

Cisco DNA Center Data Migration Guide

First Published: 2020-12-10

Last Modified: 2023-06-14

Cisco DNA Center Data Migration Guide

Data Migration Overview

This document covers the various data migration scenarios that may become applicable when using Cisco DNA Center to manage your network and describes how to complete them.

Supported Appliances

The following table lists the Cisco DNA Center appliances that support data migration:

Appliance Type	Cisco Part Number
First-generation 44-core appliance	DN1-HW-APL
Second-generation 44-core appliance	DN2-HW-APL
44-core promotional appliance	DN2-HW-APL-U
56-core appliance	DN2-HW-APL-L
56-core promotional appliance	DN2-HW-APL-L-U
112-core appliance	DN2-HW-APL-XL
112-core promotional appliance	DN2-HW-APL-XL-U

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.

Scenario 1: Move a Standalone Cisco DNA Center Appliance Between Data Centers (Same IP Addresses)

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

Procedure

Step 1 (Optional) Upgrade to the latest Cisco DNA Center release. See the [Cisco DNA Center Upgrade Guide](#).

Note If you upgrade, we recommend that you back up the data on your appliance. In the [Cisco DNA 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.

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

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

Scenario 2: Move a Standalone Cisco DNA Center Appliance Between Data Centers (Different IP Addresses)

In this scenario, you are moving a Cisco DNA 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.

Procedure

Step 1 (Optional) Upgrade to the latest Cisco DNA Center release. See the [Cisco DNA Center Upgrade Guide](#).

Note If you upgrade, we recommend that you back up the data on your appliance. In the [Cisco DNA 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.
- The virtual IP addresses that you want to assign to the Enterprise and Management interfaces.

In the [Cisco DNA Center Second-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 Cisco DNA Center release that was present when the latest backup file was created. In the *Cisco DNA Center Second-Generation Appliance Installation Guide*, see the "Reimage the Appliance" topic.

Step 4 After you complete the Configuration wizard, log in to the Cisco DNA Center GUI.

Step 5 Reestablish the pxGrid connection between Cisco DNA 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 DNA 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 Cisco DNA Center can reach these servers and connectivity is established.

Step 6 Cisco DNA Center automatically pushes telemetry updates and required system certificates to your network's devices.

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 Cisco DNA Center Appliance Between Data Centers (Different IP Addresses, Same FQDN)

In this scenario, you are moving a standalone Cisco DNA 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.

Procedure

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

Note If you upgrade, we recommend that you back up the data on your appliance. In the *Cisco DNA 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.
- The virtual IP addresses that you want to assign to the Enterprise and Management interfaces.

In the *Cisco DNA Center Second-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 Cisco DNA Center release that was present when the latest backup file was created. In the *Cisco DNA Center Second-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 Cisco DNA Center GUI.
- Step 6** Reestablish the pxGrid connection between Cisco DNA 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 DNA 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 Cisco DNA Center can reach these servers and connectivity is established.
- Step 7** Cisco DNA Center automatically pushes telemetry updates and required system certificates to your network's devices.
- 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 Cisco DNA Center Appliance with an Appliance with More Cores (Same IP Addresses)

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

Procedure

- Step 1** (Optional) Upgrade to the latest Cisco DNA Center release. See the [Cisco DNA Center Upgrade Guide](#).
- Note** If you upgrade, we recommend that you back up the data on your appliance. In the [Cisco DNA Center Administrator Guide](#), see the "Back Up Data Now" topic.
- Step 2** Decommission the appliance you are replacing.
- Step 3** Set up the new appliance at your data center, ensuring that you install the same Cisco DNA Center release that was installed on the previous appliance. Also make sure that you set the same IP address for that was configured previously for the Enterprise interface. In the [Cisco DNA Center Second-Generation Appliance Installation Guide](#), see the "Configure the Primary Node Using the Maglev Wizard" topic.
- Step 4** Restore the backup file that was created on the previous appliance. In the [Cisco DNA Center Administrator Guide](#), see the "Restore Data from Backups" topic.
- Step 5** Reestablish connectivity with Cisco ISE. In the [Cisco DNA 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 Cisco DNA 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 Cisco DNA Center certificates. In the [Cisco DNA 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 Cisco DNA Center Appliance with an Appliance with More Cores (Different IP Addresses)

In this scenario, you are replacing a standalone Cisco DNA Center appliance with another appliance that has more cores (for example, replacing a 56-core appliance with a 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.

