

Name : Nirmal Omkar Maruti

CDEC B-24

Task : 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 the EKS

The screenshot shows the 'Create role' wizard in the AWS IAM console, specifically Step 1: Select trusted entity. The left sidebar shows the progress: Step 1 (Select trusted entity), Step 2 (Add permissions), and Step 3 (Name, review, and create). The main content area is titled 'Select trusted entity' and includes a 'Trusted entity type' section with five options: AWS service (selected), AWS account, Web identity, SAML 2.0 federation, and Custom trust policy. Below this is a 'Use case' section with a dropdown menu set to 'EKS' and a 'Choose a use case for the specified service' section with three options: EKS (selected), EKS - Cluster, and EKS - Nodegroup. The bottom of the screen shows the 'Add permissions' step, which includes a table of 'Permissions policies (1)' with one entry: 'AmazonEKSClusterPolicy' of type 'AWS managed'. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity

Trusted entity type

- ☒ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☐ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EKS

Choose a use case for the specified service.

Use case

- ☒ EKS
Allows EKS to manage clusters on your behalf.
- ☐ EKS - Cluster
Allows access to other AWS service resources that are required to operate clusters managed by EKS.
- ☐ EKS - Nodegroup

Permissions policies (1)

The type of role that you selected requires the following policy.

Policy name	Type
AmazonEKSClusterPolicy	AWS managed

Set permissions boundary - optional

Cancel Previous Next

Nirmal Omkar M.

[IAM](#)

>

[Roles](#)

>

Create role

Step 1

[Select trusted entity](#)

Step 2

[Add permissions](#)

Step 3

Name, review, and create

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

shashank-eks-role

Maximum 64 characters. Use alphanumeric and "+,=,@,-" characters.

Description

Add a short explanation for this role.

Allows access to other AWS service resources that are required to operate clusters managed by EKS.

Maximum 1000 characters. Use alphanumeric and "+,=,@,-" characters.

