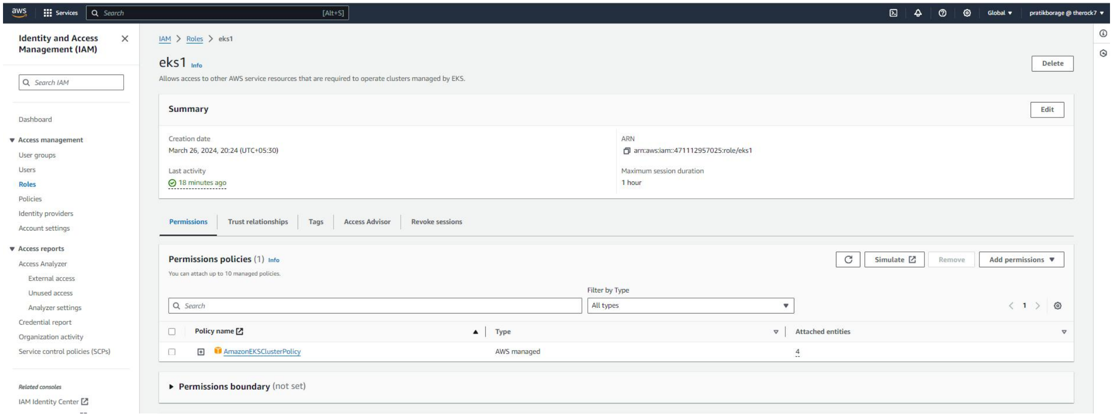
AMAZON EKS CLUSTER WITH NODEGROUP

Step 1:- Create IAM role for EKS



eks1 Info

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

Summary

Creation date: March 26, 2024, 20:24 (UTC+05:30)

ARN: arn:aws:iam::471112957025:role/eks1

Last activity: 18 minutes ago

Maximum session duration: 1 hour

Permissions policies (1) Info

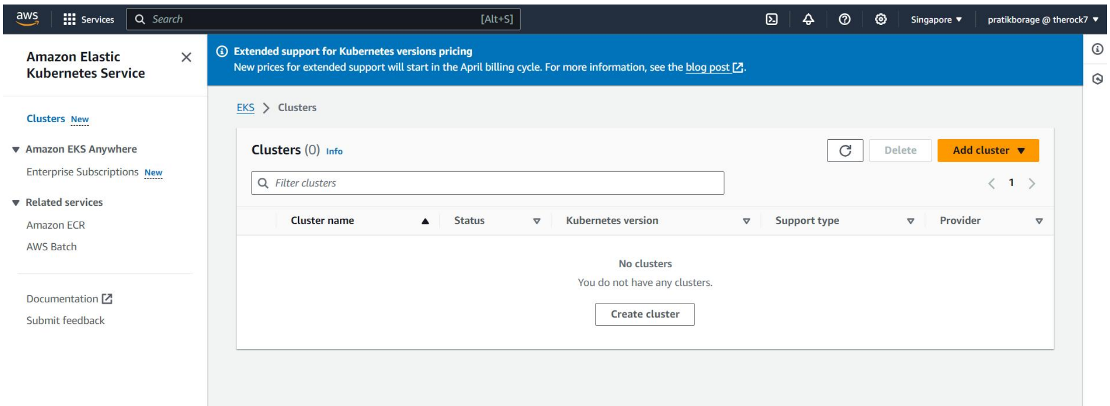
You can attach up to 10 managed policies.

Filter by Type: All types

Policy name	Type	Attached entities
AmazonEKSClusterPolicy	AWS managed	4

Permissions boundary (not set)

Step 2:- Create an EKS Cluster



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.

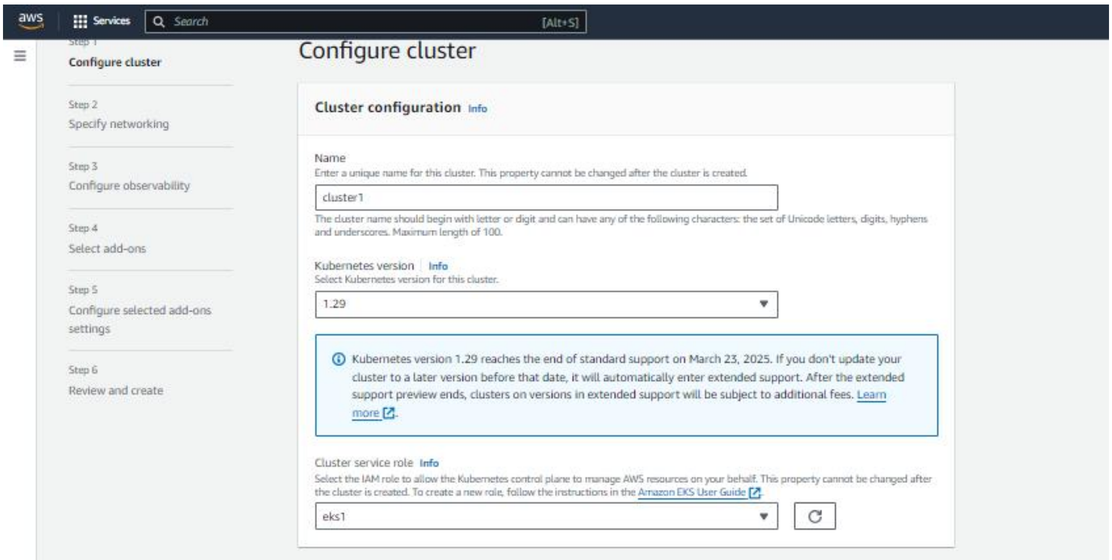
Clusters (0) Info

Cluster name	Status	Kubernetes version	Support type	Provider

No clusters

You do not have any clusters.

