

# Performing a System Upgrade, Downgrade or Recovery

- Important Notes, on page 1
- Upgrading the Software, on page 5
- Downgrading the Software, on page 14
- Performing a System Recovery, on page 29
- Triggering an Upgrade of the CCRs, on page 29

## **Important Notes**

- Important Notes For Release 25.0(3), on page 1
- General Important Notes, on page 4

#### Important Notes For Release 25.0(3)

Following are important notes for release 25.0(3) regarding the installation, upgrade or downgrade procedures for the Cisco Cloud APIC:

- Because of the move from the Cisco Cloud Services Router 1000v to the Cisco Catalyst 8000V, you must add the necessary policy before upgrading from a release prior to 25.0(3) to release 25.0(3):
- 1. Go to the infra tenant in the AWS portal.
- 2. Click IAM > Policies.
- 3. In the Policies window, click the ApicAdminFullAccess policy.

The **Summary** page for this policy is displayed.

4. Click Edit Policy.

{

- 5. Click the JSON tab.
- 6. Copy the entry below and paste it into the policy:

```
"Effect": "Allow",
"Action": "ssm:*",
```

```
"Resource": "*"
```

- 7. Click Review Policy, then click Save Changes.
- The Cisco Catalyst 8000V supports subscription-based licensing. Before upgrading from a release prior to 25.0(3) to release 25.0(3), you must first subscribe to one of the tier-based Cisco Catalyst 8000V licenses.
  - For instructions on subscribing to one of the tier-based Cisco Catalyst 8000V licenses, see Cisco Catalyst 8000V Edge Software.
  - For more information on different throughputs based on the tiers, see Requirements for the AWS Public Cloud.

Cisco Cloud APIC makes use of the "Cisco DNA Advantage" subscription. For features supported by the "Cisco DNA Advantage" subscription, see Cisco DNA SoftwareSD-WAN and Routing Matrices.

- When you upgrade your Cisco Cloud APIC to release 25.0(3), you should then upgrade the CCRs as soon after the Cisco Cloud APIC upgrade as possible. For those instructions, see:
  - Upgrading the Software, on page 5
  - Triggering an Upgrade of the CCRs, on page 29

Following are examples of how you would go through these upgrade processes:

- Single-Site Upgrade: You normally would not need to have CCRs for a single-site AWS deployment. However, if you do have CCRs deployed in this situation, once the Cisco Cloud APIC has completed the upgrade to release 25.0(3) and reached the ready state, you must then start the upgrade of the older CCRs (the Cisco Cloud Services Router 1000v) to the newer CCRs (the Cisco Catalyst 8000V) before making any configuration changes.
- Multi-Cloud/Hybrid-Cloud Upgrade: As an example of this upgrade process, assume that you
  have the following setup:
  - Site 1: AWS
  - Site 2: Azure
  - Site 3: On-premises site

You would then upgrade these sites the following way:

- **1.** Upgrade Nexus Dashboard Orchestrator to the 3.7(1) release.
- 2. Upgrade site 1 (AWS site) to the Cisco Cloud APIC release 25.0(3) using the procedures in Upgrading the Software, on page 5.

Wait until this upgrade has reached the steady state before proceeding to the next step.

**3.** Upgrade the CCRs on site 1 (AWS site) from the older CCRs (the Cisco Cloud Services Router 1000v) to the newer CCRs (the Cisco Catalyst 8000V) using the procedures in Triggering an Upgrade of the CCRs, on page 29.

Wait until the CCRs are fully upgraded to the newer Cisco Catalyst 8000Vs before proceeding to the next step.

- **4.** Once the CCRs on site 1 (AWS site) are fully upgraded, repeat these steps for site 2 (Azure site), where you will first upgrade the Cisco Cloud APIC software to release 25.0(3). After that upgrade has reached the steady state, then you will upgrade the CCRs on site 2 to the newer Cisco Catalyst 8000Vs.
- Prior to Cisco Cloud APIC release 25.0(3), the older Cisco Cloud Services Router 1000v routers were configured with number-based throughput, as described in Requirements for the AWS Public Cloud. Since the Cisco Catalyst 8000V routers will only support tier-based throughput options, during upgrades to release 25.0(3), the Cisco Cloud APIC will map the throughput values from the number-based throughput used by the older Cisco Cloud Services Router 1000v routers to the tier-based throughput used by the newer Cisco Catalyst 8000V routers.

The following table shows the mapping of throughput from the older Cisco Cloud Services Router 1000v routers to the newer Cisco Catalyst 8000V routers during an upgrade:

Throughput on Cisco Cloud Services Router 1000v	Throughput on Cisco Catalyst 8000V
10M	T0 (up to 15M throughput)
50M	T1 (up to 100M throughput)
100M	T1 (up to 100M throughput)
250M	T2 (up to 1G throughput)
500M	T2 (up to 1G throughput)
16	T2 (up to 1G throughput)
2.5G	T3 (up to 10G throughput)
5G	T3 (up to 10G throughput)
7.5G	T3 (up to 10G throughput)
10G	T3 (up to 10G throughput)

When migrating from the older Cisco Cloud Services Router 1000v routers to the newer Cisco Catalyst 8000V routers during an upgrade, the Cisco Cloud APIC will migrate the comparable bandwidth as described above. When these Cisco Catalyst 8000V routers come up, they will try to register for that bandwidth to the smart licensing account. If the smart licensing server does not have these licenses, then the Cisco Catalyst 8000V will fall back to the default bandwidth and will fail to service the existing workload traffic. So you must procure and provision the required Cisco Catalyst 8000V licenses in your smart account before migrating from the older Cisco Cloud Services Router 1000v routers to the newer Cisco Catalyst 8000V routers during an upgrade.

• Similarly, when downgrading from release 25.0(3) to an earlier release, the Cisco Cloud APIC will map the throughput values from the tier-based throughput used by the newer Cisco Catalyst 8000V routers to the number-based throughput used by the older Cisco Cloud Services Router 1000v routers.

The following table shows the mapping of throughput from the newer Cisco Catalyst 8000V routers to the number-based throughput used by the older Cisco Cloud Services Router 1000v routers during a downgrade:

Throughput on Cisco Catalyst 8000V	Throughput on Cisco Cloud Services Router 1000v
T0 (up to 15M throughput)	10M
T1 (up to 100M throughput)	100M
T2 (up to 1G throughput)	16
T3 (up to 10G throughput)	10G



**Note** Do not make any configuration changes when the Cisco Cloud APIC and the CCRs are in incompatible mode. When upgrading to release 25.0(3), verify that both the Cisco Cloud APIC and the CCRs are upgraded to that latest release before making any configuration changes.

#### **General Important Notes**

Following are general important notes:

- Cisco Cloud APIC supports policy-based upgrades for the following upgrade paths:
  - Release 5.2(1) to 25.0(2), 25.0(3), or 25.0(4)
  - Release 25.0(1) to 25.0(2), 25.0(3), or 25.0(4)
  - Release 25.0(2) to 25.0(3) or 25.0(4)
  - Release 25.0(3) to 25.0(4)
- When you downgrade from release 5.0(x) to a previous release, as the CCRs downgrade to a lower release, you could see some of the tunnels in a "down" state in the CCRs. This could occur due to stale VPN resources in the AWS accounts that did not get cleaned up.

To correct this issue, manually clean up the stale VPN connections.

- As noted in Requirements for the AWS Public Cloud, the supported instance type for the Cisco Cloud APIC deployment has changed for release 5.0(x) or later:
  - For releases prior to release 5.0(x), Cisco Cloud APIC is deployed using the m4.2xlarge instance.
  - For release 5.0(x) and later, Cisco Cloud APIC is deployed using the m5.2xlarge instance.

When upgrading from a 4.2(x) release to release 5.0(x) or later, policy-based upgrades are not supported because you cannot change the instance type through a policy-based upgrade; instead, for these upgrades, you must upgrade using a migration procedure, as provided in Migration-Based Upgrade, on page 9.

• There is an issue with the upgrade process where an upgrade from release 5.2(1g) to any later release will fail.

To work around this issue, enable the Ignore Compatibility Check option:

 Follow the normal upgrade instructions provided in Upgrading the Software Using the Policy-Based Upgrade Process, on page 8 until you get to the Ignore Compatibility Check step in the Schedule Upgrade window. 2. Enter a check mark in the box next to the **Ignore Compatibility Check** field to enable the **Ignore Compatibility Check** option.

Enabling the Ignore Compatibility Check option allows this specific upgrade to proceed normally.

- **3.** Complete the upgrade to the post-5.2(1g) release.
- 4. Once you have completed the upgrade to the post-5.2(1g) release, return to the Schedule Upgrade window and remove the check mark in the box next to the Ignore Compatibility Check field.

This disables the Ignore Compatibility Check option, which is the default setting for this field.

• Due to the issue described in the previous bullet, if you are upgrading from a release prior to release 5.2(1) to a 5.2(1) release, we recommend that you upgrade directly to release  $5.2(1\mathbf{h})$  and not release  $5.2(1\mathbf{g})$ .

## Upgrading the Software

The following sections provide information on upgrading the Cisco Cloud APIC software using either a policy-based upgrade or a migration-based upgrade.

Cisco Cloud APIC supports policy-based upgrades for the following upgrade paths:

- Release 5.2(1) to 25.0(2), 25.0(3), or 25.0(4)
- Release 25.0(1) to 25.0(2), 25.0(3), or 25.0(4)
- Release 25.0(2) to 25.0(3) or 25.0(4)
- Release 25.0(3) to 25.0(4)

Go to Policy-Based Upgrade, on page 6 for those procedures.



**Note** If the policy-based upgrade does not work for some reason, you can upgrade using the migration-based process as described in Migration-Based Upgrade, on page 9.

#### **Upgrading the CCRs**

Regardless of the method that you use to upgrade your Cisco Cloud APIC software, the CCRs must also be upgraded whenever the Cloud APIC software is upgraded.

