Revised: August 1, 2025

Cisco Catalyst Center Data Migration

Before you migrate

The topics in this section provide information you'll need to plan and prepare for the migration of data from your current Catalyst Center deployment to one with third-generation appliances.

Supported appliances

This table lists the Catalyst Center appliances that support data migration.

Machine profile	Machine profile alias	Cisco part number	Number of cores	End of sale date	Last day of support date
medium	medium	First-generation: • DN1-HW-APL • DN1-HW-APL-U (promotional)	44	2019-03-01	2025-03-31
		Second-generation: • **DN2-HW-APL** • **DN2-HW-APL-U (promotional)**		2024-03-30	2029-03-31
		Third-generation: • **DN3-HW-APL** • **DN3-HW-APL-U (promotional)**	32	—	—
t2_large	large	Second-generation: • DN2-HW-APL-L • DN2-HW-APL-L-U (promotional)	56	2024-03-30	2029-03-31
		Third-generation: • **DN3-HW-APL-L** • **DN3-HW-APL-L-U (promotional)**		—	—

Machine profile	Machine profile alias	Cisco part number	Number of cores	End of sale date	Last day of support date
t2_2xlarge	extra large	Second-generation: • DN2-HW-APL-XL • DN2-HW-APL-XL-U (promotional)	112	2024-03-30	2029-03-31
		Third-generation: • **DN3-HW-APL-XL** • **DN3-HW-APL-XL-U (promotional)**	80	—	—

Important

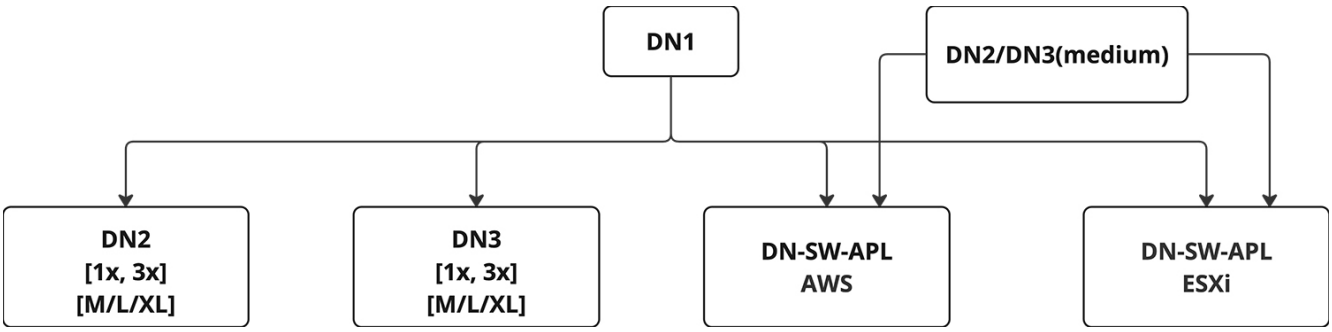
Catalyst Center 2.3.7.9 and later support mixed three-node clusters that have HA enabled. A valid mixed cluster meets these requirements:

- It consists of second- and third-generation Catalyst Center appliances. First-generation appliances are not supported.
- Its three appliances have the same machine profile. For example, a cluster with two second-generation large appliances and one third-generation large appliance is a valid mixed cluster.

Supported migration paths

These figures illustrate the supported Catalyst Center appliance migration paths.

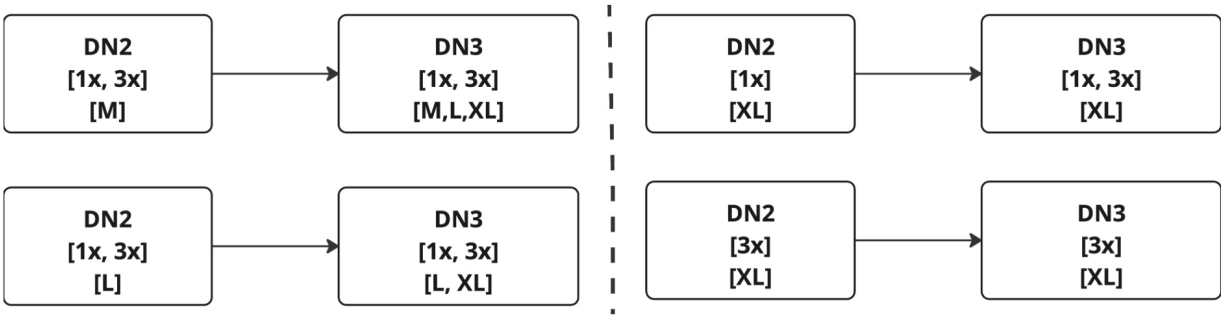
Figure 1: Appliance migration paths



Important

The AWS and ESXi virtual appliances do not support three-node clusters with HA enabled.

Figure 2: Second-generation to third-generation appliance migration paths



Feature rollout schedule

This table lists key Catalyst Center features.

Feature	Availability date	Corresponding Catalyst Center version
Disaster recovery support of mixed clusters	2024-04-08	2.3.7.5
First ship of the third-generation appliance	2024-04-19	2.3.7.5
Support of mixed three-node clusters that have HA enabled	2025-04-15	2.3.7.9

Prerequisites

Before you complete any of data migration procedures described in this document, back up your appliance's automation and Assurance data. For scenarios that require users to have the current and new clusters running at the same time during the migration process, we recommend that you provide a unique backup path for each cluster.

Important

NetFlow data is not backed up when you back up Catalyst Center automation and Assurance data.

Plan your migration

When planning your migration to a third-generation Catalyst Center appliance, ask yourself these questions:

- Will my new appliance use the same IP address as my current appliance?
- Will my appliance use a third-party certificate?
- Will disaster recovery be enabled in my deployment?
- Do I need to update my appliance's Cisco IMC firmware?
- Am I converting a single-node cluster to a three-node cluster, or vice versa?
- Am I moving from a smaller appliance to a larger one?

- Will this be an air-gapped deployment?

Prepare for migration

To prepare for migration, do the following:

1. Install your appliances, as described in the *Cisco Catalyst Center Third-Generation Installation Guide's* "Install the Appliance" chapter.
2. Have the following information available:
   - The network configuration for all Catalyst Center appliances.
   - If using a third-party certificate, the certificate and its private key.
   - If you are migrating a disaster recovery deployment, the disaster recovery configuration (including VIPs) and BGP configuration.

