Cisco DCNM Installation and Upgrade Guide for SAN Deployment, Release 11.3(1)

First Published: 2019-12-20

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.

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

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

© 2019–2021 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Overview** 1

Introduction 1

Installation Options 2

Deployment Options 3

Upgrading Cisco DCNM 3

System Requirements 4

Clearing Browser Cache 10

CHAPTER 2 **Guidelines and Limitations** 13

Guidelines and Limitations 13

Checking TPM Partition before Converting DCNM-SE to Nexus Dashboard 14

CHAPTER 3 **Prerequisites** 17

General Prerequisites 17

Before you begin 17

Initial Setup Routine 18

Preparing to Configure the Switch 19

Default Login 20

Setup Options 20

Assigning Setup Information 21

Configuring Out-of-Band Management 21

Configuring In-Band Management 25

Using the setup Command 28

Starting a Switch in the Cisco MDS 9000 Family 29

Accessing the Switch 29

Prerequisites for Installing DCNM on Windows 30

Prerequisites for Installing DCNM on Linux 31
Antivirus exclusion 31
Oracle Database for DCNM Servers 32
Oracle SQLPlus Command-Line Tool 32
init.ora File 33
Backing up the Oracle Database 33
Preparing the Oracle Database 33
Logging Into Oracle 34
Increasing the SYSTEM Tablespace 34
Increasing the Number of Sessions and Processes to 150 Each 35
Increasing the Number of Open Cursors to 1000 35
Creating an Oracle DB User using the Command Prompt 36
Connecting to an Oracle RAC with SCAN Feature Type DB 37
Database for Federation Setup 37
Remote Oracle Database Utility Scripts for Backup and Restore 37
Local PostgreSQL Database Utility Scripts for Backup and Restore 38

CHAPTER 4 **Installing Cisco DCNM** 39
Installing Cisco DCNM on Windows 39
Uninstalling the Cisco DCNM on Windows 39
Downloading the Cisco DCNM Windows Installer and Properties File 40
Installing Cisco DCNM on Windows Using the GUI 40
Installing Cisco DCNM Windows in a Server Federation Environment using GUI 44
Installing Cisco DCNM Windows through Silent Installation 44
Installing Cisco DCNM on Linux 46
Uninstalling the Cisco DCNM on Linux 46
Downloading the Cisco DCNM Linux Installer and Properties File 47
Installing Cisco DCNM on Linux Using the GUI 48
Installing Cisco DCNM Linux in a Server Federation Environment Using GUI 51
Installing Cisco DCNM Linux Through Silent Installation 52
Installing DCNM on Open Virtual Appliance 53
Downloading the Open Virtual Appliance File 54
Deploying the Open Virtual Appliance as an OVF Template 54
Installing the Cisco DCNM OVA in Standalone Mode 58

Installing DCNM on ISO Virtual Appliance 61
Downloading the ISO Virtual Appliance File 61
Installing the DCNM ISO Virtual Appliance on UCS (Bare Metal) 62
Installing the DCNM ISO Virtual Appliance on KVM 69
Installing Cisco DCNM ISO in Standalone Mode 70
Launching SAN Client and Device Manager 73
Launching SAN Client and Device Manager from Web UI 74
Launching SAN Client and Device Manager from DCNM Server 74
Launching DCNM SAN Client from DCNM SAN for Windows deployment with Custom SSL Certificate 75
Launching DCNM SAN Client from DCNM SAN for Linux deployment with Custom SSL Certificate 76
Launching DCNM SAN Client from DCNM SAN for OVA/ISO deployment with Custom SSL Certificate 78
Launching DCNM SAN Client from Cisco SAN OVA/ISO Server 79

CHAPTER 5 **Upgrading Cisco DCNM 81**
Upgrading Cisco DCNM 81
Retaining the CA Signed Certificate 82
Upgrading to Cisco SAN on OVA/ISO 83
PM Data Migration from 10.4(x) SAN OVA/ISO/Windows to the New DCNM 11.3(1) OVA/ISO 84
PM Data Migration from 11.1(1) and 11.2(1) Windows to fresh install of 11.3(1) OVA/ISO 85
PM Data Migration from 11.1(1) and 11.2(1) Linux to fresh install of 11.3(1) OVA/ISO 88

CHAPTER 6 **Running Cisco DCNM Behind a Firewall 93**
Running Cisco DCNM Behind a Firewall 93
Configuring Custom Firewalls 101

CHAPTER 7 **User and Schemas 105**
Creating New Users 105
Creating New Schema for Existing Users 105

CHAPTER 8 **Certificates 107**
Retaining the CA Signed Certificate 107

Certificates Management for SAN Windows/Linux 108
Enabling SSL/HTTPS on Cisco DCNM in Federation on RHEL or Windows 108
Using a Self-Signed SSL Certificate 109
Using an SSL Certificate when certificate request is generated using Keytool on Windows 109
Using an SSL Certificate When Certificate Request Is Generated Using Keytool on Linux 110
Using a SSL Certificate when certificate request is generated using OpenSSL on Linux 111
Certificate Management for SAN OVA/ISO 112
Best practices for Certificate Management 113
Display Installed Certificates 113
Installing a CA Signed Certificate 114
Installing a CA Signed Certificate on Cisco DCNM Standalone Setup 115
Restoring the certificates after an upgrade 116
Restoring Certificates on Cisco DCNM Standalone setup after Upgrade 117
Restoring Certificates on Cisco DCNM Native HA setup after Upgrade 118
Recovering and Restoring Previously Installed CA Signed Certificates 119
Verifying the installed certificate 119

CHAPTER 9 **Managing Utility Services After DCNM Deployment** 121
Editing Network Properties Post DCNM Installation 121
Modifying Network Interfaces (eth0 and eth1) Post DCNM Installation 122
Configuring Enhanced-Fabric-Inband Interface (eth2) Post DCNM Installation 130
Modifying Network Properties on DCNM in Standalone Mode 132
Changing the DCNM Server Password on Standalone Setup 134
Changing the DCNM Server Password on Native HA Setup 134
Changing the DCNM Database Password on Standalone Setup 135
Utility Services Details 136
Network Management 136
Orchestration 136
Device Power On Auto Provisioning 137
Managing Applications and Utility Services 137
Verifying the Application and Utility Services Status after Deployment 138
Stopping, Starting, and Resetting Utility Services 139
Updating the SFTP Server Address for IPv6 140

CHAPTER 10 **Installing Software Maintenance Update for log4j2 Vulnerability** 141

Installing Software Maintenance Update on Cisco DCNM Windows and Linux Deployment 141

Installing the SMU on Cisco DCNM Windows Appliance 141

Installing the SMU on Cisco DCNM Linux Appliance 143

Installing Software Maintenance Update on Cisco DCNM OVA/ISO Deployment 144

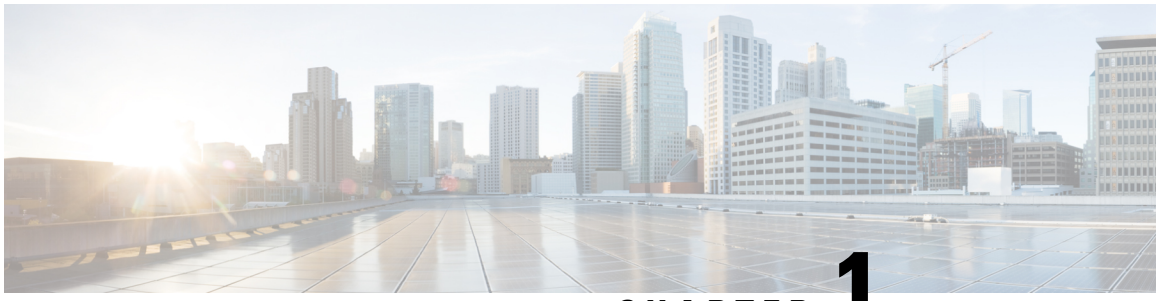
Installing SMU on Cisco DCNM 11.3(1) Standalone Deployment 144

Sample Output of Commands to address Log4j vulnerability 146

Scanning for Log4j2 Vulnerabilities 151

Validating of SMU Installation 154

Upgrading DCNM Release 11.3(1) from Previous Versions 155



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 3
- Upgrading Cisco DCNM, on page 3
- System Requirements, on page 4
- Clearing Browser Cache, on page 10

Introduction

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

In addition to complete configuration and status monitoring capabilities for Cisco MDS 9000 switches, Cisco DCNM-SAN provides powerful fiber channel troubleshooting tools. The in-depth health and configuration analysis capabilities leverage unique MDS 9000 switch capabilities: Fiber Channel Ping and Traceroute.

Beginning with Release 11.1(1), Cisco DCNM allows you to monitor Cisco UCS Blade servers also.

Cisco DCNM includes these management applications:

Cisco DCNM Server

The Cisco DCNM-SAN Server component must be started before running Cisco DCNM-SAN. Cisco DCNM-SAN server is installed as a service. This service can then be administered using the Windows Services in the control panel. Cisco DCNM-SAN Server is responsible for discovery of the physical and logical fabric and for listening for SNMP traps, syslog messages, and Performance Manager threshold events.

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. You can configure the MDS9000 Fabric, also.

Cisco DCNM-SAN Client

The Cisco DCNM-SAN Client displays a map of your network fabrics, including Cisco MDS 9000 Family switches, third-party switches, hosts, and storage devices. The Cisco DCNM-SAN Client provides multiple menus for accessing the features of the Cisco DCNM SAN functionality.

Device Manager

The Device Manager is embedded with the Cisco DCNM Web UI. After the switches are discovered, navigate to **Inventory > Switches > Device Manager** to launch the Device Manager.

Cisco DCNM-SAN automatically installs the Device Manager. Device Manager provides two views of a single switch:

- **Device View**: displays a graphic representation of the switch configuration and provides access to statistics and configuration information.
- **Summary View**: displays a summary of xE ports (Inter-Switch Links), Fx ports (fabric ports), and Nx ports (attached hosts and storage) on the switch, Fibre Channels, and IP neighbor devices. You can create charts, print, or save the summary or real-time statistics to a file in tab-delimited format.

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.

DCNM Windows Installer

This installer is available as an executable (.exe) file.

DCNM Linux Installer

This installer is available as a binary (.bin) file.

Deployment Options

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

Standalone Server

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

Standalone with external Oracle

If you have more switches in your setup or you expect your setup to grow over time, we recommend that you use an external Oracle server. This mode of deployment requires the default installation setup, followed by steps to configure DCNM to use the external Oracle. For more information about Scalability, see *Verified Scalability Guide for Cisco DCNM*.

DCNM Federation

Cisco DCNM federation is the HA mechanism for SAN devices. Every node in the DCNM federated setup can manage many groups of SAN devices. A single client interface can manage all devices. Federation mode is used for resilience and scalability. It allows you to monitor 20,000 FC ports. DCNM Windows and Linux Installers can be deployed in Federation mode to have resilience in case of application or OS failures. For Cisco DCNM-SAN federation, the database URL (properties) must remain the same for all Cisco DCNM-SAN nodes in the federation.

Upgrading Cisco DCNM

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. However, there is not upgrade path for SAN OVA\ISO.

From Release 11.3(1), Cisco DCNM OVA and ISO is supported for SAN functionality.

The following table summarizes the type of upgrade that you must follow to upgrade to Release 11.3(1).

Table 1: Type of Upgrade for Cisco DCNM SAN deployments

Current Release Number	Upgrade type to upgrade to Release 11.3(1)
11.2(1)	To Windows—Inline Upgrade To Linux—Inline Upgrade To OVA\ISO— 1. Fresh 11.3(1) SAN Only Installation. 2. Migrate Performance Manager Collections **Note** The old Performance Manager data will replace any existing Performance Manager data on 11.3(1).
11.1(1)	To Windows—Inline Upgrade To Linux—Inline Upgrade To OVA\ISO— 1. Fresh 11.3(1) SAN Only Installation. 2. Migrate Performance Manager Collections **Note** The old Performance Manager data will replace any existing Performance Manager data on 11.3(1).
10.4(2) OVA 10.4(1) OVA	To 11.3(1) OVA\ISO— 1. Fresh 11.3(1) SAN Only Installation. 2. Migrate Performance Manager Collections **Note** The old Performance Manager data will replace any existing Performance Manager data on 11.3(1).

System Requirements

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

This section describes the various system requirements for proper functioning of your Cisco DCNM, Release 11.3(1).

Java Requirements

The Cisco DCNM Server is distributed with JRE 11.0.2 into the following directory:

```
DCNM_root_directory/java/jdk11
```

Server Requirements

Cisco DCNM, Release 11.3(1), supports the Cisco DCNM Server on these 64-bit operating systems:

- **SAN Deployments:**
  - Microsoft Windows 2016
  - Microsoft Windows 2012 R2
  - Red Hat Enterprise Linux Release 7.3, 7.4, 7.6, and 7.7
  - Open Virtual Appliance (OVA) with an integrated CentOS Linux release 7.6
  - ISO Virtual Appliance (ISO) with an integrated CentOS Linux release 7.6

Cisco DCNM Release 11.3(1) supports the following databases:

- Oracle11g Express (XE), Standard, and Enterprise Editions, and Oracle 11g Real Application Clusters (RAC)
- Oracle 12c Enterprise Edition (Conventional)—(Nonpluggable installation)

Note Cisco DCNM Release 11.3(1) doesn't support the Oracle 12c pluggable database version installation.

- Oracle 12c RAC (nonpluggable installation)
- PostgreSQL 9.4.5

Note The database size increases according to the number of nodes and ports that the DCNM manages, with Performance Manager Collections enabled. You cannot restrict the database size. If you choose an Oracle database, we recommend that you use Oracle SE or Enterprise edition, instead of Oracle XE due to table space limitations.

Note You are responsible for all the support that is associated with the Oracle databases, including maintenance, troubleshooting, and recovery. We recommend that you take regular backup of the database; either daily or weekly, to ensure that all the data is preserved.

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

From Release 11.2(1), 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]
Cisco UCS C240M4	UCSC-C240-M4S	32G / 500G 16 vCPUs
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 16vCPUs, 64G RAM, and 500GB hard disk. Ensure that you do not install the Compute node on 32G RAM server.

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 as well, despite Cisco is only testing on Cisco UCS.

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.

Note vCenter server is mandatory to deploy the Cisco DCNM OVA Installer.

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

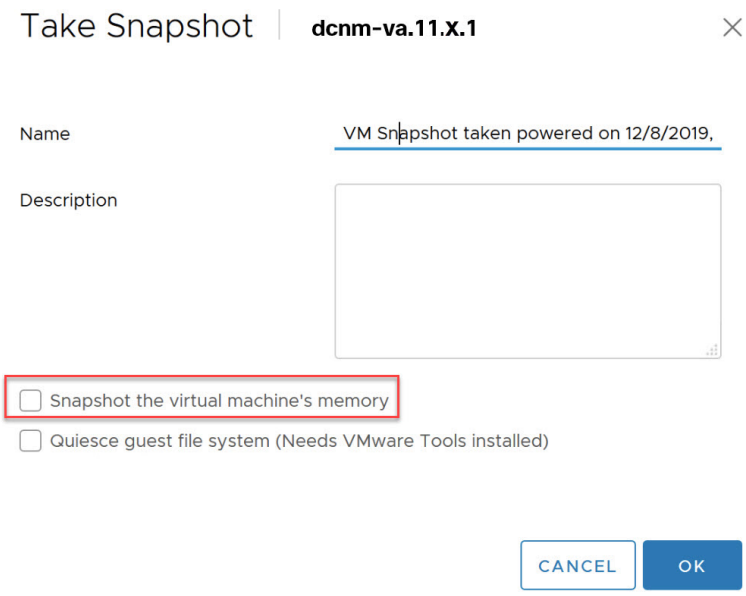
1. Right-click the virtual machine the inventory and select **Snapshots > Take Snapshot**.
2. In the Take Snapshot dialog box, enter a **Name** and description for the snapshot.
3. Click **OK** to save the snapshot.

The following snapshots are available for VMs.

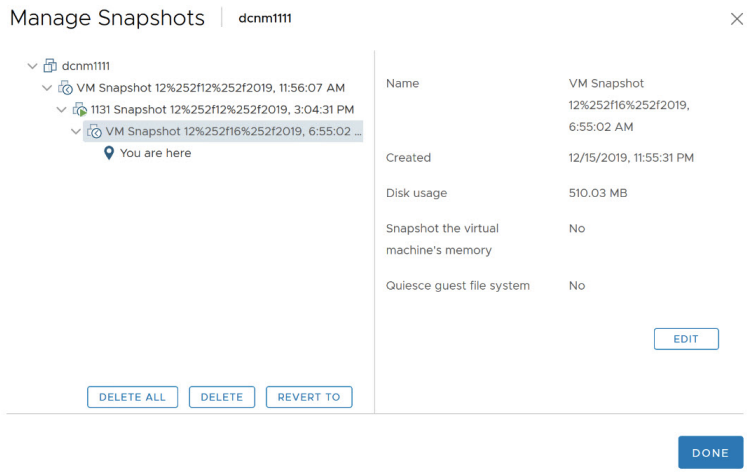
- When VM is powered off.
- When VM is powered on, and active.

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.

Note that the 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**.

Table 2: Snapshot Support for Classic LAN, LAN Fabric, Media Controller, and SAN OVA Deployments

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

Server Resource Requirements

Deployment	Deployment Type	Small (Lab or POC)	Large (Production)	Huge (Production)	Compute
SAN	Windows	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB	Not Applicable	Not Applicable
	Linux (standalone or VM)	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB Disk: 500 GB	With SAN Insights: • CPU: 32 vCPUs • RAM: 128 GB • DISK: 2 TB	Not Applicable
	• OVA standalone • ISO standalone	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB	CPU: 32vCPUs RAM: 128 GB DISK: 2 TB (with SAN Insights)	Not Applicable

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.

Ensure that there is enough disk space to the root partition or mount another disk where the `/tmp` directory can be mounted during the installation or upgrade.

You can add additional disk space to your DCNM set up. Logon to DCNM server using SSH. Extend the disk file system using **appmgr system scan-disks-and-extend-fs** command.

Note

- From Release 11.3(1), Cisco DCNM Windows deployments does not support the SAN Insights feature.
- Cisco SAN Insights feature is only supported with the Huge deployment.
- You can use the SAN Insights feature on a medium-sized deployment with 2 TB disk space.
- Every federation deployment consists of three large configuration nodes.
- From Cisco DCNM Release 11.2(1), synchronize the Federation nodes from the Primary node only.

Client Requirements

Cisco DCNM SAN desktop client and Cisco Device Manager support Microsoft Windows 10, Microsoft Windows 2012, Microsoft Windows 2016, and Red Hat Linux. The following table lists the minimum hardware requirements for these client systems.

Table 3: Client Hardware Requirements

Hardware	Minimum Requirements
RAM (free)	6 GB or more
CPU speed	3 GHz or faster
Disk space (free)	20 GB

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.

Some Cisco DCNM features require a license. Before using the licensed features, you must install a Cisco DCNM license for each Nexus-managed or MDS-managed platform. For information about Licensing in DCNM, see https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/11_x/licensing/cisco_dcnm_licensing_guide_11_x.html.

Supported Web Browsers

Cisco DCNM supports the following web browsers:

- Google Chrome Version 79.0.3945.79
- Mozilla Firefox Version 71.0 (32/64 bit)
- Microsoft Internet Explorer Version 11.706 update version 11.0.120

Other Supported Software

The following table lists the other software that is supported by Cisco DCNM, Release 11.3(1).

Table 4: Other Supported Software

Component	Features
Security	• ACS versions 4.0, 5.1, 5.5, and 5.8 • ISE version 2.6 • Telnet Disabled: SSH Version 1, SSH Version 2, Global Enforce SNMP Privacy Encryption. • Web Client and Cisco DCNM-SAN Server Encryption: HTTPS with TLS 1, 1.1 and 1.2 • TLS 1.3
OVA\ISO Installers	CentOS 7.6/Linux Kernel 3.10.x

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

Qualified Security Certifications

Security Certifications	Date run on DCNM 11.4(1)
Nessus	6/29/2020
Appscan	6/29/2020
Qualsys	6/29/2020

Clearing Browser Cache

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

Cisco DCNM supports the following web browsers:

- Mozilla Firefox
- Microsoft Internet Explorer
- Google Chrome version

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

Mozilla Firefox

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

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

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

2. From the **Time range to clear:** drop-down list, select the desired range. To clear your entire cache, select all options.
3. Click the down arrow next to Details to choose which elements of the history to clear. To clear the entire cache, select all items.

   Click **Clear Now**.

4. Restart browser.

Google Chrome

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

1. In the browser bar, enter **chrome://settings/clearBrowserData**, and press **Enter**.
2. On the Advanced tab, select the following:

- Cookies and other site data
- Cached images and files

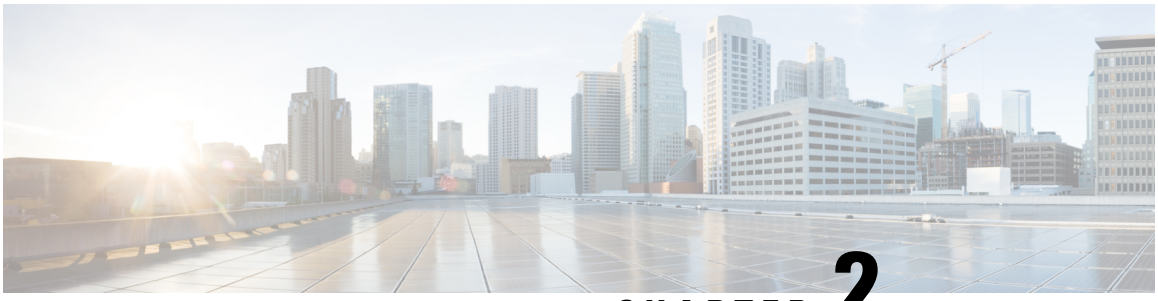
3. From the **Time range** drop-down list, you can choose the period of time for which you want to clear cached information. To clear your entire cache, select **All time**.
4. Click **Clear Data**.
5. Restart browser.

Internet Explorer

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

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

   If the menu bar is hidden, press **Alt** to make it visible.
2. Deselect **Preserve Favorites website data**, and select **Cookies or Cookies and website data**.
3. Click **Delete**. You will see a confirmation at the bottom of the window when the process is complete.
4. Restart browser.



CHAPTER 2

Guidelines and Limitations

- Guidelines and Limitations, on page 13
- Checking TPM Partition before Converting DCNM-SE to Nexus Dashboard, on page 14

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 Windows and Linux installers, the installer installs Cisco DCNM-SAN and Cisco SMI-S agent on your system.
- From Release 11.3(1), you can install a Cisco DCNM SAN Deployment on OVA and ISO.

Upgrade

- Before you start to upgrade, close all instances of DCNM SAN client, both SAN Client and Device Manager running on the server.
- For Windows and Linux installers, the default is to upgrade to the latest version of Cisco DCNM.
- If you need to run Network Insights applications, you must install 3 compute nodes.

