

Task

Creating an Amazon EKS (Elastic Kubernetes Service) cluster

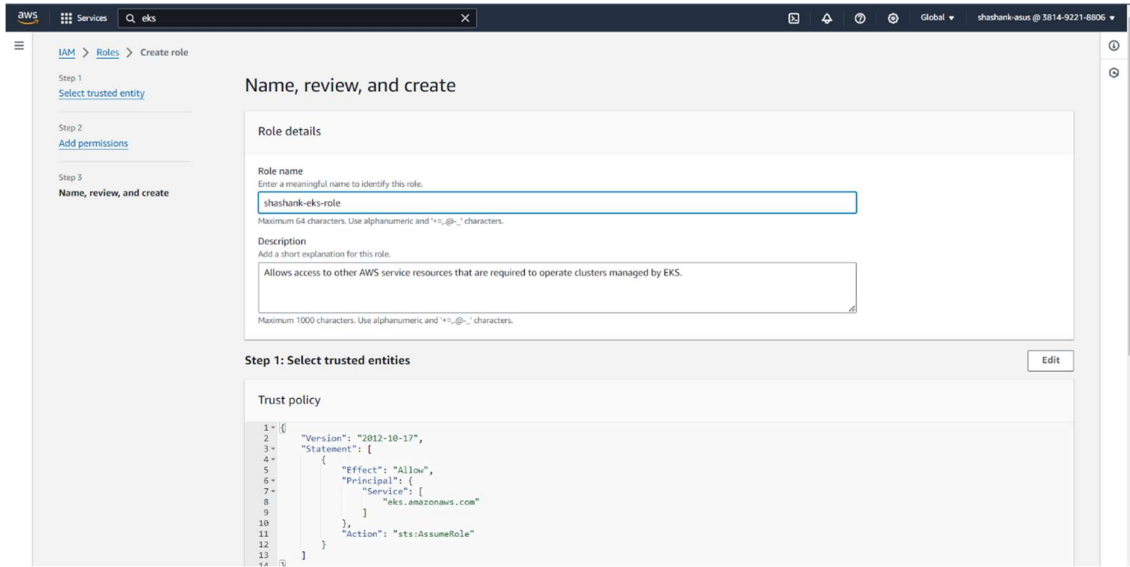
Name- Shashank Sharma

1. Set up IAM roles for EKS.

- Go to aws IAM service and create a new role for the EKS

The first screenshot shows the 'Select trusted entity' step in the AWS IAM console. The 'Trusted entity type' section has five options: 'AWS service' (selected), 'AWS account', 'Web identity', 'SAML 2.0 federation', and 'Custom trust policy'. The 'Use case' section has a dropdown menu set to 'EKS' and three radio button options: 'EKS' (unselected), 'EKS - Cluster' (selected), and 'EKS - Nodegroup' (unselected).

The second screenshot shows the 'Add permissions' step. It displays a table with one row: 'Policy name' is 'AmazonEKSClusterPolicy' and 'Type' is 'AWS managed'. Below the table is a link 'Set permissions boundary - optional'. At the bottom right are 'Cancel', 'Previous', and 'Next' buttons.



2. Create an EKS cluster.

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

The screenshot shows the 'Configure cluster' page in the Amazon EKS console. The page is divided into several sections for configuring the cluster:

- Cluster configuration:** Includes a 'Name' field with the value 'shashank-eks-cluster' and a 'Kubernetes version' dropdown set to '1.29'. A warning message states: '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](#).' The 'Cluster service role' is set to 'shashank-eks-role'.
- Cluster access:** Includes a section for 'Bootstrap cluster administrator access' with two radio buttons: 'Allow cluster administrator access' (selected) and 'Disallow cluster administrator access'. Below this is the 'Cluster authentication mode' section with three radio buttons: 'EKS API', 'EKS API and ConfigMap' (selected), and 'ConfigMap'.
- Secrets encryption:** A section with a radio button labeled 'Turn on envelope encryption of Kubernetes secrets using KMS' (selected).
- Tags:** A section titled 'Tags (0)' with a button 'Add new tag' and a note 'You can add up to 50 tags.'

At the bottom of the page, there are 'Cancel' and 'Next' buttons. The footer of the console shows 'CloudShell', 'Feedback', and copyright information for Amazon Web Services.

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-0e775bf6e85bf0ac us-west-1a 172.31.0.0/20 subnet-04a74e5846e6c229c 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-00347dff4666f2e2

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

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](#)

aws

Services

Search

[Alt+S]

N. California

shashank-asus @ 3814-9221-8806

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]

N. California

shashank-asus @ 3814-9221-8806

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

Category: security

Status: Ready to install

Version: Select the version for this add-on.
v1.2.0-eksbuild.1

Remove add-on

Cancel

Previous

Next

CloudShell Feedback

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

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

<div><div><div></div><div>Find add-on</div></div></div>			<div>< 1</div>
Add-on name	Type	Status	
coredns	networking	<div><div></div>Installed by default</div>	
eks-pod-identity-agent	security	<div><div></div>Ready to install</div>	
kube-proxy	networking	<div><div></div>Installed by default</div>	
vpc-cni	networking	<div><div></div>Installed by default</div>	

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.

The screenshot shows the 'Create role' wizard in the AWS IAM console. The left sidebar indicates the current step is 'Step 1: Select trusted entity'. The main content area is titled 'Select trusted entity' and includes an 'Info' icon. Under the 'Trusted entity type' section, five options are listed: 'AWS service' (selected), 'AWS account', 'Web identity', 'SAML 2.0 federation', and 'Custom trust policy'. The 'AWS service' option is highlighted with a blue border. Below this, the 'Use case' section is visible, showing 'EC2' selected in the 'Service or use case' dropdown. Under 'Choose a use case for the specified service', the 'EC2' option is selected, with a description: 'Allows EC2 instances to call AWS services on your behalf.' Other options include 'EC2 Role for AWS Systems Manager' and 'EC2 Spot Fleet Role'.

Step 1: 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

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

Step 2: Add permissions

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.

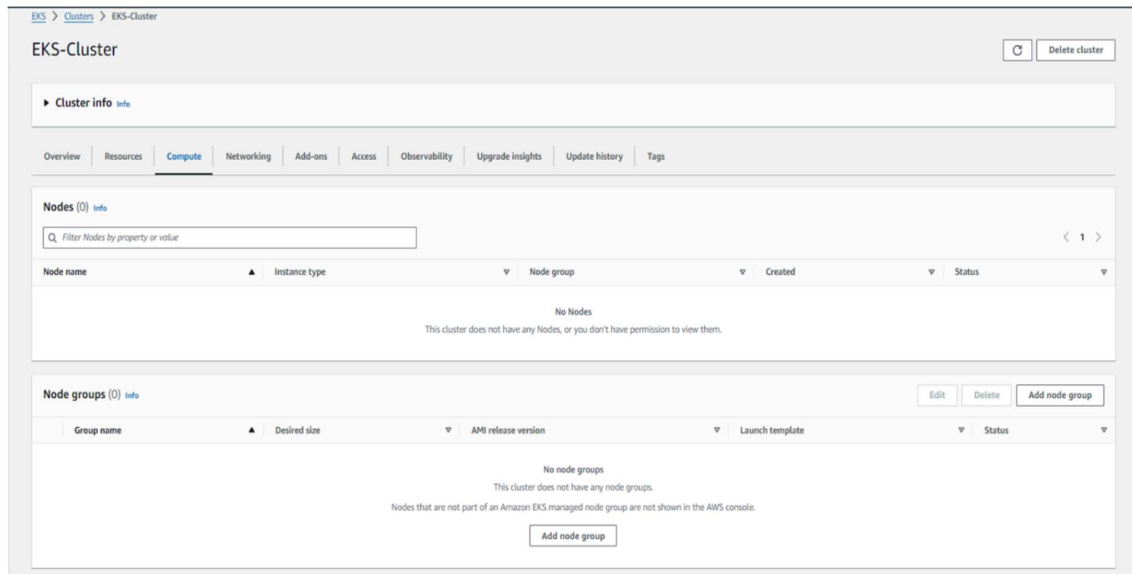
- Open aws cloudshell & configure aws.

The screenshot shows the AWS CloudShell interface. The top bar displays 'CloudShell' and the region 'us-west-1'. The terminal window shows the command `aws configure` being executed. The output displays the configuration details for the AWS CLI, including the Access Key ID and Secret Access Key, which are redacted with a white oval. The default region is set to 'us-west-1' and the default output format is 'None'.

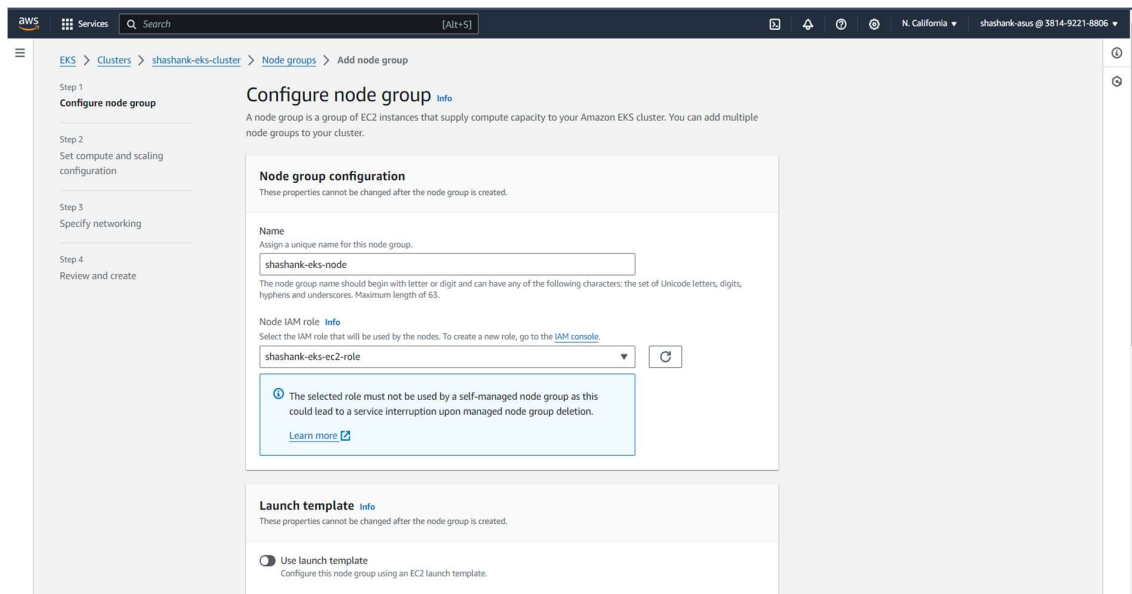
```
[cloudshell-user@ip-10-4-18-207 ~]$ aws configure
AWS Access Key ID [None]:
AWS Secret Access Key [None]:
Default region name [us-west-1]:
Default output format [None]:
[cloudshell-user@ip-10-4-18-207 ~]$
```

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”.



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

The screenshot displays the AWS Management Console interface for configuring a new node group. The breadcrumb navigation shows the path: EKS > Clusters > shashank-eks-cluster > Node groups > Add node group. The left-hand navigation pane lists four steps: Step 1 (Configure node group), Step 2 (Set compute and scaling configuration - currently active), Step 3 (Specify networking), and Step 4 (Review and create). The main content area is titled 'Set compute and scaling configuration' and contains three sections: 'Node group compute configuration', 'Node group scaling configuration', and 'Node group update configuration'. In the 'Node group compute configuration' section, the AMI type is set to 'Amazon Linux 2 (AL2_x86_64)', the capacity type is 'On-Demand', the instance type is 't3.medium' (shown in a dropdown menu), and the disk size is '20 GiB'. The 'Node group scaling configuration' section shows 'Desired size' as 1, 'Minimum size' as 1, and 'Maximum size' as 2. The 'Node group update configuration' section has 'Maximum unavailable' set to 'Number' with a value of 1. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

aws Services Search [Alt+S] N. California shashank-asus @ 3814-9221-8806

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.
Enter an instance type
t3.medium vCPU: 2 vCPUs Memory: 4 GiB Network: Up to 5 Gbps Max ENI: 3 Max IPI: 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.

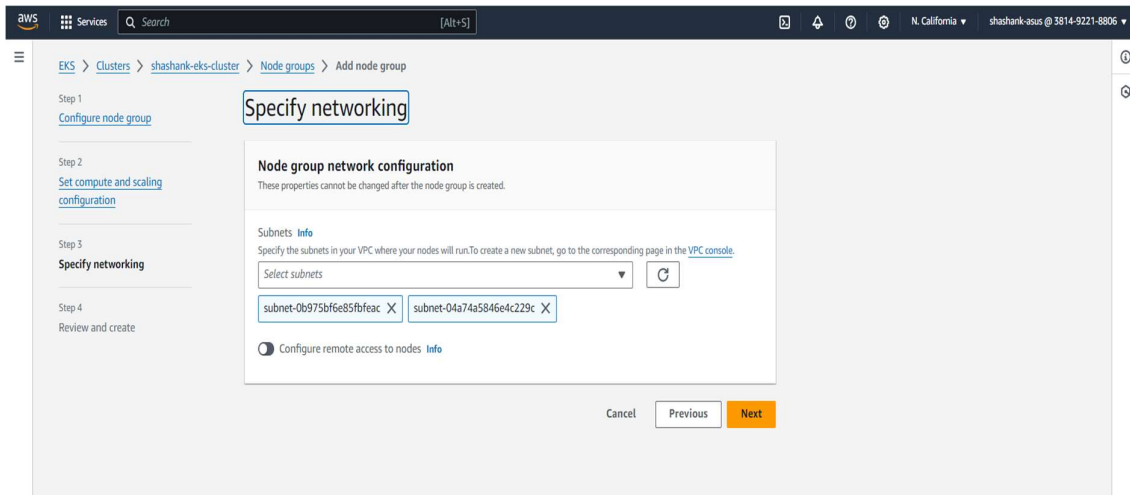
☒ Number Enter a number ☐ Percentage Specify a percentage

Value
1 node
Node count must be greater than 0.

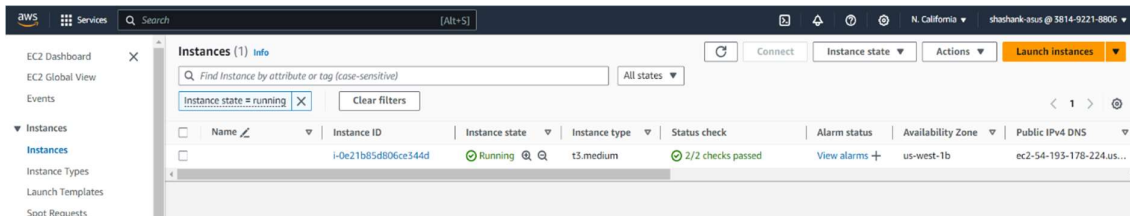
Cancel Previous **Next**

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]: AKIAVRUVJ03GSDVAFXB
AWS Secret Access Key [*****3fh]: jZ5YTVWA6ywKzfe/KnN/yReJyQtHIWhXZpaf/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 ~]$
```