



# Administering AWS EKS Clusters

Integrating Cisco Container Platform with Amazon Web Services (AWS) allows you to deploy and run containerized applications across both Cisco-based on-prem environments and the AWS cloud.

This chapter contains the following topics:

- [Prerequisites for Configuring AWS EKS Clusters, on page 1](#)
- [Amazon IAM Authentication, on page 4](#)
- [Creating AWS EKS Clusters, on page 5](#)
- [Scaling AWS EKS Clusters, on page 6](#)
- [Deleting AWS EKS Clusters, on page 6](#)

## Prerequisites for Configuring AWS EKS Clusters

The prerequisites for configuring AWS EKS clusters are as follows:

### Amazon Resource Requirements

The following table describes the default limits for the Amazon resources that you may need to increase depending on your Cisco Container Platform deployment requirements.



**Note** To increase the limits for a specific resource, you need to contact [Amazon support](#).

Amazon Resource	Default Limit	Description
Network Address Translation (NAT) gateway for each AWS account	14	Each EKS cluster uses three NAT gateways. With the default setting, you are limited to four clusters.
Amazon Virtual Private Cloud (Amazon VPC) for each AWS account	3	Each tenant cluster requires a separate Amazon VPC.

Amazon Resource	Default Limit	Description
Amazon Elastic Container Service for Kubernetes (Amazon EKS) cluster for each AWS account	3	<b>Note</b> Changes to the Amazon EKS cluster limit are updated only on Thursdays.
Elastic IP address for each region	5	Each EKS cluster uses three elastic IP addresses. For more information, see <a href="#">Amazon VPC Limits</a> .
Internet gateway for each region	5	Each EKS cluster uses one internet gateway.

## Adding AMI Files to your Amazon Account

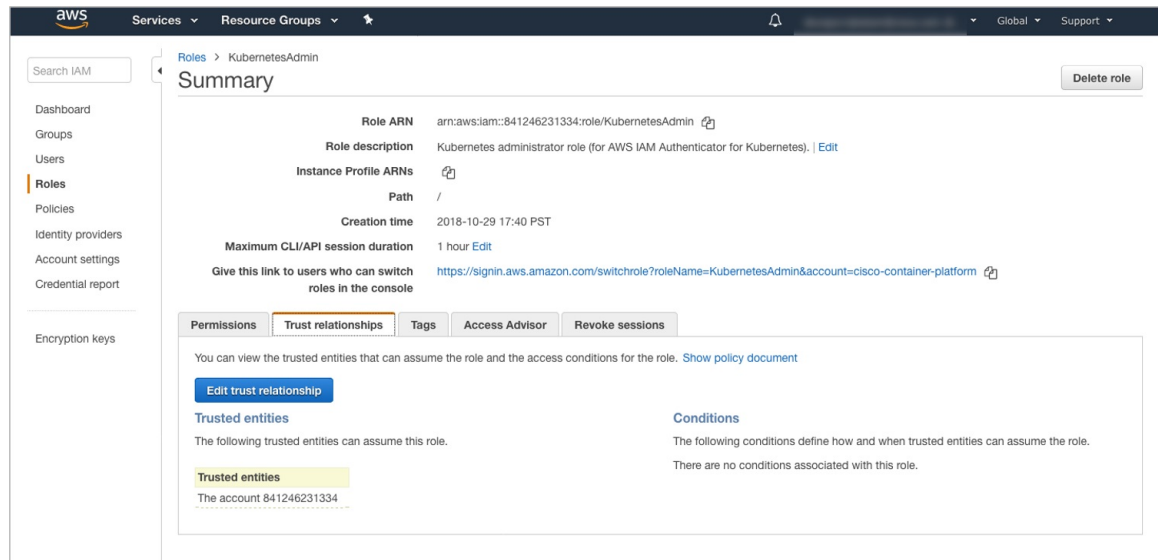
Cisco Container Platform generates a specific AMI (Amazon Machine Image) file with each product release. The AMI file ensures that compatible packages are available for successful tenant cluster creation.

To make the AMI file available to your Amazon account, you must [submit a support case](#) that includes your 12 digit Amazon account ID. You will be notified when the AMI is available within your Amazon account.

## Creating AWS Roles

- 
- Step 1** Log in to the AWS Management Console and open the IAM console at <https://console.aws.amazon.com/iam/>.
- Step 2** From the navigation pane of the IAM console, click **Roles**, and then click **Create role**.
- Step 3** Under **Select type of trusted entity**, click **Another AWS account**.
- Step 4** In the **Account ID** field, enter your **AWS Account ID**, and then click **Next**.  
The AWS account number must be a trusted entity so that Cisco Container Platform can use the Role ARN during EKS cluster creation.
- Step 5** Skip the screen to choose permission policies and permission boundary and click **Next**.
- Step 6** Add metadata to the role by attaching tags of your choice as key–value pairs and click **Next**.
- Step 7** In the **Role name** field, enter the name for the role as `k8s-ccp-user` or any other name of your choice.
- Step 8** In the **Description** field, enter a description of your choice and click **Create role**.
- Step 9** After the role is created, navigate to the created role and verify the following details of the role:
- Click the **Permissions** tab to verify that permissions are not set.
  - Click the **Trust Relationships** tab to verify that a trust relationship exists for the AWS account that you entered during creation of the Role ARN.

Figure 1: AWS Management Console-Trust Relationships Tab



## AWS Account Policy Requirements

### Provider permissions

If the AWS provider account is not a root account then you must ensure that the account has the permissions needed to create the EKS and EC2 resources.

The minimum permissions needed are included in the [Sample aws-provider-policy.json File](#). You can create and import this file to configure the necessary permissions.

### Sample aws-provider-policy.json File

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:*",
        "elasticloadbalancing:*",
        "autoscaling:*",
        "ec2:*",
        "eks:*",
        "ecr:*",
        "ecs:*",
        "s3:*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

```

        "iam:Get*",
        "iam:PassRole",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:CreateRole",
        "iam:CreateInstanceProfile",
        "iam>DeleteInstanceProfile",
        "iam>DeleteRole",
        "iam>DeleteRolePolicy",
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePolicy",
        "iam:*AccessKey*",
        "iam:*MFA*"
    ],
    "Resource": "*"
  }
}

```

## Amazon IAM Authentication

By default, the AWS IAM identity is used to authenticate EKS clusters to establish connection. Cisco Container Platform uses [AWS IAM Authenticator](#) to authenticate on-prem cluster using the AWS IAM identity. This authentication provides a consistent, unified identity scheme across both on-premise and AWS EKS clusters.

The AWS IAM Authenticator fulfills both a client and server function. On the client side, the authenticator generates, tokenizes and transmits a pre-signed URL to the server-side for identity validation. The client is a Go binary, installed on your workstation, which is transparently invoked by kubectl each time you interact with your Kubernetes cluster. The server-side is a containerized instance of AWS IAM Authenticator running as a DaemonSet on the Kubernetes master nodes. This interacts with the AWS Secure Token Service (STS) to perform identity validation. Cisco Container Platform takes care of the initial server-side configuration and provides a preconfigured `kubeconfig` file for admin users to download.




---

**Note** You need to ensure that the AWS IAM Authenticator is available within your `$PATH` while using kubectl to interact with the clusters.

---

## Enabling Common Identity

Within the Cisco Container Platform web interface, users are able to select a common identity scheme for clusters. After the clusters are provisioned, you can apply a shared RBAC policy.




---

**Note** The use of IAM Authentication is implicitly enabled for EKS clusters. Cisco Container Platform can map a user supplied IAM role to the EKS cluster and configuring IAM auth for on-premises clusters.

---

# Creating AWS EKS Clusters

## Before you begin

- Ensure that you have added your Amazon provider profile. For more information, see [Adding Amazon Provider Profile](#).
- Ensure that you have added the required AMI files to your account. For more information, see [Adding AMI Files to your Amazon Account, on page 2](#).
- Ensure that you have created an AWS IAM Role for the Cisco Container Platform usage to create AWS EKS Clusters. For more information, see [Creating AWS Roles, on page 2](#).

---

**Step 1** From the left pane, click **Clusters**, and then click the **AWS** tab.

**Step 2** Click **NEW CLUSTER**.

**Step 3** In the **Basic Information** screen, enter the following information:

- a) From the **INFRASTRUCTURE PROVIDER** drop-down list, choose the provider related to the appropriate Amazon account.
- b) From the **AWS REGION** drop-down list, choose an appropriate AWS region.

**Note** Not all regions support EKS. Ensure that you select a supported region. Currently, Cisco Container Platform only supports the **us-west-2** and **us-east-1** regions.

- c) In the **KUBERNETES CLUSTER NAME** field, enter a name for your cluster.
- d) Click **NEXT**.

**Step 4** In the **Node Configuration** screen, provide the following information:

- a) From the **INSTANCE TYPE** drop-down list, choose an [instance type](#) for your cluster.
- b) From the **MACHINE IMAGE** drop-down list, choose an appropriate Cisco Container Platform Amazon Machine Image (AMI) file.  
To add AMI files to your Amazon account, see [Adding AMI Files to your Amazon Account, on page 2](#).
- c) In the **WORKER COUNT** field, enter an appropriate number of worker nodes.
- d) In the **SSH PUBLIC KEY** drop-down field, choose an appropriate authentication key.  
This field is optional. It is needed if you want to ssh to the worker nodes for troubleshooting purposes. Ensure that you use the Ed25519 or ECDSA format for the public key.

**Note:** As RSA and DSA are less secure formats, Cisco prevents the use of these formats.

- e) In the **IAM ACCESS ROLE ARN** field, enter the Amazon Resource Name (ARN) information.

**Note** By default, the AWS credentials specified at the time of Amazon EKS cluster creation, that is the credentials configured in the Infrastructure Provider, are mapped to the `kubernetes cluster-admin ClusterRole`. A default `ClusterRoleBinding` binds the credentials to the `system:masters` group, thereby granting super-user access to the holders of the IAM identity. The **IAM ACCESS ROLE ARN** field allows you to specify the ARN of an additional AWS IAM role or IAM user who is also granted administrative control of the cluster.

- f) Click **NEXT**.

**Step 5** In the **VPC Configuration** screen, provide the following information:

- a) In the **SUBNET CIDR** field, enter a value of the overall subnet CIDR for your cluster.
- b) In the **PUBLIC SUBNET CIDR** field, enter values for your cluster on separate lines.
- c) In the **PRIVATE SUBNET CIDR** field, enter values for your cluster on separate lines.

**Step 6** In the **Summary** screen, review the cluster information and then click **FINISH**.

Cluster creation can take up to 20 minutes. You can monitor the cluster creation status on the **Clusters** screen.

**Note** If you receive the Could not get token: AccessDenied error message, it indicates that the AWS account is not a trusted entity for the Role ARN.

For information on adding your AWS account as a trusted entity, see [Creating AWS Roles, on page 2](#).

---

## Scaling AWS EKS Clusters

You can scale EKS clusters by adding or removing worker nodes to them based on the demands of the workloads you want to run.

---

**Step 1** From the right pane, click **EDIT**.

The **Edit Cluster** dialog box appears.

**Step 2** From the **INSTANCE TYPE** drop-down list, choose an [instance type](#) for your cluster.

**Step 3** From the **MACHINE IMAGE** drop-down list, choose an appropriate Cisco Container Platform Amazon Machine Image (AMI) file.

To add AMI files to your Amazon account, see [Adding AMI Files to your Amazon Account, on page 2](#).

**Step 4** In the **WORKER COUNT** field, change the number of work nodes as necessary.

**Step 5** Click **UPDATE**.

---

## Deleting AWS EKS Clusters

### Before you begin

Ensure that the AWS EKS cluster that you want to delete is not currently in use, as deleting a cluster removes the containers and data associated with it.

---

**Step 1** From the left pane, click **Clusters**, and then click the **EKS Clusters** tab.

**Step 2** From the drop-down list displayed under the **ACTIONS** column, choose **Delete** for the cluster that you want to delete.

**Step 3** Click **DELETE** in the confirmation dialog box.

Upon deleting an AWS EKS cluster, it takes about 10 minutes for the cluster resources to be released.

---