# **Deploy and Manage Business Process Automation Applications on Amazon EKS: a Practical Guide**

# Contents

# Abstract

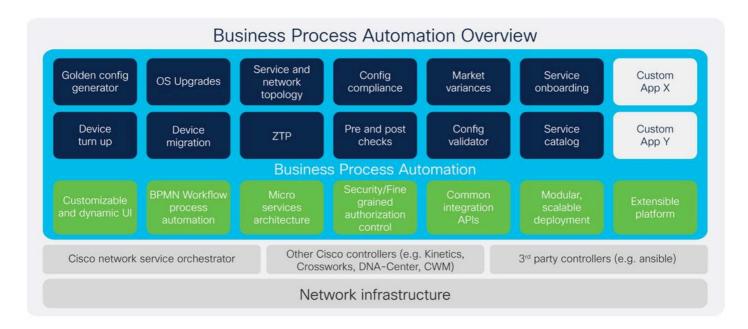
This paper presents a comprehensive guide on deploying and managing Business Process Automation (BPA) applications using Amazon Elastic Kubernetes Service (EKS). It outlines the prerequisites, highlights the benefits of utilizing EKS, and provides step-by-step instructions for setting up an EKS cluster, Amazon RDS database, and MongoDB Atlas. Additionally, the paper delves into the deployment architecture and specifies the environment requirements, offering a thorough resource for organizations aiming to leverage EKS for their containerized BPA applications.

# Keywords

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

# Introduction

# BPA



In today's digital era, enterprises seek to streamline and automate complex business processes across a diverse range of IT environments. Business Process Automation (BPA) has emerged as a pivotal technology, enabling organizations to enhance operational efficiency, reduce errors, and improve service delivery. BPA introduces several key innovations and enhancements aimed at advancing workflow

automation, service provisioning, and off-the-shelf automation applications.

The BPA platform hosts business and IT/operational use cases and applications, such as OS upgrades, service provisioning, and integration to orchestration engines. Customers have access to a lifecycle of services and BPA capabilities including advisory, implementation, business critical services, and solution support delivered through Cisco experts, best practices, and proven techniques and methodologies that help automate their business processes and de-risk their systems.

These lifecycle capabilities can be subscription-based or customized to individual needs. Implementation services help define, integrate, and deploy tools and processes to accelerate automation. Cisco experts conduct a formal process for gathering requirements, designs and develops user stories based on agile processes and Continuous Integration and Continuous Delivery (CICD) tools, and implements flexible services with automated testing of new or existing workflows, devices, and services. With Solution Support, customers get access to 24/7, centralized support with a focus on software-centric issues coupled with multivendor and open-source support offered through Cisco's tiered software model. Cisco solution support experts help manage your case from first call to final resolution and act as the main point of contact working with multiple vendors simultaneously. You could experience up to 44 percent fewer issues working with solution-level experts, helping you maintain business continuity and get faster return on your BPA investment.

Key technical features, such as support for FMC and Ansible-managed devices, parallel executions using the Advanced Queuing Framework (AQF), and expanded configuration compliance for NDFC and FMC devices, position BPA as a comprehensive solution for large-scale enterprise automation. With added capabilities in SD-WAN management, device onboarding, and firewall policy governance, the release addresses critical aspects of network security and automation, catering to the demands of large-scale, multi-vendor environments.

# EKS

Amazon Elastic Kubernetes Service (EKS) is a fully managed Kubernetes service provided by Amazon Web Services (AWS). Launched in 2018, EKS simplifies the process of deploying, managing, and scaling containerized applications using Kubernetes, an open-source container orchestration platform. EKS abstracts the complexities of Kubernetes cluster management, allowing developers to focus on building and running applications without the need to handle the underlying infrastructure.

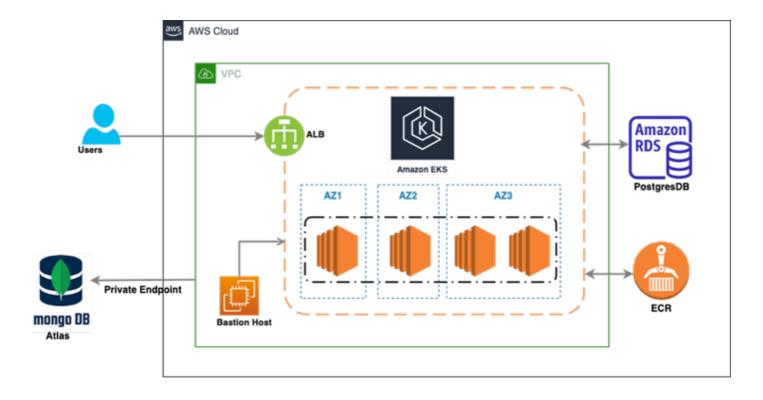
# **Benefits of Using Amazon EKS for Application Deployment**

Amazon EKS offers several benefits for application deployment, making it a popular choice for organizations leveraging containerized applications and microservices.

# Key advantages include:

- Managed Kubernetes Control Plane: EKS handles the deployment, scaling, and maintenance of the Kubernetes control plane, reducing operational burden.
- **Simplified Cluster Management**: EKS abstracts the complexities of setting up and managing Kubernetes clusters.
- Scalability: EKS allows for easy scaling of clusters to accommodate growing workloads.
- **High Availability**: EKS supports multi-Availability Zone deployments, enhancing availability and fault tolerance.

- Integration with AWS Services: EKS integrates seamlessly with various AWS services.
- **DevOps Automation**: EKS supports continuous integration and continuous deployment (CI/CD) for containerized applications.