- Prior to release 5.2(1), the CCRs are upgraded automatically whenever you trigger an upgrade for the Cisco Cloud APIC.
- Beginning with release 5.2(1), you can trigger upgrades to the CCRs and monitor those CCR upgrades, independent from the Cisco Cloud APIC upgrades. This is useful to reduce traffic loss by allowing you to split up the upgrades for the management plane (Cisco Cloud APIC) and the data plane (CCRs).

See Triggering an Upgrade of the CCRs, on page 29 for more information.

## **Policy-Based Upgrade**

Use the procedures in the following sections to perform a policy-based upgrade of your Cisco Cloud APIC software.

#### **Backing Up Your Existing Configuration**

We recommend that you back up your existing configuration before performing any policy-based upgrades.

If you decide to downgrade back to that previous release at some point afterward using the procedures provided in Downgrading the Software, on page 14, you will need the backed-up configuration files in order to perform that downgrade successfully.

**Step 1** Enable Global AES encryption before performing the backup.

a) In your Cisco Cloud APIC GUI, navigate to Infrastructure > System Configuration.

You should see the General tab selected by default; if not, click the General tab.

b) Click the pencil icon at the upper right part of the Global AES Encryption area.

The Global AES Encryption Settings window appears.

c) Click the box next to the **Encryption: Enabled** area, enter a passphrase in the **Passphrase/Confirm Passphrase** fields, then click **Save** at the bottom of the window.

Make a note of the passphrase that you entered in this step, as you will need it if you need as part of the backup restoration process.

**Step 2** Make a note of the infra VPC pool that you configured during the stack deployment.

For the infra VPC pool, you might have multiple infra subnet pools, so be sure to locate the information for the infra subnet that was used when you launched the original Cisco Cloud APIC.

a) Log into your AWS account for the infra tenant:

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

b) Click the Services link at the top of the screen, then click the CloudFormation link.

The **CloudFormation** screen appears.

c) On the AWS CloudFormation dashboard, click your existing Cloud APIC stack.

The Stack details window appears for your Cloud APIC stack.

- d) Click the Parameters tab in the Stack details window.
- e) Locate the **pInfraVPCPool** line in the **Paramaters** table.

Make a note of the entry in the **pInfraVPCPool** line. This is infra VPC pool that you configured during the stack deployment.

- **Step 3** Back up your existing configuration.
  - a) Navigate to **Operations** > **Backup & Restore**.
  - b) Click the **Backup Policies** tab.
  - c) Click Actions > Create Backup Configuration.
  - d) Back up your existing configuration.

For more information on the options available in the **Create Backup Configuration**, see the "Creating a Backup Configuration Using the Cisco Cloud APIC GUI" procedure in the *Cisco Cloud APIC for AWS User Guide*.

#### **Downloading an Image**

- **Step 1** Log in to your Cisco Cloud APIC, if you aren't logged in already.
- **Step 2** From the Navigation menu, choose Operations > Firmware Management.

The Firmware Management window appears.

- Step 3 Click the Images tab in the Firmware Management window.
- **Step 4** Click Actions, then choose Add Firmware Image from the scroll-down menu.

The Add Firmware Image pop-up appears.

- **Step 5** Determine if you want to add the firmware image from a local or a remote location.
  - If you want to add the firmware image from a *local* location, click the **Local** radio button in the **Image Location** field. Click the **Choose File** button, then navigate to the folder on your local system with the firmware image that you want to import and select the file. Go to Step 6, on page 8.
  - If you want to import the firmware image from a *remote* location, click the **Remote** radio button in the **Image Location** field, then perform the following actions:
  - a) In the Protocol field, click either the HTTP or the SCP radio button.
  - b) In the URL field, enter the URL from where the image will be downloaded.
    - If you selected the HTTP radio button in the previous step, enter the http source that you want to use to download the software image. An example URL is
       10.67.82.87:/home/<username>/ACI/aci-capic-dk9.25.0.2f.iso. Go to Step 6, on page 8.
    - If you selected the SCP radio button in the previous step, enter the Secure Copy Protocol (SCP) source that you want to use to download the software image, using the format <SCP server>:/<path>. An example URL is 10.67.82.87:/home/<username>/ACI/aci-capic-dk9.25.0.2f.iso.
  - c) In the Username field, enter your username for secure copy.
  - d) In the **Authentication Type** field, select the type of authentication for the download. The type can be:
    - Password
    - SSH Key

The default is Password.

- e) If you selected **Password**, in the **Password** field, enter your password for secure copy. Go to Step 6, on page 8.
- f) If you selected **SSH Key**, enter the following information:
  - SSH Key Content The SSH Key Content is used to create the SSH Key File which is required when creating a Remote location for the download.

- **Note** The public key is generated at the time of the transfer. After the transfer the key files that were generated in the background are deleted. The temporary key files are stored in dataexport directory of the Cisco Cloud APIC.
- SSH Key Passphrase The SSH Key Passphrase is used to create the SSH Key File which is required when creating a Remote location for the download.
- Note The Passphrase field can remain empty.

## Step 6Click Select.Wait for the Cisco Cloud APIC firmware images to download.

#### Upgrading the Software Using the Policy-Based Upgrade Process

Use the procedures in the following sections to perform a policy-based upgrade of your Cisco Cloud APIC software.

#### Before you begin

Verify that you have downloaded an image using the procedures provided in Downloading an Image, on page 7.

#### **Step 1** Back up your existing configuration before performing the policy-based upgrade.

We recommend that you back up the configuration for your existing release using the information provided in Backing Up Your Existing Configuration, on page 6 before performing a policy-based upgrade.

After you have completed the policy-based upgrade, if you decide to downgrade back to the previous release at some point afterward using the procedures provided in Downgrading the Software, on page 14, you will need the backed-up configuration files from the previous release in order to perform that downgrade successfully.

**Step 2** In the Cloud APIC GUI, from the **Navigation** menu, choose the **Operations** > **Firmware Management**.

The Firmware Management window appears.

Step 3 Click Schedule Upgrade.

The Schedule Upgrade pop-up appears.

If you see a message that says that faults are present in your fabric, we recommend that you resolve these faults before performing a upgrade. See "Viewing Health Details Using the Cisco Cloud APIC GUI" in the *Cisco Cloud APIC for AWS User Guide* for more information.

- **Step 4** In the **Target Firmware** field, choose a firmware image from the scroll-down menu.
- **Step 5** In the **Upgrade Start Time** field, determine if you want to begin the upgrade now or later.
  - Click Now if you want to schedule the upgrade for now. Go to Step 6, on page 9.
  - Click Later if you want to schedule the upgrade for a later date or time, then select the date and time from the pop-up calendar for the scheduled upgrade.

**Step 6** In the **Ignore Compatibility Check** field, leave the setting in the default off (unchecked) setting, unless you are specifically told to disable the compatibility check feature.

In Cloud APIC, there is a compatibility check feature that verifies if an upgrade path from the currently-running version of the system to a specific newer version is supported or not. The **Ignore Compatibility Check** setting is set to off by default, so the system automatically checks the compatibility for possible upgrades by default.

**Note** If you choose to disable the compatibility check feature by entering a check mark in the box next to the **Ignore Compatibility Check** field, you run the risk of making an unsupported upgrade to your system, which could result in your system going to an unavailable state.

#### Step 7 Click Schedule Upgrade.

You can monitor the progress of the upgrade in the main **Firmware Management** window, under the **Upgrade Status** area.

### **Migration-Based Upgrade**

The following section provides migration-based upgrade procedures, which will allow you to upgrade without losing traffic flow.

#### Upgrading Your Cloud APIC Software Using Migration Procedures

This section provides the migration-based upgrade procedures for your Cisco Cloud APIC. There should be no effect on traffic with this migration.

- **Step 1** Enable the encryption passphrase control, if it is not enabled already.
  - a) In your Cloud APIC GUI, navigate to **Infrastructure** > **System Configuration**.

You should be underneath the General tab by default; if not, click the General tab.

- b) Determine if the encrypted passphrase control is enabled already.
  - In the Global AES Encryption area, if you see Yes underneath the Encryption and Key Configured fields, then you have the encrypted passphrase control enabled already. Go to Step 2, on page 9.
  - If you do not see Yes underneath the Encryption and Key Configured fields:
    - 1. Click the pencil icon at the upper right part of the Global AES Encryption area.

The Global AES Encryption Settings window appears.

- 2. Click the box next to the Encryption: Enabled area, enter a passphrase in the Passphrase/Confirm Passphrase fields, then click Save at the bottom of the window.
- **Step 2** Back up your existing Cloud APIC configuration.

There are a number of different ways that you can back up your Cloud APIC configuration. See the *Cloud APIC for AWS Users Guide* for more information. Note that if you want to use a remote backup, you will also need to add a remote location first.

**Step 3** Terminate the Cloud APIC EC2 instance from the AWS infra account.

 a) 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/

- b) Go into **Instances** in the EC2 Dashboard in the AWS Management Console.
- c) Locate the Cloud APIC instance.
  - For releases prior to release 5.0(x), Cisco Cloud APIC is deployed using the m4.2xlarge instance.
  - For release 5.0(x) and later, Cisco Cloud APIC is deployed using the m5.2xlarge instance.
- d) Check the box next to the Cloud APIC instance to select it, then click Actions > Instance State > Terminate.

In the **Terminate Instances** popup window, select **Yes, Terminate** to terminate this instance.

The **Instances** window reappears and the status changes to **shutting-down** in the **Instance State** row for the Cloud APIC instance. Even though you are terminating the Cloud APIC instance here, there should be no traffic drop for your Cloud APIC.

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

#### http://cs.co/capic-aws

- Step 5 Click Continue to Subscribe.
- **Step 6** In the **Subscribe to this software** page, click the **Continue to Configuration** button.

