Managing Cisco Container Platform Infrastructure Configuration

This chapter contains the following topics:

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.

Caution Use of local authentication is not recommended and is considered less secure for production data.

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 5.

Step 1 In the left pane, click **User Management**, and then click the **Users** tab.
The **Add User** screen appears.

Step 2 Click **ADD USER**.

Step 3 In the **USERNAME** field, enter a username.

Step 4 From the **ROLE** drop-down list, choose one of the following roles:

- Administrator
- User

Step 5 If you want to generate a passphrase automatically:

a) Click the **AUTOMATICALLY GENERATE PASSPHRASE** toggle button.
The **User Details** screen appears.
b) Click **COPY PASSPHRASE** to copy the passphrase to your clipboard.
c) Click **CLOSE**.

Step 6 If you want to type a passphrase of your own, enter a passphrase in the **PASSPHRASE** field.

a) In the **FIRST NAME** field, enter the first name of your user.
b) In the **LAST NAME** field, enter the last name of your user.
c) Click **ADD**.

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.

Modifying Local Authentication Policy

Caution There will be a temporary downtime for the Cisco Container Platform API during this procedure.

Follow these steps to modify the local authentication policies for the local accounts.

Step 1 SSH to a control plane master node.

Step 2 Edit the API auth configmap `kaas-api-auth`.

```
kubectl edit cm kaas-api-auth
```

Step 3 Modify the local authentication parameters under `data.authentication_settings.py`.

For example:

```
apiVersion: v1
    data:
    authentication_settings.py: |-
        PASSWORD_MIN_STRENGTH=0.40
        PASSWORD_LIFETIME_DAYS=365
        PASSWORD_WARNING_DAYS=20
        PASSWORD_GRACE_DAYS=1
        VALIDATOR_STRENGTH_ENABLE=False
    kind: ConfigMap
    metadata:
    name: api-auth
    namespace: default
```

For more information on the local authentication parameters, see Local Authentication Parameters, on page 3.

Step 4 Delete the pod to restart the API service.

```
kubectl delete pod -l app=api
```

Local Authentication Parameters

The following table describes the parameters used for local authentication.

Parameter	Default Setting	Description
VALIDATOR_MIN_LEN	8	Minimum character length of passphrase.
PASSWORD_LIFETIME_DAYS	0 (Forever)	Number of days for which a passphrase is valid before requiring a change
PASSWORD_WARNING_DAYS	14	Number of days for which a warning is sent to the user to warn expiry of passphrase
PASSWORD_GRACE_DAYS	0	Number of days after a passphrase has expired during which you are allowed to continue to login
PASSWORD_HISTORY_COUNT	0	Passphrase reuse limitation value
PASSWORD_HISTORY_DAYS	0	Number of days after which passphrase reuse is allowed
VALIDATOR_FORBIDDEN_WORDS	{"cisco123", "ccp123"}	Explicit list of restricted passphrases
VALIDATOR_COMMON_ENABLE	True	Restrict passphrases based on a common dictionary
VALIDATOR_STRENGTH_ENABLE	True	Enable passphrase complexity requirement
PASSWORD_MIN_STRENGTH	0.20	Passphrase complexity requirement (range 0.00..0.99)
LOGIN_THROTTLE_ENABLED	True	Enable rate-limiting on login endpoint
THROTTLE_ANON_LOGIN_BURST	'60/min'	Rate-limiting burst limit for unsuccessful login attempts
THROTTLE_ANON_LOGIN_SUSTAINED	False	Rate-limiting sustained limit for unsuccessful login attempts, for example: '100/day'

Note Rate limit applies to each worker process of an API service. An API service is backed by 10 worker processes, which serve requests in a round-robin fashion. The overall number of requests before throttle occurs is calculated using the formula: Rate value x 10

For example: The default allowed overall requests for login attempts is calculated as follows: (THROTTLE_ANON_LOGIN_BURST) * 10

= (60) x 10

= 600 requests/mins

Changing Login Passphrase

Step 1 In 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 **Change passphrase** corresponding to your name.