# **BPA Deployment Architecture**

This image represents a high-level architecture of a cloud-based infrastructure deployed on AWS, using several key components. Here's a breakdown of the diagram:

- 1. Amazon EKS (Elastic Kubernetes Service): At the core of the diagram, Amazon EKS is deployed across three availability zones (AZ1, AZ2, AZ3), with Kubernetes worker nodes inside each zone. This indicates a highly available and fault-tolerant setup, as the workloads are spread across multiple availability zones.
- 2. **ALB** (**Application Load Balancer**): This is positioned at the front, receiving traffic from users and distributing it across the EKS cluster for handling application workloads. The load balancer ensures that the requests are evenly distributed and can handle scaling based on traffic demand.
- 3. Amazon RDS (Relational Database Service) PostgreSQL: On the right side of the diagram, an Amazon RDS instance running PostgreSQL is present. This database can be accessed by applications running within the EKS cluster.
- 4. ECR (Elastic Container Registry): This is where Docker container images are stored and managed, which are then deployed to Amazon EKS for running the workloads.
- 5. **MongoDB** Atlas: On the left side, MongoDB Atlas is integrated into the architecture through a private endpoint. MongoDB Atlas is a cloud-hosted NoSQL database service, used here to handle document-based database requirements. The private endpoint ensures secure, private communication between the MongoDB Atlas instance and other AWS components.
- 6. Bastion Host: Positioned within the VPC (Virtual Private Cloud), a Bastion Host provides a secure

entry point for administrators to access resources inside the VPC without directly exposing them to the internet.

Overall, this architecture provides a highly available, scalable, and secure solution for deploying and managing containerized applications using Amazon EKS, with support for both relational (PostgreSQL) and NoSQL (MongoDB) databases.

### • EKS Cluster Setup

To create an Amazon EKS cluster using the AWS CLI, the eksctl command-line utility can be used. This is an example command:

```
eksctl create cluster \
    --name <my-eks-cluster> \
    --region us-west-2 \
    --nodegroup-name standard-workers \
    --node-type t3.medium \
    --nodes 4 \
    --nodes-min 4 \
    --nodes-max 6
```

### • RDS Database Setup

Deploying a relational database on Amazon RDS involves these steps:

- Access the AWS Management Console and navigate to the Amazon RDS service.
- Create a new database instance with the desired specifications.
- Configure the security group to allow incoming connections from your Amazon EKS cluster.

Choose a database creation method Info							
• Standard create You set all of the configuration options, including ones for availability, security, backups, and maintenance.	<ul> <li>Easy create</li> <li>Use recommended best-practice configurations. Some configuration options can be changed after the database is created.</li> </ul>						
Engine options							
Engine type Info							
Aurora (MySQL Compatible)	Aurora (PostgreSQL Compatible)						
O MySQL	O MariaDB						
PostgreSQL							
O Microsoft SQL Server	о івм db2 IBM <b>Db2</b>						
Engine version Info View the engine versions that support the following database Hide filters	features.						
Show versions that support the Multi-AZ DB cluss Create a A Multi-AZ DB cluster with one primary DB insta to 2x faster transaction commit latency and automatic fa	ance and two readable standby DB instances. Multi-AZ DB clusters provide						
Engine Version PostgreSQL 16.3-R2							

Using the drop-down menu, select the most recent version of PostgreSQL. In our case, it is "PostgreSQL 16.3-R1."

		Services	Q Search [Option+S]							
		Creates	a single DB instance with no standby DB instances.							
	C	Creates	AZ DB instance s a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, b y DB instance doesn't support connections for read workloads.	out the						
<ul> <li>Multi-AZ DB Cluster</li> <li>Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a difference Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.</li> </ul>										
	s	Setting	s							
	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.									
	bpa-postgres									
			ster identifier is case-insensitive, but is stored as all lowercase (as in "mydbcluster"). Constraints: 1 to 60 alphanumeric First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.	c characters						
			ntials Settings							
	N T	Aaster use	ername Info n ID for the master user of your DB cluster.							
	м Т 1 С	Master use ype a login kong to 16 alph Credential	ername Info							
	м Т 1 С	Master use ype a login kong to 16 alph Credential You can use O Man RDS	ername Info n ID for the master user of your DB cluster. hanumeric characters. The first character must be a letter. Is management	password						
	м Т 1 С	Aaster use ype a login kong to 16 alph Credential ou can use Man RDS throu	ername Info n ID for the master user of your DB cluster. hanumeric characters. The first character must be a letter. Is management a AWS Secrets Manager or manage your master user credentials. haged in AWS Secrets Manager - most secure generates a password for you and manages it Self managed Create your own password or have RDS create a p	password						
	M [] 1 Y	Aaster use ype a login kong to 16 alph Credential Crede	ername Info In ID for the master user of your DB cluster. hanumeric characters. The first character must be a letter. Is management a AWS Secrets Manager or manage your master user credentials. haged in AWS Secrets Manager - most secure generates a password for you and manages it ughout its lifecycle using AWS Secrets Manager. generate password	password						
	M [] 1 Y	Aaster use ype a login kong to 16 alph Credential Crede	ername Info In ID for the master user of your DB cluster. hanumeric characters. The first character must be a letter. Is management e AWS Secrets Manager or manage your master user credentials. Inaged in AWS Secrets Manager - most secure generates a password for you and manages it ughout its lifecycle using AWS Secrets Manager. Igenerate password In RDS can generate a password for you, or you can specify your own password. Info	password						
	M T 1 1 V V	Aaster use ype a login kong to 16 alph Credential ou can use Man RDS throu Amazon Aaster pas	ername Info In ID for the master user of your DB cluster. hanumeric characters. The first character must be a letter. Is management e AWS Secrets Manager or manage your master user credentials. Inaged in AWS Secrets Manager - most secure generates a password for you and manages it ughout its lifecycle using AWS Secrets Manager. Igenerate password In RDS can generate a password for you, or you can specify your own password. Info	password						
		Aaster use ype a login kong to 16 alph redential ou can use O Man RDS throu Amazon Aaster pas Password	ername Info n ID for the master user of your DB cluster. hanumeric characters. The first character must be a letter. Is management a AWS Secrets Manager or manage your master user credentials. haged in AWS Secrets Manager - most secure generates a password for you and manages it ughout its lifecycle using AWS Secrets Manager.  Self managed Create your own password or have RDS create a p that you manage.  generate password n RDS can generate a password for you, or you can specify your own password.  ssword Info	password						
		Aaster use ype a login kong to 16 alph Credential ou can use O Man RDS throu Amazon Aaster pas 'assword d	ername Info n ID for the master user of your DB cluster. hanumeric characters. The first character must be a letter. Is management a AWS Secrets Manager or manage your master user credentials. haged in AWS Secrets Manager - most secure generates a password for you and manages it ughout its lifecycle using AWS Secrets Manager.  generate password n RDS can generate a password for you, or you can specify your own password.  strength Neutral	password						

For this give the database instance a name and create a username and password.

