Cisco DCNM Installation Guide for Media Controller Deployment, Release 11.0(1)

First Published: 2019-02-14

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 NONINFRINGEMENT 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

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 datacenter network infrastructure, the Cisco DCNM provides a comprehensive feature-set that meets the routing, switching, and storage administration needs of datacenters. 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

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. Performance Manager stores data into Elastic search time series database. API access to Elastic search is not supported.

collection will backup files on Elastic Search which aids in better scalability and API access.

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. Image signature can be verified by following the steps in 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 (.iso). The installer is a bundle of OS, DCNM and other applications needed for Dynamic Fabric Automation.

Deployment Options

The installer available for Cisco DCNM can be deployed in one of the below 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

The DCNM Virtual appliances, both OVA and ISO, can be deployed in High Availability mode to have resilience in case of application or OS failures.

Upgrade Paths

Prior to Cisco DCNM Release 11.0(1), DCNM OVA and ISO supported SAN functionality. Beginning with Cisco DCNM 11.0(1), OVA and ISO does not ship with SAN support. You can upgrade to Release 11.0(1) only from DCNM Release 10.4(2).

System Requirements for Cisco DCNM, Release 11.0(1)

Server Requirements

Cisco DCNM, Release 11.0(1), supports the Cisco DCNM Server on these 64 bit operating systems:

- **LAN Fabric, Classic LAN, and IP For Media (IPFM) Deployments:**
    - Open Virtual Appliance (OVA) with integrated Operating System

- ISO Virtual Appliance (ISO) with integrated Operating System

Cisco DCNM Release 11.0(1) supports the following databases:

- PostgreSQL 9.4.5

Note Cisco DCNM 11.0(1) for LAN is not supported with an external database.

Note The ISO/OVA installation only supports the embedded PostreSQL 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 11.0(1) supports ISO installation on a bare-metal server (no hypervisor) on the following server platform:

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 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 RAID operation (large)
Cisco UCS C240 M5S	UCSC-C240-M5SX	24G / 500G 8-vCPU Cores with Cisco hardware RAID Controller [UCSC-SAS-M5] for RAID operation (small)
Cisco UCS C220 M5L	UCSC-C220-M5L	24G / 500G 32G / 500G 16-vCPU Cores with Cisco hardware RAID Controller [UCSC-SAS-M5] for RAID operation (small)

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

Cisco DCNM Release 11.0(1) supports the running of the Cisco DCNM Server on the following hypervisors:

- VMware ESXi 5.5
- VMware ESXi 6.0
- VMware ESXi 6.5
- VMware ESXi 6.7
- VMware ESXi 6.7 U1
- VMware vCenter 6.0
- VMware vCenter 6.5
- VMware vCenter 6.7
- VMware vCenter 6.7 U1

Note

- vCenter server is mandatory to deploy the Cisco DCNM OVA Installer.
- When you log into the VMware vSphere Web Client, the Adobe Shockwave Flash crashes with the latest Google Chrome 62.0.3202.62 (64 bit), Mozilla Firefox 56.0.1 (64 bit), and Internet Explorer 8.0.7601.17514. Hence you cannot install Cisco DCNM on VMware ESX using VMware vSphere Web Client. This is a known issue with Adobe Shockwave Flash version 27.0.0.159. For more information, see https://kb.vmware.com/s/article/2151945.

Server Resource Requirements

Table 1: Server Resource Requirements

Deployment	Deployment Type	Small (Lab or POC)	Large (Production)
LAN Fabric, Classic LAN, IP For Media (IPFM)	OVA	CPU: 8 vCPUs RAM: 24 GB RAM DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB
LAN Fabric, Classic LAN, IP For Media (IPFM)	ISO	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 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

The SAN Insights feature is not supported on small deployment.

The Cisco DCNM Release 11.0(1) does not support OVA/ISO for SAN.

Supported Web Browsers

Cisco DCNM supports the following web browsers:

- Mozilla Firefox Version 61.0 (64/32 bit)
- Microsoft Internet Explorer 11.0.9600.19035CO update Version: 11.0.65(KB4230450)
- Google Chrome version 67.0.3396.99 (Official Build)

Other Supported Software

The following table lists the other software that are supported by Cisco DCNM, Release 11.0(1).

Table 2: Other Supported Software

Component	Minimum Requirements
Security	• 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
DHCP Server	• Cisco Network Registrar 8.2
OVA/ISO Installers	CentOS 7.4 / Linux Kernel 3.10.x

Clearing Browser Cache

While upgrading, Cisco DCNM allows you to use the same IP Addresses for Release 11.0(1) that were used for Release 10.4(2). To optimize loading times, DCNM 11 stores scripts and other assets in a browser's offline storage. Therefore, you must clear the browser cache before you launch the Cisco DCNM 11.0(1) Web UI using the Management Network IP address.

Cisco DCNM supports the following web browsers:

- Mozilla Firefox
- Microsoft Internet Explorer
- Google Chrome version

Based on your browser, you can perform the following task to clear the browser cache.

Mozilla Firefox

To clear cache on the Mozilla Firefox browser, perform the following task:

1. From the History menu, select **Clear Recent History**.

   If the menu bar is hidden, press **Alt** to make it visible.

2. From the **Time range to clear:** drop-down list, select the desired range. To clear your entire cache, select all options.

3. Click the down arrow next to Details to choose which elements of the history to clear. To clear the entire cache, select all items.

   Click **Clear Now**.

4. Restart browser.

Google Chrome

To clear cache on the Google Chrome browser, perform the following task:

1. In the browser bar, enter **chrome://settings/clearBrowserData**, and press **Enter**.

2. On the Advanced tab, select the following:

   - Cookies and other site data
   - Cached images and files

3. From the **Time range** drop-down list, you can choose the period of time for which you want to clear cached information. To clear your entire cache, select **All time**.

4. Click **Clear Data**.

5. Restart browser.

Internet Explorer

To clear cache on the Internet Explorer browser, perform the following task:

1. Select **Tools > Safety > Delete browsing history...**.

   If the menu bar is hidden, press **Alt** to make it visible.

