

TASK = create a Amazon EKS (Elastic Kubernetes services)

NAME = Akshay choudhary

CDEC BATCH 24

Step 1

- Set up IAM ROLE for EKS
- Go to a IAM service and create a new role for eks

The screenshot shows the 'Add permissions' step in the AWS IAM console. At the top, a dropdown menu is set to 'EKS'. Below it, the text 'Choose a use case for the specified service.' is followed by 'Use case' options: 'EKS' (unchecked), 'EKS - Cluster' (checked), and 'EKS - Nodegroup' (unchecked). The 'EKS - Cluster' option is selected, and its description is 'Allows access to other AWS service resources that are required to operate clusters managed by EKS.' Below this, the breadcrumb 'IAM > Roles > Create role' is shown. The left sidebar indicates 'Step 2: Add permissions'. The main area is titled 'Add permissions' and shows 'Permissions policies (1)'. A table lists the policy 'AmazonEKSServiceRolePolicy' with the type 'AWS managed'.

Policy name	Type
AmazonEKSServiceRolePolicy	AWS managed

Step 2

Create a EKS cluster

- Open the amazon EKS console

Name

Enter a unique name for this cluster. This property cannot be changed after the cluster is created.



EKS cluster

The cluster name should begin with letter or digit and can have any of the following characters: the set of Unicode letters, digits, hyphens and underscores. Maximum length of 100.

Kubernetes version [Info](#)

Select Kubernetes version for this cluster.

1.29

 Kubernetes version 1.29 reaches the end of standard support on March 23, 2025. If you don't update your cluster to a later version before that date, it will automatically enter extended support. After the extended support preview ends, clusters on versions in extended support will be subject to additional fees. [Learn more](#) .

Cluster service role [Info](#)

Select the IAM role to allow the Kubernetes control plane to manage AWS resources on your behalf. This property cannot be changed after the cluster is created. To create a new role, follow the instructions in the [Amazon EKS User Guide](#) .

shashank-EKS-role



Cluster access [Info](#)

Control how IAM principals can access this cluster.

Bootstrap cluster administrator access [Info](#)

Choose whether the IAM principal creating the cluster has Kubernetes cluster administrator access.

☒ **Allow cluster administrator access**
Allow cluster administrator access for your IAM principal.

☐ **Disallow cluster administrator access**
Disallow cluster administrator access for your IAM principal.

Cluster authentication mode [Info](#)

Configure which source the cluster will use for authenticated IAM principals.

- ☐ **EKS API**
The cluster will source authenticated IAM principals only from EKS access entry APIs.
- ☒ **EKS API and ConfigMap**
The cluster will source authenticated IAM principals from both EKS access entry APIs and the aws-auth ConfigMap.
- ☐ **ConfigMap**
The cluster will source authenticated IAM principals only from the aws-auth ConfigMap.

Specify networking

Networking [Info](#)

IP address family and service IP address range cannot be changed after cluster creation.

VPC [Info](#)

Select a VPC to use for your EKS cluster resources. To create a new VPC, go to the [VPC console](#).

vpc-025eacd99f6367260 | Default

Subnets [Info](#)

Choose the subnets in your VPC where the control plane may place elastic network interfaces (ENIs) to facilitate communication with your cluster. To create a new subnet, go to the corresponding page in the [VPC console](#).

Select subnets

subnet-0af1e89c160bc4732
ap-northeast-2c 172.31.32.0/20

subnet-0d8c89837a0b05753
ap-northeast-2a 172.31.0.0/20

subnet-0666b57b24916eaa3
ap-northeast-2b 172.31.16.0/20

subnet-02d4d668bdbba8cd
ap-northeast-2d 172.31.48.0/20

Security groups [Info](#)

Choose the security groups to apply to the EKS-managed Elastic Network Interfaces that are created in your control plane subnets. To create a new security group, go to the corresponding page in the [VPC console](#).

Select security groups

sg-0442dc058691fb188

Choose cluster IP address family [Info](#)

Specify the IP address type for pods and services in your cluster.

☒ IPv4

☐ IPv6

☐ Configure Kubernetes service IP address range [Info](#)

Specify the range from which cluster services will receive IP addresses.

Cluster endpoint access [Info](#)

Configure access to the Kubernetes API server endpoint.

☒ Public

The cluster endpoint is accessible from outside of your VPC. Worker node traffic will leave your VPC to connect to the endpoint.

☐ Public and private

The cluster endpoint is accessible from outside of your VPC. Worker node traffic to the endpoint will stay within your VPC.

☐ Private

The cluster endpoint is only accessible through your VPC. Worker node traffic to the endpoint will stay within your VPC.

► Advanced settings

Cancel

Previous

Next

Configure observability

► About observability


Metrics

Prometheus [Info](#)

- ☐ Send Prometheus metrics to Amazon Managed Service for Prometheus
Monitor your application and infrastructure metrics with Amazon Managed Service for Prometheus. These metrics include system health and performance data.