Configure cluster



Configure cluster

Cluster configuration Info

Name

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

cluster1

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.

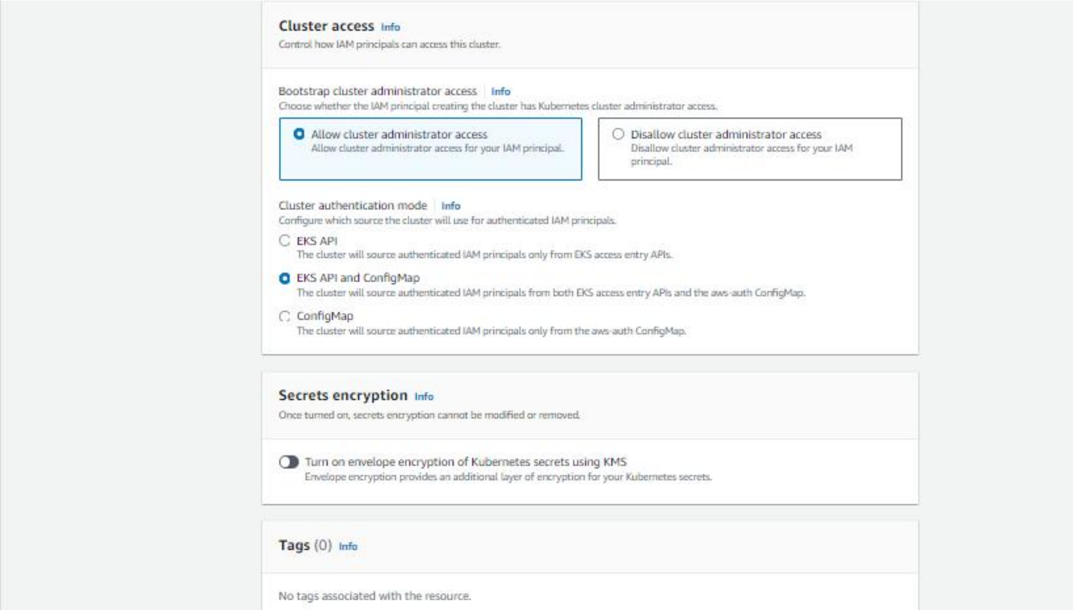
1.29

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.

eks1



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.

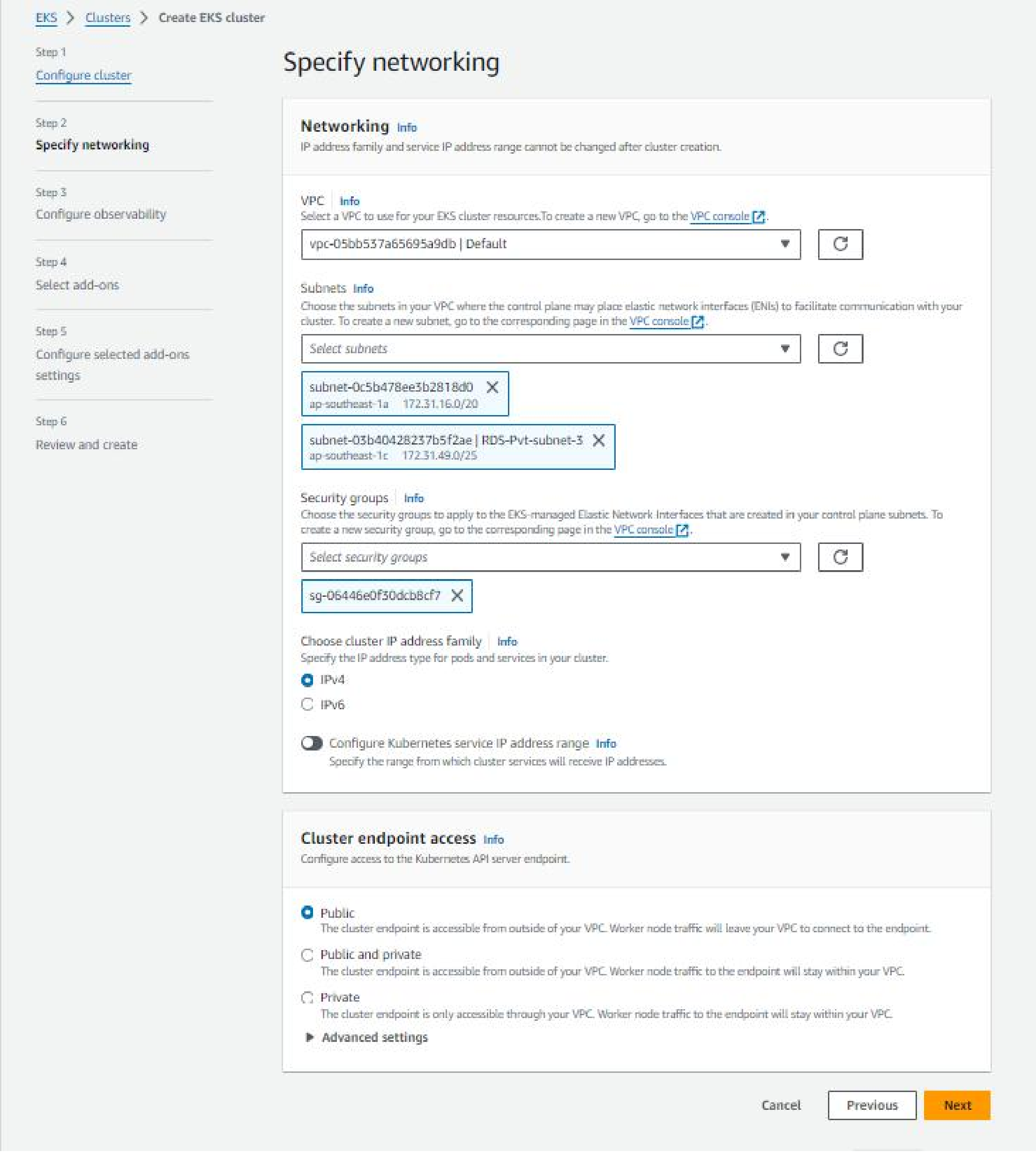
Secrets encryption Info

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.