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 11.3(1) 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
...
```

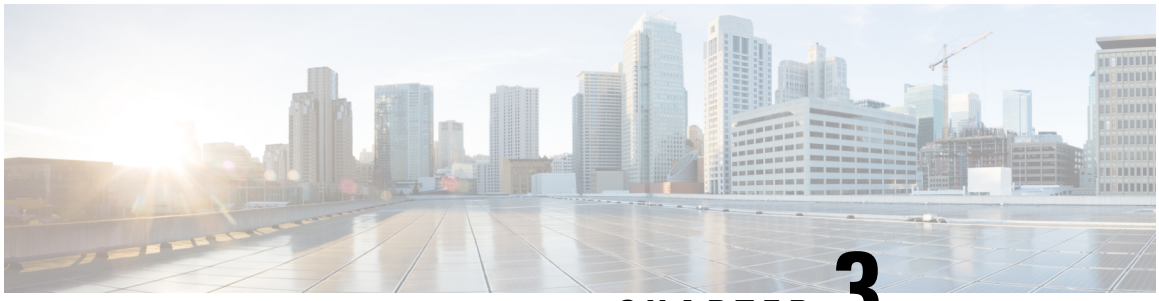
- **Example2**

  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*.

- General Prerequisites, on page 17
- Prerequisites for Installing DCNM on Windows, on page 30
- Prerequisites for Installing DCNM on Linux, on page 31
- Oracle Database for DCNM Servers, on page 32
- Remote Oracle Database Utility Scripts for Backup and Restore , on page 37
- Local PostgreSQL Database Utility Scripts for Backup and Restore, on page 38

General Prerequisites

This section includes the following topics:

Before you begin

Before you can install Cisco DCNM, ensure that the Cisco DCNM system meets the following prerequisites:

- Before installing Cisco DCNM, ensure that the host name is mapped with the IP address in the hosts file under the following location:
  - Microsoft Windows–`C:\WINDOWS\system32\drivers\etc\hosts`
  - Linux–`/etc/hosts`

Note If Oracle RAC is chosen as the database for Cisco DCNM, ensure that the database host IP addresses and virtual IP addresses are added to the hosts file with their host-names.

- For RHEL, the maximum shared memory size must be 256 MB or more. To configure the maximum shared memory to 256 MB, use the following command:

  sysctl -w kernel.shmmax=268435456

This setting, kernel.shmmax=268435456, should be saved in the `/etc/sysctl.conf` file. If this setting is not present or if it is less than 268435456, the Cisco DCNM server will fail after the server system is rebooted. For more information, visit the following URL:

http://www.postgresql.org/docs/8.3/interactive/kernel-resources.html

The server system must be registered with the DNS servers. The server hosting DCNM application must be dedicated to run DCNM alone and must not be shared with any other applications which utilizes memory and system resources.

- While using Remote PostgreSQL Database server, ensure that the Cisco DCNM Host IP addresses are added to the `pg_hba.conf` file present in the PostgreSQL installation directory. After the entries are added, restart the database.
- Users installing Cisco DCNM must have full administrator privileges to create user accounts and start services. Users should also have access to all ports. For more information, see Running Cisco DCNM Behind a Firewall, on page 93.
- When you connect to the server for the first time, Cisco DCNM checks to see if you have the correct Sun Java Virtual Machine version installed on your local workstation. Cisco DCNM desktop clients look for version 1.8(x) during installation. If required, install the Sun Java Virtual Machine software.

Note When launching the Cisco DCNM installer, the *console* command option is not supported.

Note Using the Cisco DCNM installer in GUI mode requires that you must log in to the remote server using VNC or XWindows. Using Telnet or SSH to install Cisco DCNM in GUI mode is not possible.

Before you can use Cisco DCNM to manage network switches, you must complete the following tasks:

- Install a supervisor module on each switch that you want to manage.
- Configure the supervisor module with the following values using the setup routine or the CLI:
  - IP address assigned to the mgmt0 interface
  - SNMP credentials (v3 user name and password or v1/v2 communities), maintaining the same user name and password for all the switches in the fabric.

Initial Setup Routine

The first time that you access a Cisco NXOS-based switch for MDS or Nexus, it runs a setup program that prompts you for the IP address and other configuration information necessary for the switch to communicate over the supervisor module Ethernet interface. This information is required to configure and manage the switch. All Cisco Nexus or Cisco MDS switches have the network administrator as a default user (Admin). You cannot change the default user at any time. You must explicitly configure a strong password for any switch in the Cisco Nexus or Cisco MDS. The setup scenario differs based on the subnet to which you are adding the new switch:

- Out-of-band management—This feature provides a connection to the network through a supervisor module front panel Ethernet port.
- In-band management—This feature provides IP over Fibre Channel (IPFC) to manage the switches. The in-band management feature is transparent to the network management system (NMS).

Note IP address for a Cisco Nexus switch or a Cisco MDS switch can be set via CLI or USB key or POAP.

Preparing to Configure the Switch

Before you configure a switch in the Cisco Nexus or Cisco MDS 9000 Family for the first time, you need the following information:

- Administrator password, including:
  - Creating a password for the administrator (required).
  - Creating an additional login account and password (optional).
- IP address for the switch management interface—The management interface can be an out-of-band Ethernet interface or an in-band Fibre Channel interface (recommended).
- Subnet mask for the switch's management interface (optional).
- IP addresses, including:
  - Destination prefix, destination prefix subnet mask, and next-hop IP address if you want to enable IP routing. Also, provide the IP address of the default network (optional).
  - Otherwise, provide an IP address of the default gateway (optional).
- SSH service on the switch—To enable this optional service, select the type of SSH key (dsa/rsa/rsa1) and number of key bits (768 to 2048).
- DNS IP address (optional).
- Default domain name (optional).
- NTP server IP address (optional).
- SNMP community string (optional).
- Switch name—This is your switch prompt (optional).

Note Be sure to configure the IP route, the IP default network address, and the IP default gateway address to enable SNMP access. If IP routing is enabled, the switch uses the IP route and the default network IP address. If IP routing is disabled, the switch uses the default gateway IP address.

Note You should verify that the Cisco DCNM-SAN Server host name entry exists on the DNS server, unless the Cisco DCNM-SAN Server is configured to bind to a specific interface during installation.

Default Login

All Cisco Nexus and Cisco MDS 9000 Family switches have the network administrator as a default user (Admin). You cannot change the default user at any time (see the Security Configuration Guide, Cisco DCNM for SAN).

You have an option to enforce a secure password for any switch in the Cisco MDS 9000 Family. If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a secure password (see the Security Configuration Guide, Cisco DCNM for SAN). If you configure and subsequently forget this new password, you have the option to recover this password (see the Security Configuration Guide, Cisco DCNM for SAN).

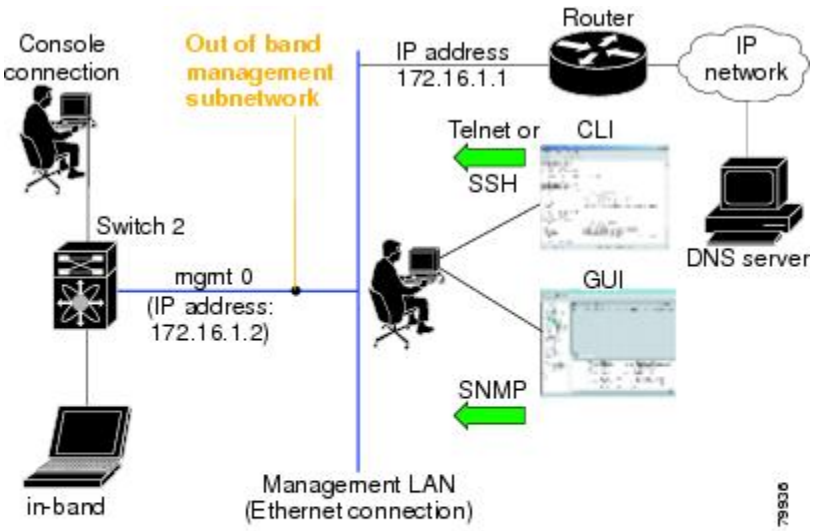
Note Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application might not function properly:

- It must be at least 8 characters long and contain at least one alphabet and one numeral.
- It can contain a combination of alphabets, numerals, and special characters.
- Do not use any of these special characters in the DCNM password for any deployment mode: <SPACE> & $ % ‘ “ ^ = < > ; :

Setup Options

The setup scenario differs based on the subnet to which you are adding the new switch. You must configure a Cisco MDS 9000 Family switch or a Cisco Nexus switch with an IP address to enable management connections from outside of the switch (see Figure 1: Management Access to Switches, on page 21).

Figure 1: Management Access to Switches



Assigning Setup Information

This section describes how to initially configure the switch for both out-of-band and in-band management.

Note Press **Ctrl + C** at any prompt to skip the remaining configuration options and proceed with what is configured until that point. Entering a new password for the administrator is a requirement and cannot be skipped.

Tip If you do not wish to answer a previously configured question, or if you wish to skip answers to any questions, press **Enter**. If a default answer is not available (for example, switch name), the switch uses what was previously configured and skips to the next question.

Configuring Out-of-Band Management

You can configure both in-band and out-of-band configuration together by entering **Yes** in both in the following procedure.

Procedure

Step 1 Power on the switch. Switches in the Cisco Nexus and Cisco MDS 9000 Family boot automatically.

```
Do you want to enforce secure password standard (Yes/No)?
```

Step 2 Enter Yes to enforce a secure password.

a) Enter the administrator password.

```
Enter the password for admin: 2008asdf*lkjh17
```

Note The password can contain a combination of alphabets, numeric, and special characters. Do not use any of these special characters in the DCNM password for any deployment mode: <SPACE> & $ % ' " ^ = < > ; :

b) Confirm the administrator password.

```
Confirm the password for admin: 2008asdf*lkjh17
```

Tip If a password is trivial (short, easy to decipher), your password configuration is rejected. Be sure to configure a secure password as shown in the sample configuration. Passwords are case sensitive.

Step 3 Enter **yes** to enter the setup mode.

Note This setup utility guides you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

```
Please register Cisco MDS 9000 Family devices promptly with your supplier.
Failure to register may affect response times for initial service calls. MDS devices must
be registered to receive entitled support services.
Press Enter anytime you want to skip any dialog. Use ctrl-c at anytime to skip away remaining
 dialogs.
Would you like to enter the basic configuration dialog (yes/no): yes
```

The setup utility guides you through the basic configuration process. Press **Ctrl + C** at any prompt to end the configuration process.

Step 4 Enter the new password for the administrator (Admin is the default).

```
Enter the password for admin: admin
```

Step 5 Enter **yes** (no is the default) to create additional accounts.

```
Create another login account (yes/no) [n]: yes
```

While configuring your initial setup, you can create an additional user account (in the network administrator role) in addition to the administrator's account. See the Security Configuration Guide, Cisco DCNM for SAN for information on default roles and permissions.

Note User login IDs must contain non-numeric characters.

a) Enter the user login ID [administrator].

```
Enter the user login ID: user_name
```

b) Enter the user password.

```
Enter the password for user_name: user-password
```

The password can contain a combination of alphabets, numeric, and special characters. Do not use any of these special characters in the DCNM password for any deployment mode: <SPACE> & $ % ' " ^ = < > ; :

c) Confirm the user password.

```
Confirm the password for user_name: user-password
```

Step 6 Enter yes (no is the default) to create an SNMPv3 account.

```
Configure read-only SNMP community string (yes/no) [n]: yes
```

a) Enter the username (Admin is the default).

```
SNMPv3 user name [admin]: admin
```

b) Enter the SNMPv3 password (minimum of eight characters). The default is admin123.

```
SNMPv3 user authentication password: admin_pass
```

Step 7 Enter **yes** (no is the default) to configure the read-only or read-write SNMP community string.

```
Configure read-write SNMP community string (yes/no) [n]: yes
```

a) Enter the SNMP community string.

```
SNMP community string: snmp_community
```

Step 8 Enter a name for the switch.

```
Enter the switch name: switch_name
```

Step 9 Enter **yes** (yes is the default) to configure out-of-band management.

```
Continue with Out-of-band (mgmt0) management configuration? [yes/no]: yes
```

a) Enter the mgmt0 IP address.

```
Mgmt0 IPv4 address: ip_address
```

b) Enter the mgmt0 subnet mask.

```
Mgmt0 IPv4 netmask: subnet_mask
```

Step 10 Enter **yes** (yes is the default) to configure the default gateway (recommended).

```
Configure the default-gateway: (yes/no) [y]: yes
```

a) Enter the default gateway IP address.

```
IPv4 address of the default gateway: default_gateway
```

Step 11 Enter **yes** (no is the default) to configure advanced IP options such as in-band management, static routes, default network, DNS, and domain name.

```
Configure Advanced IP options (yes/no)? [n]: yes
```

a) Enter **no** (no is the default) at the in-band management configuration prompt.

```
Continue with in-band (VSAN1) management configuration? (yes/no) [no]: no
```

b) Enter **yes** (no is the default) to enable IP routing capabilities.

```
Enable the ip routing? (yes/no) [n]: yes
```

c) Enter **yes** (no is the default) to configure a static route (recommended).

```
Configure static route: (yes/no) [n]: yes
```

Enter the destination prefix.

```
Destination prefix: dest_prefix
```

Enter the destination prefix mask.

```
Destination prefix mask: dest_mask
```

Enter the next-hop IP address.

```
Next hop ip address: next_hop_address
```

Note Be sure to configure the IP route, the default network IP address, and the default gateway IP address to enable SNMP access. If IP routing is enabled, the switch uses the IP route and the default network IP address. If IP routing is disabled, the switch uses the default gateway IP address.

d) Enter **yes** (no is the default) to configure the default network (recommended).

```
Configure the default network: (yes/no) [n]: yes
```

Enter the default network IP address.

Note The default network IP address is the destination prefix provided in .

```
Default network IP address [dest_prefix]: dest_prefix
```

e) Enter **yes** (no is the default) to configure the DNS IP address.

```
Configure the DNS IPv4 address? (yes/no) [n]: yes
```

Enter the DNS IP address.

```
DNS IPv4 address: name_server
```

f) Enter **yes** (default is no) to configure the default domain name.

```
Configure the default domain name? (yes/no) [n]: yes
```

Enter the default domain name.

```
Default domain name: domain_name
```

Step 12 Enter yes (no is the default) to enable Telnet service.

```
Enable the telnet server? (yes/no) [n]: yes
```

Step 13 Enter **yes** (no is the default) to enable the SSH service.

```
Enabled SSH server? (yes/no) [n]: yes
```

Step 14 Enter the SSH key type.

```
Type the SSH key you would like to generate (dsa/rsa)? dsa
```

Step 15 Enter the number of key bits within the specified range.

```
Enter the number of key bits? (768 to 2048): 768
```

Step 16 Enter **yes** (no is the default) to configure the NTP server.

```
Configure NTP server? (yes/no) [n]: yes
Configure clock? (yes/no) [n] :yes
Configure clock? (yes/no) [n] :yes
Configure timezone? (yes/no) [n] :yes
Configure summertime? (yes/no) [n] :yes
Configure the ntp server?  (yes/no) [n] : yes
```

a) Enter the NTP server IP address.

```
NTP server IP address: ntp_server_IP_address
```

Step 17 Enter **noshut** (shut is the default) to configure the default switch port interface to the shut state.

```
Configure default switchport interface state (shut/noshut) [shut]: noshut
```

Step 18 Enter **on** (on is the default) to configure the switch port trunk mode.

```
Configure default switchport trunk mode (on/off/auto) [on]: on
```

Step 19 Enter no (no is the default) to configure switchport port mode F.

```
Configure default switchport port mode F (yes/no) [n] : no
```

Step 20 Enter **permit** (deny is the default) to deny a default zone policy configuration.

```
Configure default zone policy (permit/deny) [deny]: permit
```

This step permits traffic flow to all members of the default zone.

Step 21 Enter **yes** (no is the default) to disable a full zone set distribution (see the Fabric Configuration Guide, Cisco DCNM for SAN). Disables the switch-wide default for the full zone set distribution feature.

```
Enable full zoneset distribution (yes/no) [n]: yes
```

You see the new configuration. Review and edit the configuration that you have just entered.

Step 22 Enter **no** (no is the default) if you are satisfied with the configuration.

```
The following configuration will be applied:
  username admin password admin_pass role network-admin
  username user_name password user_pass role network-admin
  snmp-server community snmp_community ro
  switchname switch
  interface mgmt0
    ip address ip_address subnet_mask
    no shutdown
  ip routing
  ip route dest_prefix dest_mask dest_address
  ip default-network dest_prefix
  ip default-gateway default_gateway
  ip name-server name_server
  ip domain-name domain_name
  telnet server enable
ssh key dsa 768 force
  ssh server enable
  ntp server ipaddr ntp_server
  system default switchport shutdown
  system default switchport trunk mode on
  system default port-channel auto-create
  zone default-zone permit vsan 1-4093
  zoneset distribute full vsan 1-4093
Would you like to edit the configuration? (yes/no) [n]: no
```

Step 23 Enter yes (yes is default) to use and save this configuration:

```
Use this configuration and save it? (yes/no) [y]: yes
```

Caution If you do not save the configuration at this point, none of your changes are updated the next time the switch is rebooted. Enter **yes** to save the new configuration to ensure that the kickstart and system images are also automatically configured.

Configuring In-Band Management

The in-band management logical interface is VSAN 1. This management interface uses the Fibre Channel infrastructure to transport IP traffic. An interface for VSAN 1 is created on every switch in the fabric. Each

switch should have its VSAN 1 interface that is configured with an IP address in the same subnetwork. A default route that points to the switch that provides access to the IP network should be configured on every switch in the Fibre Channel fabric (see Fabric Configuration Guide, Cisco DCNM for SAN).

Note You can configure both in-band and out-of-band configuration together by entering in the following procedure.

Procedure

Step 1 Power on the switch. Switches in the Cisco MDS 9000 Family boot automatically.

Step 2 Enter the new password for the administrator.

```
Enter the password for admin: 2004asdf*lkjh18
```

The password can contain a combination of alphabets, numeric, and special characters. The password can contain a combination of alphabets, numeric, and special characters. Do not use any of these special characters in the DCNM password for any deployment mode: <SPACE> & $ % ‘ “ ^ = < > ; :

Step 3 Enter **yes** to enter the setup mode.

```
This setup utility will guide you through the basic configuration of the system. Setup
configures only enough connectivity for management of the system.
Please register Cisco MDS 9000 Family devices promptly with your supplier. Failure to
register may affect response times for initial service calls.
MDS devices must be registered to receive entitled support services.
Press Enter incase you want to skip any dialog. Use ctrl-c at anytime to skip away remaining
 dialogs.
Would you like to enter the basic configuration dialog (yes/no): yes
```

The setup utility guides you through the basic configuration process. Press **Ctrl-C** at any prompt to end the configuration process.

Step 4 Enter **no** (no is the default) if you do not wish to create more accounts.

```
Create another login account (yes/no) [no]: no
```

Step 5 Configure the read-only or read-write SNMP community string.

a) Enter **no** (no is the default) to avoid configuring the read-only SNMP community string.

```
Configure read-only SNMP community string (yes/no) [n]: no
```

Step 6 Enter a name for the switch.

Note The switch name is limited to 32 alphanumeric characters. The default is switch.

```
Enter the switch name: switch_name
```

Step 7 Enter **no** (yes is the default) at the configuration prompt to configure out-of-band management.

```
Continue with Out-of-band (mgmt0) management configuration? [yes/no]: no
```

Step 8 Enter **yes** (yes is the default) to configure the default gateway.

```
Configure the default-gateway: (yes/no) [y]: yes
```

a) Enter the default gateway IP address.

```
IP address of the default gateway: default_gateway
```

Step 9 Enter **yes** (no is the default) to configure advanced IP options such as in-band management, static routes, default network, DNS, and domain name.

```
Configure Advanced IP options (yes/no)? [n]: yes
```

a) Enter **yes** (no is the default) at the in-band management configuration prompt.

```
Continue with in-band (VSAN1) management configuration? (yes/no) [no]: yes
```

Enter the VSAN 1 IP address.

```
VSAN1 IP address: ip_address
```

Enter the subnet mask.

```
VSAN1 IP net mask: subnet_mask
```

b) Enter **no** (yes is the default) to enable IP routing capabilities.

```
Enable ip routing capabilities? (yes/no) [y]: no
```

c) Enter **no** (yes is the default) to configure a static route.

```
Configure static route: (yes/no) [y]: no
```

d) Enter **no** (yes is the default) to configure the default network.

```
Configure the default-network: (yes/no) [y]: no
```

e) Enter **no** (yes is the default) to configure the DNS IP address.

```
Configure the DNS IP address? (yes/no) [y]: no
```

f) Enter **no** (no is the default) to skip the default domain name configuration.

```
Configure the default domain name? (yes/no) [n]: no
```

Step 10 Enter **no** (yes is the default) to disable Telnet service.

```
Enable the telnet service? (yes/no) [y]: no
```

Step 11 Enter **yes** (no is the default) to enable the SSH service.

```
Enabled SSH service? (yes/no) [n]: yes
```

Step 12 Enter the SSH key type (see the Security Configuration Guide, Cisco DCNM for SAN) that you want to generate.

```
Type the SSH key you would like to generate (dsa/rsa/rsa1)? rsa
```

Step 13 Enter the number of key bits within the specified range.

```
Enter the number of key bits? (768 to 1024): 1024
```

Step 14 Enter **no** (no is the default) to configure the NTP server.

```
Configure NTP server? (yes/no) [n]: no
```

Step 15 Enter **shut** (shut is the default) to configure the default switch port interface to the shut state.

```
Configure default switchport interface state (shut/noshut) [shut]: shut
```

Note The management Ethernet interface is not shut down at this point—only the Fibre Channel, iSCSI, FCIP, and Gigabit Ethernet interfaces are shut down.

Step 16 Enter **auto** (off is the default) to configure the switch port trunk mode.

```
Configure default switchport trunk mode (on/off/auto) [off]: auto
```

Step 17 Enter **deny** (deny is the default) to deny a default zone policy configuration.

```
Configure default zone policy (permit/deny) [deny]: deny
```

This step denies traffic flow to all members of the default zone.

Step 18 Enter **no** (no is the default) to disable a full zone set distribution.

```
Enable full zoneset distribution (yes/no) [n]: no
```

This step disables the switch-wide default for the full zone set distribution feature.

You see the new configuration. Review and edit the configuration that you have entered.

Step 19 Enter **no** (no is the default) if you are satisfied with the configuration.

```
The following configuration will be applied:
  username admin password admin_pass role network-admin
  snmp-server community snmp_community rw
  switchname switch
  interface vsan1
    ip address ip_address subnet_mask
    no shutdown
  ip default-gateway default_gateway
  no telnet server enable
  ssh key rsa 1024 force
  ssh server enable
  no system default switchport shutdown
  system default switchport trunk mode auto
  no zone default-zone permit vsan 1-4093
  no zoneset distribute full vsan 1-4093
Would you like to edit the configuration? (yes/no) [n]: no
```

Step 20 Enter yes (yes is default) to use and save this configuration.

```
Use this configuration and save it? (yes/no) [y]: yes
```

Caution If you do not save the configuration at this point, none of your changes are updated the next time the switch is rebooted. Enter **yes** to save the new configuration. To ensure that the kickstart and system images are also automatically configured.

Using the setup Command

To make changes to the initial configuration at a later time, you can enter the **setup** command in EXEC mode.

```
switch# setup
---- Basic System Configuration Dialog ----
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup always assumes a predefined defaults irrespective
of the current system configuration when invoked from CLI.
Press Enter incase you want to skip any dialog. Use ctrl-c at anytime
to skip away remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): yes
```

The setup utility guides you through the basic configuration process.

Starting a Switch in the Cisco MDS 9000 Family

The following procedure is a review of the tasks you should have completed during hardware installation, including starting up the switch. These tasks must be completed before you can configure the switch.

Note You must use the CLI for initial switch start up.

Procedure

Step 1 Verify the following physical connections for the new Cisco MDS 9000 Family switch:

- The console port is physically connected to a computer terminal (or terminal server).
- The management 10/100 Ethernet port (mgmt0) is connected to an external hub, switch, or router.

Tip Save the host ID information for future use (for example, to enable licensed features). The host ID information is provided in the Proof of Purchase document that accompanies the switch.

Step 2 Verify that the default console port parameters are identical to those of the computer terminal (or terminal server) attached to the switch console port:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity

Step 3 Power on the switch.

The switch boots automatically and the switch# prompt appears in your terminal window.

Accessing the Switch

After initial configuration, you can access the switch in one of the three ways:

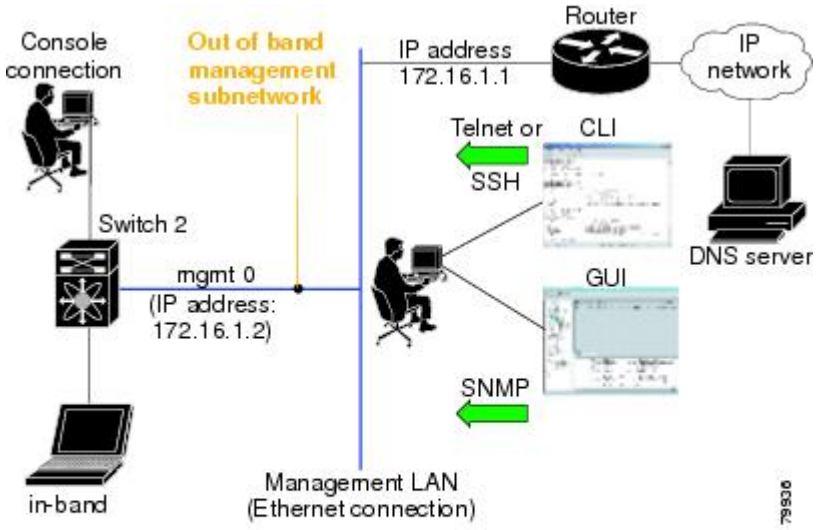
- Serial console access—You can use a serial port connection to access the CLI.
- In-band IP (IPFC) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use SNMP to connect to a Cisco DCNM-SAN application.
- Out-of-band (10/100BASE-T Ethernet) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use SNMP to connect to a Cisco DCNM-SAN application.

After initial configuration, you can access the switch in one of three ways (see Figure 2: Switch Access Options, on page 30):

- Serial console access—You can use a serial port connection to access the CLI.

- In-band IP (IPFC) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use Cisco DCNM-SAN to access the switch.
- Out-of-band (10/100BASE-T Ethernet) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use Cisco DCNM-SAN to access the switch.

Figure 2: Switch Access Options



Prerequisites for Installing DCNM on Windows

- During the initial installation, disable all security andpost antivirus tools that are running on your Windows server.
- Do not run any other management applications on the Cisco DCNM server or the Cisco DCNM database server.
- Before installing Cisco DCNM, ensure that the hostname is mapped with the IP address in the hosts file under the location **C:\WINDOWS\system32\drivers\etc\hosts**.
- On Windows, remote Cisco DCNM installations or upgrades must be done through the console using VNC or through the Remote Desktop Client (RDC) in console mode (ensuring RDC is used with the **/Console** option). This process is important if the default PostgreSQL database is used with Cisco DCNM, because this database requires the local console for all installations and upgrades.
- Telnet Client application is not installed by default on Microsoft Windows Vista. To install Telnet Client, choose **Start > Programs > Control Panel > Click Turn Windows features on or off** (if you have UAC turned on, provide permissions to continue). Check **Telnet Client** check box and click **Ok**.

- You can run CiscoWorks on the same PC as Cisco DCNM although the Java requirements are different. When installing the later Java version for Cisco DCNM, make sure that it does not overwrite the earlier Java version that is required for CiscoWorks. Both versions of Java can coexist on your PC.
- Ensure that you use the same Operating System for all the nodes in the Federation setup.
- In the Federation setup, ensure that the server time is synchronized across all the nodes of the Federation setup. The servers will not be able to communicate if the time is not synchronized. We recommend that you use NTP server to synchronize time across all the nodes.
- Ensure that you uninstall the Windows Defender application, and restart Windows 2016 server before installing Cisco DCNM on Windows 2016 server.

Prerequisites for Installing DCNM on Linux

- For RHEL, the maximum shared memory size must be 256 MB or more. To configure the maximum shared memory to 256 MB, use the following command: **sysctl -w kernel.shmmax=268435456**. Save the **kernel.shmmax=268435456** value in the **/etc/sysctl.conf** file. If this value is not correct, the Cisco DCNM server fails after the server system reboots. For more information, visit the following URL:

  http://www.postgresql.org/docs/8.4/interactive/kernel-resources.html

Note Ensure that you've installed Visual C++ Redistributable Packages for Visual Studio 2013 64 bit before installing or upgrading to Cisco DCNM Release 11.4(1).

- The server system must be registered with the DNS servers.
- No other programs must be running on the server.
- Ensure that you select English as the preferred language during RHEL installation.
- Ensure that you use the same Operating System for all the nodes in the Federation setup.
- In the Federation setup, ensure that the server time is synchronized across all the nodes of the Federation setup. The servers will not be able to communicate if the time is not synchronized. We recommend that you use NTP server to synchronize time across all the nodes.
- After you upgrade from Cisco DCNM Release 11.2(1) on Linux Standalone server, ensure that you clear the browser cache and Java console cache before you launch the Web UI and download the SAN Client. The Java console remembers the previous version of the SAN client data. If you do not clear Java console cache, you will not be able to use the latest downloaded SAN Client.

Antivirus exclusion

Scanning the Cisco DCNM includes the scanning of the database files. This process will hamper the performance on the DCNM while operation. While scanning the Cisco DCNM on Linux RHEL server, exclude the directory `/usr/local/cisco/dcm/db and /var/lib/dcnm`.

For more information, refer to https://wiki.postgresql.org.

Note We recommend you to stop Anti-Virus scanning while installing DCNM because the port being used or blocked might cause failures. After the installation, you can enable or install Anti-Virus application with specific guidelines to avoid DCNM directories as part of the scan.

Oracle Database for DCNM Servers

This section details about the database required for the installation of DCNM server.

Note This section is not applicable for Cisco DCNM Native HA installation.

Cisco DCNM supports the following databases:

- Oracle Database 11g
- Oracle Database 12c
- Oracle RAC 11g, and 12c

You can change from the local database to an external Oracle database, if required.

Note Cisco DCNM is configured with AL32UTF8 character set.

The Cisco DCNM Database size is not limited and increases based on the number of nodes and ports that the DCNM manages with Performance Manager Collections enabled. You cannot restrict the database size. Cisco recommends that you use Oracle SE or Enterprise edition, instead of Oracle XE, due to table space limitations.

This section contains the following:

Oracle SQLPlus Command-Line Tool

The Oracle database procedures in this section require the use of the SQL*Plus command-line tool. The SQL*Plus executable is typically installed in the bin directory under the Oracle home directory.

Linux Environment Variables

If you are using Linux, before you use the SQL*Plus command-line tool, ensure that the ORACLE_HOME and ORACLE_SID environment variables are set to correct values.

For example, if you are using Oracle 11g on Linux, the following commands set the environment variables to the default Oracle home directory and SID if you are using a bash shell:

