



Cisco DCNM Installation and Upgrade Guide for LAN Fabric Deployment, Release 11.1(1)

First Published: 2018-12-14

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org>)

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

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: <http://www.cisco.com/go/trademarks>. 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. (1110R)

© 2018 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Overview 1

- Introduction 1
- Installation Options 2
- Deployment Options 2
- System Requirements for Cisco DCNM, Release 11.1(1) 2

CHAPTER 2

Guidelines and Limitations 7

- Guidelines and Limitations 7

CHAPTER 3

Prerequisites 9

- Prerequisites for DCNM Open Virtual Appliance 9
- Prerequisites for DCNM ISO Virtual Appliance 10
- Prerequisites for Cisco DCNM Virtual Appliance HA 10
 - Deploying Cisco DCNM Virtual Appliances in HA mode 10
 - Availability of Virtual IP Addresses 11
 - Installing an NTP Server 11

CHAPTER 4

Installing Cisco DCNM 13

- Installing DCNM on Open Virtual Appliance 13
 - Downloading the Open Virtual Appliance File 13
 - Deploying the Open Virtual Appliance as an OVF Template 14
 - Installing the Cisco DCNM OVA in Standalone Mode 17
 - Installing the Cisco DCNM OVA in Native HA mode 20
- Installing DCNM on ISO Virtual Appliance 26
 - Downloading the ISO Virtual Appliance File 26
 - Installing the DCNM ISO Virtual Appliance on UCS (Bare Metal) 26

Installing the DCNM ISO Virtual Appliance on KVM 30

Installing Cisco DCNM ISO in Standalone Mode 32

Installing the Cisco DCNM ISO in Native HA mode 34

Installing Cisco DCNM SE ISO on Cisco APIC SE 40

Installing Cisco DCNM Compute Node 42

CHAPTER 5

Upgrading Cisco DCNM 47

Upgrading ISO or OVA using the DCNM Upgrade Tool 48

 Downloading the DCNM Upgrade Tool 48

 Backup Using the Upgrade Tool 48

 Upgrading and Restoring DCNM Virtual Appliance in Standalone mode 49

 Upgrading and Restoring DCNM Virtual Appliance in Native HA Mode 51

Upgrading ISO or OVA through Inline Upgrade 56

 Inline Upgrade for DCNM Virtual Appliance in Standalone Mode 56

 Inline Upgrade for DCNM Virtual Appliance in Native HA Mode 58

CHAPTER 6

Disaster Recovery (Backup and Restore) 63

Backup and Restore Cisco DCNM and Application Data on Standalone DCNM setup 63

Backup and Restore Cisco DCNM and Application Data on Native HA setup 64

Recovering Cisco DCNM Single HA Node 65

CHAPTER 7

Running Cisco DCNM Behind a Firewall 69

Running Cisco DCNM Behind a Firewall 69

CHAPTER 8

Secure Client Communications for Cisco DCNM Servers 73

Secure Client Communications for Cisco DCNM Servers 73

 Enabling SSL/HTTPS on Cisco DCNM in HA Environment on Virtual Appliance 73

CHAPTER 9

Managing Applications in a High-Availability Environment 75

Information About Application Level HA in the Cisco DCNM Open Virtual Appliance 75

 Automatic Failover 76

 Manually Triggered Failovers 76

 Native HA Failover and Troubleshooting 76

Application High Availability Details	78
Data Center Network Management	78
RabbitMQ	80
Repositories	81

CHAPTER 10**Managing Utility Services After DCNM Deployment 83**

Editing Network Properties Post DCNM Installation	83
Modifying Network Interfaces (eth0 and eth1) Post DCNM Installation	84
Configuring Enhanced-Fabric-Inband Interface (eth2) Post DCNM Installation	92
Changing the DCNM Server Password Post DCNM Installation	94
Utility Services Details	95
Network Management	95
Orchestration	95
Device Power On Auto Provisioning	95
Managing Applications and Utility Services	96
Verifying the Application and Utility Services Status after Deployment	96
Stopping, Starting, and Resetting Utility Services	97
Updating the SFTP Server Address for IPv6	98



CHAPTER 1

Overview

Cisco Data Center Network Manager (DCNM) is a management system for Cisco NXOS-based programmable fabrics and Cisco NXOS-based storage fabrics. In addition to provisioning, monitoring, and troubleshooting the data center network infrastructure, the Cisco DCNM provides a comprehensive feature-set that meets the routing, switching, and storage administration needs of data centers. It streamlines the provisioning for the Programmable Fabric and monitors the SAN components.

Cisco DCNM provides a high level of visibility and control through a single web-based management console for Cisco Nexus Series Switches, Cisco MDS, and Cisco Unified Computing System (UCS) products. Cisco DCNM also includes Cisco DCNM-SAN client and Device Manager functionality.

This section contains the following sections:

- [Introduction, on page 1](#)
- [Installation Options, on page 2](#)
- [Deployment Options, on page 2](#)
- [System Requirements for Cisco DCNM, Release 11.1\(1\), on page 2](#)

Introduction

Cisco DCNM provides an alternative to the command-line interface (CLI) for switch configuration commands.

Cisco DCNM includes these management applications:

Cisco DCNM Web UI

Cisco DCNM Web UI allows operators to monitor and obtain reports for Cisco MDS and Nexus events, performance, and inventory from a remote location using a web browser. Licensing and discovery are part of the Cisco DCNM Web UI.

Performance Manager

Performance Manager presents detailed traffic analysis by capturing data with SNMP. This data is compiled into various graphs and charts that can be viewed on the Cisco DCNM Web UI.

Installation Options

Cisco DCNM software images are packaged with the Cisco DCNM installer, signature certificate, and signature verification script. Unzip the desired Cisco DCNM installer image ZIP file to a directory. Verify the image signature by following the steps in the README file. The installer from this package installs the Cisco DCNM software.

DCNM Open Virtual Appliance (OVA) Installer

This installer is available as an Open Virtual Appliance file (.ova). The installer contains a pre-installed OS, DCNM, and other applications needed for programmable fabric.

DCNM ISO Virtual Appliance (ISO) Installer

This installer is available as an ISO image file (.iso). The installer is a bundle of OS, DCNM, and other applications needed for dynamic fabric automation.

Deployment Options

You can deploy the Cisco DCNM installer in one of the following modes:

Standalone Server

All types of installers are packaged along with PostgreSQL database. The default installation steps for the respective installers result in this mode of deployment.

High Availability for Virtual Appliances

You can deploy the DCNM Virtual appliances, both OVA and ISO, in High Availability mode to have resilience in case of application or OS failures.

System Requirements for Cisco DCNM, Release 11.1(1)

**Note**

We recommend that you do not upgrade any underlying third-party software separately. All the necessary software components will be updated during the inline upgrade procedure. Upgrading the components outside of DCNM upgrade will cause performance issues.

Server Requirements

Cisco DCNM, Release 11.1(1), supports the Cisco DCNM Server on these 64-bit operating systems:

- **LAN Fabric and Classic LAN Deployments:**

- Open Virtual Appliance (OVA) with an integrated CentOS Linux release 7.6.1810 (Core)
- ISO Virtual Appliance (ISO) with an integrated CentOS Linux release 7.6.1810 (Core)

Cisco DCNM Release 11.1(1) supports the following databases:

- PostgreSQL 9.4.5



Note Cisco DCNM 11.1(1) for LAN is not supported with an external database.



Note The ISO/OVA installation only supports the embedded PostgreSQL database.



Note The Cisco DCNM database size is not limited, and increases according to the number of nodes and ports that the DCNM manages with Performance Manager Collections enabled. You cannot restrict the database size.

Cisco DCNM Release 11.1(1) supports the ISO installation on a bare-metal server (no hypervisor) on the following server platforms:¹

Server	Product ID (PID)	Recommended minimum memory, drive capacity, and CPU count
Cisco UCS C240M4	UCSC-C240-M4S	24G / 500G 8-vCPU Cores with Cisco hardware RAID Controller [UCSC-MRAID12G-1GB/2 GB] for the RAID operation (small)
Cisco UCS C240M4	UCSC-C240-M4L	32G / 500G 16-vCPU Cores with Cisco hardware RAID Controller [UCSC-MRAID12G- GB/2 GB] for the RAID operation (large)
Cisco UCS C240 M5S	UCSC-C240-M5SX	24G / 500G 8-vCPU Cores with Cisco hardware RAID Controller [UCSC-SAS-M5] for the RAID operation (small)
Cisco UCS C220 M5L	UCSC-C220-M5L	32G / 500G 16-vCPU Cores with Cisco hardware RAID Controller [UCSC-SAS-M5] for the RAID operation (small)

¹ Install the Cisco DCNM Compute node with 16vCPUs, 64G RAM, and 500GB hard disk. Ensure that you do not install the Compute node on 32G RAM server.



Note Cisco DCNM can work on an alternative computing hardware as well, despite Cisco is only testing on Cisco UCS.

Cisco DCNM Release 11.1(1) supports the running of the Cisco DCNM Server on the following hypervisors:

Table 1: VMware Snapshot Support for DCNM LAN Fabric and DCNM LAN Classic Deployments

VMware vSphere Hypervisor (ESXi)	6.0	6.5	6.7	6.7 update 1
VMware vCenter Server	6.0	6.5	6.7	6.7 update 1



Note Only Warm and Cold VMware snapshot is supported
vCenter server is mandatory to deploy the Cisco DCNM OVA Installer.

Server Resource Requirements

Table 2: Server Resource Requirements

Deployment	Deployment Type	Small (Lab or POC)	Large (Production)	Compute
LAN Fabric	• OVA	CPU: 8 vCPUs	CPU: 16 vCPUs	CPU: 16 vCPUs
Classic LAN	• ISO	RAM: 24 GB DISK: 500 GB	RAM: 32 GB DISK: 500 GB	RAM: 64 GB DISK: 500 GB



Note

- Small deployment scenario for Classic LAN and SAN—Fewer than 50 switches
- Small deployment scenario for LAN Fabric—Fewer than 15 switches

Supported Web Browsers

Cisco DCNM supports the following web browsers:

- Google Chrome version 71.0.3578.80
- Mozilla Firefox Version 63.0.3 (32/64 bit)
- Microsoft Internet Explorer 11.0.96 update version 11.0.90

Other Supported Software

The following table lists the other software that is supported by Cisco DCNM, Release 11.1(1).

Table 3: Other Supported Software

Component	Features
Security	<ul style="list-style-type: none">• ACS versions 4.0, 5.1, and 5.5• Telnet Disabled: SSH Version 1, SSH Version 2, Global Enforce SNMP Privacy Encryption.• Web Client Encryption: HTTPS with TLS 1, 1.1 and 1.2
OVA/ISO Installers	CentOS 7.6/Linux Kernel 3.10.x



CHAPTER 2

Guidelines and Limitations

- [Guidelines and Limitations, on page 7](#)

Guidelines and Limitations

The guidelines and limitations for installing and upgrading Cisco DCNM are as follows:

General Guidelines and Limitations

- Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application might not function properly:
 - It must be at least 8 characters long and contain at least one alphabet and one numeral.
 - It can contain a combination of alphabets, numerals, and special characters.
 - Do not use any of these special characters in the DCNM password: <SPACE> " & \$ % ' ^ = < > ; : ` \ | / , . *`
 - From Cisco DCNM Release 11.0(1), the characters that are allowed in the Administrative password is restricted for OVA and ISO installations. Therefore while upgrading, the old password used in DCNM 11.0(1) is not valid. However, different passwords are allowed during Upgrade.

The new Administrative password that is entered is used in the following scenarios.

—accessing the DCNM appliance via its console.

—accessing the appliance via SSH

—for applications running on the appliance, e.g. Postgres DBMS

However, after the upgrade, since Postgres DBMS is restored from the backup that is taken on DCNM 10.4(2), you must logon to the Cisco DCNM Web UI using the password used on DCNM Release 10.4(2) appliance.

- Do not interrupt the boot process (such as pressing the Ctrl+ALT + DELETE keys) when installing DCNM. If you interrupt, you must restart the installation process.
- Ensure that you configure the timezone after installation or upgrade, before performing any other operations on the Cisco DCNM Appliance. Use the NTP server for configuring timezones.

- To check the status of the running Postgres database in Native HA setup, use **pg_ctl** command. Do not use the **systemctl** command.
- Do not begin the password with Hash (#) symbol. Cisco DCNM considers the password as an encrypted text if it begins with # symbol.
- We recommend that you do not upgrade any underlying third-party software separately. All the necessary software components will be updated during the inline upgrade procedure. Upgrading the components outside of DCNM upgrade will cause performance issues.

Fresh Installation

- For Virtual Appliances (OVA/ISO), the installer installs the Operating system and Cisco DCNM components.
- The DCNM OVA cannot be deployed by connecting the vSphere client directly to the ESXi server.

Upgrade

- Ensure that you do not perform inline upgrade from an SSH session. The session may timeout and result in an incomplete upgrade.
- Disable Telemetry in the earlier release before you upgrade to Cisco DCNM Release 11.1(1).
- Disable Telemetry before you deploy Compute Nodes. You can enable Telemetry after deploying compute nodes.

For DCNM in Native HA mode, Telemetry is supported with 3 compute nodes only.

- Disable Telemetry before modifying Interface settings. You can enable Telemetry after modifying the settings.
- During a backup and restore process, the compute nodes are also included in the backup. After you deploy the new compute, you can restore the backup on the compute node.

If there was no backup, disconnect the 3 compute nodes, and erase the data on all the compute nodes. On the Cisco DCNM Web Client UI, navigate to **Application > Compute**. Select the + icon to join the compute nodes.

- To erase data on the compute node, logon to the compute node through an SSH session and erase the data using the **rm -rf /var/afw/vols/data** command.



Note You must run the above command separately on all compute nodes to erase data.



CHAPTER 3

Prerequisites

This chapter provides release-specific prerequisites information for your deployment of *Cisco Data Center Network Manager*.

- [Prerequisites for DCNM Open Virtual Appliance, on page 9](#)
- [Prerequisites for DCNM ISO Virtual Appliance, on page 10](#)
- [Prerequisites for Cisco DCNM Virtual Appliance HA, on page 10](#)

Prerequisites for DCNM Open Virtual Appliance

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

- VMware vCenter Server that is running on a Windows server (or alternatively, running as a virtual appliance).
- VMware ESXi host imported into vCenter.
- Three port groups on the ESXi host—DCNM Management Network, Enhanced Fabric Management Network, and InBand interface for EPL and Telemetry features.
- Determine the number of switches in your Cisco Programmable Fabric that will be managed by the Cisco DCNM Open Virtual Appliance.
- Ensure that no anti-virus software (such as McAfee) is running on the host where the VMware vCenter web client is launched for the DCNM OVA installation. If the anti-virus software is running, the DCNM installation might fail.
- The DCNM Open Virtual Appliance is compatible to be deployed in ESXi host as well. For deploying in the ESXi host, VMware vSphere Client application is mandatory.
- To upgrade from Release 10.4(2) to 11.1(1), you must download the **DCNMUpgradeTool**.



Note For more information about the CPU and memory requirements, see the *Server Resource Requirements* section of the Cisco DCNM Release Notes, Release 11.1(1).

Prerequisites for DCNM ISO Virtual Appliance

Ensure that you do not add an additional Active or Standby node to an existing Active-Standby Native HA DCNM Appliance. The installation fails.

You have to set up the host or the hypervisor before you install the Cisco DCNM ISO Virtual Appliance. Based on the requirement, set up the setup Host machine or Hypervisor based on CPU and Memory requirement.

To upgrade from Release 10.4(2) to 11.1(1), you must download the **DCNMUpgradeTool**.



Note For more information about the CPU and memory requirements, see the *Server Resource Requirements* section of the *Cisco DCNM Release Notes*.

You can set up one of the following hosts to install the DCNM ISO Virtual Appliance.

VMware ESXi

The host machine is installed with ESXi and two port groups are created—one for EFM network and the other for DCNM Management network. Enhanced Fabric In-Band network is optional.

Kernel-based Virtual Machine (KVM)

The host machine is installed with Red Hat Enterprise Linux (RHEL) 5.x or 6.x or 7.x, with KVM libraries and Graphical User Interface (GUI) access. The GUI allows you to access the Virtual Machine Manager, to deploy and manage the Cisco DCNM Virtual Appliances. Two networks are created—EFM network and DCNM Management network. Typically, the DCNM management network is bridged to gain access from other subnets. Refer the KVM documentation on how to create different types of networks.



Note KVM on other platforms like CentOS or Ubuntu will not be supported as it increases the compatibility matrix.

Prerequisites for Cisco DCNM Virtual Appliance HA

This section contains the following topics that describe the prerequisites for obtaining a high-availability (HA) environment.

Deploying Cisco DCNM Virtual Appliances in HA mode

You must deploy two standalone Virtual Appliance (OVA and ISO). When you deploy both Virtual Appliances, you must meet the following criteria:

- The eth0 of the active OVA must be in the same subnet as eth0 of the standby Virtual Appliance. The eth1 of the active Virtual Appliance must be in the same subnet as eth1 of the standby OVA. The eth2 of the active virtual appliance must be in the same subnet as the eth2 of the standby appliance.
- Both Virtual Appliances must be deployed with the same administrative password. This process ensures that both Virtual Appliances are duplicates of each other.

- If you try to add an additional Active or Standby node to an existing Active-Standby Native HA DCNM Appliance, the installation fails.

Availability of Virtual IP Addresses

Two free IP addresses are needed to set up the server eth0 and eth1 interfaces. However, eth2 IP address is optional. The first IP address will be used in the management access network; it should be in the same subnet as the management access (eth0) interface of the OVAs. The second IP address should be in the same subnet as enhanced fabric management (eth1) interfaces (switch/POAP management network).

If you choose to configure inband management (eth2) for the DCNM Server, you must reserve another IP Address. For Native HA setup, the eth2 interface on Primary and Secondary servers must be in same subnet.

Installing an NTP Server

For most of the HA functionality to work, you must synchronize the time on both OVAs by using an NTP server. The installation would typically be in the management access network (eth0) interfaces.



CHAPTER 4

Installing the Cisco DCNM

This chapter contains the following sections:

- [Installing DCNM on Open Virtual Appliance, on page 13](#)
- [Installing DCNM on ISO Virtual Appliance, on page 26](#)
- [Installing Cisco DCNM SE ISO on Cisco APIC SE, on page 40](#)
- [Installing Cisco DCNM Compute Node, on page 42](#)

Installing DCNM on Open Virtual Appliance

This chapter contains the following sections:

Downloading the Open Virtual Appliance File

The first step to install the Open Virtual Appliance is to download the `dcnm.ova` file. 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.

Procedure

- Step 1** Go to the following site: <http://software.cisco.com/download/>.
- Step 2** In the Select a Product search box, enter **Cisco Data Center Network Manager**.
Click **Search** icon.
- Step 3** Click **Data Center Network Manager** from the search results.
A list of the latest release software for Cisco DCNM available for download is displayed.
- Step 4** In the Latest Releases list, choose Release 11.1(1).
- Step 5** Locate the DCNM Open Virtual Appliance Installer and click the **Download** icon.

- Step 6** Save the `dcnm.ova` file to your directory that is easy to find when you start to deploy the OVF template.
-

Deploying the Open Virtual Appliance as an OVF Template

After you download the Open Virtual Appliance file, you must deploy the OVF template from the vSphere Client application or the vCenter Server.



Note Deploy two OVAs for the HA setup.

Procedure

- Step 1** Open the vCenter Server application and connect to the vCenter Server with your vCenter user credentials.

Note ESXi host must be added to the vCenter Server application.

Depending on the version of the VMware vSphere web HTML5 interface may not work properly when deploying Huge or Compute OVA, as it does not allow users to specify extra disk size. Therefore, we recommend that you use Flex interface for deploying VMs.

If you're deploying OVF template using the ESXi 6.7, the installation fails if you use Internet Explorer browser with HTML5. Ensure that you one of the following options to successfully deploy OVF template with ESXi and 6.7:

- Mozilla Firefox browser, with HTML 5 support
Use flex interface if HTML 5 is not supported
- Mozilla Firefox browser, with flex\flash support
- Google Chrome browser, with HTML 5 support
Use flex interface if HTML 5 is not supported

- Step 2** Navigate to **Home > Inventory > Hosts and Clusters** and choose the host on which the OVF template is deployed.

- Step 3** On the correct Host, right-click and select **Deploy OVF Template**.

You can also choose **Actions > Deploy OVF Template**.

