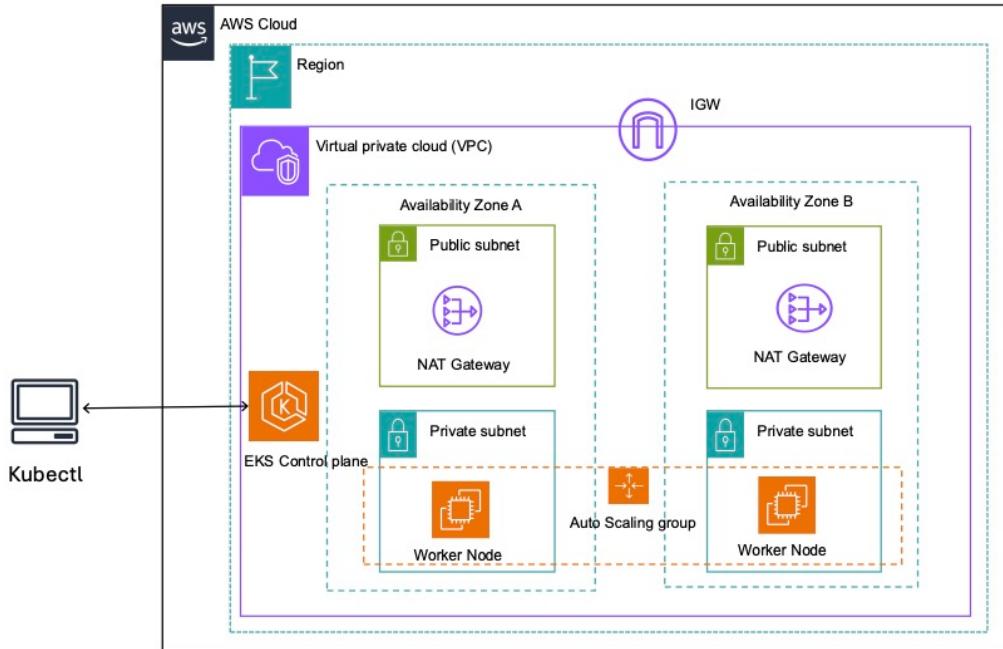


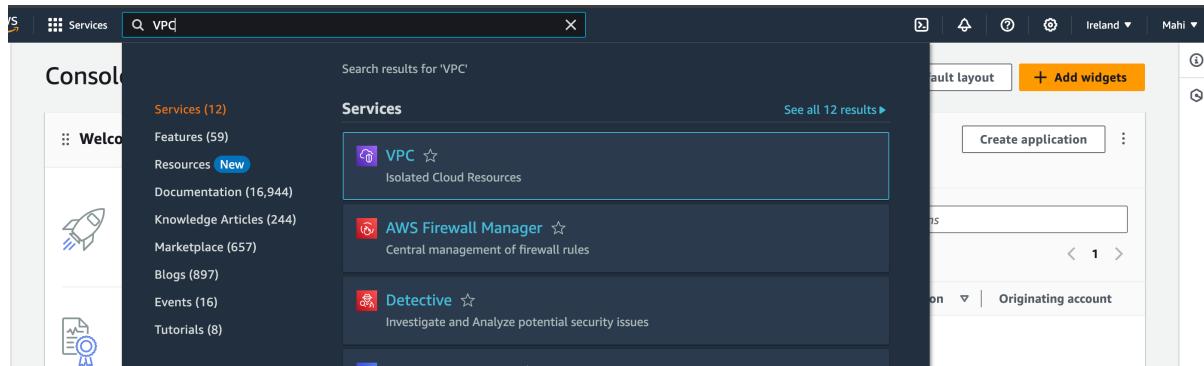
# Deploying a Production-Ready Amazon EKS Cluster