Reduce migration downtime

If you want to keep your current deployment of first- or second-generation Catalyst Center appliances running during the migration process, as well as minimize the amount of downtime, we recommend that you do the following:

1. Bring up and configure the third-generation appliances, using a different IP address scheme from the one that's used by your current appliances.
2. Ensure that the same packages and package versions that are installed on your current appliances are also installed on your third-generation appliances.
3. While your current appliances are still running, restore your deployment's backup file onto your third-generation appliances.
4. Perform a graceful shutdown of your current appliances.
5. Reconfigure the IP addresses on the third-generation appliances to match the IP address scheme used on your current appliances.

Important

If you plan to use the same IP address scheme on your third-generation Catalyst Center appliances that your current appliances use, you won't be able to bring up the third-generation appliances while your current appliances are running. As a result, the steps you'll need to complete are different:

1. Back up your current Catalyst Center deployment.
2. Shut down your current appliances before bringing up and configuring your third-generation appliances.
3. Ensure that the same packages and package versions that are installed on your current appliances are also installed on your third-generation appliances.
4. Restore your deployment's backup file onto your third-generation appliances.

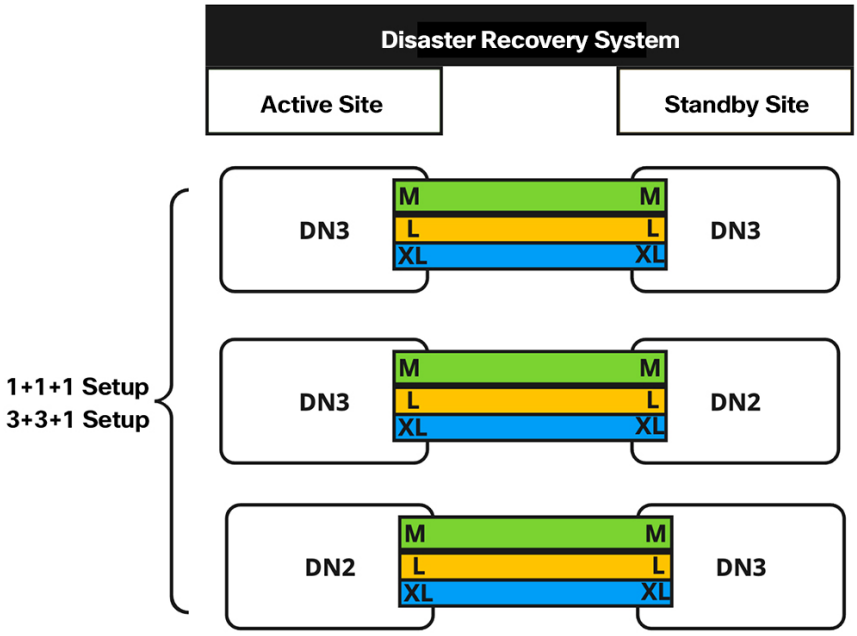
Conversion and appliance upgrade considerations

Keep the following points in mind when restoring a standalone node's backup file on a three-node cluster, or restoring a three-node cluster's backup file on a standalone node. These points also apply when upgrading to a higher-end Catalyst Center appliance:

- You can restore a backup file to an appliance with the same machine profile. For example, you can restore the backup file from a medium appliance to another medium appliance.
- You can restore a backup file from a lower-end appliance to a higher-end appliance. For example, you can restore the backup file from a medium appliance to a large or extra-large appliance.
- You *cannot* restore a backup file from a higher-end appliance to a lower-end appliance. So, the following scenarios are not supported:
  - Restoring a large appliance's backup file to a medium appliance.
  - Restoring an extra-large appliance's backup file to either a large or medium appliance.
- You can restore a standalone node's backup file to a three-node cluster or vice versa, provided that the target appliance has the same machine profile or is a higher-end appliance. The one exception is that you can't restore the backup file from a three-node cluster consisting of extra-large appliances to a standalone extra-large appliance.

Disaster recovery considerations

- Restore your appliance data and validate the Catalyst Center items indicated previously *before* setting up and activating disaster recovery (see the "Implement Disaster Recovery" chapter in the *Cisco Catalyst Center Administrator Guide*).
- Disaster recovery supports the use of second- and third-generation appliances together. The only requirement is that all of the devices at each disaster recovery site are of the same generation. For example, disaster recovery supports a configuration where your active site is made up of third-generation appliances, and your standby site consists of second-generation appliances. Disaster recovery does not support a configuration where one or both sites contain a mix of second- and third-generation appliances.
- The following figure summarizes the supported migration paths for Catalyst Center appliances in a deployment where disaster recovery is active.



Migration scenarios

Review and complete the migration scenario that applies to your deployment.

Scenario 1: Move a standalone Catalyst Center appliance between data centers (same IP addresses)

In this scenario, you are moving a Catalyst Center appliance from one data center to another one, keeping the same IP addresses that are already configured for the appliance's interfaces.

Step 1 (Optional) Upgrade to the latest Catalyst Center release. See the *Cisco Catalyst Center Upgrade Guide*.

Note If you upgrade, we recommend that you back up the data on your appliance. In the *Cisco Catalyst Center Administrator Guide*, see the "Back Up Data Now" topic.

Step 2 Open an SSH console to the appliance and run the **shutdown -h now** command to perform a graceful shutdown.

Step 3 After the appliance is powered off, move it to the new data center.

Step 4 Power on the appliance.

Step 5 Ensure that connectivity is established between Catalyst Center and the devices it manages.

Note For deployments running non-Cisco ISE AAA servers, use the System Health tool to confirm that Catalyst Center can reach these servers and connectivity is established.

Scenario 2: Move a standalone Catalyst Center appliance between data centers (different IP addresses)

In this scenario, you are moving a Catalyst Center appliance from one data center to another one, using different IP addresses than the ones that are currently configured for the appliance's interfaces.

Step 1 (Optional) Upgrade to the latest Catalyst Center release. See the *Cisco Catalyst Center Upgrade Guide*.

Note If you upgrade, we recommend that you back up the data on your appliance. In the *Cisco Catalyst Center Administrator Guide*, see the "Back Up Data Now" topic.

Step 2 Open an SSH console to the appliance and run the **shutdown -h now** command to perform a graceful shutdown.

Step 3 After the appliance is powered off, move it to the new data center.

Step 4 Power on the appliance, then use the Configuration wizard to specify the:

- IP addresses that you want to assign to the appliance's Enterprise, Management, and Internet interfaces.
- Virtual IP addresses that you want to assign to the Enterprise and Management interfaces.

