



Managing Cisco Container Platform Infrastructure Configuration

This chapter contains the following topics:

- [Managing Users and RBAC, on page 1](#)
- [Managing Provider Profile, on page 3](#)
- [Managing ACI Profile, on page 5](#)
- [Managing Networks, on page 6](#)

Managing Users and RBAC

Cisco Container Platform provides Role-based Access Control (RBAC) through built-in static roles, namely the *Administrator* and *User* roles. Role-based access allows you to use local accounts and LDAP for authentication and authorization.

Configuring Local Users

Cisco Container Platform allows you to manage local users. An administrator can add a user, and assign an appropriate role and cluster(s) to the user.

Before you begin

Ensure that you have configured LDAP Server for authentication of Cisco Container Platform users.

For more information, see [Configuring AD Servers, on page 2](#).

Step 1 From the left pane, click **User Management**, and then click the **Users** tab.

Step 2 Click **NEW USER**.

Step 3 Specify information such as first name, last name, username, passphrase, and role for the user.

Step 4 Click **SUBMIT**.

The new user is displayed on the **User Management** page.

Note You can edit or delete a user by using the options available under the **ACTIONS** column.

Changing Login Passphrase

- Step 1** From the left pane, click **User Management**, and then click the **Users** tab.
- Step 2** From the drop-down list displayed under the **ACTIONS** column, choose **Edit** corresponding to your name.
- Note** Administrators can change passphrase and role for other users as well.
- Step 3** Change the passphrase and role assigned as necessary, and click **SUBMIT**.
-

Configuring AD Servers

LDAP authentication is performed using a service account that can access the LDAP database and query for user accounts. You will need to configure the AD server and service account in Cisco Container Platform.

- Step 1** From the left pane, click **User Management**, click the **Active Directory** tab, and then click **EDIT**.
- Step 2** In the **SERVER IP ADDRESS** field, type the IP address of the AD server.
- Step 3** In the **PORT** field, type the port number for the AD server.
- Step 4** For improved security, we recommend that you check **STARTTLS**.
- Step 5** In the **BASE DN** field, specify the domain name of the AD server for all the accounts that you have.
- Step 6** In the **ACCOUNT USERNAME** field, specify the service account name that is used for accessing the LDAP server.
- Step 7** In the **PASSPHRASE** field, type the passphrase of the AD account.
- Step 8** Click **SUBMIT**.
-

Configuring AD Groups

Cisco Container Platform allows you to manage users using AD groups. An administrator can add users to AD groups, and then assign appropriate roles and clusters to the groups.

Before you begin

Ensure that you have configured the AD server that you want to use.

For more information on configuring AD servers, see [Configuring AD Servers, on page 2](#).

- Step 1** From the left pane, click **User Management**, and then click the **Groups** tab.
- Step 2** Click **ADD GROUP**.
- Step 3** Specify information such as the name of the AD group and the role you want to assign to the group.
- Note** If the AD group is associated with the *Administrator* role, by default, access is provided to all clusters. But, if the AD group is associated with the *User* role, you need to assign a cluster.
- Step 4** From the **CLUSTERS** drop-down list, choose the names of the cluster that you want to assign to the AD group.

Step 5 Click **SUBMIT**.

Managing Provider Profile

Cisco Container Platform enables you to define the provider profile on which clusters can be created.

You can configure multiple provider profiles in an instance of Cisco Container Platform and use the same provider profile for multiple clusters.

Adding Provider Profile

After your Cisco Container Platform control plane is available, log in to the Cisco Container Platform web interface, and then add the required provider profiles.

This section contains the following topics:

- [Adding vSphere Provider Profile](#), on page 3
- [Adding Amazon Provider Profile](#), on page 3

Adding vSphere Provider Profile

Before you begin

Cisco Container Platform interacts with vSphere through the user that you configure when you add a provider profile. Hence, you need to ensure that this user has the necessary privileges.