The Configure this software page appears.

- **Step 7** Select the following parameters:
  - Delivery Method: 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 8** 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 9** In the **Choose Action** field, choose **Launch CloudFormation**, then click **Launch** to go directly to the CloudFormation service in the correct region, with the correct Amazon S3 template URL already populated. The **Specify template** page appears within the **Create stack** page.
- **Step 10** In the **Specify template** page, make the following selections:
  - Prerequisite Prepare template field: Leave the default Template is ready option selected.
  - Specify template area:
    - In the Template source field, leave the default Amazon S3 URL option selected.
    - In the Amazon S3 URL field, leave the automatically-generated entry as-is.
    - · Click View in designer.

- **Step 11** In the **template1** area in the lower half of the screen:
  - Leave the Choose template language selection as JSON.
  - Place your cursor at the very beginning of the text string on line 1, press the Shift key and scroll down to the bottom of the window to select the entire text string in the window, then copy all of the text in this window (press Ctrl+C, or right-click and select **Copy**).
- **Step 12** On your local computer, navigate to an appropriate folder and create a text file, giving it a unique name, and paste the text string that you just copied into the text file.

This will be the Cloud APIC CFT, which has the m5.2xlarge instance type.

- **Step 13** Save and close the text file.
- **Step 14** Upload the Cloud APIC CFT to AWS.
  - a) Log in to the AWS CloudFormation console:

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

- b) On the AWS CloudFormation dashboard, click your existing Cloud APIC stack, then click Update.
- c) In the Update Stack wizard, in the Prepare template screen, select Replace current template. The Specify template area appears.
- d) In the Update Stack wizard, on the Specify template area, select Upload a template file.

The Upload a template file option appears.

- e) Click **Choose file** underneath the **Upload a template file** option and navigate to the area where you created the Cloud APIC CFT.
- f) Select the Cloud APIC CFT and then click Next.
- g) In the **Specify stack details** screen, verify that the instance type shown in the **Other parameters** area at the bottom of the screen is correctly set to **m5.2xlarge**, then click **Next**.

Do not change the instance type to **m4.2xlarge** in this step.

- h) In the Configure stack options screen, click Next.
- i) In the **Review** screen, click **Update stack**.

The following actions take place at this point:

- The AWS infra detects three IAM resources that will be updated (shown as False in the Replacement column).
- The AWS infra detects one EC2 instance that will be replaced (shown as **True** in the Replacement column).

Changes (4)											
Q Search char	Q Search changes										
Action	Logical ID	Physical ID	Resource type	Replacement							
Modify	rApicAdminFullAccess Policy	am:aws:iam::70289519 7007:policy/ApicAdmin FullAccess 🚺	AWS::IAM::ManagedPolicy	False							
Modify	rApicAdminReadOnly Role	ApicAdminReadOnly 🖸	AWS::IAM::Role	False							
Modify	rApicAdminRole	ApicAdmin 🔼	AWS::IAM::Role	False							
Modify	rCAPICInstance	i-0a767732513c1010c	AWS::EC2::Instignce	True							

This will bring up the new Cloud APIC instance with the release image, with the same public IP address as you had previously. You can check the progress of the new Cloud APIC instance coming up by navigating back to **Instances** in the EC2 Dashboard in the AWS Management Console.

**Step 15** When you see the **Instance State** change to **running**, you can then log into your Cloud APIC is you did previously.

The Cloud APIC will come up with no configurations at this point.

- Note If you see an error message when you try to log in, such as **REST Endpoint user authentication datastore** is not initialized - Check Fabric Membership Status of this fabric node, wait for several minutes, then try again after a few minutes. You might also have to refresh the page in order to log in.
- **Step 16** Enable the same encryption passphrase.
  - a) In your Cloud APIC GUI, navigate to Infrastructure > System Configuration.

You should be underneath the General tab by default; if not, click the General tab.

b) In the **Global AES Encryption** area, click the pencil icon at the upper right part of the **Global AES Encryption** area.

The Global AES Encryption Settings window appears.

c) Click the box next to the Encryption: Enabled area, enter the same passphrase in the Passphrase/Confirm Passphrase fields that you used in Step 1, on page 9, then click Save at the bottom of the window.

#### **Step 17** Import the configuration that you backed up in Step 2, on page 9.

If you configured a remote location when you backed up your configuration, you might have to create the remote location again to access the backup.

- a) In your Cloud APIC GUI, navigate to **Operations** > **Backup & Restore**.
- b) In the Backup & Restore window, click the Backups tab.
- c) Click the Actions scrolldown menu, then choose Restore Configuration.

The Restore Configuration window appears.

d) Enter the necessary information to restore the configuration that you backed up in Step 2, on page 9.

Use the following settings:

- In the **Restore Type** field, choose **Merge**.
- In the **Restore Mode** field, choose **Best Effort**.

Click **Restore Configuration** when you have entered the necessary information in this window. Click the **Job Status** tab in the **Backup & Restore** window to get the status of the backup restore.

**Step 18** Run the CapicTenantRole update to change the set for all trusted tenants.

a) 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) Click the tenant role CFT link.

The Overview page for this tenant role CFT appears.

c) Click the box next to the **tenant-cft.json** entry on the **Overview** page.

A slide-in pane appears for this JSON-formatted tenant role CFT.

d) Click Download to 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.

- e) In AWS, go to the user account of the trusted tenants, then click CloudFormation.
- f) On the AWS CloudFormation dashboard, locate the trusted tenant stack and click on the stack name for that trusted tenant.

The stack properties page appears for this particular stack.

- g) Click the Change sets tab.
- h) In the Change sets area, click Create change set .
- i) In the Create change set window for this stack, click **Replace current template**.
- j) In the **Specify template** area, click the circle next to **Upload a template file**, then click the **Choose File** button.
- k) Navigate to the location on your computer where you downloaded the tenant role CFT and select that template file.
- 1) Click **Next** in the Create change set window for this stack.

The Create Change Set pop-up appears.

m) Click Create Change Set in the Create Change Set pop-up window.

The Status will show as **CREATE\_PENDING** for a period of time, then will change to **CREATE\_COMPLETE**.

n) Repeat these steps for each trusted tenant.

On each trusted tenant, use this **tenant-cft.json** file to create a change set and run that change set.

**Step 19** In your Cloud APIC GUI, verify that all the configurations that you previously had for your Cloud APIC prior to the migration are present now.

Note that for releases prior to 5.2(1), the CCRs will also get upgraded automatically, from the 16.x version to the 17.x version. You can verify this by navigating to **Instances** in the EC2 Dashboard in the AWS Management Console and locating the CCR instances to verify that they are also upgraded.

For release 5.2(1) and later, CCRs are no longer upgraded automatically when the Cisco Cloud APIC is upgraded, so you must trigger the CCR upgrades separately after the Cisco Cloud APIC has finished upgrading. See Triggering an Upgrade of the CCRs, on page 29 for more information.

## **Downgrading the Software**

The following sections provide the necessary information that you will need to successfully downgrade your Cisco Cloud APIC software.

### Downgrading the Software: Release 25.0(1) to 5.2(1)

These procedures describe how to downgrade the software from release 25.0(1) to release 5.2(1).

These procedures assume the following scenario:

- 1. At some point previously, you were running release 5.2(1) and you decided to upgrade to release 25.0(1). Before you performed that upgrade, however, you backed up your release 5.2(1) configuration and saved that backed-up configuration file.
- 2. You then performed a policy-based upgrade to release 25.0(1) and, at some pointer later on, decided to revert back to release 5.2(1).

These procedures describe how to revert back to release 5.2(1), but you will need that backed-up release 5.2(1) configuration file in order for these downgrade procedures to work.

**Step 1** Verify that you have the backed-up release 5.2(1) configuration file, as described in Backing Up Your Existing Configuration, on page 6.

Do not use these procedures to downgrade from release 25.0(1) if you do not have that backed-up release 5.2(1) configuration file available. You will need that backup configuration file for these downgrade procedures.

- **Step 2** Verify that there are non-home region CCRs configured.
- **Step 3** Remove the CCRs from the home region.

There will be an intersite traffic loss for around 3-5 minutes while the home region CCRs are getting deleted and the traffic flow switches to the non-home region CCRs.

- a) In your Cloud APIC GUI, click the Intent icon (the icon with an arrow pointing into several circles) and choose Cloud APIC Setup.
- b) In the Region Management area, click Edit Configuration.

The **Regions to Manage** window appears.

- c) Unselect (remove checks from boxes) in the Cloud Routers column for the home region (the region that has the text Cloud APIC Deployed).
- d) Click **Next**, then enter the necessary information in the following page and click **Save and Continue**.

The process of removing the CCRs might take 5-10 minutes. You can monitor the process of the CCR removal by looking at the virtual machines in AWS portal.

**Note** Do not proceed to the next step until the CCRs in the home region have been completely removed.

**Step 4** From the infra account in the AWS portal, manually delete all infra VPC peering connections between the home region VPC and any remote region VPCs.

- a) In the navigation pane, choose **Peering connections**.
- b) Select the VPC peering connection, then choose Actions > Delete VPC peering connection.
- c) Inside the **Delete VPC peering connection** dialog box, review the connection details, check the **Delete related** route table entries checkbox to remove the necessary routes, then choose **Yes, Delete** to delete the selected VPC peering connection.

Do not alter any VPC peering connections from a remote region VPC to other remote region VPCs.