Deploy OVF Template Wizard opens.

- Step 4** On the Select template screen, navigate to the location where you have downloaded the OVA image.

You can choose the OVA file by one of the following methods:

- Select the **URL** radio button. Enter the path of the location of the image file.
- Select **Local File** radio button. Click **Browse**. Navigate to the directory where the image is stored. Click **OK**.

Click **Next**.

- Step 5** Verify the OVA template details and click **Next**.
- Step 6** On the End User License Agreement screen, read the license agreement.
Click **Accept** and click **Next**.
- Step 7** On the Select name and location screen, enter the following information:
- In the Name field, enter an appropriate name for the OVF.
Note Ensure that the VM name is unique within the Inventory.
 - In the Browse tab, select **Datacenter** as the deployment location under the appropriate ESXi host.
- Click **Next**.
- Step 8** On the Select configuration screen, select the configuration from the drop-down list.
- Choose **Small** (Lab or POC) to configure the virtual machine with 8 vCPUs, 24GB RAM.
Choose Small for proof-of-concept and other small-scale environments with fewer than 50 switches that are not expected to grow with time.
 - Choose **Large** (Production) to configure the virtual machine with 16 vCPUs, 32GB RAM.
We recommend that you use a Large deployment configuration when you are managing more than 50 devices to leverage better RAM, heap memory, and CPUs. For setups that could grow, choose Large.
 - Choose **Huge** to configure the virtual machine with 32 vCPUs, 128GB RAM.
- Click **Next**.
- Step 9** On **Select a resource** screen, select the host on which you want to deploy the OVA template.
Click **Next**.
- Step 10** On **Select storage** screen, based on the Datastore and Available space choose the disk format and the destination storage for the virtual machine file.
- a) Select the virtual disk format from the drop-down list.
- The available disk formats are:
- Note** 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 later on first write from the virtual disk.
 - **Thin Provision:** The disk space available is less than 100 GB. The initial disk consumption is 3GB and increases as the size of the database increases with the number of devices being managed.
 - **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.
- Note** With 500G, the DCNM installation will appear to be stuck with option Thick Provision Eager Zeroed. However, it takes longer time to complete.
- b) Select the VM storage policy from the drop-down list.

By default, no policy is selected.

- c) Check the **Show datastores from Storage DRS clusters** to view the clusters' datastores.
- d) Select the destination storage for the virtual machine, available in the datastore.

Click **Next**.

Step 11 On the Select Networks screen, map the networks that are used in the OVF template to networks in your inventory.

- **dcnm-mgmt network**

This network provides connectivity (SSH, SCP, HTTP, HTTPS) to the Cisco DCNM Open Virtual Appliance. Associate this network with the portgroup that corresponds to the subnet that is associated with the DCNM Management network.

- **enhanced-fabric-mgmt**

This network provides enhanced fabric management of Nexus switches. You must associate this network with the port group that corresponds to management network of leaf and spine switches.

- **enhanced-fabric-inband**

This network provides in-band connection to the fabric. You must associate this network with port group that corresponds to a fabric in-band connection.

Note If you do not configure enhanced-fabric-inband network, Endpoint Locator and Telemetry features are not operational.

However, you can configure the network after installation, if required. For more information, see [Configuring Enhanced-Fabric-Inband Interface \(eth2\) Post DCNM Installation, on page 92](#).

From the Destination Network drop-down list, choose to associate the network mapping with the port group that corresponds to the subnet that is associated with the corresponding network.

If you are deploying more than one DCNM Open Virtual Appliance for HA functionality, you must meet the following criteria:

- Both OVAs must have their management access (eth0), enhanced fabric management (eth1) and inband management (eth2) interfaces in the same subnet.
- Each OVA must have their eth0-eth1 and eth2 interfaces in different subnets.
- Both OVAs must be deployed with the same administrative password. This is to ensure that both OVAs are duplicates of each other for application access.

Do not use the following characters in your password: <SPACE> " & \$ % ' ^ = < > ; : ` \ | / , . *

Click **Next**.

Step 12 On **Customize template** screen, enter the Management Properties information.

Enter the **IP Address** (for the outside management address for DCNM), **Subnet Mask**, and **Default Gateway**.

Note During Native HA installation and upgrade, ensure that you provide appropriate Management Properties for both Active and Standby appliances.

Click **Next**.

Step 13 On **Ready to Complete** screen, review the deployment settings.

Click **Back** to go to the previous screens and modify the configuration.

Click **Finish** to deploy the OVF template.

You can see the deployment status in the Recent Tasks area on the vSphere Client.

Note If this deployment is a part of the upgrade process, do not Power on the VM. Edit and provide the 11.0(1) MAC address and power on the VM.

Step 14 After the installation is complete, right click on the installed VM and select **Power > Power On**.

Note Before you power on the VM, ensure that you have reserved appropriate resources for the VM, such as CPU and memory, based on the chosen deployment configuration.

You can see the status in the Recent Tasks area.

Step 15 Navigate to the Summary tab and click **Settings** icon and select **Launch Web Console**.

A message indicating that the DCNM appliance is configuring appears on the screen.

```
*****
Please point your web browser to
http://<IP-address>:<port-number>
to complete the application
*****
```

Copy and paste the URL to the browser to complete the installation, using the Web Installer.

What to do next

The DCNM installer creates a _deviceImage-0.iso in the DCNM VM folder and mounts the ISO permanently to the VM. If this ISO is removed or the CD/DVD is disconnected, the VM will not boot. The VM will enter Emergency Mode and prompt you with the message: Give root password for maintenance. If the VM is down, CD/DVD drive can be disconnected. However, after you power it up again, the VM will enter Emergency Mode and provide a prompt.

You can choose to install DCNM in Standalone mode or Native HA mode. Refer to [Installing Cisco DCNM ISO in Standalone Mode, on page 32](#) or [Installing the Cisco DCNM ISO in Native HA mode, on page 34](#) for more information.

Installing the Cisco DCNM OVA in Standalone Mode

Paste the URL displayed on the Console tab and hit Enter key. A welcome message appears.

To complete the installation of Cisco DCNM from the web installer, perform the following procedure.

Procedure

Step 1 On **Welcome to Cisco DCNM** screen, click **Get Started**.

Step 2 On **Cisco DCNM Installer** screen, select **Fresh Installation – Standalone** radio button.

Click **Continue**.

Step 3 On **Administration** tab, enter the password that is used to connect to all the applications in the Cisco DCNM Open Virtual Appliance.

Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application may not function properly.

- It must be at least eight characters long and contain at least one alphabet and one numeral.
- It can contain a combination of alphabets, numerals, and special characters.
- Do not use any of these special characters in the DCNM password for all platforms:
<SPACE> " & \$ % ' ^ = < > ; : ` \ | / , . *

Select the **Show passwords in clear text** checkbox to view the password you have typed.

Click **Next**.

Step 4 In **Install Mode** tab, from the drop-down list, choose **LAN Fabric** installation mode for the OVA DCNM Appliance.

Click **Next**.

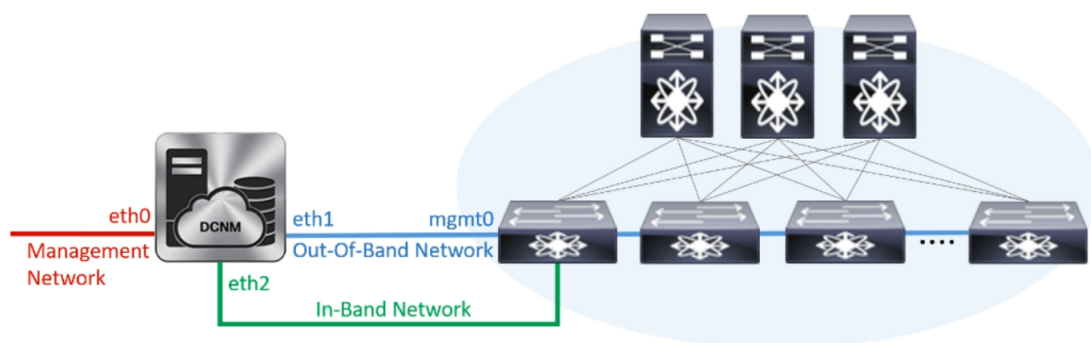
Step 5 On the **System Settings** tab, configure the settings for the DCNM Appliance.

- In the Fully Qualified Hostname field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.
- In the DNS Server Address field, enter the DNS IP address.
- In the NTP Server field, enter the IP address of the NTP server.
The value must be an IP address or RFC 1123 compliant name.

Click **Next**.

Step 6 On **Network Settings** tab, configure the network parameters.

Figure 1: Cisco DCNM Management Network Interfaces



a) In **Management Network** area, verify if the auto-populated IP Address and Default Gateway address are correct. Modify, if necessary.

(Optional) Enter a valid IPv6 address along with the prefix to configure the Management address and the Management Network Default IPv6 Gateway.

b) In **Out-of-Band Network** area, enter the IP address, gateway IP Address, and DNS server address. If DCNM is on the IPv6 network, configure the network with an IPv6 Address.

Out-of-band management provides a connection to the device management ports (Typically mgmt0).

Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

- c) In **In-Band Network** area, enter the IP Address and gateway IP Address for the in-band network.

The In-Band Network provides reachability to the devices via the front-panel ports.

Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

However, you can configure the in-band network after installation, if necessary. For more information, see [Configuring Enhanced-Fabric-Inband Interface \(eth2\) Post DCNM Installation, on page 92](#).

Note To modify the already configured in-band network (eth2 interface), execute the **ifconfig eth2 0.0.0.0** command and run the **appmgr setup inband** command again. Refer to [Configuring Enhanced-Fabric-Inband Interface \(eth2\) Post DCNM Installation, on page 92](#) to run the **appmgr setup inband** command.

Click **Next**.

Step 7 On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM Installation for the chosen deployment mode.

A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A success message appears with the URL to access DCNM Web UI.

```
*****
Your Cisco Data Center Network Manager software has been installed.
DCNM Web UI is available at
https://<<IP Address>>
You will be redirected there in 60 seconds.
Thank you
*****
```

Note If the Cisco DCNM is running behind a firewall, ensure that you open the port 2443 to launch Cisco DCNM Web UI.

Note If you try to access the DCNM Web UI using the Management IP address while the installation is still in progress, an error message appears on the console.

```
*****
*Preparing Appliance*
*****
```

What to do next

Log on to the DCNM Web UI with appropriate credentials.

Click the **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

If you have configured inband management (eth2) IP addresses for device management, login to standalone server and configure the inband network reachability from eth2 of the server to the switches by using the following commands:

```
dcnm# appmgr setup inband-route --subnet switches-fabric-links-IP-subnet/mask
dcnm# appmgr setup inband-route --subnet switch-loopback-IP-subnet>/mask
```

For example: If you have four switches with all fabric links connected through 10.0.0.x/30 subnet, and if all switches are configured with the loopback interface for inband reachability in subnet 40.1.1.0/24, use the following commands:

```
dcnm# appmgr setup inband-route --subnet 10.0.0.0/24
dcnm# appmgr setup inband-route --subnet 40.1.1.0/24
```

Installing the Cisco DCNM OVA in Native HA mode

The native HA is supported on DCNM appliances with ISO or OVA installation only.

By default, an embedded PostgreSQL database engine with the Cisco DCNM. The native HA feature allows two Cisco DCNM appliances to run as active and standby applications, with their embedded databases synchronized in real time. Therefore, when the active DCNM is not functioning, the standby DCNM takes over with the same database data and resume the operation.

Perform the following task to set up Native HA for DCNM.

Procedure

-
- Step 1** Deploy two DCNM Virtual Appliances (either OVA or ISO).
For example, let us indicate them as **dcnm1** and **dcnm2**.
- Step 2** Configure **dcnm1** as the Primary node. Paste the URL displayed on the Console tab of **dcnm1** and press **Enter** key.
- A welcome message appears.
- On the Welcome to Cisco DCNM screen, click **Get Started**.
 - On the Cisco DCNM Installer screen, select **Fresh Installation - HA Primary** radio button, to install **dcnm1** as Primary node.
Click **Continue**.
 - On the Administration tab, enter the password that is used to connect to all the applications in the Cisco DCNM Open Virtual Appliance.
Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application may not function properly.
 - It must be at least eight characters long and contain at least one alphabet and one numeral.
 - It can contain a combination of alphabets, numerals, and special characters.
 - Do not use any of these special characters in the DCNM password for Linux, Windows, OVA, and ISO platforms:
<SPACE> " & \$ % ' ^ = < > ; : ` \ | / , . *

Select the **Show passwords in clear text** checkbox to view the password you have typed.

Click **Next**.

- d) In the Install Mode tab, from the drop-down list, choose **LAN Fabric** installation mode for the DCNM Appliance.

Click **Next**.

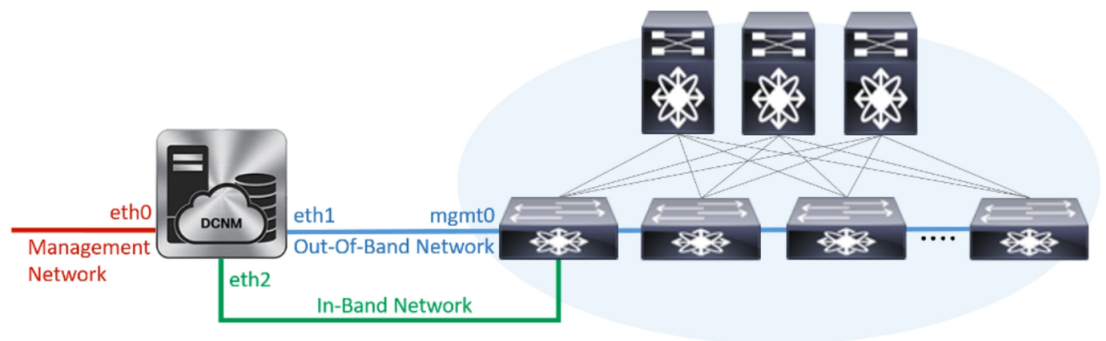
- e) On the System Settings, configure the settings for the DCNM Appliance.

- In the Fully Qualified Hostname field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.
- In the DNS Server Address field, enter the DNS IP address.
- In the NTP Server field, enter the IP address of the NTP server.
The value must be an IP address or RFC 1123 compliant name.

Click **Next**.

- f) On the **Network Settings** tab, configure the network parameters.

Figure 2: Cisco DCNM Management Network Interfaces



- In the Management Network area, verify if the auto-populated IP Address and Default gateway address are correct. Modify, if necessary.

(Optionally) Enter a valid IPv6 address along with the prefix to configure the Management address and the Management Network Default IPv6 Gateway.

- In the Out-of-Band Network area, enter the IP address, gateway IP Address, and DNS server address. If DCNM is on the IPv6 network, configure the network with an IPv6 Address.

Out-of-band management provides a connection to the device management ports (Typically mgmt0).

- In the In-Band Network area, enter the VIP Address and gateway IP Address for the in-band network. The In-Band Network provides reachability to the devices via the front-panel ports.

Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

However, you can configure the in-band network after installation, if necessary. For more information, see [Configuring Enhanced-Fabric-Inband Interface \(eth2\) Post DCNM Installation, on page 92](#).

Note To modify the already configured in-band network (eth2 interface), execute the **ifconfig eth2 0.0.0.0** command and run the **appmgr setup inband** command again. Refer to [Configuring Enhanced-Fabric-Inband Interface \(eth2\) Post DCNM Installation, on page 92](#) to run the **appmgr setup inband** command

Click **Next**.

- g) On the HA Settings tab, a confirmation message appears.

```
You are installing the primary DCNM HA node.
Please note that HA setup information will need to
be provided when the secondary DCNM HA node is
installed.
```

Click **Next**.

- h) On the **Applications** tab, in the IPv4 Subnet field, enter the IP subnet to access the applications that run internally to DCNM.

All the applications use the IP Address from this subnet.

The Cluster Mode configuration area appears only if you have selected the Enable Clustered Mode checkbox in Step 2.d, on page 21.

Note In Clustered mode, the Cisco DCNM Applications run on separate DCNM Compute Nodes.

1. In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the out-of-band IPv4 network to be used in the Clustered Mode.

The address must be a smaller prefix of available IP addresses from the eth1 subnet. For example: Use 10.1.1.240/28 if the eth1 subnet was configured as 10.1.1.0/24 during installation.

This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

2. In the **Out-of-Band IPv6 Network Address Pool**, enter the address pool from the out-of-band IPv6 network to be used in the Clustered Mode. The address pool must be an IPv6 subnet.

3. In the **In-Band IPv4 Network Address Pool**, enter the address pool from the out-of-band IPv4 network to be used in the Clustered Mode.

The address must be a smaller prefix of available IP addresses eth2 subnet. For example: Use 11.1.1.240/28 if the eth2 subnet was configured as 11.1.1.0/24 during installation.

This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

4. In the **In-Band IPv6 Network Address Pool**, enter the address pool from the in-band IPv6 network to be used in the Clustered Mode. The address pool must be an IPv6 subnet.

Click **Next**.

- i) On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM Installation for the chosen deployment mode.

A progress bar appears to show the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A warning message appears stating that the setup is not complete until you install the Secondary node.

```
WARNING: DCNM HA SETUP IS NOT COMPLETE!  
Your Cisco Data Center Network Manager software has been installed on  
this HA primary node.  
However, the system will be ready to be used only after installation  
of the secondary node has been completed.  
Thank you.
```

Step 3 Configure **dcnm2** as the Secondary node. Paste the URL displayed on the Console tab of **dcnm2** and hit Enter.

A welcome message appears.

- a) On the Welcome to Cisco DCNM screen, click **Get Started**.
- b) On the Cisco DCNM Installer screen, select **Fresh Installation - HA Secondary** radio button, to install **dcnm2** as Secondary node.

Click **Continue**.

- c) On the Administration tab, enter the password that is used to connect to all the applications in the Cisco DCNM Open Virtual Appliance.

Note The password for the secondary node must be the same as the Administrative password for primary, as entered in Step 2.c, on page 20.

Click **Next**.

- d) In the Install Mode tab, from the drop-down list, choose the same installation mode that you selected for the Primary node.

Note The HA installation fails if you do not choose the same installation mode as Primary node.

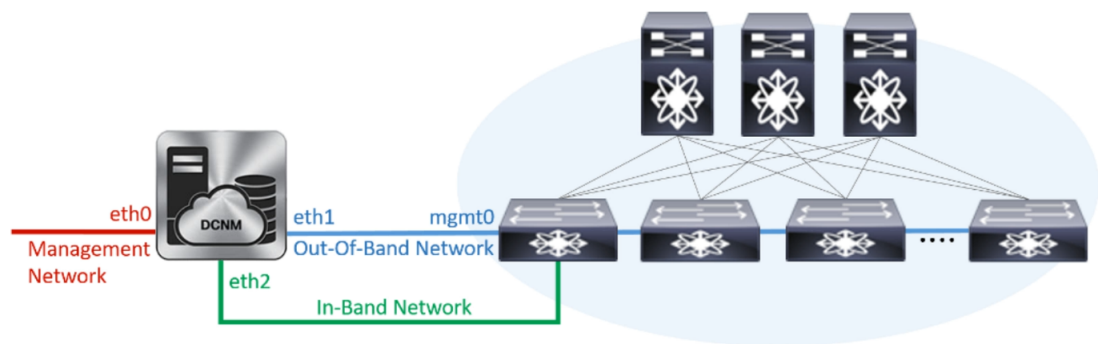
Click **Next**.

- e) On the System Settings, configure the settings for the DCNM Appliance.
 - In the Fully Qualified Hostname field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.
 - In the DNS Server Address field, enter the DNS IP address.
 - In the NTP Server field, enter the IP address of the NTP server.
The value must be an IP address or RFC 1123 compliant name.

Click **Next**.

- f) On the Network Settings tab, configure the network parameters.

Figure 3: Cisco DCNM Management Network Interfaces



- In the Management Network area, verify the auto-populated IP Address and Default gateway address are correct. Modify, if necessary.

Note Ensure that the IP Address belongs to the same Management Network as configured on the Primary node for HA setup to complete successfully.

(Optionally) Enter a valid IPv6 address along with the prefix to configure the Management address and the Management Network Default IPv6 Gateway.

- In the Out-of-Band Network area, enter the IP address, gateway IP Address, and DNS server address. If DCNM is on the IPv6 network, configure the network with an IPv6 Address.

Out-of-band management provides a connection to the device management ports (Typically mgmt0).

