Cisco Data Center Network Manager Fundamentals Guide, Release 10.0(x)

December, 2017

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Cisco Data Center Network Manager Fundamentals Guide, Release 10.0(x)

CONTENTS

Text Part Number:

Preface

This preface describes the audience, organization, and conventions of the *Cisco DCNM Fundamentals Guide*. It also provides information on how to obtain related documentation.

Audience

This guide is for experienced network administrators who are responsible for configuring and maintaining the Nexus family switch and Cisco MDS 9000 Family of multilayer directors and fabric switches.

Organization

This *guide* is organized as follows:

Chapter	Title	Description
Chapter 1	Introduction to Cisco Data Center Network Manager	Provides a brief overview of Cisco DCNM Fundamentals.
Chapter 2	Cisco DCNM User Roles	Provides the information about the user roles of Cisco DCNM.
Chapter 4	Cisco DCNM Web Client	Provides the features of Cisco DCNM Web Client and the major changes in the latest release.
Chapter 6	Cisco DCNM-SAN Overview	Provides a brief overview of Cisco DCNM-SAN.
Chapter 7	Configuring Cisco DCNM-SAN Server	Provides in-depth descriptions of GUI and capabilities of Cisco DCNM-SAN Server.
Chapter 8	Configuring Authentication in Cisco DCNM-SAN	Describes the authentication schemes between Cisco DCNM-SAN components and fabric switches.
Chapter 9	Configuring Cisco DCNM-SAN Client	Provides in-depth descriptions of GUI and capabilities of Cisco DCNM-SAN.
Chapter 10	Device Manager	Provides in-depth descriptions of GUI and capabilities of Device Manager.

Chapter	Title	Description
Chapter 11	Configuring Performance Manager	Provides overview of the Performance Manager architecture.
Chapter 12	Monitoring the Network	Provides details on monitoring the network.
Chapter 13	Monitoring Performance	Provides details on using Performance Manager.

Document Conventions

Command descriptions use these conventions:

boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Screen examples use these conventions:

`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
`< >`	Nonprinting characters, such as passwords, are in angle brackets.
`[ ]`	Default responses to system prompts are in square brackets.
`!, #`	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

In this document, the following shortened names are used:

- Cisco Data Center Network Manager for SAN is also referred to as DCNM-SAN.
- Cisco Data Center Network Manager for LAN is also referred to as DCNM-LAN.

Related Documentation

This section contains information about the documentation available for Cisco DCNM and for the platforms that Cisco DCNM manages.

This section includes the following topics:

Cisco DCNM Documentation

The Cisco DCNM documentation is available at the following URL:

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

The documentation set for Cisco DCNM includes the following documents:

Release Notes

Cisco DCNM Release Notes, Release 10.0.x

Cisco DCNM

The following publications support both Cisco DCNM for LAN and DCNM for SAN, and address the new licensing model, the new installation process, and the new features of Cisco DCNM:

- Cisco DCNM Fundamentals Guide, Release 10.0.x
- Cisco DCNM Installation Guide, Release 10.0.x

Cisco DCNM for SAN Configuration Guides

System Management Configuration Guide, Cisco DCNM for SAN

Interfaces Configuration Guide, Cisco DCNM for SAN

Fabric Configuration Guide, Cisco DCNM for SAN

Quality of Service Configuration Guide, Cisco DCNM for SAN

Security Configuration Guide, Cisco DCNM for SAN

IP Services Configuration Guide, Cisco DCNM for SAN

Intelligent Storage Services Configuration Guide, Cisco DCNM for SAN

High Availability and Redundancy Configuration Guide, Cisco DCNM for SAN

Inter-VSAN Routing Configuration Guide, Cisco DCNM for SAN

SMI-S and Web Services Programming Guide, Cisco DCNM for SAN

Cisco Nexus 1000V Series Switch Documentation

The Cisco Nexus 1000V Series switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Cisco Nexus 2000 Series Fabric Extender Documentation

The Cisco Nexus 2000 Series Fabric Extender documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps10110/tsd_products_support_series_home.html

Cisco Nexus 3000 Series Switch Documentation

The Cisco Nexus 3000 Series switch documentation is available at the followingURL:

http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html

Cisco Nexus 4000 Series Switch Documentation

The Cisco Nexus 4000 Series switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps10596/tsd_products_support_series_home.html

Cisco Nexus 5000 Series Switch Documentation

The Cisco Nexus 5000 Series switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

Cisco Nexus 7000 Series Switch Documentation

The Cisco Nexus 7000 Series switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Additional Related Documentation for Cisco MDS 9000

The documentation set for the Cisco MDS 9000 Family includes the following documents. To find a document online, use the Cisco MDS NX-OS Documentation Locator at:

http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/roadmaps/doclocater.htm

Release Notes

- Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Releases
- Cisco MDS 9000 Family Release Notes for MDS SAN-OS Releases
- Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images

Regulatory Compliance and Safety Information

- Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family

Compatibility Information

- Cisco Data Center Interoperability Support Matrix
- Cisco MDS 9000 NX-OS Hardware and Software Compatibility Information and Feature Lists
- Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide

Hardware Installation

- Cisco MDS 9500 Series Hardware Installation Guide
- Cisco MDS 9200 Series Hardware Installation Guide
- Cisco MDS 9100 Series Hardware Installation Guide
- Cisco MDS 9124 and Cisco MDS 9134 Multilayer Fabric Switch Quick Start Guide

Software Installation and Upgrade

- Cisco MDS 9000 NX-OS Software Upgrade and Downgrade Guide

Cisco NX-OS

- Cisco MDS 9000 Family NX-OS Licensing Guide
- Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide
- Cisco MDS 9000 Family NX-OS System Management Configuration Guide
- Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide
- Cisco MDS 9000 Family NX-OS Fabric Configuration Guide
- Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide
- Cisco MDS 9000 Family NX-OS Security Configuration Guide
- Cisco MDS 9000 Family NX-OS IP Services Configuration Guide
- Cisco MDS 9000 Family NX-OS Intelligent Storage Services Configuration Guide
- Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide

- Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide
- Cisco MDS 9000 Family Cookbook for Cisco MDS SAN-OS

Command-Line Interface

- Cisco MDS 9000 Family Command Reference

Intelligent Storage Networking Services Configuration Guides

- Cisco MDS 9000 Family I/O Acceleration Configuration Guide
- Cisco MDS 9000 Family SANTap Deployment Guide
- Cisco MDS 9000 Family Data Mobility Manager Configuration Guide
- Cisco MDS 9000 Family Storage Media Encryption Configuration Guide

Troubleshooting and Reference

- Cisco MDS 9000 Family and Nexus 7000 Series System Messages Reference
- Cisco MDS 9000 Family SAN-OS Troubleshooting Guide
- Cisco MDS 9000 Family NX-OS MIB Quick Reference
- Cisco DCNM for SAN Database Schema Reference

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

New and Changed Information

This chapter introduces new and changed information for Cisco Data Center Network Manager, Release 10.0.x. For more information about the operation on the Cisco DCNM Web Client and SAN Client, please refer to Web Client Online Help.

The following table lists the New and Changed topics for this guide.

Table ii-1 New and Changed Topics for Cisco DCNM Release 10.0.x

Feature	New or Changed Topics	Changed in Release	Where Documented
Device Packs Installation and Uninstallation	Device Packs	10.0(1)DP1	Chapter 3, "Device Pack for Cisco DCNM"
Revised next generation GUI with fresh new look and Navigations	Main Updates in Release 10.0	10.0.x	Cisco DCNM Web Client, page 1
LAN Client Migration - Remove LAN thick client	Migration of DCNM function for LAN to Unified Web Client	10.0.x	Multi-Site-Manager, page 9
SAN Client Migration	Migrated CiscoCisco DCNM SAN Client Functionality	10.0.x	Migrated Cisco DCNM SAN Client Functionality, page 10
Enhanced Topology	Enhanced Topology	10.0.x	Enhanced Topology, page 9
Multi-Manager visibility and synchronization across multiple sites	Multi Site Manager	10.0.x	Multi-Site-Manager, page 9
Multi-Fabric management capability from one DCNM	Multi-Fabric	10.0.x	Multi-Fabric, page 8
Support ISSU, SMU and GIR	Image Management	10.0.x	Image Management, page 10
Patch deployment tool supported	Moulder Device Support	10.0.x	Modular Device Support, page 11
Role Based Access Control	Role Based Access Control	10.0.x	Role Based Access Control, page 13

Table ii-1 New and Changed Topics for Cisco DCNM Release 10.0.x (continued)

Feature	New or Changed Topics	Changed in Release	Where Documented
Configuration Archive	Configuration Archive	10.0.x	Configuration Archive, page 14
Installing and un-installing Device Packs	Device Pack for Cisco DCNM	10.0.x	Device Pack for Cisco DCNM, page 1

CHAPTER 1

Introduction to Cisco Data Center Network Manager

Cisco Data Center Network Manager (DCNM) is a network management solution for next generation Data Centers. DCNM provides Fabric Automation, LAN administration for Cisco Nexus product line and SAN administration for the Cisco MDS product line - this may also include storage functionality on certain Cisco Nexus products. Cisco DCNM's goal is to reduce Operation expense by providing efficient operations and troubleshooting.

Cisco DCNM increases overall data center infrastructure uptime and reliability, thereby improving business continuity. It provides a robust framework and comprehensive feature set that meets the routing, switching, and storage administration needs of data centers. Cisco DCNM streamlines the provisioning for the unified fabric and monitors the SAN and LAN components. Cisco 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 products.

Cisco DCNM LAN Thick Client has been omitted from release 10.0.x. Now you can perform the functionalities on the unified Cisco DCNM Web Client instead of another LAN thick client. DCNM SAN and DCNM DM Clients are an installation option. All Cisco DCNM Web Client and Cisco DCNM for SAN product documentation is now published to the Data Center Network Manager listing page on Cisco.com:

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

CHAPTER 2

Cisco DCNM User Roles

Cisco DCNM defines what operations a user can perform in Cisco DCNM Web Client by controlling what features are available in the menu and tool bar items. Cisco DCNM role-based authorization limits access to the server operations depending on the user roles.

This chapter contains following sections:

Cisco DCNM Credentials

Cisco DCNM has two sets of credentials, namely:

- Device credentials—used to discover and manage devices
- Cisco DCNM credentials—used to access the Cisco DCNM server.

This document describes about DCNM credentials and how user roles are mapped to specific set of DCNM server operations.

Cisco DCNM Users

Cisco DCNM user-based access allows the administrator to control the access to the Cisco DCNM server by using the DCNM client (Web Client or LAN client). The user access is secured by a password.

Note Beginning from Release 10.0(x), DCNM does not allow you to reset the password using adduser script. You must logon to Cisco DCNM Web UI to reset the password. The adduser script is used only to add a new DCNM user on the existing DCNM setup.

DCNM Roles

Cisco DCNM performs authorization of access to the users based on roles. The role-based authorization limits access to the Cisco DCNM server operations based on the roles to which the users are assigned. Cisco DCNM does not define new roles to access the DCNM server; however, the Cisco DCNM leverages the existing roles that are supported on the devices monitored, such as Cisco MDS 9000 Series Switches, and Cisco Nexus Switches.

Cisco DCNM supports following roles:

- global-admin
- network-admin
- lan-network-admin
- san-network-admin
- san-admin
- server-admin
- sme-admin
- sme-stg-admin
- sme-kmc-admin
- sme-recovery
- network-operator

In a typical enterprise environment, users and their roles are defined in a centralized place such as, TACACS+, RADIUS or LDAP. As Cisco DCNM supports the existing device roles, the administrator need not define new roles specifically.

Roles from Cisco DCNM Perspective

Cisco DCNM perspective defines the operations a user can perform on the Cisco DCNM client by controlling the menu and tool bar items. Different perspectives define different set of operations.

For example, the **Admin** perspective allows all the operations by showing all the menu and tool bar items where as **Operator** perspective allows limited set of operation by hiding Admin and Config Menu items.

Each DCNM user role is mapped to a particular DCNM perspective, which allows limited access to server features. DCNM clients support following four perspectives:

- Admin Perspective, page 2-3
- Server Admin Perspective, page 2-3
- SME Perspective, page 2-4
- Operator Perspective, page 2-5

Table 2-1 describes how DCNM roles are mapped to client perspectives.

Table 2-1 DCNM Roles and Perspectives Mapping Table

Role	Perspective
global-admin	Admin Perspective
network-admin	
san-admin	
san-network-admin	
lan-network-admin (Web Client)	
server-admin	Server Admin Perspective
sme-admin	SME Perspective
sme-sgt-admin	
sme-kmc-admin	
sme-recovery	
network-operator	Operator Perspective
lan-network-admin (SAN Thick Client)	

Admin Perspective

Admin Perspective can be accessed through the Cisco DCNM Web Client and SAN Client only, by the users who are assigned the role of global-admin, network-admin, san-admin, san-network-admin and lan-network-admin.

Web Client Admin Perspective

Web client admin perspective has full control of the DCNM server and can access all the features. Via the access to the **Admin** menu items, the users also has full control of Cisco DCNM authentication settings.

SAN Thick Client Admin Perspective

SAN thick client admin perspective has full control of the DCNM server and can access all the features. All the top-level menu items are accessible.

Server Admin Perspective

Server admin perspective can be accessed via web client and SAN thick client only by the users who are assigned the role of server-admin.

Web Client Server Admin Perspective

Web client server admin perspective has access to all the web client features. Via the access to the **Admin** menu items, the users also has full control of Cisco DCNM authentication settings.

SAN Thick Client Server Admin Perspective

The configuration capabilities of a server admin role are limited to FlexAttach and relevant data. The server admin can pre-configure SAN for new servers, move a server to another port on the same NPV device or another NPV device and replace a failed server onto the same port without involving the SAN administrator. The server admin will not be able to manage Fabric Manager users or connected clients. The menu items that are not related to server management are not accessible, e.g. **Zone**, **Performance**, etc. SAN thick client server admin perspective has no access to **Discover** button, **Fabrics** and **License Files** tabs. The server admin is not able to manage Fabric Manager users or connected clients in SAN thick client.

SME Perspective

Storage Media Encryption (SME) perspective is designed for sme-admin, sme-sgt-admin, sme-kmc-admin and sme-recovery role-based users. It can be categorized to five different sme admin perspective according to the roles:

- Web Client SME Admin Perspective, page 2-4
- SME Storage Perspective, page 2-4
- SME Key Management Perspective, page 2-4
- SME Recovery Perspective, page 2-4
- SAN Thick Client SME Perspective, page 2-5

Web Client SME Admin Perspective

Web client sme admin perspective is designed to sme-admin role users who have no access to **Admin** and **Config** menu items in the Web client and cannot use features under those menu items. On the other hand, the SME provision features are accessible.

SME Storage Perspective

SME storage perspective is designed to the sme-stg-admin role users. sme-stg-admin role users have same perspective as sme-admin role except you cannot manage the key management features.

SME Key Management Perspective

SME key management perspective is designed to the sme-kmc-admin role users. sme-kmc-admin role users have same perspective as sme-admin role except that you cannot perform SME configurations.

SME Recovery Perspective

SME recovery perspective is designed to the sme-recovery role users for master key recovery. sme-recovery role users have same perspective as sme-admin role except that you cannot perform the storage and key management features.

SAN Thick Client SME Perspective

SAN thick client SME perspective has no access to **Discover** button, **Fabrics** and **License Files** tabs.All the SME related perspective would not be able to manage Fabric Manager users or connected clients, as well as operator perspective.

Operator Perspective

Operator perspective is designed for network-operator and lan-network-admin role users, and lan-network-admin role only has SAN thick client operator perspective.

Web Client Operator Perspective

Web client operator perspective has no access to **Admin** and **Config** menu items and the features under those menu items cannot be used. All the other features can be used.

SAN Thick Client Operator Perspective

SAN thick client operator perspective has no access to **Discover** button, **Fabrics** and **License Files** tabs, and would not be able to manage Fabric Manager users or connected clients.

CHAPTER 3

Device Pack for Cisco DCNM

The device pack is a modular installation that can be applied on Cisco DCNM. The device pack adds support for the Cisco Nexus Switches to Cisco DCNM versions.

Installing the Device Pack

Perform the following steps to install the device pack with DCNM.

Step 1 Navigate to www.cisco.com/go/dcnm, and download the latest device pack.

```
Example:
dcnm-device-pack.10.0.1.DP.1.zip
```

Step 2 Copy the zip file to the DCNM machine.

Step 3 Stop the DCNM applications by using the appropriate command.

- For Cisco DCNM in Standalone and Federation modes, use **appmgr stop dcnm** command.
- For Cisco DCNM in Native HA mode, use **appmgr stop ha-apps** command.
- For Cisco DCNM in Linux Standalone and Federation modes, use **stopSANServer.sh** command.
- For Cisco DCNM in Windows Standalone and Federation modes, use **stopSanService.bat** command.

Step 4 Navigate to the location where you have saved the device pack and extract the files

Step 5 Execute the patch file by using the following command:

./patch.sh *<patchname_with_path>*

```
Example:
/usr/local/cisco/dcm/fm/bin/patch.sh /root/dcnm-device-pack.10.0.1.DP.1.zip
```

The patch installation process begins.

Note For Federation and Native-HA setup with Cisco DCNM, ensure that the device pack is installed on both primary and secondary devices.

Step 6 After the patch installation is complete, restart DCNM applications using the appropriate command.

- For Cisco DCNM in Standalone and Federation modes, use **appmgr start dcnm** command.
- For Cisco DCNM in Native HA mode, use **appmgr start ha-apps** command.

- For Cisco DCNM in Linux Standalone and Federation modes, use **startSANServer.sh** command.
- For Cisco DCNM in Windows Standalone and Federation modes, use **startSanService.bat** command.