In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Reconfigure the Appliance Using the Configuration Wizard" topic.

Note: If you want to change the appliance's intracluster IP address, you must first reimage the appliance, installing the Catalyst Center release that was present when the latest backup file was created. In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Reimage the Appliance" topic.

Step 5 After you complete the Configuration wizard, log in to the Catalyst Center GUI.

Step 6 Reestablish the pxGrid connection between Catalyst Center and Cisco ISE (which was severed when you updated the Enterprise interface's IP and virtual IP addresses in the previous step). In the *Cisco Catalyst Center Administrator Guide*, see the "Configure Authentication and Policy Servers" topic.

Note: For deployments running non-Cisco ISE AAA servers, use the System Health tool to confirm that Catalyst Center can reach these servers and connectivity is established.

Step 7 If you plan to change the Enterprise interface's virtual IP address, update the telemetry settings for your network's devices. Complete the steps described in the *Cisco Catalyst Center User Guide's* "Update telemetry settings to use a new cluster virtual IP address" topic.

Note: Because you are using the same appliance (with its data intact), you don't need to restore its latest backup file.

Scenario 3: Move a standalone Catalyst Center appliance between data centers (different IP addresses, same FQDN)

In this scenario, you are moving a standalone Catalyst Center appliance from one data center to another one. The appliance will use different IP addresses than the ones that are currently configured for its interfaces. It will also continue to use its current FQDN.

Step 1 Upgrade to the latest Catalyst Center release. See the *Cisco Catalyst Center Upgrade Guide*.

Note: We recommend that you back up the data on your appliance. In the *Cisco Catalyst Center Administrator Guide*, see the "Back Up Data Now" topic.

Step 2 Power off the appliance, then move it to the new data center.

Step 3 Power on the appliance, then use the Configuration wizard to specify the:

- IP addresses that you want to assign to the appliance's Enterprise, Management, and Internet interfaces.
- Virtual IP addresses that you want to assign to the Enterprise and Management interfaces.

In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Reconfigure the Appliance Using the Configuration Wizard" topic.

Note: If you want to change the appliance's intracluster IP address, you must first reimage the appliance, installing the Catalyst Center release that was present when the latest backup file was created. In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Reimage the Appliance" topic.

Step 4 You'll use the same hostname and domain name for the appliance, but you must update your DNS server with the IP address that's used for lookup entries.

Step 5 After you complete the Configuration wizard, log in to the Catalyst Center GUI.

Step 6 Reestablish the pxGrid connection between Catalyst Center and Cisco ISE (which was severed when you updated the Enterprise interface's IP and virtual IP addresses in the previous step). In the *Cisco Catalyst Center Administrator Guide*, see the "Configure Authentication and Policy Servers" topic.

Note For deployments running non-Cisco ISE AAA servers, use the System Health tool to confirm that Catalyst Center can reach these servers and connectivity is established.

Step 7 If you plan to change the Enterprise interface's virtual IP address, update the telemetry settings for your network's devices. Complete the steps described in the *Cisco Catalyst Center User Guide's* "Update telemetry settings to use a new cluster virtual IP address" topic.

Note

- Because you are using the same appliance (with its data intact), you don't need to restore its latest backup file.
- Because the FQDN is unchanged, PnP and other use cases that use FQDN should work without any issues.

Scenario 4: Replace a standalone Catalyst Center appliance with an appliance with more cores (same IP addresses)

In this scenario, you are replacing a standalone Catalyst Center appliance with another appliance that has more cores (for example, replacing a second-generation 56-core appliance with a second-generation 112-core appliance). The new appliance will use the same IP addresses that were configured for the previous appliance's interfaces.

Step 1 Upgrade to the latest Catalyst Center release. See the *Cisco Catalyst Center Upgrade Guide*.

Step 2 Back up the data on your appliance. In the *Cisco Catalyst Center Administrator Guide*, see the "Back Up Data Now" topic.

Step 3 Decommission the appliance that you are replacing.

Step 4 Set up the new appliance at your data center, ensuring that you install the same Catalyst Center release that was installed on the previous appliance. Also, make sure that you set the same IP address that was configured previously for the Enterprise interface. In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Configure the Primary Node Using the Maglev Wizard" topic.

Step 5 Restore the backup file that was created on the previous appliance. In the *Cisco Catalyst Center Administrator Guide*, see the "Restore Data from Backups" topic.

Step 6 Reestablish connectivity with Cisco ISE. In the *Cisco Catalyst Center Administrator Guide*, see the "Configure Authentication and Policy Servers" topic.

Note For deployments running non-Cisco ISE AAA servers, use the System Health tool to confirm that Catalyst Center can reach these servers and connectivity is established.

Step 7 If self-signed certificates were in place on your network's devices, reprovision them in order to update their Catalyst Center certificates. In the *Cisco Catalyst Center User Guide*, see the "Update Device Configuration Using Telemetry" topic.

Note If CA certificates signed by a third party are installed on your network's devices, you can skip this step.

Scenario 5: Replace a standalone Catalyst Center appliance with an appliance with more cores (different IP addresses)

In this scenario, you are replacing a standalone Catalyst Center appliance with another appliance that has more cores (for example, replacing a second-generation 56-core appliance with a second-generation 112-core appliance). The new appliance's interfaces will use different IP addresses than the ones that were used on the appliance that's being replaced.

Step 1 (Optional) Upgrade to the latest Catalyst Center release. See the *Cisco Catalyst Center Upgrade Guide*.

Note If you upgrade, we recommend that you back up the data on your appliance. In the *Cisco Catalyst Center Administrator Guide*, see the "Back Up Data Now" topic.

Step 2 Decommission the appliance that you are replacing.

Step 3 Set up the new appliance at your data center, ensuring that you install the same Catalyst Center release that was installed on the previous appliance. Use the Maglev wizard to specify new:

- IP addresses for the appliance's interfaces.
- Virtual IP addresses for the Enterprise and Management interfaces.

In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Configure the Primary Node Using the Maglev Wizard" topic.

Step 4 When the new appliance is up and running, restore the backup file that was created on the previous appliance. In the *Cisco Catalyst Center Administrator Guide*, see the "Restore Data from Backups" topic.

Step 5 In the *Cisco Catalyst Center Security Best Practices Guide*, complete the steps described in the "Update the Catalyst Center Server Certificate" topic.

Important Update the server certificate *after* you restore the backup file. If you update the certificate beforehand, the new certificate will be overwritten by the certificate that's currently in place.