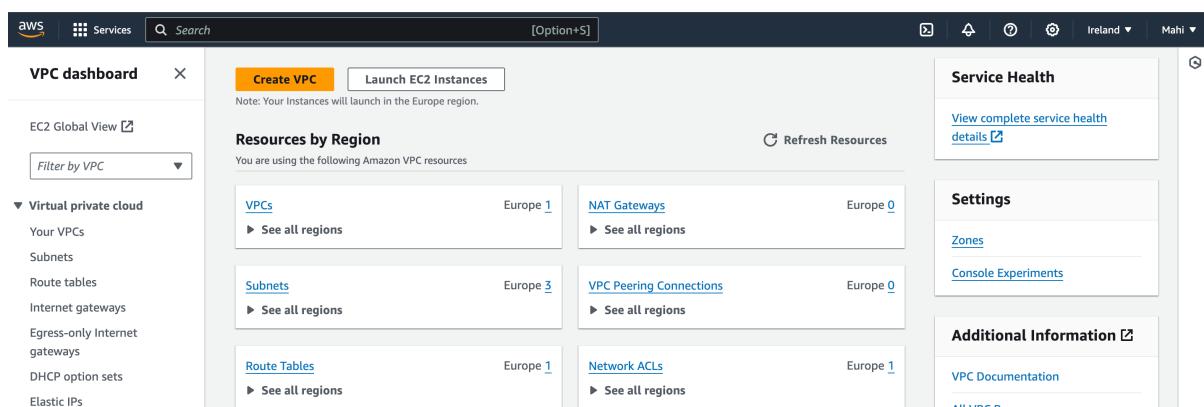
By  
Mahendran Selvakumar  
<https://devopstronaut.com/>

## 1. Create your Own VPC Network

Search for 'VPC' in the AWS Management Console and click on 'VPC'



Click "Create VPC"



Choose 'VPC and more,' then provide the Name tag for auto-generation and set the CIDR block as 10.0.0.0/16

The screenshot shows the 'Create VPC' configuration page. Under 'VPC settings', the 'Resources to create' dropdown is set to 'VPC and more'. The 'Name tag auto-generation' field has 'Auto-generate' checked and contains 'devopstronaut'. The 'IPv4 CIDR block' field is set to '10.0.0.0/16'. Under 'Tenancy', 'Default' is selected. On the right, the 'Preview' section shows the newly created VPC named 'devopstronaut-vpc' and its associated Subnets (4) under the 'eu-west-1a' and 'eu-west-1b' route tables.

Choose the tenancy, number of Availability Zones, number of Public Subnets, number of Private Subnets, and set the NAT gateways to 1 per AZ

Tenancy [Info](#)

Default



Number of Availability Zones (AZs) [Info](#)

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1    2    3

► **Customize AZs**

Number of public subnets [Info](#)

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0    2

Number of private subnets [Info](#)

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0    2    4

► **Customize subnets CIDR blocks**

NAT gateways (\$) [Info](#)

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None    In 1 AZ    1 per AZ

If desired, you can enable VPC endpoints; otherwise, choose 'None' and click 'Create VPC'

## VPC endpoints [Info](#)

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

**None**

**S3 Gateway**

## DNS options [Info](#)

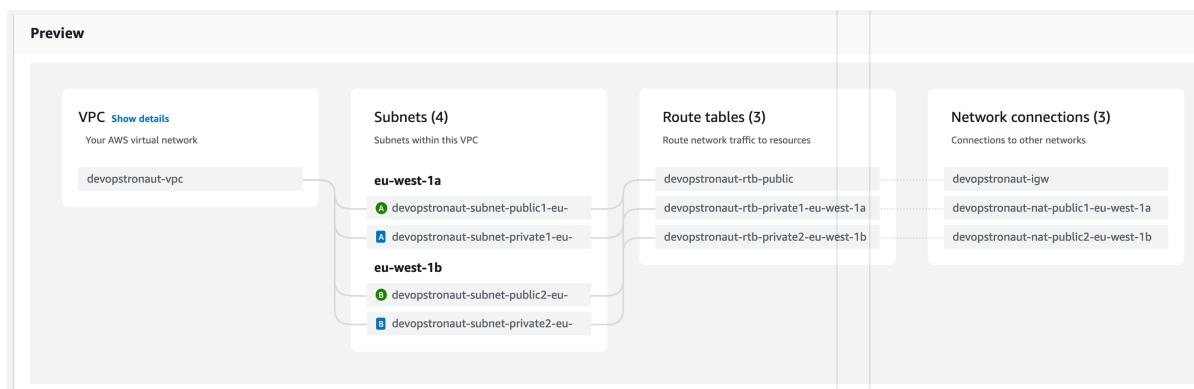
- Enable DNS hostnames
- Enable DNS resolution

