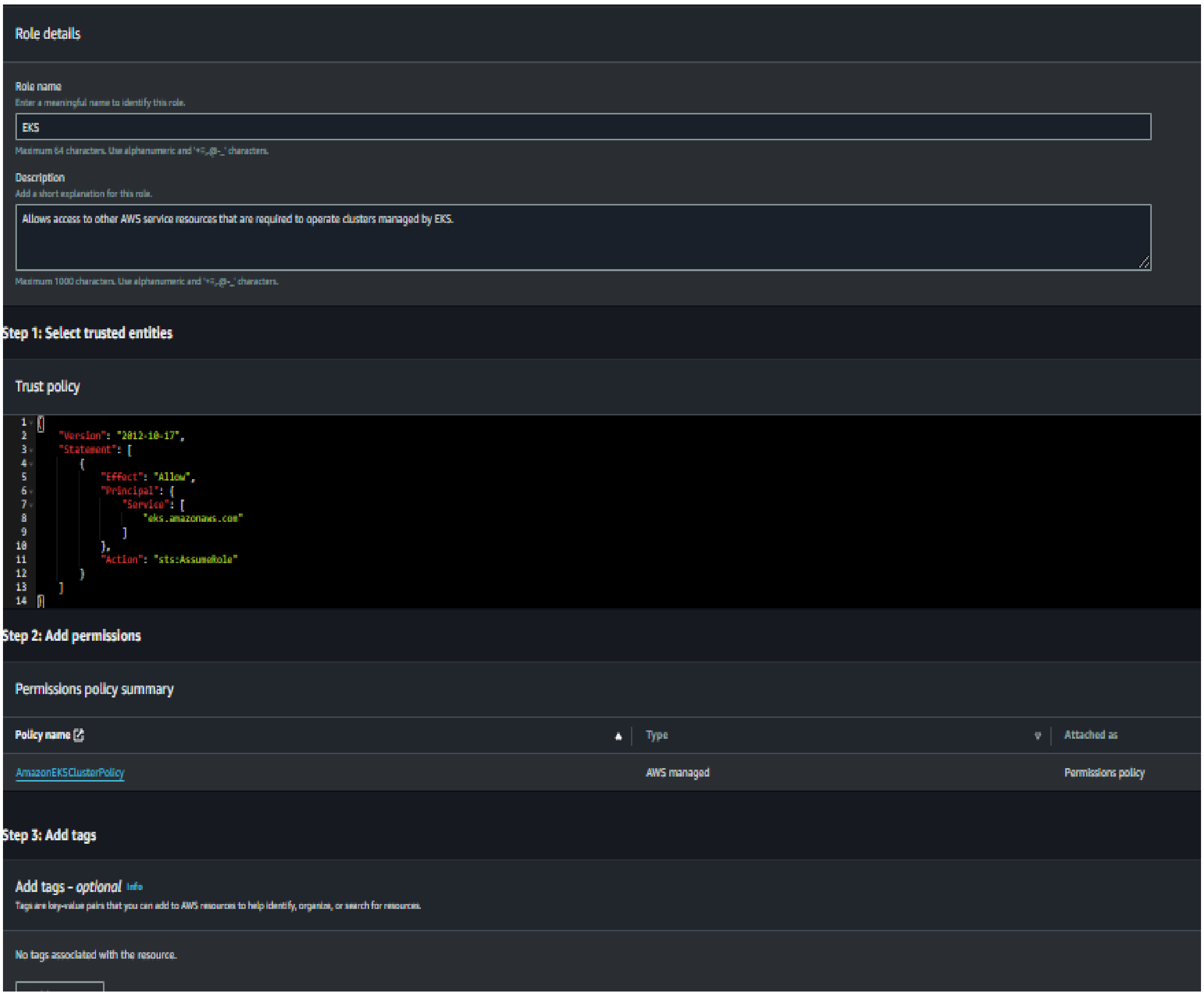
CDEC – B24

Name – Vaibhav Navneet Jorvekar

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**



Role details

Role name
Enter a meaningful name to identify this role.
EKS
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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "eks.amazonaws.com"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Step 2: Add permissions