Step 6 Reestablish the pxGrid connection between Catalyst Center and Cisco ISE (which was severed when you updated the Enterprise interface's IP and virtual IP addresses). In the *Cisco Catalyst Center Administrator Guide*, see the "Configure Authentication and Policy Servers" topic.

Note For deployments running non-Cisco ISE AAA servers, use the System Health tool to confirm that Catalyst Center can reach these servers and connectivity is established.

Step 7 If you plan to change the Enterprise interface's virtual IP address, update the telemetry settings for your network's devices. Complete the steps described in the *Cisco Catalyst Center User Guide's* "Update telemetry settings to use a new cluster virtual IP address" topic.

Scenario 6: Replace a standalone Catalyst Center appliance with an appliance with more cores (different FQDN)

In this scenario, you are replacing a standalone Catalyst Center appliance with another appliance that has more cores (for example, replacing a second-generation 56-core appliance with a second-generation 112-core appliance). The new appliance will use an FQDN that's different from the one used by the appliance that's being replaced.

Step 1 (Optional) Upgrade to the latest Catalyst Center release. See the *Cisco Catalyst Center Upgrade Guide*.

Note If you upgrade, we recommend that you back up the data on your appliance. In the *Cisco Catalyst Center Administrator Guide*, see the "Back Up Data Now" topic.

Step 2 Decommission the appliance that you are replacing.

Step 3 Set up the new appliance at your data center, ensuring that you:

- Install the same Catalyst Center release that was installed on the previous appliance.
- Use the same IP address that was assigned to the previous appliance's Enterprise interface.

Step 4 When the new appliance is up and running, restore the backup file that was created on the previous appliance. In the *Cisco Catalyst Center Administrator Guide*, see the "Restore Data from Backups" topic.

Step 5 Reestablish connectivity with Cisco ISE. In the *Cisco Catalyst Center Administrator Guide*, see the "Configure Authentication and Policy Servers" topic.

Note For deployments running non-Cisco ISE AAA servers, use the System Health tool to confirm that Catalyst Center can reach these servers and connectivity is established.

Step 6 If self-signed certificates were in place on your network's devices, reprovision them in order to update their Catalyst Center certificates. In the *Cisco Catalyst Center User Guide*, see the "Update Device Configuration Using Telemetry" topic.

Note If CA certificates signed by a third party are installed on your network's devices, you can skip this step.

Scenario 7: Move a three-node Catalyst Center cluster between data centers (same IP addresses)

In this scenario, you are moving a three-node Catalyst Center cluster from one data center to another one (using the same interface IP addresses).

Step 1 (Optional) Upgrade to the latest Catalyst Center release. See the *Cisco Catalyst Center Upgrade Guide*.

Note If you upgrade, we recommend that you back up the data on your appliance. In the *Cisco Catalyst Center Administrator Guide*, see the "Back Up Data Now" topic.

Step 2 From an SSH console, power off the three appliances by running the **sudo shutdown -h now** command on all of the appliances at the same time.

Step 3 Move the appliances to the new data center, then power them on.

Step 4 Ensure that connectivity is established between Catalyst Center and the devices it manages.

Scenario 8: Move a three-node Catalyst Center cluster between data centers (different IP addresses)

In this scenario, you are moving a three-node Catalyst Center cluster from one data center to another one, using different IP addresses than the ones that are currently configured for the appliance interfaces.

Step 1 (Optional) Upgrade to the latest Catalyst Center release. See the *Cisco Catalyst Center Upgrade Guide*.

Note If you upgrade, we recommend that you back up the data on your appliance. In the *Cisco Catalyst Center Administrator Guide*, see the "Back Up Data Now" topic.

Step 2 Power off the appliances, then move them to the new data center.

Step 3 Power on the appliances, then use the Configuration wizard to specify the:

- IP addresses you want to assign to the appliances' Enterprise, Management, and Internet interfaces.
- Virtual IP addresses you want to assign to the Enterprise and Management interfaces.

In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Reconfigure the Appliance Using the Configuration Wizard" topic.

Note If you want to change an appliance's intracluster IP address, you must first reimage the appliance, installing the Catalyst Center release that was present when the latest backup file was created. In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Reimage the Appliance" topic.

Step 4 Restore the backup file that you created after upgrading the appliances. In the *Cisco Catalyst Center Administrator Guide*, see the "Restore Data from Backups" topic.

Step 5 Reestablish the pxGrid connection between Catalyst Center and Cisco ISE (which was severed when you updated the Enterprise interface's IP and virtual IP addresses). In the *Cisco Catalyst Center Administrator Guide*, see the "Configure Authentication and Policy Servers" topic.

Note For deployments running non-Cisco ISE AAA servers, use the System Health tool to confirm that Catalyst Center can reach these servers and connectivity is established.

Step 6 If you plan to change the Enterprise interface's virtual IP address, update the telemetry settings for your network's devices. Complete the steps described in the *Cisco Catalyst Center User Guide's* "Update telemetry settings to use a new cluster virtual IP address" topic.

Scenario 9: Change a standalone Catalyst Center appliance to a three-node HA cluster

In this scenario, you are changing a standalone Catalyst Center appliance to a three-node high availability (HA) cluster by adding two additional nodes.

Step 1 Use the Configuration wizard to specify the following:

- The IP addresses that you want to assign to the appliance's Enterprise, Management, and Internet interfaces.
- The virtual IP addresses that you want to assign to the Enterprise and Management interfaces.

In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Reconfigure the Appliance Using the Configuration Wizard" topic.

Note If you want to change the appliance's intracluster IP address, you must first reimage the appliance, installing the Catalyst Center release that was present when the latest backup file was created. In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Reimage the Appliance" topic.

Step 2 Reestablish the pxGrid connection between Catalyst Center and Cisco ISE. In the *Cisco Catalyst Center Administrator Guide*, see the "Configure Authentication and Policy Servers" topic.

Step 3 Upgrade the appliance to the latest Catalyst Center release. See the *Cisco Catalyst Center Upgrade Guide*.

Step 4 Back up the data on your appliance. In the *Cisco Catalyst Center Administrator Guide*, see the "Back Up Data Now" topic.

Step 5 Before you complete Steps 5 and 6, confirm that the appliances you're adding to the cluster have the same number of cores as the primary node.

Note With regard to 44-core appliances, your cluster can consist of both the first-generation 44-core appliance (Cisco part number DN1-HW-APL) and the second-generation 44-core appliance (Cisco part numbers DN2-HW-APL and DN2-HW-APL-U).

