS account.   
[Show instruction](#)

**Your Subnet IDs**  
You can find this in your list of Subnets in the Subnet dashboard in your AWS account.   
[Show instruction](#)

**Run this command with the aws-cli to create your VPC Interface Endpoint**

```
aws ec2 create-vpc-endpoint --vpc-id vpc-0cbb5ed36d2dc744a --region us-east-1 --service-name com.amazonaws.vpce.us-east-1.vpce-svc-02b2d38f3a8e7b201 --vpc-endpoint-type Interface --subnet-ids subnet-036661cba23dee34a subnet-08d7b854baf5f5b58 subnet-0baa2601a4abebb9b
```

ءاشن ا قوف رقناو VPC ءي اهن ءطقن فرعم قصلل ىلاتلا قوف رقنا

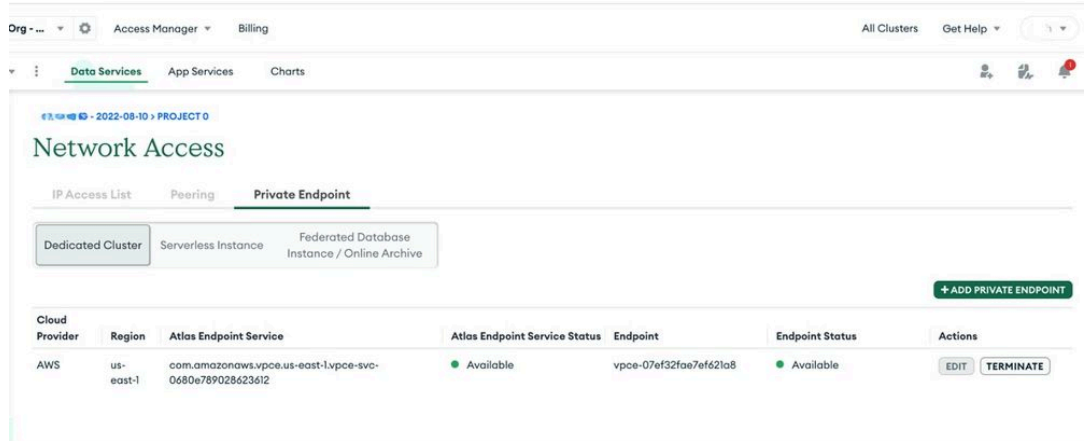
**Create a Private Endpoint** M10 & ABOVE ONLY

✓ Cloud Provider ✓ Service Endpoint ✓ Interface Endpoint **Finalize Endpoint Connection**

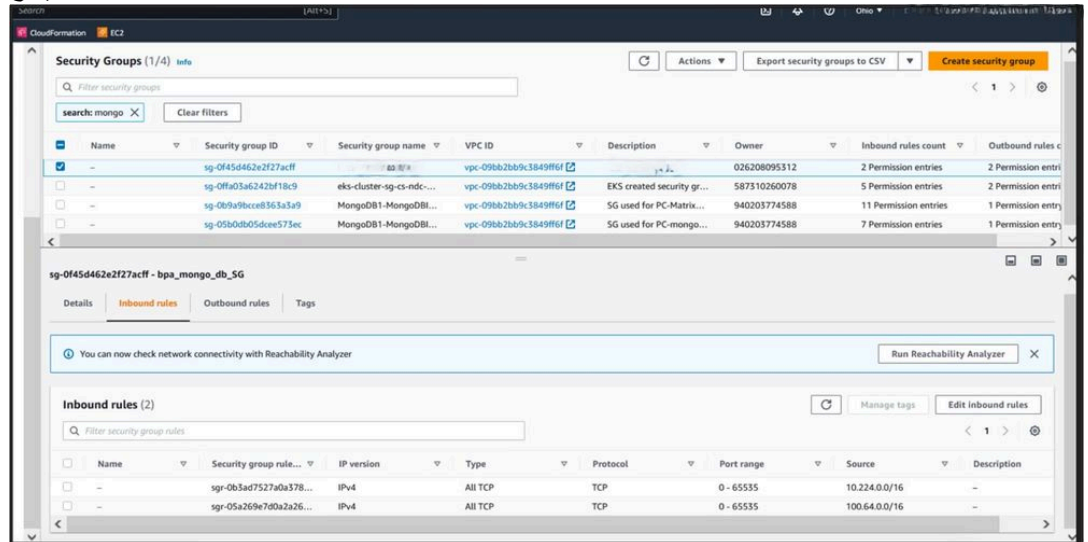
In order to verify and finalize your Endpoint Connection, we need to collect your VPC Endpoint ID.