```
export ORACLE_HOME=<usr_home_directory>/app/oracle/product/11.2.0/
(or identify the Oracle home on the Oracle installed server)
export ORACLE_SID=XE
```

init.ora File

The init.ora file specifies startup parameters. The default name and location of the file is platform specific, as shown in the following table.

Table 5: Name and Default Location of init.ora File

Oracle Version	Operating System	Location of init.ora File
12c	Microsoft Windows	C:\app\Administrator\virtual\product\12.2.0\dbhome_1\srvm\admin\init.ora
	Linux	/usr/lib/oracle/orcl/app/oracle/product/12.2.0/db_1/srvm/initORCL.ora
11g	Microsoft Windows	C:\app\Administrator\product\11.1.0\db_1\dbs\initORCL.ora
	Linux	/usr/lib/oracle/orcl/app/oracle/product/11.1.0/db_1/dbs/initORCL.ora

Backing up the Oracle Database

Copy the oracle backup/restore script from the Cisco DCNM server directory `DCNM_SERVER_Install/dcm/dcnm/bin`.

For Linux, the script name is backup-remote-oracledb.sh/restore-remote-oracledb.sh and edit the DB_HOME variable to point to the Oracle installation.

For Windows, the script name is **backup-remote-oracledb.bat/restore-remote-oracledb.bat** and edit *DB_HOME* variable to point to the Oracle installation.

Use the following path for Oracle DBHOME:

- On Linux– `/usr/lib/oracle/xe/app/oracle/product/10.2.0/server`

  Replace `/usr/lib/oracle` with the Oracle installation path.

- On windows– `C:\oraclexe\app\oracle\product\10.2.0\server`

  Replace `C:\oraclexe` with the Oracle installation path.

Preparing the Oracle Database

You can prepare an Oracle database.

Procedure

Step 1 Increase the number of sessions and processes to 150 each. For more information, see the Increasing the Number of Sessions and Processes to 150 Each, on page 35.

Step 2 Increase the number of open cursors to 1000. For more information, see the Increasing the Number of Open Cursors to 1000, on page 35.

Logging Into Oracle

You can log into the Oracle database by using the SQL*Plus command-line tool.

Before you begin

Ensure that you know the database administrator username and password.

Procedure

Step 1 Run the SQL*Plus executable.

A command prompt appears.

Step 2 Enter the **connect** command.

The Username prompt appears.

Step 3 Enter the database administrator username.

The Password prompt appears.

Step 4 Enter the password for the username that you specified.

For example, if the Oracle administrator username is system and the password is oracle, you would log in as follows:

Example:

```
Username: sys as sysdba
Password: oracle
```

What to do next

For more information about using SQL*Plus, see the documentation for the Oracle database version that you are using.

Increasing the SYSTEM Tablespace

You can increase the SYSTEM tablespace.

Procedure

Step 1 Use the SQL*Plus command-line tool to log in to the Oracle database. For more information, see the Oracle SQLPlus Command-Line Tool, on page 32.

Step 2 Enter the following command:

```
select file_name, bytes, autoextensible, maxbytes
from dba_data_files where tablespace_name='SYSTEM';
```

Step 3 Enter the following command:

```
alter database datafile filename autoextend on next 100m maxsize 2000m;
```

where *file_name* is the filename from the output of the **select** command in the previous step.

The SYSTEM tablespace is increased.

Step 4 Enter the **exit** command.

Increasing the Number of Sessions and Processes to 150 Each

For each DCNM instance configured in the same Oracle database, the number of cursors and processes must be increased to more than the 150 and 1000.

For example, if two DCNM standalone (non HA) instances are configured to use the same Oracle database, the cursors and process must be increased to 300 and 2000 approximately, depending on any performance degradation or SQL Exception errors occurred during normal operations of either of the DCNM instances.

Procedure

Step 1 Ensure that the `init.ora` file exists and that it contains the single line that is applicable for your Oracle database installation. If there are additional lines, remove them.

For more information, see the init.ora File, on page 33.

Step 2 Use the SQL*Plus command-line tool to log in to the Oracle database. For more information, see the Oracle SQLPlus Command-Line Tool, on page 32.

Step 3 Shut down the system by entering the **shutdown** command. If the command fails, use the **shutdown abort** command.

Step 4 Enter the following command:

```
startup pfile='init_file_name';
```

where *init_file_name* is the init.ora filename for your Oracle database installation. For more information, see the init.ora File, on page 33.

Step 5 Set the number of sessions to 150 by entering the following command:

```
alter system set sessions = 150 scope=spfile;
```

Step 6 Shut down the system by entering the **shutdown** command. If the command fails, use the **shutdown abort** command.

Step 7 Start up the system by entering the **startup** command.

Step 8 Verify that the number of sessions and processes is changed to 150 by entering the following command:

```
show parameter sessions
```

Step 9 Exit by entering the **exit** command.

Increasing the Number of Open Cursors to 1000

You can increase the number of open cursors to 1000.

Procedure

Step 1 Ensure that the init.ora file exists and that it contains the single line that is applicable for your Oracle database installation. If there are additional lines in the file, remove them.

For more information, see the init.ora File, on page 33.

Step 2 Use the SQL*Plus command-line tool to log in to the Oracle database. For more information, see the Oracle SQLPlus Command-Line Tool, on page 32.

Step 3 Shut down the system by entering the **shutdown** command. If the command fails, use the **shutdown abort** command.

Step 4 Enter the following command:

```
startup pfile='init_file_name'
```

where *init_file_name* is the init.ora filename for your Oracle database installation. For more information, see the init.ora File, on page 33.

Step 5 Set the number of open cursors to 1000 by entering the following command:

```
alter system set open_cursors = 1000 scope=spfile;
```

Step 6 Shut down the system by entering the **shutdown** command. If the command fails, use the **shutdown abort** command.

Step 7 Start up the system by entering the **startup** command.

Step 8 Verify that the number of open cursors is changed to 1000 by entering the following command:

```
show parameter open_cursors
```

Step 9 Exit by entering the **exit** command.

Creating an Oracle DB User using the Command Prompt

To create an Oracle DB user using the command prompt, follow these steps:

```
export ORACLE_SID=XE
export ORACLE_HOME=/usr/lib/oracle/xe/app/oracle/product/10.2.0/server
cd $ORACLE_HOME/bin
sqlplus
sys as sysdba
create user dcnmdbusername identified by dcnmdbuserpassword default tablespace users temporary
 tablespace temp;
grant connect, resource to dcnmdbusername;
grant create session to dcnmdbusername;
grant dba to dcnmdbusername;
```

Note Ensure you set the Oracle_SID and Oracle_Home and enter the values for the DB Username and password fields.

Note When a DBA account cannot be created, an account with DML/DDL/schema privilege is sufficient.

Connecting to an Oracle RAC with SCAN Feature Type DB

To connect to an Oracle RAC with SCAN Feature type DB, enter the following command:

```
# appmgr update -u jdbc:oracle:thin:@//[ip_addr]:1521/[service name] -n [username] -p
[password]
```

Database for Federation Setup

Cisco DCNM can be deployed as Cisco DCNM-SAN federation. For Cisco DCNM-SAN federation, the database URL (properties) must remain the same for all Cisco DCNM-SAN nodes in the federation.

Note Ensure that you do not provide multicast addresses to form the federation.

Remote Oracle Database Utility Scripts for Backup and Restore

Irrespective of the platform, Cisco DCNM is installed (Windows or Linux), the following scripts to backup and restore the remote Oracle database.

Utility scripts for Oracle database that is installed on Linux platform are;

1. backup-remote-oracledb.sh
2. restore-remote-oracledb.sh

Utility scripts for Oracle database that is installed on Windows platform are:

1. backup-remote-oracledb.bat
2. restore-remote-oracledb.bat

Cisco DCNM host is configured to run with a remote Oracle database. As part of housekeeping, you can copy DCNM utility scripts to a remote Oracle database and restore the DCNM database schema.

To run the utility scripts, you need the database administrator credentials. These scripts will prompt you for:

1. DCNM database password (the user name is already present)
2. Username/password of the admin user.

While entering the DBA user credentials, ensure that you do not to enter “sys” as sysdba" because in some versions of Oracle, the presence of space might cause the backup/restore to fail. Instead, user should provide valid user credentials that does not have a space in the user name, for example, system or sysdba. The admin credentials are not saved/cached and hence they do not leak sensitive credential information.

Note User scripts under **dcnm/bin** can be run only by administrator user.

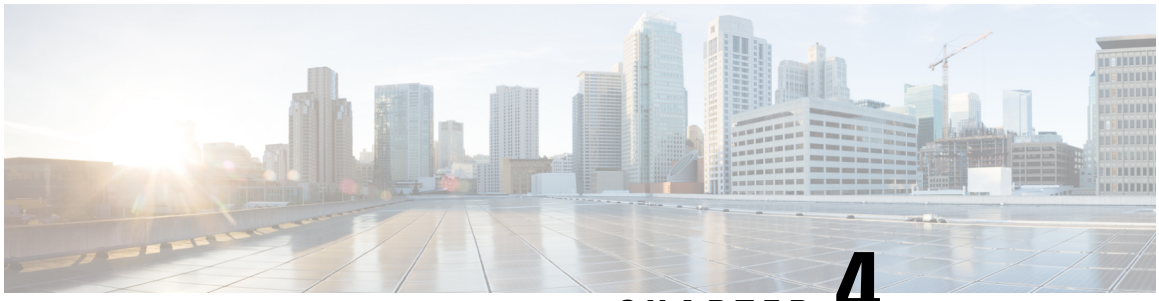
Local PostgreSQL Database Utility Scripts for Backup and Restore

Utility scripts for Local PostgreSQL database that is installed in RHEL machine are:

1. backup-pgsql-dcnm-db.sh
2. restore-pgsql-dcnm-db.sh

Utility scripts for Local PG database that is installed in Windows machine are:

1. backup-pgsql-dcnm-db.bat
2. restore-pgsql-dcnm-db.bat



CHAPTER 4

Installing the Cisco DCNM

This chapter contains the following sections:

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

- Installing Cisco DCNM on Windows, on page 39
- Installing Cisco DCNM on Linux, on page 46
- Installing DCNM on Open Virtual Appliance, on page 53
- Installing DCNM on ISO Virtual Appliance, on page 61
- Launching SAN Client and Device Manager, on page 73

Installing Cisco DCNM on Windows

Perform the following tasks to install Cisco DCNM on Windows.

Uninstalling the Cisco DCNM on Windows

Perform this procedure to uninstall Cisco DCNM on Windows.

Note We recommend that you follow these steps in the same order.

Before you begin

You must remove the Cisco DCNM instance completely before you use the same server to install a different version of DCNM. Ensure that you delete the `pgevent.dll` (located at `dcm db path \db\lib\pgevent.dll`) before beginning to upgrade.

Procedure

Step 1 Stop Cisco DCNM Services.

Step 2 Uninstall the Postgres database.

Step 3 Uninstall the Cisco DCNM.

Step 4 Navigate to `C:\Users\Administrator` location, and delete **.cisco_mds9000** folder.

Step 5 Navigate to `C:\Program Files\Zero G Registry` location, and delete the **Zero G Registry** folder.

Step 6 Navigate to `C:\Users\Administrator` location, and delete **InstallAnywhere** folder.

Step 7 Ensure that all the ports required for Cisco DCNM installation are free and available.

Step 8 Delete the Cisco DCNM directory.

Step 9 Restart the Windows VM.

Downloading the Cisco DCNM Windows Installer and Properties File

The first step to installing the DCNM on Windows is to download the `dcnm.exe` file.

Note If you plan to use Federation application functions, you must deploy the dcnm.exe file twice.

Procedure

Step 1 Go to the following site: http://software.cisco.com/download/ .

Step 2 In the Select a Product search box, enter Cisco Data Center Network Manager.

Click on Search icon.

Step 3 Click on **Data Center Network Manager** from the search results.

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

Step 4 In the Latest Releases list, choose Release 11.3(1).

Step 5 Locate the DCNM Windows Installer and click the **Download** icon.

The installer file is of the format `dcnm-installer-x64.11.3.1.exe`.

Step 6 Locate the DCNM Silent Installer Property Files and click the **Download** icon.

This file will be used during Silent Installation.

Step 7 Save both the files to your directory that will be easy to find when you begin the installation.

Installing Cisco DCNM on Windows Using the GUI

Perform the following steps to install DCNM Windows using the GUI:

Procedure

Step 1 Locate the `dcnm.exe` file that you have downloaded.

Double click on the `dcnm.exe` file.

InstallAnywhere progress bar appears to show the progress.

Step 2 On the Introduction screen, read the instructions.

Choose a vendor from the OEM Vendor drop-down list.

- Cisco Systems, Inc—to install Cisco Data Center Network Manager.
- IBM—to install the IBM Data Center Network Manager.

Click **Next**.

Step 3 Check **Add server to existing federation** checkbox if DCNM is installed as a secondary appliance in a Federation setup.

Step 4 Check **Secure Ciphers** checkbox to allow only switches with strong ciphers to be discovered by DCNM.

Step 5 To install DCNM-SAN and SMI-S for the first time, choose the location for installation. In the Install Location field, click **Choose**, and provide the appropriate folder path. Click **Restore Default Folder** if DCNM is installed as a part of the Federation setup.

Click **Next**.

Step 6 Choose the appropriate RDBMS for the DCNM server.

Select the database that is based on your requirement.

- Install PostgreSQL—Installs the PostgreSQL database that is bundled along with the dcnm.exe.
- Existing PostgreSQL 9.4
- Existing Oracle 10g/11g/12c
- Existing Oracle 10g/11g/12c RAC

  In the Service Name field, enter the service name of the Oracle RAC server. Enter a maximum of three host IP addresses. Click OK. The DB URL is generated.

If the Cisco DCNM installer detected an existing RDBMS installation, the DB URL field shows the hostname.

Cisco DCNM installation with existing PostgresSQL requires an existing schema with the same name as the DCNM username, which is owned by the same username. When there are no schemas existing with the DCNM username, or if you don't have the ownership of the schema with the same dcnmuser name, the tables are created in the default schema, which is known as "public".

Note You can't upgrade the DCNM Server with tables created in the default public schema.

Note In Oracle, when a new user is created, a schema name with the same name as the username is created automatically.

In the DCNM DB User field, enter the username that the Cisco DCNM uses to access the database. In the DCNM DB Password field, enter the password for the database user account that you specified. If you select **Add Server to an existing federation**, modify the database URL by selecting the corresponding RDBMS option. Because all the servers in federation refer to the same database, you must provide the dcnmuser name and password of the primary server.

Click **Next**. Review the limitations with Oracle Database and click **OK**.

Click **Next**.

Step 7 In the Port Configuration Options screen, choose the interface and web ports for Cisco DCNM.

- From the Server IP Address list, choose the IP address that you want to use for the Cisco DCNM server. The list shows only the IP addresses currently that are assigned to network interfaces on the server system.
- If you want to change the port that the Cisco DCNM-SAN web server listens to, enter the new port number in the SAN Web Server Port field. By default, the Cisco DCNM-SAN web server listens to TCP port 443.

  Note During Cisco DCNM installation, use port numbers that are not commonly used. For example, 87 and 23 are reserved or restricted web ports.

Click **Next**.

Step 8 In the Choose archive Folder for DCNM screen, provide a folder path to store device configuration files, user preferences and so on.

Perform one of the following:

- Click **Choose** to select a path to store the DCNM LAN archive directory.

  Note If you must choose a remote system, provide the UNC path. For example: `//Server/Share/directorypath`.

- Click **Restore Default Folder** to retain the default folder.

  Note Ensure that this folder is accessible by all nodes in the Federation setup.

Click **Next**.

Step 9 In the Local User Credentials screen, provide a valid username and password to access both DCNM SAN and DCNM LAN appliances.

- In the Admin Username field, enter a name for a Cisco DCNM server user. The installer creates the Cisco DCNM server user and assigns the Administrator role to it.
- In the Password field, enter a password for the user, and in the Confirm Password field, reenter the password.

  Adhere to the following password requirements. If you don’t comply with the requirements, the DCNM application may not function properly:

  - It must be at least 8 characters long and contain at least one alphabet and one numeral.
  - It can contain a combination of alphabets, numerals, and special characters.
  - Do not use any of these special characters in the DCNM password for any deployment mode: <SPACE> & $ % ‘ “ ^ = < > ; :

Click **Next**.

Step 10 In the Authentication Settings screen, choose the authentication method that the Cisco DCNM server should use to authenticate users who log on to the Cisco DCNM client. You can choose one of the following:

- **Local**—Cisco DCNM client users are authenticated by the Cisco DCNM server user accounts only.
- **RADIUS**—Cisco DCNM client users are authenticated by a RADIUS server.
- **TACACS+**—Cisco DCNM client users are authenticated by a TACACS+ server.

You can configure LDAP authentication after installing DCNM.

Note After TACACS/RADIUS/LDAP is enabled, Local user "admin" can't be accessible. This is default behavior.

Only if the TACACS/RADIUS/LDAP server isn't reachable or down, the Local user will be validated and is able to log in.

If LDAP/RADIUS/TACACS server is reachable and authentication fails on TACACS/LDAP/RADIUS, then no fall back to local.

Step 11 If you chose RADIUS or TACACS+, do the following:

a) In the primary server address field, enter the IPv4 address of the server in dotted-decimal format.
b) In the primary server key field, enter the shared secret of the server.
c) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.
d) In the secondary server address field, enter the IPv4 address of the server in dotted-decimal format.
e) In the secondary server key field, enter the shared secret of the server.
f) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.
g) In the tertiary server address field, enter the address of the server in the dotted-decimal format.
h) In the tertiary server key field, enter the shared secret of the server.
i) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.

Click **Next**.

Step 12 In the Choose Shortcut Folder screen, specify path where you want to create the DCNM icons.

If you want the installer to create the shortcuts for all users who can log into the server system, check the **Create icons for All Users** check box.

Click **Next**.

Step 13 In the Pre-Installation Summary screen, review the installation configuration.

Click **Previous** to go to the previous tabs and modify the configuration.

Click **Next**.

Step 14 On the confirmation window, click **Yes** to begin the DCNM installation.

The progress bar description shows the process during the installation.

Step 15 On the Install Complete screen, the installed components are listed. Click **Done** to start the DCNM server.

Note Do not close the installer, nor kill the wizard. Ensure that you click **Done**.

Wait until the DCNM is deployed on the system.

The prompt will return after the silent install is complete.

Step 16 Open a browser and enter **https://<<DCNM_server_IP_Address>>**.

Press **Return** key to launch the Web Interface of Cisco DCNM on Windows for LAN and SAN Management.

Installing Cisco DCNM Windows in a Server Federation Environment using GUI

To install DCNM in a server federation environment:

Before you begin

- Ensure that you have installed DCNM on the Primary server. Follow the instructions provided in Installing Cisco DCNM on Windows Using the GUI, on page 40 section.
- Ensure that both the Primary and Secondary servers are in the same DCNM version.

Procedure

Step 1 While installing DCNM on the Secondary server, check **Add server to existing federation** checkbox.

This makes the DCNM installed as a secondary appliance in a Federation setup. The Pre-installation Summary screen displays the Federation status and nodes in the Federation Settings area.

Step 2 Check Secure Ciphers checkbox to allow only switches with strong ciphers to be discovered by DCNM, only if the Secure Ciphers was enabled on the Primary.

Cisco DCNM uses both strong and weak ciphers when connecting to switches. If user you wants to use only strong ciphers for network, select the checkbox. Ensure that the switches in your network support strong ciphers before you select checkbox, as DCNM will not be able to connect to switches which do not support strong ciphers.

Step 3 Modify the database URL by selecting the corresponding RDBMS option.

Note All the servers in federation refer to the same database, and therefore you must provide the DCNM user name and password of the primary server. Also, you must provide the database user name and password of the primary server.

The user name and password of the database are same for all the server installation forming the federation. Similarly, the user name and password of DCNM are same for all the server installation forming the federation.

Installing Cisco DCNM Windows through Silent Installation

Cisco DCNM supports Silent installation only on Local Authorization mode and not on Remote Authorization mode.

Perform the following steps to install DCNM Windows through silent installation.

Procedure

Step 1 Unzip, extract and open the `installer.properties` file and update the following properties.

```
#-----------------BASIC Properties---------------------
DCNM_IP_ADDRESS=<ip_address_of_host_machine>
```

```
USER_INSTALL_DIR=C:\\Program Files\\Cisco Systems
INSTALLATION_TYPE=NEW_INSTALL
#INSTALLATION_TYPE=UPGRADE
SAN_FEDERATION=FALSE
#SAN_FEDERATION=TRUE
```

Step 2 Configure the database parameters.

If you are using PostgreSQL database, edit this block:

```
#------------------DATABASE Properties--------------------
#User can configure these properties to use existing database or
# install fresh Postgres as database for the DCNM. Existing database
# can be postgres (remote or local), Oracle (remote or local)
# or it can be Oracle RAC.
#-----------------------------------------------------
USE_EXISTING_DB=FALSE
#USE_EXISTING_DB=TRUE

PG_DB_PATH=C:\\Program Files\\Cisco Systems\\dcm\\db

#----------New Postgres---------------------------------
DCNM_DB_URL=jdbc\:postgresql\://localhost\:5432/dcmdb
DCNM_DB_NAME=dcmdb
SELECTED_DATABASE=postgresql
DCNM_DB_USERNAME=dcnmuser
DCNM_DB_USER_PASSWORD=dcnmuser
```

If you are using the Oracle database, edit this block:

```
#------------------DATABASE Properties--------------------
#User can configure these properties to use existing database or
# install fresh Postgres as database for the DCNM. Existing database
# can be postgres (remote or local), Oracle (remote or local)
# or it can be Oracle RAC.
#-----------------------------------------------------
USE_EXISTING_DB=FALSE
#USE_EXISTING_DB=TRUE

ORA_DB_PATH=C:\\oraclexe\\app\\oracle\\product\\10.2.0\\server
```

Step 3 Configure the user credentials for DCNM.

