

Cisco DCNM Installation and Upgrade Guide for LAN Fabric Deployment, Release 11.5(1)

First Published: 2020-12-23

Last Modified: 2021-12-22

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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

© 2020–2021 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Overview** 1

Introduction 1

Installation Options 2

Deployment Options 2

root and sysadmin User Privileges 3

Upgrading to Cisco DCNM Release 11.5(1) 4

System Requirements 4

CHAPTER 2 **Guidelines and Limitations** 11

Guidelines and Limitations 11

Checking TPM Partition before Converting DCNM-SE to Nexus Dashboard 13

CHAPTER 3 **Prerequisites** 15

Prerequisites for DCNM Open Virtual Appliance 15

Prerequisites for DCNM ISO Virtual Appliance 16

Prerequisites for Cisco DCNM Virtual Appliance HA 16

Deploying Cisco DCNM Virtual Appliances in HA mode 16

Availability of Virtual IP Addresses 17

Installing an NTP Server 17

CHAPTER 4 **Installing the Cisco DCNM** 19

Installing DCNM on Open Virtual Appliance 19

Downloading the Open Virtual Appliance File 19

Deploying the Open Virtual Appliance as an OVF Template 20

Installing the Cisco DCNM OVA in Standalone Mode 24

Installing the Cisco DCNM OVA in Native HA mode 28

Installing DCNM on ISO Virtual Appliance 36
Downloading the ISO Virtual Appliance File 37
Installing the DCNM ISO Virtual Appliance on UCS (Bare Metal) 37
Installing the DCNM ISO Virtual Appliance on KVM 44
Installing the DCNM ISO Virtual Appliance on Nexus Dashboard 45
Installing the DCNM ISO Virtual Appliance on Windows Hyper-V 46
Creating Virtual Switches 47
Creating Virtual Machines 48
Installing DCNM ISO Virtual Appliance 52
Installing Cisco DCNM ISO in Standalone Mode 55
Installing the Cisco DCNM ISO in Native HA mode 60
Convert Standalone Setup to Native-HA Setup 68
Installing Cisco DCNM Compute Node 72

CHAPTER 5 **Upgrading Cisco DCNM 77**
Upgrading to Cisco DCNM Release 11.5(1) 77
Upgrading ISO or OVA through Inline Upgrade 77
Inline Upgrade for DCNM Virtual Appliance in Standalone Mode 78
Inline Upgrade for DCNM Virtual Appliance in Native HA Mode 81
Inline Upgrade for DCNM Compute Nodes 85
Dropping Performance Manager Data 87

CHAPTER 6 **Upgrading the Cisco DCNM Classic LAN Deployment 91**
Overview 91
Migration of Fabrics 92
Supported Switch Roles in LAN Fabric Post Upgrade 94
Classic LAN Templates in LAN Fabric 94
Upgrading from the Classic LAN Deployment to the LAN Fabric Deployment 98
LAN Classic Fabric Template Functionalities 101

CHAPTER 7 **Deployment Best Practices 103**
Best Practices for Deploying Cisco DCNM and Computes 103
Guidelines to Use the Best Practices 104
Deployments for Redundancy in Cisco DCNM 104

IP Address Configurations in Cisco DCNM 105
Scenario 1: All 3 Ethernet Interfaces are in Different Subnets 105
Scenario 2: eth2 Interface in Different Subnet 108
Physical Connectivity of Cisco DCNM and Compute Nodes 110

CHAPTER 8 **Disaster Recovery (Backup and Restore) 115**
Backup and Restore Cisco DCNM and Application Data on Standalone DCNM setup 115
Backup and Restore Cisco DCNM and Application Data on Native HA setup 116
Recovering Cisco DCNM Single HA Node 117
Recovering admin Account 119
HA Disaster Avoidance using SRM 120
Backup and Restore Cisco DCNM on a Cluster Setup 122

CHAPTER 9 **Certificates 125**
Certificate Management 125
Best practices for Certificate Management 126
Display Installed Certificates 126
Installing a CA Signed Certificate 128
Installing a CA Signed Certificate on Cisco DCNM Standalone Setup 128
Installing a CA Signed Certificate on Cisco DCNM Native HA setup 129
Exporting certificate from Active Node to Standby Node 131
Restoring the certificates after an upgrade 132
Restoring Certificates on Cisco DCNM Standalone setup after Upgrade 134
Restoring Certificates on Cisco DCNM Native HA setup after Upgrade 134
Recovering and Restoring Previously Installed CA Signed Certificates 135
Verifying the installed certificate 136

CHAPTER 10 **Running Cisco DCNM Behind a Firewall 139**
Running Cisco DCNM Behind a Firewall 139
Configuring Custom Firewalls 141

CHAPTER 11 **Secure Client Communications for Cisco DCNM Servers 145**
Secure Client Communications for Cisco DCNM Servers 145
Enabling SSL/HTTPS on Cisco DCNM in HA Environment on Virtual Appliance 145

CHAPTER 12 **Managing Applications in a High-Availability Environment** 147

Information About Application Level HA in the Cisco DCNM Open Virtual Appliance 147

Automatic Failover 148

Manually Triggered Failovers 148

Native HA Failover and Troubleshooting 148

Application High Availability Details 150

Data Center Network Management 150

RabbitMQ 152

Repositories 153

CHAPTER 13 **Managing Utility Services After DCNM Deployment** 155

Editing Network Properties Post DCNM Installation 155

Modifying Network Interfaces (eth0 and eth1) Post DCNM Installation 156

Modifying Network Properties on DCNM in Standalone Mode 164

Modifying Network Properties on DCNM in Native HA Mode 166

Changing the DCNM Server Password on Standalone Setup 174

Changing the DCNM Server Password on Native HA Setup 175

Changing the DCNM Database Password on Standalone Setup 176

Changing the DCNM Database Password on Native HA Setup 176

Convert Standalone Setup to Native-HA Setup 177

Utility Services Details 181

Network Management 181

Orchestration 182

Device Power On Auto Provisioning 182

Managing Applications and Utility Services 183

Verifying the Application and Utility Services Status after Deployment 183

Stopping, Starting, and Resetting Utility Services 184

Updating the SFTP Server Address for IPv6 185

CHAPTER 14 **Tetration Agent With DCNM Validation** 187

Tetration Agent With DCNM Validation 187

CHAPTER 15 **Setup Authentication via TACACS+ Server** 191

Setup SSH Authentication via TACACS+ Server 191

CHAPTER 16 **Installing Software Maintenance Update for log4j2 Vulnerability** 195

Installing Software Maintenance Update on Cisco DCNM OVA/ISO Deployment 195

Installing SMU on Cisco DCNM 11.5(x) Standalone Deployment 195

Installing SMU on Cisco DCNM 11.5(x) Native HA Deployment 197

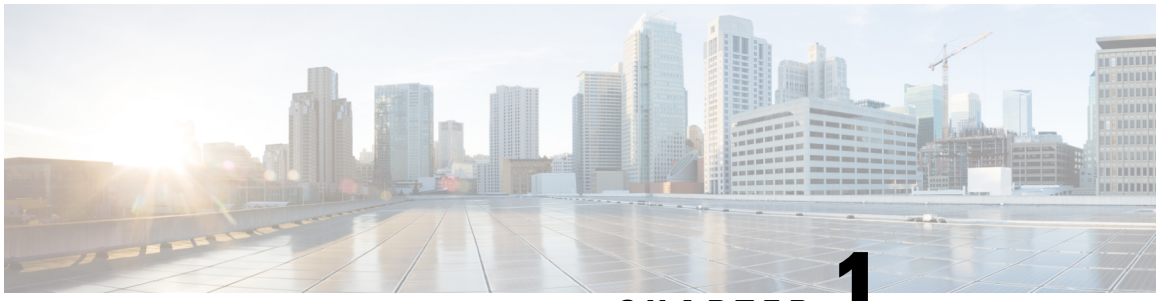
Installing SMU on Cisco DCNM 11.5(x) Compute Nodes 200

Sample Output of Commands to address Log4j vulnerability 202

Scanning for Log4j2 Vulnerabilities 215

Validating of SMU Installation 218

Upgrading DCNM Release 11.5(x) from Previous Versions 218



CHAPTER 1

Overview

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

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

This section contains the following sections:

- Introduction, on page 1
- Installation Options, on page 2
- Deployment Options, on page 2
- root and sysadmin User Privileges, on page 3
- Upgrading to Cisco DCNM Release 11.5(1), on page 4
- System Requirements, on page 4

Introduction

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

Cisco DCNM includes these management applications:

Cisco DCNM Web UI

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

Performance Manager

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

Installation Options

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

DCNM Open Virtual Appliance (OVA) Installer

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

DCNM ISO Virtual Appliance (ISO) Installer

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

Note If you are installing Cisco DCNM on SE, install the DCNM ISO Virtual Appliance (.iso) installer.

Deployment Options

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

Supported Latency

The supported latency for Cisco DCNM LAN Fabric deployment is defined below:

- Between Native HA Primary and Secondary appliances, latency is 50ms.
- Between DCNM Native HA Primary appliance to Switches, latency is 50ms.
- Between DCNM Computes latency is 50ms.

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.

Note We recommend that you deploy Cisco DCNM in Native HA Mode.

High Availability for Virtual Appliances

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

DCNM Computes

Compute nodes are scale out application hosting nodes that run resource-intensive services to provide services to the larger Fabric. When compute nodes are added, all services that are containers, run only on these nodes. This includes Config Compliance, Endpoint Locator, and Virtual Machine Manager.

DCNM in Clustered Mode

In a clustered mode, the Cisco DCNM Server with more compute nodes provides an architecture to expand resources, as you deploy more applications. The DCNM Servers do not run containerized applications. All applications that work in unclustered mode works in the clustered mode, also.

DCNM in Unclustered Mode

In unclustered mode, the Cisco DCNM runs some of its internal services as containers. Cisco DCNM leverages resources from the Standby node for running some containers applications. The Cisco DCNM Active and Standby nodes work together to extend resources to the overall functionality and deployment of DCNM and its applications. However, it has limited resources to run some of the advanced applications and to extend the system to deploy more applications delivered through the Cisco AppCenter.

root and sysadmin User Privileges

The following table summarizes the user privileges differences between DCNM 11.5 and previous releases.



Note This is applicable to Cisco DCNM OVA/ISO deployments only.

Description	Functionality in DCNM 11.5 Release	Functionality in DCNM 11.4(1) and 11.3(1) Releases	Remarks
su command	Requires local **root** password. **sysadmin** user can't run **sudo su** command	Requires sysadmin password **su** is an alias for **sudo su**	The **su** command requires the local password even when the remote authentication is configured.
appmgr change_pwd ssh root command	Only **root** user can run this command.	**sysadmin** can also run this command.	-
appmgr root-access {permit|deny|…} command	Only **root** user can run this command	**sysadmin** user can also run this command	-
appmgr remote-auth command	Only **root** user can run this command	Not available	-
Other **appmgr** commands	**root** or **sysadmin** user can run these commands	**root** or **sysadmin** user can run these commands	-

Upgrading to Cisco DCNM Release 11.5(1)

Before Cisco DCNM Release 11.0(1), DCNM OVA, and ISO supported SAN functionality. From Cisco DCNM Release 11.3(1), you can install Cisco DCNM for SAN Deployment on both OVA and ISO virtual appliances.

The following table summarizes the type of upgrade that you must follow to upgrade to Release 11.5(1).

Table 1: Type of Upgrade for LAN Fabric deployments

Current Release Number	Upgrade type to upgrade to Release 11.5(1)
11.4(1)	Inline Upgrade
11.3(1)	Inline Upgrade
11.2(1)	Inline Upgrade
11.1(1)	11.1(1) → 11.2(1) → 11.5(1) 11.1(1) → 11.3(1) → 11.5(1) 11.1(1) → 11.4(1) → 11.5(1) → represents an Inline Upgrade

System Requirements

This section describes the various system requirements for proper functioning of your Cisco DCNM Release 11.5(1).

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

- Java Requirements, on page 5
- Server Requirements, on page 5
- Supported Latency
- Database Requirements, on page 5
- Hypervisors, on page 5
- Server Resource (CPU/Memory) Requirements, on page 6
- VMware Snapshot Support for Cisco DCNM, on page 8
- Supported Web Browsers, on page 9

- Other Supported Software, on page 10

Note If you are deploying Network Insights applications on the Cisco DCNM Compute cluster, refer to the app-specific release notes for additional CPU or memory requirements for Computes.

Java Requirements

The Cisco DCNM server is distributed with JRE 11.0.8 into the following directory:

```
DCNM_root_directory/java/jdk11
```

Server Requirements

Cisco DCNM Release 11.5(1), supports the Cisco DCNM server on these 64-bit operating systems:

- **IP for Media, and LAN Fabric Deployments:**
  - Open Virtual Appliance (OVA) with an integrated CentOS Linux release 7.8
  - ISO Virtual Appliance (ISO) with an integrated CentOS Linux release 7.8

Supported Latency

The supported latency for Cisco DCNM LAN Fabric deployment is defined below:

- Between Native HA Primary and Secondary appliances, latency is 50ms.
- Between DCNM Native HA Primary appliance to Switches, latency is 50ms.
- Between DCNM Computes latency is 50ms.

Database Requirements

Cisco DCNM Release 11.5(1) supports the following databases:

- PostgreSQL 10.15 - For OVA/ISO deployments

Note The ISO and OVA installations support only the embedded PostgreSQL database.

Hypervisors

Cisco DCNM supports the ISO installation on a bare-metal server, no hypervisor, on the following server platforms:

Server	Product ID (PID)	Recommended minimum memory, drive capacity, and CPU count [1] [2]
Cisco UCS C240M4	UCSC-C240-M4S	32G / 500G 16 vCPUs

Server	Product ID (PID)	Recommended minimum memory, drive capacity, and CPU count [1] [2]
Cisco UCS C240M4	UCSC-C240-M4L	32G / 500G 16 vCPUs
Cisco UCS C240 M5S	UCSC-C240-M5SX	32G / 500G 16 vCPUs
Cisco UCS C220 M5L	UCSC-C220-M5L	32G / 500G 16 vCPUs

1 Install the Cisco DCNM Compute node with 16 vCPUs, 64G RAM, and 500GB hard disk.
2 If you are deploying Network Insights applications on the Cisco DCNM Compute cluster, refer to the app-specific Release Notes for additional CPU/memory requirements for the Computes.

Note Cisco DCNM can work on an alternative computing hardware with appropriate specifications, despite Cisco is only testing on Cisco UCS.

Supported Hypervisors

You can use the Cisco DCNM Server on the following hypervisors:

Hypervisor supported	Data Center Manager server application	Supported deployments
ESXi 7.0	vCenter 7.0	All
ESXi 6.7 P01	vCenter 6.7 P01	All
ESXi 6.5	vCenter 6.5	All
ESXi 6.0	vCenter 6.0	All
RedHat 7.6 KVM with QEMU version 1.5.3	Virtual Machine Manager (comes with RHEL 7.6)	LAN Fabric
Hyper-V on Windows Server 2019	Hyper-V Manager (comes with Windows Server 2019)	LAN Fabric This is supported with Native HA mode, and not in Cluster mode.

Server Resource (CPU/Memory) Requirements

Note If you install Cisco DCNM on a virtual machine, you must reserve resources equal to the server resource requirements to ensure a baseline with the physical machines.

If the existing Elasticsearch database is more than 250GB, Cisco DCNM Server requires more than 500GB HDD space to complete reindexing.

Table 2: System Requirements for Cisco DCNM LAN Fabric Deployment

Deployment Type	Small (Lab or POC)	Large (Production)	Compute for 81-350 switches scale (without Network Insights)	Compute for up to 80 switches (with Network Insights)
OVA/ISO	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 64 GB DISK: 500 GB	CPU: 32 vCPUs RAM: 64 GB DISK: 500 GB

Note For Huge and Compute deployments, you can add extra disk. The size of the disk can range from a minimum of 32GB to a maximum of 1.5TB.

If the existing Elasticsearch database is more than 250GB, Cisco DCNM Server requires more than 500GB HDD space to complete reindexing.

Allocate sufficient disk space to the root partition to complete DCNM installation and for stable continuous operation of the DCNM applications. Refer to the applications' User guides for disk space requirements. You can mount another disk where the `/tmp` directory can be mounted during the installation or upgrade. You can also add additional disk space and the disk file system using **appmgr system scan-disks-and-extend-fs** command.

Cisco DCNM LAN Fabric Deployment Without Network Insights (NI)

Note For information about various system requirements for proper functioning of Cisco DCNM LAN Fabric deployment, see System Requirements.

Refer to *Network Insights User guide* for sizing information for Cisco DCNM LAN Deployment with Network Insights (NI).

To see the verified scale limits for Cisco DCNM 11.5(1) for managing LAN Fabric deployments, see *Verified Scale Limits for Cisco DCNM*.

Table 3: Upto 80 Switches

Node	CPU Deployment Mode	CPU	Memory	Storage	Network
DCNM	OVA/ISO	16 vCPUs	32G	500G HDD	3xNIC
Computes	NA	—	—	—	—

Table 4: 81–350 Switches

Node	CPU Deployment Mode	CPU	Memory	Storage	Network
DCNM	OVA/ISO	16 vCPUs	32G	500G HDD	3xNIC
Computes	OVA/ISO	16 vCPUs	64G	500G HDD	3xNIC

VMware Snapshot Support for Cisco DCNM

Snapshots capture the entire state of the virtual machine at the time you take the snapshot. You can take a snapshot when a virtual machine is powered on, powered off. The following table shows snapshot support for your deployment.

VMware vSphere Hypervisor (ESXi)	6.0	6.5	6.7	6.7 P01	7.0
VMware vCenter Server	6.0	6.5	6.7	6.7 P01	7.0

Note You need VMware vCenter server to deploy Cisco DCNM OVA Installer. However, to install DCNM directly on VMware ESXi without vCenter, you can choose DCNM ISO deployment. Ensure that correct CPU, Memory, Disk, and NIC resources are allocated to that VM.

To take a snapshot on the VM, perform the following steps:

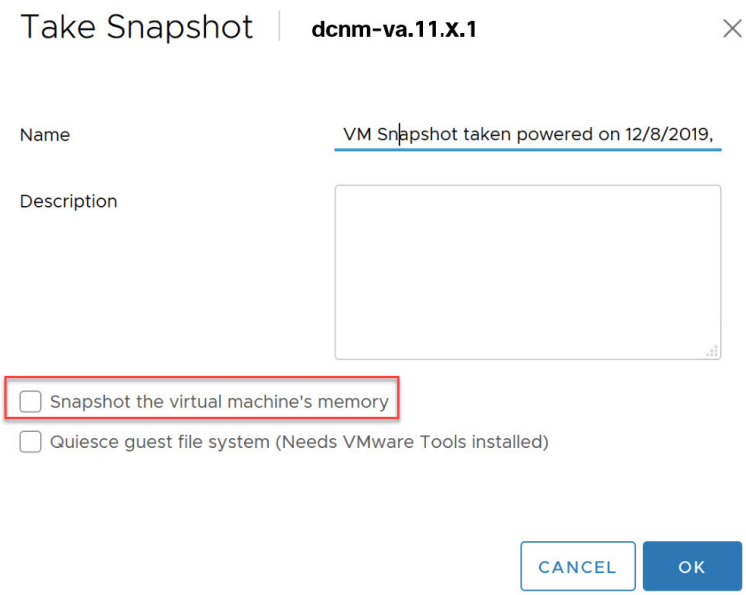
1. Right-click the virtual machine the inventory and select **Snapshots** > **Take Snapshot**.
2. In the **Take Snapshot** dialog box, enter a name and description for the snapshot.
3. Click **OK** to save the snapshot.

The following snapshots are available for VMs.

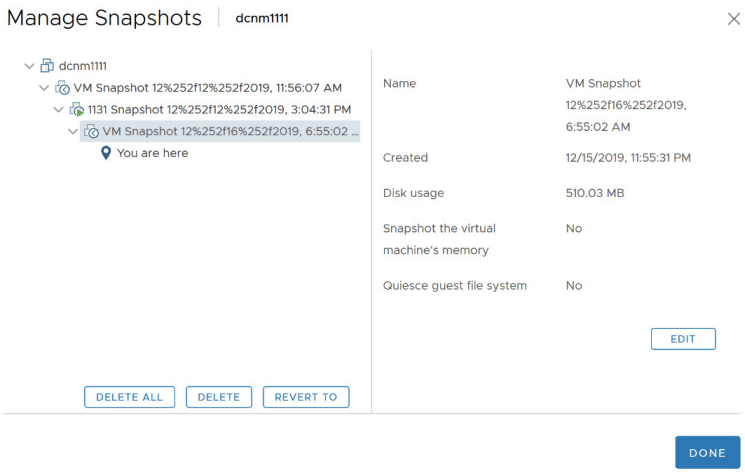
- When VM is powered off.
- When VM is powered on, and active.

Note Cisco DCNM supports snapshots when VM is either powered on or powered off. DCNM doesn't support snapshots when the Virtual Machine memory option is selected.

Ensure that **Snapshot the Virtual Machine's memory** check box must not be selected, as shown in the following figure. However, it is grayed out when the VM is powered off.



You can restore VM to the state in a Snapshot.



Right-click on the Virtual Machine and select **Manage Snapshot**. Select the snapshot to restore, and click **Done**.

Supported Web Browsers

Cisco DCNM supports the following web browsers:

- Google Chrome version: 86.0.4240.198
- Mozilla Firefox version: 82.0.3 (64-bit)
- Microsoft Edge version: 86.0.622.63

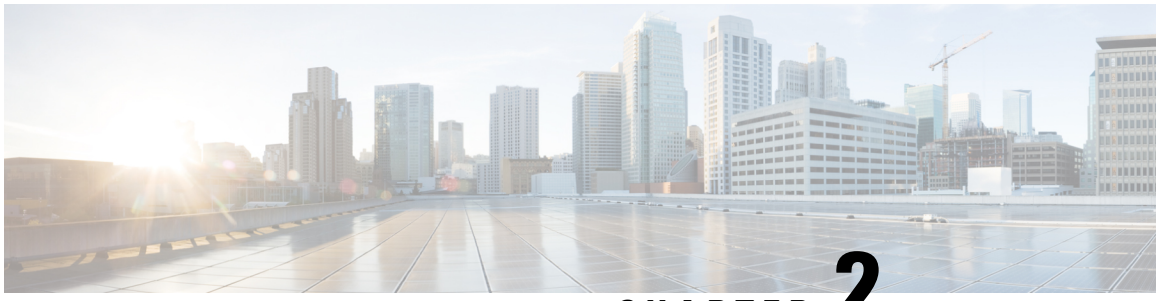
Other Supported Software

The following table lists the other software that is supported by Cisco DCNM Release 11.5(1).

Table 5: Other Supported Software

Component	Features
Security	• ACS versions 4.0, 5.1, 5.5, and 5.8 • ISE version 2.6 • ISE version 3.0 • 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 • TLS 1.3
OVA\ISO Installers	CentOS 7.8/Linux Kernel 3.10.x

Also, Cisco DCNM supports call-home events, fabric change events, and events that are forwarded by traps and email.



CHAPTER 2

Guidelines and Limitations

- Guidelines and Limitations, on page 11
- Checking TPM Partition before Converting DCNM-SE to Nexus Dashboard, on page 13

Guidelines and Limitations

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

General Guidelines and Limitations

- Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application might not function properly:
  - It must be at least 8 characters long and contain at least one alphabet and one numeral.
  - It can contain a combination of alphabets, numerals, and special characters.
  - Do not use any of these special characters in the DCNM password: <SPACE> " & $ % ' ^ = < > ; : ` \ | / , .*
  - From Cisco DCNM Release 11.0(1), the characters that are allowed in the Administrative password is restricted for OVA and ISO installations. Therefore while upgrading, the old password used in DCNM 11.0(1) or 11.1(1) is not valid. However, different passwords are allowed during Upgrade.

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

    —accessing the DCNM appliance via its console.

    —accessing the appliance via SSH

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

    However, after the upgrade, since Postgres DBMS is restored from the backup that is taken on DCNM 10.4(2), you must logon to the Cisco DCNM Web UI using the password used on DCNM Release 10.4(2) appliance.
- Do not interrupt the boot process (such as pressing the Ctrl+ALT + DELETE keys) when installing DCNM. If you interrupt, you must restart the installation process.
- Ensure that you configure the timezone after installation or upgrade, before performing any other operations on the Cisco DCNM Appliance. Use the NTP server for configuring timezones.

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

Fresh Installation

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

Upgrade

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

  For DCNM in Native HA mode, Telemetry is supported with 3 compute nodes only.
- If you need to run Network Insights applications, you must install 3 compute nodes.
- Disable Telemetry before modifying Interface settings. You can enable Telemetry after modifying the settings.
- During a backup and restore process, the compute nodes are also included in the backup. After you deploy the new compute, you can restore the backup on the compute node.

  If there was no backup, disconnect the 3 compute nodes, and erase the data on all the compute nodes. On the Cisco DCNM Web Client UI, navigate to **Application > Compute**. Select the **+** icon to join the compute nodes.
- To erase data on the compute node, logon to the compute node through an SSH session and erase the data using the **rm -rf /var/afw/vols/data** command.



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

- Before starting NIR application after upgrade, on the DCNM Web UI, choose **Application > Preferences**. Modify the network settings as required. If you do not modify the network settings after upgrade before you enable the Telemetry on the Fabrics, the configuration will not complete. You must stop the NIR app, modify the network settings and start the app again, to resolve the issue.

Checking TPM Partition before Converting DCNM-SE to Nexus Dashboard

A few Cisco Application Services Engine (SE) nodes that was factory pre-installed with DCNM 11.5(1) or earlier may have a corrupted TPM partition. This causes the installation of Cisco Nexus Dashboard software to fail. You must check the TPM Partition before upgrading from Cisco DCNM-SE to Cisco Nexus Dashboard.



Note TPM is not a requirement for DCNM 11.x releases. Therefore, this issue does not affect existing DCNM 11.x functionality of the device, even if the device is affected by this issue. No further action is required until you decide to upgrade to Cisco Nexus Dashboard.

To identify if your Cisco DCNM-SE is affected by this issue, perform the following steps:

Procedure

Step 1 SSH to Cisco Application Services Engine using **sysadmin** user.

Step 2 Run the following command to view the list of models and their vendors.

lsblk-S

```
[root@dcnm-se-active sysadmin]$ lsblk -S
NAME   HCTL       TYPE     VENDOR   MODEL             REV TRAN
...
sdc    0:2:2:0    disk     Cisco    UCSC-RAID12G-2GB  5.10
sdd    0:2:3:0    disk     Cisco    UCSC-RAID12G-2GB  5.10
sde    0:2:4:0    disk     Cisco    UCSC-RAID12G-2GB  5.10
sdf    7:0:0:0    disk     UNIGEN   PQT8000           1100 usb  /*identiifying device from
 UNIGEN Vendor*/
sdg    8:0:0:0    disk     UNIGEN   PHF16H0CM1-ETG    PMAP usb
sdl    1:0:0:0    disk     ATA      Micron_5100_MTFD  H072 sata
...
```

Applications Services Engine from **UNIGEN** vendor is detected with device name **sdf**.

Step 3 Run the following command to view the partitions in the disk.

lsblk -s or **lsblk**

- **Example1**

  The following example shows functioning TPM disk with two partitions sdf1 and sdf2. This can be installed with Cisco Nexus Dashboard software with no issues.

```
[root@dcnm-se-active sysadmin]$ lsblk
NAME                MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
...
sdc                   8:32   0   2.2T  0 disk
sdd                   8:48   0   2.2T  0 disk
sde                   8:64   0   371.6G  0 disk
sdf                   8:80   1   7.7G  0 disk  /*functioning TPM with partition*/
 |--sdf1                8:81   1    60M  0 part
 |--sdf2                8:82   1   3.7G  0 part
```

```
nvme0n1              259:0    0   1.5T  0 disk
 |--nvme0n1p1          259:1    0   1.5T  0 part
   |--flashvg-flashvol 253:3    0   1.5T  0 lvm  /var/afw/vols/data/flash
...
```

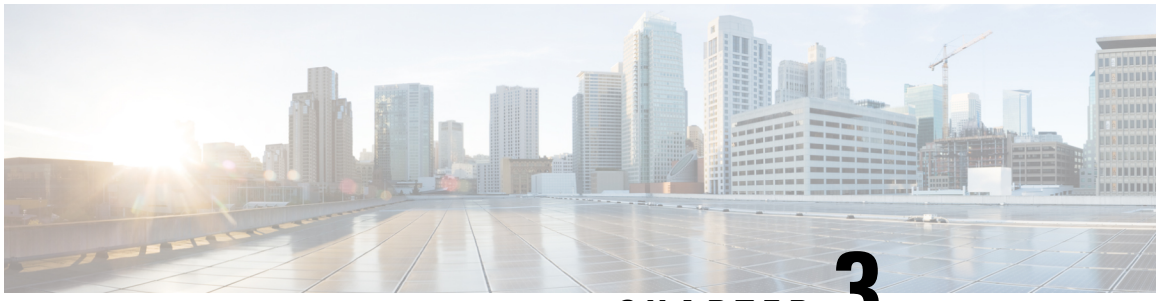
- **Example2**

  The following example shows defective or corrupted TPM disk with no partitions defined on device **sdf**. This unit cannot be used to install Cisco Nexus Dashboard software, and must be replaced.

```
[root@dcnm-se-active sysadmin]$ lsblk
NAME                 MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
...
sdc                    8:32   0   2.2T  0 disk
sdd                    8:48   0   2.2T  0 disk
sde                    8:64   0   371.6G  0 disk
sdf                    8:80   1   16G  0 disk  /*corrupted TPM without partition*/
nvme0n1              259:0    0   1.5T  0 disk
 |--nvme0n1p1          259:1    0   1.5T  0 part
   |--flashvg-flashvol 253:3    0   1.5T  0 lvm  /var/afw/vols/data/flash
...
```

Step 4 If your device has a TPM disk with no partitions, contact Cisco Technical Assistance Center (TAC) to initiate RMA and replace the device.

No further action is required if your TPM has partitions.



CHAPTER 3

Prerequisites

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

- Prerequisites for DCNM Open Virtual Appliance, on page 15
- Prerequisites for DCNM ISO Virtual Appliance, on page 16
- Prerequisites for Cisco DCNM Virtual Appliance HA, on page 16

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 .

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*.

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

VMware ESXi

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

Kernel-based Virtual Machine (KVM)

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



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

Prerequisites for Cisco DCNM Virtual Appliance HA

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

Deploying Cisco DCNM Virtual Appliances in HA mode

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

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

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

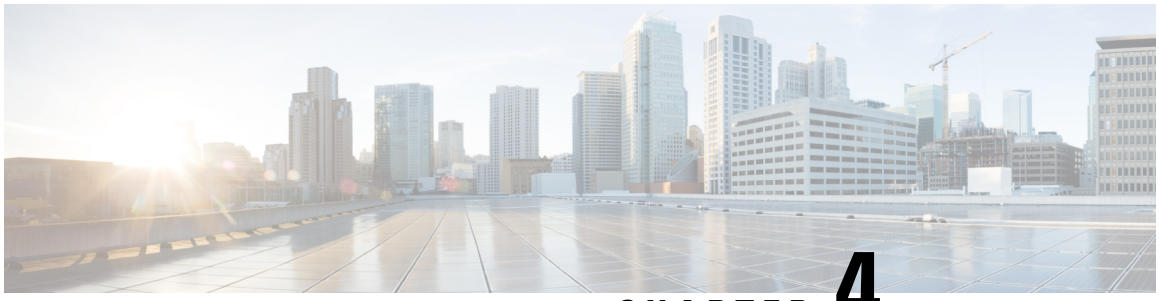
Availability of Virtual IP Addresses

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

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

Installing an NTP Server

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



CHAPTER 4

Installing the Cisco DCNM

Supported Latency

The supported latency for Cisco DCNM LAN Fabric deployment is defined below:

- Between Native HA Primary and Secondary appliances, latency is 50ms.
- Between DCNM Native HA Primary appliance to Switches, latency is 50ms.
- Between DCNM Computes latency is 50ms.

This chapter contains the following sections:

If you are installing Cisco DCNM on SE, install the DCNM ISO Virtual Appliance (.iso) installer.

- Installing DCNM on Open Virtual Appliance, on page 19
- Installing DCNM on ISO Virtual Appliance, on page 36
- Convert Standalone Setup to Native-HA Setup, on page 68
- Installing Cisco DCNM Compute Node, on page 72

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/http://software.cisco.com/download/.

A list of the latest release software for Cisco DCNM available for download is displayed.

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 11.5(1).

Step 5 Locate the DCNM Open Virtual Appliance Installer and click the **Download** icon.

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

Deploying the Open Virtual Appliance as an OVF Template

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



Note Deploy two OVAs for the HA setup.

Procedure

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

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

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

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

- Mozilla Firefox browser, with HTML 5 support

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

  Use flex interface if HTML 5 is not supported

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

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

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

Deploy OVF Template Wizard opens.

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

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

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

Click **Next**.

Step 5 Verify the OVA template details and click **Next**.

Step 6 On the End User License Agreement screen, read the license agreement.

Click **Accept** and click **Next**.

Step 7 On the Select name and location screen, enter the following information:

- In the Name field, enter an appropriate name for the OVF.

  Note
  Ensure that the VM name is unique within the Inventory.

- In the Browse tab, select **Datacenter** as the deployment location under the appropriate ESXi host.

Click **Next**.

Step 8 On the Select configuration screen, select the configuration from the drop-down list.

- Choose **Small** (Lab or POC) to configure the virtual machine with 8 vCPUs, 24GB RAM.

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

- Choose **Large** (Production) to configure the virtual machine with 16 vCPUs, 32GB RAM.

  We recommend that you use a Large deployment configuration when you are managing more than 50 devices to leverage better RAM, heap memory, and CPUs. For setups that could grow, choose Large.

- Choose **Compute** to configure the virtual machine with 16 vCPUs, 64GB RAM.

  You must have DCNM deployed in Compute mode to use applications in your deployment.

- Choose **Huge** to configure the virtual machine with 32 vCPUs, 128GB RAM.

  This configuration is recommended if you deploy DCNM for SAN Management and use SAN Insights feature.

- Choose **ComputeHuge** to configure the virtual machine with 32vCPUs and 128GB RAM with 2TB disk.

  This configuration is recommended if you use Cisco Network Insights applications.

Click **Next**.

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

Click **Next**.

Step 10 On **Select storage** screen, based on the Datastore and Available space choose the disk format and the destination storage for the virtual machine file.

a) Select the virtual disk format from the drop-down list.

The available disk formats are:

Note
Choose one of the thick provision types if you have enough storage capacity as required by the virtual appliance and want to set a specific allocation of space for the virtual disks.

- **Thick Provision Lazy Zeroed**: The space that is required for the virtual disk is allocated when the virtual disk is created. The data that remains on the physical device is not erased when the virtual disk is created but is zeroed out on demand later on first write from the virtual disk.
- **Thin Provision**: The disk space available is less than 100 GB. The initial disk consumption is 3GB and increases as the size of the database increases with the number of devices being managed.
- **Thick Provision Eager Zeroed**: The space that is required for the virtual disk is allocated when the virtual disk is created. Unlike the Lazy Zeroed option, the data that remains on the physical device is erased when the virtual disk is created.

  Note
  With 500G, the DCNM installation will appear to be stuck with option Thick Provision Eager Zeroed. However, it takes longer time to complete.

b) Select the VM storage policy from the drop-down list.

By default, no policy is selected.

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

Click **Next**.

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

- **dcnm-mgmt network**

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

- **enhanced-fabric-mgmt**

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

- **enhanced-fabric-inband**

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

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

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation, on page 155.

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.

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

Click **Next**.

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

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

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

Ensure that add valid values for the **Management Network** properties. Properties with invalid values will not be assigned. The VM will not power on until you enter valid values.

From Release 11.3(1), for Huge and Compute configurations, you can add extra disk space on the VM. You can add from 32GB up to 1.5TB of disk space. In the **Extra Disk Size** field, enter the extra disk size that will be created on the VM.

Click **Next**.

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

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

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

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

Note
If this deployment is a part of the upgrade process, do not Power on the VM. Edit and provide the 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
https://<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 the Cisco DCNM OVA in Standalone Mode, on page 24 or Installing the Cisco DCNM OVA in Native HA mode, on page 28.

Installing the Cisco DCNM OVA in Standalone Mode

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

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

Procedure

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

Caution
If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

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

Click **Next**.

Step 3 On the **Install Mode** tab, choose your DCNM deployment type.

From the **Installation mode** drop-down list, choose **LAN Fabric** installation mode for the DCNM Appliance.

Check the **Enable Clustered Mode** check box, if you want to deploy Cisco DCNM in Cluster mode. The Compute nodes will be displayed on the Cisco DCNM **Web UI > Applications > Compute**. The applications will run on the **Compute** nodes. You can add the compute nodes to a Cluster, later.

If you require Compute Cluster, ensure that you have 3NICs while you configure the virtual appliance. Installing NICs later is not supported. If you do not have 3 NICs, **Enable Clustered Mode** is not available.

Note
If **Enable Clustered Mode** is selected, applications such as, Config Compliance, EPL, and NIA, and NIR won't work until you install the compute nodes.

Click **Next**.

Step 4 On the **Administration** tab, enter information about passwords.

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

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

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

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

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

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

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

- In the **Superuser Password (root)** field, enter the password for the Superuser to access root privileges.

  Enter the password again in the **Superuser Password** field.

  Note
  If the Superuser Password is left blank, it shall consider the Administrator password as the Superuser password. However, we recommend that you configure a strong password for security reasons.

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

Click **Next**.

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

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

  You can also configure the DNS server using an IPv6 address.

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

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

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

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

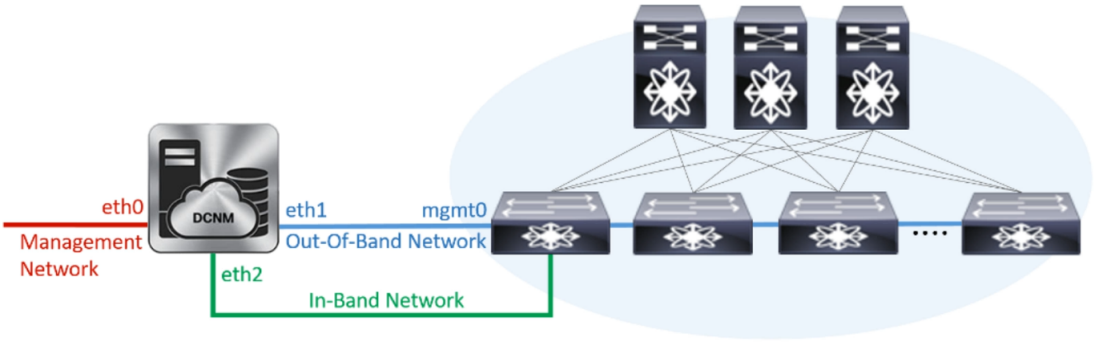
  From Release 11.3(1), you can configure more than one NTP server.

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

Click **Next**.

Step 6 On the **Network Settings** tab, configure the network parameters used to reach the DCNM Web UI.

Figure 1: Cisco DCNM Management Network Interfaces



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

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

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

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

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

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

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

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

This field is mandatory if you have selected the Enable Cluster mode in Step Step 3, on page 24.

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

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

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

If you require Compute Cluster, ensure that you have 3NICs while you configure the virtual appliance. Installing NICs later is not supported. If you do not have 3 NICs, **Enable Clustered Mode** is not available, and therefore, you cannot configure the eth2 interface.

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation, on page 155.

Click **Next**.

Step 7 On the **Applications** tab, configure the Device Connector and Internal Applications Services Network, and Cluster mode settings.

Note
Device Connector is enabled by default.

The Device connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform.

a) (Optional) In the **Proxy Server** field, enter the IP address for the proxy server.

The proxy server must be of RFC1123-compliant name.

Note
By default, port 80 is used for proxy server. Use **<proxy-server-ip>:<port>** to use proxy server is a different port.

If the proxy server must require authentication, enter relevant username and password in the **Proxy Server Username** and **Proxy Server Password** fields.

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

All the applications use the IP Address from this subnet.

c) In the **Clustered mode configuration** area, configure the network settings to deploy the DCNM instance in Clustered mode. In Clustered mode, applications run on separate compute nodes.

The Cluster Mode configuration area appears only if you have selected the **Enable Clustered Mode** check box in Step Step 3, on page 24.

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

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

  Optionally, you can also enter an IPv6 address pool in the **Out-of-Band IPv6 Network Address Pool** field.

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

  Optionally, you can also enter an IPv6 address pool in the **In-Band IPv6 Network Address Pool** field.

The address must be a smaller prefix of available IP addresses from the eth1 subnet. For example: Use 10.1.1.240/28 if the eth1 subnet was configured as 10.1.1.0/24 during installation. This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

Click **Next**.

Step 8 On the Summary tab, review the configuration details.

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

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

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

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

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

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

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

************************************
```

What to do next

Log on to the DCNM Web UI with appropriate credentials.

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

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

```
dcnm# appmgr update network-properties add route ipv4 eth2 <ipv4-network-ip-address/prefix>
```

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

```
dcnm# appmgr update network-properties session start
dcnm# appmgr update network-properties add route ipv4 eth2 10.0.0.0/24
dcnm# appmgr update network-properties add route ipv4 eth2 40.1.1.0/24
dcnm# appmgr update network-properties session apply
```

Installing the Cisco DCNM OVA in Native HA mode

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

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

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

Procedure

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

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

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

A welcome message appears.

a) On the **Welcome to Cisco DCNM** screen, click **Get Started**.

Caution
If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

b) On the **Cisco DCNM Installer** tab, select **Fresh Installation - HA Primary** radio button, to install **dcnm1** as Primary node.

Click **Next**.

c) On the **Install Mode** tab, choose your DCNM deployment type.

From the **Installation mode** drop-down list, choose **LAN Fabric** installation mode for the DCNM Appliance.

Check the **Enable Clustered Mode** check box, if you want to deploy Cisco DCNM in Cluster mode. The Compute nodes will be displayed on the Cisco DCNM **Web UI > Applications > Compute**. The applications will run on the **Compute** nodes. You can add the compute nodes to a Cluster, later.

If you require Compute Cluster, ensure that you have 3NICs while you configure the virtual appliance. Installing NICs later is not supported. If you do not have 3 NICs, **Enable Clustered Mode** is not available.

Note
If **Enable Clustered Mode** is selected, applications such as, Config Compliance, EPL, and NIA, and NIR won't work until you install the compute nodes.

Click **Next**.

d) On the **Administration** tab, enter information about passwords.

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

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

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

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

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

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

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

- In the **Superuser Password (root)** field, enter the password for the Superuser to access root privileges.

  Enter the password again in the **Superuser Password** field.

  Note
  If the Superuser Password is left blank, it shall consider the Administrator password as the Superuser password. However, we recommend that you configure a strong password for security reasons.

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

Click **Next**.

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

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

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

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

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

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

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

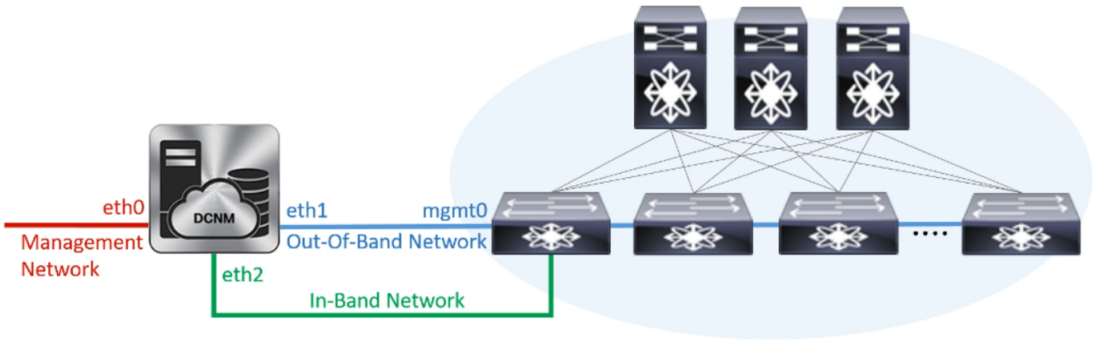
  From Release 11.3(1), you can configure more than one NTP server.

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

Click **Next**.

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

Figure 2: Cisco DCNM Management Network Interfaces



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

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

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

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

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

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

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

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

   This field is mandatory if you have selected the **Enable Cluster** mode..

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

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

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

If you require Compute Cluster, ensure that you have 3NICs while you configure the virtual appliance. Installing NICs later is not supported. If you do not have 3 NICs, **Enable Clustered Mode** is not available, and therefore, you cannot configure the eth2 interface.

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation, on page 155.

Click **Next**.

g) On the **Applications** tab, configure the Device Connector and Internal Applications Services Network.

Note
Device Connector is enabled by default.

The Device connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform.

1. In the **Proxy Server** field, enter the IP address for the proxy server.

   The proxy server must be of RFC1123-compliant name.

   Note
   By default, port 80 is used for proxy server. Use **<proxy-server-ip>:<port>** to use proxy server is a different port.

   If the proxy server must require authentication, enter relevant username and password in the **Proxy Server Username** and **Proxy Server Password** fields.

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

   All the applications use the IP Address from this subnet. By default, the

   The Cluster Mode configuration area appears only if you have selected the **Enable Clustered Mode** check box in Step 2.c, on page 29.

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

3. In the **Clustered mode configuration** area, configure the network settings to deploy the DCNM instance in Clustered mode. In Clustered mode, applications run on separate compute nodes.

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

     Optionally, you can also enter an IPv6 address pool in the **Out-of-Band IPv6 Network Address Pool** field.

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

     Optionally, you can also enter an IPv6 address pool in the **In-Band IPv6 Network Address Pool** field.

   The address must be a smaller prefix of available IP addresses from the eth1 subnet. For example: Use 10.1.1.240/28 if the eth1 subnet was configured as 10.1.1.0/24 during installation. This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

h) On the **HA Settings** tab, a confirmation message appears.

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

   Click **Next**.

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

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

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

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

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

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

A welcome message appears.

a) On the **Welcome to Cisco DCNM** screen, click **Get Started**.

Caution
If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

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

Click **Continue**.

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

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

Check the **Enable Clustered Mode** check box, if you have configured the Cisco DCNM Primary in Clustered mode.

Click **Next**.

d) On the **Administration** tab, enter information about passwords.

Note
All the passwords must be same as the passwords that you provided while configuring the Primary node.

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

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

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

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

  Note
  If you're using Network Insights applications, ensure that the DNS server is valid and reachable.
- In the **NTP Server Address List** field, enter the IP address of the NTP server.

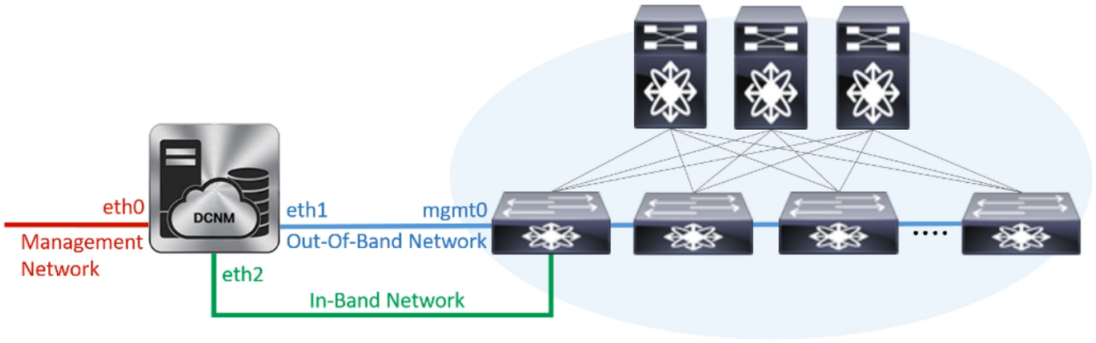
  The value must be an IP or IPv6 address or RFC 1123 compliant name.

  From Release 11.3(1), you can configure more than one NTP server.
- From the **Timezone** drop-down list, select the timezone in which you are deploying the DCNM.

Click **Next**.

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

Figure 3: Cisco DCNM Management Network Interfaces



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

   Note
   Ensure that the IP address belongs to the same Management Network configured on the Primary node.

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

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

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

   Note
   Ensure that the IP addresses belong to the same Out-of-Band network configured on the Primary node.

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

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

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

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

   Note
   Ensure that the IP addresses belong to the same In-Band network configured on the Primary node.

   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.

Click **Next**.

g) On the **Applications** tab, configure the Internal Applications Services Network, and Cluster mode settings.

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

2. In the **Clustered mode configuration** area, configure the network settings to deploy the DCNM instance in Clustered mode. In Clustered mode, applications run on separate compute nodes.
   - In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the Out-of-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **Out-of-Band IPv6 Network Address Pool** field.
   - In the **In-Band IPv4 Network Address Pool**, enter the address pool from the In-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **In-Band IPv6 Network Address Pool** field.

   Ensure that the IP addresses belong to the same pool as configured on the Primary node.

h) On the **HA Settings** tab, configure the system settings for the Secondary node.
   - In the **Management IPv4 Address of Primary DCNM node** field, enter the appropriate IP Address to access the DCNM UI.
   - In the **VIP Fully qualified Host Name** field, enter hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Host names with only digits is not supported.
   - In the **Management Network VIP address** field, enter the IP address used as VIP in the management network.

     Optionally, you can also enter an IPv6 VIP address in the **Management Network VIPv6 address** field.

     Note
     If you have configured the Management network using IPv6 address, ensure that you configure the Management Network VIPv6 Address.
   - In the **Out-of-Band Network VIP Address** field, enter the IP address used as VIP in the Out-of-Band network.

     Optionally, you can also enter an IPv6 VIP address in the **Out-of-Band Network VIPv6 Address** field.
   - In the **In-Band Network VIP Address** field, enter the IP address used as VIP in the Out-of-Band network.

     Optionally, you can also enter an IPv6 VIP address in the **In-Band Network VIPv6 Address** field.

     Note
     This field is mandatory if you have provided an IP address for In-Band network in the **Network Settings** tab.
   - In the **HA Ping Feature IPv4 Address** field, enter the HA ping IP address and enable this feature, if necessary.

     Note
     The configured IPv4 address must respond to the ICMP echo pings.

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

You must configure the HA ping IPv4 Address to avoid the Split Brain scenario. This IP address must belong to Enhanced Fabric management network.

Click **Next**.

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

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

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

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

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

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

What to do next

Log on to the DCNM Web UI with appropriate credentials.

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

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

