

# Creating an Amazon EKS (Elastic Kubernetes Service) cluster

## 1. Set Up IAM Roles for EKS:

- Go to aws IAM Service and create a new role for eks.

The screenshot shows the 'Create role' page in the AWS IAM console, specifically Step 1: Select trusted entity. The left sidebar shows the navigation menu with 'IAM' selected, and 'Roles' and 'Create role' in the breadcrumb. The main content area is titled 'Select trusted entity' and includes an 'info' icon. Under 'Trusted entity type', there are five radio button options: 'AWS service' (selected), 'AWS account', 'Web identity', 'SAML 2.0 federation', and 'Custom trust policy'. Each option has a brief description. Below this, the 'Use case' section is titled 'Allow an AWS service like EC2, Lambda, or others to perform actions in this account.' It features a dropdown menu for 'Service or use case' with 'EKS' selected. Below the dropdown, it says 'Choose a use case for the specified service.' and 'Use case'. There are two radio button options: 'EKS' and 'EKS - Cluster' (selected). The 'EKS - Cluster' option has a description: 'Allows access to other AWS service resources that are required to operate clusters managed by EKS.'

The screenshot shows the 'Add permissions' page in the AWS IAM console, specifically Step 2: Add permissions. The left sidebar shows the navigation menu with 'IAM' selected, and 'Roles' and 'Add permissions' in the breadcrumb. The main content area is titled 'Add permissions' and includes an 'info' icon. Under 'Permissions policies (1)', it says 'The type of role that you selected requires the following policy.' Below this, there is a table with one row: 'Policy name' (AmazonEKSClusterPolicy) and 'Type' (AWS managed). Below the table, there is a section for 'AmazonEKSClusterPolicy' with a 'Copy JSON' button. The JSON policy is displayed in a code editor with line numbers 62 to 81. The policy allows the 'iam:createServiceLinkedRole' action on the resource '\*' with the condition 'StringEquals: iam:AWSServiceName: elasticloadbalancing.amazonaws.com'. At the bottom, there is a checkbox for 'Set permissions boundary - optional'. The bottom right corner has 'Cancel', 'Previous', and 'Next' buttons.

```
62     "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
63     "elasticloadbalancing:RegisterTargets",
64     "elasticloadbalancing:SetLoadBalancerPoliciesForBackendServer",
65     "elasticloadbalancing:SetLoadBalancerPoliciesOfListener",
66     "kms:DescribeKey"
67   },
68   "Resource": "*"
69 },
70 {
71   "Effect": "Allow",
72   "Action": "iam:createServiceLinkedRole",
73   "Resource": "*",
74   "Condition": {
75     "StringEquals": {
76       "iam:AWSServiceName": "elasticloadbalancing.amazonaws.com"
77     }
78   }
79 }
80 ]
81 ]
```

## 2. Create an EKS Cluster:

- Open the Amazon EKS console.
- Click on "Create cluster" and choose the "AWS Management Console" method.

EKS > Clusters > Create EKS cluster

Step 1  
Configure cluster

Step 2  
Specify networking

Step 3  
Configure observability

Step 4  
Select add-ons

Step 5  
Configure selected add-ons settings

Step 6  
Review and create

### Configure cluster

#### Cluster configuration [Info](#)

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

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](#) [↗](#).

AWS\_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.

#### Secrets encryption [Info](#)

Once turned on, secrets encryption cannot be modified or removed.

☒ **Turn on envelope encryption of Kubernetes secrets using KMS**  
Envelope encryption provides an additional layer of encryption for your Kubernetes secrets.

#### Tags (0) [Info](#)

No tags associated with the resource.

Add new tag

You can add up to 50 tags.

Cancel

Next

aws

Services

Search

[Alt+S]

ES

IAM

Extended support for Kubernetes versions pricing

New prices for extended support will start in the April billing cycle. For more information, see the [blog post](#).