```
#-----------------User Configuration-----------------
#DCNM User Configuration Properties
#If you want to use special characters in DCNM_ADMIN
#credentials,Please use escape character(\) before
#the symbol [For eg. Password  "an$6x12" must be specified as "an\$6x12" ].
#-----------------------------------------------------

DECRYPT_PASSWORDS=FALSE
DCNM_ADMIN_USER=admin
DCNM_ADMIN_USER_PASSWORD=admin123

#-----------------User Configuration-----------------
```

Step 4 Enable the Secure Ciphers.

```
#----------------Secure Ciphers-------------------------------------
#DCNM uses both strong and weak ciphers when connecting to switches
#If user wants to use only strong ciphers for connection, please set
#property to TRUE. Make sure your switches support strong ciphers before
#setting the property as DCNM will not be able to connect to switches which
#support only weak ciphers.
```

```
#-------------------------------------------------------------------------
SECURE_CIPHER=FALSE
#SECURE_CIPHER=TRUE
#-------------------------------------------------------------------------
```

Step 5 Configure IBM Raven to install IBM Data Center Network Manager.

```
#------------------------------IBM Raven Support----------------------
#Set true if Vendor is IBM, by default false
#---------------------------------------------------------------------

IBM_INSTALL=FALSE /*Does not install IBM Data Center Network Manager*/
#---------------------------------------------------------------------
```

Step 6 Navigate to the directory where you downloaded the Cisco DCNM Windows software and run the appropriate installer by using the following command:

dcnm-release.exe -i silent -f *path_of_installer.properties_file*

You can check the status of installation in the Task Manager process.

Step 7 Open a browser and enter **https://<<DCNM_server_IP_Address>>**.

Press **Return** key to launch the Web Interface of Cisco DCNM for SAN Management.

Installing Cisco DCNM on Linux

Perform the following tasks to install Cisco DCNM on Linux.

Uninstalling the Cisco DCNM on Linux

Perform this procedure to uninstall Cisco DCNM on Linux.

Note We recommend that you follow these steps in the same order.

Before you begin

You must remove the Cisco DCNM instance completely before you use the same server to install a different version of DCNM.

Procedure

Step 1 Stop DCNM services on the DCNM server using the **/root/Stop_DCNM_Servers** command.

Step 2 Uninstall the Postgres database using the <<*dcnm_directory_location*>**/db/uninstall-postgresql** command.

Step 3 Uninstall the Cisco DCNM Server using the **/root/Uninstall_DCNM** command.

Step 4 Delete the hidden `.cisco_mds9000` file, using the **rm -rf .cisco_mds9000** command.

Step 5 Delete the Zero G Registry using the **rm -rf /var/.com.zerog.registry.xml** command.

Step 6 Delete the hidden `InstallAnywhere` folder using the **rm -rf .InstallAnywhere** command.

Step 7 Ensure that all the ports required for Cisco DCNM installation are free and available.

Step 8 Delete the DCNM directory using the **rm -rf /usr/local/cisco/***. Delete the DCNM directory if you've saved in any other directory.

Step 9 Restart the RHEL system.

Uninstalling the Cisco DCNM on Linux

The following sample shows the list of commands that you must run, to uninstall te Cisco DCNM on Linux.

```
[dcnm-linux]# /root/Stop_DCNM_Servers
[dcnm-linux]# /<<dcnm_installed dir>>/db/uninstall-postgresql
[dcnm-linux]# /root/Uninstall_DCNM    /* for uninstalling RHEL 7.x */

[dcnm-linux]# rm -rf .cisco_mds9000
[dcnm-linux]# rm -rf /var/.com.zerog.registry.xml
[dcnm-linux]# rm -rf .InstallAnywhere
[dcnm-linux]# rm -rf /usr/local/cisco/*
[dcnm-linux]# restart
[dcnm-linux]#
```

Downloading the Cisco DCNM Linux Installer and Properties File

The first step to installing the DCNM on Linux is to download the dcnm.bin file.

Note If you plan to use Federation application functions, you must deploy the dcnm.bin file twice.

Procedure

Step 1 Go to the following site: http://software.cisco.com/download/ .

Step 2 In the Select a Product search box, enter Cisco Data Center Network Manager.

Click on Search icon.

Step 3 Click on **Data Center Network Manager** from the search results.

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

Step 4 In the Latest Releases list, choose Release 11.3(1).

Step 5 Locate the DCNM Linux Installer and click the **Download** icon.

The installer file is of the format `dcnm-installer-x64.11.3.1.bin`.

Step 6 Locate the DCNM Silent Installer Property Files and click the **Download** icon.

This file will be used during Silent Installation.

Step 7 Save both the files to your directory that will be easy to find when you begin the installation.

Installing Cisco DCNM on Linux Using the GUI

Perform the following steps to install DCNM Linux using the GUI:

Before you begin

Ensure that the DISPLAY variable is set to 1.

- Check if DISPLAY variable is set to 1 by using the following command:

  echo $DISPLAY
- Set DISPLAY variable to 1 by using the following command:

  export DISPLAY=:1

Procedure

Step 1 Locate the `dcnm-installer-x64.<release-name>.bin` file that you have downloaded.

Run the `dcnm.bin` installer file.

InstallAnywhere progress bar appears showing the progress.

Step 2 On the Introduction screen, read the instructions.

Choose a vendor from OEM Vendor drop-down list.

- Cisco Systems, Inc—to install Cisco Data Center Network Manager
- IBM—to install IBM Data Center Network Manager

Click **Next**.

Step 3 Check **Add server to existing federation** checkbox if DCNM is installed as a secondary appliance in a Federation setup.

Step 4 Check **Secure Ciphers** checkbox to allow only switches with strong ciphers to be discovered by DCNM.

Step 5 To install DCNM-SAN and SMI-S for the first time, choose the location for installation.

Note The location for installation must be within the partition where the required disk space is provisioned. Ensure that there is sufficient disk space for deployment.

In the Install Location field, click **Choose**, and provide the appropriate folder path. Click **Restore Default Folder** if DCNM is installed as a part of the Federation setup.

Click **Next**.

Step 6 Choose the appropriate RDBMS for the DCNM server.

Select the database that is based on your requirement.

- Install PostgreSQL—Installs the PostgreSQL database that is bundled along with the `dcnm.bin`.

- Existing PostgreSQL 9.4—Existing PostgreSQL database that is already set up, with a clean schema.
- Existing Oracle 10g/11g/12c—Existing Oracle database that is already set up, with a clean schema.
- Existing Oracle 10g/11g/12c RAC—Existing Oracle database that is already set up, with a clean schema.

In the Service Name field, enter the service name of the Oracle RAC server. Enter a maximum of three host IP addresses. Click **OK**. The DB URL is generated.

If the Cisco DCNM installer detected an existing RDBMS installation, the DB URL field shows the hostname.

Note Cisco DCNM installation with existing PostgresSQL requires an existing schema with the same name as the DCNM username, which is owned by the same username. When there is no schema existing with the DCNM username, or if you do not have the ownership of the schema with the same dcnmuser name, the tables are created in the default schema, known as “public”.

If the tables are created in the default schema, you may encounter authentication issues after upgrading Cisco DCNM. You will have to create a schema with the sane name as the DCNM username owned by the same username. For instructions, see User and Schemas, on page 105.

Note In Oracle, when a new user is created, a schema name with the same name as the username is created automatically.

In the **DCNM DB User** field, enter the username that Cisco DCNM user uses to access the database. In the **DCNM DB Password** field, enter the password for the database user account that you specified. If you select **Add Server to an existing federation**, modify the database URL by selecting the corresponding RDBMS option. Because all the servers in Federation refer to the same database, you must provide the dcnmuser name and password of the primary server.

Click **Next**. Review the limitations with Oracle Database and click **OK**.

Click **Next**.

Step 7 In the Port Configuration Options screen, choose the interface and web ports for Cisco DCNM.

- From the Server IP Address list, choose the IP address that you want to use for the Cisco DCNM server. The list shows only the IP addresses currently that are assigned to network interfaces on the server system.
- If you want to change the port that the Cisco DCNM-SAN web server listens to, enter the new port number in the SAN Web Server Port field. By default, the Cisco DCNM-SAN web server listens to TCP port 443.

  Note During Cisco DCNM installation, use port numbers that are free. For example, 87 and 23 are reserved or restricted web ports.

Click **Next**.

Step 8 In the Choose archive Folder for DCNM screen, provide a folder path to store device configuration files, user preferences and so on.

Perform one of the following:

- Click **Choose** to select a path to store the DCNM archive directory.

  Note If you must choose a remote system, provide the UNC path. For example: `//Server/Share/directorypath`.

- Click **Restore Default Folder** to retain the default folder.

Click **Next**.

Step 9 In the Local User Credentials screen, provide a valid username and password to access DCNM SAN appliances.

- In the Admin Username field, enter a name for a Cisco DCNM server user. The installer creates the Cisco DCNM server user and assigns the Administrator role to it.
- In the Password field, enter a password for the user, and in the Confirm Password field, reenter the password.

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

  - It must be at least eight characters long and contain at least one alphabet and one numeral.
  - It can contain a combination of alphabets, numerals, and special characters.
  - Do not use any of these special characters in the DCNM password for any deployment mode: <SPACE> & $ % ‘ “ ^ = < > ; :

Click **Next**.

Step 10 In the Authentication Settings screen, choose the authentication method that the Cisco DCNM server must use to authenticate users who log on to the Cisco DCNM client. You can choose one of the following:

- **Local**—Cisco DCNM client users are authenticated by the Cisco DCNM server user accounts only.
- **RADIUS**—Cisco DCNM client users are authenticated by a RADIUS server.
- **TACACS+**—Cisco DCNM client users are authenticated by a TACACS+ server.

Step 11 If you chose RADIUS or TACACS+, do the following:

a) In the primary server address field, enter the IPv4 address of the server in dotted-decimal format.
b) In the primary server key field, enter the shared secret of the server.
c) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.
d) In the secondary server address field, enter the IPv4 address of the server in dotted-decimal format.
e) In the secondary server key field, enter the shared secret of the server.
f) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.
g) In the tertiary server address field, enter the address of the server in the dotted-decimal format.
h) In the tertiary server key field, enter the shared secret of the server.
i) (Optional) If you want to ensure that Cisco DCNM can communicate with the server, click **Verify**.

Click **Next**.

The Choose Link Folder is skipped and by default the location is `/root` directory.

Step 12 In the Pre-Installation Summary screen, review the installation configuration.

Click **Previous** to go to the previous tabs and modify the configuration.

Click **Next**.

Step 13 On the confirmation window, click **Yes** to begin the DCNM installation.

The progress bar description shows the process during the installation.

Step 14 On the Install Complete screen, the installed components are listed. Click **Done** to start the DCNM server.

Wait until the DCNM is deployed on the system.

Step 15 Open a browser and enter **https://<<DCNM_server_IP_Address>>**.

Press **Return** key to launch the Web Interface of Cisco DCNM for SAN Management.

Installing Cisco DCNM Linux in a Server Federation Environment Using GUI

To install DCNM in a server federation environment:

Before you begin

- Ensure that you have installed DCNM on the Primary server. Follow the instructions in Installing Cisco DCNM on Linux Using the GUI, on page 48 section.
- Ensure that the DISPLAY variable is set to 1.
  - Check if DISPLAY variable is set to 1 by using the following command:

    echo $DISPLAY
  - Set DISPLAY variable to 1 by using the following command:

    export DISPLAY=:1
- Ensure that both the Primary and Secondary servers are in the same DCNM version.

Procedure

Step 1 While installing DCNM on the Secondary server, check **Add server to existing federation** checkbox.

This makes the DCNM installed as a secondary appliance in a Federation setup. The Pre-installation Summary screen displays the Federation status and nodes in the Federation Settings area.

Step 2 Check Secure Ciphers checkbox to allow only switches with strong ciphers to be discovered by DCNM, only if the Secure Ciphers were enabled on the Primary.

Cisco DCNM uses both strong and weak ciphers when connecting to switches. If you use only strong ciphers for the network, select the checkbox. Ensure that the switches in your network support strong ciphers before you select checkbox, as DCNM will not be able to connect to switches which do not support strong ciphers.

Step 3 Modify the database URL by selecting the corresponding RDBMS option.

Note All the servers in federation refer to the same database, and therefore you must provide the DCNM username and password of the primary server. Also, you must provide the database username and password of the primary server.

The username and password of the database are same for all the server installation forming the federation. Similarly, the username and password of DCNM are same for all the server installation forming the federation.

Installing Cisco DCNM Linux Through Silent Installation

Cisco DCNM supports Silent installation only on Local Authorization mode and not on Remote Authorization mode.

Perform the following steps to install DCNM Linux through silent installation.

Before you begin

Ensure that you have execution permissions to the /tmp directory before you begin to install Cisco DCNM on Linux.

Procedure

Step 1 Unzip, extract, and open the `installer.properties` file and update the following properties.

```
#-----------------BASIC Properties---------------------
DCNM_IP_ADDRESS=<ip_address_of_host_machine>
USER_INSTALL_DIR=/usr/local/cisco/dcm
INSTALLATION_TYPE=NEW_INSTALL
#INSTALLATION_TYPE=UPGRADE
SAN_FEDERATION=FALSE
#SAN_FEDERATION=TRUE
```

Step 2 Configure the database parameters.

If you are using PostgreSQL database, edit this block:

```
#--------------New Postgress---------------------------
PG_DB_PATH=/usr/local/cisco/dcm/db

#PG_DB_PATH=/opt/dctest/cisco/dcm/db /*non-default installation directory*/
#BACKUP_FILE=/opt/dctest/cisco/dcm/dcnm/bin/<backup-filename> /*non-default backup file
directory*/

DCNM_DB_URL=jdbc\:postgresql\://localhost\:5432/dcmdb
DCNM_DB_NAME=dcmdb
SELECTED_DATABASE=postgresql
DCNM_DB_USERNAME=dcnmuser
DCNM_DB_USER_PASSWORD=dcnmuser
#CLEAN_DATABASE=TRUE
```

If you are using the Oracle database, edit this block:

```
#-----------------DATABASE Properties--------------------
#User can configure these properties to use existing database or
# install fresh Postgres as database for the DCNM. Existing database
# can be postgres (remote or local), Oracle (remote or local)
# or it can be Oracle RAC.
#------------------------------------------------------
USE_EXISTING_DB=FALSE
#USE_EXISTING_DB=TRUE
ORA_DB_PATH=C:\\oraclexe\\app\\oracle\\product\\10.2.0\\server
```

Step 3 Configure the Data Path for DCNM.

```
#---------------------DATA PATH----------------
#Data path is the folder location where DCNM LAN related
#information like Config archives, templates etc. are stored.
# In DCNM LAN Cluster mode this folder has to be a shared folder.
#For linux and windows it will be different as the folder structure vaires
```

```
#-------------------------------------------------

DATA_PATH=/usr/local/cisco/dcm/dcnm
#---------------------DATA PATH----------------
```

Step 4 Configure the user credentials for DCNM.

```
#-----------------User Configuration-----------------
#DCNM User Configuration Properties
#If you want to use special characters in DCNM_ADMIN
#credentials,Please use escape character(\) before
#the symbol [For eg. Password  "an$6x12" must be specified as "an\$6x12" ].
#-------------------------------------------------

DECRYPT_PASSWORDS=FALSE
DCNM_ADMIN_USER=admin
DCNM_ADMIN_USER_PASSWORD=admin123

#-----------------User Configuration-----------------
```

Step 5 Enable the Secure Ciphers.

```
#----------------Secure Ciphers-------------------------------------
#DCNM uses both strong and weak ciphers when connecting to switches
#If user wants to use only strong ciphers for connection, please set
#property to TRUE. Make sure your switches support strong ciphers before
#setting the property as DCNM will not be able to connect to switches which
#support only weak ciphers.

#-------------------------------------------------------------------------
SECURE_CIPHER=FALSE
#SECURE_CIPHER=TRUE
#-------------------------------------------------------------------------
```

Step 6 Configure IBM Raven to install IBM Data Center Network Manager.

```
#-----------------------------IBM Raven Support----------------------
#Set true if Vendor is IBM, by default false
#--------------------------------------------------------------------

IBM_INSTALL=FALSE /*Does not install IBM Data Center Network Manager*/
#--------------------------------------------------------------------
```

Step 7 Navigate to the directory where you downloaded the Cisco DCNM Linux software and run the appropriate installer by using the following command:

dcnm-release.bin -i silent -f *path_of_installer.properties_file*

You can check the status of installation by using the following command **ps -ef | grep 'LAX'**. The prompt will return after the silent install is complete.

Step 8 Open a browser and enter **https://<<DCNM_server_IP_Address>>**.

Press **Return** key to launch the Web Interface of Cisco DCNM on Linux for SAN Management.

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/.

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 11.3(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.
- Choose **Huge** to configure the virtual machine with 32 vCPUs, 128GB RAM.

  We recommend that you choose this configuration if you are deploying the SAN Insights features.

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.

  Note This network is optional for Cisco DCNM SAN OVA/ISO Deployments.

- **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 This network is not applicable for Cisco DCNM SAN OVA/ISO Deployments.

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 121.

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.

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**.

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.

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

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

You can choose to install DCNM in Standalone mode or Native HA mode. Refer to Installing Cisco DCNM ISO in Standalone Mode, on page 70 for more information.

Installing the Cisco DCNM OVA in Standalone Mode

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

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

Procedure

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

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

Click **Continue**.

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

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

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

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

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

Click **Next**.

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

Click **Next**.

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

- In the Fully Qualified Hostname field, enter the hostname that is a fully qualified domain name (FQDN) as per RFC1123, section 2.1.

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

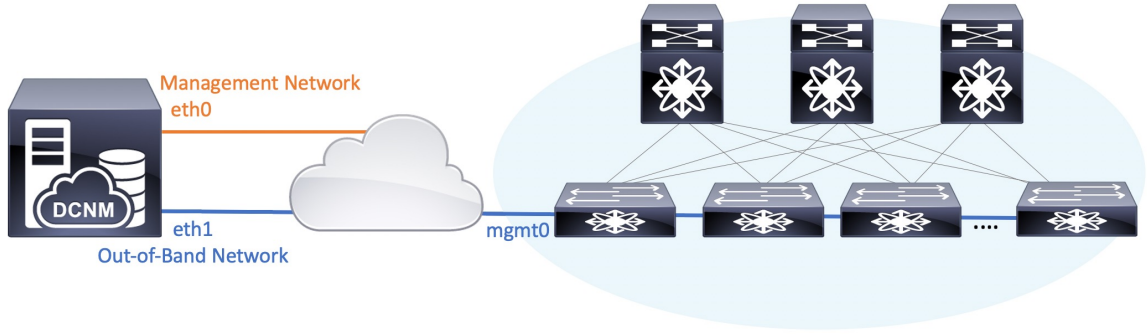
  The value must be an IP or IPv6 address or RFC 1123 compliant name.

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

Click **Next**.

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

Figure 3: Cisco DCNM Management Network Interfaces



Note Cisco DCNM for SAN OVA/ISO deployment allows you to configure only eth0 or both eth0 and eth1 (either in same or different subnets) based on the requirements, in respective environments. Establish IP reachability to switches for management/monitoring either over eth0 or eth1 interface. SAN Insights streaming is supported over both eth0 and eth1 interfaces. However, ensure that streaming is configured to the DCNM the interface with IP reachability from the respective switches. For more information, refer to Configuring SAN Insights in *Cisco DCNM SAN Management for OVA and ISO Deployments Configuration Guide*.

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

Note You can also use an IPv6 address for the Management Network. However, SAN Insights streaming is supported with IPv4 address configuration only.

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

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

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

c) (Optional) **In-Band Network** configuration is not required for Cisco DCNM SAN for OVA/ISO deployment.

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 121.

Click **Next**.

Step 7 On the **Applications** tab, in the IPv4 Subnet field, enter the IP subnet to access the applications that run internally to DCNM.

All the applications use the IP Address from this subnet.

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

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

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

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

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

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

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

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

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

Click **Next**.

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

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

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

Installing DCNM on ISO Virtual Appliance

This chapter contains the following sections:

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

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/.

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 11.3(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 69 or Installing the DCNM ISO Virtual Appliance on UCS (Bare Metal), on page 62 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.

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.

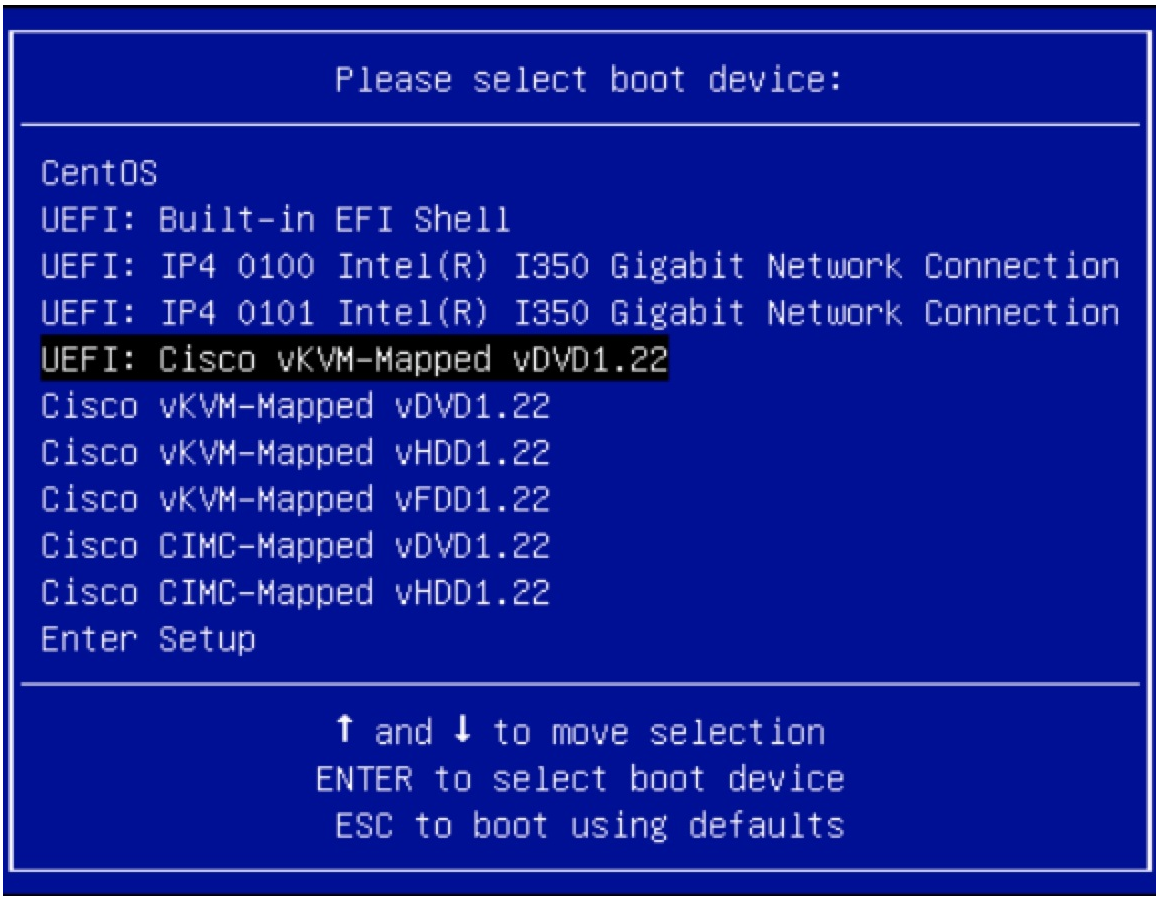
For more information about using the UCS KVM Console window, see the Cisco UCS Server Configuration Utility, Release 3.1 User Guide at the following URL:

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.

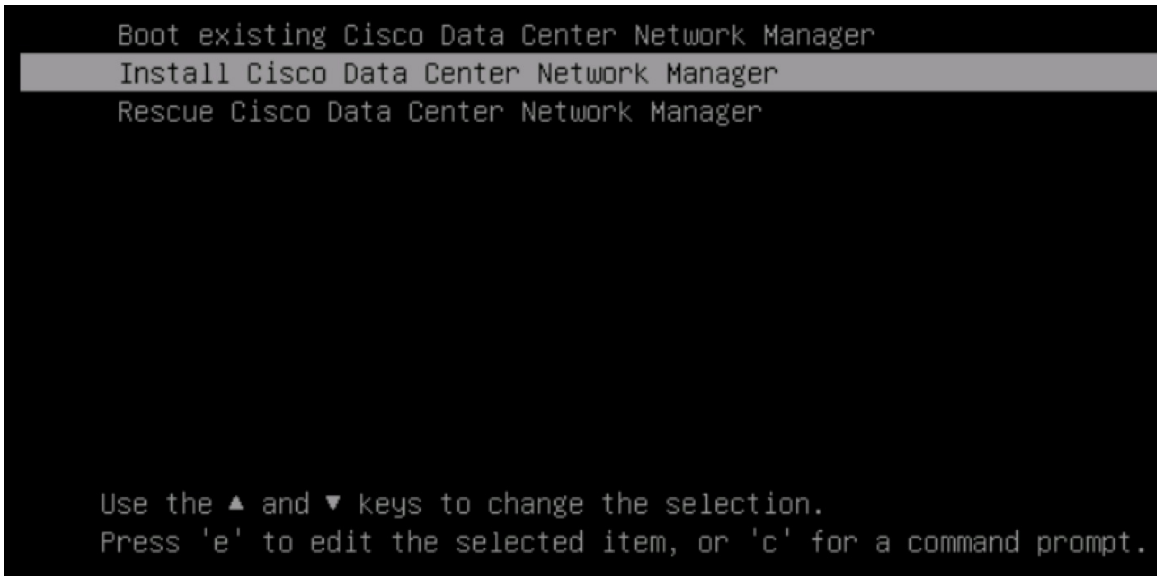
UEFI is mandatory for a system with minimum of 2TB disks.



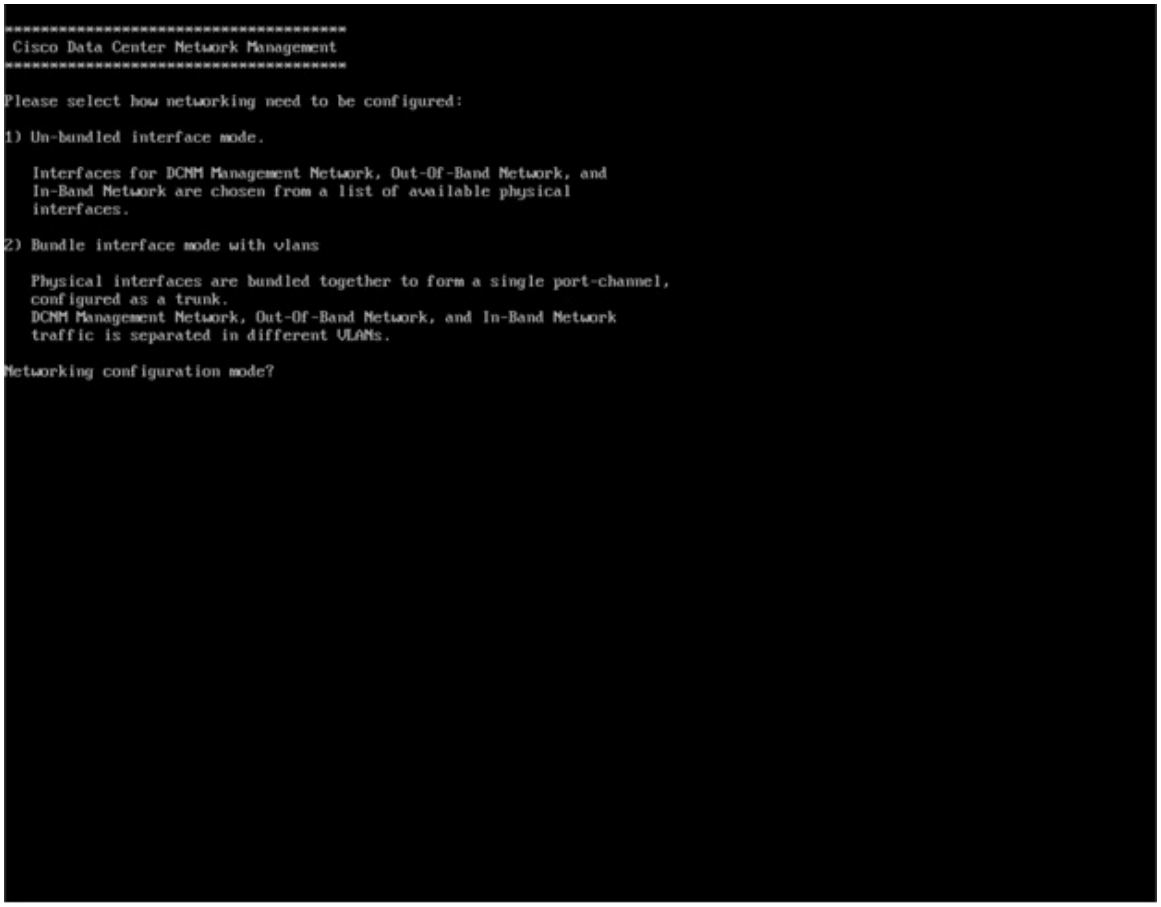
For Cisco UCS with the disk size of 2TB or higher and with 4K sector size drivers, the UEFI boot option is required. For more information, see UEFI Boot Mode.

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
```