## ► Additional tags

**Cancel**

**Create VPC**

Below is the preview of the VPC Network



The VPC has been created

## Create VPC workflow

Success

▼ Details

- Create VPC: [vpc-0e0d67302ce6a6e5d](#)
- Enable DNS hostnames
- Enable DNS resolution
- Verifying VPC creation: [vpc-0e0d67302ce6a6e5d](#)
- Create subnet: [subnet-03159bfbb3ccead18](#)
- Create subnet: [subnet-02a12fdf4fdcfdb86](#)
- Create subnet: [subnet-0621fbe3661d2460c](#)
- Create subnet: [subnet-02c9890bdf74dff79](#)
- Create internet gateway: [igw-038e3c23dc5ac782a](#)
- Attach internet gateway to the VPC
- Create route table: [rtb-07f018847ec93e5f0](#)
- Create route
- Associate route table
- Associate route table
- Allocate elastic IP: [eipalloc-0dfa91417117ab2ed](#)
- Allocate elastic IP: [eipalloc-0fadfe4fe56ed7453](#)
- Create NAT gateway: [nat-070f5d7e817268503](#)
- Create NAT gateway: [nat-0c51f14891fb2c9f7](#)
- Wait for NAT Gateways to activate
- Create route table: [rtb-06b8aebba8dd44ac9](#)
- Create route
- Associate route table
- Create route table: [rtb-0ed8254b07bf45f19](#)
- Create route
- Associate route table
- Verifying route table creation

[View VPC](#)

## 2.Create an EKS Cluster

Search for 'Elastic Kubernetes Service'

The screenshot shows the AWS search interface with the query 'EKS' entered. On the left, there's a sidebar with categories like Services (16), Features (16), Resources (New), Documentation (10,231), Knowledge Articles (362), Marketplace (773), Blogs (1,755), Events (28), and Tutorials (11). The main area displays a list of services under 'Services'. The first item is 'Elastic Kubernetes Service' with a star icon, followed by 'Batch', 'AWS FIS', and 'Detective'. Each service entry includes a brief description and a link to more details.

Click “Add cluster”

This screenshot shows the 'Clusters' management page. It has a header with 'EKS > Clusters'. Below the header, there's a table with columns: Cluster name, Status, Kubernetes version, Support period, Upgrade policy, Created, and Provider. A search bar labeled 'Filter clusters' is at the top of the table. A large message 'No clusters' with the subtext 'You do not have any clusters.' is centered. At the bottom of the page is a 'Create cluster' button.

Provide the Cluster Name and create a cluster service role if one is not available

This screenshot shows the 'Configure cluster' step of a wizard. It has a title 'Cluster configuration' with an 'Info' link. Under 'Name', there's a field containing 'devopstronaut' with a note below it: 'Enter a unique name for this cluster. This property cannot be changed after the cluster is created.' Below this is a note: '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.' Under 'Cluster service role', there's a note: '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](#).' A dropdown menu is open, showing 'Select role' and a 'Filter roles' search bar. The search bar contains 'Q Filter roles'. Below the search bar is a message: 'No roles found. Follow the link above to create a new role.' To the right of the dropdown is a button 'Create a role in IAM console' with a link icon.

Choose 'AWS Service,' set the Use case as 'EKS,' select the specified service use case as 'EKS-Cluster,' and click 'Next'

Step 1  
Select trusted entity [Info](#)

Step 2  
Add permissions

Step 3  
Name, review, and create

**Trusted entity type**

- AWS service** Allow AWS services like EC2, Lambda, or others 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.
- Web identity** Allows users federated by the specified external web identity provider to assume this role 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

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** Allows 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](#)

Click "Next"

Add permissions [Info](#)

**Permissions policies (1)** [Info](#)  
The type of role that you selected requires the following policy.

Policy name [Edit](#) Type [Edit](#)  
 **AmazonEKSClusterPolicy** AWS managed

► Set permissions boundary - optional

[Cancel](#) [Previous](#) [Next](#)

Provide the Role name and click 'Create Role'

Name, review, and create

**Role details**

Role name [Edit](#)  
**devopsonline-eks** Must be meaningful name to identify this role.

Description [Edit](#)  
Any text explanation for this role.