Step 7 Navigate to Cisco DCNM **Web Client > Administration > DCNM Server > Modular Device Support** for view the list of patches applied to the Cisco DCNM. You can verify the patch installation on the Cisco DCNM Web Client.

CHAPTER 4f

Cisco DCNM Web Client

Using Cisco DCNM Web Client, you can monitor Cisco MDS and Nexus family switch events, performance and inventory, and perform minor administrative tasks.

The default user credentials to access Cisco DCNM, Release 10.0.x are as configured during the deployment of the installers.

Cisco DCNM Web Client provides the following features:

Navigating DCNM Web Client

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. Cisco DCNM provides a comprehensive feature set that meets the routing, switching, and storage administration needs of data centers. Cisco DCNM streamlines the provisioning for the unified fabric and monitors the SAN and LAN components. Cisco 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 to install applications related to Unified Fabric only for Unified Fabric-mode installations.

The DCNM Web Client has standardized certain navigation conventions.

Scope Menu

Beginning with Cisco NX-OS Release 6.x, a new drop-down list called Scope is added to Cisco DCNM Web Client that applies to all pages except the Administration and Configure pages.

You can use the scope menu to filter network information by:

- Data Center
- Default_LAN
- Default_SAN
- Individual Fabric Various other custom scopes created by the users.

The features accessible from the tabs are limited to the areas that you choose in the filter tree.

Admin Menu

You can use the admin menu to:

- **DCNM SAN**: Launch the SAN Client.
- **DCNM DM**: Launch the Device Manager Client which is part of the SAN option.
- **Change Password**: Changes the password for the current logged in user.
- **Help Content**: Pops out the online help of the current page.
- **About**: Display the information about Cisco Data Center Network Manager.
- **Logout**: Logout from the DCNM Web Client.

Table and Filtering Navigation

Some tables that can be filtered will have a filter option to view subsets of the information. Either choose the filter menu or click **Filter**. An editable row at the top of the table appears. Enter values into the table cells and click **Return** to display matching rows.

Printing

Click **Print** to view the table in a printer-friendly format. You can then print the page from the browser.

Exporting to a File

An Export icon is in the upper right corner of some tables or top right corner of the window. Click this icon to export the data to Microsoft Excel.

Sorting Columns

Not all columns are sortable but you can click a sortable column head to sort the information for that column.

Cisco DCNM Web Search Engine

The search engine helps you to locate records according to the following search criteria:

- Search by Name.
- Search by IP Address.
- Search by WWN.
- Search by Alias.
- Search by MAC Address.
- Search by Serial Number.

Using the Cisco DCNM Search Engine

Step 1 Click **Search box** on the top right corner of the main window.

You see the search text box.

Step 2 Use the drop-down to search by:

- Name
- IP Address
- WWN
- Alias
- MAC Address
- Serial Number

Step 3 Enter the value based on the search option and click the arrow to begin the search.

The search results are displayed in a new window.

Downloading Cisco DCNM-SAN Client

You must use Cisco DCNM Web Client to launch Cisco DCNM-SAN Client.

Step 1 On the top right of the DCNM Web Client home screen, click the settings icon next to the login user. Select **DCNM-SAN** option.

Step 2 If you have the latest Java version installed, a Warning message is displayed.

Step 3 Click **Run with the latest version** button.

Step 4 Enter the user credentials to log on to Cisco DCNM-SAN client. This message appears only the first time you launch Cisco DCNM-SAN Client.

Downloading Cisco Device Manager Client

You must use Cisco DCNM Web Client to Install Cisco Device Manager client.

Note Device Manager Client is part of the SAN option.

Step 1 On the top right of the DCNM Web Client home screen, click the settings icon next to the login user. Select **DCNM DM** option.

Step 2 If you have the latest Java version installed, a Warning message is displayed.

Note Cisco DCNM Device Manager supports JRE versions 1.6 and 1.7. Follow the instructions in the Cisco Device Manager installer wizard to proceed with the installation.

Step 3 Once the installation is complete, enter the user credentials to log on to the Cisco Device Manager client.

Viewing Dashboard Information

The Cisco DCNM Web Client dashboard gives you comprehensive information of the following:

- Summary - You can view the summary dashboard which displays the overall functioning of all the devices connected. It gives you daily statistics of the connected devices. New panels has been introduced in release 10.0.x to simplify the management of LAN and SAN clients.
- Network - You can view the information of switches including status and license, as well as detailed switch dashboard information for a specific switch.
- Storage - You can view details about the storage device along with its events and topology.
- Compute - You can view the details and events for a particular Host along with its events and topology.

Note Compute is available only with SAN installation

For more information about the Dashboard tab, refer to the Web Client Online Help.

Viewing Topology Information

Topology is a first class menu item in this release with the intention that it is fully functional for providing detailed access to configuration as well as monitoring functionality. The Cisco DCNM topology consolidates functionality in the existing Fabric topology as well as the current Dashboard topology into a new fully featured topology which includes the following features in a single view:

- Optional display of Vinci Balls or device icons.
- Display of Multi-link, Port-channels, VPCs.
- Display of Inter-fabric links.
- VDC and Pod Groupings.

- Device-Scope, Fabric and Datacenter drill-down.
- Automatic VPC Peer and FEX Groupings.
- Ability to select devices and take action consistent with other areas of the product.

For more information about Topology, refer to the Web Client Online Help.

Viewing Inventory Information

Beginning with Cisco DCNM release 6.x, you can view the inventory and the performance for both SAN and LAN switches by using the global Scope pane. You can select LAN, SAN, or both to view the inventory information. You can also export and print the inventory information. In this tab, you can find the discovered LAN switches, SAN switches, Storage devices and Virtual Machine Manager. You can also add a new discovery LAN or SAN switch as well.

For more information about Inventory tab, refer to the Web Client Online Help.

Viewing Monitor Information

You can get the performance statistics of CPU, Memory, Traffic, others, accounting and events information. You can also view performance information about SAN and LAN. You can also create customized reports based on historical performance, events, and inventory information gathered in this tab. You can create aggregate reports with summary and detailed views. You can also view previously saved reports.

For more information about Monitor tab, refer to the Web Client Online Help.

Viewing Configure Information

Allow user to view and configure Zoning, Device Alias, Port Monitoring and Device Credentials.

For more information about Configure tab, refer to the Web Client Online Help.

Viewing Administration Information

You can view and configure DCNM servers, DCNM users, performance setup and event setup.

For more information about Administration tab, refer to the Web Client Online Help.

Using Cisco DCNM Web Client with SSL

From release 10.0.x, Cisco DCNM Web Client uses HTTPs. If you want to install SSL certificates and use Cisco DCNM Web Client over HTTPs (using TCP port 443 or another custom port), you need a certificate for each external IP address that accepts secure connections. You can purchase these certificates from a well-known Certificate Authority (CA).

To enable SSL, you must set up the keystore to use either a self-signed certificate or a certificate from a trusted third-party company such as VeriSign.

This section includes the following topics:

Creating a Local Certificate

Step 1 Set up a keystore to use a self-signed certificate (local certificate). From the command line, enter the following command on windows:

```
%JAVA_HOME%/bin/keytool -genkey -alias tomcat -keyalg RSA -keystore "C:\Program
Files\Cisco Systems\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks"
```

Step 2 Enter your name, organization, state, and country. Enter **change it** when prompted for a keystore password. If you prefer to use your own password, do not forget to change the keystorepass attribute in the server.xml file. When prompted for a key password, press **Enter** or use the same password as the keystore password.

Note You can now follow the steps in the next section for modifying DCNM Web Client to use SSL.

To obtain a certificate from the Certificate Authority of your choice, you must create a Certificate Signing Request (CSR). The CSR is used by the certificate authority to create a certificate that identifies your website as secure.

Creating a Certificate Request

Step 1 Create a local certificate (as described in the previous section).

Note You must enter the domain of your website in the fields First and Last name in order to create a working certificate.

Step 2 Create the CSR with this commandon windows:

```
keytool -certreq -keyalg RSA -alias tomcat -file certreq.csr -keystore "C:\Program
Files\Cisco Systems\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks"
```

Now you have a file called certreq.csr. The file is encoded in PEM format. You can submit it to the certificate authority. You can find instructions for submitting the file on the Certificate Authority website.

Step 3 After you have your certificate, you can import it into your local keystore. You must first import a Chain Certificate or Root Certificate into your keystore. You can then import your certificate.

Step 4 Download a Chain Certificate from the Certificate Authority where you obtained the certificate:

- For Verisign.com commercial certificates, go to this URL:

  http://www.verisign.com/support/install/intermediate.html

- For Verisign.com trial certificates, go to this URL:

  http://www.verisign.com/support/verisign-intermediate-ca/Trial_Secure_Server_Root/index.html

- For Trustcenter.de, go to this URL:

  http://www.trustcenter.de/certservices/cacerts/en/en.htm#server

- For Thawte.com, go to this URL:

  http://www.thawte.com/certs/trustmap.html

- Import the Chain Certificate into your keystore by entering the **keytool -import -alias root -keystore " C:\Program Files\Cisco Systems\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -trustcacerts -file** *filename_of_the_chain_certificate* **command.**
- Import the new certificate in X509 format by entering the **keytool -import -alias tomcat -keystore " C:\Program Files\Cisco Systems\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -trustcacerts** *-file your_certificate_filename* **command.**

Major Changes on Cisco DCNM Web Client

In release 10.0.x, Cisco DCNM replaces Flash with HTML5 and makes GUI consolidation. Cisco DCNM release 10.0.x introduces new look and feel for all GUI screens including:

- Migration of DCNM function for LAN to Unified Web Client, page 4-7
- Multi-Fabric, page 4-8
- Enhanced Topology, page 4-9
- Multi-Site-Manager, page 4-9
- Migrated Cisco DCNM SAN Client Functionality, page 4-10
- Image Management, page 4-10
- Modular Device Support, page 4-11
- Role Based Access Control, page 4-13
- Configuration Archive, page 4-14

Migration of DCNM function for LAN to Unified Web Client

For the simplification of management, Cisco DCNM LAN Thick Client has been omitted from release 10.0.x. Now you can perform the functionalities on the unified Cisco DCNM Web Client instead of another LAN thick client. DCNM SAN and DCNM DM Clients are an installation option.

The LAN client and server related components are removed from the installer. The Database tables related to LAN are not created during installation which reduces the size of the installer as well as the installation time and download time.

For more information about the usage of the Cisco DCNM Web Client, please refer to Web Client Online Help.

Multi-Fabric

Starting from Cisco DCNM release 10.0.x, Cisco DCNM supports multi-fabric which means fabrics of different encapsulation type such as FabricPath and VXLAN fabric, can co-exist and fabric level consistency can be validated.

The multi-fabric workflow includes fabric object creation, fabric bring-up per fabric plan, fabric provisioning, and fabric monitoring via topology.

Creating Fabric Object

You can add a LAN fabric through Cisco DCNM Web Client.

From the menu bar, choose **Configure > LAN Fabric Settings > LAN Fabrics**.

A fabric instance can encapsulate and define not just the properties of the Fabric, but also serve as a container to group all the Leaf, Spine, Border Leaf, Edge Router and other entities that fall into the purview of the Fabric.

The advantages of grouping of the Fabric includes:

- Fabrics of different encapsulation types like FP or VxLAN co-reside in DCNM now.
- Device types and template instances are validated and users can be warned accordingly since the intent of the Fabric is well defined at the beginning of the Fabric design.
- Topology and other visualization tools can feed off this Fabric instance information to make prudent judgments on layout design.
- Fabric level health computation is more meaningful because the meta-data provided by the user about the Fabric helps define the actual intent and behavior of the Fabric.

Fabric Plan

You can add a LAN fabric through Cisco DCNM Web Client.

From the menu bar, choose **Configure > LAN Fabric Settings > LAN Fabrics**. Click the **Add Fabric Plan** icon.

Fabric plan is a paradigm to define the intent and characteristics of the Fabric, so that this definition can help guide the rest of the Fabric deployment, management and monitoring.

During fabric plan creation, you can specify the spine, leaf and border switches count, type, and supply the subnets used for numbered IP fabric interfaces as well as VPC peer leaf and keep-alive interfaces. In addition, you can choose to override the default POAP templates that DCNM pre-selects for the switches based on the switch role. DCNM will then auto-generate the cabling plan and auto-populate the POAP definitions for all the switches within the fabric. You are able to update those auto-populated values. After the switch is powered on, DCNM will auto-associate switch according to the serial number with entries in cable plan based on switch's neighbor info gathered during switch boot-up. If needed, DCNM will auto-apply the corresponding POAP definition on the switches to bring up the complete fabric.

Fabric Provision

Similar as previous releases, fabric provision data is organized in organization, partition and network hierarchy. Instead of a flat structure for all the fabrics managed by the same DCNM, the provision data is separated at fabric level so as to be easily traversed, backed-up and restored.

There are 2 exclusive options to provision fabric:

- Switch initiates auto-configuration and Cisco DCNM triggers auto-pull, which requires switch to support auto-configuration feature.
- Cisco DCNM controlled configuration deployment. That means, DCNM manages the VLAN (de)allocation, (un)deploys and tracks the configuration on switches.

Fabric Monitoring

In addition to the fabric topology that depicts all the switches within the fabric and interaction across fabric, DCNM provides fabric level aggregation of information such as switch summary, licensing tracking, provision distribution and health score. The fabric level aggregation data will also be consumed by multi-site feature.

Enhanced Topology

Topology becomes a first class menu item in release 10.0.x with the intention that it is fully functional for providing detailed access to configuration as well as monitoring functionality.

The Cisco DCNM topology includes the following features in a single view:

- Optional display of Fabric topology or device icons
- Display of Multi-link, Port-channels, VPCs
- Display of Inter-fabric links
- VDC and Pod Groupings
- Device-Scope, Fabric and Datacenter drill-down
- Automatic VPC Peer and FEX Groupings
- Ability to select devices and take action consistent with other areas of the product.

The enhanced Topology provides the following functionality:

- Display Link state.
- You can drag, pan, and zoom on the topology page. Device layout is in a tiered topology by default. Customized views can be saved.
- Click on the switch device or the links, port-channel or vpc loop on the topology page, it pops out the summary configuration and status information panel.
- Mouse-over:
  - Link mouse-over provides summary performance information.
  - Device mouse-over displays the quick information about the device.
- Search for VLAN, VNI, FP, VRF, etc.

For more information about Topology, refer to the Web Client Online Help.

Multi-Site-Manager

From the menu bar, choose **Administration > DCNM Server > Multi Site Manager**.

Multi Site Manager (MsM) provides a single pane for customer to globally search for switches and virtual machine's location which Cisco DCNM server owns it. Hyperlink will be provided to access the corresponding switch, host, or the virtual machine (if applicable). Enter the user name and password to

login. The page also plays the role of remote site registration. The registration only allows the current Cisco DCNM server to access the remote DCNM server or site. For the remote site to access the current Cisco DCNM server, registration is required on the remote site as well. After you have done the registration, the MSM panel will display a diagram to show the overall health and status of the remote site, and the content of the panel will be subject to change.

MSM supports the following:

- Allow user to see the overall health of the switches (inside SAN and LAN Fabric) in each site.
- Allow user to find out which DCNM Server (site) is managing a given switch.
- On demand finding out the upstream LAN switch of a given host/virtual machine.
- On demand finding out which LAN switches have active VXLAN segment.

Migrated Cisco DCNM SAN Client Functionality

Above from release 10.0.x, Cisco DCNM has supported zone configuration, device alias management and port monitoring for SAN in web client.

From the menu bar, choose **Configure > SAN > Zoning**.

Zonesets, Zones, Zone Members and **Available to Add** panels are displayed in a single screen which is more easier to do the zone operation.

From the menu bar, choose **Configure > SAN > Device Alias**.

You can create, delete and edit the device alias in the device alias table. You can also **Commit**, **Abort** changes on the selected switch and **Clear CFS Lock** on the **CFS** tab.

From the menu bar, choose **Configure > SAN > Port Monitoring**.

You can select a set of non-editable default policy including **Normal, Default, Aggressive, Most-Aggressive** and **Slowdrain** which are bundled in DCNM to push to the selected switches. You can customize the policy based on the default policy and push the customized policy to the SAN switch. You can view the existing PMON policy on SAN switch.

For more information about the usage of the Cisco DCNM Web Client, please refer to Web Client Online Help.

Image Management

Data center administrators have the onus of tracking the images installed on switches in the network and upgrading them whenever Cisco releases new software images. Image management on the Cisco Nexus devices is done by In-Service Software Upgrade (ISSU), Software Maintenance Upgrades (SMU), and Graceful Insertion and Removal (GIR) through Cisco DCNM web client.

On Cisco DCNM web client, you can:

- Tack images installed on the switches.
- Do upgrade or downgrade of images on multiple switches.
- Schedule the image installation.

From the menu bar, choose **Configure > Image Management > Upgrade**.

Cisco Nexus Series switches and any connected FEXs can be upgraded without any traffic disruption.

From the menu bar, choose **Configure > Image Management > Patch**.

SMUs are created to respond to immediate issues and do not include new features. Typically, SMUs do not have a large impact on device operations. You can install and uninstall the SMU tasks in this page.

From the menu bar, choose **Configure > Image Management > GIR**.

You can change the system mode to GIR mode for the selected switch on this page. GIR mode provides an easy method for isolating a switch for maintenance windows and then bringing it back into service.

From the menu bar, choose **Configure > Image Management > Repositories**.

You can see the history of ISSU jobs that were triggered from Cisco DCNM for each of the device. This helps for accounting purpose and to find the images installed on the devices.