Note Ensure that the IP Address, IP address gateway, and the IPv6 address belong to the same Out-of-Band Network as configured on the Primary node for HA setup to complete successfully.

You can also configure an IPv6 address for out-of-band management network.

- In the In-Band Network area, enter the IP Address and gateway IP Address for the in-band network. The In-Band Network provides reachability to the devices via the front-panel ports.

Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

However, you can configure the in-band network after installation, if necessary. For more information, see [Configuring Enhanced-Fabric-Inband Interface \(eth2\) Post DCNM Installation](#), on page 92.

Click **Next**.

- g) On the HA Settings tab, configure the system settings..
- In the Management IP Address of primary DCNM node field, enter the appropriate IP Address to access the DCNM UI.
 - In the VIP Fully qualified Host Name field, enter hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.
 - Enter the Management Network VIP address, and OOB Network VIP address appropriately.
 - Enter OOB Network VIPv6 Address to configure IPv6 address for VIP.

- In the In-Band Network area, enter the VIP Address for the in-band network.

This is the VIP address for the In-Band network. This field is mandatory if you have provided an IP address for In-Band network in the Network Settings tab.

- Enter the HA ping IP address if necessary.

HA_PING_ADDRESS, must be different from the DCNM Active and Standby addresses.

You must configure the HA ping IP Address to avoid the Split Brain scenario. This address must belong to Enhanced Fabric management network.

Click **Next**.

- h) On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM OVA Installation for the chosen deployment mode.

A progress bar appears to show the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A success message appears with the URL to access DCNM Web UI.

```
*****
Your Cisco Data Center Network Manager software has been installed.
DCNM Web UI is available at
https://<<IP Address>>
You will be redirected there in 60 seconds.
Thank you
*****
```

Note If the Cisco DCNM is running behind a firewall, ensure that you open the port 2443 to launch Cisco DCNM Web UI.

What to do next

Log on to the DCNM Web UI with appropriate credentials.

Click the **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

If you have configured inband management (eth2) IP addresses for device management, login to standalone server and configure the inband network reachability from eth2 of the server to the switches by using the following commands:

```
dcnm# appmgr setup inband-route --subnet switches-fabric-links-IP-subnet/mask
dcnm# appmgr setup inband-route --subnet switch-loopback-IP-subnet>/mask
```

For example: If you have four switches with all fabric links connected through 10.0.0.x/30 subnet, and if all switches are configured with the loopback interface for inband reachability in subnet 40.1.1.0/24, use the following commands:

```
dcnm# appmgr setup inband-route --subnet 10.0.0.0/24
dcnm# appmgr setup inband-route --subnet 40.1.1.0/24
```

Installing DCNM on ISO Virtual Appliance

This chapter contains the following sections:



Note The screenshots in this section may change in your setup based on how you are booting the ISO; you will either see the blue (BIOS) screen or the black (UEFI) screen.

Downloading the ISO Virtual Appliance File

The first step to installing the ISO Virtual Appliance is to download the `dcnm.iso` file. You must point to that `dcnm.iso` file on your computer when preparing the server for installing DCNM.



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

Procedure

- Step 1** Go to the following site: <http://software.cisco.com/download/>.
 - Step 2** In the Select a Product search box, enter Cisco Data Center Network Manager.
Click on Search icon.
 - Step 3** Click on **Data Center Network Manager** from the search results.
A list of the latest release software for Cisco DCNM available for download is displayed.
 - Step 4** In the Latest Releases list, choose Release 11.1(1).
 - Step 5** Locate the DCNM ISO Virtual Appliance Installer and click the **Download** icon.
 - Step 6** Locate the DCNM VM templates at DCNM Virtual Appliance definition files for VMWare (.ovf) and KVM (domain XMLs) environment and click **Download**.
 - Step 7** Save the `dcnm.iso` file to your directory that will be easy to find when you being the installation.
-

What to do next

You can choose to install DCNM On KVM or Baremetal servers. Refer to [Installing the DCNM ISO Virtual Appliance on KVM, on page 30](#) or [Installing the DCNM ISO Virtual Appliance on UCS \(Bare Metal\), on page 26](#) for more information.

Installing the DCNM ISO Virtual Appliance on UCS (Bare Metal)

Perform the following tasks to install the DCNM ISO virtual appliance on UCS.

Procedure

- Step 1** Launch Cisco Integrated Management Controller (CIMC).
- Step 2** Click the **Launch KVM** button.
- You can either launch Java-based KVM or HTML-based KVM.
- Step 3** Click the URL displayed on the window to continue loading the KVM client application.
- Step 4** On the Menu bar, click **Virtual Media > Activate Virtual Devices**.
- Step 5** Click **Virtual Media** and choose one of the following mediums to browse and upload DCNM ISO images from the following:
- Map CD/DVD
 - Map Removable Disk
 - Map Floppy Disk
- Navigate to the location where the ISO image is located and load the ISO image.
- Step 6** Select **Power > Reset System (warm boot)** and Ok to continue and restart the UCS box.
- Step 7** Press **F6** interrupt the reboot process when the server starts to select a boot device. The boot selection menu appears.
- For more information about using the UCS KVM Console window, see the Cisco UCS Server Configuration Utility, Release 3.1 User Guide at the following URL:
- https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/ucsscu/user/guide/31/UCS_SCU/booting.html#wp1078073
- Step 8** Use the arrow keys to select Cisco Virtual CD/DVD and press **Enter**. The server boots with the DCNM ISO image from the mapped location.
- Note** The following image highlights UEFI installation. However, you can also choose **Cisco vKVM-Mapped vDVD1.22** for BIOS installation. ISO can be booted in both modes, BIOS, and UEFI.
- UEFI is mandatory for a system with minimum of 2TB disks.

```
Please select boot device:

CentOS
UEFI: Built-in EFI Shell
UEFI: IP4 0100 Intel(R) I350 Gigabit Network Connection
UEFI: IP4 0101 Intel(R) I350 Gigabit Network Connection
UEFI: Cisco vKVM-Mapped vDVD1.22
Cisco vKVM-Mapped vDVD1.22
Cisco vKVM-Mapped vHDD1.22
Cisco vKVM-Mapped vFDD1.22
Cisco CIMC-Mapped vDVD1.22
Cisco CIMC-Mapped vHDD1.22
Enter Setup

↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults
```

For Cisco UCS with the disk size of 2TB or higher and with 4K sector size drivers, the UEFI boot option is required. For more information, see [UEFI Boot Mode](#).

- Step 9** Select **Install Cisco Data Center Network Manager** using the up or down arrow keys. Press **Enter**.
The option shown in the following image appears when the ISO image is booted with UEFI.

```

Boot existing Cisco Data Center Network Manager
Install Cisco Data Center Network Manager
Rescue Cisco Data Center Network Manager

```

```

Use the ▲ and ▼ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.

```

Step 10 On the Cisco Management Network Management screen, select the interface for the networks. The list of available interfaces is displayed on the screen.

Choose the Management Interface (eth0) and Out-of-Band interface (eth1) from the Network Interface List. You can also configure the in-band interface (eth2) if necessary.

```

*****
Cisco Data Center Network Management
*****

Network Interface List
-----
1) 0b:00.0 Cisco Systems Inc VIC Ethernet NIC (rev a2)
   Address: 70:69:5a:f9:5e:19   Link:UP
2) 0c:00.0 Cisco Systems Inc VIC Ethernet NIC (rev a2)
   Address: 70:69:5a:f9:5e:1a   Link:DOWN
3) 01:00.0 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: 00:be:75:49:c2:86   Link:UP
4) 01:00.1 Intel Corporation I350 Gigabit Network Connection (rev 01)
   Address: 00:be:75:49:c2:87   Link:UP

Please select the interfaces to use from the list above:
Management Interface (eth0) : 3
Out-Of-Band Interface (eth1) : 4

Configure In-Band Interface (eth2)? [y/n]: y
In-Band Interface (eth2) : 1

```

Note If you do not configure In-Band interface, Endpoint Locator and Telemetry features are not operational.

However, you can configure the network after installation, if required. For more information, see [Configuring Enhanced-Fabric-Inband Interface \(eth2\) Post DCNM Installation, on page 92](#).

- Step 11** Review the selected interfaces. Press **y** to confirm and continue with the installation.
- Step 12** Configure the Management Network for Cisco DCNM. Enter the IP address, Subnet Mask, and Gateway. Press **y** to continue with the installation.
- After the installation is complete, the system reboots and a message indicating that the DCNM appliance is configuring appears on the screen.

```
*****
Please point your web browser to
http://<IP-address>:<port-number>
to complete the application
*****
```

Copy and paste the URL to the browser to complete the installation using the Web Installer.

What to do next

You can choose to install DCNM in Standalone mode or Native HA mode. Refer to [Installing Cisco DCNM ISO in Standalone Mode, on page 32](#) or [Installing the Cisco DCNM ISO in Native HA mode, on page 34](#) for more information.

Installing the DCNM ISO Virtual Appliance on KVM

Perform the following tasks to install the ISO virtual appliance on KVM.

Procedure

- Step 1** Unzip and extract **dcnm-va-ovf-kvm-files.11.1.1.zip** and locate the **dcnm-kvm-vm.xml** file.
- Step 2** Upload this file on the RHEL server that is running KVM to the same location as the ISO.
- Step 3** Connect to the RHEL server running KVM via SCP File transfer terminal.
- Step 4** Upload the **dcnm-va.11.1.1.iso** and **dcnm-kvm-vm.xml** to the RHEL server.
- Step 5** Close the file transfer session.
- Step 6** Connect to the RHEL server running KVM via SSH terminal.
- Step 7** Navigate to the location where both the ISO and domain XMLs is downloaded.
- Step 8** Create the VM (or Domains, as they are known in the KVM terminology) using the **virsh** command.

need info on dcnm-kvm-vm-huge.xml

```
sudo virsh define [{dcnm-kvm-vm-huge.xml | dcnm-kvm-vm-compute.xml |
dcnm-kvm-vm-large.xml | dcnm-kvm-vm-small.xml}]
```

- Step 9** Enable a VNC server and open the required firewall ports.
- Step 10** Close the SSH session.
- Step 11** Connect to the RHEL server running KVM via a VNC terminal.
- Step 12** Navigate to **Applications > System Tools > Virtual Machine Manager (VMM)**.
- A VM is created in the Virtual Machine Manager.

Step 13 From Virtual Machine Manager, edit the VM by selecting the VM in the listing. Click **Edit > Virtual Machine Details > Show virtual hardware details**.

Step 14 In the Virtual Hardware Details, navigate to **Add Hardware > Storage**.

Step 15 Create a hard disk with Device type with the following specifications:

- device type: IDE disk
- cache-mode: default
- storage format: raw

We recommend that you use storage size of 500GB.

Step 16 Select IDE CDROM on the edit window of the Virtual Machine and click **Connect**.

Step 17 Navigate to dcnm-va.iso and click **OK**.

Step 18 Select both the NICs and assign appropriate networks that are created.

Step 19 Power on the Virtual Machine.

Note Before you power on the VM, ensure that you have reserved appropriate resources for the VM, such as CPU and memory, based on the chosen deployment configuration.

The operating system is installed.

Step 20 On the Cisco Management Network Management screen, select the interface for the networks. The list of available interfaces is displayed on the screen.

Choose the Management Interface (eth0) and Out-of-Band interface (eth1) from the Network Interface List. You can also configure in-band interface (eth2) if necessary.

Note If you do not configure in-band interface (eth2), Endpoint Locator and Telemetry features are not operational.

However, you can configure the network after installation, if required. For more information, see [Configuring Enhanced-Fabric-Inband Interface \(eth2\) Post DCNM Installation, on page 92](#).

Step 21 Press **y** to confirm and continue with the installation.

Step 22 Configure the Management Network. Enter the IP address, Subnet Mask, and Gateway. Press **y** to continue with the installation.

After the installation is complete, the system reboots and a message indicating that the DCNM appliance is configuring appears on the screen.

```
*****
Please point your web browser to
http://<IP-address>:<port-number>
to complete the application
*****
```

Copy and paste the URL to the browser to complete the installation using the Web Installer.

What to do next

You can choose to install DCNM in Standalone mode or Native HA mode. Refer to [Installing Cisco DCNM ISO in Standalone Mode, on page 32](#) or [Installing the Cisco DCNM ISO in Native HA mode, on page 34](#) for more information.

Installing Cisco DCNM ISO in Standalone Mode

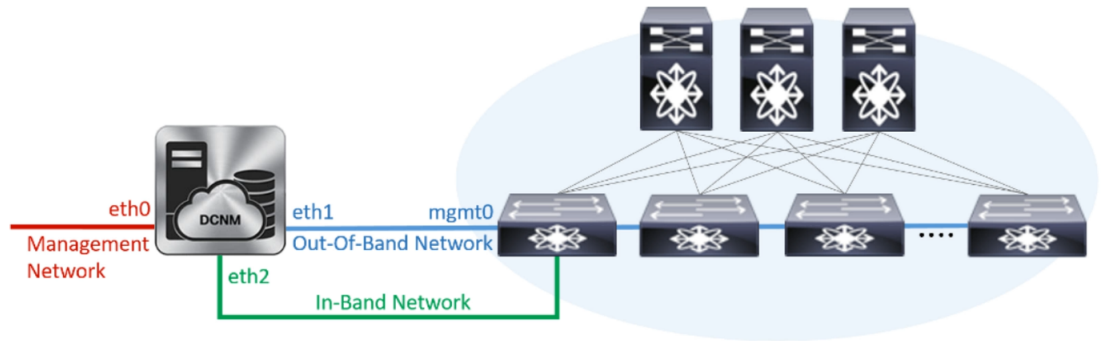
Paste the URL displayed on the Console tab and hit Enter key. A welcome message appears.

To complete the installation of Cisco DCNM from the web installer, perform the following procedure.

Procedure

-
- Step 1** On **Welcome to Cisco DCNM** screen, click **Get Started**.
- Step 2** On **Cisco DCNM Installer** screen, select **Fresh Installation – Standalone** radio button.
Click **Continue**.
- Step 3** On **Administration** tab, enter the password that is used to connect to all the applications in the Cisco DCNM Open Virtual Appliance.
Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application may not function properly.
- It must be at least eight characters long and contain at least one alphabet and one numeral.
 - It can contain a combination of alphabets, numerals, and special characters.
 - Do not use any of these special characters in the DCNM password for all platforms:
`<SPACE> " & $ % ' ^ = < > ; : ` \ | / , . *``
- Select the **Show passwords in clear text** checkbox to view the password you have typed.
Click **Next**.
- Step 4** In **Install Mode** tab, from the drop-down list, choose **LAN Fabric** installation mode for the OVA DCNM Appliance.
Click **Next**.
- Step 5** On the **System Settings** tab, configure the settings for the DCNM Appliance.
- In the Fully Qualified Hostname field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.
 - In the DNS Server Address field, enter the DNS IP address.
 - In the NTP Server field, enter the IP address of the NTP server.
The value must be an IP address or RFC 1123 compliant name.
- Click **Next**.
- Step 6** On **Network Settings** tab, configure the network parameters.

Figure 4: Cisco DCNM Management Network Interfaces



- a) In **Management Network** area, verify if the auto-populated IP Address and Default Gateway address are correct. Modify, if necessary.

(Optional) Enter a valid IPv6 address along with the prefix to configure the Management address and the Management Network Default IPv6 Gateway.

- b) In **Out-of-Band Network** area, enter the IP address, gateway IP Address, and DNS server address. If DCNM is on the IPv6 network, configure the network with an IPv6 Address.

Out-of-band management provides a connection to the device management ports (Typically mgmt0).

Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

- c) In **In-Band Network** area, enter the IP Address and gateway IP Address for the in-band network.

The In-Band Network provides reachability to the devices via the front-panel ports.

Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

However, you can configure the in-band network after installation, if necessary. For more information, see [Configuring Enhanced-Fabric-Inband Interface \(eth2\) Post DCNM Installation, on page 92](#).

Note To modify the already configured in-band network (eth2 interface), execute the **ifconfig eth2 0.0.0.0** command and run the **appmgr setup inband** command again. Refer to [Configuring Enhanced-Fabric-Inband Interface \(eth2\) Post DCNM Installation, on page 92](#) to run the **appmgr setup inband** command.

Click **Next**.

Step 7 On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM Installation for the chosen deployment mode.

A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A success message appears with the URL to access DCNM Web UI.

```
*****
Your Cisco Data Center Network Manager software has been installed.
```

```
DCNM Web UI is available at
https://<<IP Address>>
You will be redirected there in 60 seconds.
Thank you
*****
```

Note If the Cisco DCNM is running behind a firewall, ensure that you open the port 2443 to launch Cisco DCNM Web UI.

Note If you try to access the DCNM Web UI using the Management IP address while the installation is still in progress, an error message appears on the console.

```
*****
*Preparing Appliance*
*****
```

What to do next

Log on to the DCNM Web UI with appropriate credentials.

Click the **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

If you have configured inband management (eth2) IP addresses for device management, login to standalone server and configure the inband network reachability from eth2 of the server to the switches by using the following commands:

```
dcnm# appmgr setup inband-route --subnet switches-fabric-links-IP-subnet/mask
dcnm# appmgr setup inband-route --subnet switch-loopback-IP-subnet>/mask
```

For example: If you have four switches with all fabric links connected through 10.0.0.x/30 subnet, and if all switches are configured with the loopback interface for inband reachability in subnet 40.1.1.0/24, use the following commands:

```
dcnm# appmgr setup inband-route --subnet 10.0.0.0/24
dcnm# appmgr setup inband-route --subnet 40.1.1.0/24
```

Installing the Cisco DCNM ISO in Native HA mode

The native HA is supported on DCNM appliances with ISO or OVA installation only.

By default, an embedded PostgreSQL database engine with the Cisco DCNM. The native HA feature allows two Cisco DCNM appliances to run as active and standby applications, with their embedded databases synchronized in real time. Therefore, when the active DCNM is not functioning, the standby DCNM takes over with the same database data and resume the operation.

Perform the following task to set up Native HA for DCNM.

Procedure

Step 1 Deploy two DCNM Virtual Appliances (either OVA or ISO).

For example, let us indicate them as **dcnm1** and **dcnm2**.

Step 2 Configure **dcnm1** as the Primary node. Paste the URL displayed on the Console tab of **dcnm1** and press **Enter** key.

A welcome message appears.

- a) On the Welcome to Cisco DCNM screen, click **Get Started**.
- b) On the Cisco DCNM Installer screen, select **Fresh Installation - HA Primary** radio button, to install **dcnm1** as Primary node.

Click **Continue**.

- c) On the Administration tab, enter the password that is used to connect to all the applications in the Cisco DCNM Open Virtual Appliance.

Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application may not function properly.

- It must be at least eight characters long and contain at least one alphabet and one numeral.
- It can contain a combination of alphabets, numerals, and special characters.
- Do not use any of these special characters in the DCNM password for Linux, Windows, OVA, and ISO platforms:

<SPACE> " & \$ % ' ^ = < > ; : ` \ | / , . *`

Select the **Show passwords in clear text** checkbox to view the password you have typed.

Click **Next**.

- d) In the Install Mode tab, from the drop-down list, choose **LAN Fabric** installation mode for the DCNM Appliance.

Click **Next**.

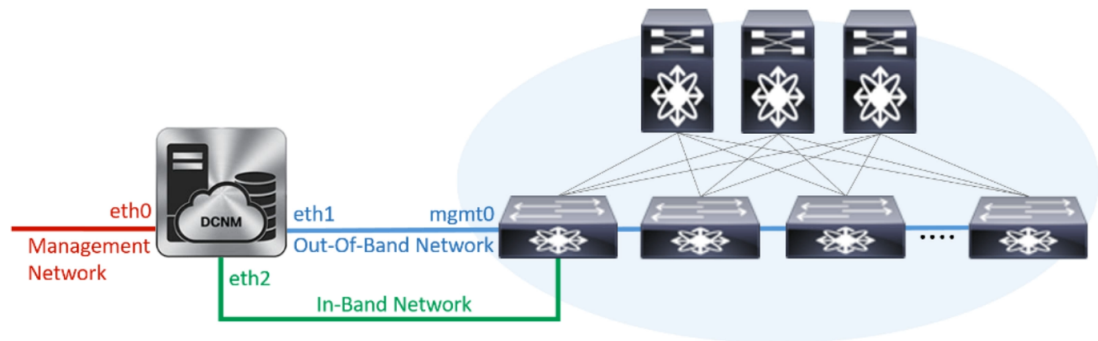
- e) On the System Settings, configure the settings for the DCNM Appliance.
 - In the Fully Qualified Hostname field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.
 - In the DNS Server Address field, enter the DNS IP address.
 - In the NTP Server field, enter the IP address of the NTP server.