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

**Step 1: Select trusted entities**

Trust policy

```

1: {
2:   "Version": "2012-10-17",
3:   "Statement": [
4:     {
5:       "Effect": "Allow",
6:       "Principal": "*",
7:       "Action": "sts:AssumeRole",
8:       "Condition": {
9:         "StringEquals": {
10:           "AWS:SourceAccount": "442840900000"
11:         }
12:       }
13:     }
14:   ]
}

```

**Step 2: Add permissions**

Permissions policy summary

Policy name <a href="#">Edit</a>	Type <a href="#">Edit</a>	Attached as <a href="#">Edit</a>
<b>AmazonEKSClusterPolicy</b>	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 this resource.

[Add new tag](#) You can add up to 30 more tags.

[Cancel](#) [Previous](#) [Create role](#)

The Role has been created

A screenshot of the AWS IAM Roles page. At the top, a green banner says 'Role devopstronaut-eks created.' Below it, the 'Roles' section shows a list of 19 roles. The newly created role, 'devopstronaut-eks', is highlighted with a blue border. The list includes other standard service roles like 'AWSLambdaBasicExecutionRole' and 'AmazonSSMManagedInstanceCore'. The 'Create role' button is visible at the top right.

After creating the IAM Role, choose the role

A screenshot of the 'Cluster service role' selection screen. It shows a dropdown menu with 'devopstronaut-eks' selected. Below the dropdown is a 'Filter roles' input field. To the right, there's a button to 'Create a role in IAM console' with a checkmark icon.

Choose the Kubernetes version, set the Upgrade Policy to 'Standard,' enable 'Allow Cluster Administrator Access,' and select 'EKS API' and 'ConfigMap' for Cluster Authentication Method

## Kubernetes version settings

**Kubernetes version** | [Info](#)  
Select Kubernetes version for this cluster.

1.30 ▾

**Upgrade policy** | [Info](#)  
Choose one of the following options. You can switch the setting later while the standard support period is in effect.

- Extended**  
This option supports the Kubernetes version for 26 months after the release date. The extended support period has an additional hourly cost that begins after the standard support period ends. When extended support ends, your cluster will be auto upgraded to the next version.
- Standard**  
This option supports the Kubernetes version for 14 months after the release date. There is no additional cost. When standard support ends, your cluster will be auto upgraded to the next version.

## 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.

Turn on encryption of Kubernetes secrets using KMS and click 'Next'

**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.

[Add new tag](#)  
You can add up to 50 tags.

[Cancel](#) [Next](#)

Choose the VPC, select the Private Subnets, and choose a Security Group

## 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-0e0d67302ce6a6e5d | devopstronaut-vpc



#### 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-0621fbe3661d2460c | devopstronaut-subnet-private1-eu-west-1a X  
eu-west-1a 10.0.128.0/20

Clear selected subnets

subnet-02c9890bdf74dff79 | devopstronaut-subnet-private2-eu-west-1b X  
eu-west-1b 10.0.144.0/20

#### 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-0536c3d9c80e109ba | default X  
default VPC security group

#### 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.

Choose the cluster endpoint access as 'Public and Private'

### 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](#)

Click “Next”

## 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.

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.

[Cancel](#) [Previous](#) **Next**

Select the add-ons and click ‘Next’

## 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

#### 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 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](#)

Leave it as default and click 'Next'

## 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.8

### kube-proxy [Info](#)

[Remove add-on](#)

Category  
networking

Status  
 Ready to install

Version

Select the version for this add-on.

v1.30.0-eksbuild.3

### Amazon VPC CNI [Info](#)

[Remove add-on](#)

Category  
networking

Status  
 Ready to install

Version

Select the version for this add-on.

v1.18.1-eksbuild.3

### Amazon EKS Pod Identity Agent [Info](#)

[Remove add-on](#)

Category  
security

Status  
 Ready to install

Version

Select the version for this add-on.

v1.3.0-eksbuild.1

[Cancel](#)[Previous](#)[Next](#)

Click “Create”

**Step 5: Versions**

**Edit**

**Selected add-ons version**

< 1 >

Add-on name	Version
coredns	v1.11.1-eksbuild.8
eks-pod-identity-agent	v1.3.0-eksbuild.1
kube-proxy	v1.30.0-eksbuild.3
vpc-cni	v1.18.1-eksbuild.3