Note Image management is a licensed feature. Hence you are able to select only the licensed devices. Only Cisco Nexus 3000, Cisco Nexus 5000, Cisco Nexus 6000, Cisco Nexus 7000 and Cisco Nexus 9000 devices are supported.

For more information about the usage of the Cisco DCNM Web Client, please refer to Web Client Online Help.

Modular Device Support

Start from release 10.0.x, Cisco DCNM has supported to apply the patch to the released software that are running in production. In order to support any new hardware which doesn't require many major changes, a patch can be delivered instead of waiting for the next DCNM release. This feature helps to deliver and apply the DCNM patch releases. An authorized DCNM administrator can apply the patch deliverables to the production setup using this tool. Patch releases can be applicable for the following scenarios.

- Support any new hardware (Chassis/Line cards).
- Support latest Cisco NX-OS versions.
- Support critical fixes as patches.

Applying the patch

Step 1 Stop DCNM services.

Step 2 Execute the following command to apply the patch in command prompt or console:

- **Windows**

```
patch.bat <absolute patch of patch>
```

Note patch.bat is present in C:\Program Files\Cisco Systems\dcm\fm\bin

Example:

```
> cd C:\Program Files\Cisco Systems\dcm\fm\bin
> patch.bat C:\patches\Hafnium-testing.zip
```

- **Linux**

```
./patch.sh <absolute patch of patch>
```

Note patch.sh is present in /usr/local/cisco/dcm/fm/bin.

Example:

```
> cd /usr/local/cisco/dcm/fm/bin
>./patch.sh  /root/patches/Hafnium-testing.zip
```

Step 3 To view the patch details, open the DCNM web UI and go to **Administration > Modular Device Support**. This window will show the patch deployed on each DCNM server.

- **Federation**

  Patch needs to be applied on all servers in federation separately.

  Before applying the patch stop DCNM service on all servers in Federation

- **Native HA**

  Patch needs to be both Active and Standby Servers separately

  Before applying the patch stop all service primary service should be stopped.

Rollback

Rollback will removes patch applied most recently. To rollback multiple patch run rollback operation multiple times.

Rollback the patch

Step 1 Stop the DCNM services.

Step 2 Execute the following command to roll back the patch.

- **Windows**
  - Run the following command:

    patch rollback

Note patch.bat is present in C:\Program Files\Cisco Systems\dcm\fm\bin.

  - Start the DCNM services on windows.
- **Linux**
  - Run the following command to roll back the patch.

    ./patch.sh rollback

Note patch.sh is present in /usr/local/cisco/dcm/fm/bin.

  - Start the DCNM services on Linux

Step 3 Once the patch is rolled back, corresponding information will not be shown in **Administration > Modular Device Support** window in web UI.

Role Based Access Control

Cisco DCNM allows the administrator to manage users' access to the Cisco DCNM server and assign a role to each user by using the Cisco DCNM Web client.

- If you are assigned the role as **user**,
  - You cannot change the Cisco DCNM authentication mode.
  - You cannot add or delete Cisco DCNM local user accounts.
  - You can change the details of your own local user account.
- If you are assgned the role as **admin**:
  - You have full control of Cisco DCNM authentication settings.

Starting from release 10.0.x, the new introduced Role Based Access Control (RBAC) feature allows the **admin** to associate **user** to one or more device scope or group, so that the **admin** can control **users**' access to devices or fabrics from Cisco DCNM web client or SAN client, and the user can see only the associated switch groups in the **Scope** drop-down list. This way **admin** can restrict **users** to view or configure only sub-set of discovered devices.

Local Authentication for RBAC

You can do local authentication when you are assigned the role as **Network Admin**.

Step 1 Login the Cisco DCNM Web Client using the **Network Admin** account. You have full device access, i.e. Data Center group access.

Step 2 From the left menu bar, choose **Administration > DCNM Server > Switch Groups**. Click the **Add** icon to create a new group.

Step 3 From the left menu bar, choose **Administration > Management Users > Local**. Click **Add User** to create a new user and assign the role for the user.

Step 4 To manage the access for the user, select the user and click **User Access.** Check the box before the group or scope that you want the user to access to.

Step 5 When the newly created user logs into Cisco DCNM Web Client, he will see only the associated scope or groups in the **Scope** drop-down list at the top of the window and he can view only the devices belongs to those group.

Remote Authentication for RBAC

Cisco DCNM supports **TACACS+, Radius, Switch** and **LDAP** remote authentication. You can perform remote authentication when you are assigned the role as **Network Admin**.

Note Anonymous LDAP bind or access is disabled in Cisco DCNM Release 10.1. A read-only LDAP user has been introduced since DCNM 7.1(1), DCNM 7.0(2) and 7.0(1). We recommend you to upgrade to a later version for authenticated LDAP access.

Step 1 Login the Cisco DCNM Web Client using the **Network Admin** account. You have full device access, i.e. Data Center group access.

Step 2 From the left menu bar, choose **Administration > DCNM Server > Switch Groups**. Click the **Add** icon to create a new group.

Step 3 From the left menu bar, choose **Administration > Management Users > Remote AAA**.

– If you choose **TACACS+** or **Radius** authentication mode, *cisco-av-pair* attribute has been extended by adding the *dcnm-access* key in addition to *role*. To assign a Cisco DCNM user role by T**ACACS+** and **Radius**, Cisco DCNM use the returned *cisco-av-pair* attribute-value pair from TACACS+ and Radius remote authentication.

Table 1:cisco-av-pair Attribute-Value Pair, page 4-14 shows the *cisco-av-pair* attribute-value pair

Table 1: cisco-av-pair Attribute-Value Pair

Cisco DCNM Role	RADIUS Cisco-AV-Pair Value	TACACS+ Shell cisco-av-pair Value
User	*shell:roles = "network-operator" dcnm-access="group1 group2 group5"*	*cisco-av-pair=shell:roles="network-operator" dcnm-access="group1 group2 group5"*
Admin	*shell:roles = "network-admin" dcnm-access="group1 group2 group5"*	*cisco-av-pair=shell:roles="network-admin" dcnm-access="group1 group2 group5"*

Admin can configure the group information using the key *dcnm-access* with groups separated by commas as in the above table.

By getting the access information from the remote authentication, logged in user will be able to see only those associated group devices. If the remote authentication response does not assign groups, user can see all the devices.

– If you choose **LDAP** authentication mode, specify the **Access Map** text field to associate the accessible groups for the user. The format is: *userDomain1:group1,group2;userDomain2:group3*.

Note For **Switch** authentication mode, the RBAC is not supported.

Configuration Archive

The configuration archive feature allows you to backup device configurations, both running configuration and startup configurations as a regular text file in the file system. The backup files can be stored in the DCNM server host or on a file server.

You can also configure the archive system to support scheduling of jobs for the selected list of devices. You can configure only one job for a switch.

You can find this feature in the DCNM Web Client under **Configure > Backup > Switch Configuration**.

You can perform following tasks using this feature:

- Import the configuration file from the file server to the Cisco DCNM.
- Compare the configuration file with another version of the same configuration or with the configuration file of another device.
- Copy the configuration files to the same device, to another device, or multiple devices concurrently.

- Restore the configuration file from the selected switches or from the Golden backup.
- View or edit the configuration file on the device.
- Delete the configuration file from the device.
- Archive jobs.

For more information about the configuration archive feature, please refer to Web Client Online Help.

Configuring DCNM Native High Availability

This chapter describes the DCNM Native High Availability (HA) configuration and troubleshooting. This chapter contains the following sections:

DCNM HA Overview

DCNM Native HA provides a high availability solution for the DCNM. It consists of two DCNM nodes in which one node assumes the role of the active node and the other node assumes the role of the standby node.

The native HA is supported on Linux platform with ISO and OVA installation. For standalone installation, we will not support native HA as there might be missing Linux packages which are required for native HA. Native HA is also not supported on Windows platform.

By default, DCNM is bundled with an embedded database engine PostgreSQL. The DCNM native HA is achieved by two DCNM's running as Active / Warm Standby, with their embedded databases synchronized in real time. So once the active DCNM is down, the standby will take over with the same database data and resume the operation.

DCNM Native HA Installation

For detailed DCNM native HA setup process, please refer to Cisco DCNM Installation Guide, Release 10.0(x).

DCNM License Usage and Limitations

Cisco DCNM license is tied to host Mac Address. In DCNM native HA setup, there are two hosts with different Mac addresses. Here is how it works:

In DCNM native HA, only primary DCNM (node 1) is allowed to load license, the secondary (node 2) can only apply the licenses. This is similar to DCNM Federation where DCNM with Id 0 could load licenses, all others can only apply the licenses.

In DCNM native HA, the licenses should be generated only for the primary DCNM. Only primary DCNM (node 1) is allowed to load license. There are no extra DCNM server license and switch-based license required for secondary DCNM in Native-HA.

Note DCNM recommends having licenses on one instance and a spare matching license on the second instance.

Native HA Failover and Split-Brain

DCNM failover can be manually triggered, or if the standby DCNM detected the active DCNM is not responsive, the standby will then takeover and act as active.

In DCNM native HA, the VIP(s) are always associated with active host. When failover occurs, the active host shall disassociate the VIP(s) and shutdown the DCNM process; and the standby shall associate the VIP(s) with the host, change the database from stream replication mode to normal mode, and start up the DCNM process.

Split-Brain syndrome occurs when the communication on enhanced fabric interface between two HA peer is lost. As the result, both hosts will act as Active. When the communication resumes, both hosts shall negotiate and eventually one will become active, the other standby.

Disk File Replication

In addition to database real-time synchronization between two DCNM HA peers, there are also bunch of disk files which need to be replicated.

The disk files which need replication include POAP templates, performance data (RRD files), etc.

Replace HA Hosts

If you need to replace an HA host machine, please follow the procedures:

Note The IP addresses or VIPs are assumed not to be changed.
Hosts that having "Deployed role: Standby" can only be replaced.

Step 1 Stop the DCNM on the standby host (no IP change).

Step 2 Stop the DCNM on the active host (no IP change).

Step 3 Take backup of Standby DCNM.

Step 4 Take a local copy of ha-properties file from **/root/packaged-files/properties/ path.**

Step 5 On the new host which is supposed to replace the old host, configure the IP addresses on eth0 and eth1to be identical to the old host.

Step 6 If the host is a virtual machine, configure the mac address to be identical to the old host, so there will be no need to get new licenses for the new host.

Step 7 On the new host which will join the HA setup, run the HA setup script, just like in the normal HA setup procedure.

Step 8 Restart the DCNM on the active host, then restart the DCNM on the standby host.

DCNM Native HA with Scaled Up Test

Different HA scale limits have been mentioned under DCNM 10.x release. Please refer to Cisco DCNM Release Notes, Release 10 for scale requirement and scale limits.

AAA Configuration

For AAA configuration, you need to install Cisco DCNM native HA with local user credentials. Once the installation is done, please log into the DCNM web client and go to **Administrator > Management Users > Remote AAA** and select the required authentication mode.

Note When doing remote AAA authentication, Cisco DCNM is sending out request using its own eth0 IP rather than VIP. Therefore, on the AAA server, we need to put two entries for DCNM IP, one for active DCNM, the other for standby IP, but not VIP.

Troubleshooting DCNM Native HA

When Cisco DCNM native HA setup is in an uncertain situation, stop both hosts and resolve the problem. Start only one host and ensure that it is fully functional, and the device data is correct before you bring up the second host as standby.

Note Throughout this Troubleshooting procedure, **dcnm1** is considered as the Active host and **dcnm2** is considered for Secondary host.

This contains the following sections:

- "Resolving HA Status Failure condition" section on page 5-7
- "Bringing up Database on Standby Host" section on page 5-8

Recovering DCNM when both hosts are Powered Down

Perform the following to troubleshoot the DCNM Native HA setup when both the hosts are powered down.

Step 1 Power on **dcnm1**.

Step 2 Wait for all the applications to be operational.

Use the **appmgr status all** command to check the status of the applications.

```
dcnm1# appmgr status all
```

Logon to DCNM. Verify if it is fully functional. Check if the device data is correct. If success, power on **dcnm2** as Secondary host. Terminate the troubleshooting procedure.

Step 3 If the host fails to bring up all the applications, or if the device data is incorrect, use the **appmgr stop all** command to stop the process.

Wait for all the applications to stop.

Step 4 Power on **dcnm2**.

Wait for all the applications to be operational.

Step 5 Use the **appmgr status all** command to check the status of the applications.

```
dcnm2# appmgr status all
```

Logon to DCNM. Verify if it is fully functional. Check if the device data is correct. If success, power on **dcnm1** as Secondary host. Terminate the troubleshooting procedure.

Step 6 If **dcnm2** fails to bring up all the applications, or if the device data is incorrect, use the **appmgr stop all** command to stop the process.

Step 7 Restore both hosts from backup.

Recovering from Split-Brain syndrome

Perform the following to recover Cisco DCNM from the split brain syndrome.

Step 1 Stop both Active and Standby Cisco DCNM hosts.

Use the **appmgr stop all** command, to stop the applications

```
dcnm1# appmgr stop all
dcnm2# appmgr stop all
```

Step 2 Wait for all the applications to stop.

Use the **appmgr status all** command to check the status of the applications.

```
dcnm1# appmgr status all
dcnm2# appmgr status all
```

Resolve the communication problem between two hosts which causes the Split-Brain Syndrome.

Step 3 Ping the peer host eth1 IP address from both hosts and make sure it is reachable.

Step 4 Start all the applications on **dcnm1**. Wait for all the applications to be operational.

Use the **appmgr status all** command to check the status of the applications.

```
dcnm1# appmgr status all
```

Step 5 Logon to **dcnm1** and verify if it is fully functional and if all the data is correct.

If all the data is correct, proceed to Step 7.

If data loss is seen, proceed to Step 6.

Step 6 Use the **appmgr stop all** command, to stop the applications

```
dcnm1# appmgr stop all
```

Step 7 Start all the applications on **dcnm2**. Wait for all the applications to be operational.

Use the **appmgr status all** command to check the status of the applications.

```
dcnm2# appmgr status all
```

Step 8 Logon to DCNM. Verify if it is fully functional.

Check if the device data is correct. If success, power on **dcnm1** as Secondary host. Terminate the troubleshooting procedure.

Step 9 If data loss is seen on **dcnm2**, stop all the applications.

Use the **appmgr stop all** command, to stop the applications

```
dcnm2# appmgr stop all
```

Step 10 Restore both hosts from backup.

Checking Cisco DCNM Native HA Status

Perform the following to determine the status of the Cisco DCNM Native HA.

Step 1 Login into Cisco DCNM Web Client.

Step 2 Navigate to **Web Client > Administration > Native HA**.

Step 3 Check for HA Status.

The status of the Native HA and their description is as depicted in the table below.

HA Status	Description
OK	Implies that the Native HA is operational. Both the hosts on the Native HA are synchronized.
Stopped	Implies that the Standby host is not operation. The database is not synchronized.

HA Status	Description
Failed	Implies that the Active host is unable to synchronize with the Standby host. Check the log files for more information. The log file is located at: `/usr/local/cisco/dcm/fm/logs/fms_ha.log`
Not Ready	Implies that the Standby host is not setup or not configured.

Verifying if the Active and Standby Hosts are Operational

Perform the following to determine if the hosts are operational.

Step 1 Check the HA role on the host.

Step 2 Use the **appmgr show ha-role** command to view the current role of the host.

```
dcnm1# show ha-role
Active

dcnm2# show ha-role
Standby
```

Step 3 Check the VIP, using the **ip address** command.

On the Active host, both eth0 and eth1 must have two IP addresses configured, with VIP assigned as the secondary IP address; on standby host, only one IP address for both eth0 and eth1 interfaces

Step 4 Check the DCNM java process.

Use **ps -ef | grep java** command to verify the java process associated with the DCNM.

```
dcnm1# ps -ef | grep java
```
The results must show one Java process, appended with **standalone-san.xml**.

```
dcnm2# ps -ef | grep java
```
There should no be any Java process, appended with **standalone-san.xml**.

Step 5 Check the heartbeat of the DCNM hosts.

```
dcnm1# /etc/init.d/heartbeat status
heartbeat OK

dcnm2# /etc/init.d/heartbeat status
heartbeat OK
```

Step 6 Check if the database engine PostgreSQL is operational.

```
dcnm1# /etc/init.d/postgresql-9.4 status
server is running ……

dcnm2# /etc/init.d/postgresql-9.4 status
server is running ……
```

Step 7 Check the HA cluster information.

```
dcnm1# cl_status listnodes
dcnm2# cl_status listnodes
```

The two hostnames of the HA cluster will be displayed.

Step 8 Check the HA heartbeat status.

```
dcnm1# cl_status nodestatus <hostname>
dcnm2# cl_status nodestatus <hostname>
```

If this command returns “active”, the heartbeat on the host is OK.

If the command returns “dead”, the heartbeat on the host is not running or not recognized.

Verifying HA Database Synchronization

Perform the following to verify if the databases synchronization on both hosts is in progress.

When running DCNM Native HA, both the host database must be operational, one host as Active and another host as Standby. Any changes made in the Active database must synchronize with the Standby database in real time.

To verify if the database is synchronizing, use **ps -ef | grep post** command.

```
dcnm1# ps -ef | grep post
postgres: wal sender process postgres 172.23.244.222(40826) streaming 0/9A846C04

dcnm2# ps -ef | grep post
postgres: wal receiver process   streaming 0/9A84E00
```

Resolving HA Status Failure condition

Perform the following to resolve if the HA status check results in failure.

Step 1 Logon to Cisco DCNM Web UI.

Step 2 Navigate to **Administration > Native HA**.

Click the **Test** icon.

Check if there are errors. Click **Detailed Logs** for more information.