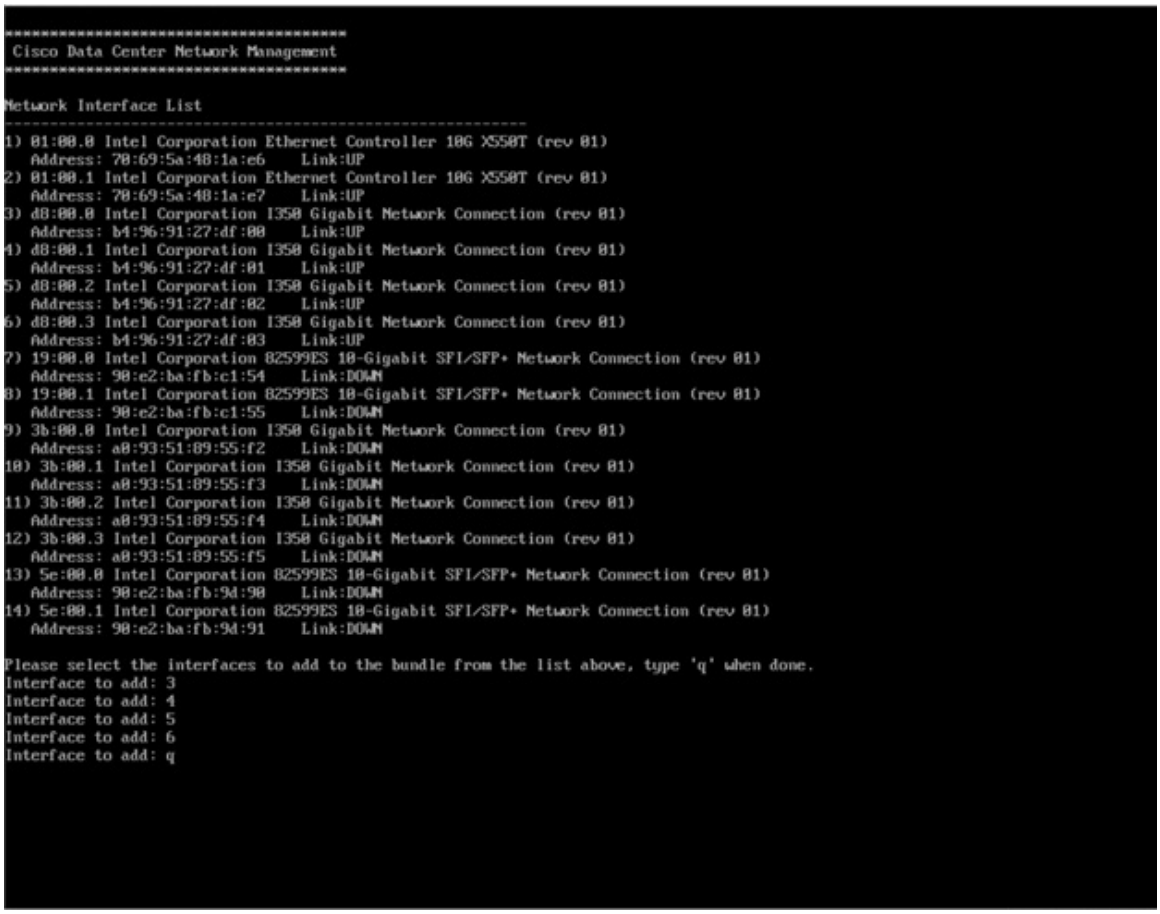
However, you can edit the network properties after installation, if required, using the **appmgr update network-properties** command. For more information, see Editing Network Properties Post DCNM Installation, on page 121.

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.

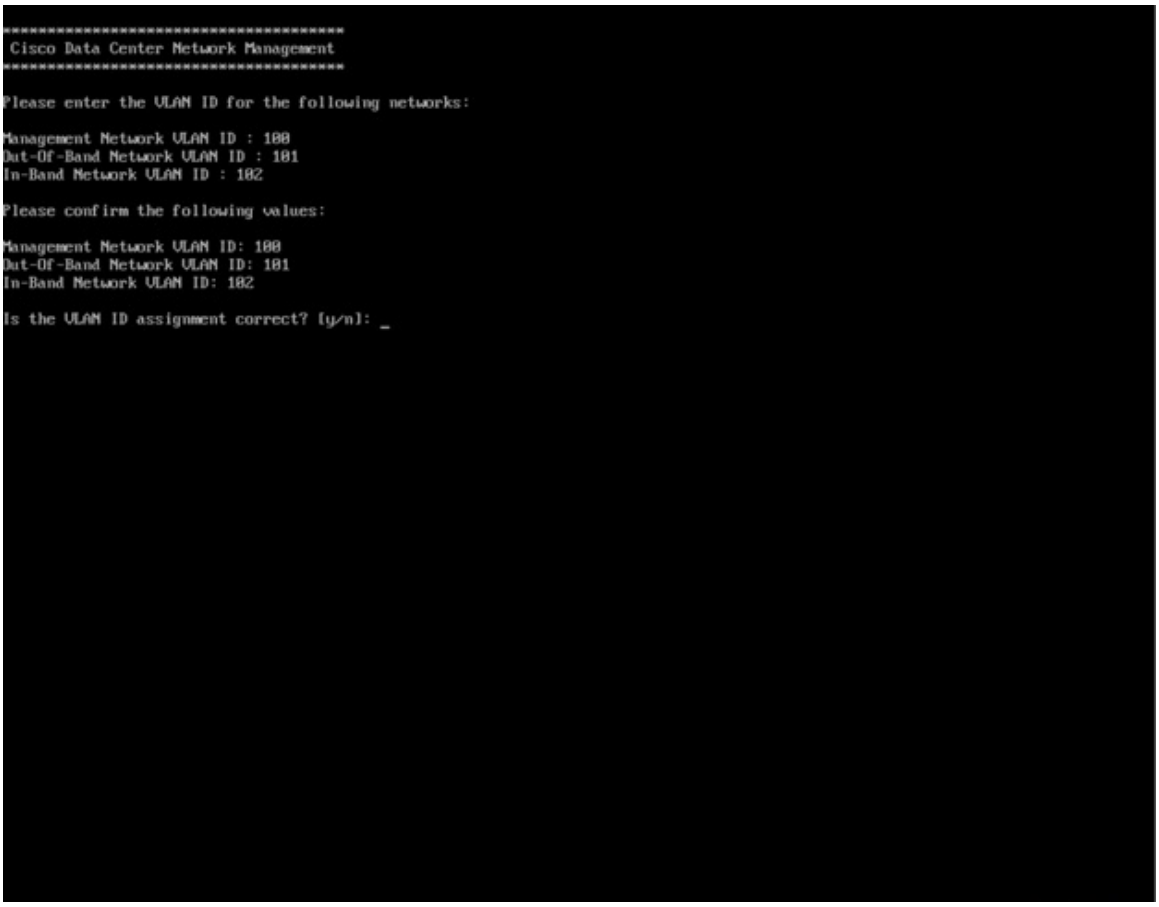
Enter **q** after you enter all the interface that must be added to the bundle.



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. Refer to *Installing Cisco DCNM ISO in Standalone 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 **dcnm-va-ovf-kvm-files.11.3.1.zip** and locate the **dcnm-kvm-vm.xml** file.

Step 2 Upload this file on the RHEL server that is running KVM to the same location as the ISO.

Step 3 Connect to the RHEL server running KVM via SCP File transfer terminal.

Step 4 Upload the **dcnm-va.11.3.1.iso** and **dcnm-kvm-vm.xml** to the RHEL server.

Step 5 Close the file transfer session.

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

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

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

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

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

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

Step 10 Close the SSH session.

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

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

A VM is created in the Virtual Machine Manager.

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

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

Step 15 Create a hard disk with Device type 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.

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 121.

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. Refer to *Installing Cisco DCNM ISO in Standalone Mode* sections for more information.

Installing Cisco DCNM ISO in Standalone Mode

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

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

Procedure

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

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

Click **Continue**.

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

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

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

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

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

Click **Next**.

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

Click **Next**.

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

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

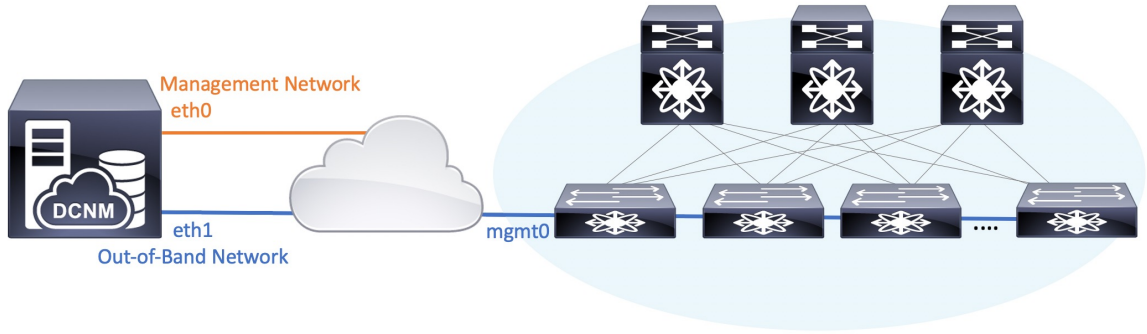
  The value must be an IP or IPv6 address or RFC 1123 compliant name.

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

Click **Next**.

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

Figure 4: Cisco DCNM Management Network Interfaces



Note Cisco DCNM for SAN OVA/ISO deployment allows you to configure only eth0 or both eth0 and eth1 (either in same or different subnets) based on the requirements, in respective environments. Establish IP reachability to switches for management/monitoring either over eth0 or eth1 interface. SAN Insights streaming is supported over both eth0 and eth1 interfaces. However, ensure that streaming is configured to the DCNM the interface with IP reachability from the respective switches. For more information, refer to Configuring SAN Insights in *Cisco DCNM SAN Management for OVA and ISO Deployments Configuration Guide*.

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

Note You can also use an IPv6 address for the Management Network. However, SAN Insights streaming is supported with IPv4 address configuration only.

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

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

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

c) (Optional) **In-Band Network** configuration is not required for Cisco DCNM SAN for OVA/ISO deployment.

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 121.

Click **Next**.

Step 7 On the **Applications** tab, in the IPv4 Subnet field, enter the IP subnet to access the applications that run internally to DCNM.

All the applications use the IP Address from this subnet.

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

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

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

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

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

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

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

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

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

Click **Next**.

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

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

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

Launching SAN Client and Device Manager

This following sections explain the various methods to launch Cisco DCNM SAN Client and Device Manager.

Note For OVA/ISO deployments, you must update the certificates after upgrading to Cisco DCNM Release 11.5(1), before launching the SAN Client or Device Manager. Use the **appmgr afw update-cert-dcnm-client** command to update the certificates.

Launching SAN Client and Device Manager from Web UI

To launch Cisco DCNM SAN Client and Device Manager from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Log in to Cisco DCNM Web UI after installing Cisco DCNM SAN deployment.

Step 2 Click on the gear icon, and click **DCNM SAN & DM**.

Save the `dcnm-client.zip` to your directory.

Step 3 Extract the contents of `dcnm-client.zip` to `dcnm-clientzip/bin` directory.

Step 4 To launch the SAN Client and Device Manager:

- **If you are launching DCNM on Windows environment:**

  Double-click on the **FMClient.bat** file to launch the Cisco DCNM SAN Client.

  Double-click on the **DeviceManager.bat** to launch the Cisco DCNM Device Manager.

- **If you are launching DCNM on Linux environment:**

  Run **./FMClient.sh** Script to launch SAN Client.

  Run **./Devicemanager.sh** script to launch Device Manager.

Launching SAN Client and Device Manager from DCNM Server

By default, the SAN Client and Device Manager are installed along with the Cisco DCNM Server, when you install DCNM. To launch Cisco DCNM SAN Client and Device Manager from the Cisco DCNM Server, perform the following steps:

Procedure

Step 1 Log in to the DCNM server.

Step 2 Navigate to `Cisco Systems\dcm\fm\bin\` directory.

Step 3 To launch the SAN Client and Device Manager:

- **For Windows deployment:**

  Double-click on the **FabricManager.bat** file to launch the Cisco DCNM SAN Client.

  Double-click on the **DeviceManager.bat** file to launch the Cisco DCNM Device Manager.

- **For Linux deployment:**

  Run the **./ FabricManager.sh** script to launch the Cisco DCNM SAN Client.

Run the **./DeviceManager.sh** script to launch the Cisco DCNM Device Manager.

Launching DCNM SAN Client from DCNM SAN for Windows deployment with Custom SSL Certificate

When you install Cisco DCNM for Windows with custom SSL configured on the DCNM server, you can't launch the SAN Client. Modify the certificates to launch the SAN Client successfully.

To modify the certificates and launch the DCNM SAN Client from Windows Deployment, perform the following steps:

Procedure

Step 1 Extract public key using the following command. command.

keytool.exe -exportcert -file dcnmweb.crt -alias sme -keystore C:\[DCNM Install directory]\cisco\dcm\wildfly-14.0.1.Final\Standalone\configuration\fmserver.jks

Step 2 Generate key store using the following command.

keytool.exe -importcert -trustcacerts -file dcnmweb.crt -keystore fmtrust.jks -storetype jks

Step 3 Copy the newly created **fmtrust.jks** to `\fm\lib\fm` directory.

Step 4 Locate the **dcnm-client.zip**, downloaded from Web UI or DCNM server.

Step 5 Unzip and replace the **bin\fmtrust.jks** with the newly created **fmtrust.jks** file.

Step 6 Run the **FabricManager.bat** batch file to launch the Cisco DCNM SAN Client.

Example

The following sample example shows the command to modify the certificates and launch the DCNM SAN Client from Windows Deployment.

```
// extract public key from the new fmserver.jks and save it to dcnmweb.crt,
alias "sme",  password "<<storepass-kwd>>"
c:\[DCNM install directory]\dcm\java\jdk11\bin>
keytool.exe -exportcert -file dcnmweb.crt -alias sme -keystore C:\[DCNM Install directory]
\cisco\dcm\wildfly-14.0.1.Final\Standalone\configuration\fmserver.jks
Enter keystore password:
Certificate stored in file <dcnmweb.crt>
c:\[DCNM install directory]\dcm\java\jdk11\bin> dir
chain-cert.pem  dcnmweb.crt  jjs         keytool  rmiregistry
dcnm.csr        java         jrunscript  rmid


// generate key store without password,  during the command,
just use random password  dcnm123
c:\[DCNM install directory]\dcm\java\jdk11\bin> keytool.exe -importcert -trustcacerts
-file dcnmweb.crt -keystore fmtrust.jks -storetype jks
Enter keystore password:
```

```
Re-enter new password:
Owner: CN=Lin, OU=cisco, O=cisco, L=sj, ST=ca, C=US
Issuer: CN=rhel144, OU=DCBu, O=Cisco, L=BGL, ST=KA, C=IN
Serial number: 1086
Valid from: Wed Nov 13 12:17:23 PST 2019 until: Thu Nov 12 12:17:23 PST 2020
Certificate fingerprints:
         SHA1: F8:19:CB:79:FC:93:08:54:74:9A:BC:F3:8F:CB:9C:A7:22:56:3D:0F
         SHA256: 8F:06:1F:72:15:FD:12:B5:E9:43:E4:61:0E:00:E0:1C:96:CE:9C:90:82:
                 3C:5C:EA:A1:49:A8:A9:66:9B:86:31
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.16.840.1.113730.1.13 Criticality=false
0000: 16 1D 4F 70 65 6E 53 53   4C 20 47 65 6E 65 72 61  ..OpenSSL Genera
0010: 74 65 64 20 43 65 72 74   69 66 69 63 61 74 65     ted Certificate

#2: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: C9 1E 9B 17 EF AE E4 AF   7A E3 88 BC 2D C9 B9 E9  ........z...-...
0010: FC EC 40 82                                        ..@.
]
]#3: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:false
  PathLen: undefined
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 9A 9E B4 98 95 8C 9F FB   0B 57 A5 6D 78 EB 8D C1  .........W.mx...
0010: BB 80 00 DE                                        ....
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
c:\[DCNM install directory]\dcm\java\jdk11\bin>dir
chain-cert.pem  dcnmweb.crt  java  jrunscript  rmid
dcnm.csr        fmtrust.jks  jjs   keytool     rmiregistry


c:\[DCNM install directory]\dcm\java\jdk11\bin> cp fmtrust.jks ..\..\..\fm\lib\fm
cp: overwrite â..\..\..\fm\lib\fm\fmtrust.jks? y


c:\[DCNM install directory]\dcm\java\jdk11\bin> FabricManager.bat
```

Launching DCNM SAN Client from DCNM SAN for Linux deployment with Custom SSL Certificate

When you install Cisco DCNM for Linux with custom SSL configured on the DCNM server, you cant launch the SAN Client. You must modify the certificates to launch the SAN Client successfully.

To modify the certificates and launch the DCNM SAN Client from Linux Deployment, perform the following steps:

Procedure

Step 1 Extract public key using the following command.

./keytool -exportcert -file dcnmweb.crt -alias sme -keystore /usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks

Step 2 Generate key store using the following command.

./keytool -importcert -trustcacerts -file dcnmweb.crt -keystore fmtrust.jks -storetype jks

Step 3 Copy the newly created **fmtrust.jks** to `/fm/lib/fm` directory.

Step 4 Locate the **dcnm-client.zip**, downloaded from Web UI or DCNM server.

Step 5 Replace the **fmtrust.jks** in the `/bin` directory with the newly created **fmtrust.jks** file.

Step 6 Run the **./ FabricManager.sh** script to launch the Cisco DCNM SAN Client.

Example

The following sample example shows the command to modify the certificates and launch the DCNM SAN Client from Linux Deployment.

```
// extract public key from the new fmserver.jks and save it to dcnmweb.crt,
alias "sme",  password "<<storepass-pwd>>"
[root@dcnm-lnx1 bin]# ./keytool -exportcert -file dcnmweb.crt -alias sme
-keystore /usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks
Enter keystore password:
Certificate stored in file <dcnmweb.crt>
[root@dcnm-M5-2-lnx1 bin]# ls
chain-cert.pem  dcnmweb.crt  jjs         keytool  rmiregistry
dcnm.csr        java         jrunscript  rmid


// generate key store without password,  during the command.
[root@dcnm-lnx1 bin]# ./keytool -importcert -trustcacerts -file dcnmweb.crt
-keystore fmtrust.jks -storetype jks
Enter keystore password:       //Navigate to
/usr/local/cisco/dcm/fm/conf/serverstore.properties.
//Fetch the keystore password from dcnmtrustedclient.token field.
Re-enter new password:
Owner: CN=Lin, OU=cisco, O=cisco, L=sj, ST=ca, C=US
Issuer: CN=rhel144, OU=DCBu, O=Cisco, L=BGL, ST=KA, C=IN
Serial number: 1086
Valid from: Wed Nov 13 12:17:23 PST 2019 until: Thu Nov 12 12:17:23 PST 2020
Certificate fingerprints:
         SHA1: F8:19:CB:79:FC:93:08:54:74:9A:BC:F3:8F:CB:9C:A7:22:56:3D:0F
         SHA256: 8F:06:1F:72:15:FD:12:B5:E9:43:E4:61:0E:00:E0:1C:96:CE:9C:90:82:
                 3C:5C:EA:A1:49:A8:A9:66:9B:86:31
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.16.840.1.113730.1.13 Criticality=false
0000: 16 1D 4F 70 65 6E 53 53   4C 20 47 65 6E 65 72 61  ..OpenSSL Genera
```

```
0010: 74 65 64 20 43 65 72 74   69 66 69 63 61 74 65     ted Certificate

#2: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: C9 1E 9B 17 EF AE E4 AF   7A E3 88 BC 2D C9 B9 E9  ........z...-...
0010: FC EC 40 82                                        ..@.
]
]

#3: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:false
  PathLen: undefined
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 9A 9E B4 98 95 8C 9F FB   0B 57 A5 6D 78 EB 8D C1  .........W.mx...
0010: BB 80 00 DE                                        ....
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
[root@dcnm-M5-2-lnx1 bin]# ls
chain-cert.pem  dcnmweb.crt  java  jrunscript  rmid
dcnm.csr        fmtrust.jks  jjs   keytool     rmiregistry
[root@dcnm-M5-2-lnx1 bin]# pwd
/usr/local/cisco/dcm/java/jdk11/bin

[root@dcnm-M5-2-lnx1 bin]#

[root@dcnm-M5-2-lnx1 bin]# cp fmtrust.jks ../../../fm/lib/fm
cp: overwrite â../../../fm/lib/fm/fmtrust.jks? y


[root@dcnm-M5-2-lnx1 dcm]# cd fm/download/
[root@dcnm-M5-2-lnx1 download]# pwd
/usr/local/cisco/dcm/fm/download
[root@dcnm-M5-2-lnx1 download]# ls
dcnm-clientzip.zip
// for remote access, in fm/download/dcnm-clientzip.zip,
replace bin/fmtrust.jks with this new fmtrust.jks


[root@dcnm-M5-2-lnx1 bin]# ./ FabricManager.sh
```

Launching DCNM SAN Client from DCNM SAN for OVA/ISO deployment with Custom SSL Certificate

When you install Cisco DCNM SAN OVA/ISO with custom SSL configured on the DCNM server, you can't launch the SAN Client. Install the CA signed certificate, and then, download and launch the DCNM SAN Client from the Web UI.