**Cancel** **Previous** **Create**

The Cluster has been created

EKS > Clusters > devopstronaut

## devopstronaut

**Cluster info** [Info](#)

Status <b>Active</b>	Kubernetes version <a href="#">Info</a> 1.30	Support period <b>Standard support until July 28, 2025</b>	Provider EKS
-------------------------	---	---	-----------------

[Overview](#) [Resources](#) [Compute](#) [Networking](#) [Add-ons](#) [Access](#) [Observability](#) [Upgrade insights](#) [Update](#) >

### Details

API server endpoint <a href="https://E8A959500AF327345E80FCE4DABEFF6A.gr7.eu-west-1.eks.amazonaws.com">https://E8A959500AF327345E80FCE4DABEFF6A.gr7.eu-west-1.eks.amazonaws.com</a>	OpenID Connect provider URL <a href="https://oidc.eks.eu-west-1.amazonaws.com/id/E8A959500AF327345E80FCE4DABEFF6A">https://oidc.eks.eu-west-1.amazonaws.com/id/E8A959500AF327345E80FCE4DABEFF6A</a>	Created 12 minutes ago
Certificate authority <a href="#">View in IAM</a>	Cluster IAM role ARN <a href="arn:aws:iam::851725583489:role/devopstronaut-eks">arn:aws:iam::851725583489:role/devopstronaut-eks</a> <a href="#">View in IAM</a>	Cluster ARN <a href="arn:aws:eks:eu-west-1:851725583489:cluster/devopstronaut">arn:aws:eks:eu-west-1:851725583489:cluster/devopstronaut</a>
		Platform version <a href="#">Info</a> eks.6

### 3.Create Node group and Nodes

Go to 'Compute' and click 'Add Node Group'

The screenshot shows the AWS EKS Compute interface. At the top, there are tabs: Overview, Resources, Compute (which is selected), Networking, Add-ons, Access, Observability, Upgrade insights, and Update. Below the tabs, there are two main sections:

- Nodes (0) [Info](#)**: This section has a search bar labeled "Filter Nodes by property or value". It includes columns for Node name, Instance type, Node group, Created, and Status. A message "No Nodes" indicates that the cluster does not have any nodes.
- Node groups (0) [Info](#)**: This section includes buttons for Edit, Delete, and Add node group. It has columns for Group name, Desired size, AMI release version, Launch template, and Status. A message "No node groups" indicates that the cluster does not have any node groups.

Provide the node group name and create an IAM role for the node if one is not available

The screenshot shows the "Configure node group" wizard at Step 2. The left sidebar lists steps: Step 1 (Configure node group), Step 2 (Set compute and scaling configuration), Step 3 (Specify networking), and Step 4 (Review and create). The main area is titled "Configure node group [Info](#)". It explains that a node group is a group of EC2 instances that supply compute capacity to your Amazon EKS cluster. The "Node group configuration" section contains a "Name" field where "devopstronaut-nodegroup" is entered. It also includes a "Node IAM role" section with a dropdown menu for "Select role", a search bar "Filter roles", and a button "Create a role in IAM console".

Select 'AWS Service,' choose 'EC2,' and click 'Next'

This screenshot shows the 'Select trusted entity' step of the AWS IAM Role creation wizard. It includes sections for 'Trusted entity type' (with options for AWS service, AWS account, SAML 2.0 federation, and custom trust policy), 'Use case' (with a dropdown set to 'EC2'), and a detailed list of EC2 permissions. At the bottom right are 'Cancel' and 'Next' buttons.

Click "Next"

This screenshot shows the 'Add permissions' step of the AWS IAM Role creation wizard. It displays a list of AWS managed policies under 'Permissions policies' (3/951). A search bar, filter, and pagination controls are visible. At the bottom right are 'Cancel', 'Previous', and 'Next' buttons.

Provide the role name and click 'Create Role'

Name, review, and create

**Role details**

**Role name**  
Enter a meaningful name to identify this role.  
**devopstronaut-ng-role**  
Maximum 48 characters. Use alphanumeric and "+", "-", ".", "@" characters.

**Description**  
Add a short explanation for this role.  
Allows EC2 instances to call AWS services on your behalf.

**Step 1: Select trusted entities**  
Edit

**Trust policy**

```
1- {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": [
        "ec2.amazonaws.com"
      ]
    }
  ]
}
```

**Step 2: Add permissions**  
Edit

**Permissions policy summary**

Policy name	Type	Attached as
AmazonECSContainerRegistryReadOnly	AWS managed	Permissions policy
AmazonEKS_CNI_Policy	AWS managed	Permissions policy
AmazonEKSWorkerNodePolicy	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.  
[Add new tag](#)  
You can add up to 50 more tags.

[Cancel](#) [Previous](#) [Create role](#)

## The Role has been created

**Role devopstronaut-ng-role created.**

**IAM > Roles**

**Roles [19] [Info](#)**  
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entities	Last activity
AWSServiceRoleForAmazonEKS	AWS Service: eks[Service-Linked Role]	30 minutes ago
AWSServiceRoleForAmazonEKSNodegroup	AWS Service: eks-nodegroup[Service]	4 days ago
AWSServiceRoleForAmazonSSM	AWS Service: ssm[Service-Linked Role]	2 hours ago
AWSServiceRoleForAutoScaling	AWS Service: autoscaling[Service-Link]	4 days ago
AWSServiceRoleForEC2	AWS Service: ec2[Service-Linked Role]	19 days ago
AWSServiceRoleForAWSLambda	AWS Service: lambda[Service]	2 days ago
AWSServiceRoleForGitSync	AWS Service: repository.sync[codeco]	13 days ago

[View roles](#) [Delete](#) [Create role](#)

## Refresh the Node IAM role list and choose the role

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**

**Filter roles**

**devopstronaut-ng-role**  
arn:aws:iam::851725583489:role/devopstronaut-ng-role

[Learn more](#)

**Create a role in IAM console**

Click “Next”

**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.

**Kubernetes labels** [Info](#)

This node group does not have any labels.

**Add label**

Remaining labels available to add: 50

**Kubernetes taints** [Info](#)

This node group does not have any taints.

**Add taint**

Remaining taints available to add: 50

**Tags** [Info](#)

No tags associated with the resource.

**Add new tag**

You can add up to 50 tags.

**Cancel** **Next**

Choose the AMI type, capacity type, instance type, and disk size

## 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

t2.micro

vCPU: 1 vCPU Memory: 1 GiB Network: Low to Moderate Max ENI: 2 Max IPs: 4



#### Disk size

Select the size of the attached EBS volume for each node.

20 GiB

Provide the desired, minimum, and maximum number of nodes, configure the node group update settings, and then click 'Next'

## 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

## Select the Private 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-02c9890bdf74dff79 | devopstronaut-subnet-private2-eu-west-1b X  
eu-west-1b 10.0.144.0/20

Clear selected subnets

subnet-0621fbe3661d2460c | devopstronaut-subnet-private1-eu-west-1a X  
eu-west-1a 10.0.128.0/20

Configure remote access to nodes Info

Cancel

Previous

Next

Review the configuration and click “Create”

The screenshot shows the "Node group update configuration" step of a Lambda function creation wizard. It displays the following information:

- Maximum unavailable:** 1 node

**Step 3: Networking** (with an **Edit** button)

**Node group network configuration**

Subnets	Configure remote access to nodes
subnet-02c9890bdf74dff79 subnet-0621fbe3661d2460c	off

**Create** (highlighted in orange) | **Cancel** | **Previous**

The node and node group have been created

The screenshot shows the AWS Lambda Compute tab with the following details:

**Nodes (1) Info**

Node name	Instance type	Node group	Created	Status
ip-10-0-158-108.eu-west-1.compute.internal	t2.micro	devopstronaut-nodegroup	Created a minute ago	Ready

**Node groups (1) Info**

Group name	Desired size	AMI release version	Launch template	Status
devopstronaut-nodegroup	1	1.30.2-20240817	-	Active

## 4.Create an Access entry for the User

Go to 'Access' and click 'Create Access Entry' for the user who needs access

The screenshot shows the 'Access configuration' section of the AWS EKS console. At the top, there are tabs for Overview, Resources, Compute, Networking, Add-ons, Access (which is selected), Observability, Upgrade insights, Update history, and Tags. Below the tabs, it says 'Authentication mode: EKS API and ConfigMap'. Under 'IAM access entries (2)', there is a table with columns: IAM principal ARN, Type, Username, Group names, and Access policies. The first entry is for an EC2 Linux role with ARN arn:aws:iam::851725583489:role/devopstronaut-nginx-role, and the second is for a Standard user with ARN arn:aws:iam::851725583489:root.

IAM principal ARN	Type	Username	Group names	Access policies
arn:aws:iam::851725583489:role/devopstronaut-nginx-role	EC2 Linux	system:node:{{EC2PrivateDNSName}}	system:nodes	-
arn:aws:iam::851725583489:root	Standard	arn:aws:iam::851725583489:root	-	AmazonEKSClusterAdminPolicy

Choose the User IAM Principal for accessing the EKS cluster and set the IAM access entry to 'Standard'

The screenshot shows the 'Configure IAM access entry' wizard. It has three main sections: 'IAM principal', 'Type - Optional', and 'Username - Optional'.

- IAM principal:** Set to 'arn:aws:iam::851725583489:user/mahi'. A note says: 'The IAM principal ARN can't be changed after access entry creation.'
- Type - Optional:** Set to 'Standard'. A note says: 'The type can't be changed after access entry creation.'
- Username - Optional:** Left empty. A note says: 'If you don't specify a username, EKS will auto-generate one for you while it creates the access entry.'

Click 'Next'

The screenshot shows the 'Groups - Optional' section with a note about Kubernetes groups and a button to add new group names. The 'Tags - Optional' section shows no tags associated with the resource and a button to add new tags. At the bottom, there are 'Cancel', 'Skip to Review and create', and 'Next' buttons.

**Groups - Optional (0) [Info](#)**  
The name of one or more groups that you've specified as subjects in Kubernetes RoleBindings or ClusterRoleBindings.  
No Kubernetes groups are configured for this IAM access entry.  
**Add new group name**  
You can add up to 50 more group names

**Tags - Optional (0) [Info](#)**  
No tags associated with the resource.  
**Add new tag**  
You can add up to 50 tags.

[Cancel](#) [Skip to Review and create](#) [Next](#)

Select the Access policy and set the cluster scope to 'Cluster'

The screenshot shows the 'Access policies' section where 'AmazonEKSClusterAdminPolicy' is selected. It also shows the 'Access scope' section with 'Cluster' selected. There is a 'Add policy' button and a summary of added policies. At the bottom, there are 'Cancel', 'Previous', and 'Next' buttons.

**Access policies [Info](#)**  
Select an access policy to associate to the access entry and the scope of the access policy.

**Policy name**  
Policy to associate

**Access scope**  
Type of access scope  
 Cluster  
 Kubernetes namespace

**Add policy**

**Added policies**  
No access policies added.

[Cancel](#) [Previous](#) [Next](#)

Click 'Create'

**Tags (0) Info**  
Tags that you've added. Each tag consists of a key and an optional value.

< 1 >

Key	Value
No tags No tags to display	

**Step 2: Add access policies** Edit

**Access policies (0) Info**  
Select an access policy to associate to the access entry and the scope of the access policy.

No access policies added.

Cancel Previous Create

## 5. Configure Context for EKS Cluster

Set the context for EKS Cluster

```
mahendralselvakumar@Mahendrals-MBP .aws % aws eks --region eu-west-1 update-kubeconfig --name devopstronaut
Added new context arn:aws:eks:eu-west-1:851725583489:cluster/devopstronaut to /Users/mahendralselvakumar/.kube/config
mahendralselvakumar@Mahendrals-MBP .aws %
```

Use the `kubectl` command to get the namespaces and nodes, then check the results

```
mahendralselvakumar@Mahendrals-MBP .aws % kubectl get ns
NAME      STATUS   AGE
default   Active   119m
kube-node-lease   Active   119m
kube-public   Active   119m
kube-system   Active   119m
mahendralselvakumar@Mahendrals-MBP .aws % kubectl get nodes
NAME                  STATUS   ROLES   AGE   VERSION
ip-10-0-158-108.eu-west-1.compute.internal   Ready   <none>   24m   v1.30.2-eks-1552ad0
mahendralselvakumar@Mahendrals-MBP .aws %
```

Keep Learning, Keep Deploying!!!

Feel free to reach out to me, if you have any other queries or suggestions

Stay connected on Linkedin: <https://www.linkedin.com/in/mahendran-selvakumar-36444a77/>