Step 3 Check log file at the location.

```
/usr/local/cisco/dcm/fm/logs/fms_ha.log
```

There should be some log messages indicating why the HA status is Failed.

Step 4 Verify if Standby host is running is operational.

See Verifying if the Active and Standby Hosts are Operational, page 5-6, for more information. Check is any applications are not operational.

Generally, the HA status shows Failed due to Standby database being down or rejected connection.

If the connection to standby database is rejected, the HA status shows as Failed. Check the file located at:

```
/usr/local/cisco/dcm/db/data/pg_hba.conf
```

The configuration file must contain entries for all IP addresses listed on active host **ip address**.

If not, we recommend that you contact the Technical Support for further assistance.

Step 5 If Standby database is completely down, see Bringing up Database on Standby Host, page 5-8.

Bringing up Database on Standby Host

Normally, the database must be running on both Active or Standby host, regardless of DCNM being operational or stopped. However, the database could be down mostly because of the initial database synchronization failure.

Perform the following to bring up the database on the Standby host.

Step 1 Start the Standby database, using the **/etc/init.d/postgresql-9.4 start** command.

Step 2 If the return value is PostgreSQL 9.4 started successfully, the Standby database is OK. The HA status shows OK within a few minutes.

If the database is not started successfully, the database files may be corrupted. This condition occurs due to initial synchronization failure. In such a condition, navigate to the located at:

```
/usr/local/cisco/dcm/db/replication
```

Step 3 Check for the file **pgsql-standby-backup.tgz**.

If the file exists, perform the following to restore database files, and start database again:.

a. Enter the **ps -ef | grep post** command and ensure that the Postgres process is not running.

b. If the Postgres process is running, stop by using the **kill <pid>** command.

c. Remove all the database files by using the following commands:

```
cd /usr/local/cisco/dcm/db
rm -rf data/*
```

d. Restore the database files from the backup by using **tar xzf replication/pgsql-standby-backup.tgz data** command.

e. Restart the database by using the **/etc/init.d/postgresql-9.4 start** command.

Check if the database has started successfully.

CHAPTER 6

Cisco DCNM-SAN Overview

This chapter provides an overview of the basic Cisco DCNM-SAN components and includes the following sections:

DCNM-SAN Server

DCNM-SAN Server is a platform for advanced MDS monitoring, troubleshooting, and configuration capabilities. DCNM-SAN Server provides centralized MDS management services and performance monitoring. SNMP operations are used to efficiently collect fabric information.

Cisco DCNM Release 10.0(x) supports the Cisco DCNM Server on these 64-bit operating systems:

- Microsoft Windows 2008 R2 SP1
- Microsoft Windows 2008 Standalone SP2
- Microsoft Windows 2012 R2
- Red Hat Enterprise Linux Release 6.3, 6.4, 6.6 and 7.0
- OVA and ISO with integrated operating system

Cisco DCNM Release 10.0(x) supports the running of the Cisco DCNM server on the following hypervisors:

- VMware ESXi 5.1
- VMware vCenter 5.1
- VMware ESXi 5.5
- VMware vCenter 5.5

- VMWare ESXi 6.0
- VMware vCenter 6.0

Each computer configured as a Cisco DCNM-SAN Server can monitor multiple Fibre Channel SAN fabrics. Up to 16 clients (by default) can connect to a single Cisco DCNM-SAN Server concurrently. The Cisco DCNM-SAN Clients can also connect directly to an MDS switch in fabrics that are not monitored by a Cisco DCNM-SAN Server, which ensures that you can manage any of your MDS devices from a single console.

DCNM-SAN Client

Cisco DCNM-SAN Client is a Java and SNMP-based network fabric and device management tool with a GUI that displays real-time views of your network fabric, including Cisco Nexus 5000 Series switches, Cisco MDS 9000 Family switches and third-party switches, hosts, and storage devices.

DCNM-SAN Client provides Fibre Channel troubleshooting tools, in addition to complete configuration and status monitoring capabilities for Cisco MDS 9000 Family switches and Cisco Nexus 5000 Series switches. You can use these health and configuration analysis tools on the MDS 9000 Family switch or Cisco Nexus 5000 Series switch to perform Fibre Channel ping and traceroute.

Fabric Manager Release 4.1(1b) and later releases provide a multilevel security system by adding a server admin role that allows access to limited features. The configuration capabilities of a server admin is limited to configuring FlexAttach and relevant data. Advanced mode option is available only for network administrators and provides all of the DCNM-SAN features, including security, IVR, iSCSI, and FICON.

Device Manager

Device Manager provides a graphical representation of a Cisco MDS 9000 Family switch chassis, Cisco Nexus 5000 Series switch chassis, or Cisco Nexus 7000 Series switch chassis (FCoE only) along with the installed switching modules, the supervisor modules, the status of each port within each module, the power supplies, and the fan assemblies.

The tables in the DCNM-SAN Information pane basically correspond to the dialog boxes that appear in Device Manager. However, while DCNM-SAN tables show values for one or more switches, a Device Manager dialog box shows values for a single switch. Device Manager also provides more detailed information for verifying or troubleshooting device-specific configuration than DCNM-SAN.

Device Manager provides two views: Device View and Summary View. Use Summary View to monitor interfaces on the switch. Use Device View to perform switch-level configurations including the following configurations:

- Configuring virtual Fibre Channel interfaces
- Configuring Fibre Channel over Ethernet (FCoE) features
- Configuring zones for multiple VSANs
- Managing ports, PortChannels, and trunking
- Managing SNMPv3 security access to switches
- Managing CLI security access to the switch
- Managing alarms, events, and notifications
- Saving and copying configuration files and software image

- Viewing hardware configuration
- Viewing chassis, module, port status, and statistics

DCNM Web Client

With DCNM Web Client you can monitor Cisco MDS switch events, performance, and inventory from a remote location using a web browser.

- Performance Manager Summary reports—The Performance Manager summary report provides a high-level view of your network performance. These reports list the average and peak throughput and provides hot-links to additional performance graphs and tables with additional statistics. Both tabular and graphical reports are available for all interconnections monitored by Performance Manager.
- Performance Manager drill-down reports—Performance Manager can analyze daily, weekly, monthly and yearly trends. You can also view the results for specific time intervals using the interactive zooming functionality. These reports are only available if you create a collection using Performance Manager and start the collector.
- Zero maintenance database for statistics storage—No maintenance is required to maintain Performance Manager's round-robin database, because its size does not increase over time. At prescribed intervals the oldest samples are averaged (rolled-up) and saved. A full two days of raw samples are saved for maximum resolution. Gradually the resolution is reduced as groups of the oldest samples are rolled up together.

Performance Manager

The primary purpose of DCNM-SAN is to manage the network. A key management capability is network performance monitoring. Performance Manager, which is part of DCNM server, gathers network device statistics historically and provides this information graphically using a web browser. Performance Manager presents recent statistics in detail and older statistics in summary. Performance Manager also integrates with external tools such as Cisco Traffic Analyzer.

Performance Manager has three operational stages:

- Definition—The Flow Wizard sets up flows in the switches.
- Collection—The Web Server Performance Collection screen collects information on desired fabrics.
- Presentation—Generates web pages to present the collected data through DCNM-SAN Web Server.

Performance Manager can collect statistics for ISLs, hosts, storage elements, and configured flows. Flows are defined based on a host-to-storage (or storage-to-host) link. Performance Manager gathers statistics from across the fabric based on collection configuration files. These files determine which SAN elements and SAN links Performance Manager gathers statistics for. Based on this configuration, Performance Manager communicates with the appropriate devices (switches, hosts, or storage elements) and collects the appropriate information at fixed five-minute intervals.

Authentication in DCNM-SAN Client

Administrators launch DCNM-SAN Client and select the seed switch that is used to discover the fabric. The user name and password are passed to DCNM-SAN Server and are used to authenticate to the seed switch. If this user name and password are not a recognized SNMP user name and password, either

DCNM-SAN Client or DCNM-SAN Server opens a CLI session to the switch (SSH or Telnet) and retries the user name and password pair. If the user name and password are recognized by the switch in either the local switch authentication database or through a remote AAA server, then the switch creates a temporary SNMP user name that is used by DCNM-SAN Client and DCNM-SAN Server.

Cisco Traffic Analyzer

Cisco Traffic Analyzer provides real-time analysis of SPAN traffic or analysis of captured traffic through a Web browser user interface. Traffic encapsulated by one or more Port Analyzer Adapter products can be analyzed concurrently with a single workstation running Cisco Traffic Analyzer, which is based on ntop, a public domain software enhanced by Cisco for Fibre Channel traffic analysis.

Cisco Traffic Analyzer monitors round-trip response times, SCSI I/Os per second, SCSI read or traffic throughput and frame counts, SCSI session status, and management task information. Additional statistics are also available on Fibre Channel frame sizes and network management protocols.

Network Monitoring

DCNM-SAN provides extensive SAN discovery, topology mapping, and information viewing capabilities. DCNM-SAN collects information on the fabric topology through SNMP queries to the switches connected to it. DCNM-SAN recreates a fabric topology, presents it in a customizable map, and provides inventory and configuration information in multiple viewing options such as fabric view, device view, summary view, and operation view.

Once DCNM-SAN is invoked, a SAN discovery process begins. Using information polled from a seed Cisco MDS 9000 Family switch, including Name Server registrations, Fibre Channel Generic Services (FC-GS), Fabric Shortest Path First (FSPF), and SCSI-3, DCNM-SAN automatically discovers all devices and interconnects on one or more fabrics. All available switches, host bus adapters (HBAs), and storage devices are discovered. The Cisco MDS 9000 Family switches use Fabric-Device Management Interface (FMDI) to retrieve the HBA model, serial number and firmware version, and host operating-system type and version discovery without host agents. DCNM-SAN gathers this information through SNMP queries to each switch. The device information discovered includes device names, software revision levels, vendor, ISLs, PortChannels, and VSANs.

Performance Monitoring

DCNM-SAN and Device Manager provide multiple tools for monitoring the performance of the overall fabric, SAN elements, and SAN links. These tools provide real-time statistics as well as historical performance monitoring.

Real-time performance statistics are a useful tool in dynamic troubleshooting and fault isolation within the fabric. Real-time statistics gather data on parts of the fabric in user-configurable intervals and display these results in DCNM-SAN and Device Manager.

Device Manager provides an easy tool for monitoring ports on the Cisco MDS 9000 Family switches. This tool gathers statistics at a configurable interval and displays the results in tables or charts. These statistics show the performance of the selected port in real-time and can be used for performance monitoring and troubleshooting. For a selected port, you can monitor any of a number of statistics including traffic in and out, errors, class 2 traffic, and FICON data. You can set the polling interval from ten seconds to one hour, and display the results based on a number of selectable options including absolute value, value per second, and minimum or maximum value per second.

Configuring Cisco DCNM-SAN Server

This chapter describes Cisco DCNM-SAN Server, which is a platform for advanced MDS monitoring, troubleshooting, and configuration capabilities. No additional software needs to be installed. The server capabilities are an integral part of the Cisco DCNM-SAN software.

This chapter contains the following sections:

Information About Cisco DCNM-SAN Server

Install Cisco DCNM-SAN Server on a computer that you want to provide centralized MDS management services and performance monitoring. SNMP operations are used to efficiently collect fabric information.

Cisco DCNM Release 10.0(x) supports the Cisco DCNM Server on these 64-bit operating systems:

- Microsoft Windows 2008 R2 SP1
- Microsoft Windows 2008 Standalone SP2
- Microsoft Windows 2012 R2
- Red Hat Enterprise Linux Release 6.3, 6.4, 6.6 and 7.0
- OVA and ISO with integrated operating system

Cisco DCNM Release 10.0(x) supports the running of the Cisco DCNM server on the following hypervisors:

- VMware ESXi 5.1
- VMware vCenter 5.1
- VMware ESXi 5.5
- VMware vCenter 5.5

- VMWare ESXi 6.0
- VMware vCenter 6.0

Each computer configured as a Cisco DCNM-SAN Server can monitor multiple Fibre Channel SAN fabrics. Up to 16 clients (by default) can connect to a single Cisco DCNM-SAN Server concurrently. The Cisco DCNM-SAN Clients can also connect directly to an MDS switch in fabrics that are not monitored by a Cisco DCNM-SAN Server, which ensures you can manage any of your MDS devices from a single console.

DCNM-SAN Server Features

Cisco DCNM-SAN Server has the following features:

- **Multiple fabric management**— DCNM-SAN Server monitors multiple physical fabrics under the same user interface. This facilitates managing redundant fabrics. A licensed DCNM-SAN Server maintains up-to-date discovery information on all configured fabrics so device status and interconnections are immediately available when you open the DCNM-SAN Client.
- **Continuous health monitoring—**MDS health is monitored continuously, so any events that occurred since the last time you opened the DCNM-SAN Client are captured.
- **Roaming user profiles**—The licensed DCNM-SAN Server uses the roaming user profile feature to store your preferences and topology map layouts on the server, so that your user interface will be consistent regardless of what computer you use to manage your storage networks.

Note You must have the same release of Cisco DCNM-SAN Client and Cisco DCNM-SAN Server.

Note You will not be able to manage a SAN fabric if the DCNM-SAN Server is going through a IP NAT firewall to access the SAN fabric. All the IP addresses that are discovered in a SAN fabric must be directly reachable by the DCNM-SAN Server.

Licensing Requirements For Cisco DCNM-SAN Server

When you first install Cisco DCNM-SAN, the basic unlicensed version of Cisco DCNM-SAN Server is installed with it. You get a 30-day trial license with the product. However, trial versions of the licensed features such as Performance Manager, remote client support, and continuously monitored fabrics are available. To enable the trial version of a feature, you run the feature as you would if you had purchased the license. You see a dialog box explaining that this is a demo version of the feature and that it is enabled for a limited time.

To get the licensed version after 30 days, you need to buy and install the Cisco DCNM-SAN Server package. You need to get either a switch based FM_SERVER_PKG license file and install it on your switches, or you need to get DCNM server based license files and add them to your server. Please go to **Administration > Licenses** on the DCNM Web Client, or go to the **license files** tab of the DCNM-SAN Client control panel to find the license files. You can assign the licenses to the switches through either the **Administration > Licenses** window on the DCNM Web Client or the **license assignment** tab of the DCNM-SAN Client control panel.

Installing and Configuring Cisco DCNM-SAN Server

Note Prior to running Cisco DCNM-SAN Server, you should create a special Cisco DCNM-SAN administrative user on each switch in the fabric or on a remote AAA server. Use this user to discover your fabric topology.

DETAILED STEPS

Step 1 Install Cisco DCNM-SAN Client and Cisco DCNM-SAN Server on your workstation. See the "Installing Cisco DCNM-SAN Server" section on page 7-3.

Step 2 Log in to DCNM-SAN.

Step 3 Set Cisco DCNM-SAN Server to continuously monitor the fabric. See the "Managing a Cisco DCNM-SAN Server Fabric" section on page 7-4.

Step 4 Repeat Step 2 through Step 3 for each fabric that you want to manage through Cisco DCNM-SAN Server.

Step 5 Install DCNM-SAN Web Server. See the "Verifying Performance Manager Collections" section on page 7-4.

Step 6 Verify Performance Manager is collecting data. See the "Verifying Performance Manager Collections" section on page 7-4.

Installing Cisco DCNM-SAN Server

When you firsts install Cisco DCNM, the basic version of the Cisco DCNM-SAN Server (unlicensed) is installed with it. After you click the DCNM-SAN icon, a dialog box opens and you can enter the IP address of a computer running the Cisco DCNM-SAN Server component. If you do not see the Cisco DCNM-SAN Server IP address text box, click **Options** to expand the list of configuration options. If the server component is running on your local machine, leave **localhost** in that field. If you try to run DCNM-SAN without specifying a valid server, you are prompted to start the Cisco DCNM-SAN Server locally.

From Release 10.0(1), Cisco DCNM has supported to choose from the following options during installation. Based on the option you select, the application will be installed:

- DCNM Web Client
- DCNM SAN + LAN Client

To download the software from Cisco.com, go to the following website:

http://cisco.com/cgi-bin/tablebuild.pl/mds-fm

For detailed Cisco DCNM installation steps, please refer to

Cisco DCNM Installation Guide, Release 10.0(x).

Data Migration in Cisco DCNM-SAN Server

The database migration should be limited to the existing database. Data collision can occur when you merge the data between the several databases.

When you upgrade a non federation mode database to a federation mode database for the first time, the cluster sequence table is filled with the values larger than the corresponding ones in the sequence table and conforming to the cluster sequence number format for that server ID.

Verifying Performance Manager Collections

Once Performance Manager collections have been running for five or more minutes, you can verify that the collections are gathering data by choosing **Performance Manager > Reports** in DCNM-SAN. You see the first few data points gathered in the graphs and tables.

Managing a Cisco DCNM-SAN Server Fabric

You can continuously manage a Cisco DCNM-SAN Server fabric, whether or not a client has that fabric open. A continuously managed fabric is automatically reloaded and managed by Cisco DCNM-SAN Server whenever the server starts.

Selecting a Fabric to Manage Continuously

DETAILED STEPS

Step 1 Choose **Server > Admin**.

You see the Control Panel dialog box with the Fabrics tab ope.

Note The Fabrics tab is only accessible to network administrators.

Note You can preconfigure a user name and password to manage fabrics. In this instance, you should use a local switch account, not a TACACS+ server.

Step 2 Choose one of the following Admin options:

a. **Manage Continuously**—The fabric is automatically managed when Cisco DCNM-SAN Server starts and continues to be managed until this option is changed to Unmanage.

b. **Manage**—The fabric is managed by Cisco DCNM-SAN Server until there are no instances of DCNM-SAN viewing the fabric.

c. **Unmanage—Cisco DCNM-SAN Server stops managing this fabric.**

Step 3 Click **Apply**.

