Overview

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

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

This section contains the following sections:

Introduction

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

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.

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, as well as Fibre Channel and IP neighbor devices. Summary or real-time statistics can be charted, printed, or saved 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. Performance Manager stores data into Elastic search time series database. API access to Elastic search is not supported.

Installation Options

Cisco DCNM Software images are packaged with the Cisco DCNM installer, signature certificate, and signature verification script. Unzip the desired Cisco DCNM Installer image zip file to a directory. Image signature can be verified by following the steps in README file. The installer from this package installs the Cisco DCNM software.

DCNM Windows Installer

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

DCNM Linux Installer

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

Deployment Options

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

Standalone Server

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

Standalone with external Oracle

If you have more switches in your setup or if you expect your setup to grow over time, an external Oracle server is recommended. 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 https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/11_0_1/scalability_guide/b_scale_guide_dcnm_11.html.

DCNM Federation

Cisco DCNM federation is the HA mechanism for SAN devices. Groups of SAN devices can be managed by each node in the DCNM federated setup. All the devices can be managed using a single client interface. 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 the Cisco DCNM

Before Cisco DCNM Release 11.0(1), DCNM OVA, and ISO supported SAN functionality. From Cisco DCNM 11.0(1), OVA, and ISO does not ship with SAN support.

The following table summarizes the upgrade options for Cisco DCNM Release .

System Requirements for Cisco DCNM, Release

Server Requirements

Cisco DCNM, Release , 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 and 7.4

Cisco DCNM Release 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 does not support the Oracle 12c pluggable database version installation.

- Oracle 12c RAC (nonpluggable installation)

Note Cisco DCNM for LAN is not supported with an external database.

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

Note The Cisco DCNM database size is not limited, and increases according to the number of nodes and ports that the DCNM manages with Performance Manager Collections enabled. You cannot restrict the database size. If you choose 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 database backups, either daily or weekly, to ensure that all the data is preserved.

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

Server Resource Requirements

Table 1: Server Resource Requirements

Deployment	Deployment Type	Small (Lab or POC)	Large (Production)	Compute
SAN	Windows, Linux (standalone or VM)	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs **Note** Standalone functioning of SAN Insights require 28 vCPUs. RAM: 128 GB RAM(with SAN Insights) or 32 GB (without SAN Insights) DISK: 10 TB Disk (with SAN Insights) or 500 GB (without SAN Insights)	Not Applicable

Note

- The SAN Insights feature is not supported on small deployment.
- You can use the SAN Insights feature on a medium-sized deployment with 2 TB disk space as well.
- Every Federation node must consists of 3 Large configuration nodes.

Client Requirements

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

Table 2: 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:

-
-
-

Other Supported Software

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

Table 3: Other Supported Software

Component	Features
Security	• ACS versions 4.0, 5.1, and 5.5 • Telnet Disabled: SSH Version 1, SSH Version 2, Global Enforce SNMP Privacy Encryption. • Web Client and Cisco DCNM-SAN Server Encryption: HTTPS with TLS 1, 1.1 and 1.2

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.