Refer to Installing a CA Signed Certificate, on page 114 for instructions on how to install the CA signed certificate on the Cisco DCNM SAN OVA/ISO server.

For OVA/ISO deployments, you must update the certificates after upgrading to Cisco DCNM Release 11.5(1), before launching the SAN Client or Device Manager. Use the **appmgr afw update-cert-dcnm-client** command to update the certificates.

Launch the Web UI. Download the DCNM SAN Client. Launch the DCNM SAN Client and Device Manager.

Launching DCNM SAN Client from Cisco SAN OVA/ISO Server

To launch DCNM SAN client on the Cisco DCNM SAN OVA/ISO server, perform the following steps:

Note Do not install any GUI package / X11 or VNC on DCNM SAN OVA/ISO server.

Before you begin

For OVA/ISO deployments, you must update the certificates after upgrading to Cisco DCNM Release 11.5(1), before launching the SAN Client or Device Manager. Use the **appmgr afw update-cert-dcnm-client** command to update the certificates.

Procedure

Step 1 VNC to any DCNM server where VNC is installed, for example, `vnc-lnx:2`.

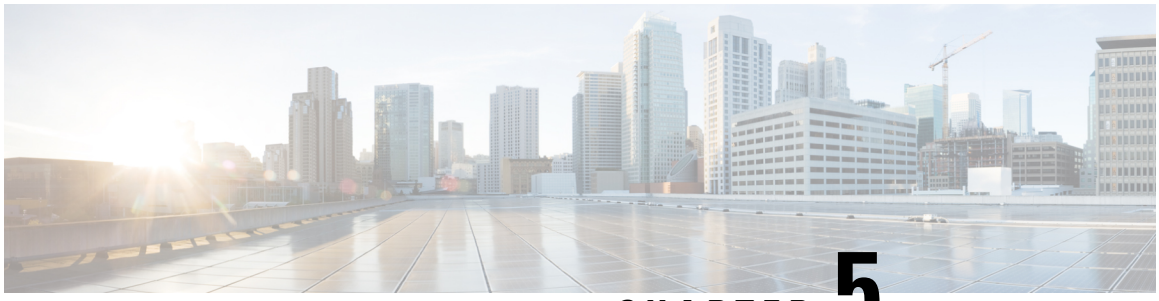
Step 2 Open two terminals in `vnc-lnx`.

Step 3 In one terminal execute the command **xhost +**.

Step 4 In the second terminal, SSH to DCNM OVA server.

Step 5 Export **DISPLAY=vnc-lnx:2.0**.

Step 6 Launch the SAN client from the terminal in Step Step 4, on page 79.



CHAPTER 5

Upgrading Cisco DCNM

This chapter provides information about upgrading Cisco DCNM, and contains the following section:

- Upgrading Cisco DCNM, on page 81
- Retaining the CA Signed Certificate, on page 82
- Upgrading to Cisco SAN on OVA/ISO, on page 83

Upgrading Cisco DCNM

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. However, there is not upgrade path for SAN OVA\ISO.

From Release 11.3(1), Cisco DCNM OVA and ISO is supported for SAN functionality.

The following table summarizes the type of upgrade that you must follow to upgrade to Release 11.3(1).

Table 6: Type of Upgrade for Cisco DCNM SAN deployments

Current Release Number	Upgrade type to upgrade to Release 11.3(1)
11.2(1)	To Windows—Inline Upgrade To Linux—Inline Upgrade To OVA\ISO— **1.** Fresh 11.3(1) SAN Only Installation. **2.** Migrate Performance Manager Collections **Note** The old Performance Manager data will replace any existing Performance Manager data on 11.3(1).

Current Release Number	Upgrade type to upgrade to Release 11.3(1)
11.1(1)	To Windows—Inline Upgrade To Linux—Inline Upgrade To OVA\ISO— 1. Fresh 11.3(1) SAN Only Installation. 2. Migrate Performance Manager Collections **Note** The old Performance Manager data will replace any existing Performance Manager data on 11.3(1).
10.4(2) OVA 10.4(1) OVA	To 11.3(1) OVA\ISO— 1. Fresh 11.3(1) SAN Only Installation. 2. Migrate Performance Manager Collections **Note** The old Performance Manager data will replace any existing Performance Manager data on 11.3(1).

Retaining the CA Signed Certificate

Perform this procedure if you need to retain the CA signed SSL Certificate after upgrade.

When you configure a 3-node federation setup and apply external CA certificate, do the following:

1. Stop DCNM servers in Federation.
   - For Windows – Navigate to `C:\Program Files\Cisco Systems\dcm\dcnm\bin`. Double-click on the `StopLANSANServer.bat` to stop the services.
   - For Linux – Logon to `/root`. Execute **/root/Stop_DCNM_Servers** command to stop services.
2. Generate CA certificates for Primary Servers, and apply the same CA certificate in the three secondary servers.
3. Start the Primary server first, then the secondary, third server thereafter, on Federation.

Note that if you change the keystore password or alias, you need to update it in the **standalone-san.xml** document located at:

`<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\standalone-san.xml`

Update the password in the **keystore** tag and alias:

```
<keystore key-password>="fmserver_1_2_3 key-alias="updated-key-alias"
keystore-password="updated-password"
path="<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks">
```

Procedure

Step 1 Backup the signed certificate from the location:

- For Windows: **<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks**
- For Linux: **<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks**

Step 2 Upgrade to Cisco DCNM Release 11.3(1).

Step 3 After upgrade, copy the certificate to the same location on the upgraded version of the Cisco DCNM.

Note You must load the certificates to the same location as mentioned in Step 1, on page 83.

Step 4 Restart the DCNM Services.

Upgrading to Cisco SAN on OVA/ISO

From Release 11.3(1), you can install Cisco DCNM SAN on OVA\ISO. However, you cannot migrate the older release DCNM to Release 11.3(1). Instead, perform a fresh install of Cisco DCNM for SAN on OVA or ISO, and import the Performance Manager data from the older version.

Note Before you start to upgrade, close all instances of DCNM SAN client, both SAN Client and Device Manager running on the server.

For instructions, see *Inline Upgrade for DCNM Virtual Appliance in Standalone Mode* section.

PM Data Migration

There is no upgrade path to DCNM SAN for OVA/ISO. However, fresh installation of Cisco DCNM 11.3(1) allows you to migrate the Performance Manager data from the following releases:

Use the following upgrade paths to upgrade to Cisco DCNM Release 11.3(1).

- 11.2(1) SAN to 11.3(1) SAN OVA/ISO
- 11.1(1) SAN to 11.3(1) SAN OVA/ISO
- 10.4(2) SAN OVA to 11.3(1) SAN OVA/ISO

Note If you choose to conserve the Performance Manager data when you upgrade to Release , we recommend that you contact Cisco TAC for further assistance.

Note Ensure that you stop Performance Manager on Cisco DCNM 11.3(1) before migrating the performance manager data. You must start performance manager data collection after the upgrade completes.

Note The newly collected data in the Cisco DCNM 11.3(1) will be replaced with migrated Performance Manager collections data.

SAN Insights data from older releases

SAN Insights data from older releases is too large and it is refreshed every two weeks. We recommend that you do not migrate the SAN Insight data to the fresh DCNM 11.3(1) OVA/ISO installation.

If you are using Performance Monitoring on the fabric(s), migrate the Performance Manager data using the procedure in this section. However, this procedure copies everything in the Elasticsearch database. Therefore, before using this procedure, remove the SAN Insights data for each of the switch that is streaming data to DCNM, using the following command:

*<DCNM Install Location>***\dcm\fm\bin\FMGeneric.bat com.cisco.dcbu.analytics.CleanupSanInsightES** *<switchname_in_lowercase> <switch_ip_address>*

```
C:\Program Files\CiscoDCNM\dcm\fm\bin\FMGeneric.bat
com.cisco.dcbu.analytics.CleanupSanInsightES mds9396t-174145 XXX.XX.XXX.XXX
```

The following sections provide instructions to migrate PM data to the newly installed Cisco DCNM 11.3(1) appliance.

PM Data Migration from 10.4(x) SAN OVA/ISO/Windows to the New DCNM 11.3(1) OVA/ISO

In Release 10.4(1) OVA or 10.4(2) OVA the performance manager uses RRD as database to store all raw data. Cisco DCNM offers an inline migration process to migrate RRD files to Elastic database.

To migrate 10.4(1) or 10.4(2) OVA data to 11.3(1) OVA\ISO, perform the following steps:

Procedure

Step 1 Stop the DCNM 10.4(1) or 10.4(2) server.

- For Windows – Navigate to `C:\Program Files\Cisco Systems\dcm\dcnm\bin`. Double-click on the `StopLANSANServer.bat` to stop the services.
- For Linux – Logon to `/root`. Execute **/root/Stop_DCNM_Servers** command to stop services.

Step 2 Navigate to `/usr/local/cisco/dcm/fm/pm/db` where the RRD files are located.

Copy the RRD files to a safe location.

For Windows – Right-click on the RRD files folder and click **Copy**. Paste the contents to a safe directory.

For Linux – Execute the copy **/usr/local/cisco/dcm/fm/pm/db/**<<*rrd_directory*>> to copy all the RRD files to a safe directory.

Step 3 In the new installed DCNM 11.3(1) SAN OVA\ISO server, discover the same fabric.

Step 4 After fabric discovery, enable SAN Collections to begin Performance Manager collections.

Choose Cisco DCNM **Web UI > Administration > DCNM Server > Server Status > Performance Collector**. Verify the Status column.

Allow the DCNM server for 60 to 70 minutes to ensure that the Performance manager is collecting data from the Cisco DCNM Web UI.

Step 5 Provide root access to the DCNM Server by using **appmgr root-access permit** command.

Step 6 On the 11.3(1) DCNM Server, navigate to `/usr/local/cisco/dcm/fm/pm/db/` directory.

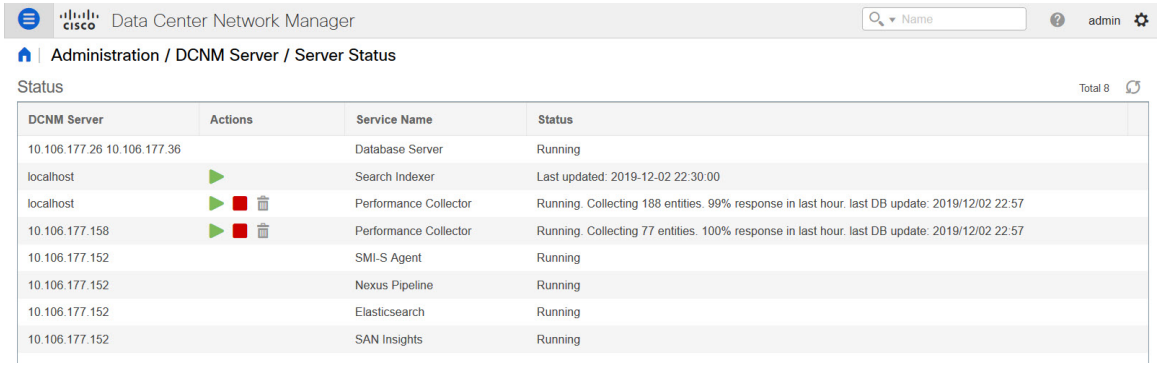
Copy the RRD files from the older DCNM to this directory.

Step 7 Change the read and write permissions to all RRD files using the chmod -R 777 command.

Step 8 Choose **Administration > DCNM Server > Server Status**.

Identify the Performance Collector Service.

Step 9 Under the **Actions** column, click **Stop Service** icon to stop the performance collector service. Click **Re(Start) Service** icon to start the collections.



Based on the volume of RRD files, the migration can take longer duration. After data migration, all the migrated RRD files is copied to the `db_backup` location. You can view the historical data from the Web UI.

PM Data Migration from 11.1(1) and 11.2(1) Windows to fresh install of 11.3(1) OVA/ISO

Note The data from Windows Federation can't be migrated to Release 11.3(1) SAN OVA\ISO Deployment.

In the fresh install 11.3(1) OVA, discover the same fabric and enable performance manager. When you import the old data to 11.3(1), it replaces the data existing data on 11.3(1).

To migrate 11.1(1) or 11.2(1) DCNM Windows performance manager data to 11.3(1) SAN OVA\ISO deployment, perform the following steps:

Procedure

Step 1 Stop the elastic search service on the older DCNM version.

On the Web UI, choose **Administration > DCNM Server > Server Status**. Stop Performance Manager collections.

Step 2 Take a backup of the Performance Manager collections directory files located at `\\DCNM_Install_Directory\dcm\elasticsearch\data\`.

Zip all the files and save files to a safe location.

Note The zip file must have the root folder and nodes and all the subfolder with data.

```
[root@dcnm173 ~]# unzip -l nodes.zip
Archive:  nodes.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
        0  10-15-2019 04:34   nodes/
        0  10-15-2019 04:34   nodes/0/
        0  10-15-2019 04:34   nodes/0/indices/
        0  10-15-2019 04:34   nodes/0/indices/5AJ72Xv0SXKfXaD9IDMbdw/
        0  10-15-2019 04:34   nodes/0/indices/5AJ72Xv0SXKfXaD9IDMbdw/0/
        0  10-15-2019 04:34   nodes/0/indices/5AJ72Xv0SXKfXaD9IDMbdw/0/index/
      615  10-15-2019 04:33   nodes/0/indices/5AJ72Xv0SXKfXaD9IDMbdw/0/index/segments_11
        0  10-10-2019 00:28   nodes/0/indices/5AJ72Xv0SXKfXaD9IDMbdw/0/index/write.lock
       82  10-15-2019 03:58   nodes/0/indices/5AJ72Xv0SXKfXaD9IDMbdw/0/index/_1ay.dii
        .
        ..
        ...
     2037  10-10-2019 00:28   nodes/0/indices/CMzGQjhtS-W3xyPoT1ktnw/_state/state-13.st
        0  10-10-2019 00:12   nodes/0/node.lock
        0  10-15-2019 04:34   nodes/0/_state/
     4668  10-10-2019 00:24   nodes/0/_state/global-7.st
       71  10-10-2019 00:12   nodes/0/_state/node-0.st
---------                     -------
129921151                     487 files
[root@dcnm173 ~]#
```

Step 3 On 11.3(1) DCNM server, provide root access to the DCNM Server, by using **appmgr root-access permit** command.

Step 4 Copy the zip file to the freshly installed DCNM 11.3(1) SAN OVA\ISO server.

Note You can copy the zip file contents to any safe directory.

Step 5 Stop the Performance Manager on the DCNM 11.3(1) Windows SAN appliance.

Step 6 Migrate the Performance Manager data using the **appmgr migrate-pm-es-data** command.

Note After the old version DCNM Performance Manager data is migrated, the original 11.3(1) Performance Manager data is erased.

```
dcnm11-3-1# appmgr migrate-pm-es-data nodes.zip
stop elasticsearch
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Archive:  nodes.zip
   creating: /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/

   creating: /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/
```

```
   creating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/
   creating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDModw/

   creating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDModw/0/

   creating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDModw/0/index/

  inflating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDModw/0/index/segments_11

 extracting:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDModw/0/index/write.lock

 extracting:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDModw/0/index/_1ay.dii

  inflating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDModw/0/index/_1ay.dim

           .
           ..
           ...
    ending: inflating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/CMzGQjhtS-W3xyPoT1ktnw/_state/state-13.st
extracting:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/node.lock
  creating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/_state/
 inflating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/_state/global-7.st
extracting:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/_state/node-0.st
Started AFW Server Processes
Started AFW Agent Processes
dcnm11-3-1#
```

Wait for approximately 30 minutes for the data to be migrated.

Step 7 Verify the status of elastic search by using the **docker ps** command.

```
dcnm11-3-1# docker ps
CONTAINER ID        IMAGE                                       COMMAND
CREATED             STATUS              PORTS                    NAMES
8dfa2935cb0d        127.0.0.1:5000/afwapiproxy:2.0              "/bin/entry.sh"          20
seconds ago      Up 17 seconds       0.0.0.0:443->443/tcp   AfwApiProxy
6839a3d88cb4        127.0.0.1:5001/saninsightpost:1.0           "java -Xms1G -Xmx7..."   20
seconds ago      Up 17 seconds
saninsightpost_Cisco_afw.9hfm7g3g0l6y7as0f8e4e288m.qk3gw8a4wm1g7pg8k4rsx4qme
6bbdff07fc8a        127.0.0.1:5001/epltwo:2.0                   "/bin/sh -c /usr/l..."   22
seconds ago      Up 19 seconds
epltwo_Cisco_afw.9hfm7g3g0l6y7as0f8e4e288m.0newc0fzp1frqt08i8xjjdx5h
896336c7689a        127.0.0.1:5001/saninsightcol:1.0            "/bin/pipeline.sh "      23
seconds ago      Up 20 seconds
saninsightcol_Cisco_afw.9hfm7g3g0l6y7as0f8e4e288m.vzqkxe8owuf9y18icawns3abw
9bc609916781        127.0.0.1:5001/dcnmelastic:5.6.7_11.2.2     "/docker-entrypoin..."   25
seconds ago      Up 22 seconds       9200/tcp, 9300/tcp
elasticsearch_Cisco_afw.9hfm7g3g0l6y7as0f8e4e288m.owdosoye1rco3rr4790429zky
ee78966aef89        127.0.0.1:5000/registry:2                   "/sbin/entry.sh"         26
seconds ago      Up 23 seconds
registry_cisco_afw.1.xwsd91ty6oajfp7ukfvw2iutd
```

```
cc635ab41796        registry:2                                "/sbin/entry.sh"         42
seconds ago      Up 40 seconds                                AfwAppRegistry
```

Step 8 Restart the DCNM Server by using the **appmgr restart all** command.

Wait for 10 minutes for DCNM to stabilize and connect to the new performance manager data.

PM Data Migration from 11.1(1) and 11.2(1) Linux to fresh install of 11.3(1) OVA/ISO

Note The data from Linux Federation can't be migrated to Release 11.3(1) SAN OVA\ISO Deployment.

In the fresh install 11.3(1) OVA, discover the same fabric and enable performance manager. When you import the old data to 11.3(1), it replaces the data existing data on 11.3(1).

To migrate 11.1(1) or 11.2(1) DCNM Linux performance manager data to 11.3(1) SAN OVA\ISO deployment, perform the following steps:

Procedure

Step 1 Stop the elastic search service on the older DCNM version.

On the Web UI, choose **Administration > DCNM Server > Server Status**. Stop Performance Manager collections.

Step 2 Take a backup of the Performance Manager collections directory files located at `\\DCNM_Install_Directory\dcm\elasticsearch\data\`.

Zip all the files and save files to a safe location.

Note The zip file must have the root folder and nodes and all the subfolder with data.

```
[root@dcnm]# unzip -l nodes.zip
Archive:  nodes.zip
  Length      Date    Time    Name
---------  ---------- -----   ----
        0  10-15-2019 04:34   nodes/
        0  10-15-2019 04:34   nodes/0/
        0  10-15-2019 04:34   nodes/0/indices/
        0  10-15-2019 04:34   nodes/0/indices/5AJ72Xv0SXKfXaD9IDMbdw/
        0  10-15-2019 04:34   nodes/0/indices/5AJ72Xv0SXKfXaD9IDMbdw/0/
        0  10-15-2019 04:34   nodes/0/indices/5AJ72Xv0SXKfXaD9IDMbdw/0/index/
      615  10-15-2019 04:33   nodes/0/indices/5AJ72Xv0SXKfXaD9IDMbdw/0/index/segments_11
        0  10-10-2019 00:28   nodes/0/indices/5AJ72Xv0SXKfXaD9IDMbdw/0/index/write.lock
       82  10-15-2019 03:58   nodes/0/indices/5AJ72Xv0SXKfXaD9IDMbdw/0/index/_1ay.dii
        .
        ..
        ...
     2037  10-10-2019 00:28   nodes/0/indices/CMzGQjhtS-W3xyPoT1ktnw/_state/state-13.st
        0  10-10-2019 00:12   nodes/0/node.lock
        0  10-15-2019 04:34   nodes/0/_state/
     4668  10-10-2019 00:24   nodes/0/_state/global-7.st
```

```
       71  10-10-2019 00:12   nodes/0/_state/node-0.st
---------                     -------
129921151                     487 files
[root@dcnm]#
```

Step 3 Zip all the files and save files to a safe location, using the **zip -r myPMData.zip ./** command.

Note The zip file must have the root folder and nodes and all the subfolder with data.

```
[root@dcnm]# zip -r nodes.zip nodes
  adding: nodes/ (stored 0%)
  adding: nodes/0/ (stored 0%)
  adding: nodes/0/indices/ (stored 0%)
  adding: nodes/0/indices/CMzGQjhtS-W3xyPoT1ktnw/ (stored 0%)
  adding: nodes/0/indices/CMzGQjhtS-W3xyPoT1ktnw/3/ (stored 0%)
  adding: nodes/0/indices/CMzGQjhtS-W3xyPoT1ktnw/3/index/ (stored 0%)
  adding: nodes/0/indices/CMzGQjhtS-W3xyPoT1ktnw/3/index/_114o.fdx (deflated 2%)
  adding: nodes/0/indices/CMzGQjhtS-W3xyPoT1ktnw/3/index/_1bsm.fnm (deflated 87%)
  adding: nodes/0/indices/CMzGQjhtS-W3xyPoT1ktnw/3/index/_1cs1.si (deflated 23%)
  adding: nodes/0/indices/CMzGQjhtS-W3xyPoT1ktnw/3/index/_1bsm.si (deflated 38%)
  .
  ..
  ...
  adding: nodes/0/indices/5AJ72Xv0SXKfXaD9IDMbdw/2/_state/ (stored 0%)
  adding: nodes/0/indices/5AJ72Xv0SXKfXaD9IDMbdw/2/_state/state-0.st (deflated 5%)
  adding: nodes/0/indices/5AJ72Xv0SXKfXaD9IDMbdw/_state/ (stored 0%)
  adding: nodes/0/indices/5AJ72Xv0SXKfXaD9IDMbdw/_state/state-3.st (deflated 9%)
  adding: nodes/0/node.lock (stored 0%)
  adding: nodes/0/_state/ (stored 0%)
  adding: nodes/0/_state/global-7.st (deflated 72%)
  adding: nodes/0/_state/node-0.st (deflated 7%)
[root@dcnm]#
```

Step 4 On 11.3(1) DCNM server, provide root access to the DCNM Server, by using **appmgr root-access permit** command.

Step 5 Copy the zip file to the freshly installed DCNM 11.3(1) SAN OVA\ISO server.

Note You can copy the zip file contents to any safe directory.

Step 6 Stop the Performance Manager on the DCNM 11.3(1) Linux SAN appliance.

Step 7 Migrate the Performance Manager data using the **appmgr migrate-pm-es-data** command.

Note After the old version DCNM Performance Manager data is migrated, the original 11.3(1) Performance Manager data is erased.

```
dcnm11-3-1# appmgr migrate-pm-es-data nodes.zip
stop elasticsearch
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Archive:  nodes.zip
   creating: /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/

   creating: /var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/

   creating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/
   creating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDMbdw/

   creating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDMbdw/0/
```

```
   creating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDModw/0/index/

  inflating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDModw/0/index/segments_11

 extracting:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDModw/0/index/write.lock

 extracting:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDModw/0/index/_1ay.dii

  inflating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/5AJ72Xv0SXKfXaD9IDModw/0/index/_1ay.dim

           .
           ..
           ...
    ending: inflating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/indices/CMzGQjhtS-W3xyPoTlktnw/_state/state-13.st
extracting:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/node.lock
  creating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/_state/
 inflating:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/_state/global-7.st
extracting:
/var/afw/vols/data/elasticsearch_Cisco_afw/usr/share/elasticsearch/data/nodes/0/_state/node-0.st
Started AFW Server Processes
Started AFW Agent Processes
dcnm11-3-1#
```

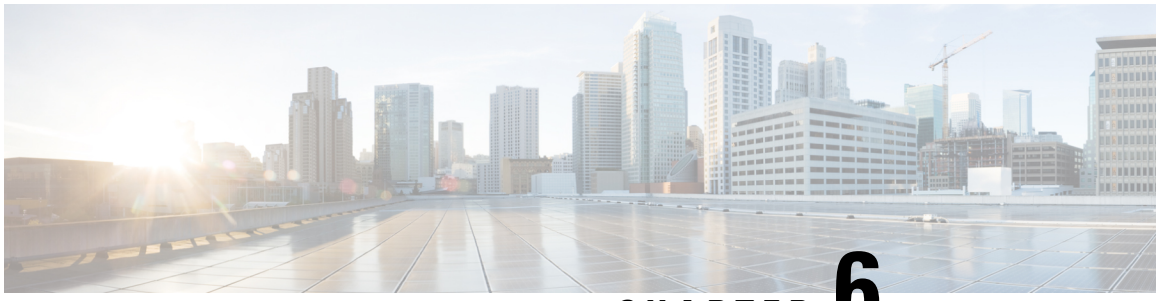
Wait for approximately 30 minutes for the data to be migrated.