Note If you are collecting data on these fabrics using Performance Manager, you should now configure flows and define the data collections.

Cisco DCNM-SAN Server Properties File

The Cisco DCNM-SAN Server properties file (**MDS 9000\server.properties**) contains a list of properties that determine how the Cisco DCNM-SAN Server will function. You can edit this file with a text editor, or you can set the properties through the DCNM-SAN Web Services GUI, under the Admin tab.

Note As of Cisco NX-OS Release 4.1(1b) and later, you can optionally encrypt the password in the server.properties and the AAA.properties files.

The server properties file contains these nine general sections:

- **GENERAL**—Contains the general settings for the server.
- **SNMP SPECIFIC**—Contains the settings for SNMP requests, responses, and traps.
- **SNMP PROXY SERVER SPECIFIC**—Contains the settings for SNMP proxy server configuration and TCP port designation.
- **GLOBAL FABRIC**—Contains the settings for fabrics, such as discovery and loading.
- **CLIENT SESSION**—Contains the settings for DCNM-SAN Clients that can log into the server.
- **EVENTS**—Contains the settings for syslog messages.
- **PERFORMANCE CHART**—Contains the settings for defining the end time to generate a Performance Manager chart.
- **EMC CALL HOME**—Contains the settings for the forwarding of traps as XML data using e-mail, according to EMC specifications.
- **EVENT FORWARD SETUP**—Contains the settings for forwarding events logged by Cisco DCNM-SAN Server through e-mail.

The following server properties are added or changed in the Cisco DCNM-SAN Release 3.x and later.

SNMP Specific

- **snmp.preferTCP**—If this option is set to true, TCP is the default protocol for Cisco DCNM-SAN Server to communicate with switches. By default, this setting is **true**. For those switches that do not have TCP enabled, Cisco DCNM-SAN Server uses UDP. The advantage of this setting is the ability to designate one TCP session for each SNMP user on a switch. It also helps to reduce timeouts and increase scalability.

Note If you set this option to false, the same choice must be set in DCNM-SAN. The default value of snmp.preferTCP for DCNM-SAN is true.

Performance Chart

- **pmchart.currenttime**—Specifies the end time to generate a Performance Manager chart. This should only be used for debugging purposes.

EMC Call Home

- **server.callhome.enable**—Enables or disables EMC Call Home. By default, it is disabled.
- **server.callhome.location**—Specifies the Location parameter.
- **server.callhome.fromEmail**—Specifies the From Email list.
- **server.callhome.recipientEmail**—Specifies the recipientEmail list.
- **server.callhome.smtphost**—Specifies the SMTP host address for outbound e-mail.
- **server.callhome.xmlDir**—Specifies the path to store the XML message files.
- **server.callhome.connectType**—Specifies the method to use to remotely connect to the server.
- **server.callhome.accessType**—Specifies the method to use to establish remote communication with the server.
- **server.callhome.version**—Specifies the version number of the connection type.
- **server.callhome.routerIp**—Specifies the public IP address of the RSC router.

Event Forwarding

- **server.forward.event.enable**—Enables or disables event forwarding.
- **server.forward.email.fromAddress**—Specifies the From Email list.
- **server.forward.email.mailCC**—Specifies the CC Email list.
- **server.forward.email.mailBCC**—Specifies the BCC Email list.
- **server.forward.email.smtphost**—Specifies the SMTP host address for outbound e-mail.

Deactivation

- **deactivate.confirm=deactivate**—Specific Request for User to type a String for deactivation.

Note In a federated server environment, you should not change Cisco DCNM-SAN Server properties by modifying server.properties file. You must modify the server.properties using web client menu **Admin > Configure > Preferences**.

Modifying Cisco DCNM-SAN Server

You can modify certain Cisco DCNM-SAN Server settings without stopping and starting the server.

Changing the Cisco DCNM-SAN Server Username and Password

You can modify the username or password used to access a fabric from DCNM-SAN Client without restarting Cisco DCNM-SAN Server.

DETAILED STEPS

Step 1 Choose **Server > Admin**.

You see the Control Panel dialog box with the Fabrics tab open.

Step 2 Set the Name or Password for each fabric that you are monitoring with Cisco DCNM-SAN Server.

Step 3 Click **Apply** to save these changes.

Changing the DCNM-SAN Server Fabric Discovery Username and Password

DETAILED STEPS

Step 1 Click **Server > Admin** in Cisco DCNM-SAN.

You see the Control Panel dialog box with the Fabrics tab open.

Step 2 Click the fabrics that have updated user name and password information.

Step 3 From the Admin listbox, select **Unmanage** and then click **Apply**.

Step 4 Enter the appropriate user name and password and then click **Apply.**

For more information, see the “"Performance Manager Authentication” section on page 8-3”.

Changing the Polling Period and Fabric Rediscovery Time

Cisco DCNM-SAN Server periodically polls the monitored fabrics and periodically rediscovers the full fabric at a default interval of five cycles.You can modify these settings from DCNM-SAN Client without restarting Cisco DCNM-SAN Server.

DETAILED STEPS

Step 1 Choose **Server > Admin**.

You see the Control Panel dialog box with the Fabrics tab open.

Step 2 For each fabric that you are monitoring with Cisco DCNM-SAN Server, set the Polling Interval to determine how frequently Cisco DCNM-SAN Server polls the fabric elements for status and statistics.

Step 3 For each fabric that you are monitoring with Cisco DCNM-SAN Server, set the Rediscover Cycles to determine how often Cisco DCNM-SAN Server rediscovers the full fabric.

Step 4 Click **Apply** to save these changes.

Changing the IP Address of the Cisco DCNM-SAN & DCNM-SMIS WINDOWS Server

To change the IP address of a Cisco DCNM-SAN & DCNM-SMIS Server, follow these steps:

Detailed Steps

Step 1 Stop the Cisco DCNM-SAN and DCNM-SMIS Servers.

Step 2 Change the old IP Address with the new IP Address in the following files

- *$INSTALLDIR\jboss-as-7.2.0.Final\bin\service\sanservice.bat*
- *$INSTALLDIR\jboss-as-7.2.0.Final\standalone\configuration\standalone-san.xml(Including DB url)*
- *$INSTALLDIR\fm\conf\server.properties*

Step 3 Enter the following command to assign a new IP address.

```
run $INSTALLDIR\fm\bin\PLMapping.bat -p newipaddress 0
```

Assume $INSTALLDIR is the top directory of DCNM installation. The above command is for single server instance, where 0 is the server ID.

Step 4 Change the old IP Address with the new IP Address in the file *$INSTALLDIR\fm\conf\smis.properties*

Step 5 Start the Cisco DCNM-SAN and DCNM-SMIS Servers.

Changing the IP Address of the Cisco DCNM-SAN for Federated Windows Setup

To change the IP address of a Cisco DCNM-SAN for federated Windows OS, follow these steps:

- Changing the IP address of primary server
- Changing the IP address of secondary server

Changing the IP address of primary server

Step 1 Stop the Cisco DCNM-SAN and DCNM-SMIS Servers.

Step 2 Change the old IP Address with the new IP Address in the file $INSTALLDIR\jboss-as-7.2.0.Final\bin\service\sanservice.bat

Step 3 Change the old IP Address with the new IP Address in the file $INSTALLDIR\jboss-as-7.2.0.Final\standalone\configuration\standalone-san.xml.

Step 4 Change the old IP Address with the new IP Address in the file $INSTALLDIR\fm\conf\server.properties

Note If DB is installed locally(URL pointing to LocalHost),No DB URL change required in standalone-san.xml , server.properties .

Step 5 Enter the following command to assign a new IP address.

run $INSTALLDIR\fm\bin\PLMapping.bat -p newipaddress 0

Assume $INSTALLDIR is the top directory of DCNM installation. The above command is for primary server instance, where 0 is the server ID.

Step 6 Change the old IP Address with the new IP Address in the file $INSTALLDIR\fm\conf\smis.properties

Step 7 Start the Cisco DCNM-SAN and DCNM-SMIS Servers.

Changing the IP address of secondary server

Step 1 Stop the Cisco DCNM-SAN and DCNM-SMIS Servers.

Step 2 Change the old IP Address with the new IP Address in the file $INSTALLDIR\jboss-as-7.2.0.Final\bin\service\sanservice.bat

Step 3 Change the old IP Address with the new IP Address in the file $INSTALLDIR\jboss-as-7.2.0.Final\standalone\configuration\standalone-san.xml

Step 4 Change the old IP Address with the new IP Address in the file $INSTALLDIR\fm\conf\server.properties.

Step 5 Change DB URL in standalone-san.xml, server.properties, postgresql.cfg.xml\ oracle.cfg.xml files, if there is ipaddress change in primary server.

postgresql.cfg.xml\ oracle.cfg.xml can be found under $INSTALLDIR\jboss-as-7.2.0.Final\standalone\conf\ directory.

Step 6 Enter the following command to assign a new IP address.

run $INSTALLDIR\fm\bin\PLMapping.bat -p newipaddress 1 .

Note ServerID can be got by run $INSTALLDIR\fm\bin\PLMapping.bat -show.

Assume $INSTALLDIR is the top directory of DCNM installation. The above command 1 is the server ID.

Step 7 Change the old IP Address with the new IP Address in the file $INSTALLDIR\fm\conf\smis.properties

Step 8 Start the Cisco DCNM-SAN and DCNM-SMIS Servers.

Changing the IP Address of the Cisco DCNM-SAN & DCNM-SMIS LINUX Server

To change the IP address of a Cisco DCNM-SAN & DCNM-SMIS Server, follow these steps:

Detailed Steps

Step 1 Stop the Cisco DCNM-SAN and DCNM-SMIS Servers.

Step 2 Change the old IP Address with the new IP Address in the following files:

- *$INSTALLDIR/jboss-as-7.2.0.Final/bin/init.d/sanservice.sh*
- */etc/init.d/FMServer*
- *$INSTALLDIR/jboss-as-7.2.0.Final/standalone/configuration/standalone-san.xml (Including DB url)*
- *$INSTALLDIR/fm/conf/server.properties*

Step 3 Enter the following command to assign a new IP address.

```
run $INSTALLDIR/fm/bin/PLMapping.sh -p newipaddress 0
```

Assume $INSTALLDIR is the top directory of DCNM installation. The above command is for single server instance, where 0 is the server ID.

Step 4 Change the old IP Address with the new IP Address in the file *$INSTALLDIR/fm/conf/smis.properties.*

Note If this is a DCNM virtual appliance (OVA/ISO) deployed without any Fabric enhancements, update the property DCNM_IP_ADDRESS in the file */root/packaged-files/properties/installer.properties* with the new IP Address.

Step 5 Start the Cisco DCNM-SAN and DCNM-SMIS Servers.

Using Device Aliases or FC Aliases

You can change whether DCNM-SAN uses FC aliases or global device aliases from DCNM-SAN Client without restarting Cisco DCNM-SAN Server.

DETAILED STEPS

Step 1 Choose **Server > Admin**.

You see the Control Panel dialog box with the Fabrics tab open.

Step 2 For each fabric that you are monitoring with Cisco DCNM-SAN Server, check or uncheckthe **FC Alias** check box.

If you check the **FC Alias** checkbox, DCNM-SAN will use FC Alias from DCNM-SAN Client. If you uncheck the **FC Alias** checkbox, DCNM-SAN will use global device alias from DCNM-SAN Client.

Step 3 Click **Apply** to save these changes.

Configuring Security Manager

The security at Fabric Manager Server level control access to different features of the Fabric Manager. The existing security controls in the Fabric Manager allows a user to continue even after many unsuccessful login attempts. With the new security manager, the Fabric Manager will perform a lock-out for the specific user after a specified number of unsuccessful login attempts. System administrators will be able to generate a report of login attempts.

To see the number of failed login attempts, in the Fabric Manager Control Panel, click **Local FM Users**.

You see the control panel.

Server Federation

Server Federation is a distributed system that includes a collection of intercommunicated servers or computers that is utilized as a single, unified computing resource. With Cisco DCNM-SAN Server Federation, you can communicate with multiple servers together in order to provide scalability and easy manageability of data and programs running within the federation. The core of server federation includes several functional units such as Cisco DCNM-SAN Server, embedded web servers, database and DCNM-SAN Client that accesses the servers.

The Cisco DCNM-SAN Server in the federation uses the same database to store and retrieve data. The database is shared among different servers to share common information. A DCNM-SAN Client or DCNM-SAN Web Client can open fabrics from the Cisco DCNM-SAN Server using the mapping table. A fabric can be moved from one logical server to another. A logical server also can be moved from one physical machine to another machine.

Restrictions

- You cannot upgrade more than one Cisco DCNM-SAN Server in an existing federation. If you choose to do so, you may not be able to migrate the Performance Manager statistics and other information on that server.
- You may require to synchronize the time on all the DCNM-SAN Servers in a federated server environment.

Mapping Fabric ID to Server ID

The IP address of the physical server will be mapped to the server ID during the installation of the Cisco DCNM-SAN Server whenever the IP address of the physical server is changed, you need to map the IP address to the server ID using the PLMapping script provided with the Cisco DCNM-SAN Server. Whenever the you open or discover a fabric, the fabric ID will be mapped to the server ID . You can move a fabric to a different server ID using the control panel.

DETAILED STEPS

Step 1 Choose **Server > Admin**.

You see the Control Panel.

Step 2 Select the fabric that you want to move to a different server and then click **Move**.

You see the Move Fabric dialog box.

Step 3 You see the fabrics that you selected in the Fabrics to Move list box. From the **Move To Server** drop-down list select the server you want to move the fabric to.

Step 4 Click **Move**.

Opening the Fabric on a Different Server

DETAILED STEPS

Step 1 Choose **Server > Admin**.

You see the Control Panel.

Step 2 Click **Discover**.

You see the Discover New Fabric dialog box.

Step 3 In the Seed Switch list box, enter the IP Address of the seed switch.

Step 4 In the User Name field, enter the username.

Step 5 In the password field, enter the password.

Step 6 From the Auth-Privacy drop-down list, choose the privacy protocol you want to apply.

Step 7 To open the selected fabric in a different server, select the server ID from the Server drop-down list.

Step 8 Click **Discover**.

Note You may receive an error message when you discover a fabric in a federation while another Cisco DCNM-SAN Server is joining the federation. You can discover the fabric on after the installation or upgradation is complete.

Viewing the Sessions in a Federation

DETAILED STEPS

Step 1 Choose **Server > Admin**.

Step 2 Click the **Connected Clients** tab.

You see the Control Panel.

Viewing the Servers in a Federation

DETAILED STEPS

Step 1 Choose **Server** > **Admin**.

Step 2 Click the **Servers** tab.

You see the Control Panel.

Discover Devices Managed by SVI

Step 1 Log on to the DCNM Web Client.

Step 2 Select **Admin>Server Properties**.

Step 3 Scroll down to the **GENERAL->DATA SOURCE FABRIC** section.

Step 4 Set the **fabric.managementIpOverwrite** property to **false**.

Step 5 Click **Apply**.

Step 6 Restart the DCNM service.

Note If you experiences technical issues using DCNM, you must restart the database service manually.

Step 7 Delete any previously discovered switch that incorrectly shows the **mgmt0** IP address.

Step 8 Retry the discovery.

Note Each SVI switch must be discovered separately.

Additional References

- Server Federation is a licensed feature. For more information on Cisco DCNM-SAN Server Licensing, see *Cisco MDS 9000 Family NX-OS Licensing Guide*.
- For more information on deploying Cisco DCNM-SAN Server in a federation, see *Cisco Fabric Manager Server Federation Deployment Guide*.

Configuring Authentication in Cisco DCNM-SAN

This chapter describes the interdependent software components in Cisco DCNM-SAN that communicate with the switches, authentication steps and the best practices for setting up your fabric and components for authentication.

This chapter contains the following sections:

Information About Cisco DCNM-SAN Authentication

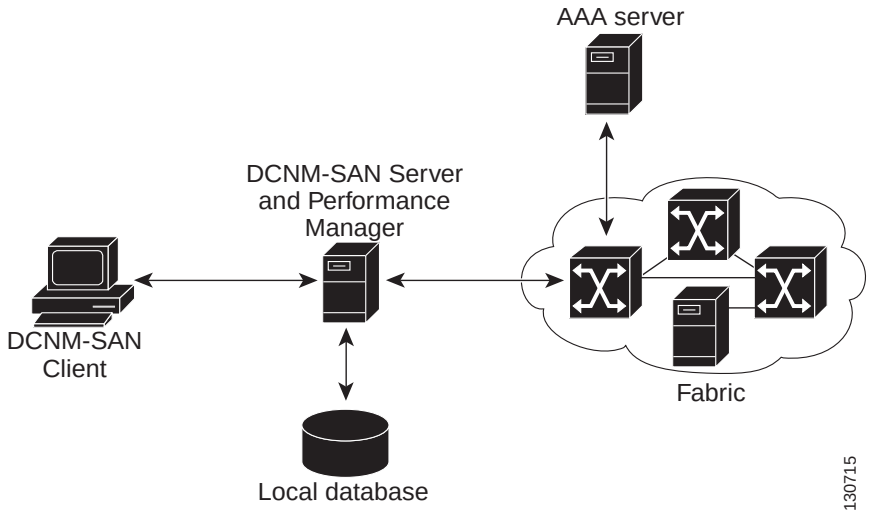
Cisco DCNM-SAN contains multiple components that interact to manage a fabric.

These components include:

- Cisco DCNM-SAN Client
- Cisco DCNM-SAN Server
- Performance Manager
- Interconnected fabric of Cisco MDS 9000 switches and storage devices
- AAA server (optional)

Figure 8-1 shows an example configuration for these components.