Step 1: Select trusted entities

Trust policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": {
7         "Service": [
8           "eks.amazonaws.com"
9         ]
10      },
11      "Action": "sts:AssumeRole"
12    }
13  ]
14 }
```

2. Create an EKS cluster.

- Open the Amazon EKS console.
- Click on “Create Cluster” and choose the “AWS management Console” method.

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 cluster

Cluster configuration

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

Kubernetes version
Select Kubernetes version for this cluster.
1.29

Cluster service role
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
Control how IAM principals can access this cluster.

Bootstrap cluster administrator access
Choose whether the IAM principal creating the cluster has Kubernetes cluster administrator access.
☒ Allow cluster administrator access
☐ Disallow cluster administrator access

Cluster authentication mode
Configure which source the cluster will use for authenticated IAM principals.
☐ EKS API
☒ EKS API and ConfigMap
☐ ConfigMap

Secrets encryption
Once turned on, secrets encryption cannot be modified or removed.
☒ Turn on envelope encryption of Kubernetes secrets using KMS

Tags
No tags associated with the resource.
Add new tag

Cancel Next

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

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-0f692367e7315726d | 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-0b975bf6e85fbf6ac | us-west-1a | 172.31.0.0/20

subnet-04a74a5846c4c229c | us-west-1b | 172.31.16.0/20

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-00347fd4666ef2e2

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

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

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

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

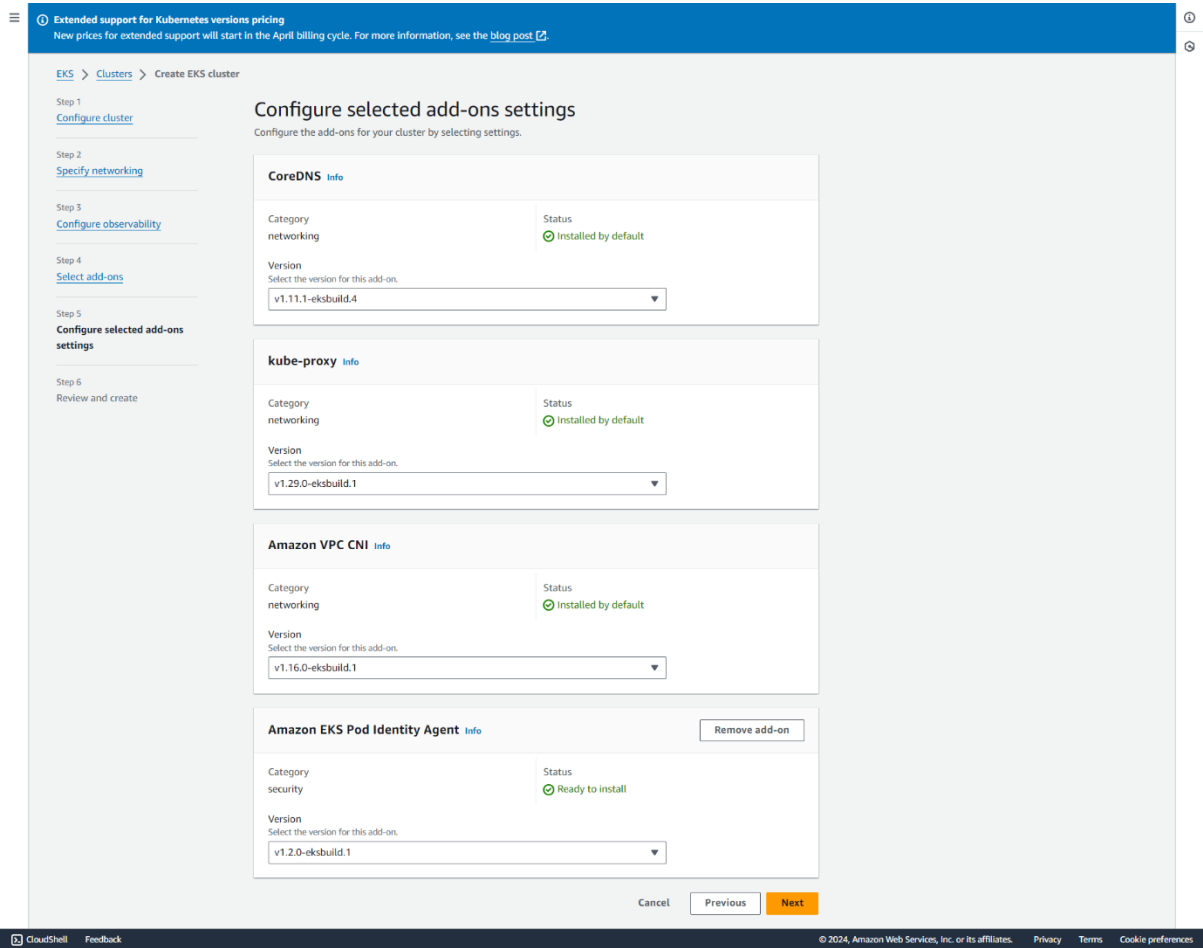
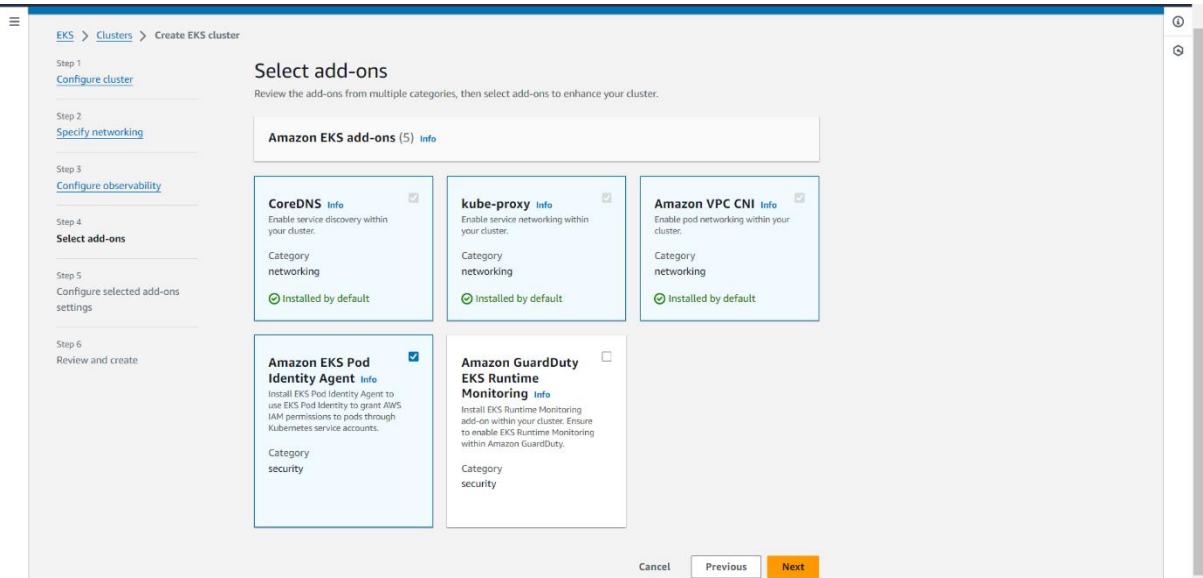
Previous

Next

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)



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

Review and create

Step 1: Cluster

Edit

Cluster configuration

Name	shashank-eks-cluster	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	Subnets	Security groups
vpc-0f692367e7315726d	subnet-0b975bf6e85fbfeac subnet-04a74a5846e4c229c	sg-00347fdf46666f2e2
Cluster IP address family	IPv4	

Cluster endpoint access