```
dcnm# appmgr update network-properties add route ipv4 eth2 <ipv4-network-ip-address/prefix>
```

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

```
dcnm# appmgr update network-properties session start
dcnm# appmgr update network-properties add route ipv4 eth2 10.0.0.0/24
dcnm# appmgr update network-properties add route ipv4 eth2 40.1.1.0/24
dcnm# appmgr update network-properties session apply
```

Installing DCNM on ISO Virtual Appliance

This chapter contains the following sections:

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

If you are installing Cisco DCNM on SE, install the DCNM ISO Virtual Appliance (.iso) installer.

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/http://software.cisco.com/download/.

A list of the latest release software for Cisco DCNM available for download is displayed.

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 11.5(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 44 or Installing the DCNM ISO Virtual Appliance on UCS (Bare Metal), on page 37 for more information.

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

From Release 11.3(1), you can install Cisco DCNM ISO using an additional mode where the physical interfaces are bound together for a port channel or ethernet channel configured as a trunk with the management traffic, out-of-band traffic, and in-band traffic separated in different VLANs.

Ensure that the switch is configured correctly for bundled interface mode. The following shows a sample switch configuration for bundled interface mode:

```
vlan 100
vlan 101
vlan 102
interface port-channel1
  switchport
  switchport mode trunk

interface Ethernet101/1/1
  switchport mode trunk
  channel-group 1
  no shutdown

interface Ethernet101/1/2
  switchport mode trunk
  channel-group 1
  no shutdown

interface Ethernet101/1/3
  switchport mode trunk
  channel-group 1
  no shutdown

interface Ethernet101/1/4
  switchport mode trunk
  channel-group 1
  no shutdown
```

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

Note **appmgr** commands are run by a shell (Bash) and some characters have a different interpretation. Therefore, passwords provided in the command itself containing special characters must be quoted. Alternatively, you can run **appmgr change_pwd ssh root** and provide the password at the prompt.

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.

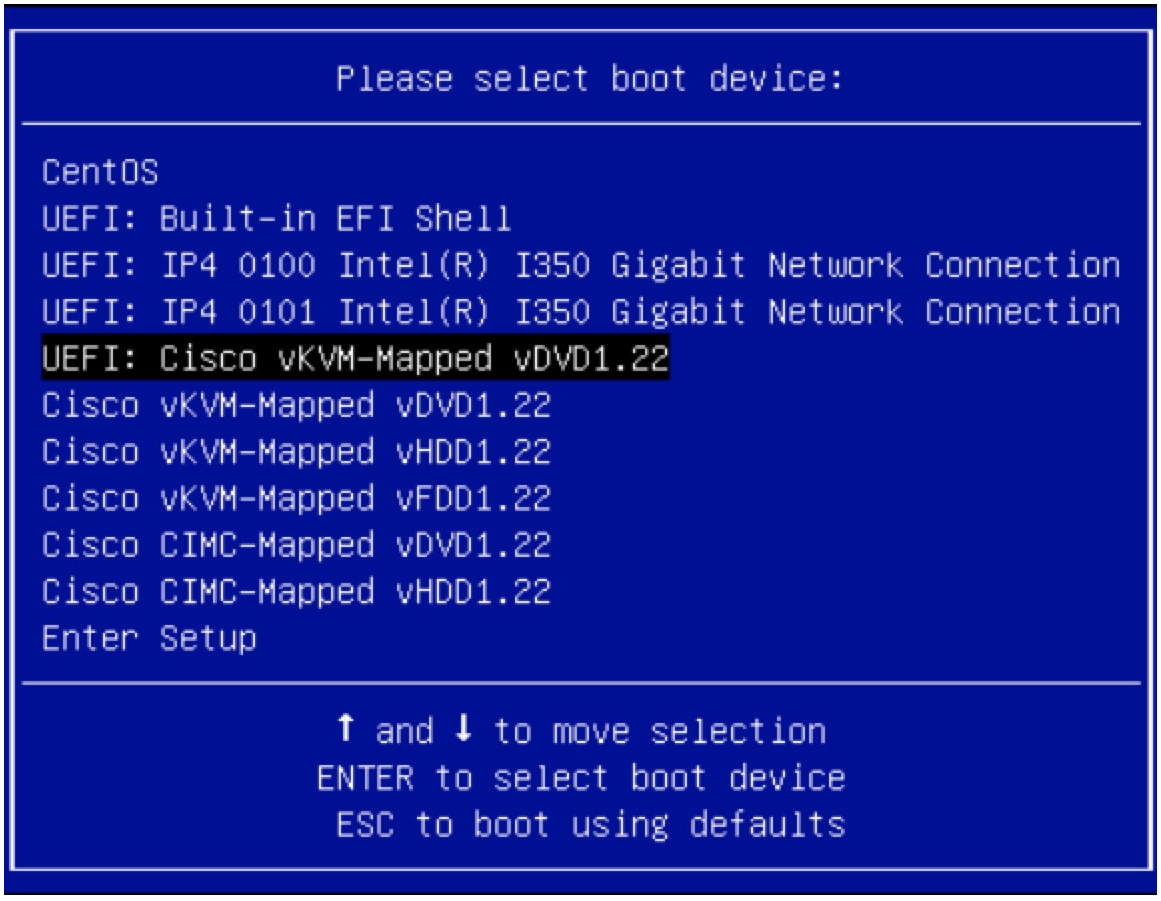
For more information about using the UCS KVM Console window, see the Cisco UCS Server Configuration Utility, Release 3.1 User Guide at the following URL:

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.

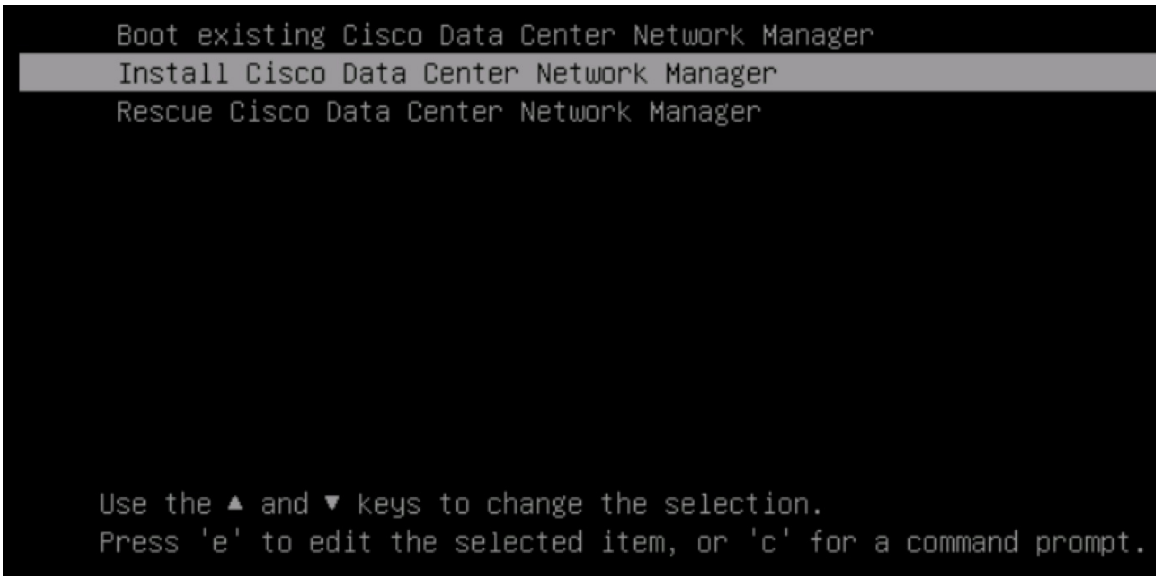
UEFI is mandatory for a system with minimum of 2TB disks.



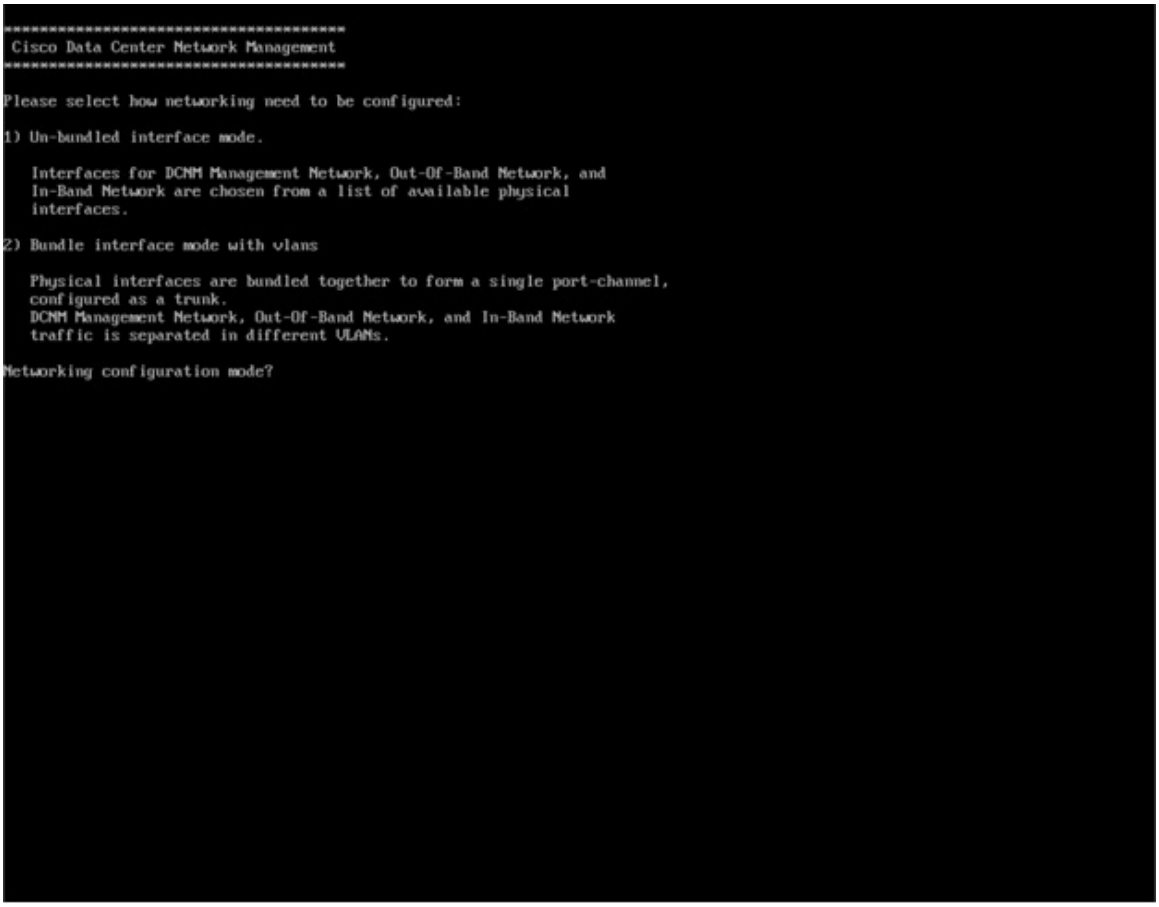
For Cisco UCS with the disk size of 2TB or higher and with 4K sector size drivers, the UEFI boot option is required. For more information, see UEFI Boot Mode.

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.



Step 10 On the Cisco Management Network Management screen, select the mode to configure the network.



Enter 1 to configure the Cisco DCNM network interfaces from the available physical interfaces.

Enter 2 to configure the Cisco DCNM network interfaces from the available physical interfaces that are bundled together to form a single port-channel, configured as a trunk.

Step 11 If you entered 1, to install Cisco DCNM ISO in un-bundled interface mode, 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.

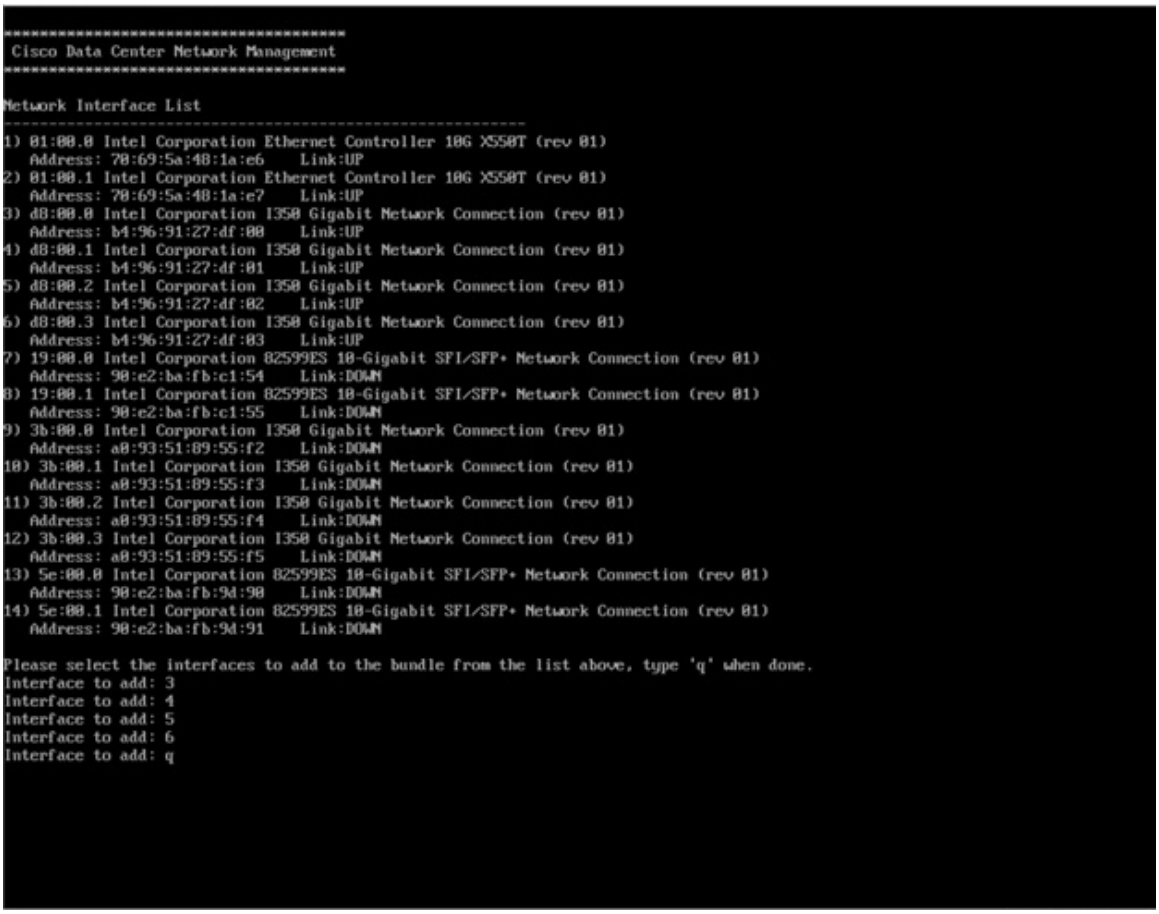
However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation, on page 155.

Step 12 If you entered 2, to install Cisco DCNM ISO in bundled interface mode, perform the following tasks:

a) Select interface from the list to form a bundle.

Note
A minimum of one physical interface must be a part of the bundle.

Enter **q** after you enter all the interface that must be added to the bundle.



b) Enter the VLAN IDs to be used for Management Network, Out-Of-Band Network and In-band Network Select interface from the list to form a bundle.

Verify and confirm if the correct VLAN IDs are assigned.

Note
The VLAN IDs for Management Network and Out-Of-Band Network can be the same when Management Network and Out-Of-Band Network use the same subnet (that is, when eth0/eth1 are in the same subnet)



Step 13 Review the selected interfaces. Press **y** to confirm and continue with the installation.

Step 14 Configure the Management Network for Cisco DCNM. Enter the IP address, Subnet Mask, and Gateway. Press **y** to continue with the installation.

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

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

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

What to do next

You can choose to install DCNM in Standalone mode or Native HA mode. Refer to *Installing Cisco DCNM ISO in Standalone Mode* or *Installing Cisco DCNM ISO in Native HA Mode* sections 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 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 and **dcnm-kvm-vm.xml** to the RHEL server.

Step 5 Close the file transfer session.

Step 6 Connect to the RHEL server running KVM via SSH terminal.

Step 7 Navigate to the location where both the ISO and domain XMLs is downloaded.

Step 8 Create the VM (or Domains, as they are known in the KVM terminology) using the **virsh** command.

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

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

Step 9 Enable a VNC server and open the required firewall ports.

Step 10 Close the SSH session.

Step 11 Connect to the RHEL server running KVM via a VNC terminal.

Step 12 Navigate to **Applications > System Tools > Virtual Machine Manager (VMM)**.

A VM is created in the Virtual Machine Manager.

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

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

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

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

We recommend that you use storage size of 500GB.

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

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

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

Step 19 Power on the Virtual Machine.

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

The operating system is installed.

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

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

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

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation, on page 155.

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

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

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

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

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

What to do next

You can choose to install DCNM in Standalone mode or Native HA mode. Refer to *Installing Cisco DCNM ISO in Standalone Mode* or *Installing Cisco DCNM ISO in Native HA Mode* sections for more information.

Installing the DCNM ISO Virtual Appliance on Nexus Dashboard

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

Before you begin

Set up the hardware and network connectivity, as described in Cisco Nexus Dashboard Hardware Setup Guide.

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 click **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.

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.

Step 9 Select **Install Cisco Data Center Network Manager** using the up or down arrow keys. Press **Enter**.

Step 10 Review the selected interfaces. Press **y** to confirm and continue with the installation.

Step 11 Configure the Management Network for Cisco DCNM. Enter the IP address, Subnet Mask, and Gateway. Press **y** to continue with the installation.

The provided IP addresses are used to configure the management network interface (eth0). The system will now be reachable over the network.

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

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

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

What to do next

You can choose to install DCNM in Standalone mode or Native HA mode. Refer to Installing Cisco DCNM ISO in Standalone Mode, on page 55 or Installing the Cisco DCNM ISO in Native HA mode, on page 60 for more information.

Installing the DCNM ISO Virtual Appliance on Windows Hyper-V

Hyper-V Manager provides management access to your virtualization platform. You can install DCNM ISO virtual appliance using Hyper-V manager.

Launch the Windows Server Manager using appropriate credentials. To launch the Hyper-V Manager, from the Menu bar, choose **Tools** > **Hyper-V Manager**.

Note DCNM ISO Virtual Appliance on Windows Hyper-V doesn't support Clustered mode.

To install Cisco DCNM ISO Virtual Appliance on Windows Hyper-V, perform the following tasks:

Creating Virtual Switches

Cisco DCNM requires three virtual switches for network interfaces:

- dcnm-mgmt network (eth0) interface
- enhanced-fabric-mgmt (eth1) interface
- enhanced-fabric-inband (eth2) interface

To create Virtual Switches on the Hyper-V Manager, perform the following steps:

Procedure

Step 1 On the Action pane, click **Virtual Switch Manager**.

The Virtual Switch Manager for the Windows Hyper-V window appears.

Step 2 On the left pane, under Virtual Switches, click **New virtual network switch** to create a virtual switch.

Step 3 Create the virtual switch for DCNM Management network.

a) Select **External** and click **Create Virtual Switch**.
b) In the Name field, enter the enter an appropriate name for the **eth0** interface.

Note
Ensure that the virtual switch name is unique within the Inventory.

c) From the External network drop-down list, select the appropriate physical interface available on the server.
d) Click **Apply**.

Step 4 Create the virtual switch for Enhanced Fabric Management interface.

a) Select **External** and click **Create Virtual Switch**.
b) In the Name field, enter the enter an appropriate name for the **eth1** interface.

Note
Ensure that the virtual switch name is unique within the Inventory.

c) From the External network drop-down list, select the appropriate physical interface available on the server.
d) Click **Apply**.

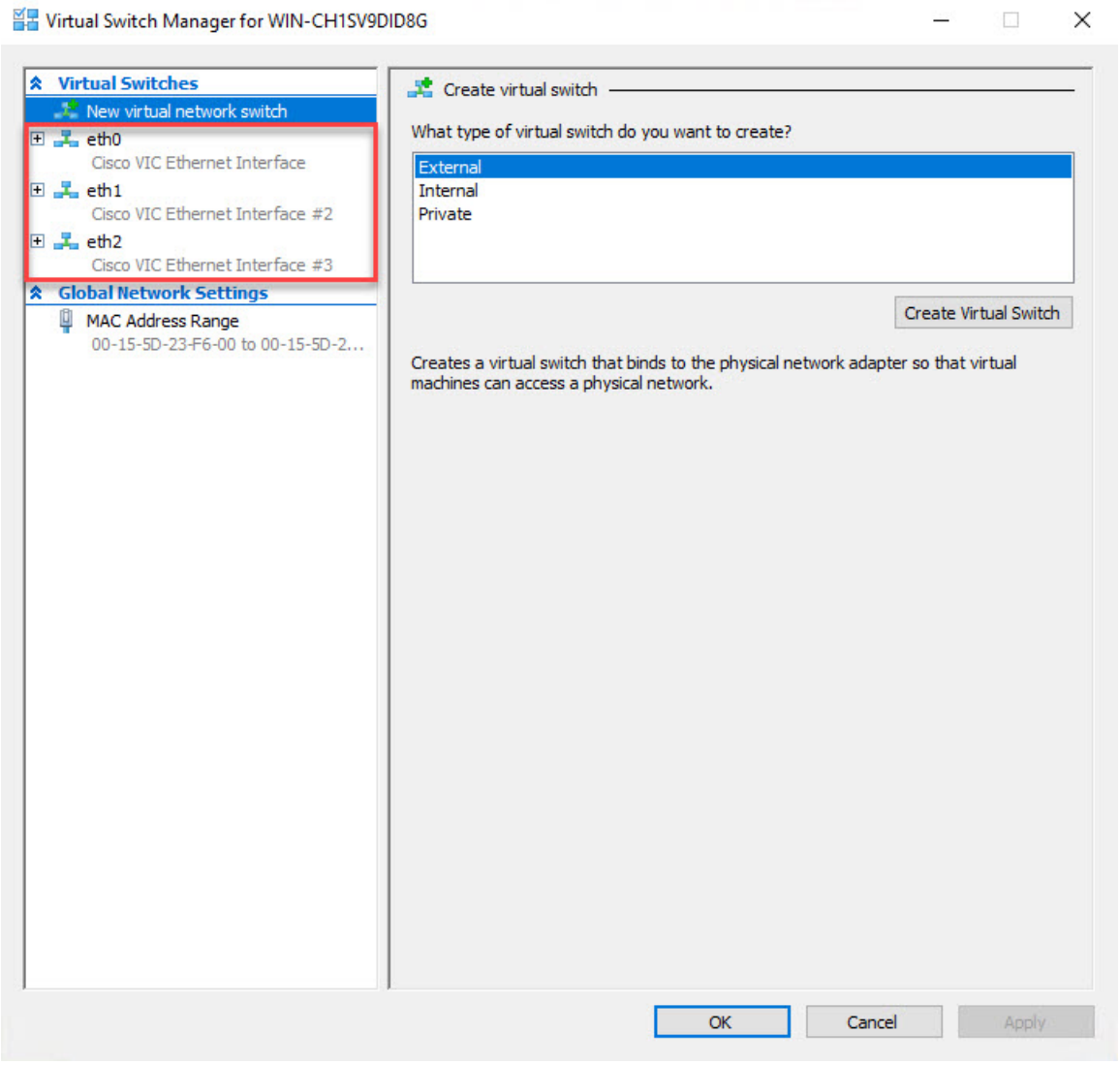
Step 5 Create the virtual switch for Enhanced Fabric Inband interface.

a) Select **External** and click **Create Virtual Switch**.
b) In the Name field, enter the enter an appropriate name for the **eth2** interface.

Note
Ensure that the virtual switch name is unique within the Inventory.

c) From the External network drop-down list, select the appropriate physical interface available on the server.
d) Click **Apply**.

All the interfaces appear under the Virtual Switches in the left pane, as shown in the following figure.



What to do next

Create the Virtual Machines to mount the ISO. Refer to Creating Virtual Machines, on page 48 for more information.

Creating Virtual Machines

To create virtual machines for either Standalone, or Primary and Secondary nodes for Native HA setup, perform the following procedure:

Before you begin

If you're installing Cisco DCNM in Native HA Mode, you must create two virtual machines; one for Primary node, and one for Secondary node.

Procedure

Step 1 In the Actions pane, from the New drop-down list, select **Virtual Machine**.

The New Virtual Machine Wizard appears.

Step 2 In the Before You Begin screen, click **Next**.

Step 3 In the Specify Name and Location screen, enter the name for the Active DCNM node.

Click **Next**.

Step 4 In the Specify Generation screen, select **Generation 2**.

This virtual machine supports new virtualization features, has UEFI-based firmware, and requires 64-bit operating system.

Click **Next**.

Step 5 In the Assign Memory screen, in the **Startup memory** field, enter **32768** MB to configure the virtual machine with 32GB memory.

Step 6 In the Configuration Networking screen, from the **Connection** drop-down list, select the interface for this VM. Select **eth0** (Management Network interface).

Click **Next**.

Step 7 In the Connect Virtual Hard Disk screen, create a virtual hard disk.

a) Select **Create a virtual hard disk**.

b) Enter appropriate **Name**, **Location**, and **Size** of the hard disk.

Note
The default name for the virtual hard disk is derived from the virtual machine name that you provided in the Specify Name and Location screen.

The size of the hard disk must be minimum of 500GB.

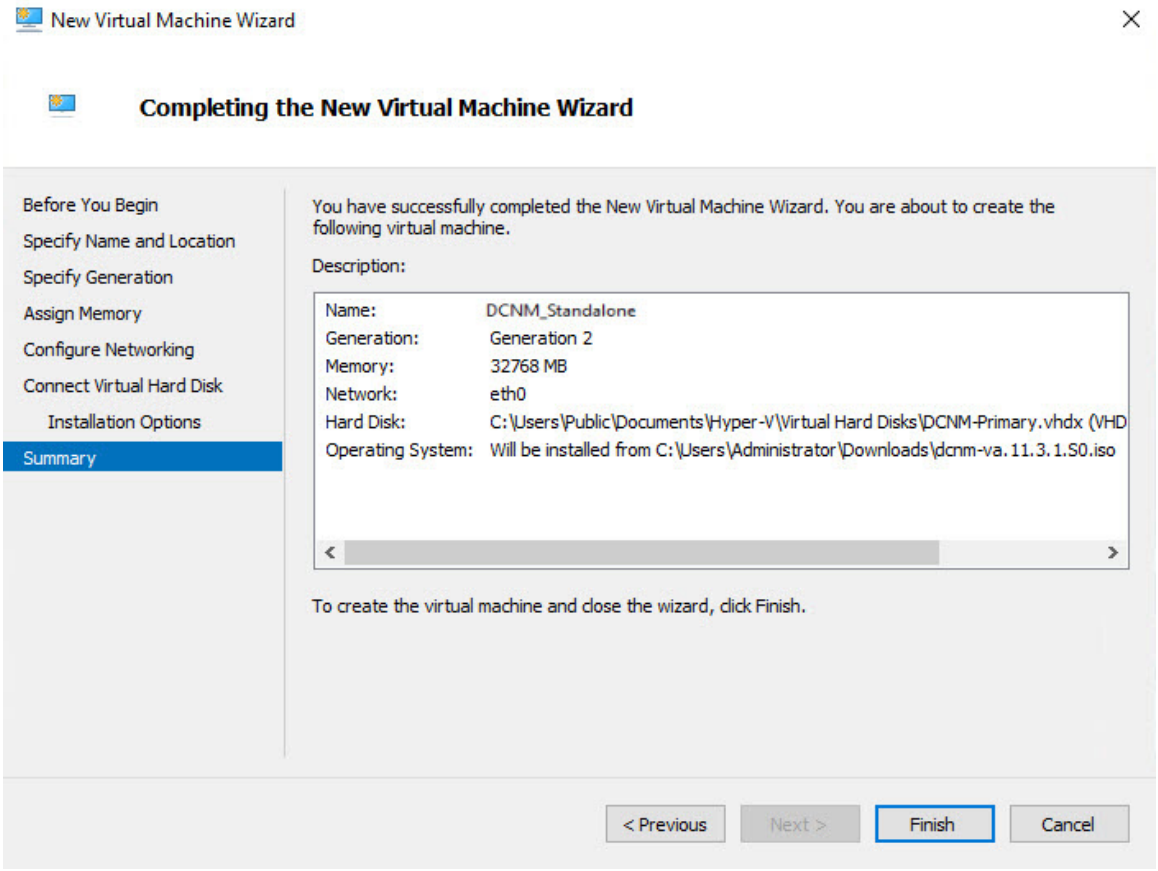
Click **Next**.

Step 8 In the Installation Options screen, select **Install as operating system from a bootable image file**.

In the Image file (.iso) field, click **Browse**. Navigate to the directory and select the DCNM ISO image.

Click **Next**.

Step 9 In the Summary screen, review the configuration details.



Click **Finish** to create the DCNM Active node.

The newly created virtual machine appears in the Virtual Machines block on the Hyper-V Manager.

Step 10 Right click on the virtual machine and select **Settings**.

The Settings screen for DCNM node appears.

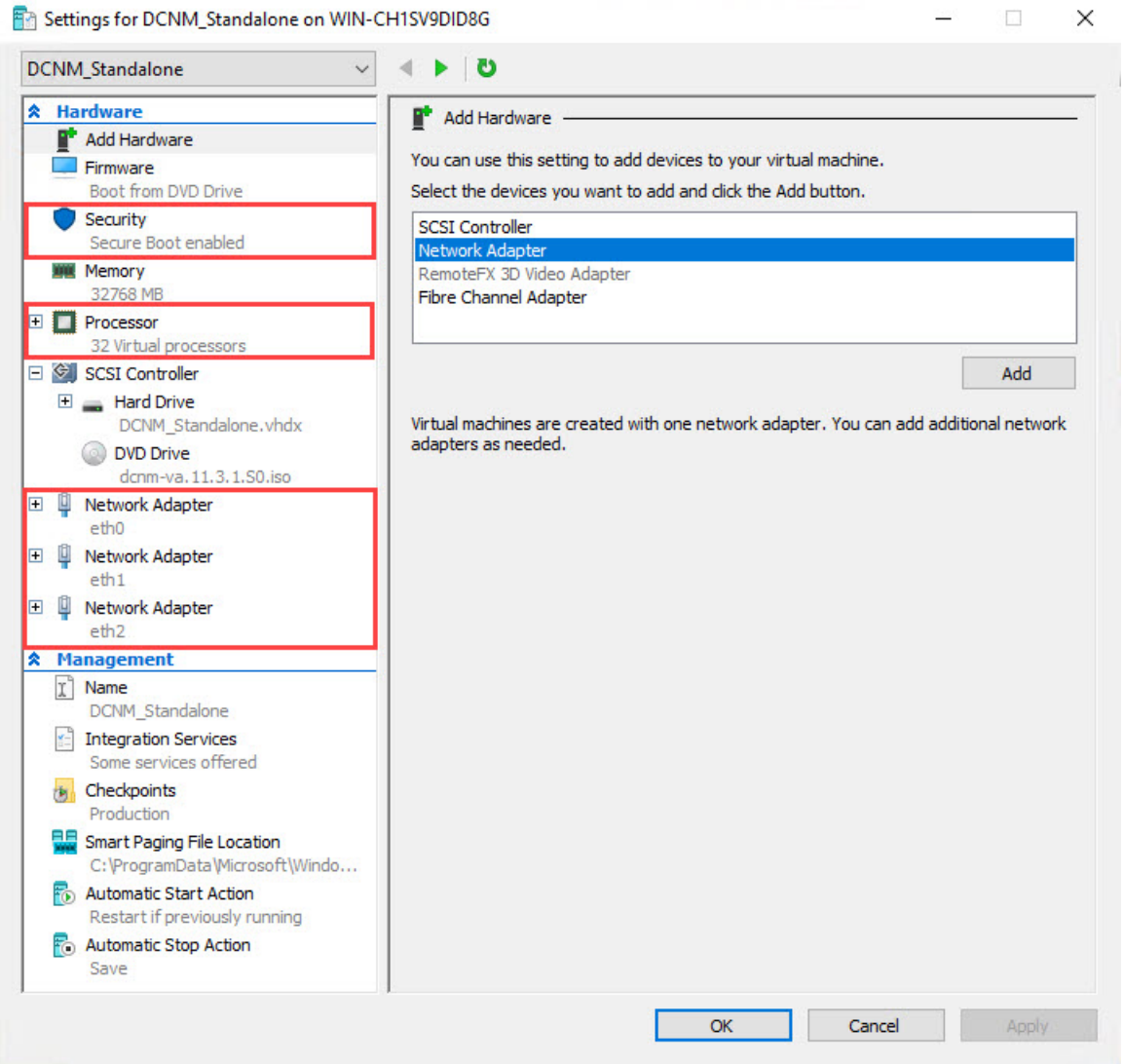
Step 11 On the left pane, in the Hardware block, click **Add Hardware**.

Step 12 In the main pane, select **Network Adapter** and click **Add**.

Step 13 In the Network Adapter screen, create network adapter for the virtual switch.

- From the **Virtual Switch** drop-down list, select the **eth1** virtual switch. Click **Apply**.
- From the **Virtual Switch** drop-down list, select the **eth2** virtual switch. Click **Apply**.

All the three Network Adapters are displayed in the left pane, under the **Hardware** section.



Step 14 In the left pane, select **Security**.

In the main pane, from the template drop-down list, select **Microsoft UEFI Certificate Authority**.

Note
This template is a mandatory if you've selected the Generation 2 hyper-V virtual machines.

Click **Apply**.

Step 15 In the Settings screen, click **Processor**.

In the main pane, in the **Number of virtual processors** field, enter **32**, to choose 32vCPUs. Click **Apply**.

Click **OK** to confirm the settings for the DCNM node.

What to do next

Install the Cisco DCNM ISO on the Windows Hyper-V. Refer to Installing DCNM ISO Virtual Appliance, on page 52 for more information.

Installing DCNM ISO Virtual Appliance

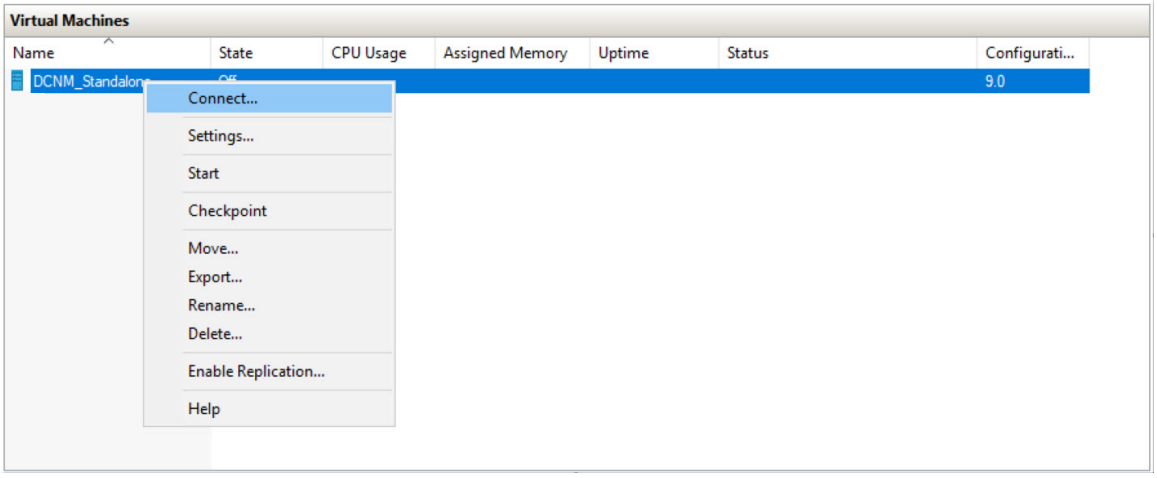
To configure the DCNM ISO virtual appliance for either Standalone, or Primary and Secondary nodes for Native HA setup, perform the following procedure:

Before you begin

Ensure that the Virtual Machine is configured correctly with proper security settings.

Procedure

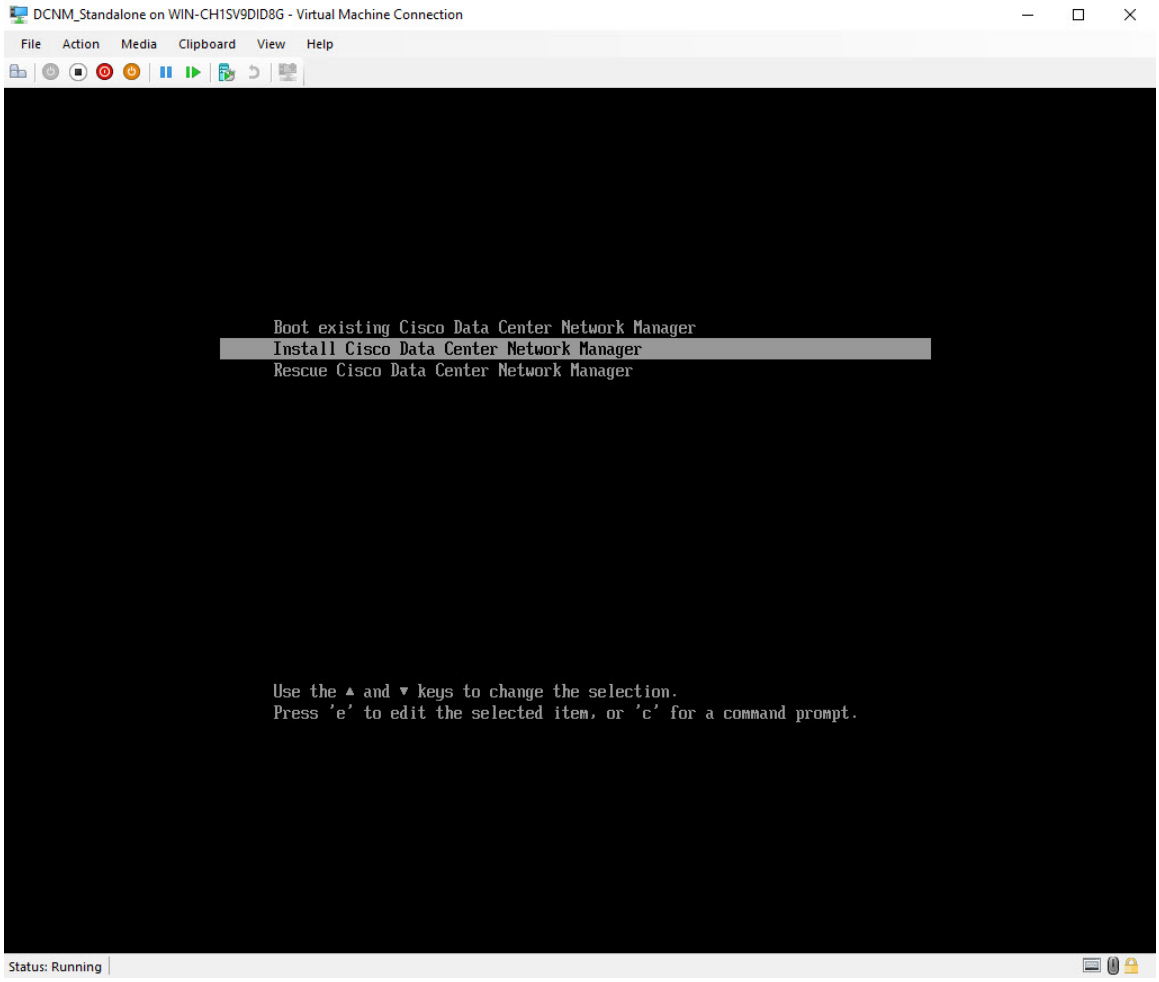
Step 1 From the Virtual Machines block, right click n the Active node and select **Connect**.



Step 2 In the Virtual Machine Connection screen, from the Menu bar, select **Media > DVD Drive** to verify the image selected.

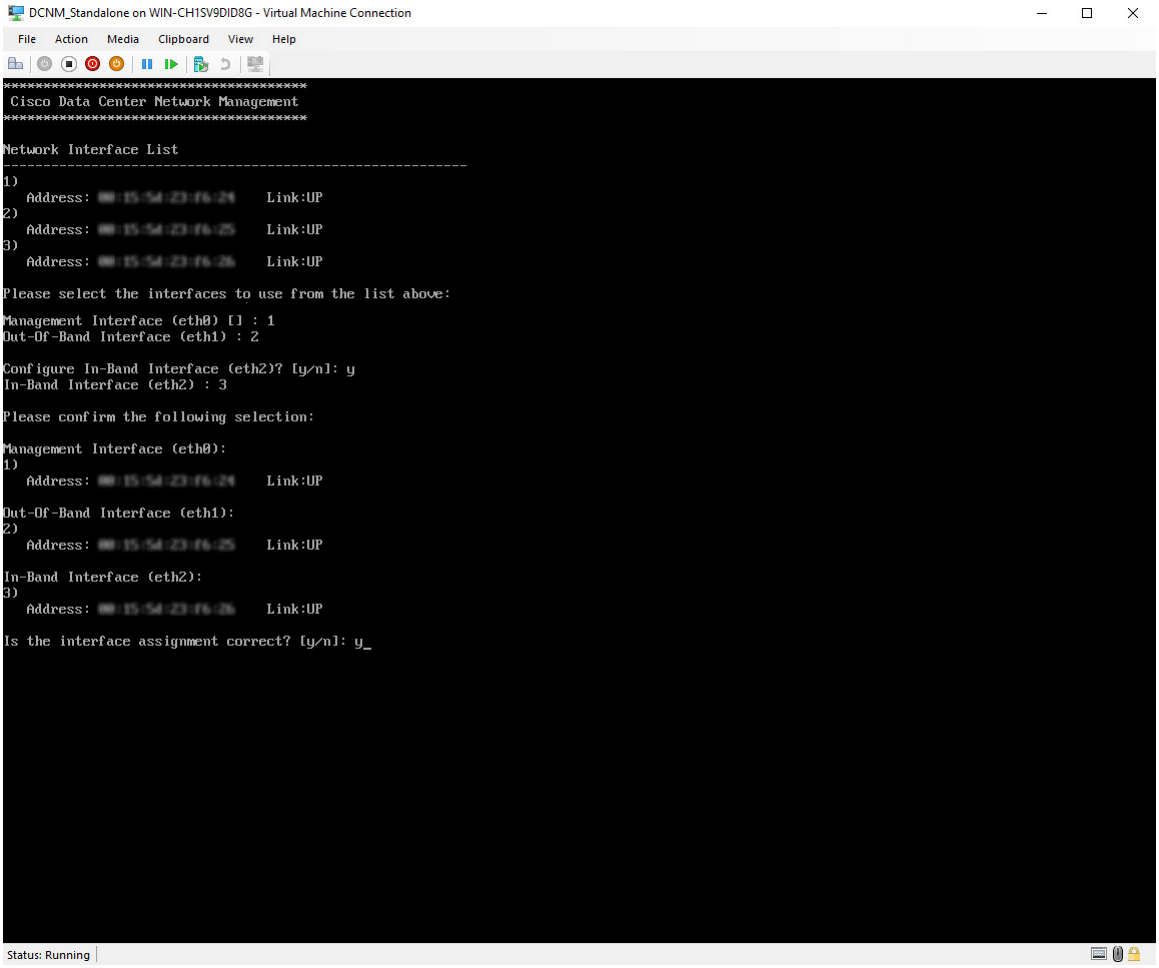
Click **Start**. The DCNM Server boots.

Step 3 Select **Install Cisco Data Center Network Manager** using the up or down arrow keys. Press **Enter** to install the Cisco DCNM Active node.



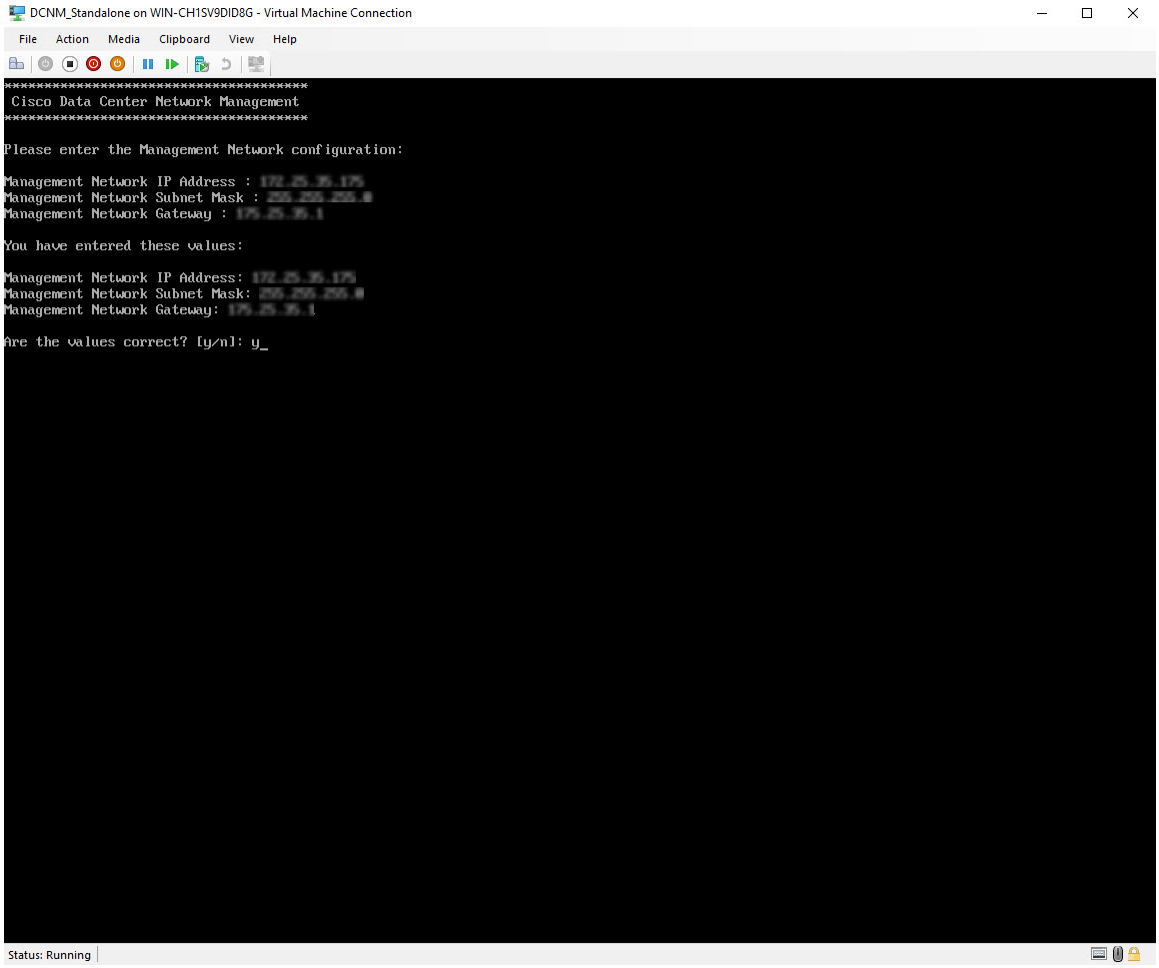
Step 4 On the Cisco Management Network Management screen, select the interface for the networks. The list of available interfaces is displayed on the screen.

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.



Review the selected interfaces. Press **y** to confirm and continue with the installation.

Step 5 Configure the Management Network for Cisco DCNM. Enter the **IP address**, **Subnet Mask**, and **Gateway**. Verify the values and 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. For more information, see Installing Cisco DCNM ISO in Standalone Mode, on page 55 or Installing the Cisco DCNM ISO in Native HA mode, on page 60.

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**.

Caution
If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

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

Click **Next**.

Step 3 On the **Install Mode** tab, choose your DCNM deployment type.

From the **Installation mode** drop-down list, choose **LAN Fabric** installation mode for the DCNM Appliance.

Check the **Enable Clustered Mode** check box, if you want to deploy Cisco DCNM in Cluster mode. The Compute nodes will be displayed on the Cisco DCNM **Web UI > Applications > Compute**. The applications will run on the **Compute** nodes. You can add the compute nodes to a Cluster, later.

If you require Compute Cluster, ensure that you have 3NICs while you configure the virtual appliance. Installing NICs later is not supported. If you do not have 3 NICs, **Enable Clustered Mode** is not available.

Note
If **Enable Clustered Mode** is selected, applications such as, Config Compliance, EPL, and NIA, and NIR won't work until you install the compute nodes.

Click **Next**.

Step 4 On the **Administration** tab, enter information about passwords.

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

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

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

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

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

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

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

- In the **Superuser Password (root)** field, enter the password for the Superuser to access root privileges.

  Enter the password again in the **Superuser Password** field.

  Note

If the Superuser Password is left blank, it shall consider the Administrator password as the Superuser password. However, we recommend that you configure a strong password for security reasons.

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

Click **Next**.

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

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

  You can also configure the DNS server using an IPv6 address.

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

  Note
  If you're using Network Insights applications, ensure that the DNS server is valid and reachable.
- In the **NTP Server Address List** field, enter the IP address of the NTP server.

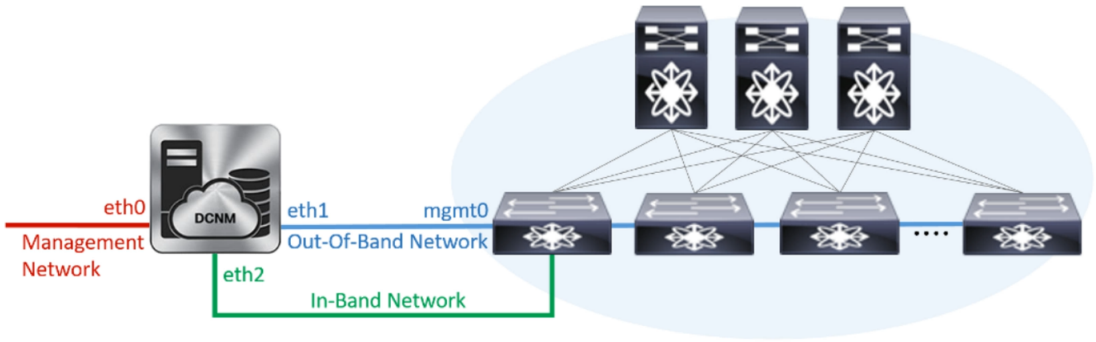
  The value must be an IP or IPv6 address or RFC 1123 compliant name.

  From Release 11.3(1), you can configure more than one NTP server.
- From the **Timezone** drop-down list, select the timezone in which you are deploying the DCNM.

Click **Next**.

Step 6 On the **Network Settings** tab, configure the network parameters used to reach the DCNM Web UI.

Figure 4: Cisco DCNM Management Network Interfaces



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

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

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

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

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

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

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

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

This field is mandatory if you have selected the Enable Cluster mode in Step Step 3, on page 56.

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

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

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

If you require Compute Cluster, ensure that you have 3NICs while you configure the virtual appliance. Installing NICs later is not supported. If you do not have 3 NICs, **Enable Clustered Mode** is not available, and therefore, you cannot configure the eth2 interface.

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation, on page 155.

Click **Next**.

Step 7 On the **Applications** tab, configure the Device Connector and Internal Applications Services Network, and Cluster mode settings.

Note
Device Connector is enabled by default.

The Device connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform.

a) (Optional) In the **Proxy Server** field, enter the IP address for the proxy server.

The proxy server must be of RFC1123-compliant name.

Note
By default, port 80 is used for proxy server. Use **<proxy-server-ip>:<port>** to use proxy server is a different port.

If the proxy server must require authentication, enter relevant username and password in the **Proxy Server Username** and **Proxy Server Password** fields.

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

All the applications use the IP Address from this subnet.

c) In the **Clustered mode configuration** area, configure the network settings to deploy the DCNM instance in Clustered mode. In Clustered mode, applications run on separate compute nodes.

The Cluster Mode configuration area appears only if you have selected the **Enable Clustered Mode** check box in Step Step 3, on page 56.

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

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

  Optionally, you can also enter an IPv6 address pool in the **Out-of-Band IPv6 Network Address Pool** field.

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

  Optionally, you can also enter an IPv6 address pool in the **In-Band IPv6 Network Address Pool** field.

The address must be a smaller prefix of available IP addresses from the eth1 subnet. For example: Use 10.1.1.240/28 if the eth1 subnet was configured as 10.1.1.0/24 during installation. This subnet must be a minimum of /28 (16 addresses) and maximum of /24 (256 addresses). It should also be longer than the east-west pool. This subnet is assigned to containers, to communicate with the switches.

Click **Next**.

Step 8 On the Summary tab, review the configuration details.

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

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

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

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

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

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

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

************************************
```

What to do next

Log on to the DCNM Web UI with appropriate credentials.

