Configuring the Cloud Formation Template Information for the Cisco Cloud APIC

Deploying the Cloud APIC in AWS

Before you begin

- Verify that you have met the requirements that are outlined in Requirements for Extending the Cisco ACI Fabric to the Public Cloud before proceeding with the tasks in this section. For example, verify that you have the correct number of elastic IP addresses and that you have checked the limits allowed to deploy the instances.
- Verify that you have the full Administrator Access on AWS, because specific AWS IAM roles and permissions are required for the installation and operation of the Cisco Cloud APIC.

  When installing Cloud APIC using the CloudFormation template (CFT), we recommend installation by a user who has the full Administrator Access on AWS (for example, by a user who has the permission policy ARN **arn:aws:iam::aws:policy/AdministratorAccess** attached to it, either directly, by using a role policy, or with a user group). However, if there is no one with AWS Administrator Access available, the person installing Cloud APIC must have a minimum set of permissions. See AWS IAM Roles and Permissions for more information on these AWS IAM roles and permissions.
- If you are using AWS Organizations to control access policies and permissions for various accounts and you want to use Cloud APIC to manage these accounts, verify that the AWS account where you are deploying the Cloud APIC in these procedures (the Cloud APIC infra tenant) is the master account for that AWS organization. When the Cloud APIC is deployed in the master account for an AWS organization, you can add any AWS accounts that are part of the organization as tenants through the Cloud APIC GUI. See Support for AWS Organizations and Organization User Tenant and Configuring a Shared Tenant for more information.
- If you are deploying Cloud APIC on AWS GovCloud, review the information provided in the section "AWS GovCloud Support" in Extending the Cisco ACI Fabric to the Public Cloud for information specific to those deployments.

Step 1 Log into your Amazon Web Services account for the Cloud APIC infra tenant and go to the AWS Management Console, if you are not there already:

https://signin.aws.amazon.com/

https://console.aws.amazon.com/

Step 2 In the upper right corner of the AWS Management Console screen, locate the area that shows a region, and choose the region in AWS that you want to have managed by Cloud APIC (where the Cloud APIC AMI image will be brought up).

Step 3 Create an Amazon EC2 SSH key pair:

a) Click the **Services** link at the top left area of the screen, then click the **EC2** link.

The **EC2 Dashboard** screen appears.

b) In the **EC2 Dashboard** screen, click the **Key Pairs** link.

The **Create Key Pair** screen appears.

c) Click **Create Key Pair**.

d) Enter a unique name for this key pair (for example, `CloudAPICKeyPair`), then click **Create**.

A screen is displayed that shows the public key that is stored in AWS. In addition, a Privacy Enhanced Mail (PEM) file is downloaded locally to your system with the private key.

e) Move the private key PEM file to a safe location on your system and note the location.

You will navigate back to the private key PEM file in this location in a step later in these procedures.

Step 4 Go to the Cloud APIC page on the AWS Marketplace:

http://cs.co/capic-aws

Step 5 Click **Subscribe**.

Step 6 Review and accept the End User License Agreement (EULA) by clicking the **Accept Terms** button.

Step 7 After a minute, you should see the message `Subscription should be processed`. Click the **Continue to Configuration** button.

The **Configure this software** page appears.

Step 8 Select the following parameters:

- **Fulfillment Option:** Cisco Cloud APIC Cloud Formation Template (selected by default)
- **Software Version:** Select the appropriate version of the Cloud APIC software
- **Region:** Region where Cloud APIC will be deployed

Step 9 Click the **Continue to Launch** button.

The **Launch this software** page appears, which shows a summary of your configuration and lets you launch the cloud formation template.

Step 10 Click **Launch** to go directly to the CloudFormation service in the correct region, with the correct Amazon S3 template URL already populated.

Step 11 Click **Next** at the bottom of the screen.

The **Specify Details** page appears within the **Create stack** page.

Step 12 Enter the following information on the **Specify Details** page.

- **Stack name:** Enter the name for this Cloud APIC configuration.
- **Fabric name:** Leave the default value as-is or enter a fabric name. This entry will be the name for this Cloud APIC.
- **Infra VPC Pool:** The VPC (Virtual Private Cloud) CIDR. This field is automatically populated from the CFT with a default value of 10.10.0.0/24. Change the value in this field if the default value overlaps with your infra pool from your on-premises fabric. This entry must be a /24 subnet.