 Agentless Prometheus metrics collection requires the cluster API server to be available privately. To make the following toggle available, select either the Public and private option or the Private option for Cluster endpoint access in Specify networking.

CloudWatch [Info](#)

 You can enable CloudWatch Container Insights in your clusters through the CloudWatch Observability add-on. After your cluster is created, navigate to the add-ons tab and install CloudWatch Observability add-on to enable Container Insights and start ingesting infrastructure telemetry into CloudWatch.

Control plane logging [Info](#)

Send audit and diagnostic logs from the Amazon EKS control plane to CloudWatch Logs.

- ☐ **API server**
Logs pertaining to API requests to the cluster.
- ☐ **Audit**
Logs pertaining to cluster access via the Kubernetes API.
- ☐ **Authenticator**
Logs pertaining to authentication requests into the cluster.
- ☐ **Controller manager**
Logs pertaining to state of cluster controllers.
- ☐ **Scheduler**
Logs pertaining to scheduling decisions.

Cancel

Previous

Next

Select add-ons

Review the add-ons from multiple categories, then select add-ons to enhance your cluster.

Amazon EKS add-ons (5) [Info](#)

CoreDNS [Info](#)

Enable service discovery within your cluster.

Category
networking

✔ Installed by default

kube-proxy [Info](#)

Enable service networking within your cluster.

Category
networking

✔ Installed by default

Amazon VPC CNI [Info](#)

Enable pod networking within your cluster.

Category
networking

✔ Installed by default

Amazon EKS Pod Identity Agent [Info](#)

Install EKS Pod Identity Agent to use EKS Pod Identity to grant AWS IAM permissions to pods through Kubernetes service accounts.

Category
security

Amazon GuardDuty EKS Runtime Monitoring [Info](#)

Install EKS Runtime Monitoring add-on within your cluster. Ensure to enable EKS Runtime Monitoring within Amazon GuardDuty.

Category
security

Cancel

Previous

Next

Configure selected add-ons settings

Configure the add-ons for your cluster by selecting settings.

CoreDNS [Info](#)

Category
networking

Status
✔ Installed by default

Version
Select the version for this add-on

v1.11.1-eksbuild.4

kube-proxy [Info](#)

Category
networking

Status
✔ Installed by default

Version
Select the version for this add-on

v1.29.0-eksbuild.1

Amazon VPC CNI [Info](#)

Category
networking

Status
✔ Installed by default

Version
Select the version for this add-on

v1.16.0-eksbuild.1

Amazon EKS Pod Identity Agent [Info](#)

Remove add-on

Category
security

Status
✔ Ready to install

Version
Select the version for this add-on

v1.2.0-eksbuild.1

Cancel

Previous

Next

Review and create

Step 1: Cluster

[Edit](#)

Cluster configuration

Name eks-services	Kubernetes version 1.29
Cluster service role arn:aws:iam::381492218806:role/shashank-EKS-role	Kubernetes cluster administrator access Allow cluster administrator access
Authentication mode EKS API and ConfigMap	

Tags (0)

Tags that you've added. Each tag consists of a key and an optional value.

[<](#) **1** [>](#)

Key	Value
No tags. This cluster does not have any tags.	

Step 2: Networking

[Edit](#)

Networking

These properties cannot be changed after the cluster is created.

VPC vpc-025eacd99f6367260	Subnets subnet-0af1e89c160bc4732 subnet-0d8c89637a0b05753 subnet-0666b57b24916eaa3 subnet-02d4d668bdbdba8cd	Security groups sg-0442dc058691fb188
Cluster IP address family IPv4		







Cluster endpoint access

API server endpoint access Public	Public access source allowlist 0.0.0.0/0
--------------------------------------	---

Step 3: Observability

[Edit](#)

- #set up IAM ROLES for ec2

<input type="checkbox"/>	Policy name ↗	Type	Attached entities
<input type="checkbox"/>	 AmazonEC2ContainerRegist...	AWS managed	2
<input type="checkbox"/>	 AmazonEKS_CNI_Policy	AWS managed	2
<input type="checkbox"/>	 AmazonEKSClusterPolicy	AWS managed	3
<input type="checkbox"/>	 AmazonEKSServicePolicy	AWS managed	2
<input type="checkbox"/>	 AmazonEKSVPCResourceCo...	AWS managed	1
<input type="checkbox"/>	 AmazonEKSWorkerNodePolicy	AWS managed	2

▶ **Permissions boundary** (not set)

```
[cloudshell-user@ip-10-2-29-13 ~]$ aws configure
[cloudshell-user@ip-10-2-29-13 ~]$ aws configure
AWS Access Key ID [None]: AKIAVRUVVJ03BFRKTUIY
AWS Secret Access Key [None]: LjjjG7FHsNbfBU+knVYyvu+3vqEZG40lA1qSdW3
Default region name [None]:
Default output format [None]:
[cloudshell-user@ip-10-2-29-13 ~]$
```

- Add the aws EKS console select your cluster
- In cluster go to the compute services

Review and create

Step 1: Cluster Edit

Cluster configuration

Name
eks-services

Cluster service role
arn:aws:iam::381492218806:role/shashank-EKS-role

Authentication mode
EKS API and ConfigMap

Kubernetes version
1.29

Kubernetes cluster administrator access
Allow cluster administrator access

Tags (0)
Tags that you've added. Each tag consists of a key and an optional value.