Note Administrators can change passphrase and role for other users as well.

Step 3 If you want to generate a passphrase automatically:

a) Click the **AUTOMATICALLY GENERATE PASSPHRASE** toggle button.
b) Click **CHANGE**.
The **User Details** screen appears.
c) Click **COPY PASSPHRASE** to copy the passphrase to your clipboard.
d) Click **CLOSE**.

Step 4 If you want to use a passphrase of your own:

a) Enter a passphrase in the **PASSPHRASE** field.
b) Click **CHANGE**.

The passphrase is changed successfully.

Recovering Login Passphrase for Local Admin

Step 1 Perform one of the following steps:

a) If you have SSH access to the Cisco Container Platform Control Plane nodes, log in to a Cisco Container Platform Control Plane node.
b) If you have the Kubeconfig file, save it in the `$HOME/.kube` directory. You can specify other kubeconfig files by setting the KUBECONFIG environment variable or by setting the `--kubeconfig` flag.

Step 2 List the available pods.

```
kubectl get pods
```

Step 3 Search for the pod that has the following format:

```
kaas-corc-xxxxxxxx-xxxx
```

Step 4 Reset the login passphrase for the admin user.

```
kubectl exec kaas-corc-7df5d76f87-55n7b ./password_reset
Password reset for 'admin' user : <50-char-long-random-string>
```

The local admin passphrase is reset to a 50-character random string. You can choose to continue using this passphrase, or reset the passphrase by Changing Login Passphrase.

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 In 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, type the domain name of the AD server for all the accounts that you have.

For example:

CN=Users,DC=example,DC=com

Note You can use a comma-separated list to enter multiple domain names.

Step 6 2. In the **ACCOUNT USERNAME** field, enter an LDAP CN.

For example:

CN=UserName,OU=Folder,DC=example,DC=cisco,DC=com

Step 7 In the **PASSPHRASE** field, type the passphrase of the AD account.

Step 8 Click **SUBMIT**.

Troubleshooting AD User Credentials

Step 1 Run the `ldapwhoami` command-line tool to validate the AD service account credentials.

Command:

```
ldapwhoami -x -W -D <ACCOUNT USERNAME> -H ldap://<SERVER IP ADDRESS>/
```

Example:

```
ldapwhoami -x -W -D cn=admin,dc=example,dc=org -H ldap://10.10.10.100/
```

Step 2 When prompted, type the passphrase of the AD account.

If the user credential validation fails, an `Invalid Credentials` message is displayed.

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 5.

Step 1 In the left pane, click **User Management**, and then click the **Groups** tab.

Step 2 Click **ADD GROUP**.

Step 3 In the **ACTIVE DIRECTORY GROUP** field, type the list of distinguished names for all the accounts that you have.

For example, type **`CN=CCP-Cluster1-Admin,CN=Users,DC=aervacan-lab,DC=local`**, where the distinguished names are entered using a comma-separated list.

Step 4 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 5 From the **CLUSTERS** drop-down list, choose the names of the cluster that you want to assign to the AD group.

Step 6 Click **SUBMIT**.

Troubleshooting AD Groups

Consider an AD group with the following parameters:

- **SERVER IP ADDRESS:** 10.10.10.100
- **PORT:** 389
- **BASE DN:** dc=example,dc=org
- **ACCOUNT USERNAME:** cn=admin,dc=example,dc=org

Step 1 Run the `ldapsearch` command-line tool to view users who belong to the `cn=Admin Users,dc=example,dc=org` group.

```
ldapsearch -x -D "cn=admin,dc=example,dc=org" -W -b "dc=example,dc=org" -h 10.10.10.100
\'(&(memberOf=cn=Admin Users,dc=example,dc=org))' 'sAMAccountName'
```

Step 2 Run the `ldapsearch` command-line tool to view the list of groups to which the `cn=user,dc=example,dc=org` user belongs.

```
ldapsearch -x -D "cn=admin,dc=example,dc=org" -W -b "cn=user,dc=example,dc=org" -h 10.10.10.100
'memberOf'
```

The group information that is configured in the AD service is displayed.