Step 6 Configure your cluster's second appliance. In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Configure a Secondary Node Using the Maglev Wizard" topic.

Step 7 Configure your cluster's third appliance. In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Configure a Secondary Node Using the Maglev Wizard" topic.

Step 8 Confirm that the three cluster nodes have the same Catalyst Center release installed.

Step 9 Activate HA to initiate the redistribution of services.

a) From the main menu, choose **System** > **Settings** > **System Configuration** > **High Availability**.

b) Click **Activate High Availability**.

Scenario 10: Change a three-node HA cluster to 1+1+1 disaster recovery

In this scenario, you are changing a three-node Catalyst Center cluster with HA enabled to a cluster with a 1+1+1 disaster recovery setup.

Step 1 Upgrade the cluster to the latest Catalyst Center release. See the *Cisco Catalyst Center Upgrade Guide*.

Step 2 Back up the cluster's data. In the *Cisco Catalyst Center Administrator Guide*, see the "Back Up Data Now" topic.

Step 3 At the data center where your disaster recovery system's main site will reside, set up the appliance that will serve as the main site. You can either use one node from the current HA cluster for this purpose or set up a new appliance.

Note If you want to continue using the same IP scheme you're using now, set up the appliance in an isolated network to avoid IP overlap with the existing cluster.

a) If you are using an appliance from the HA cluster, reimage it. In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Reimage the Appliance" topic.

Note If you setting up a new appliance, skip this step and start with Step 3b.

b) Install the same Catalyst Center release that was installed in Step 1.

c) Restore the backup file you created in Step 2. In the *Cisco Catalyst Center Administrator Guide*, see the "Restore Data from Backups" topic.

Step 4 Power off the HA cluster's second and third nodes (as the first node has already been removed).

Step 5 Remove network isolation on the newly formed standalone node cluster.

Step 6 At the data center where the recovery site will reside, set up the appliance that will serve as the recovery site (either a new appliance or one of the HA cluster's appliances).

As you complete this step, ensure the following:

- The Catalyst Center release installed on this appliance is the same as the release installed on the main site appliance.

- The main site and recovery site appliances have the same number of cores.

Note With regard to 44-core appliances, your cluster can consist of both the first-generation 44-core appliance (Cisco part number DN1-HW-APL) and the second-generation 44-core appliance (Cisco part numbers DN2-HW-APL and DN2-HW-APL-U).

Step 7 Set up your witness site in a different location than your main and recovery sites and confirm that it's reachable from both of these sites. In the *Cisco Catalyst Center Administrator Guide*, see the "Install the Witness Site" topic.

Step 8 Generate one third-party certificate and install this certificate on both the main and recovery sites. Otherwise, site registration will fail. In the *Cisco Catalyst Center Security Best Practices Guide*, see the "Generate a Certificate Request Using Open SSL" topic.

Step 9 In the *Cisco Catalyst Center Administrator Guide*, confirm that the prerequisites in "Implement Disaster Recovery" have been met before you enable disaster recovery.

Step 10 Configure your disaster recovery system. In the *Cisco Catalyst Center Administrator Guide*, see the "Configure Disaster Recovery" topic.

Scenario 11: Change a three-node HA cluster to 3+3+1 disaster recovery

In this scenario, you are changing a three-node Catalyst Center cluster with HA enabled to a cluster with a 3+3+1 disaster recovery setup.

Step 1 Upgrade the appliances to the latest Catalyst Center release. See the *Cisco Catalyst Center Upgrade Guide*.

Step 2 Back up the cluster's data. In the *Cisco Catalyst Center Administrator Guide*, see the "Back Up Data Now" topic.

Step 3 Set up a three-node HA cluster as your disaster recovery system's recovery site at the data center where it will reside:

a) Configure the recovery site's primary node. In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Configure the Primary Node Using the Maglev Wizard" topic.

b) Configure the recovery site's two secondary nodes. In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Configure a Secondary Node Using the Maglev Wizard" topic.

c) Activate HA:

1. From the main menu, choose **System** > **Settings** > **System Configuration** > **High Availability**.
2. Click **Activate High Availability**.

d) Ensure that the same Catalyst Center release is installed on the appliances at your disaster recovery system's main and recovery site. Also make sure that the appliances at both sites have the same number of cores.

For a detailed description of all the prerequisites that need to be met, see the *Cisco Catalyst Center Administrator Guide*.

Step 4 Set up your witness site in a different location than your main and recovery sites and confirm that it's reachable from both of these sites. In the *Cisco Catalyst Center Administrator Guide*, see the "Install the Witness Site" topic.

Step 5 Generate one third-party certificate and install this certificate on both the main and recovery sites. Otherwise, site registration will fail. In the *Cisco Catalyst Center Security Best Practices Guide*, see the "Generate a Certificate Request Using Open SSL" topic.

Step 6 Configure your disaster recovery system. In the *Cisco Catalyst Center Administrator Guide*, see the "Configure Disaster Recovery" topic.

Scenario 12: Change 1+1+1 disaster recovery to a three-node HA cluster

In this scenario, you are changing a Catalyst Center cluster with a 1+1+1 disaster recovery setup to a three-node HA cluster.

Step 1 Pause your disaster recovery system (resulting in two standalone appliances). In the *Cisco Catalyst Center Administrator Guide*, see the "Place Your System on Pause" topic.

Step 2 Deregister the system. In the *Cisco Catalyst Center Administrator Guide*, see the "Deregister Your System" topic.

Step 3 Upgrade the first appliance to the latest Catalyst Center release. See the *Cisco Catalyst Center Upgrade Guide*.

Step 4 Back up the first appliance's data. In the *Cisco Catalyst Center Administrator Guide*, see the "Back Up Data Now" topic.

Step 5 Configure the second appliance as the second node in the three-node HA cluster. In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Configure a Secondary Node Using the Maglev Wizard" topic.

Step 6 Confirm that the second appliance has the same Catalyst Center release that's already installed on the first appliance. Also confirm that it has the same number of cores.

Note With regard to 44-core appliances, your cluster can consist of both the first-generation 44-core appliance (Cisco part number DN1-HW-APL) and the second-generation 44-core appliance (Cisco part numbers DN2-HW-APL and DN2-HW-APL-U).

Step 7 Add a third appliance to the three-node HA cluster. Ensure that it has the same Catalyst Center release that's installed on the other two appliances, as well as the same number of cores. In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Configure a Secondary Node Using the Maglev Wizard" topic.