**Step 5** Wait 10-15 minutes for the remaining configurations to be deleted automatically.

The following configurations should be deleted automatically after 10-15 minutes:

- The connect peers for the transit gateway connect attachment in the home region
- The transit gateway connect attachment
- The transit gateway attachment to the infra VPC

If they do not delete automatically, delete them manually as follows:

- a) For the transit gateway connect attachment in the home region, delete the connect peers.
  - 1. In the navigation pane, choose Transit Gateway Attachments.
  - 2. Select the Connect attachment.
  - In the Connect peers tab, select the Transit Gateway Connect peer and choose Actions > Delete Connect peer.
  - 4. In the confirmation dialog box, choose Yes, Delete.
  - 5. Repeat these steps to delete additional connect peers for the transit gateway connect attachment in the home region.
- b) Delete the transit gateway connect attachment.
  - 1. In the navigation pane, choose Transit Gateway Attachments.
  - 2. Select the Connect attachment.
  - **3.** Choose **Actions** > **Delete**.
  - 4. When prompted for confirmation, choose Delete.
- c) Delete the transit gateway attachment to the infra VPC.
  - 1. In the navigation pane, choose **Transit Gateway Attachments**.
  - 2. Select the infra VPC attachment only.

There may be other user VPC attachments, so verify that you are selecting the infra VPC attachment for this procedure.

- **3.** Choose Actions > Delete.
- 4. When prompted for confirmation, choose Delete.

- **Step 6** Delete the stack.
  - a) In the AWS console, navigate to Services > CloudFormation > Stacks.
  - b) Select the stack that you want to delete.
  - c) Click Delete Stack.

This will delete the Cisco Cloud APIC VM and will attempt to delete the other resources.

**Step 7** Wait 15-20 minutes for the stack to be deleted.

If the stack deletion is stuck in Delete in Progress, then delete the infra VPC manually in the home region:

- a) In the AWS console, navigate to Services > Virtual Private Cloud > Your VPCs.
- b) Select the infra VPC.
- c) Choose Actions > Delete VPC.
- The **Delete VPC** window appears.
- d) Type delete in the To confirm deletion, type delete in the field area, then click Delete.
- **Step 8** Recreate a fresh stack with the cloud formation template for the release image that you're downloading to.
  - **Note** Alternatively, you can deploy a cloud formation template from the AWS Marketplace in place of steps a-c below.
  - a) In the AWS console, navigate to **Services** > **CloudFormation** > **Stacks**.
  - b) Click Create Stack > With new resources (standard). The Create stack window appears.
  - c) In the **Specify template** area, click the circle next to **Upload a template file**, then click the **Choose File** button.
  - Navigate to the location on your computer with the appropriate JSON-formatted tenant role CFT and select that template file, then click Next.

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

- e) Enter the necessary 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:** Use the same infra VPC pool information that you originally had when you first deployed your Cloud APIC.

You should have noted this infra VPC pool information as part of the procedures in Backing Up Your Existing Configuration, on page 6.

- Availability Zone: Select an availability zone for the Cloud APIC subnets from the scroll-down menu.
- Instance Type: Select the EC2 instance type.
- **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.

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 means that anyone is allowed to connect to Cloud APIC.

• 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.
- f) Click **Next** at the bottom of the screen.

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

g) Accept all the default values in the **Options** screen, then click **Next** at the bottom of the **Options** screen.

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

h) 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.

- i) 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.
- j) Click the **Create stack** 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.

- k) When the **CREATE\_COMPLETE** message is shown, verify that the instance is ready before proceeding.
  - 1. Click the Services link at the top of the screen, then click the EC2 link.

The EC2 Dashboard screen appears.

2. 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.

**3.** Wait until you see that instance is ready before proceeding.

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

- **Step 9** Enable Global AES encryption using the same passphrase that you noted when you backed up your configuration in Backing Up Your Existing Configuration, on page 6.
  - a) In your Cisco Cloud APIC GUI, navigate to Infrastructure > System Configuration.

It should be underneath the General tab by default; if not, click the General tab.

b) Click the pencil icon at the upper right part of the Global AES Encryption area.

The Global AES Encryption Settings window appears.

- c) Click the box next to the **Encryption: Enabled** area, then enter the passphrase that you noted in Backing Up Your Existing Configuration, on page 6 in the **Passphrase/Confirm Passphrase** fields.
- d) Click **Save** at the bottom of the window.
- **Step 10** Import the release 5.2(1) configuration that you backed up before you upgraded to release 25.0(1) and verify that the previous configurations converge.

Use the following settings when importing the release 5.2(1) configuration that you backed up:

- In the **Restore Type** field, choose **Merge**.
- In the Restore Mode field, choose Best Effort.

The home region CCR creation will automatically begin after this step.

- Step 11 If the site is managed by ACI Multi-Site Orchestrator/Nexus Dashboard Orchestrator, update the new Cloud APIC VM IP address.
  - a) Log into ACI Multi-Site Orchestrator/Nexus Dashboard.
  - b) Edit and reregister the site.
    - 1. In Nexus Dashboard, navigate to Sites and click on the correct site.
    - 2. Click the Details icon to bring up the Overview window.
    - 3. Click on the pencil icon to edit the information for this site.
    - Click the box next to Re-register Site and enter the necessary information to update with the new Cloud APIC VM IP address.
    - 5. Click Save.
  - c) Go into ACI Multi-Site Orchestrator/Nexus Dashboard Orchestrator and verify that the site is still managed.
    - 1. In Nexus Dashboard Orchestrator, navigate to Sites.
    - 2. Locate your site and verify that Managed is displayed in the State column.
  - d) Perform a cloud site refresh.
    - In Nexus Dashboard Orchestrator, navigate to Infrastructure > Infra Configuration, then click Configure Infra.
    - 2. Select the site in the left nav bar, then click **Refresh**.

Click **Yes** in the confirmation window to continue with the cloud site refresh.

e) Click **DEPLOY** > **Deploy Only** to deploy the infra configuration.

## Downgrading the Software: Release 25.0(2) to 25.0(1) or 5.2(1)

These procedures describe how to downgrade the software from release 25.0(2) to 25.0(1) or 5.2(1).

These procedures assume the following scenario:

- 1. At some point previously, you were running release 25.0(1) or 5.2(1) and you decided to upgrade to release 25.0(2). Before you performed that upgrade, however, you backed up your release 25.0(1) or 5.2(1) configuration and saved that backed-up configuration file, as described in Backing Up Your Existing Configuration, on page 6.
- 2. You then performed a policy-based upgrade to release 25.0(2) and, at some pointer later on, decided to revert back to release 25.0(1) or 5.2(1).

These procedures describe how to revert back to that previous release, but you will need that backed-up configuration file for that previous release in order for these downgrade procedures to work.

**Step 1** Verify that you have the backed-up configuration file from the previous release, as described in Backing Up Your Existing Configuration, on page 6.

Do not use these procedures to downgrade from release 25.0(2) if you do not have that backed-up configuration file from the previous release available. You will need that backup configuration file for these downgrade procedures.

**Step 2** Create a duplicate of the SSH key with the same contents (the same public or private key).

- a) Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
- b) In the navigation pane, choose Key Pairs.
- c) Choose Import key pair.

Key	pairs (1/3) Info		C	Actions 🔺	Create key pair
0	er key pairs			Import key pair	
-	inter ney puils			Delete	••••••
	Name	⊽ Туре	▽	Manage tags	▽
	capic_downgrade	rsa		e5:06:7b:0d:fd:f9:ff:	4a:53:ef:70:5a:42:
	capic_upgrade	rsa		d4:db:17:e2:ff:dc:f9:	ce:a0:da:12:39:13:
	cisco	rsa		f3:b0:47:b6:6e:42:55	5:45:ef:5b:39:9f:f4:

d) For **Name**, enter a descriptive name for the public key. The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

**Note** When you connect to your instance from the EC2 console, the console suggests this name for the name of your private key file.

- e) Either choose **Browse** to navigate to and select your public key, or paste the contents of your public key into the **Public key contents** field.
- f) Choose Import key pair.

g) Verify that the public key that you imported appears in the list of key pairs.

- **Note** If the **Import key pair** process doesn't work for any reason, you can create a new key pair using the **Create key pair** option, and use that in Step 7, on page 21, if necessary.
- **Step 3** Navigate to the EC2 instance area and terminate the Cloud APIC VM instance.

- a) In the navigation pane, choose Instances.
- b) Check the box next to the Cloud APIC VM instance.
- c) Right-click on the line for the Cloud APIC VM instance and choose Instance State > Terminate.

It will take a few minutes for the Cloud APIC VM instance to terminate.

aws Services •		Q. Search for services,	features, marketplace products, a	nd docs	[Option+S]		∳ adm	in/vernovva@cisco.cor	n @ 9210-0878-	1758	♥ N. California ♥ Supp	ort 🔻
New EC2 Experience ×	Launch Instance 💌	Connect Actions ~									• 4 e	• •
EC2 Dashboard	Q. Filter by tags and attrit	outes or search by keyword										> >i
Events	name	- Name	- Instance ID		- Instance Type -	Availability Zone -	Instance State +	Status Checks -	Alarm Status		Public DNS (IPv4) -	IPv4 Put
Tags	case_sanity_stack	Capic-1	Connect	164	m5.2xlarge	us-west-1a	🥥 running	Ø 2/2 checks	None	34	ec2-54-193-157-146.us	54,193.1
Limits	case_sanity_stack	Capio-1	Get Windows Paseword	ad.	m5.2xlarge	us-west-1a	terminated		None	2		-
♥ Instances	case_sanity_stack	Capic-1	Create Template From Instance Launch More Like This	-	m5.2xlarge	us-west-1a	🥥 terminated		None	2		*
Instances			Instance State		rt 👘							
Instance Types			Instance Settings	<ul> <li>Sto</li> </ul>	¢							
Launch Templates			Image Networking	• 010 • Ref	ip - Hibernale							
Spot Requests			CloudWatch Monitoring	. Ton	monte							
Savings Plans												
Reserved Instances												
Dedicated Hosts												
Capacity Reservations												

After you the Cloud APIC VM instance is terminated, the two interfaces associated with the VM will hang at this point. Once the new VM comes up as part of the upgrade, it will get reattached to the same interfaces.