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

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

```
dcnm# appmgr update network-properties add route ipv4 eth2 <ipv4-network-ip-address/prefix>
```

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

```
dcnm# appmgr update network-properties session start
dcnm# appmgr update network-properties add route ipv4 eth2 10.0.0.0/24
dcnm# appmgr update network-properties add route ipv4 eth2 40.1.1.0/24
dcnm# appmgr update network-properties session apply
```

Installing the Cisco DCNM ISO in Native HA mode

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

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

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

Procedure

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

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

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

A welcome message appears.

a) On the **Welcome to Cisco DCNM** screen, click **Get Started**.

Caution
If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

b) On the **Cisco DCNM Installer** tab, select **Fresh Installation - HA Primary** radio button, to install **dcnm1** as Primary node.

Click **Next**.

c) On the **Install Mode** tab, choose your DCNM deployment type.

From the **Installation mode** drop-down list, choose **LAN Fabric** installation mode for the DCNM Appliance.

Check the **Enable Clustered Mode** check box, if you want to deploy Cisco DCNM in Cluster mode. The Compute nodes will be displayed on the Cisco DCNM **Web UI > Applications > Compute**. The applications will run on the **Compute** nodes. You can add the compute nodes to a Cluster, later.

If you require Compute Cluster, ensure that you have 3NICs while you configure the virtual appliance. Installing NICs later is not supported. If you do not have 3 NICs, **Enable Clustered Mode** is not available.

Note
If **Enable Clustered Mode** is selected, applications such as, Config Compliance, EPL, and NIA, and NIR won't work until you install the compute nodes.

Click **Next**.

d) On the **Administration** tab, enter information about passwords.

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

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

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

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

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

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

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

- In the **Superuser Password (root)** field, enter the password for the Superuser to access root privileges.

  Enter the password again in the **Superuser Password** field.

  Note
  If the Superuser Password is left blank, it shall consider the Administrator password as the Superuser password. However, we recommend that you configure a strong password for security reasons.

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

Click **Next**.

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

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

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

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

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

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

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

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

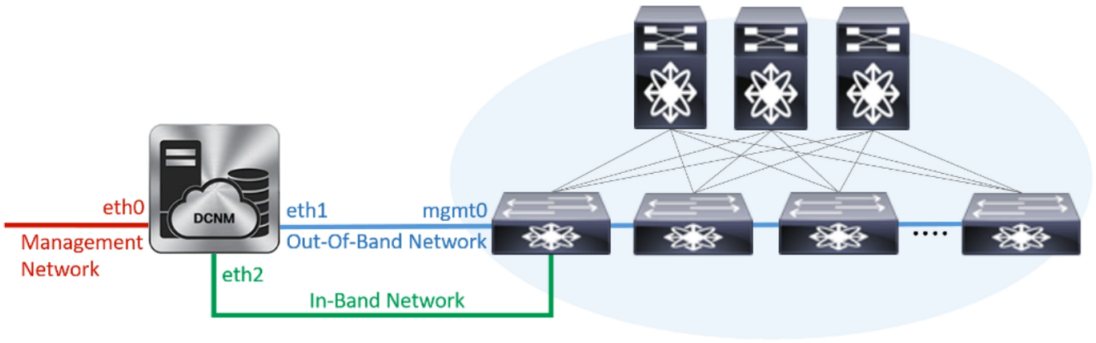
From Release 11.3(1), you can configure more than one NTP server.

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

Click **Next**.

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

Figure 5: Cisco DCNM Management Network Interfaces



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

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

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

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

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

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

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

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

   This field is mandatory if you have selected the **Enable Cluster** mode..

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

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

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

If you require Compute Cluster, ensure that you have 3NICs while you configure the virtual appliance. Installing NICs later is not supported. If you do not have 3 NICs, **Enable Clustered Mode** is not available, and therefore, you cannot configure the eth2 interface.

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation, on page 155.

Click **Next**.

g) On the **Applications** tab, configure the Device Connector and Internal Applications Services Network.

Note
Device Connector is enabled by default.

The Device connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform.

1. In the **Proxy Server** field, enter the IP address for the proxy server.

   The proxy server must be of RFC1123-compliant name.

   Note
   By default, port 80 is used for proxy server. Use **<proxy-server-ip>:<port>** to use proxy server is a different port.

   If the proxy server must require authentication, enter relevant username and password in the **Proxy Server Username** and **Proxy Server Password** fields.

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

   All the applications use the IP Address from this subnet. By default, the

   The Cluster Mode configuration area appears only if you have selected the **Enable Clustered Mode** check box in Step 2.c, on page 60.

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

3. In the **Clustered mode configuration** area, configure the network settings to deploy the DCNM instance in Clustered mode. In Clustered mode, applications run on separate compute nodes.

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

     Optionally, you can also enter an IPv6 address pool in the **Out-of-Band IPv6 Network Address Pool** field.

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

     Optionally, you can also enter an IPv6 address pool in the **In-Band IPv6 Network Address Pool** field.

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

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

h) On the **HA Settings** tab, a confirmation message appears.

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

Click **Next**.

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

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

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

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

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

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

A welcome message appears.

a) On the **Welcome to Cisco DCNM** screen, click **Get Started**.

Caution
If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

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

Click **Continue**.

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

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

Check the **Enable Clustered Mode** check box, if you have configured the Cisco DCNM Primary in Clustered mode.

Click **Next**.

d) On the **Administration** tab, enter information about passwords.

Note
All the passwords must be same as the passwords that you provided while configuring the Primary node.

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

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

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

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

  Note
  If you're using Network Insights applications, ensure that the DNS server is valid and reachable.
- In the **NTP Server Address List** field, enter the IP address of the NTP server.

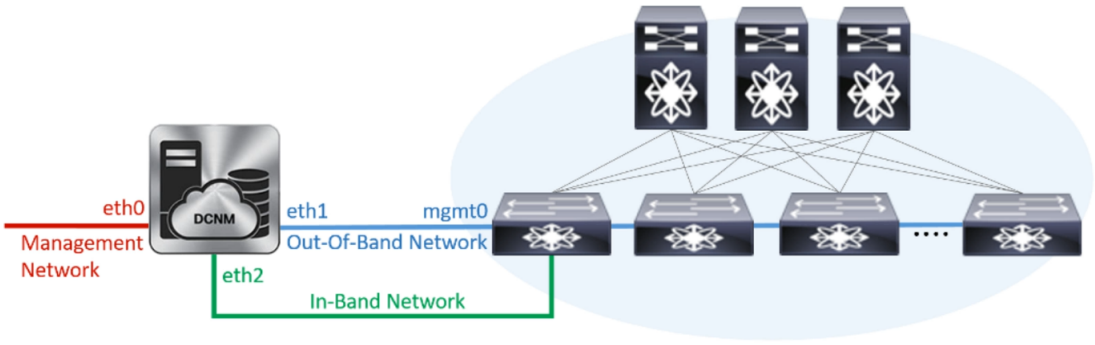
  The value must be an IP or IPv6 address or RFC 1123 compliant name.

  From Release 11.3(1), you can configure more than one NTP server.
- From the **Timezone** drop-down list, select the timezone in which you are deploying the DCNM.

Click **Next**.

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

Figure 6: Cisco DCNM Management Network Interfaces



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

   Note
   Ensure that the IP address belongs to the same Management Network configured on the Primary node.

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

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

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

   Note
   Ensure that the IP addresses belong to the same Out-of-Band network configured on the Primary node.

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

   Note

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

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

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

   Note
   Ensure that the IP addresses belong to the same In-Band network configured on the Primary node.

   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.

Click **Next**.

g) On the **Applications** tab, configure the Internal Applications Services Network, and Cluster mode settings.

1. In the **Internal Application Services Network** area, in the **IPv4 Subnet field**, enter the IP subnet to access the applications that run internally to DCNM.
2. In the **Clustered mode configuration** area, configure the network settings to deploy the DCNM instance in Clustered mode. In Clustered mode, applications run on separate compute nodes.
   - In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the Out-of-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **Out-of-Band IPv6 Network Address Pool** field.
   - In the **In-Band IPv4 Network Address Pool**, enter the address pool from the In-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **In-Band IPv6 Network Address Pool** field.

Ensure that the IP addresses belong to the same pool as configured on the Primary node.

h) On the **HA Settings** tab, configure the system settings for the Secondary node.

- In the **Management IPv4 Address of Primary DCNM node** field, enter the appropriate IP Address to access the DCNM UI.
- In the **VIP Fully qualified Host Name** field, enter hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Host names with only digits is not supported.
- In the **Management Network VIP address** field, enter the IP address used as VIP in the management network.

  Optionally, you can also enter an IPv6 VIP address in the **Management Network VIPv6 address** field.

  Note
  If you have configured the Management network using IPv6 address, ensure that you configure the Management Network VIPv6 Address.

- In the **Out-of-Band Network VIP Address** field, enter the IP address used as VIP in the Out-of-Band network.

  Optionally, you can also enter an IPv6 VIP address in the **Out-of-Band Network VIPv6 Address** field.

- In the **In-Band Network VIP Address** field, enter the IP address used as VIP in the Out-of-Band network.

  Optionally, you can also enter an IPv6 VIP address in the **In-Band Network VIPv6 Address** field.

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

- In the **HA Ping Feature IPv4 Address** field, enter the HA ping IP address and enable this feature, if necessary.

  Note
  The configured IPv4 address must respond to the ICMP echo pings.

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

  You must configure the HA ping IPv4 Address to avoid the Split Brain scenario. This IP address must belong to Enhanced Fabric management network.

Click **Next**.

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

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

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

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

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

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

What to do next

Log on to the DCNM Web UI with appropriate credentials.

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

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

```
dcnm# appmgr update network-properties add route ipv4 eth2 <ipv4-network-ip-address/prefix>
```

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

```
dcnm# appmgr update network-properties session start
dcnm# appmgr update network-properties add route ipv4 eth2 10.0.0.0/24
dcnm# appmgr update network-properties add route ipv4 eth2 40.1.1.0/24
dcnm# appmgr update network-properties session apply
```

Convert Standalone Setup to Native-HA Setup

To convert an existing Cisco DCNM Standalone setup to a Native HA setup, perform the following steps:

Before you begin

Ensure that the Standalone setup is active and operational, by using the **appmgr show version** command.

```
dcnm# appmgr show version

Cisco Data Center Network Manager
Version: 11.5(1)
Install mode: LAN Fabric
Standalone node. HA not enabled.
dcnm#
```

Procedure

Step 1 On the Standalone setup, launch SSH and enable **root** user access by using the **appmgr root-access permit** command:

```
dcnm# appmgr root-access permit
```

Step 2 Deploy a new DCNM as secondary node. Choose **Fresh installation - HA Secondary**

For example, let us indicate the existing setup as **dcnm1** and the new DCNM as secondary node as **dcnm2**.

Caution
If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

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

A welcome message appears.

a) On the **Welcome to Cisco DCNM** screen, click **Get Started**.

Caution

If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

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

Click **Continue**.

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

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

Check the **Enable Clustered Mode** check box, if you have configured the Cisco DCNM Primary in Clustered mode.

Click **Next**.

d) On the **Administration** tab, enter information about passwords.

Note
All the passwords must be same as the passwords that you provided while configuring the Primary node.

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

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

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

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

  Note
  If you’re using Network Insights applications, ensure that the DNS server is valid and reachable.
- In the **NTP Server Address List** field, enter the IP address of the NTP server.

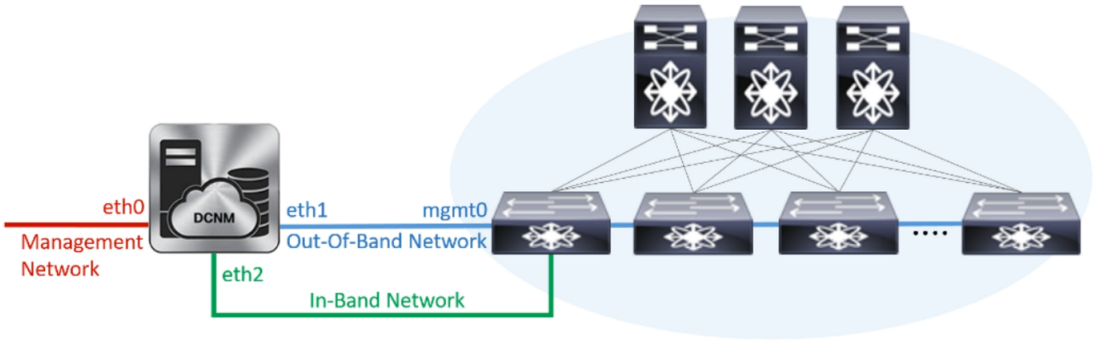
  The value must be an IP or IPv6 address or RFC 1123 compliant name.

  From Release 11.3(1), you can configure more than one NTP server.
- From the **Timezone** drop-down list, select the timezone in which you are deploying the DCNM.

Click **Next**.

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

Figure 7: Cisco DCNM Management Network Interfaces



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

   Note
   Ensure that the IP address belongs to the same Management Network configured on the Primary node.

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

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

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

   Note
   Ensure that the IP addresses belong to the same Out-of-Band network configured on the Primary node.

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

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

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

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

   Note
   Ensure that the IP addresses belong to the same In-Band network configured on the Primary node.

   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.

Click **Next**.

g) On the **Applications** tab, configure the Internal Applications Services Network, and Cluster mode settings.

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

2. In the **Clustered mode configuration** area, configure the network settings to deploy the DCNM instance in Clustered mode. In Clustered mode, applications run on separate compute nodes.
   - In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the Out-of-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **Out-of-Band IPv6 Network Address Pool** field.
   - In the **In-Band IPv4 Network Address Pool**, enter the address pool from the In-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **In-Band IPv6 Network Address Pool** field.

   Ensure that the IP addresses belong to the same pool as configured on the Primary node.

h) On the **HA Settings** tab, configure the system settings for the Secondary node.
   - In the **Management IPv4 Address of Primary DCNM node** field, enter the appropriate IP Address to access the DCNM UI.
   - In the **VIP Fully qualified Host Name** field, enter hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Host names with only digits is not supported.
   - In the **Management Network VIP address** field, enter the IP address used as VIP in the management network.

     Optionally, you can also enter an IPv6 VIP address in the **Management Network VIPv6 address** field.

     Note
     If you have configured the Management network using IPv6 address, ensure that you configure the Management Network VIPv6 Address.
   - In the **Out-of-Band Network VIP Address** field, enter the IP address used as VIP in the Out-of-Band network.

     Optionally, you can also enter an IPv6 VIP address in the **Out-of-Band Network VIPv6 Address** field.
   - In the **In-Band Network VIP Address** field, enter the IP address used as VIP in the Out-of-Band network.

     Optionally, you can also enter an IPv6 VIP address in the **In-Band Network VIPv6 Address** field.

     Note
     This field is mandatory if you have provided an IP address for In-Band network in the **Network Settings** tab.
   - In the **HA Ping Feature IPv4 Address** field, enter the HA ping IP address and enable this feature, if necessary.

     Note
     The configured IPv4 address must respond to the ICMP echo pings.

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

You must configure the HA ping IPv4 Address to avoid the Split Brain scenario. This IP address must belong to Enhanced Fabric management network.

Click **Next**.

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

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

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

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

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

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

What to do next

Verify the HA role by using the appmgr show ha-role command.

On the Active node (old standalone node):

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

On the Standby node (newly deployed node):

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

Installing Cisco DCNM Compute Node

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

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

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

When NIR/NIA applications is enabled at higher scale, that is, with 250 switches and 10000 Hardware telemetry flows, DCNM Computes nodes must be connected on all eth0, eth1, and eth2 interfaces using a 10Gig link.

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

Before you begin

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

By default, the **ComputeHuge** configuration has 32vCPUs and 128GB RAM with 2TB disk. This configuration is recommended if you use Cisco Network Insights applications.

Procedure

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

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

Click **Continue**.

Step 3 On the **Install Mode** tab, choose **Compute** to deploy this DCNM instance as a compute node.

Note
Compute option appears in the drop-down list only if you have chosen **Compute** or **ComputeHuge** while configuring the OVF template or ISO hypervisors.

Click **Next**.

Step 4 On the **Administration** tab, enter information about passwords.

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

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

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

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

Click **Next**.

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

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

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

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

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

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

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

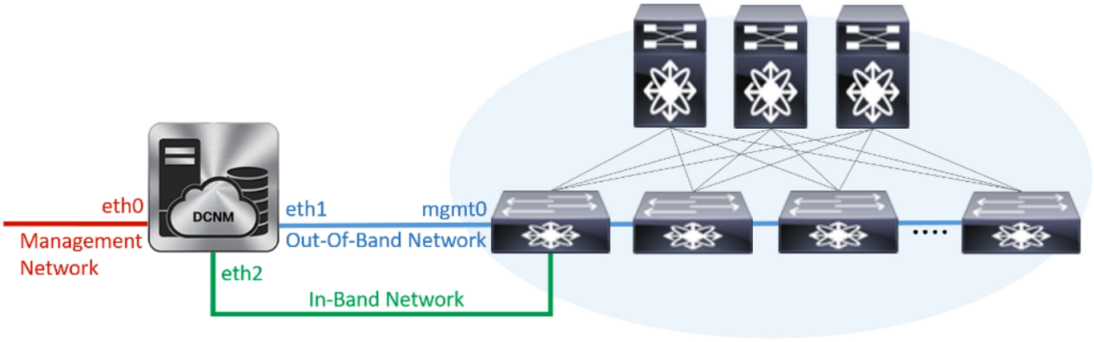
  From Release 11.3(1), you can configure more than one NTP server.

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

Click **Next**.

Step 6 On the **Network Settings** tab, configure the network parameters used to reach the DCNM Web UI.

Figure 8: Cisco DCNM Management Network Interfaces



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

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

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

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

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

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

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

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

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

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

Note

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

However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation, on page 155.

Click **Next**.

Step 7 In the **Internal Application Services Network** area, in the **IPv4 Subnet field**, enter the IP subnet to access the applications that run internally to DCNM.

All the applications use the IP Address from this subnet.

Click **Next**.

Step 8 On the **Summary** tab, review the configuration details.

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

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

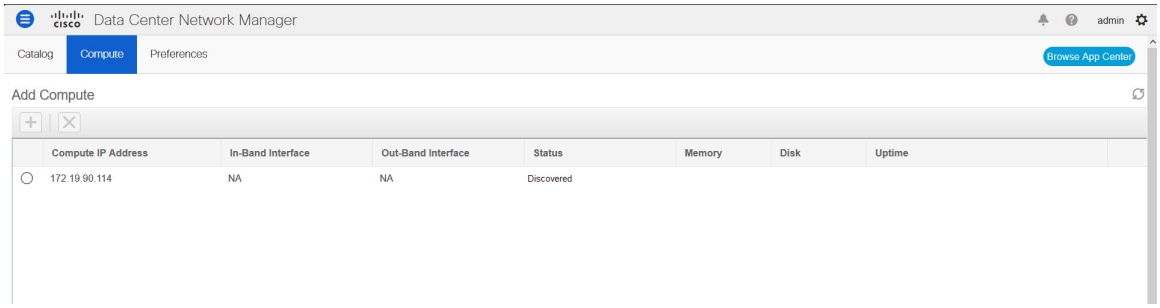
A success message appears with the URL to access DCNM Compute Node.

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

What to do next

Log on to the DCNM Web UI with appropriate credentials.

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

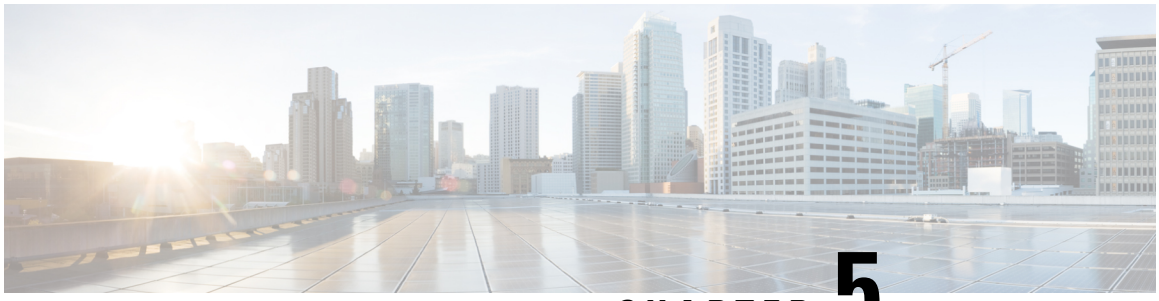


To add the compute nodes to a cluster, see Adding Computes to a Cluster Node in your deployment-specific *Cisco DCNM Configuration Guide* for more information.



Note If you did not enable clustered mode while installing DCNM, use the **appmgr afw config-cluster** command to enable the compute cluster. For instructions, refer to Enabling the Compute Cluster in the Cisco DCNM LAN Fabric Configuration Guide.

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



CHAPTER 5

Upgrading Cisco DCNM

This chapter provides information about upgrading Cisco DCNM, and contains the following section:

- Upgrading to Cisco DCNM Release 11.5(1), on page 77
- Upgrading ISO or OVA through Inline Upgrade, on page 77
- Dropping Performance Manager Data, on page 87

Upgrading to Cisco DCNM Release 11.5(1)

Before Cisco DCNM Release 11.0(1), DCNM OVA, and ISO supported SAN functionality. From Cisco DCNM Release 11.3(1), you can install Cisco DCNM for SAN Deployment on both OVA and ISO virtual appliances.

The following table summarizes the type of upgrade that you must follow to upgrade to Release 11.5(1).

Table 6: Type of Upgrade for LAN Fabric deployments

Current Release Number	Upgrade type to upgrade to Release 11.5(1)
11.4(1)	Inline Upgrade
11.3(1)	Inline Upgrade
11.2(1)	Inline Upgrade
11.1(1)	11.1(1) → 11.2(1) → 11.5(1) 11.1(1) → 11.3(1) → 11.5(1) 11.1(1) → 11.4(1) → 11.5(1) → represents an Inline Upgrade

Upgrading ISO or OVA through Inline Upgrade

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

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

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

To restore certificates after upgrade, see Restoring the certificates after an upgrade, on page 132.

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

Note For Classic LAN Deployment upgrade, the deployment is automatically converted to LAN Fabric deployment mode when you upgrade to DCNM Release 11.5(1).

Inline Upgrade for DCNM Virtual Appliance in Standalone Mode

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

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

Before you begin

If the Cisco DCNM setup is in clustered mode, ensure that you stop the Network Insights - Resources (NIR) 2.x application. On the Cisco DCNM Web UI, choose **Applications > Catalog**. On the NIR app, click **Stop** icon to stop the application. Click **Delete** to remove the application from the Catalog.

Procedure

Step 1 Log on to the Cisco DCNM appliance console.

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

- For OVA Installation: On the OVF template deployed for the host, right click and select **Settings > Launch Web Console**.
- For ISO Installation: Select the KVM console or UCS (Bare Metal) console.

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

OR

Run the following command to create a screen session.

```
dcnm# screen
```

This creates a session which allows you to execute the commands. The commands continue to run even when the window is not visible or if you get disconnected.

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

```
dcnm# appmgr backup
```

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

Step 3 Log on to the `/root/` directory, by using the **su** command.

```
dcnm# su
Enter password: <<enter-password>>
[root@dcnm]#
```

Note
Ensure that you have access to the `/root/` folder before you mount the ISO to the directory.

Step 4 Unzip the `dcnm-va.11.5.1.iso.zip` file and upload the `DCNM 11.5(1) ISO` file to the `/root/` folder in the DCNM setup that you want to upgrade.

Step 5 Create folder that is named **iso** using the **mkdir /mnt/iso** command.

```
[root@dcnm]# mkdir /mnt/iso
```

Step 6 Mount the DCNM 11.5(1) ISO file on the standalone setup in the `/mnt/iso` folder.

mount -o loop <*DCNM 11.5(1) image*> **/mnt/iso**

```
[root@dcnm]# mount -o loop dcnm-va.11.5.1.iso /mnt/iso
```

Step 7 Navigate to **/mnt/iso/packaged-files/scripts/** and run the **./inline-upgrade.sh** script.

```
[root@dcnm]# cd /mnt/iso/packaged-files/scripts/
dcnm# ./inline-upgrade.sh
Do you want to continue and perform the inline upgrade to 11.5(1)? [y/n]: y
```

Note
The prompt to enter a new sysadmin password appears while you're upgrading from Cisco DCNM Release 11.2(1) only.

Step 8 Provide the new sysadmin user password at the prompt:

Note
The prompt to enter a new sysadmin password appears while you're upgrading from Cisco DCNM Release 11.2(1) only.

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

After the upgrade is complete, the appliance reboots. After reboot, the SSH \root access is disabled by default. Use **sysadmin** user.

As the Elasticsearch versions in earlier releases is not compatible with the Elasticsearch supported with 11.5(1), you must reindex the Elasticsearch data after upgrading to Release 11.5(1).

The following message is generated:

```
********************************************************************
WARNING: Elasticsearch indices for historical Performance Monitoring (PM)
data need to be reindexed manually.
```

```
Check DCNM installation and upgrade guide for more details.
********************************************************************
```

A confirmation message appears. Enter **y** to continue to upgrade.

The system reboots after upgrade.

Step 9 Ensure that the DCNM application is functional, by using the **appmgr status all** command.

```
[root@dcnm]# appmgr status all
```

Step 10 To verify that you have successfully installed the Cisco DCNM Release 11.5(1), use the **appmgr show version** command.

```
[root@dcnm]# appmgr show version

Cisco Data Center Network Manager
Version: 11.5(1)
Install mode: LAN Fabric
Standalone node. HA not enabled.
```

Step 11 Terminate the **screen** session, by using the **exit** command.

```
[root@dcnm]# exit
```

Step 12 Unmount the **dcnm-va-patch.11.5.1.iso** file from the DCNM setup.

Note
You must terminate the screen session before unmounting the **.iso** file.

```
[root@dcnm]# umount /mnt/iso
```

What to do next

Log on to the DCNM Web UI with appropriate credentials.

Note In Release 11.3(1), the sysadmin and the root user's password are not identical. When you upgrade to 11.5(1), the sysadmin and root user passwords are preserved.

However, when you perform backup and restore on Cisco DCNM after upgrade, the sysadmin user inherits the password from the root user, and therefore both the users will have the same password. You can change the password for both the users after restore is complete.

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

The old PM data is retained in Elasticsearch. Elasticsearch shows as reindex required on Cisco DCNM **Web UI > Dashboard > Health** and **Administration > DCNM Server > Server Status**.

If you choose to conserve the Performance Manager data when you upgrade to Release 11.5(1), we recommend that you contact Cisco TAC for further assistance.

If you choose to conserve the Performance Manager data, we recommend that you contact Cisco TAC for further assistance.

To gracefully onboard Cisco DCNM Release 11.2(1), Release 11.3(1), or Release 11.4(1) managed VXLAN BGP EVPN fabric(s) comprising Cisco Nexus 9000 switches post upgrade to Cisco DCNM Release 11.5(1), see Post DCNM 11.5(1) Upgrade for VXLAN BGP EVPN, External, and MSD Fabrics.

Inline Upgrade for DCNM Virtual Appliance in Native HA Mode

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

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

Before you begin

- Ensure that both the Cisco DCNM Active and Standby peers are up and running.
- Before upgrading Cisco DCNM in Clustered mode, stop the Network Insights - Resources (NIR) 2.x application. On the Cisco DCNM Web UI, choose **Applications** > **Catalog**. On the NIR app, click Stop icon to stop the application. Click Delete to remove the application from the Catalog.



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

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

  Example:

  On the Active node:

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

  On the Standby node:

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

Procedure

Step 1 Unzip the `dcnm-va.11.5.1.iso.zip` file and upload the `DCNM 11.5(1) ISO` file to the `/root/` folder in both Active and Standby node of the DCNM setup that you want to upgrade.

Note
For example, let us indicate Active and Standby appliances as **dcnm1** and **dcnm2** respectively.

Step 2 Log on to the Cisco DCNM appliance console.

Caution

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

- For OVA Installation: On the OVF template that is deployed for the host, right click and select **Settings > Launch Web Console**.
- For ISO Installation: Select the KVM console or UCS (Bare Metal) console.

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

OR

Run the following command to create a screen session.

```
dcnm1# screen
dcnm2# screen
```

This creates a session which allows you to execute the commands. The commands continue to run even when the window is not visible or if you get disconnected.

Step 3 Take a backup of the application data using the **appmgr backup** command on both Active and Standby appliances.

```
dcnm1# appmgr backup
dcnm2# appmgr backup
```

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

Step 4 Log on to the **/root/** directory by using the **su** command.

```
dcnm1# su
Enter password: <<enter-password>>
[root@dcnm1]#
```

```
dcnm2# su
Enter password: <<enter-password>>
[root@dcnm2]#
```

Note
Ensure that you have access to the /root/ folder before you mount the ISO to the directory.

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

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

```
[root@dcnm1]# mkdir /mnt/iso
```

b) Mount the DCNM 11.5(1) ISO file on the Active node in the `/mnt/iso` folder.

```
[root@dcnm1]# mount -o loop dcnm-va.11.5.1.iso /mnt/iso
```

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

```
[root@dcnm1]# cd /mnt/iso/packaged-files/scripts/
dcnm1# ./inline-upgrade.sh
```

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

```
[root@dcnm1]# Do you want to continue and perform the inline upgrade to 11.5(1)? [y/n]:
 y
```

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

Note
The prompt to enter a new sysadmin password appears while you're upgrading from Cisco DCNM Release 11.1(1) or Release 11.2(1) only.

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

After the upgrade is complete, the appliance reboots. After reboot, the SSH \root access is disabled by default. Use **sysadmin** user.

As the Elasticsearch versions in earlier releases is not compatible with the Elasticsearch supported with 11.5(1), you must reindex the Elasticsearch data after upgrading to Release 11.5(1).

The following message is generated:

```
********************************************************************
WARNING: Elasticsearch indices for historical Performance Monitoring (PM)
data need to be reindexed manually.
Check DCNM installation and upgrade guide for more details.
********************************************************************
```

A confirmation message appears. Enter **y** to continue to upgrade.

The system reboots after upgrade.

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

```
[root@dcnm1]# appmgr status all
```

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

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

```
[root@dcnm1]# appmgr show ha-role

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

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

Step 6 On the Standby node, perform the inline upgrade.

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

```
[root@dcnm2]# mkdir /mnt/iso
```

b) Mount the DCNM 11.5(1) ISO file on the Standby node in the `/mnt/iso` folder.

```
[root@dcnm2]# mount -o loop dcnm-va.11.5.1.iso /mnt/iso
```

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

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

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

```
[root@dcnm2]# Do you want to continue and perform the inline upgrade to 11.5(1)? [y/n]:
 y
```

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

Note
The prompt to enter a new sysadmin password appears while you're upgrading from Cisco DCNM Release 11.1(1) or Release 11.2(1) only.

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

After the upgrade is complete, the appliance reboots. After reboot, the SSH \root access is disabled by default. Use **sysadmin** user.

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

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

Step 7 Terminate the **screen** session, by using the **exit** command.

```
[root@dcnm1]# exit
[root@dcnm2]# exit
```

Step 8 Unmount the **dcnm-va-patch.11.5.1.iso** file in both Active and Standby node of the DCNM setup.

Note
You must terminate the screen session before unmounting the **.iso** file.

```
[root@dcnm1]# umount /mnt/iso
[root@dcnm2]# umount /mnt/iso
```

What to do next

Log on to the DCNM Web UI with appropriate credentials.

Note In Release 11.3(1), the sysadmin and the root user's password are not identical. When you upgrade to 11.5(1), the sysadmin and root user passwords are preserved.

However, when you perform backup and restore on Cisco DCNM after upgrade, the sysadmin user inherits the password from the root user, and therefore both the users will have the same password. You can change the password for both the users after restore is complete.

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

The old PM data is retained in Elasticsearch. Elasticsearch shows as reindex required on Cisco DCNM **Web UI > Dashboard > Health** and **Administration > DCNM Server > Server Status**.

If you choose to conserve the Performance Manager data, we recommend that you contact Cisco TAC for further assistance.

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

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

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

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

To gracefully onboard Cisco DCNM Release 11.2(1), Release 11.3(1), or Release 11.4(1) managed VXLAN BGP EVPN fabric(s) comprising Cisco Nexus 9000 switches post upgrade to Cisco DCNM Release 11.5(1), see Post DCNM 11.5(1) Upgrade for VXLAN BGP EVPN, External, and MSD Fabrics.

Inline Upgrade for DCNM Compute Nodes

You can upgrade the DCNM compute nodes from Release 11.2(1) or Release 11.3(1) or Release 11.4(1) to Release 11.5(1) using the inline upgrade. Inline upgrade allows you to upgrade the compute node by imposing the new DCNM version to the existing compute node.

Note You can upgrade the Compute nodes on Cisco Application Services Engine for Cisco DCNM Release 11.3(1) to Release 11.5(1) using the inline upgrade procedure. For more information, refer to https://www.cisco.com/c/en/us/support/data-center-analytics/nexus-dashboard/products-installation-guides-list.html.

Perform the following task to upgrade the DCNM compute node in both Standalone and Native HA modes.

Before you begin

Cisco DCNM Servers in either Standalone node or Native HA mode must be upgraded to Release 11.5(1), before upgrading the DCNM compute nodes.

Procedure

Step 1 Log on to the Cisco DCNM Compute console.

Caution
Don’t perform an Inline Upgrade from an SSH Session. The session may timeout and result in an incomplete upgrade.

Caution

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

OR

Run the following command to create a screen session on the compute node.

```
dcnm-compute# screen
```

This creates a session which allows you to execute the commands. The commands continue to run even when the window isn't visible or if you get disconnected.

Step 2 Unzip the `dcnm-va.11.5.1.iso.zip` file and upload the `DCNM 11.5(1) ISO` file to the `/root/` folder in all the compute nodes.

Step 3 Create folder that is named **iso** using the **mkdir /mnt/iso** command, on all the computes.

```
dcnm-compute# mkdir /mnt/iso
```

Step 4 Mount the DCNM 11.5(1) ISO file on the compute node in the `/mnt/iso` folder.

mount -o loop <*DCNM 11.5(1) image*> **/mnt/iso**

```
dcnm-compute# mount -o loop dcnm-va.11.5.1.iso /mnt/iso
```

Mount the ISO on all the compute nodes.

Step 5 Navigate to **/mnt/iso/packaged-files/scripts** and run the **./inline-upgrade.sh** script.

```
dcnm-compute# cd /mnt/iso/packaged-files/scripts
dcnm-compute# ./inline-upgrade.sh --task-disable updatePoapUser
dcnm-compute# ./inline-upgrade.sh
Do you want to continue and perform the inline upgrade to 11.5(1)? [y/n]: y
```

Note
If some services are still running, a prompt to stop the services appears. When prompted, press **y** to continue.

Note
The prompt to enter a new sysadmin password appears while you're upgrading from Cisco DCNM Release 11.1(1) or Release 11.2(1) only.

Step 6 Provide the new sysadmin user password at the prompt:

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

After the upgrade is complete, the compute node reboots. After reboot, the SSH \root access is disabled by default. Use **sysadmin** user.

Step 7 Verify that you have successfully upgraded to Cisco DCNM Release 11.5(1), using the **appmgr show version** command.

```
dcnm-compute# appmgr show version

Cisco Data Center Network Manager
Version: 11.5(1)
Install mode: Compute
```

Step 8 Terminate the **screen** session, by using the **exit** command on all compute nodes.

```
dcnm-compute# exit
```

Step 9 Unmount the **dcnm-va-patch.11.5.1.iso** file from all compute nodes of the DCNM setup.

Note
You must terminate the screen session on all compute nodes before unmounting the **.iso** file.

```
dcnm-compute# umount /mnt/iso
```

What to do next

You must upgrade all the three compute nodes in the cluster.

After the Upgrade process is complete, each compute node will reboot and join the cluster automatically. On the Cisco DCNM Web UI, choose **Applications > Compute** to verify if the compute node appears as **Joined**.

To gracefully onboard Cisco DCNM Release 11.2(1), Release 11.3(1), or Release 11.4(1) managed VXLAN BGP EVPN fabric(s) comprising Cisco Nexus 9000 switches post upgrade to Cisco DCNM Release 11.5(1), see Post DCNM 11.5(1) Upgrade for VXLAN BGP EVPN, External, and MSD Fabrics.

Dropping Performance Manager Data



Note If you choose to conserve the Performance Manager data when you upgrade to Release 11.5(1), we recommend that you contact Cisco TAC for further assistance.

To drop the Performance Manager (PM) data, perform the following steps:

Before you begin

- Ensure that the DCNM appliance is operational. (for standalone upgrade)
- If you have a Federation setup, ensure that all the nodes in the DCNM Federation setup are operational. (for Federation setup)

Procedure

Step 1 Launch the SSH session and run the following command to view the PMDB indices.

Identify the PMDB indices in the performance manager database.

For example:

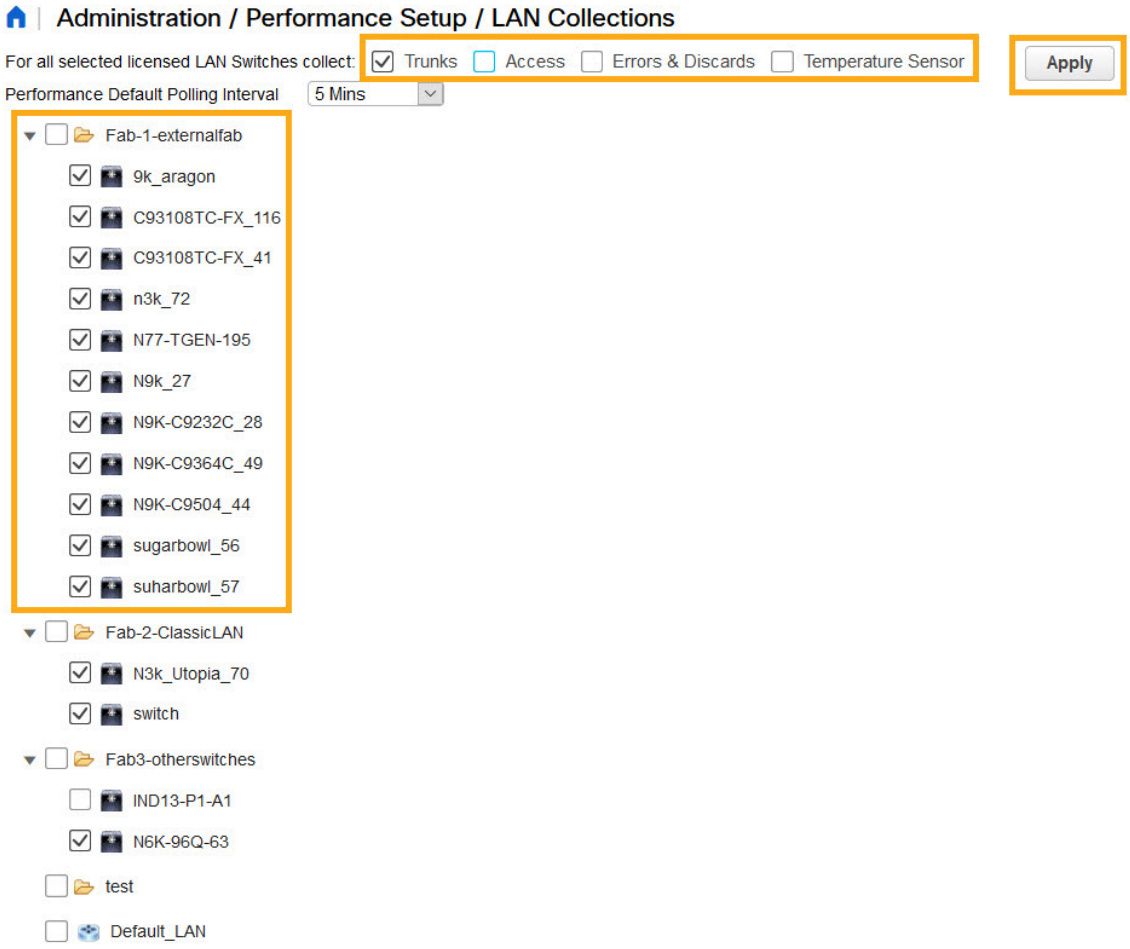
```
dcnm-root-11-4# curl http://127.0.0.1:33500/_cat/indices?pretty | grep pmdb

  % Total    % Received % Xferd  Average Speed    Time    Time     Time  Current
                                 Dload   Upload   Total   Spent    Left  Speed
100  2448  100  2448    0     0   4523      0 --:--:-- --:--:-- --:--:--  4524
green open pmdb_cpumemdata                          rb-CJf-NR0my8M3mO-7QkA 5 1  7286   0
1.4mb 760.2kb
green open pmdb_ethintfratedata                     P18gMKdPTkCODv0TomYAdw 5 1  9283   0
2.4mb   1.2mb
```

You will see indices prefixed with "pmdb_"

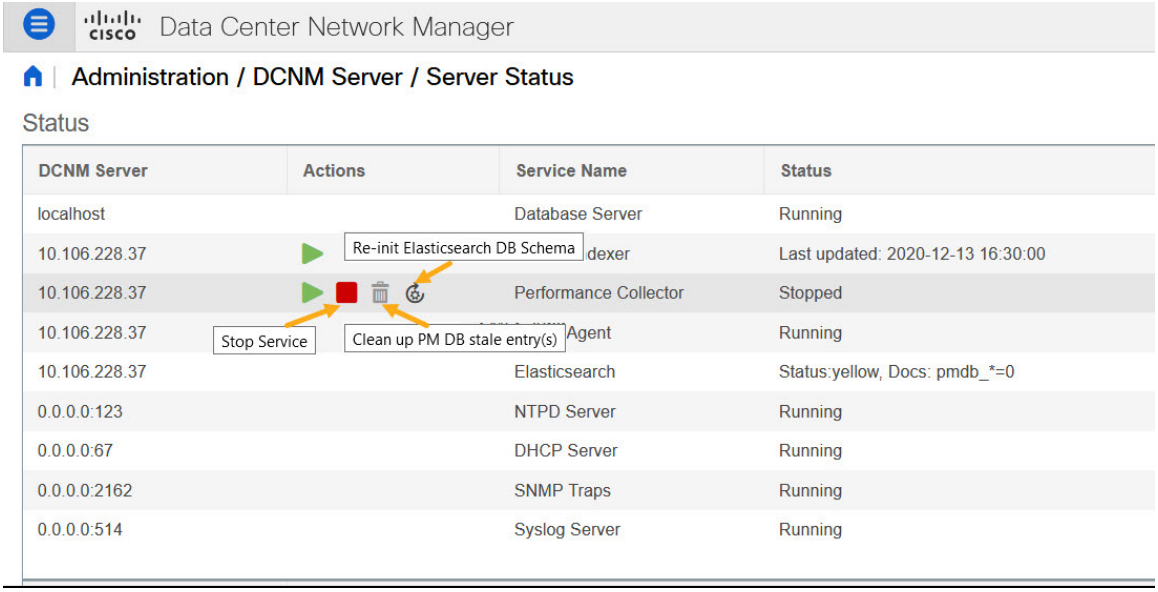
Step 2 On the Cisco DCNM Web UI, choose **Administration > Performance Setup > LAN Collections**.

Uncheck all the check boxes and click **Apply** to disable all switches and collections.



Step 3 Choose **Administration > DCNM Server > Server Status**.

Step 4 Against the **Performance Collector** service, click the stop icon in the Actions column to stop the data collection.



Step 5 Click the delete icon to clean the Performance Manager database.

This action deletes the stale entries in the performance manager database.

Step 6 Click on the reinitialize icon to reindex the Elasticsearch database schema.

This operation cleans the performance manager data in the Elasticsearch database and restarts the performance manager. It may take a few minutes to complete.

Step 7 Click **Continue**.

The status of the Performance Collector service shows **Stopped**.

Step 8 Ensure that you've deleted all the PMDB entries using the following command:

- For upgrading from Release 11.1(1)

  curl https://127.0.0.1:33500/_cat/indices?pretty | grep pmdb
- For upgrading from Release 11.2(1)

  curl https://127.0.0.1:33500/_cat/indices?pretty | grep pmdb
- For upgrading from Release 11.3(1)

  curl http://127.0.0.1:33500/_cat/indices?pretty | grep pmdb
- For upgrading from Release 11.4(1)

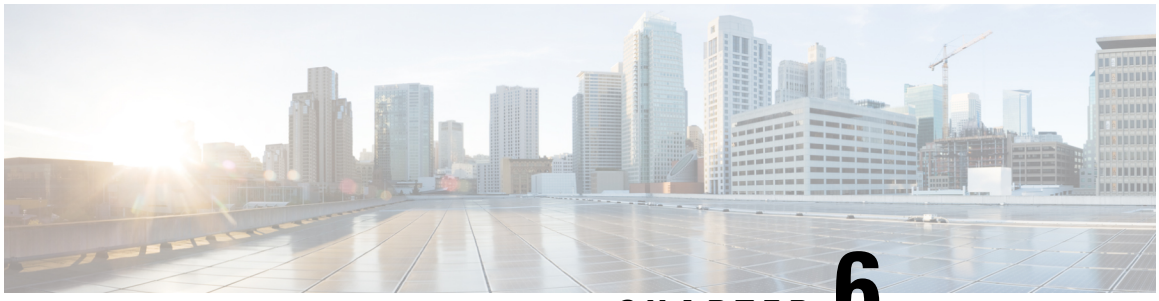
  curl http://127.0.0.1:33500/_cat/indices?pretty | grep pmdb

For example:

```
dcnm-root-11-4# curl http://127.0.0.1:33500/_cat/indices?pretty | grep pmdb

  % Total    % Received % Xferd  Average  Speed   Time    Time     Time  Current
                                 Dload    Upload  Total   Spent    Left  Speed
100  2244  100  2244    0     0   3638      0 --:--:-- --:--:-- --:--:--  3636
```

Step 9 Proceed to upgrade the DCNM to Release 11.5(1).



CHAPTER 6

Upgrading the Cisco DCNM Classic LAN Deployment

- Overview, on page 91
- **Migration of Fabrics**, on page 92
- Supported Switch Roles in LAN Fabric Post Upgrade, on page 94
- Classic LAN Templates in LAN Fabric, on page 94
- Upgrading from the Classic LAN Deployment to the LAN Fabric Deployment, on page 98
- LAN Classic Fabric Template Functionalities, on page 101

Overview

Starting from Cisco DCNM Release 11.4(1), the Classic LAN deployment is unsupported. If you are planning to upgrade your Classic LAN deployment to DCNM Release 11.5(1), refer to the upgrade options listed in the below table. The LAN Classic installation will automatically be converted to the LAN Fabric installation mode during the inline upgrade.

In the LAN Fabric deployment, there are two new fabric templates that you can use to manage your switches. For more information, see Managing Switches Using Classic LAN Templates.

The following table summarizes upgrades for your Classic LAN deployment to the Cisco DCNM Release 11.5(1):

Table 7: Classic LAN Upgrade

From Classic LAN deployment in DCNM Release	To LAN Fabric deployment in DCNM Release	Upgrade
11.3(1)	11.5(1)	Inline upgrade
11.2(1)	11.5(1)	Inline upgrade

When you perform the inline upgrade from older releases to Cisco DCNM Release 11.5(1), automatic conversion to LAN Fabric mode using **LAN_Classic** and **Fabric_Group** fabric templates is done.

Note We recommend that you to familiarize yourself with the Cisco DCNM LAN Fabric functionalities before proceeding with the upgrade. For information, see Cisco DCNM LAN Fabric Configuration Guide, Release 11.5(1).

Prerequisites

- Review the Cisco DCNM 11.5(1) LAN Fabric System Requirements to ensure that your existing deployment meets those criteria. See System Requirements.
- Review the Cisco DCNM LAN Fabric Verified Scalability section to ensure your existing deployment needs are met. See *Verified Scalability Guide for Cisco DCNM*.

Guidelines and Limitations

- In the Classic LAN deployment, if you are managing switches using the in-band interfaces, upgrading to the LAN Fabric deployment is not supported. You need to change to managing switches using the management (mgmt0) interfaces, and then upgrade.

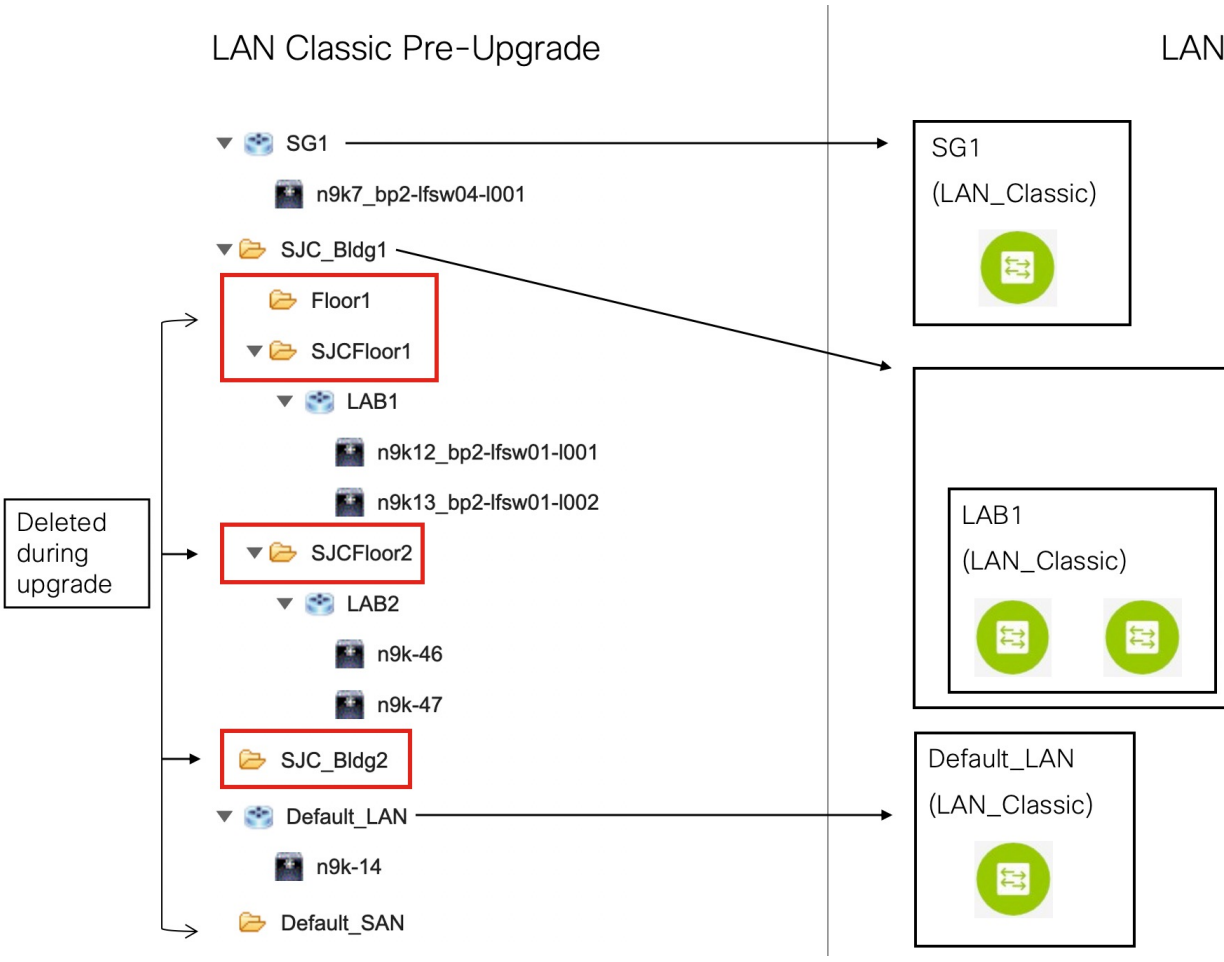
  The support for in-band interface management is expected to be available in a future release.
- VDC Auto-Provisioning (VOAP) for Cisco Nexus 7000 Series switches is not supported in the LAN Fabric installation mode.
- The following configurations are not migrated from Classic LAN to the LAN Fabric Deployment:
  - Config archive jobs.

    Post upgrade, you should configure the fabric backups from the fabric settings.
  - CLI jobs.
  - POAP DHCP configuration.

    Post upgrade, you should configure the Fabric Settings for POAP.

Migration of Fabrics

The DCNM upgrade from Classic LAN automatically creates fabric instances in LAN Fabric to match the Classic LAN switch and container groups. The inline upgrade to the LAN Fabric mode preserves only two levels of hierarchy if nested grouping is present. All intermediate and/or empty groups are automatically removed. For reference, see the following image:



The summary of the migration behavior is as follows:

- Only switch groups that hold switches will be migrated over to a fabric instance using the **LAN_Classic** fabric template. In this example, **SG1**, **LAB1, LAB2,** and **Default_LAN** are migrated.
- Only two levels of hierarchy is maintained during the upgrade. Any intermediate groups are deleted, and the lowest level switch groups are promoted to the top of the hierarchy.

  In this example:

  - **SJC_Bldg1** is the top-level container group that has valid switch groups in Classic LAN. Therefore, a fabric instance for **SJC_Bldg1** is created in LAN Fabric, and it uses the **Fabric_Group** template.
  - Fabric instances for **LAB1** and **LAB2**are created using the **LAN_Classic** fabric template in LAN Fabric. These fabric instances are made member fabrics of **SJC_Bldg1**.
  - The intermediate **SJCFloor1** and **SJCFloor2** containers are not carried over to LAN Fabric.

- Container groups that do not have any valid switch groups are not migrated. In this example, **Floor1** and **SJC_Bldg2** are not migrated.
- Switch groups will be migrated to standalone fabric instances using the **LAN_Classic** fabric template. In this example, **Default_LAN** is migrated to LAN Fabric with the **LAN_Classic** fabric template.

- After migration, the devices will be placed in the **Migration Mode** in fabrics associated with the **LAN_Classic** fabric template. The fabric will be in the **Fabric Monitor Mode**.

  For more information about the next steps, see *Upgrading from the Classic LAN Deployment to the LAN Fabric Deployment*.

Supported Switch Roles in LAN Fabric Post Upgrade

Some of the switch roles supported in the Classic LAN installation mode are not available in LAN Fabric. The following table shows the switch roles in Classic LAN and their equivalents in LAN Fabric:

Classic LAN (Pre-Upgrade)	LAN Fabric (Post Upgrade)
Border PE	Border
Edge	Edge Router
FEX Host Admin VDC	Access

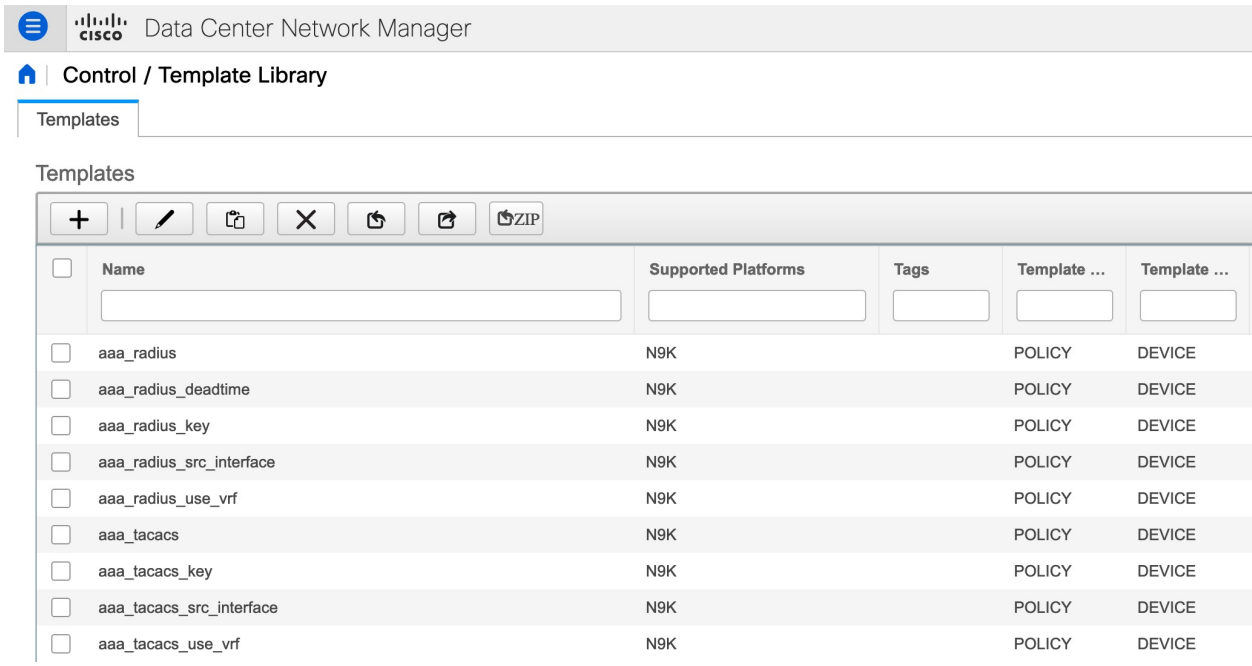
Note that these roles are automatically mapped to their equivalent roles in LAN Fabric after the upgrade.

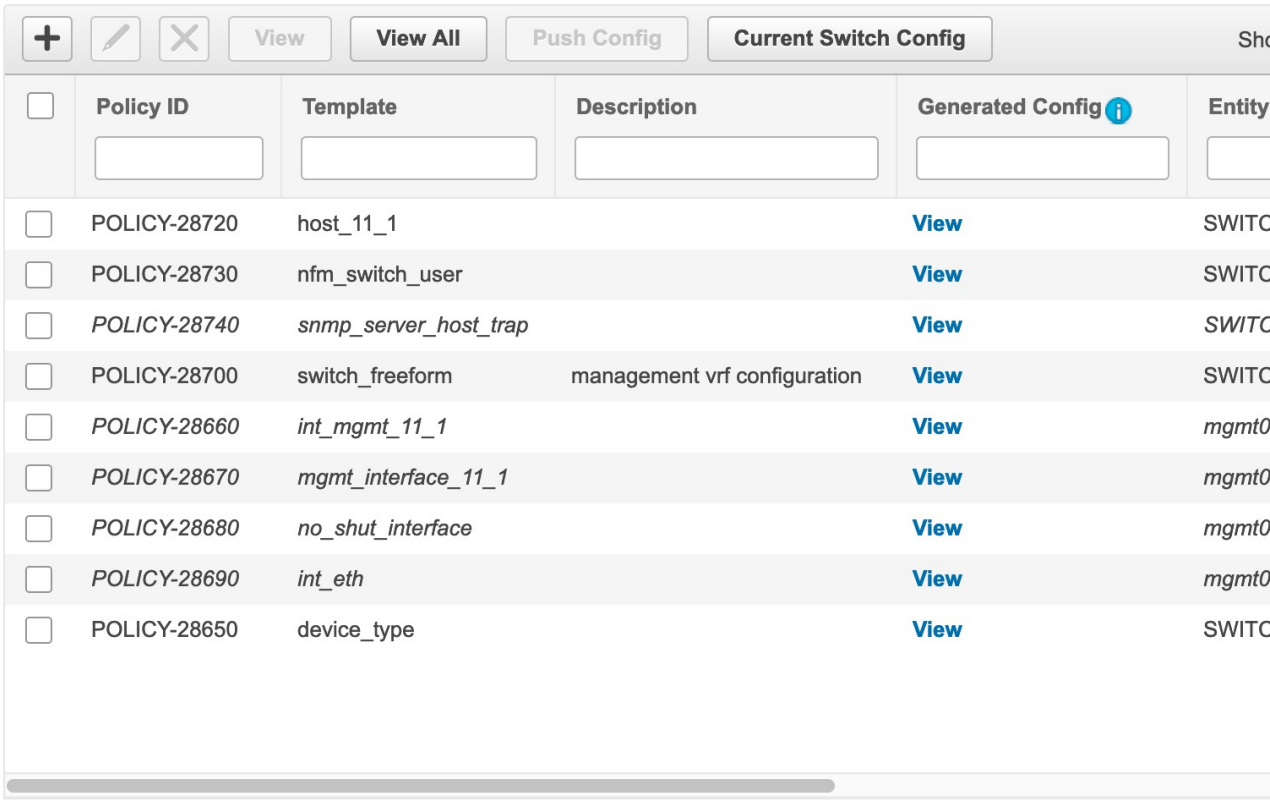
The following switch roles remain the same in LAN Fabric after the upgrade:

- Spine
- Leaf
- Border Spine
- Border
- Border Gateway
- Edge Router
- Core Router
- Access
- Aggregation

Classic LAN Templates in LAN Fabric

The templates of **templateType = CLI** are converted to **templateType = POLICY**. These templates are displayed in **Control > Template Library**. If needed, PTIs can be created from the **View/Edit Policies** window.


Data Center Network Manager
Control / Template Library
Templates
Templates
ZIP
Name
Supported Platforms
Tags
Template ...
Template ...
aaa_radius N9K POLICY DEVICE
aaa_radius_deadtime N9K POLICY DEVICE
aaa_radius_key N9K POLICY DEVICE
aaa_radius_src_interface N9K POLICY DEVICE
aaa_radius_use_vrf N9K POLICY DEVICE
aaa_tacacs N9K POLICY DEVICE
aaa_tacacs_key N9K POLICY DEVICE
aaa_tacacs_src_interface N9K POLICY DEVICE
aaa_tacacs_use_vrf N9K POLICY DEVICE



Note If policies that are updated automatically need to be reviewed, a backup of the original file is saved with a .bak extension in the following directory on DCNM: `/usr/local/cisco/dcm/dcnm/data/templates/.`

Some of the template language constructs that are available in Classic LAN are not supported in LAN Fabric installation. For example:

- Custom prompt handling
- Command execution logic
- Derived/Inherited templates

Note The templates need to be edited appropriately to work with LAN Fabric.

Unsupported Template Language Content

The following Classic LAN template language features are not supported in the LAN Fabric installation mode.

Note that the existing templates using this content are not supported. They need to be reviewed and/or edited to create compatible templates.

1. Interactive command handling:

   Include prompt and response as part of the template content for handling interactive commands.

   For example:

```
##template variables
string srcFile;
string srcDir;
string password;
string vrf;
##

##template content
copy scp://root@10.127.117.65/$$srcFile$$ bootflash: vrf $$vrf$$ <prompt:'(yes/no)?',
response:'yes'> <prompt:'(y/n)?[n]',
response:'y'> <prompt:'password:',
response:'$$password$$'>
```

2. Dynamic decision

   Config template provides a special internal variable **LAST_CMD_RESPONSE**.

   For example:

```
##template content
 show vlan id $$vlan_id$$
 if($$LAST_CMD_RESPONSE$$ contains
        "not found"){
 vlan $$vlan_id$$
 }
 else{
 }
```

3. Template referencing

   In this case, templates are referenced from another template.

   Derived Template:

```
##template properties
 [snip]
 imports = baseTemplate1,baseTemplate2;

        ##
```

For more information about templates, see Cisco DCNM Classic LAN Configuration Guide, Release 11.3(1) and Cisco DCNM LAN Fabric Configuration Guide, Release 11.4(1).

Upgrading from the Classic LAN Deployment to the LAN Fabric Deployment

Procedure

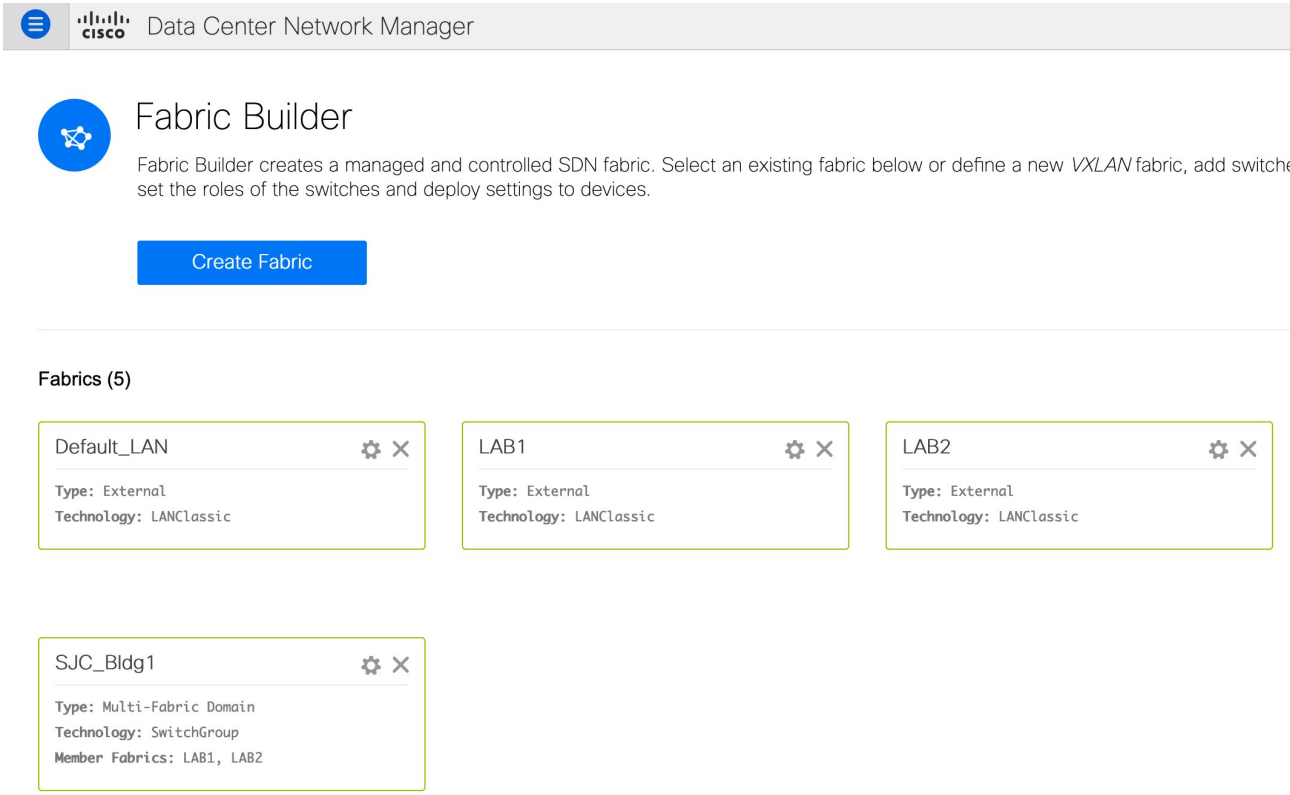
Step 1 Make sure that all switches are reachable from Cisco DCNM before the upgrade.

Note
If nested switch groups are in DCNM 11.3(1) and telemetry is enabled on them, you need to disable telemetry on those switch groups before upgrade.

Step 2 Follow the inline upgrade procedure to upgrade to the LAN Fabric deployment.

For information, see Upgrading ISO or OVA through Inline Upgrade.

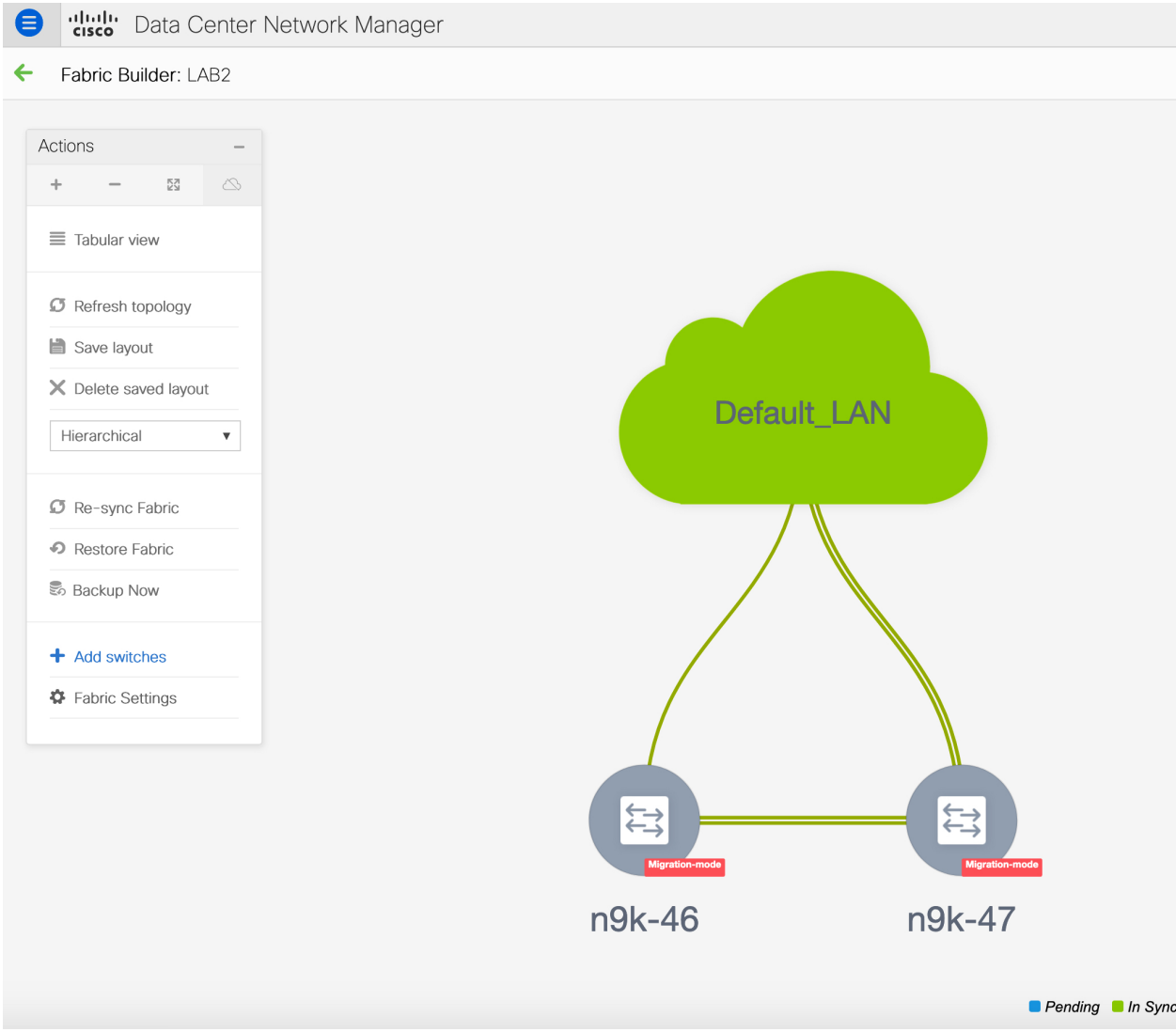
Step 3 Post upgrade, the DCNM installation type will be automatically changed to LAN Fabric and appropriate fabric instances are created. For information about the fabric, see Migration of Fabrics, on page 92.

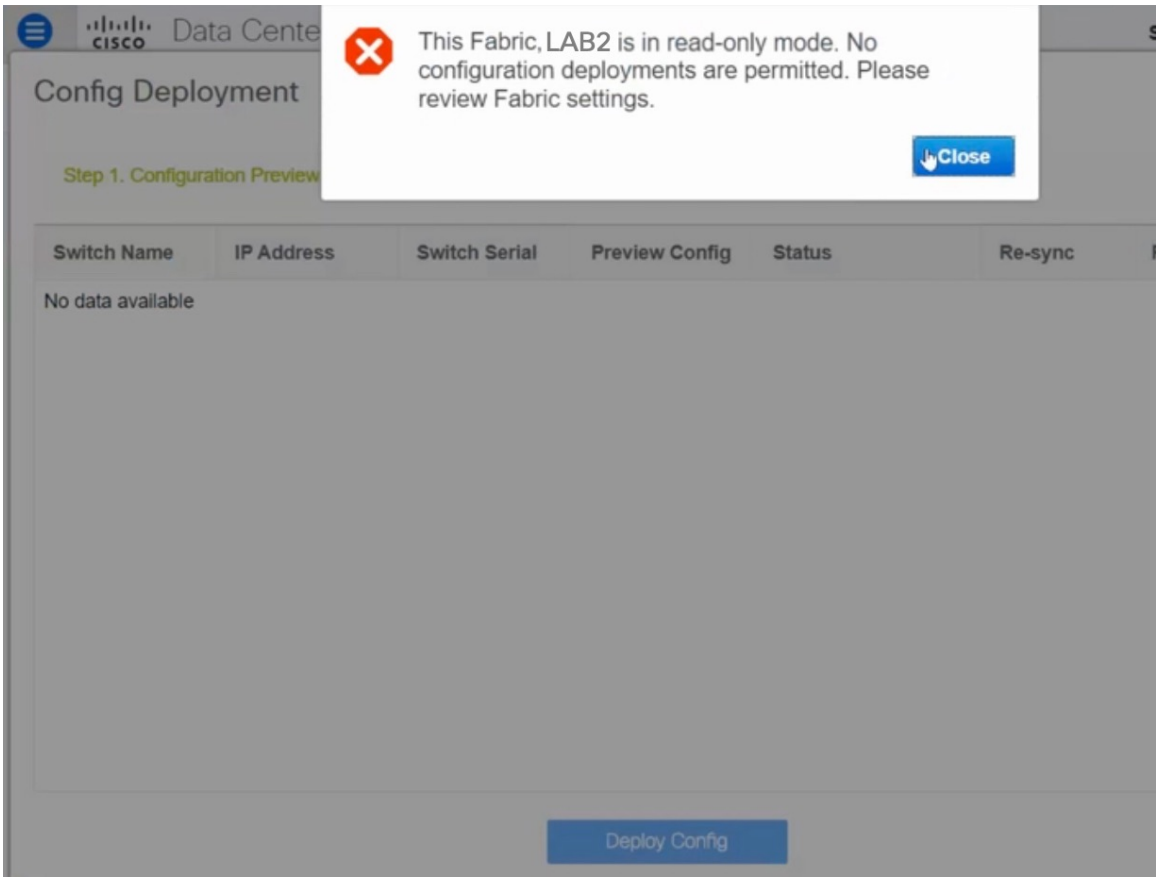


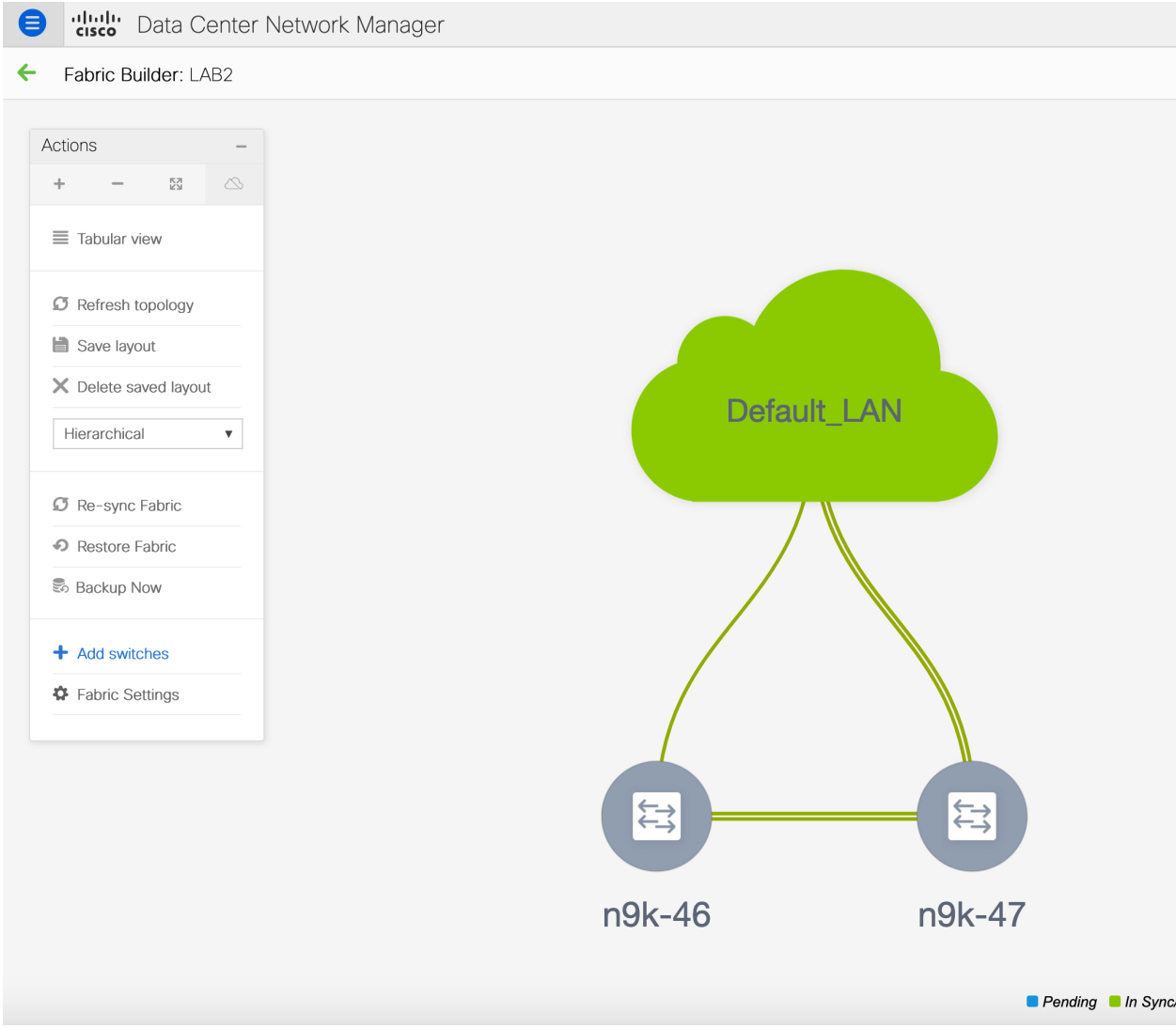
Step 4 The switches are placed in the **Migration Mode**. Navigate to each **LAN_Classic** fabric and click **Save & Deploy**.

Note

The fabrics are in the **Monitor Mode** by default. An error message is seen because of this mode, and it can be ignored.




Data Cente
Config Deployment
This Fabric, LAB2 is in read-only mode. No configuration deployments are permitted. Please review Fabric settings.
Close
Step 1. Configuration Preview
Switch Name
IP Address
Switch Serial
Preview Config
Status
Re-sync
No data available
Deploy Config



This step ensures that the minimum configuration intent is captured for the switches. The switches continue to remain in the **Migration Mode** till any connectivity issue and errors are resolved. To move the switches out of this mode, subsequent **Save & Deploy** operations are needed.

LAN Classic Fabric Template Functionalities

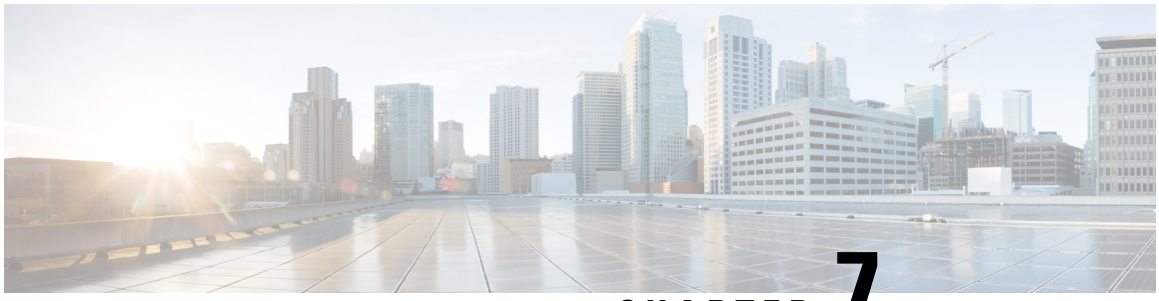
The following features in the LAN_Classic template provide the same support as they do for the External_Fabric_11_1 template:

The following features are supported:

- Configuration compliance
- Backup or restore of fabric/switch

- Network Insights
- Performance monitoring
- VMM
- Topology view
- Kubernetes visualization
- RBAC

For more information, refer to the feature specific sections.



CHAPTER 7

Deployment Best Practices

- Best Practices for Deploying Cisco DCNM and Computes, on page 103

Best Practices for Deploying Cisco DCNM and Computes

This chapter describes the document best practices to deploy Cisco DCNM OVA and ISO in clustered and unclustered modes. The following sections explain the recommended design for configurations of IP addresses and relevant IP pools during the Cisco DCNM installation.

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

- dcnm-mgmt network (eth0) interface

  This network provides connectivity (SSH, SCP, HTTP, HTTPS) to the Cisco DCNM.

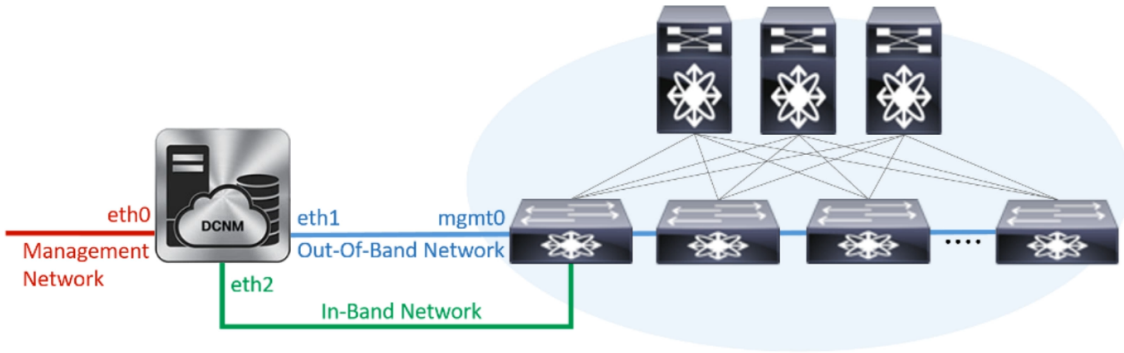
- enhanced-fabric-mgmt (eth1) interface

  This network provides enhanced fabric management of Cisco Nexus switches through the out-of-band or mgmt0 interface.

- enhanced-fabric-inband (eth2) interface

  This network provides in-band connection to the fabric through the front-panel ports. This network interface is used for applications such as Endpoint Locator (EPL) and Network Insights Resources (NIR).

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



Guidelines to Use the Best Practices

The following are the guidelines to remember while you use the best practices for deploying DCNM and Computes.

- The IP addresses specified in this document are sample addresses. Ensure that your setup reflects the IP addresses used in the production network.
- Ensure that the eth2 interface subnet is different from the subnet that is associated with the eth0 interface and the eth1 interface.
- As eth0 and eth1 interfaces are both on the same subnet, the DHCP returns the same IP address, two responses but same for both queries.
- Cisco DCNM Native HA consists of two Cisco DCNM appliances, that run as Active and Standby applications. The embedded databases of both Active and Standby appliances are synchronized in real time. The eth0, eth1, and eth2 interfaces of the Cisco DCNM and Compute nodes, in a clustered mode, must be Layer-2 adjacent.
- For information about Cluster Mode in your Cisco DCNM Deployment, refer to Applications chapter in the *Cisco DCNM Configuration Guide* for your deployment type.

Deployments for Redundancy in Cisco DCNM

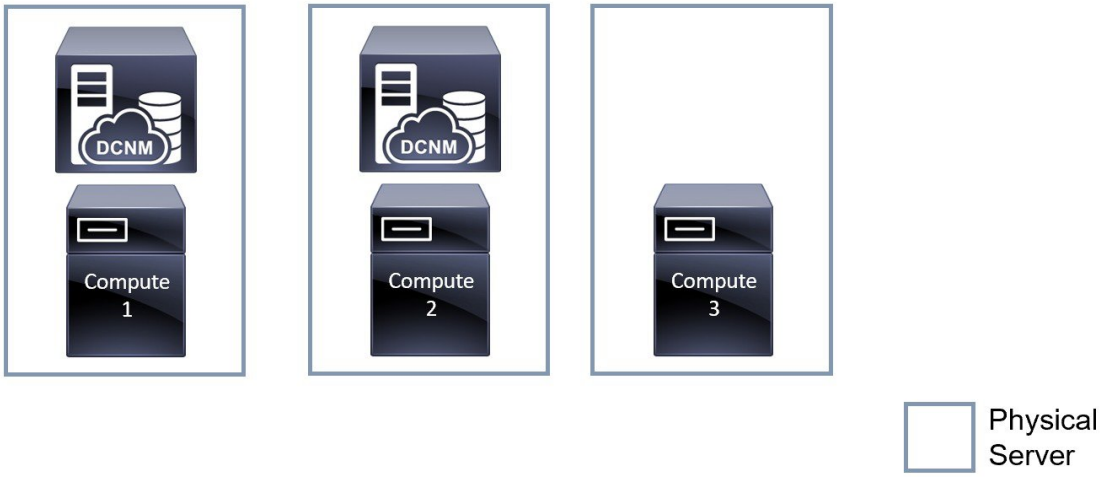
This section describes the recommended deployments for redundancy of DCNM operations. As a general assumption, the DCNM and the compute nodes are installed as Virtual Machines. During Cisco DCNM ISO installation on Virtual Appliance on UCS (Bare Metal), all DCNMs and computes have their own individual servers.

Deployment 1: Minimum Redundancy Configuration

The recommended configuration for minimum redundancy in a Cisco DCNM Cluster mode installation is as follows:

- DCNM Active Node and Compute Node 1 in Server 1
- DCNM Standby Node and Compute Node 2 in Server 2
- Compute Node 3 in Server 3
- Compute VMs deployed on an exclusive disk
- No oversubscription of memory or CPU of the physical servers

Figure 9: Cisco DCNM Cluster Mode: Physical Server to VM Mapping

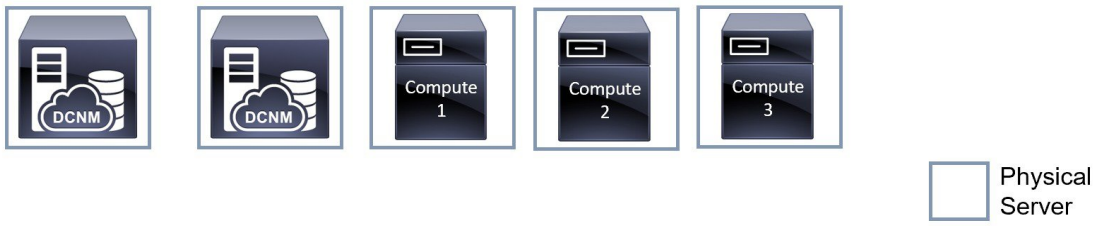


Deployment 2: Maximum Redundancy Configuration

The recommended configuration for maximum redundancy in a DCNM Cluster mode installation is as follows:

- DCNM Active Node(Active) in Server 1
- DCNM Standby Node in Server 2
- Compute Node 1 in Server 3
- Compute Node 2 in Server 4
- Compute Node 3 in Server 5

Figure 10: Cisco DCNM Cluster Mode: Physical Server to VM Mapping



IP Address Configurations in Cisco DCNM

This section describes the best practices and recommended deployments for IP address configurations of all interfaces of the Cisco DCNM and Compute nodes.

Scenario 1: All 3 Ethernet Interfaces are in Different Subnets

In this scenario, consider all three Ethernet interfaces of DCNM on different subnets.

For example:

- eth0 – 172.28.8.0/24
- eth1 – 10.0.8.0/24
- eth2 – 192.168.8.0/24

The possible deployments are as follows:

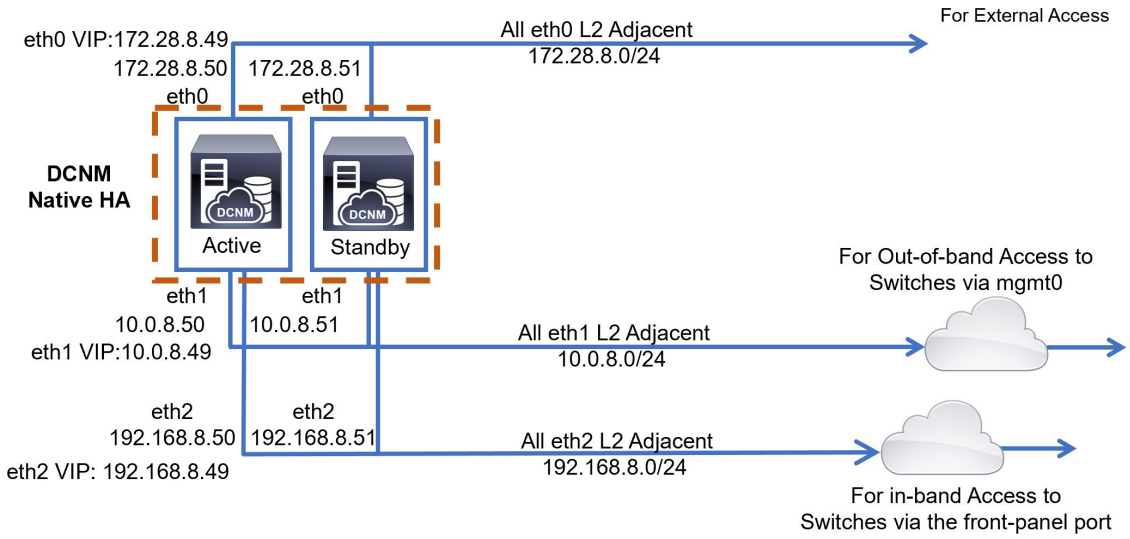
- Cisco DCNM Unclustered mode, on page 106
- Cisco DCNM Clustered Mode, on page 107

Cisco DCNM Unclustered mode

Figure 11: Cisco DCNM Standalone Deployment without Compute Cluster



Figure 12: Cisco DCNM HA Deployment without Compute Cluster



Cisco DCNM Clustered Mode

Figure 13: Cisco DCNM Standalone Deployment with Compute Cluster

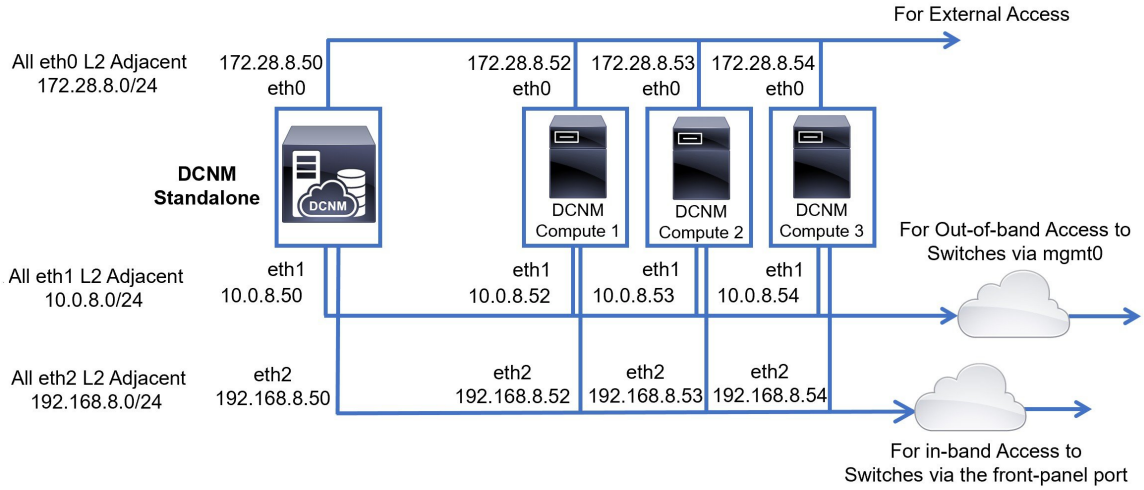
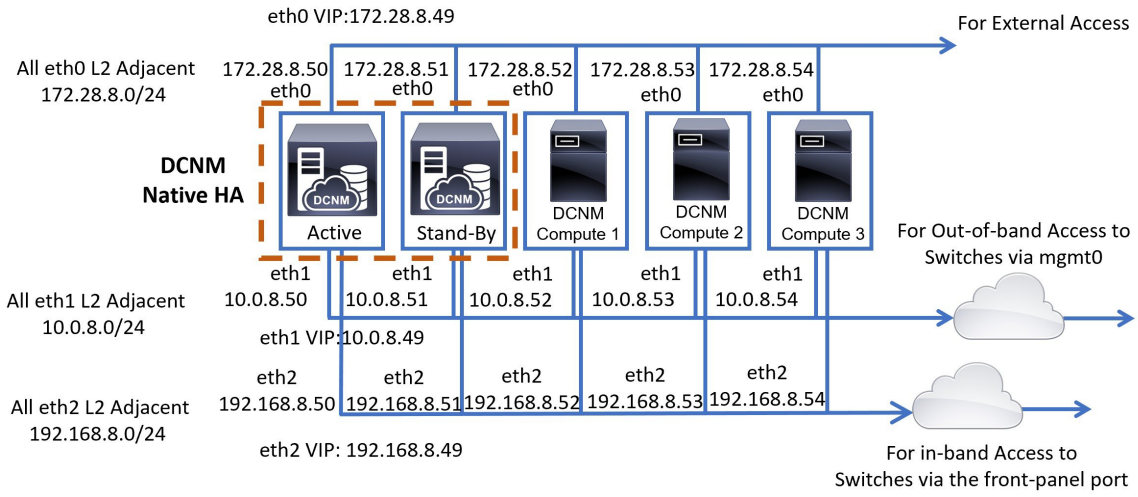


Figure 14: Cisco DCNM HA Deployment with Compute Cluster



Scenario 2: eth2 Interface in Different Subnet

In this scenario, consider that the eth0 and eth1 interfaces are in the same subnet, and eth2 interfaces of DCNMs and Computes are in a different subnet.

For example:

- eth0 – 172.28.8.0/24
- eth1 – 172.28.8.0/24
- eth2 – 192.168.8.0/24

The possible deployments are as follows:

- Cisco DCNM Unclustered Mode, on page 109
- Cisco DCNM Clustered Mode, on page 110

Cisco DCNM Unclustered Mode

Figure 15: Cisco DCNM Standalone deployment (No HA) without Compute Cluster

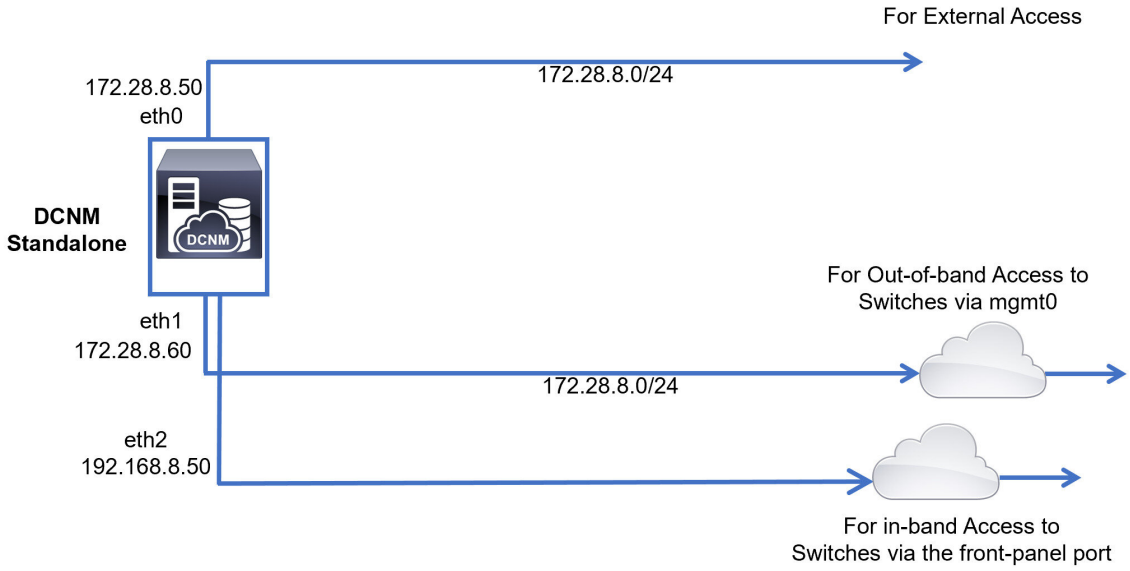
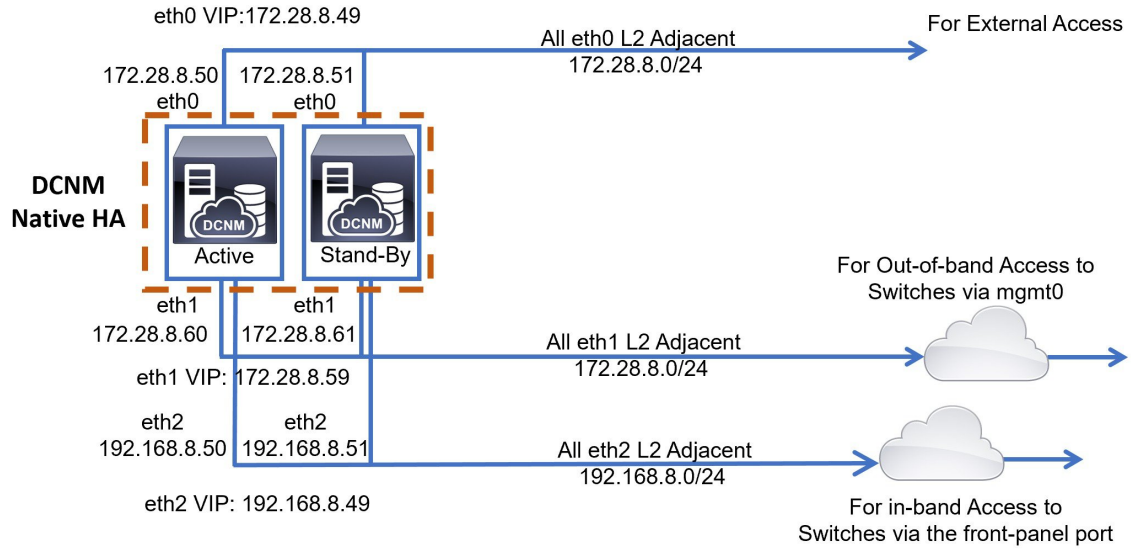


Figure 16: Cisco DCNM Native HA deployment without Compute Cluster



Cisco DCNM Clustered Mode

Figure 17: Cisco DCNM Standalone Deployment with Compute Cluster

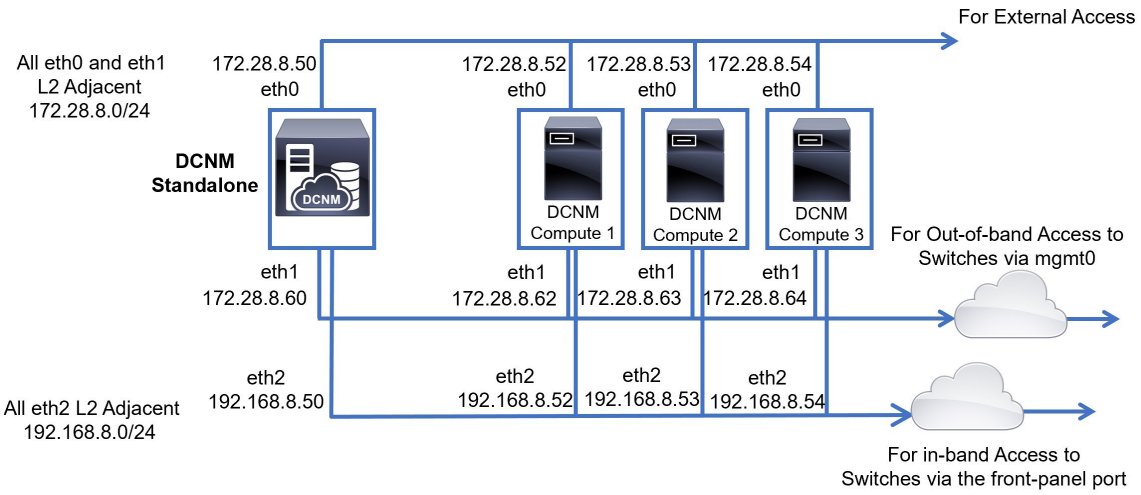
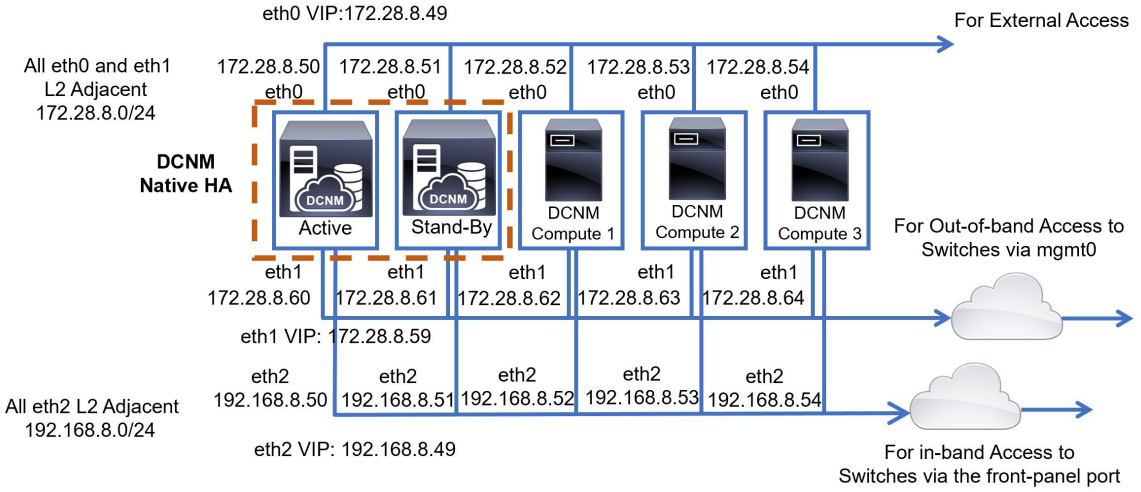


Figure 18: Cisco DCNM Native HA Deployment with Compute Cluster



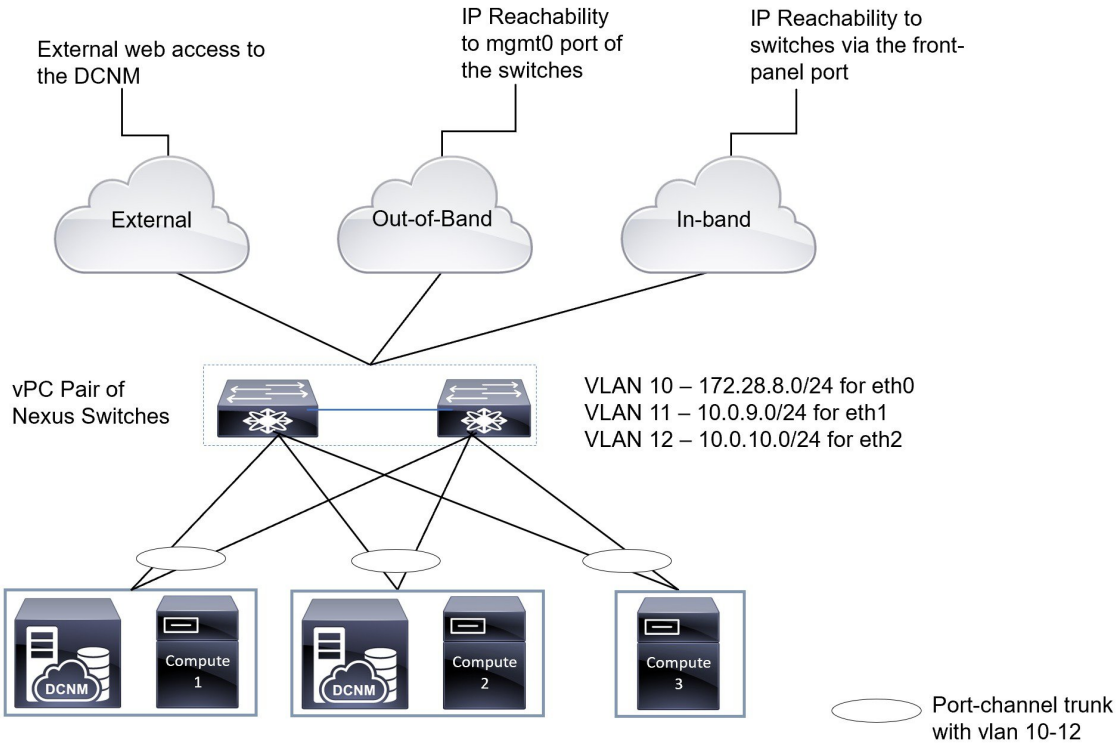
Physical Connectivity of Cisco DCNM and Compute Nodes

This section describes the physical connectivity of the Cisco DCNM and Compute nodes in both Virtual Machines and Bare Metal installations.

Virtual Machines

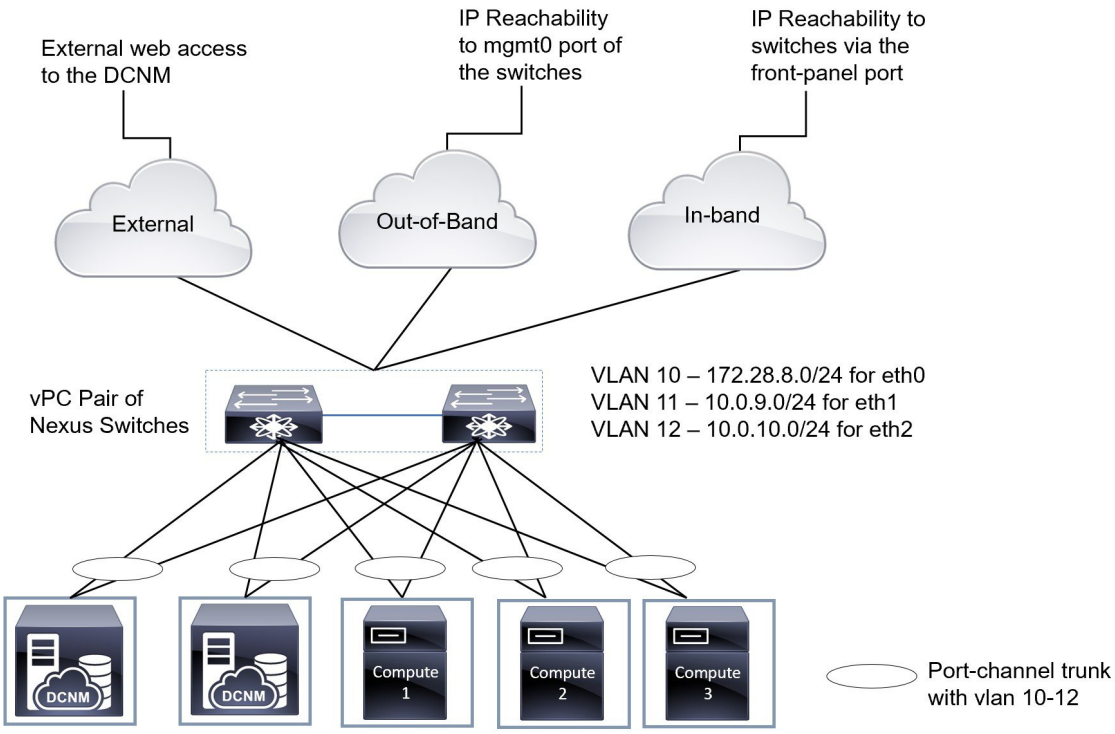
The following image shows the physical connectivity of DCNM and compute nodes supported in a 3 server redundancy configuration. The physical servers must be connected to a vPC pair of switches via port-channels. This provides adequate fault-tolerance, if a single link fails or a single switch fails. The vPC pair of switches is considered as the infra vPC pair that provides management connectivity to the physical servers.

Figure 19: Cisco DCNM VM Physical Connectivity with 3 servers



The following image shows the physical connectivity of Cisco DCNM and Compute nodes supported in an VM installation in a 5 server redundancy configuration.

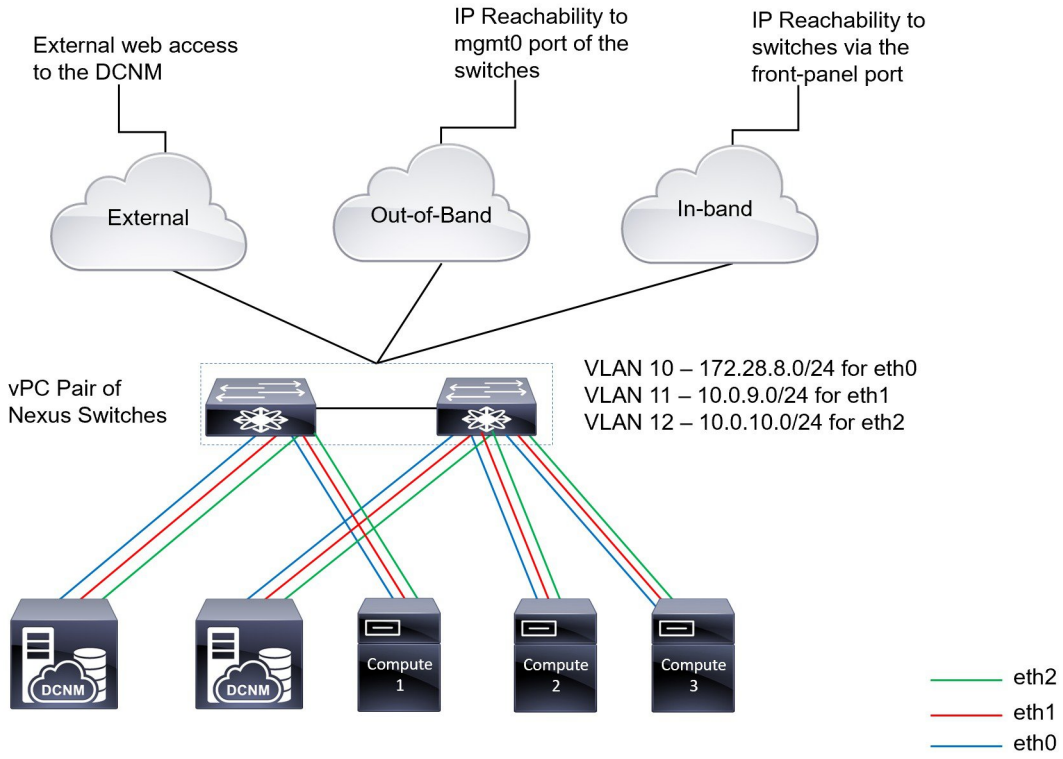
Figure 20: Cisco DCNM VM Physical Connectivity with 5 servers

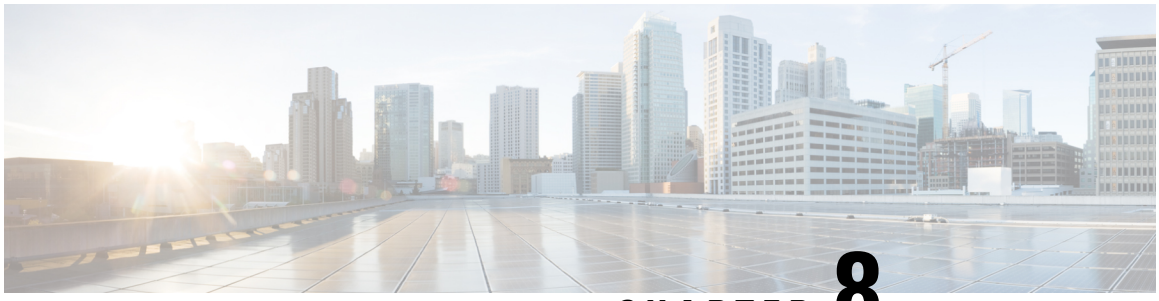


Bare Metal Installation

For installing Cisco DCNM on Bare Metal, 5 servers are required. The following image shows the physical connectivity of Cisco DCNM and Compute nodes. Note that, there are 3 physical interfaces on each server that map to the eth0, eth1, and eth2 interfaces, respectively. If the physical server consists of a managed network adapter such as the Cisco UCS VIC 1455 Virtual Interface Card, you can have a port-channel connectivity from the servers to the switches, similar to the Virtual Machines.

Figure 21: Cisco DCNM and Compute Bare Metal Physical Connectivity





CHAPTER 8

Disaster Recovery (Backup and Restore)

This chapter contains the following sections:

- Backup and Restore Cisco DCNM and Application Data on Standalone DCNM setup, on page 115
- Backup and Restore Cisco DCNM and Application Data on Native HA setup, on page 116
- Recovering Cisco DCNM Single HA Node, on page 117
- Recovering admin Account, on page 119
- HA Disaster Avoidance using SRM, on page 120
- Backup and Restore Cisco DCNM on a Cluster Setup, on page 122

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

You can take a backup of Cisco DCNM application data for analytics and troubleshooting.

Note In Release 11.3(1), the sysadmin and the root user's password are not identical. When you upgrade to 11.5(1), the sysadmin and root user passwords are preserved.

However, when you perform backup and restore on Cisco DCNM after upgrade, the sysadmin user inherits the password from the root user, and therefore both the users will have the same password. You can change the password for both the users after restore is complete.

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
```