2. Deselect **Preserve Favorites website data**, and select **Cookies or Cookies and website data**.

3. Click **Delete**. You will see a confirmation at the bottom of the window when the process is complete.

4. Restart browser.

CHAPTER 2

Guidelines and Limitations

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:
- 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.

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.

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

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.

Note For more information about the CPU and memory requirements, see the Server Resource Requirements section of the Cisco DCNM Release Notes, Release 11.0(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.

Note For more information about the CPU and memory requirements, see the Server Resource Requirements section of the Cisco DCNM Release Notes, Release 11.0(1).

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.

- After the DCNM Virtual Appliance is powered up, verify that all the applications are up and running by using the **appmgr status all** command.
- When the Virtual Appliance is started up for the first time, please wait for all the applications to run before you shut down any of the applications or power off the virtual appliance.
- 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 Cisco DCNM for Media Controller deployment

This chapter contains the following sections:

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 11.0(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.

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 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 devices to leverage better RAM, heap memory, and CPUs. For setups that could grow, choose Large.

Click **Next**.

Step 9 On the Select a resource screen, select the host on which you want to deploy the OVA template.

Click **Next**.

Step 10 On the 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.

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 55.

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 the 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 the 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 10.4(2) 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

You can choose to install DCNM in Standalone mode or Native HA mode. For more information, see Installing Cisco DCNM OVA in Standalone Mode, on page 17 or #unique_24.

Installing 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 the Welcome to Cisco DCNM screen, click **Get Started**.

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

Click **Continue**.

Step 3 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 all platforms:

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

Click **Next**.

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

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

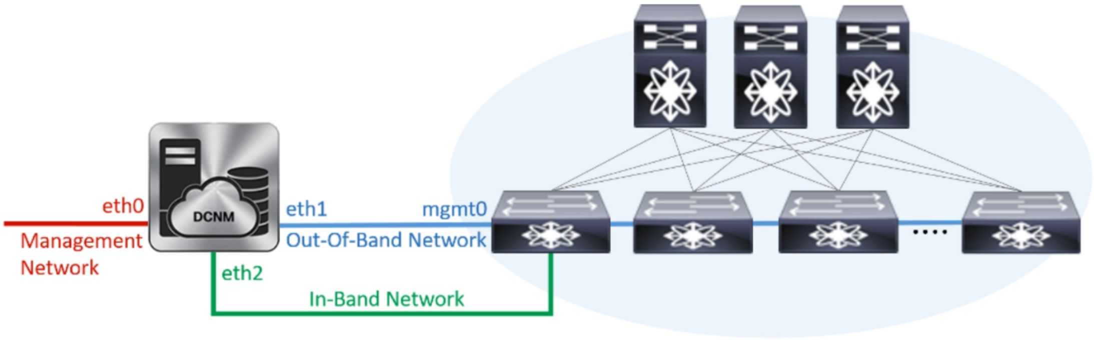
- In the Fully Qualified Hostname field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.
- In the DNS Server Address field, enter the DNS IP address.
- In the NTP Server field, enter the IP address of the NTP server.

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

Click **Next**.

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

Figure 1: Cisco DCNM Management Network Interfaces



a) In the Management Network area, verify is the autopopulated IP Address and Default gateway address are correct. Modify, if necessary.

b) 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 IP Address.

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

c) (Optional) 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 required. For more information, see Configuring Enhanced-Fabric-Inband Interface (eth2) Post DCNM Installation, on page 55.

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 OVA 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
```

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 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 OVA in Native HA mode

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

By default, Cisco DCNM is bundled with an embedded PostgreSQL database engine. 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 will take over with the same database data and resume the operation.

Perform the following task to setup Native HA for DCNM.

Procedure

Step 1 Deploy two DCNM virtual appliances (OVA/ISO).

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

If both eth0 and eth1 interfaces are in the same subnet, edit the `/etc/sysctl.conf` file for DCNM ISO Virtual appliance Native HA installation on both Active and Standby nodes for both the appliances, as follows:

- Change the value of `net.ipv4.conf.default.rp_filter` from 1 to **2**.
- Add **net.ipv4.conf.all.rp_filter** = **2** to the `sysctl.conf` file.

Save and close the file. On the SSH terminal, execute the **sysctl --system** command.

Step 2 Wait for all the applications to be operational.

Use the **appmgr status all** command to check the status of the applications.

Example:

```
dcnm1# appmgr status all
dcnm2# appmgr status all
```

Step 3 Use the **appmgr stop all** command to shut down all applications on both the Cisco DCNM applications.

Use the **appmgr status all** command to check the status of the applications.

Example:

```
dcnm1# appmgr stop all
dcnm2# appmgr status all
```

Step 4 On the active node, edit the `ha-setup.properties` file, by using the following command:

vi /root/packaged-files/properties/ha-setup.properties

Example:

```
dcnm1# vi /root/packaged-files/properties/ha-setup.properties
```

Note Do not turn on **auto_failback** in heartbeat configuration file.

Step 5 Edit the active node parameters and enter appropriate values.

Please refer to #unique_26 section for more information.

Step 6 Install Native HA on the Active node with the following command:

appmgr setup native-ha active

Example:

```
dcnm1# appmgr setup native-ha active
```

Step 7 On the Standby node, check if the below property values are updated in the `ha-setup.properties` file, by using the following command:

vi /root/packaged-files/properties/ha-setup.properties

Example:

```
dcnm2# vi /root/packaged-files/properties/ha-setup.properties
```

Step 8 Verify if the Standby node parameters are updated.

Note To setup Cisco DCNM Native HA successfully, it is important to use valid FQDN as hostname for both hosts while installing DCNM OVA/ISO. After installation, you must be able to ping the FQDN for both hosts. If the ping is not successful, the Native HA setup may fail.

Step 9 If it is auto-populated and validated, install Native HA on the stand-by node, using the following command:

appmgr setup native-ha standby

Example:

```
dcnm2# appmgr setup native-ha standby
```

What to do next

Refer to Native HA Failover and Troubleshooting, on page 48 for troubleshooting Native HA.

Example for DCNM Native HA Installation

The example in this section considers the following parameters and shows how to install DCNM Native HA.

Parameter	Active	Standby	Virtual IP (VIP)
Eth0 IP	1.1.1.1/24	1.1.1.2/24	1.1.1.3/24
Eth1 IP	2.2.0.1/16	2.2.0.2/16	2.2.0.3/16

Parameter	Active	Standby	Virtual IP (VIP)
Hostname (FQDN)	dcnm1.cisco.com	dcnm2.cisco.com	dcnm3.cisco.com

On the active node, edit the property file by using the following command:

vi /root/packaged-files/properties/ha-setup.properties

```
#Copyright (c) 2017 by Cisco Systems, Inc.
#All rights reserved.
# NODE_ID refers the role of this node in HA.
# Example:  NODE_ID=1
# Example:  NODE_ID=1
NODE_ID=1

# IPv4 address of the peer
# Example : PEER_ETH0_IP=172.28.172.82
PEER_ETH0_IP=172.28.172.82

# IPv4 address of the Virtual IP address on the DCNM management network (eth0 network)
# Example : VIP_ADDRESS=172.28.172.83
VIP_ADDRESS=172.28.172.83

# Network prefix of Virtual IP address on DCNM management network, example : for a
255.255.255.0 network mask, enter the prefix as 24
# Example : VIP_PREFIX=24
VIP_PREFIX=24

# IPv4 address of the Virtual IP address on the Enhanced Fabric management network (eth1
network)
# Example : VIP1_ADDRESS=4.110.1.83
VIP1_ADDRESS=4.110.1.83

# Network prefix of Virtual IP address on Enhanced Fabric management network, example :
for a 255.255.255.0 network, enter the prefix as 24
# Example : VIP1_PREFIX=24
VIP1_PREFIX=24

# Optional eth1 VIP address for IPv6 if configured. If not configured, leave them empty
# IPv6 address has to be in long format, no '::' in it.
VIP1_ADDRESS_IPV6=
VIP1_PREFIX_IPV6=

# IPv4 address of the Virtual IP address on the Inband Fabric management network (eth2
network)
# Example : VIP2_ADDRESS=
VIP2_ADDRESS=

# Network prefix of Virtual IP address on Inband Fabric management network, example : for
 a 255.255.255.0 network, enter the prefix as 24
# Example : VIP2_PREFIX=
VIP2_PREFIX=

# Fully Qualified Domain name for the Virtual IP
# Example : VIP_FQDN=mhari-tb-83.cisco.com
VIP_FQDN=mhari-tb-83.cisco.com

# NTP server IP address (1.2.3.4) or the hostname (clock.cisco.com)
NTP_SERVER=ntp.esl.cisco.com

# If set, this address must be pingable for DCNM services
# to be running in Native HA systems. This address must
# belong to Enhanced Fabric management network
# HA_PING_ADDRESS=X.X.X.X
```

Enter the HA ping IP address if necessary.

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

Note You must configure the HA ping IP Address to avoid the Split Brain scenario.

On the standby node, check if the property values are updated in /root/packaged-files/properties/ha-setup.properties

vi /root/packaged-files/properties/ha-setup.properties

```
#Copyright (c) 2017 by Cisco Systems, Inc.
#All rights reserved.
# NODE_ID refers the role of this node in HA.
# Example:  NODE_ID=2
# Example:  NODE_ID=2
NODE_ID=2

# IPv4 address of the peer
# Example : PEER_ETH0_IP=172.28.172.81
PEER_ETH0_IP=172.28.172.81

# IPv4 address of the Virtual IP address on the DCNM management network (eth0 network)
# Example : VIP_ADDRESS=172.28.172.83
VIP_ADDRESS=172.28.172.83

# Network prefix of Virtual IP address on DCNM management network, example : for a
255.255.255.0 network mask, enter the prefix as 24
# Example : VIP_PREFIX=24
VIP_PREFIX=24

# IPv4 address of the Virtual IP address on the Enhanced Fabric management network (eth1
network)
# Example : VIP1_ADDRESS=4.110.1.83
VIP1_ADDRESS=4.110.1.83

# Network prefix of Virtual IP address on Enhanced Fabric management network, example :
for a 255.255.255.0 network, enter the prefix as 24
# Example : VIP1_PREFIX=24
VIP1_PREFIX=24

# Optional eth1 VIP address for IPv6 if configured. If not configured, leave them empty
# IPv6 address has to be in long format, no '::' in it.
VIP1_ADDRESS_IPV6=
VIP1_PREFIX_IPV6=

# IPv4 address of the Virtual IP address on the Inband Fabric management network (eth2
network)
# Example : VIP2_ADDRESS=
VIP2_ADDRESS=

# Network prefix of Virtual IP address on Inband Fabric management network, example : for
 a 255.255.255.0 network, enter the prefix as 24
# Example : VIP2_PREFIX=
VIP2_PREFIX=

# Fully Qualified Domain name for the Virtual IP
# Example : VIP_FQDN=mhari-tb-83.cisco.com
VIP_FQDN=mhari-tb-83.cisco.com