EKS

>

Clusters

>

Create EKS cluster

Step 1

Configure cluster

Step 2

Specify networking

Step 3

Configure observability

Step 4

Select add-ons

Step 5

Configure selected add-ons settings

Step 6

Review and create

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-07c4b4fcb8e26ac1c | 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-0708607040050060b

us-east-2b

172.31.16.0/20

X

subnet-0a8d9eb2640519b4b

us-east-2c

172.31.32.0/20

X

subnet-08cc7bde8b1cd2b2a

us-east-2a

172.31.0.0/20

X

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-0050a2ffd29d4f6e1

X

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

aws

Services

Search

[Alt+S]

iam

Extended support for Kubernetes versions pricing

New prices for extended support will start in the April billing cycle. For more information, see the [blog post](#).

EKS

Clusters

Create EKS cluster

Step 1

Configure cluster

Step 2

Specify networking

Step 3

Configure observability

Step 4

Select add-ons

Step 5

Configure selected add-ons settings

Step 6

Review and create

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.

1

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

1

You can enable CloudWatch Observability 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 CloudWatch Application Signals and Container Insights and start ingesting 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

**Extended support for Kubernetes versions pricing**

New prices for extended support will start in the April billing cycle. For more information, see the [blog post](#).

[EKS](#) > [Clusters](#) > Create EKS cluster

Step 1

[Configure cluster](#)

Step 2

[Specify networking](#)

Step 3

[Configure observability](#)

Step 4

**Select add-ons**

Step 5

Configure selected add-ons settings

Step 6

Review and create

## 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](#)

aws

Services

Search

[Alt+S]

iam

Extended support for Kubernetes versions pricing

New prices for extended support will start in the April billing cycle. For more information, see the [blog post](#).

EKS > Clusters > Create EKS cluster

Step 1

Configure cluster

Step 2

Specify networking

Step 3

Configure observability

Step 4

Select add-ons

Step 5

Configure selected add-ons settings

Step 6

Review and create

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

aws

Services

Search

[Alt+S]

AP IAM

Controller manager  
off

Scheduler  
off

Step 4: Add-ons

Edit

Selected add-ons

Find add-on

< 1 >

Add-on name	Type	Status
coredns	networking	Installed by default
eks-pod-identity-agent	security	Ready to install
kube-proxy	networking	Installed by default
vpc-cni	networking	Installed by default

Step 5: Versions

Edit

Selected add-ons version

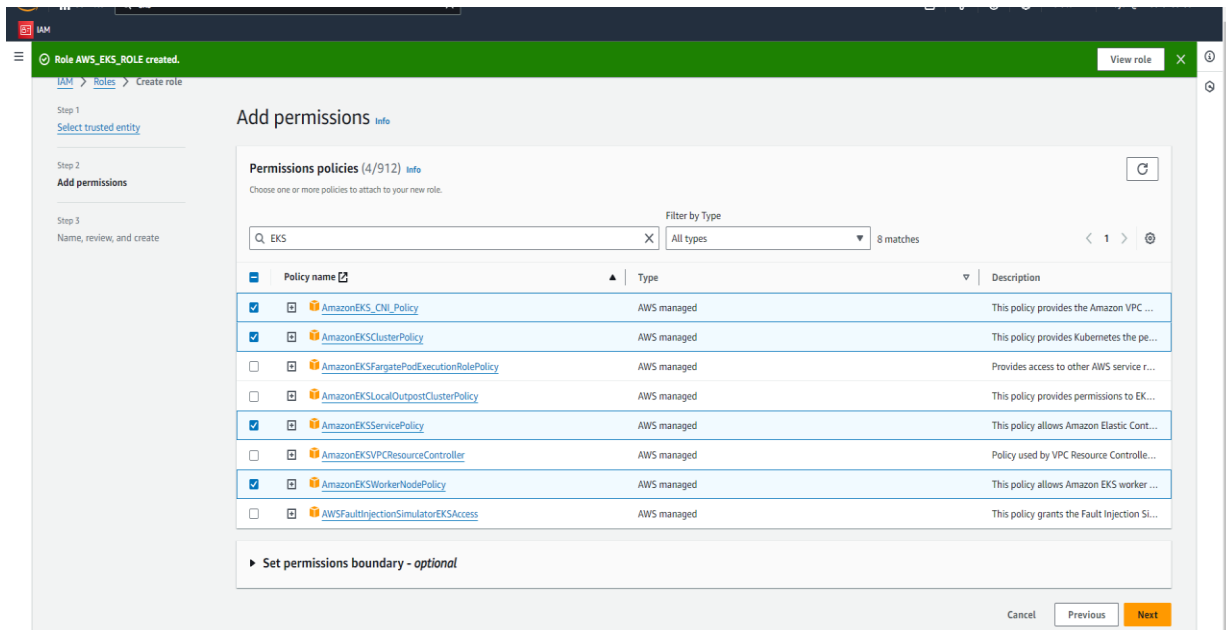
Add-on name	Version
coredns	v1.11.1-eksbuild.4
Add-on name	Version
kube-proxy	v1.29.0-eksbuild.1
Add-on name	Version
vpc-cni	v1.16.0-eksbuild.1
Add-on name	Version
eks-pod-identity-agent	v1.2.0-eksbuild.1