Once the termination process is completed for the Cloud APIC VM, you will note that the VPCs and other network resources, such as the CIDRs and subnets, are still intact.

Services V				Q. Search	for services, fe	atures, marketp	iace products, a	nd docs	[Option+S]		4	admin/vemovval	Boisco.com @ 9210-06	878-1738 ¥	N, California 🔻	Support •
New VPC Experience		You	r VPCs (1/4) Info										C	Actions ¥	Create	VPC
VPC Dashboard		Q,	Filter VPCs												< 1 >	۲
EC2 Global View tow	4	•	Name		v VP	PC ID	v	State	⊽ IP	r4 CIDR	IPv6 CIDR		IPv6 pool			HCP optio
Q. Select a VPC			Default-VPC-MAIN		vpr	c-074162198b2	Odfc64	O Availabl	17	2.31.0.0/16	1.00		-			lopt-d9540
			capic-bastion-vpc		vp	c-09c4da8097cl	83dcf6	🕗 Availabi	10	10.5.0/24	-		-			lopt-d9540
VIRTUAL PRIVATE CLOUD			context-[overlay-1]	-addr-{10.10.1.0	)/25] vpc	c-0a1014922dc	e8c381	🕗 Availabi	10	10.1.0/25	-		-			lopt-d9540
Your VPCs			case-infra-vpc		vps	c-005358d8dd0	e6ece7	⊘ Availabi	17	2.35.0.0/16	-		-			lopt-d9540
Subnets																
Route Tables new																
Internet Gateways																
Egress Only Internet Gateways																
DHCP Options Sets																
Elastic IPs																
Services     Services     New VPC Experience     Tel us what you from		Sub	nets (5) info	Q. Searci	1 for services, h	eatures, marketp	olaca products, i	and docs	(Option+5)	J		Gr accurvemove	C	Actions ¥	N. California 🔻	Support
VPC Dashboard		Q	Filter submets												< 1	0
EC2 Global View www Filter by VPC:	4		Name	v Subne	et ID	v	State	<b>v</b> 1	/PC	4	IPv4 CIDR	v IP	v6 CIDR	v /	wailable IPv4	addresses
Q Select a VPC			-	subne	t-06d49aab057	711b32c	<ul> <li>Available</li> </ul>	1	pc-09c4da809	7c83dcf6   capi	10.10.5.0/25	-		1	23	
			-	subne	t-Of72babd29c	016:003	<ul> <li>Available</li> </ul>		pc-074162198	b20dfc64   Def	172.31.0.0/20	-		4	091	
CLOUD			-	subne	t-Oabcfd8b21f	1c1d83	⊘ Available		pc-074162198	b20dfc64   Def	172.31.16.0/20	-		4	091	
Your VPCs			subnet-[10.10.1.1	5 subne	t-056b9b57c90	05d0c32	<ul> <li>Available</li> </ul>		pc-0a1014922	dealle \$81 Loop	10.10.1.16/28	-		1	-	
			subset-[10.10.1.0.							occorso i l'contra					0	
Subnets			addiner Trot rot rod	subne	t-0a18a90c69e	ef58af7	O Available		pc-0a1014922	dce8c381   con	10.10.1.0/28	-		,	0	
Subnets Route Tables New			and the first sector	subne	t-0a18a90c69e	ef58af7	⊘ Available		pc-0a1014922	dce8c381   con	10.10.1.0/28			,	0	

**Step 4** When the termination process is completed for the Cloud APIC VM, go back to the stack and verify that it is still in the running state.

Navigate to the **CloudFormation** area and verify that the Cloud APIC stack is still in the running state.

**Step 5** Click the circle next to the Cloud APIC stack and click **Update**.

L

Stacks (1)				C	Delete Hodate Stack actions	· Create stack ·
stacks (1)					Dente Opuste State actions	· Create stack ·
Q, Filter by stack name			Active	*	View nested	<1>
Stack name	Status	Created time	Ŧ	Descripti	on	
O capic-1	CREATE_COMPLETE	2021-09-08 18:36	5:10 UTC-0700	This temp environm	plate creates the environment to launch a cloud API ent.	IC cluster in an AWS

The Update stack window appears.

#### Step 6 Click Use current template, then click Next.

Because you are not changing anything in the template, you will choose the **Use current template** option in this window.

Q Search for services, featur	res, marketplace products, and docs	[Option+S]	😞 admin/vemovva@cisco.com @
> Update stack			
Update stack			
Prerequisite - Prepare templat	te		
Prepare template Every stack is based on a template. A template	is a JSON or YAML file that contains configura	tion information about the AWS resour	rces you want to include in the stack.
O Use current template	<ul> <li>Replace current temp</li> </ul>	late O Edit	t template in designer
•			
•			Cancel Next
	Search for services, feature     Update stack  Update stack  Prerequisite - Prepare template Prepare template Decry stack is based on a template     Update stack  Use current template	Q. Search for services, features, marketplace products, and docs     Update stack     Update stack     Prerequisite - Prepare template     Prepare template     Cvery stack is based on a template. A template is a 350N or VAML, file that contains configure     O. Use current template     Replace current temp	Q. Search for services, features, marketplace products, and docs       [Option+S]         > Update stack       Update stack         Prerequisite - Prepare template       Prepare template         Every stack is based on a template. A template is a JSON or VAM, file that contains configuration information about the AWS resource         Q. Use current template       Replace current template         Edit       Replace current template

The Specify stack details window appears.

=

Step 7 In the Specify stack details window, leave all of the fields as-is, except for the SSH Key Pair field.

In the **SSH Key Pair** field, select the new SSH key file name that you configured in Step 2, on page 19.

**Step 8** Click **Next** at the bottom of the **Specify stack details** window, then navigate through the remaining windows in the **Update stack** windows, verifying that you see the new SSH key file name in the fields in those windows.

aws Services •	Q Search for services, features, marketplace products, and docs	[Option+S]	A admin/vemovva@
	pExtNw	0.0.0/0	
	pFabricName	Cloud-APIC	
	pInfraVPCPool	10.10.1.0/24	
	pinstanceType	m5.2xlarge	
	pKeyName	case-ssh-key-2	
	pPassword	Use existing value	
	Tags (1)		
	- A star of regio		
	Key 🔺	Value	Ψ.
	name	case_sanity_stack	
	Permissions		

**Step 9** Click on **Update stack** at the end of the process.

The update for the stack begins.

Services V	Q Search for services, featu	res, marketplace products, and docs [Op	tion+5]	43x admin/vemov	vağıcısco.com @ 9210-0878-1738 ♥ N. California ♥ Support ♥
${\bf CloudFormation} \qquad \times \qquad$	CloudFormation > Stacks > capic-1				
Stacks	🖸 Stacks (1)	Update Stack actions V Create stack V			
Drifts	Q. Filter by stack nome	Stack info Events Resource	s Outputs Parameter	s Template Change se	ts
StackSets Exports	Active • View nested < 1 >				
	capic-1	Events (82)			C
Designer	2021-09-08 18:36:10 UTC-0700 ⊘ UPCATE_COMPLETE	Q. Search events			0
		Timestamp 🖤	Logical ID	Status	Status reason
Registry     Public extensions		2021-09-08 19:03:38 UTC-0700	capic-1	O UPDATE_COMPLETE	
Activated extensions		2021-09-08 19:03:38 UTC-0700	rCAPICInstance	O DELETE_COMPLETE	
Publisher		2021-09-08 19:03:21 UTC-0700	rCAPICInstance	DELETE_IN_PROGRESS	
		2021-09-08 19:03:20 UTC-0700	capic-1	UPDATE_COMPLETE_CLE ANUP_IN_PROGRESS	
		2021-09-08 19:03:17 UTC-0700	rCAPICInstance	O UPDATE_COMPLETE	
Feedback		2021-09-08 19:03:09 UTC-0700	rCAPICInstance	UPDATE_IN_PROGRESS	Resource creation Initiated
		2021-09-08 19:03:07 UTC-0700	rCAPICInstance	UPDATE_IN_PROGRESS	Requested update requires the creation of a new physical resource; hence creating one.
		2021-09-08 19:02:59 UTC-0700	capic-1	UPDATE_IN_PROGRESS	User Initiated

**Step 10** Monitor the progress of the update for the stack.

The update for the stack will go through the following stages:

- AWS will first create a new Cloud APIC VM.
- As part of the stack update, it will try to delete the old Cloud APIC VM, which was already deleted manually.
- The Cisco Cloud APIC will be posted in the stack.
- **Step 11** Wait until you see the **UPDATE\_COMPLETE** message in the **Stacks** window, then navigate back to the **Instances** window.
  - The Cloud APIC instance will have the new instance ID and will be using the new SSH key.
  - The old interfaces will be reattached to the new instance, and the CIDRs and subnets will all remain the same.
  - The Cloud APIC management IP address will also be the same.
- **Step 12** After roughly 5-10 minutes, verify that the version is correct in the Cloud APIC.

Log into your Cloud APIC using the management IP address. You should see the version of release that was running previously, before you upgraded to release 25.0(2).

- **Step 13** Enable Global AES encryption using the same passphrase that you noted when you backed up your configuration in Backing Up Your Existing Configuration, on page 6.
  - a) In your Cisco Cloud APIC GUI, navigate to Infrastructure > System Configuration.

It should be underneath the General tab by default; if not, click the General tab.

b) Click the pencil icon at the upper right part of the Global AES Encryption area.

The Global AES Encryption Settings window appears.

- c) Click the box next to the **Encryption: Enabled** area, then enter the passphrase that you noted in Backing Up Your Existing Configuration, on page 6 in the **Passphrase/Confirm Passphrase** fields.
- d) Click Save at the bottom of the window.

**Step 14** Import the configuration for the previous release that you backed up before you upgraded to release 25.0(2) and verify that the previous configurations converge.

Use the following settings when importing the configuration for the previous release that you backed up:

- In the **Restore Type** field, choose **Merge**.
- In the Restore Mode field, choose Best Effort.