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

Before you begin

Cisco Container Platform interacts with vSphere through the user that you configure when you add a provider profile. You need to ensure that this user has the necessary privileges. For more information, see Minimum User Privileges on vSphere.

Step 1 In 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

Cisco Container Platform interacts with Amazon through the user that you configure when you add a provider profile. You need to ensure that this user has the necessary privileges. For more information on minimum user privileges on AWS, see Minimum User Privileges on AWS.

Before you begin

Ensure that you have completed the prerequisites for configuring clusters on AWS EKS. For more information, see Prerequisites for Configuring Clusters on AWS EKS.

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

Step 2 Click **NEW PROVIDER** and specify 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 access key ID for the related Amazon account.
For more information on creating an access key ID, see Creating Access Keys.
c) In the **SECRET ACCESS KEY** field, enter the access key for the related Amazon account.
For more information on creating a secret access key, see Creating Access Keys.
d) Click **ADD**.

Note The access key and secret must not be from your AWS root user account.

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

For more information, see Administering Clusters on Amazon Web Services (AWS) EKS.

Adding OpenStack Provider Profile

Step 1 In 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 OpenStack account.
b) From the **PROTOCOL** drop-down list, choose the protocol that you want to use.
c) In the **AUTH URL** field, enter the URL that is used to authenticate against an Identity Server.
d) In the **REGION** field, enter an appropriate OpenStack region.
e) In the **DOMAIN NAME** field, enter the domain name account that is used for accessing the OpenStack server.
f) In the **PROJECT NAME** field, enter project name that you want to use.
g) In the **USERNAME** field, enter the username for the OpenStack provider profile.
h) In the **PASSPHRASE** field, enter a passphrase for the OpenStack provider profile.
i) In the **CA CERTIFICATE** field, add a root CA certificate to allow tenant clusters to securely connect to additional services.
j) Click **ADD**.

The OpenStack provider profile that you added is displayed on the **Infrastructure Providers** > **Openstack** screen. For more information on administering clusters on OpenStack, see Administering Clusters on OpenStack.

Adding Azure Provider Profile

Cisco Container Platform interacts with Azure through the user that you configure when you add a provider profile. You need to ensure that this user has the necessary privileges. For more information on minimum user privileges on Azure see, Minimum User Privileges on AKS.

Before you begin

Ensure that you have created a service principal in your Azure account and noted down the values of the `id`, `appID`, `password`, and `tenant` parameters. For more information, see Creating Service Principals, on page 9.

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

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

a) In the **NAME** field, enter a name for your Azure account.
b) If you want to use Virtual Kubelet to provision pods on Azure Container Instance in your clusters on AKS, in the **APPLICATION NAME** field, enter the name of the service principal that you have created for your Azure cluster.
c) In the **CLIENT ID** field, enter the value of the `appID` parameter from Creating Service Principals, on page 9.
d) In the **CLIENT SECRET** field, enter the value of the `password` parameter from Creating Service Principals, on page 9.
e) In the **TENANT ID** field, enter the value of the `tenant` parameter from Creating Service Principals, on page 9.
f) In the **SUBSCRIPTION ID** field, enter the value of the `id` parameter from Creating Service Principals, on page 9.
g) Click **ADD**.

The Azure provider profile is displayed on the **Infrastructure Providers** > **Azure** screen.

For more information on administering Azure Kubernetes Service (AKS) clusters, see Administering Clusters on Azure Kubernetes Service (AKS).

Creating Service Principals

Step 1 Login to the Azure Portal.

Step 2 Install the Azure CLI.

Step 3 Follow these steps to configure the Azure CLI to use the Azure account that you want to use with Cisco Container Platform:

a) Log in to the Azure CLI.

```
az login
```

The URL to the device login page and an authentication code is displayed.
b) Use a browser to access the device login page, enter the code that you have received, and then click **Continue**.
c) Choose your Azure account.

Step 4 From the command output on the Azure CLI, note down the value of the `id` parameter. This value is required while Adding Azure Provider Profile to Cisco Container Platform.