The value must be an IP address or RFC 1123 compliant name.

Click **Next**.

- f) On the **Network Settings** tab, configure the network parameters.

Figure 5: Cisco DCNM Management Network Interfaces



- In the Management Network area, verify the auto-populated IP Address and Default gateway address are correct. Modify, if necessary.
(**Optionally**) Enter a valid IPv6 address along with the prefix to configure the Management address and the Management Network Default IPv6 Gateway.
- In the Out-of-Band Network area, enter the IP address, gateway IP Address, and DNS server address. If DCNM is on the IPv6 network, configure the network with an IPv6 Address.
Out-of-band management provides a connection to the device management ports (Typically mgmt0).
- In the In-Band Network area, enter the VIP Address and gateway IP Address for the in-band network. The In-Band Network provides reachability to the devices via the front-panel ports.

Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

However, you can configure the in-band network after installation, if necessary. For more information, see [Configuring Enhanced-Fabric-Inband Interface \(eth2\) Post DCNM Installation, on page 92](#).

Note To modify the already configured in-band network (eth2 interface), execute the **ifconfig eth2 0.0.0.0** command and run the **appmgr setup inband** command again. Refer to [Configuring Enhanced-Fabric-Inband Interface \(eth2\) Post DCNM Installation, on page 92](#) to run the **appmgr setup inband** command

Click **Next**.

- g) On the HA Settings tab, a confirmation message appears.

```
You are installing the primary DCNM HA node.
Please note that HA setup information will need to
be provided when the secondary DCNM HA node is
installed.
```

Click **Next**.

- h) On the **Applications** tab, in the IPv4 Subnet field, enter the IP subnet to access the applications that run internally to DCNM.

All the applications use the IP Address from this subnet.

The Cluster Mode configuration area appears only if you have selected the Enable Clustered Mode checkbox in Step 2.d, on page 35.

Note In Clustered mode, the Cisco DCNM Applications run on separate DCNM Compute Nodes.

1. In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the out-of-band IPv4 network to be used in the Clustered Mode.

The address must be a smaller prefix of available IP addresses from the eth1 subnet. For example: Use 10.1.1.240/28 if the eth1 subnet was configured as 10.1.1.0/24 during installation.

This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

2. In the **Out-of-Band IPv6 Network Address Pool**, enter the address pool from the out-of-band IPv6 network to be used in the Clustered Mode. The address pool must be an IPv6 subnet.

3. In the **In-Band IPv4 Network Address Pool**, enter the address pool from the out-of-band IPv4 network to be used in the Clustered Mode.

The address must be a smaller prefix of available IP addresses eth2 subnet. For example: Use 11.1.1.240/28 if the eth2 subnet was configured as 11.1.1.0/24 during installation.

This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

4. In the **In-Band IPv6 Network Address Pool**, enter the address pool from the in-band IPv6 network to be used in the Clustered Mode. The address pool must be an IPv6 subnet.

Click **Next**.

- i) On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM Installation for the chosen deployment mode.

A progress bar appears to show the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A warning message appears stating that the setup is not complete until you install the Secondary node.

```
WARNING: DCNM HA SETUP IS NOT COMPLETE!  
Your Cisco Data Center Network Manager software has been installed on  
this HA primary node.  
However, the system will be ready to be used only after installation  
of the secondary node has been completed.  
Thank you.
```

Step 3 Configure **dcnm2** as the Secondary node. Paste the URL displayed on the Console tab of **dcnm2** and hit Enter.

A welcome message appears.

- a) On the Welcome to Cisco DCNM screen, click **Get Started**.
- b) On the Cisco DCNM Installer screen, select **Fresh Installation - HA Secondary** radio button, to install **dcnm2** as Secondary node.

Click **Continue**.

- c) On the Administration tab, enter the password that is used to connect to all the applications in the Cisco DCNM Open Virtual Appliance.

Note The password for the secondary node must be the same as the Administrative password for primary, as entered in Step 2.c, on page 35.

Click **Next**.

- d) In the Install Mode tab, from the drop-down list, choose the same installation mode that you selected for the Primary node.

Note The HA installation fails if you do not choose the same installation mode as Primary node.

Click **Next**.

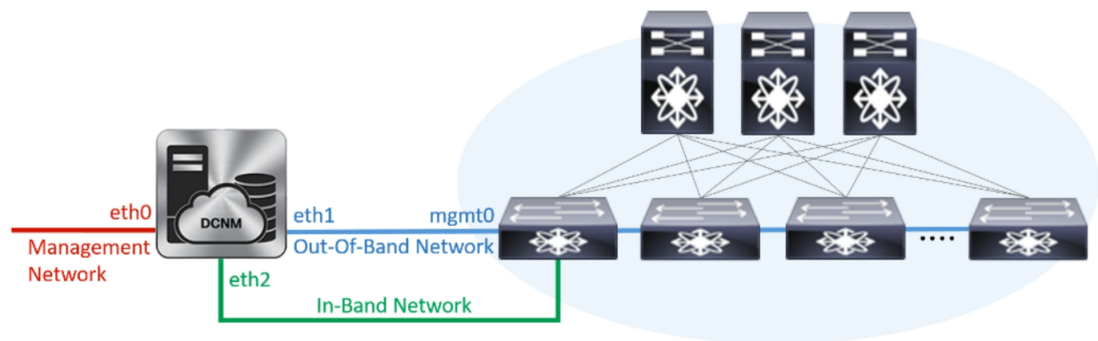
- e) On the System Settings, configure the settings for the DCNM Appliance.

- In the Fully Qualified Hostname field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.
- In the DNS Server Address field, enter the DNS IP address.
- In the NTP Server field, enter the IP address of the NTP server.
The value must be an IP address or RFC 1123 compliant name.

Click **Next**.

- f) On the Network Settings tab, configure the network parameters.

Figure 6: Cisco DCNM Management Network Interfaces



- In the Management Network area, verify if the auto-populated IP Address and Default gateway address are correct. Modify, if necessary.

Note Ensure that the IP Address belongs to the same Management Network as configured on the Primary node for HA setup to complete successfully.

(Optionally) Enter a valid IPv6 address along with the prefix to configure the Management address and the Management Network Default IPv6 Gateway.

- In the Out-of-Band Network area, enter the IP address, gateway IP Address, and DNS server address. If DCNM is on the IPv6 network, configure the network with an IPv6 Address.

Out-of-band management provides a connection to the device management ports (Typically mgmt0).

Note Ensure that the IP Address, IP address gateway, and the IPv6 address belong to the same Out-of-Band Network as configured on the Primary node for HA setup to complete successfully.

You can also configure an IPv6 address for out-of-band management network.

- In the In-Band Network area, enter the IP Address and gateway IP Address for the in-band network. The In-Band Network provides reachability to the devices via the front-panel ports.

Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

However, you can configure the in-band network after installation, if necessary. For more information, see [Configuring Enhanced-Fabric-Inband Interface \(eth2\) Post DCNM Installation, on page 92](#).

Click **Next**.

- g) On the HA Settings tab, configure the system settings..

- In the Management IP Address of primary DCNM node field, enter the appropriate IP Address to access the DCNM UI.
- In the VIP Fully qualified Host Name field, enter hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.
- Enter the Management Network VIP address, and OOB Network VIP address appropriately.
- Enter OOB Network VIPv6 Address to configure IPv6 address for VIP.
- In the In-Band Network area, enter the VIP Address for the in-band network.

This is the VIP address for the In-Band network. This field is mandatory if you have provided an IP address for In-Band network in the Network Settings tab.

- Enter the HA ping IP address if necessary.

HA_PING_ADDRESS, must be different from the DCNM Active and Standby addresses.

You must configure the HA ping IP Address to avoid the Split Brain scenario. This address must belong to Enhanced Fabric management network.

Click **Next**.

- h) On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM OVA Installation for the chosen deployment mode.

A progress bar appears to show the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A success message appears with the URL to access DCNM Web UI.

```
*****
Your Cisco Data Center Network Manager software has been installed.
DCNM Web UI is available at
https://<<IP Address>>
You will be redirected there in 60 seconds.
Thank you
*****
```

Note If the Cisco DCNM is running behind a firewall, ensure that you open the port 2443 to launch Cisco DCNM Web UI.

What to do next

Log on to the DCNM Web UI with appropriate credentials.

Click the **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

If you have configured inband management (eth2) IP addresses for device management, login to standalone server and configure the inband network reachability from eth2 of the server to the switches by using the following commands:

```
dcnm# appmgr setup inband-route --subnet switches-fabric-links-IP-subnet/mask
dcnm# appmgr setup inband-route --subnet switch-loopback-IP-subnet>/mask
```

For example: If you have four switches with all fabric links connected through 10.0.0.x/30 subnet, and if all switches are configured with the loopback interface for inband reachability in subnet 40.1.1.0/24, use the following commands:

```
dcnm# appmgr setup inband-route --subnet 10.0.0.0/24
dcnm# appmgr setup inband-route --subnet 40.1.1.0/24
```

Installing Cisco DCNM SE ISO on Cisco APIC SE

You can install both DCNM and APIC on Cisco Application Services Engine. If you have ordered APIC ASE PID, and later choose to install Cisco DCNM Release 11.3(1) or 11.4(1) on the same ASE, the following error message appears.

```

Cisco Integrated Management Controller
admin

File View Macros Tools Power Boot Device Virtual Media Help

storage.reset()
File "/usr/lib/python2.7/site-packages/blivet/__init__.py", line 511, in reset
self.devicetree.populate(cleanUpOnly=cleanUpOnly)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 2256, in populate
self._populate()
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 2323, in _populate
self.addUdevDevice(dev)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1293, in addUdevDevice
self.handleUdevDeviceFormat(info, device)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 2089, in handleUdevDeviceFormat
self.handleUdevLUMPUFormat(info, device)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1651, in handleUdevLUMPUFormat
self.handleUgLvS(ug_device)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1588, in handleUgLvS
addLU(lv)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1531, in addLU
addRequiredLU(origin_device_name, "failed to locate origin lv")
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1432, in addRequiredLU
addLU(lv_info.name)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1531, in addLU
addRequiredLU(origin_device_name, "failed to locate origin lv")
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1432, in addRequiredLU
addLU(lv_info.name)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1531, in addLU
addRequiredLU(origin_device_name, "failed to locate origin lv")
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1432, in addRequiredLU
addLU(lv_info.name)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1531, in addLU
addRequiredLU(origin_device_name, "failed to locate origin lv")
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1432, in addRequiredLU
addLU(lv_info.name)
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1531, in addLU
addRequiredLU(origin_device_name, "failed to locate origin lv")
File "/usr/lib/python2.7/site-packages/blivet/devicetree.py", line 1558, in addLU
exists=True, **lv_kwargs)
File "/usr/lib/python2.7/site-packages/blivet/devices/lvm.py", line 554, in __init__
exists=exists)
File "/usr/lib/python2.7/site-packages/blivet/devices/dm.py", line 73, in __init__
parents=parents, sysfsPath=sysfsPath)
File "/usr/lib/python2.7/site-packages/blivet/devices/storage.py", line 131, in __init__
Device.__init__(self, name, parents=parents)
File "/usr/lib/python2.7/site-packages/blivet/devices/device.py", line B4, in __init__
raise ValueError("%s is not a valid name for this device" % name)
ValueError: 18fc8614ba7b7c8c8279b588de8861b578bc356b3151834ead1482f9ab94339b is not a valid name for this device

anaconda1:~# 1:main* 2:shell 3:log 4:storage-log 5:program-log Switch tab: Alt+Tab | Help: F1

```

To install Cisco DCNM 11.3(1) or 11.4(1) on an existing APIC ASE, perform the following steps:

Procedure

- Step 1** At the prompt, press **CTRL-ALT-F2** to move to a different console. A shell prompt appears.
 - Step 2** Get the list of disks by using the **lsblk -d** command.
 - Step 3** For each disk, execute the following command:
- Note** Ensure that you do not run this command on the UNIGEN 16GB disk.

```
dd if=/dev/zero of=/dev/<disk> bs=10M count=1
```

```

root@se-appliance$ lsblk -d
NAME HCTL          TYPE VENDOR  MODEL          REV TRAN
sda  0:2:0:0         disk Cisco    UCSC-RAID12G-2GB 5.10
sdb  0:2:1:0         disk Cisco    UCSC-RAID12G-2GB 5.10
sdc  0:2:2:0         disk Cisco    UCSC-RAID12G-2GB 5.10
sdd  0:2:3:0         disk Cisco    UCSC-RAID12G-2GB 5.10
sde  0:2:4:0         disk Cisco    UCSC-RAID12G-2GB 5.10
sdf  2:0:0:0         disk ATA     Micron_5100_MTFD H072 sata

```

```
sdg 1:0:0:0    disk UNIGEN    PHF16H0CM1-ETG    PMAP usb
root@se-appliance$
```

- Step 4** Reboot the Cisco Applications Service Engine.
- Step 5** Install the Cisco DCNM ISO Release 11.3(1) or 11.4(1).

Refer the following URLs for more information.

- [Cisco Application Services Engine Installation Guide For Cisco DCNM, Release 11.3 \(1\)](#)
- [Cisco Application Services Engine Installation Guide For Cisco DCNM, Release 11.4\(1\)](#)

Installing Cisco DCNM Compute Node

Paste the URL displayed on the Console tab and hit Enter key. A welcome message appears. You can install compute nodes on both Cisco DCNM OVA and ISO deployments.



Note Compute nodes allows users to scale DCNM, as application load can be shared across all the compute nodes, instead of the usual 1 or 2 (if you have HA) nodes.



Note If **Enable Clustered Mode** was selected during DCNM installation, applications such as, Configuration Compliance, EPL, NIA, and NIR won't work until you install the compute nodes.

To complete the installation of Cisco DCNM Compute Node from the web installer, perform the following procedure.

Before you begin

Ensure that you have 16 vCPUs, 64GB RAM, and 500GB hard disc to install compute nodes.

Procedure

- Step 1** On the **Welcome to Cisco DCNM** screen, click **Get Started**.
- Step 2** On the Cisco DCNM Installer screen, select the **Fresh Installation – Standalone** radio button. Click **Continue**.
- Step 3** On the **Install Mode** tab, choose **Compute** to deploy this DCNM instance as a compute node.
- Note** **Compute** option appears in the drop-down list only if you have chosen **Compute** while configuring the OVF template or ISO hypervisors.
- Click **Next**.
- Step 4** On the **Administration** tab, enter information about passwords.

- In the **Administrator Password** field, enter the password that is used to connect to the applications in the Cisco DCNM.

All special characters, except %\$^=;.*\'' <SPACE> is allowed in the password.

Enter the password again in the **Repeat Administrator Password** field.

- In the **Database Password** field, enter the password for the PostgreSQL database.

All special characters, except %\$^=;.*\'' <SPACE> is allowed in the password.

Enter the password again in the **Repeat Database Password** field.

Note If this field is left blank, it shall consider the Administrator password as the PostgreSQL password.

Select the **Show passwords in clear text** check box to view the password that you have entered.

Click **Next**.

Step 5

On the **System Settings**, configure the settings for the DCNM Appliance.

- In the **Fully Qualified Hostname** field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Hostnames with only digits is not supported.

- In the **DNS Server Address List** field, enter the DNS IP address.

Beginning with Release 11.2(1), you can also configure the DNS server using an IPv6 address.

From Release 11.3(1), you can configure more than one DNS server.

Note If you're using Network Insights applications, ensure that the DNS server is valid and reachable.

- In the **NTP Server Address List** field, enter the IP address of the NTP server.

The value must be an IP or IPv6 address or RFC 1123 compliant name.

From Release 11.3(1), you can configure more than one NTP server.

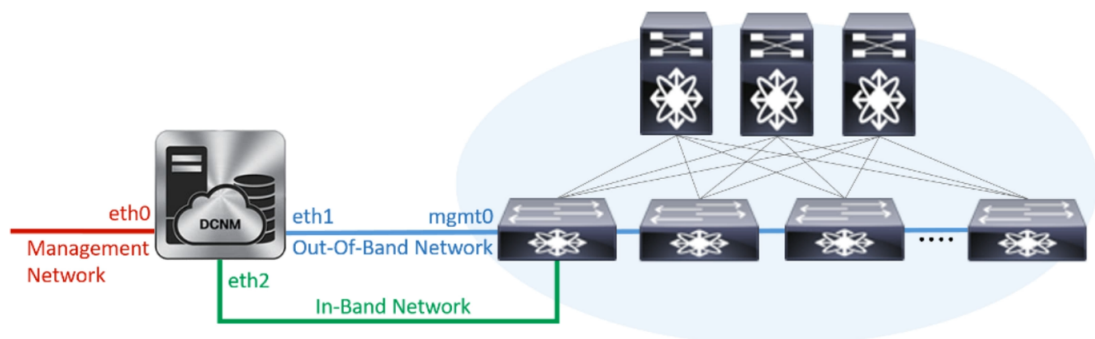
- From the **Timezone** drop-down list, select the timezone in which you are deploying the DCNM.

Click **Next**.

Step 6

On the **Network Settings** tab, configure the network parameters used to reach the DCNM Web UI.

Figure 7: Cisco DCNM Management Network Interfaces



- a) In the **Management Network** area, verify if the auto-populated addresses for **Management IPv4 Address** and **Management Network Default IPv4 Gateway** are correct. Modify, if necessary.

Note Beginning with Cisco DCNM Release 11.2(1), you can also use an IPv6 address for the Management Network.

(Optionally) Enter a valid IPv6 address along with the prefix to configure the **Management IPv6 Address** and the **Management Network Default IPv6 Gateway**.

- b) In the **Out-of-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address**.

If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

Out-of-band management provides a connection to the device management ports (Typically mgmt0).

Note If the out-of-band network is not configured, you cannot configure Cisco DCNM in Cluster mode.

- c) In the **In-Band Network** area, enter the **IPv4 address** and **Gateway IPv4 Address** for the in-band network.

If DCNM is on the IPv6 network, configure the network by entering relevant IPv6 Address for **IPv6 address** and **Gateway IPv6 Address**.

The In-Band Network provides reachability to the devices via the front-panel ports.

Note If you do not configure in-band network, Endpoint Locator and Telemetry features are not operational.

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see [Editing Network Properties Post DCNM Installation, on page 83](#).

Click **Next**.

Step 7

In the **Internal Application Services Network** area, in the **IPv4 Subnet field**, enter the IP subnet to access the applications that run internally to DCNM.

All the applications use the IP Address from this subnet.

Click **Next**.

Step 8

On the **Summary** tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** to complete the Cisco DCNM Installation for the chosen deployment mode.

A progress bar appears to show the completed percentage, description of the operation, and the elapsed time during the installation. After the progress bar shows 100%, click **Continue**.

A success message appears with the URL to access DCNM Compute Node.

```
*****
Your Cisco DCNM Compute Node has been installed.
Click on the following link to go to DCNM GUI's Application page:
DCNM GUI's Applications
You will be redirected there in 60 seconds.
Thank you
*****
```

Step 9 Log on to the compute node via SSH, using `sysadmin@<dcnm-compute-eth0-ip-address>`.

Step 10 Run the `sudo reboot` command to ensure that this compute node joins the Cluster in a fully initialized state.

```
dcnm-compute# sudo reboot
```

After reboot, verify if you can SSH into the compute node using `sysadmin@<dcnm-compute-eth0-ip-address>`.

What to do next

Log on to the DCNM Web UI with appropriate credentials.

The **Applications** tab displays all the services running on the DCNM deployment that you have installed. Click **Compute** tab to view the new Compute in Discovered state on the Cisco DCNM Web UI.

Compute IP Address	In-Band Interface	Out-Band Interface	Status	Memory	Disk	Uptime
172.19.90.114	NA	NA	Discovered			

To add the compute nodes to a cluster, see [Adding Computes to a Cluster Node](#) in your deployment-specific *Cisco DCNM Configuration Guide* for more information.

When a compute node goes through an unscheduled powercycle and restarts, the Elasticsearch container will not start. It is possible that some filesystems are corrupted. To resolve this issue, reboot the Compute node in safe mode by using `fsck -y` command.