Procedure

Step 1 (Optional) Upgrade to the latest Cisco DNA Center release. See the [Cisco DNA Center Upgrade Guide](#).

Note If you upgrade, we recommend that you back up the data on your appliance. In the [Cisco DNA Center Administrator Guide](#), see the "Back Up Data Now" topic.

Step 2 Decommission the appliance you are replacing.

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

- Specify new IP addresses for the appliance's interfaces.
- Specify new virtual IP addresses for the Enterprise and Management interfaces.

In the [Cisco DNA Center Second-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 DNA Center Administrator Guide](#), see the "Restore Data from Backups" topic.

Step 5 Complete the steps described in the [Cisco DNA Center Security Best Practices Guide's](#) "Update the Cisco DNA Center Server Certificate" topic.

Important Make sure you 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 Cisco DNA Center and Cisco ISE (which was severed when you updated the Enterprise interface's IP and virtual IP addresses). In the [Cisco DNA 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 Cisco DNA Center can reach these servers and connectivity is established.

Cisco DNA Center automatically pushes telemetry updates and required system certificates to your network's devices.

Scenario 6: Replace a Standalone Cisco DNA Center Appliance with an Appliance with More Cores (Different FQDN)

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

Procedure

- Step 1** (Optional) Upgrade to the latest Cisco DNA Center release. See the [Cisco DNA Center Upgrade Guide](#).
- Note** If you upgrade, we recommend that you back up the data on your appliance. In the [Cisco DNA Center Administrator Guide](#), see the "Back Up Data Now" topic.
- Step 2** Decommission the appliance you are replacing.
- Step 3** Set up the new appliance at your data center, ensuring that you do the following:
- Install the same Cisco DNA 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 DNA Center Administrator Guide](#), see the "Restore Data from Backups" topic.
- Step 5** Reestablish connectivity with Cisco ISE. In the [Cisco DNA 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 Cisco DNA 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 Cisco DNA Center certificates. In the [Cisco DNA 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 Cisco DNA Center Cluster Between Data Centers (Same IP Addresses)

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

Procedure

-
- Step 1** (Optional) Upgrade to the latest Cisco DNA Center release. See the [Cisco DNA Center Upgrade Guide](#).
- Note** If you upgrade, we recommend that you back up the data on your appliance. In the [Cisco DNA 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 between Cisco DNA Center and the devices it manages is established.
-

Scenario 8: Move a Three-Node Cisco DNA Center Cluster Between Data Centers (Different IP Addresses)

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

Procedure

-
- Step 1** (Optional) Upgrade to the latest Cisco DNA Center release. See the [Cisco DNA Center Upgrade Guide](#).
- Note** If you upgrade, we recommend that you back up the data on your appliance. In the [Cisco DNA 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.
 - The virtual IP addresses you want to assign to the Enterprise and Management interfaces.

In the [Cisco DNA Center Second-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 Cisco DNA Center release that was present when the latest backup file was created. In the *Cisco DNA Center Second-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 DNA Center Administrator Guide*, see the "Restore Data from Backups" topic.

Step 5 Reestablish the pxGrid connection between Cisco DNA Center and Cisco ISE (which was severed when you updated the Enterprise interface's IP and virtual IP addresses). In the *Cisco DNA 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 Cisco DNA Center can reach these servers and connectivity is established.

Step 6 Cisco DNA Center automatically pushes telemetry updates and required system certificates to your network's devices.