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

Step 3: Observability

Edit

Control plane logging

API server	Audit	Authenticator
off	off	off
Controller manager	Scheduler	
off	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

CloudShell

Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Nirmal Omkar M.

3. Set up IAM roles for EC2.

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

☒ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case
EC2

Choose a use case for the specified service.
Use case

☒ EC2
Allows EC2 instances to call AWS services on your behalf.

☐ EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

☐ EC2 Spot Fleet Role

15
16

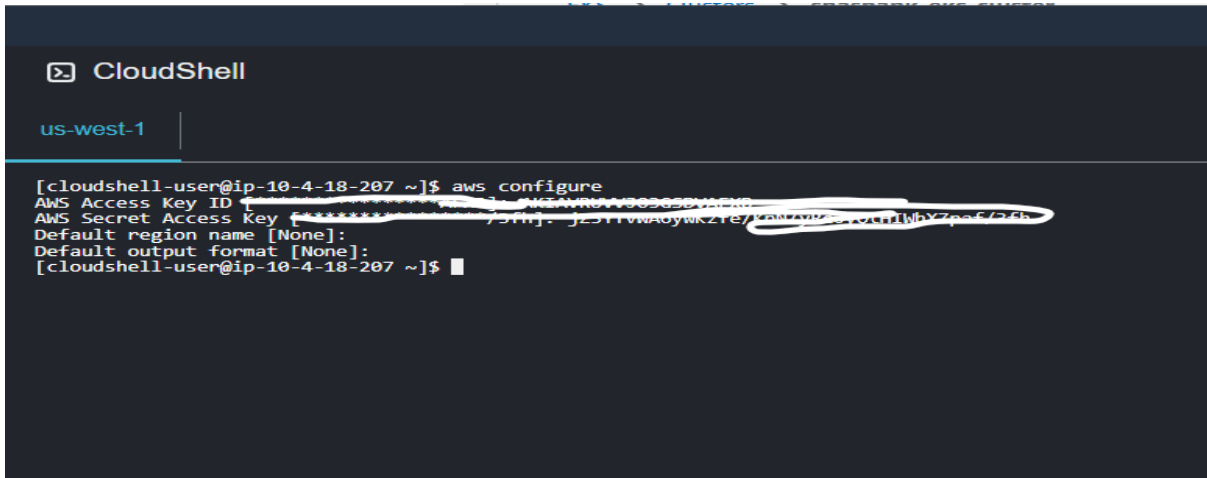
Step 2: Add permissions Edit

Permissions policy summary

Policy name	Type	Attached as
AmazonEC2ContainerRegistryReadOnly	AWS managed	Permissions policy
AmazonEKS_CNI_Policy	AWS managed	Permissions policy
AmazonEKSClusterPolicy	AWS managed	Permissions policy
AmazonEKSServicePolicy	AWS managed	Permissions policy
AmazonEKSWorkerNodePolicy	AWS managed	Permissions policy

4. Configure the AWS Cloudshell.

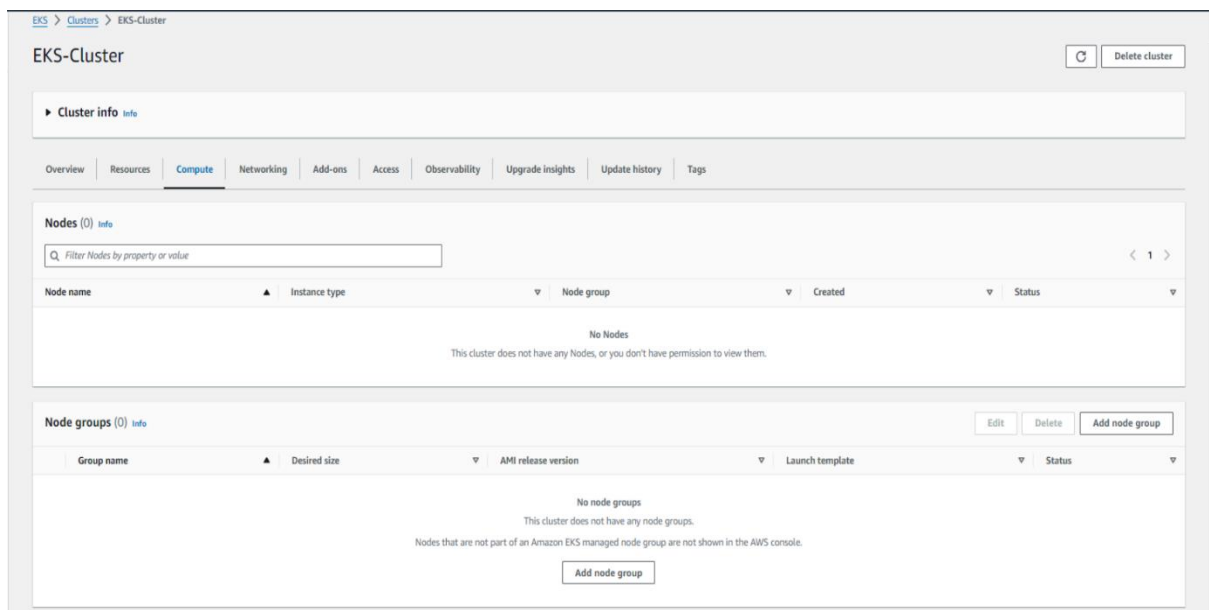
- Open aws cloudshell & configure aws.