CHAPTER 5

Upgrading Cisco DCNM

This section includes instructions for upgrading your Cisco DCNM Appliance installation in the following scenarios:

Cisco DCNM Installer version	Release from which you can upgrade
DCNM 11.1(1)	<ul style="list-style-type: none">• DCNM 11.0(1) using Inline Upgrade• DCNM 10.4(2) using DCNMUpgradeTool

The following table summarizes the upgrade options for Cisco DCNM Release 11.1(1) .

Table 4: Type of Upgrade

Current Release Number	Upgrade type to upgrade to Release 11.1(1)
11.0(1)	Inline Upgrade
10.4(2)	Upgrade using the DCNMUpgradeTool

Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application might not function properly:

- It must be at least 8 characters long and contain at least one alphabet and one numeral.
- It can contain a combination of alphabets, numerals, and special characters.
- Do not use any of these special characters in the DCNM password for all platforms:
<SPACE> " & \$ % ' ^ = < > ; : ` \ | / , . *
- From Cisco DCNM Release 11.0(1), the characters that are allowed in the Administrative password is restricted for OVA and ISO installations. Therefore while upgrading, the old password used in DCNM 10.4(2) is not valid. However, different passwords are allowed during Upgrade.

The new Administrative password that is entered is used in the following scenarios.

- accessing the DCNM appliance via its console.
- accessing the appliance via SSH
- for applications running on the appliance, e.g. Postgres DBMS

However, after the upgrade, since Postgres DBMS is restored from the backup that is taken on DCNM 10.4(2), you must logon to the Cisco DCNM Web UI using the password used on DCNM Release 10.4(2) appliance.

This chapter contains the following:

- [Upgrading ISO or OVA using the DCNM Upgrade Tool, on page 48](#)
- [Upgrading ISO or OVA through Inline Upgrade, on page 56](#)

Upgrading ISO or OVA using the DCNM Upgrade Tool

This section contains the procedure to download **DCNMUpgradeTool** and upgrade DCNM to the latest version.

Downloading the DCNM Upgrade Tool

The first step to upgrading the DCNM is to download the DCNMUpgradeTool script.



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

Procedure

- Step 1** Go to the following site: <http://software.cisco.com/download/>.
- Step 2** In the Select a Product search box, enter **Cisco Data Center Network Manager**.
Click the **Search** icon.
- Step 3** Click on **Data Center Network Manager** from the search results.
A list of the latest release software for Cisco DCNM available for download is displayed.
- Step 4** In the Latest Releases list, choose Release 11.1(1).
- Step 5** Locate the DCNM Upgrade Tool and click **Download** icon.
Save the file to the appliance `/root` directory.
-

Backup Using the Upgrade Tool

Beginning with Release 11.0(1), you can download the DCNMUpgradeTool from the Software Downloads page, to take a backup of the DCNM Appliance. This data from this backup file is restored after you upgrade the appliance to DCNM Release 11.1(1).

Perform the following task to run the DCNMUpgradeTool to take a backup of all the applications and data on DCNM 10.4(2).

Before you begin

Ensure that you have copied the DCNMUpgradeTool script to the /root directory of your appliance. Enable read and write permissions on the script using the **chmod 777** or **chmod +x** command.

Procedure

Step 1 Copy the **DCNMUpgradeTool** to the root folder of the Cisco DCNM server.

Step 2 Execute the upgrade tool command.

```
dcnm1# ./DCNMUpgradeTool
```

The tool will analyse the DCNM appliance data and decide if you can upgrade to 11.1(1) or not.

Note The backup that is generated by using this tool can be used to restore data, after upgrade.

Step 3 Enter **y** to continue.

Example:

```
Continue? [y/n] y
```

The tool inspects the systems, checks all constraints, and determines whether the appliance can be upgraded. It also checks for any SAN configuration and default fabrics. If the upgrade criteria is met, the system displays as shown below.

```
This system version: 10.4(2)
```

```
- Checking SAN config
- Checking default fabric
...
```

```
Congratulations! You can upgrade to DCNM 11.1(1)
```

If the criteria is not met, the upgrade is terminated.

Step 4 Enter **y** to create a backup file.

```
Create backup file? [y/n]: y
```

After the backup is completed successfully, the following message is displayed.

```
*****
Backup is available at /root/backup.DD_MM_YYYY_HH_MM_SS.tar.gz
*****
```

Copy the backup file to a safe location and shut down the application.

Upgrading and Restoring DCNM Virtual Appliance in Standalone mode



Note This procedure applied to both DCNM OVA and ISO upgrade.

Perform the following task to upgrade the DCNM appliance and restore data.

Before you begin

Ensure that you have copied the backup generated from `DCNMUpgradeTool` to a safe location.

Procedure

-
- Step 1** Update the interface MAC address of the Active and Standby appliance. Right-click on **VM > Edit Settings > Hardware**.
- For both Network Adapters, update the MAC address to be the same as Cisco DCNM 10.4(2). This ensures that the same MAC address is used for the new Virtual Machine (VM); licenses on Cisco DCNM will not need to be regenerated in the event of an upgrade.
- Step 2** Right click on the OVF and select **Power > Power on**.
- Step 3** After the VM is powered on click on **Console** tab.
- A message indicating that the DCNM appliance is configuring appears on the screen.
- Copy and paste the URL to the browser to continue with restore process.
- Step 4** On the Cisco DCNM Web Installer UI, click **Get Started**.
- Step 5** On the Cisco DCNM Installer screen, select **Fresh Installation with backup file for upgrade or restore** radio button.
- Click **Continue**.
- Step 6** Select the backup file that was generated using the `DCNMUpgradeTool`.
- You can choose perform either on one of the following.
- Click **Upload backup file**. Navigate to the backup file generated for the Active node. Select the appropriate backup file. Click **OK**.
 - Click **Copy remote backup file**. Provide the Remote machine information.
- Note** You must SSH or RSync must be installed on the Remote machine.
- Click **OK**.
- Verify if the correct backup filename appears in the Select backup file field. Click **Continue**.
- Note** If the backup file was generated without using the `DCNMUpgradeTool`, an error appears and you will not be able to upgrade the DCNM.
- Step 7** After the backup file is uploaded, the DCNM server will read and auto-populate the values in some fields.
- The prefill is based on the content of the backup file that was provided. You can verify the values and modify if necessary.
- Step 8** In the Administration tab, ensure that the correct password is entered.
- Click **OK** on the Note pop-up message.
- Click **Next**.
- Step 9** In the Install Mode tab, from the drop-down list, choose Easy Fabric installation mode for the OVA DCNM Appliance.

Note Only the supported upgrade mode will appear in the drop down list.

Click **Next**.

Step 10 On the System Settings, verify the Hostname, DNS Server Address and NTP server information. Modify the configuration, if required and click **Next**.

Step 11 On the Network Settings tab, verify the network settings configuration. Modify the configuration if required and click **Next**.

Step 12 On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** complete Cisco DCNM Virtual Appliance Installation for the chosen deployment mode.

A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation.

After the progress bar shows 100%, click **Continue**.

A warning message appears with information that the system is upgraded to DCNM 11.1(1).

```
Your Cisco Data Center Network Manager software has been installed.  
DCNM Web UI is available at  
https://<<IP-Address>>  
You will be redirected there in 60 seconds.  
Thank you.
```

What to do next

Logon to the DCNM Web UI with appropriate credentials.



Note Logon to the Cisco DCNM Web UI using the password used on DCNM Release 10.4(2) appliance.

Ensure that you clear the browser cache before you launch the Cisco DCNM Web UI using the Management Network IP address.

Click **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

To gracefully onboard Cisco DCNM 10.4(2) or 11.0(1) managed VXLAN BGP EVPN fabric(s) comprising Cisco Nexus 9000 switches post upgrade to DCNM 11.1(1), see [Post DCNM 10.4\(2\) or 11.0\(1\) to DCNM 11.1\(1\) Upgrade for VXLAN BGP EVPN and MSD Fabrics](#).

Upgrading and Restoring DCNM Virtual Appliance in Native HA Mode

The native HA is only supported on DCNM appliances with ISO or OVA installation. Unlike HA mechanisms, it doesn't require any external dependencies like an Oracle database or a shared NFS file system.

The native HA feature allows two Cisco DCNM appliances to run as active and standby applications, with their embedded databases synchronized in real time. Therefore, when the active DCNM is not functioning, the standby DCNM takes over with the same database data and resume the operation.

Perform the following to upgrade the Cisco DCNM Native HA appliances to Release 11.1(1).

Before you begin

- Ensure that both the Cisco DCNM 10.4(2) Active and Standby peers are up and running.
- Check and ensure that the Active and Standby servers are operational, by using the `appmgr show ha-role` command:

Example:

On the Active node:

```
dcnm1# appmgr show ha-role
Native HA enabled.
Deployed role: Active
Current role: Active
```

On the Standby node:

```
dcnm2# appmgr show ha-role
Native HA enabled.
Deployed role: Standby
Current role: Standby
```

Procedure

-
- Step 1** Copy the DCNMUpgradeTool to the root folder of both Active and Standby servers.
- Note** For example, let us indicate Active and Standby appliances as **dcnm1** and **dcnm2** respectively.
- Step 2** Run the DCNMUpgradeTool on both the DCNM 10.4(2) appliances and save the backup to your local directory.
- Note** Ensure that the Current role of Active and Standby nodes are correct. Verify using the **appmgr show ha-role** command on both nodes.
- For instructions, see [Backup Using the Upgrade Tool, on page 48](#).
- Check if separate `.tar` archives are stored in an external file system.
- Step 3** Copy the interface MAC address of the Active and Standby appliance. Right-click on **VM > Edit Settings > Hardware**.
- For both Network Adapters, update the MAC address to be the same as Cisco DCNM 10.4(2). This ensures that the same MAC address is used for the new Virtual Machine (VM); licenses on Cisco DCNM will not need to be regenerated for the appliances after upgrade.
- Step 4** Shut down both the appliances using the **shutdown -h** command.
- Note** Ensure that you shutdown the Standby appliance first, and then shutdown the Active appliance.
- ```
dcnm2# shutdown -h now
dcnm1# shutdown -h now
```
- You can also right on the VM, select **Power > Power Off**.
- Step 5** Install Cisco DCNM 11.1(1) on two appliances, one for Active and one for Standby.
- You can either deploy DCNM as OVA or ISO. You must first deploy OVA as an OVF template, or configure KVM or Baremetal for ISO installation. For instructions, see:

- OVA—[Deploying the Open Virtual Appliance as an OVF Template, on page 14](#)
- ISO—either one of the following.
  - [Installing the DCNM ISO Virtual Appliance on KVM, on page 30](#)
  - [Installing the DCNM ISO Virtual Appliance on UCS \(Bare Metal\), on page 26](#)

**Note** If this deployment is a part of the upgrade process, do not Power on the VM. Edit and provide the 10.4(2) MAC address and power on the VM.

**Step 6** Update the interface MAC address of the Active and Standby appliance. Right-click on **VM > Edit Settings > Hardware**.

For both Network Adapters, update the MAC address to be the same as Cisco DCNM 10.4(2). This ensures that the same MAC address is used for the new Virtual Machine (VM); licenses on Cisco DCNM will not need to be regenerated in the event of an upgrade.

**Step 7** After the VM or Baremetal is powered on, click **Console** tab.

**Note** Before you power on the VM, ensure that you have reserved appropriate resources for the VM, such as CPU and memory, based on the chosen deployment configuration.

A message indicating that the DCNM appliance is configuring appears on the screen.

Copy and paste the URL to the browser to continue with restore process.

**Step 8** On the Active node DCNM Web Installer UI, upload and validate the backup file.

- a) Click **Get Started**.
- b) On the Cisco DCNM Installer screen, select **Fresh Installation with backup file for upgrade or restore** radio button.

Click **Continue**.

- c) Select the Active node backup file that was generated using the `./DCNMUpgradeTool` script.

You can choose perform either on one of the following:

- Click **Upload backup file**. Navigate to the backup file generated for the Active node. Select the appropriate backup file. Click **OK**.
- Click **Copy remote backup file**. Provide the Remote machine information. Click **OK**.

Verify if the correct backup file name appears in the Select backup file field. Click **Continue**.

**Note** If the backup file was generated without using the DCNMUpgradeTool, an error appears and you will not be able to upgrade the DCNM.

- d) After the backup file is uploaded, the DCNM server will read and auto populate the values in some fields.

**Note** If the primary node was not in HA active state when the backup was taken, the system will not be restored correctly and you will experience data loss.

The prefill is based on the content of the backup file that was provided.

- e) In the Administration tab, ensure that the correct password is entered and click **Next**.

Select the **Show passwords in clear text** checkbox to view the password entered.

- f) In the Install Mode tab, from the drop-down list, choose Easy Fabric installation mode for the OVA DCNM Appliance.

**Note** Only the supported upgrade mode appears in the drop-down list.

Click **Next**.

- g) On the System Settings, verify the Hostname, DNS Server Address, and NTP server information.

Modify the configuration, if necessary and click **Next**.

- h) On the Network Settings tab, verify the network settings configuration.

Modify the configuration if necessary and click **Next**.

- i) In the HA Settings tab, the following message is displayed.

```
You are installing the primary DCNM HA mode.
Please note that HA setup information will need to be
provided when the secondary DCNM HA node is installed.
```

- j) On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** complete Cisco DCNM Virtual Appliance Installation for the chosen deployment mode.

A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation.

After the progress bar shows 100%, click **Continue**.

A warning message appears with information that the system is not ready until the upgrade process on the Standby node is complete.

```
WARNING: RESTORE/UPGRADE IS NOT COMPLETE!
Your Cisco Data Center Network Manager software has been installed on this
HA primary node. However, the system will be ready to be used only after the
upgrade/restore of the secondary node has been completed.
Thank you.
```

## Step 9

On the Standby node DCNM Web Installer UI, upload and validate the backup file.

- Click **Get Started**.
- On the Cisco DCNM Installer screen, select **Fresh Installation with backup file for upgrade or restore** radio button.

Click **Continue**.

- Select the Standby node backup file that was generated using the `./DCNMUpgradeTool` script.

You can choose perform either on one of the following:

- Click **Upload backup file**. Navigate to the backup file generated for the Standby node. Select the appropriate backup file. Click **OK**.
- Click **Copy remote backup file**. Provide the Remote machine information. Click **OK**.

Verify if the correct backup file name appears in the Select backup file field. Click **Continue**.

If the backup file was generated without using the DCNMUpgradeTool, an error appears and you will not be able to upgrade the DCNM.

- After the backup file is uploaded, the DCNM server will read and auto populate the values in some fields.

**Note** If the standby node was not in HA standby state when the backup was taken, the system will not be restored correctly and you will experience data loss.

The prefill is based on the content of the backup file that was provided.

- e) In the Administration tab, ensure that the correct password is entered and click **Next**.

**Note** This password must match the Administration Password of the Primary DCNM node for HA setup to complete successfully.

Select the **Show passwords in clear text** checkbox to view the password entered.

- f) In the Install Mode tab, from the drop-down list, choose Easy Fabric installation mode for the OVA DCNM Appliance.

**Note** Ensure that you select the same installation mode for the standby node that was chosen for the primary node.

Click **Next**.

- g) On the System Settings, verify the Hostname, DNS Server Address, and NTP server information.

Modify the configuration, if necessary and click **Next**.

- h) On the Network Settings tab, verify the network settings configuration.

Modify the configuration if necessary and click **Next**.

- i) In the HA Settings tab, the following message is displayed.

Enter a valid HA Ping IP Address, if necessary. Ensure that this IP address must be different from the DCNM Active and Standby IP addresses.

**Note** If set, the **HA ping feature IP Address** must be pingable for DCNM services to be running in Native HA systems. This address must belong to Enhanced Fabric management network.

- j) On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** complete Cisco DCNM Virtual Appliance Installation for the chosen deployment mode.

A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation.

After the progress bar shows 100%, click **Continue**.

A success message appears with the URL to access DCNM Web UI.

```
Your Cisco Data Center Network Manager software has been installed.
DCNM Web UI is available at https://<<IP Address>>
You will be redirected there in 60 seconds.
Thank you
```

**Step 10** After the data is restored, check the status using the **appmr status all** command on both Active and standby nodes.

**Step 11** Verify the role of the appliances using the **appmgr show ha-role** command.

**Step 12** Log on to the DCNM Web UI with appropriate credentials.

**What to do next**

Logon to the DCNM Web UI with appropriate credentials.



**Note** After the upgrade, since Postgres DBMS is restored from the backup that is taken on DCNM 10.4(2), you must log on to the Cisco DCNM Web UI using the password used on DCNM Release 10.4(2) appliance.

Click **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

To gracefully onboard Cisco DCNM 10.4(2) or 11.0(1) managed VXLAN BGP EVPN fabric(s) comprising Cisco Nexus 9000 switches post upgrade to DCNM 11.1(1), see [Post DCNM 10.4\(2\) or 11.0\(1\) to DCNM 11.1\(1\) Upgrade for VXLAN BGP EVPN and MSD Fabrics](#).

## Upgrading ISO or OVA through Inline Upgrade

Inline upgrade allows you to upgrade DCNM by imposing the new DCNM version to the existing DCNM. After the inline upgrade, ensure that you clear your browser cache before launching the DCNM application.

When you install Cisco DCNM, a self-signed certificate is installed, by default. However, after upgrading to the latest Cisco DCNM Release, you must restore the certificates.



**Note** Restoring certificates is a disruptive mechanism; it requires you to stop and restart applications. Restore the certificates only when the upgraded system is stable, that is, you must be able to log in to Cisco DCNM Web UI.

This section contains the procedure to upgrade the DCNM using the Inline Upgrade method.

## Inline Upgrade for DCNM Virtual Appliance in Standalone Mode

You can upgrade from Release 11.0(1) to Release 11.1(1) using the inline upgrade. Inline upgrade allows you to upgrade DCNM by imposing the new DCNM version to the existing DCNM. After the inline upgrade, ensure that you clear your browser cache before launching the DCNM application.

Perform the following task to upgrade the DCNM virtual appliance in standalone mode.

### Procedure

**Step 1** Log on to the Cisco DCNM appliance console.

**Caution** If the system requirements do not meet the minimum resource requirements, every time you log on to DCNM via the console or SSH, **SYSTEM RESOURCE ERROR** is displayed. Modify the system requirements logon to DCNM via Console/SSH.

- For OVA Installation: On the OVF template deployed for the host, right click and select **Settings > Launch Web Console**.

- For ISO Installation: Select the KVM console or UCS (Bare Metal) console.

**Caution** Do not perform an Inline Upgrade from an SSH Session. The session may timeout and result in an incomplete upgrade.

**Step 2** Take a backup of the application data using the **appmgr backup** command.

```
dcnm# appmgr backup
```

Copy the backup file to a safe location outside the DCNM server.

**Step 3** Unzip the `dcnm-va.11.1.1.iso.zip` file and upload the DCNM 11.1(1) ISO file to the `/root/` folder in the DCNM setup that you want to upgrade.

**Step 4** Create folder that is named **iso** using the **mkdir /mnt/iso** command.

```
dcnm# mkdir /mnt/iso
```

**Step 5** Mount the DCNM 11.1(1) ISO file on the standalone setup in the `/mnt/iso` folder.

**mount -o loop <DCNM 11.1(1) image> /mnt/iso**

```
dcnm# mount -o loop dcnm-va.11.1.1.iso /mnt/iso
```

**Step 6** Navigate to `/mnt/iso/packaged-files/scripts/` and run the `./inline-upgrade.sh` script.

```
dcnm# cd /mnt/iso/packaged-files/scripts/
```

```
dcnm# ./inline-upgrade.sh
```

```
Do you want to continue and perform the inline upgrade to ? [y/n]: y
```

**Note** If some services are still running, you will receive a prompt that the services will be stopped. When prompted, press **y** and continue.

```
Do you want to do the inline upgrade to 11.1(1)?
```

```
The DCNM and Elasticsearch will go down (if it is running) and come up after the upgrade
```

```
[y/n] n ? y
```

**Step 7** Provide the new sysadmin user password at the prompt:

```
Enter the password for the new sysadmin user: <<sysadmin_password>>
```

```
Enter it again for verification: <<sysadmin_password>>
```

After the upgrade is complete, the appliance reboots.

**Step 8** Ensure that the DCNM application is functional, by using the **appmgr status all** command.

```
dcnm# appmgr status all
```

**Step 9** To verify that you have successfully installed the Cisco DCNM Release 11.1(1), use the **appmgr show version** command.

```
dcnm# appmgr show version
```

```
Cisco Data Center Network Manager
```

```
Version: 11.1(1)
```

```
Install mode: LAN Fabric
```

```
Standalone node. HA not enabled.
```

## What to do next

Log on to the DCNM Web UI with appropriate credentials.