Amazon RDS X   Urricin Indiabard   Databased PolypedQL 33-341   Carbonated Rudseys Indiabard Respective Resp				
Debbord   Debbord   Debbord   Debbord   Cyrriferion   Stappidsis   Automated backups   Dereved instances   Productor groups   Debrording   Definitions   Cyrriferions   Definitions   Definitions </th <th>Amazon RDS</th> <th>×</th> <th>Verdin</th> <th></th>	Amazon RDS	×	Verdin	
Avery folfor   Very folfor    Very folfor    Very f	Dashboard			
ardmanne indigits   reportions   reportions   evervale intances   revise   revise   revise   verts	atabases			
ardmanusci lindjitis:   repriotes:   repriotes:   automated landpuis:   repriotes:   reserved instances:   repriotes:	Query Editor			
Inclusions a sample to regulate to most your one cans.  Concernent standards  Concernent			Templates	
Automated backups kerrord instances werds werd			Choose a sample template to meet your use case.	
eerved instances rooks				
troka:     ubnet groups   wends    wends <td></td> <td></td> <td></td> <td></td>				
trades performance    performance   ubnet groups   arameter groups pploin groups    Settings   uents   wents   wents   wents   wents dubacriptions   Dimensional for your DB Instance identifier info Type a num for your DB Instance identifier info Type a num for your DB Instance identifier info Type a num for your DB Instance identifier info Type a num for your DB Instance identifier info Type a num for your DB Instance identifier info Type a num for your DB Instance identifier info Type a num for your DB Instance identifier info Type a num for your DB Instance. Implements the location instance information is a particulation in the current AUSE Region. The De Instance identifier info Type a num for your DB Instance. Implements the location instance information is a particulation in the current AUSE Region. The De Instance identifier info Type a num for your DB Instance. Implements the location instance information. The Ide alphanument character must be a letter. Implements character instance in particulation. The Ide alphanument character must be a letter. Implements character instance in provide information. The Ide alphanument character must be a letter. Implements character instance in provide information. The Ide alphanument character instance in provide information. Implements character instance in provide information. The Ide alphanument character must be a letter. Implements character in the location. Implements character in the loca	eserved instances			
Buildhent groups   arameter groups   Option groups     Settings     Bernstance (entrifier)   Wends   Wends   Wends   Settings     Deprotore stems     Settings              Deprotore stems   Settings <b>Settings Deprotore stems  <b>Deprotore stems  <b>Deprotore stems  <b>Deprotore stems  </b></b></b></b>	Proxies		performance. production environment. applications, or gain hands-on experience with Amazon RDS.	
harameter grups   bytion groups     wents   wents   wents subscriptions     DB instance identifier info   The Db instance identifier info   Data   Data   Commendations   Image: Commendations <			Info	
Settings   Settings   Verits	ubnet groups			
species groups     DB instance (doubtifier info   Sivents subscriptions     becommendations     Certificate update     DB instance (doubtifier info   DB instance (doubtifier info   To a login (Doubtifier)   DB instance (doubtifier info)   Sivents subscriptions     becommendations     Certificate update     DB instance (doubtifier info)   Type a login (D for the master user of your DB instance)   Constraints (1 to 1) alphanumeric thractors. That character must be a letter.   Instance (Doubtifier)   Auto generate a password   Auto generate a password for your on password.   Master password info   Centraints. At load for the master user of your on password.   Centraints. Auto ag through (AGC) (doubters. Can't contain two on password.   Master password info   Centraints. At load for the password for your on password.   Centraints. At load for the password for your on password.	Parameter groups			
ivents       Type a runn for your DB instance. The name must be unque across al. DB instances counted by your AWS account in the current AWS hours of the polymour AWS account in the polymour AWS account in the polymour AWS account in the current AWS hours of the polymour AWS account in the current AWS hours of the polymour AWS account in the polymour AWS account and the polymour AWS account and the polymour AWS a	Option groups		Settings	
inpart possignessi      tecommendation:       tecommendation:     Tereifficate update:   Master users of your DB instance:     tecommendation:     Type a login Ib for the master user of your DB instance:  <	ivents	_	Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS	
characters or hyphers, First character must be a letter, Carit contain two consecutive hyphers. Carit end with a hyphen.   Letrificate update   characters or hyphers, First character must be a letter, Carit contain two consecutive hyphers. Carit end with a hyphen.   Cententials Settings   v Credentials Settings   Master uservame info   Type a login ID for the muster user of your DB instance.   kong   1 to 16 Alphanumeric characters. First character must be a letter.   Auto generate a password   Ansacen BDS cari generate a password   Ansacen BDS cari generate a password   Centraints. At least B printable ASCII characters. Carit contain noy of the following. / blachly, 'binglin quotel, 'binzbin	vent subscriptions		bpa-postgresql	
lecommendation:  Certificate update				
terrificate update <ul> <li></li></ul>			characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.	
Master username Info         Type a legis ID for the master user of your DB instance.         kong         1 to 14 alphanumeric characters. First character must be a letter.         Auto generate a password         Amazen IBDS can generate a password for you, or you can specify your own password.         Master password info         constraints: At least B printable ASCII characters. Curt centain any of the following: / blackbi, 'birable quotel, 'birable quotel, 'distuble quotel, and generate a password.	-		T Credentials Settions	
Type a login ID for the misster user of your DB instance.   kong  To 16 alphanumeric characters. First character must be a letter.  Auto generate a password Anison RIGG any generate a password for your on password.  Master password info  Centralities. At least 8 printable ASCII characters. Cart contain any of the following: / Islandi, "Visuality quote," Visuality quote, "Visuality quote," of passible quote, "Visuality quote," of passible quote, "Visuality quote," Visuality quote, "Visuality quote," Visuality quote, "Visuality quote," Visuality quote, "Visuality quote," Visuality, "Visuality," Visuality, "Visuality," Visuality, "Visuality, "Visuality," Visuality, "Visuality," Visuality," Visuality, "Visuality," Visuality," Visuality, "Visuality," Visuality," Visuality, "Visuality," Visuality, "Visuality," Visuality, "Visuality," Visuality, "Visuality," Visuality, "Visuality," Visuality," Visuality, "Visuality," Visuality," Visuality," Visuality," Visuality," Visuality," Visual	Jertimoate update			
T to 16 alphanumeric character. First character must be a letter.  Auto generate a password Amazen RBS can generate a password for you, or you can specify your own password.  Master password Info  Centralnes. At least 8 printable ASCII characters. Cart centain any of the following: / bladd, 'bingle quote,' (double quote,) and ge				
Auto generate a password     Ansaun RDS can generate a password for you, or you can specify your own password.  Master password info			kong	
Amazon RUS can generate a password for you, or you can specify your own password.  Master password field  Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (sizah), "birgle quote," (double quote) and ge			1 to 16 alphanumeric characters. First character must be a letter.	
Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / biach], 'binging quotes], 'tidouble quotes] and ga				
Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (sizeh), "birglie quote), "bidouble quote), and go			Master password Info	

Ensure that the default settings for "DB instance size" and "Storage" are selected.