Step 8 Activate HA to initiate the redistribution of services:

a) From the main menu, choose **System** > **Settings** > **System Configuration** > **High Availability**.

b) Click **Activate High Availability**.

Scenario 13: Change from 1+1+1 to 3+3+1 disaster recovery

In this scenario, you are changing a 1+1+1 disaster recovery setup to a 3+3+1 setup.

Step 1 At the data center where your main site will reside, do the following:

a) Pause your disaster recovery system (resulting in two standalone appliances). In the *Cisco Catalyst Center Administrator Guide*, see the "Place Your System on Pause" topic.

b) Deregister your system's sites in order to delete all of the settings that were previously configured for them. In the *Cisco Catalyst Center Administrator Guide*, see the "Deregister Your System" topic.

c) Upgrade both appliances to the latest Catalyst Center release. See the *Cisco Catalyst Center Upgrade Guide*.

d) Back up the first appliance's data. In the *Cisco Catalyst Center Administrator Guide*, see the "Back Up Data Now" topic.

e) Add the second appliance, which will act as the second node in a three-node HA cluster. In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Configure a Secondary Node Using the Maglev Wizard" topic.

f) Add a third appliance, which will act as the third node in a three-node HA cluster. In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Configure a Secondary Node Using the Maglev Wizard" topic.

g) Ensure that all three appliances have the same Catalyst Center release installed and have the same number of cores.

Note With regard to 44-core appliances, your cluster can consist of both the first-generation 44-core appliance (Cisco part number DN1-HW-APL) and the second-generation 44-core appliance (Cisco part numbers DN2-HW-APL and DN2-HW-APL-U).

Step 2 At the data center where your recovery site will reside, do the following:

a) Confirm that the appliances you'll add to the recovery site cluster have the same Catalyst Center release that's already installed on the main site's appliances. Also confirm that they have the same number of cores.

b) Configure the appliance that will serve as the primary node. In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Configure the Primary Node Using the Maglev Wizard" topic.

c) Configure the recovery site's second and third appliance. In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Configure a Secondary Node Using the Maglev Wizard" topic.

Step 3 Activate HA to initiate the redistribution of services:

a) From the main menu, choose **System** > **Settings** > **System Configuration** > **High Availability**.

b) Click **Activate High Availability**.

You'll need to complete these steps on both the main and recovery site clusters.

Step 4 Set up your witness site in a different location than your main and recovery sites and confirm that it's reachable from both of these sites. In the *Cisco Catalyst Center Administrator Guide*, see the "Install the Witness Site" topic.

Step 5 Generate one third-party certificate and install this certificate on both the main and recovery sites. Otherwise, site registration will fail. In the *Cisco Catalyst Center Security Best Practices Guide*, see the "Generate a Certificate Request Using Open SSL" topic.

Step 6 In the *Cisco Catalyst Center Administrator Guide*, confirm that the prerequisites in "Implement Disaster Recovery" have been met before you enable disaster recovery.

Step 7 Reconfigure your disaster recovery system. In the *Cisco Catalyst Center Administrator Guide*, see the "Configure Disaster Recovery" topic.

Scenario 14: Migrate data from a first-generation Catalyst Center appliance

In this scenario, you are migrating data from a first-generation Catalyst Center appliance to either an individual Catalyst Center second-generation appliance or a three-node cluster of second-generation appliances.

Before you begin, have the following information available:

- The IP addresses that are configured for the interfaces on your first-generation appliance. This is applicable only if you plan to configure the same addresses on your second-generation appliance.
- A list of the Catalyst Center packages that are installed on your first-generation appliance and their release number. To obtain this information, log in to the appliance and run the **maglev package status** command. Alternatively, in the top-right corner of the Catalyst Center GUI, click the **Help** icon and choose **About** > **Packages**.
- The configuration information for your backup server.

Step 1 On your first- or second-generation appliance, do the following:

a) Back up the appliance’s Automation and Assurance data.

In the *Cisco Catalyst Center Administrator Guide*, see the "Back Up Data Now" topic.

b) Disconnect the appliance from your network.

Step 2 On your third-generation appliance, do the following:

a) Configure the IP addresses that you want to use for your appliance’s interfaces.

You can use the same IP addresses that are configured on your first-generation appliance or specify different IP addresses.

In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the topic that is specific to the configuration wizard you want to use and your appliance type:

- If you are configuring a third-generation appliance using the Maglev Configuration wizard, see the "Configure the Primary Node Using the Maglev Wizard" topic.
- If you are configuring a 32- or 56-core third-generation appliance using the browser-based configuration wizard, see the "Configure the Primary Node Using the Advanced Install Configuration Wizard" topic in the "Configure the 32- and 56-Core Appliances Using the Browser-Based Wizard" chapter.
- If you are configuring an 80-core second-generation appliance using the browser-based configuration wizard, see the "Configure the Primary Node Using the Advanced Install Configuration Wizard" topic in the "Configure the 80-Core Appliance Using the Browser-Based Wizard" chapter.

Note When reconfiguring your access switches to match the high-throughput settings on your Catalyst Center appliances, be aware of the following differences between first-generation and second/third-generation appliances:

- Unlike first-generation appliances, where the configured VLAN must be set up on a switch port and match what is configured on the appliance's Cisco UCS Virtual Interface Card (VIC) 1227, second- and third-generation appliances only support native VLANs.
- First-generation appliances only support the **trunk** switchport mode, while second-generation appliances only support the **access** switchport mode.

b) Install the same releases of the Catalyst Center packages that are installed on your first-generation appliance.

In the *Cisco Catalyst Center Administrator Guide*, see the "Download and Install Packages and Updates" topic.

c) Restore the data that you backed up in Step 1.

In the *Cisco Catalyst Center Administrator Guide*, see the "Restore Data from Backups" topic.

d) Integrate Cisco ISE with Catalyst Center.

In the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*, see the "Integrate Cisco ISE with Catalyst Center" topic.

Step 3 Ensure that Cisco ISE is integrated correctly with Catalyst Center and that your wireless LAN controller is operational.

- If you are migrating data to only one second-generation appliance, stop here.
- If you are setting up a three-node cluster, proceed to Step 4.

Step 4 Configure the second and third appliances in your Catalyst Center cluster.