From Release 11.4(1), Cisco DCNM allows you to configure a cron job that allows saves the backup to a remote scp server. Use **appmgr backup schedule** command to configure a scheduled backup.

```
dcnm# appmgr backup schedule [day] <hh<hh>:<mm>
[destination <user>@<host>:[<dir>]]
```

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 radio button.

Select the backup file that was generated in Step 2, on page 115.

Continue to deploy the DCNM.

Step 8 On the Summary tab, review the configuration details.

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

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

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

Step 9 After the data is restored, check the status using the **appmgr status all** command.

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

You can take a backup of Cisco DCNM application data for analytics and troubleshooting.

Note In Release 11.3(1), the sysadmin and the root user's password are not identical. When you upgrade to 11.5(1), the sysadmin and root user passwords are preserved.

However, when you perform backup and restore on Cisco DCNM after upgrade, the sysadmin user inherits the password from the root user, and therefore both the users will have the same password. You can change the password for both the users after restore is complete.

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
```

From Release 11.4(1), Cisco DCNM allows you to configure a cron job that allows saves the backup to a remote scp server. Use **appmgr backup schedule** command to configure a scheduled backup.

```
dcnm# appmgr backup schedule [day] <hh<hh>:<mm>
[destination <user>@<host>:[<dir>]]
```

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 radio button.

Select the backup file that was generated in Step Step 3, on page 117.

The values for parameters are read from the backup file, and auto-populated. Modify the values, if required.

Continue to deploy the DCNM.

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

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

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

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

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

Recovering Cisco DCNM Single HA Node

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

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

Failure type	Node/Database to recover	Primary backup available	Secondary backup available	Recovery procedure
Primary node is lost. Secondary node is now Primary (due to fail over).	Primary Node	—	—	1. Convert Secondary node to Primary node. 2. Configure new Secondary node.
Primary and Secondary server database is lost. Secondary node is now Primary (due to fail over)	Primary database	—	—	The Active Secondary node will restart and sync to the Standby Primary node.
Active Secondary node is lost. Primary node is now active due to fail over.	Secondary node	—	No	Configure new Secondary node.
Active Secondary node is lost. Primary node is not active due to fail over.	Secondary node	—	Yes	Configure new Secondary node, using the Web Installer. Choose **Fresh installation with backup file for restore**. Select **Restore secondary DCNM node only** in HA settings screen.
Secondary standby node is lost.	Secondary node	—	No	Configure new Secondary node.
Secondary standby node lost	Secondary node	—	Yes	Configure new Secondary node, using the Web Installer. Choose **Fresh installation with backup file for restore**. Select **Restore secondary DCNM node only** in HA settings screen.
Primary node is active. Secondary standby database lost.	Secondary database	—	—	Primary node will restart to sync with Secondary node.

Converting Secondary node to Primary node

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

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

```
NODE_ID 1
```

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

Configuring Secondary node

To configure the secondary node, perform the following steps:

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



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

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

Recovering admin Account

If you have the network-admin user/password credentials, you can login and recover the password for other users from the Cisco DCNM Web UI. See Step 5, on page 120.

To recover the Cisco DCNM Web UI user or password, perform the following steps:

Before you begin

Ensure that you have privileges to change the password.

Procedure

Step 1 Launch SSH and login to the DCNM server as a **/root** user.

```
[root@dcnm]#
```

Step 2 Navigate to `/usr/local/cisco/dcm/fm/bin` folder.

```
[root@dcnm]# cd /usr/local/cisco/dcm/fm/bin
[root@dcnm bin]#
```

Step 3 Execute **addUser.sh** script to create a new network-admin user. Provide a new username, password and the database password.

```
[root@dcnm bin]# ./addUser.sh <user> <password> <dbpassword>
```

The following message is generated and a new user is created.

```
----------------------- OUTPUT ----------------------------
----insertUser--------
----username----------john123
----role--------------network-admin
----insertUser--------done...
    Added user : john123 successful!
----------------------- END -----------------------------
```

Step 4 Login to the Cisco DCNM Web UI with new user to Cisco DCNM Web UI.

Step 5 Choose **Administration > Management Users > Local**.

The new user is displayed in the list.

Step 6 Select the user to recover the password, and click **Edit** icon.

Step 7 On the Edit User window, modify the **Role** and **Password** for the user.

You can also set the password to expire in 180 days.

Step 8 Click **Apply** to save your changes.

HA Disaster Avoidance using SRM

Cisco DCNM Release 11.5(1) can be successfully deployed on the VM Site Recovery Manager (SRM). SRM is a disaster recovery software that provides automated orchestration of failover and fail-back to minimize downtime.

Note This document provides a high-level work flow. Fro detailed information, refer to https://docs.vmware.com/en/Site-Recovery-Manager/index.html.

To setup the DCNM and migrate to SRM, perform the following task:

1. Configure a management server (ESXi 6.7) running vCenter, SRM, VM replicator manager running on Site 1.
2. Similarly, configure a management server (ESXi 6.7) running vCenter, SRM, VM replicator manager running on Site 2.

   VRM helps replicate VMs from one site to another.

Note All VMs must be deployed together in the same site. When migrating DCNM VMs (planned recovery or disaster recovery), all DCNM VMs must be migrated to the recovery site.

3. Replicate Site1 to Site2 to sync.
4. Migrate Site1 and Site2 to the Site Recovery Manager.
5. Deploy the VMs on the Recovery Site.

Compatibility:

- ESXi 6.7
- SRM 8.3

To configure the SRM for DCNM HA disaster recovery, perform the following task:

1. Launch the SRM.
2. Pair Site1 and Site2. After the replication is complete, both the Sites are synchronized.
3. Click View Details.

   The Summary page opens.
4. On the Summary tab,
   a. Click Network Mappings and map the networks used by the VM on both Site1 and Site2.
   b. Click Folder Mappings. Map all the folders used by vCenter for the VMs.
   c. Click Resource Mappings. Map the resources on each component in Site1 to components in Site2. Choose Yes under Reverse Mapping.
   d. Click on Placeholder Datastores. Map hosts/clusters to the correct datastores. For example, the VMs in the Host/Cluster will be replicated to the mapped Datastore.



Note Ensure that VMs are replicated to the correct datastores. Recovery plan fails, otherwise.

5. On the Replications tab
   a. Replicate VMs from a source site to a target site with vSphere Replication.
   b. Click Outgoing in the left pane. All the data synchronized with site2 are displayed.
   c. If you're on Site1 and everything replication on Site2, this tab will be empty.
   d. Click Incoming in the left pane. Status of all the VMs synchronizing with Site2 are displayed.
   e. Configure a Recovery Point Objective (RPO) value during replication configuration, to determine the maximum data loss that you can tolerate.
   f. Click New to configure Replication Latency to configure the Recovery Point Objective. Click on the arrow before the VM to view configuration data for the VM.
6. On the Protection Groups tab:

   Configure one or more protection groups in a recovery plan. A recovery plan specifies how Site Recovery Manager recovers the virtual machines in the protection groups that it contains.

7. On the Recovery Plans tab,

   After you configure Site Recovery Manager at the protected and recovery sites, you can create, test, and run a recovery plan.

   a. When you create or modify a recovery plan, test it before you try to use it for planned migration or for disaster recovery.

   b. You can run a recovery plan under planned circumstances to migrate virtual machines from the protected site to the recovery site. If the protected site suffers an unforeseen event that might result in data loss, you can also run a recovery plan under unplanned circumstances.

   c. You can customize the actions of Site Recovery Manager during recovery by creating, testing, and running recovery plans.

   d. Running this plan in recovery mode will attempt to shut down the VMs at the protected site and recover the VMs at the recovery site.

   e. You can choose one of the recovery type:

      - **Planned migration** – replicates recent changes to the recovery site and cancel recovery if errors are encountered. Do not perform and resource intense operations during planned migration.
      - **Disaster recovery** – attempts to replicate recent changes to the recovery site, but otherwise use the most recent storage synchronization data. It continues the recovery even if errors are encountered.

   f. Click on … after Run and click Reprotect to protect the VMs or click Cancel to stop the recovery plan.

After Site Recovery Manager performs a recovery, the virtual machines start up on the recovery site. By running reprotect when the protected site comes back online, you reverse the direction of replication to protect the recovered virtual machines on the recovery site back to the original protected site.

Backup and Restore Cisco DCNM on a Cluster Setup

You can take a backup of Cisco DCNM application data for analytics and troubleshooting.

Perform the following task to take perform backup and restore of data in a Cisco DCNM Cluster setup.

Before you begin

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

Example:

On the Active node:

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

On the Standby node:

```
dcnm2-standby# appmgr show ha-role
Native HA enabled.
```

```
Deployed role: Standby
Current role: Standby
```

Procedure

Step 1 Log on to the Cisco DCNM appliance using SSH.

Step 2 Take a backup of the application data using the **appmgr backup** command on both Active, Standby appliances, and on all Compute nodes.

```
dcnm-active# appmgr backup
dcnm-standby# appmgr backup
dcnm-compute1# appmgr backup
dcnm-compute2# appmgr backup
dcnm-compute3# appmgr backup
```

Copy the backup files of all nodes 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 Install two Cisco DCNM Release 11.5(1) appliances.

Note
Ensure that the Hostnames match the earlier Active and Standby appliances.

For instructions, see Installing the Cisco DCNM.

Step 5 Install three Cisco DCNM Compute nodes.

Note
Ensure that the Hostnames match the earlier Compute nodes.

For instructions, see Installing Cisco DCNM Compute Node.

Step 6 Provide access to the `/root` directory on all nodes using the following command.

```
dcnm# appmgr root-access permit
```

Step 7 Stop telemetry on Active and Standby nodes using the following command:

```
dcnm-active# systemctl stop pmn-telemetry
dcnm-standby# systemctl stop pmn-telemetry
```

Step 8 Set the environment variable to allow restore process using CLI and restore the node with the same hostname as respective Active and Standby backup files, using the following command:

Note
Ensure that you perform the restore in the same order—Active, Standby, Compute1, Compute2, and Compute3.

```
dcnm-active# APPMGR_ALLOW_RESTORE=1 appmgr restore <dcnm1-backup-file>
dcnm-standby# APPMGR_ALLOW_RESTORE=1 appmgr restore <dcnm2-backup-file>
dcnm-compute1# APPMGR_ALLOW_RESTORE=1 appmgr restore <compute1-backup-file>
dcnm-compute2# APPMGR_ALLOW_RESTORE=1 appmgr restore <compute2-backup-file>
dcnm-compute3# APPMGR_ALLOW_RESTORE=1 appmgr restore <dcnm2-backup-file>
```

Step 9 After the data is restored, check the status using the **appmgr status all** command.

What to do next

Log on to the DCNM Web UI with appropriate credentials.

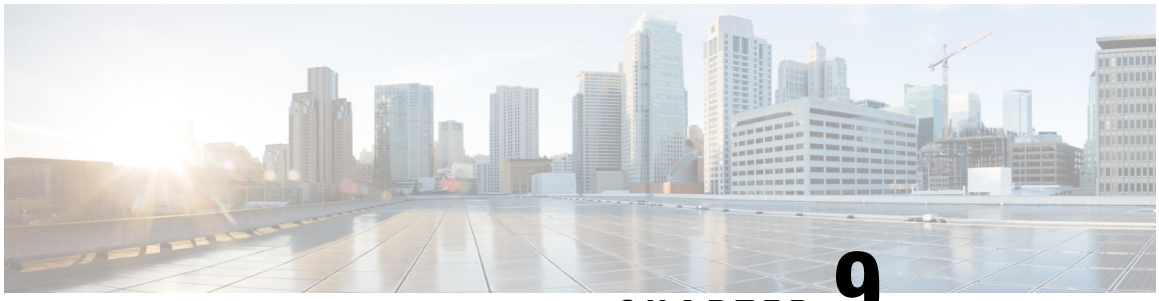
The Applications tab displays all the services running on the DCNM deployment that you have installed. Click Compute tab to view the new Compute in Discovered state on the Cisco DCNM Web UI.

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



Note If you didn't enable clustered mode while installing DCNM, use the **appmgr afw config-cluster** command to enable the compute cluster. For instructions, refer to Enabling the Compute Cluster in the Cisco DCNM LAN Fabric Configuration Guide.

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



CHAPTER 9

Certificates

- Certificate Management, on page 125

Certificate Management

Note This section to applicable only for DCNM OVA/ISO deployments.

From Release 11.2(1), Cisco DCNM allows new methods and new CLIs for installing, restoring after upgrade, and verifying certificates on the system. You can export certificates from the Active node to the Standby node, to ensure that both peers on the Native HA setup have the same certificates.

In a Cisco DCNM Native HA setup, after you install a CA certificate on the Active node and start the services, the certificates are automatically synchronized with the Standby node. If you need the same internal certificate on both Active and Standby nodes, you must export the certificate from the Active node to the Standby node. This ensures that both the peers on the Cisco Native HA setup have the same certificates.

Note From Release 11.3(1), you must use **sysadmin** role for certificate management.

Cisco DCNM stores two certificates:

- Self-signed certificate, for internal communication between the Cisco DCNM Server and various applications
- CA (Certificate Authority) Signed certificate, for communicating with the external world, such as Web UI.

Note Until you install a CA Signed certificate, Cisco DCNM retains a self-signed certificate for the communicating with the external network.

Best practices for Certificate Management

The following are the guidelines and best practices for Certificate Management in Cisco DCNM.

- Cisco DCNM provides CLI based utilities to display, install, restore, and export or import of certificates. These CLIs are available through SSH console, and only a **sysadmin** user can accomplish these tasks.
- When you install Cisco DCNM, a self-signed certificate is installed, by default. This certificate is used to communicate with the external world. After Cisco DCNM installation, you must install a CA-Signed certificate on the system.
- On Cisco DCNM Native HA setup, we recommend that you install a CA-Signed certificate on the DCNM Active Node. The CA-Signed certificate will synchronize with the Standby node automatically. However, if you want to keep the same internal and CA-Signed certificate on both Active node and Standby node, you must export the certificates from Active node and import it to the Standby node. Both the Active node and Standby node will have the same set of certificates.



Note Compute nodes in a cluster deployment do not require any action, as the compute nodes use internally managed certificates.

- Generate a CSR on Cisco DCNM with a CN (common name). Provide a VIP FQDN (Virtual IP Address FQDN) as CN to install a CA Signed certificate. The FQDN is the fully qualified domain name for the management subnet VIP (VIP of eth0) interface that is used to access Cisco DCNM Web UI.
- If the CA Signed certificate was installed prior to upgrading the Cisco DCNM, then you must restore the CA Signed certificate after you upgrade the Cisco DCNM.



Note You need not take a backup of certificates when you perform inline upgrade or backup and restore.

Display Installed Certificates

You can view the details of the installed certificate by using the following command:

appmgr afw show-cert-details

In the following sample output for the **appmgr afw show-cert-details** command, **CERTIFICATE 1** represents the certificate offered to the external network and to the Web browsers. **CERTIFICATE 2** represents the internally used certificate.

```
dcnm# appmgr afw show-cert-details

****CERTIFICATE 1****
[Certificate available to web gateway. This certificate is offered to webclients]:
--------------Web gateway certificate----------------------------------------
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4202 (0x106a)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=IN, ST=KA, L=BGL, O=xyz, OU=ABC, CN=<FQDN/IP>
```

```
        Validity
            Not Before: Jun  4 13:55:25 2019 GMT
            Not After : Jun  3 13:55:25 2020 GMT
        Subject: C=IN, ST=KA9, L=BGL9, O=XYZ123, OU=ABC123, CN=<FQDN/IP>
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:bb:52:1e:7f:24:d7:2e:24:62:5a:83:cc:e4:88:
--------------Certificate output is truncated to first 15 lines--------------

****CERTIFICATE 2****
[Certificate available in keystore(jks). CA signed certificate is installed here till DCNM
 version 11.1.x]
If you have upgraded from DCNM version 11.1.x to later version please see installation guide
 to restore
CA signed certificate to upgraded version.
--------------Keystore certificate-----------------------------------------
alias = sme, storepass = <<storepass-pwd>>
Alias name: sme
Creation date: Oct 14, 2018
Entry type: PrivateKeyEntry
Certificate chain length: 2
Certificate[1]:
Owner: CN=localhost, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Issuer: CN=dcnmca, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Serial number: 62044620
Valid from: Sun Oct 14 20:39:39 PDT 2018 until: Fri Oct 13 20:39:39 PDT 2023
Certificate fingerprints:
         MD5:  E5:F8:AD:17:4D:43:2A:C9:EE:35:5F:BE:D8:22:7D:9C
         SHA1: 38:66:F1:CD:10:61:27:E7:43:85:10:41:3D:A3:4B:5C:C9:CC:17:5E
         SHA256:
E0:87:D8:34:71:18:FE:8C:AB:18:0B:D7:85:B1:91:A8:4B:75:A3:91:BA:90:83:46:72:87:FE:FE:FE:04:F0:E1
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
--------------Certificate output is truncated to first 15 lines--------------
dcnm#
```

Note <<*storepass-pwd*>> is the password string generated while installing DCNM Server. This string is located in the `<install dir>/dcm/fm/conf/serverstore.properties` directory. Fetch the **dcnm.fmserver.token** value for the **storepass-pwd**.

The Web UI refers to the **CERTIFICATE 1** after installation. If **CERTIFICATE 1** is not available, you must stop and restart all applications, using the following commands:

Note Ensure that you follow the same sequence of commands on the Cisco DCNM to troubleshoot this scenario.

On the Cisco DCNM Standalone appliance, run the following commands to stop and start all Cisco DCNM applications to troubleshoot **CERTIFICATE 1**:

```
dcnm# appmgr stop all /* stop all the applications running on Cisco DCNM */
dcnm# appmgr start all /* start all the applications running on Cisco DCNM */
```

On the Cisco DCNM Native HA appliance, run the following commands to stop and start all Cisco DCNM applications to troubleshoot CERTIFICATE 1:

For example, let us indicate the Active node as **dcnm1**, and Standby node **dcnm2**.

Stop the applications running on the both the nodes.

```
dcnm2# appmgr stop all /* stop all the applications running on Cisco DCNM Standby Node */
dcnm1# appmgr stop all /* stop all the applications running on Cisco DCNM Active Node */
```

Start the applications on both nodes.

```
dcnm1# appmgr start all /* start all the applications running on Cisco DCNM Active Node*/
dcnm2# appmgr start all /* start all the applications running on Cisco DCNM Standby Node*/
```

Note Ensure that you clear the browser cache before you launch the Cisco DCNM Web UI, using the Management IP Address.

The **CERTIFICATE 1** is displayed in the Security settings on the browser.

Installing a CA Signed Certificate

We recommend that you install a CA Signed certificate as a standard security practice. The CA Signed certificates are recognized, and verified by the browser. You can also verify the CA Signed certificate manually.

Note The Certificate Authority can be an Enterprise Signing Authority, also.

Installing a CA Signed Certificate on Cisco DCNM Standalone Setup

To install a CA Signed certificate on the Cisco DCNM, perform the following steps.

Procedure

Step 1 Logon to the DCNM server via SSH terminal.

Step 2 Generate a CSR on the Cisco DCNM server using the **appmgr afw gen-csr** command:

Note
CSR is unique to a Cisco DCNM, and only a corresponding CSR signed certificate must be installed on a given Cisco DCNM.

```
dcnm# appmgr afw gen-csr
Generating CSR....
..
...
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:CA
Locality Name (eg, city) [Default City]:San Jose
Organization Name (eg, company) [Default Company Ltd]:Cisco
Organizational Unit Name (eg, section) []:DCBG
Common Name (eg, your name or your server's hostname) []:dcnmhost.cisco.com
Email Address []:dcnm@cisco.com

Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []: /* This field is not mandatory */
```

```
An optional company name []: /* This field is not mandatory */
...
```

A CSR file `dcnmweb.csr` is created in the `/var/tmp/` directory.

```
********** CA certificate installation not completed yet. Please do followings. **********
CSR is generated and placed at /var/tmp/dcnmweb.csr.
Please download or copy the content to your certificate signing server.
```

Step 3 Send this CSR to your Certificate signing server.

Note
The CA Signing server is local to your organization.

Step 4 Get the certificate signed by your Certificate Authority.

The Certificate Authority (CA) returns 3 certificates, namely, Primary, Intermediate (also known as Issuing/Subordinate), and Root certificates. Combine all the three certificates into one `.pem` file to import to DCNM.

Step 5 Copy the new CA Signed certificate to Cisco DCNM server.

Ensure that the certificate is located at `/var/tmp` directory on the Cisco DCNM Server.

Step 6 Install the CA Signed certificate on the Cisco DCNM by using the following commands:

Note
We recommend that you run the following commands in the same sequence as shown below.

```
dcnm# appmgr stop all /* Stop all applications running on Cisco DCNM
dcnm# appmgr afw install-CA-signed-cert <CA-signed certificate directory>
/* CA-signed certificate with full or relative path */
Making the signed certificate available to web gateway....

CA signed certificate CA-signed-cert.pem is installed. Please start all applications as
followings:
On standalone setup execute: 'appmgr start all'
```

Step 7 Restart all applications with the new certificate on Cisco DCNM using the **appmgr start all** command.

```
dcnm# appmgr start all
```

Step 8 Verify the newly installed CA Signed certificate using the **appmgr afw show-cert-details** command.

The system is now armed with the CA Signed certificate, which is verified at the browser.

Note
CSR is unique to a Cisco DCNM, and only a corresponding CSR signed certificate must be installed on a given Cisco DCNM.

Installing a CA Signed Certificate on Cisco DCNM Native HA setup

To install a CA Signed certificate on the Cisco DCNM, perform the following steps.



Note We recommend that you run the following commands in the same sequence as shown below.

Procedure

Step 1 On the Active node, logon to the DCNM server via SSH terminal.

Note
For example, let us indicate the Cisco DCNM Active and Standby appliances as **dcnm1** and **dcnm2** respectively.

Step 2 Generate a CSR on the Cisco DCNM server using the **appmgr afw gen-csr** command:

Note
CSR is unique to a Cisco DCNM, and only a corresponding CSR signed certificate must be installed on a given Cisco DCNM.

```
dcnm1# appmgr afw gen-csr
Generating CSR....
..
...
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:CA
Locality Name (eg, city) [Default City]:San Jose
Organization Name (eg, company) [Default Company Ltd]:Cisco
Organizational Unit Name (eg, section) []:DCBG
Common Name (eg, your name or your server's hostname) []:dcnmhost.cisco.com
/* Provide a VIP FQDN name of the eth0 interface*/
Email Address []:dcnm@cisco.com

Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password []: /* This field is not mandatory */
An optional company name []: /* This field is not mandatory */
...
```

Note
For generating CSR on the Active node, we recommend that you provide a VIP FQDN name of eth0 interface, when for prompted for Common Name.

This FQDN must be the web server address that you enter on the browser to launch the Cisco DCNM Web UI.

A CSR file `dcnmweb.csr` is created in the `/var/tmp/` directory.

```
********** CA certificate installation not completed yet. Please do followings. **********
CSR is generated and placed at /var/tmp/dcnmweb.csr.
Please download or copy the content to your certificate signing server.
```

Step 3 Send this CSR to your Certificate signing server.

Note
The CA Signing server is local to your organization.

The CA Signing server can be the CA certificate signing authority in your organizations, or your local CA to your organization.

Step 4 Get the certificate signed by your Certificate Authority.

Step 5 Copy the new CA Signed certificate to Cisco DCNM server.

Ensure that the certificate is located at `/var/tmp` directory on the Cisco DCNM Server.

Step 6 On the Standby node, logon to the DCNM server via SSH terminal.

Step 7 Stop all the applications on the Standby node using the **appmgr stop all** command.

```
dcnm2# appmgr stop all /* Stop all applications running on Cisco DCNM Standby Node
dcnm2#
```

Step 8 On the Active node, stop all the applications by using the **appmgr stop all** command.

```
dcnm1# appmgr stop all /* Stop all applications running on Cisco DCNM Active Node
dcnm2#
```

Step 9 On the Active node, install the CA Signed certificate on the Cisco DCNM by using the **appmgr afw install-CA-signed-cert** command.

```
dcnm1# appmgr afw install-CA-signed-cert <CA-signed certificate directory>
/* CA-signed certificate with full or relative path */
Making the signed certificate available to web gateway....

CA signed certificate CA-signed-cert.pem is installed. Please start all applications as
followings:
On standalone setup execute: 'appmgr start all'
```

Step 10 On the Active node, restart all applications with the new certificate on Cisco DCNM using the **appmgr start all** command.

```
dcnm1# appmgr start all  /* Start all applications running on Cisco DCNM Active Node
```

Ensure that all services on Cisco DCNM Active node is operational before you proceed further.

Note
Logon to the Cisco DCNM Web UI and check if the Certificate details are correct.

Step 11 On the Standby node, restart all applications with the new certificate on Cisco DCNM using the **appmgr start all** command.

```
dcnm2# appmgr start all  /* Start all applications running on Cisco DCNM Standby Node
```

This will ensure that the Standby node makes a fresh peer relationship with the Active Node. Therefore, the newly installed CA Signed certificate on the Active node will be synchronized on the Standby node.

Step 12 Verify the newly installed CA Signed certificate using the **appmgr afw show-cert-details** command, on both Active and Standby nodes.

The system is now armed with the CA Signed certificate, which is verified at the browser.

Note
If the Certificates information is not displayed, we recommend that you wait for a few minutes. The Secondary node takes a while to synchronize with the Active node.

If you want to retain the same internal and CA Signed certificate on both peers on a Native HA setup, first install the certificates on the Active node. After installing certificates on the Active node, export the certificates from Active node and import the same certificates to the Standby node.

Exporting certificate from Active Node to Standby Node

The following procedure applies to the Cisco DCNM Native HA setup only. The CA Signed certificate installed on the Active node is always synced to the Standby node. However, the internal certificate differs on both

Active and Standby nodes. If you want to keep the same set of certificates on both peers, you must perform the procedure described in this section.



Note You may choose not to export any certificates, because the internal certificates are internal to the system. These certificates can differ on Active and Standby nodes without having any functional impact.

To export the CA Signed certificate from Active node and import the certificate to the Standby node, perform the following procedure.

Procedure

Step 1 On the Active node, logon to the DCNM server via SSH terminal.

Step 2 Create a certificate bundle, by using the **appmgr afw export-import-cert-ha-peer export** command.

```
dcnm1# appmgr afw export-import-cert-ha-peer export
```

Step 3 Copy the certificate bundle to the Standby node.

Note
Ensure that you copy the certificate on the Standby node to the location as specified on the SSH terminal.

Step 4 On the Standby node, stop all the applications by using the **appmgr stop all** command.

```
dcnm2# appmgr stop all /* Stop all applications running on Cisco DCNM Standby Node
dcnm2#
```

Step 5 Import the certificates to the Standby node by using the **appmgr afw export-import-cert-ha-peer import** command.

The certificates bundle is imported and installed on the Standby node.

Step 6

Step 7 On the Standby node, restart all applications with the new certificate on Cisco DCNM using the **appmgr start all** command.

```
dcnm2# appmgr start all  /* Start all applications running on Cisco DCNM Standby Node
```

This ensures that the new imported certificate are effective when applications are started on the Standby node.

Step 8 On the Standby node, verify the newly imported CA Signed certificate using the **appmgr afw show-cert-details** command.

The system is now armed with same certificates on both Active and Standby nodes.

Restoring the certificates after an upgrade

This mechanism applies to Cisco DCNM Upgrade procedure using the inline upgrade process only. This procedure is not required for the backup and restore of data on the same version of the Cisco DCNM appliance.

Note that certificate restore is a disruptive mechanism; it requires you to stop and restart applications. Restore must performed only when the upgraded system is stable, that is, you must be able to login to Cisco DCNM Web UI. On a Cisco DCNM Native HA setup, both the Active and Standby nodes must have established peer relationship.



Note A certificate needs to be restored only in following situations:

- if a CA signed certificate was installed on the system before upgrade, and,
- if you're upgrading from a version prior to 11.2(1) to version 11.2(1) or later.

After upgrading the Cisco DCNM, you must always verify the certificate before restoring to check if **CERTIFICATE 1** is the CA signed certificate. You must restore the certificates, if otherwise.

Verify the certificates using the **appmgr afw show-cert-details** as shown in the sample output below.

```
dcnm# appmgr afw show-cert-details
****CERTIFICATE 1****
[Certificate available to web gateway. This certificate is offered to webclients]:
--------------Web gateway certificate--------------------------------
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1575924977762797464 (0x15decf6aec378798)
    Signature Algorithm: sha256WithRSAEncryption
       Issuer: C=US, ST=CA, L=San Jose, O=Enterprise CA inc, OU=Data Center, CN=dcnm1.ca.com

        Validity
            Not Before: Dec  9 20:56:17 2019 GMT
            Not After : Dec  9 20:56:17 2024 GMT
        Subject: C=US, ST=CA, L=San Jose, O= Enterprise CA inc, OU=Data Center,
CN=dcnm1.ca.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:cf:6e:cd:c6:a9:30:08:df:92:98:38:49:9c:2a:
--------------Certificate output is truncated to first 15 lines--------------

****CERTIFICATE 2****
[Certificate available in keystore(jks). CA signed certificate is installed here till DCNM
 version 11.1.x]
If you have upgraded from DCNM version 11.1.x to later version please see installation guide
 to restore
CA signed certificate to upgraded version.
--------------Keystore certificate-----------------------------------------
Alias name: sme
Creation date: Oct 14, 2018
Entry type: PrivateKeyEntry
Certificate chain length: 2
Certificate[1]:
Owner: CN=localhost, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Issuer: CN=dcnmca, OU=Data Center, O=Cisco Systems Inc, L=San Jose, ST=CA, C=US
Serial number: 62044620
Valid from: Sun Oct 14 20:39:39 PDT 2018 until: Fri Oct 13 20:39:39 PDT 2023
Certificate fingerprints:
  SHA1: 38:66:F1:CD:10:61:27:E7:43:85:10:41:3D:A3:4B:5C:C9:CC:17:5E
  SHA256:
E0:87:D8:34:71:18:FE:8C:AB:18:0B:D7:85:B1:91:A8:4B:75:A3:91:BA:90:83:46:72:87:FE:FE:FE:04:F0:E1
Signature algorithm name: SHA256withRSA
```

```
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3
--------------Certificate output is truncated to first 15 lines------
dcnm#
```

Restoring Certificates on Cisco DCNM Standalone setup after Upgrade

To restore the certificates after you upgrade the Cisco DCNM Standalone deployment to Release , perform the following:

Procedure

Step 1

Note
When you upgrade to Release , a backup of the CA Signed certificate is created.

After you have successfully upgraded the Cisco DCNM Standalone appliance, logon to the DCNM server via SSH.

Step 2 Stop all the applications using the following command:

appmgr stop all

Step 3 Restore the certificate by using the following command:

appmgr afw restore-CA-signed-cert

Step 4 Enter **yes** to confirm to restore the previously installed certificate.

Step 5 Start all the applications using the following command:

appmgr start all

Step 6 Verify the newly installed CA Signed certificate using the **appmgr afw show-cert-details** command.

The system is now armed with the CA Signed certificate, which is verified at the browser.

Restoring Certificates on Cisco DCNM Native HA setup after Upgrade

In a Cisco DCNM Native HA setup, the certificate is installed on both the Active and Standby nodes. You must restore the certificate only on the Active node. The certificate will synchronize with the Standby node automatically.

To restore the certificates after you upgrade the Cisco DCNM Standalone deployment to Release , perform the following:

Procedure

Step 1 Logon to the Cisco DCNM server via SSH.

Note
For example, let us indicate Active and Standby appliances as **dcnm1** and **dcnm2** respectively.

Step 2 On the Standby node, stop all the applications using the **appmgr stop all** command.