Depending on the cluster size and data requirements, select the appropriate DB instance size and storage type.

Based on our use case, we have chosen the following configuration:

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

Services	Q Search [Option+S]
Instarr	
	e configuration ance configuration options below are limited to those supported by the engine that you selected above.
DB instan	ce class Info
Standa	ard classes (includes m classes)
O Memo	ry optimized classes (includes r classes)
Complete	ute optimized classes (includes c classes)
db.m5d. 8 vCPUs	2xlarge     The second se
Storage	
Storage ty Provisioned	/pe Info IOPS SSD (io2) storage volumes are now available.
	red IOPS SSD (io2) v, highly durable, I/O intensive storage
Allocated	storage Info
400	GiB
The minimu	m value is 100 GiB and the maximum value is 65,536 GiB
	er you modify the storage for a DB instance, the status of the DB instance will be in storage-optimization ur instance will remain available as the storage-optimization operation completes. Learn more 🗹
Provisione	ed IOPS Info
3000	© IOPS
The minimu	m 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

Select appropriate values according to your use case. We have selected the default values.

Services	Q Search	[Option+S]								
Connec	tivity Info		C							
Choose wh	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 data	<ul> <li>Don't connect to an EC2 compute resource</li> <li>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.</li> </ul>									
	Virtual private cloud (VPC) Info Choose the VPC. The VPC defines the virtual networking environment for this DB cluster.									
	2az123001nd (vpc-055eca9021e79cfc7) ts, 3 Availability Zones	~								
	with a corresponding DB subnet group are listed.									
		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 select bpasubnetgroup 2 Subnets, 2 Availability Zones								
Choose the bpasubr	DB subnet group. The DB subnet group defines which su etgroup	ubnets and IP ranges the DB cluster can use in	the VPC that you selecte							
Choose the bpasubr 2 Subnets	DB subnet group. The DB subnet group defines which su etgroup	s) for the Multi-AZ DB Edit	the VPC that you selecter							
Choose the bpasubr 2 Subnets M Th clu sul Public acc O Yes RDS as cluster. can cor	DB subnet group. The DB subnet group defines which su etgroup , 2 Availability Zones e DB subnets must be in 3 Availability Zones (AZ ster. The current subnets are in <b>2 AZs (us-west-</b> onet in a different AZ than the current subnets.	s) for the Multi-AZ DB Edit 2a ,us-west-2b). Add a	t new subnet 🖸							
Choose the bpasubr 2 Subnets Th clu sul Public acc O Yes RDS as cluster. can cor	DB subnet group. The DB subnet group defines which su etgroup , 2 Availability Zones e DB subnets must be in 3 Availability Zones (AZ ster. The current subnets are in <b>2 AZs (us-west-</b> onet in a different AZ than the current subnets. ess Info iigns a public IP address to the cluster. Amazon EC2 insta Resources inside the VPC can also connect to the cluster	s) for the Multi-AZ DB Edit 2a ,us-west-2b). Add a ances and other resources outside of the VPC of the VPC security groups that con EC2 instances and other resources inside the	t new subnet [2]							
Choose the bpasubr 2 Subnets Th clu sub Public acc O Yes RDS as cluster. can cor No RDS do your clu	DB subnet group. The DB subnet group defines which su etgroup , 2 Availability Zones e DB subnets must be in 3 Availability Zones (AZ ster. The current subnets are in <b>2 AZs (us-west-</b> conet in a different AZ than the current subnets. ess Info signs a public IP address to the cluster. Amazon EC2 insta Resources inside the VPC can also connect to the cluster nect to the cluster. esn't assign a public IP address to the cluster. Only Amaz ister. Choose one or more VPC security groups that speci ity group (firewall) Info or more VPC security groups to allow access to your date	s) for the Multi-AZ DB Edit 2a ,us-west-2b). Add a ances and other resources outside of the VPC of the VPC security groups that con EC2 instances and other resources inside the fy which resources can connect to the cluster.	t new subnet [2]							

Make sure in "Database authentication" we have selected Password authentication. Authenticates using database passwords.