The home region CCR creation will automatically begin after this step.

- **Step 15** If the site is managed by ACI Multi-Site Orchestrator/Nexus Dashboard Orchestrator, update the new Cloud APIC VM IP address.
  - a) Log into ACI Multi-Site Orchestrator/Nexus Dashboard.
  - b) Edit and reregister the site.
    - 1. In Nexus Dashboard, navigate to Sites and click on the correct site.
    - 2. Click the Details icon to bring up the Overview window.
    - 3. Click on the pencil icon to edit the information for this site.
    - Click the box next to Re-register Site and enter the necessary information to update with the new Cloud APIC VM IP address.
    - 5. Click Save.
  - c) Go into ACI Multi-Site Orchestrator/Nexus Dashboard Orchestrator and verify that the site is still managed.
    - 1. In Nexus Dashboard Orchestrator, navigate to Sites.
    - 2. Locate your site and verify that Managed is displayed in the State column.
  - d) Perform a cloud site refresh.
    - 1. In Nexus Dashboard Orchestrator, navigate to Infrastructure > Infra Configuration, then click Configure Infra.
    - 2. Select the site in the left nav bar, then click **Refresh**.

Click Yes in the confirmation window to continue with the cloud site refresh.

e) Click **DEPLOY** > **Deploy Only** to deploy the infra configuration.

### Downgrading the Software: Release 25.0(3) to 25.0(2), 25.0(1), or 5.2(1)

These procedures describe how to downgrade the software from release 25.0(3) to 25.0(2), 25.0(1), or 5.2(1).

These procedures assume the following scenario:

At some point previously, you were running release 25.0(2), 25.0(1), or 5.2(1) and you decided to upgrade to release 25.0(3). Before you performed that upgrade, however, you backed up your release 25.0(2), 25.0(1), or 5.2(1) configuration and saved that backed-up configuration file, as described in Backing Up Your Existing Configuration, on page 6.

2. You then performed a policy-based upgrade to release 25.0(3) and, at some pointer later on, decided to revert back to release 25.0(2), 25.0(1), or 5.2(1).

These procedures describe how to revert back to that previous release, but you will need that backed-up configuration file for that previous release in order for these downgrade procedures to work.

**Step 1** Verify that you have the backed-up configuration file from the previous release, as described in Backing Up Your Existing Configuration, on page 6.

Do not use these procedures to downgrade from release 25.0(3) if you do not have that backed-up configuration file from the previous release available. You will need that backup configuration file for these downgrade procedures.

- **Step 2** Create a duplicate of the SSH key with the same contents (the same public or private key).
  - a) Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
  - b) In the navigation pane, choose **Key Pairs**.
  - c) Choose Import key pair.

Key	pairs (1/3) Info	Actions 🔺	Create key pair					
Q /	Filter kev pairs			Import key pair				
-	ter key pairs		Delete	• • • •				
	Name	⊽ Туре	▽	Manage tags	▽			
	capic_downgrade	rsa		e5:06:7b:0d:fd:f9:ff:4a:53:ef:70:5a:42:				
<b>~</b>	capic_upgrade	rsa		d4:db:17:e2:ff:dc:f9:ce:a0:da:12:39:13:				
	cisco	rsa	f3:b0:47:b6:6e:42:55:45:ef:5b:39:9f:f4					

- d) For **Name**, enter a descriptive name for the public key. The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.
  - **Note** When you connect to your instance from the EC2 console, the console suggests this name for the name of your private key file.
- e) Either choose **Browse** to navigate to and select your public key, or paste the contents of your public key into the **Public key contents** field.
- f) Choose Import key pair.
- g) Verify that the public key that you imported appears in the list of key pairs.
- **Note** If the **Import key pair** process doesn't work for any reason, you can create a new key pair using the **Create** key pair option, and use that in #unique\_67 unique\_67 Connect\_42 step\_it2\_mtz\_yrb, if necessary.
- **Step 3** Navigate to the EC2 instance area and terminate the Cloud APIC VM instance.
  - a) In the navigation pane, choose Instances.
  - b) Check the box next to the Cloud APIC VM instance.
  - c) Right-click on the line for the Cloud APIC VM instance and choose Instance State > Terminate.

It will take a few minutes for the Cloud APIC VM instance to terminate.

L

aws Services V			Q Sea	rch for services	, features, marketplace products, a	nd do	s (0	ption+S]		¢ ≉d	min/vernovva@cisco.com	@ 9210-0878	-1758 •	N. California 🔻	Supp	ort 🔻
New EC2 Experience ×	Lou	nch instance 👻	Connect	Actions ~										• 4	0	• •
EC2 Dashboard	Q	Filter by tags and attri	butes or search	h by keyword										0 1C < 1 to 3	of 3	> >i
Events		name	- Name		- Instance ID			Instance Type -	Availability Zone -	Instance State	Status Checks	Alarm Statu		Public DNS (IPv4)		IPv4 Put
Tags		case_sanity_stack	Capic-	1	Connect	<b>D</b> P		m5.2xlarge	us-west-1a	🥥 running	Ø 2/2 checks	None	14	ec2-54-193-157-146	us	54,193.1
Limits		case_sanity_stack	Capio-	1	Get Windows Paseword			m5.2xlarge	us-west-1a	terminated		None	2			-
♥ Instances		case_sanity_stack	Capio-		Create Template From Instance Launch More Like This	ľ		m5.2xlarge	us-west-1a	terminated		None	2			*
instances					Instance State											
Instance Types					Instance Settings		Stop									
Caunch remplates					Networking		Reboot	TERES								
Spot mequests					CloudWatch Monitoring		Terracete									
Savings Plans						-		_								
Reserved Instances																
Dedicated Hosts																
Capacity Reservations																

After you the Cloud APIC VM instance is terminated, the two interfaces associated with the VM will hang at this point. Once the new VM comes up as part of the upgrade, it will get reattached to the same interfaces.

Once the termination process is completed for the Cloud APIC VM, you will note that the VPCs and other network resources, such as the CIDRs and subnets, are still intact.