```
dcnm2# appmgr stop all /* Stop all applications running on Cisco DCNM Standby Node
```

Step 3 On the Active node, stop all the applications using the **appmgr stop all** command.

```
dcnm1# appmgr stop all /* Stop all applications running on Cisco DCNM Active Node
```

Step 4 Restore the certificate on the Active node by using the **appmgr afw restore-CA-signed-cert** command.

```
dcnm1# appmgr afw restore-CA-signed-cert
```

Step 5 Enter **yes** to confirm to restore the previously installed certificate.

Step 6 On the Active node, start all the applications using the **appmgr start all** command.

```
dcnm1# appmgr start all /* Start all applications running on Cisco DCNM Active Node
```

Ensure that all services on Cisco DCNM Active node is operational before you proceed further.

Note
Logon to the Cisco DCNM Web UI and check if the Certificate details are correct.

Step 7 On the Standby node, start all the applications using the **appmgr start all** command.

```
dcnm2# appmgr start all  /* Start all applications running on Cisco DCNM Standby Node
```

Wait for some time, while the Standby node synchronizes with the Active node.

Step 8 Verify the newly installed CA Signed certificate using the **appmgr afw show-cert-details** command, on both Active and Standby nodes.

The system is now armed with the CA Signed certificate, which is verified at the browser.

Recovering and Restoring Previously Installed CA Signed Certificates

Installing, restoring, managing CA signed certificate is a time-consuming process as a third-party signing server is involved. This may also lead to omissions or mistakes which can result in installing wrong certificates. In such a scenario, we recommend that you restore the certificates that were installed prior to the latest install or upgrade.

To recover and restore the previously installed CA signed certificates, perform the following steps.

Procedure

Step 1 Logon to the DCNM server via SSH terminal.

Step 2 Navigate to the `/var/lib/dcnm/afw/apigateway/` directory.

```
dcnm# cd /var/lib/dcnm/afw/apigateway/
dcnm# ls -ltr /* View the contents of the folder
total 128
-rw------- 1 root root 1844 Nov 18 13:14 dcnmweb.key.2019-11-20T132939-08:00
-rw-r--r-- 1 root root 1532 Nov 18 13:14 dcnmweb.crt.2019-11-20T132939-08:00
-rw------- 1 root root 1844 Nov 20 10:15 dcnmweb.key.2019-11-20T132950-08:00
-rw-r--r-- 1 root root 1532 Nov 20 10:15 dcnmweb.crt.2019-11-20T132950-08:00
-rw------- 1 root root 1844 Dec 22 13:59 dcnmweb.key
```

```
-rw-r--r-- 1 root root 1532 Dec 22 13:59 dcnmweb.crt

.
..
...
```

dcnmweb.key and **dcnmweb.crt** are the key and certificate files that are installed on the system, currently. Similar filenames, with timestamp suffix, help you in identifying the key and certificate pairs installed prior to the recent upgrade or restore.

Step 3 Stop all applications running on Cisco DCNM using **appmgr stop all** command.

Step 4 Take a backup of `dcnmweb.key` and `dcnmweb.crt` files.

Step 5 Identify the older key and certificate pair that you want to restore.

Step 6 Copy the key and certificate pair as **dcnmweb.key** and **dcnmweb.crt** (without timestamp suffix).

Step 7 Start all applications running on Cisco DCNM using **appmgr start all** command.

Step 8 Verify the details of the certificate using the **appmgr afw show-cert-details** command. CERTIFICATE 1 is the CA signed certificate.

Note
If the CA signed certificate is not visible to Cisco DCNM Web UI, or if the DCNM Server sends any failure message, you must reboot the system.

Verifying the installed certificate

While the installed certificate can be verified using the **appmgr afw show-cert-details** command, the web browser verifies if the certificate is effective or not. Cisco DCNM supports all standard browsers (Chrome, IE, Safari, Firefox). However, each browser display the certificate information differently.

We recommend that you refer to the browser specific information on that browser provider website.

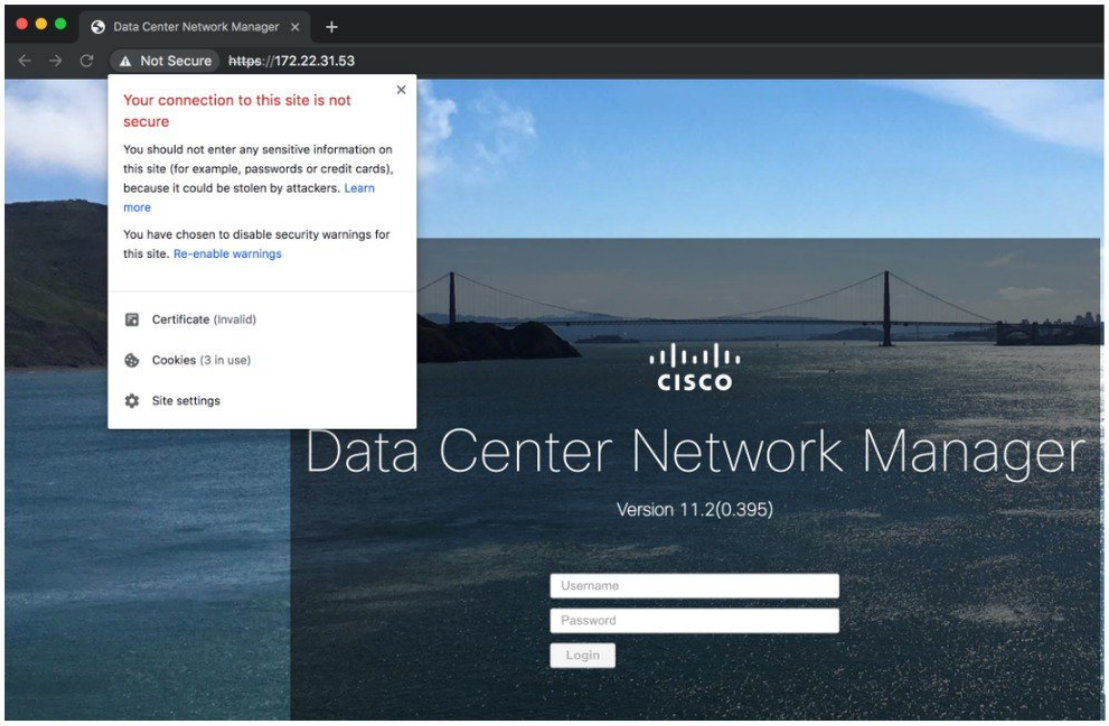
The following snippet is a sample from the Chrome Browser, Version 74.0.3729.169, to verify the certificate.

1. Enter URL **https://<dcnm-ip-address>** or **https://<FQDN>** in the address bar on the browser.

   Press the **Return** key.

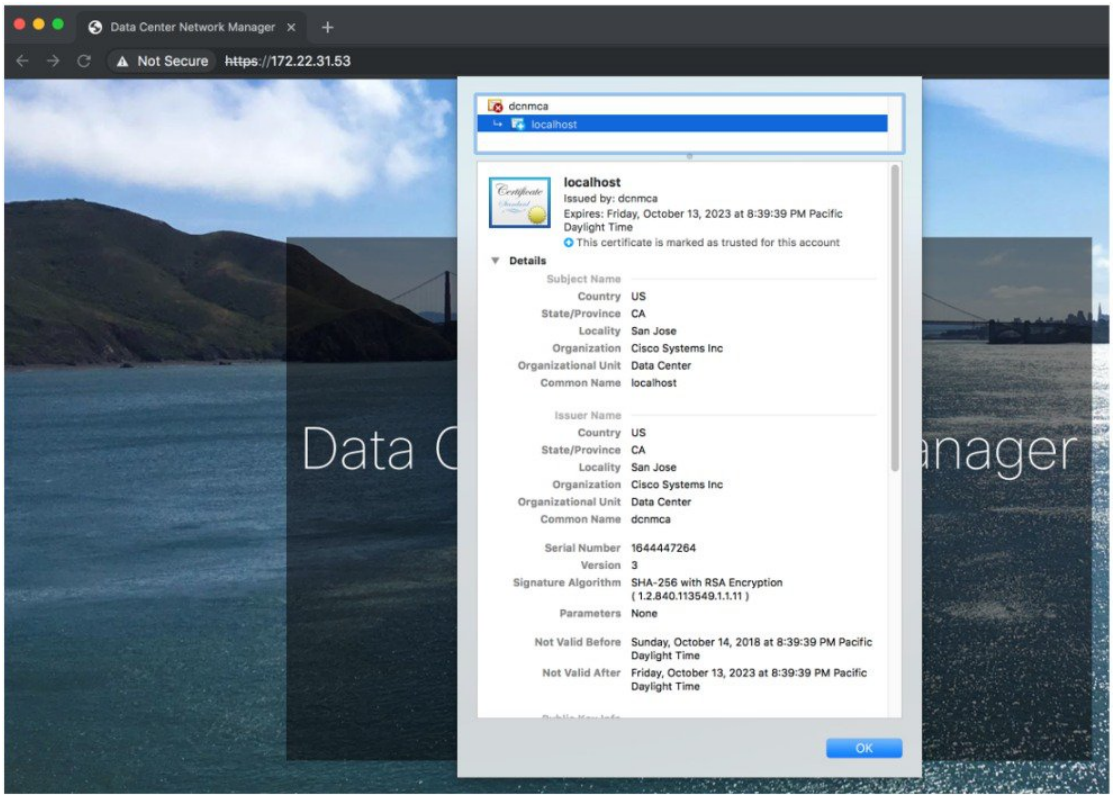
2. Based on the type of certificate, the icon on the left of the URL field shows a lock icon [ ] or an alert icon [ ].

   Click on the icon.

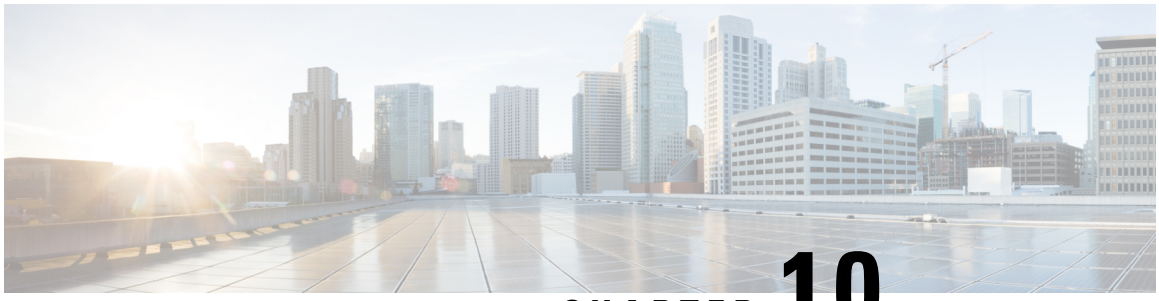


3. On the card, click **Certificate** field.

   The information in the certificate is displayed.



The information that is displayed must match with the details as displayed on CERTIFICATE 1 when you view the certificate details using the **appmgr afw show-cert-details**.



CHAPTER 10

Running Cisco DCNM Behind a Firewall

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

- Running Cisco DCNM Behind a Firewall, on page 139
- Configuring Custom Firewalls, on page 141

Running Cisco DCNM Behind a Firewall

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

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

Note When you add or discover LAN devices in DCNM, java is used as a part of the discovery process. If firewall blocks the process then it uses TCP connection port 7 as a discovery process. Ensure that the **cdp.discoverPingDisable** server property is set to **true**. Choose **Web UI > Administration > DCNM Server > Server Properties** to set the server property.

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.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
2443	TCP	HTTPS	Client to DCNM Server	Required during installation, to reach the server. DCNM closes this port after installation completes.

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	UDP	DHCP	Device to DCNM Server	
69	TCP	TFTP	Device to DCNM Server	Required for POAP
161	TCP/UDP	SNMP	Server to DCNM Device	DCNM configured via `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

Configuring Custom Firewalls



Note This is applicable for DCNM OVA/ISO deployments only.

Cisco DCNM Server deploys a set of IPTables rules, known as DCNM Local Firewall. These rules open TCP/UDP ports that are required for Cisco DCNM operations. You can't manipulate the built-in Local Firewall without accessing the OS interface, through SSH, and change the rules. Don't change the Firewall rules, as it may become vulnerable to attacks, or impact the normal functioning of DCNM.

To cater to a given deployment or a network, Cisco DCNM allows you to configure your own firewall rules, from Release 11.3(1), using CLIs.

Note These rules can be broad or granular, and supersedes the built-in Local Firewall rules. Therefore, configure these rules carefully, during a maintenance period.

You don't need to stop or restart DCNM server or applications to configure custom firewalls.

Caution IPTable prioritizes the rules in the order that they are configured. Therefore, more granular rules must be installed in the beginning. To ensure that the order of the rules is as required, you can create all rules in a text editor, and then execute the CLIs in the desired order. If rules need to be adjusted, you can flush all rules and configure the rules in the desired order.

You can perform the following operations on the Custom Firewalls.

Note Run all the commands on the Cisco DCNM server using SSH.

Custom Firewall CLI

View the custom firewall CLI chain help and examples using the **appmgr user-firewall** command.

```
dcnm# appmgr user-firewall
dcnm# appmgr user-firewall – h
```

Configure Rules for Custom Firewall

Configure the custom firewall rules using the **appmgr user-firewall {add | del}** command.

```
appmgr user-firewall {add|del} proto {tcp|udp} port {<port><port range n1:n2>}
[{in|out} <interface name>] [srcip <ip-address> [/<mask>]] [dstip <ip-address> [/<mask>]]
action {permit|deny}
```

Note The custom firewall rules supersede the local Firewall rules. Therefore, be cautious and ensure that the functionalities aren't broken.

Example: Sample Custom Firewall Rules

- `dcnm# appmgr user-firewall add proto tcp port 7777 action deny`

  This rule drops all TCP port 7777 traffic on all interfaces.

- `dcnm# appmgr user-firewall add proto tcp port 443 in eth1 action deny`

  This rule drops all TCP port 443 incoming traffic on interface eth1.

- `dcnm# appmgr user-firewall add proto tcp port 7000:7050 srcip 1.2.3.4 action deny`

  This rule drops TCP port range 10000-10099 traffic coming from IP address 1.2.3.4.

Preserving Custom Firewall Rules

Preserve the custom firewall rules across reboots, using the **appmgr user-firewall commit** command.



Note Each time you modify the rules, you must execute this command to preserve the rules across reboots.

Installing Custom Firewall Rules on Native HA Standby Node

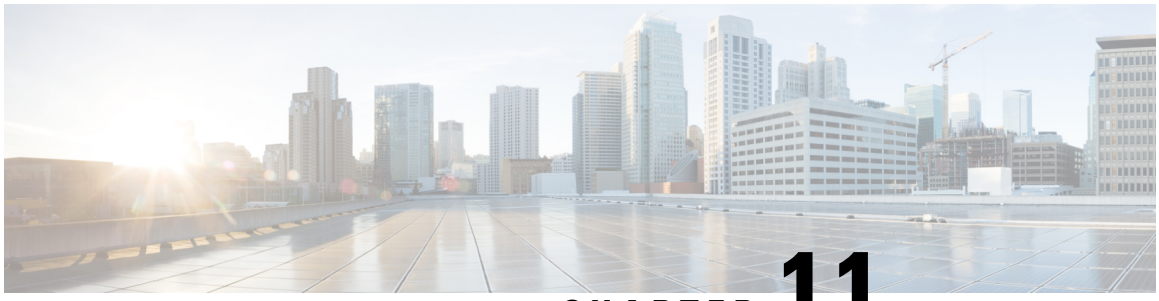
In a Cisco DCNM Native HA setup, when you execute the **appmgr user-firewall commit** on the Active node, the rules are synchronized to the Standby node automatically. However, the new rules are operational only after a system reboot.

To apply the rules immediately, install the custom firewall rules on Standby node using the **appmgr user-firewall user-policy-install** command.

Deleting Custom Firewalls

Delete all the custom firewalls using the **appmgr user-firewall flush-all** command.

To delete the custom firewalls permanently, use the **appmgr user-firewall commit** command.



CHAPTER 11

Secure Client Communications for Cisco DCNM Servers

• Secure Client Communications for Cisco DCNM Servers, on page 145

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

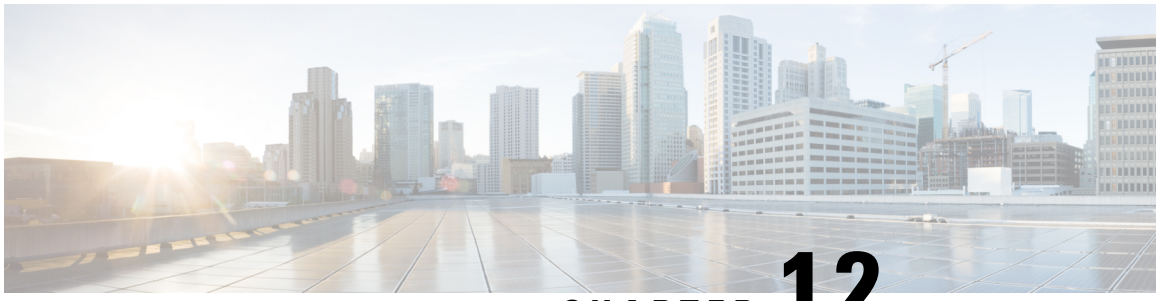
`<DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks.old`

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 12

Managing Applications in a High-Availability Environment

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

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

This chapter contains the following sections:

- Information About Application Level HA in the Cisco DCNM Open Virtual Appliance, on page 147
- Native HA Failover and Troubleshooting, on page 148
- Application High Availability Details, on page 150

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

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

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

In this scenario:

1. All applications run on both appliances.

   The application data is either constantly synchronized or applications share a common database as applicable.

2. Only one of the applications running on the two appliances serves the client requests. Initially this would be the applications running on OVA-A. The application continues to do so until one of the following happens:

- The application on OVA-A crashes.
- The operating system on OVA-A crashes.
- OVA-A is powered off for some reason.

3. At this point, the application running on the other appliance (OVA-B) takes over.

   For DHCP, when the first node fails, the second node starts serving the IP addresses.

4. The existing connections to OVA-A are dropped and the new connections are routed to OVA-B.

   This scenario demonstrates why one of the nodes (OVA-A) is initially referred to as the Active node and OVA-B is referred as the Standby node.

Automatic Failover

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

- If any of the applications managed by the load-balancing software (DCNM/AMQP) goes down on OVA-A, the Active node that handles the client requests detects the failure and redirects subsequent requests to the Standby node (OVA-B). This process provides an application-level switchover.
- If the Active node (OVA-A) fails or is powered-off for some reason, the Standby node (OVA-B) detects the failure and enables the VIP address for Cisco 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 148; subsequent requests to the AMQP Virtual IP address are redirected to OVA-B.

Native HA Failover and Troubleshooting

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

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

Native HA Failover from Active Host to Standby Host

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

1. Log on to 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 the OVA management network
Repositories	—	—	External repositories have to be used

Data Center Network Management

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



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.

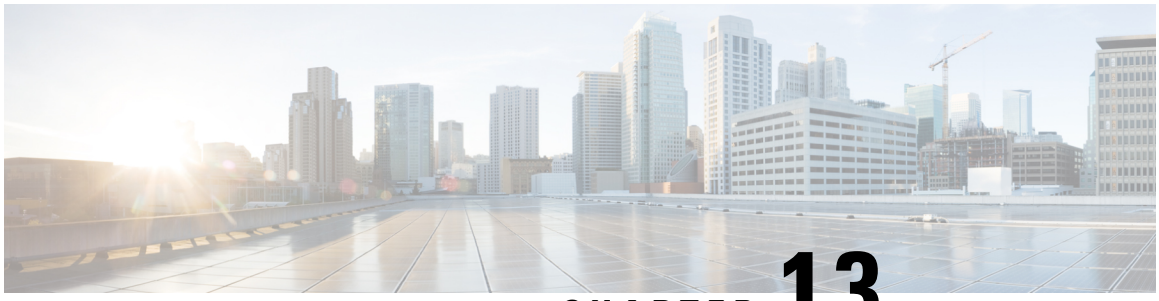
Virtual-IP Failbacks

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 13

Managing Utility Services After DCNM Deployment

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

Table 8: Cisco DCNM Utility Services

Category	Application	Username	Password	Protocol Implemented
Network Management	Data Center Network Manager	admin	User choice [3]	Network Management

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

This chapter contains the following sections:

- Editing Network Properties Post DCNM Installation, on page 155
- Convert Standalone Setup to Native-HA Setup, on page 177
- Utility Services Details, on page 181
- Managing Applications and Utility Services , on page 183
- Updating the SFTP Server Address for IPv6, on page 185

Editing Network Properties Post DCNM Installation

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

- dcnm-mgmt network (eth0) interface

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

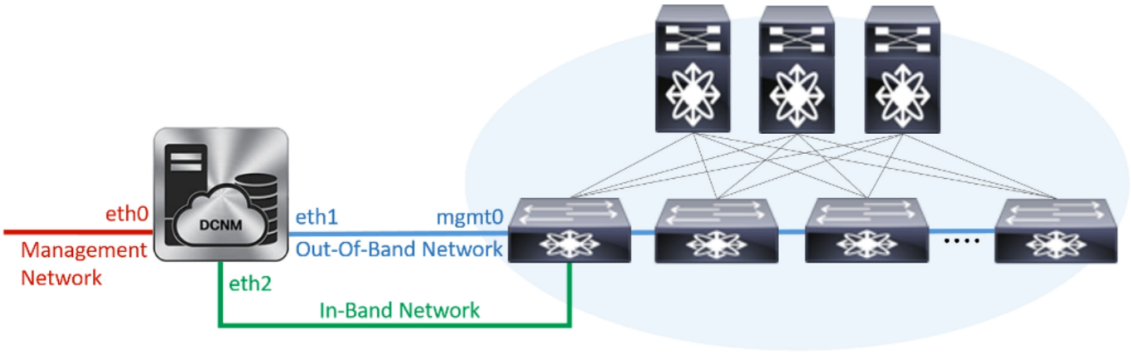
- enhanced-fabric-mgmt (eth1) interface

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

- enhanced-fabric-inband (eth2) interface

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

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



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

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

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

Modifying Network Interfaces (eth0 and eth1) Post DCNM Installation

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

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

- Modifying Network Properties on DCNM in Standalone Mode, on page 156

  Sample Command Output for Modifying Network Parameters in the Cisco DCNM Standalone Setup, on page 157

- Modifying Network Properties on DCNM in Native HA Mode, on page 158

  Sample Command Output for Modifying Network Parameters in the Cisco DCNM Native HA Setup, on page 160

Modifying Network Properties on DCNM in Standalone Mode

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

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

1. Initiate a session on the console, using the following command:

   appmgr update network-properties session start

2. Update the Network Properties using the following command:

   appmgr update network-properties set ipv4 {eth0|eth1}*<ipv4-address> <network-mask> <gateway>*

   Enter the new IPv4 address for the Management (eth0) interface, along with the subnet mask and gateway IP addresses.

3. View and verify the changes by using the following command:

   appmgr update network-properties session show {config | changes | diffs}

4. After you validate the changes, apply the configuration using the following command:

   appmgr update network-properties session apply

   Wait for a few minutes before you can logon to the Cisco DCNM Web UI using the eth0 Management Network IP address.

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

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

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

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

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

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

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

            PLEASE STOP ALL APPLICATIONS MANUALLY
**********************************************************************

Have applications been stopped? [y/n]: y
Applying changes
DELETE 1
Node left the swarm.
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
log4j:WARN No appenders could be found for logger (fms.db).
```

```
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
UPDATE 1
UPDATE 1
DELETE 1
server signaled
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the
 'tentative' state
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the
 'tentative' state
**********************************************************************
Please run 'appmgr start afw; appmgr start all' to restart your nodes.
**********************************************************************

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

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

Modifying Network Properties on DCNM in Native HA Mode

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

Note

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

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

   appmgr stop all

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

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

   appmgr stop all

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

   appmgr update network-properties session start

4. On the Active node, modify the network interface parameters by using the following commands:

   a. Configure the IP address for eth0 and eth1 address by using the following command:

appmgr update network-properties set ipv4 {eth0|eth1}*<ipv4-address> <network-mask> <gateway>*

Enter the new IPv4 or IPv6 address for the eth1 interface, along with the subnet mask and gateway IP addresses.

b. Configure the VIP IP address by using the following command:

appmgr update network-properties set ipv4 {vip0|vip1}*<ipv4-address> <network-mask>*

Enter the vip0 address for eth0 interface. Enter the vip1 address for eth1 interface.

c. Configure the peer IP address by using the following command:

appmgr update network-properties set ipv4 {peer0|peer1}*<ipv4-address>*

Enter the eth0 address of the Standby node as peer0 address for Active node. Enter the eth1 address of the Standby node as peer1 address for Active node.

d. View and validate the changes that you have made to the network parameters by using the following command:

appmgr update network-properties session show{*config* | *changes* | *diffs*}

View the changes that you have configured by using the following command:

5. On the Standby node, modify the network interface parameters using the commands described in Step 4.
6. After you validate the changes, apply the configuration on the Active node by using the following command:

   appmgr update network-properties session apply

   Wait until the prompt returns, to confirm that the network parameters are updated.
7. After you validate the changes, apply the configuration on the Standby node by using the following command:

   appmgr update network-properties session apply
8. Start all the applications on the Active node by using the following command:

   appmgr start all

Note Wait until all the applications are running successfully on the Active node, before proceeding to the next step.

9. Start all the applications on the Standby node by using the following command:

   appmgr start all
10. Establish peer trust key on the Active node by using the following command:

    appmgr update ssh-peer-trust
11. Establish peer trust key on the Standby node by using the following command:

    appmgr update ssh-peer-trust

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

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



Note For example, let us indicate Active and Standby appliances as **dcnm1** and **dcnm2** respectively.

```
[root@dcnm2]# appmgr stop all
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.

Stopping and halting node rabbit@dcnm2 ...
Note: Forwarding request to 'systemctl enable rabbitmq-server.service'.
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
[root@dcnm2]#

[root@dcnm1]# appmgr stop all
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.

Stopping and halting node rabbit@dcnm1 ...
Note: Forwarding request to 'systemctl enable rabbitmq-server.service'.
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
[root@dcnm1]#

[root@dcnm1]# appmgr update network-properties session start
[root@dcnm2]# appmgr update network-properties session start

[root@dcnm1]# appmgr update network-properties set ipv4 eth0 172.28.10.244 255.255.255.0
172.28.10.1
[root@dcnm1]# appmgr update network-properties set ipv4 eth1 100.0.0.244 255.0.0.0
****************************************************************
 WARNING: fabric/poap configuration may need to be changed
 manually after changes are applied.
****************************************************************
[root@dcnm1]# appmgr update network-properties set ipv4 vip0 172.28.10.238 255.255.255.0
[root@dcnm1]# appmgr update network-properties set ipv4 vip1 100.0.0.238 255.0.0.0
[root@dcnm1]# appmgr update network-properties set ipv4 peer0 172.28.10.245
[root@dcnm1]# appmgr update network-properties set ipv4 peer1 100.0.0.245
[root@dcnm1]# appmgr update network-properties session show changes

[root@dcnm2]# appmgr update network-properties set ipv4 eth0 172.28.10.245 255.255.255.0
172.28.10.1
[root@dcnm2]# appmgr update network-properties set ipv4 eth1 100.0.0.245 255.0.0.0
****************************************************************
 WARNING: fabric/poap configuration may need to be changed
 manually after changes are applied.
```

```
**************************************************************
[root@dcnm2]# appmgr update network-properties set ipv4 vip0 172.28.10.238 255.255.255.0
[root@dcnm2]# appmgr update network-properties set ipv4 vip1 100.0.0.238 255.0.0.0
[root@dcnm2]# appmgr update network-properties set ipv4 peer0 172.28.10.244
[root@dcnm2]# appmgr update network-properties set ipv4 peer1 100.0.0.244
[root@dcnm2]# appmgr update network-properties session show changes

[root@dcnm1]# appmgr update network-properties session show changes
eth0 IPv4 addr  172.28.10.246/255.255.255.0  ->  172.28.10.244/255.255.255.0
eth1 IPv4 addr  1.0.0.246/255.0.0.0          ->  100.0.0.244/255.0.0.0
eth0 VIP        172.28.10.248/24             ->  172.28.10.238/24
eth1 VIP        1.0.0.248/8                  ->  100.0.0.238/8
Peer eth0 IP    172.28.10.247                ->  172.28.10.245
Peer eth1 IP    1.0.0.245                    ->  100.0.0.245

[root@dcnm1]# appmgr update network-properties session show config
======= Current configuration ======
NTP Server      1.ntp.esl.cisco.com
eth0 IPv4 addr  172.28.10.246/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 DNS        171.70.168.183
eth0 IPv6 addr  2001:420:284:2004:4:112:210:20/112
eth0 IPv6 GW    2001:420:284:2004:4:112:210:1
eth1 IPv4 addr  1.0.0.246/255.0.0.0
eth1 IPv4 GW
eth1 DNS        1.0.0.246
eth1 IPv6 addr
eth2 IPv4 addr  /
eth2 IPv4 GW
Peer eth0 IP    172.28.10.247
Peer eth1 IP    1.0.0.247
Peer eth2 IP
eth0 VIP        172.28.10.248/24
eth1 VIP        1.0.0.248/8
eth2 VIP        /
eth0 VIPv6      /
eth1 VIPv6      /

====== Session configuration ======
NTP Server      1.ntp.esl.cisco.com
eth0 IPv4 addr  172.28.10.244/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 DNS        171.70.168.183
eth0 IPv6 addr  2001:420:284:2004:4:112:210:20/112
eth0 IPv6 GW    2001:420:284:2004:4:112:210:1
eth1 IPv4 addr  100.0.0.244/255.0.0.0
eth1 IPv4 GW
eth1 DNS        1.0.0.246
eth1 IPv6 addr
eth2 IPv4 addr  /
eth2 IPv4 GW
Peer eth0 IP    172.28.10.245
Peer eth1 IP    100.0.0.245
Peer eth2 IP
eth0 VIP        172.28.10.238/24
eth1 VIP        100.0.0.238/8
eth2 VIP        /
eth0 VIPv6      /
eth1 VIPv6      /
[root@dcnm1]#

[root@dcnm2]# appmgr update network-properties session show config
======= Current configuration ======
NTP Server      1.ntp.esl.cisco.com
```

```
eth0 IPv4 addr  172.28.10.247/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 DNS        171.70.168.183
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr  1.0.0.247/255.0.0.0
eth1 IPv4 GW
eth1 DNS        1.0.0.247
eth1 IPv6 addr
eth2 IPv4 addr  /
eth2 IPv4 GW
Peer eth0 IP    172.28.10.246
Peer eth1 IP    1.0.0.246
Peer eth2 IP
eth0 VIP        172.28.10.248/24
eth1 VIP        1.0.0.248/8
eth2 VIP        /
eth0 VIPv6      /
eth1 VIPv6      /

====== Session configuration ======
NTP Server      1.ntp.esl.cisco.com
eth0 IPv4 addr  172.28.10.245/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 DNS        171.70.168.183
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr  100.0.0.245/255.0.0.0
eth1 IPv4 GW
eth1 DNS        1.0.0.247
eth1 IPv6 addr
eth2 IPv4 addr  /
eth2 IPv4 GW
Peer eth0 IP    172.28.10.244
Peer eth1 IP    100.0.0.244
Peer eth2 IP
eth0 VIP        172.28.10.238/24
eth1 VIP        100.0.0.238/8
eth2 VIP        /
eth0 VIPv6      /
eth1 VIPv6      /
[root@dcnm2]#

[root@dcnm1]# appmgr update network-properties session apply
**********************************************************************
                          WARNING

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

            PLEASE STOP ALL APPLICATIONS MANUALLY
**********************************************************************

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

```
server signaled
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the
 'tentative' state
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the
 'tentative' state
**********************************************************************
Please run 'appmgr start afw; appmgr start all' to restart your nodes.
**********************************************************************
**********************************************************************
Please run 'appmgr update ssh-peer-trust' on the peer node.
**********************************************************************
[root@dcnm1]#

[root@dcnm2]# appmgr update network-properties session apply
**********************************************************************
                          WARNING

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

            PLEASE STOP ALL APPLICATIONS MANUALLY
**********************************************************************

Have applications been stopped? [y/n]: y
Applying changes
DELETE 1
Node left the swarm.
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
log4j:WARN No appenders could be found for logger (fms.db).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
UPDATE 1
UPDATE 1
DELETE 1
afwnetplugin:0.1
server signaled
**********************************************************************
Please run 'appmgr start afw; appmgr start all' to restart your nodes.
**********************************************************************
**********************************************************************
Please run 'appmgr update ssh-peer-trust' on the peer node.
**********************************************************************
[root@dcnm2]#

[root@dcnm1]# appmgr start afw; appmgr start all
Started AFW Server Processes
Started AFW Agent Processes
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO:  Resource is stopped
Done.

Warning: PID file not written; -detached was passed.
AMQP User Check
Started AFW Server Processes
Started AFW Agent Processes
[root@dcnm1]#
```

Wait until dcnm1 becomes active again.

```
[root@dcnm2]# appmgr start afw; appmgr start all
Started AFW Server Processes
```

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

Warning: PID file not written; -detached was passed.
AMQP User Check
Started AFW Server Processes
Started AFW Agent Processes
[root@dcnm2]#

[root@dcnm1]# appmgr update ssh-peer-trust
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -o 'StrictHostKeyChecking=no' '172.28.10.245'"
and check to make sure that only the key(s) you wanted were added.
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -o 'StrictHostKeyChecking=no' '100.0.0.245'"
and check to make sure that only the key(s) you wanted were added.
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1
Now try logging into the machine, with:   "ssh -o 'StrictHostKeyChecking=no'
'dcnm-247.cisco.com'"
and check to make sure that only the key(s) you wanted were added.
[root@dcnm1]#

[root@dcnm2]# appmgr update ssh-peer-trust
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -o 'StrictHostKeyChecking=no' '172.28.10.244'"
and check to make sure that only the key(s) you wanted were added.
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -o 'StrictHostKeyChecking=no' '100.0.0.244'"
and check to make sure that only the key(s) you wanted were added.
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -o 'StrictHostKeyChecking=no'
'dcnm-246.cisco.com'"
and check to make sure that only the key(s) you wanted were added.
[root@dcnm2]#
```

Modifying Network Properties on DCNM in Standalone Mode



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

To change the Network Properties on Cisco DCNM Standalone setup, perform the following steps:

Procedure

Step 1 Initiate a session on the console, using the following command:

appmgr update network-properties session start

Step 2 Update the Network Properties using the following command:

appmgr update network-properties set ipv4 {eth0|eth1|eth2}<*ipv4-address*> <*network-mask*> <*gateway*>

Step 3 View and verify the changes by using the following command:

appmgr update network-properties session show {config | changes | diffs}

Step 4 After you validate the changes, apply the configuration using the following command:

appmgr update network-properties session apply

Wait for a few minutes before you can logon to the Cisco DCNM Web UI using the eth0 Management Network IP address.

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

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

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

dcnm# appmgr update network-properties set ipv4 eth0 172.28.10.244 255.255.255.0 172.28.10.1
dcnm# appmgr update network-properties set ipv4 eth1 100.0.0.244 255.0.0.0
dcnm# appmgr update network-properties set ipv4 eth2 2.0.0.251 255.0.0.0 2.0.0.1
****************************************************************
 WARNING: fabric/poap configuration may need to be changed
 manually after changes are applied.
****************************************************************

dcnm# appmgr update network-properties session show changes
eth0 IPv4 addr  172.28.10.246/255.255.255.0  ->  172.28.10.244/255.255.255.0
eth1 IPv4 addr  1.0.0.246/255.0.0.0          ->  100.0.0.244/255.0.0.0
eth2 IPv4 addr  10.0.0.246/255.0.0.0         ->  2.0.0.251/255.0.0.0 2.0.0.1

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

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

            PLEASE STOP ALL APPLICATIONS MANUALLY
*********************************************************************

Have applications been stopped? [y/n]: y
Applying changes
DELETE 1
Node left the swarm.
```

```
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
log4j:WARN No appenders could be found for logger (fms.db).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
UPDATE 1
UPDATE 1
DELETE 1
server signaled
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the
 'tentative' state
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the
 'tentative' state
**********************************************************************
Please run 'appmgr start afw; appmgr start all' to restart your nodes.
**********************************************************************

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

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

Modifying Network Properties on DCNM in Native HA Mode

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

Ensure that you execute the commands in the same order as mentioned in the following steps.

Note Native HA nodes must be considered as a single entity. When you change the Active node eth1 IP address, you must also change the Standby node eth1 IP address.

When you change the eth0 IP address in any node, you must change the eth2 IP address for that node.

To change the Network Properties on Cisco DCNM Native HA setup, perform the following steps:

Procedure

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

appmgr stop all

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

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

appmgr stop all

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

appmgr update network-properties session start

Step 4 On the Active node, modify the network interface parameters by using the following commands:

a) Configure the IP address for eth0, eth1, and eth2 address by using the following command:

appmgr update network-properties set ipv4 {eth0|eth1|eth2}<*ipv4-address*> <*network-mask*> <*gateway*>

Enter the new IPv4 or IPv6 address for the interface, along with the subnet mask and gateway IP addresses.

b) Configure the VIP IP address by using the following command:

appmgr update network-properties set ipv4 {vip0|vip1|vip2}<*ipv4-address*> <*network-mask*>

Enter the vip0 address for eth0 interface. Enter the vip1 address for eth1 interface. Enter the vip2 address for eth2 interface.

c) Configure the peer IP address by using the following command:

appmgr update network-properties set ipv4 {peer0|peer1|peer2}<*ipv4-address*>

Enter the eth0 address of the Standby node as peer0 address for Active node. Enter the eth1 address of the Standby node as peer1 address for Active node. Enter the eth2 address of the Standby node as peer2 address for Active node.

d) View and validate the changes that you have made to the network parameters by using the following command:

appmgr update network-properties session show{*config* | *changes* | *diffs*}

Step 5 On the Standby node, modify the network interface parameters using the commands described in procedure in Step Step 4, on page 167.

Step 6 After you validate the changes, apply the configuration on the Active node by using the following command:

appmgr update network-properties session apply

Wait until the prompt returns, to confirm that the network parameters are updated.

Step 7 After you validate the changes, apply the configuration on the Standby node by using the following command:

appmgr update network-properties session apply

Step 8 Start all the applications on the Active node by using the following command:

appmgr start all

Note
Wait until all the applications are running successfully on the Active node, before proceeding to the next step.

Step 9 Start all the applications on the Standby node by using the following command:

appmgr start all

Step 10 Establish peer trust key on the Active node by using the following command:

appmgr update ssh-peer-trust

Step 11 Establish peer trust key on the Standby node by using the following command:

appmgr update ssh-peer-trust

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

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



Note For example, let us indicate Active and Standby appliances as **dcnm1** and **dcnm2** respectively.

```
[root@dcnm2 ~]# appmgr stop all
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.
Stopping and halting node rabbit@dcnm-dcnm2 ...
Note: Forwarding request to 'systemctl enable rabbitmq-server.service'.
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
[root@dcnm2 ~]#

[root@dcnm1 ~]# appmgr stop all
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.
Stopping and halting node rabbit@dcnm1 ...
Note: Forwarding request to 'systemctl enable rabbitmq-server.service'.
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
[root@dcnm-1 ~]#

[root@dcnm1 ~]# appmgr update network-properties session start
[root@dcnm1 ~]#

[root@dcnm2 ~]# appmgr update network-properties session start
[root@dcnm2 ~]#

[root@dcnm1 ~]# appmgr update network-properties set ipv4 eth0 172.28.10.244 255.255.255.0
 172.28.10.1
[root@dcnm1 ~]# appmgr update network-properties set ipv4 eth1 1.0.0.244 255.0.0.0 1.0.0.1
**************************************************************
 WARNING: fabric/poap configuration may need to be changed
 manually after changes are applied.
**************************************************************
[root@dcnm1 ~]# appmgr update network-properties set ipv4 eth2 2.0.0.244 255.0.0.0 2.0.0.1
```

```
[root@dcnm1 ~]# appmgr update network-properties set ipv4 peer0 172.29.10.238
[root@dcnm1 ~]# appmgr update network-properties set ipv4 peer1 1.0.0.238
[root@dcnm1 ~]# appmgr update network-properties set ipv4 peer2 2.0.0.238
[root@dcnm1 ~]# appmgr update network-properties set ipv4 vip0 172.28.10.239 255.255.255.0
[root@dcnm1 ~]# appmgr update network-properties set ipv4 vip1 1.0.0.239 255.0.0.0
[root@dcnm1 ~]# appmgr update network-properties set ipv4 vip2 2.0.0.239 255.0.0.0
[root@dcnm1 ~]# appmgr update network-properties set hostname local dcnm3.cisco.com
[root@dcnm1 ~]# appmgr update network-properties set hostname peer dcnm4.cisco.com
[root@dcnm1 ~]# appmgr update network-properties set hostname vip dcnm5.cisco.com
[root@dcnm1 ~]#

[root@dcnm2 ~]# appmgr update network-properties set ipv4 eth0 172.28.10.238 255.255.255.0
 172.28.10.1
[root@dcnm2 ~]# appmgr update network-properties set ipv4 eth1 1.0.0.238 255.0.0.0 1.0.0.1
**************************************************************
 WARNING: fabric/poap configuration may need to be changed
 manually after changes are applied.
**************************************************************
[root@dcnm2 ~]# appmgr update network-properties set ipv4 eth2 2.0.0.238 255.0.0.0 2.0.0.1
[root@dcnm2 ~]# appmgr update network-properties set ipv4 peer0 172.29.10.244
[root@dcnm2 ~]# appmgr update network-properties set ipv4 peer1 1.0.0.244
[root@dcnm2 ~]# appmgr update network-properties set ipv4 peer2 2.0.0.244
[root@dcnm2 ~]# appmgr update network-properties set ipv4 vip0 172.28.10.239 255.255.255.0
[root@dcnm2 ~]# appmgr update network-properties set ipv4 vip1 1.0.0.239 255.0.0.0
[root@dcnm2 ~]# appmgr update network-properties set ipv4 vip2 2.0.0.239 255.0.0.0
[root@dcnm2 ~]# appmgr update network-properties set hostname local dcnm3.cisco.com
[root@dcnm2 ~]# appmgr update network-properties set hostname peer dcnm4.cisco.com
[root@dcnm2 ~]# appmgr update network-properties set hostname vip dcnm5.cisco.com
[root@dcnm2 ~]#

[root@dcnm2 ~]#
[root@dcnm1 ~]# appmgr update network-properties session show changes
eth0 IPv4 addr     172.28.10.246/255.255.255.0    ->    172.28.10.244/255.255.255.0
eth1 IPv4 addr     1.0.0.246/255.0.0.0            ->    1.0.0.244/255.0.0.0
eth1 IPv4 GW                                      ->    1.0.0.1
eth2 IPv4 addr     /                              ->    2.0.0.244/255.0.0.0
eth2 IPv4 GW                                      ->    2.0.0.1
Hostname           dcnm1.cisco.com                ->    dcnm3.cisco.com
eth0 VIP           172.28.10.248/24               ->    172.28.10.239/24
eth1 VIP           1.0.0.248/8                    ->    1.0.0.239/8
eth2 VIP           /                              ->    2.0.0.239/8
Peer eth0 IP       172.28.10.247                  ->    172.29.10.238
Peer eth1 IP       1.0.0.247                      ->    1.0.0.238
Peer eth2 IP                                      ->    2.0.0.238
Peer hostname      dcnm2.cisco.com                ->    dcnm4.cisco.com
VIP hostname       dcnm6.cisco.com                ->    dcnm5.cisco.com

[root@dcnm1 ~]# appmgr update network-properties session show config
======= Current configuration ======
Hostname dcnm1.cisco.com
NTP Server         1.ntp.esl.cisco.com
DNS Server         171.70.168.183,1.0.0.246
eth0 IPv4 addr     172.28.10.246/255.255.255.0
eth0 IPv4 GW       172.28.10.1
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr     1.0.0.246/255.0.0.0
eth1 IPv4 GW
eth1 IPv6 addr
eth1 IPv6 GW
eth2 IPv4 addr     /
eth2 IPv4 GW
eth2 IPv6 addr
```

```
eth2 IPv6 GW
Peer hostname dcnm2.cisco.com
Peer eth0 IP     172.28.10.247
Peer eth1 IP     1.0.0.247
Peer eth2 IP
Peer eth0 IPv6
Peer eth1 IPv6
eth0 VIP         172.28.10.248/24
eth1 VIP         1.0.0.248/8
eth2 VIP         /
eth0 VIPv6       /
eth1 VIPv6       /
VIP hostname dcnm6.cisco.com

====== Session configuration ======
Hostname dcnm3.cisco.com
NTP Server       1.ntp.esl.cisco.com
DNS Server       171.70.168.183,1.0.0.246
eth0 IPv4 addr   172.28.10.244/255.255.255.0
eth0 IPv4 GW     172.28.10.1
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr   1.0.0.244/255.0.0.0
eth1 IPv4 GW     1.0.0.1
eth1 IPv6 addr
eth1 IPv6 GW
eth2 IPv4 addr   2.0.0.244/255.0.0.0
eth2 IPv4 GW     2.0.0.1
eth2 IPv6 addr
eth2 IPv6 GW
Peer hostname     dcnm4.cisco.com
Peer eth0 IP      172.29.10.238
Peer eth1 IP      1.0.0.238
Peer eth2 IP      2.0.0.238
Peer eth0 IPv6
Peer eth1 IPv6
eth0 VIP          172.28.10.239/24
eth1 VIP          1.0.0.239/8
eth2 VIP          2.0.0.239/8
eth0 VIPv6 /
eth1 VIPv6 /
VIP hostname dcnm5.cisco.com
[root@dcnm1 ~]#

[root@dcnm2 ~]# appmgr update network-properties session show changes
eth0 IPv4 addr     172.28.10.247/255.255.255.0     ->     172.28.10.238/255.255.255.0
eth1 IPv4 addr     1.0.0.247/255.0.0.0             ->     1.0.0.238/255.0.0.0
eth1 IPv4 GW                                       ->     1.0.0.1
eth2 IPv4 addr     /                               ->     2.0.0.238/255.0.0.0
eth2 IPv4 GW                                       ->     2.0.0.1
Hostname           dcnm2.cisco.com                 ->     dcnm4.cisco.com
eth0 VIP           172.28.10.248/24                ->     172.28.10.239/24
eth1 VIP           1.0.0.248/8                     ->     1.0.0.239/8
eth2 VIP           /                               ->     2.0.0.239/8
Peer eth0 IP       172.28.10.246                   ->     172.29.10.244
Peer eth1 IP       1.0.0.246                       ->     1.0.0.244
Peer eth2 IP                                       ->     2.0.0.244
Peer hostname     dcnm1.cisco.com                  ->     dcnm3.cisco.com
VIP hostname      dcnm6.cisco.com                  ->     dcnm5.cisco.com
[root@dcnm2 ~]# appmgr update network-properties session show configuration
======= Current configuration ======
Hostname dcnm2.cisco.com
NTP Server        1.ntp.esl.cisco.com
DNS Server        171.70.168.183,1.0.0.247
```

```
eth0 IPv4 addr    172.28.10.247/255.255.255.0
eth0 IPv4 GW      172.28.10.1
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr    1.0.0.247/255.0.0.0
eth1 IPv4 GW
eth1 IPv6 addr
eth1 IPv6 GW
eth2 IPv4 addr    /
eth2 IPv4 GW
eth2 IPv6 addr
eth2 IPv6 GW
Peer hostname     dcnm1.cisco.com
Peer eth0 IP      172.28.10.246
Peer eth1 IP      1.0.0.246
Peer eth2 IP
Peer eth0 IPv6
Peer eth1 IPv6
eth0 VIP         172.28.10.248/24
eth1 VIP         1.0.0.248/8
eth2 VIP         /
eth0 VIPv6       /
eth1 VIPv6       /
VIP hostname dcnm6.cisco.com

====== Session configuration ======
Hostname dcnm4.cisco.com
NTP Server        1.ntp.esl.cisco.com
DNS Server        171.70.168.183,1.0.0.247
eth0 IPv4 addr    172.28.10.238/255.255.255.0
eth0 IPv4 GW      172.28.10.1
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr    1.0.0.238/255.0.0.0
eth1 IPv4 GW      1.0.0.1
eth1 IPv6 addr
eth1 IPv6 GW
eth2 IPv4 addr    2.0.0.238/255.0.0.0
eth2 IPv4 GW      2.0.0.1
eth2 IPv6 addr
eth2 IPv6 GW
Peer hostname dcnm3.cisco.com
Peer eth0 IP      172.29.10.244
Peer eth1 IP      1.0.0.244
Peer eth2 IP      2.0.0.244
Peer eth0 IPv6
Peer eth1 IPv6
eth0 VIP         172.28.10.239/24
eth1 VIP         1.0.0.239/8
eth2 VIP         2.0.0.239/8
eth0 VIPv6       /
eth1 VIPv6       /
VIP hostname dcnm5.cisco.com
[root@dcnm2 ~]#

[root@dcnm1 ~]# appmgr update network-properties session apply
**********************************************************************
                          WARNING
Applications of both nodes of the DCNM HA system need to be stopped
for the changes to be applied properly.
            PLEASE STOP ALL APPLICATIONS MANUALLY
**********************************************************************

Have applications been stopped? [y/n]: y
```

```
Applying changes
DELETE 1
Node left the swarm.
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
log4j:WARN No appenders could be found for logger (fms.db).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
UPDATE 1
UPDATE 1
DELETE 1
server signaled
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the
 'tentative' state
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the
 'tentative' state
**********************************************************************
Please run 'appmgr start afw; appmgr start all' to restart your nodes.
**********************************************************************
**********************************************************************
Please run 'appmgr update ssh-peer-trust' on the peer node.
**********************************************************************
[root@dcnm1 ~]#


[root@dcnm2 ~]# appmgr update network-properties session apply
**********************************************************************
                          WARNING
Applications of both nodes of the DCNM HA system need to be stopped
for the changes to be applied properly.
            PLEASE STOP ALL APPLICATIONS MANUALLY
**********************************************************************

Have applications been stopped? [y/n]: y
Applying changes
DELETE 1
Node left the swarm.
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
log4j:WARN No appenders could be found for logger (fms.db).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
UPDATE 1
UPDATE 1
DELETE 1
afwnetplugin:0.1
server signaled
**********************************************************************
Please run 'appmgr start afw; appmgr start all' to restart your nodes.
**********************************************************************
**********************************************************************
Please run 'appmgr update ssh-peer-trust' on the peer node.
**********************************************************************
[root@dcnm2 ~]#


Step 7

[root@dcnm1 ~]# appmgr start afw; appmgr start all
Started AFW Server Processes
Started AFW Agent Processes
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO:  Resource is stopped
```

```
Done.
Warning: PID file not written; -detached was passed.
AMQP User Check
Started AFW Server Processes
Started AFW Agent Processes
[root@dcnm1 ~]#

Waiting for dcnm1 to become active again.