Figure 8-1 Cisco DCNM-SAN Authentication Example



Administrators launch Cisco DCNM-SAN Client and select the seed switch that is used to discover the fabric. The user name and password used are passed to Cisco DCNM-SAN Server and used to authenticate to the seed switch. If this user name and password are not a recognized SNMP user name and password, either Cisco DCNM-SAN Client or Cisco DCNM-SAN Server opens a CLI session to the switch (SSH or Telnet) and retries the user name and password pair. If the user name and password are recognized by the switch in either the local switch authentication database or through a remote AAA server, then the switch creates a temporary SNMP user name that is used by Cisco DCNM-SAN Client and server.

Note You may encounter a delay in authentication if you use a remote AAA server to authenticate Cisco DCNM-SAN or Device Manager.

Note You must allow CLI sessions to pass through any firewall that exists between Cisco DCNM-SAN Client and Cisco DCNM-SAN Server.

Note We recommend that you use the same password for the SNMPv3 user name authentication and privacy passwords as well as the matching CLI user name and password.

Best Practices for Discovering a Fabric

Cisco DCNM-SAN Server monitors multiple physical fabrics under the same user interface. This facilitates managing redundant fabrics. A licensed Cisco DCNM-SAN Server maintains up-to-date discovery information on all configured fabrics so device status and interconnections are immediately available when you launch Cisco DCNM-SAN Client.

Caution If the Cisco DCNM-SAN Server's CPU usage exceeds 50 percent, it is recommended that you switch to a higher CPU-class system.

We recommend that you use these best practices for discovering your network and setting up Performance Manager. This ensures that Cisco DCNM-SAN Server has a complete view of the fabric. Subsequent Cisco DCNM-SAN Client sessions can filter this complete view based on the privileges of the client logging in. For example, if you have multiple VSANs in your fabric and you create users that are limited to a subset of these VSANs, you want to initiate a fabric discovery through Cisco DCNM-SAN Server using a network administrator or network operator role so that Cisco DCNM-SAN Server has a view of all the VSANs in the fabric. When a VSAN-limited user launches Cisco DCNM-SAN Client, that user sees only the VSANs they are allowed to manage.

Note Cisco DCNM-SAN Server should always monitor fabrics using a local switch account, do not use a AAA (RADIUS or TACACS+) server. You can use a AAA user account to log into the clients to provision fabric services.

Note Even when remote AAA server authentication is enabled on the switch, use the local switch account that is not defined in the remote AAA server for fabric discovery. In other words, when a user is not found in the remote AAA server, then local switch user authentication will be allowed by the switch for SNMPv3 clients like DCNM.

Setting Up Discovery for a Fabric

DETAILED STEPS

Step 1 Create a special Cisco DCNM-SAN administrative user name in each switch on your fabric with network administrator or network operator roles. Or, create a special Cisco DCNM-SAN administrative user name in your AAA server and set every switch in your fabric to use this AAA server for authentication.

Step 2 Verify that the roles used by this Cisco DCNM-SAN administrative user name are the same on all switches in the fabric and that this role has access to all VSANs.

Step 3 Launch Cisco DCNM-SAN Client using the Cisco DCNM-SAN administrative user. This step ensures that your fabric discovery includes all VSANs.

Step 4 Set Cisco DCNM-SAN Server to continuously monitor the fabric.

Step 5 Repeat Step 4 for each fabric that you want to manage through Cisco DCNM-SAN Server.

Performance Manager Authentication

Performance Manager uses the user name and password information stored in the Cisco DCNM-SAN Server database. If this information changes on the switches in your fabric while Performance Manager is running, you need to update the Cisco DCNM-SAN Server database and restart Performance Manager. Updating the Cisco DCNM-SAN Server database requires removing the fabric from Cisco DCNM-SAN Server and rediscovering the fabric.

DETAILED STEPS

Step 1 Click **Server > Admin** in Cisco DCNM-SAN.

You see the Control Panel dialog box with the Fabrics tab open.

Step 2 Click the fabrics that have updated user name and password information.

Step 3 From the Admin listbox, choose **Unmanage** and then click **Apply**.

Step 4 Enter the appropriate user name and password and then click **Apply.**

Step 5 From the Admin listbox, choose **Manage** and then click **Apply**.

Step 6 To rediscover the fabric, click **Open** tab and check the check box(es) next to the fabric(s) you want to open in the Select column.

Step 7 Click **Open** to rediscover the fabric. Cisco DCNM-SAN Server updates its user name and password information.

Step 8 Repeat Step 3 through Step 7 for any fabric that you need to rediscover.

Step 9 Choose **Performance > Collector > Restart** to restart Performance Manager and use the new user name and password.

Cisco DCNM-SAN Web Client Authentication

Cisco DCNM-SAN Web Server does not communicate directly with any switches in the fabric. Cisco DCNM-SAN Web Server uses its own user name and password combination that is either stored locally or stored remotely on an AAA server.

We recommend that you use a RADIUS or TACACS+ server to authenticate users in Cisco DCNM-SAN Web Server.

DETAILED STEPS

Step 1 Launch Cisco DCNM-SAN Web Client.

Step 2 Choose **Admin > Management Users > Remote AAA** to update the authentication used by Cisco DCNM-SAN Web Client.

Step 3 Set the authentication mode attribute to **radius**.

Step 4 Set the RADIUS server name, shared secret, authentication method, and ports used for up to three RADIUS servers.

Step 5 Click **Modify** to save this information.

Step 1 Launch Cisco DCNM-SAN Web Client.

Step 2 Choose **Admin > Management Users > Remote AAA** to update the authentication used by Cisco DCNM-SAN Web Client.

Step 3 Set the authentication mode attribute to **tacacs**.

Step 4 Set the TACACS+ server name, shared secret, authentication method, and port used for up to three TACACS+ servers.

Step 5 Click **Modify** to save this information.

Note Cisco DCNM-SAN does not support SecureID because it is not compatible with SNMP authentication. Cisco DCNM-SAN uses the same login credentials for all the switches in a fabric. Since SecureID cannot be used more than once for authentication, Cisco DCNM-SAN will not be able to establish a connection to the second switch using a SecureID.

Configuring Cisco DCNM-SAN Client

This chapter describes about the Cisco DCNM-SAN Client, which is a java-based GUI application that provides access to the Cisco DCNM-SAN applications from a remote workstation.

This chapter contains the following sections:

Information About DCNM-SAN Client

Cisco DCNM-SAN is a Java and SNMP-based network fabric and device management tool with a GUI that displays real-time views of your network fabric, including Cisco Nexus 5000 Series switches, Cisco MDS 9000 Family and third-party switches, hosts, and storage devices.

In addition to complete configuration and status monitoring capabilities for Cisco MDS 9000 Family switches and Cisco Nexus 5000 Series switches, Cisco DCNM-SAN Client provides Fibre Channel troubleshooting tools. You can use these health and configuration analysis tools on the MDS 9000 Family switch or Cisco Nexus 5000 Series switch to perform Fibre Channel ping and traceroute.

Cisco DCNM-SAN Release 4.1(1b) and later provides multilevel security system by adding a *server admin* role that allows access to limited features. The configuration capabilities of a *server admin* is limited to FlexAttach and relevant data.

Note You must use the same release of Cisco DCNM-SAN Client and Cisco DCNM-SAN Server.

Cisco DCNM-SAN Advanced Mode

Advanced mode is enabled by default and provides the full suite of Cisco DCNM-SAN features, including security, IVR, iSCSI, and FICON. To simplify the user interface, from the list box in the upper right corner of the Cisco DCNM-SAN Client, choose **Simple**. In simple mode, you can access basic MDS 9000 features such as VSANs, zoning, and configuring interfaces. Advanced mode option is not available for *server admin* role.

Cisco DCNM-SAN Client Quick Tour: Server Admin Perspective

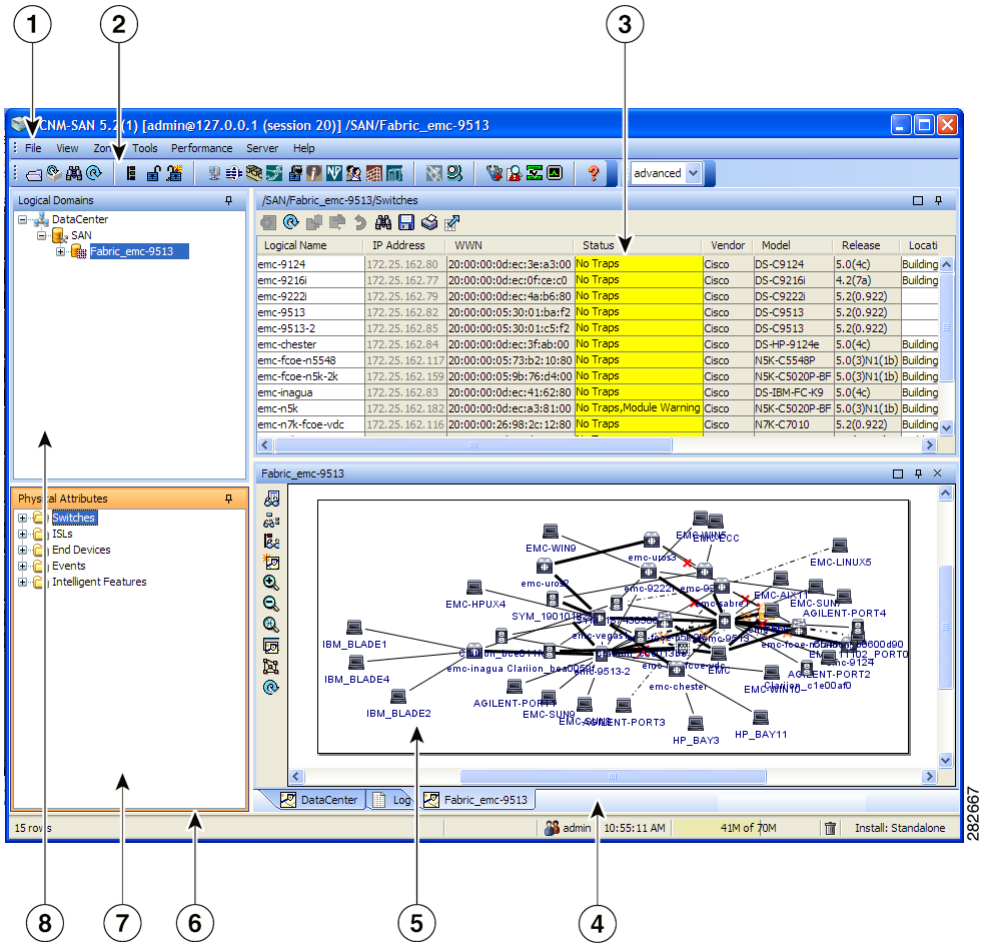
Cisco DCNM-SAN provides a multilevel security system by adding a *server admin* role that allows access only to limited features. The configuration capabilities of a *server admin role* is limited to FlexAttach and relevant data. The *server admin* can pre-configure SAN for new servers, move a server to another port on the same NPV device or another NPV device and replace a failed server onto the same port without involving the SAN administrator. The *server role admin* will not be able to manage Cisco DCNM-SAN users or connected clients.

Cisco DCNM-SAN provides a much improved user interface by including movable and dockable panes to let users arrange the Physical Attributes pane, Logical Domains pane, Fabric pane and Information pane according to requirements, making it easier to manage the workflow. The dockable panes are also called as dockable frames. A dockable frame can be standalone (floating), minimized or maximized. The logical, physical, information and the fabric panes can be can be collapsed and expanded as needed. These panes can also be docked at either the right side left side or to the bottom of the workspace.

Cisco DCNM-SAN Main Window

This section describes the Cisco DCNM-SAN Client interface that is specific to *server admin* users as shown in Figure 9-1.

Figure 9-1 Cisco DCNM-SAN Main Window: Server Admin Perspective



1	Menu bar—Provides access to options that are organized by menus.
2	Toolbar—Provides icons for direct access to the most commonly used options on the File, Tools, and Help menus.
3	Information pane—Displays information about whatever option is selected in the menu tree.
4	Status Bar (right side)—Shows the last entry displayed by the discovery process and the possible error message.
5	Fabric pane—Displays a map of the network fabric, including switches, hosts, and storage. It also provides tabs for displaying log and event data.
6	Status Bar (left side)—Shows short-term transient messages, such as the number of rows displayed in a table.
7	Physical Attributes pane—Displays a tree of available configuration tasks depending on the fabric, VSAN, or zone selected previously. Lists the switches in the logical selection.
8	Logical Domains pane—Displays a tree of configured SAN, fabrics and user-defined groups.

Menu Bar

The menu bar at the top of the Cisco DCNM-SAN main window provides options for managing and for controlling the display of information on the Fabric pane. *Server admin* will not have all the options that are available for *SAN admin*. The menu bar provides the following menus:

- File—Opens a new fabric, rediscovers the current fabric, locates switches, sets preferences, prints the map.
- View—Changes the appearance of the map (these options are duplicated on the Fabric pane toolbar).
- Tools—Manages the Server and configuration using the FlexAttach virtual pWWN feature.
- Help—Displays online help topics for specific dialog boxes in the Information pane.

Tool Bar

The Cisco DCNM-SAN main toolbar (specific to *server admin*) provides icons for accessing the most commonly used menu bar options as shown in Table 9-1.

Table 9-1 Cisco DCNM-SAN Client Main Toolbar

Icon	Description
	Opens switch fabric.
	Rediscovers current fabric.
	Finds in the map.
	Shows online help.

Logical Domains Pane

Use the Logical Domains pane to view fabrics and to access user-defined groups. You can expand the groups to see different user-defined groups. The non-editable groups created for each core switch contains their NPV switches.

Physical Attributes Pane

Use the Physical Attributes pane to display a tree of the options available for managing the switches in the currently selected fabric or group.

To select an option, click a folder to display the options available and then click the option. You see the table with information for the selected option in the Information pane. The Physical Attributes pane provides the following main folders:

- Switches—Views and configures hardware, system, licensing, and configuration files.
- Interfaces—Views and configures FC physical, FC logical, VFC (FCoE), Ethernet, SVC, and PortChannel interfaces.

Information Pane

Use the Information pane to display tables of information associated with the option selected from the menu tree in the Logical Domains or Physical Attributes panes. The Information pane toolbar provides buttons for performing one or more of the operations shown in Table 5-2.

Table 9-2 Information Pane Toolbar

Icons	Description
	Applies configuration changes.
	Refreshes table values.
	Copies data from one row to another.
	Pastes the data from one row to another.
	Undoes the most recent change.
	Finds a specified string in the table.
	Exports and saves information to a file.
	Prints the contents of the Information pane.
	Displays a non-editable copy of the table in the Information pane in its own window, which you can move around the screen.

Fabric Pane

Use the Fabric pane to display the graphical representation of your fabric. Table 5-1 explains the graphics you may see displayed, depending on which devices you have in your fabric.

The bottom of the Fabric pane has the following tabs:

- Fabric—When displaying multiple fabrics, each fabric has its own tab. You can switch between fabrics by clicking on their respective tabs.
- Log—Displays messages that describe Cisco DCNM-SAN operations, such as fabric discovery. .

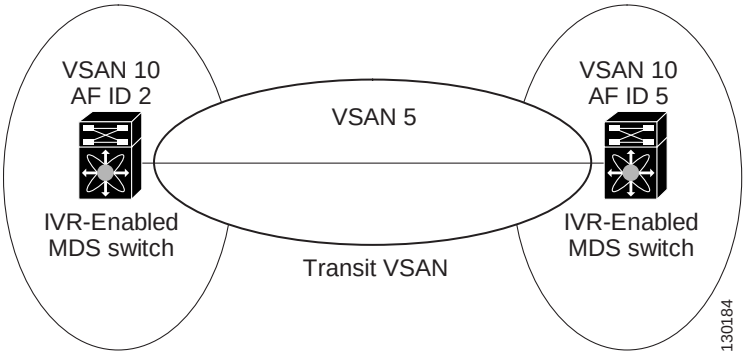
Note Fabric map display is based on what you select in the logical domain pane. When you select a fabric node, all the switches that belong to that fabric will be enabled. When you select the group node, all the switches that belong to the groups listed under that group node will be enabled. When you select only a group, all the switches that belong to the specific group will be enabled.

Note You can view information about Events using the DCNM Web Client.

Cisco DCNM-SAN Client Quick Tour: Admin Perspective

This section describes the Cisco DCNM-SAN Client interface shown in Figure 9-2.

Figure 9-2 Cisco DCNM-SAN Main Window



1	Menu bar—Provides access to options that are organized by menus.
2	Toolbar—Provides icons for direct access to the most commonly used options on the File, Tools, and Help menus.
3	Information pane—Displays information about whatever option is selected in the menu tree.
4	Status Bar (right side)—Shows the last entry displayed by the discovery process and the possible error message.
5	Fabric pane—Displays a map of the network fabric, including switches, hosts, and storage. It also provides tabs for displaying log and event data.
6	Status Bar (left side)—Shows short-term transient messages, such as the number of rows displayed in a table.
7	Physical Attributes pane—Displays a tree of available configuration tasks depending on the fabric, VSAN, or zone selected previously. Lists the switches and end devices in the logical selection.
8	Logical Domains pane—Displays a tree of configured SAN, fabrics, VSANs, and zones, and provides access to user-defined groups. The label next to the segmented VSAN indicates the number of segments.

Note You can resize each pane by dragging the boundaries between each region or by clicking the **Minimize** or **Maximize** controls.