Scenario 9: Change a Standalone Cisco DNA Center Appliance to a Three-Node HA Cluster

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

Procedure

Step 1 Use the Configuration wizard to specify the IP address and virtual IP address that you want to set for the appliance's Enterprise interface. In the *Cisco DNA Center Second-Generation Appliance Installation Guide*, see the "Reconfigure the Appliance Using the Configuration Wizard" topic.

- 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 DNA Center Second-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 Cisco DNA Center release that was present when the latest backup file was created. In the *Cisco DNA Center Second-Generation Appliance Installation Guide*, see the "Reimage the Appliance" topic.

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

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

Step 4 Back up the data on your appliance. In the *Cisco DNA 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 DNA Center Second-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 DNA Center Second-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 Cisco DNA Center release installed.
- Step 9** Activate HA to initiate the redistribution of services.
- From the top-left corner, click the menu icon and choose **System > Settings > System Configuration > High Availability**.
 - 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 Cisco DNA Center cluster with HA enabled to a cluster that has a 1+1+1 disaster recovery setup.

Procedure

- Step 1** Upgrade the cluster to the latest Cisco DNA Center release. See the [Cisco DNA Center Upgrade Guide](#).
- Step 2** Back up the cluster's data. In the [Cisco DNA 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.
- If you are using an appliance from the HA cluster, reimage it. In the [Cisco DNA Center Second-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.
 - Install the same Cisco DNA Center release that was installed in Step 1.
 - Restore the backup file you created in Step 2. In the [Cisco DNA 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 Cisco DNA 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 DNA 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 DNA Center Security Best Practices Guide*, see the "Generate a Certificate Request Using Open SSL" topic.
- Step 9** Confirm that the prerequisites described in the *Cisco DNA Center Administrator Guide's* "Prerequisites" topic have been met before you enable disaster recovery.
- Step 10** Configure your disaster recovery system. In the *Cisco DNA 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 Cisco DNA Center cluster with HA enabled to a cluster with a 3+3+1 disaster recovery setup.

Procedure

- Step 1** Upgrade the appliances to the latest Cisco DNA Center release. See the *Cisco DNA Center Upgrade Guide*.
- Step 2** Back up the cluster's data. In the *Cisco DNA 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 DNA Center Second-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 DNA Center Second-Generation Appliance Installation Guide*, see the "Configure a Secondary Node Using the Maglev Wizard" topic.
 - c) Activate HA:
 1. From the top-left corner, click the menu icon and choose **System > Settings > System Configuration > High Availability**.
 2. Click **Activate High Availability**.
 - d) Ensure that the same Cisco DNA 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 DNA Center Administrator Guide's* "Prerequisites" topic.

- 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 DNA 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 DNA 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 DNA 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 Cisco DNA Center cluster with a 1+1+1 disaster recovery setup to a three-node HA cluster.

Procedure

- Step 1** Pause your disaster recovery system (resulting in two standalone appliances). In the *Cisco DNA Center Administrator Guide*, see the "Place Your System on Pause" topic.
- Step 2** Deregister the system. In the *Cisco DNA Center Administrator Guide*, see the "Deregister Your System" topic.
- Step 3** Upgrade the first appliance to the latest Cisco DNA Center release. See the *Cisco DNA Center Upgrade Guide*.
- Step 4** Back up the first appliance's data. In the *Cisco DNA 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 DNA Center Second-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 Cisco DNA 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 Cisco DNA Center release that's installed on the other two appliances, as well as the same number of cores. In the *Cisco DNA Center Second-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:
- From the top-left corner, click the menu icon and choose **System > Settings > System Configuration > High Availability**.
 - 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.

