



## CHAPTER 2

# Installing Cisco DCNM OVA Management Software

---

This chapter describes how to install Cisco Data Center Network Manager (DCNM) Open Virtual Appliance (OVA) components and includes the following sections:

- [Information About the Cisco DCNM OVA section, page 2-1](#)
- [Cisco DCNM OVA and Cisco Dynamic Fabric Automation section, page 2-1](#)
- [Installing the Cisco DCNM OVA section, page 2-2](#)
- [Configuring the Oracle Database for DCNM section, page 2-8](#)
- [Upgrading Cisco DCNM 7.0\(1\) to Version 7.0\(2\) section, page 2-9](#)

## Information About the Cisco DCNM OVA

An Open Virtual Appliance (OVA) is a prebuilt software solution that comprises one or more virtual machines (VMs) that are packaged, maintained, updated, and managed as a single unit. The Cisco DCNM OVA has a preinstalled operating system (CentOS 6.3) and includes application functionality that is necessary for Dynamic Fabric Automation (DFA) functionality. DCNM as an OVA can be deployed on a VMWare Vsphere infrastructure.

## Cisco DCNM OVA and Cisco Dynamic Fabric Automation

To bring up Cisco DFA, you can use the Cisco DCNM OVA to link the following two subnets:

- Management access (the outside subnet) to access and administer the DFA network
- Enhanced fabric management network (the inside network) which is connected to the devices through the mgmt0 interface of each device.

When installing Cisco DCNM OVA, you can choose to enable Cisco DFA functionality that simplifies fabric management.

Cisco DCNM provides a management system that offers the following benefits:

- Ease of deployment and use
- Standards-based control protocols and components
- Unlimited level of customization and integration with an operations support systems (OSS) network

**Note**

For more information about Cisco Dynamic Fabric Automation, see to the *Cisco Dynamic Fabric Automation Solutions Guide*.

Cisco DCNM OVA includes the following application functionality:

- Network management
  - Cisco DCNM
- Network services
  - Network Service Controller (NSC) Adapter
- Orchestration
  - RabbitMQ AMQP Message Broker
  - Python integration script
  - OpenLDAP
- Device Power-on Auto Provisioning (POAP)
  - DHCP server
  - TFTP Repository for boot scripts
  - SCP repository for storing images and configurations
- Group provisioning of switches
  - XCP Extensible Messaging and Presence Protocol (XMPP) server (Cisco Jabber)

**Note**

For detailed information about each of the applications that provide the Cisco DFA CPOM functions in Cisco DCNM, see [Chapter 3, “Managing Applications After the DCNM OVA Deployment”](#).

## Installing the Cisco DCNM OVA

Three steps are required to install the OVA:

1. Verify Prerequisites. You must install various VMware components before you install the OVA.
2. Download the OVA file. You can access the required dcnm.ova file from [www.cisco.com](http://www.cisco.com).
3. Deploy the OVA as an OVF template. A step-by-step template in the vSphere Client guides you through this process. After you have completed the step-by-step template, you can review all of the information that you provided, make any corrections, and then deploy the OVA.

**Note**

If you are using a high-availability (HA) environment for applications that are bundled within the DCNM OVA, you must download the OVA and deploy twice, once for Active and once for Host-Standby. For more information, see [Chapter 4, “Managing Applications in a High-Availability Environment”](#).

## Verifying Prerequisites

Before you install the Cisco DCNM OVA, you will need to meet following software and database requirements:

- VMware vCenter Server 5.1.0 that is running on a Windows server (or alternatively, running as a virtual appliance)
- VMware ESXi 5.1.0 host imported into vCenter
- Two port groups on the ESXi host: one for the dcnm-mgmt-network and one for the enhanced-fabric-mgmt network.
- VMware vSphere client application installed on your desktop



**Note** The OVA cannot be deployed by connecting the vSphere client directly to the ESXi server.

- Determine the number of switches in your Cisco DFA fabric that will be managed by the Cisco DCNM OVA.
  - If you will be managing more than 50 switches or you expect the number of switches to grow over time, use an Oracle database.

See “[Configuring the Oracle Database for DCNM](#)” section on page 2-8 for information on configuring the Oracle database.