# NTP server IP address (1.2.3.4) or the hostname (clock.cisco.com)
NTP_SERVER=ntp.esl.cisco.com

# If set, this address must be pingable for DCNM services
# to be running in Native HA systems. This address must
# belong to Enhanced Fabric management network
# HA_PING_ADDRESS=X.X.X.X
```

Note The Virtual IP (VIP) is seen on the active node. You can verify VIP by using the **ip address show** command.

Installing DCNM on ISO Virtual Appliance

This chapter contains the following sections:

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 11.0(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 29 or Installing the DCNM ISO Virtual Appliance on UCS (Bare Metal), on page 25 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.

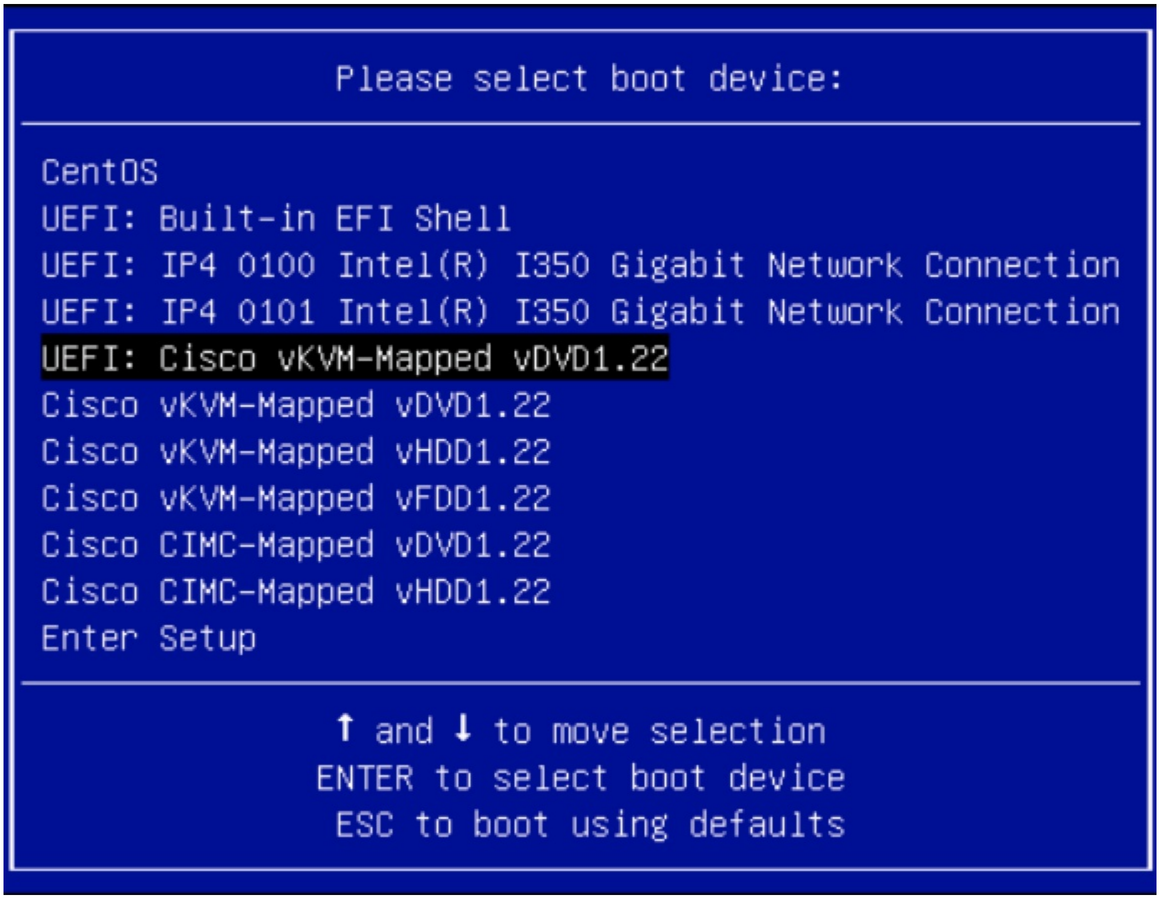
For more information about using the UCS KVM Console window, see the Cisco UCS Server Configuration Utility, Release 3.1 User Guide at the following URL:

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.

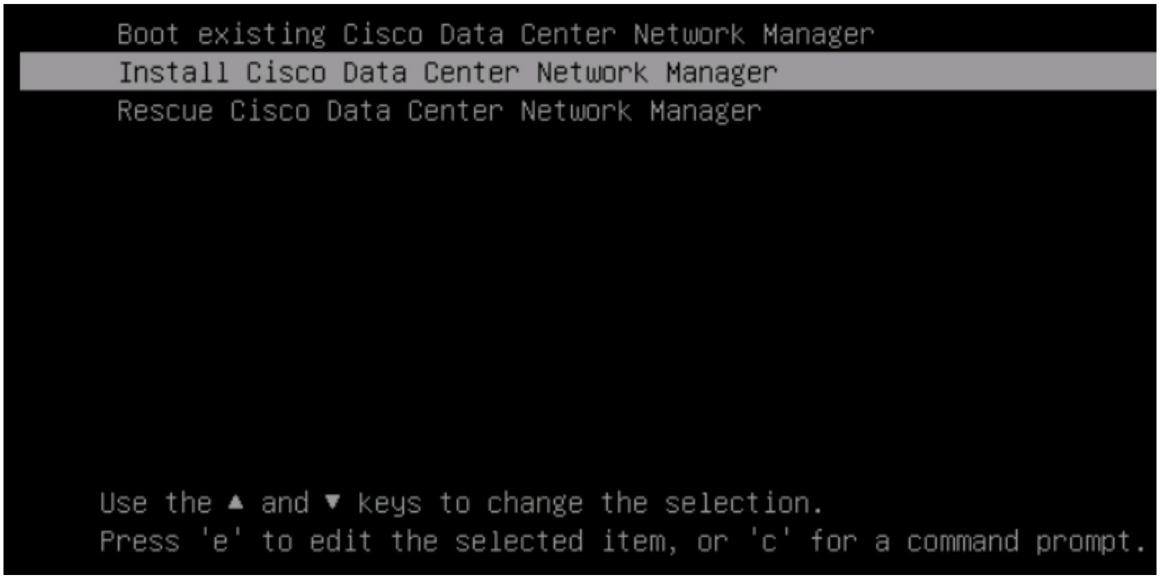


```
Please select boot device:

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**.