  Note We recommend that you do not use any subnet from 172.17.0.0/16 (for example, 172.17.10.0/24) as the infra VPC CIDR, as this might cause a conflict with the Docker bridge IP subnet, as described in Resolving Subnet Conflict Issue With Infra Subnet, on page 4.

- **Availability Zone:** Select an availability zone for the Cloud APIC subnets from the scroll-down menu.

  The availability zone options that are presented will be based on the region that you selected in Step 2, on page 2. Select the lowest availability zone from the list. For example, if you see `us-west-1a` and `us-west-1b` as the availability zone options, select `us-west-1a`.

- **Password/Confirm Password:** Enter and confirm an admin password. This entry is the password that you will use to log into the Cloud APIC after you have enabled SSH access.
- **SSH Key Pair:** Choose the name of the SSH key pair that you created in Step 3, on page 2.

  You will use this SSH key pair to log into the Cloud APIC.

- **Access Control:** Enter the IP addresses and subnets of the external networks that you will allow to connect to Cloud APIC (for example, 192.0.2.0/24). Only the IP addresses from this subnet are allowed to connect to Cloud APIC. Entering a value of `0.0.0.0/0` means that anyone is allowed to connect to Cloud APIC.
- **Other parameters: Assign Public IP address**: Select whether to assign a public IP address to the Out-of-Band (OOB) management interface for the Cloud APIC or not.

  Prior to release 5.2(1), the management interface of the Cloud APIC was assigned a public IP address and a private IP address. Beginning with release 5.2(1), a private IP address is assigned to the management interface of the Cloud APIC and assigning a public IP address is optional. For more information, see the "Private IP Address Support for Cisco Cloud APIC and CCR" topic in the *Cisco Cloud APIC for AWS User Guide*, Release 5.2(1) or later.

  - **true**: Assigns a public IP address to the Out-of-Band (OOB) management interface for the Cloud APIC.
  - **false**: Disables the public IP address and assigns a private IP address to the Out-of-Band (OOB) management interface for the Cloud APIC.

Step 13 Click **Next** at the bottom of the screen.

The **Options** page appears within the **Create stack** page.

Step 14 Accept all the default values in the **Options** screen.

There is a **Permissions: IAM Role** area on this page. An IAM role is an IAM entity that defines a set of permissions for making Amazon Web Services service requests. You can use roles to delegate access to users, applications, or services that don't normally have access to your Amazon Web Services resources.

There is no need for IAM role information with regards to the Cloud APIC, but if you want to assign an IAM role for another reason, choose the appropriate role in the **IAM Role** field.

Step 15 Click **Next** at the bottom of the **Options** screen.

The **Review** page appears within the **Create stack** page.

Step 16 Verify that all the information on the **Review** page is correct.

If you see any errors on the **Review** page, click the **Previous** button to go back to the page with the incorrect information.

Step 17 When you have verified that all the information on the **Review** page is correct, check the box next to the **I acknowledge that AWS CloudFormation might create IAM resources with custom names** area.

Step 18 Click the **Create** button at the bottom of the page.

The **CloudFormation** page reappears, and the Cloud APIC template that you created is displayed with the text **CREATE_IN_PROGRESS** displayed in the Status column.

The system now uses the information that you provided in the template to create the Cisco Cloud APIC instance. This process takes 5-10 minutes to complete. You can monitor the progress of the creation process by checking the box next to the name of your Cisco Cloud APIC template, then clicking on the Events tab. The text **CREATE_IN_PROGRESS** is displayed in the Status column under the Events tab.

Step 19 When the **CREATE_COMPLETE** message is shown, verify that the instance is ready before proceeding.

a) Click the **Services** link at the top of the screen, then click the **EC2** link.

The **EC2 Dashboard** screen appears.

b) In the EC2 Dashboard screen, you should see text displaying the number of running instances in the **Resources** area (for example, **1 Running Instances**). Click this running instances link.

The **Instances** screen appears.

c) Wait until you see that instance is ready before proceeding.

You will see the new instance going through the **Initializing** stage under Status Checks. Wait until you see the **2/2 Checks Passed** message under Status Checks before proceeding.

What to do next

Go to Setting Up the AWS Account for the User Tenant, on page 6 to set up the AWS account for the user tenant.