Step 8 Verify the status of elastic search by using the **docker ps** command.

```
dcnm11-3-1# docker ps
CONTAINER ID        IMAGE                                       COMMAND
CREATED             STATUS              PORTS                    NAMES
8dfa2935cb0d        127.0.0.1:5000/afwapiproxy:2.0              "/bin/entry.sh"          20
seconds ago      Up 17 seconds       0.0.0.0:443->443/tcp   AfwApiProxy
6839a3d88cb4        127.0.0.1:5001/saninsightpost:1.0           "java -Xms1G -Xmx7..."   20
seconds ago      Up 17 seconds
saninsightpost_Cisco_afw.9hfm7g3g0l6y7as0f8e4e288m.qk3gw8a4wm1g7pg8k4rsx4qme
6bbdff07fc8a        127.0.0.1:5001/epltwo:2.0                   "/bin/sh -c /usr/l..."   22
seconds ago      Up 19 seconds
epltwo_Cisco_afw.9hfm7g3g0l6y7as0f8e4e288m.0newc0fzp1frqt08i8xjjdx5h
896336c7689a        127.0.0.1:5001/saninsightcol:1.0            "/bin/pipeline.sh "      23
seconds ago      Up 20 seconds
saninsightcol_Cisco_afw.9hfm7g3g0l6y7as0f8e4e288m.vzqkxe8owuf9y18icawns3abw
9bc609916781        127.0.0.1:5001/dcnmelastic:5.6.7_11.2.2     "/docker-entrypoin..."   25
seconds ago      Up 22 seconds       9200/tcp, 9300/tcp
elasticsearch_Cisco_afw.9hfm7g3g0l6y7as0f8e4e288m.owdosoye1rco3rr4790429zky
ee78966aef89        127.0.0.1:5000/registry:2                   "/sbin/entry.sh"         26
seconds ago      Up 23 seconds
registry_cisco_afw.1.xwsd91ty6oajfp7ukfvw2iutd
cc635ab41796        registry:2                                  "/sbin/entry.sh"         42
seconds ago      Up 40 seconds                                AfwAppRegistry
```

Step 9 Restart the DCNM Server by using the **appmgr restart all** command.

Wait for 10 minutes for DCNM to stabilize and connect to the new performance manager data.



CHAPTER 6

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 93
- Configuring Custom Firewalls, on page 101

Running Cisco DCNM Behind a Firewall

Generally, an Enterprise (external world) and Datacenter is separated by a firewall, i.e., DCNM is configured behind a firewall. The Cisco DCNM Web Client, Cisco DCNM SAN Client, and Cisco Device Manager connectivity will pass-through that firewall. A firewall can be placed between the DCNM Server and DCNM-managed devices also.

Beginning with Cisco DCNM Release 11.0(1), DCNM SAN Client initiates communication with DCNM SAN Server on HTTPS port 443. However, both DCNM SAN Client and Device Manager communicate with the devices directly also. Device Manager can be invoked through DCNM SAN Server UI and it runs within the context of the DCNM SAN Server. The Device Manager communication with devices remains same, as if it was running independently.

DCNM SNMP proxy services on DCNM SAN Server use a configurable TCP port (9198 by default) for SNMP communications between the DCNM SAN Client or Device Manager, and DCNM Server.

Performance Manager uses TCP, by default, for data collections.

The UDP SNMP_TRAP local ports are between 1163-1170, for both Cisco DCNM-SAN and Device Manager. DCNM-SAN Client and Device Manager use the first available UDP port for sending and receiving SNMP responses.

You can select the UDP port that the Device Manager uses for SNMP responses by uncommenting the following statement:

- On a Windows desktop, uncomment the following in the `DeviceManager.bat` file in the `C:\Program Files\Cisco Systems\MDS9000\bin` directory:

  ```
  rem JVMARGS=%JVMARGS% -Dsnmp.localport=[localport]
  ```

  Where [localport] is the value of free local port.

Note On the windows VM, run the **netstat -nab** command, to view the ports that are used by the `javaw.exe` process.

- On a LINUX desktop, uncomment the following in the `DeviceManager.sh` file in the `$HOME/.cisco_mds9000/bin` directory:

  ```
  # JVMARGS=$JVMARGS -Dsnmp.localport=[localport]
  ```

  Where [localport] is the value of free local port.

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 DCNM Web Client, DCNM SAN Client, Device Manager, SSH Client, and DCNM Server.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
22	TCP	SSH	SSH to DCNM SAN Server	SSH access to external world is optional.
443	TCP	HTTPS	Client to DCNM SAN Server	Cisco DCNM Web Client, Cisco DCNM SAN Client to the Cisco DCNM Server
1099	TCP	Java RMI	Client to DCNM SAN Server	Cisco DCNM SAN Client to Server
1163 to 1170	UDP	SNMP_TRAP	Device to SAN Client and Device Manager	Cisco DCNM SAN Client and Cisco Device Manager use same range of ports.
2443	TCP	HTTPS	Client to DCNM Server	Required during installation, to reach the server. DCNM closes this port after installation completes. Required only for DCNM SAN OVA/ISO during installation, to reach the server. DCNM SAN server closes this port after installation completes.
3528	TCP	JBOSS	Client to DCNM SAN Server	Wildfly JBOSS IIOP
3529	TCP	JBOSS	Client to DCNM SAN Server	Wildfly JBOSS IIOP SSL

Port Number	Protocol	Service Name	Direction of Communication	Remarks
9198	UDP/TCP	SNMP	SAN Client, Device Manager to DCNM SAN Server. Cisco DCNM SAN Client picks a random free local port (UDP) or 9198 (TCP) if SNMP proxy is enabled. The port can be changed with the `client -Dsnmp.localport` option. Cisco Device Manager picks a random free local port (UDP) or 9198 (TCP) if SNMP proxy is enabled. The port can be changed in `server.properties` file. DCNM SNMP proxy is used when SAN Client or Device Manager cannot reach managed devices directly and SNMP responses coming to DCNM SAN Server from managed devices can be relayed to SAN Client and Device Manager. DCNM SAN Client and Device Manager must reach to DCNM SAN Server port 9198 (or whatever port is configured) to get the SNMP response.	Cisco DCNM SNMP proxy services use the TCP port (9198 by default) for SNMP communications between the Cisco DCNM SAN Client or Cisco Device Manager and the Cisco DCNM Server.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
61616	TCP	Messaging	DCNM SAN Client to DCNM SAN Server	

The following table lists all the ports that are used for communication between the Cisco DCNM Server and other services which can be hosted on either side of the firewall.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
49	TCP/UDP	TACACS+	Cisco DCNM SAN Server to ACS Server	ACS Server can be on either side of the firewall.
53	TCP/UDP	DNS	Cisco DCNM SAN Server to DNS Server	DNS Server can be on either side of the firewall.
123	UDP	NTP	Cisco DCNM SAN Server to NTP Server	NTP Server can be on either side of the firewall.
1521	TCP	Oracle	DCNM SAN Server to the Oracle database Server	This is necessary if the Oracle server is installed external to the DCNM host machine. Oracle server may be configured to listen on a different port and in that case that port in question must be taken into account. **Note** You can choose the Oracle server port during DCNM SAN installation and must not be modified later, after installation.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
5432	TCP	Postgres	Cisco DCNM SAN Server to Postgres Server	The default installation of DCNM does not need this port. This is necessary if Postgres is installed externally to the DCNM host machine.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
9198	UDP\TCP	SNMP	DCNM SAN Client, Device Manager to DCNM SAN Server	

Port Number	Protocol	Service Name	Direction of Communication	Remarks
				Cisco DCNM SNMP proxy services use the TCP port (9198 by default) on DCNM SAN Server for SNMP communications between the Cisco DCNM SAN Client or Cisco Device Manager and the Cisco DCNM Server. Cisco DCNM SAN Client picks a random free local port (UDP) or 9198 (TCP) to reach SNMP proxy. The port can be changed with the client -Dsnmp.localportoption. Cisco Device Manager picks a random free local port (UDP) or 9198 (TCP) to reach SNMP proxy. The port can be changed in the server.properties file. DCNM SNMP proxy is used when SAN Client or Device Manager cannot reach the managed devices directly and SNMP responses coming to DCNM SAN Server from managed devices can be relayed to SAN Client and Device Manager. DCNM

Port Number	Protocol	Service Name	Direction of Communication	Remarks
				SAN Client and Device Manager must reach to DCNM SAN Server port 9198 (or whatever port is configured) to get the SNMP response.

The following table lists all the ports that are used for communication between Cisco DCNM Server and Managed devices.

Port Number	Protocol	Service Name	Direction of Communication	Remarks
22	TCP	SSH	Both Direction	Server to Device – To manage devices. Device to Server – SCP (POAP)
67	UDP	DHCP	Device to DCNM SAN Server	
69	TCP	TFTP	Device to DCNM SAN Server	Required for POAP
161	TCP/UDP	SNMP	DCNM SAN Server to Device	Cisco DCNM configured via `server.properties` to use TCP on port 161 instead of UDP port 161.
514	UDP	Syslog	Device to DCNM SAN Server	
2162	UDP	SNMP_TRAP	Device to DCNM SAN Server	

Port Number	Protocol	Service Name	Direction of Communication	Remarks
5989	TCP	SMI-S Agent	Both direction	Server to Device. This is where the Storage device listens. An application to DCNM Server – When DCNM Server is acting as storage proxy. Server to the Storage device port number is depended upon where the storage device is listening on. It could be 5989, 5888, or other ports.
57500	TCP	gRPC	Device to DCNM SAN Server	SAN 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

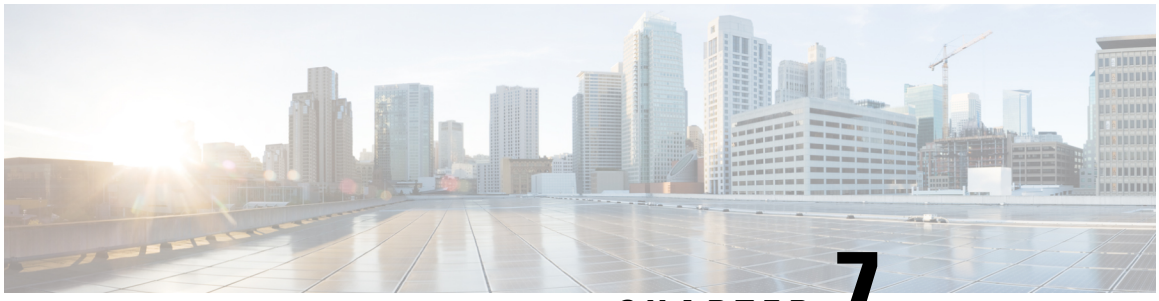
In a Cisco DCNM Native HA setup, when you execute the **appmgr user-firewall commit** on the Active node, the rules are synchronized to the Standby node automatically. However, the new rules are operational only after a system reboot.

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 7

User and Schemas

This chapter provides information about creating Users and user-specific schema for *Cisco Data Center Network Manager*.

- Creating New Users, on page 105
- Creating New Schema for Existing Users, on page 105

Creating New Users

Perform this task, to create a new user.

Procedure

Step 1 Logon to the SSH terminal of the DCNM Appliance.

Step 2 Create a new user using the **create user** *username* command.

Step 3 Enter a valid password at the password prompt.

Step 4 Create a new schema with same name as the user, using the **create schema***username***authorization***username*.

Step 5 Enable all permissions on the schema, using the **grant all on schema***username***to***username*.

Example

The following example shows the sample output for creating new users

```
dcnm# create user user1
password: password
dcnm# create schema user1 authorization user1;
dcnm# grant all on schema user1 to user1;
```

Creating New Schema for Existing Users

Perform this task to retain the same create new schema to an existing user.

Procedure

Step 1 Logon to the SSH terminal of the DCNM Appliance.

Step 2 Drop the existing user by using the **drop user***username***cascade** command.

Step 3 Drop the existing schema with same name as username, by using the **drop schema***username***cascade** command.

Step 4 Create a new user using the **create user** *username* command.

Step 5 Enter a valid password at the password prompt.

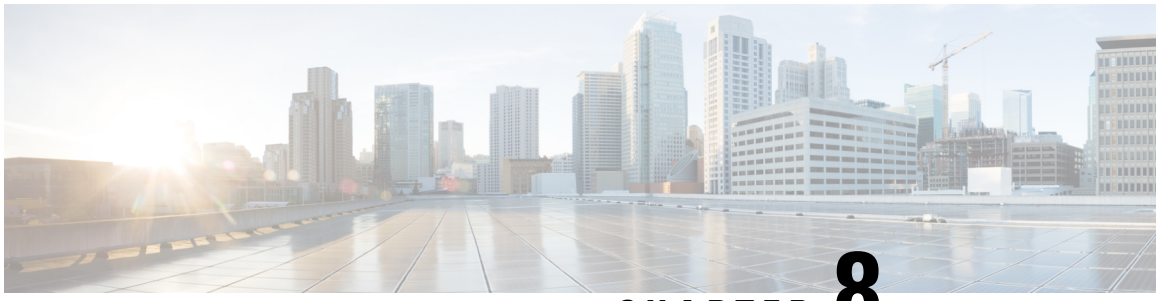
Step 6 Create a new schema with same name as the user, using the **create schema***username***authorization***username* command.

Step 7 Enable all permissions on the schema, using the **grant all on schema***username***to***username*.

Example

The following example shows the sample output for creating new users

```
dcnm# drop user user_old cascade
dcnm# drop schema user_old cascade
dcnm# create user user_new
password: password
dcnm# create schema user_new authorization user_new;
dcnm# grant all on schema user_new to user_new;
```



CHAPTER 8

Certificates

- Retaining the CA Signed Certificate, on page 107
- Certificates Management for SAN Windows/Linux, on page 108
- Certificate Management for SAN OVA/ISO, on page 112

Retaining the CA Signed Certificate

Perform this procedure if you need to retain the CA signed SSL Certificate after upgrade.

When you configure a 3-node federation setup and apply external CA certificate, do the following:

1. Stop DCNM servers in Federation.
   - For Windows – Navigate to `C:\Program Files\Cisco Systems\dcm\dcnm\bin`. Double-click on the `StopLANSANServer.bat` to stop the services.
   - For Linux – Logon to `/root`. Execute **/root/Stop_DCNM_Servers** command to stop services.
2. Generate CA certificates for Primary Servers, and apply the same CA certificate in the three secondary servers.
3. Start the Primary server first, then the secondary, third server thereafter, on Federation.

Note that if you change the keystore password or alias, you need to update it in the **standalone-san.xml** document located at:

`<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\standalone-san.xml`

Update the password in the **keystore** tag and alias:

```
<keystore key-password>="fmserver_1_2_3 key-alias="updated-key-alias"
keystore-password="updated-password"
path="<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks">
```

Procedure

Step 1 Backup the signed certificate from the location:

- For Windows: **<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks**

- For Linux: **<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks**

Step 2 Upgrade to Cisco DCNM Release 11.3(1).

Step 3 After upgrade, copy the certificate to the same location on the upgraded version of the Cisco DCNM.

Note You must load the certificates to the same location as mentioned in Step 1, on page 107.

Step 4 Restart the DCNM Services.

Certificates Management for SAN Windows/Linux

This section describes three ways on how to configure the certificates in Cisco DCNM.

Note that if you change the keystore password or alias, you need to update it in the **standalone-san.xml** document located at:

`<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\standalone-san.xml`

Update the password in the **keystore** tag and alias in the **key-alias** tag:

```
<keystore key-password>="fmserver_1_2_3 key-alias="updated-key-alias"
keystore-password="updated-password"
path="<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks">
```

This section contains the following topics:

Enabling SSL/HTTPS on Cisco DCNM in Federation on RHEL or Windows

To enable SSL/HTTPS on RHEL or Windows for Cisco DCNM in Federation, 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, perform one of the following:

- While executing the installer, choose HTTPS upfront and select to run in the HTTPs mode.
- While silent installation, choose HTTPs while you execute the installer.

Using a Self-Signed SSL Certificate

Procedure

Step 1 Stop the DCNM services.

Step 2 Rename the keystore located at

`<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks`

to

`<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks.old`

Step 3 From command prompt, navigate to .`<DCNM install root>\dcm\java\jdk11\bin\`

Step 4 Generate a self signed certificate using following command:

keytool -genkey -trustcacerts -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore <DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks -storepass fmserver_1_2_3 -validity 360 -keysize 2048

Step 5 Start the DCNM services.

Using an SSL Certificate when certificate request is generated using Keytool on Windows

Procedure

Step 1 Stop the DCNM services.

Step 2 Rename the keystore located at

`<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks`

to

`<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks.old`

Step 3 From command prompt, navigate to .`<DCNM install root>\dcm\java\jdk11\bin\`

Step 4 Generate the public-private key pair in DCNM keystore by using the following command:

keytool -genkey -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore "<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3 -validity 360 -keysize 2048

Step 5 Generate the certificate-signing request (CSR) from the public key generated in Step 4, on page 109.

keytool -certreq -alias sme -file dcnm.csr -keystore "<DCNM install root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3

Note The `dcnm.csr` file is created in the keytool directory, located at `/usr/local/cisco/dcm/java/jdk11/bin`.

Step 6 Submit the CSR to CA, and download the signed certificate chain in Base-64 format which creates the .p7b file.

CA may provide the certificate and signing certificate as certificate chain in PKCS 7 format (.p7b file) or PEM (.pem) file. If CA provided PKCS 7 format go to Step 7, on page 110 to convert it to PEM format. If CA provided PEM format, then go to Step 8, on page 110.

Step 7 Convert the PKCS 7 certificate chain to X509 certificate chain using openssl.

openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem

Note Ensure that the user provides either absolute or relative path to the correct location of `cert-chain.p7b` file in the above command.

Step 8 Import the intermediate certificate first, then the root certificate, and finally the signed certificate by following these steps:

keytool -importcert -trustcacerts -file cert-chain.pem -keystore "<DCNM_install_root>\dcm\wildfly-14.0.1.Final\standalone\configuration\fmserver.jks" -storepass fmserver_1_2_3 -alias sme

Note Ensure that the user provides either the absolute path or relative path to the correct location of the `cert-chain.pem` file in the above command.

Step 9 Start the DCNM service.

Step 10 To enable launching of SAN Client, copy the **fmtrust.jks** on server1 located at **/usr/local/cisco/dcm/fm/lib/fm/fmtrust.jks** to both second and third servers in the Federation setup.

For further instructions, refer to Launching SAN Client and Device Manager, on page 73.

Using an SSL Certificate When Certificate Request Is Generated Using Keytool on Linux

Procedure

Step 1 Stop the DCNM services, or the DCNM application by using the **appmgr stop dcnm** command.

Step 2 Rename the keystore that is located at:

`<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks`

To

`<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks.old`

Step 3 From command prompt, navigate to the appropriate folder:

`<DCNM install root>/dcm/java/jdk11/bin/`

Step 4 Generate the public-private key pair in DCNM keystore by using the following command:

./keytool -genkey -keyalg RSA -sigalg SHA256withRSA -alias sme -keystore <DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks -storepass fmserver_1_2_3 -validity 360 -keysize 2048

Step 5 Generate the certificate-signing request (CSR) from the public key that is generated in Step 4, on page 110.

./keytool -certreq -alias sme -file dcnm.csr -keystore "<DCNM install root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks" -storepass fmserver_1_2_3

Note The dcnm.csr file is created in the keytool directory, which is located at `/usr/local/cisco/dcm/java/jdk11/bin`.

Step 6 Submit the CSR to CA, and download the signed certificate chain in Base-64 format which creates the `.p7b` file.

CA may provide the certificate and signing certificate as a certificate chain in PKCS 7 format (.p7b file) or PEM (.pem) file. If CA provided the certificate chain in PKCS 7 format, go to Step 7, on page 111 to convert it to PEM format. If CA provided the certificate chain in PEM format, then go to Step 8, on page 111.

Step 7 Convert the PKCS 7 certificate chain to the X509 certificate chain using OpenSSL.

openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem

Note Ensure that the user provides either absolute or relative path to the correct location of cert-`chain.p7b` file in the above command.

Step 8 Import the intermediate certificate first, then the root certificate, and finally the signed certificate by following these steps:

./keytool -importcert -trustcacerts -file cert-chain.pem -keystore <DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks -storepass fmserver_1_2_3 -alias sme

Note Ensure that the user provides either the absolute path or relative path to the correct location of the `cert-chain.pem` file in the above command.

Step 9 Start the DCNM service.

Using a SSL Certificate when certificate request is generated using OpenSSL on Linux

To configure SSL certificates in Cisco DCNM, using certificate request generated using open SSL, perform the following steps.

Procedure

Step 1 Stop the DCNM services, or the DCNM application by using the **appmgr stop dcnm** command.

Step 2 Rename the keystore located at:

`<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks`

to

`<DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks.old`

Step 3 From command prompt, navigate to `<DCNM install root>/dcm/java/jdk11/bin/`.

Step 4 Generate the RSA private key using OpenSSL.

openssl genrsa -out dcnm.key 2048

Step 5 Generate a certificate-signing request (CSR) by using following command:

openssl req -new -key dcnm.key –sha256 -out dcnm.csr

Step 6 Submit the CSR to Certificate signing authority, and download the signed certificate chain in Base-64 format which creates the **.p7b** file.

CA may provide the certificate and signing certificate as certificate chain in PKCS 7 format (.p7b file) or PEM (.pem) file. If CA provids the PKCS 7 format, go to Step 7, on page 112 to convert it to PEM format. If CA provides the PEM format, go to Step 8, on page 112.

Step 7 Convert the PKCS 7 certificate chain to X509 certificate chain.

openssl pkcs7 -print_certs -in cert-chain.p7b -out cert-chain.pem

Step 8 Convert the X509 certificate chain and private key to PKCS 12 format

openssl pkcs12 -export -in cert-chain.pem -inkey dcnm.key -out dcnm.p12 -password pass fmserver_1_2_3 -name sme

Note Ensure that the user provides either absolute path or relative path to the correct location of dcnm.key & `dcnm.p12` files in the above command.

Step 9 Import the intermediate certificate, the root certificate, and the signed certificate in the same order.

./keytool -importkeystore -srckeystore dcnm.p12 -srcstoretype PKCS12 -destkeystore <DCNM_install_root>/dcm/wildfly-14.0.1.Final/standalone/configuration/fmserver.jks -deststoretype JKS -alias sme

Note Ensure that the user provides either absolute path or relative path to the correct location of `cert-chain.pem`, `dcnm.key`, and `dcnm.p12` files in the above command.

Step 10 Start the DCNM service.

Step 11 To enable launching of SAN Client, copy the **fmtrust.jks** on server1 located at **/usr/local/cisco/dcm/fm/lib/fm/fmtrust.jks** to both second and third servers in the Federation setup.

For further instructions, refer to Launching SAN Client and Device Manager, on page 73.

Certificate Management for SAN OVA/ISO

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.

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.
- 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#
```

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 */
```

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.

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 11.3(1), perform the following:

Procedure

Step 1 **Note** When you upgrade to Release 11.3(1), 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 11.3(1), 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.

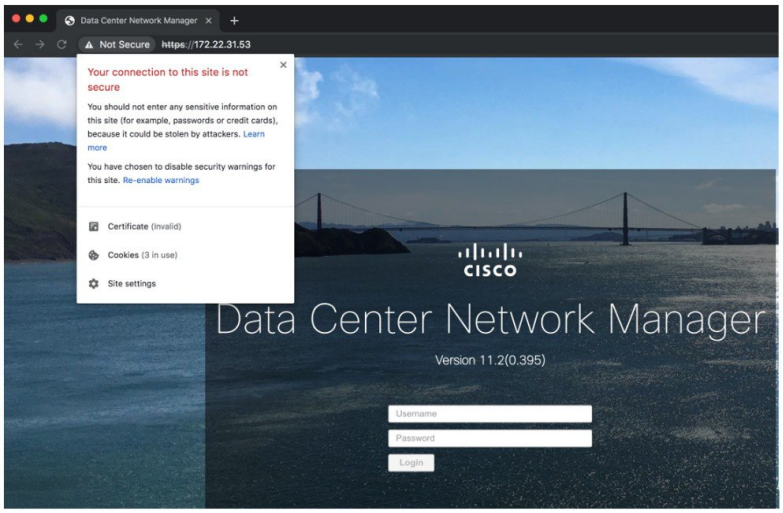
The following snippet is a sample from the Chrome Browser, Version 74.0.3729.169, to verify the certificate.

1. Enter URL **https://<dcnm-ip-address>** or **https://<FQDN>** in the address bar on the browser.

   Press the **Return** key.

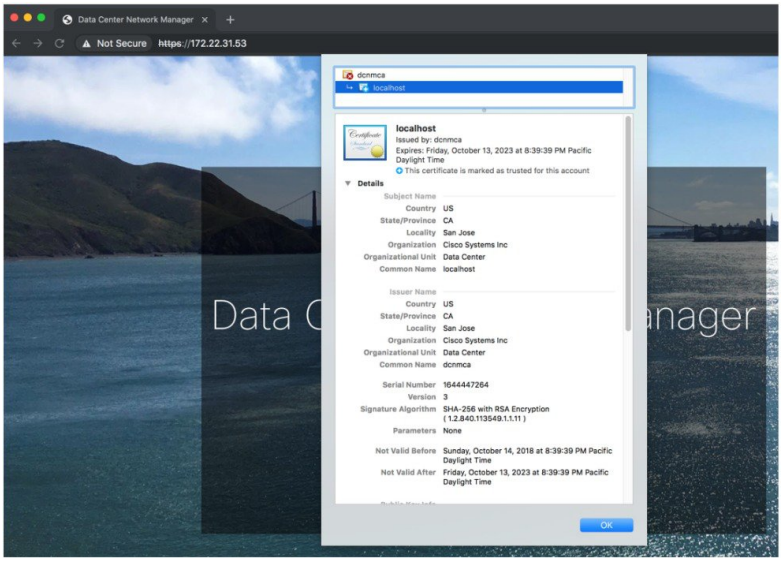
2. Based on the type of certificate, the icon on the left of the URL field shows a lock icon [ ] or an alert icon [ ].