Click **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

To reindex the performance manager data, use the **appmgr es-reindex pmdb** command.

To gracefully onboard Cisco DCNM 10.4(2) or 11.0(1) managed VXLAN BGP EVPN fabric(s) comprising Cisco Nexus 9000 switches post upgrade to DCNM 11.1(1), see [Post DCNM 10.4\(2\) or 11.0\(1\) to DCNM 11.1\(1\) Upgrade for VXLAN BGP EVPN and MSD Fabrics](#).

## Inline Upgrade for DCNM Virtual Appliance in Native HA Mode

You can upgrade from Release 11.0(1) to Release 11.1(1) using the inline upgrade.

Inline upgrade allows you to upgrade DCNM by imposing the new DCNM version to the existing DCNM. After the inline upgrade, ensure that you clear your browser cache before launching the DCNM application.

Perform the following task to upgrade the DCNM virtual appliance in Native HA mode.

### Before you begin

- Ensure that both the Cisco DCNM 11.0(1)Active and Standby peers are up and running.
- If the Cisco DCNM setup is in clustered mode, ensure that you perform the following:




---

**Note** Inline upgrade of Cisco DCNM in Clustered mode is supported from Release 11.2(1). Release 11.1(1) doesn't support inline upgrade for DCNM in clustered mode.

---

- Stop the Network Insights - Resources (NIR) 2.x application. On the Cisco DCNM Web UI, choose **Applications > Catalog**. On the NIR app, click **Stop** icon to stop the application. Click **Delete** to remove the application from the Catalog.
- Stop all the applications running on the Cisco DCNM Compute nodes using the **appmgr stop afw** command.

```
dcnm-compute# appmgr stop afw
```

- Check and ensure that the Active and Standby servers are operational, using the **appmgr show ha-role** command.

Example:

On the Active node:

```
dcnm1# appmgr show ha-role
Native HA enabled.
Deployed role: Active
Current role: Active
```

On the Standby node:

```
dcnm2# appmgr show ha-role
Native HA enabled.
Deployed role: Standby
Current role: Standby
```



## Procedure

- Step 1** Unzip the `dcnm-va.11.1.1.iso.zip` file and upload the DCNM 11.1(1) ISO file to the `/root/` folder in both Active and Standby node of the DCNM setup that you want to upgrade.
- Note** For example, let us indicate Active and Standby appliances as **dcnm1** and **dcnm2** respectively.
- Step 2** Log on to the Cisco DCNM appliance console.
- Caution** If the system requirements do not meet the minimum resource requirements, every time you log on to DCNM via the console or SSH, **SYSTEM RESOURCE ERROR** is displayed. Modify the system requirements logon to DCNM via Console/SSH.
- For OVA Installation: On the OVF template that is deployed for the host, right click and select **Settings > Launch Web Console**.
  - For ISO Installation: Select the KVM console or UCS (Bare Metal) console.
- Caution** Do not perform an Inline Upgrade from an SSH Session. The session may timeout and result in an incomplete upgrade.
- Step 3** Take a backup of the application data using the **appmgr backup** command on both Active and Standby appliances.
- ```
dcnm1# appmgr backup
dcnm2# appmgr backup
```
- Copy the backup file to a safe location outside the DCNM server.
- Step 4** On the Active node, perform the inline upgrade.
- Create a folder named **iso** using the **mkdir /mnt/iso** command.


```
dcnm1# mkdir /mnt/iso
```
 - Mount the DCNM 11.1(1) ISO file on the Active node in the `/mnt/iso` folder.


```
dcnm1# mount -o loop dcnm-va.11.1.1.iso /mnt/iso
```
 - (Optional) Stop the HA applications on the Standby appliance using the **appmgr stop ha-apps** command.


```
dcnm2# appmgr stop ha-apps
```
 - Navigate to `/mnt/iso/packaged-files/scripts/` location and run the `./inline-upgrade.sh` script.


```
dcnm1# cd /mnt/iso/packaged-files/scripts/
dcnm1# ./inline-upgrade.sh
```

Note If some services are still running, you will receive a prompt that the services will be stopped. When prompted, press **y** to continue.

```
Do you want to do the inline upgrade to 11.1(1)?
The DCNM and Elasticsearch will go down (if it is running) and
come up after the upgrade [y/n] n ? y
```
 - Provide the new sysadmin user password at the prompt:


```
Enter the password for the new sysadmin user: <<sysadmin_password>>
Enter it again for verification: <<sysadmin_password>>
```

After the upgrade is complete, the appliance reboots.

- f) Ensure the DCNM application is functional, by using the **appmgr status all** command.

```
dcnm1# appmgr status all
```

Note Ensure that all the services are up and running on the Cisco DCNM Active node before proceeding to upgrade Standby node.

- g) Verify the role of the Active node, by using **appmgr show ha-role** command. Current role must show as Active.

```
dcnm1# appmgr show ha-role
```

```
Native HA enabled.
Deployed role: Active
Current role: Active
```

Warning We recommend that you do not continue to upgrade the Standby node, unless the Active node Current role is Active.

Step 5 On the Standby node, perform the inline upgrade.

- a) Create folder named **iso** using the **mkdir /mnt/iso** command.

```
dcnm2# mkdir /mnt/iso
```

- b) Mount the DCNM 11.1(1) ISO file on the Standby node in the **/mnt/iso** folder.

```
dcnm2# mount -o loop dcnm-va.11.1.1.iso /mnt/iso
```

- c) Navigate to **/mnt/iso/packaged-files/scripts/** location and run the **./inline-upgrade.sh** script.

```
dcnm2# cd /mnt/iso/packaged-files/scripts/
dcnm2# ./inline-upgrade.sh --standby
```

Note If some services are still running, you will receive a prompt that the services will be stopped. When prompted, press **y** and continue.

```
Do you want to do the inline upgrade to 11.1(1)?
The DCNM and Elasticsearch will go down (if it is running) and
come up after the upgrade [y/n] n ? y
```

- d) Provide the new sysadmin user password at the prompt:

```
Enter the password for the new sysadmin user: <<sysadmin_password>>
Enter it again for verification: <<sysadmin_password>>
```

After the upgrade is complete, the appliance reboots.

After the upgrade is complete, the appliance reboots. Verify the role of the appliance, using the following command:

```
dcnm2# appmgr show ha-role
Native HA enabled.
Deployed role: Standby
Current role: Standby
```

What to do next

Log on to the DCNM Web UI with appropriate credentials.

Click **Settings** icon and choose **About DCNM**. You can view and verify the Installation type that you have deployed.

Verify the role of both the appliances using the **appmgr show ha-role**

```
dcnm1# appmgr show ha-role
Native HA enabled.
Deployed role: Active
Current role: Active
```

```
dcnm2# appmgr show ha-role
Native HA enabled.
Deployed role: Standby
Current role: Standby
```

Verify the status of all applications using the **appmgr status all** command.

To gracefully onboard Cisco DCNM 10.4(2) or 11.0(1) managed VXLAN BGP EVPN fabric(s) comprising Cisco Nexus 9000 switches post upgrade to DCNM 11.1(1), see [Post DCNM 10.4\(2\) or 11.0\(1\) to DCNM 11.1\(1\) Upgrade for VXLAN BGP EVPN and MSD Fabrics](#).



CHAPTER 6

Disaster Recovery (Backup and Restore)

This chapter contains the following sections:

- [Backup and Restore Cisco DCNM and Application Data on Standalone DCNM setup, on page 63](#)
- [Backup and Restore Cisco DCNM and Application Data on Native HA setup, on page 64](#)
- [Recovering Cisco DCNM Single HA Node, on page 65](#)

Backup and Restore Cisco DCNM and Application Data on Standalone DCNM setup

You can take a backup of Cisco DCNM application data for analytics and troubleshooting. Perform the following task to take a backup of Cisco DCNM and Application data.

Procedure

- Step 1** Logon to the Cisco DCNM appliance using SSH.
- Step 2** Take a backup of the application data using the **appmgr backup** command.
- ```
dcnm# appmgr backup
```
- Copy the backup file to a safe location and shut down the DCNM Appliance.
- Step 3** Right click on the installed VM and select **Power > Power Off**.
- Step 4** Deploy the new DCNM appliance.
- Step 5** After the VM is powered on, click on **Console** tab.
- A message indicating that the DCNM appliance is configuring appears on the screen.
- Copy and paste the URL to the browser to continue with restore process.
- Step 6** On the DCNM Web Installer UI, click **Get Started**.
- Step 7** On the Cisco DCNM Installer screen, select **Fresh Installation with backup file for upgrade or restore** radio button.
- Select the backup file that was generated in [Step 2, on page 63](#).
- Continue to deploy the DCNM.

- Step 8** On the Summary tab, review the configuration details.
- Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** complete Cisco DCNM Virtual Appliance Installation for the chosen deployment mode.
- A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation.
- After the progress bar shows 100%, click **Continue**.
- Step 9** After the data is restored, check the status using the **appmgr status all** command.
- 

## Backup and Restore Cisco DCNM and Application Data on Native HA setup

You can take a backup of Cisco DCNM application data for analytics and troubleshooting. Perform the following task to take perform backup and restore of data in a Native HA setup.

### Before you begin

Ensure that the Active node is operating and functional.

### Procedure

---

- Step 1** Check if the Active node is operational. Otherwise, trigger a failover.
- Step 2** Logon to the Cisco DCNM appliance using SSH.
- Step 3** Take a backup of the application data using the **appmgr backup** command on both Active and Standby appliances.
- ```
dcnm1# appmgr backup
dcnm2 appmgr backup
```
- Copy the backup file of both active and standby appliances to a safe location and shut down the DCNM Appliance.
- Step 4** Right click on the installed VM and select **Power > Power Off**.
- Step 5** Deploy the new DCNM appliance in Native HA mode.
- Step 6** For both the Active and Standby appliances, after the VM is powered on, click on **Console** tab.
- A message indicating that the DCNM appliance is configuring appears on the screen.
- Copy and paste the URL to the browser to continue with restore process.
- Step 7** On the DCNM Web Installer UI, click **Get Started**.
- Step 8** On the Cisco DCNM Installer screen, select **Fresh Installation with backup file for upgrade or restore** radio button.
- Select the backup file that was generated in Step [Step 3, on page 64](#).
- The values for parameters are read from the backup file, and auto-populated. Modify the values, if required.

Continue to deploy the DCNM.

Step 9 On the Summary tab, review the configuration details.

Click **Previous** to go to the previous tabs and modify the configuration. Click **Start Installation** complete Cisco DCNM Virtual Appliance Installation for the chosen deployment mode.

A progress bar appears showing the completed percentage, description of the operation, and the elapsed time during the installation.

After the progress bar shows 100%, click **Continue**.

Step 10 After the data is restored, check the status using the **appmgr status all** command.

Recovering Cisco DCNM Single HA Node

This section details the scenarios and provides instructions to recover Cisco DCNM Single HA node.

The following table details all the recovery procedures when one or both the nodes fail in a Cisco DCNM Native HA set up.

Failure type	Node/Database to recover	Primary backup available	Secondary backup available	Recovery procedure
Primary node is lost. Secondary node is now Primary (due to fail over).	Primary Node	—	—	<ol style="list-style-type: none"> Convert Secondary node to Primary node. Configure new Secondary node.
Primary and Secondary server database is lost. Secondary node is now Primary (due to fail over)	Primary database	—	—	The Active Secondary node will restart and sync to the Standby Primary node.
Active Secondary node is lost. Primary node is now active due to fail over.	Secondary node	—	No	Configure new Secondary node.
Active Secondary node is lost. Primary node is not active due to fail over.	Secondary node	—	Yes	Configure new Secondary node, using the Web Installer. Choose Fresh installation with backup file for restore . Select Restore secondary DCNM node only in HA settings screen.
Secondary standby node is lost.	Secondary node	—	No	Configure new Secondary node.

Failure type	Node/Database to recover	Primary backup available	Secondary backup available	Recovery procedure
Secondary standby node lost	Secondary node	—	Yes	Configure new Secondary node, using the Web Installer. Choose Fresh installation with backup file for restore . Select Restore secondary DCNM node only in HA settings screen.
Primary node is active. Secondary standby database lost.	Secondary database	—	—	Primary node will restart to sync with Secondary node.

Converting Secondary node to Primary node

To convert the secondary node to Primary node, perform the following steps:

1. Log on to the DCNM server via SSH on the Secondary node.
2. Stop all the applications on the Secondary node by using the **appmgr stop all** command.
3. Navigate to the `ha-setup.properties` file.
4. Set the node ID to 1 to configure the secondary node as the primary node.

```
NODE_ID 1
```

After you change the node ID for the secondary node to 1, reboot the server. The old Secondary will restart as the new Primary Node. Consider the lost Primary as lost secondary node, and configure the new secondary node.

Configuring Secondary node

To configure the secondary node, perform the following steps:

1. Install a standalone Cisco DCNM. Use the same configuration settings as the lost secondary node.



Note If the Primary node was lost, and the old secondary node was converted to primary node, configure the new standalone node with the lost primary configuration.

2. Log on to the new DCNM standalone server via SSH, and stop all applications, using the **appmgr stop all** command.
3. Provide access to the `/root` directory on the new node, using the **appmgr root-access permit**.
4. Log on to the primary node via SSH, and stop all applications, using the **appmgr stop all** command.
5. Provide access to the `/root` directory on the Primary node, using the **appmgr root-access permit**.
6. On the Primary node, edit the `/root/.DO_NOT_DELETE` file. Set the **NATIVE_HA_STATUS** parameter to **NOT_TRIGGERED** on the primary node.
7. Configure the Primary node as Active, using the **appmgr setup native-ha active** command.

8. Configure the Secondary node as Standby, using the **appmgr setup native-ha secondary** command.



CHAPTER 7

Running Cisco DCNM Behind a Firewall

This chapter provides information about running Cisco DCNM behind a firewall.

- [Running Cisco DCNM Behind a Firewall, on page 69](#)

Running Cisco DCNM Behind a Firewall

Generally, an Enterprise (external world) and Data center is separated by a firewall, i.e., DCNM is configured behind a firewall. The Cisco DCNM Web Client and SSH connectivity must pass-through that firewall. Also, a firewall can be placed between the DCNM Server and DCNM-managed devices.

All Cisco DCNM Native HA nodes must be on the same side of the firewall. The internal DCNM Native HA ports are not listed, as it is not recommended to configure a firewall in between the Native HA nodes.



Note When you add or discover LAN devices in DCNM, ICMP echo packets are sent as part of the discovery process. If you have a firewall that blocks ICMP messages, the discovery process fails. You can skip sending the ICMP echo packets by setting the `cdp.discoverPingDisable` server property to `true`. For more information about how to set a server property, Cisco DCNM Web UI **Administration > DCNM Server > Server Properties**.

Any standard port where the Ingress traffic enters from clients cannot be modified unless you disable the local firewall.

The following table lists all ports that are used for communication between Cisco DCNM Web Client, SSH Client, and Cisco DCNM Server.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
22	TCP	SSH	Client to DCNM Server	SSH access to external world is optional.
443	TCP	HTTPS	Client to DCNM Server	This is needed to reach DCNM Web Server.

The following table lists all ports that are used for communication between Cisco DCNM Server and other services.



Note The services can be hosted on either side of the firewall.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
49	TCP/UDP	TACACS+	DCNM Server to DNS Server	ACS Server can be either side of the firewall.
53	TCP/UDP	DNS	DCNM Server to DNS Server	DNS Server can be either side of the firewall.
123	UDP	NTP	DCNM Server to NTP Server	NTP Server can be either side of the firewall.
5000	TCP	Docker Registry	Incoming to DCNM Server	Docker Registry Service on DCNM Server listening to requests from DCNM compute nodes.
5432	TCP	Postgres	DCNM Server to Postgres DB Server	Default installation of DCNM does not need this port. This is needed only when Postgres is installed external to the DCNM host machine.

The following table lists all ports that are used for communication between DCNM Server and managed devices:

Port Number	Protocol	Service Name	Direction of Communication	Remarks
22	TCP	SSH	Both Direction	DCNM Server to Device – To manage devices. Device to DCNM Server – SCP (POAP).

Port Number	Protocol	Service Name	Direction of Communication	Remarks
67	UDP	DHCP	Device to DCNM Server	
69	TCP	TFTP	Device to DCNM Server	Required for POAP
161	TCP/UDP	SNMP	Server to DCNM Device	DCNM configured via <code>server.properties</code> to use TCP uses TCP port 161, instead of UDP port 161.
514	UDP	Syslog	Device to DCNM Server	
2162	UDP	SNMP_TRAP	Device to DCNM Server	
33000-33499	TCP	gRPC	Device to DCNM Server	LAN Telemetry Streaming



CHAPTER 8

Secure Client Communications for Cisco DCNM Servers

This section describes how to configure HTTPS on Cisco Data Center Network Manager Servers.



Note You must enable SSL/HTTPS on the Cisco DCNM before you add a CA signed SSL certificate. Therefore, perform the procedure in the below mentioned order.

This section includes the following topics:

- [Secure Client Communications for Cisco DCNM Servers, on page 73](#)

Secure Client Communications for Cisco DCNM Servers

This section describes how to configure HTTPS on Cisco Data Center Network Manager Servers.



Note You must enable SSL/HTTPS on the Cisco DCNM before you add a CA signed SSL certificate. Therefore, perform the procedure in the below mentioned order.

This section includes the following topics:

Enabling SSL/HTTPS on Cisco DCNM in HA Environment on Virtual Appliance

To enable SSL/HTTPS on a Virtual Appliance for Cisco DCNM in HA mode, perform the following:

Procedure

Step 1 Configure the primary server with a self signed SSL certificate.

Note In a CA signed certificate, each server has their own certificate generated. Ensure that the certificate is signed by the signing certificate chain which is common for both the servers.

Step 2 On the secondary server, locate the keystore.

Step 3 Rename the keystore located at

```
<DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks  
to
```

```
<DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks.old
```

Step 4 Copy the file `fmserver.jks` generated in primary server to secondary server into folders

```
<dcnm-home> /dcm/wildfly-10.1.0.Final/standalone/configuration/  
<dcnm-home>/dcm/fm/conf/cert/
```

What to do next

If you have created a self-signed certificate or imported an SSL certificate to the keystore, you must copy the new `fmserver.jks` located at

```
/usr/local/cisco/dcm/wildfly-10.1.0.Final/standalone/configuration to  
/etc/elasticsearch. If you do not copy the fmserver.jks file to the elasticsearch directory, you will  
not be able to get the Alarms and Policies. As the elasticsearch database will be stabilizing, you cannot  
configure any Alarm Policy on the Cisco DCNM Web UI Monitor > Alarms > Alarm Policies.
```




CHAPTER 9

Managing Applications in a High-Availability Environment

This chapter describes how to configure a high-availability (HA) environment in your Cisco DCNM Open Virtual Appliance deployment for your Cisco Programmable Fabric solution. It also includes details about the HA functionality for each of the applications bundled within the Cisco DCNM Open Virtual Appliance.



Note Ensure that the NTP server is synchronized between active and standby peers is essential for proper HA functioning in DCNM

This chapter contains the following sections:

- [Information About Application Level HA in the Cisco DCNM Open Virtual Appliance, on page 75](#)
- [Native HA Failover and Troubleshooting, on page 76](#)
- [Application High Availability Details, on page 78](#)

Information About Application Level HA in the Cisco DCNM Open Virtual Appliance

To achieve HA for applications that are run on the Cisco DCNM Open Virtual Appliance, you can run two virtual appliances. You can run one in Active mode and the other in Standby mode.



Note This document refers to these appliances as OVA-A and OVA-B, respectively.

In this scenario:

1. All applications run on both appliances.
The application data is either constantly synchronized or applications share a common database as applicable.
2. Only one of the applications running on the two appliances serves the client requests. Initially this would be the applications running on OVA-A. The application continues to do so until one of the following happens:

- The application on OVA-A crashes.
 - The operating system on OVA-A crashes.
 - OVA-A is powered off for some reason.
3. At this point, the application running on the other appliance (OVA-B) takes over.
For DHCP, when the first node fails, the second node starts serving the IP addresses.
 4. The existing connections to OVA-A are dropped and the new connections are routed to OVA-B.
This scenario demonstrates why one of the nodes (OVA-A) is initially referred to as the Active node and OVA-B is referred as the Standby node.