Understand       Interface         Use severe cardinate 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 cardinate that is automatically installed on all databases that you provision.         If you don't select a cardinate that is automatically installed on all databases that you provision.       Image: Content of the second	5	Ⅲ	Services	Q Search	[Option+S]							
rds-ca-rsa2048-g1 (default)         Expiry: May 25, 2061         If you don't select a certificate authority, RDS chooses one for you.         v         Additional configuration         Database port info         TCP/IP port hat 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 options info         • Password authentication         Autenticates using thatbase 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 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)         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)         Authenticates using the database password and user credentials through AWS IAM users and roles.         • P			Using a serve	er certificate provides an extra layer of secur								
Expiry: May 25, 2061   If you don't select a certificate authority, RDS chooses one for you. <ul> <li>✓ Additional configuration</li> </ul> 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 potions   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 AVS IAM users and roles.   Password and IAM database password and user credentials through AVS IAM users and roles.   Password and Kerberos authentication (not available for Multi-AZ DB cluster)   Authenticates using the database password and user credentials through AVS IAM users and roles.   Password and Kerberos authentication (not available for Multi-AZ DB cluster)   Authenticates using the database password and user credentials through AVS IAM users and roles.   Password and Kerberos authentication (not available for Multi-AZ DB cluster)   Authenticates using the database password and user credentials through AVS IAM users and roles.					y installed on all databases that you provision.							
• Additional configuration    Database port info   TC/IP port that the database will use for application connections.   5432 <b>Tags - optional</b> 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. <b>Database authentication Database authentication</b> Mutenticates using database passwords. Password and IAM database password and user credentials through AWS IAM uses and roles. Password and IAM database password and user credentials through AWS IAM uses and roles. Password and IAM database password and user credentials through AWS IAM uses and roles. Password and IAM database password and user credentials through AWS IAM uses and roles. Password and IAM database password and user credentials through AWS IAM uses and roles. Password and Karberos authentication (not available for Multi-AZ DB cluster) Choose a directory in which you want to allow authorized users to authenticate with this DB			•									
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 options Info   Database authentication   Database authentication   Mutenticates using database passwords.   Password and IAM database apasword and user credentials through AWS IAM users and roles.   Password and Kerberos 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)   Authenticates using the database database database database for Multi-AZ DB cluster)   Authenticates using the database data												
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 options Info         Password authentication         Authenticates using thatabase passwords.         Password and IAM 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		1	Additional configuration									
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					unactions							
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) Authenticates using the database password and user credentials through AWS IAM users and roles.												
A tag consists of a case-sensitive key-value pair.  A tag consists of a case-sensitive key-value pair.  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												
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) Authenticates using the database password and user credentials through AWS IAM users and roles.												
No tags associated with the resource.          Add new tag         You can add up to 50 more tags.         Database authentication         Database authentication options Info         Question options Info         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			-									
Add new tag         You can add up to 50 more tags.         Database authentication         Database authentication options Info         O 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			A tag consist	ts of a case-sensitive key-value pair.								
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			No tags as	sociated with the resource.								
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			Add no	w tag								
Database authentication         Database authentication options Info         O 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												
<ul> <li>Database authentication options Info</li> <li>Password authentication Authenticates using database passwords.</li> <li>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.</li> <li>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</li> </ul>		_										
<ul> <li>Database authentication options Info</li> <li>Password authentication Authenticates using database passwords.</li> <li>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.</li> <li>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</li> </ul>												
<ul> <li>Password authentication Authenticates using database passwords.</li> <li>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.</li> <li>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</li> </ul>			Databas	e authentication								
<ul> <li>Authenticates using database passwords.</li> <li>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.</li> <li>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</li> </ul>			Database a	authentication options Info								
<ul> <li>Authenticates using the database password and user credentials through AWS IAM users and roles.</li> <li>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</li> </ul>		1										
Choose a directory in which you want to allow authorized users to authenticate with this DB												
			Choose a	a directory in which you want to allow autho								

	cional configuration e options, encryption turned on, backup turned on, backtrack turned off, maintenance, CloudWatch Logs, delete protection on.
Databas	e options
Initial data	base name Info
Not supp	orted for Multi-AZ DB cluster
If you do no	t specify a database name, Amazon RDS does not create a database.
DB cluster	parameter group Info
default.p	ostgres16
Option gr	pup Info
Not supp	orted for Multi-AZ DB cluster
Creates Backup re	automated backups a point-in-time snapshot of your DB cluster tention period Info
Enable Creates Backup re	a point-in-time snapshot of your DB cluster
<ul> <li>Enable Creates</li> <li>Backup re The number</li> <li>7</li> <li>Backup with</li> </ul>	a point-in-time snapshot of your DB cluster tention period Info of days (1-35) for which automatic backups are kept.
Enable Creates     Backup re The number     7     Backup wi Select the p     Choose	a point-in-time snapshot of your DB cluster tention period Info of days (1-35) for which automatic backups are kept. days ndow Info eriod for which you want automated backups of the DB cluster to be created by Amazon RDS. e a window
<ul> <li>Enable Creates</li> <li>Backup re The number</li> <li>7</li> <li>Backup wi Select the p</li> </ul>	a point-in-time snapshot of your DB cluster tention period Info of days (1-35) for which automatic backups are kept. days ndow Info eriod for which you want automated backups of the DB cluster to be created by Amazon RDS. e a window
<ul> <li>Enable Creates</li> <li>Backup re The number</li> <li>7</li> <li>Backup wi Select the p</li> <li>Choose</li> <li>No pre</li> </ul>	a point-in-time snapshot of your DB cluster tention period Info of days (1-35) for which automatic backups are kept. days ndow Info eriod for which you want automated backups of the DB cluster to be created by Amazon RDS. e a window
<ul> <li>Enable Creates</li> <li>Backup re The number</li> <li>7</li> <li>Backup wi Select the p</li> <li>Choose</li> <li>No pre</li> </ul>	a point-in-time snapshot of your DB cluster tention period Info of days (1-35) for which automatic backups are kept. days andow Info eriod for which you want automated backups of the DB cluster to be created by Amazon RDS. a window ference ags to snapshots
<ul> <li>Enable Creates</li> <li>Backup re The number</li> <li>7</li> <li>Backup wi Select the p</li> <li>Choose</li> <li>No pre</li> <li>Copy t</li> <li>Encrypt</li> <li>Enable Choose</li> </ul>	a point-in-time snapshot of your DB cluster tention period Info of days (1-35) for which automatic backups are kept. days andow Info eriod for which you want automated backups of the DB cluster to be created by Amazon RDS. a window ference ags to snapshots
<ul> <li>Enable Creates</li> <li>Backup re The number</li> <li>7</li> <li>Backup wi Select the p</li> <li>Choose</li> <li>No pre</li> <li>Copy t</li> <li>Encrypt</li> <li>Enable Choose</li> </ul>	a point-in-time snapshot of your DB cluster tention period Info of days (1-35) for which automatic backups are kept. days ndow Info eriod for which you want automated backups of the DB cluster to be created by Amazon RDS. a window ference ags to snapshots to encryption to encrypt the given cluster. Master key IDs and aliases appear in the list after they have been created using the AWS Key ment Service (KMS) console. Info

aws	Services	Q Search	[Option+S]							
	Encrypti	ion								
	Choose	encryption to encrypt the given cluster. Master key IDs and aliases appear in the list after they have ment Service (KMS) console. Info	ave been created u	ising the AWS Key						
	AWS KMS	key Info								
	(default)	aws/rds	•							
	Account 19367046	3418								
	KMS key II 61e6c956-	D -745e-42be-8fd1-77953104ad4f								
	Log exp	orts								
	Select the lo	pg types to publish to Amazon CloudWatch Logs								
	Postgree     Upgrace	eSQL log de log								
	IAM role The followin	ng service-linked role is used for publishing logs to CloudWatch Logs.								
	RDS serv	ice-linked role								
	Mainten	ance								
	Auto minor	version upgrade Info								
	Enabling	auto minor version upgrade g auto minor version upgrade will automatically upgrade to new minor versions as th d. The automatic upgrades occur during the maintenance window for the database.	ey are							
		nce window Info eriod you want pending modifications or maintenance applied to the database by An	nazon RDS.							
	⊖ Choose	e a window								
	No presidente	ference								
	Deletion protection									
		deletion protection s the database from being deleted accidentally. While this option is enabled, you can'	t delete the databa	ase cluster.						
	③ 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						

Once that is verified, we are ready to create the database. Return to the Amazon RDS dashboard. Confirm that the instance is available for use.