   Click on the icon.

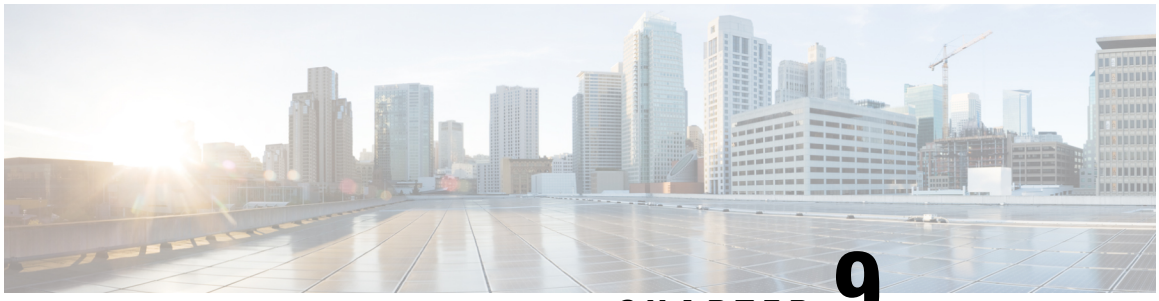


3. On the card, click **Certificate** field.

   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 9

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 7: Cisco DCNM Utility Services

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

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

This chapter contains the following sections:

- Editing Network Properties Post DCNM Installation, on page 121
- Utility Services Details, on page 136
- Managing Applications and Utility Services , on page 137
- Updating the SFTP Server Address for IPv6, on page 140

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.

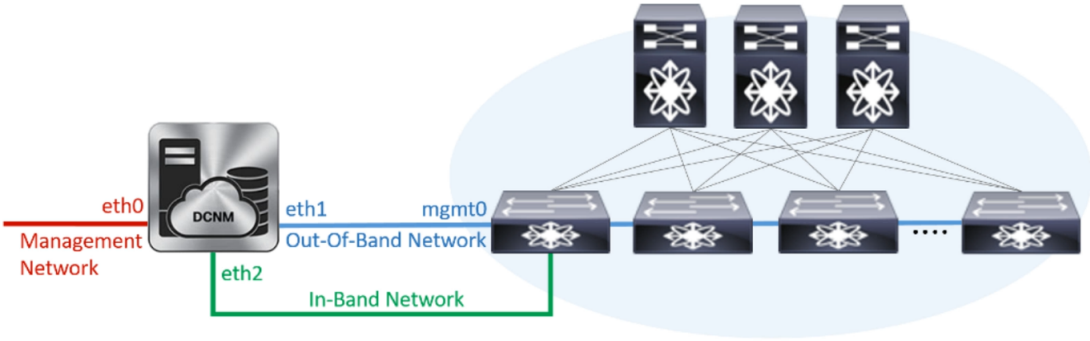
- enhanced-fabric-mgmt (eth1) interface

  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 122

  Sample Command Output for Modifying Network Parameters in the Cisco DCNM Standalone Setup, on page 123

- Modifying Network Properties on DCNM in Native HA Mode, on page 124

  Sample Command Output for Modifying Network Parameters in the Cisco DCNM Native HA Setup, on page 125

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 nex
9. Start all the applications on the Standby node by using the following command:

   appmgr start all
10. Establish peer trust key on the Active node by using the following command:

    appmgr update ssh-peer-trust
11. Establish peer trust key on the Standby node by using the following command:

    appmgr update ssh-peer-trust

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

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

Note For example, let us indicate Active and Standby appliances as **dcnm1** and **dcnm2** respectively.

```
[root@dcnm2]# appmgr stop all
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.

Stopping and halting node rabbit@dcnm2 ...
Note: Forwarding request to 'systemctl enable rabbitmq-server.service'.
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
[root@dcnm2]#

[root@dcnm1]# appmgr stop all
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.

Stopping and halting node rabbit@dcnm1 ...
Note: Forwarding request to 'systemctl enable rabbitmq-server.service'.
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
[root@dcnm1]#

[root@dcnm1]# appmgr update network-properties session start
[root@dcnm2]# appmgr update network-properties session start

[root@dcnm1]# appmgr update network-properties set ipv4 eth0 172.28.10.244 255.255.255.0
172.28.10.1
[root@dcnm1]# appmgr update network-properties set ipv4 eth1 100.0.0.244 255.0.0.0
**************************************************************
 WARNING: fabric/poap configuration may need to be changed
 manually after changes are applied.
**************************************************************
[root@dcnm1]# appmgr update network-properties set ipv4 vip0 172.28.10.238 255.255.255.0
[root@dcnm1]# appmgr update network-properties set ipv4 vip1 100.0.0.238 255.0.0.0
[root@dcnm1]# appmgr update network-properties set ipv4 peer0 172.28.10.245
[root@dcnm1]# appmgr update network-properties set ipv4 peer1 100.0.0.245
[root@dcnm1]# appmgr update network-properties session show changes

[root@dcnm2]# appmgr update network-properties set ipv4 eth0 172.28.10.245 255.255.255.0
172.28.10.1
[root@dcnm2]# appmgr update network-properties set ipv4 eth1 100.0.0.245 255.0.0.0
**************************************************************
 WARNING: fabric/poap configuration may need to be changed
 manually after changes are applied.
**************************************************************
[root@dcnm2]# appmgr update network-properties set ipv4 vip0 172.28.10.238 255.255.255.0
[root@dcnm2]# appmgr update network-properties set ipv4 vip1 100.0.0.238 255.0.0.0
[root@dcnm2]# appmgr update network-properties set ipv4 peer0 172.28.10.244
[root@dcnm2]# appmgr update network-properties set ipv4 peer1 100.0.0.244
[root@dcnm2]# appmgr update network-properties session show changes
```

```
[root@dcnm1]# appmgr update network-properties session show changes
eth0 IPv4 addr  172.28.10.246/255.255.255.0  ->  172.28.10.244/255.255.255.0
eth1 IPv4 addr  1.0.0.246/255.0.0.0          ->  100.0.0.244/255.0.0.0
eth0 VIP        172.28.10.248/24             ->  172.28.10.238/24
eth1 VIP        1.0.0.248/8                  ->  100.0.0.238/8
Peer eth0 IP    172.28.10.247                ->  172.28.10.245
Peer eth1 IP    1.0.0.245                    ->  100.0.0.245

[root@dcnm1]# appmgr update network-properties session show config
======= Current configuration ======
NTP Server      1.ntp.esl.cisco.com
eth0 IPv4 addr  172.28.10.246/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 DNS        171.70.168.183
eth0 IPv6 addr  2001:420:284:2004:4:112:210:20/112
eth0 IPv6 GW    2001:420:284:2004:4:112:210:1
eth1 IPv4 addr  1.0.0.246/255.0.0.0
eth1 IPv4 GW
eth1 DNS        1.0.0.246
eth1 IPv6 addr
eth2 IPv4 addr  /
eth2 IPv4 GW
Peer eth0 IP    172.28.10.247
Peer eth1 IP    1.0.0.247
Peer eth2 IP
eth0 VIP        172.28.10.248/24
eth1 VIP        1.0.0.248/8
eth2 VIP        /
eth0 VIPv6      /
eth1 VIPv6      /

====== Session configuration ======
NTP Server      1.ntp.esl.cisco.com
eth0 IPv4 addr  172.28.10.244/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 DNS        171.70.168.183
eth0 IPv6 addr  2001:420:284:2004:4:112:210:20/112
eth0 IPv6 GW    2001:420:284:2004:4:112:210:1
eth1 IPv4 addr  100.0.0.244/255.0.0.0
eth1 IPv4 GW
eth1 DNS        1.0.0.246
eth1 IPv6 addr
eth2 IPv4 addr  /
eth2 IPv4 GW
Peer eth0 IP    172.28.10.245
Peer eth1 IP    100.0.0.245
Peer eth2 IP
eth0 VIP        172.28.10.238/24
eth1 VIP        100.0.0.238/8
eth2 VIP        /
eth0 VIPv6      /
eth1 VIPv6      /
[root@dcnm1]#

[root@dcnm2]# appmgr update network-properties session show config
======= Current configuration ======
NTP Server      1.ntp.esl.cisco.com
eth0 IPv4 addr  172.28.10.247/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 DNS        171.70.168.183
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr  1.0.0.247/255.0.0.0
```

```
eth1 IPv4 GW
eth1 DNS        1.0.0.247
eth1 IPv6 addr
eth2 IPv4 addr  /
eth2 IPv4 GW
Peer eth0 IP    172.28.10.246
Peer eth1 IP    1.0.0.246
Peer eth2 IP
eth0 VIP        172.28.10.248/24
eth1 VIP        1.0.0.248/8
eth2 VIP        /
eth0 VIPv6      /
eth1 VIPv6      /

====== Session configuration ======
NTP Server      1.ntp.esl.cisco.com
eth0 IPv4 addr  172.28.10.245/255.255.255.0
eth0 IPv4 GW    172.28.10.1
eth0 DNS        171.70.168.183
eth0 IPv6 addr
eth0 IPv6 GW
eth1 IPv4 addr  100.0.0.245/255.0.0.0
eth1 IPv4 GW
eth1 DNS        1.0.0.247
eth1 IPv6 addr
eth2 IPv4 addr  /
eth2 IPv4 GW
Peer eth0 IP    172.28.10.244
Peer eth1 IP    100.0.0.244
Peer eth2 IP
eth0 VIP        172.28.10.238/24
eth1 VIP        100.0.0.238/8
eth2 VIP        /
eth0 VIPv6      /
eth1 VIPv6      /
[root@dcnm2]#

[root@dcnm1]# appmgr update network-properties session apply
*********************************************************************
                          WARNING

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

            PLEASE STOP ALL APPLICATIONS MANUALLY
*********************************************************************

Have applications been stopped? [y/n]: y
Applying changes
DELETE 1
Node left the swarm.
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
log4j:WARN No appenders could be found for logger (fms.db).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
UPDATE 1
UPDATE 1
DELETE 1
server signaled
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the
 'tentative' state
INFO      : [ipv6_wait_tentative] Waiting for interface eth0 IPv6 address(es) to leave the
 'tentative' state
*********************************************************************
```

```
Please run 'appmgr start afw; appmgr start all' to restart your nodes.
********************************************************************************
********************************************************************
Please run 'appmgr update ssh-peer-trust' on the peer node.
********************************************************************
[root@dcnm1]#

[root@dcnm2]# appmgr update network-properties session apply
********************************************************************
                          WARNING

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

            PLEASE STOP ALL APPLICATIONS MANUALLY
********************************************************************

Have applications been stopped? [y/n]: y
Applying changes
DELETE 1
Node left the swarm.
Server configuration file loaded: /usr/local/cisco/dcm/fm//conf/server.properties
log4j:WARN No appenders could be found for logger (fms.db).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
UPDATE 1
UPDATE 1
DELETE 1
afwnetplugin:0.1
server signaled
********************************************************************
Please run 'appmgr start afw; appmgr start all' to restart your nodes.
********************************************************************************
********************************************************************
Please run 'appmgr update ssh-peer-trust' on the peer node.
********************************************************************
[root@dcnm2]#

[root@dcnm1]# appmgr start afw; appmgr start all
Started AFW Server Processes
Started AFW Agent Processes
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO:  Resource is stopped
Done.

Warning: PID file not written; -detached was passed.
AMQP User Check
Started AFW Server Processes
Started AFW Agent Processes
[root@dcnm1]#
```

Wait until dcnm1 becomes active again.

```
[root@dcnm2]# appmgr start afw; appmgr start all
Started AFW Server Processes
Started AFW Agent Processes
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO:  Resource is stopped
```

```
Done.

Warning: PID file not written; -detached was passed.
AMQP User Check
Started AFW Server Processes
Started AFW Agent Processes
[root@dcnm2]#

[root@dcnm1]# appmgr update ssh-peer-trust
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -o 'StrictHostKeyChecking=no' '172.28.10.245'"
and check to make sure that only the key(s) you wanted were added.
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -o 'StrictHostKeyChecking=no' '100.0.0.245'"
and check to make sure that only the key(s) you wanted were added.
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1
Now try logging into the machine, with:   "ssh -o 'StrictHostKeyChecking=no'
'dcnm-247.cisco.com'"
and check to make sure that only the key(s) you wanted were added.
[root@dcnm1]#

[root@dcnm2]# appmgr update ssh-peer-trust
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -o 'StrictHostKeyChecking=no' '172.28.10.244'"
and check to make sure that only the key(s) you wanted were added.
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -o 'StrictHostKeyChecking=no' '100.0.0.244'"
and check to make sure that only the key(s) you wanted were added.
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
Number of key(s) added: 1

Now try logging into the machine, with:   "ssh -o 'StrictHostKeyChecking=no'
'dcnm-246.cisco.com'"
and check to make sure that only the key(s) you wanted were added.
[root@dcnm2]#
```

Configuring Enhanced-Fabric-Inband Interface (eth2) Post DCNM Installation

During the DCNM installation, you can configure the In-Band Management interface. You must associate this network with the port group that corresponds to a fabric in-band connection. The In-Band Network provides reachability to the devices via the front-panel ports.

Note If you need to modify the already configured in-band network (eth2 interface), execute the **ifconfig eth2 0.0.0.0** command and run the **appmgr setup inband** command again.

Note You cannot use Endpoint Locator and Telemetry features if the eth2 interface is not configured.

To configure the eth2 interface for the in-band management network, use the **appmgr setup inband** command.

The following example shows a sample output for the **appmgr setup inband** command for a Cisco DCNM Standalone Appliance.

```
[root@dcnm]# appmgr setup inband
Configuring Interface for InBand Connectivity...
Please enter the information as prompted:
InBand Physical IP [e.g. 2.2.2.69]: 2.0.0.250
InBand Network Mask [e.g. 255.255.255.0]: 255.0.0.0
InBand Gateway [e.g. 2.2.2.1]: 2.0.0.1
Validating Inputs ...

You have entered these values..
PIP=2.0.0.250
NETMASK=255.0.0.0
GATEWAY=2.0.0.1

Press 'y' to continue configuration, 'n' to discontinue [y] y
{"ResponseType":0,"Response":"Refreshed"}
{"ResponseType":0,"Response":{"AfwServerEnabled":true,"AfwServerReady":true,"InbandSubnet":"2.0.0.0/8",
"InbandGateway":"2.0.0.1","OutbandSubnet":"0.0.0.0/8","OutbandGateway":"0.0.0.0","UnclusteredMode":true}}

Done.
[root@dcnm]#
```

The following example shows a sample output for the **appmgr setup inband** command for a Cisco DCNM Native HA Appliance.

On Cisco DCNM Primary appliance:

```
[root@dcnm-primary]# appmgr setup inband
Configuring Interface for InBand Connectivity...
Please enter the information as prompted:
InBand Physical IP [e.g. 2.2.2.69]: 2.0.0.244
InBand Network Mask [e.g. 255.255.255.0]: 255.0.0.0
InBand Gateway [e.g. 2.2.2.1]: 2.0.0.1
InBand Virtual IP for HA setup [e.g. 2.2.2.60]: 2.0.0.243
InBand Virtual Network Mask [mandatory for HA setup] [e.g. 255.255.255.0]: 255.0.0.0
Peer Inband IP [mandatory for HA setup] [e.g. 2.2.2.59]: 2.0.0.244
Validating Inputs ...

You have entered these values..
PIP=2.0.0.244
NETMASK=255.0.0.0
GATEWAY=2.0.0.1
VIP=2.0.0.243
VIP_NETMASK=255.0.0.0
PEER_ETH2=2.0.0.244

Press 'y' to continue configuration, 'n' to discontinue [y] y

Done.
[root@dcnm-primary]#
```

On Cisco DCNM Secondary appliance:

```
[root@dcnm-secondary]# appmgr setup inband
Configuring Interface for InBand Connectivity...
Please enter the information as prompted:
InBand Physical IP [e.g. 2.2.2.69]: 2.0.0.245
InBand Network Mask [e.g. 255.255.255.0]: 255.0.0.0
InBand Gateway [e.g. 2.2.2.1]: 2.0.0.1
InBand Virtual IP for HA setup [e.g. 2.2.2.60]: 2.0.0.243
InBand Virtual Network Mask [mandatory for HA setup] [e.g. 255.255.255.0]: 255.0.0.0
Peer Inband IP [mandatory for HA setup] [e.g. 2.2.2.59]: 2.0.0.244
Validating Inputs ...

You have entered these values..
PIP=2.0.0.245
NETMASK=255.0.0.0
GATEWAY=2.0.0.1
VIP=2.0.0.243
VIP_NETMASK=255.0.0.0
PEER_ETH2=2.0.0.244

Press 'y' to continue configuration, 'n' to discontinue [y] y
HA Role is Active {"ResponseType":0,"Response":"Refreshed"}
Done.

[root@dcnm-secondary]#
```

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#
```

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
```

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.

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

- Repositories

  The TFTP server hosts boot scripts that are used for POAP.

  The SCP server downloads the database files, configuration files, and the software images.

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

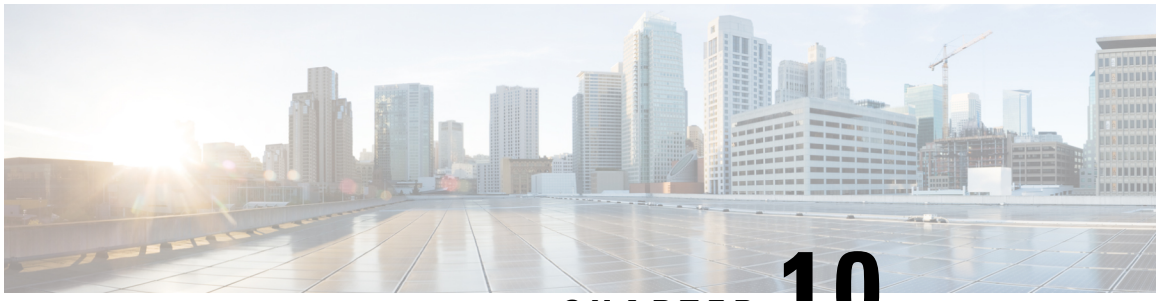
After deploying the DCNM OVA/ISO successfully with EFM IPv4 and IPv6, by default the SFTP address is pointed to IPv4 only. You need to change the IPv6 address manually in the following two places:

- 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 10

Installing Software Maintenance Update for log4j2 Vulnerability

- Installing Software Maintenance Update on Cisco DCNM Windows and Linux Deployment, on page 141
- Installing Software Maintenance Update on Cisco DCNM OVA/ISO Deployment, on page 144

Installing Software Maintenance Update on Cisco DCNM Windows and Linux Deployment

This section provides instructions to install Software Maintenance Update (SMU) on Cisco Windows and Linux deployments Release 11.3(1) 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.

Note Only a **root** or **admin** user can install the SMU on the Cisco DCNM setup.

This section contains the following topics:

Installing the SMU on Cisco DCNM Windows Appliance

To install the SMU on Cisco DCNM Windows appliance, perform the following:

Before you begin

- Take a backup of the Cisco DCNM application. 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 11.3(1) is up and running.

Note Only a **root** user can install the SMU on the Cisco DCNM Release 11.3(1) 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 11.3(1).

c) Locate **DCNM 11.3(1) Maintenance Update for Windows and Linux Servers to address CVE-2021-45046 and CVE-2021-44228** and click Download icon.

Save the `dcnm-win-linux-patch.11.3.1.zip` file to your directory that is easy to find when you start to apply the maintenance update (patch).

Step 2 Upload the file to the **`C:\Users\<UserName>\Desktop\`** folder in the DCNM setup.

Step 3 Log on to Cisco DCNM using SSH as a **Administrator** user.

Step 4 Unzip the **`dcnm-win-linux-patch.11.3.1.zip`** file in **`c:\Users\<UserName>\Desktop\`** directory.

Step 5 Open **Command prompt** and run as **Administrator**.

Step 6 Change directory to **`/patch`** using **c:\Users\<UserName>\Desktop\patch** command.

Step 7 Apply the patch.

```
c:\Users\<UserName>\Desktop\patch> patch.bat
Enter DCNM root directory [C:\Program Files\Cisco Systems\dcm]:
c:\Users\<UserName>\Desktop\patch

"Backing up dcm.ear ..."
        1 file(s) copied.
        1 file(s) copied.

"Stopping DCNM service..."
The Cisco DCNM SAN Server service was stopped successfully.

Waiting for  0 seconds, press CTRL+C to quit ...

"Applying patch...."
Initializing, please wait...
Patching DCNM server, please wait...

"Stopping Elasticsearch...."
The Elasticsearch 6.8.3 (elasticsearch-service-x64-683) service is stopping..
The Elasticsearch 6.8.3 (elasticsearch-service-x64-683) service was stopped successfully.

Waiting for  0 seconds, press CTRL+C to quit ...
        1 file(s) copied.
        1 file(s) copied.
        1 file(s) copied.

"Starting Elasticsearch...."
The Elasticsearch 6.8.3 (elasticsearch-service-x64-683) service is starting..
```

```
The Elasticsearch 6.8.3 (elasticsearch-service-x64-683) service was started successfully.

Waiting for  0 seconds, press CTRL+C to quit ...

"Starting DCNM server..."
The Cisco DCNM SAN Server service is starting.
The Cisco DCNM SAN Server service was started successfully.
```

Installing the SMU on Cisco DCNM Linux Appliance

To install the SMU on Cisco DCNM Linux appliance, perform the following:

Before you begin

- Take a backup of the Cisco DCNM application. 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 11.3(1) is up and running.

Note Only a **root** user can install the SMU on the Cisco DCNM Release 11.3(1) 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 11.3(1).

c) Locate **DCNM 11.3(1) Maintenance Update for Windows and Linux Servers to address CVE-2021-45046 and CVE-2021-44228** and click Download icon.

Save the `dcnm-win-linux-patch.11.3.1.zip` file to your directory that is easy to find when you start to apply the maintenance update (patch).

Step 2 Upload the file to the **`/root/`** folder in the DCNM setup.

Step 3 Log on to Cisco DCNM using SSH as a **root** user.

Step 4 Unzip the **`dcnm-win-linux-patch.11.3.1.zip`** file in **`/root/`** directory.

Step 5 Change directory to **`/patch`**.

```
[root@dcnm]# cd patch
```

Step 6 Apply the patch.

```
[root@dcnm]# ./patch.sh
Please enter DCNM install directory.  Press Enter to select default.
[Default:/usr/local/cisco/dcm]:
DCNM Home Dir: /usr/local/cisco/dcm
Backing up dcm.ear and SanAnalytics.war...
Stopping DCNM service...
Stopping FMServer (via systemctl):   [  OK  ]
Applying patch....
Patching ear file, please wait...
Patching war file, please wait...
Stopping Elasticsearch...
Stopping elasticsearch (via systemctl):    [  OK  ]
Starting Elasticsearch...
Starting elasticsearch (via systemctl):    [  OK  ]
Starting DCNM server...
Starting FMServer (via systemctl):     [  OK  ]
```

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 11.3(1).

This section contains the following topics:

Installing SMU on Cisco DCNM 11.3(1) 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 11.3(1) is up and running.

Note Only a **root** user can install the SMU on the Cisco DCNM Release 11.3(1) 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 11.3(1).

c) Locate **DCNM 11.3.1 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.11.3.1-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.11.3.1-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 11.3(1) SMU file in the `/mnt/iso` folder.

```
[root@dcnm]# mount -o loop dcnm-va-patch.11.3.1-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.11.3.1-p1.iso** file from the DCNM setup.

Note You must terminate the **screen** session before unmounting the SMU file.

```
[root@dcnm]# umount /mnt/iso
```

Sample Output of Commands to address Log4j vulnerability

The following is a sample output while installing the SMU on Cisco DCNM Release 11.3(1).

Sample Output to Install SMU in DCNM Standalone Deployment

```
[root@dcnm]# ./inline-upgrade.sh

================================================================
============ Inline Upgrade to DCNM 11.3(1)-p1 =============
================================================================

Upgrading from version: 11.3(1)
Upgrading from install option: LAN Fabric
System type: Standalone
Compute only: No

Do you want to continue and perform the inline upgrade to 11.3(1)-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 ====
********************************************************************************
```

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/deployment8b48c896c390adc/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/deployment8b48c896c390adc/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.

Refer to Upgrading DCNM Release 11.3(1) from Previous Versions, on page 155 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 154.

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

To validate that the patch has been successfully applied on Cisco DCNM appliances, 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 11.3(1) from Previous Versions

When upgrading from an older DCNM 11.x version to 11.3(1) 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.

```
./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:

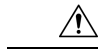
```
docker info | grep overlay2
Storage Driver: overlay2              /* above command must display this output*/
```

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.