See the following topics in the *Cisco Catalyst Center Third-Generation Appliance Installation Guide*:

- If you are configuring a third-generation appliance using the Maglev Configuration wizard, see the "Configure a Secondary Node Using the Maglev Wizard" topic.
- If you are configuring a 32- or 56-core second-generation appliance using the browser-based configuration wizard, see the "Configure a Secondary Node Using the Advanced Install Configuration Wizard" topic in the "Configure the 32- and 56-Core Appliances Using the Browser-Based Wizard" chapter.

- If you are configuring an 80-core second-generation appliance using the browser-based configuration wizard, see the "Configure a Secondary Node Using the Advanced Install Configuration Wizard" topic in the "Configure the 80-Core Appliance Using the Browser-Based Wizard" chapter.

Scenario 15: Migrate data to a third-generation Catalyst Center appliance

In this scenario, you are migrating data from first- or second-generation Catalyst Center appliances to third-generation appliances.

Migrate your data

Complete the following procedure to migrate data from first- or second-generation Catalyst Center appliances to third-generation appliances.

Step 1 Prepare your first- or second-generation appliances for migration:

a) Chart out the upgrade path using the *Cisco Catalyst Center Upgrade Guide*. Based on your current Catalyst Center release, make sure to install any intermediate upgrades required before upgrading to release 2.3.7.7 or later.

Important We recommend that you create a backup file before starting the upgrade process, as well as before each intermediate upgrade.

b) Upgrade the appliances to Catalyst Center 2.3.7.7 or later. See the *Cisco Catalyst Center Upgrade Guide*.

c) Do one of the following:

- To set up an air-gapped deployment, complete Step 2d.
- To set up a cloud-tethered deployment, proceed to Step 3.

d) If you are setting up an air-gapped Catalyst Center deployment, do the following and then proceed to Step 3:

- Obtain a copy of the Catalyst Center upgrade bundle (release 2.3.7.7 or later) and place it on the node where catalogserver is running.
- Execute the Catalyst Center binary Air Gap binary file (release 2.3.7.7 or later).
- Using the GUI, upgrade to Catalyst Center 2.3.7.7 or later.
- Create a backup file. See the "Backup and Restore" chapter in the *Cisco Catalyst Center Administrator Guide*.

Step 2 Back up your current Catalyst Center deployment. See the "Backup and Restore" chapter in the *Cisco Catalyst Center Administrator Guide*.

Step 3 Prepare your third-generation appliances for migration:

Note Any third-party certificates used by your current Catalyst Center deployment will be carried over automatically when you restore the backup file you'll create in Step 3 to your third-generation appliances.

a) Confirm that Catalyst Center 2.3.7.7 or later is installed on your appliance.

b) Install any missing packages that are installed on your current deployment.

c) (Optional) If you are setting up an air-gapped Catalyst Center deployment, do the following:

- Run the Air Gap conversion script to enable Air Gap mode.
- Install any missing packages that are installed on your current deployment.

For more information, see the *Cisco Catalyst Center Standard Air Gap Deployment Guide*.

Step 4 Restore the backup file on your third-generation appliances:

a) Configure the same automation and Assurance (if applicable) backup settings that are configured on your current Catalyst Center deployment.

b) Ensure that the backup file you create for your existing deployment is listed as **Compatible** and has a green indicator in the Backup and Restore settings configuration page.

c) Start the restoration of the backup file. See the "Backup and Restore" chapter in the *Cisco Catalyst Center Administrator Guide*.

d) Monitor the restore and ensure it completes successfully.

Important Contact Cisco TAC or the Cisco escalation team if you encounter any issues while restoring the backup file.

Frequently asked questions

Q. What Catalyst Center release does the third-generation appliance support?

A. The appliance supports release 2.3.7.5 and later.

Q. Can I install a different Catalyst Center release on a third-generation appliance, such as 2.3.5.5 or earlier?

A. No. The appliance only supports release 2.3.7.5 and later.

Q. Can I mix first-generation and third-generation appliances in an HA cluster?

A. No. HA clusters consisting of first- and third-generation appliances are not supported.

Q. Can I mix second-generation and third-generation appliances in an HA cluster?

A. Yes. Catalyst Center 2.3.7.9 and later support mixed HA clusters. For more information, see the "Supported Appliances" topic in the *Cisco Catalyst Center High Availability Guide*.

Q. Can I use first-generation appliances at one disaster recovery site and third-generation appliances at another disaster recovery site?

A. No. The use of first- and third-generation appliances in a disaster recovery environment is not supported.

Q. Can I use second-generation appliances at one disaster recovery site and third-generation appliances at another disaster recovery site?

A. Yes. Migration is supported as long as all of the appliances at each site are of the same generation. For more information, see Disaster recovery considerations, on page 5.

Q. Can I migrate from a standalone first- or second-generation appliance to a three-node cluster of third-generation appliances?

A. Yes. For more information, see Conversion and appliance upgrade considerations, on page 4.

Q. Can I migrate from a three-node cluster with first- or second-generation appliances to a standalone third-generation appliance?

A. Yes. You can migrate from a three-node cluster consisting of first- or second-generation Catalyst Center appliances to a standalone third-generation appliance. The one exception is migration from a three-node cluster consisting of appliances with the XL

machine profile to a standalone appliance with the XL machine profile. For more information, see Conversion and appliance upgrade considerations, on page 4.

Q. Which Cisco IMC versions does the third-generation appliance support?
A. Cisco IMC Versions 4.3(2.230270) and 4.3(2.240009).

Scenario 16: Migrate data to a Catalyst Center on ESXi virtual appliance

Complete these steps to migrate data to a Catalyst Center on ESXi virtual appliance from one of the following Catalyst Center appliances:

- First-generation medium appliance: Cisco part number DN1-HW-APL
- First-generation medium promotional appliance: Cisco part number DN1-HW-APL-U
- Second-generation medium appliance: Cisco part number DN2-HW-APL
- Second-generation medium promotional appliance: Cisco part number DN2-HW-APL-U
- Third-generation medium appliance: Cisco part number DN3-HW-APL
- Third-generation medium promotional appliance: Cisco part number DN3-HW-APL-U

Important

- This procedure is supported in Catalyst Center 2.3.7.5 onwards.
- Catalyst Center on ESXi supports cross-version backup and restore; that is, you can create a backup of a physical Catalyst Center appliance and restore it to a virtual appliance running Catalyst Center on ESXi. The only requirement is that the same base version of Catalyst Center is installed on both appliances. For example, a backup of a physical appliance with Catalyst Center 2.3.7.10-1234 installed can be restored to a virtual appliance with Catalyst Center on ESXi 2.3.7.10-5678 installed.