Cancel

Previous

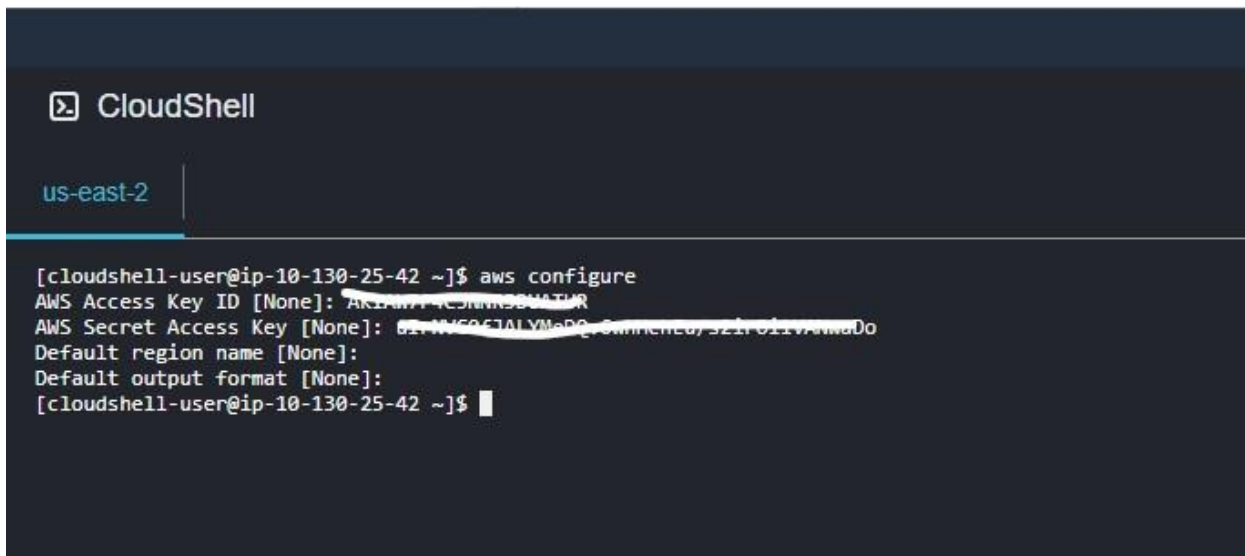
Create

### 3. Set Up IAM Roles for EC2:



#### 4. Configure the AWS Cloudshell:

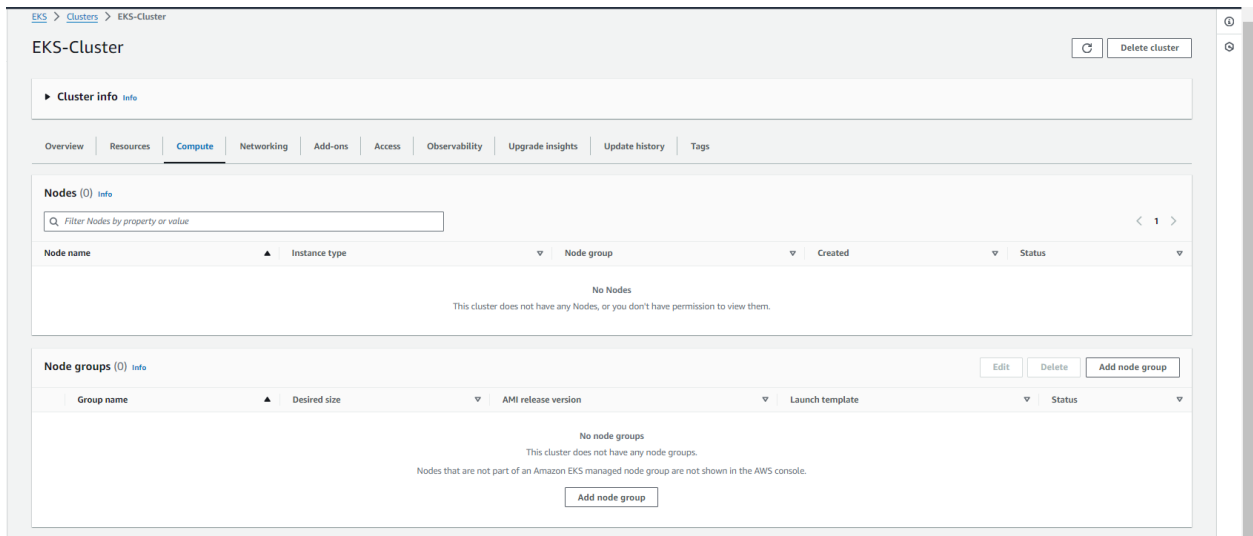
Open aws Cloud shell.



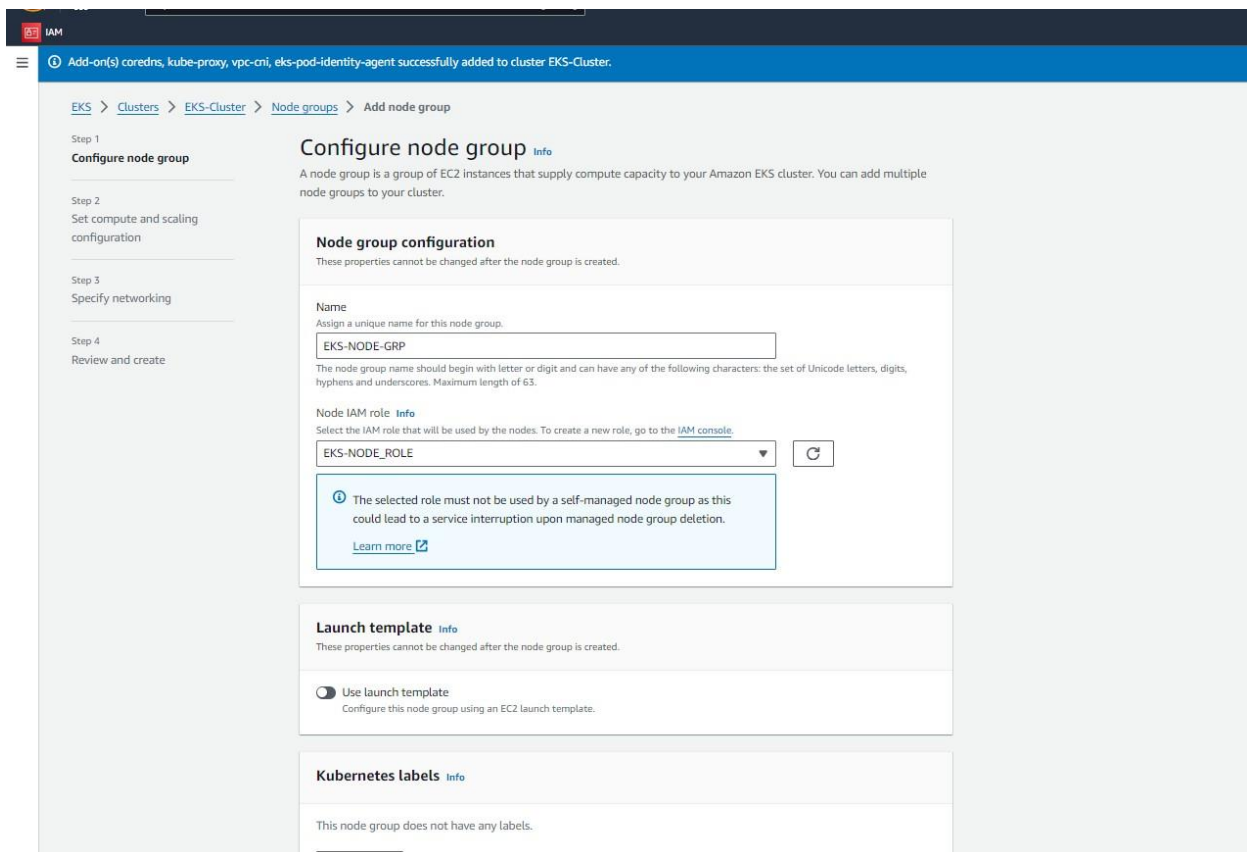
#### 5. Add Worker Nodes:

- In the AWS EKS console select your cluster.
- In Cluster go to compute service.





- Click on “Add Node Group”
- Select the “NAME” & “IAM ROLE”



- Click on Next
- Select the values for the node configuration as below

aws

Services

Q Search

[Alt+S]

iam

IAM

Step 2

Set compute and scaling configuration

Step 3

Specify networking

Step 4

Review and create

**Node group compute configuration**

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.

1 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.

1 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.

- Click on next
- Select the subnets

aws Services Search [Alt+S]

iam

Add-on(s) coredns, kube-proxy, vpc-cni, eks-pod-identity-agent successfully added to cluster EKS-Cluster.

EKS > Clusters > EKS-Cluster > Node groups > Add node group

Step 1  
Configure node group

Step 2  
Set compute and scaling configuration

Step 3  
Specify networking

Step 4  
Review and create

## 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-0708607040050060b X subnet-0a8d9eb2640519b4b X

subnet-08cc7bde8b1cd2b2a X

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

Cancel Previous Next

- Click on “next” and then “Create”
- Go to the EC2 AWS console & Check whether your node is running or not.

aws Services Search [Alt+S]

iam

EC2 Dashboard

EC2 Global View

Events

Instances

Instances (1) [Info](#)

Find instance by attribute or tag (case-sensitive) Running

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
	i-09e542ecc65e2d01c	Running	t3.medium	Initializing	View alarms	us-east-2c	ec2-3-16-108-120 us-e...	3.16.108.120	-

Launch instances

## 6. Verify the Cluster:

- Open Cloudshell and execute the following commands.

```
# aws eks --region <region> update-kubeconfig --name <cluster-name>
```

```
# kubectl cluster-info
```

```
[cloudshell-user@ip-10-130-25-42 ~]$ aws eks update-kubeconfig --r
[cloudshell-user@ip-10-130-25-42 ~]$ aws eks update-kubeconfig --region us-east-2 --name EKS-Cluster
Added new context arn:aws:eks:us-east-2:479954393947:cluster/EKS-Cluster to /home/cloudshell-user/.kube/config
[cloudshell-user@ip-10-130-25-42 ~]$ kubectl cluster-info
-bash: kubectl: command not found
[cloudshell-user@ip-10-130-25-42 ~]$ kubectl cluster-info
Kubernetes control plane is running at https://17f99EDAC682E4D0FB9D4226F2A3EEA7.gr7.us-east-2.eks.amazonaws.com
CoreDNS is running at https://17f99EDAC682E4D0FB9D4226F2A3EEA7.gr7.us-east-2.eks.amazonaws.com/api/v1/namespaces/kube-system/services/kube-dns:dns/proxy

To further debug and diagnose cluster problems, use 'kubectl cluster-info dump'.
[cloudshell-user@ip-10-130-25-42 ~]$
```