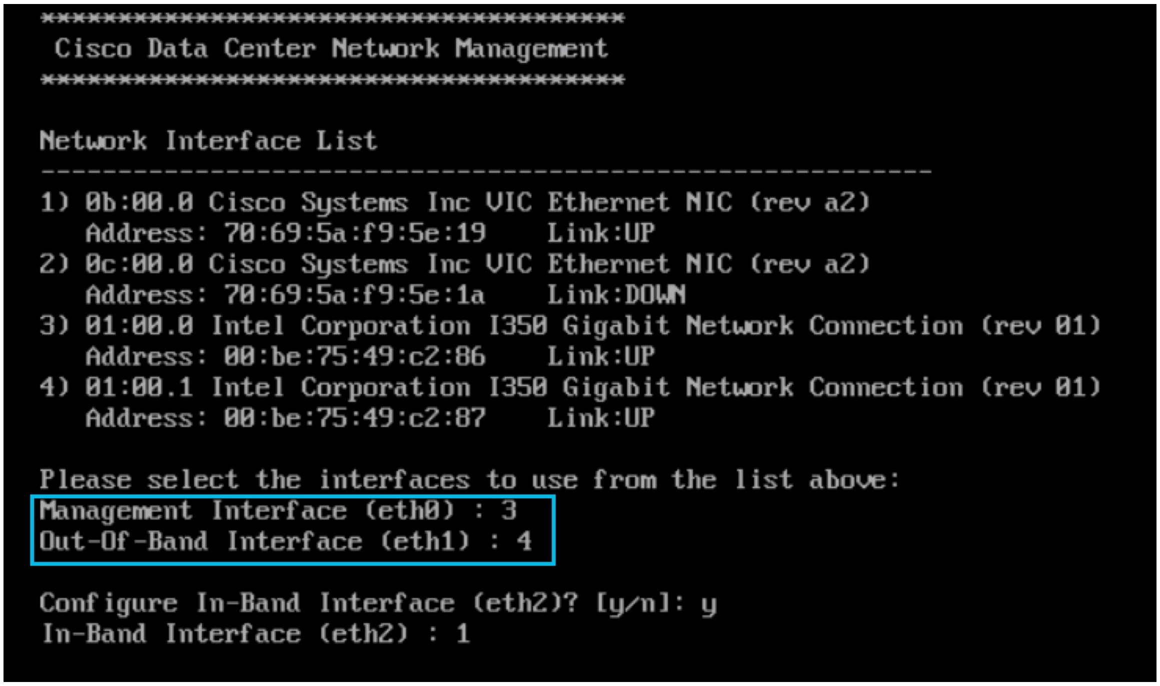
The option shown in the following image appears when the ISO image is booted with UEFI.



```
        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 55.

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 #unique_34 or #unique_24 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.11.0.1.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.11.0.1.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.

sudo virsh define dcnm-kvm-vm.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 withe the following specifications:

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

We recommend that you use storage size of 100GB for Programmable Fabric deployments.

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 55.

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 #unique_34 or #unique_24 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 the Welcome to Cisco DCNM screen, click **Get Started**.

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

Click **Continue**.

Step 3 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 all platforms:

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

Click **Next**.

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

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

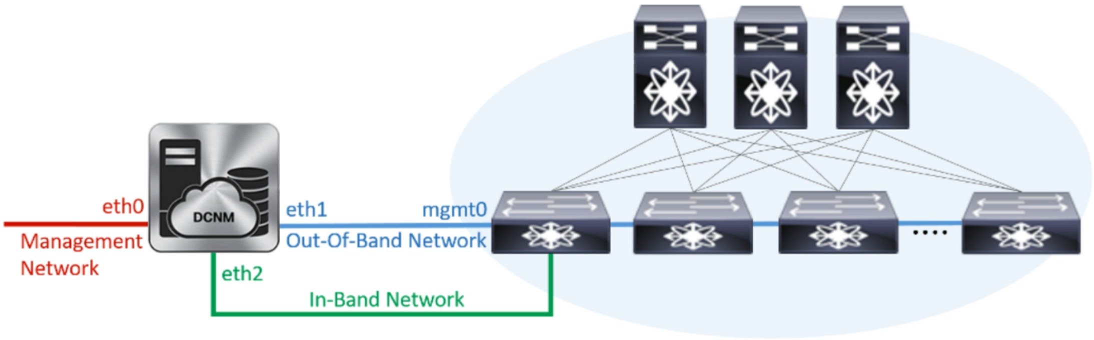
- In the Fully Qualified Hostname field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.
- In the DNS Server Address field, enter the DNS IP address.
- In the NTP Server field, enter the IP address of the NTP server.

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

Click **Next**.

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

Figure 2: Cisco DCNM Management Network Interfaces



a) In the Management Network area, verify is the autopopulated IP Address and Default gateway address are correct. Modify, if necessary.

b) 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 IP Address.

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

c) (Optional) 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 required. For more information, see Configuring Enhanced-Fabric-Inband Interface (eth2) Post DCNM Installation, on page 55.

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 OVA 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
```

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 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 ISO in Native HA mode

Procedure

Step 1 Deploy two DCNM virtual appliances (OVA/ISO).

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

If both eth0 and eth1 interfaces are in the same subnet, edit the `/etc/sysctl.conf` file for DCNM ISO Virtual appliance Native HA installation on both Active and Standby nodes for both the appliances, as follows:

- Change the value of `net.ipv4.conf.default.rp_filter` from 1 to **2**.
- Add **net.ipv4.conf.all.rp_filter** = **2** to the `sysctl.conf` file.

Save and close the file. On the SSH terminal, execute the **sysctl --system** command.

Step 2 Wait for all the applications to be operational.

Use the **appmgr status all** command to check the status of the applications.

Example:

```
dcnm1# appmgr status all
dcnm2# appmgr status all
```

Step 3 Use the **appmgr stop all** command to shut down all applications on both the Cisco DCNM applications.

Use the **appmgr status all** command to check the status of the applications.

Example:

```
dcnm1# appmgr stop all
dcnm2# appmgr status all
```

Step 4 On the active node, edit the `ha-setup.properties` file, by using the following command:

vi /root/packaged-files/properties/ha-setup.properties

Example:

```
dcnm1# vi /root/packaged-files/properties/ha-setup.properties
```

Note Do not turn on **auto_failback** in heartbeat configuration file.

Step 5 Edit the active node parameters and enter appropriate values.

Please refer to #unique_26 section for more information.

Step 6 Install Native HA on the Active node with the following command:

appmgr setup native-ha active

Example:

```
dcnm1# appmgr setup native-ha active
```

Step 7 On the Standby node, check if the below property values are updated in the `ha-setup.properties` file, by using the following command:

vi /root/packaged-files/properties/ha-setup.properties

Example:

```
dcnm2# vi /root/packaged-files/properties/ha-setup.properties
```

Step 8 Verify if the Standby node parameters are updated.