[root@dcnm2 ~]# appmgr start afw; appmgr start all
Started AFW Server Processes
Started AFW Agent Processes
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO:  Resource is stopped
Done.
Warning: PID file not written; -detached was passed.
AMQP User Check
Started AFW Server Processes
Started AFW Agent Processes
[root@dcnm2 ~]#


[root@dcnm1 ~]# appmgr update ssh-peer-trust
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -o 'StrictHostKeyChecking=no' '172.28.10.245'"
and check to make sure that only the key(s) you wanted were added.

/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -o 'StrictHostKeyChecking=no' '100.0.0.245'"
and check to make sure that only the key(s) you wanted were added.

/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -o 'StrictHostKeyChecking=no'
'dcnm2.cisco.com'"
and check to make sure that only the key(s) you wanted were added.

[root@dcnm1 ~]#


[root@dcnm2 ~]# appmgr update ssh-peer-trust
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -o 'StrictHostKeyChecking=no' '172.28.10.244'"
and check to make sure that only the key(s) you wanted were added.

/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"

Number of key(s) added: 1
```

```
Now try logging into the machine, with:   "ssh -o 'StrictHostKeyChecking=no' '100.0.0.244'"
and check to make sure that only the key(s) you wanted were added.

/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -o 'StrictHostKeyChecking=no'
'dcnm1.cisco.com'"
and check to make sure that only the key(s) you wanted were added.

[root@dcnm2 ~]#
```

Changing the DCNM Server Password on Standalone Setup

The password to access Cisco DCNM Web UI is configured while installing the Cisco DCNM for your deployment type. However, you can modify this password post installation also, if required.

To change the password post installation, perform the following steps:

Procedure

Step 1 Stop the applications using the **appmgr stop all** command.

Wait until all the applications stop running.

Step 2 Change the password for the management interface by using the **appmgr change_pwd ssh {root|poap|sysadmin}**[*password* command.

Ensure that the new password adheres to the following password requirements. If you do not comply with the requirements, the DCNM application might not function properly:

- It must be at least 8 characters long and contain at least one alphabet and one numeral.
- It can contain a combination of alphabets, numerals, and special characters.
- Do not use any of these special characters in the DCNM password: <SPACE> " & $ % ' ^ = < > ; : ` \ | / , .*

Step 3 Start the application using the **appmgr start all** command.

Example

```
dcnm# appmgr stop all

dcnm# appmgr change_pwd ssh root <<new-password>>
dcnm# appmgr change_pwd ssh poap <<new-password>>
dcnm# appmgr change_pwd ssh sysadmin <<new-password>>

dcnm# appmgr start all
```

Changing the DCNM Server Password on Native HA Setup

The password to access Cisco DCNM Web UI is configured while installing the Cisco DCNM for your deployment type. However, you can modify this password post installation also, if required.

To change the password post installation, perform the following steps:

Procedure

Step 1 Stop all the applications on the Standby appliance using the **appmgr stop all** command.

Ensure that all the applications have stopped using the **appmgr status all** command.

Step 2 Stop all the applications on the Active appliance using the **appmgr stop all** command.

Ensure that all the applications have stopped using the **appmgr status all** command.

Step 3 Change the password for the management interface by using the **appmgr change_pwd ssh {root|poap|sysadmin}**[*password*] command. on both Active and Standby nodes.

Note
You provide the same password for both the nodes at the prompt.

Ensure that the new password adheres to the following password requirements. If you do not comply with the requirements, the DCNM application might not function properly:

- It must be at least 8 characters long and contain at least one alphabet and one numeral.
- It can contain a combination of alphabets, numerals, and special characters.
- Do not use any of these special characters in the DCNM password: <SPACE> " & $ % ' ^ = < > ; : ` \ | / , .*

Step 4 Start the applications on the Active appliance, using the **appmgr start all** command.

Ensure that all the applications have started using the **appmgr status all** command.

Step 5 Start the applications on the Standby appliance, using the **appmgr start all** command.

Ensure that all the applications have started using the **appmgr status all** command.

Example

Let us consider Active and standby as dcnm1 and dcnm2, respectively.

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

dcnm1# appmgr change_pwd ssh root <<new-password>>
dcnm1# appmgr change_pwd ssh poap <<new-password>>
dcnm1# appmgr change_pwd ssh sysadmin <<new-password>>

dcnm2# appmgr change_pwd ssh root <<new-password>>
dcnm2# appmgr change_pwd ssh poap <<new-password>>
```

```
dcnm2# appmgr change_pwd ssh sysadmin <<new-password>>

dcnm1# appmgr start all
dcnm2# appmgr start all
```

Changing the DCNM Database Password on Standalone Setup

To change the Postgres database password on Cisco DCNM Standalone setup, perform the following steps:

Procedure

Step 1 Stop all the applications using the **appmgr stop all** command.

Ensure that all the applications have stopped using the **appmgr status all** command.

Step 2 Change the Postgres password by using the **appmgr change_pwd db** command.

Provide the new password at the prompt.

Step 3 Start the application using the **appmgr start all** command.

Ensure that all the applications have started using the **appmgr status all** command.

Example

```
dcnm# appmgr stop all
dcnm# appmgr change_pwd db <<new-password>>
dcnm# appmgr start all
```

Changing the DCNM Database Password on Native HA Setup

To change the Postgres database password on Cisco DCNM Native HA setup, perform the following steps:

Procedure

Step 1 Stop all the applications on the Standby appliance using the **appmgr stop all** command.

Ensure that all the applications have stopped using the **appmgr status all** command.

Step 2 Stop all the applications on the Active appliance using the **appmgr stop all** command.

Ensure that all the applications have stopped using the **appmgr status all** command.

Step 3 Change the Postgres password by using the **appmgr change_pwd db** command on both Active and Standby nodes.

Ensure that you provide the same password at the prompt.

Step 4 Start the applications on the Active appliance, using the **appmgr start all** command.

Ensure that all the applications have started using the **appmgr status all** command.

Step 5 Start the applications on the Standby appliance, using the **appmgr start all** command.

Ensure that all the applications have started using the **appmgr status all** command.

Example

Let us consider Active and standby as **dcnm1** and **dcnm2**, respectively.

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

dcnm1# appmgr change_pwd db <<new-password>>
dcnm2# appmgr change_pwd db <<new-password>>

dcnm1# appmgr start all
dcnm2# appmgr start all
```

Convert Standalone Setup to Native-HA Setup

To convert an existing Cisco DCNM Standalone setup to a Native HA setup, perform the following steps:

Before you begin

Ensure that the Standalone setup is active and operational, by using the **appmgr show version** command.

```
dcnm# appmgr show version

Cisco Data Center Network Manager
Version: 11.5(1)
Install mode: LAN Fabric
Standalone node. HA not enabled.
dcnm#
```

Procedure

Step 1 On the Standalone setup, launch SSH and enable **root** user access by using the **appmgr root-access permit** command:

```
dcnm# appmgr root-access permit
```

Step 2 Deploy a new DCNM as secondary node. Choose **Fresh installation - HA Secondary**

For example, let us indicate the existing setup as **dcnm1** and the new DCNM as secondary node as **dcnm2**.

Caution
If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

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

A welcome message appears.

a) On the **Welcome to Cisco DCNM** screen, click **Get Started**.

Caution
If the system configuration does not meet minimum resource requirements, **SYSTEM RESOURCE ERROR** is displayed on the Web Installer, and the installation will be aborted. Modify the system requirements, and launch the Web Installer to complete the installation.

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

Click **Continue**.

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

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

Check the **Enable Clustered Mode** check box, if you have configured the Cisco DCNM Primary in Clustered mode.

Click **Next**.

d) On the **Administration** tab, enter information about passwords.

Note
All the passwords must be same as the passwords that you provided while configuring the Primary node.

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

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

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

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

  Note
  If you're using Network Insights applications, ensure that the DNS server is valid and reachable.
- In the **NTP Server Address List** field, enter the IP address of the NTP server.

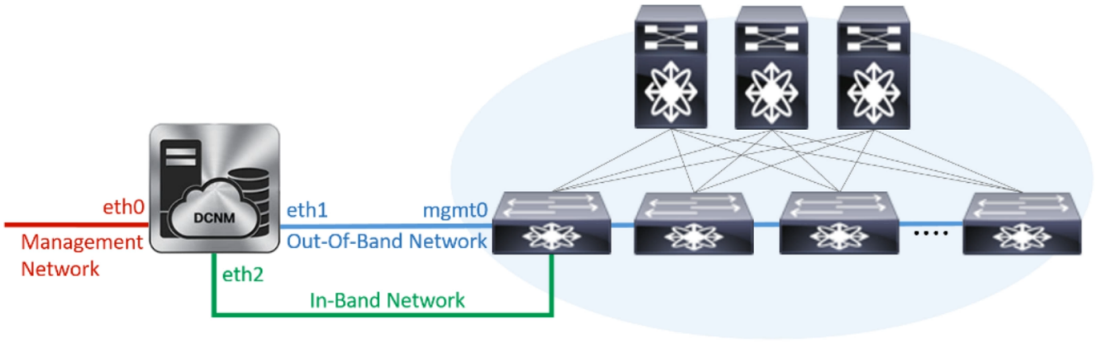
  The value must be an IP or IPv6 address or RFC 1123 compliant name.

  From Release 11.3(1), you can configure more than one NTP server.
- From the **Timezone** drop-down list, select the timezone in which you are deploying the DCNM.

Click **Next**.

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

Figure 22: Cisco DCNM Management Network Interfaces



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

   Note
   Ensure that the IP address belongs to the same Management Network configured on the Primary node.

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

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

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

   Note
   Ensure that the IP addresses belong to the same Out-of-Band network configured on the Primary node.

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

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

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

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

   Note
   Ensure that the IP addresses belong to the same In-Band network configured on the Primary node.

   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.

Click **Next**.

g) On the **Applications** tab, configure the Internal Applications Services Network, and Cluster mode settings.

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

2. In the **Clustered mode configuration** area, configure the network settings to deploy the DCNM instance in Clustered mode. In Clustered mode, applications run on separate compute nodes.
   - In the **Out-of-Band IPv4 Network Address Pool**, enter the address pool from the Out-of-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **Out-of-Band IPv6 Network Address Pool** field.
   - In the **In-Band IPv4 Network Address Pool**, enter the address pool from the In-Band IPv4 network to be used in the Clustered Mode.

     Optionally, you can also enter an IPv6 address pool in the **In-Band IPv6 Network Address Pool** field.

   Ensure that the IP addresses belong to the same pool as configured on the Primary node.

h) On the **HA Settings** tab, configure the system settings for the Secondary node.
   - In the **Management IPv4 Address of Primary DCNM node** field, enter the appropriate IP Address to access the DCNM UI.
   - In the **VIP Fully qualified Host Name** field, enter hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1. Host names with only digits is not supported.
   - In the **Management Network VIP address** field, enter the IP address used as VIP in the management network.

     Optionally, you can also enter an IPv6 VIP address in the **Management Network VIPv6 address** field.

     Note
     If you have configured the Management network using IPv6 address, ensure that you configure the Management Network VIPv6 Address.
   - In the **Out-of-Band Network VIP Address** field, enter the IP address used as VIP in the Out-of-Band network.

     Optionally, you can also enter an IPv6 VIP address in the **Out-of-Band Network VIPv6 Address** field.
   - In the **In-Band Network VIP Address** field, enter the IP address used as VIP in the Out-of-Band network.

     Optionally, you can also enter an IPv6 VIP address in the **In-Band Network VIPv6 Address** field.

     Note
     This field is mandatory if you have provided an IP address for In-Band network in the **Network Settings** tab.
   - In the **HA Ping Feature IPv4 Address** field, enter the HA ping IP address and enable this feature, if necessary.

     Note
     The configured IPv4 address must respond to the ICMP echo pings.

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

You must configure the HA ping IPv4 Address to avoid the Split Brain scenario. This IP address must belong to Enhanced Fabric management network.

Click **Next**.

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

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

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

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

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

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

What to do next

Verify the HA role by using the appmgr show ha-role command.

On the Active node (old standalone node):

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

On the Standby node (newly deployed node):

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

Utility Services Details

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

Network Management

The data center network management function is provided by the Cisco Data Center Network Manager (DCNM) server. Cisco DCNM provides the setup, visualization, management, and monitoring of the data

center infrastructure. Cisco DCNM can be accessed from your browser: `http://<<hostname/IP address>>`.

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

Orchestration

RabbitMQ

Rabbit MQ is the message broker that provides the Advanced Messaging Queuing Protocol (AMQP). The RabbitMQ message broker sends events from the vCloud Director/vShield Manager to the Python script for parsing. You can configure this protocol by using certain CLI commands from the Secure Shell (SSH) console of the firmware.

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

After upgrade, enable RabbitMQ management service stop the service and start the services using the following commands:

```
dcnm# appmgr stop amqp
dcnm# appmgr start amqp
```

If AMQP is not running. the memory space must be exhausted that is indicated in the file `/var/log/rabbitmq/erl_crash.dump`.

Device Power On Auto Provisioning

Power On Auto Provisioning (POAP) occurs when a switch boots without any startup configuration. It is accomplished by two components that were installed:

- DHCP Server

  The DHCP server parcels out IP addresses to switches in the fabric and points to the location of the POAP database, which provides the Python script and associates the devices with images and configurations.

  During the Cisco DCNM installation, you define the IP Address for the inside fabric management address or OOB management network and the subnets associated with the Cisco Programmable Fabric management.

- Repositories

  The TFTP server hosts boot scripts that are used for POAP.

  The SCP server downloads the database files, configuration files, and the software images.

- You can change POAP password, using **command appmgr change_pwd ssh poap**. Ensure that you run the command on both active and standby HA nodes.

Managing Applications and Utility Services

You can manage the applications and utility services for Cisco Programmable Fabric in the Cisco DCNM through commands in an SSH terminal.

Enter the **appmgr** command from the SSH terminal by using the following credentials:

- Username: **root**
- Password: **Administrative password provided during deployment**

Note For your reference, context sensitive help is available for the **appmgr** command. Use the **appmgr** command to display help.

Use the **appmgr tech_support** command to produce a dump of the log files. You can then provide this information to the TAC team for troubleshooting and analysis of your setup.

Note This section does not describe commands for Network Services using Cisco Prime Network Services Controller.

This section includes the following:

Verifying the Application and Utility Services Status after Deployment

After you deploy the OVA/ISO file, you can determine the status of various applications and utility services that were deployed in the file. You can use the **appmgr status** command in an SSH session to perform this procedure.

Note Context-sensitive help is available for the **appmgr status** command. Use the **appmgr status ?** command to display help.

Procedure

Step 1 Open up an SSH session:

a) Enter the **ssh root DCNM network IP address** command.

b) Enter the administrative password to login.

Step 2 Check the status by using the following command:

appmgr status all

Example:

```
DCNM Status
 PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
 ===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
```

```
 1891 root 20 02635m 815m  15m S  0.0 21.3    1:32.09  java

LDAP Status
 PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
 ===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
 1470 ldap      20   0  692m  12m 4508 S  0.0  0.3   0:00.02 slapd

AMQP Status
 PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
 ===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
1504 root      20   0 52068  772  268 S  0.0  0.0   0:00.00 rabbitmq

TFTP Status
 PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
 ===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
 1493 root      20   0 22088 1012  780 S  0.0  0.0   0:00.00 xinetd

DHCP Status
 PID  USER      PR   NI VIRT RES  SHR  S  %CPU %MEM  TIME+   COMMAND
 ===  =====    ===   == ==== ===  ===  =  ==== ===== ======  =======
 1668 dhcpd 20   0 46356 3724 408 S  0.0  0.0   0:05.23 dhcp
```

Stopping, Starting, and Resetting Utility Services

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

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

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

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

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

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

```
# appmgr restart tftp
Restarting TFTP...
Stopping xinetd:     [  OK  ]
Starting xinetd:     [  OK  ]
```



Note From Cisco DCNM Release 7.1.x, when you stop an application by using the **appmgr stop** *app_name* command, the application will not start during successive reboots.

For example, if DHCP is stopped by using the **appmgr stop dhcp** command, and the OS is rebooted, the DHCP application will still be down after the OS is up and running.

To start again, use the command **appmgr start dhcp**. The DHCP application will be started after reboots also. This is to ensure that when an environment uses an application that is not packaged as part of the virtual appliance (like CPNR instead of DHCP), the application locally packaged with the virtual appliance will not interfere with its function after any OS reboots.

Note When a DCNM appliance (ISO/OVA) is deployed, the Cisco SMIS component will not get started by default. However, this component can be managed using the appmgr CLI: **appmgr start/stop dcnm-smis**

appmgr start/stop dcnm will start or stop only the DCNM web component.

Updating the SFTP Server Address for IPv6

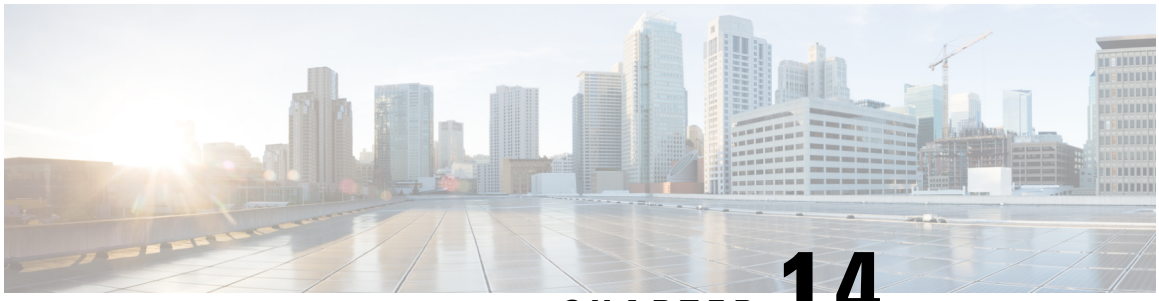
After deploying the DCNM OVA/ISO successfully with EFM IPv4 and IPv6, by default the SFTP address is pointed to IPv4 only. You need to change the IPv6 address manually in the following two places:

- In the DCNM Web Client, choose **Administration > Server Properties** and then update the below fields to IPv6 and click the **Apply Changes** button.

```
#_____________________________________________________________________
# GENERAL>xFTP CREDENTIAL
#
# xFTP server's ip address for copying switch files:
server.FileServerAddress
```

- Log in to the DCNM through ssh and update the SFTP address with IPv6 manually in the server.properties file (/usr/local/cisco/dcm/fm/conf/server.properties).

```
# xFTP server's ip address for copying switch files:
server.FileServerAddress=2001:420:5446:2006::224:19
```



CHAPTER 14

Tetration Agent With DCNM Validation

A tetration software agent is a small software application running on a host system. Its core functionality is to monitor and collect network flow information. It also collects other host information such as network interfaces and active processes running on the system. The information collected by the agent is exported to a set of collectors running within the Tetration cluster for further analytical processing.

- Tetration Agent With DCNM Validation, on page 187

Tetration Agent With DCNM Validation

Using the installer script is the recommended method for deploying deep visibility enforcement agents on Linux platforms.

Before you begin

If the installed agent is to be connected to a Tetration cluster, the **ACTIVATION_KEY** and **HTTPS_PROXY** parameters will be required. If the installer script is used, it will automatically populate the **ACTIVATION_KEY**, while you need to insert the HTTPS_PROXY information directly into the script.

If manual deployment is used, manually insert both **ACTIVATION_KEY** and **HTTPS_PROXY** parameters yourself. For more information, see User Configuration for Tetration SaaS.

Procedure

Step 1 Log into the Cisco TetrationOS Software Web UI with your credentials.

Step 2 Choose **Agent Config** from the **Settings** menu to display the **Agent Config** window.

Step 3 Navigate to the **Software Agent Download** tab.

Step 4 Choose **Linux** in the **Select Platform** section.

Step 5 Choose **Deep Visibility** or **Enforcement** in the **Select Agent Type** section.

Step 6 Click the **Download Installer** button and save the file to a local disk.

Step 7 Log into your DCNM with the root privileges. Copy the installer shell script and execute the script.

Note
The installer script will not proceed if the agent was already installed.

The installer script command syntax is as follows:

```
$ tetration_linux_installer.sh [-skip-pre-check] [-noInstall]
        [-logFile=filename] [-proxy=proxy_string>] [-skip-ipv6-check]
 [-help] [-version] [-sensor-version=version_info] [-ls] [-file=filename]
 [-save=filename] [-new]
```

-skip-pre-check	Skips pre-installation checks.
-noInstall	The sensor package is not downloaded and installed on the system.
-logFile filename	Writes the log to the file specified by filename .
-proxy proxy_string	Sets the value of `HTTPS_PROXY`. Use this if a proxy server is needed to communicate with the cluster. The string should be formatted as `http://`*proxy*`:`*port*
-skip-ipv6-check	Skips IPv6 verification.
-help	Prints this help information.
-version	Prints the current script's version.
-sensorVersion version_info	Downloads a particular sensor version; default is the latest version. An example of the version_info entry is `-sensor-version=3.1.1.53.devel`
-ls	Lists all available sensor versions for your system (does not list pre-3.1 packages). This is a listing only; does not download any package.
-file filename	Let's you specify a local zip file to use to install the sensor instead of downloading from the cluster.
-save filename	Downloads the installer zip file from the Tetration cluster, saving it locally with filename as its name.
-new	Uninstalls/removes all copies of the Tetration agent if it was already installed on this local machine.

Step 8 Run the following command to verify if the agent is installed.

```
sudo rpm -q tet-sensor
```

An entry appears as follows:

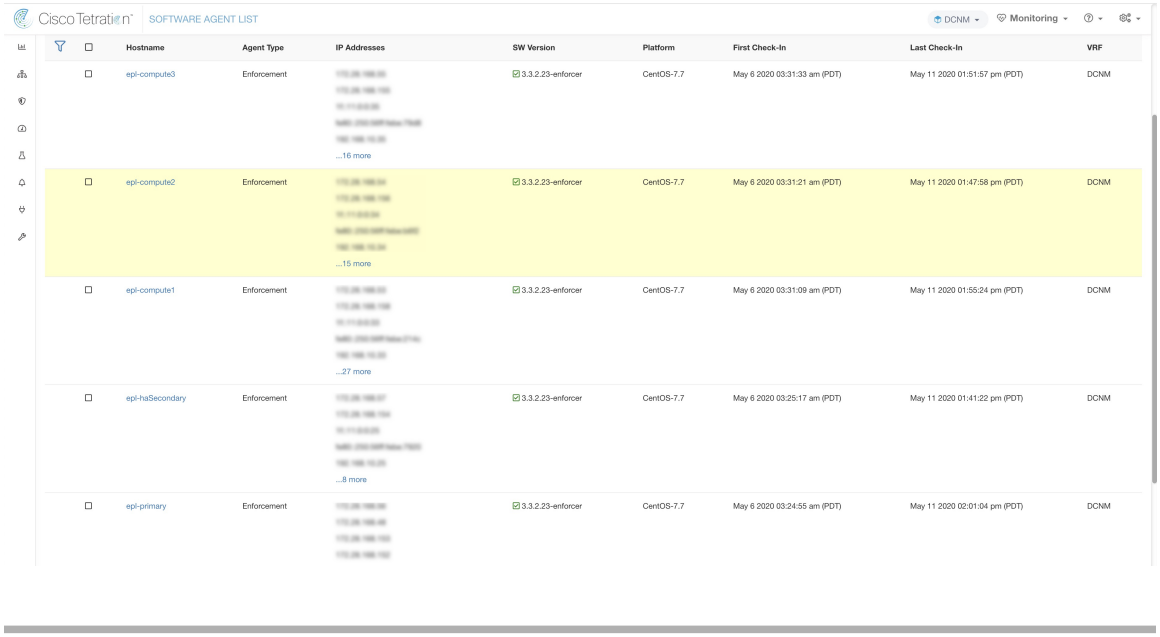
```
$ sudo rpm -q tet-sensor

tet-sensor-3.1.1.50-1.el6.x86_64
```

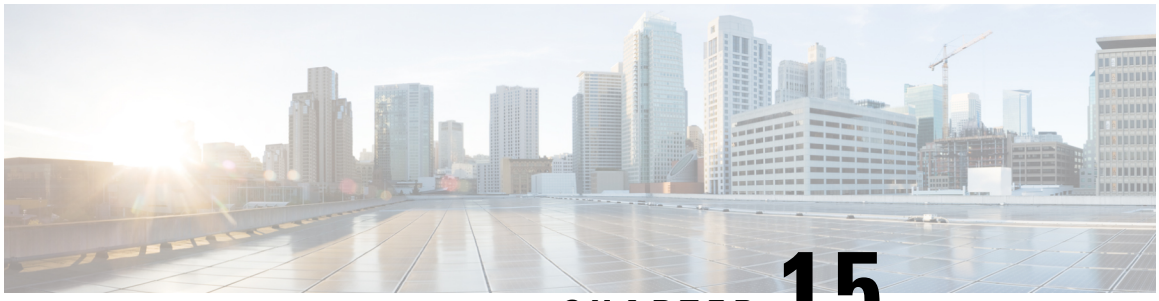
Note
There are five nodes in a DCNM native HA cluster deployment, namely, DCNM Primary, DCNM Secondary, and three Compute Nodes. Install the tetration agent on each of these nodes for full visibility of the DCNM cluster.

Tetration Agent With DCNM Validation

Figure 23: Tetration Agent with DCNM Clusters



Tetration Agent With DCNM Validation



CHAPTER 15

Setup Authentication via TACACS+ Server

• Setup SSH Authentication via TACACS+ Server, on page 191

Setup SSH Authentication via TACACS+ Server

From Release 11.5(1), DCNM provides **appmgr** command to set up authentication for ssh access via TACACS+. For SSH access to DCNM, the credentials are sent to previously configured TACACS+ server, to determine if access is allowed. In case of success, SSH access to DCNM is allowed. When the TACACS+ server is not reachable, the system reverts to local authentication.

DCNM permits SSH access for the following three users—sysadmin, poap, root. The **sysadmin** user has general SSH access to DCNM. SSH access to the **root** user is disabled by default. However, the DCNM Primary and Secondary servers communicate with each other through SSH, using the **root** user with passwordless access, for Native HA setup and maintenance. The **poap** user is employed for SSH/SCP access of information between the DCNM and NX-OS switches. This is typically used for functions such as POAP, and Image management. When you enable TACACS+ authentication for SSH access on the DCNM, you must create three users (sysadmin, poap, root) on the Remote AAA server, and enable TACACS+. Later, any SSH access to the DCNM is authenticated and the TACACS+ server audit logs track all SSH access to DCNM.

Remote authentication is supported only for SSH sessions. The **su** command always uses local authentication. Log in from DCNM console always uses local authentication, to prevent users from system lock-out.

Note For a DCNM Setup in Cluster mode, you must enable and configure remote authentication on all nodes, namely, Primary, Secondary, and all Compute nodes.

Removing Remote Authentication

To remove remote authentication, use the following command:

appmgr remote-auth set none

Note The **appmgr remote-auth set** command always replaces the old configuration with the new one.

Configuring Remote Authentication using TACACS+

To configure remote authentication using TACACS+, use the following command:

appmgr remote-auth set tacacs [**auth** {**pap** | **chap** | **ascii** }] {**server** <*address*> <*secret*> }

Where,

- **auth** defines the Authentication type. If omitted, the default is PAP. ASCII and MSCHAP are also supported.
- *address* is the address of a server. The server address can be hostname, IPv4 address or IPv6 address format. You can also specify a port number. For example: **my.tac.server.com:2049**

  The IPv6 address must a fully qualified IPv6 format as per RFC2732. The IPv6 address must be enclosed in [ ] or the feature won't function properly.

  For example:

  - [2001:420:1201:2::a] – *correct*
  - 2001:420:1201:2::a – *incorrect*

- *secret* is the secret shared between DCNM and the TACACS+ server. Secrets with spaces aren't allowed/supported.

Enabling or Disabling Remote Authentication

To enable or disable remote authentication, use the following command.

appmgr remote-auth { **enable** | **disable** }

Viewing Remote Authentication Password

To view the remote authentication password, use the following command:

appmgr remote-auth show

Sample output:

```
dcnm# appmgr remote-auth show
Remote Authentication is DISABLED
```

```
dcnm# appmgr remote-auth show
Remote Authentication is ENABLED
Protocol: tacacs+
Server: 172.28.11.77, secret: ********
Authentication type: ascii
dcnm#
```

By default, shared secrets aren't displayed in clear-text unless [-S or --show-secret] keyword is used.

Examples

1. Configure and enable 172.28.11.77 as remote authentication server with cisco123 as shared secret.

   ```
   dcnm# appmgr remote auth set tacacs server 172.28.11.77 cisco123
   dcnm# appmgr remote auth enable
   ```

2. Configure 172.28.11.77 as remote authentication server with cisco 123 as share secret using MSCHAP as authentication type.

```
dcnm# appmgr remote auth set tacacs auth mschap 172.28.11.77 cisco123
dcnm# appmgr remote auth enable
```

3. Configure three servers with different shared secrets.

```
dcnm# appmgr remote auth set tacacs server tac1.cisco.com:2049 cisco123 server
                tac2.cisco.com Cisco_123 server tac3.cisco.com C1sco_123
dcnm# appmgr remote auth enable
```

4. Disable and removes authentication configuration.

```
dcnm# appmgr remote auth set tacacs none
```

5. Disable remote-authentication without removing the configuration.

```
dcnm# appmgr remote auth disable
```

6. Enable current remote-authentication configuration.

```
dcnm# appmgr remote auth enable
```

Remote authentication & POAP

When remote authentication is enabled, the local password of **poap** user must be the same as the password on TACACS server; POAP fails otherwise.

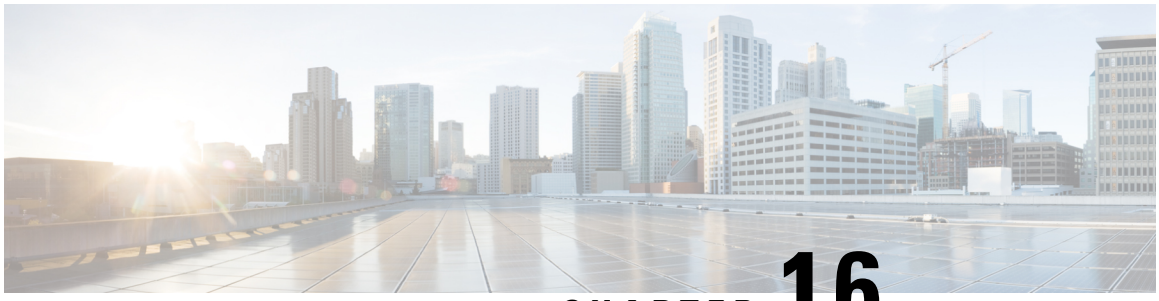
To synchronize local poap password, after setting or changing the password on the TACACS server, use the following command:

appmgr change_pwd ssh poap

In Cisco DCNM Native HA setup, execute this command on the Primary node only.

Remote authentication in DCNM Native HA setup

For scenarios in which a standalone DCNM needs to be converted to a native HA setup, ensure that remote authentication if enabled, should be disabled prior to adding a secondary HA node, and before running **appmgr update ssh-peer-trust** command.



CHAPTER 16

Installing Software Maintenance Update for log4j2 Vulnerability

- Installing Software Maintenance Update on Cisco DCNM OVA/ISO Deployment, on page 195

Installing Software Maintenance Update on Cisco DCNM OVA/ISO Deployment

Cisco DCNM provides a Software Maintenance Update (SMU) to address the **CVE-2021-45046 and CVE-2021-44228** issue in Release 11.5(x). This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

This section contains the following topics:

Installing SMU on Cisco DCNM 11.5(x) Standalone Deployment

This section provides instructions to install Software Maintenance Update (SMU) on Cisco DCNM OVA/ISO appliance to address **CVE-2021-45046 and CVE-2021-44228** issue. Note that CVE-2021-45105 has a lower severity and not used in DCNM with default configuration, and therefore it is not addressed here.

To apply the Software Maintenance Update (SMU) on Cisco DCNM OVA/ISO in Standalone deployment mode, perform the following steps:

Before you begin

- Take a backup of the application data using the **appmgr backup** command on the DCNM appliance.

  ```
  dcnm# appmgr backup
  ```

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

- If Cisco DCNM appliance is installed in VMware environment, ensure that you take VM snapshots for all nodes. For instructions, refer to *VMware Snapshot Support* section in your Cisco DCNM Release Notes.

- Ensure that you plan for a maintenance window to install SMU.

- Ensure that Cisco DCNM 11.5(x) is up and running.

This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

Note Only a **root** user can install the SMU on the Cisco DCNM Release 11.5(x) appliance

Procedure

Step 1 Download the SMU file.

a) Go to the following site: https://software.cisco.com/download/.

A list of the latest release software for Cisco DCNM available for download is displayed.

b) In the Latest Releases list, choose Release 11.5(x).

This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

c) Locate **DCNM 11.5.x Maintenance Update for VMWare, KVM, Bare-metal, and Appliance servers to address log4j2 CVE-2021-45046 and CVE-2021-44228** file and click **Download** icon.

d) Save the **dcnm-va-patch.11.5.x-p1.iso.zip** file to your directory that is easy to find when you start to apply the SMU.

Step 2 Unzip the **dcnm-va-patch.11.5.x-p1.iso.zip** file and upload the file to the `/root/` folder in the DCNM node.

Step 3 Log on to the Cisco DCNM appliance using SSH as a **sysadmin** user.

Run the **su** command to enable **root** user.

```
dcnm# su
Enter the root password:
[root@dcnm]#
```

Step 4 Run the following command to create a screen session.

```
[root@dcnm]# screen
```

This creates a session which allows you to execute the commands. The commands continue to run even when the window is not visible or if you get disconnected.

Step 5 Create a folder named **iso** using the **mkdir /mnt/iso** command.

```
[root@dcnm1]# mkdir -p /mnt/iso
```

Step 6 Mount the DCNM 11.5(x) SMU file in the `/mnt/iso` folder.

```
[root@dcnm]# mount -o loop dcnm-va-patch.11.5.x-p1.iso /mnt/iso
```

Step 7 Navigate to **/scripts/** directory.

```
[root@dcnm]# cd /mnt/iso/packaged-files/scripts/
```

Step 8 Run the **./inline-upgrade.sh** script.

```
[root@dcnm]# ./inline-upgrade.sh
```

The progress is displayed on the screen. When the installation of SMU is complete, a successful message appears.

Note
After the SMU is installed successfully, the DCNM process restarts. This results in a momentary loss of access to the DCNM Web UI.

Step 9 Ensure the DCNM application is functional, by using the **appmgr status all** command.

```
[root@dcnm]# appmgr status all
```

Step 10 Terminate the **screen** session, by using the **exit** command.

```
[root@dcnm]# exit
```

Step 11 Unmount the **dcnm-va-patch.11.5.x-p1.iso** file from the DCNM setup.

Note
You must terminate the **screen** session before unmounting the SMU file.

```
[root@dcnm]# umount /mnt/iso
```

Installing SMU on Cisco DCNM 11.5(x) Native HA Deployment

This section provides instructions to install Software Maintenance Update (SMU) on Cisco DCNM OVA/ISO appliance to address **CVE-2021-45046 and CVE-2021-44228** issue. Note that CVE-2021-45105 has a lower severity and not used in DCNM with default configuration, and therefore it is not addressed here.

To apply the Software Maintenance Update (SMU) on Cisco DCNM OVA/ISO in Native HA deployment mode, perform the following steps:

Before you begin

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

  Example:

  On the Active node:

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

  On the Standby node:

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

- Take a backup of the application data using the **appmgr backup** command on both Active and Standby appliances.

  ```
  dcnm1# appmgr backup
  ```

  ```
  dcnm2# appmgr backup
  ```

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

- If Cisco DCNM appliance is installed in VMware environment, ensure that you take VM snapshots for all nodes. For instructions, refer to *VMware Snapshot Support* section in your Cisco DCNM Release Notes.
- Ensure that you plan for a maintenance window to install SMU.
- Ensure that both the Cisco DCNM 11.5(x) Active and Standby peers are up and running.

  This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

  To apply this software maintenance update on Cisco DCNM Virtual Appliance in Native HA Mode, apply this update on the Active and Standby appliance. Wait until the role of the Active appliance is Active again. Apply the update on the Standby appliance, later.

  For Native HA cluster deployments, install the SMU on Active and Standby appliances, before installing SMU on the compute nodes.

Note Only a **root** user can install the SMU on the Cisco DCNM Release 11.5(x) appliance.

Procedure

Step 1 Download the SMU file.

a) Go to the following site: https://software.cisco.com/download/.

A list of the latest release software for Cisco DCNM available for download is displayed.

b) In the Latest Releases list, choose Release 11.5(x).

This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

c) Locate **DCNM 11.5.x Maintenance Update for VMWare, KVM, Bare-metal, and Appliance servers to address log4j2 CVE-2021-45046 and CVE-2021-44228** file and click **Download** icon.

d) Save the **dcnm-va-patch.11.5.x-p1.iso.zip** file to your directory that is easy to find when you start to apply the SMU.

Step 2 Unzip the **dcnm-va-patch.11.5.x-p1.iso.zip** file and upload the file to the `/root/` folder in both Active and Standby node of the DCNM setup.

Note
For example, let us indicate Active and Standby appliances as **dcnm1** and **dcnm2** respectively.

Step 3 Log on to the Cisco DCNM appliance using SSH as a **sysadmin** user.

Run the **su** command to enable **root** user.

```
dcnm1# su
Enter the root password:
[root@dcnm1]#
```

```
dcnm2# su
Enter the root password:
[root@dcnm2]#
```

Step 4 Run the following command to create a screen session.

```
[root@dcnm1]# screen
```

```
[root@dcnm2]# screen
```

This creates a session which allows you to execute the commands. The commands continue to run even when the window is not visible or if you get disconnected.

Step 5 On the Active node, install the SMU.

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

```
[root@dcnm1]# mkdir -p /mnt/iso
```

b) Mount the DCNM 11.5(x) SMU file on the Active node in the `/mnt/iso` folder.

```
[root@dcnm1]# mount -o loop dcnm-va-patch.11.5.x-p1.iso /mnt/iso
```

c) Navigate to **/scripts/** directory.

```
[root@dcnm1]# cd /mnt/iso/packaged-files/scripts/
```

d) Run the **./inline-upgrade.sh** script.

```
[root@dcnm1]# ./inline-upgrade.sh
```

The progress is displayed on the screen. When the installation of SMU is complete, a successful message appears.

Note
After the SMU is installed successfully, the DCNM process restarts. This results in a momentary loss of access to the DCNM Web UI.

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

```
[root@dcnm1]# appmgr status all
```

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

Step 6 On the Standby node, install the SMU.

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

```
[root@dcnm2]# mkdir -p /mnt/iso
```

b) Mount the DCNM 11.5(x) SMU file on the Standby node in the `/mnt/iso` folder.

```
[root@dcnm2]# mount -o loop dcnm-va-patch.11.5.x.iso /mnt/iso
```

c) Navigate to **/scripts/** directory.

```
[root@dcnm2]# cd /mnt/iso/packaged-files/scripts/
```

d) Run the **./inline-upgrade.sh** script.

```
[root@dcnm2]# ./inline-upgrade.sh --standby
```

The progress is displayed on the screen. When the installation of SMU is complete, a successful message appears.

Note
After the SMU is installed successfully, the DCNM process restarts. This results in a momentary loss of access to the DCNM Web UI.

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

```
[root@dcnm2]# appmgr status all
```

Step 7 Terminate the **screen** session, by using the **exit** command.

```
[root@dcnm1]# exit
```

```
[root@dcnm2]# exit
```

Step 8 Unmount the **dcnm-va-patch.11.5.x-p1.iso** file in both Active and Standby node of the DCNM setup.

Note
You must terminate the **screen** session before unmounting the SMU file.

```
[root@dcnm1]# umount /mnt/iso
```

```
[root@dcnm2]# umount /mnt/iso
```

Installing SMU on Cisco DCNM 11.5(x) Compute Nodes

This section provides instructions to install Software Maintenance Update (SMU) on Cisco DCNM OVA/ISO appliance to address **CVE-2021-45046 and CVE-2021-44228** issue. Note that CVE-2021-45105 has a lower severity and not used in DCNM with default configuration, and therefore it is not addressed here.

To apply the Software Maintenance Update (SMU) on compute nodes in Cisco DCNM clustered setup, perform the following steps:

Before you begin

- You must install the SMU on Cisco DCNM Servers in Native HA mode, before upgrading the DCNM compute nodes.
- If Cisco DCNM appliance is installed in VMware environment, ensure that you take VM snapshots for all nodes. For instructions, refer to *VMware Snapshot Support* section in your Cisco DCNM Release Notes.
- Ensure that you plan for a maintenance window to install SMU.
- Ensure that Cisco DCNM 11.5(x) is up and running.

  This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.



Note Only a **root** user can install the SMU on the Cisco DCNM Release 11.5(x) appliance.

Procedure

Step 1 Download the SMU file.

a) Go to the following site: https://software.cisco.com/download/.

A list of the latest release software for Cisco DCNM available for download is displayed.

b) In the Latest Releases list, choose Release 11.5(x).

This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

c) Locate **DCNM 11.5.x Maintenance Update for VMWare, KVM, Bare-metal, and Appliance servers to address log4j2 CVE-2021-45046 and CVE-2021-44228** file and click **Download** icon.

d) Save the **dcnm-va-patch.11.5.x-p1.iso.zip** file to your directory that is easy to find when you start to apply the SMU.

Step 2 Unzip the **dcnm-va-patch.11.5.x-p1.iso.zip** file and upload the file to the `/root/` folder in all three compute nodes of the DCNM setup.

For example, let us indicate the three Compute Nodes as Compute1, Compute2, and Compute3.

Step 3 Log on to the Cisco DCNM appliance using SSH as a **sysadmin** user.

Run the **su** command to enable **root** user.

```
dcnm-compute1# su
Enter the root password:
[root@dcnm-compute1]#
```

Step 4 Run the following command to create a screen session.

```
[root@dcnm-compute1]# screen
```

This creates a session which allows you to execute the commands. The commands continue to run even when the window is not visible or if you get disconnected.

Step 5 On Compute1 node, install the SMU.

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

```
[root@dcnm-compute1]# mkdir -p /mnt/iso
```

b) Mount the DCNM 11.5(x) SMU file on Compute1 node in the `/mnt/iso` folder.

```
[root@dcnm-compute1]# mount -o loop dcnm-va-patch.11.5.x-p1.iso /mnt/iso
```

c) Navigate to **/scripts/** directory.

```
[root@dcnm-compute1]# cd /mnt/iso/packaged-files/scripts/
```

d) Run the **./inline-upgrade.sh** script.

```
[root@dcnm-compute1]# ./inline-upgrade.sh
```

The progress is displayed on the screen. When the installation of SMU is complete, a successful message appears.

If some services are still running, a prompt to stop the services appears. When prompted, press **y** to continue.

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

```
[root@dcnm-compute1]# appmgr status all
```

Note
Ensure that all the services are up and running on the **dcnm-compute1** node.

f) Terminate the **screen** session, by using the **exit** command.

```
[root@dcnm-compute1]# exit
```

g) Unmount the **dcnm-va-patch.11.5.x-p1.iso** file from the Compute1.

Note
You must terminate the **screen** session before unmounting the SMU file.