```
[cloudshell-user@ip-10-4-18-207 ~]$ aws configure
AWS Access Key ID [*****]:
AWS Secret Access Key [*****]:
Default region name [None]:
Default output format [None]:
[cloudshell-user@ip-10-4-18-207 ~]$
```

5. Add worker nodes.

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



- Click on “Ad Node Group”.
- Select the “Name” & “IAM ROLE”.

The screenshot shows the 'Configure node group' page in the AWS Management Console. The breadcrumb trail is 'EKS > Clusters > shashank-eks-cluster > Node groups > Add node group'. On the left, a sidebar lists four steps: 'Step 1: Configure node group' (active), 'Step 2: Set compute and scaling configuration', 'Step 3: Specify networking', and 'Step 4: Review and create'. The main content area is titled 'Configure node group' with an 'info' icon. Below the title is a descriptive paragraph: '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.' The 'Node group configuration' section contains a warning: 'These properties cannot be changed after the node group is created.' It includes a 'Name' field with the value 'shashank-eks-node' and a 'Node IAM role' dropdown menu with the value 'shashank-eks-ec2-role'. A blue information box below the dropdown states: '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'. The 'Launch template' section also has a warning and a radio button labeled 'Use launch template' which is selected.

EKS > Clusters > shashank-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

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.
shashank-eks-node
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](#).
shashank-eks-ec2-role

ⓘ 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.

- Click on next.
- Select the values for the node configuration a below.

EKS > Clusters > shashank-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

Set compute and scaling configuration

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.

Cancel

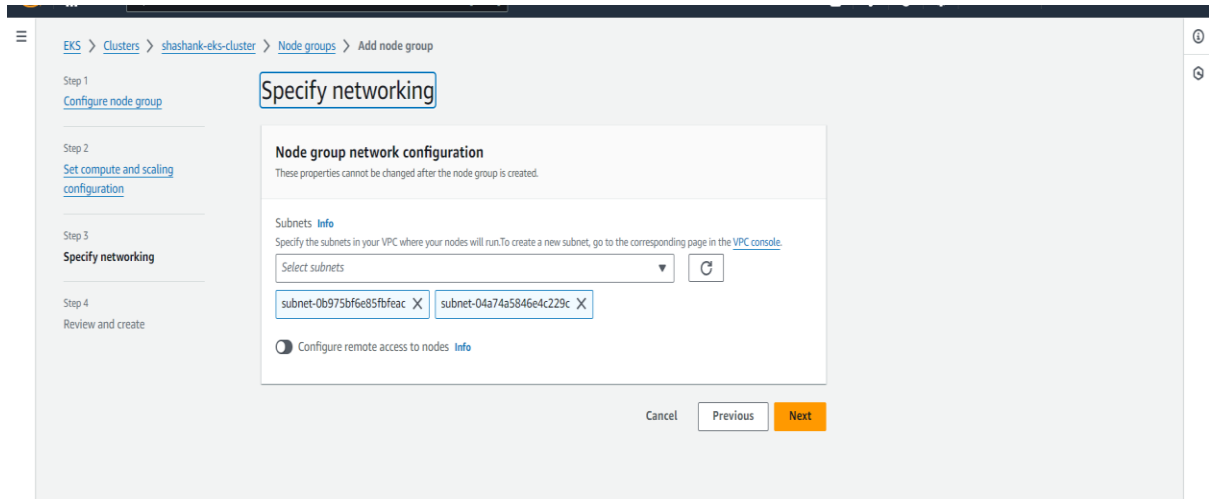
Previous

Next

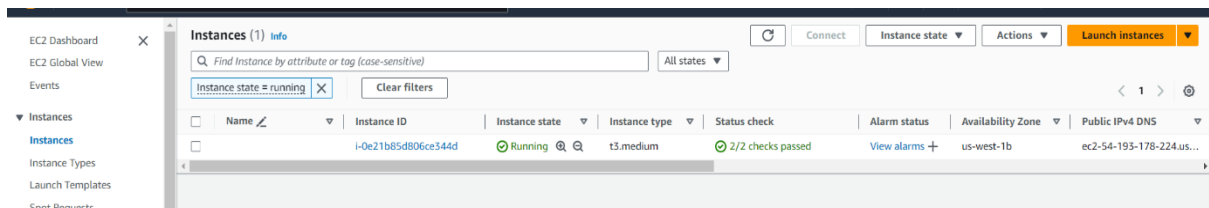
CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- Click on next.
- Select the subnets.



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



6. Verify the cluster.

- Open cloudshell and execute the following commands.
aws eks update-kubeconfig --region <region> --name
<cluster-name>
kubectl cluster-info

```
us-west-1
[cloudshell-user@ip-10-4-18-207 ~]$ aws configure
AWS Access Key ID [*****AFXB]: A
AWS Secret Access Key [*****3fh]: 
Default region name [None]: 
Default output format [None]: 
[cloudshell-user@ip-10-4-18-207 ~]$ aws eks update-kubeconfig --region us-west-1 --name shashank-eks-cluster
Added new context arn:aws:eks:us-west-1:381492218806:cluster/shashank-eks-cluster to /home/cloudshell-user/.kube/config
[cloudshell-user@ip-10-4-18-207 ~]$ kubectl cluster-info
Kubernetes control plane is running at https://3C992A1AEE61B2203AFF45986F808873.sk1.us-west-1.eks.amazonaws.com
CoreDNS is running at https://3C992A1AEE61B2203AFF45986F808873.sk1.us-west-1.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-10-4-18-207 ~]$
```