



CHAPTER 1

Overview

Cisco Data Center Network Manager (DCNM) is a management system for the Cisco Unified Fabric. It enables you to provision, monitor, and troubleshoot the data center network infrastructure. It provides visibility and control of the unified data center so that you can optimize for the quality of service (QoS) required to meet service-level agreements.

Cisco Prime DCNM provides a comprehensive feature set that meets the routing, switching, and storage administration needs of data centers. Cisco Prime DCNM streamlines the provisioning for the unified fabric and monitors the SAN and LAN components. Cisco Prime DCNM provides a high level of visibility and control through a single web-based management console for Cisco Nexus, Cisco MDS, and Cisco Unified Computing System (UCS) products.

During the DCNM installation, you can choose install applications related to Unified Fabric only for Unified Fabric-mode installations. Cisco Prime DCNM also includes Cisco Prime DCNM-SAN and Cisco Prime DCNM-LAN client functionality.

All Cisco Prime DCNM for SAN and Cisco Prime DCNM for LAN product documentation is now published to the Data Center Network Manager listing page at the location:

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_configure.html

This chapters contains the following:

- [Introduction of Cisco Prime DCNM, page 1-1](#)
- [Unified Fabric and non-Unified Fabric, page 1-4](#)
- [Installation Options, page 1-5](#)
- [Deployment Options, page 1-5](#)

Introduction of Cisco Prime DCNM

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

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

Cisco Prime DCNM-SAN includes these management applications:

- [Cisco Prime DCNM Server, page 1-2](#)
- [Cisco Prime DCNM Web Client, page 1-2](#)

- [Cisco Prime DCNM-LAN Client, page 1-2](#)
- [Cisco Prime DCNM-LAN Server, page 1-2](#)
- [Cisco Prime DCNM-SAN Client, page 1-3](#)
- [Device Manager, page 1-3](#)
- [Performance Manager, page 1-4](#)

Cisco Prime DCNM Server

The Cisco Prime DCNM-SAN Server component must be started before running Cisco Prime DCNM-SAN. On a Windows PC, Cisco Prime DCNM-SAN Server is installed as a service. This service can then be administered using the Windows Services in the control panel. Cisco Prime 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 Prime DCNM Web Client

The Cisco Prime DCNM Web Client 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 Prime DCNM web client.

Cisco Prime DCNM-LAN Client

The Cisco Prime DCNM-LAN Client displays a map of discovered Ethernet Networks including the Cisco Nexus 9000 Series, Cisco Nexus 7000 Series, Cisco Nexus 5000 Series, Cisco Nexus 4000 Series, Cisco Nexus 3000 Series, Cisco Nexus 2000 Series, and Cisco Nexus 1000 Series switches and the Catalyst 6500 Series switches. The Cisco Prime DCNM-LAN client provides provisioning, monitoring of Ethernet interfaces for the Ethernet switches. It allows you to configure complex features such as vPC, VDC, and FabricPath and provides the topology representation of vPC, port channel, VLAN mappings, and FabricPath.

Cisco Prime DCNM-LAN Server

This section describes the Cisco Data Center Network Manager for LAN (DCNM-LAN) servers.

- [Secure Client Communications, page 1-2](#)
- [SMTP Servers, page 1-3](#)

Secure Client Communications

This section describes how to configure Cisco Data Center Network Manager for LAN (DCNM-LAN) for secure client-server communications.

**Note**

Use the HTTPs option for secured communication between the server and client.

This section includes the following topics:

- [Encrypted Client-Server Communications, page 1-3](#)
- [Firewall Support for Client-Server Communications, page 1-3](#)

Encrypted Client-Server Communications

By default, communication between the Cisco Prime DCNM-LAN client and server is unencrypted; however, you can enable secure client-server communications, which uses Transport Layer Security (TLS), a protocol based on the Secure Sockets Layer (SSL) 3.0 protocol. In particular, communications between the Cisco Prime DCNM-LAN client and the EJB port on the Cisco Prime DCNM-LAN server are encrypted when you enable secure client communications.

Enabling secure client communications does not affect how users download, install, and log into the Cisco Prime DCNM-LAN client.

Firewall Support for Client-Server Communications

Cisco Prime DCNM-LAN supports client-server connections across gateway devices such as a firewall; however, you must configure any gateway devices to allow the connections that the client must open to the Cisco Prime DCNM-LAN server.

By default, the secondary server bind port is assigned a random port number when the Cisco Prime DCNM-LAN server starts. To support client-server communications across a gateway device, you must configure the Cisco Prime DCNM-LAN server to use a specific port for the secondary server bind service.

SMTP Servers

The Cisco Prime DCNM-LAN client supports a feature where you can specify rising or falling threshold rules for sample variables in collected statistical data. When one of these thresholds has been crossed, you can specify that an e-mail alert be sent. The Cisco Prime DCNM-LAN server can be configured to send e-mail to an SMTP server.