New VPC Experience		You	r VPCs (1/4) Info										C	Actions	Create	VPC
VPC Dashboard		Q,	Filter VPCs												< 1 >	۲
EC2 Global View	4	•	Name		v	VPC ID		State	v	IPv4 CIDR	IPv6 CIDR		IPv6 pool	ι		HCP optio
O Select a VPC			Default-VPC-MAI	4		vpc-0741621	98b20dfc64	@ Ava	lable	172.31.0.0/16	-		-		d	opt-d9540
G OBBLIERO			capic-bastion-vpc			vpc-09c4da8	097c83dcf6	@ Ava	lable	10.10.5.0/24	-		-		d	opt-d9540
VIRTUAL PRIVATE			context-[overlay-	]-addr-[10.1	0.1.0/25]	vpc-0a10149	22dce8c381	@ Ava	lable	10.10.1.0/25	-		-		d	opt-d9540
Your VPCs			case-infra-vpc			vpc-005358d	8dd0e6ece7	⊘ Ava	lable	172.35.0.0/16	-		-		d	opt-d9540
Subnets																
Route Tables new																
Internet Gateways																
Egress Only Internet Gateways																
DHCP Options Sets																
DHCP Options Sets Elastic IPs																
DHCP Options Sets Elastic IPs																
DHCP Options Sets Elastic IPs Services				ų s	earch for service	os, features, ma	rketplace prod	icts, and doc	s [Opt	on+5į	4	), adminivemov	vellicescs.com 61 9210	5-08/8-1758 ♥	N. Galfornia ¥	Support ¥
DHCP Options Sets Elastic IPs  Services  New VPC Experience  Very and the perience		Sub	nets (5) Info	u s	earch for service	os, features, me	rkelplace prod	ucts, and doc	s (Opt	on+5j		), adminivemov		Actions ¥	N. California V	Support ¥
DHCP Options Sets     Eastic IPs     Services     New VPC Experience     Ind as what you fink     VPC Dashbourd		Sub	nets (5) mfo	u s	earch for service	od, featlured, me	rkelplace prod	ucts, and doc	s [Opt	on+3)	4	), adminivemov	Halloteca.com & 1010	Actions V	N. California V Create su < 1	Support V
CHCP Options Sets Elastic IPs Services V New VPC Experience Init a stat you thin VPC Dashboard EC2 Global View Team		Sub	nets (5) sofo filter subnets Name	ų s	ourch for service	ee, Yeasturiee, me	vietnisse javod	ucts, and doc	s [Opt	on+b)	IPv4 CIDR	) administration		Actions ¥	N. California V Create su < 1 > Available IPv4 a	Buccourt •
DHCP Options Sets Bastic IPs Services V New VPC Experience New VPC Dashboard EC2 Global View www filter by VPC:	4	Sub	nets (5) unfo Filter subrats Name	<b>u</b> s	aarch for service ubnet ID	ot, festuret, me	v State	vota, and doo	s (Op) VPC	on-bj	IPv4 CIDR	а. 1 Р вазаливаном	C [	Actions ¥	N California V Create su < 1 > Available IPv4 a	buet ibnet
DHCP Options Sets Bastic IPs New VPC Experience New VPC Experience New VPC Dashbard EC2 Global View ver- Filter by VPC: Q. Select a VPC	4	Sub	nets (5) toto Filter subrets Name	v 5	ubnet ID ubnet-06d49aat	65. Yestures, m b05711b32c	⊽ State ⊘Ava	octs, and doc 97 Lable	vpc	on+5;  da8097c83dcf6   capiu ₽	1Pv4 CIDR 10.10.5.0/25		C [	Actions V	N. California V Creato su < 1 2 Available IPv4 a 123	Bupport V Ibnet
DHCP Options Sets Bastic IPs New VPC Experience New VPC Experience New VPC Dashboard EC2 Global View New PPC Dashboard EC2 Global View New Quert by VPC: Quert by VPC: Quert a VPC VIRTUAL PRIVATE	4	Sub	nets (5) into Alter subnets Name - -	₹ ₹ \$ \$	ubnet ID ubnet ID ubnet-06d49aat	55. Yestisres, 7m b05711b32c 129c0f6d03	⊽ State ⊘Ava ⊘Ava	roth, and doco P lable lable	vpc vpc-09c4 vpc-0741	21142] → da8097c83dcf6   capi 621985c20dfc64   Def	IPv4 CIDR 10.10.5.0/25 172.310.0/20	× 1	C [	Actions V	A California V Create su ( 1 ) Available IPv4 a 123 4091	Buscort • Ibnet ©
DHCP Options Sets Bastic IPs Control Set Denv VPC Experience Init a vite pis first VPC Dashboard EC2 Global View New C2 Global View New C3 Setect a VPC WITTUAL PRIVATE CLOUD	4	Sub	nets (5) info Filter subnets Name - - -	<b>U</b> 8 V 5 S	ubnet ID Jonet-O6d49aal Jonet-O6d49aal Jonet-O672babc	60, features, m 605711632c 529c0f6d03 521f1c1d83	✓ State ⊘ Ava ⊘ Ava ⊘ Ava ⊘ Ava ⊘ Ava	ve na more discr v lable lable	vpc vpc-0741 vpc-0741	011+52 ↓ daB097c83dcf6   capl 62198520df664   Def 62198520df64   Def	IP+4 CIDR 10.10.5.0/25 172.31.0.0/20 172.31.16.0/20	× 1	C C	Actions ¥	Ac California V Create su ( 1 ) Available IPv4 a 123 4091	Bupport V Ibreet
HCP Options Sets Static IPs Very VPC Experience bit united pro-trees VPC Dashboard ECC Global Very New Tet by VPC: Q Select a VPC VINTUAL PRIVATE CLOUD Your VPCs	4	Sub (4) (3) (4) (4) (4) (4) (4) (4) (4) (4	riter subnets	♥ 5 9 9 16 5	ubnet ID ubnet -06d49aat ubnet-072babc ubnet-04d49abb	68. Seatures, me b05711b32c 529c0f6d03 521f1c1d83 7c9050c52	✓ State ⊘ Ava ⊘ Ava ⊘ Ava ⊘ Ava	able table	s (Cpt) VPC Vpc-09c4 Vpc-0741 Vpc-0741 Vpc-0310	9110) 448097(836df6   cpl 62198120dfc64   Def 62198120dfc64   Def 14822dce8c181   con	IP=4 CIDR 10.10.5.0/25 172.31.0.0/20 172.31.00/20 10.10.1.16/28	V 1	C [	Actions V	N. California V Create su < 1 2 Available IPv4 a 123 4091 10	Bupport + Ibreet ©
DHCP Options Sets Bastic IPs UNC Experience D New VPC Experience That are target with that are target with Select a VPC Q Select a VPC CLOUD Select a VPC Submats	•	Sub	rets (5) toto Filter submets - - - submet-[10,10,1,1 submet-[10,10,1,1	♥ 5 8 8 16 8	ubnet ID ubnet ID ubnet-06/49aal ubnet-0472babe ubnet-0472babe ubnet-04609b5	0. (000000 pro- b05711b32c 529c06603 521f1c1d83 7c905d0c32 c69ef58a77	♥ State Ø Ava	v Lable Lable Lable Lable Lable	vpc-09c4 vpc-09c4 vpc-0741 vpc-0741 vpc-0a10 vpc-0a10	0110 da8097(83ddf6   capl 62198/20df64   0ef 62198/20df64   0ef 14922dde8158   (om 14922dde81581   com	IPv4 CIDR 10.10.5.0/25 172.31.6.0/20 172.31.16.0/20 10.10.1.16/28	× 1	C [	Actions V	Nt customer 4 Create su < 1 2 Available IPv4 a 123 4091 10 10	Busport • binet © ddresses
DHCP Options Sets Exator IPs Diver VPG Experience bits and any test. VPC Dashboard EC2 Dickold View rew Filter by VPC: Q: Setect a VPC Q: Setect a VPC Stort VPG Is Solutions Route Tables see	4	Sub	Intes (5) Info Filter subnets Name - - subnet-[10.10.1,1]	♥ 5 9 9 9 6 9	ubnet ID ubnet ID ubnet-06649aal ubnet-072bb ubnet-0266965 ubnet-0366965 ubnet-0318a900	0.000000000000000000000000000000000000	♥ State ⊘Ava ⊘Ava ⊘Ava ⊘Ava ⊘Ava	v labie labie labie labie	VPC vpc-09c4 vpc-0741 vpc-0a10 vpc-0a10	20110 488007015466 [ cspl 621980204664 [ 0ef 6219802004664 [ 0ef 1492240e86381 [ con	BPv4 CID8 10.10.5.0/25 172.31.0.0/20 172.31.16.0/20 10.10.1.16/28 10.10.1.0/28	× 1	C (	Actions ¥	Available IPv4 a Available IPv4 a 123 4091 10	Busson

**Step 4** When the termination process is completed for the Cloud APIC VM, go back to the stack and verify that it is still in the running state.

Navigate to the **CloudFormation** area and verify that the Cloud APIC stack is still in the running state.

**Step 5** Click the circle next to the Cloud APIC stack and click **Update**.

Q. Filter by stack name     Active     View nested     < 1       Stack name     Status     Created time     View Description	. /
Q, Filter by stack name Active View nested	. /
Stacks (1) C Delete Update Stack actions V Creat	e stack

The Update stack window appears.

#### Step 6 Click Use current template, then click Next.

Because you are not changing anything in the template, you will choose the **Use current template** option in this window.

Coouronnation / stacks /	capic-1 / update stack			
Step 1 Specify template	Update stack			
Step 2 Specify stack details	Prerequisite - Prepare templa	te		
Step 3	Prepare template Every stack is based on a template. A template	is a JSON or YAML file that contains configuration information	about the AWS resources you want to include in the stack.	
Configure stack options	O Use current template	Replace current template	O Edit template in designer	
Step 4	•			

The Specify stack details window appears.

Step 7 In the Specify stack details window, leave all of the fields as-is, except for the SSH Key Pair field.

In the **SSH Key Pair** field, select the new SSH key file name that you configured in #unique\_67 unique\_67\_Connect\_ 42\_step\_ayv\_tsz\_yrb.

Step 8Click Next at the bottom of the Specify stack details window, then navigate through the remaining windows in the<br/>Update stack windows, verifying that you see the new SSH key file name in the fields in those windows.

aws	Services V	Q. Search for services, features, marketplace products, an	d docs. [Option+S]	👃 admin/vemovva@v
=		pExtNw	0.0.0.0/0	
		pFabricName	Cloud-APIC	
		pinfraVPCPool	10.10.1.0/24	
		pinstanceType	m5.2xlarge	
		pKeyName	case-ssh-key-2	
		pPassword	Use existing value	
		Tags (1)		Luc
		Tags (1)		
		Q Search tags		
		Key	Value	v •
		name	case_sanity_stack	
		Permissions		

**Step 9** Click on **Update stack** at the end of the process.

The update for the stack begins.

Services V	Q. Search for services, featu	res, marketplace products, and docs [Option+5]	ې admin/vemo	vvaĝicisco.com ĝi 9210-0878-1758 ♥ N. California ♥ Support ♥
${\rm CloudFormation}  \times $	CloudFormation > Stacks > capic-1			
Stacks Stack details Drifts	C Stacks (1) C .	Capic-1 Stack info Events Resources Output	Delete s Parameters Template Change :	Update Stack actions V Create stack V
StackSets Exports	Active View nested	Events (82)		a
Designer	Capic-1 2021-09-08 18:36:10 UTC-0700 ⊘ UPDATE_COMPLETE	Q. Search events		•
		Timestamp 🤟 Logical ID	Status	Status reason
Registry     Public extensions		2021-09-08 19:03:38 UTC-0700 capic-1	@ UPDATE_COMPLETE	
Activated extensions		2021-09-08 19:03:38 UTC-0700 rCAPICInsta		
Publisher		2021-09-08 19:03:21 UTC-0700 rCAPICInsta	NC O DELETE_IN_PROGRESS	
		2021-09-08 19:03:20 UTC-0700 capic-1	UPDATE_COMPLETE_CLE ANUP_IN_PROGRESS	×
CloudFormation ×  Stacks Stack details Drifts Stackdets Exports Designer  Registry Public extensions Activated extensions Publisher  Feedback		2021-09-08 19:03:17 UTC-0700 rCAPICInsta	CO UPDATE_COMPLETE	
		2021-09-08 19:03:09 UTC-0700 rCAPICInsta	Ce UPDATE_IN_PROGRESS	Resource creation Initiated
		2021-09-08 19:03:07 UTC-0700 rCAPICInstan	CO UPDATE_IN_PROGRESS	Requested update requires the creation of a new physical resource; hence creating one.
		2021-09-08 19:02:59 UTC-0700 capic-1	UPDATE_IN_PROGRESS	User Initiated

**Step 10** Monitor the progress of the update for the stack.

The update for the stack will go through the following stages:

- AWS will first create a new Cloud APIC VM.
- As part of the stack update, it will try to delete the old Cloud APIC VM, which was already deleted manually.
- The Cisco Cloud APIC will be posted in the stack.
- **Step 11** Wait until you see the **UPDATE\_COMPLETE** message in the **Stacks** window, then navigate back to the **Instances** window.
  - The Cloud APIC instance will have the new instance ID and will be using the new SSH key.
  - The old interfaces will be reattached to the new instance, and the CIDRs and subnets will all remain the same.
  - The Cloud APIC management IP address will also be the same.
- **Step 12** After roughly 5-10 minutes, verify that the version is correct in the Cloud APIC.