Menu Bar

The menu bar at the top of the Cisco DCNM-SAN main window provides options for managing and troubleshooting the current fabric and for controlling the display of information on the Fabric pane. The menu bar provides the following menus:

- File—Opens a new fabric, rediscovers the current fabric, locates switches, sets preferences, prints the map, and exports the Fabric pane log.
- View—Changes the appearance of the map (these options are duplicated on the Fabric pane toolbar).
- Zone—Manages zones, zone sets, and inter-VSAN routing (IVR).
- Tools—Verifies and troubleshoots connectivity and configuration, as described in the "Cisco DCNM-SAN Troubleshooting Tools" section on page 9-35.
- Performance—Runs and configures Performance Manager and Cisco Traffic Analyzer, and generates reports.
- Server—Runs administrative tasks on clients and fabrics. Provides Cisco DCNM-SAN Server management and a **purge** command. Lists fabrics being managed.
- Help—Displays online help topics for specific dialog boxes in the Information pane.

File

The file menu provides the following options:

- Open Fabric—Opens a new switch fabric.
- Locate Switches and Devices— Uses the SNMPv2 protocol to discover devices responding to SNMP requests with the read-only community string public. You may use this feature if you want to locate other Cisco MDS 9000 switches in the subnet, but are not physically connected to the fabric.
- Rediscover—Initiates an on-demand discovery to learn recent changes from the switches and update the Cisco DCNM-SAN Client. You may use this option when Cisco DCNM-SAN Server is not in sync with switches in the fabric and you do not want to wait until the next polling cycle. The rediscover option does not delete the fabric and add it again. You may delete and add the fabric only if the rediscover option fails to update Cisco DCNM-SAN Server.
- Resync All Open Fabrics— Cisco DCNM-SAN Server forces all the fabrics to close and re-open. You may use this option when Cisco DCNM-SAN Client is not in sync with Cisco DCNM-SAN Server.
- Rediscover SCSI Targets— Initiates an on-demand discovery to learn recent changes from the SCSI target switches. You may use this option when Cisco DCNM-SAN Server is not in sync with SCSI target switches in the fabric and you do not want to wait until the next polling cycle.
- Preferences—Sets your preferences to customize the behavior of the Cisco DCNM-SAN Client.
- Import Enclosures—Imports saved enclosures.
- Export
  - Map Image—Generates and export the map to a specified location.

  - Visio—Exports the map to a Visio file.
  - Table—Exports the table data to a text file.
  - Log—Exports the log to a text file.
  - Events—Exports the events to a text file.
  - Enclosures—Exports the enclosure values to a text file.
- Print —Prints the map.
- Exit—Exit Cisco DCNM-SAN.

View

View menu provides the following options:

- Refresh Map—Refreshes the current map.
- Layout
  - Cancel—Cancels the current layout.
  - Spring—Displays the layout based on spring algorithm.
  - Quick—Quickly displays the layout when the switch has many end devices.
- Zoom
  - In—Zooms in the view.
  - Out—Zooms out the view.
  - Fit—Fits the view in the fabric pane.
- Grid—Enables the grid view.
- Overview Window—Allows you to center the Fabric pane on the area of the fabric that you want to see. This option is useful for large fabrics that cannot be displayed entirely within the Fabric pane.
- Legend—Shows all the legends used in the fabric map.
- Find in Map—Finds a device in the fabric map.

Zone

The zone menu provides the following options:

- Edit Local Full Zone Database—Allows you to create zones across multiple switches. Zones provide a mechanism for specifying access control. Zone sets are a group of zones to enforce access control in the fabric. All zoning features are available through the Edit Local Full Zone Database dialog box.
- Deactivate Zoneset—Deactivates an active zone set.
- Copy Full Zone Database—Creates a new zone set. On the Cisco MDS Family switches, you cannot edit an active zone set. However, you can copy an active zone set to create a new zone set that you can edit.
- Merge Analysis—Enables you to determine if zones will merge successfully when two Cisco MDS switches are interconnected. If the interconnected switch ports allow VSANs with identical names or contain zones with identical names, then Cisco DCNM-SAN verifies that the zones contain identical members. You can use merge analysis tool before attempting a merge, or after fabrics are interconnected to determine zone merge failure causes.

- Merge Fail Recovery—Recovers the port from its isolated state either by importing the neighboring switch's active zone set database and replacing the current active or by exporting the current database to the neighboring switch.
- Migrate Non-MDS Database—Migrate a non-MDS database using Cisco DCNM-SAN (you may need to use the Zone Migration Wizard to accomplish this task).
- IVR
  - Deactivate Zoneset—Deactivates an active zone set.
  - Copy Full Zone Database—Recovers an IVR zone database by copying the IVR full zone database from another switch.
  - Copy Full Topology—Recovers a topology by copying from the active zone database or the full zone database.

Tools

Tools menu provides the following options:

- Health
  - Switch Health—Determines the status of the components of a specific switch.
  - Fabric Configuration—Analyzes the configuration of a switch by comparing the current configuration to a specific switch or to a policy file. You can save a switch configuration to a file and then compare all switches against the configuration in the file.
  - Show Tech Support—Collects large amount of information about your switch for troubleshooting purposes. When you issue a **show tech support** command from Cisco DCNM-SAN for one or more switches in a fabric, the results of each command are written to a text file, one file per switch, in a directory you specify. You can then view these files using Cisco DCNM-SAN.
- Connectivity
  - End to End Connectivity—Determines connectivity and routes among devices with the switch fabric. This tool checks to see that every pair of end devices can talk to each other, using a Ping test and by determining if they are in the same VSAN or in the same active zone.
  - Ping—Determines connectivity from another switch to a port on your switch.
  - Trace Route—Verifies connectivity between two end devices that are currently selected on the Fabric pane.
  - Compact Flash Report—Automatically scans the fabric and generate a report that shows the status of CompactFlash.
- NPV
  - CFS Static Peer Setup—Manage the peer list used during CFS on NPV-enabled switches. After setting up the static peers list, the CFS discovery on the switches will be changed to static mode for all peers in the list. Cisco DCNM-SAN does not automatically update static peers list. You may need to update the list using the CFS Static Peer Setup Wizard when a new switch is added to the fabric.
  - Traffic Map Setup—Configures the list of external interfaces to the servers, and enabling or disabling disruptive load balancing. Using Traffic Map Setup you can specify the external ports that a server should use for traffic management.

  - Flex Attach Pre-Configure Server—Sets the port configurations for all the ports in a switch such as enabling or disabling FlexAttach, setting the default VSAN ID, and setting the interface status.
  - Flex Attach Move Server—Moves a server to another port on the same NPV device or another NPV device without changing the SAN.
  - Flex Attach Replace Server—Replaces a failed server with a new server on the same port without changing the SAN.
- Data Mobility Manager
  - Server Based—Performs server-based data migration.
  - Storage based—Performs storage-based data migration.
  - Server LUN Discovery—Performs LUN discovery to select the LUNs available for migration and automates the session creation by matching the LUNs in the existing and new storage.
- FCoE—Launches the FCoE Configuration Wizard to create virtual Fibre Channel interfaces.
- Port Channel—Creates PortChannels from selected ISL either manually or automatically.
- DPVM Setup—Establishes dynamic port VSAN membership, enables autolearning, and activates the DPVM database.
- IP SAN
  - FCIP Tunnel—Creates FCIP links between Gigabit Ethernet ports. Enables Fibre Channel write acceleration and IP compression.
  - iSCSI Setup—Creates zones for iSCSI initiators and adds a VSAN to a target-allowed VSAN list.
  - SAN Extension Tuner—Optimizes FCIP performance by generating either direct access (magnetic disk) or sequential access (magnetic tape) SCSI I/O commands and directing such traffic to a specific virtual target. This option is used to generate SCSI I/O commands (read and write) to the virtual target based on your configured options.
- Security
  - Port Security—Prevents unauthorized access to a switch port in the Cisco MDS 9000 Family, rejects intrusion attempts and reports these intrusions to the administrator.
  - IP ACL—Creates an ordered list of IP filters in a named IPv4-ACL or IPv6-ACL profile using the IPv4-ACL Wizard.
- Install
  - License—Facilitate download and installation of licenses in selected switches in the fabric.
  - Software—Verifies image compatibility and installs software images on selected switches in the fabric.
- Flow Load Balance Calculator—Allows you to get the best load-balancing configuration for your FICON flows. The calculator does not rely on any switch or flow discovery in the fabric.
- Device Manager—Invokes Device Manager for a switch.
- Command Line Interface —Enables command-line operations.
- Run CLI Commands—Runs command-line operations on more than one switch at a time.

Performance

The performance menu provides the following options:

- Create Flows—Creates host-to-storage, storage-to-host, or bidirectional flows. You can add these flows to a collection configuration file to monitor the traffic between a host or storage element pair.

Server

The server menu provides the following options:

- Admin—Opens the control panel.
- Purge Down Elements—Purges all down elements in the fabric.

Help

The help menu provides the following options:

- Contents —Launches the online help contents.
- Config Guide—Launches the Cisco DCNM-SAN Configuration Guide.
- About—Displays information about Cisco DCNM-SAN.

Toolbar

The Cisco DCNM-SAN main toolbar provides icons for accessing the most commonly used menu bar options as shown in Table 9-3.

Table 9-3 Cisco DCNM-SAN Client Main Toolbar

Icon	Description
	Opens switch fabric.
	Rediscovers current fabric.
	Finds in the map.
	Creates VSAN.
	Launches DPVM wizard.
	Launches Port Security wizard.
	Edits full zone database.

Table 9-3 Cisco DCNM-SAN Client Main Toolbar (continued)

Icon	Description
	Launches IVR zone wizard.
	Launches the FCoE configuration wizard.
	Launches PortChannel wizard.
	Launches FCIP wizard.
	Launches iSCSI wizard.
	Launches NPVM wizard.
	Launches QoS wizard.
	Configures users and roles.
	Launches IP-ACL wizard.
	Launches License Install wizard.
	Launches Software Install wizard.
	Performs switch health analysis.
	Performs fabric configuration analysis.
	Performs end-to-end connectivity analysis.

Table 9-3 Cisco DCNM-SAN Client Main Toolbar (continued)

Icon	Description
	Monitors ISL performance. Brings up real-time ISL performance information for all interfaces in the fabric, in the Information pane.
	Shows online help.

Logical Domains Pane

Use the Logical Domains pane to manage attributes for fabrics, VSANs, and zones, and to access user-defined groups. Starting from NX-OS Release 4.2(0), SAN and LAN nodes are listed under Datacenter node and all the fabrics are listed under SAN node. When you select Datacenter node in the tree, Cisco DCNM-SAN displays all the switches and ISLs. When you select LAN node, Cisco DCNM-SAN displays only Ethernet switches and Ethernet links. Under the fabric node, VSANs are ordered by a VSAN ID. The segmented VSANs are placed under the fabric node. The label next to the segmented VSAN indicates the number of segments. You can expand a segmented VSAN and the segments under that VSAN. Right-click one of the folders in the tree and click a menu item from the pop-up menu. You see the appropriate configuration dialog box.

The default name for the fabric is the name, IP address, or WWN for the principal switch in VSAN 1. If VSAN 1 is segmented, the default name is chosen from a principal switch with the smallest WWN. The fabric names you see are as follows:

- Fabric <sysName>
- Fabric <ipAddress>
- Fabric <sWWN>

You can change the fabric name using Cisco DCNM-SAN.

DETAILED STEPS

Step 1 Choose **Server** > **Admin**.

You see the Control Panel dialog box.

Step 2 Double-click the fabric name and enter the new name of the fabric.

Step 3 Click **Apply** to change the name.

Filtering

Cisco DCNM-SAN has a filtering mechanism that displays only the data that you are interested in. To filter, first select the fabric and VSAN from the Logical Domains pane. This action narrows the scope of what is displayed in the Fabric pane. Any information that does not belong to the selected items is dimmed. Also, any information that does not belong to the selected items is not displayed in the tables in the Information pane. The filter that you select is displayed at the top right of the Cisco DCNM-SAN window.

To further narrow the scope, select attributes from the Physical Attributes pane. The Cisco DCNM-SAN table, display, and filter criteria change accordingly.

Physical Attributes Pane

Use the Physical Attributes pane to display a tree of the options available for managing the switches in the currently selected fabric, VSAN, or zone.

To select an option, click a folder to display the options available and then click the option. You see the table with information for the selected option in the Information pane. The Physical Attributes pane provides the following main folders:

- Switches—Views and configures hardware, system, licensing, and configuration files.
- Interfaces—Views and configures FC physical, FC logical, VFC (FCoE), Ethernet, SVC, and PortChannel interfaces.
- FC Services—Views and configures Fibre Channel network configurations.
- IP—Views and configures IP storage and IP services.
- Security—Views and configures MDS management and FC-SP security.
- FCoE—Views and configures FCoE interfaces.
- ISLs—Views and configures Inter-Switch Links.
- End Devices—Views and configures end devices.

Note You cannot view the detailed physical attributes of the data center switches or monitor the connections. When you select either a data center node or a LAN node the physical attributes pane will be blank.

Context Menu for Tables

When you right-click in the table, you see a pop-up menu with options that vary depending on the type of option you selected in the Physical Attributes pane. You can perform various operations by right-clicking the device listed in the table. To view various options available for switches, ISLs, and end devices, refer to the procedures in the sections that follows:

Viewing Switch Options

When you select the datacenter node, the switch table displays all the switches that are discovered. When you select the SAN node or the fabric node, the switch table displays all the Fibre Channel switches and when you select the LAN node, the switch table displays all the Ethernet switches.

DETAILED STEPS

Step 1 Click **Switches** in the Physical Attributes pane.

Step 2 Right-click the device in the table.

The pop-up menu provides the following options:

- Apply Changes—Applies the changes to the switch.
- Refresh Values—Refreshes the current values.

- Undo Changes—Undoes modifications to the switch.
- Export to File—Export the values to a file.
- Print Table—Prints the table.
- Detach Table—Detaches the table.
- Switch Attributes—Changes the switch properties.
- Interface Attributes—Changes the interface properties.
- Element Manager—Manages this switch.
- Command Line Interface—Enables to perform command line operations.
- Copy—Copies the switch.
- Purge—Purges the switch.
- Fix Location—Fixes the switch in the current location.
- Align—Aligns the switch.
- Show End Devices—Shows the end devices.
- Expand Multiple Links—Expands the links to this switch.
- Other—Other options.
- Group—Groups switches.

Viewing ISL Options

When you select the data center node, the ISLs table displays all of the Fibre Channel and Ethernet links. When you select the LAN node, the ISLs table displays all the Ethernet links.

DETAILED STEPS

Step 1 In the Physical Attributes pane, click **ISLs** and then click **Summary** tab.

Step 2 Right-click the device in the table.

The pop-up menu provides the following options:

- Refresh Values—Refreshes the current values.
- Copy—Copies information from a specific field.
- Find—Conducts search based on the input string.
- Export to File—Exports the values to a file.
- Print Table—Prints the table.
- Detach Table—Detaches the table.
- Interface Attributes—Changes the interface properties.
- Element Manager—Manages the device.
- FCIP Tunnel Attributes—Changes FCIP tunneling properties.
- Create Port Channel—Creates port channel.
- Re-enable—Reenables a disabled device.
- Enable FC-SP—Enables FC-SP.

- SAN Extention Tuner—Optimizes FCIP performance.
- Purge—Purges the device.

Note When you select a port channel from the table, the pop-up menu will have the following additional options:

- Member Attributes—Changes the member properties.
- Channel Attributes—Changes the port channel properties.
- Edit—Edits the channel properties.

Viewing End Device Options

DETAILED STEPS

Step 1 In the Physical Attributes pane, click **End Devices** and then click the **Summary** tab.

Step 2 Right-click the device in the table.

The pop-up menu provides the following options:

- Apply Changes—Applies the changes to the device.
- Refresh Values—Refreshes the current values.
- Copy—Copies the information specific to the field.
- Paste—Pastes the copied text.
- Undo Changes—Undoes modifications to the device.
- Find—Searches for information depending on the input string.
- Export to File—Exports the values to a file.
- Print Table—Prints the table.
- Detach Table—Detaches the table.
- Device Attributes—Changes the device properties.
- Interface Attributes—Changes the interface properties.
- Element Manager—Manages this device.
- Command Line Interface—Enables you to perform command line operations.
- Copy—Copies the switch.
- Purge—Purges the switch.
- Fix Location—Fixes the switch in the current location.
- Align—Aligns the switch.
- Ping—Pings another device.
- Trace Route—Determines the route taken by packets across the network.
- Select Dependent Ports—Selects dependent ports.
- Group—Groups devices.

Information Pane

Use the Information pane to display tables of information associated with the option selected from the menu tree in the Logical Domains or Physical Attributes panes. The Information pane toolbar provides buttons for performing one or more of the operations shown in Table 9-4.

Table 9-4 Information Pane Toolbar

Icon	Description
	Applies configuration changes.
	Refreshes table values.
	Opens the appropriate dialog box to make a new row in the table.
	Deletes the currently highlighted rows from the table.
	Copies data from one row to another.
	Pastes the data from one row to another.
	Undoes the most recent change.
	Finds a specified string in the table.
	Exports and saves information to a file.
	Prints the contents of the Information pane.
	Displays a non-editable copy of the table in the Information pane in its own window, which you can move around the screen.

Note After making changes, you must save the configuration or the changes will be lost when the device is restarted.

Note The buttons that appear on the toolbar vary according to the option that you select. They are activated or deactivated (dimmed) according to the field or other object that you select in the Information pane.

Detachable Tables

Detachable tables in Cisco DCNM-SAN allow you to detach tables and move them to different areas on your desktop so that you can compare similar tables from different VSANs. You can keep informational tables open from one view while you examine a different area in Cisco DCNM-SAN. To detach tables, click the **Detach Table** icon in the Information pane in Cisco DCNM-SAN.