Automatic Failover

The application-level and virtual machine (VM)-level and switchover process is as follows.

- If any of the applications managed by the load-balancing software (DCNM/AMQP) goes down on OVA-A, the Active node that handles the client requests detects the failure and redirects subsequent requests to the Standby node (OVA-B). This process provides an application-level switchover.
- If the Active node (OVA-A) fails or is powered-off for some reason, the Standby node (OVA-B) detects the failure and enables the VIP address for Cisco DCM/AMQP on OVA-B. It also sends a gratuitous ARP to the local switch to indicate the new MAC address that is associated with the IP address. For applications not using VIP, the DHCPD running on OVA-B detects the failure of DHCPD on OVA-A and activates itself; whereas LDAP running on OVA-B continues running as LDAP is deployed Active-Active. Consequently, a VM-level failover is accomplished for all four applications (DCNM/AMQP/DHCP/LDAP).

Manually Triggered Failovers

An application-level failover can also be triggered manually. For instance, you might want to run AMQP on OVA-B and the rest of the applications on OVA-A. In that case, you can log in to the SSH terminal of OVA-A and stop AMQP by using the **appmgr stop amqp** command.

This failover triggers the same process that is described in the [Automatic Failover, on page 76](#); subsequent requests to the AMQP Virtual IP address are redirected to OVA-B.

Native HA Failover and Troubleshooting

Due to the nature of Native HA, the role of the host might alternate from Active to Standby or from Standby to Active.

The following sections provide information on troubleshooting in different use cases.

Native HA Failover from Active Host to Standby Host

Perform the following steps when the Native HA failover occurs from Active to Standby host:

1. Log on to DCM Web UI, and navigate to **Administrator > Native HA**.

2. Verify the status of HA. If the DCNM HA status is not in **OK** mode, you cannot perform Failover operation. Click **Failover**. The Cisco DCNM server will shutdown and the DCNM Standby appliance will be operational.
3. Refresh the Cisco DCNM Web UI.
After the DCNM server is operational, you can log on to the DCNM Web UI.



Note We recommend that you do not run **appmgr stop all** or **appmgr stop ha-apps** commands on the Active host to trigger failover. If Cisco DCNM HA status is not in **OK** mode, a failover may cause loss of data, as the Standby DCNM appliance is not synchronized with the Active appliance before failover.

Issue with DCNM Application Framework

If DCNM Web UI is not accessible, and a failover operation is necessary, execute one of the following commands under Linux console:

appmgr failover—This command triggers the HA heartbeat failover.

Or

reboot -h now—This command triggers the Linux host to reboot, which causes a failover.

However, we recommend that you use DCNM Web UI to perform failover, as all other methods carry a risk of data loss when both HA peers are not in sync.

Stop and Restart DCNM

To completely stop DCNM and restart it, perform the following:

1. On the Standby appliance, stop all the applications by using the **appmgr stop all** command.
2. Check if all the applications have stopped, using the **appmgr status all** command.
3. On the Active appliance, stop all the applications using the **appmgr stop all** command.
4. Verify if all the applications are stopped using the **appmgr status all** command.
5. On the deployed Active host, start all the applications using the **appmgr start all** command.
Verify if all the applications are running. Log on to the DCNM Web UI to check if it is operational.
6. On the deployed Standby host, start all the applications using the **appmgr start all** command.
On the Web UI, navigate to **Administration > Native HA** and ensure that the HA status displays **OK**.

Restart Standby Host

Perform this procedure to restart only the Standby host:

1. On the Standby host, stop all the applications using the **appmgr stop all** command.
2. Verify if all the applications have stopped using the **appmgr status all** command.
3. Start all the applications using the **appmgr start all**.

On the Web UI, navigate to **Administration > Native HA** and ensure that the HA status displays **OK**.

Application High Availability Details

This section describes all of the Cisco Programmable Fabric HA applications.

Cisco DCNM Open Virtual Appliance has two interfaces: one that connects to the Open Virtual Appliance management network and one that connects to the enhanced Programmable Fabric network. Virtual IP addresses are defined for both interfaces.

- From the Open Virtual Appliance management network, the DCNM-REST API, DCNM interface, and AMQP are accessed through the VIP address
- From the enhanced fabric management network, LDAP and DHCP are accessed directly.

Only three Virtual IPs are defined:

- DCNM REST API (on dcnm management network)
- DCNM REST API (on enhanced fabric management network)
- AMQP (on dcnm management network)



Note Although DCNM Open Virtual Appliance in HA sets up a VIP, the VIP is intended to be used for the access of DCNM, REST API. For GUI access, we still recommend that you use the individual IP addresses of the DCNM HA peers and use the same to launch DCNM SAN Java clients, etc.

See the following table for a complete list of Programmable Fabric applications and their corresponding HA mechanisms.

Programmable Fabric Application	HA Mechanism	Use of Virtual IPs	Comments
Data Center Network Manager	DCNM Clustering/Federation	Yes	Two VIPs defined, one on each network
RabbitMQ	RabbitMQ Mirrored Queues	Yes	One VIP defined on the OVA management network
Repositories	—	—	External repositories have to be used

Data Center Network Management

The data center network management function is provided by the Cisco Data Center Network Manager (DCNM) server. Cisco DCNM provides the setup, visualization, management, and monitoring of the data center infrastructure. Cisco DCNM can be accessed from your browser at [http://\[host/ip\]](http://[host/ip]).



Note For more information about Cisco DCNM, see <http://cisco.com/go/dcnm>.

HA Implementation

Cisco DCNMs that run on both OVAs are configured in clustering and federated modes for HA. Cisco DCNM federation is the HA mechanism for SAN devices. Groups of SAN devices can be managed by each node in the DCNM federated setup. All the devices can be managed using a single client interface.

You can enable automatic failover in the Cisco DCNM UI by choosing: **Admin > Federation**. If you enable an automatic failover and the Cisco DCNM that is running on OVA-A fails, the automatic failover moves only the fabrics and shallow-discovered LANs that are managed by OVA-A to OVA-B automatically.

DCNM Virtual IP Usage

An Open Virtual Appliance HA setup has two VIP addresses (one for each network) for the Cisco DCNM at the default HTTP port. These VIPs can be used for accessing the DCNM RESTful services on the Open Virtual Appliance management network and the enhanced fabric management network. For example, external systems such as Cisco UCS Director can point to the VIP in the Open Virtual Appliance management network and the request gets directed to the active Cisco DCNM. Similarly, the switches in an enhanced fabric management network access the VIP address on the enhanced fabric management network during the POAP process.

You can still directly connect to Cisco DCNM real IP addresses and use them as you would in a DCNM in a cluster/federated set up.



Note Cisco recommends that you must use VIP addresses only for accessing DCNM REST API. To access the Cisco DCNM Web or SAN client, you must connect using the IP address of the server.

Licenses

For Cisco DCNM, we recommend that you have licenses on the first instance and a spare matching license on the second instance.

Application Failovers

Enable an automatic failover option in the Cisco DCNM UI when an Open Virtual Appliance HA pair is set up by choosing: **Administration > DCNM Server > Native HA**. This process ensures that if the DCNM that is running on OVA-A fails, all the fabrics and shallow-discovered LANs managed by DCNM-A are managed by DCNM-B automatically after a given time interval (usually about 5 minutes after the failure of DCNM on OVA-A).

The Cisco DCNM VIP address still resides on OVA-A. The Representational State Transfer Web Services (REST) calls initially hit the VIP addresses on OVA-A and get redirected to the Cisco DCNM that is running on OVA-B.

Application Failbacks

When the Cisco DCNM on OVA-A comes up, the VIP address automatically redirects the REST requests to DCNM-A.

Virtual-IP Failovers

The VIP address that is configured for Cisco DCNM REST API on OVA-A can fail due to two reasons:

- The load-balancing software running on OVA-A fails.
- OVA-A fails.

The VIP address of Cisco DCNM automatically migrates to OVA-B. The only difference is which DCNM will be used after the failover.

- If a load-balancing software failure occurs, the VIP address on OVA-B directs the requests to DCNM-A.
- If an OVA-A failure occurs, the VIP address on OVA-B directs the requests to DCNM-B.

The automatic failover ensures that the ownership of all of the fabrics and shallow-discovered LANs managed by DCNM-A automatically change to DCNM-B.

Virtual-IP Failbacks

When OVA-A is brought up and Cisco DCNM is running, the VIP addresses keep running on the Standby node. The failback of Virtual IP addresses from OVA-B to OVA-A occurs only in the following sequence.

1. OVA-A comes up.
2. Cisco DCNM runs on OVA-A.
3. OVA-B goes down or the load-balancing software fails on OVA-B.

RabbitMQ

RabbitMQ is the message broker that provides the Advanced Messaging Queuing Protocol (AMQP).



Note

You need to stop and restart AMQP on both DCNM's server in HA within 30 seconds, otherwise AMQP may not start. For more information about RabbitMQ, go to <https://www.rabbitmq.com/documentation.html>.

HA Implementation

Enabling the HA on the Open Virtual Appliance creates a VIP address in the Open Virtual Appliance management network. Orchestration systems such as vCloud Director, set their AMQP broker to the VIP address.

Enabling the HA on the Open Virtual Appliance also configures the RabbitMQ broker that runs on each node to be a duplicate of the broker that is running on the other node. Both OVAs act as “disk nodes” of a RabbitMQ cluster, which means that all the persistent messages stored in durable queues are replicated. The RabbitMQ policy ensures that all the queues are automatically replicated to all the nodes.

Application Failovers

If RabbitMQ-A fails, the VIP address on OVA-A redirects the subsequent AMQP requests to RabbitMQ-B.

Application Failbacks

When RabbitMQ-A comes up, the VIP address automatically starts directing the AMQP requests to RabbitMQ-A.

Virtual-IP Failovers

The VIP address configured for the AMQP broker on OVA-A can fail due to two reasons:

- The load-balancing software running on OVA-A fails.
- OVA-A fails.

In both cases, the VIP address of the AMQP automatically migrates to OVA-B. The only difference is which AMQP broker will be used after the failover.

- In a load-balancing software failure, the VIP address on OVA-B directs the requests to RabbitMQ-A.
- In an OVA-A failure, the VIP address on OVA-B directs the requests to RabbitMQ-B.

Virtual-IP Failbacks

When OVA-A is brought up and AMQP-A is running, the VIP addresses keep running on the OVA-B (directing the requests to AMQP-A). The failback of the RabbitMQ VIP from OVA-B to OVA-A occurs only in the following sequence.

1. OVA-A comes up.
2. RabbitMQ runs on OVA-A.
3. OVA-B goes down or the load-balancing software fails on OVA-B.

Repositories

All repositories must be remote.



CHAPTER 10

Managing Utility Services After DCNM Deployment

This chapter describes how to verify and manage all of the utility services that provide DC3 (Programmable Fabric) central point of management functions after the DCNM is deployed.

Table 5: Cisco DCNM Utility Services

Category	Application	Username	Password	Protocol Implemented
Network Management	Data Center Network Manager	admin	User choice ²	Network Management

² User choice refers to the administration password entered by the user during the deployment.

This chapter contains the following sections:

- [Editing Network Properties Post DCNM Installation, on page 83](#)
- [Utility Services Details, on page 95](#)
- [Managing Applications and Utility Services , on page 96](#)
- [Updating the SFTP Server Address for IPv6, on page 98](#)

Editing Network Properties Post DCNM Installation

The Cisco DCNM OVA or the ISO installation consists of 3 network interfaces:

- dcnm-mgmt network (eth0) interface

This network provides connectivity (SSH, SCP, HTTP, HTTPS) to the Cisco DCNM Open Virtual Appliance. Associate this network with the port group that corresponds to the subnet that is associated with the DCNM Management network.

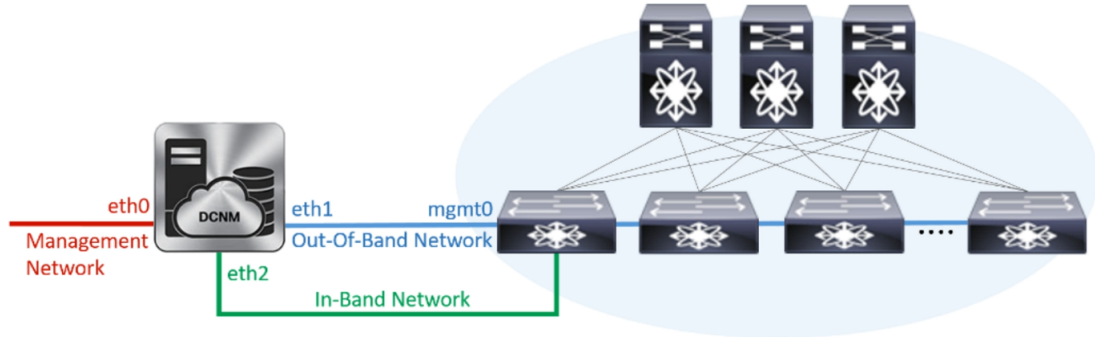
- enhanced-fabric-mgmt (eth1) interface

This network provides enhanced fabric management of Nexus switches. Associate this network with the port group that corresponds to management network of leaf and spine switches.

- enhanced-fabric-inband (eth2) interface

This network provides in-band connection to fabric. Associate this network with the port group that corresponds to a fabric in-band connection.

The following figure shows the network diagram for the Cisco DCNM Management interfaces.



During Cisco DCNM installation for your deployment type, you can configure these interfaces. However, from Cisco DCNM Release 11.2(1), you can edit and modify the network settings post installation.



Note We recommend that you use **appmgr** commands to update network properties. Do not restart network interfaces manually.

You can modify the parameters as explained in the following sections:

Modifying Network Interfaces (eth0 and eth1) Post DCNM Installation

Along with the eth0 and eth1 IP address (IPv4 and/or IPv6), you can also modify the DNS and the NTP server configuration using the **appmgr update network-properties** command.

For step-by-step instructions on how to modify the network parameters using the **appmgr update network-properties** commands, see the following sections.

- [Modifying Network Properties on DCNM in Standalone Mode, on page 84](#)
Sample Command Output for Modifying Network Parameters in the Cisco DCNM Standalone Setup, on page 85
- [Modifying Network Properties on DCNM in Native HA Mode, on page 86](#)
Sample Command Output for Modifying Network Parameters in the Cisco DCNM Native HA Setup, on page 87

Modifying Network Properties on DCNM in Standalone Mode

The following sample shows the output for the **appmgr update network-properties** command for a Cisco DCNM Standalone Appliance.



Note Execute the following commands on the DCNM Appliance console to avoid a premature session timeout.

1. Initiate a session on the console, using the following command:
appmgr update network-properties session start
2. Update the Network Properties using the following command:
appmgr update network-properties set ipv4 {eth0|eth1}<ipv4-address> <network-mask> <gateway>
Enter the new IPv4 address for the Management (eth0) interface, along with the subnet mask and gateway IP addresses.
3. View and verify the changes by using the following command:
appmgr update network-properties session show {config | changes | diffs}
4. After you validate the changes, apply the configuration using the following command:
appmgr update network-properties session apply
Wait for a few minutes before you can logon to the Cisco DCNM Web UI using the eth0 Management Network IP address.

Sample Command Output for Modifying Network Parameters in the Cisco DCNM Standalone Setup

The following sample example shows how to modify the network parameters post installation for a Cisco DCNM Standalone setup.

```

dcnm# appmgr update network-properties session start

dcnm# appmgr update network-properties set ipv4 eth0 172.28.10.244 255.255.255.0 172.28.10.1
dcnm# appmgr update network-properties set ipv4 eth1 100.0.0.244 255.0.0.0
*****
WARNING: fabric/poap configuration may need to be changed
manually after changes are applied.
*****

dcnm# appmgr update network-properties session show changes
eth0 IPv4 addr 172.28.10.246/255.255.255.0 -> 172.28.10.244/255.255.255.0
eth1 IPv4 addr 1.0.0.246/255.0.0.0 -> 100.0.0.244/255.0.0.0

dcnm# appmgr update network-properties session apply
*****
WARNING

Applications of both nodes of the DCNM HA system need to be stopped
for the changes to be applied properly.

PLEASE STOP ALL APPLICATIONS MANUALLY
*****

Have applications been stopped? [y/n]: y
Applying changes
DELETE 1
Node left the swarm.
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
log4j:WARN No appenders could be found for logger (fms.db).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
UPDATE 1
UPDATE 1
DELETE 1

```

```

server signaled
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the
'tentative' state
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the
'tentative' state
*****
Please run 'appmgr start afw; appmgr start all' to restart your nodes.
*****

dcnm# appmgr start afw; appmgr start all
Started AFW Server Processes
Started AFW Agent Processes
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO: Resource is stopped
Done.

Warning: PID file not written; -detached was passed.
AMQP User Check
Started AFW Server Processes
Started AFW Agent Processes
dcnm#

```

Modifying Network Properties on DCNM in Native HA Mode

The following sample shows output to modify the network parameters using the **appmgr update network-properties** command for a Cisco DCNM Native HA Appliance.



Note

- Execute the following commands on the DCNM Active and Standby node console to avoid premature session timeout.
- Ensure that you execute the commands in the same order as mentioned in the following steps.

1. Stop the DCNM Applications on the Standby node by using the following command:

```
appmgr stop all
```

Wait until all the applications stop on the Standby node before you go proceed.

2. Stop the DCNM Applications on the Active node by using the following command:

```
appmgr stop all
```

3. Initiate a session on the Cisco DCNM console of both the Active and Standby nodes by using the following command:

```
appmgr update network-properties session start
```

4. On the Active node, modify the network interface parameters by using the following commands:

- a. Configure the IP address for eth0 and eth1 address by using the following command:

```
appmgr update network-properties set ipv4 {eth0|eth1}<ipv4-address> <network-mask>
<gateway>
```

Enter the new IPv4 or IPv6 address for the eth1 interface, along with the subnet mask and gateway IP addresses.

- b. Configure the VIP IP address by using the following command:

```
appmgr update network-properties set ipv4 {vip0|vip1}<ipv4-address> <network-mask>
```

Enter the vip0 address for eth0 interface. Enter the vip1 address for eth1 interface.

- c. Configure the peer IP address by using the following command:

```
appmgr update network-properties set ipv4 {peer0|peer1}<ipv4-address>
```

Enter the eth0 address of the Standby node as peer0 address for Active node. Enter the eth1 address of the Standby node as peer1 address for Active node.

- d. View and validate the changes that you have made to the network parameters by using the following command:

```
appmgr update network-properties session show {config | changes | diffs}
```

View the changes that you have configured by using the following command:

5. On the Standby node, modify the network interface parameters using the commands described in [Step 4](#).
6. After you validate the changes, apply the configuration on the Active node by using the following command:

```
appmgr update network-properties session apply
```

Wait until the prompt returns, to confirm that the network parameters are updated.

7. After you validate the changes, apply the configuration on the Standby node by using the following command:

```
appmgr update network-properties session apply
```

8. Start all the applications on the Active node by using the following command:

```
appmgr start all
```



Note

Wait until all the applications are running successfully on the Active node, before proceeding to the next step.

9. Start all the applications on the Standby node by using the following command:

```
appmgr start all
```

10. Establish peer trust key on the Active node by using the following command:

```
appmgr update ssh-peer-trust
```

11. Establish peer trust key on the Standby node by using the following command:

```
appmgr update ssh-peer-trust
```

Sample Command Output for Modifying Network Parameters in the Cisco DCNM Native HA Setup

The following sample example shows how to modify the network parameters post installation for a Cisco DCNM Native HA setup.