Log into your Cloud APIC using the management IP address. You should see the version of release that was running previously, before you upgraded to release 25.0(3).

**Step 13** Trigger a CCR downgrade to the older Cisco Cloud Services Router 1000v.

As part of the upgrade to 25.0(3), you also moved from the older Cisco Cloud Services Router 1000v to the newer Cisco Catalyst 8000V. Downgrading from 25.0(3) to an earlier release therefore requires downgrading the CCR back to the older Cisco Cloud Services Router 1000v.

When the downgrade is completed, the system will recognize that the CCRs are now incompatible with the Cisco Cloud APIC. You will see a message saying that the CCRs and the Cisco Cloud APIC are incompatible and that any new policies configured for the Cisco Cloud APIC will not be applied to the CCRs until you've downgraded the CCRs.

You can begin the process of triggering the CCR downgrade using either of the following methods. Note that while the menu option is shown as **Upgrade CCRs** in both methods, you are actually downgrading the CCRs in this situation by selecting this option.

- In the banner at the top of the screen when your first log into the Cisco Cloud APIC, click on the Upgrade CCRs link, or
- Through the CCRs area in the Firmware Management page by navigating to:

**Operations > Firmware Management** 

Click the CCRs tab, then choose Upgrade CCRs.

- **Step 14** Enable Global AES encryption using the same passphrase that you noted when you backed up your configuration in Backing Up Your Existing Configuration, on page 6.
  - a) In your Cisco Cloud APIC GUI, navigate to **Infrastructure** > **System Configuration**.

It should be underneath the General tab by default; if not, click the General tab.

b) Click the pencil icon at the upper right part of the Global AES Encryption area.

The Global AES Encryption Settings window appears.

- c) Click the box next to the **Encryption: Enabled** area, then enter the passphrase that you noted in Backing Up Your Existing Configuration, on page 6 in the **Passphrase/Confirm Passphrase** fields.
- d) Click Save at the bottom of the window.
- **Step 15** Import the configuration for the previous release that you backed up before you upgraded to release 25.0(3) and verify that the previous configurations converge.

Use the following settings when importing the configuration for the previous release that you backed up:

- In the Restore Type field, choose Merge.
- In the Restore Mode field, choose Best Effort.

The home region CCR creation will automatically begin after this step.

- **Step 16** If the site is managed by ACI Multi-Site Orchestrator/Nexus Dashboard Orchestrator, update the new Cloud APIC VM IP address.
  - a) Log into ACI Multi-Site Orchestrator/Nexus Dashboard.
  - b) Edit and reregister the site.
    - 1. In Nexus Dashboard, navigate to Sites and click on the correct site.
    - 2. Click the Details icon to bring up the Overview window.
    - 3. Click on the pencil icon to edit the information for this site.
    - 4. Click the box next to **Re-register Site** and enter the necessary information to update with the new Cloud APIC VM IP address.
    - 5. Click Save.
  - c) Go into ACI Multi-Site Orchestrator/Nexus Dashboard Orchestrator and verify that the site is still managed.
    - 1. In Nexus Dashboard Orchestrator, navigate to Sites.
    - 2. Locate your site and verify that Managed is displayed in the State column.
  - d) Perform a cloud site refresh.

- In Nexus Dashboard Orchestrator, navigate to Infrastructure > Infra Configuration, then click Configure Infra.
- 2. Select the site in the left nav bar, then click Refresh.

Click Yes in the confirmation window to continue with the cloud site refresh.

e) Click **DEPLOY** > **Deploy Only** to deploy the infra configuration.

## Performing a System Recovery

The procedures for performing a system recovery is identical to the procedures for performing a migration-based upgrade. Refer to the section Migration-Based Upgrade, on page 9 for those procedures.

## Triggering an Upgrade of the CCRs

The following topics provide information and procedures for triggering an upgrade of the CCRs.

### Triggering an Upgrade of the CCRs

Prior to Release 5.2(1), the CCRs are upgraded automatically whenever you trigger an upgrade for the Cisco Cloud APIC. Beginning with Release 5.2(1), you can trigger upgrades to the CCRs and monitor those CCR upgrades, independent from the Cisco Cloud APIC upgrades. This is useful to reduce traffic loss by allowing you to split up the upgrades for the management plane (Cisco Cloud APIC) and the data plane (CCRs).

Beginning with Release 5.2(1), this feature is enabled by default, where the default assumption is that you will be triggering the upgrades to the CCRs after you trigger an upgrade to the Cisco Cloud APIC. You cannot disable this feature once it's enabled.

When this feature is enabled, the proper upgrade sequence for the Cisco Cloud APIC and the CCRs is as follows.



- **Note** Following are upper-level steps to describe the overall process for triggering upgrades to the CCRs. For specific step-by-step instructions, see Triggering an Upgrade of the CCRs Using the Cisco Cloud APIC GUI, on page 30.
  - 1. Upgrade Cisco Cloud APIC using the instructions provided in this chapter.
  - 2. Wait for the Cisco Cloud APIC upgrade process to complete. When that upgrade is completed, the system will recognize that the CCRs are now incompatible with the Cisco Cloud APIC. You will then see a message saying that the CCRs and the Cisco Cloud APIC are incompatible and that any new policies configured for the Cisco Cloud APIC will not be applied to the CCRs until you've upgraded the CCRs.

	▲ CSR Router	s are incompatible with the current version of Cloud APIC and need to be updated to version 17.	3.2. Upgrade CSRs	
Ŧ		cisco Cloud APIC aws	◙๏๗ቢở๗	
Dashboard		Dashboard	Last Updated: a few seconds ago	0
Topology				

- 3. View and accept the terms and conditions for the CCRs on the AWS portal.
- 4. Trigger the CCR upgrade so that it is now at a compatible version as the Cisco Cloud APIC.

You can begin the process of triggering the CCR upgrade using either of these two methods:

- In the banner at the top of the screen, click on the Upgrade CCRs link, or
- Through the CCRs area in the Firmware Management page. Navigate to:

**Operations > Firmware Management** 

Click the CCRs tab, then choose Upgrade CCRs.

You can also trigger the CCR upgrade through the REST API. See Triggering an Upgrade of the CCRs Using the REST API, on page 31 for those instructions.

#### **Guidelines and Limitations**

- After you have upgraded the Cisco Cloud APIC, if you do not see the message saying that the CCRs and the Cisco Cloud APIC are incompatible, you might have to refresh the browser for that message to appear.
- Trigger an upgrade to the CCRs *after* you have upgraded the Cisco Cloud APIC. Do not trigger an upgrade to the CCRs before you have upgraded the Cisco Cloud APIC.
- Once you have triggered an upgrade to the CCRs, it cannot be stopped.
- If you see any errors after you trigger an upgrade to the CCRs, check and resolve those errors. The CCR upgrade will continue automatically once those CCR upgrade errors have been resolved.

### Triggering an Upgrade of the CCRs Using the Cisco Cloud APIC GUI

This section describes how to trigger an upgrade to the CCRs using the Cisco Cloud APIC GUI. For more information, see Triggering an Upgrade of the CCRs, on page 29.

**Step 1** Begin the process of triggering the CCR upgrade to a compatible CCR version.

You can begin the process of triggering the CCR upgrade using either of these two methods:

- In the banner at the top of the screen, click on the Upgrade CCRs link, or
- Through the CCRs area in the Firmware Management page. Navigate to:

#### **Operations > Firmware Management**

Click the CCRs tab, then choose Upgrade CCRs.

A warning appears after clicking **Upgrade CCRs**, stating that upgrading the CCRs will cause the CCRs to reboot, which may cause temporary disruption in traffic.

**Step 2** If this is a good time to upgrade the CCRs and have a temporary disruption in traffic, click **Confirm Upgrade** in the warning message.

The CCR software upgrade begins. A banner appears at the top of the screen, saying that the CCR upgrade is in process. Click **View CCR upgrade status** in the message to view the status of the CCR upgrade.

**Step 3** Fix any faults that might occur during the upgrade of the CCRs.

If a fault occurs during the upgrade, you can get more information on the fault by navigating to:

**Operations** > **Event Analytics** > **Faults** 

### Triggering an Upgrade of the CCRs Using the REST API

This section describes how to trigger an upgrade to the CCRs using the REST API. For more information, see Triggering an Upgrade of the CCRs, on page 29.

Set the value for the routerUpgrade field to "true" in the cloud template to trigger an upgrade to the CCRs through the REST API (routerUpgrade="true").

```
<polUni>
<fvTenant name="infra">
    <cloudtemplateInfraNetwork name="default" vrfName="overlay-1">
       <cloudtemplateProfile name="defaultxyz" routerUsername="SomeFirstName" routerPassword="SomePass"
 routerUpgrade="true">
        </cloudtemplateProfile>
        <cloudtemplateExtSubnetPool subnetpool="10.20.0.0/16"/>
        <cloudtemplateIntNetwork name="default">
            <cloudRegionName provider="aws" region="us-west-1"/>
            <cloudRegionName provider="aws" region="us-west-2"/>
        </cloudtemplateIntNetwork>
        <cloudtemplateExtNetwork name="default">
            <cloudRegionName provider="aws" region="us-west-2"/>
            <cloudtemplateVpnNetwork name="default">
                <cloudtemplateIpSecTunnel peeraddr="23.2.1.1/32" />
                <cloudtemplateIpSecTunnel peeraddr="23.0.1.1/32" />
                <cloudtemplateIpSecTunnel peeraddr="23.1.1.1/32" />
                <cloudtemplateOspf area="0.0.0.1"/>
            </cloudtemplateVpnNetwork>
           <cloudtemplateBqpEvpn peeraddr="34.1.1.1/32" asn="63000" siteId="123" password="abcd1234"
 />
        </cloudtemplateExtNetwork>
    </cloudtemplateInfraNetwork>
</fvTenant>
</polUni>
```