For more information on the vSphere user privileges, see [User Privileges on vSphere](#).

Step 1 From the left pane, click **Infrastructure Providers**.
The **Infrastructure Providers** screen appears.

Step 2 Click **NEW PROVIDER** and enter information such as name, description, address, port, username and passphrase of the provider profile.

Step 3 Click **ADD**.
The vSphere provider profile that you added is displayed on the **Infrastructure Providers > vSphere** screen.

Adding Amazon Provider Profile

Step 1 From the left pane, click **Infrastructure Provider**.
The **Infrastructure Providers** screen appears.

Step 2 Click the **NEW PROVIDER** and enter the following information:

- a) In the **PROVIDER NAME** field, enter a name for the related Amazon account.
- b) In the **ACCESS KEY ID** field, enter the key ID for the related Amazon account.
- c) In the **SECRET ACCESS KEY** field, enter the access key for the related Amazon account.

d) Click **ADD**.

The Amazon provider profile that you added is displayed on the **Infrastructure Providers > AWS** screen.

For more information on administering AWS EKS clusters, see [Administering AWS EKS Clusters](#).

Modifying Provider Profile

This section contains the following topics:

- [Modifying vSphere Provider Profile, on page 4](#)
- [Modifying Amazon Provider Profile, on page 4](#)

Modifying vSphere Provider Profile

- Step 1** From the left pane, click **Infrastructure Providers**.
The **Infrastructure Providers** screen appears.
- Step 2** Click the **vSphere** tab.
- Step 3** From the drop-down list displayed under the **ACTIONS** column, choose **Edit** corresponding to the provider profile that you want to modify.
- Step 4** Change the provider details as necessary and click **SUBMIT**.
-

Modifying Amazon Provider Profile

- Step 1** From the left pane, click **Infrastructure Providers**.
The **Infrastructure Providers** screen appears.
- Step 2** Click the **AWS** tab.
- Step 3** For the provider profile that you want to rename, from the drop-down list displayed under the **ACTIONS** column, choose **Rename**.
- Step 4** Change the provider name as necessary and click **RENAME**.
-

Deleting Provider Profile

- Step 1** From the left pane, click **Infrastructure Providers**.
- Step 2** Click the **vSphere** or **AWS** tab as necessary.
- Step 3** From the drop-down list displayed under the **ACTIONS** column, choose **Delete** corresponding to the provider profile that you want to delete.
- Step 4** Click **DELETE** in the confirmation dialog box.
-

Managing ACI Profile

Cisco Container Platform enables you to define ACI profiles using which tenant clusters can be created.

You can define multiple ACI profiles and use the same profile for multiple clusters.

Adding ACI Profile

Step 1 From the left pane, click **ACI Profiles**.

Step 2 Click **Add New ACI Profile** and perform these steps:

- a) Specify information such as profile name, IP address, username, and passphrase of the ACI instance.

Note If there is more than one host, use a comma-separated host list in the **APIC IP ADDRESSES** field.

- b) In the **NAMESERVERS** field, enter the IP address of all the DNS servers that the ACI fabric can access.
- c) From the **VMM DOMAIN** drop-down list, choose the Virtual Machine Manager Domain (VMMMD) that you want to use.
- d) In the **INFRASTRUCTURE VLAN ID** field, enter the VLAN number for layer 2 networking.
- e) From the **VRF** drop-down list, choose the Virtual Routing and Forwarding (VRF) IP address.
- f) From the **L3OUT POLICY NAME** drop-down list, choose the ACI object for allowing external internet connectivity.
- g) From the **L3OUT NETWORK NAME** drop-down list, choose the external network that is reachable through the L3OUT object.
- h) From the **AAEP NAME** drop-down list, choose an Attachable Access Entity Profile (AAEP) name to associate the VMM domain with an AAEP.
- i) In the **STARTING SUBNET FOR PODS** field, enter the starting IP address for the IP pool that is used to allocate IP addresses to the pods.
- j) In the **STARTING SUBNET FOR SERVICE** field, enter the starting IP address for the IP pool that is used to allocate IP addresses to the service VLAN.
- k) In the **CONTROL PLANE CONTRACT NAME** field, enter the name of the contract that is provided by the Control Plane endpoint group to allow traffic from the Control Plane cluster to the tenant cluster.
- l) In the **NODE VLAN START ID** field, enter the starting VLAN ID that is used to allocate VLAN to the node.
- m) In the **NODE VLAN END ID** field, enter the ending VLAN ID that is used to allocate VLAN to the node.
- n) In the **OPFLEX MULTICAST RANGE** field, enter a range for the Opflex multicast.