Procedure

-
- Step 1** At the data center where your main site will reside, do the following:
- Pause your disaster recovery system (resulting in two standalone appliances). In the [Cisco DNA Center Administrator Guide](#), see the "Place Your System on Pause" topic.
 - Deregister your system's sites in order to delete all of the settings that were previously configured for them. In the [Cisco DNA Center Administrator Guide](#), see the "Deregister Your System" topic.
 - Upgrade both appliances to the latest Cisco DNA Center release. See the [Cisco DNA Center Upgrade Guide](#).
 - Back up the first appliance's data. In the [Cisco DNA Center Administrator Guide](#), see the "Back Up Data Now" topic.
 - Add the second appliance, which will act as the second node in a three-node HA cluster. In the [Cisco DNA Center Second-Generation Appliance Installation Guide](#), see the "Configure a Secondary Node Using the Maglev Wizard" topic.
 - Add a third appliance, which will act as the third node in a three-node HA cluster. In the [Cisco DNA Center Second-Generation Appliance Installation Guide](#), see the "Configure a Secondary Node Using the Maglev Wizard" topic.
 - Ensure that all three appliances have the same Cisco DNA 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:
- Confirm that the appliances you'll add to the recovery site cluster have the same Cisco DNA Center release that's already installed on the main site's appliances. Also confirm that they have the same number of cores.
 - Configure the appliance that will serve as the primary node. In the [Cisco DNA Center Second-Generation Appliance Installation Guide](#), see the "Configure the Primary Node Using the Maglev Wizard" topic.
 - Configure the recovery site's second and third appliance. In the [Cisco DNA Center Second-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:
- From the top-left corner, click the menu icon and choose **System > Settings > System Configuration > High Availability**.
 - 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 DNA 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 DNA Center Security Best Practices Guide*, see the "Generate a Certificate Request Using Open SSL" topic.
- Step 6** Confirm that the prerequisites described in the *Cisco DNA Center Administrator Guide's* "Prerequisites" topic have been met before you enable disaster recovery.
- Step 7** Reconfigure your disaster recovery system. In the *Cisco DNA Center Administrator Guide*, see the "Configure Disaster Recovery" topic.
-

Scenario 14: Migrate Data from a First-Generation Cisco DNA Center Appliance

In this scenario, you are migrating data from a first-generation Cisco DNA Center appliance to either an individual Cisco DNA 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 Cisco DNA Center packages that are installed on your first-generation appliance and their release number. To get this information, do one of the following:
 - Log in to the appliance and run the **maglev package status** command.
 - For Cisco DNA Center Release 1.3.3.0 and earlier, in the top-right corner of the Cisco DNA Center GUI, choose  > **About** > **Show Packages**.
 - For Cisco DNA Center Release 2.1.2 and later, in the top-right corner of the Cisco DNA Center GUI, click the **Help** icon and choose **About** > **Packages**.
- The configuration information for your backup server.

Procedure

- Step 1** On your first-generation appliance, do the following:
- a) Back up the appliance's Automation and Assurance data.
In the *Cisco DNA Center Administrator Guide*, see the "Back Up Data Now" topic.
 - b) Disconnect the appliance from your network.
- Step 2** On your second-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 DNA Center Second-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 second-generation appliance using the Maglev Configuration wizard, see the "Configure the Primary Node Using the Maglev Wizard" topic.
- If you are configuring a 44- or 56-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 44/56-Core Appliance Using the Browser-Based Wizard" chapter.
- If you are configuring a 112-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 112-Core Appliance Using the Browser-Based Wizard" chapter.

Note When reconfiguring your access switches to match the high-throughput settings on your Cisco DNA Center appliances, be aware of the following differences between first-generation and second-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-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 Cisco DNA Center packages that are installed on your first-generation appliance.

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

- d) Integrate Cisco ISE with Cisco DNA Center.

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

Step 3 Ensure that Cisco ISE is integrated properly with Cisco DNA 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 Cisco DNA Center cluster.

See the following topics in the *Cisco DNA Center Second-Generation Appliance Installation Guide*:

- If you are configuring a second-generation appliance using the Maglev Configuration wizard, see the "Configure a Secondary Node Using the Maglev Wizard" topic.
- If you are configuring a 44- 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 44/56-Core Appliance Using the Browser-Based Wizard" chapter.

- If you are configuring a 112-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 112-Core Appliance Using the Browser-Based Wizard" chapter.
-

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020–2023 Cisco Systems, Inc. All rights reserved.