```
[root@dcnm]# umount /mnt/iso
```

Step 6 Install the SMU on the other two Compute nodes also.

Follow the instructions as explained in Step Step 5, on page 201.

What to do next

After the installation is complete, each compute node joins the cluster automatically. On the Web UI, choose **Applications** > **Compute** to verify if the compute node appears as **Joined**.

Note If you try to install the SMU again, an error message appears stating that the patch is already applied on the Cisco DCNM/Compute.

Sample Output of Commands to address Log4j vulnerability

The following is a sample output while installing the SMU on Cisco DCNM Release 11.5(x).

This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

- Sample Output to Install SMU in DCNM Standalone Deployment, on page 202
- Sample output to install SMU in DCNM Native HA Deployment, on page 208
- Sample Output to Install SMU in DCNM Compute Nodes, on page 214

Sample Output to Install SMU in DCNM Standalone Deployment

This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

```
[root@dcnm]# ./inline-upgrade.sh

============================================================
============ Inline Upgrade to DCNM 11.5(x)-p1 =============
============================================================

Upgrading from version: 11.5(x)
```

```
Upgrading from install option: LAN Fabric
System type: Standalone
Compute only: No

Do you want to continue and perform the inline upgrade to 11.5(x)-p1? [y/n]: y
==== Fri Dec 17 11:26:51 PST 2021 - Task checkAfwStatus started ====
==== Fri Dec 17 11:26:51 PST 2021 - Task checkAfwStatus finished ====
==== Fri Dec 17 11:26:51 PST 2021 - Task updateAfwApps started ====
==== Fri Dec 17 11:26:51 PST 2021 - Updating AFW applications ====
Pausing Services that need to be patched
Deleted Containers:
992d06574c57882cf1a86bf7c19414055c6f501073a262b9e97cee0a75718a55
324f8ecfc34223f9d71abb86a807af54a720b40121aa8f38f6aa2dccbc233071
f7fe8656838af352d0d128163b1e9e4dcca9e5b73ea3a0956e4199e867f69a34
ab0f0dd90b98dacca8e01c944c6b07390bad8cd8247cf8cdf7629503bd01d252
52d0d5ad7edf990424b43c57d95ba836191fa913e556e6c1b75a65f171de6be6
4daf92fd8ba5445a81913df573343c0d6617b436330d103b8abf631a477c9b91
786768ab289596fbfb3904b1115a14717057bc83a06e555aa1abb76abb4c3a9e
1f5f52c42e532b4be9cff0eb22844824d969c6838436b98251236efdf4f85f57
b780eff0776d9dfa752ef28446dcaffcffffac6ac20a2b41738ac23e6d060ed3
756097c7bd5028ee5eafc74c7fb90eae20104b1584f2611ea1b3089340d0011c

Total reclaimed space: 1.418MB
pauseAfwApp: calling PUT with  {pause}
pauseAfwApp:  value of Wait:  false

HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:26:52 GMT
Content-Length : 99
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Paused for elasticsearch_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {pause}
pauseAfwApp:  value of Wait:  false

HTTP/1.1 200 OK
Content-Length : 96
Content-Type : text/plain; charset=utf-8
Date : Fri, 17 Dec 2021 19:27:12 GMT
{
  "ResponseType": 0,
  "Response": "Application is Paused for watchtower_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {pause}
pauseAfwApp:  value of Wait:  false

HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:27:32 GMT
Content-Length : 91
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Paused for eplui_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {pause}
pauseAfwApp:  value of Wait:  false

HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:27:52 GMT
Content-Length : 100
Content-Type : text/plain; charset=utf-8
{
```

```
  "ResponseType": 0,
  "Response": "Application is Paused for elasticservice_Cisco_afw. Check for status"
}
Now Removing Images from Runtime
Untagged: 127.0.0.1:5001/dcnmelastic:6.8.3_11.5.2
Untagged:
127.0.0.1:5001/dcnmelastic@sha256:a872d49e3b5a0fc58ec9c1e8d8908c62604258cbfb1a02ac418227ed7f928128
Untagged: 127.0.0.1:5000/dcnmelastic:6.8.3_11.5.2
Untagged:
127.0.0.1:5000/dcnmelastic@sha256:a872d49e3b5a0fc58ec9c1e8d8908c62604258cbfb1a02ac418227ed7f928128
Untagged: dcnmelastic:6.8.3_11.5.2
Deleted: sha256:0173109c0612f48ed4165de7e5fa96f2243fe48756405bd0a0b4f12279785db1
Deleted: sha256:8d0b16f607caee532685643cf21550079881b67db9edf7d54a50ba4dec673c45
Deleted: sha256:63f9d6a3667c56f4a64d986b13b0059353fb983495b34f840b6a38c63e39938c
Deleted: sha256:af6e5eed783b56a675c53698ad4d374a77222218ebf706ad9891785b4ec2a537
Deleted: sha256:37dab1fa0ee831d1979104edd0ea820a1b3de3fe818aa75200021f868b221998
Deleted: sha256:cf1569581d9385a63ebd156e15dc795ab82de8d0a27fc5a3205dac339b591ee5
Deleted: sha256:3d293d026d9a7552a3630a75500d860083763a558191e1f28ebb6344c985b09d
Deleted: sha256:b285cfcb6bcb0850c0121d404c51ef0a333380cf332b3b776e75b45a94c2e8a7
Deleted: sha256:6e43279655973e51749e6c13dbf63733802071ff665927375f9f98827857b548
Deleted: sha256:544fc6ed244eef6449d95305179600648f339c0adbcbcbf93cc4f9e402122c53
Deleted: sha256:6810a2c88653fe864294296c70a5a657caa0f638689ff58f13493acc532f5c77
Untagged: 127.0.0.1:5001/elasticservice:1.3
Untagged:
127.0.0.1:5001/elasticservice@sha256:bf0293e69d144bbf2dbd4192f59884fb596629bb6b1b09522a75bd599b2461b2
Untagged: 127.0.0.1:5000/elasticservice:1.3
Untagged:
127.0.0.1:5000/elasticservice@sha256:bf0293e69d144bbf2dbd4192f59884fb596629bb6b1b09522a75bd599b2461b2
Untagged: elasticservice:1.3
Deleted: sha256:c6cd18e3bcc36ab60a3d741e8fa6ec166ec53de742cd959fbef572b2d6e75fdb
Deleted: sha256:be5892dd6be6e671d8dbf07949d2559cdd43ccc537a0cb4f18ee4b74f634238c
Deleted: sha256:e0f9a768f8fc9a173f00b6babcb017789713195b566f97470d9501bbbbba8e74
Deleted: sha256:213b03f962fe9b6df0da77ccabe174c74ccb790d084a25f7221076f45958ced9
Deleted: sha256:1ef5822648e60b2be83c8641db64375be04ecb6f5acd66a142919e14f8af3b4d
Untagged: 127.0.0.1:5001/watchtower:2.1
Untagged:
127.0.0.1:5001/watchtower@sha256:793aee652b615cd3161c8dd9c60eb89b6afd684fc89c6518f84ff71563bee99e
Untagged: 127.0.0.1:5000/watchtower:2.1
Untagged:
127.0.0.1:5000/watchtower@sha256:793aee652b615cd3161c8dd9c60eb89b6afd684fc89c6518f84ff71563bee99e
Untagged: watchtower:2.1
Deleted: sha256:b44bcfbcd001b7c85a2028e813ef6919e316d6af37732a092151639d1c3d2b45
Deleted: sha256:3d30de4d2f50296af6affe5baa20e58a91b84abab65f89cb379ac78308c47b1e
Deleted: sha256:a066f951d571bcead85b9a6530b14a7b82cca834a174c28de1bc037bb80a2edd
Deleted: sha256:cf95f9ed8314cec412869a95a1a50b7b7d04f29bbc5b8a3d149a424ca6c83e49
Untagged: 127.0.0.1:5001/eplui:2.2
Untagged:
127.0.0.1:5001/eplui@sha256:af90fd9362f9244ed03bdd13318f6123817a7be64e089c42f5094fd570ebb03d
Untagged: 127.0.0.1:5000/eplui:2.2
Untagged:
127.0.0.1:5000/eplui@sha256:af90fd9362f9244ed03bdd13318f6123817a7be64e089c42f5094fd570ebb03d
Untagged: eplui:2.2
Deleted: sha256:5cca4a674f345d289c814ae0a3f24ec9aac76937046beb4273b51cc29c4b6408
Deleted: sha256:d6886b2e02aaf7ebf7cfd0423bedffbd27905d12f81d0908d4ab02b2e9973cc1
Deleted: sha256:301f9eb3ba05164dbd29cab2c93dad24e5e1fea3cf2abd2f1585c25df6a75c34
Deleted: sha256:0af470c810372aa3ecee7f4f5b6cdbab0dc857ef371d658668bb43fb2e50f2ef
Checking and starting a writable registry
Error response from daemon: no such image: AfwAppRegistry: invalid reference format:
repository name must be lowercase
f11dc4cb9677d2cb7e0fe215050f69fdbb60ed583762f3867290c8ae4a712b2a
Achieved Pause state for all services, Now Patching services
Loading Images into the writable registry
Loaded image: eplui:2.2
Loaded image: dcnmelastic:6.8.3_11.5.2
```

```
Loaded image: elasticservice:1.3
Loaded image: watchtower:2.1
The push refers to a repository [127.0.0.1:5000/dcnmelastic]
97da84f99ba3: Preparing
a0bb674f2b12: Preparing
1d07ed4e39fa: Preparing
8d8a48fd5741: Preparing
b14eb3458281: Preparing
f13999d3b63e: Preparing
d1c75bcbeb10: Preparing
f51f8d284b3b: Preparing
617b86abcd6d: Preparing
d3071a656898: Preparing
0bcab5b3cf37: Preparing
5d50c3ca45af: Preparing
9785ac5771f5: Preparing
d1c75bcbeb10: Waiting
d3071a656898: Waiting
f51f8d284b3b: Waiting
5d50c3ca45af: Waiting
617b86abcd6d: Waiting
fbb373121c59: Preparing
7b9f72883f99: Preparing
9785ac5771f5: Waiting
fbb373121c59: Waiting
5fb2dee77c93: Preparing
bc2717dd2942: Preparing
7b9f72883f99: Waiting
5fb2dee77c93: Waiting
bc2717dd2942: Waiting
0bcab5b3cf37: Waiting
1d07ed4e39fa: Pushed
97da84f99ba3: Pushed
a0bb674f2b12: Pushed
8d8a48fd5741: Pushed
b14eb3458281: Pushed
d1c75bcbeb10: Pushed
f13999d3b63e: Pushed
f51f8d284b3b: Pushed
617b86abcd6d: Pushed
d3071a656898: Layer already exists
0bcab5b3cf37: Layer already exists
5d50c3ca45af: Layer already exists
fbb373121c59: Layer already exists
9785ac5771f5: Layer already exists
7b9f72883f99: Layer already exists
5fb2dee77c93: Layer already exists
bc2717dd2942: Layer already exists
6.8.3_11.5.2: digest: sha256:0e407eefbc956a3e4c5b1705ab3add29c883e63da1b84d8e89f2345fe2fc557f
 size: 3882
The push refers to a repository [127.0.0.1:5000/elasticservice]
e9e60715acea: Preparing
83082b3681a8: Preparing
ec805d3c2de0: Preparing
fa8a90cb6518: Preparing
5d50c3ca45af: Preparing
9785ac5771f5: Preparing
fbb373121c59: Preparing
7b9f72883f99: Preparing
5fb2dee77c93: Preparing
bc2717dd2942: Preparing
fbb373121c59: Waiting
7b9f72883f99: Waiting
5fb2dee77c93: Waiting
```

```
bc2717dd2942: Waiting
9785ac5771f5: Waiting
5d50c3ca45af: Layer already exists
9785ac5771f5: Layer already exists
fbb373121c59: Layer already exists
fa8a90cb6518: Pushed
5fb2dee77c93: Layer already exists
bc2717dd2942: Layer already exists
e9e60715acea: Pushed
83082b3681a8: Pushed
7b9f72883f99: Layer already exists
ec805d3c2de0: Pushed
1.3: digest: sha256:ece5bb0b46547a166907f38f4958e40fd5202bf015728ea89dda2af342d28727 size:
 2422
The push refers to a repository [127.0.0.1:5000/watchtower]
7bb58c00bab0: Preparing
69c967d71211: Preparing
ea7268754985: Preparing
5d50c3ca45af: Preparing
9785ac5771f5: Preparing
fbb373121c59: Preparing
7b9f72883f99: Preparing
5fb2dee77c93: Preparing
bc2717dd2942: Preparing
7b9f72883f99: Waiting
5fb2dee77c93: Waiting
bc2717dd2942: Waiting
fbb373121c59: Waiting
5d50c3ca45af: Layer already exists
9785ac5771f5: Layer already exists
7b9f72883f99: Layer already exists
fbb373121c59: Layer already exists
5fb2dee77c93: Layer already exists
bc2717dd2942: Layer already exists
7bb58c00bab0: Pushed
ea7268754985: Pushed
69c967d71211: Pushed
2.1: digest: sha256:2aeded0fa00d3c92c4e78a5339eb116e27b0ac5fbed36c241fd26676a6642d91 size:
 2214
The push refers to a repository [127.0.0.1:5000/eplui]
4d33a08042c4: Preparing
a6480cd96594: Preparing
53cebfe822f4: Preparing
5d50c3ca45af: Preparing
9785ac5771f5: Preparing
fbb373121c59: Preparing
7b9f72883f99: Preparing
5fb2dee77c93: Preparing
bc2717dd2942: Preparing
7b9f72883f99: Waiting
fbb373121c59: Waiting
5fb2dee77c93: Waiting
9785ac5771f5: Layer already exists
5d50c3ca45af: Layer already exists
fbb373121c59: Layer already exists
4d33a08042c4: Pushed
53cebfe822f4: Pushed
7b9f72883f99: Layer already exists
bc2717dd2942: Layer already exists
5fb2dee77c93: Layer already exists
a6480cd96594: Pushed
2.2: digest: sha256:6a6b2266bb21bbcb88cd2fc3f01c7127d2793b663026ffa88d0665eb82f8d354 size:
 2214
AfwAppRegistry
```

```
Loaded images, now unpausing services
pauseAfwApp: calling PUT with  {unpause}

HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:30:22 GMT
Content-Length : 100
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Running for elasticsearch_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {unpause}

HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:30:43 GMT
Content-Length : 97
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Running for watchtower_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {unpause}

HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:31:04 GMT
Content-Length : 92
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Running for eplui_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {unpause}

HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:31:25 GMT
Content-Length : 101
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Running for elasticservice_Cisco_afw. Check for status"
}
Nothing to Patch in NI Base image is not installed here
==== Fri Dec 17 11:30:45 PST 2021 - Task updateAfwApps finished ====
==== Fri Dec 17 11:30:45 PST 2021 - Task disableAppsOnStandby started ====

Stopping HA apps on Standby node
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.

==== Fri Dec 17 11:31:45 PST 2021 - Task disableAppsOnStandby finished ====

==== Fri Dec 17 11:31:45 PST 2021 - Task stopDcnmServer started ====
==== Fri Dec 17 11:31:45 PST 2021 - Trying to upgrade your DCNM, so stopping the dcnm to
proceed... ====
Stopping FMServer (via systemctl):  [  OK  ]
==== Fri Dec 17 11:32:20 PST 2021 - Task stopDcnmServer finished ====
==== Fri Dec 17 11:32:20 PST 2021 - Task updatePackagedFiles started ====
==== Fri Dec 17 11:32:20 PST 2021 - Updating packaged-files ====
==== Fri Dec 17 11:32:20 PST 2021 - Task updatePackagedFiles finished ====
==== Fri Dec 17 11:32:20 PST 2021 - Task updateFmServer started ====
==== Fri Dec 17 11:32:20 PST 2021 - Updating FMServer ====
```

```
==== Fri Dec 17 11:32:20 PST 2021 - Backing up dcm.ear ====
==== Fri Dec 17 11:32:21 PST 2021 - Applying patch... ====
Patching ear file, please wait...
Patching war file, please wait...
==== Fri Dec 17 11:32:30 PST 2021 - Task updateFmServer finished ====
==== Fri Dec 17 11:32:30 PST 2021 - Task updatePatchList started ====
==== Fri Dec 17 11:32:30 PST 2021 - Task updatePatchList finished ====
==== Fri Dec 17 11:32:30 PST 2021 - Task startDcnmServer started ====
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO:  Resource is stopped
Done.

==== Fri Dec 17 11:33:23 PST 2021 - Task startDcnmServer finished ====
==== Fri Dec 17 11:33:23 PST 2021 - Task completeUpgrade started ====

********************************************************************************
Inline upgrade of this Standalone DCNM node is complete.

==== Sat Dec 17 11:33:23 PST 2021 - Task completeUpgrade finished ====
********************************************************************************
```

Sample output to install SMU in DCNM Native HA Deployment

This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

Installing DCNM SMU for Release 11.5(x) on Active Node

```
============================================================
============ Inline Upgrade to DCNM 11.5(x)-p1 =============
============================================================
Upgrading from version: 11.5(x)
Upgrading from install option: LAN Fabric
System type: HA
Compute only: No
Do you want to continue and perform the inline upgrade to 11.5(x)-p1? [y/n]: y

==== Fri Dec 17 11:26:51 PST 2021 - Task checkAfwStatus started ====
==== Fri Dec 17 11:26:51 PST 2021 - Task checkAfwStatus finished ====
==== Fri Dec 17 11:26:51 PST 2021 - Task updateAfwApps started ====
==== Fri Dec 17 11:26:51 PST 2021 - Updating AFW applications ====
Pausing Services that need to be patched
Deleted Containers:
992d06574c57882cf1a86bf7c19414055c6f501073a262b9e97cee0a75718a55
324f8ecfc34223f9d71abb86a807af54a720b40121aa8f38f6aa2dccbc233071
f7fe8656838af352d0d128163b1e9e4dcca9e5b73ea3a0956e4199e867f69a34
ab0f0dd90b98dacca8e01c944c6b07390bad8cd8247cf8cdf7629503bd01d252
52d0d5ad7edf990424b43c57d95ba836191fa913e556e6c1b75a65f171de6be6
4daf92fd8ba5445a81913df573343c0d6617b436330d103b8abf631a477c9b91
786768ab289596fbfb3904b1115a14717057bc83a06e555aa1abb76abb4c3a9e
1f5f52c42e532b4be9cff0eb22844824d969c6838436b98251236efdf4f85f57
b780eff0776d9dfa752ef28446dcaffcffffac6ac20a2b41738ac23e6d060ed3
756097c7bd5028ee5eafc74c7fb90eae20104b1584f2611ea1b3089340d0011c
Total reclaimed space: 1.418MB

pauseAfwApp: calling PUT with {pause}
pauseAfwApp: value of Wait: false
HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:26:52 GMT
Content-Length : 99
Content-Type : text/plain; charset=utf-8
{
```

```
"ResponseType": 0,
"Response": "Application is Paused for elasticsearch_Cisco_afw. Check for status"
}

pauseAfwApp: calling PUT with {pause}
pauseAfwApp: value of Wait: false
HTTP/1.1 200 OK
Content-Length : 96
Content-Type : text/plain; charset=utf-8
Date : Fri, 17 Dec 2021 19:27:12 GMT
{
"ResponseType": 0,
"Response": "Application is Paused for watchtower_Cisco_afw. Check for status"
}

pauseAfwApp: calling PUT with {pause}
pauseAfwApp: value of Wait: false
HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:27:32 GMT
Content-Length : 91
Content-Type : text/plain; charset=utf-8
{
"ResponseType": 0,
"Response": "Application is Paused for eplui_Cisco_afw. Check for status"
}

pauseAfwApp: calling PUT with {pause}
pauseAfwApp: value of Wait: false
HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:27:52 GMT
Content-Length : 100
Content-Type : text/plain; charset=utf-8
{
"ResponseType": 0,
"Response": "Application is Paused for elasticservice_Cisco_afw. Check for status"
}

Now Removing Images from Runtime
Untagged: 127.0.0.1:5001/dcnmelastic:6.8.3_11.5.2
Untagged:
127.0.0.1:5001/dcnmelastic@sha256:a872d49e3b5a0fc58ec9c1e8d8908c62604258cbfb1a02ac418227ed7f928128
Untagged: 127.0.0.1:5000/dcnmelastic:6.8.3_11.5.2
Untagged:
127.0.0.1:5000/dcnmelastic@sha256:a872d49e3b5a0fc58ec9c1e8d8908c62604258cbfb1a02ac418227ed7f928128
Untagged: dcnmelastic:6.8.3_11.5.2
Deleted: sha256:0173109c0612f48ed4165de7e5fa96f2243fe48756405bd0a0b4f12279785db1
Deleted: sha256:8d0b16f607caee532685643cf21550079881b67db9edf7d54a50ba4dec673c45
Deleted: sha256:63f9d6a3667c56f4a64d986b13b0059353fb983495b34f840b6a38c63e39938c
Deleted: sha256:af6e5eed783b56a675c53698ad4d374a77222218ebf706ad9891785b4ec2a537
Deleted: sha256:37dab1fa0ee831d1979104edd0ea820a1b3de3fe818aa75200021f868b221998
Deleted: sha256:cf1569581d9385a63ebd156e15dc795ab82de8d0a27fc5a3205dac339b591ee5
Deleted: sha256:3d293d026d9a7552a3630a75500d860083763a558191e1f28ebb6344c985b09d
Deleted: sha256:b285cfcb6bcb0850c0121d404c51ef0a333380cf332b3b776e75b45a94c2e8a7
Deleted: sha256:6e43279655973e51749e6c13dbf63733802071ff665927375f9f98827857b548
Deleted: sha256:544fc6ed244eef6449d95305179600648f339c0adbcbcbf93cc4f9e402122c53
Deleted: sha256:6810a2c88653fe864294296c70a5a657caa0f638689ff58f13493acc532f5c77

Untagged: 127.0.0.1:5001/elasticservice:1.3
Untagged:
127.0.0.1:5001/elasticservice@sha256:bf0293e69d144bbf2dbd4192f59884fb596629bb6b1b09522a75bd599b2461b2
Untagged: 127.0.0.1:5000/elasticservice:1.3
Untagged:
127.0.0.1:5000/elasticservice@sha256:bf0293e69d144bbf2dbd4192f59884fb596629bb6b1b09522a75bd599b2461b2
Untagged: elasticservice:1.3
```

```
Deleted: sha256:c6cd18e3bcc36ab60a3d741e8fa6ec166ec53de742cd959fbef572b2d6e75fdb
Deleted: sha256:be5892dd6be6e671d8dbf07949d2559cdd43ccc537a0cb4f18ee4b74f634238c
Deleted: sha256:e0f9a768f8fc9a173f00b6babcb017789713195b566f97470d9501bbbbba8e74
Deleted: sha256:213b03f962fe9b6df0da77ccabe174c74ccb790d084a25f7221076f45958ced9
Deleted: sha256:1ef5822648e60b2be83c8641db64375be04ecb6f5acd66a142919e14f8af3b4d

Untagged: 127.0.0.1:5001/watchtower:2.1
Untagged:
127.0.0.1:5001/watchtower@sha256:793aee652b615cd3161c8dd9c60eb89b6afd684fc89c6518f84ff71563bee99e
Untagged: 127.0.0.1:5000/watchtower:2.1
Untagged:
127.0.0.1:5000/watchtower@sha256:793aee652b615cd3161c8dd9c60eb89b6afd684fc89c6518f84ff71563bee99e
Untagged: watchtower:2.1

Deleted: sha256:b44bcfbcd001b7c85a2028e813ef6919e316d6af37732a092151639d1c3d2b45
Deleted: sha256:3d30de4d2f50296af6affe5baa20e58a91b84abab65f89cb379ac78308c47b1e
Deleted: sha256:a066f951d571bcead85b9a6530b14a7b82cca834a174c28de1bc037bb80a2edd
Deleted: sha256:cf95f9ed8314cec412869a95a1a50b7b7d04f29bbc5b8a3d149a424ca6c83e49

Untagged: 127.0.0.1:5001/eplui:2.2
Untagged:
127.0.0.1:5001/eplui@sha256:af90fd9362f9244ed03bdd13318f6123817a7be64e089c42f5094fd570ebb03d
Untagged: 127.0.0.1:5000/eplui:2.2
Untagged:
127.0.0.1:5000/eplui@sha256:af90fd9362f9244ed03bdd13318f6123817a7be64e089c42f5094fd570ebb03d
Untagged: eplui:2.2

Deleted: sha256:5cca4a674f345d289c814ae0a3f24ec9aac76937046beb4273b51cc29c4b6408
Deleted: sha256:d6886b2e02aaf7ebf7cfd0423bedffbd27905d12f81d0908d4ab02b2e9973cc1
Deleted: sha256:301f9eb3ba05164dbd29cab2c93dad24e5e1fea3cf2abd2f1585c25df6a75c34
Deleted: sha256:0af470c810372aa3ecee7f4f5b6cdbab0dc857ef371d658668bb43fb2e50f2ef

Checking and starting a writable registry
Error response from daemon: no such image: AfwAppRegistry: invalid reference format:
repository name must be lowercase
f11dc4cb9677d2cb7e0fe215050f69fdbb60ed583762f3867290c8ae4a712b2a
Achieved Pause state for all services, Now Patching services
Loading Images into the writable registry
Loaded image: eplui:2.2
Loaded image: dcnmelastic:6.8.3_11.5.2
Loaded image: elasticservice:1.3
Loaded image: watchtower:2.1

The push refers to a repository [127.0.0.1:5000/dcnmelastic]
97da84f99ba3: Preparing
a0bb674f2b12: Preparing
1d07ed4e39fa: Preparing
8d8a48fd5741: Preparing
b14eb3458281: Preparing
f13999d3b63e: Preparing
d1c75bcbeb10: Preparing
f51f8d284b3b: Preparing
617b86abcd6d: Preparing
d3071a656898: Preparing
0bcab5b3cf37: Preparing
5d50c3ca45af: Preparing
9785ac5771f5: Preparing
d1c75bcbeb10: Waiting
d3071a656898: Waiting
f51f8d284b3b: Waiting
5d50c3ca45af: Waiting
617b86abcd6d: Waiting
fbb373121c59: Preparing
```

```
7b9f72883f99: Preparing
9785ac5771f5: Waiting
fbb373121c59: Waiting
5fb2dee77c93: Preparing
bc2717dd2942: Preparing
7b9f72883f99: Waiting
5fb2dee77c93: Waiting
bc2717dd2942: Waiting
0bcab5b3cf37: Waiting
1d07ed4e39fa: Pushed
97da84f99ba3: Pushed
a0bb674f2b12: Pushed
8d8a48fd5741: Pushed
b14eb3458281: Pushed
d1c75bcbeb10: Pushed
f13999d3b63e: Pushed
f51f8d284b3b: Pushed
617b86abcd6d: Pushed
d3071a656898: Layer already exists
0bcab5b3cf37: Layer already exists
5d50c3ca45af: Layer already exists
fbb373121c59: Layer already exists
9785ac5771f5: Layer already exists
7b9f72883f99: Layer already exists
5fb2dee77c93: Layer already exists
bc2717dd2942: Layer already exists
6.8.3_11.5.2: digest: sha256:0e407eefbc956a3e4c5b1705ab3add29c883e63da1b84d8e89f2345fe2fc557f
 size: 3882

The push refers to a repository [127.0.0.1:5000/elasticservice]
e9e60715acea: Preparing
83082b3681a8: Preparing
ec805d3c2de0: Preparing
fa8a90cb6518: Preparing
5d50c3ca45af: Preparing
9785ac5771f5: Preparing
fbb373121c59: Preparing
7b9f72883f99: Preparing
5fb2dee77c93: Preparing
bc2717dd2942: Preparing
fbb373121c59: Waiting
7b9f72883f99: Waiting
5fb2dee77c93: Waiting
bc2717dd2942: Waiting
9785ac5771f5: Waiting
5d50c3ca45af: Layer already exists
9785ac5771f5: Layer already exists
fbb373121c59: Layer already exists
fa8a90cb6518: Pushed
5fb2dee77c93: Layer already exists
bc2717dd2942: Layer already exists
e9e60715acea: Pushed
83082b3681a8: Pushed
7b9f72883f99: Layer already exists
ec805d3c2de0: Pushed
1.3: digest: sha256:ece5bb0b46547a166907f38f4958e40fd5202bf015728ea89dda2af342d28727 size:
 2422

The push refers to a repository [127.0.0.1:5000/watchtower]
7bb58c00bab0: Preparing
69c967d71211: Preparing
ea7268754985: Preparing
5d50c3ca45af: Preparing
9785ac5771f5: Preparing
```

```
fbb373121c59: Preparing
7b9f72883f99: Preparing
5fb2dee77c93: Preparing
bc2717dd2942: Preparing
7b9f72883f99: Waiting
5fb2dee77c93: Waiting
bc2717dd2942: Waiting
fbb373121c59: Waiting
5d50c3ca45af: Layer already exists
9785ac5771f5: Layer already exists
7b9f72883f99: Layer already exists
fbb373121c59: Layer already exists
5fb2dee77c93: Layer already exists
bc2717dd2942: Layer already exists
7bb58c00bab0: Pushed
ea7268754985: Pushed
69c967d71211: Pushed
2.1: digest: sha256:2aeded0fa00d3c92c4e78a5339eb116e27b0ac5fbed36c241fd26676a6642d91 size:
 2214

The push refers to a repository [127.0.0.1:5000/eplui]
4d33a08042c4: Preparing
a6480cd96594: Preparing
53cebfe822f4: Preparing
5d50c3ca45af: Preparing
9785ac5771f5: Preparing
fbb373121c59: Preparing
7b9f72883f99: Preparing
5fb2dee77c93: Preparing
bc2717dd2942: Preparing
7b9f72883f99: Waiting
fbb373121c59: Waiting
5fb2dee77c93: Waiting
9785ac5771f5: Layer already exists
5d50c3ca45af: Layer already exists
fbb373121c59: Layer already exists
4d33a08042c4: Pushed
53cebfe822f4: Pushed
7b9f72883f99: Layer already exists
bc2717dd2942: Layer already exists
5fb2dee77c93: Layer already exists
a6480cd96594: Pushed
2.2: digest: sha256:6a6b2266bb21bbcb88cd2fc3f01c7127d2793b663026ffa88d0665eb82f8d354 size:
 2214

AfwAppRegistry
Loaded images, now unpausing services
pauseAfwApp: calling PUT with {unpause}
HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:30:22 GMT
Content-Length : 100
Content-Type : text/plain; charset=utf-8
{
"ResponseType": 0,
"Response": "Application is Running for elasticsearch_Cisco_afw. Check for status"
}

pauseAfwApp: calling PUT with {unpause}
HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:30:43 GMT
Content-Length : 97
Content-Type : text/plain; charset=utf-8
{
"ResponseType": 0,
```

```
"Response": "Application is Running for watchtower_Cisco_afw. Check for status"
}

pauseAfwApp: calling PUT with {unpause}
HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:31:04 GMT
Content-Length : 92
Content-Type : text/plain; charset=utf-8
{
"ResponseType": 0,
"Response": "Application is Running for eplui_Cisco_afw. Check for status"
}

pauseAfwApp: calling PUT with {unpause}
HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:31:25 GMT
Content-Length : 101
Content-Type : text/plain; charset=utf-8
{
"ResponseType": 0,
"Response": "Application is Running for elasticservice_Cisco_afw. Check for status"
}

Nothing to Patch in NI Base image is not installed here
==== Fri Dec 17 11:30:45 PST 2021 - Task updateAfwApps finished ====
==== Fri Dec 17 11:30:45 PST 2021 - Task disableAppsOnStandby started ====
Stopping HA apps on Standby node
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.

==== Fri Dec 17 11:31:45 PST 2021 - Task disableAppsOnStandby finished ====
==== Fri Dec 17 11:31:45 PST 2021 - Task stopDcnmServer started ====
==== Fri Dec 17 11:31:45 PST 2021 - Trying to upgrade your DCNM, so stopping the dcnm to
proceed... ====
Stopping FMServer (via systemctl): [ OK ]
==== Fri Dec 17 11:32:20 PST 2021 - Task stopDcnmServer finished ====
==== Fri Dec 17 11:32:20 PST 2021 - Task updatePackagedFiles started ====
==== Fri Dec 17 11:32:20 PST 2021 - Updating packaged-files ====
==== Fri Dec 17 11:32:20 PST 2021 - Task updatePackagedFiles finished ====
==== Fri Dec 17 11:32:20 PST 2021 - Task updateFmServer started ====
==== Fri Dec 17 11:32:20 PST 2021 - Updating FMServer ====
==== Fri Dec 17 11:32:20 PST 2021 - Backing up dcm.ear ====
==== Fri Dec 17 11:32:21 PST 2021 - Applying patch... ====

Patching ear file, please wait...
Patching war file, please wait...

==== Fri Dec 17 11:32:30 PST 2021 - Task updateFmServer finished ====
==== Fri Dec 17 11:32:30 PST 2021 - Task updatePatchList started ====
==== Fri Dec 17 11:32:30 PST 2021 - Task updatePatchList finished ====
==== Fri Dec 17 11:32:30 PST 2021 - Task startDcnmServer started ====

Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO: Resource is stopped
Done.
==== Fri Dec 17 11:33:23 PST 2021 - Task startDcnmServer finished ====
==== Fri Dec 17 11:33:23 PST 2021 - Task completeUpgrade started ====
********************************************************************************
```

```
Inline upgrade of this Active DCNM node is complete.
Please wait until this node is Active again
before upgrading the Standby node.
==== Sat Dec 17 11:33:23 PST 2021 - Task completeUpgrade finished ====
```

Installing DCNM SMU for Release 11.5(x) on Standby Node

```
[root@dcnm2]# ./inline-upgrade.sh --standby

============================================================
============ Inline Upgrade to DCNM 11.5(x)-p1 =============
============================================================
Upgrading from version: 11.5(x)
Upgrading from install option: LAN Fabric
System type: HA
Compute only: No
Do you want to continue and perform the inline upgrade to 11.5(x)-p2? [y/n]: y

==== Fri Dec 17 18:15:05 PST 2021 - Task checkAfwStatus started ====
==== Fri Dec 17 18:15:05 PST 2021 - Task checkAfwStatus finished ====
==== Fri Dec 17 18:15:05 PST 2021 - Task updateAfwApps started ====
==== Fri Dec 17 18:15:05 PST 2021 - Task updateAfwApps finished ====
==== Fri Dec 17 18:15:05 PST 2021 - Task disableAppsOnStandby started ====
==== Fri Dec 17 18:15:05 PST 2021 - Task disableAppsOnStandby finished ====
==== Fri Dec 17 18:16:05 PST 2021 - Task stopDcnmServer started ====
==== Fri Dec 17 18:16:05 PST 2021 - Task stopDcnmServer finished ====
==== Fri Dec 17 18:16:05 PST 2021 - Task updatePackagedFiles started ====
==== Fri Dec 17 18:16:05 PST 2021 - Updating packaged-files ====
==== Fri Dec 17 18:16:05 PST 2021 - Task updatePackagedFiles finished ====
==== Fri Dec 17 18:16:05 PST 2021 - Task updateFmServer started ====
==== Fri Dec 17 18:16:05 PST 2021 - Updating FMServer ====
==== Fri Dec 17 18:16:05 PST 2021 - Backing up dcm.ear ====
==== Fri Dec 17 18:16:07 PST 2021 - Applying patch... ====

Patching ear file, please wait...
Patching war file, please wait...

==== Fri Dec 17 18:16:21 PST 2021 - Task updateFmServer finished ====
==== Fri Dec 17 18:16:21 PST 2021 - Task updatePatchList started ====
==== Fri Dec 17 18:16:21 PST 2021 - Task updatePatchList finished ====
==== Fri Dec 17 18:16:21 PST 2021 - Task startDcnmServer started ====

updating the Navigation file
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO: Resource is stopped
Done.
==== Fri Dec 17 18:16:25 PST 2021 - Task startDcnmServer finished ====
==== Fri Dec 17 18:16:25 PST 2021 - Task completeUpgrade started ====

********************************************************************************
Inline upgrade of the HA DCNM system is complete.
********************************************************************************
==== Fri Dec 17 18:16:25 PST 2021 - Task completeUpgrade finished ===
```

Sample Output to Install SMU in DCNM Compute Nodes

This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

```
[root@dcnm-compute1]# ./inline-upgrade.sh
============================================================
============ Inline Upgrade to DCNM 11.5(x)-p1 =============
```

```
============================================================

Upgrading from version: 11.5(x)
Upgrading from install option: N/A
System type: HA
Compute only: Yes

********************************************************************************
ALERT: AFTER THE UPGRADE MAKE SURE COMPUTE NODE IS BACK IN JOINED STATE.
USE DCNM "APPLICATIONS->COMPUTE" GUI TO CHECK STATUS
********************************************************************************

Do you want to continue and perform the inline upgrade to 11.5(x)-p1? [y/n]: y

==== Fri Dec 17 20:36:14 PST 2021 - Task updatePackagedFiles started ====
==== Fri Dec 17 20:36:14 PST 2021 - Updating packaged-files ====
==== Fri Dec 17 20:36:14 PST 2021 - Task updatePackagedFiles finished ====
==== Fri Dec 17 20:36:14 PST 2021 - Task updatePatchList started ====
==== Fri Dec 17 20:36:14 PST 2021 - Task updatePatchList finished ====
==== Fri Dec 17 20:36:14 PST 2021 - Task completeUpgrade started ====
********************************************************************************
Inline updgrade of this compute is complete
********************************************************************************
==== Fri Dec 17 20:36:14 PST 2021 - Task completeUpgrade finished ====
```

Scanning for Log4j2 Vulnerabilities

Download a scanner (such as logpresso) from https://github.com/logpresso/CVE-2021-44228-Scanner.

Warning Use this utility only to scan for vulnerabilities. DO NOT use it to fix anything in the system.

Caution After installing the SMU, ensure that the DCNM Web UI is up and running. Also, ensure that all the processes are up and running, by using the **appmgr status all** command. Ensure that the **Applications > Compute** shows all nodes in **Joined** state.

Before running the scan again, clear the old docker images that are no longer used, by using the following command:

If **docker ps -a** shows many containers in Exited state, then first run the following:

```
docker container prune
WARNING! This will remove all stopped containers.
Are you sure you want to continue? [y/N] y
Deleted Containers:
33d2a44706663870d062b7ee8b4aba18ea94ea6fdc285b6ba1d133334f226d73
9fba3140120f7fbc41993a97d0bc6bec254ffed638da1445e3a91fb04614cba6
67d4cd575d1febdec54fe161d716334908eb18d1a9a5d053a8f21ed1e3089d8c
4b8f2463cf899341fd5a028078a3d6b98790807db1ba6f6ece13a5a0a7783749
5b066b6eb334986d0cb0442249218d8582936439f8c8b3a3c81426ab81beaac3
14b965917498dcaaaa3e586d0d65e702d884c3cef7e425e60215a192cbff9945
359ab2ca568d10c42e406fec6a6f7499637936080b0ca109e307c51ca9431532
a18a752de7208d3802989f9209893140cac404cf33dcdf5cb362ebbddbde4e04
519e0e7654ecff8601f868c2a55fd1507a9ce52d137c33c79067fe3d7f834048
03e0c0ccaa35e2b4d07c6afae90c758f3db5ea639528afcc550a26e9c1ef1b43
Total reclaimed space: 155.4MB
```

If there are no containers in Exited state, then you can directly run the **docker image prune** to clean up the old images, as follows:

```
docker image prune –a
WARNING! This will remove all images without at least one container associated to them.
Are you sure you want to continue? [y/N] y
Deleted Images:
untagged: 127.0.0.1:5001/eplui:2.1
untagged:
127.0.0.1:5001/eplui@sha256:6b788e837561f5b56378d9872885abd078105b6e18f17f8b28ff7d58106288ed
deleted: sha256:9a9bb56bcf9e5807e25743522e7cc3b7946ca39b875418b5f85894b383443276
deleted: sha256:d09c3547766a3130d2e48d85d5c33304fd912abbcc0fd8f6d877ca4a5a7513d8
deleted: sha256:19acc971e6674459c817bd011ed8e5969bc4f47f3f733fe9ffb617227d5081e0
deleted: sha256:5f5a7996ee7ba7d79772caa9a24f95cceb8463bab030c7ed8f534b14eda099db
untagged: 127.0.0.1:5001/elasticservice:1.1
untagged:
127.0.0.1:5001/elasticservice@sha256:b7b7a082aa225301e92c55ab93647a7f4e5b49e28152733075995a6b237aa798
deleted: sha256:f9078f534739f1367d9a67187f14f4c32cc9fc904c8fd6579564c848b06f9185
deleted: sha256:f0e44e2f9afc9e180056d5bc6fceed743c2d2e4936a71ae8feb2c5e317ccea25
deleted: sha256:0cab6e9119a4779b58e3f8a2ab48ec892db599ca53a784a63ed2d03aa422a87e
deleted: sha256:60546313de31095f5363f479ea12b74ff02375f96cb5ab5ba23e85027f3be2c4
deleted: sha256:c9d22e3ec2ce60122c9da1d8e8bafb18dd9b61db39c3e8e8ad70be6ec907c48c
untagged: dcnmelastic:6.8.3_11.4.1
deleted: sha256:9e6493318e1189b662683cb288532e9b3177464684e9c17f06ebcd1a6bd3c317
deleted: sha256:f1b3c86a97ad0767ffcc89c31b73d34643a2bb838e317c82f00167bb8cfb270e
deleted: sha256:19c89e64341aff41ec5508ebb2b73107fee9581d71d78b0787279817dd14facc
deleted: sha256:907f6e93fa619661d70a65dc3fd12d0257e3d7afb0ced3961620fa419c5dd792
deleted: sha256:044e562105291191158e417ae9d33dd16022a881562114a970d1fadb116e8e5a
deleted: sha256:48c418ce6e32de81f4171ae073e79b04b3c227afe5f4013e6a0bd5932eee3853
deleted: sha256:7b6c7e6083bffb94f1b9acd4f83acec0f4cdc0685efda47fb6a9735fb0c3ec65
deleted: sha256:59908c99dea86854472cb0d7b64236e4a903f815d652845f56ec30204a12f550
deleted: sha256:11124a752156a4ec945d79172f11be3f025c96f1989886dff9b0b3608303dc3e
untagged: kibana:2.0
deleted: sha256:ea95ed7a67f68301e64e46653af6864cb6e18e496e725432505595936b560f26
deleted: sha256:b153b99c46885f4cd2b05173fb1b5481bda9f10c39130e5cbb38b7cd18884508
deleted: sha256:02033d4e0a299ba71df33ceaff68959d74d4a62fc0be69b689a01e6322f8e64c
deleted: sha256:9ed6d76808f43ff63909ba38cdda9430109b4848c4cb5b7e8db63e9a9f5e9f7e
deleted: sha256:c4ca19d8d6603e6020c28b9eefba5fe056bab61099a7c15a1b0793281601ea54
deleted: sha256:eac1498f3113436c89751c285e6d52c13edfa05810abce2dc042c9750f4b64b6
deleted: sha256:5f265142267b87373fafa5ccff18c1d7f2c7ce8b25ad870263dba4a9ff3a8540
deleted: sha256:f98eb78bb8712f2786ef0580037d916d4ff0d3bf398900f093c94301cad4d705
deleted: sha256:6262d3d4d32bb0a107cfac0c58c563426fdc657116c903e36334a452a4818d68
deleted: sha256:045f4e8b3ed31fb7d27aa34e59cfdd2e8aa5b24d9cde5b84de18635a5b7f3765
deleted: sha256:af643141c457d060c8c88f4b3901d8404bab5b93abdcba1c5050666de50765e2
untagged: watchtower:2.1
deleted: sha256:0a54bd9e96a8483fdb76042b7906909aa1f3fd4deb513a5a7194a8aaf86af7dc
deleted: sha256:f8f11cb198e25e36212a5650d5b8fbcc9f4a515afe91e6d4e678d71c60d6040d
deleted: sha256:224ec704095b7d5d185a405f0e468bc015d6cb9c50cd3ab4ca9de092763ddc5a
deleted: sha256:45268517a253b8f483eedfa7f9f2641361d3f40d5e6f235f179ee3f583ebfc38
untagged: compliance:4.0.0
deleted: sha256:d6750c132fb5e9059f86d0d6b1f54bebd0f00d0b84ab9688813526bd63c6ced8
deleted: sha256:4d10e42b5db7aafabef673b889c6916e79c9f1cf6a5411304b02e158dfac0cbc
deleted: sha256:7ffadb4dd9f304c2d5314f66461d351622fe72e6c2a043942e0cd7fcc8aa2b66
deleted: sha256:516e697bbb7ff9ec971280964b9383fa22cc72ced415362720903ad5281c0852
deleted: sha256:0ef534a6e063d02b7bc5f1ff0a0053478502a8bc76f88cd2dddb58b8225c80a4
deleted: sha256:4a7f56d08ea1e6fcda2d9fd2b37c85eee0e963c9d8c6275997a4028171a15c07
deleted: sha256:544c874de2ace981da4bd06ee33cd8a00d03059b598cc4a02fc4ab9b57610133
deleted: sha256:5f0a9421371e6f218eaf9788eccfc987d40cc7c66291536465f271cf0abdcd04
deleted: sha256:c1968f6e62beccbad147b8f8d0a239b4d308133ee0bc77cd4ee9cfc941f29e50
deleted: sha256:aa9e87a76c7b54bb7dba91db45a84a23542bf647751fe1211764f1395f97ec6f
Total reclaimed space: 794.1MB
```

After that, the log4j scanner tool can be run. A sample post patch run output is depicted below:

CLI snap of a sample result - CVE-2021-44228 Vulnerability Scanner 2.3.6 (2021-12-20)

```
[root@dcnm]# ./log4j2-scan /
Logpresso CVE-2021-44228 Vulnerability Scanner 2.3.6 (2021-12-20)
Scanning directory: /, ./log4j2-scan, / (without devtmpfs, tmpfs, shm)
Running scan (10s): scanned 4653 directories, 41925 files, last visit:
/usr/local/cisco/dcm/fm/download
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/sandeployments/dcm.ear
(lib/log4j-core-2.16.0.jar), log4j 2.16.0
Running scan (26s): scanned 6980 directories, 62226 files, last visit:
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/sandeployments
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/tmp/vfs/deployment/deployment8848896c390adc/log4j-core-2.16.0.jar-f0e635d46279bf/log4j-core-2.16.0.jar,
 log4j 2.16.0
Running scan (36s): scanned 9856 directories, 90359 files, last visit:
/usr/local/cisco/dcm/wildfly-14.0.1.Final/modules/system/layers/base/org/infinispan/main
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/root/packaged-files/pmn/pmn-telemetry.jar, log4j 2.16.0
[*] Found CVE-2021-44228 (log4j 2.x) vulnerability in /root/patch-11.4.1-p2.backup/dcm.ear
 (lib/log4j-core-2.8.2.jar), log4j 2.8.2
Running scan (52s): scanned 24714 directories, 141807 files, last visit:
/root/patch-11.4.1-p2.backup
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/tmp/.inline-upgrade.16121/fmserver-patch/log4j-core-2.16.0.jar, log4j 2.16.0
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/tmp/.inline-upgrade.16121/fmserver-patch/dcm.ear (lib/log4j-core-2.16.0.jar), log4j 2.16.0
Running scan (62s): scanned 30813 directories, 183000 files, last visit:
/usr/share/elasticsearch/modules/lang-groovy
Running scan (72s): scanned 34709 directories, 216946 files, last visit:
/usr/local/cisco/dcm/smis/client/lib
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/sandeployments/dcm.ear
(lib/log4j-core-2.16.0.jar), log4j 2.16.0
Running scan (88s): scanned 36975 directories, 231284 files, last visit:
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/sandeployments
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/tmp/vfs/deployment/deployment8848896c390adc/log4j-core-2.16.0.jar-f0e635d46279bf/log4j-core-2.16.0.jar,
 log4j 2.16.0
Running scan (98s): scanned 39835 directories, 259398 files, last visit:
/usr/local/cisco/dcm/wildfly-14.0.1.Final/modules/system/layers/base/org/bouncycastle/main
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/root/packaged-files/pmn/pmn-telemetry.jar, log4j 2.16.0
[*] Found CVE-2021-44228 (log4j 2.x) vulnerability in /root/patch-11.4.1-p2.backup/dcm.ear
 (lib/log4j-core-2.8.2.jar), log4j 2.8.2
Running scan (114s): scanned 54709 directories, 310865 files, last visit:
/root/patch-11.4.1-p2.backup
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/tmp/.inline-upgrade.16121/fmserver-patch/log4j-core-2.16.0.jar, log4j 2.16.0
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/tmp/.inline-upgrade.16121/fmserver-patch/dcm.ear (lib/log4j-core-2.16.0.jar), log4j 2.16.0
Scanned 59990 directories and 338115 files
Found 12 vulnerable files
Found 0 potentially vulnerable files
Found 0 mitigated files
Completed in 124.16 seconds
```



Note Installing SMU on Cisco DCNM addresses CVE-2021-44228 and CVE-2021-45046. As CVE-2021-45105 is lower severity, and refers to an issue with a configuration which is not used in Cisco DCNM with the default shipping configuration. Therefore, CVE-2021-45105 is not addressed in this SMU installation.

The backup contains original unaltered files which are still vulnerable. They are not used, but are retained as a reference. If you choose to delete, no functionality will be impacted. There are few files which are inside of container filesystem layers. These files record the changes to the container filesystems and are not a concern until they do not appear in the “merged” container files. These files are not available to processes at run-time. There are no vulnerable files in the merged resultant container filesystems.

This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

Refer to Upgrading DCNM Release 11.5(x) from Previous Versions, on page 218 for instructions to install SMU on other DCNM releases. You can upgrade to DCNM Releases through multiple hops from Release 11.0 or later. The log4j2 scanner flags few stale docker/overlay related file system issues. Ensure that you validate the SMU installation. For more information, see Validating of SMU Installation, on page 218.



Note After DCNM HA failover, the log4j2 scan may show some vulnerabilities. This is due to the old docker image package bundle in the Standby server, which is not available for use at run-time for any process. If the CVE reports are still seen, execute the **docker image prune -a** command. This results in clearing the stale entries on the Standby node. After clearing stale entries, there will be no issues during further DCNM HA failovers. If the scan report still shows some CVE errors, we recommend that you contact Cisco TAC.

Validating of SMU Installation

This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

To validate that the patch has been successfully applied on Cisco DCNM appliances and Compute nodes, check the contents of the file located at **`/root/packaged-files/properties/dcnm-version.txt`**. If the patch is successfully applied, an extra line is included in the dcnm-version.txt as shown below:

PATCH_LIST=X

where,

X is the number of patches installed on your Cisco DCNM appliance.



Note After the SMU is installed, the **Health Monitor** application (previously known as **Watchtower**) will not display any old or new data.

Upgrading DCNM Release 11.5(x) from Previous Versions

When upgrading from an older DCNM 11.x version to 11.5(x) or higher, post upgrade and patch application, the log4j scanner may show more vulnerabilities related to findings in the **`/var/lib/docker/overlay`** file system. A sample output of a system upgraded from DCNM 11.2(1) to 11.5(1) is shown below after installing the SMU. The sample output shows multiple vulnerabilities all in the docker/overlay file system. The two vulnerabilities seen for **`docker/overlay2`** filesystem for elasticsearch doesn't cause any issues.

This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

```
./log4j2-scan /
Logpresso CVE-2021-44228 Vulnerability Scanner 2.2.0 (2021-12-18)
Scanning directory: / (without devtmpfs, tmpfs, shm)
[*] Found CVE-2021-44228 (log4j 2.x) vulnerability in
```

```
/var/lib/docker/overlay/2a7db7cebfce3ac7ca67206122b55e813ea19801593c433b5fd730c69d0a1b69/root/
usr/share/elasticsearch/lib/log4j-core-2.9.1.jar, log4j 2.9.1
[*] Found CVE-2021-44228 (log4j 2.x) vulnerability in /var/lib/docker/overlay/2811b1325950ad4c
438cdd1b2631adb0a1adfa0b49e474279f3499cfd2e49ad3/root/usr/share/elasticsearch/lib/log4j-core-2.9.1.jar,
 log4j 2.9.1
[*] Found CVE-2021-44228 (log4j 2.x) vulnerability in
/var/lib/docker/overlay/8b6416f75366e50688
1755714e39a6f23e581bb5886386eaab935f5d8ed923ad/root/usr/share/elasticsearch/lib/log4j-core-2.9.1.jar,
 log4j 2.9.1
.
..
...
Running scan (95s): scanned 223603 directories, 1965175 files, last visit:
/tmp/.inline-upgrade.11270/fmserver-patch
Running scan (107s): scanned 236660 directories, 2034298 files, last visit:
/usr/local/cisco/dcm/
wildfly-14.0.1.Final/standalone/sandeployments
[*] Found CVE-2021-44228 (log4j 2.x) vulnerability in /root/patch-11.5.1-p1.backup/dcm.ear
 (lib/
log4j-core-2.8.2.jar), log4j 2.8.2
Running scan (117s): scanned 243726 directories, 2095783 files, last visit:
/root/patch-11.5.1-p1.backup
Scanned 243914 directories and 2096444 files
Found 29 vulnerable files
Found 0 potentially vulnerable files
Found 0 mitigated files
Completed in 117.36 seconds
```

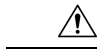
From DCNM release 11.3(1), the Application Framework uses the overlay2 file system for docker. You can verify by using the following command:

```
docker info | grep overlay2
Storage Driver: overlay2              /* above command must display this output*/
```

If the output of the above command indicates docker is using **overlay2**, the directory **`/var/lib/docker/overlay`** is not used, and therefore, the errors reported by scanner are remnants, and not used by any running service on the DCNM. To cleanup these remnants, please do the following on the node where errors are reported.

Remove the remnants on the node where additional vulnerabilities are reported by using the following command:

```
rm -rf /var/lib/docker/overlay
```



Caution Ensure that you execute the above command correctly. If overlay2 is deleted accidentally, the DCNM services will not be operational.

Run the log4j scanner. The displayed output shows that all the vulnerabilities related to **`/var/lib/docker/overlay`** are removed.