Note For example, let us indicate Active and Standby appliances as **dcnm1** and **dcnm2** respectively.

```
[root@dcnm2]# appmgr stop all
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.

Stopping and halting node rabbit@dcnm2 ...
Note: Forwarding request to 'systemctl enable rabbitmq-server.service'.
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
[root@dcnm2]#

[root@dcnm1]# appmgr stop all
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.

Stopping and halting node rabbit@dcnm1 ...
Note: Forwarding request to 'systemctl enable rabbitmq-server.service'.
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
[root@dcnm1]#

[root@dcnm1]# appmgr update network-properties session start
[root@dcnm2]# appmgr update network-properties session start

[root@dcnm1]# appmgr update network-properties set ipv4 eth0 172.28.10.244 255.255.255.0
172.28.10.1
[root@dcnm1]# appmgr update network-properties set ipv4 eth1 100.0.0.244 255.0.0.0
*****
WARNING: fabric/poap configuration may need to be changed
manually after changes are applied.
*****
[root@dcnm1]# appmgr update network-properties set ipv4 vip0 172.28.10.238 255.255.255.0
[root@dcnm1]# appmgr update network-properties set ipv4 vip1 100.0.0.238 255.0.0.0
[root@dcnm1]# appmgr update network-properties set ipv4 peer0 172.28.10.245
[root@dcnm1]# appmgr update network-properties set ipv4 peer1 100.0.0.245
[root@dcnm1]# appmgr update network-properties session show changes

[root@dcnm2]# appmgr update network-properties set ipv4 eth0 172.28.10.245 255.255.255.0
172.28.10.1
[root@dcnm2]# appmgr update network-properties set ipv4 eth1 100.0.0.245 255.0.0.0
*****
WARNING: fabric/poap configuration may need to be changed
manually after changes are applied.
*****
[root@dcnm2]# appmgr update network-properties set ipv4 vip0 172.28.10.238 255.255.255.0
[root@dcnm2]# appmgr update network-properties set ipv4 vip1 100.0.0.238 255.0.0.0
[root@dcnm2]# appmgr update network-properties set ipv4 peer0 172.28.10.244
[root@dcnm2]# appmgr update network-properties set ipv4 peer1 100.0.0.244
[root@dcnm2]# appmgr update network-properties session show changes
```

```
[root@dcnm1]# appmgr update network-properties session show changes
eth0 IPv4 addr 172.28.10.246/255.255.255.0 -> 172.28.10.244/255.255.255.0
eth1 IPv4 addr 1.0.0.246/255.0.0.0 -> 100.0.0.244/255.0.0.0
eth0 VIP 172.28.10.248/24 -> 172.28.10.238/24
eth1 VIP 1.0.0.248/8 -> 100.0.0.238/8
Peer eth0 IP 172.28.10.247 -> 172.28.10.245
Peer eth1 IP 1.0.0.245 -> 100.0.0.245
```

```
[root@dcnm1]# appmgr update network-properties session show config
```

```
=====  
Current configuration  
=====  
NTP Server 1.ntp.esl.cisco.com  
eth0 IPv4 addr 172.28.10.246/255.255.255.0  
eth0 IPv4 GW 172.28.10.1  
eth0 DNS 171.70.168.183  
eth0 IPv6 addr 2001:420:284:2004:4:112:210:20/112  
eth0 IPv6 GW 2001:420:284:2004:4:112:210:1  
eth1 IPv4 addr 1.0.0.246/255.0.0.0  
eth1 IPv4 GW  
eth1 DNS 1.0.0.246  
eth1 IPv6 addr  
eth2 IPv4 addr /  
eth2 IPv4 GW  
Peer eth0 IP 172.28.10.247  
Peer eth1 IP 1.0.0.247  
Peer eth2 IP  
eth0 VIP 172.28.10.248/24  
eth1 VIP 1.0.0.248/8  
eth2 VIP /  
eth0 VIPv6 /  
eth1 VIPv6 /
```

```
=====  
Session configuration  
=====  
NTP Server 1.ntp.esl.cisco.com  
eth0 IPv4 addr 172.28.10.244/255.255.255.0  
eth0 IPv4 GW 172.28.10.1  
eth0 DNS 171.70.168.183  
eth0 IPv6 addr 2001:420:284:2004:4:112:210:20/112  
eth0 IPv6 GW 2001:420:284:2004:4:112:210:1  
eth1 IPv4 addr 100.0.0.244/255.0.0.0  
eth1 IPv4 GW  
eth1 DNS 1.0.0.246  
eth1 IPv6 addr  
eth2 IPv4 addr /  
eth2 IPv4 GW  
Peer eth0 IP 172.28.10.245  
Peer eth1 IP 100.0.0.245  
Peer eth2 IP  
eth0 VIP 172.28.10.238/24  
eth1 VIP 100.0.0.238/8  
eth2 VIP /  
eth0 VIPv6 /  
eth1 VIPv6 /  
[root@dcnm1]#
```

```
[root@dcnm2]# appmgr update network-properties session show config
```

```
=====  
Current configuration  
=====  
NTP Server 1.ntp.esl.cisco.com  
eth0 IPv4 addr 172.28.10.247/255.255.255.0  
eth0 IPv4 GW 172.28.10.1  
eth0 DNS 171.70.168.183  
eth0 IPv6 addr  
eth0 IPv6 GW  
eth1 IPv4 addr 1.0.0.247/255.0.0.0
```

```

eth1 IPv4 GW
eth1 DNS      1.0.0.247
eth1 IPv6 addr
eth2 IPv4 addr /
eth2 IPv4 GW
Peer eth0 IP  172.28.10.246
Peer eth1 IP  1.0.0.246
Peer eth2 IP
eth0 VIP      172.28.10.248/24
eth1 VIP      1.0.0.248/8
eth2 VIP      /
eth0 VIPv6    /
eth1 VIPv6    /

```

```

===== Session configuration =====
NTP Server    1.ntp.esl.cisco.com
eth0 IPv4 addr 172.28.10.245/255.255.255.0
eth0 IPv4 GW   172.28.10.1
eth0 DNS       171.70.168.183
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr 100.0.0.245/255.0.0.0
eth1 IPv4 GW
eth1 DNS       1.0.0.247
eth1 IPv6 addr
eth2 IPv4 addr /
eth2 IPv4 GW
Peer eth0 IP   172.28.10.244
Peer eth1 IP   100.0.0.244
Peer eth2 IP
eth0 VIP       172.28.10.238/24
eth1 VIP       100.0.0.238/8
eth2 VIP       /
eth0 VIPv6    /
eth1 VIPv6    /
[root@dcnm2]#

```

```
[root@dcnm1]# appmgr update network-properties session apply
```

```
*****
```

WARNING

Applications of both nodes of the DCNM HA system need to be stopped for the changes to be applied properly.

PLEASE STOP ALL APPLICATIONS MANUALLY

```
*****
```

```
Have applications been stopped? [y/n]: y
```

```
Applying changes
```

```
DELETE 1
```

```
Node left the swarm.
```

```
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
```

```
log4j:WARN No appenders could be found for logger (fms.db).
```

```
log4j:WARN Please initialize the log4j system properly.
```

```
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
```

```
UPDATE 1
```

```
UPDATE 1
```

```
DELETE 1
```

```
server signaled
```

```
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the 'tentative' state
```

```
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the 'tentative' state
```

```
*****
```



```

Please run 'appmgr start afw; appmgr start all' to restart your nodes.
*****
*****
Please run 'appmgr update ssh-peer-trust' on the peer node.
*****
[root@dcnm1]#

[root@dcnm2]# appmgr update network-properties session apply
*****
WARNING

Applications of both nodes of the DCNM HA system need to be stopped
for the changes to be applied properly.

PLEASE STOP ALL APPLICATIONS MANUALLY
*****

Have applications been stopped? [y/n]: y
Applying changes
DELETE 1
Node left the swarm.
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
log4j:WARN No appenders could be found for logger (fms.db).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
UPDATE 1
UPDATE 1
DELETE 1
afwnetplugin:0.1
server signaled
*****
Please run 'appmgr start afw; appmgr start all' to restart your nodes.
*****
*****
Please run 'appmgr update ssh-peer-trust' on the peer node.
*****
[root@dcnm2]#

[root@dcnm1]# appmgr start afw; appmgr start all
Started AFW Server Processes
Started AFW Agent Processes
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO: Resource is stopped
Done.

Warning: PID file not written; -detached was passed.
AMQP User Check
Started AFW Server Processes
Started AFW Agent Processes
[root@dcnm1]#

Wait until dcnm1 becomes active again.

[root@dcnm2]# appmgr start afw; appmgr start all
Started AFW Server Processes
Started AFW Agent Processes
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO: Resource is stopped

```

Done.

```
Warning: PID file not written; -detached was passed.
AMQP User Check
Started AFW Server Processes
Started AFW Agent Processes
[root@dcnm2]#
```

```
[root@dcnm1]# appmgr update ssh-peer-trust
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1
```

```
Now try logging into the machine, with: "ssh -o 'StrictHostKeyChecking=no' '172.28.10.245'"
and check to make sure that only the key(s) you wanted were added.
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1
```

```
Now try logging into the machine, with: "ssh -o 'StrictHostKeyChecking=no' '100.0.0.245'"
and check to make sure that only the key(s) you wanted were added.
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1
Now try logging into the machine, with: "ssh -o 'StrictHostKeyChecking=no'
'dcnm-247.cisco.com'"
and check to make sure that only the key(s) you wanted were added.
[root@dcnm1]#
```

```
[root@dcnm2]# appmgr update ssh-peer-trust
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1
```

```
Now try logging into the machine, with: "ssh -o 'StrictHostKeyChecking=no' '172.28.10.244'"
and check to make sure that only the key(s) you wanted were added.
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1
```

```
Now try logging into the machine, with: "ssh -o 'StrictHostKeyChecking=no' '100.0.0.244'"
and check to make sure that only the key(s) you wanted were added.
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1
```

```
Now try logging into the machine, with: "ssh -o 'StrictHostKeyChecking=no'
'dcnm-246.cisco.com'"
and check to make sure that only the key(s) you wanted were added.
[root@dcnm2]#
```

Configuring Enhanced-Fabric-Inband Interface (eth2) Post DCNM Installation

During the DCNM installation, you can configure the In-Band Management interface. You must associate this network with the port group that corresponds to a fabric in-band connection. The In-Band Network provides reachability to the devices via the front-panel ports.



Note If you need to modify the already configured in-band network (eth2 interface), execute the **ifconfig eth2 0.0.0.0** command and run the **appmgr setup inband** command again.



Note You cannot use Endpoint Locator and Telemetry features if the eth2 interface is not configured.

To configure the eth2 interface for the in-band management network, use the **appmgr setup inband** command.

The following example shows a sample output for the **appmgr setup inband** command for a Cisco DCNM Standalone Appliance.

```
[root@dcnm]# appmgr setup inband
Configuring Interface for InBand Connectivity...
Please enter the information as prompted:
InBand Physical IP [e.g. 2.2.2.69]: 2.0.0.250
InBand Network Mask [e.g. 255.255.255.0]: 255.0.0.0
InBand Gateway [e.g. 2.2.2.1]: 2.0.0.1
Validating Inputs ...

You have entered these values..
PIP=2.0.0.250
NETMASK=255.0.0.0
GATEWAY=2.0.0.1

Press 'y' to continue configuration, 'n' to discontinue [y] y
{"ResponseType":0,"Response":"Refreshed"}
{"ResponseType":0,"Response":{"AfwServerEnabled":true,"AfwServerReady":true,"InbandSubnet":"2.0.0.0/8",
"InbandGateway":"2.0.0.1","OutbandSubnet":"0.0.0.0/8","OutbandGateway":"0.0.0.0","UnclusteredMode":true}}

Done.
[root@dcnm]#
```

The following example shows a sample output for the **appmgr setup inband** command for a Cisco DCNM Native HA Appliance.

On Cisco DCNM Primary appliance:

```
[root@dcnm-primary]# appmgr setup inband
Configuring Interface for InBand Connectivity...
Please enter the information as prompted:
InBand Physical IP [e.g. 2.2.2.69]: 2.0.0.244
InBand Network Mask [e.g. 255.255.255.0]: 255.0.0.0
InBand Gateway [e.g. 2.2.2.1]: 2.0.0.1
InBand Virtual IP for HA setup [e.g. 2.2.2.60]: 2.0.0.243
InBand Virtual Network Mask [mandatory for HA setup] [e.g. 255.255.255.0]: 255.0.0.0
Peer Inband IP [mandatory for HA setup] [e.g. 2.2.2.59]: 2.0.0.244
Validating Inputs ...

You have entered these values..
PIP=2.0.0.244
NETMASK=255.0.0.0
GATEWAY=2.0.0.1
VIP=2.0.0.243
VIP_NETMASK=255.0.0.0
PEER_ETH2=2.0.0.244

Press 'y' to continue configuration, 'n' to discontinue [y] y

Done.
[root@dcnm-primary]#
```

On Cisco DCNM Secondary appliance:

```
[root@dcnm-secondary]# appmgr setup inband
Configuring Interface for InBand Connectivity...
Please enter the information as prompted:
InBand Physical IP [e.g. 2.2.2.69]: 2.0.0.245
InBand Network Mask [e.g. 255.255.255.0]: 255.0.0.0
InBand Gateway [e.g. 2.2.2.1]: 2.0.0.1
InBand Virtual IP for HA setup [e.g. 2.2.2.60]: 2.0.0.243
InBand Virtual Network Mask [mandatory for HA setup] [e.g. 255.255.255.0]: 255.0.0.0
Peer Inband IP [mandatory for HA setup] [e.g. 2.2.2.59]: 2.0.0.244
Validating Inputs ...

You have entered these values..
PIP=2.0.0.245
NETMASK=255.0.0.0
GATEWAY=2.0.0.1
VIP=2.0.0.243
VIP_NETMASK=255.0.0.0
PEER_ETH2=2.0.0.244

Press 'y' to continue configuration, 'n' to discontinue [y] y
HA Role is Active {"ResponseType":0,"Response":"Refreshed"}
Done.

[root@dcnm-secondary]#
```

Changing the DCNM Server Password Post DCNM Installation

The password to access Cisco DCNM Web UI is configured while installing the Cisco DCNM for your deployment type. However, you can modify this password post installation also, if required.

To change the password post installation, perform the following steps:

Procedure

-
- Step 1** Stop the applications using the **appmgr stop all** command.
- Wait until all the applications stop running.
- Step 2** Change the password for the management interface by using the **appmgr change_pwd ssh {root|poap}[password]** command.
- Ensure that the new password adheres to the following password requirements. If you do not comply with the requirements, the DCNM application might not function properly:
- It must be at least 8 characters long and contain at least one alphabet and one numeral.
 - It can contain a combination of alphabets, numerals, and special characters.
 - Do not use any of these special characters in the DCNM password: <SPACE> " & \$ % ' ^ = < > ; : ` \ | / , . *
- Step 3** Start the application using the **appmgr start all** command.
-

Utility Services Details

This section describes the details of all the utility services within the functions they provide in Cisco DCNM. The functions are as follows:

Network Management

The data center network management function is provided by the Cisco Data Center Network Manager (DCNM) server. Cisco DCNM provides the setup, visualization, management, and monitoring of the data center infrastructure. Cisco DCNM can be accessed from your browser: `http://<<hostname/IP address>>`.



Note For more information about Cisco DCNM, see <http://cisco.com/go/dcnm>.

Orchestration

RabbitMQ

Rabbit MQ is the message broker that provides the Advanced Messaging Queuing Protocol (AMQP). The RabbitMQ message broker sends events from the vCloud Director/vShield Manager to the Python script for parsing. You can configure this protocol by using certain CLI commands from the Secure Shell (SSH) console of the firmware.



Note You need to stop and restart AMQP on both DCNM's server in HA within 30 seconds, otherwise AMQP may not start. For more information about RabbitMQ, go to <https://www.rabbitmq.com/documentation.html>.

After upgrade, enable RabbitMQ management service stop the service and start the services using the following commands:

```
dcnm# appmgr stop amqp
dcnm# appmgr start amqp
```

If AMQP is not running, the memory space must be exhausted that is indicated in the file `/var/log/rabbitmq/erl_crash.dump`.

Device Power On Auto Provisioning

Power On Auto Provisioning (POAP) occurs when a switch boots without any startup configuration. It is accomplished by two components that were installed:

- DHCP Server

The DHCP server parcels out IP addresses to switches in the fabric and points to the location of the POAP database, which provides the Python script and associates the devices with images and configurations.

During the Cisco DCNM installation, you define the IP Address for the inside fabric management address or OOB management network and the subnets associated with the Cisco Programmable Fabric management.

- Repositories

The TFTP server hosts boot scripts that are used for POAP.

The SCP server downloads the database files, configuration files, and the software images.

Managing Applications and Utility Services

You can manage the applications and utility services for Cisco Programmable Fabric in the Cisco DCNM through commands in an SSH terminal.

Enter the **appmgr** command from the SSH terminal by using the following credentials:

- Username: **root**
- Password: **Administrative password provided during deployment**



Note For your reference, context sensitive help is available for the **appmgr** command. Use the **appmgr** command to display help.

Use the **appmgr tech_support** command to produce a dump of the log files. You can then provide this information to the TAC team for troubleshooting and analysis of your setup.



Note This section does not describe commands for Network Services using Cisco Prime Network Services Controller.

This section includes the following:

Verifying the Application and Utility Services Status after Deployment

After you deploy the OVA/ISO file, you can determine the status of various applications and utility services that were deployed in the file. You can use the **appmgr status** command in an SSH session to perform this procedure.



Note Context-sensitive help is available for the **appmgr status** command. Use the **appmgr status ?** command to display help.

Procedure

Step 1 Open up an SSH session:

- a) Enter the `ssh root DCNM network IP address` command.
- b) Enter the administrative password to login.

Step 2 Check the status by using the following command:

appmgr status all

Example:

```
DCNM Status
PID  USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM  TIME+  COMMAND
===  =====  ==  ==  =====  ==  ==  =  =====  =====  =====  =====
1891 root    20  0  2635m  815m  15m  S  0.0  21.3   1:32.09  java
```

```
LDAP Status
PID  USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM  TIME+  COMMAND
===  =====  ==  ==  =====  ==  ==  =  =====  =====  =====  =====
1470 ldap    20  0  692m  12m  4508  S  0.0  0.3    0:00.02  slapd
```

```
AMQP Status
PID  USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM  TIME+  COMMAND
===  =====  ==  ==  =====  ==  ==  =  =====  =====  =====  =====
1504 root     20  0  52068  772  268  S  0.0  0.0    0:00.00  rabbitmq
```

```
TFTP Status
PID  USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM  TIME+  COMMAND
===  =====  ==  ==  =====  ==  ==  =  =====  =====  =====  =====
1493 root     20  0  22088  1012  780  S  0.0  0.0    0:00.00  xinetd
```

```
DHCP Status
PID  USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM  TIME+  COMMAND
===  =====  ==  ==  =====  ==  ==  =  =====  =====  =====  =====
1668 dhcpd  20  0  46356  3724  408  S  0.0  0.0    0:05.23  dhcp
```

Stopping, Starting, and Resetting Utility Services

Use the following CLI commands for stopping, starting, and resetting utility services:

- To stop an application, use the **appmgr stop** command.

```
dcnm# appmgr stop dhcp
Shutting down dhcpd:      [ OK ]
```

- To start an application, use the **appmgr start** command.

```
dcnm# appmgr start amqp
Starting vsftpd for amqp: [ OK ]
```

- To restart an application use the **appmgr restart** command.

```
# appmgr restart tftp
Restarting TFTP...
Stopping xinetd:         [ OK ]
Starting xinetd:         [ OK ]
```



Note From Cisco DCNM Release 7.1.x, when you stop an application by using the **appmgr stop *app_name*** command, the application will not start during successive reboots.

For example, if DHCP is stopped by using the **appmgr stop dhcp** command, and the OS is rebooted, the DHCP application will still be down after the OS is up and running.

To start again, use the command **appmgr start dhcp**. The DHCP application will be started after reboots also. This is to ensure that when an environment uses an application that is not packaged as part of the virtual appliance (like CPNR instead of DHCP), the application locally packaged with the virtual appliance will not interfere with its function after any OS reboots.



Note When a DCNM appliance (ISO/OVA) is deployed, the Cisco SMIS component will not get started by default. However, this component can be managed using the appmgr CLI: **appmgr start/stop dcnm-smis**
appmgr start/stop dcnm will start or stop only the DCNM web component.

Updating the SFTP Server Address for IPv6

After deploying the DCNM OVA/ISO successfully with EFM IPv4 and IPv6, by default the SFTP address is pointed to IPv4 only. You need to change the IPv6 address manually in the following two places:

- In the DCNM Web Client, choose **Administration > Server Properties** and then update the below fields to IPv6 and click the **Apply Changes** button.

```
#
# GENERAL>xFTP CREDENTIAL
#
# xFTP server's ip address for copying switch files:
server.FileServerAddress
```

- Log in to the DCNM through ssh and update the SFTP address with IPv6 manually in the server.properties file (/usr/local/cisco/dcm/fm/conf/server.properties).

```
# xFTP server's ip address for copying switch files:
server.FileServerAddress=2001:420:5446:2006::224:19
```