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-05bb537a65695a9db | 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-0c5b478ee3b2818d0 ✕
ap-southeast-1a 172.31.16.0/20

subnet-03b40428237b5f2ae | RDS-Pvt-subnet-3 ✕
ap-southeast-1c 172.31.49.0/25

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-06446e0f30dcb8cf7 ✕

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

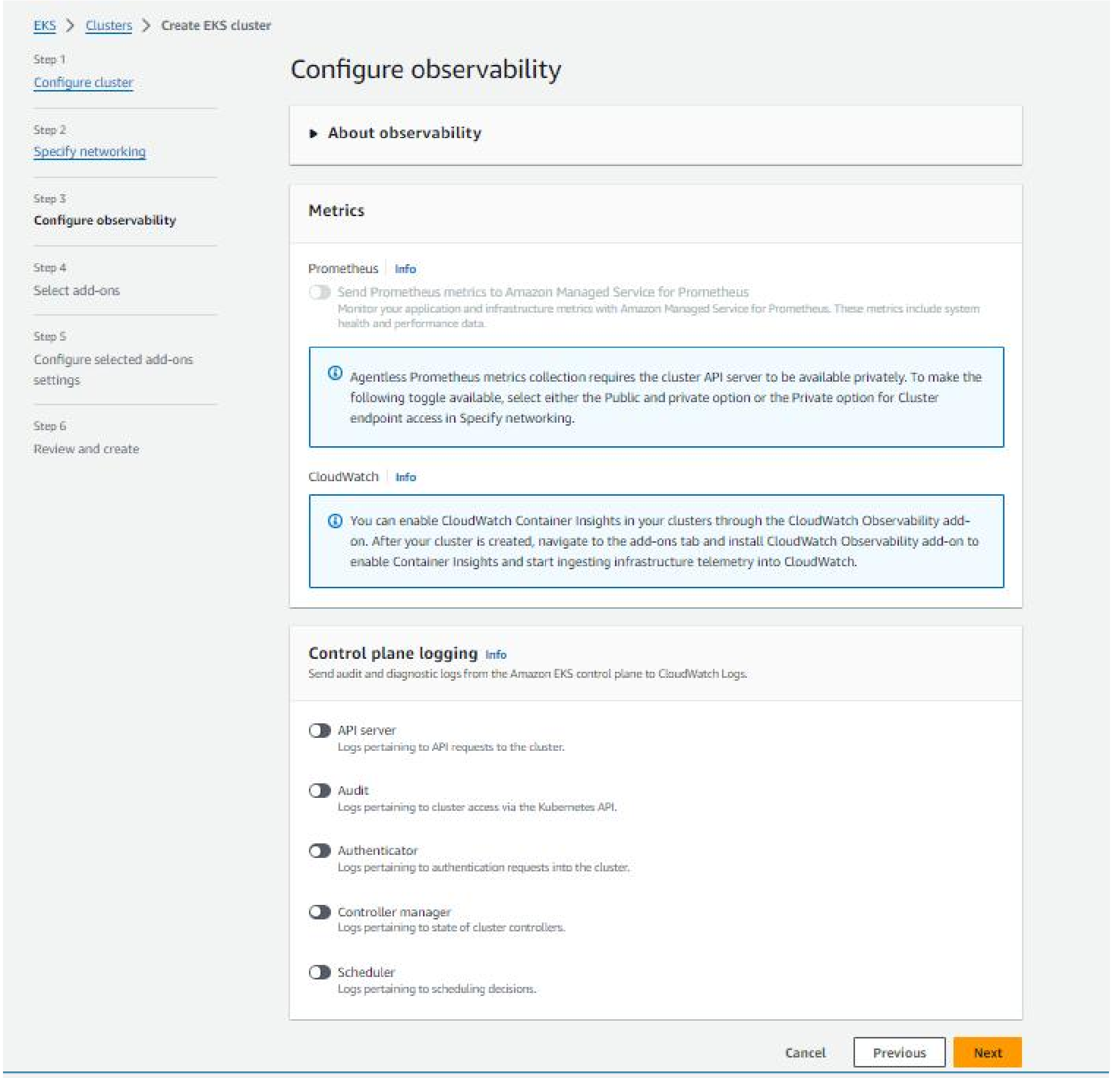
Configure access to the Kubernetes API server endpoint.

● 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



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 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.

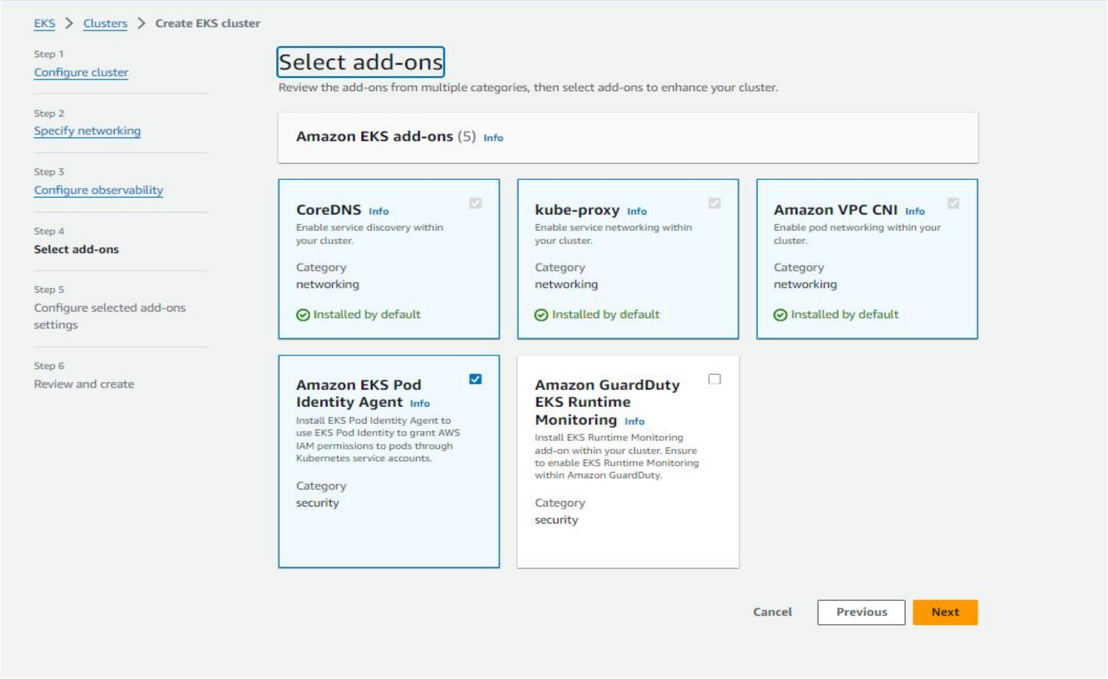
API server
Logs pertaining to API requests to the cluster.

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.



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

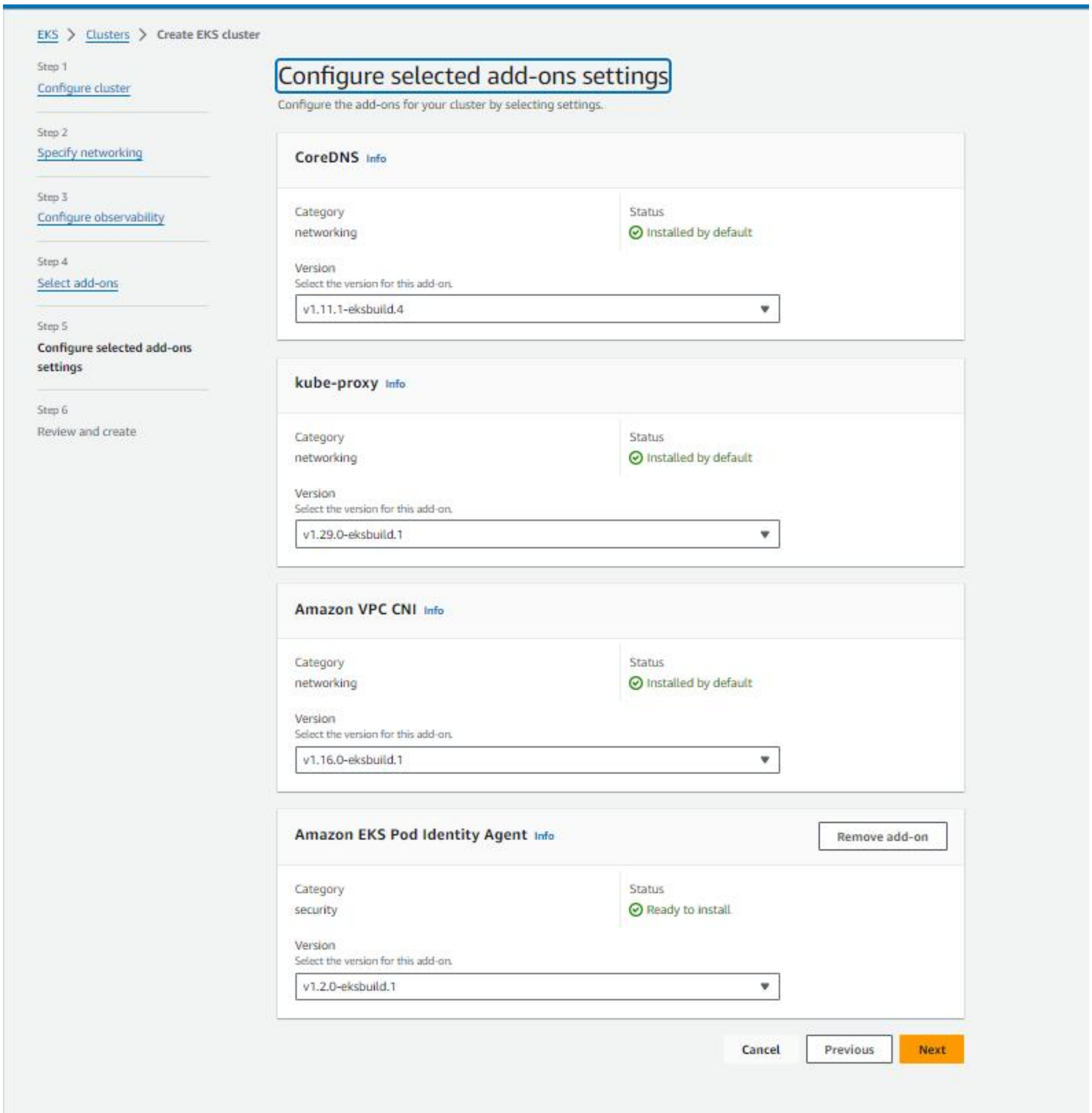
CoreDNS Info ☑
Enable service discovery within your cluster.
Category
networking
✓ Installed by default

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



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

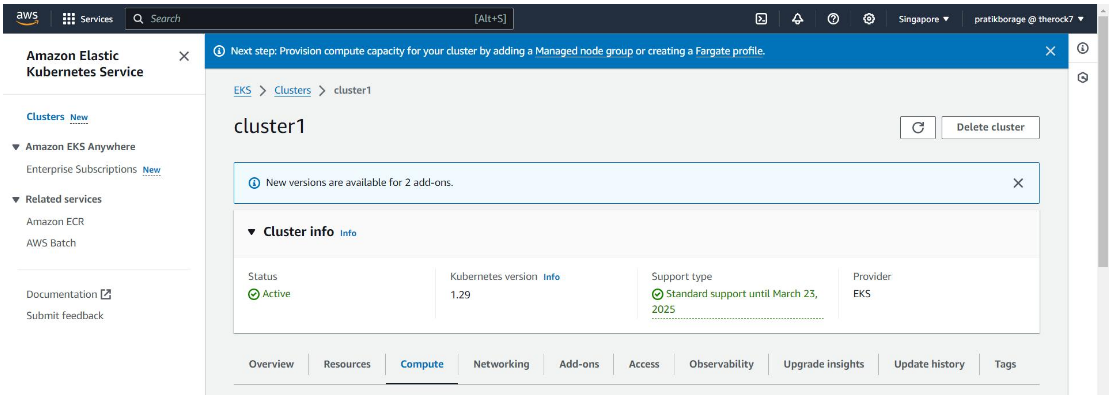
Amazon VPC CNI Info

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

Category: security
Status: ✓ Ready to install
Version — Select the version for this add-on.: v1.2.0-eksbuild.1

Cluster is created.



Next step: Provision compute capacity for your cluster by adding a Managed node group or creating a Fargate profile.

EKS > Clusters > cluster1

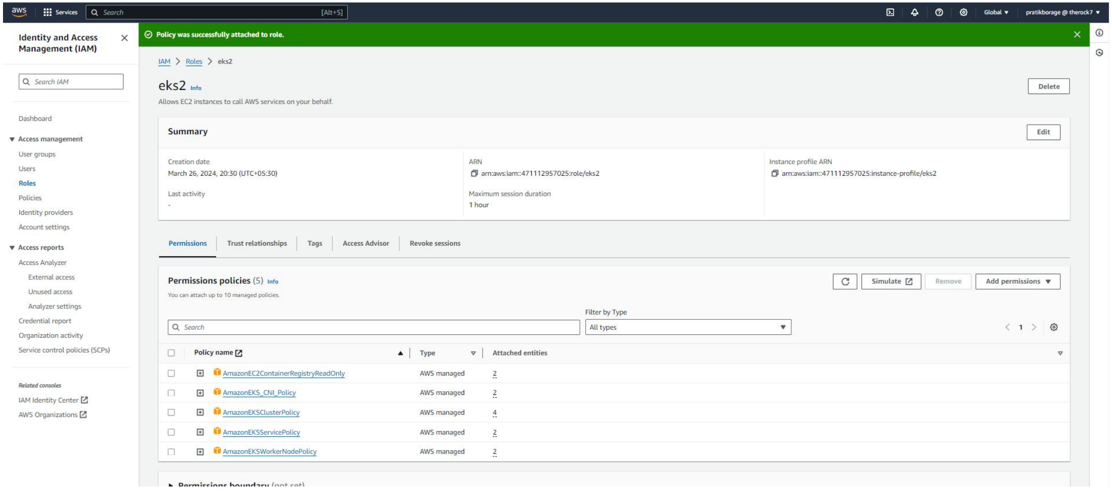
cluster1

New versions are available for 2 add-ons.

Cluster info Info

Status	Kubernetes version Info	Support type	Provider
✓ Active	1.29	✓ Standard support until March 23, 2025	EKS

Step 3:- Create IAM role for EC2 which will be used for nodegroup



Policy was successfully attached to role.

IAM > Roles > eks2

eks2 Info

Allows EC2 instances to call AWS services on your behalf.

Summary

Creation date
March 26, 2024, 20:30 (UTC+05:30)

ARN
arn:aws:iam::471112957025:role/eks2

Instance profile ARN
arn:aws:iam::471112957025:instance-profile/eks2

Last activity
-

Maximum session duration
1 hour

Permissions policies (5) Info

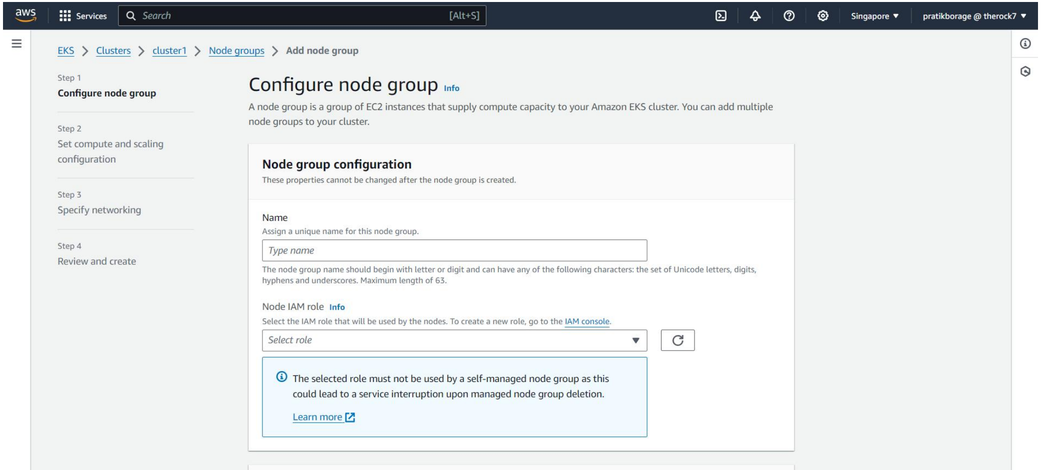
You can attach up to 10 managed policies.

Filter by Type: All types

Policy name	Type	Attached entities
AmazonEC2ContainerRegistryReadOnly	AWS managed	2
AmazonEKS_CNI_Policy	AWS managed	2
AmazonEKSClusterPolicy	AWS managed	4
AmazonEKSServicePolicy	AWS managed	2
AmazonEKSWorkerNodePolicy	AWS managed	2

Permissions boundary (not set)

Step 4:-Create nodegroup



EKS > Clusters > cluster1 > 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.

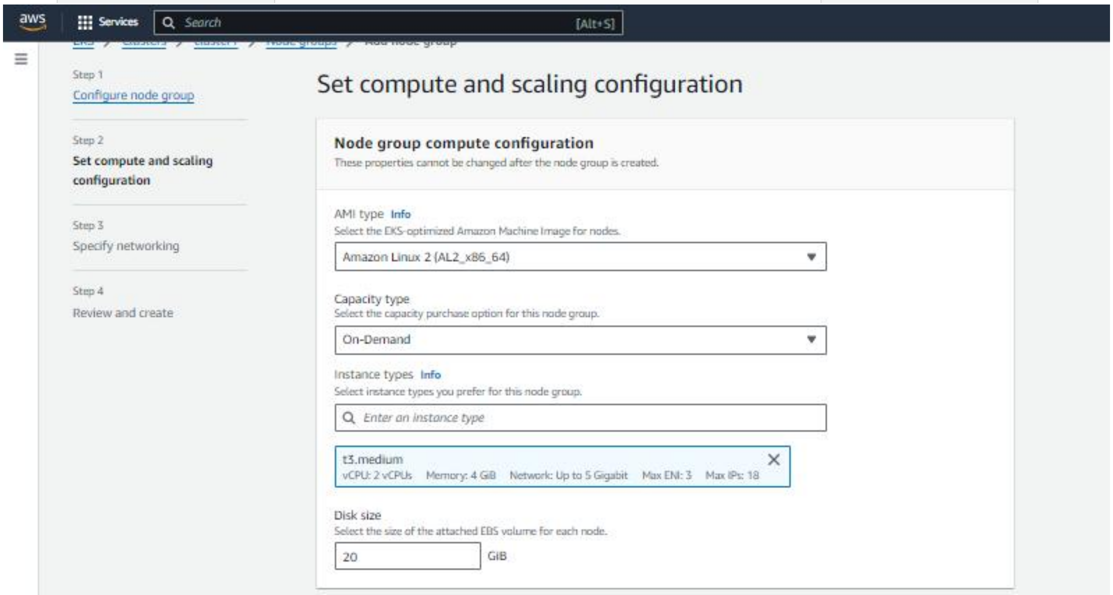
Node group configuration

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

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



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.

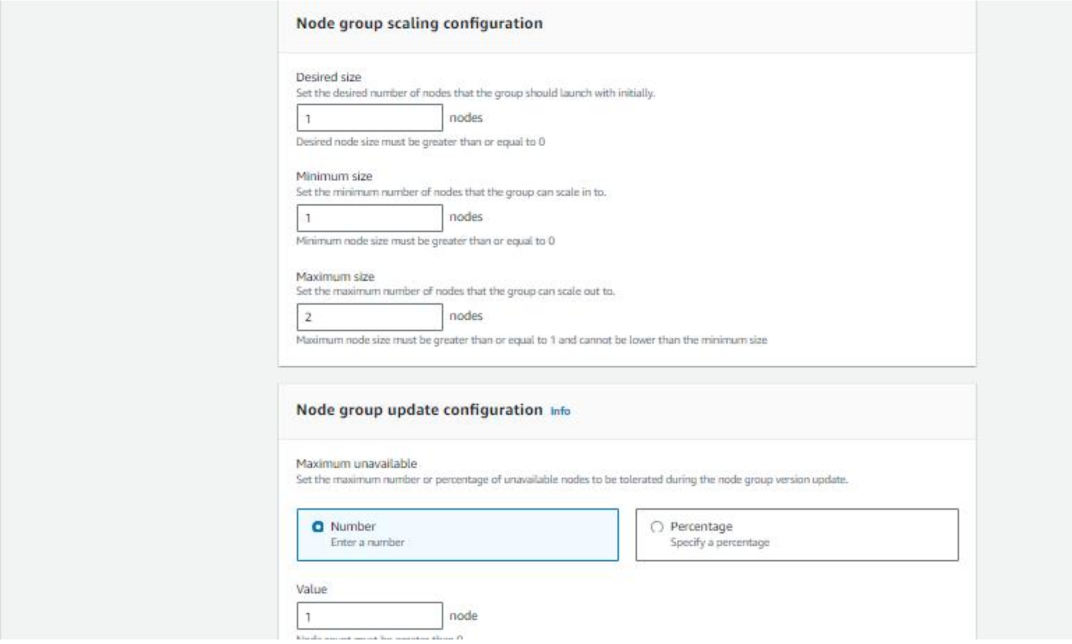
AMI type Info
Select the EKS-optimized Amazon Machine Image for nodes.
Amazon Linux 2 (AL2_x86_64)

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.
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

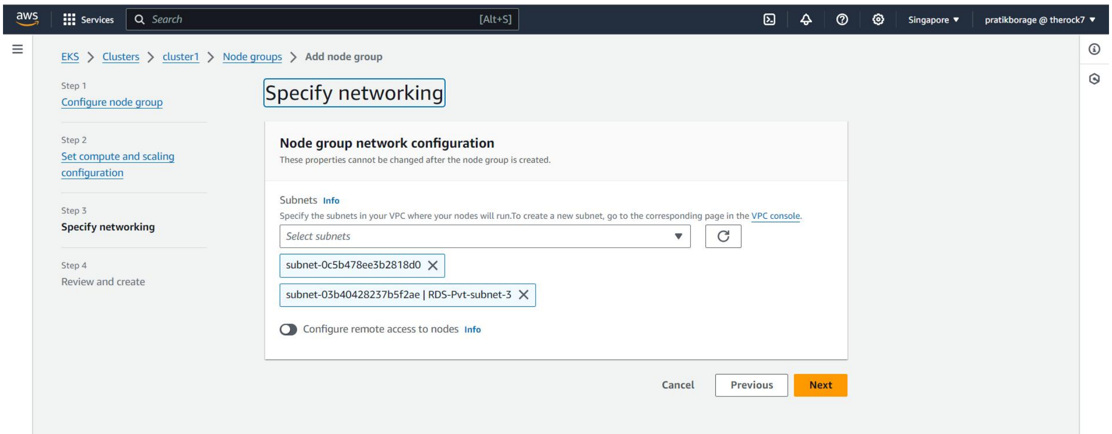
Node group update configuration Info

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



EKS > Clusters > cluster1 > 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

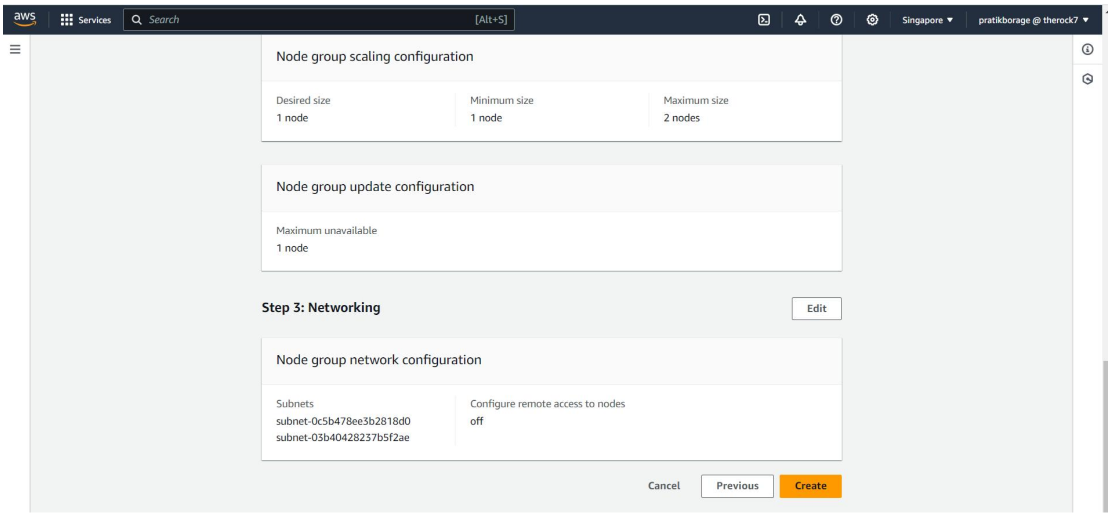
Specify networking

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-0c5b478ee3b2818d0 ✕
subnet-03b40428237b5f2ae | RDS-Pvt-subnet-3 ✕

○ Configure remote access to nodes Info

Review and create.



Node group scaling configuration

Desired size	Minimum size	Maximum size
1 node	1 node	2 nodes

Node group update configuration

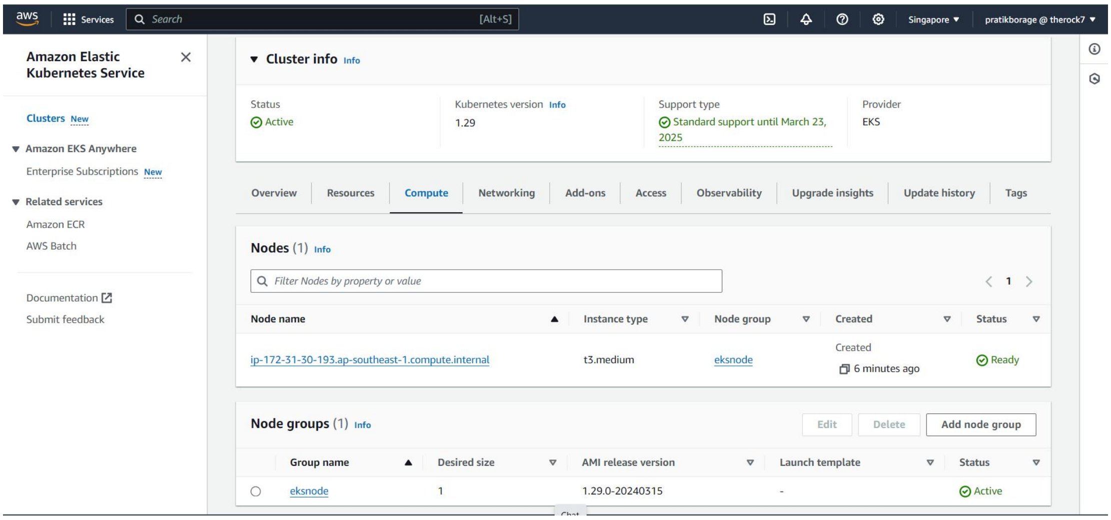
Maximum unavailable
1 node

Step 3: Networking

Node group network configuration

Subnets	Configure remote access to nodes
subnet-0c5b478ee3b2818d0 subnet-03b40428237b5f2ae	off

Cluster with nodegroup:-



Cluster info Info

Status: Active

Kubernetes version Info: 1.29

Support type: Standard support until March 23, 2025

Provider: EKS

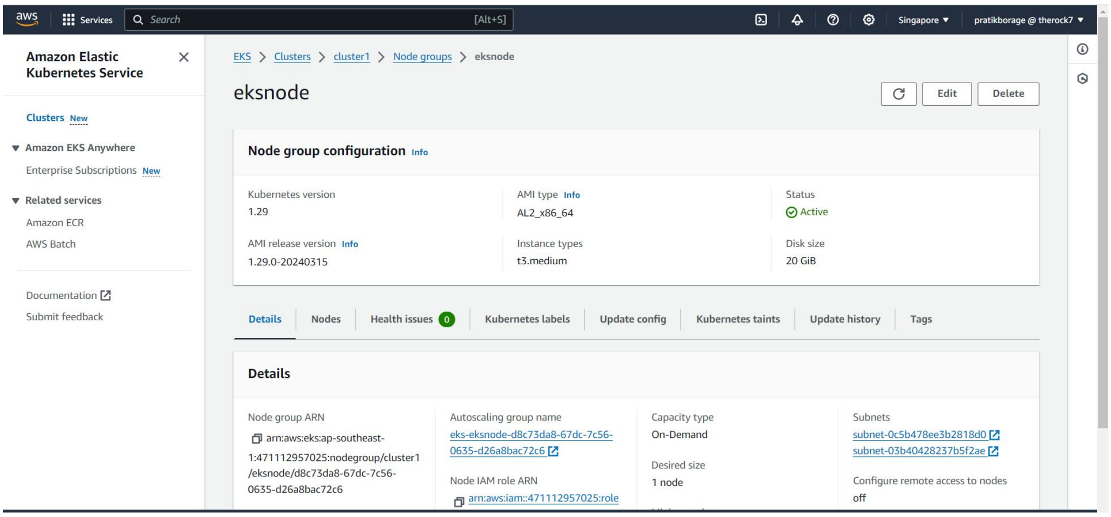
Nodes (1) Info

Filter Nodes by property or value

Node name	Instance type	Node group	Created	Status
ip-172-31-30-193.ap-southeast-1.compute.internal	t3.medium	eksnode	Created 6 minutes ago	Ready

Node groups (1) Info

Group name	Desired size	AMI release version	Launch template	Status
○ eksnode	1	1.29.0-20240315	-	Active



EKS > Clusters > cluster1 > Node groups > eksnode

eksnode

Node group configuration Info

Kubernetes version: 1.29

AMI type Info: AL2_x86_64

Status: Active

AMI release version Info: 1.29.0-20240315

Instance types: t3.medium

Disk size: 20 GiB

Details

Node group ARN: arn:aws:eks:ap-southeast-1:471112957025:nodegroup/cluster1/eksnode/d8c73da8-67dc-7c56-0635-d26a8bac72c6

Autoscaling group name: eks-eksnode-d8c73da8-67dc-7c56-0635-d26a8bac72c6

Node IAM role ARN: arn:aws:iam::471112957025:role

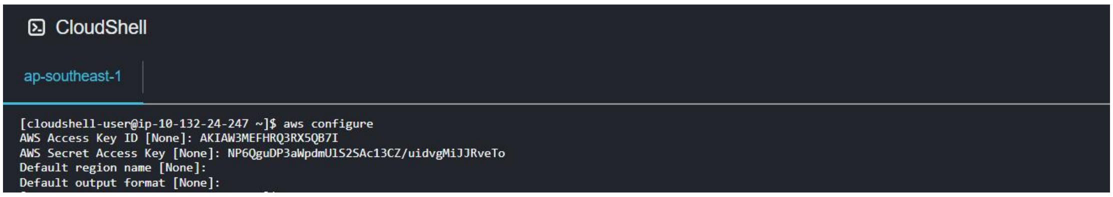
Capacity type: On-Demand

Desired size: 1 node

Subnets: subnet-0c5b478ee3b2818d0, subnet-03b40428237b5f2ae

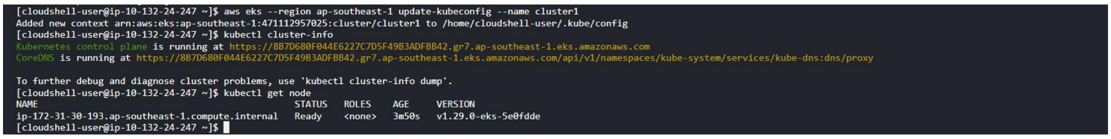
Configure remote access to nodes: off

Step 6:- Configure AWS in cloudshell



```
[cloudshell-user@ip-10-132-24-247 ~]$ aws configure
AWS Access Key ID [None]: AKIAW3MEFHRQ3RX5QB7I
AWS Secret Access Key [None]: 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
Default region name [None]:
Default output format [None]:
```

Step 7:- Checking cluster info



```
[cloudshell-user@ip-10-132-24-247 ~]$ aws eks --region ap-southeast-1 update-kubeconfig --name cluster1
Added new context arn:aws:eks:ap-southeast-1:471112957025:cluster/cluster1 to /home/cloudshell-user/.kube/config
[cloudshell-user@ip-10-132-24-247 ~]$ kubectl cluster-info
Kubernetes control plane is running at https://8B7D680F044E6227C7D5F49B3ADFBB42.gr7.ap-southeast-1.eks.amazonaws.com
CoreDNS is running at https://8B7D680F044E6227C7D5F49B3ADFBB42.gr7.ap-southeast-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-10-132-24-247 ~]$ kubectl get node
NAME                                             STATUS   ROLES    AGE     VERSION
ip-172-31-30-193.ap-southeast-1.compute.internal   Ready    <none>   3m50s   v1.29.0-eks-5e0fdde
[cloudshell-user@ip-10-132-24-247 ~]$
```