For example:

```
{
    "cloudName": "AzureCloud",
    "id": "aaaaaaaa-bbbb-1111-cc22-ddddd3333444ddd",
    "isDefault": true,
    "name": "Microsoft Azure Enterprise",
    "state": "Enabled",
    "tenantId": "xxxxx-yyyy-999z-9090-uuuuu999uuuu",
    "user": {
    "name": "user@org.com",
    "type": "user"
    }
```

Step 5 Create a service principal using the Azure CLI.

```
az ad sp create-for-rbac -n myserviceprincipal
```

Where, `myServicePrincipal` is the name of the service principal. You may give any name for your service principal.

Step 6 From the command output on the Azure CLI, note down the values of the `appID`, `password`, and `tenant` parameters. These values are required while Adding Azure Provider Profile to Cisco Container Platform.

For example:

```
{
    "appId": "qqqqqqqq-a1a1-2b2b-9z9z-wwww1111vvvv",
    "displayName": "myserviceprincipal",
    "name": "http://myserviceprincipal",
    "password": "mmmmmm-n0n0-p1p1-q3q3-uuuu0000vvvv",
    "tenant": "xxxxx-yyyy-999z-9090-uuuuu999uuuu"
}
```

Adding Google Kubernetes Engine Provider Profile

Before you begin

Ensure that you have completed the prerequisites for configuring clusters on Google Kubernetes Engine (GKE). For more information, see Prerequisites for Configuring Clusters on GKE.

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

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

a) In the **PROVIDER NAME** field, enter a name for the related GKE account.

b) In the **CREDENTIALS** field, copy and paste the content from the credentials.json file that you created on Google Cloud Platform (GCP).

For more information, see Creating User Credentials on GCP.

c) From the **PROJECT ID** drop-down list, choose the project ID in which you want to create the GKE clusters.

Step 3 Click **ADD**.

For more information on administering clusters on Google Cloud Platform (GCP), see Administering Clusters on Google Kubernetes Engine (GKE).

Modifying Provider Profile

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

Step 2 Click the **vSphere**, **AWS**, **OpenStack**, **Azure**, or **GKE** tab as necessary.

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

Step 4 Change the provider details as necessary and click **SUBMIT**.

Deleting Provider Profile

Step 1 In the left pane, click **Infrastructure Providers**.

Step 2 Click the **vSphere**, **AWS**, **OpenStack**, **Azure**, or **GKE** 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 In 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 (VMMD) 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 In 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 In 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 applies to a non-ACI environment.

Based on the information that you provided during installation, Cisco Container Platform creates a network, subnet, and an IP pool. Cisco Container Platform requires a minimum of six IP addresses. After installation, you can add or modify the IP pool range, subnet, or network by using the Cisco Container Platform web interface. The IP address pools define the IP address ranges that are managed by Cisco Container Platform.

Note You must ensure that the range of IP addresses in the VIP pools is outside of the IP addresses that are assigned by DHCP.

The IP addresses that are managed by Cisco Container Platform are used for the following purposes:

- A VIP for the Cisco Container Platform Kubernetes Master
- A VIP for the external Ingress access of Cisco Container Platform
- Static Interface IP addresses for master and worker nodes in each tenant cluster
- A VIP for the Kubernetes master of each tenant cluster
- A VIP for the external NGINX Ingress Controller of each tenant cluster

- VIPs for any LoadBalancer type Kubernetes Service of a tenant cluster

To create tenant clusters, you need to configure a subnet during cluster creation. The total number of free IP addresses across all the pools for that subnet must be at least:

3 + (Number of tenant worker nodes)

Modifying Networks

Step 1 In 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 In 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.
A gateway IP address allows a cluster to acess other networks.

Step 5 Enter the IP address of the necessary DNS nameserver.
You can click **+NAMESERVER** to enter IP addresses of additional nameservers.

Step 6 Click **SUBMIT**.

Modifying Subnets

Step 1 In 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, CIDR, gateway IP or list of nameservers as necessary.

Step 5 Click **SUBMIT**.

Adding VIP Pool

Step 1 In 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 In 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**.