**Note** Once you start using the PostgreSQL database that is built in to the Cisco DCNM OVA, you cannot migrate the data to an Oracle database.



**Note** For a complete list of prerequisites that are associated with Cisco DCNM, see the *Cisco DCNM Installation and Licensing Guide, Release 7.x*.



**Note** To accommodate for HA application functions, additional prerequisites are required. See the [Prerequisites for Cisco DCNM OVA HA section, page 4-2](#).

## Downloading the OVA File

The first step to installing the OVA is to download the dcnm.ova file. You will point to that dcnm.ova file on your computer when deploying the OVF template.



**Note** If you plan to use HA application functions, you must deploy the dcnm.ova file twice.

### DETAILED STEPS


- Step 1** Go to the following site: <http://software.cisco.com/download/navigator.html>
- Step 2** In the **Product/Technology Support** section, choose **Download Software**.

- Step 3** In the **Select a Product** section, navigate to the DCNM software by choosing **Products > Switches > Data Center Switches > Data Center Network Management > Cisco Prime Data Center Network Manager**.
- A list of the latest release software for Cisco DCNM is available for download.
- Step 4** In the **Latest Releases** list, choose **7.0.(x)**
- Step 5** Locate the DCNM OVA Installer and click the **Download** button.
- Step 6** Save the dcnm.ova file to your computer in a place that will be easy to find when you start to deploy the OVF template.
- 

## Deploying the OVA as an OVF Template

After you download the OVA file, you will deploy the OVF template from the vSphere Client application.

### DETAILED STEPS

- 
- Step 1** Log in to your vSphere Client:
- Open the VMWare vSphere client application on your desktop.
  - Connect to the vCenter Server with your vCenter user credentials.
-  **Note** You cannot deploy the OVA by connecting the vSphere Client directly to the ESXi server.
- 
- Step 2** Use the vSphere Client to access the OVF template:
- Choose **Home > Inventory > Hosts and Clusters**.
  - Choose the host on which the OVF template will be deployed.
  - Choose **File > Deploy OVF Template** to open the Deploy OVF Template window.
- Step 3** Choose the Source location:
- Click the **Browse** button.
  - Locate the dcnm.ova file that you downloaded to your computer and click **Next**.
- Step 4** Review the OVF Template Details and click **Next**.

Some of the details about the Cisco DCNM virtual appliance include:

- Version number
- Download size
- Size on disk:
  - Thin provision for the amount of disk space consumed by the virtual appliance immediately after deployment. It is the minimum amount of disk space needed to deploy the virtual appliance.
  - Thick provision for the maximum amount of disk space the virtual appliance can consume.

**Note**

For more information on thick and thin provision, see ["Step 11 - Choose the disk format." task on page 2-5](#)

**Step 5** Read and accept the End User License Agreement and click **Next**.

**Step 6** Specify the name and location of the Cisco DCNM OVA.

- a. In the **Name** box, enter a name for the virtual appliance. This name is not the hostname, but the name of the virtual appliance hardware and is specific to the vSphere infrastructure. The name can contain up to 80 alphanumeric characters and must be unique within the Inventory folder.
- b. In the **Inventory Location** tree, choose the folder location for the virtual appliance.
- c. Click **Next**.

**Step 7** Choose the deployment configuration:

- Choose **Small** to configure the virtual machine with two vCPUs and 8G RAM.
- Choose **Large** to configure the virtual machine with four vCPUs and 12G RAM.

**Note**

We recommend that you use a Large deployment configuration when you are managing more than 50 devices (and up to the upper limit of the Cisco DFA fabric) to leverage better RAM, heap memory, and CPUs.

For setups that could grow, you should choose Large.

Choose Small for proof-of-concept and other small-scale environments with fewer than 50 switches that are not expected to grow with time.

**Step 8** Click **Next**.

**Step 9** Specify the host and click **Next**.

**Note**

A host will not be available if you already selected a host in the vSphere Client before you deploy the OVA.

**Note**

The OVA should not be deployed under a vApp.