Permissions policy summary

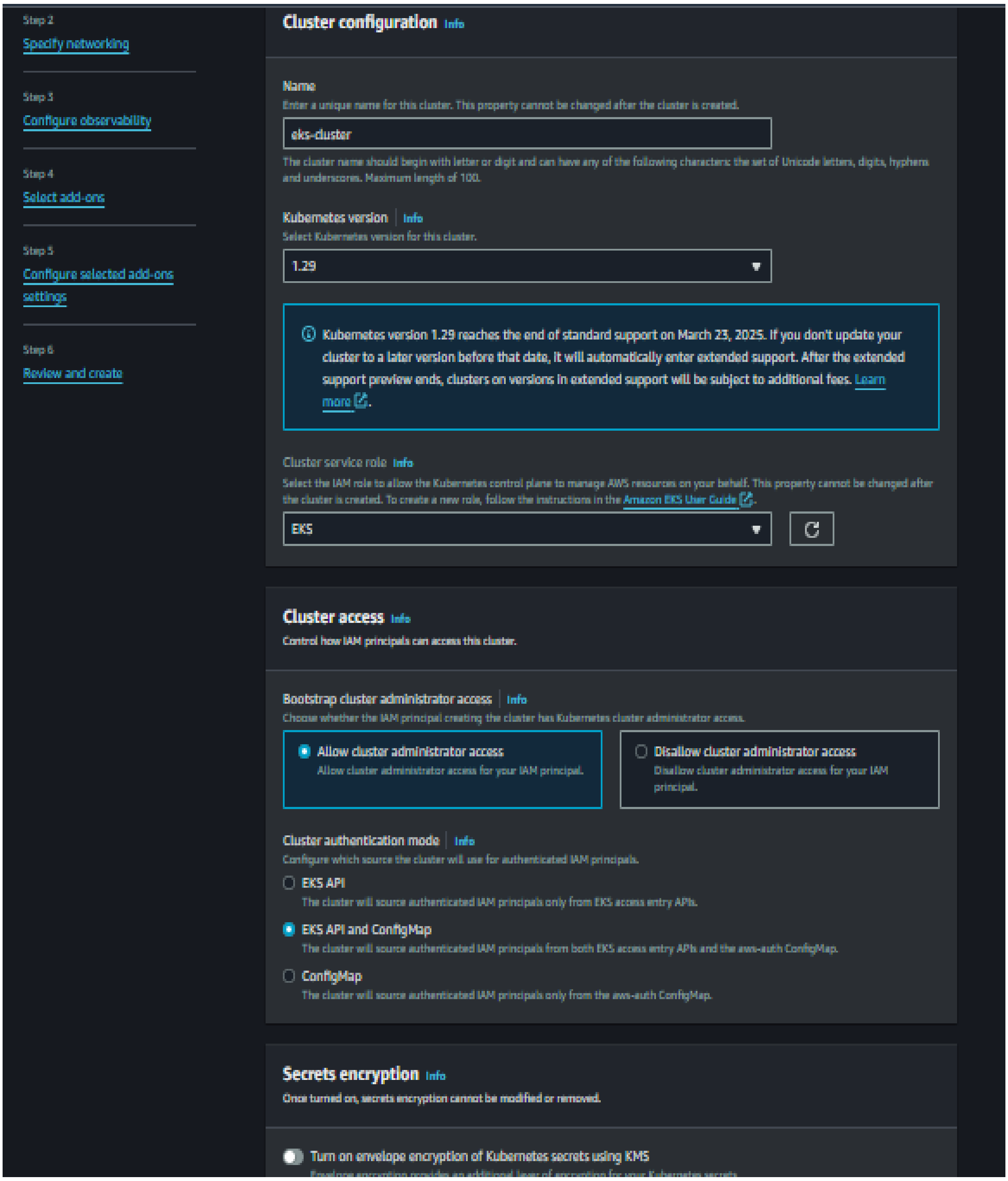
Policy name	Type	Attached as
AmazonEKSClusterPolicy	AWS managed	Permissions policy

Step 3: Add tags

Add tags - *optional* Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

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



Cluster configuration

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

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

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.

EKS

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
Allow cluster administrator access for your IAM principal.

○ Disallow cluster administrator access
Disallow cluster administrator access for your IAM principal.

Cluster authentication mode

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.

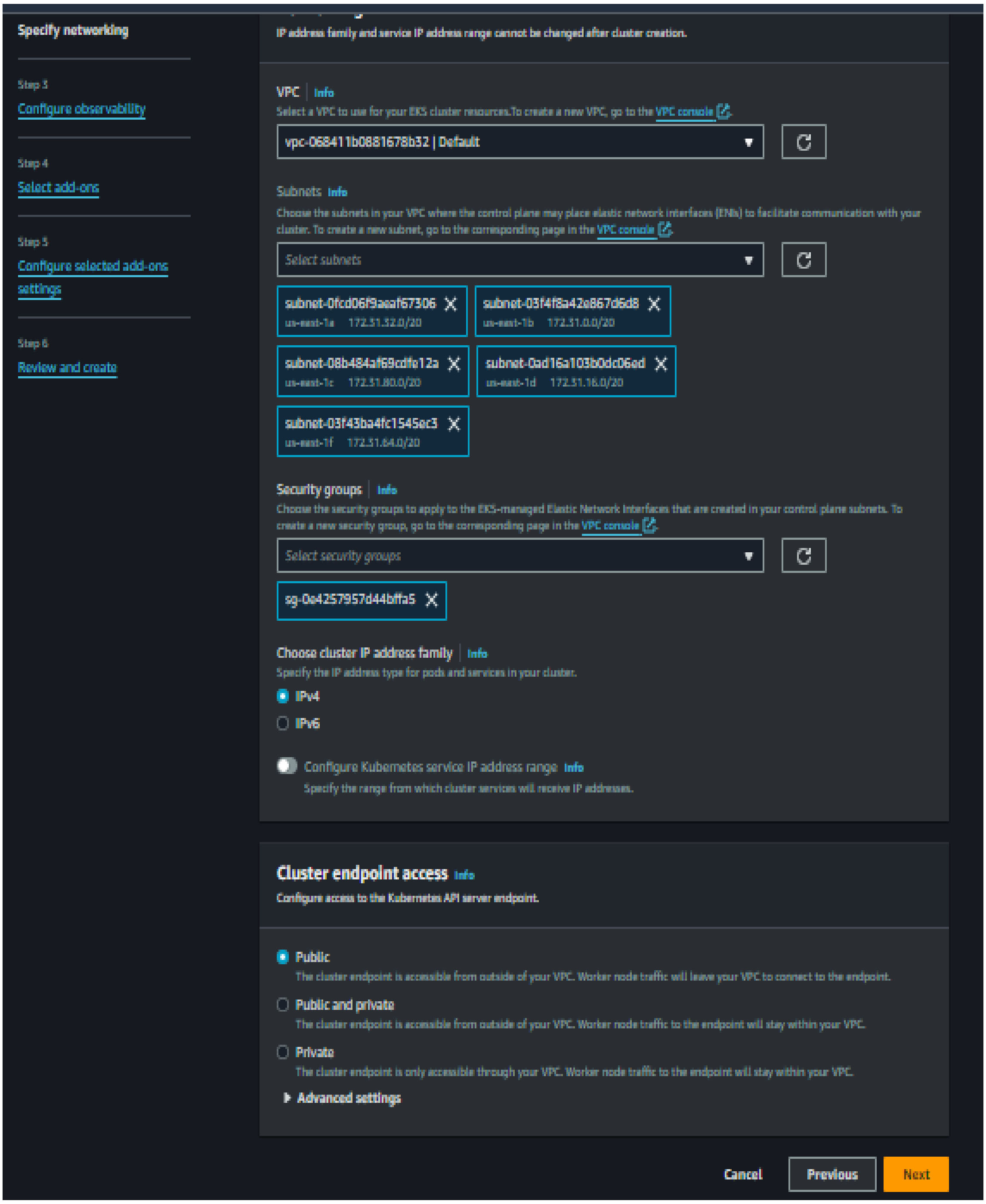
● EKS API and ConfigMap
The cluster will source authenticated IAM principals from both EKS access entry APIs and the aws-auth ConfigMap.

○ ConfigMap
The cluster will source authenticated IAM principals only from the aws-auth ConfigMap.

Secrets encryption

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.



Specify networking

Step 3
Configure observability

Step 4
Select add-ons

Step 5
Configure selected add-ons settings

Step 6
Review and create

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-068411b0881678b32 | 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-0fcd06f9aeaf67306 ✕ us-east-1a 172.31.32.0/20
- subnet-03f4f8a42e867d6d8 ✕ us-east-1b 172.31.0.0/20
- subnet-08b484af69cdfe12a ✕ us-east-1c 172.31.80.0/20
- subnet-0ad16a103b0dc06ed ✕ us-east-1d 172.31.16.0/20
- subnet-03f43ba4fc1545ec3 ✕ us-east-1f 172.31.64.0/20

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-0e4257957d44bffa5 ✕

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

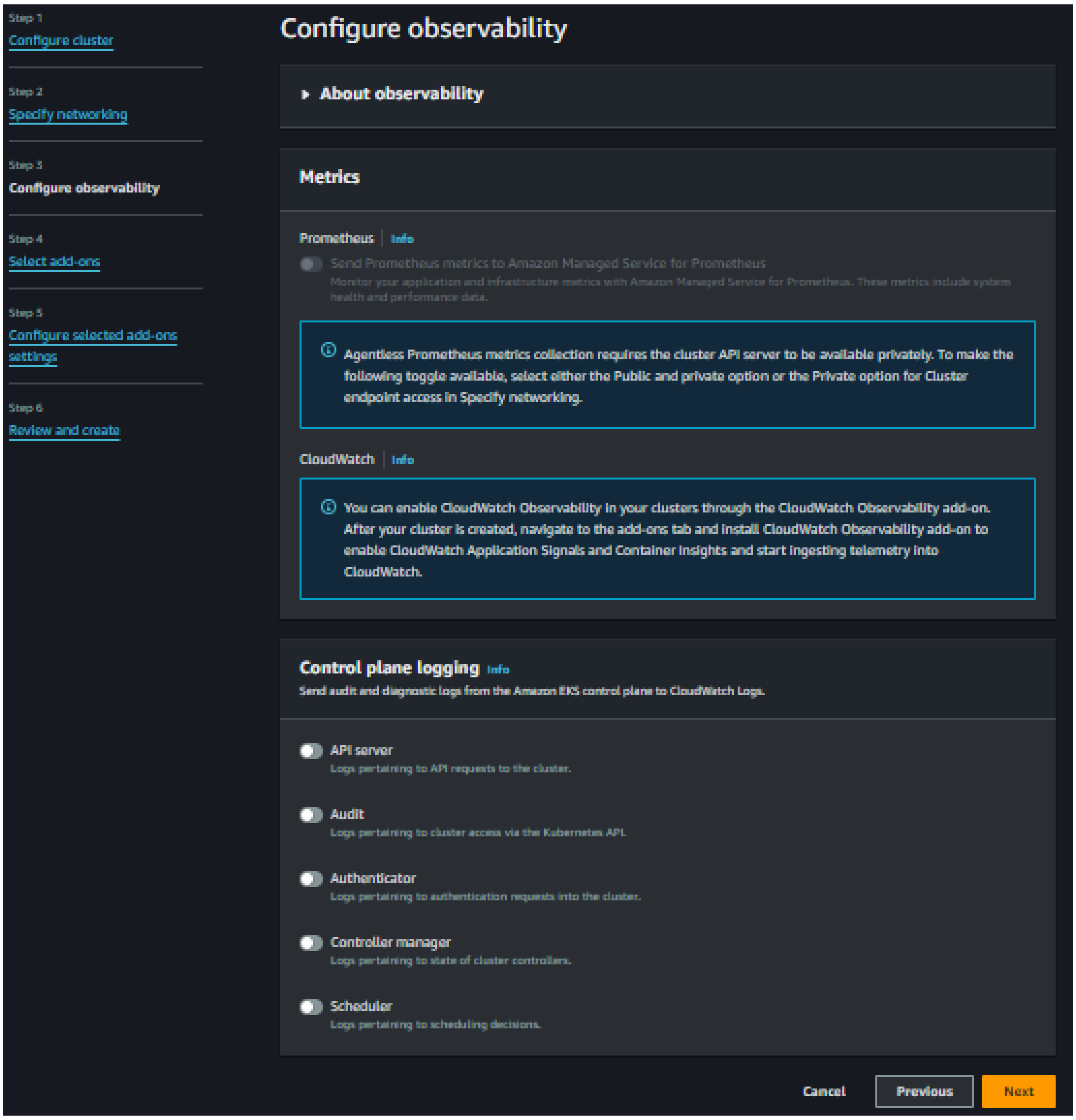
The cluster endpoint is accessible from outside of your VPC. Worker node traffic will leave your VPC to connect to the endpoint.

○ 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.



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.

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 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.

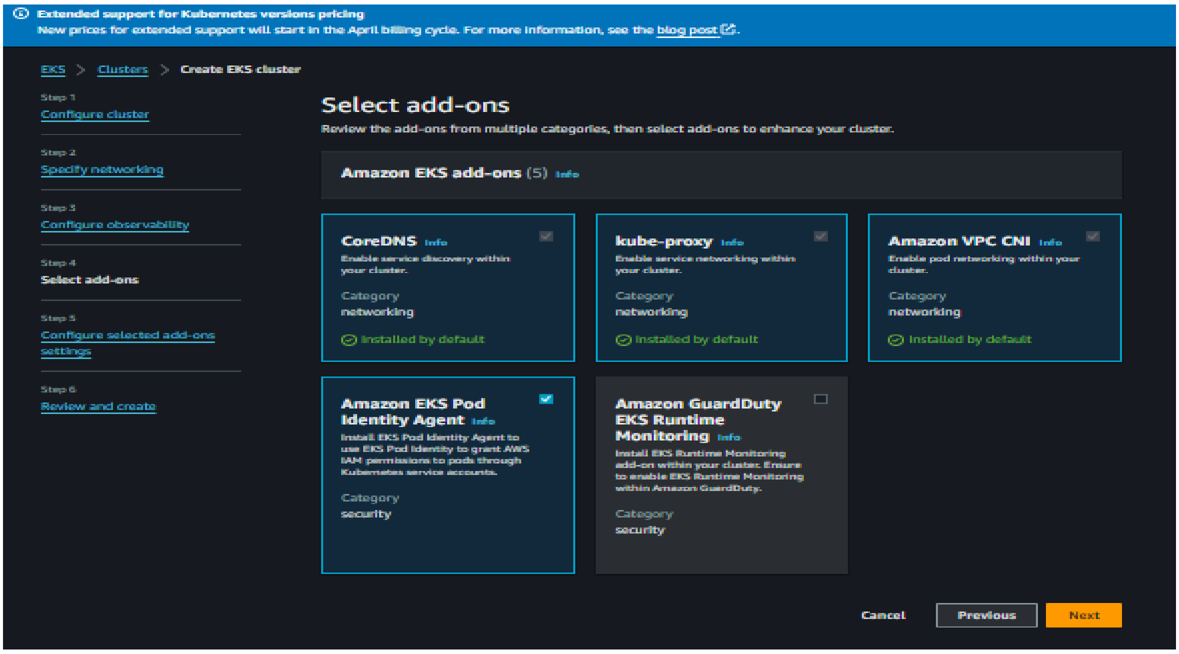
API server
Logs pertaining to API requests to the cluster.

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.



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

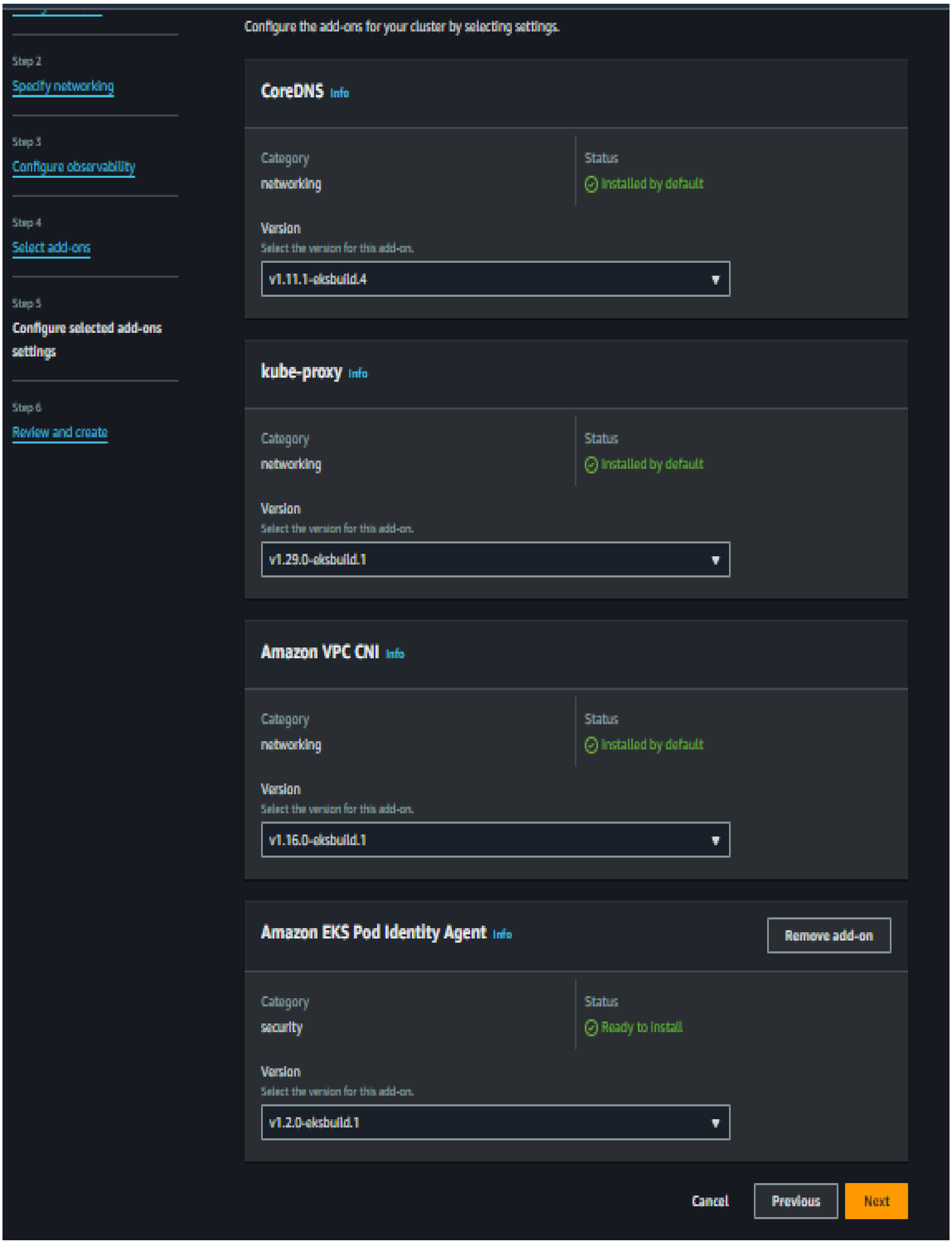
CoreDNS Info ☑
Enable service discovery within your cluster.
Category
networking
Installed by default

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



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 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

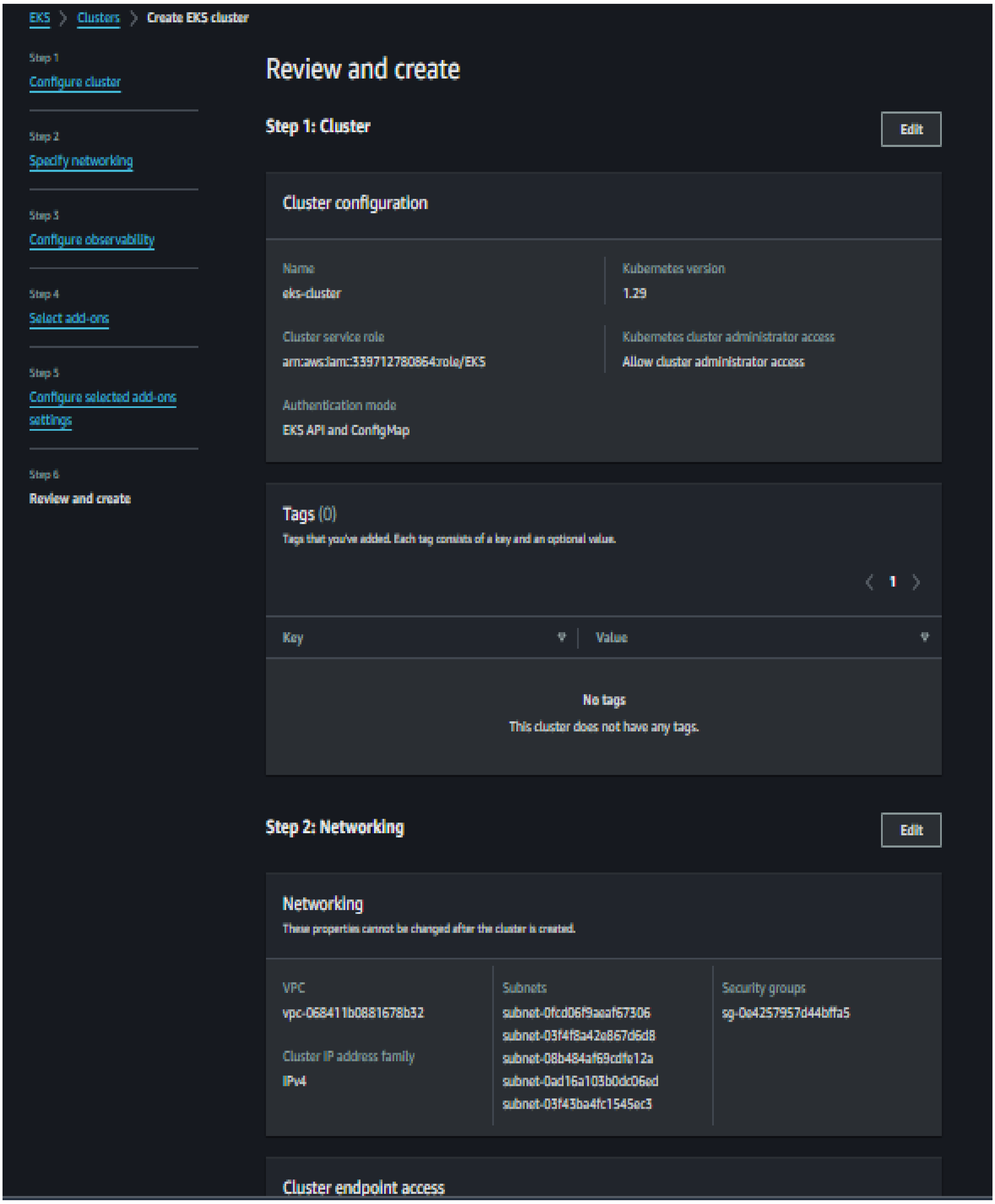
Category: security

Status: ✓ Ready to install

Version

Select the version for this add-on.

v1.2.0-eksbuild.1 ▼



Review and create

Step 1: Cluster

Cluster configuration

Name
eks-cluster

Kubernetes version
1.29

Cluster service role
arn:aws:iam::339712780864:role/EKS

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

Networking

These properties cannot be changed after the cluster is created.

VPC
vpc-068411b0881678b32

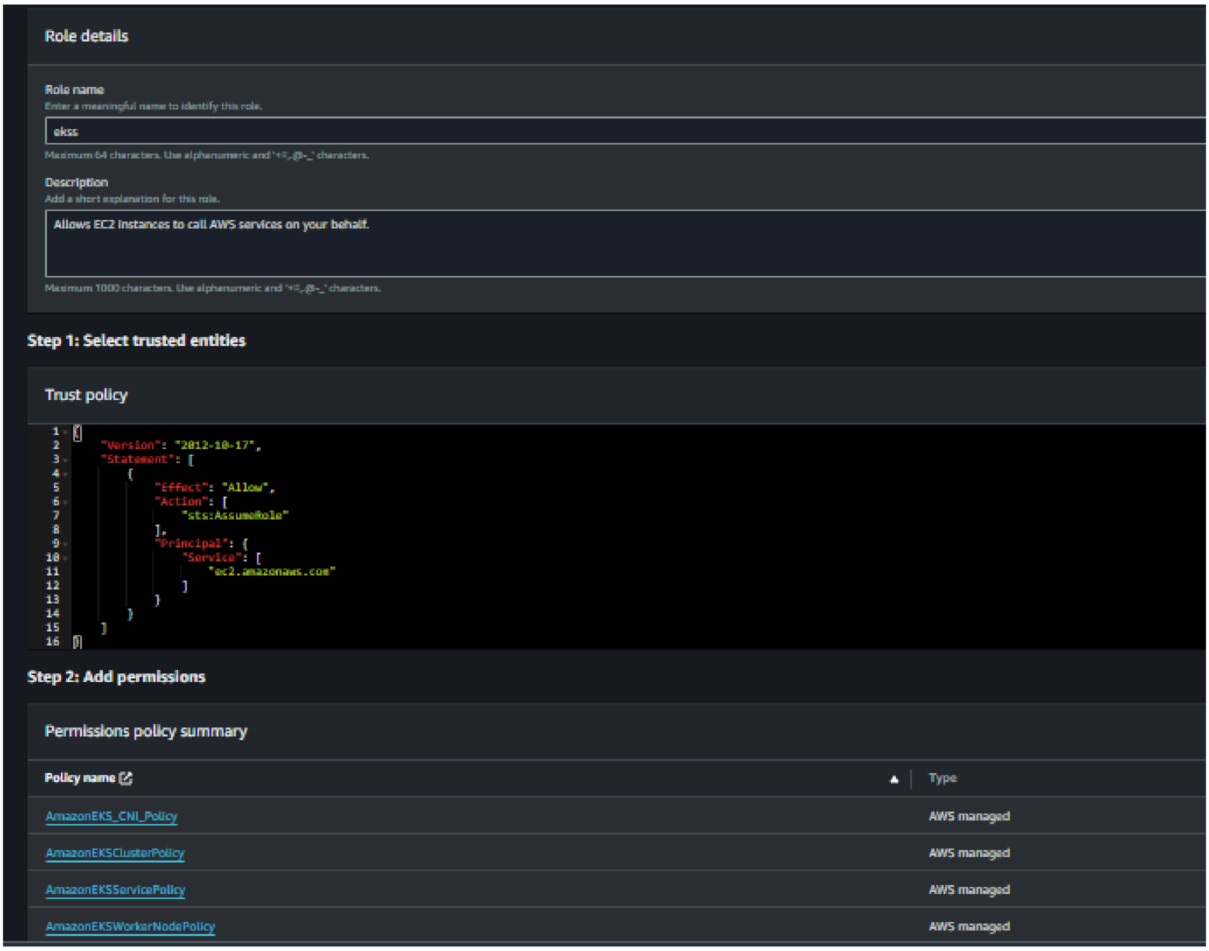
Cluster IP address family
IPv4

Subnets
subnet-0fcd06f9aeaf67306
subnet-03f4f8a42e867d6d8
subnet-08b484af69cdfe12a
subnet-0ad16a103b0dc06ed
subnet-03f43ba4fc1545ec3

Security groups
sg-0e4257957d44bffa5

Cluster endpoint access

3. Set up IAM roles for EC2.



Role details

Role name
Enter a meaningful name to identify this role.

ekss

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

Description
Add a short explanation for this role.

Allows EC2 Instances to call AWS services on your behalf.

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

Step 1: Select trusted entities

Trust policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Principal": {
                "Service": [
                    "ec2.amazonaws.com"
                ]
            }
        }
    ]
}
```

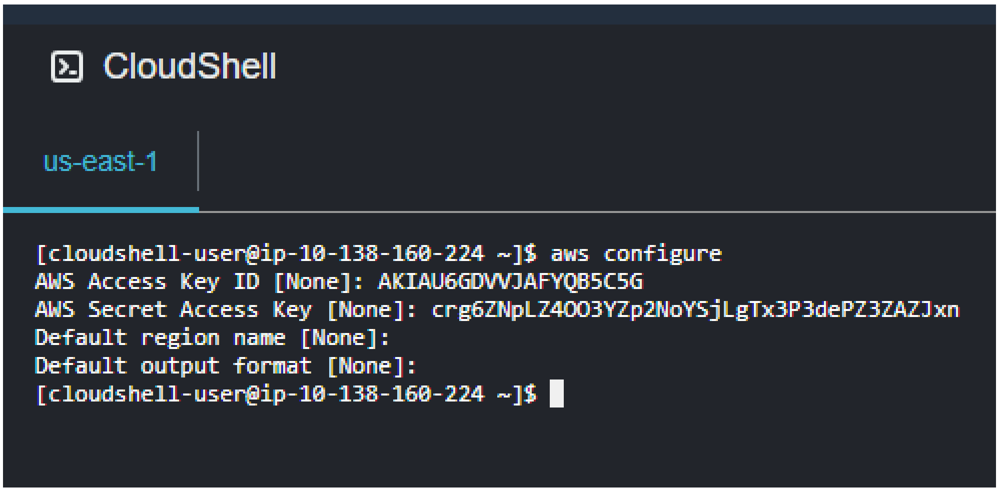
Step 2: Add permissions

Permissions policy summary

Policy name	Type
AmazonEKS_CNI_Policy	AWS managed
AmazonEKSClusterPolicy	AWS managed
AmazonEKSServicePolicy	AWS managed
AmazonEKSWorkerNodePolicy	AWS managed

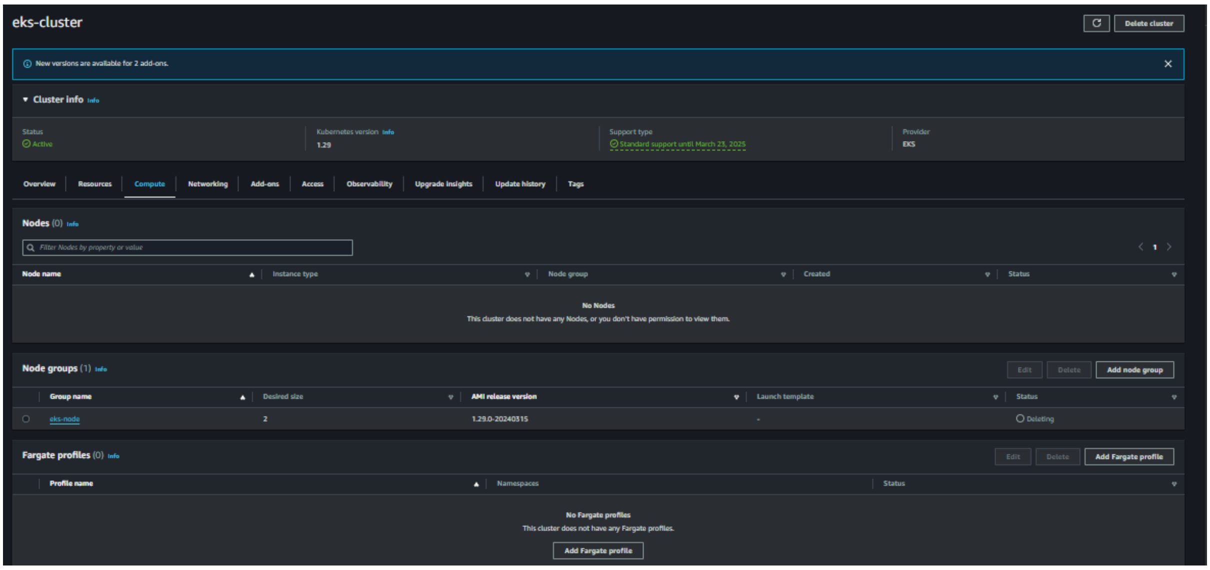
4. Configure the AWS Cloudshell.

- **Open aws cloudshell & configure aws.**



```
[cloudshell-user@ip-10-138-160-224 ~]$ aws configure
AWS Access Key ID [None]: AKIAU6GDVVJAFYQB5C5G
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]:
[cloudshell-user@ip-10-138-160-224 ~]$
```

5. **Add worker nodes.**
    - **In the AWS EKS console select your cluster.**
    - **In cluster go to compute service.**



New versions are available for 2 add-ons.

Cluster info

Status: Active

Kubernetes version: 1.29

Support type: Standard support until March 23, 2025

Provider: EKS

Nodes (0)

Node name	Instance type	Node group	Created	Status

No Nodes

This cluster does not have any Nodes, or you don't have permission to view them.

Node groups (1)

Group name	Desired size	AMI release version	Launch template	Status
eks-node	2	1.29.0-20240315	-	Deleting

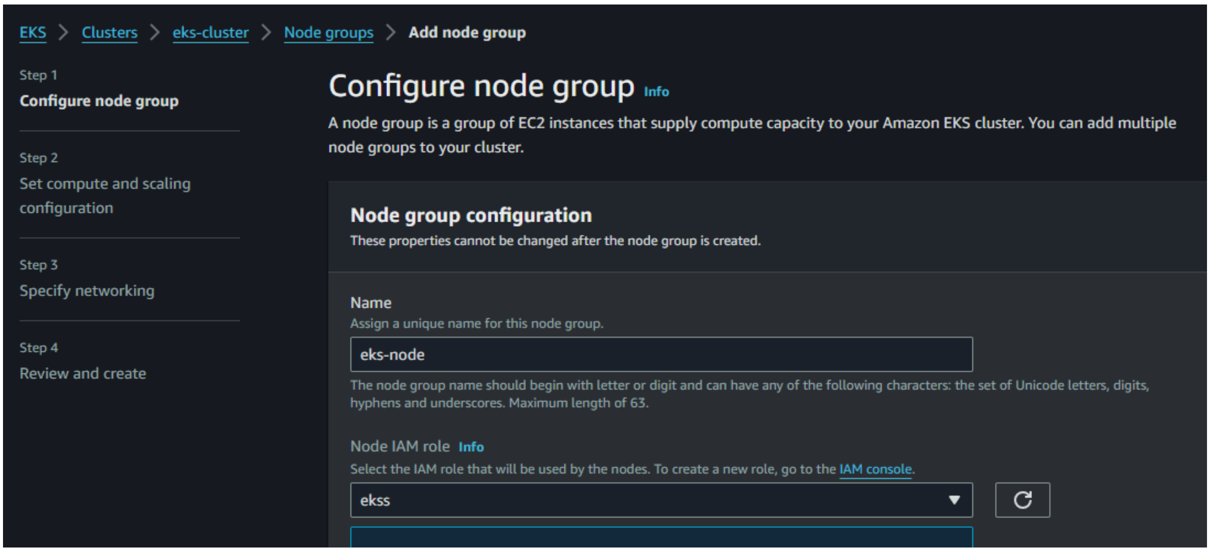
Fargate profiles (0)

Profile name	Namespaces	Status

No Fargate profiles

This cluster does not have any Fargate profiles.

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


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

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

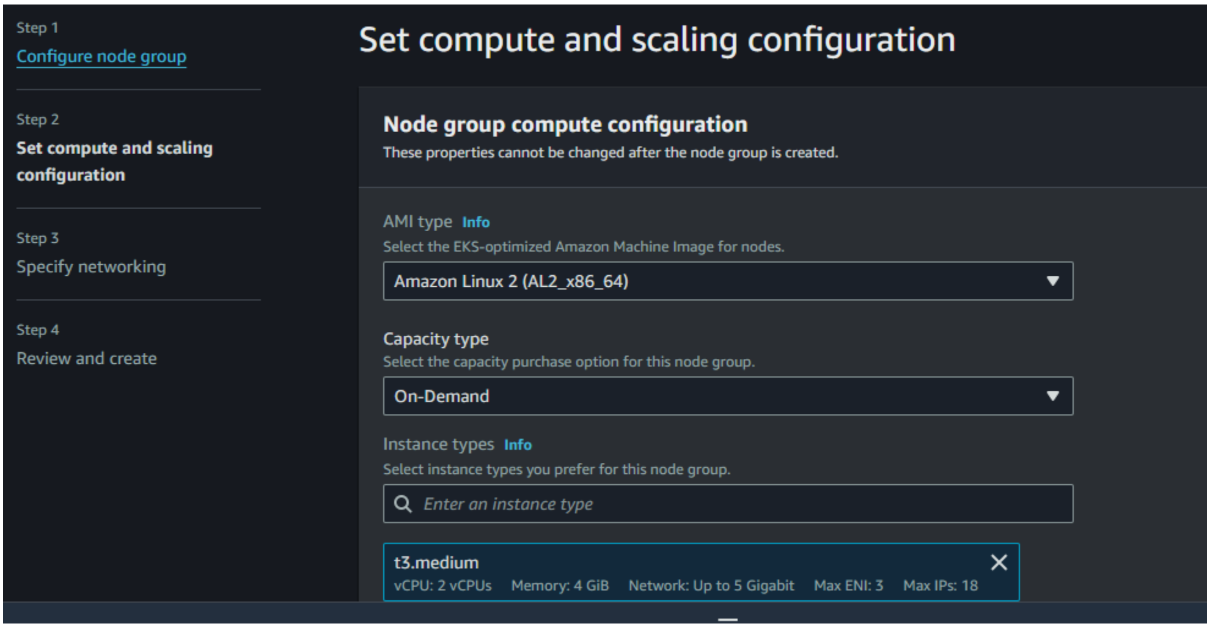
These properties cannot be changed after the node group is created.

Name
Assign a unique name for this node group.
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.
ekss

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



Set compute and scaling configuration

Node group compute configuration

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