Key	Value
No tags. This cluster does not have any tags.	

Step 2: Networking Edit

Networking
These properties cannot be changed after the cluster is created.

VPC vpc-025eacd99f6367260	Subnets subnet-0af1e89c160bc4732 subnet-0d8c89837a0b05753 subnet-0666b57b24916eaa3 subnet-02d4d668bd8dba8cd	Security groups sg-0442dc058691fb188
------------------------------	---	---

Cluster IP address family
IPv4

Cluster endpoint access

API server endpoint access Public	Public access source allowlist 0.0.0.0/0
--------------------------------------	---

Step 3: Observability Edit

- Click on ADD node group
- Select the name & IAM ROLE

Configure node group Info

A node group is a group of EC2 instances that supply compute capacity to your Amazon EKS cluster. You can add multiple node groups to your cluster.

Node group configuration

These properties cannot be changed after the node group is created.

Name
Assign a unique name for this node group.

The node group name should begin with letter or digit and can have any of the following characters: the set of Unicode letters, digits, hyphens and underscores. Maximum length of 63.

Node IAM role Info
Select the IAM role that will be used by the nodes. To create a new role, go to the [IAM console](#).

EKSACROLEPOLICE ▼

↻

The selected role must not be used by a self-managed node group as this could lead to a service interruption upon managed node group deletion.

[Learn more](#)

Launch template Info

These properties cannot be changed after the node group is created.

☒ **Use launch template**
Configure this node group using an EC2 launch template.

Kubernetes labels Info

- On click next

These properties cannot be changed after the node group is created.

AMI type [Info](#)
Select the EKS-optimized Amazon Machine Image for nodes.

Amazon Linux 2 (AL2_x86_64) ▼

Capacity type
Select the capacity purchase option for this node group.

On-Demand ▼

Instance types [Info](#)
Select instance types you prefer for this node group.

Q Enter an instance type

t3.medium
vCPU: 2 vCPUs Memory: 4 GiB Network: Up to 5 Gigabit Max ENI: 3 Max IPs: 18 ✕

Disk size
Select the size of the attached EBS volume for each node.

20 GiB

Node group scaling configuration

Desired size
Set the desired number of nodes that the group should launch with initially.

2 nodes
Desired node size must be greater than or equal to 0

Minimum size
Set the minimum number of nodes that the group can scale in to.

2 nodes
Minimum node size must be greater than or equal to 0

Maximum size
Set the maximum number of nodes that the group can scale out to.

2 nodes
Maximum node size must be greater than or equal to 1 and cannot be lower than the minimum size

Node group update configuration [Info](#)

Maximum unavailable
Set the maximum number or percentage of unavailable nodes to be tolerated during the node group version update.

☒ Number
Enter a number

☐ Percentage
Specify a percentage

Value

1 node
Node count must be greater than 0.

Cancel Previous **Next**

-
- Click on the next
- Select the subnet

> Node groups > Add node group

Specify networking

Node group network configuration
These properties cannot be changed after the node group is created.

Subnets [Info](#)
Specify the subnets in your VPC where your nodes will run. To create a new subnet, go to the corresponding page in the [VPC console](#).

Select subnets:

subnet-0af1e89c160bc4732 X

subnet-0d8c89837a0b05753 X

subnet-0666b57b24916eaa3 X

subnet-02d4d668bdbba8cd X

☐ Configure remote access to nodes [Info](#)

Cancel Previous **Next**

- Click on the next & then create
- Go to the EC2 AWS console & check if your node is running\

Find Instance by attribute or tag (case-sensitive)								
All states								
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input type="checkbox"/>		i-08874a843d51bd5d7	Running	t3.medium	Initializing	View alarms	ap-northeast-2a	ec2-13-20
<input type="checkbox"/>		i-0e250c659beff9b440	Running	t3.medium	Initializing	View alarms	ap-northeast-2b	ec2-43-20

- Verify the cluster
- Open the cloudshell
- `#aws --region <region name> update --kubeconfig --name <cluster name>`

```
[cloudshell-user@ip-10-2-29-13 ~]$ kubectl cluster-info
-bash: kubectl: command not found
[cloudshell-user@ip-10-2-29-13 ~]$ kubectl cluster-info
Kubernetes control plane is running at https://11557140C09086821290C4578DC6A6.gr7.ap-northeast-2.eks.amazonaws.com
Docker is running at https://11557140C09086821290C4578DC6A6.gr7.ap-northeast-2.eks.amazonaws.com/api/v1/namespaces/kube-system/services/kube-apiserver/proxy
To further debug and diagnose cluster problems, use 'kubectl cluster-info dump'.
[cloudshell-user@ip-10-2-29-13 ~]$
```