**Step 10** Choose the a destination storage for the virtual machine files and click **Next**.

**Step 11** Choose the disk format.

- Choose one of the thick provision types if you have enough storage capacity as required by the virtual appliance and want to set a specific allocation of space for the virtual disks:
  - **Thick Provision Lazy Zeroed:** The space that is required for the virtual disk is allocated when the virtual disk is created. The data that remains on the physical device is not erased when the virtual disk is created but is zeroed out on demand at a later time on first write from the virtual disk.
  - **Thick Provision Eager Zeroed:** The space that is required for the virtual disk is allocated when the virtual disk is created. Unlike the Lazy Zeroed option, the data that remains on the physical device *is* erased when the virtual disk is created.

- Choose **Thin Provision** if you have less than 100 GB of disk space available. The initial disk consumption will be 2.8 GB and will increase as the size of the database increases with the number of devices being managed.

**Step 12** Click **Next**.

**Step 13** Choose your network mapping.

- The **dcnm-mgmt** network provides connectivity (ssh, scp, http, https) to the Cisco DCNM OVA. In the **Destination Network** column, associate the network mapping with the port group that corresponds to the subnet that is associated with the Cisco DCNM management network.
- Map the **enhanced-fabric-mgmt** network to the port group that connects to the management network of switches.



**Note**

If you are deploying more than one OVA for HA functionality, you must meet the following criteria:

- Both OVAs should have their management access (eth0) and enhanced fabric management (eth1) interfaces in the same subnet.
- Both OVAs should be deployed with the same administrative password. This is to ensure that both OVAs are duplicates of each other for application access.

**Step 14** Click **Next**.

**Step 15** Choose the Cisco DCNM OVA Properties.

- The **Application Management** check box is selected by default to install applications related to DFA.

DFA includes implementations for the following protocols:

- XMPP
- LDAP
- DHCP
- AMQP

DFA includes implementations for the following repositories:

- TFTP
- SCP/SFTP

- In the **Management Properties** section, enter a password in the **Enter Password** and **Confirm Password** boxes to establish the password that will be used to connect all applications in the DCNM OVA.



**Note**

The password must be at least eight characters long and must contain at least one alphabetic and one numeric character. It can contain the only the following special characters: .(dot), + (plus), \_ (underscore), and - (hyphen).



If you do not comply with these password requirements, you can continue with the OVA deployment; however, you subsequently may not be able to log in to other applications like DCNM.

- In the **DCNM Network** section, complete each of the required fields:

- **Hostname** (should be a fully qualified domain name, otherwise you may encounter issues when using the XMPP application after deployment)
  - **IP Address** (for the outside management address for DCNM)
  - **Subnet Mask**
  - **Default Gateway**
  - **DNS IP**
- d. In the **Enhanced Fabric Management** section, complete each of the required fields:
- **IP Address** (for the inside fabric management address or OOB Management Network)
  - **Subnet mask**
  - **DNS IP**
- Step 16** Click **Next**
- Step 17** Review each of the deployment settings that you have established. Press the **Back** button to go to any settings if you want to change them.

After you have reviewed each of the deployment settings in the OVF template, perform the following procedure to deploy the virtual machine.

## Deploying Virtual Machines

- Step 1** Check the **Power on after deployment** check box.
- Step 2** Click the **Finish** button.
- A Deploying DNCM\_OVA window appears and the OVA deployment starts and requires some time to complete.
-  **Note** The time for the OVA deployment could take 5 to 6 minutes (or more) depending on the network latency.
- After the OVA is deployed, a Deployment Completed Successfully message appears.
- Step 3** On the **Summary** tab in the vSphere Client, review the information about the VM and make note of the IP address.
- Step 4** Check the console of the VM in the vSphere Client for the login prompt. Once the login prompt appears, log in with root credentials and use the **appmgr status all** command to check the status of the applications. After all applications are up and running, go to the next step.
-  **Note** For more information about verifying application status see the [Verifying the Application Status after Deployment](#) section, page 3-8.
- Step 5** Log in to the Cisco DCNM web UI:
- a. Put the IP address in your browser.

The Cisco Prime Data Center Network Manager window is displayed.

- b. In the **User Name** field, enter **admin**.
- c. In the **Password** field, enter the administrative password given to you during the OVA deployment.



**Note** If you are deploying multiple OVAs for HA functions, you should deploy both the OVAs with the same administrative password. This action ensures that both OVAs are duplicates of each other for application access.

You are ready to begin POAP configuration and Device Discovery.