Note To setup Cisco DCNM Native HA successfully, it is important to use valid FQDN as hostname for both hosts while installing DCNM OVA/ISO. After installation, you must be able to ping the FQDN for both hosts. If the ping is not successful, the Native HA setup may fail.

Step 9 If it is auto-populated and validated, install Native HA on the stand-by node, using the following command:

appmgr setup native-ha standby

Example:

```
dcnm2# appmgr setup native-ha standby
```

What to do next

Refer to Native HA Failover and Troubleshooting, on page 48 for troubleshooting Native HA.

Example for DCNM Native HA Installation

The example in this section considers the following parameters and shows how to install DCNM Native HA.

Parameter	Active	Standby	Virtual IP (VIP)
Eth0 IP	1.1.1.1/24	1.1.1.2/24	1.1.1.3/24
Eth1 IP	2.2.0.1/16	2.2.0.2/16	2.2.0.3/16
Hostname (FQDN)	dcnm1.cisco.com	dcnm2.cisco.com	dcnm3.cisco.com

On the active node, edit the property file by using the following command:

vi /root/packaged-files/properties/ha-setup.properties

```
#Copyright (c) 2017 by Cisco Systems, Inc.
#All rights reserved.
# NODE_ID refers the role of this node in HA.
# Example:  NODE_ID=1
# Example:  NODE_ID=1
NODE_ID=1

# IPv4 address of the peer
# Example : PEER_ETH0_IP=172.28.172.82
PEER_ETH0_IP=172.28.172.82

# IPv4 address of the Virtual IP address on the DCNM management network (eth0 network)
# Example : VIP_ADDRESS=172.28.172.83
VIP_ADDRESS=172.28.172.83

# Network prefix of Virtual IP address on DCNM management network, example : for a
255.255.255.0 network mask, enter the prefix as 24
# Example : VIP_PREFIX=24
VIP_PREFIX=24

# IPv4 address of the Virtual IP address on the Enhanced Fabric management network (eth1
network)
# Example : VIP1_ADDRESS=4.110.1.83
VIP1_ADDRESS=4.110.1.83

# Network prefix of Virtual IP address on Enhanced Fabric management network, example :
for a 255.255.255.0 network, enter the prefix as 24
# Example : VIP1_PREFIX=24
VIP1_PREFIX=24

# Optional eth1 VIP address for IPv6 if configured. If not configured, leave them empty
# IPv6 address has to be in long format, no '::' in it.
VIP1_ADDRESS_IPV6=
VIP1_PREFIX_IPV6=

# IPv4 address of the Virtual IP address on the Inband Fabric management network (eth2
network)
# Example : VIP2_ADDRESS=
VIP2_ADDRESS=

# Network prefix of Virtual IP address on Inband Fabric management network, example : for
 a 255.255.255.0 network, enter the prefix as 24
# Example : VIP2_PREFIX=
VIP2_PREFIX=

# Fully Qualified Domain name for the Virtual IP
# Example : VIP_FQDN=mhari-tb-83.cisco.com
VIP_FQDN=mhari-tb-83.cisco.com

# NTP server IP address (1.2.3.4) or the hostname (clock.cisco.com)
NTP_SERVER=ntp.esl.cisco.com

# If set, this address must be pingable for DCNM services
# to be running in Native HA systems. This address must
# belong to Enhanced Fabric management network
# HA_PING_ADDRESS=X.X.X.X
```

Enter the HA ping IP address if necessary.

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

Note You must configure the HA ping IP Address to avoid the Split Brain scenario.

On the standby node, check if the property values are updated in /root/packaged-files/properties/ha-setup.properties

vi /root/packaged-files/properties/ha-setup.properties

```
#Copyright (c) 2017 by Cisco Systems, Inc.
#All rights reserved.
# NODE_ID refers the role of this node in HA.
# Example:  NODE_ID=2
# Example:  NODE_ID=2
NODE_ID=2

# IPv4 address of the peer
# Example : PEER_ETH0_IP=172.28.172.81
PEER_ETH0_IP=172.28.172.81

# IPv4 address of the Virtual IP address on the DCNM management network (eth0 network)
# Example : VIP_ADDRESS=172.28.172.83
VIP_ADDRESS=172.28.172.83

# Network prefix of Virtual IP address on DCNM management network, example : for a
255.255.255.0 network mask, enter the prefix as 24
# Example : VIP_PREFIX=24
VIP_PREFIX=24

# IPv4 address of the Virtual IP address on the Enhanced Fabric management network (eth1
network)
# Example : VIP1_ADDRESS=4.110.1.83
VIP1_ADDRESS=4.110.1.83

# Network prefix of Virtual IP address on Enhanced Fabric management network, example :
for a 255.255.255.0 network, enter the prefix as 24
# Example : VIP1_PREFIX=24
VIP1_PREFIX=24

# Optional eth1 VIP address for IPv6 if configured. If not configured, leave them empty
# IPv6 address has to be in long format, no '::' in it.
VIP1_ADDRESS_IPV6=
VIP1_PREFIX_IPV6=

# IPv4 address of the Virtual IP address on the Inband Fabric management network (eth2
network)
# Example : VIP2_ADDRESS=
VIP2_ADDRESS=

# Network prefix of Virtual IP address on Inband Fabric management network, example : for
 a 255.255.255.0 network, enter the prefix as 24
# Example : VIP2_PREFIX=
VIP2_PREFIX=

# Fully Qualified Domain name for the Virtual IP
# Example : VIP_FQDN=mhari-tb-83.cisco.com
VIP_FQDN=mhari-tb-83.cisco.com

# NTP server IP address (1.2.3.4) or the hostname (clock.cisco.com)
NTP_SERVER=ntp.esl.cisco.com

# If set, this address must be pingable for DCNM services
# to be running in Native HA systems. This address must
# belong to Enhanced Fabric management network
# HA_PING_ADDRESS=X.X.X.X
```

Note The Virtual IP (VIP) is seen on the active node. You can verify VIP by using the **ip address show** command.

