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

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

Cisco DCNM includes these management applications:

Cisco DCNM Web UI

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

Performance Manager

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

Installation Options

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

DCNM Open Virtual Appliance (OVA) Installer

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

DCNM ISO Virtual Appliance (ISO) Installer

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

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

Deployment Options

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

Supported Latency

The supported latency for Cisco DCNM Media Controller deployment is defined below:

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

Standalone Server

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

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

High Availability for Virtual Appliances

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

root and sysadmin User Privileges

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

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

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

Upgrading to Cisco DCNM Release 11.5(4)

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

The following table summarizes the type of upgrade that you must follow to upgrade to Release 11.5(4).

Table 1: Type of Upgrade for IP for Media (IPFM) deployments

Current Release Number	Upgrade type to upgrade to Release 11.5(4)
11.5(3)	This release does not support IP for Media (IPFM) deployments.
11.5(2)	This release does not support IP for Media (IPFM) deployments.
11.5(1)	Inline Upgrade

System Requirements

This section describes the various system requirements for proper functioning of your Cisco DCNM Release 11.5(4).

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

Java Requirements

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

```
DCNM_root_directory/java/jdk11
```

Server Requirements

Cisco DCNM Release 11.5(4), supports the Cisco DCNM server on these 64-bit operating systems:

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

Supported Latency

The supported latency for Cisco DCNM deployment is defined below:

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

    (supported with LAN Fabric deployment only)

Database Requirements

Cisco DCNM Release 11.5(4) supports the following databases:

• PostgreSQL 10.19 - For OVA/ISO deployments

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

Hypervisors

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

Server	Product ID (PID)	Recommended minimum memory, drive capacity, and CPU count
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

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

Server Resource (CPU/Memory) Requirements

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

Table 2: System Requirements for Cisco DCNM IPFM Deployment

Deployment Type	Small (Lab or POC)	Large (Production)
OVA/ISO	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB

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

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

VMware Snapshot Support for Cisco DCNM

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

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

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

1. Right-click the virtual machine the inventory and select **Snapshots > Take Snapshot**.

2. In the **Take Snapshot** dialog box, enter a name and description for the snapshot.

3. Click **OK** to save the snapshot.

The following snapshots are available for VMs.

- When VM is powered off.

- When VM is powered on, and active.

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

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

Take Snapshot | **dcnm-va.11.X.1** ✕

Name   VM Snapshot taken powered on 12/8/2019,

Description

☐ Snapshot the virtual machine's memory

☐ Quiesce guest file system (Needs VMware Tools installed)

CANCEL   OK

You can restore VM to the state in a Snapshot.

Manage Snapshots | dcnm1111   ✕

∨ 🗄 dcnm1111
   ∨ 📷 VM Snapshot 12%252f12%252f2019, 11:56:07 AM
      ∨ 📷 1131 Snapshot 12%252f12%252f2019, 3:04:31 PM
         ∨ 📷 VM Snapshot 12%252f16%252f2019, 6:55:02 ...
            📍 You are here

Name   VM Snapshot
                    12%252f16%252f2019,
                    6:55:02 AM

Created   12/15/2019, 11:55:31 PM

Disk usage   510.03 MB

Snapshot the virtual   No
machine's memory

Quiesce guest file system   No

EDIT

DELETE ALL   DELETE   REVERT TO

DONE

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

Supported Web Browsers

Cisco DCNM supports the following web browsers:

- Google Chrome version: 98.0.4758.109

- Mozilla Firefox version: 97.0.1

- Microsoft Edge version: 98.0.1108.62

Other Supported Software

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

Table 3: Other Supported Software

Component	Features
Security	• ACS versions 4.0, 5.1, 5.5, and 5.8 • ISE version 2.6 • ISE version 3.0 • Telnet Disabled: SSH Version 1, SSH Version 2, Global Enforce SNMP Privacy Encryption. • Web Client Encryption: HTTPS with TLS 1, 1.1 and 1.2 • TLS 1.3
OVA\ISO Installers	CentOS 7.8/Linux Kernel 3.10.x

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

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.