**Note** See the *DCNM 7.0 Fundamentals Guide* for configuration information.

## Configuring the Oracle Database for DCNM

We recommend that you use an external Oracle database for Cisco DCNM for DFA for better performance, rather than the PostgreSQL database that is built in to the Cisco DCNM OVA.



**Note** Once you start using the PostgreSQL database that is built in to the Cisco DCNM OVA, you cannot migrate the data to an Oracle database.



**Note** If you configure a remote Oracle database for both DCNM and XMPP in an appliance (OVA/ISO), create two separate database users—one for the DCNM and the other for XMPP.

**Step 1** Prepare the Oracle database as described in the *Cisco DCNM Installation and Licensing Guide, Release 7.x*.



**Note** If you are configuring the Oracle database for an HA environment, only Step 1 is required. If you are configuring the Oracle database for a standalone DCNM, continue with the following steps in the procedure.

**Step 2** Get the JDBC database URL, database username, and database password.

**Step 3** Stop the Cisco DCNM application in the OVA.

**Step 4** Open the Secure Shell (SSH) terminal and enter the following CLI command:  
**appmgr update dcnm -u <DB\_URL> -n <DB\_USER> -p <DB\_PASSWORD>**

**Step 5** Enter the root password of the Cisco DCNM OVA. This password is used to access AMQP/LDAP by default. You can change this password later in Cisco DCNM by using the following path: **Admin -> DFA Settings**.

```
[root@DCNM ~]# appmgr update dcnm -u jdbc:oracle:thin:@10.77.247.11:1521:XE -n extuser -p extuserpwd
```



The external DCNM DB will be configured so that all DFA applications can be accessed using the root password of this server. You can later change them in the DCNM Web UI: Admin > DFA Settings

Root password :  
Enter it again for verification:  
Please wait...this could take a few minutes

done.

- Step 6** Start the Cisco DCNM application in the OVA.
- Step 7** Update the DFA setting in Cisco DCNM, if necessary.
- 

## Upgrading Cisco DCNM 7.0(1) to Version 7.0(2)

This section includes instructions for upgrading your Cisco DCNM OVA installation from version 7.0(1) to 7.0(2). You can migrate both Cisco DCNM with a local PostgreSQL database and an external Oracle database and Cisco DCNM in a High Availability (HA) environment.

### Migrating Cisco DCNM with a Local PostgreSQL Database and an External Oracle Database

Before you begin, make sure that Cisco DCNM 7.0(1) is up and running.

- 
- Step 1** Use the **appmgr backup all** command to backup all applications associated with the installation of Cisco DCNM 7.0(1).
- Step 2** Back up Cisco DCNM 7.0(1) license files.
- Backup the license files saved in the following directory: `/usr/local/cisco/dcm/licenses/`.
  - On Cisco Prime DCNM 7.0(2), ensure that the MAC address along with all network settings such as the IP address, default gateway, hostname, etc., are identical to the Cisco DCNM 7.0(1) installation.
  - Copy the contents of the Cisco DCNM 7.0(1) files you backed up from the `/usr/local/cisco/dcm/licenses/` directory into the Cisco DCNM 7.0(2) `/usr/local/cisco/dcm/licenses/` directory.
- Step 3** If you are using customized scripts like `vCDclient.py`, `CPNR.py`, move these files manually.
- Backup the following files and put these files in the same location by changing the name. (For example - `/root/utls/vCDclient_backup.py`).
- `/root/utls/vCDclient.py`  
`root/utls/vCDclient.ini.conf`  
`root/utls/CPNRclient.py`  
`root/utls/CPNRclient.ini.conf`



**Note** If you are using a customized `poap_dcnm.py` script in Cisco DCNM 7.0(1), after migration the script will be saved as `/var/lib/dcnm/poap_dcnm_backup.py` in Cisco DCNM 7.0(2) and the new `poap_dcnm.py` will be there.