# **Security Group Rules**

Update the inbound security group with the pod CIDR and node CIDR block.

Inbo	und rules (2)						C	Manage tags	Edit inbound r	ules
٩.	Search								< 1 >	0
0	Name	▼	Security group rule $\nabla$	IP version	⊽   Туре	▼   Protocol	♥ Port range	▽	Source	▽
0	-		sgr-0962e7821f1df7ede	IPv4	All traffic	All	All			
0	-		sgr-047daa40317c616	IPv4	All traffic	All	All			

# In RDS -> Databases -> DB-NAME, click configuration and refer the Parameter Group section and click the parameter group to view.

Amazon RDS ×	RDS > Databases > bpa-postgresql			
Dashboard Databases	bpa-postgresql			Modify Actions V
Query Editor Performance insights	Summary			
Snapshots Automated backups Reserved instances Proxies	DB identifier bpa-postgresgi Role Instance	CPU IIIIII.0.10% Current activity IIIIIII.0.07 sessions	Status Ø Available Engine Postger/SQL	Class db.t4g.large Region & AZ us-west-1b
Subnet groups Parameter groups Option groups	Connectivity & security Monitoring Logs & events	Configuration Maintenance & backups Tags		· )
	Instance			
Events Event subscriptions	Configuration	Instance class	Storage	Performance Insights
Recommendations 3	DB instance ID bpa-postgresql	Instance class db.t4g.large	Encryption Enabled	Performance insights enabled Turned on
Certificate update	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	Storage 20 GiB	Published logs
	Option groups default postgres-13 🕑 In sync	Master username kong	Provisioned IOPS	CloudWatch Logs PostgreSQL Upgrade
	Amazon Resource Name (ARN) amawsindsius-west-1:260251831100:dbibpa-postgresql	IAM DB authentication Not enabled	Storage autoscaling Enabled	Database activity stream
	Resource ID db-CUGRSST82842APGH22CVJ45DAM	Multi-AZ Yes	Maximum storage threshold 100 GiB	Stopped Audit policy status
	Created time July 31, 2022, 15:22 (UTC+05:30)	Secondary Zone us-west-1c		
	Parameter group bpa-postgresql-20220731094942083200000001 🕑 In sync			
Feedback Looking for language selection? Fin	Deletion protection			Amazon Web Services. Inc. or its affiliates. Privacy Terms Cookie preference

Search for "password\_encryption" and change the value to md5 from blank / other value. This is needed for camunda configurations to work.

Database Openy Giany Strainance Insights Stagistics     Parameters       Automated Instances Preses     Image: Im									000001				Parameter groups >		Amazon RDS ×		
Automated backups     Rearred instances     Modeliable v     Source v     Apply type v     Data type v     Data type v     Description       Rearred instances     Provides     mdS     mdS, scam-sha-256     true     system     dynamic     string     Encrypt password, scorption       Subret groups     rds.accepted_password_unoh_method     mdS+scam     mdS+scam     true     system     dynamic     string     Force autoentions with password, string method       Subret groups     rds.accepted_password_unoh_method     mdS+scam     mdS+scam     true     system     dynamic     bolean     restricts password-restrict password-restrict commands to method       Parameter groups     Option groups     C     Face autoenticts     0,1     true     system     static     bolean     restricts password-restrict commands to method       Parameter groups     Option groups     C     Face autoenticts     Tue     static     bolean     restricts password-restrict passwo	Edit parameters							×	:						Query Editor Performance insights		
Image: served energy for an end of			Description	Data type 🔍	Apply type 🔍	Source 🔍	Modifiable 🔻		owed values	. v	v Values		Name	•			
Image: State of groups       Image: State of groups       Image: State of groups       0, 1       Tue			Encrypt passwords.	string	dynamic	system	true		5, scram-sha-256		md5	tion	password_encryption	•			
Spelan groups Option groups Option groups Cvents Cvents States and the cvents Time Total System notes	stored locally	or connections with password stored local	Force authentication for connecti	string	dynamic	system	true		5+scram, scram	scram	md5+sc	sword_auth_method	rds.accepted_passwo		Tunes		
Recent events         Q. //terr db events           Vents         Time         V           Time         V         System notes	of rds_password	ted commands to members of rds_passwo	restricts password-related comm	boolean	static	system	true					vord_commands	rds.restrict_password		Subnet groups		
Vertis Vert subscriptions	C														Option groups		
vent subscriptions Time v System notes	< 1 >	< 1	<														
								System notes						Time			
connectations 0			No events found.														

Create these Databases along with users by connecting to the RDS.

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=WOrkFlo#ChangeNow WFE\_DB\_NAME=process-engine

• Password authentication

Authenticates using database passwords.

Atlas MongoDB Setup
 Setting up Atlas MangaDB in

Setting up Atlas MongoDB involves:

- Logging into Atlas MongoDB.
- Selecting the organization and project.
- Creating a dedicated cluster with the appropriate specifications.

IN ALL AND STROAT & OPPLIANCES	
Q. Find a database deployment	+ Create

• Select the Dedicated tier, Cloud Provider & Region.

Cloud Provider & Region		AWS, N. Virginia (us-east-1) 🔺
aws	Cloud Azure	
Distribute d	ata across clouds ﷺ ⚠ Morkload Is erformance, or introduce read-only and a	mproved availability and
★ Recommended region ①	on data currently unavailable 🕄	AUSTRALIA
▶ N. Virginia (us-east-1) ★	Stockholm (eu-north-1) 🖈	📰 Sydney (ap-southeast-2) ★
■■ Ohio (us-east-2) ★	📕 📕 Ireland (eu-west-1) 🚖	芦 Melbourne (ap-southeast-4) 🚖

 Select appropriate tier(we have used M30 as tier) dedicated cluster and provide appropriate cluster name and click on Create Cluster. It will initialize the Atlas monogodb cluster.

