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 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. Performance Manager stores data into Elastic search time series database. API access to Elastic search isn't 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. 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.

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.

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.

System Requirements for Cisco DCNM

This section describes the various system requirements for proper functioning of your Cisco DCNM, Release 11.2(1).

Java Requirements

The Cisco DCNM Server is distributed with JRE 1.8.0_201 into the following directory:

```
DCNM_root_directory/java/jre1.8
```

Server Requirements

Cisco DCNM, Release 11.2(1), supports the Cisco DCNM Server on these 64-bit operating systems:

- **IP for Media, LAN Fabric, and Classic LAN Deployments:**
  - 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 11.2(1) supports the following databases:

- PostgreSQL 9.4.5

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

Cisco DCNM Release 11.2(1) 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-vCPU Cores with Cisco hardware RAID Controller [UCSC-MRAID12G-1GB/2 GB] for the RAID operation (small)
Cisco UCS C240M4	UCSC-C240-M4L	32G / 500G 16-vCPU Cores with Cisco hardware RAID Controller [UCSC-MRAID12G- GB/2 GB] for the RAID operation (large)
Cisco UCS C240 M5S	UCSC-C240-M5SX	32G / 500G 16-vCPU Cores with Cisco hardware RAID Controller [UCSC-SAS-M5] for the RAID operation (small)
Cisco UCS C220 M5L	UCSC-C220-M5L	32G / 500G 16-vCPU Cores with Cisco hardware RAID Controller [UCSC-SAS-M5] for the RAID operation (small)

[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.

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

Note Only Warm and Cold VMware snapshot is supported.

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

Supported Hypervisors

Cisco DCNM Release 11.2(1) supports the running of the Cisco DCNM Server on the following hypervisors, for DCNM LAN Fabric and DCNM LAN Classic Deployments:

Table 1: VMware Snapshot Support for DCNM LAN Fabric and DCNM LAN Classic Deployments

VMware vSphere Hypervisor (ESXi)	6.0	6.5	6.7	6.7 update 1
VMware vCenter Server	6.0	6.5	6.7	6.7 update 1

Server Resource Requirements

Deployment	Deployment Type	Small (Lab or POC)	Large (Production)	Compute
IP for Media (IPFM)	• OVA • ISO	CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB	Not Applicable

Supported Web Browsers

Cisco DCNM supports the following web browsers:

- Google Chrome Version 74.0.3729.13
- Mozilla Firefox Version 66.0.4 (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 11.2(1).

Table 2: Other Supported Software

Component	Features
Security	• ACS versions 4.0, 5.1, 5.5, and 5.8. • 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

Component	Features
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.