Resolving Subnet Conflict Issue With Infra Subnet

In some situations, you might encounter an issue with a subnet conflict with your Cloud APIC. This issue might occur when the following conditions are met:

- Your Cloud APIC is running on release 25.0(2)
- The infra VPC subnet for your Cloud APIC is configured within the 172.17.0.0/16 CIDR (for example, if you entered `172.17.10.0/24` in the **Infra VPC Pool** field as part of the procedures in Deploying the Cloud APIC in AWS, on page 1)

- There is something else configured that overlaps with the 172.17.0.0/16 CIDR that you are using for the infra VPC subnet for your Cloud APIC (for example, if the Docker bridge IP subnet is configured with `172.17.0.0/16`, which is the default subnet in Cloud APIC).

In this situation, your Cloud APIC might not be able to reach the CCR private IP address due to this subnet conflict and the Cloud APIC will raise an SSH connectivity fault for the affected CCR.

You could determine if there might be a possible conflict by logging in as root into the Cloud APIC and entering the `route -n` command:

```
[root@ACI-Cloud-Fabric-1 ~]# route -n
```

Assume that you see output similar to the following:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.17.0.17     0.0.0.0         UG    16     0        0 oobmgmt
169.254.169.0   0.0.0.0         255.255.255.0   U     0      0        0 bond0
169.254.254.0   0.0.0.0         255.255.255.0   U     0      0        0 lxcbr0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
172.17.0.12     0.0.0.0         255.255.255.252 U     0      0        0 bond0
172.17.0.16     0.0.0.0         255.255.255.240 U     0      0        0 oobmgmt
```

In this example output, the highlighted text shows that a Docker bridge is configured with `172.17.0.0/16`.

Because this overlaps with the 172.17.0.0/16 CIDR that you used for the infra VPC subnet for your Cloud APIC, you might see an issue where you lose connectivity to the CCR, where you are not able to SSH into the CCR, and you see a Host Unreachable message when you try to ping the CCR (such as in the following example, where 172.17.0.84 is the private IP address of the CCR):

```
[root@ACI-Cloud-Fabric-1 ~]# ping 172.17.0.84
PING 172.17.0.84 (172.17.0.84) 56(84) bytes of data.
From 172.17.0.1 icmp_seq=1 Destination Host Unreachable
From 172.17.0.1 icmp_seq=2 Destination Host Unreachable
From 172.17.0.1 icmp_seq=3 Destination Host Unreachable
From 172.17.0.1 icmp_seq=5 Destination Host Unreachable
From 172.17.0.1 icmp_seq=6 Destination Host Unreachable
^C
--- 172.17.0.84 ping statistics ---
9 packets transmitted, 0 received, +5 errors, 100% packet loss, time 8225ms
pipe 4
[root@ACI-Cloud-Fabric-1 ~]#
```

To resolve the conflict in this situation, enter a REST API post similar to the following to change the IP address for the other area that is causing the conflict:

```
https://{{apic}}/api/plgnhandler/mo/.xml
<apPluginPolContr>
    <apContainerPol containerBip="<new-IP-address>" />
</apPluginPolContr>
```

For example, to move the Docker bridge IP address out from under the 172.17.0.0/16 CIDR, which was shown in the example scenario above, you might enter a REST API post such as the following:

```
https://{{apic}}/api/plgnhandler/mo/.xml
<apPluginPolContr>
    <apContainerPol containerBip="172.19.0.1/16" />
</apPluginPolContr>
```

where `172.19.0.1/16` is the new subnet for the Docker bridge. This moves the Docker bridge IP address under the 172.19.0.0/16 CIDR, where there is no longer a conflict with the infra VPC subnet for your Cloud APIC that is configured within the 172.17.0.0/16 CIDR.

You can use the same commands as before to verify that there is no longer a conflict:

```
[root@ACI-Cloud-Fabric-1 ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         172.17.0.17     0.0.0.0         UG    16     0        0 oobmgmt
169.254.169.0   0.0.0.0         255.255.255.0   U     0      0        0 bond0
169.254.254.0   0.0.0.0         255.255.255.0   U     0      0        0 lxcbr0
172.17.0.12     0.0.0.0         255.255.255.252 U     0      0        0 bond0
172.17.0.16     0.0.0.0         255.255.255.240 U     0      0        0 oobmgmt
172.19.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
```

In this example output, the highlighted text shows that a Docker bridge is configured with the IP address `172.19.0.0`. Because there is no overlap with the 172.17.0.0/16 CIDR that you are using for the infra VPC subnet for your Cloud APIC, there is no issue with connectivity with the CCR:

```
[root@ACI-Cloud-Fabric-1 ~]# ping 172.17.0.84
PING 172.17.0.84 (172.17.0.84) 56(84) bytes of data.
64 bytes from 172.17.0.84: icmp_seq=1 ttl=255 time=1.15 ms
64 bytes from 172.17.0.84: icmp_seq=2 ttl=255 time=1.01 ms
64 bytes from 172.17.0.84: icmp_seq=3 ttl=255 time=1.03 ms
64 bytes from 172.17.0.84: icmp_seq=4 ttl=255 time=1.03 ms
64 bytes from 172.17.0.84: icmp_seq=5 ttl=255 time=1.09 ms
64 bytes from 172.17.0.84: icmp_seq=6 ttl=255 time=1.06 ms
64 bytes from 172.17.0.84: icmp_seq=7 ttl=255 time=1.03 ms
64 bytes from 172.17.0.84: icmp_seq=8 ttl=255 time=1.05 ms
^C
--- 172.17.0.84 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7005ms
rtt min/avg/max/mdev = 1.014/1.061/1.153/0.046 ms
[root@ACI-Cloud-Fabric-1 ~]#
```

Setting Up the AWS Account for the User Tenant

You can set up the AWS account for the user tenant using one of the following methods:

- Where the user tenant in Cloud APIC is trusted, using the CFT. See Setting Up the AWS Account for a Trusted User Tenant Using the CFT, on page 6.
- Where the user tenant in Cloud APIC is untrusted, using the AWS access key ID and secret access key. See Setting Up the AWS Account for an Untrusted User Tenant Using the AWS Access Key ID and Secret Access Key, on page 8.
- Where you can manage policies for AWS Organization accounts through the Cloud APIC. See Setting Up the AWS Account for an Organization User Tenant, on page 10.

Setting Up the AWS Account for a Trusted User Tenant Using the CFT

Using the tenant role Cloud Formation template (CFT) in the tenant account establishes a trust relationship between the tenant and the account where the Cloud APIC is deployed.

Use the following procedures to set up the AWS account for the user tenant using the tenant role CFT.

Before you begin

Following are the rules and restrictions for configuring the Cloud APIC user tenant:

- You cannot use the same AWS account for the infra tenant and the user tenant.
- You need one AWS account for each user tenant.

Step 1 Log into your Amazon Web Services account for the user tenant:

https://signin.aws.amazon.com/

Note Do not use the infra tenant account for the user tenant.

Step 2 Click the **Services** link at the top of the screen, then click the **CloudFormation** link.

The **CloudFormation** screen appears.

Step 3 Click the **Create Stack** button.

Note Do not choose any options from the drop-down list next to the **Create Stack** button. Click directly on the **Create Stack** button instead.

The **Select Template** page appears within the **Create stack** page.

Step 4 Determine how you will select the template to use for the IAM role for the user tenant configuration.

- If you want to download the tenant role CFT from your AWS account, or if you downloaded it from your cisco.com account (formerly CCO), follow these procedures:
  - **a.** If you want to download the tenant role CFT from your AWS account, locate the tenant role CFT. The tenant role CFT is located in the S3 bucket in the AWS account for the Cisco Cloud APIC infra tenant. The name of the S3 bucket is capic-common-[capicAccountId]-data and the tenant role CFT object is tenant-cft.json in that bucket. The capicAccountId is the AWS account number for the Cisco Cloud APIC infra tenant, which is the account in which Cloud APIC is deployed.
  - **b.** Download the tenant role CFT to a location on your computer.

    For security reasons, public access to this S3 bucket in AWS is not allowed, so you must download this file and use it in the tenant account.
  - **c.** In AWS, in the **Choose a template** area, click the circle next to **Upload a template to Amazon S3**, then click the **Choose File** button.
  - **d.** Navigate to the location on your computer where you saved the JSON-formatted tenant role CFT that you received from Cisco (for example, `tenant-cft.json`) and select that template file.
- If you were given a tenant role CFT URL from Cisco, in the **Choose a template** area, click the circle next to **Specify an Amazon S3 template URL**, then enter the tenant role CFT URL that you received from Cisco into the field below the text.

Step 5 Click **Next** at the bottom of the screen.

The **Specify Details** page appears within the **Create stack** page.

Step 6 Enter the following information on the **Specify Details** page.

- **Stack name:** Enter the name for this IAM role for the user tenant configuration (for example, `IAM-Role`).
- **infraAccountId:** If you see this field, enter the AWS account for the infra tenant as described in Deploying the Cloud APIC in AWS, on page 1.

  Note that this field is displayed if you downloaded and used the tenant role CFT from your cisco.com account. It is not displayed if you downloaded and used the tenant role CFT from your AWS account because the infraAccountId information is pre-populated in the CFT when it is downloaded from the S3 bucket in the infra AWS account.

Step 7 Click **Next** at the bottom of the screen.