CHAPTER 5

Running Cisco DCNM Behind a Firewall

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

Running Cisco DCNM Behind a Firewall

Generally, an Enterprise (external world) and Datacenter 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.

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).
67	UDO	DHCP	Device to DCNM Server	
69	TCP	TFTP	Device to DCNM Server	Required for POAP

Port Number	Protocol	Service Name	Direction of Communication	Remarks
161	TCP/UDP	SNMP	Server to DCNM Device	DCNM configured via `server.properties` 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 6

Monitoring Devices

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

Monitoring Devices in In-Band Network

Perform the following task to monitor devices in the In-band network.

Procedure

Step 1 Deploy Cisco DCNM in Standalone mode or Native HA mode.

For more information, see Installing Cisco DCNM for Media Controller deployment, on page 13.

Step 2 Configure In-band route on the DCNM server using the command:

```
appmgr setup inband-route subnet  {fabric-links-subnet/maskloopback-IP-subnet/mask}
```

where,

- *fabric-links-subnet/mask* is IP address and subnet used for the switches ISL links.
- *loopback-IP-subnet/mask* is the IP address and subnet of loopback configured on switches for managing them in In-band network.

On switches, User may configure the same loopback Interface (like loopback x) and choose its IP address in a subnet with /32 mask or as appropriate for their network and while installing the DCNM server (s) also use the eth2 IPs and in native-ha bring up eth2 VIP IP also in same IP subnet as that of switch loopback IP subnet.

On Servers, User can use a summarized group mask (eg: /24 in this example) so that only a few static routes on the server are needed

Note In native HA setup run these two commands on both primary and secondary

Now ping from server to switch loopback IP or switch to the server (via vrf default) both ways ping should go through fine

Step 3 Ping the switch loopback IP address from the DCNM server, or ping the server (via default vrf) to the switch.

Ensure that you can ping both the routes successfully.

Step 4 Logon to the Cisco DCNM server.

Navigate to the `/usr/local/cisco/dcm/fm/conf` directory.

Step 5 Edit the trap registry values in the `server.properties` file.

Set the `traps.registaddress=`*eth2-VIP-IPAddress*

Save the `server.properties` file.

Step 6 Restart the Cisco DCNM using the following commands:

appmgr stop all

appmgr start all

Note On a Native HA setup, follow the following order to restart services.

dcnm 2# **appmgr stop all**

dcnm1# **appmgr stop all**

dcnm1# **appmgr start all**

dcnm2# **appmgr start all**

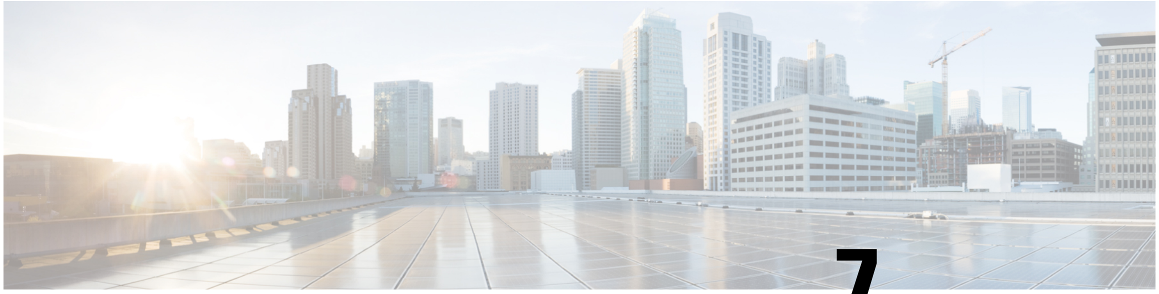
Step 7 On Cisco DCNM Web UI, discover the devices, based on loopback IP addresses of the Switch.

Ensure that the discovery occurred through the server to the switch using inband connectivity

Step 8 Edit the `pmn_telemetry_snmp` template and provide appropriate details.

```
Telemetry VRF=default
Telemetry receiver IP=<native-HA/eth2-VIP-IP-address>
snmp trap receiver=select check box
Source Interface=Loopback x/y
choose "copy running to startup" option
```

Step 9 Deploy the modified configuration to the switch.



CHAPTER 7

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

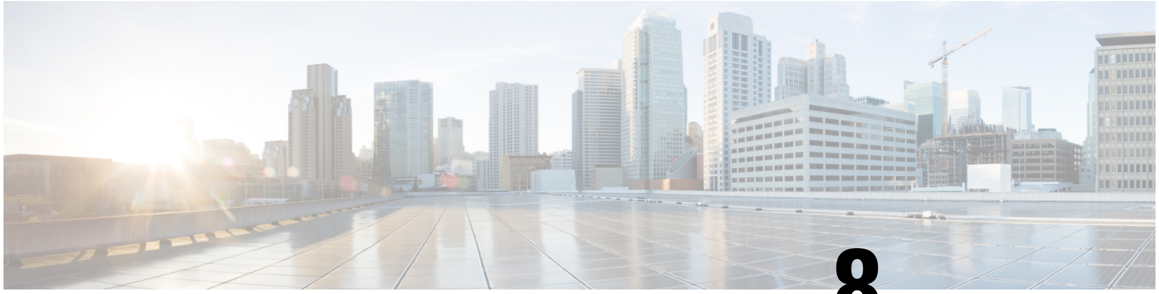
```
<DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks.old
```

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 8

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

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 DCNM REST API and AMQP, this transition is done by a load-balancing software that hides the interface address of the appliances using a Virtual IP (VIP) address.

   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 DCNM/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 48; subsequent requests to the AMQP Virtual IP address are redirected to OVA-B.

Native HA Failover and Troubleshooting

When Cisco DCNM is deployed in Native HA mode, we recommend that you do not restart applications using the **appmgr restart all** or **appmgr restart ha-apps**.

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 DCNM 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 theOVA 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].