Step 1 Install Catalyst Center 2.3.7.9 or later on the first or second-generation appliance.

Step 2 Back up your appliance's Assurance and automation data. In the *Cisco Catalyst Center Administrator Guide*, complete the steps described in the following topics:

a) "Configure Backup Servers"
b) "Back Up Data Now"

Step 3 After the backup completes successfully, open an SSH console on your NFS server and run the following commands:

- **export LOCAL_BACKUP_DIR=***NFS-server-path* (path to the server where your appliance's Assurance data is backed up)
- **export REMOTE_SERVER_DIR=***remote-server-path* (path to the server where your appliance's automation data is backed up)
- **export REMOTE_SERVER_IP=***automation-backup-server's-IP-address*
- **export REMOTE_SERVER_PORT=22**
- **export REMOTE_SERVER_USERNAME=***remote-server-username*
- **export REMOTE_SERVER_PASSWORD=***remote-server-password*

Step 4 Download **CatC_2.3.7.10-VA_MigrationScript_v1.tar.gz** (which includes the **CatC-2.3.7.10-VA_MigrationScript_v1.sh** script) from the following URL to your NFS server: https://software.cisco.com/download/home/286316341/type/286318832/release/2.3.7.9-VA.

Step 5 Extract the .tar file and copy **CatC-2.3.7.10-VA_MigrationScript_v1.sh** to your NFS server.

Step 6 Grant execute permission to the script by running the **chmod +x CatC-2.3.7.10-VA_MigrationScript_v1.sh** command.

Step 7 Start the script by running the **./CatC-2.3.7.10-VA_MigrationScript_v1.sh** command.

The script does two things:

a. It creates a copy of the automation data backup file that resides on the remote server and places it on the NFS server.

b. On the NFS server, it applies the latest Catalyst Center platform format to all backed-up data.

Step 8 After the script runs successfully, configure the NFS server that the virtual appliance will use:

a) Log in to the virtual appliance.

b) In the *Cisco Catalyst Center 2.3.7.x on ESXi Administrator Guide*, complete the steps described in the "Add the NFS Server" topic.

Enter the same NFS server IP address/hostname and path that you entered when completing Step 2.

Step 9 Restore the backup file that you created in Step 2.

In the *Cisco Catalyst Center 2.3.7.x on ESXi Administrator Guide*, complete the steps described in the "Restore Data from Backups" topic. Enter the same encryption passphrase that you entered when completing Step 2.

After the restore operation completes, the automation and Assurance data from the first or second-generation appliance is migrated to the virtual appliance.

Revert a backup file to the previous Catalyst Center platform format

If you are unable to migrate the data from a first-generation Catalyst Center appliance to a Catalyst Center on ESXi virtual appliance, complete the following steps to revert the backup file that was created during the migration procedure back to the previous Catalyst Center platform format.

Step 1 On your NFS server, run the **./backup_data_transform.sh -r** command.

This command runs a script that does the following:

- For the directory where the backup file resides, it restores the structure used by the previous platform data format.
- For the backup file, it converts its metadata back to the previous platform format.

Step 2 Restore the automation data backup file that resides on the remote server, which wasn't touched during the migration procedure.

In the *Cisco Catalyst Center Administrator Guide*, complete the steps described in the "Restore Data from Backups" topic. Enter the same encryption passphrase the you entered previously.

After the restore operation completes, the automation and Assurance data for the first-generation appliance should be in the previous Catalyst Center platform format again.

Scenario 17: Back up and restore a physical Catalyst Center appliance to a Catalyst Center VA on AWS

Complete this procedure to back up the data from a Catalyst Center hardware appliance and restore it to a Catalyst Center VA on AWS.

- Make sure that the hardware appliance used for the backup is a first, second, or third-generation medium Catalyst Center appliance.
- If you're using a Cloud backup (NFS) server, you'll need to know the backup password in order to log into the server.

  Your backup server password is dynamically created. The password is composed of the first four characters of the VA pod name and the backup server's IP address without the periods. For example, if the VA pod name is DNAC-SJC and the backup server's IP address is 10.0.0.1, the backup server password is DNAC10001.

  Note

  You can find the VA pod name on the **Dashboard** pane after you select the region that it's deployed in.

  You can find the backup server's IP address in the **View Catalyst Center** pane.

Step 1 Configure the backup server you want to use.

See the "Configure Backup Servers" topic in the *Cisco Catalyst Center Administrator Guide*.

Note Make sure that the backup server is connected to Catalyst Center through a VPN.

Step 2 Back up the data from the medium first or second-generation Catalyst Center hardware appliance and confirm that the backup was successful.

See the "Back Up Data Now" topic in the *Cisco Catalyst Center Administrator Guide*.

Step 3 Create a Catalyst Center VA, and ensure it's up and running before you proceed.

See the "Create a New Catalyst Center VA" topic in the *Cisco Catalyst 2.3.7.x on AWS Deployment Guide*.

Step 4 Connect the Catalyst Center VA to the backup server you configured in Step 1.

Make sure that the backup server is reachable from the Catalyst Center VA.

Step 5 Configure the backup server on the Catalyst Center VA.

See the "Configure Backup" topic in the *Cisco Global Launchpad 1.9 and 2.0 Administrator Guide*.

Step 6 Restore the data on to the Catalyst Center VA.

See the "Restore a Backup" topic in the *Cisco Global Launchpad 1.9 and 2.0 Administrator Guide*.

Step 7 Reestablish connectivity with Cisco ISE. For more information, see "Configure Authentication and Policy Servers" in the .*Cisco Catalyst Center Administrator Guide*

Note For deployments running non-Cisco ISE AAA servers, use the **System Health** tool to confirm that Catalyst Center can reach these servers and connectivity is established.

Step 8 If self-signed certificates were in place on your network's devices, reprovision them in order to update their Catalyst Center certificates. For more information, see "Update Device Configuration Using Telemetry" in the *Cisco Catalyst Center User Guide*.

Note You can skip this step if you have third-party CA certificates installed on your network devices.

Migration validation

After restoring your appliance data, we recommend that you validate the following Catalyst Center items:

- Site hierarchy
- Site maps
- Managed devices in inventory
- External integration services:
  - Cisco ISE
  - External IPAM (such as Infoblox)
  - Cisco Spaces
  - ThousandEyes
- Assurance charts and dashlets: It can take up to 20 minutes before they provide Assurance data.