	V-EKS Connect V	iew Monitoring Bro	wse Collections					0	DEDICATE
Connect		• R 1.8	0	Connections 50.0		In 4.1 KB/s	0	Disk Usage 5.5 GB	
nteract with	your data using the	• W 0.2 Last 6 hours		Last 6 hours		Out 22.3 KB/s		Last 18 days	
MongoDB d	rivers or shell.	1.9/s		52.0		23.1 KB/s		40.0 GB	
Dismiss	Connect								
FRSION	REGION	CLUSTER TIER	ТҮРЕ	BACKUPS	LINKED APP SERVICES	S ATLAS SQL O	NLINE ARCHIVE	ATLAS SEARCH	

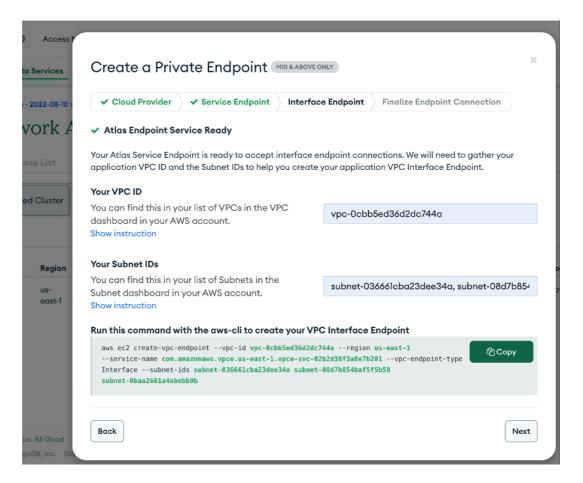
- Setting up VPC private endpoint for the Atlas and K8S cluster.
  - Click on the Network Access Select Private Endpoint à Click on Add Private Endpoint.

Database	Network Access
Data Lake PREVIEW	IP Access List Peering Private Endpoint
SERVICES	
Triggers	Dedicated Cluster Serverless Instance Federated Database Instance / Online Archive
Data API	
Data Federation	
Search	
Backup	$\bigcirc$
Database Access	- dD
Network Access	Create a Private Endnaint
Advanced	Create a Private Endpoint
	Configure AWS PrivateLink, Google Cloud Private Service Connect, or Azure Private
New On Atlas 1	Link to connect to your cluster.
Goto	Add Private Endpoint
	Learn More

• Select Cloud Provider as AWS, select respective Region and click on Next.

rg Y O Acces	55 1				All Clusters Get Help 👻 👘 👻
Data Services	Create a Private Er	ndpoint (MIO & ABOVE ONLY)		×	2, <i>9,</i> 4
We are deploying y	ou ✓ Cloud Provider Service	Endpoint VInterface Endpoint	Finalize Endpoint Connection		
P Mint DJ.>++ 2022-08-1	a) Atlas Region				
Network	A Select Atlas Region	== N. V	/irginia (us-east-1) ★	•	
		ext, you will be billed hourly for each and the Standard Load Balancers			
Dedicated Cluster	Back			Next	+ ADD PRIVATE ENDPOINT
Cloud Provider Re	gion Atlas Endpoint Service	Atlas Endpoint Service Status	Endpoint	Endpoint Status	Actions
AWS us	-east-1	<ul> <li>Creating private link</li> </ul>		Not Configured	EDIT

 Provide Respective PVC id and subnet ids. Once you enter the details, Copy the vpc end point creation command and execute it in aws console. You will get the vpc endpoint id as output.



Click on Next to paste the VPC endpoint ID and click on Create.

	dpoint 🔷 🛩 Interface Endpoint	Finalize Endpoint Connect
In order to verify and finalize your End	point Connection, we need to colled	et your VPC Endpoint ID.
Your VPC Endpoint ID This is a 22-character alphanumeric this in the AWS Endpoints Dashboar		XXXXX
Endpoints / Details / Endpoint ID. Show instruction		
Back		(
com.amazonaws.vpce.us-east-l.vpce-svc-	Available	
02b2d38f3a8e7b201		

• Once it is successfully created, Endpoint status will be Available as shown in the next picture. VPC end-point must be created for pod cidr. In our case we have used "100.64.0.0/16".

O Acces	Manager * Billing			All Clusters	Get Help *		•
: Data Services	App Services Charts					íl.	-
€7 2022-08-10	> PROJECT 0						
Network	Access						
IP Access List	Peering Private Endpoint						
Dedicated Cluster	Serverless Instance Federated Database Instance / Online Archive						
					+ ADD PRIVAT	FE ENDPO	INT
Cloud Provider Region	Atlas Endpoint Service	Atlas Endpoint Service Status	Endpoint	Endpoint Status	Actions		
AWS us- east-1	com.amazonaws.vpce.us-east-1.vpce-svc- 0680e789028623612	Available	vpce-07ef32fae7ef621a8	Available	EDIT	MINATE	)

 Add inbound rules to newly created vpc-endpoint. The vpc-endpoint will be in the parent account and a security group must be assigned to the newly created vpc-endpoint.