**Your VPC Endpoint ID**  
This is a 22-character alphanumeric string. Find this in the AWS Endpoints Dashboard under Endpoints / Details / Endpoint ID.   
[Show instruction](#)

ءروصلا يف حضوم وه امك ءي اهن لا ءطقن ءلاح رفوتتس ، اءن ب اءى اشن اءرءم بوبو انمءءتس اءنءلاء يف Pod CIDR ل VPC ءي اهن ءطقن ءاشن اءرءم بوبو . ءي لءلا "100.64.0.0/16" .



- قیاهن قطنل نوكتس . اشي دح اواشن! مت يتلا vpc قیاهن قطنل یل! دواوق قفاض! اشي دح اواشن! مت يتلا vpc قیاهن قطنل نام! قعوم جم ني عت بجي و لصأل باس حل ا یف vpc .



## روصلل لچسك ECR

یه هذہ . تاوطخ دوع اهل! Docker روص عفدو Amazon یف ECR تاعدوتسم عاشن! نمضتی عدوتسمل یل! اها عفدو Docker روص یلع قمالع عضوو ECR عدوتسم عاشن! تاوطخل! AWS CLI مادختساب

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

لادبتس!

- كب صاخال ECR عدوتسمل بوغرمل مسالاب قروصك مس!
- AWS قطنم عم قیاهن قطنل اکتقطنم

## EKS IAM رول نيوكت

بحسب تان و ذاب ق ف ر م ل ا ي ر و ر ض ل ل ا I A M ر و د ي ل ع ي و ت ح ت ( E C 2 ت ا ل ي ث م ) E K S ل م ا ع د ق ع ن ا ن م د ك ا ت ي ه ة ب و ل ط م ل ا I A M ة س ا ي س . E C R ن م ر و ص ل ل

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

EKS ل م ا ع د ق ع ب ن ر ت ق م ل ا I A M ر و د ب ج ه ن ل ا ا ذ ه ق ا ف ر ا ب م ق .

## BPA رشن

ل ل ا ل د ل ا د ا د ع ا و ، E K S ل م ا ع د ق ع ي ل ع ت ا م ا ل ع ل ا ع ض و ك ل ذ ي ف ا م ب ، ت ا و ط خ ة د ع B P A ر ش ن ن م ض ت ي H E L M . م ا د خ ت س ا ب B P A ر ش ن و ، B P A م ز ح خ س ن و ، د ق ع ل ا ي ل ع

ة ي ب ا ح س ل ا ت ا م د خ ل ا و ج م ا ر ب ل ا ن م ة ي ل ا ت ل ا ت ا ر ا د ص ا ل ا م ا د خ ت س ا ب ا ن م ق ، ا ن ي ا ل م ع ر ش ن ل ق ب س ن ل ا ب

- **BPA:** 4.0.3-6
- **RDS:** 16.3-R2 (ة ي ط ا ب ت ر ا ل ا ت ا ن ا ي ب ل ا ة د ع ا ق ة م د خ )
- **MongoDB:** 5.0.29 ر ا د ص ا ل ا س ل ط ا م ا ظ ن
- **EKS:** v1.27 (ة ن ر م ل a K u b e r n e t e s ة م د خ )

ة ر د ا ق و ر ي و ط ت ل ل ة ل ب ا ق و ة ي و ق ا ه ب م و ق ن ي ت ل ا ر ش ن ل ا ة ي ل م ع ن و ك ت ن ا ت ا ن و ك م ل ا ه ذ ه ن م ض ت ة ا ف ك ب ة ب و ل ط م ل ا ل م ع ل ا ل ا م ح ا ة ج ل ا م ي ل ع

- **EKS** ل م ا ع د ق ع ي ل ع ت ا م ا ل ع ع ض و

```
kubectl label node
```

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

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

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

```
name=node-4
```

- دقعال ىل ع لى لى ال دلا رى ضحت  
1: دقعال

```
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
```