The **Options** page appears within the **Create stack** page.

Step 8 Accept all the default values in the **Options** screen, if applicable, then click **Next** at the bottom of the screen.

The **Review** page appears within the **Create stack** page.

Step 9 In the **Review** page, check the box next to the **I acknowledge that AWS CloudFormation might create IAM resources with custom names** area, then click the **Create** button at the bottom of the page.

The **CloudFormation** page reappears, and the Cisco Cloud APIC template that you created is displayed with the text **CREATE_IN_PROGRESS** displayed in the Status column.

The system now uses the information that you provided in the template to create the IAM role for the user tenant. This process takes 5-10 minutes to complete. You can monitor the progress of the creation process by checking the box next to the name of the template, then clicking on the Events tab. The text **CREATE_IN_PROGRESS** is displayed in the Status column under the Events tab.

CREATE_COMPLETE is shown when the process is completed.

Step 10 When the **CREATE_COMPLETE** is shown, navigate to the appropriate area to verify that the IAM role for the user tenant was created successfully.

a) Click the **Services** link at the top of the screen, then click the **IAM** link.
b) Click **Roles**.

An entry with the name **ApicTenantRole** should appear under the Role name.

What to do next

Go to Configuring Cisco Cloud APIC Using the Setup Wizard to continue setting up the Cisco Cloud APIC.

Setting Up the AWS Account for an Untrusted User Tenant Using the AWS Access Key ID and Secret Access Key

Use the following procedures if you want to set up the AWS account for an untrusted user using the AWS access key ID and secret access key, where you will manually set up the AWS account for an untrusted user tenant and assign the appropriate permissions through AWS IAM.

Before you begin

Following are the rules and restrictions for configuring the Cloud APIC user tenant:

- You cannot use the same AWS account for the infra tenant and the user tenant.
- You need one AWS account for each user tenant.

Step 1 Log into your Amazon Web Services account for the user tenant:

https://signin.aws.amazon.com/

Note Do not use the infra tenant account for the user tenant.

Step 2 Go to the AWS Management Console:

https://console.aws.amazon.com/

Step 3 Click the **Services** link at the top of the screen, then click the **IAM** link.

Step 4 In the left pane, click **Users**, then click the **Add user** button.

The **Add User** page appears.

Step 5 In the **User name** field, enter a unique name for this AWS user account, such as `user1`.

Step 6 In the **Access type** field, check **Programmatic access**.

Step 7 Click the **Next: Permissions** button at the bottom of the page.

Step 8 In the **Set permissions** area, select **Attach existing policies directly**.

The screen expands to display **Filter policies** information.

Step 9 Check the box next to **Administrator Access**, then click the **Next: Tags** button at the bottom of the page.

Step 10 Leave the information in the **Add tags** page as-is and click the **Next: Review** button at the bottom of the page.

Step 11 Click the **Create User** button at the bottom of the page.

Ignore the warning that states **This user has no permissions** if that warning appears.

An access key is created for you at this point.

Step 12 Make a note of the Access Key ID and Secret Access Key information for this AWS account.

- Copy the Access Key ID and the Secret Access Key information for the user tenant to the appropriate rows in Locating CCR and Tenant Information.
- Download the .csv file or copy the information from the **Access key ID** and **Secret access key** fields to a file.

Step 13 Click the **Close** button at the bottom of the page.

Step 14 Repeat the steps in this topic for additional user accounts, if necessary.

What to do next

Go to Configuring Cisco Cloud APIC Using the Setup Wizard to continue setting up the Cisco Cloud APIC.

Setting Up the AWS Account for an Organization User Tenant

As described in Support for AWS Organizations and Organization User Tenant, beginning with Release 4.2(3), you can now manage policies for AWS Organization accounts through the Cloud APIC.

To set up the AWS account for an organization tenant, you must have the following configurations in order to use this feature:

- The Cloud APIC must be deployed in the master account. Earlier in this document, when you deployed the Cloud APIC in AWS using the instructions provided in Deploying the Cloud APIC in AWS, on page 1, verify that you deployed the Cloud APIC (the Cloud APIC infra tenant) in the master account for this AWS organization.
- Later in this document, you will assign the Organization tag to tenants through the Cloud APIC GUI, using procedures described in Configuring a Shared Tenant.