iditor	mation	EC2											_
s	ecurit	ty Groups (	1/4) Info				C Actions	▼ Export secu	rity group	os to CSV 🛛 🔻	Create s	ecurity group	,
	Q, Filts	ter security grou	ups									1 >	0
	search:	: mongo X	Clea	r filters									
		Name	v	Security group ID 🛛 🔍	Security group name 🛛	VPC ID	♥ Description ♥	Owner	v	Inbound rules co	ount 🗸	Outbound	rul
	2 -	-		sg-0f45d462e2f27acff	1 60 10/1	vpc-09bb2bb9c3849ff6f	10h	026208095312		2 Permission ent	ries	2 Permissio	ne
C	1 -	-		sg-Offa03a6242bf18c9	eks-cluster-sg-cs-ndc	vpc-09bb2bb9c3849ff6f 🖸	EKS created security gr	587310260078		5 Permission ent	ries	2 Permissio	ne
	1 -	-		sg-0b9a9bcce8363a3a9	MongoDB1-MongoDBI	vpc-09bb2bb9c3849ff6f 🖸	SG used for PC-Matrix	940203774588		11 Permission en	tries	1 Permission	n e
	) -			sg-05b0db05dcee573ec	MongoDB1-MongoDBI	vpc-09bb2bb9c3849ff6f	SG used for PC-mongo	940203774588		7 Permission ent	ries	1 Permissio	ne
	-Of45d4 Details	462e2f27acff s Inboun		ngo_db_SG Outbound rules Tags		-							
sg-	Details	s Inboun	id rules		nalyzer	-				Run Read	chability Ar		
sg-	Details	s Inboun	d rules	Outbound rules Tags	natyzer	-						nalyzer	
sg-	Details	s Inboun	d rules	Outbound rules Tags	nalyzer	-			Ø	Run Read			
s9-	Details	s Inboun	ed rules   ck network 2)	Outbound rules Tags	nalyzer	-			C		Edit in	nalyzer	<
59-	Details	s Inboun	ed rules   ck network 2)	Outbound rules Tags	nalyzer IP version 🛡	Туре. Ф	Protocol V	Port range			Edit in	nalyzer	<
59-	Details	s Inboun u can now chee und rules (2 ilter security gr	od rules ck network 2) roup rules	Outbound rules Tags			Protocol v TCP	Port range 0 - 65535	v ( s	Manage tags	Edit in	bound rules 1 > Description	<
59-	Oetails	s Inboun u can now cher und rules (2 itter security gr Name	od rules ck network 2) roup rules	Outbound rules Tags connectivity with Reachability A Security group rule, $v$	IP version $\nabla$	Туре у			v / s	Manage tags	Edit in <	halyzer >	<

### ECR as image registry

Creating Amazon ECR repositories and pushing Docker images into them involves several steps. These are the steps to create an ECR repository, tag a Docker image, and push it to the repository using the AWS CLI.

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

Replace:

- your-image-name with the desired name for your ECR repository.
- your-region with your AWS region

### **Configure IAM Role for EKS Nodes**

Ensure that the EKS worker nodes (EC2 instances) have the necessary IAM role attached with permissions to pull images from ECR. The IAM policy required is:

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

Attach this policy to the IAM role associated with your EKS worker nodes.

### **BPA Deployment**

The deployment of BPA involves several steps, including labeling EKS worker nodes, preparing directories on nodes, copying BPA packages, and deploying BPA using Helm.

For our customer deployment, we have utilized the following versions of software and cloud services:

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

These components ensure that our deployment is robust, scalable, and capable of handling the required workloads efficiently.

• Labeling EKS Worker Nodes

```
kubectl label node <worker_node_1> name=node-1
kubectl label node <worker_node_2> name=node-2
kubectl label node <worker_node_3> name=node-3
kubectl label node <worker_node_4> name=node-4
```

# • Preparing Directories on Nodes Node 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/kafka1
chmod 777 /opt/bpa/data/kafka1
sysctl -w vm.max_map_count=262144
```

```
Node 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/zookeeper2
chmod 777 /opt/bpa/data/zookeeper4
chmod 777 /opt/bpa/data/zookeeper5
```

### Node 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/zookeeper3
chmod 777 /opt/bpa/data/zookeeper4
chmod 777 /opt/bpa/data/zookeeper5
```

### Node 4:

mkdir -p /opt/bpa/data/elk mkdir -p /opt/bpa/data/metrices/prometheus mkdir -p /opt/bpa/data/metrices/grafana chmod 777 /opt/bpa/data/metrices chmod 777 /opt/bpa/data/metrices/prometheus chmod 777 /opt/bpa/data/metrices/grafana sysctl -w vm.max\_map\_count=262144

• Copying BPA Packages

scp	-r	packages	to	node1:/opt/bpa/
scp	-r	packages	to	<pre>node2:/opt/bpa/</pre>
scp	-r	packages	to	<pre>node3:/opt/bpa/</pre>
scp	-r	packages	to	<pre>node4:/opt/bpa/</pre>

• Deploying BPA Using Helm

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

### • Enabling Ingress

Update values.yamlto enable ingress:

ingress\_controller: {create: true}

### • Creating a Secret Using BPA Certificate

Navigate to the certificate directory and create a secret:

```
cd /opt/bpa/<BPA helm chart location>/bpa/conf/common/certs/
kubectl create secret tls bpa-certificate-ingress --cert=bap-cert.pem --key=bap-key.pem -n bpa-ns
```

### • Updating Ingress Controller

Add the newly created secret in the ingress-controller.yaml file:

```
cd /opt/bpa/<BPA helm chart location>/templates/
vi ingress-controller.yaml
"- --default-ssl-certificate=$(POD_NAMESPACE)/bpa-certificate-ingress"
```

### • Updating Ingress Certificate

Perform Helm delete and install to update the ingress certificate.

### **Environment Specifications**

The environment specifications include requirements for EC2 instances, load balancers, VPC endpoints, and RDS instances. Key specifications are:

### **EC2 Requirements:**

**Storage requirements:**2TB space per nodes. Mount EBS volume to /opt and add an entry in /etc/fstab for all the nodes.

Security group inbound: 30101, 443, 0 – 65535 TCP, 22 for ssh.

Security group outbound: All traffic must be enabled.

DNS Resolver: EC2 must have on-prem resolvers in /etc/resolve.conf.

### Load balancer requirements:

- Listeners ports must be 443, 30101.
- VPC End point Requirements (Atlas MongoDB).
- VPC end points created for Atlas connectivity is available in the parent account(aws-5g-ndc-prod). VPC Endpoint must have security group which allows all inbound access(0 65535).

### **RDS Requirements:**

**RDS Type**: db.r5b.2xlarge

**Postgres Engine version**: 13.7

Security group: Inboud must allow traffic from the POD CIDR source.

# **Key Concepts and Components**

Understanding Kubernetes fundamentals is essential for effectively deploying and managing applications using Amazon EKS.

# Conclusion

This paper provides a detailed guide for deploying and managing Business Process Automation (BPA) applications using Amazon EKS. By following the outlined steps and understanding the key concepts, organizations can leverage the benefits of EKS for their containerized BPA applications.

# References

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