## 2: دقعال

```
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
```

### 3: تديق عل

```
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
```

### 4: تديق عل

```
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
```

- مزح خسن 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/
```

- HELM م ادخت ساب BPA رشن

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

### لخدملا دادع

- لخدملا ني كمت

لخدملا ني كمت .yamlto ميقول ا ثي دحت

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

- **BPA** ةداهش مادختساب رس ءاشنإ  
رس ءاشنإب مقو تاداهشلا ليلد لىل لقتنا

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

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

- لوخذلا مكحت ةدحو ثي دحت  
فلم لم اي. لوخذلا مكحتم يف اثيرح هؤاشنإ مت يذلا رسلا ةفاضإ

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

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

- لوخذلا ةداهش ثي دحت  
لوخذلا ةداهش ثي دحت له تي بثتو "ملېه" فذحب مق

ةئيبلا تافصاوم

تالېثم و VPC ةياهن طاقنو لاملحال نزاوم و EC2 تالېثم تابلطتم ةئيبلا تافصاوم نمضتت  
ي: هة ئيسئيرلا تافصاوملا RDS.

**EC2 تابلطتم:**

ىلإ EBS نيزخت ةدحو ليمحتب مق. دقع لك ل تي اباري ت 2 غلبت ةحاسم: نيزختلا تابلطتم  
/etc/fstab لىل الاخذإ فضاوم /opt.

SSH ل 22 و TCP 65535 - 0 و 443 و 30101 نامأل ةعومجم لخد.

اهلماكب رورملا ةكرح ني كم ت بجي: ةرداصل نامأل ةعومجم.

/etc/resolve.conf يف ةقبسمل تادحمل لىل EC2 يوتحي نأ بجي: DNS للحم.

لأحالة نزاوم تابلطتم:

- 30101 و 443 ني عم تسمل اذفانم نوكت نأ بجي.
- VPC (Atlas MongoDB) ةياهن ةطقن تابلطتم.
- (aws-5g-ndc-prod) يلصأال باسحلا يف Atlas لاصتال اهؤاشنإ مت يتل VPC ةياهن طاقن رفوتت دراوال لوصول اعيمج حيتت نامأ ةعومجم ىلع VPC ةياهن ةطقن يوتحت نأ بجي (0 - 65535).

RDS راي عم تابلطتم:

RDS عون: db.r5b.2xlarge

Postgres ةغيص كرحم: 13.7

POD CIDR رصم نم رورملا ةكرحب Inbound حمست نأ بجي: نامأال ةعومجم

ةيس يئرلا تانوكملاو ميهافملا

مادختساب لاعف لكشب تاقيبطتلا ةرادو رشنل اي ررض Kubernetes تاي ساسأ مهف ربعتي Amazon EKS.

رارقال

اهترادو (BPA) لامعأال تاي لمع ةتمتأ تاقيبطت رشنل الصفم اليلد ةقورولا هذه مدقت ميهافملا مهفو ةددحملا تاوطلخال عابتا لالخنمو. Amazon EKS تاقيبطت مادختساب تاجت نملل يئيبلا ميبقتلا جذومن دئاوف نم ةدافتسالا تامظنم لل نكمي، ةيس يئرلا لزبا قافتا راطا يف ةدراوال اهتاقيبطت يف ةينورتكلال

عجارملا

- [تنترنال ربع]، "Amazon EKS Documentation"، بيولا ىلع نوزامأ تامدخ <https://docs.aws.amazon.com/eks/>: رفوتم
- "Kubernetes، قئاثو"، [تنترنال ىلع]، رفوتم <https://kubernetes.io/docs/home/>: رفوتم
- Cisco BPA <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/at-a-glance-c45-742579.html> ىلع ةعيرس قرظن
- BPA <https://www.cisco.com/c/dam/en/us/support/docs/bpa/v403/cisco-bpa-operations-guide-v403.pdf> تاي لمع ليلى
- BPA <https://www.cisco.com/c/dam/en/us/support/docs/bpa/v403/cisco-bpa-developer-guide-v403.pdf> روطم ليلى

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن ت س م ل ا اذ ه Cisco ت مچرت  
م ل ا ل ا اء ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و  
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems ( ر ف و ت م ط ب ا ر ل ا ) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا