AWS EKS CLUSTER CONFIGURATION

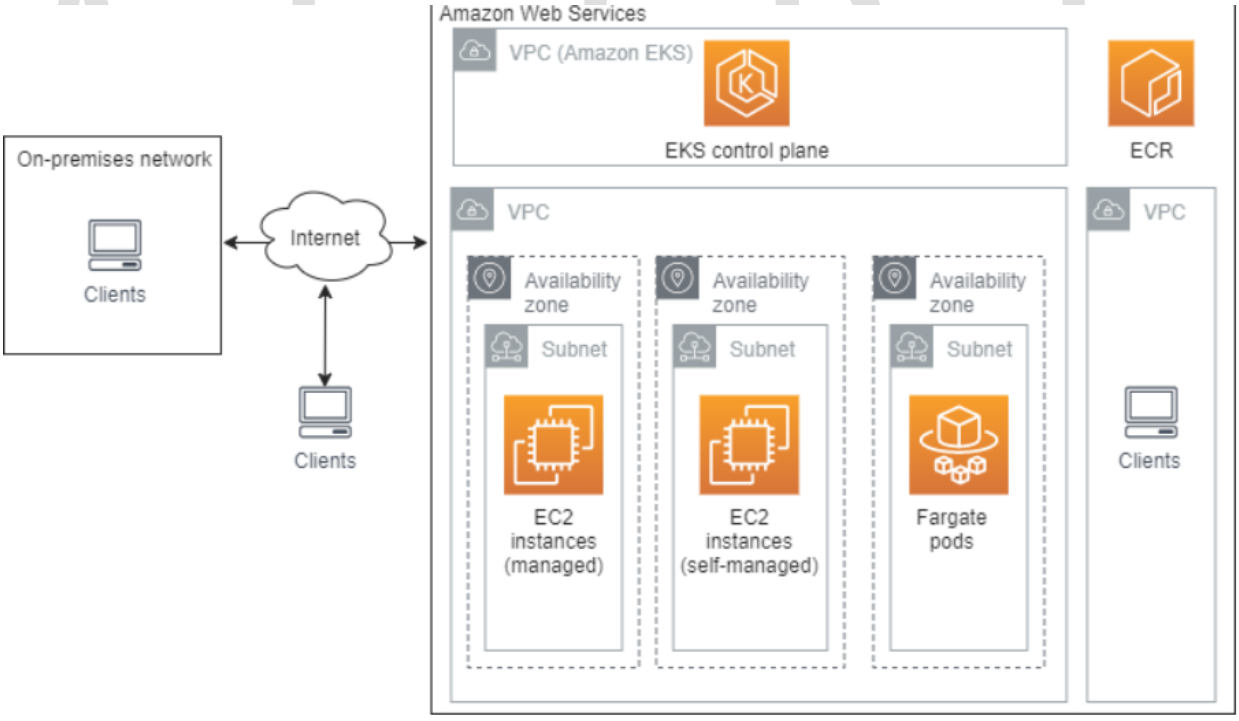
Amazon Elastic Kubernetes Service (Amazon EKS) runs the Kubernetes management infrastructure for you across multiple AWS Availability Zones to eliminate a single point of failure. Amazon EKS is certified Kubernetes-conformant, so you can use existing tooling and plugins from partners and the Kubernetes community. Applications running on any standard Kubernetes environment are fully compatible and can be migrated to Amazon EKS.

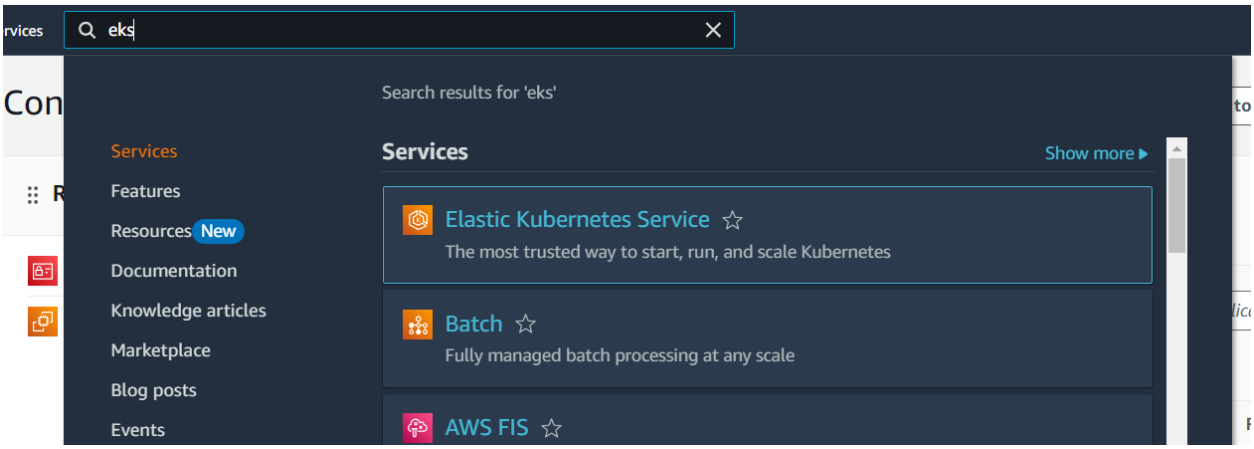
A highly available architecture that spans three Availability Zones.*

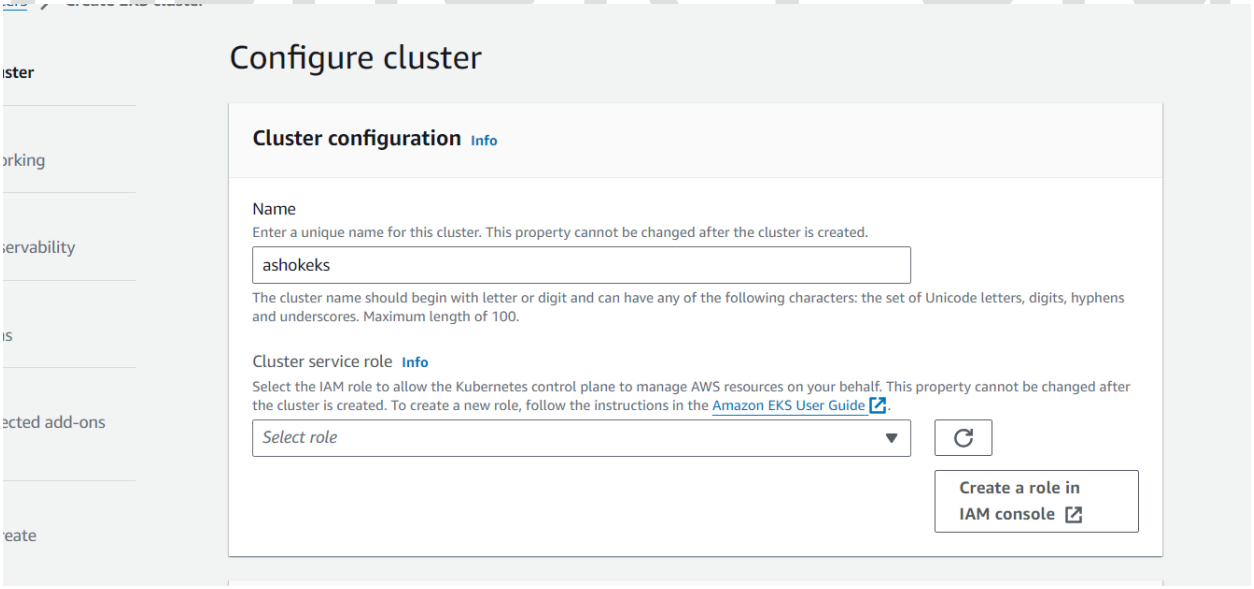
A virtual private cloud (VPC) configured with public and private subnets according to AWS best practices, to provide you with your own virtual network on AWS.*

In the public subnets, managed NAT gateways to allow outbound internet access for resources in the private subnets.*

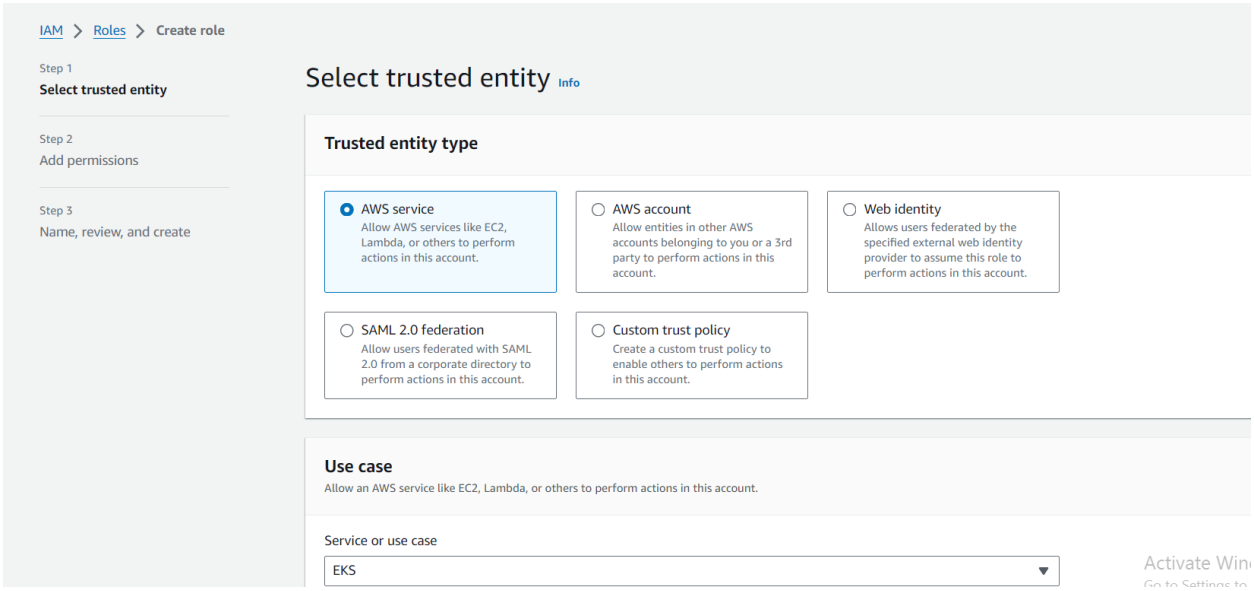
In one public subnet, a Linux bastion host in an Auto Scaling group to allow inbound Secure Shell (SSH) access to Amazon Elastic Compute Cloud (Amazon EC2) instances in private subnets. The bastion host is also configured with the Kubernetes kubectl command line interface for managing the Kubernetes cluster.

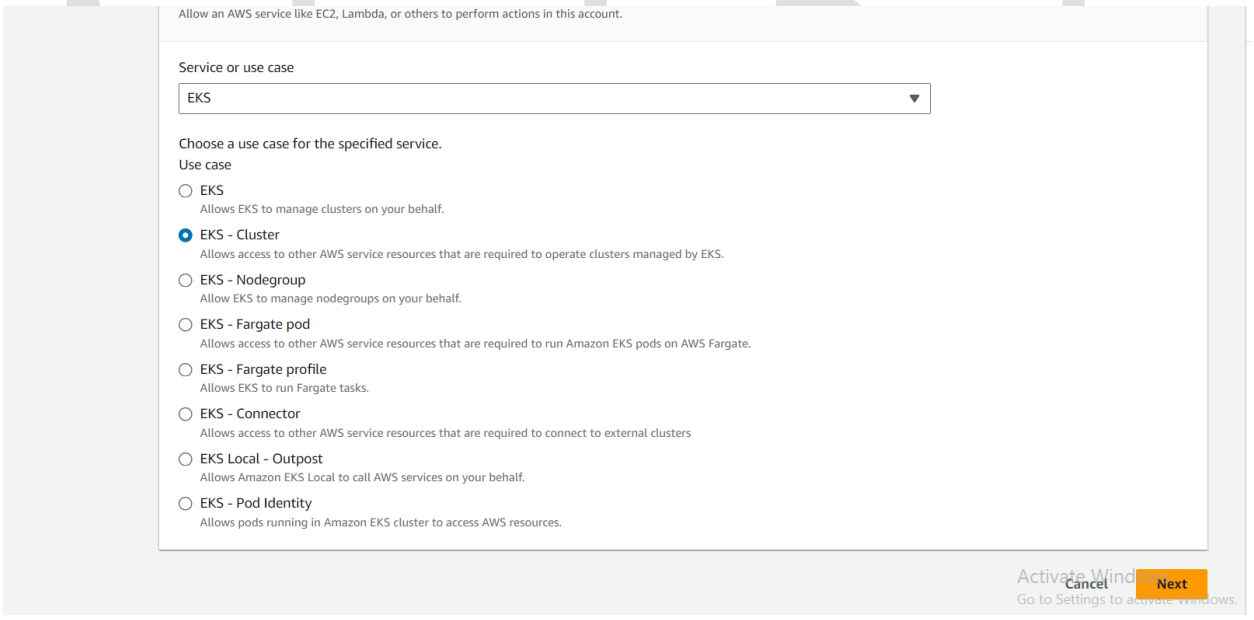


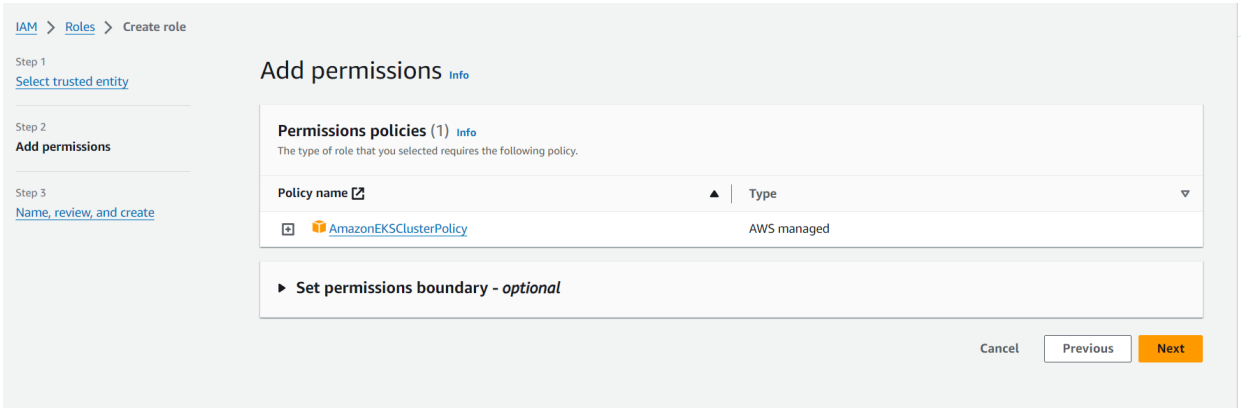


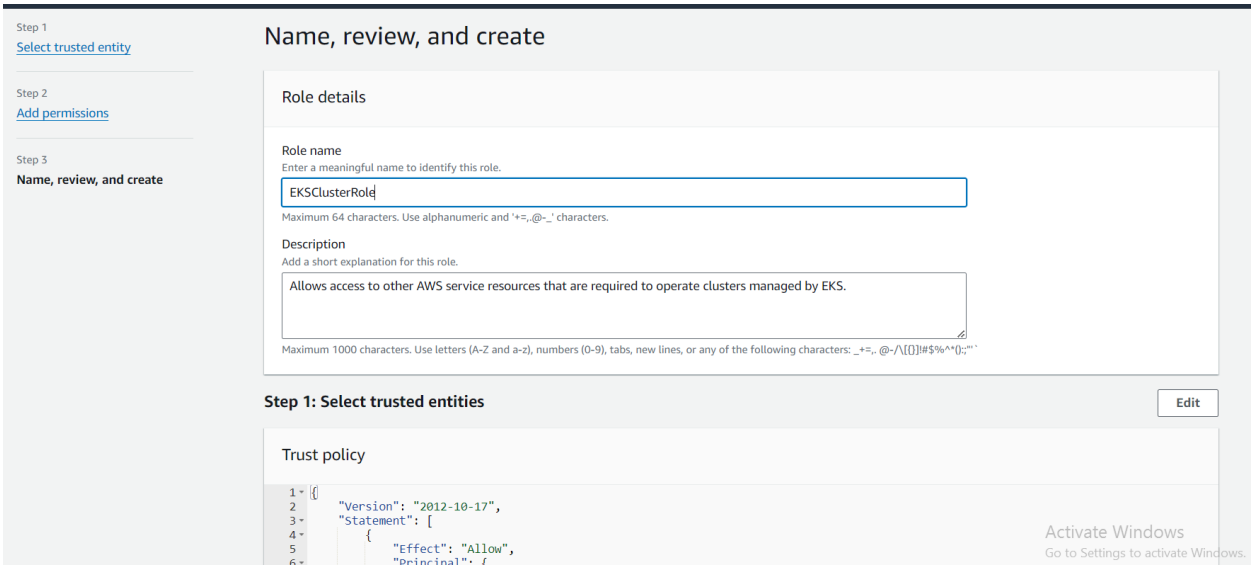


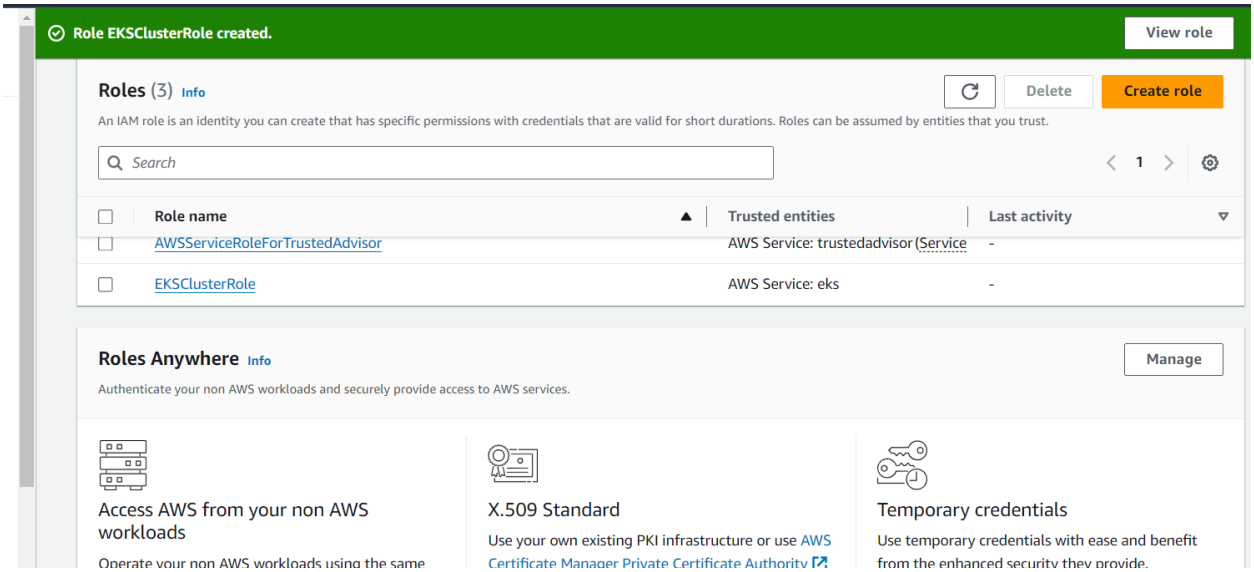
Create IAM Role:


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
EKS


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
Allow EKS to manage nodegroups on your behalf.
EKS - Fargate pod
Allows access to other AWS service resources that are required to run Amazon EKS pods on AWS Fargate.
EKS - Fargate profile
Allows EKS to run Fargate tasks.
EKS - Connector
Allows access to other AWS service resources that are required to connect to external clusters
EKS Local - Outpost
Allows Amazon EKS Local to call AWS services on your behalf.
EKS - Pod Identity
Allows pods running in Amazon EKS cluster to access AWS resources.
Cancel
Next


IAM > Roles > Create role
Step 1
Select trusted entity
Step 2
Add permissions
Step 3
Name, review, and create
Add permissions Info
Permissions policies (1) Info
The type of role that you selected requires the following policy.
Policy name
Type
AmazonEKSClusterPolicy
AWS managed
Set permissions boundary - optional
Cancel
Previous
Next


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.
EKSClusterRole
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 letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=,. @-/\[{}]!#$%^*();:"'`
Step 1: Select trusted entities
Edit
Trust policy
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
Activate Windows
Go to Settings to activate Windows.



Configure cluster

Cluster configuration Info

Name

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

ashokeks

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.

Cluster service role Info

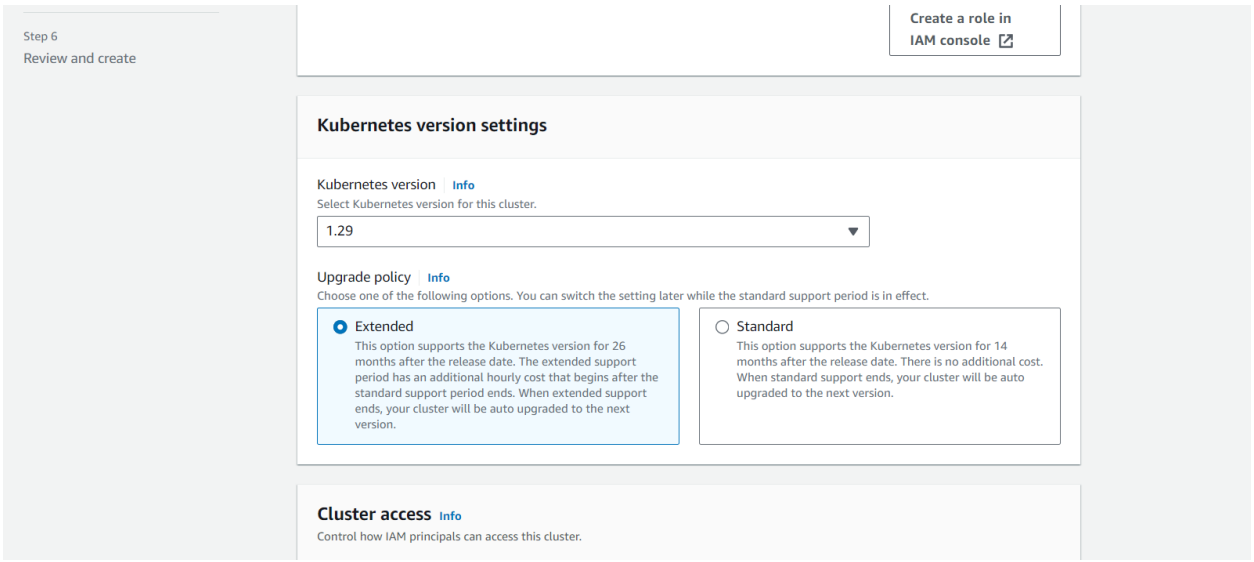
Select the IAM role to allow the Kubernetes control plane to manage AWS resources on your behalf. This property cannot be changed after the cluster is created. To create a new role, follow the instructions in the Amazon EKS User Guide.

EKSClusterRole

Create a role in IAM console

Kubernetes version settings

Kubernetes version Info



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.

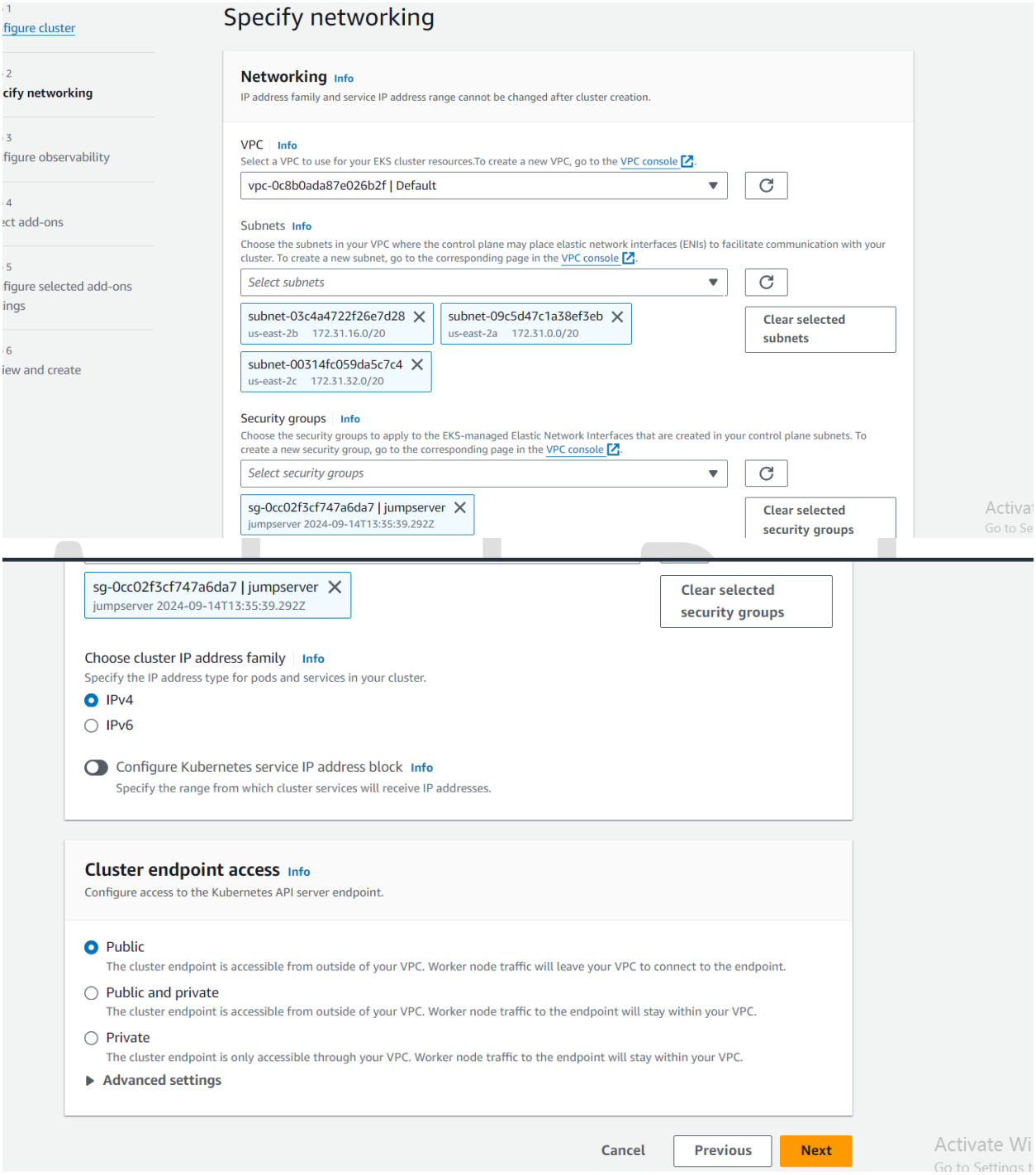
- (●) **Allow cluster administrator access**
  Allow cluster administrator access for your IAM principal.
- ( ) **Disallow cluster administrator access**
  Disallow cluster administrator access for your IAM principal.

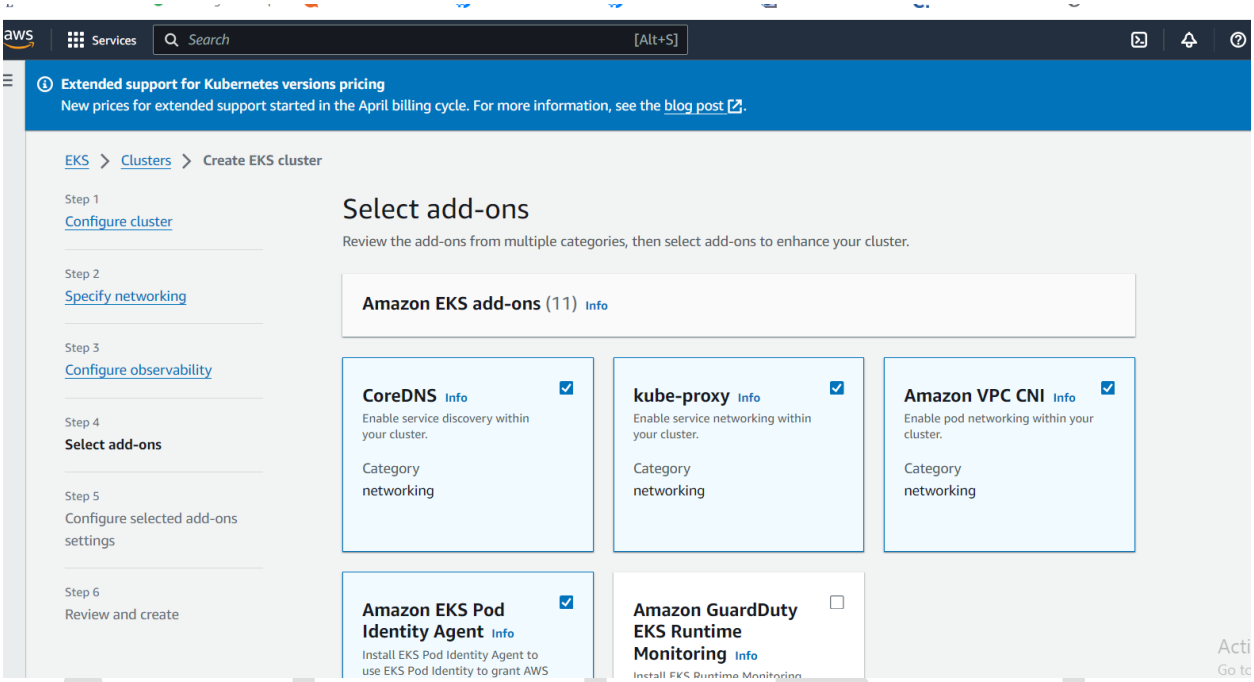
Cluster authentication mode Info

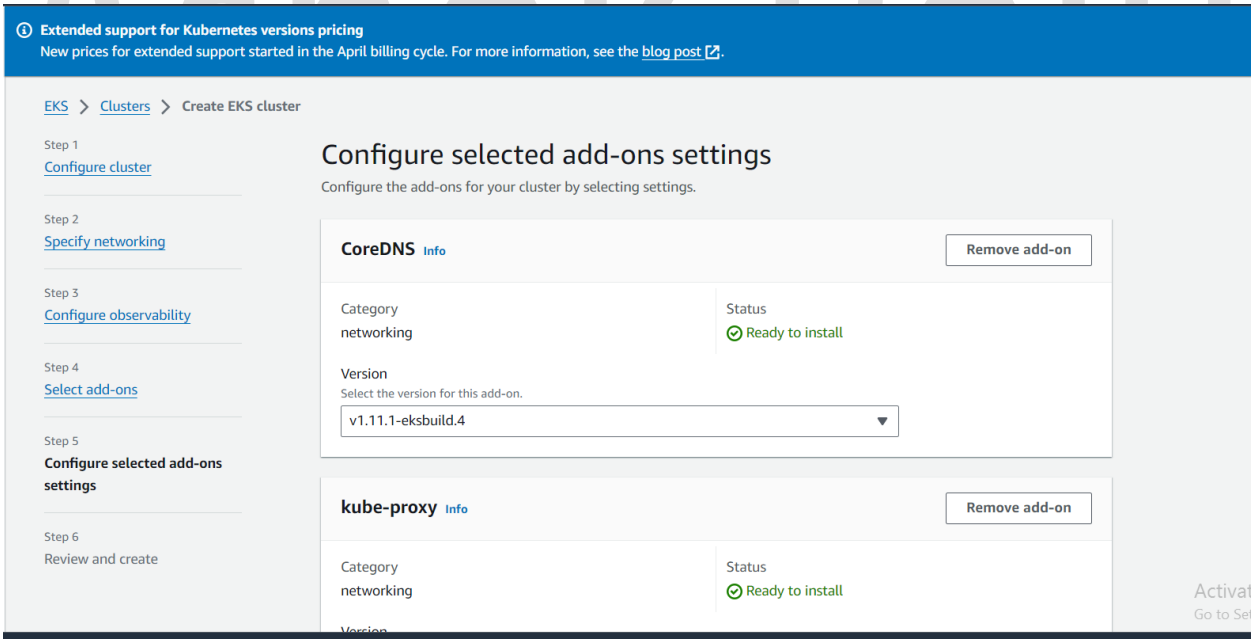
Configure which source the cluster will use for authenticated IAM principals.

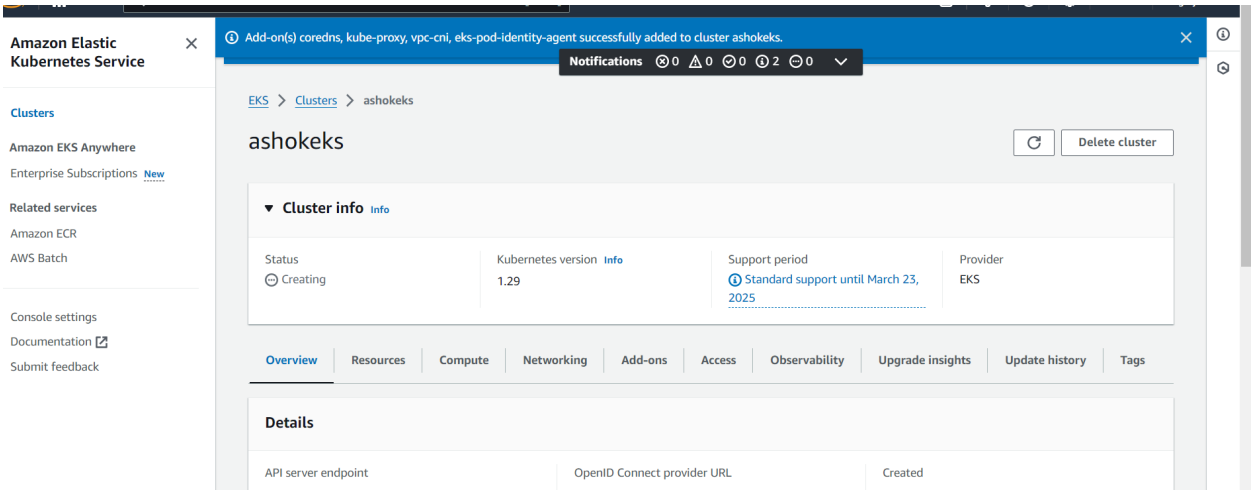
- ( ) **EKS API**
  The cluster will source authenticated IAM principals only from EKS access entry APIs.
- (●) **EKS API and ConfigMap**
  The cluster will source authenticated IAM principals from both EKS access entry APIs and the aws-auth ConfigMap.
- ( ) **ConfigMap**
  The cluster will source authenticated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

Secrets encryption Info

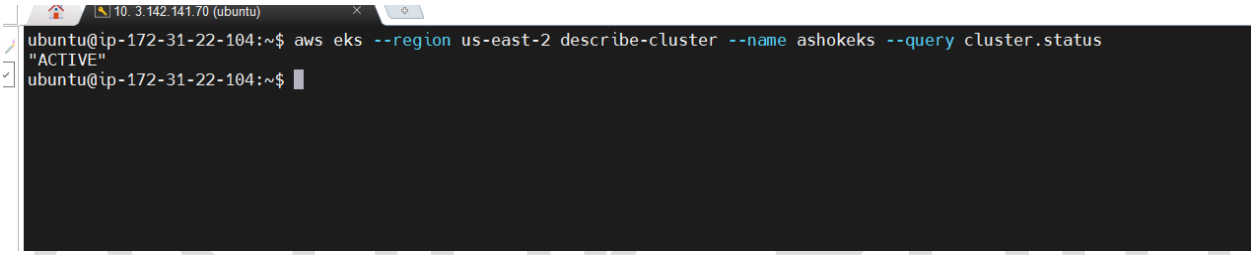

1
figure cluster
2
cify networking
3
figure observability
4
ct add-ons
5
figure selected add-ons
ings
6
iew and create
Specify networking
Networking Info
IP address family and service IP address range cannot be changed after cluster creation.
VPC Info
Select a VPC to use for your EKS cluster resources.To create a new VPC, go to the VPC console.
vpc-0c8b0ada87e026b2f | 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-03c4a4722f26e7d28
us-east-2b 172.31.16.0/20
subnet-09c5d47c1a38ef3eb
us-east-2a 172.31.0.0/20
subnet-00314fc059da5c7c4
us-east-2c 172.31.32.0/20
Clear selected subnets
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-0cc02f3cf747a6da7 | jumpserver
jumpserver 2024-09-14T13:35:39.292Z
Clear selected security groups
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 block 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]
Extended support for Kubernetes versions pricing
New prices for extended support started 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 (11) Info
CoreDNS Info
Enable service discovery within your cluster.
Category
networking
kube-proxy Info
Enable service networking within your cluster.
Category
networking
Amazon VPC CNI Info
Enable pod networking within your cluster.
Category
networking
Amazon EKS Pod Identity Agent Info
Install EKS Pod Identity Agent to use EKS Pod Identity to grant AWS
Amazon GuardDuty EKS Runtime Monitoring Info


Extended support for Kubernetes versions pricing
New prices for extended support started 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
Remove add-on
Category
networking
Status
Ready to install
Version
Select the version for this add-on.
v1.11.1-eksbuild.4
kube-proxy Info
Remove add-on
Category
networking
Status
Ready to install



aws eks --region us-east-2 describe-cluster --name ashokeks --query cluster.status



aws eks --region us-east-2 describe-cluster --name ashokeks

```
"ACTIVE"
ubuntu@ip-172-31-22-104:~$ aws eks --region us-east-2 describe-cluster --name ashokeks
{
    "cluster": {
        "name": "ashokeks",
        "arn": "arn:aws:eks:us-east-2:084828591376:cluster/ashokeks",
        "createdAt": "2024-09-14T16:51:56.526000+00:00",
        "version": "1.29",
        "endpoint": "https://C9BEFD569F5FCE0FFC61C98CF664A599.gr7.us-east-2.eks.amazonaws.com",
        "roleArn": "arn:aws:iam::084828591376:role/EKSClusterRole",
        "resourcesVpcConfig": {
            "subnetIds": [
                "subnet-03c4a4722f26e7d28",
                "subnet-09c5d47c1a38ef3eb",
                "subnet-00314fc059da5c7c4"
            ],
            "securityGroupIds": [
                "sg-0cc02f3cf747a6da7"
            ],
            "clusterSecurityGroupId": "sg-0077e51f197e81249",
            "vpcId": "vpc-0c8b0ada87e026b2f",
            "endpointPublicAccess": true,
            "endpointPrivateAccess": false,
            "publicAccessCidrs": [
                "0.0.0.0/0"
            ]
        },
        "kubernetesNetworkConfig": {
            "serviceIpv4Cidr": "10.100.0.0/16",
            "ipFamily": "ipv4"
        },
        "logging": {
            "clusterLogging": [
                {
                    "types": [
                        "api",
                        "audit",
                        "authenticator",
                        "controllerManager",
                        "scheduler"
                    ],
                    "enabled": false
```


Setup up the kubectl configuration

aws eks --region us-east-2 describe-cluster --name ashokeks --query cluster.status

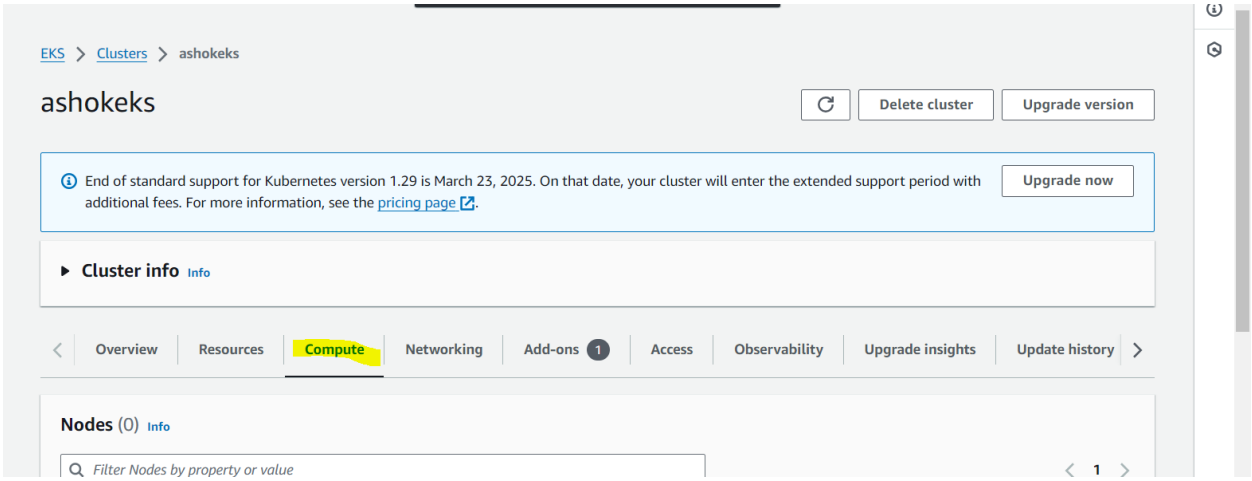
aws eks --region us-east-2 describe-cluster --name ashokeks

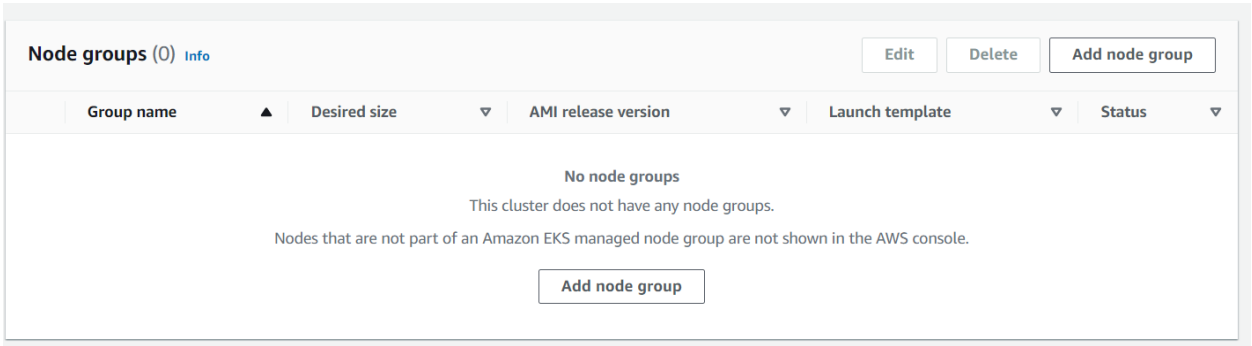
aws eks --region us-east-2 update-kubeconfig --name ashokeks

```
ubuntu@ip-172-31-22-104:~$ aws eks --region us-east-2 update-kubeconfig --name ashok-eks-cluster-cli

An error occurred (ResourceNotFoundException) when calling the DescribeCluster operation: No cluster found for name: ashok-eks-cluster-cli.
ubuntu@ip-172-31-22-104:~$ aws eks --region us-east-2 update-kubeconfig --name ashokeks
Added new context arn:aws:eks:us-east-2:084828591376:cluster/ashokeks to /home/ubuntu/.kube/config
ubuntu@ip-172-31-22-104:~$ kubectl get svc
NAME         TYPE        CLUSTER-IP   EXTERNAL-IP   PORT(S)   AGE
kubernetes   ClusterIP   10.100.0.1   <none>        443/TCP   23m
ubuntu@ip-172-31-22-104:~$ kubectl get nodes
No resources found
ubuntu@ip-172-31-22-104:~$ kubectl get all
NAME                 TYPE        CLUSTER-IP   EXTERNAL-IP   PORT(S)   AGE
service/kubernetes   ClusterIP   10.100.0.1   <none>        443/TCP   25m
ubuntu@ip-172-31-22-104:~$
```

HOW ADD WORER NODE IN TO THE EKS CLUSTER





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.

AshokManagedNode

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

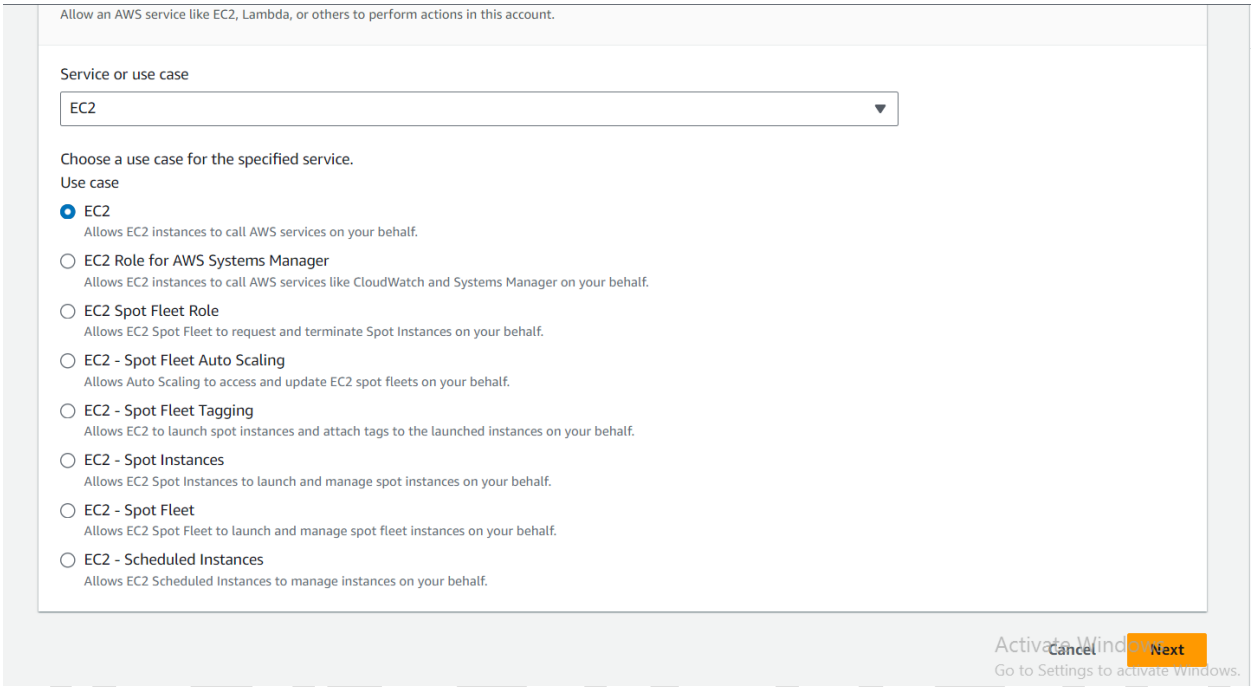
Select the IAM role that will be used by the nodes. To create a new role, go to the IAM console.

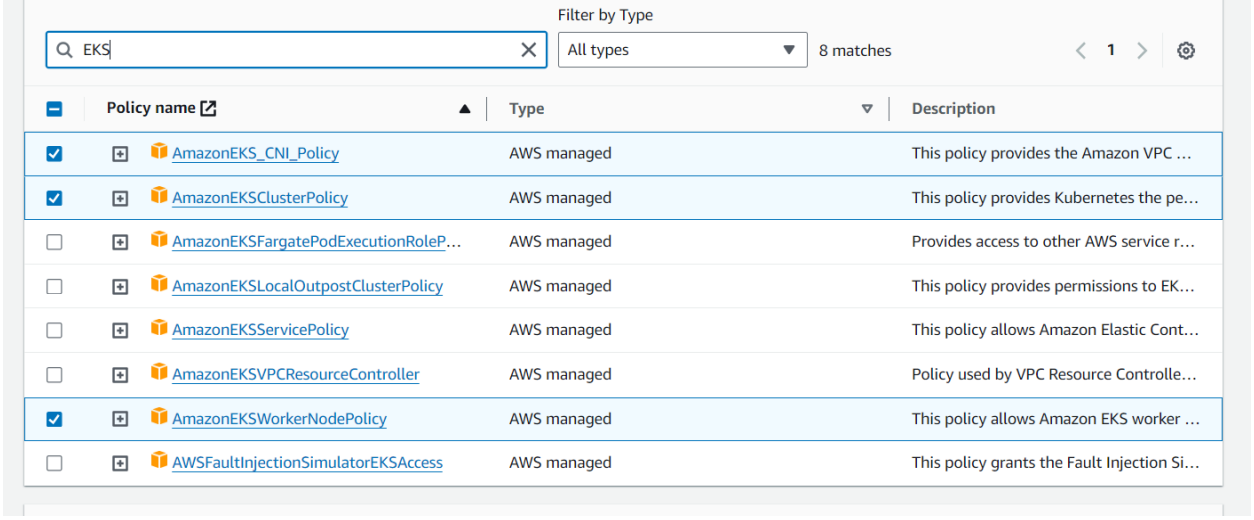
Select role

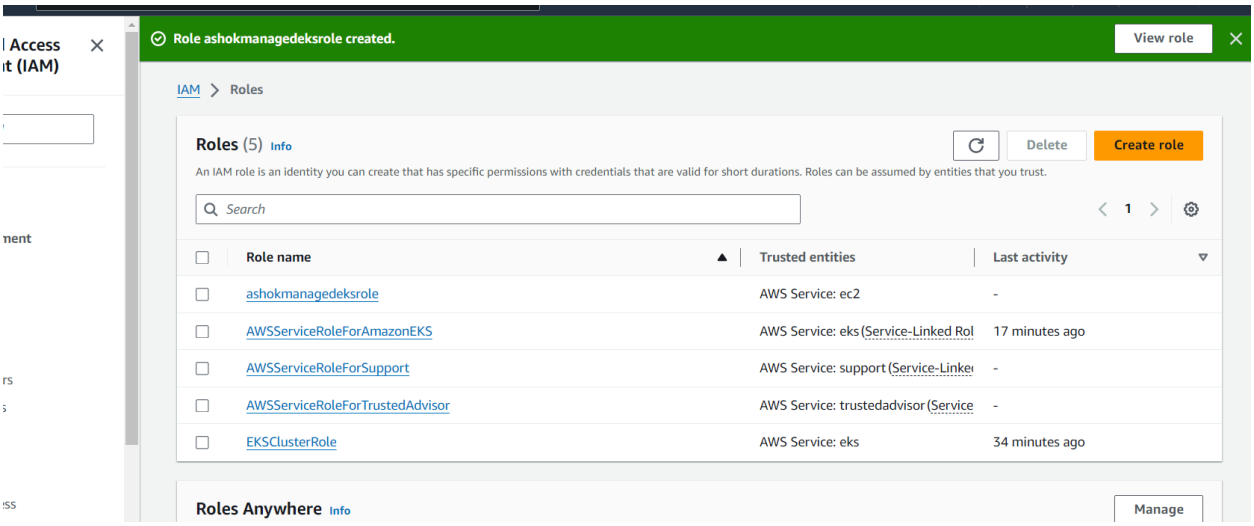
The selected role must not be used by a self-managed node group as this could lead to a service interruption upon managed node group deletion.

Learn more

Create a role in IAM console


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
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
EC2 - Spot Instances
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.
EC2 - Spot Fleet
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.
EC2 - Scheduled Instances
Allows EC2 Scheduled Instances to manage instances on your behalf.
Cancel
Next
Activate Windows
Go to Settings to activate Windows.


Filter by Type
EKS
All types
8 matches
1
Policy name
Type
Description
AmazonEKS_CNI_Policy
AWS managed
This policy provides the Amazon VPC ...
AmazonEKSClusterPolicy
AWS managed
This policy provides Kubernetes the pe...
AmazonEKSFargatePodExecutionRoleP...
AWS managed
Provides access to other AWS service r...
AmazonEKSLocalOutpostClusterPolicy
AWS managed
This policy provides permissions to EK...
AmazonEKSServicePolicy
AWS managed
This policy allows Amazon Elastic Cont...
AmazonEKSVPCResourceController
AWS managed
Policy used by VPC Resource Controlle...
AmazonEKSWorkerNodePolicy
AWS managed
This policy allows Amazon EKS worker ...
AWSFaultInjectionSimulatorEKSAccess
AWS managed
This policy grants the Fault Injection Si...



Name

Assign a unique name for this node group.

AshokManagedNode

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.

ashokmanagedeksrole

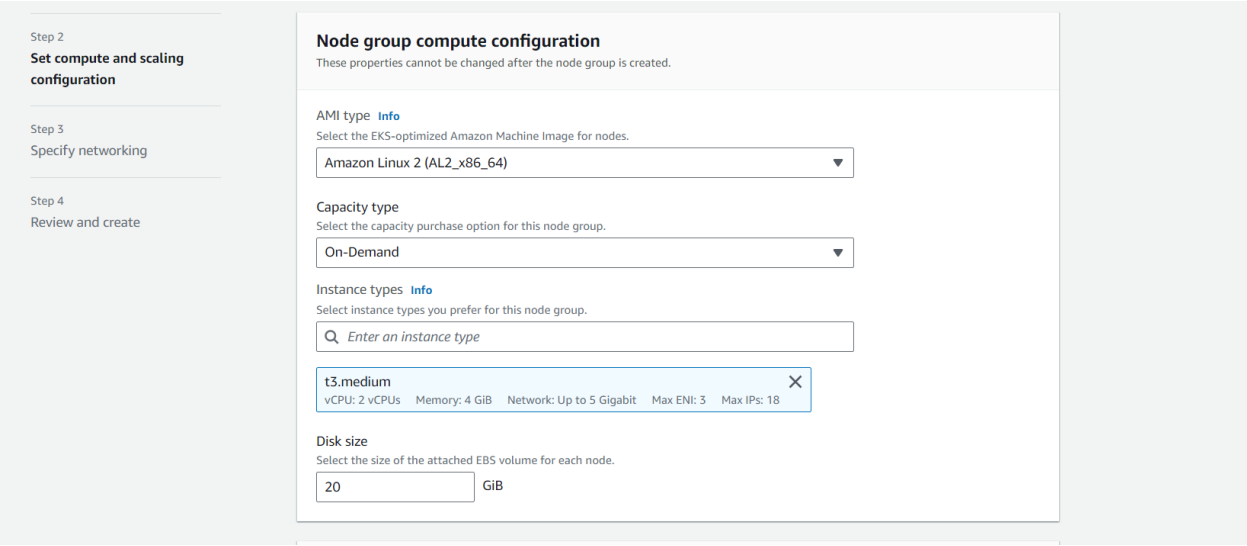
The selected role must not be used by a self-managed node group as this could lead to a service interruption upon managed node group deletion.

Learn more

Create a role in IAM console

Launch template **Info**

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



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

Set compute and scaling configuration

Step 3
Specify networking

Step 4
Review and create

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-03c4a4722f26e7d28 — us-east-2b 172.31.16.0/20
- subnet-09c5d47c1a38ef3eb — us-east-2a 172.31.0.0/20
- subnet-00314fc059da5c7c4 — us-east-2c 172.31.32.0/20

Clear selected subnets

[x] Configure remote access to nodes Info

EC2 Key Pair

Select an EC2 key pair to allow secure remote access to your nodes. To create a new EC2 key pair, go to the corresponding page in the EC2 console.

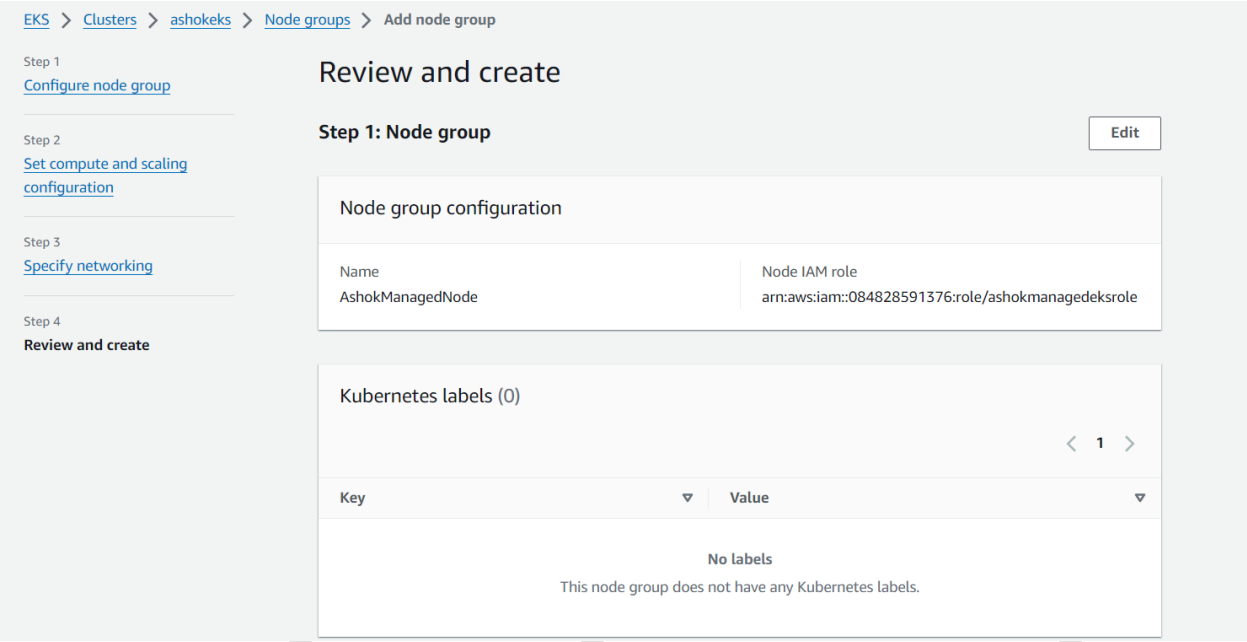
AWSEKS

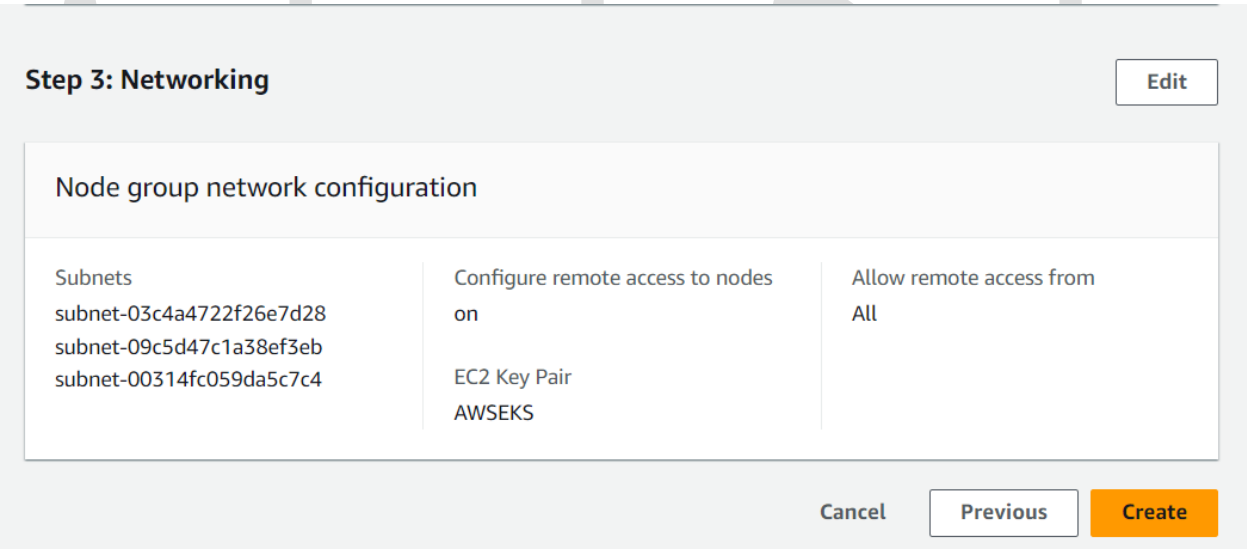
Allow remote access from

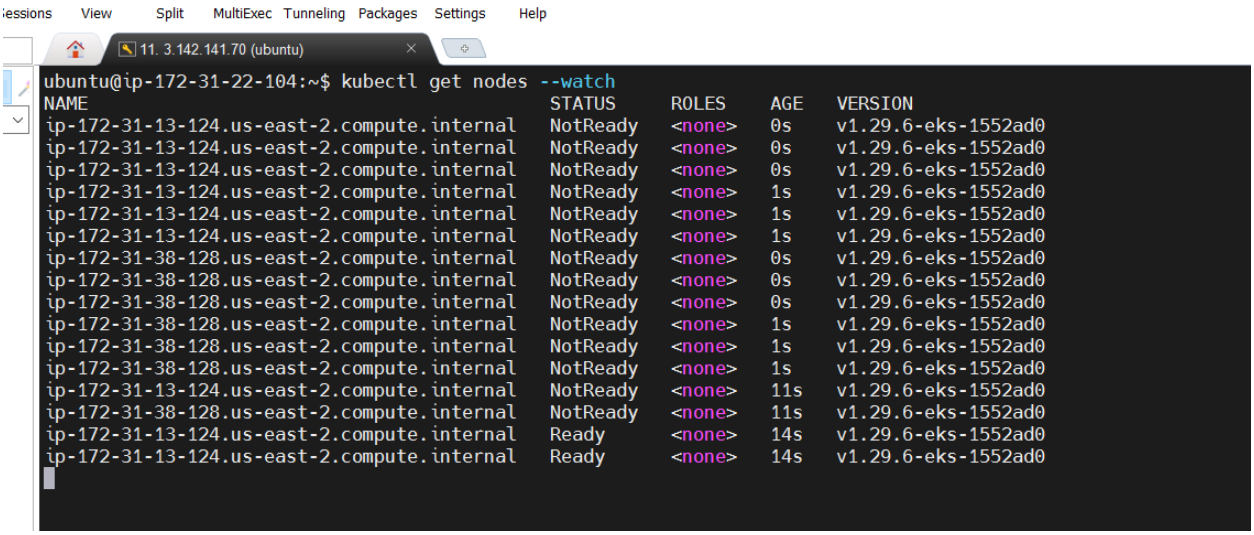
Configure the SSH client source IP ranges that can remotely access nodes.

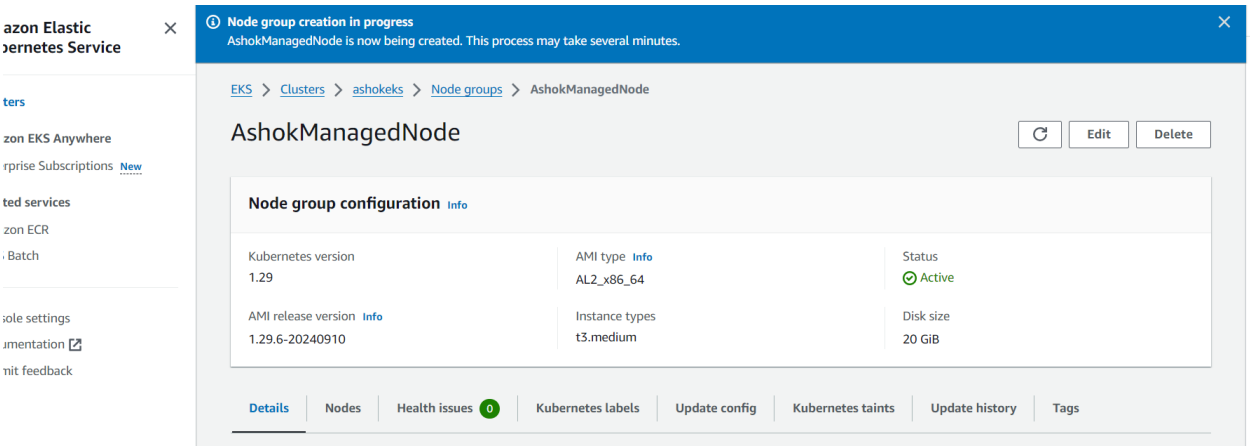
- ( ) Selected security groups — Specify security groups to restrict which source IPs can remotely access nodes.
- (●) All — Do not restrict source IPs that can remotely access nodes.

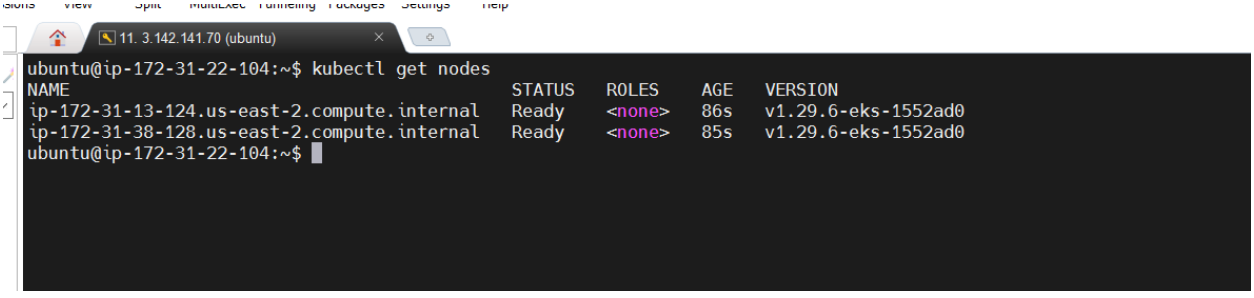
Cancel | Previous | Next


EKS > Clusters > ashokeks > 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
Review and create
Step 1: Node group
Edit
Node group configuration
Name
AshokManagedNode
Node IAM role
arn:aws:iam::084828591376:role/ashokmanagedeksrole
Kubernetes labels (0)
1
Key
Value
No labels
This node group does not have any Kubernetes labels.


Step 3: Networking
Edit
Node group network configuration
Subnets
subnet-03c4a4722f26e7d28
subnet-09c5d47c1a38ef3eb
subnet-00314fc059da5c7c4
Configure remote access to nodes
on
EC2 Key Pair
AWSEKS
Allow remote access from
All
Cancel
Previous
Create


essions View Split MultiExec Tunneling Packages Settings Help
11. 3.142.141.70 (ubuntu)
ubuntu@ip-172-31-22-104:~$ kubectl get nodes --watch
NAME STATUS ROLES AGE VERSION
ip-172-31-13-124.us-east-2.compute.internal NotReady <none> 0s v1.29.6-eks-1552ad0
ip-172-31-13-124.us-east-2.compute.internal NotReady <none> 0s v1.29.6-eks-1552ad0
ip-172-31-13-124.us-east-2.compute.internal NotReady <none> 0s v1.29.6-eks-1552ad0
ip-172-31-13-124.us-east-2.compute.internal NotReady <none> 1s v1.29.6-eks-1552ad0
ip-172-31-13-124.us-east-2.compute.internal NotReady <none> 1s v1.29.6-eks-1552ad0
ip-172-31-13-124.us-east-2.compute.internal NotReady <none> 1s v1.29.6-eks-1552ad0
ip-172-31-38-128.us-east-2.compute.internal NotReady <none> 0s v1.29.6-eks-1552ad0
ip-172-31-38-128.us-east-2.compute.internal NotReady <none> 0s v1.29.6-eks-1552ad0
ip-172-31-38-128.us-east-2.compute.internal NotReady <none> 0s v1.29.6-eks-1552ad0
ip-172-31-38-128.us-east-2.compute.internal NotReady <none> 1s v1.29.6-eks-1552ad0
ip-172-31-38-128.us-east-2.compute.internal NotReady <none> 1s v1.29.6-eks-1552ad0
ip-172-31-38-128.us-east-2.compute.internal NotReady <none> 1s v1.29.6-eks-1552ad0
ip-172-31-13-124.us-east-2.compute.internal NotReady <none> 11s v1.29.6-eks-1552ad0
ip-172-31-38-128.us-east-2.compute.internal NotReady <none> 11s v1.29.6-eks-1552ad0
ip-172-31-13-124.us-east-2.compute.internal Ready <none> 14s v1.29.6-eks-1552ad0
ip-172-31-13-124.us-east-2.compute.internal Ready <none> 14s v1.29.6-eks-1552ad0


azon Elastic
bernetes Service
ters
zon EKS Anywhere
rprise Subscriptions New
ted services
zon ECR
Batch
sole settings
umentation
nit feedback
Node group creation in progress
AshokManagedNode is now being created. This process may take several minutes.
EKS > Clusters > ashokeks > Node groups > AshokManagedNode
AshokManagedNode
Edit
Delete
Node group configuration Info
Kubernetes version
1.29
AMI type Info
AL2_x86_64
Status
Active
AMI release version Info
1.29.6-20240910
Instance types
t3.medium
Disk size
20 GiB
Details
Nodes
Health issues 0
Kubernetes labels
Update config
Kubernetes taints
Update history
Tags


11. 3.142.141.70 (ubuntu)
ubuntu@ip-172-31-22-104:~$ kubectl get nodes
NAME STATUS ROLES AGE VERSION
ip-172-31-13-124.us-east-2.compute.internal Ready <none> 86s v1.29.6-eks-1552ad0
ip-172-31-38-128.us-east-2.compute.internal Ready <none> 85s v1.29.6-eks-1552ad0
ubuntu@ip-172-31-22-104:~$

Ashok Polu