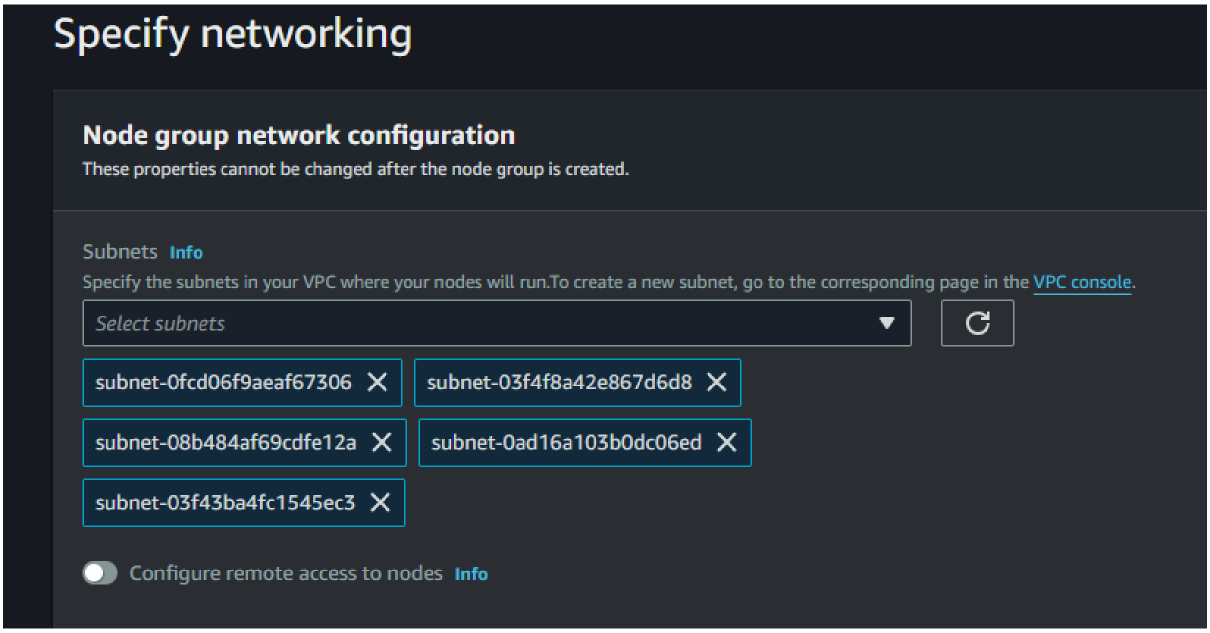
AMI type Info
Select the EKS-optimized Amazon Machine Image for nodes.
Amazon Linux 2 (AL2_x86_64)

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.
Enter an instance type

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

- **Click on next.**
- **Select the subnets.**



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-0fcd06f9aeaf67306 ✕ subnet-03f4f8a42e867d6d8 ✕

subnet-08b484af69cdfe12a ✕ subnet-0ad16a103b0dc06ed ✕

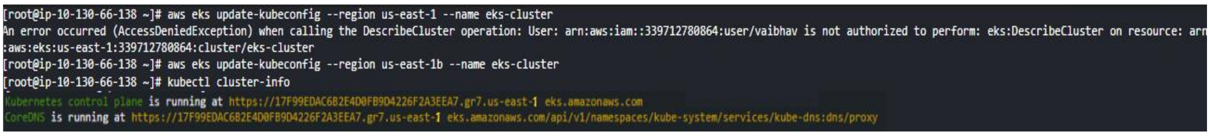
subnet-03f43ba4fc1545ec3 ✕

○ Configure remote access to nodes Info

- **Click on “next” and then ‘’Create’’**

6. Verify the cluster.

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



```
[root@ip-10-130-66-138 ~]# aws eks update-kubeconfig --region us-east-1 --name eks-cluster
An error occurred (AccessDeniedException) when calling the DescribeCluster operation: User: arn:aws:iam::339712780864:user/vaibhav is not authorized to perform: eks:DescribeCluster on resource: arn
:aws:eks:us-east-1:339712780864:cluster/eks-cluster
[root@ip-10-130-66-138 ~]# aws eks update-kubeconfig --region us-east-1b --name eks-cluster
[root@ip-10-130-66-138 ~]# kubectl cluster-info
Kubernetes control plane is running at https://17F99EDAC6B2E4D0FB9D4226F2A3EEA7.gr7.us-east-1 eks.amazonaws.com
CoreDNS is running at https://17F99EDAC6B2E4D0FB9D4226F2A3EEA7.gr7.us-east-1 eks.amazonaws.com/api/v1/namespaces/kube-system/services/kube-dns:dns/proxy
```