Cisco Prime DCNM-SAN Client

The Cisco Prime 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 Prime DCNM-SAN Client provides multiple menus for accessing the features of the Cisco Prime DCNM-SAN Server.

Device Manager

From Cisco MDS Release 5.2(1), Cisco Prime 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 detailed 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 with any web browser.

Unified Fabric and non-Unified Fabric

This section details basic overview on Unified Fabric and non-Unified Fabric.

- [Information about Unified Fabric, page 1-4](#)
- [Information about non-Unified Fabric, page 1-4](#)

Information about Unified Fabric

Cisco Unified Fabric boosts network flexibility and efficiency. Unified Fabric innovations simplify fabric management, optimize fabric infrastructure, and automate provisioning across physical and virtual environments.

Unified Fabric offers the following functionalities:

Optimized Fabric Infrastructure for Enhanced Efficiency and Scale

The optimized spine-leaf topology provides enhanced forwarding, distributed control plane, and integrated physical and virtual environments. The topologies enable any network anywhere, supporting transparent mobility for physical servers and virtual machines, including network extensibility. This increases the resiliency with smaller failure domains and multitenant scale.

Simplified Fabric Management with Open APIs for Ease of Operations

Cisco Unified Fabric allows centralized fabric management across both physical servers and virtual machines. It provides automated network provisioning, common point of fabric access, and host, network, and tenant visibility. Open APIs allow better integration with orchestration and automation tools, in addition to cloud platforms.

Automated Provisioning for Greater Agility

With complete mobility across the fabric, the Unified Fabric uses network automation and provisioning to simplify physical server and virtual machine deployments. The network administrator can define profile templates for both physical and virtual machine. When a server administrator provisions virtual machine and physical servers, instances of network policies are automatically created and applied to the network leaf switch. As virtual machines move across the fabric, the network policy is automatically applied to the leaf switch.

Information about non-Unified Fabric

Cisco Prime DCNM in non-Unified Fabric mode provisions and optimizes the overall uptime and reliability of the data center fabric. The following are the significance of Unified Fabric mode:

- centralize fabric management to facilitate resource movement including adding and editing resources

- monitors SAN and LAN, and detects performance degradation
- aids easy diagnosis and troubleshooting of data center outages
- simplifies operational management of virtualized data centers

Installation Options

Cisco Prime DCNM, Release 7.2.x offers four types of installers. The following sections describe the functionalities:

This section includes 4 options

- [DCNM Open Virtual Appliance for VMWare, page 1-5](#)
- [DCNM ISO Virtual Appliance for VMWare/KVM/CSP2100, page 1-5](#)
- [DCNM Installer for Windows \(64-bit\), page 1-5](#)
- [DCNM Installer for Linux \(64-bit\), page 1-5](#)

DCNM Open Virtual Appliance for VMWare

This installer is available as an Open Virtual Appliance file (.ova). The installer contains a pre-installed OS, DCNM and other applications needed for Unified Fabric. This requires a vCenter/ESXi 5.1/5.5 environment. This can be deployed either in Unified Fabric or in non-Unified Fabric modes. By default, it is deployed in Unified Fabric mode.

DCNM ISO Virtual Appliance for VMWare/KVM/CSP2100

This installer is available as an ISO image (.iso). The installer is a bundle of OS, DCNM and other applications needed for Dynamic Fabric Automation. This can be deployed either on VMWare ESXi 5.x environment or as a Kernel-based Virtual Machine on RHEL 6.x. This can be deployed either in Unified Fabric or in non-Unified Fabric modes. By default, it gets deployed in Unified Fabric mode.

DCNM Installer for Windows (64-bit)

This installer is available as an executable (.exe) and does not support Unified Fabric features.

DCNM Installer for Linux (64-bit)

This installer is available as a binary (.bin) and does not support Unified Fabric features.

Deployment Options

The installer available for Cisco Prime DCNM Release 7.2.x can be deployed in one of the below modes.

- [Standalone Server, page 1-6](#)
- [Standalone with external Oracle, page 1-6](#)

- [High Availability for Virtual Appliances, page 1-6](#)

Standalone Server

All types of installers (.ova, .iso, .bin, .exe) are packaged along with PostgreSQL database. This mode is the simplest setup recommended for less than 50 switches. The default installation steps for the respective installers result in this mode of deployment.

Standalone with external Oracle

If you have more than 50 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 as described under section [Oracle Database for DCNM Servers, page 2-19](#).

High Availability for Virtual Appliances

The DCNM Virtual appliances, both OVA and ISO, can be deployed in High Availability mode to have resilience in case of application or OS failures. This requires an external Oracle Database. For more information, see [Managing Applications in a High-Availability Environment](#).