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 9

Managing Applications After DCNM Deployment

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

Table 3: Cisco DCNM Applications

Category	Application	Username	Password	Protocol Implemented
Network Management	Data Center Network Manager	admin	User choice [1]	Network Management

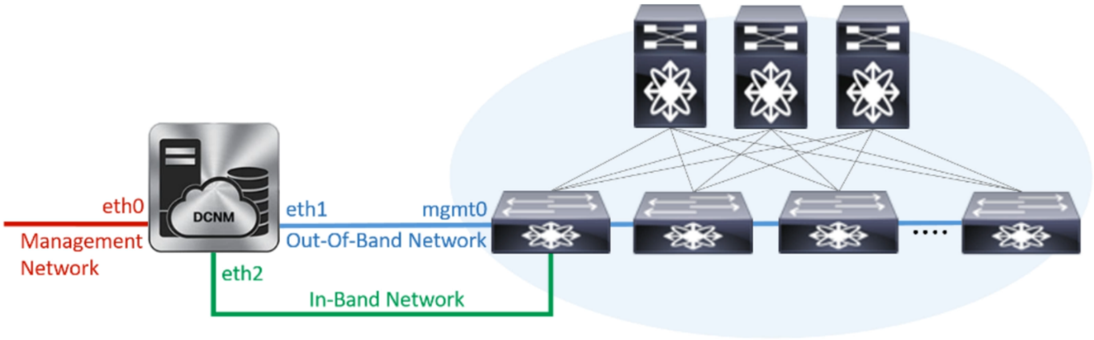
[1] User choice refers to the administration password entered by the user during the deployment.

This chapter contains the following sections:

ConfiguringEnhanced-Fabric-InbandInterface(eth2)PostDCNM 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.

Figure 3: Cisco DCNM Management Network Interfaces



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]#
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]#
```

Application Details

This section describes the details of all the applications within the functions they provide in Cisco DCNM. The functions are as follows:

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.

Note You should always configure DHCP through Cisco DCNM web UI by choosing: **Configure** > **POAP** > **DHCP Scopes**. Editing the `/etc/dhcp/dhcp.conf` file from an SSH terminal might lead to unexpected behavior.

- 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.

Backup and Restore Cisco DCNM and Application Data

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 Step 2, on page 58.

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 Logon to the appliance using SSH. Restore the data on the DCNM appliance using the following command:

appmgr restore /root/backup.tar.gz

Step 10 Click **y** to proceed to restore the backup data.

```
Do you want to proceed? [y/n] y
```

Step 11 After the data is restored, check the status using the **appmr status all** command.

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

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 59.

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 On the Active node, logon to the appliance using SSH. Restore the data on the DCNM appliance using the following command:

appmgr restore /root/backup.tar.gz

Example:

```
dcnm1 # appmgr restore /root/backup.tar.gz
```

Step 11 On the Standby node, logon to the appliance using SSH. Restore the data on the DCNM appliance using the following command:

appmgr restore /root/backup.tar.gz

Example:

```
dcnm2 # appmgr restore /root/backup.tar.gz
```

Step 12 After the data is restored, check the status using the **appmr status all** command.

Managing Applications

You can manage the applications 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 Status after Deployment

After you deploy the OVA/ISO file, you can determine the status of the applications 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 of the applications by entering this command:

appmgr status all

Example:

The following sample if taken from Cisco DCNM for Media Controller Deployment.

```
dcnm# appmgr status all

DCNM v11 will only use HTTPS. Insecure access via HTTP is disabled.
Please use the url https://<DCNM-IP-ADDRESS> or https://<HOSTNAME> to launch the DCNM UI.

DCNM Status

 PID  USER      PR  NI  VIRT    RES     SHR  S  %CPU %MEM    TIME+  COMMAND
 ===  ====      ==  == ======= ======  ===== =  ==== ====   ======= =======
27724 root      20   0   12.2g   3.9g  49328 S   0.0 16.6  60:24.10 java

Elasticsearch Status

 PID  USER      PR  NI  VIRT    RES     SHR  S  %CPU %MEM    TIME+  COMMAND
 ===  ====      ==  == ======= ======  ===== =  ==== ====   ======= =======
 2861 elastic+  20   0 6858536 346396  16484 S   6.2  1.4  11:03.40 java

Telemetry Manager Status

 PID  USER      PR  NI  VIRT    RES     SHR  S  %CPU %MEM    TIME+  COMMAND
 ===  ====      ==  == ======= ======  ===== =  ==== ====   ======= =======
 2964 root      20   0  796984   5060   3416 S   0.0  0.0   1:06.11 telemetry-mgr.b

PMN Telemetry Status

 PID  USER      PR  NI  VIRT    RES     SHR  S  %CPU %MEM    TIME+  COMMAND
 ===  ====      ==  == ======= ======  ===== =  ==== ====   ======= =======
 3779 root      20   0   10.6g 233640  16236 S   0.0  1.0   0:06.82 java

TFTP Status

 PID  USER      PR  NI  VIRT    RES     SHR  S  %CPU %MEM    TIME+  COMMAND
 ===  ====      ==  == ======= ======  ===== =  ==== ====   ======= =======
30377 root      20   0   27164   1072    820 S   0.0  0.0   0:00.00 xinetd
```

```
DHCP Status

 PID  USER       PR  NI  VIRT    RES     SHR  S  %CPU %MEM    TIME+  COMMAND
 ===  ====       ==  == ======= ======  ===== =  ==== ====   ======= =======
30416 dhcpd      20   0  105616   5656   3448 S   0.0  0.0   0:25.32 dhcpd

AMQP Status

 PID  USER       PR  NI  VIRT    RES     SHR  S  %CPU %MEM    TIME+  COMMAND
 ===  ====       ==  == ======= ======  ===== =  ==== ====   ======= =======
32157 rabbitmq   20   0 5996960  78564   4272 S   0.0  0.3   9:30.39 beam.smp
```

Stopping, Starting, and Resetting Applications

Use the following CLI commands for stopping, starting, and resetting applications:

- To stop an application, use the **appmgr stop application** command.

  ```
  # appmgr stop dhcp
  Shutting down dhcpd:      [  OK  ]
  ```

- To start an application, use the **appmgr start application** command.

  ```
  # appmgr start amqp
  Starting vsftpd for amqp:      [  OK  ]
  ```

- To restart an application use the **appmgr restart application** 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.