---

- Step 4** Transfer the backup file to an external file system.
- Step 5** Power off Cisco DCNM 7.0(1).
- Step 6** Deploy the Cisco DCNM OVA file for version 7.0(2).
- Use the same network parameters (IP/subnet/gateway/DNS).
  - Use the same administrative password.
  - Use the same vCenter port groups for both network interfaces.
  - Disable auto-power-on. (The **Power on OVA after deployment** check-box should not be selected).
- Step 7** After Cisco DCNM 7.0(2) is deployed, right-click on **VM -> Edit Settings -> Hardware**.
- For both Network Adapters, update the MAC address to be the same as Cisco DCNM 7.0(1). This will cause the same MAC address to be used for the new Virtual Machine (VM); licenses on Cisco DCNM will not need to be regenerated in the event of an upgrade.
- Step 8** Power on DCNM 7.0(2) VM.
- Step 9** Copy the Cisco DCNM 7.0(1) backup file from the external repository to Cisco DCNM 7.0(2) and other files (for example, License etc.) to corresponding places.
- Step 10** Use the **appmgr status all** command to make sure that all applications are up and running.
- Step 11** Use the **appmgr stop all** command to shut down all applications on Cisco DCNM 7.0(2).
- Step 12** Use the **appmgr upgrade <backup filename>** command to run the upgrade script on Cisco Prime DCNM 7.0(2).
- Select option [1] **Standalone DCNM with Local PostgreSQL database** or [2] **Standalone DCNM with External Oracle database** when prompted, based on your Cisco DCNM 7.0(1) setup:  
 Choose [1] Standalone DCNM with Local PostgreSQL database  
 [2] Standalone DCNM with External Oracle database  
 [3] High Availability



**Note** If you choose option [2] **Standalone DCNM with External Oracle database**, make sure that the external database is up and running.

## Migrating Cisco DCNM in a High Availability Environment

Before you begin, make sure that Cisco DCNM 7.0(1) Active and Standby peers are both up and running.



**Note** For more information on Active and Standby peers in a High Availability environment, see [“Managing Applications in a High-Availability Environment”](#).

- Step 1** Make sure that Cisco DCNM 7.0(2) Active and Standby peers are both deployed but not powered on.



**Note** Make sure that the MAC address and all network settings, such as the IP address, default gateway, hostname, etc., are identical to the Cisco DCNM 7.0(1) installation.

- Step 2** Verify that the **appmgr backup all** command was run on both the Active and Standby peers and that separate tar archives were stored in an external file system (for example, as active.tar.gz and standby.tar.gz)

- Step 3** Follow the same steps for the license files and other script files (vCDclient.py, CPNRclient.py etc) as instructed in [“Migrating Cisco DCNM with a Local PostgreSQL Database and an External Oracle Database”](#) section on page 2-9.
- Step 4** Power off the Cisco DCNM 7.0(1) Active peer.
- Step 5** Wait 4 to 5 minutes and then stop the DCNM application on the Cisco DCNM 7.0.(1) Standby peer.  
This is to ensure that write operations to LDAP are prevented (which could lead to LDAP getting into an inconsistent state).
- Step 6** Power-on the Cisco DCNM 7.0(2) Active peer.
- Step 7** Stop all of the applications on the Cisco DCNM 7.0(2) Active peer.
- Step 8** Use the **appmgr upgrade <active.tar.gz>** command to run the upgrade script.
- a. Choose option **[3] High Availability** when prompted.  

```
Choose option [1] Standalone DCNM with Local PostgreSQL database
               [2] Standalone DCNM with External Oracle database
               [3] High Availability
```
  - b. Select option **[1] Active** when prompted.  

```
Choose [1] Active [2] Standby
```
- Step 9** All applications are running on the Cisco DCNM 7.0(2) Active peer; power-off the Cisco Prime DCNM 7.0(1) Standby peer.
- Step 10** Power on the Cisco DCNM 7.0(2) Standby peer.
- Step 11** Stop all applications on the Cisco DCNM 7.0(2) Standby peer. (After waiting for all applications to start during OS boot up).
- Step 12** Use the **appmgr upgrade <standby.tar.gz>** command to run the upgrade script.
- a. Choose option **[3] High Availability** when prompted.  

```
Choose option[1] Standalone DCNM with Local PostgreSQL database
               [2] Standalone DCNM with External Oracle database
               [3] High Availability
```
  - b. Select option **[2] Standby** when prompted.  

```
Choose [1] Active [2] Standby
```
- Step 13** Invoke the following on the Active peer to establish SSH trust to the Standby peer:  

```
sh /root/sshAutoLogin.sh <STANDBY_PEER_IP>
```
-