Step 3 Click **SUBMIT**.

Modifying ACI Profile

Step 1 From the left pane, click **ACI Configuration**.

Step 2 From the drop-down list displayed under the **ACTIONS** column, choose **Edit** for the ACI profile that you want to modify.

Step 3 Change the ACI profile details as necessary and click **SUBMIT**.

Deleting ACI Profile

-
- Step 1** From the left pane, click **ACI Configuration**.
 - Step 2** From the drop-down list displayed under the **ACTIONS** column, choose **Delete** for the ACI profile that you want to delete.
 - Step 3** Click **DELETE** in the confirmation dialog box.
-

Managing Networks



Note This section is applicable only for a non-ACI environment.

Cisco Container Platform enables you to select an existing network, create a subnet in that network, and then create a Cisco Container Platform Virtual IP Address (VIP) pool within that subnet.

VIP pools are reserved ranges of IP addresses that are assigned as virtual IP addresses within the Cisco Container Platform clusters. A minimum of two IP addresses are required for each tenant cluster, namely, one for the master VIP of the Kubernetes tenant cluster and an additional VIP for the external IP address of the Ingress controller. The range of IP addresses in the VIP pools must be outside of the IP addresses that are assigned by DHCP.

Modifying Networks

-
- Step 1** From the left pane, click **Networks**.
The **Networks** page displays the default network.
 - Step 2** From the drop-down list displayed under the **ACTIONS** column, choose **Edit** for the network that you want to modify. Alternatively, click the **SUBNETS** tab or the **POOLS** tab, and then click **EDIT** from the right pane to view the **Edit** dialog box.
 - Step 3** Modify the network name as necessary and click **SUBMIT**.
-

Adding Subnets

If you want to allocate VIP from a different subnet CIDR you need to add the subnet.

- Step 1** From the left pane, click **Networks**, and then click the network to which you want to add a subnet.
- Step 2** From the right pane, click **NEW SUBNET**.
- Step 3** Enter a name and CIDR for the subnet.
- Step 4** Enter a gateway IP address that you want to use.

Step 5 Enter the DNS nameservers.

Step 6 Click **SUBMIT**.

Modifying Subnets

Step 1 From the left pane, click **Networks**, and then click the network that contains the subnet you want to modify.

Step 2 Click the **SUBNETS** tab.

Step 3 From the drop-down list displayed under the **ACTIONS** column, choose **Edit** for the subnet that you want to modify.

Step 4 Modify the subnet name and CIDR as necessary, and then click **SUBMIT**.

Adding VIP Pool

Step 1 From the left pane, click **Networks**, and then click the network to which you want to add a VIP pool.

Step 2 From the right pane, click **NEW POOL**.

Step 3 Specify a name, subnet and IP address range for the VIP pool.

Step 4 Click **SUBMIT**.

Modifying VIP Pool

Step 1 From the left pane, click **Networks**, and then click the network that contains the VIP pool you want to modify.

Step 2 Click the **POOLS** tab.

Step 3 From the drop-down list displayed under the **ACTIONS** column, choose **Edit** for the VIP pool that you want to modify.

Step 4 Change the pool name and the IP address as necessary, and then click **SUBMIT**.