Fabric Pane

Use the Fabric pane to display the graphical representation of your fabric. Table 9-5 explains the graphics you may see displayed, depending on which devices you have in your fabric.

Table 9-5 Cisco DCNM-SAN Graphics

Icon or Graphic	Description
	Director class MDS 9000 Fibre Channel switch.
	Non-director class MDS 9000 Fibre Channel switch.
	Nexus 7000 switch.
	Nexus FCoE or Fibre Channel switch.
	Catalyst LAN switch.
	Generic Fibre Channel switch.
	Cisco SN5428.

Table 9-5 Cisco DCNM-SAN Graphics (continued)

Icon or Graphic	Description
	Dashed or dotted orange line through a device indicates that the device is manageable but there are operational problems.
	Dashed or dotted orange X through a device or link indicates that the device or ISL is not working properly.
	A red line through a device indicates that the device is not manageable.
	A red X through a device or link indicates that the device is down or that the ISL is down.
	Fibre Channel HBA (or enclosure).
	Fibre Channel target (or enclosure).
	iSCSI host.
	Fibre Channel ISL and edge connection.
	Fibre Channel PortChannel.
	IP ISL and edge connection.
	IP PortChannel.
	DWDM connection.
	NPV connection.
	Fibre Channel loop (storage).

Table 9-5 Cisco DCNM-SAN Graphics (continued)

Icon or Graphic	Description
	IP cloud (hosts). This icon is also used to represent a fabric when viewing a SAN (multiple fabrics) in the Cisco DCNM-SAN Fabric pane.
	Any device, cloud, or loop with a box around it means that there are hidden links attached.

If a switch or director is grayed out, Cisco DCNM-SAN can no longer communicate with it.

The bottom of the Fabric pane has the following tabs:

- Fabric—When displaying multiple fabrics, each fabric has its own tab. You can switch between fabrics by clicking on their respective tabs.
- Log—Displays messages that describe Cisco DCNM-SAN operations, such as fabric discovery.

When viewing large fabrics in the Fabric pane, it is helpful to do the following tasks:

- Turn off end device labels.
- Collapse loops.
- Collapse expanded multiple links (collapsed multiple links are shown as very thick single lines).
- Dim or hide portions of your fabric by VSAN.

Note When a VSAN, zone, or zone member is selected in the VSAN tree, the map highlighting changes to identify the selected objects. To remove this highlighting, click the **Clear Highlight** button on the Fabric pane toolbar or choose **Clear Highlight** from the pop-up menu.

Context Menus

When you right-click an icon in the Fabric pane, you see a pop-up menu with options that vary depending on the type of icon selected. The various options available for different objects include the following:

- Open an instance of Device Manager for the selected switch.
- Open a CLI session for the selected switch.
- Copy the display name of the selected object.
- Execute a **ping** or **traceroute** command for the device.
- Show or hide end devices.
- View attributes.
- Quiesce and disable members for PortChannels.
- Set the trunking mode for an ISL.
- Create or add to a PortChannel for selected ISLs.

The Fabric pane has its own toolbar with options for saving, printing, and changing the appearance of the map. When you right-click the map, a pop-up menu appears that provides options (duplicated on the toolbar) for changing the appearance of the map.

Note You can launch web-based or non-web-based applications from the Fabric pane. To do this, you assign an IP address to the storage port or enclosure. Then right-click to bring up the pop-up menu, and select **Device Manager**.

Saving the Map

You can save the map in the Fabric Pane as an image, or as an editable Visio diagram. You can save the map with or without labels on the links. The created Visio diagram is editable and saved in two layers:

- The default layer includes all switches and links in the fabric.
- The end devices layer includes the end devices and can be turned off to remove end devices from the Visio diagram.

To save the map as a Visio diagram, choose **Files > Export > Visio** and choose **Map** or **Map with link labels**. The saved Visio diagram retains the viewing options that you selected from the Fabric pane. For example, if you collapse multiple links in the map and export the links as a Visio diagram, the Visio diagram shows those multiple links as one solid link.

The Show Tech Support option from the Tools menu also supports saving the map as a Visio diagram.

Purging Down Elements

The Fabric pane allows you to refresh the map at any time by clicking the **Refresh Map** icon. The **Refresh Map** icon redraws the map but does not purge elements that are down. To purge down elements you can:

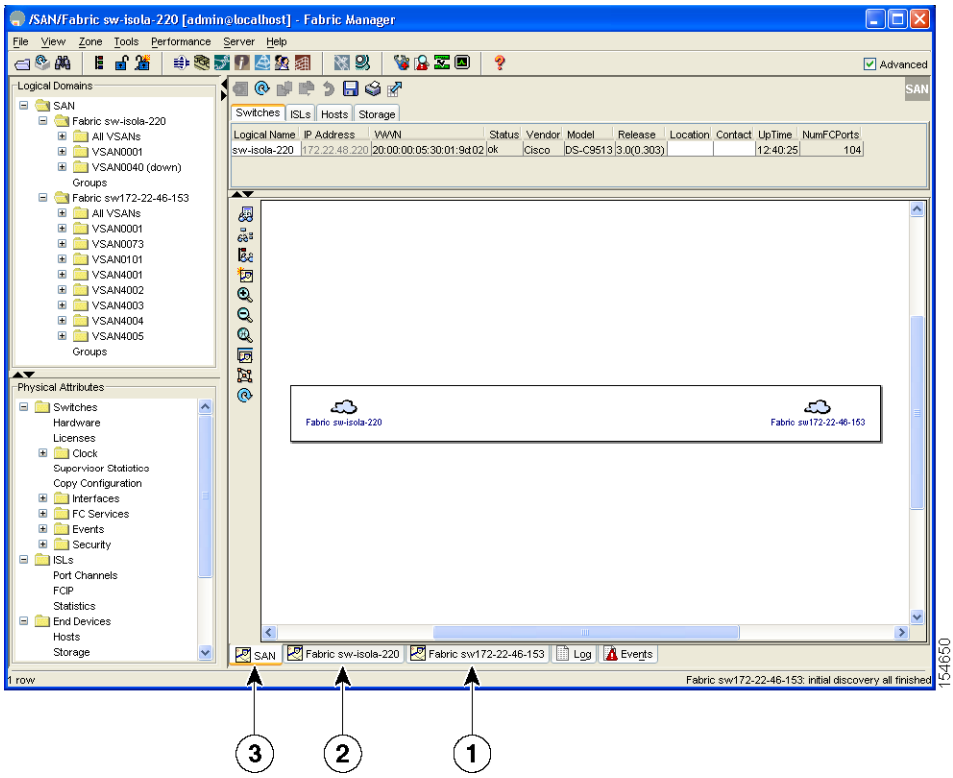
- Choose **Server > Purge Down Elements**. This purges all down elements in the fabric.
- Right-click the **Fabric** pane and choose **Purge Down Elements**.
- Right-click a down element and choose **Purge**. This action purges only this element from the fabric.

Note If you select an element that is not down and purge it, that element will reappear on the next fabric discovery cycle.

Multiple Fabric Display

Cisco DCNM-SAN can display multiple fabrics in the same pane as shown in Figure 9-3.

Figure 9-3 Cisco DCNM-SAN's Multiple Fabric Display Window



1	The Fabric view tab for fabric 172.23.46.152. When selected, the Fabric view displays fabric 172.23.46.152.
2	The Fabric view tab for fabric 172.23.46.153. When selected, the Fabric view displays fabric 172.23.46.153.
3	SAN tab (selected), showing two fabrics.

The information for both fabrics is displayed; you do not need to select a seed switch. To see details of a fabric, select the tab for that fabric at the bottom of the Fabric pane, or double-click the **Cloud** icon for the fabric in the SAN tab.

Note Enclosure names should be unique. If the same enclosure name is used for each port, Cisco DCNM-SAN shows a host/target enclosure connected to both fabrics. To fix this problem, you can either disable auto-creation or create unique enclosure names.

Filtering by Groups

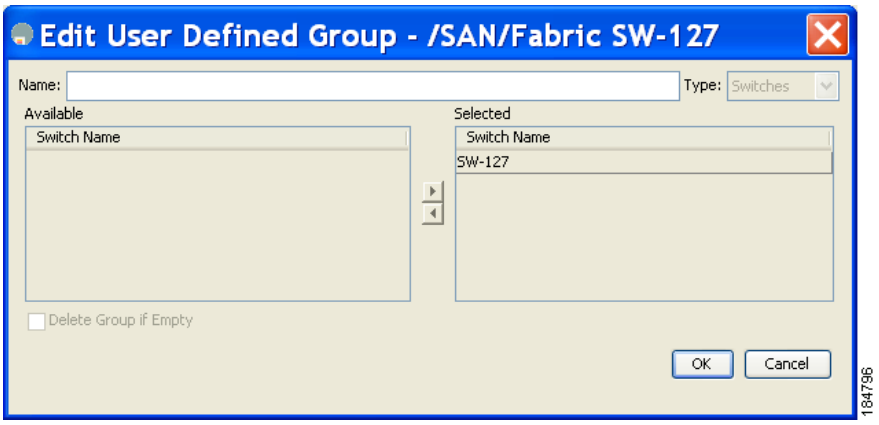
You can filter the Fabric pane display by creating groups of switches or end ports.

DETAILED STEPS

Step 1 Right-click a switch or end port in the Fabric pane map and select **Group > Create**.

You see the Edit User Defined Group dialog box as shown in Figure 9-4.

Figure 9-4 Edit User Defined Group Dialog Box



Step 2 Enter a group name in the **Name** field.

Step 3 Use the arrows to move additional switches or end ports from the **Available** column to the **Selected** column.

Step 4 Click **OK** to save the group.

To add a switch or end port to an existing group in Cisco DCNM-SAN.

DETAILED STEPS

Step 1 Right-click a switch or end device and select **Group > Add To >** ***YourGroupName***.

You see the Edit User Defined Group dialog box.

Step 2 Use the arrows to move additional switches or end ports from the **Available** column to the **Selected** column.

Step 3 Click **OK** to save the updated group.

To filter the display by a group you have created.

DETAILED STEPS

Step 1 Expand the **Groups** folder in the Logical Domains pane.

You see the list of groups that you have created.

Step 2 Click the name of the group that you want to filter.

In the Fabric pane, the switches or end devices in your group are shown normally; all other switches and end devices are shown in gray.

Step 3 Click the **Groups** folder in the Logical Domains pane to return the display to normal.

Note User-defined groups tables are filtered based on switches in the group except for switches where CFS-controlled features are enabled when all CFS member switches are displayed to avoid misconfigurations.

Status Bar

The status bar at the bottom of the Cisco DCNM-SAN window shows the last entry displayed by the discovery process, and the possible error message on the right side. The status bar displays a message stating that something has changed in the fabric and a new discovery is needed. The status bar shows both short-term, transient messages (such as the number of rows displayed in the table) and long-term discovery issues.

Launching Cisco DCNM-SAN Client

As of Cisco SAN-OS 3.x and NX-OS Release 4.x, the Fabric Manager Client login procedure has changed.

Launching Fabric Manager Client in Cisco SAN-OS Release 3.2(1) and Later

You can launch Fabric Manager Client.

Note Network administrators must initially launch Cisco DCNM-SAN Client using Cisco DCNM-SAN Web Server, as described in the following procedure. Once an administrator has installed the Cisco DCNM-SAN Client icon on your desktop, you can double-click the icon to launch the Cisco DCNM-SAN Client.

DETAILED STEPS

Step 1 Open your browser and enter the IP address where you installed Cisco DCNM-SAN Server, or enter localhost if you installed Cisco DCNM-SAN Server on your local workstation.

You see the Cisco DCNM Web Client Login dialog box.

Step 2 Enter your user name and password and click **Login**.

You see the Cisco DCNM Web Client Summary page.

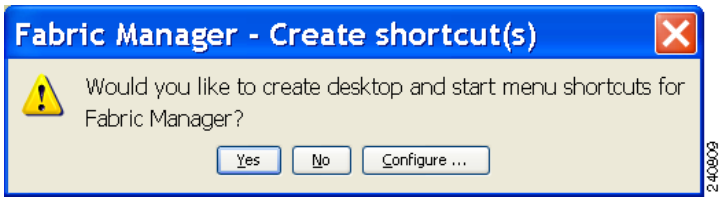
Step 3 Click the **Download** link in the upper right corner of the page.

You see the Download page for Cisco DCNM-SAN and Device Manager.

Step 4 Click the link for **Cisco DCNM-SAN**.

If you are launching Cisco DCNM-SAN Client for the first time, you see a message asking whether you want to create shortcuts for Cisco DCNM-SAN.

Figure 9-5 DCNM-SAN Create Shortcut(s) Message



Step 5 Click **Yes** to create shortcuts for Cisco DCNM-SAN.

Note This message only appears the first time you launch Cisco DCNM-SAN Client. If you select No, your selection will be remembered and you will not be prompted to make a selection again. In this case, you will need to launch Cisco DCNM-SAN Client using the Cisco DCNM-SAN Web Client.

Step 6 When the software is installed and icons are created on your desktop, double-click the Cisco DCNM-SAN icon to launch Cisco DCNM-SAN.

You see the Cisco DCNM-SAN Login dialog box.

Step 7 Enter the Cisco DCNM-SAN Server user name and password.

Step 8 Check the **Use SNMP Proxy** check box if you want Cisco DCNM-SAN Client to communicate with Cisco DCNM-SAN Server through a TCP-based proxy server.

Step 9 Click **Login**. Once you successfully log in to Cisco DCNM-SAN Server, you can set the seed switch and open the fabrics that you are entitled to access.

Note When you launch Cisco DCNM-SAN Client for the first time or when there are no available fabrics, you see the Discover New Fabric dialog box.

You see the Discover New Fabric dialog box.

Note Only network administrators can discover new fabrics.

Note Even when remote AAA server authentication is enabled on the switch, use the local switch account that is not defined in the remote AAA server for fabric discovery. In other words, when a user is not found in the remote AAA server, then local switch user authentication will be allowed by the switch for SNMPv3 clients like DCNM.

Step 10 Click the **Ethernet (CDP)** radio button to discover using Cisco Discovery Protocol (CDP).

Step 11 Starting from NX-OS Release 4.2(0), Fabric Manager uses Cisco Discovery Protocol to discover Ethernet switches such as Nexus 5000, Nexus 7000, Catalyst 4000, and Catalyst 6000 switches. You need to use a CDP seed switch for a CDP discovery.
Set the fabric seed switch to the Cisco MDS 9000 Family switch or Cisco Nexus 5000 Series that you want Fabric Manager to use.

Step 12 Choose the Auth-Privacy option according to the privacy protocol you have configured on your switch:

a. If you have not configured the switch with a privacy protocol, then choose Auth-Privacy option MD5 (no privacy).

b. If you have configured the switch with your privacy protocol, choose your Auth-Privacy choice.

Note You may use SNMP v2 credentials for CDP discovery as the most of the Catalyst switches do not use MD5-DES for configuration.

Note If you want a clean fabric discovery, remove the fabric and rediscover it. If you want a clean LAN discovery, unmanage LAN, remove the CDP seed switch and then rediscover it.

Step 13 Enter the username and password for the switch.

Step 14 (Optionsl) To limit the discovery, specify the VSAN range.
Scoping limits the resources discovered by Cisco DCNM-SAN client. You can either include a range of VSANs to be discovered or exclude a range of VSANs from being discovered.

a. To limit the discovery to a range of VSANs, click **Included VSAN List** radio button**.** Specify the range of VSANs.

b. To exclude a range of VSANs from being discovered, click **Excluded VSAN List** radio button. Specify the range of VSANs to be excluded.

Step 15 Click **Discover**.

You see the Control Panel dialog box.

You see the included and excluded VSANs list under the Fabric tab.

Note You see a message in the dialog box when the server and client are running on the same workstation and there are unlicensed fabrics in the database. You also see a message when there are unmanaged fabrics (the state of the licenses is unknown).

Note In the open tab, you see all the discovered fabrics displayed in the control panel. You need to click on the Open button to see all the discovered Ethernet switches.

Step 16 Check the check box(es) next to the fabric(s) you want to open in the Select column, or click **Discover** to add a new fabric.

Note Only network administrators can continuously manage or unmanage fabrics. For more information, see the "Selecting a Fabric to Manage Continuously" section on page 7-4.

Step 17 Click **Open** to open the selected fabric(s).

Note
- If you have an incomplete view of your fabric, rediscover the fabric with a user that has no VSAN restriction.
- If the fabric includes a Cisco Nexus 5000 Series switch, then the Layer 2 node appears under the Switches > Interfaces > Ethernet tree, the VFC (FCoE) node appears under the Switches > Interfaces tree, and the FCoE node appears under the Switches tree in the Physical Attributes pane.
- For Cisco Nexus 5000 Series switches in the fabric, the tooltip for the switch shows the bind information of a virtual Fibre Channel interface to its corresponding Ethernet interface, such as vfc2(eth1/4).

You can launch Cisco DCNM-SAN Client from within a running instance of Cisco DCNM-SAN.

DETAILED STEPS

Step 1 **Choose File > Open** or click the **Open Switch Fabric** icon on the Cisco DCNM-SAN toolbar.

You see the Control Panel dialog box.

Step 2 Check the check box(es) next to the fabric(s) you want to open in the Select column and click **Open**.

Note Changes made using Cisco DCNM-SAN are applied to the running configuration of the switches that you are managing. If you have made changes to the configuration or performed an operation (such as activating zones), Cisco DCNM-SAN prompts you to save your changes before you exit.

Launching Cisco DCNM-SAN Client Using Launch Pad

Starting from Cisco NX-OS Release 4.2(0), you can use Cisco DCNM-SAN launch pad to connect to any server by specifying the IP address of the server. With launch pad, you can connect to any Cisco DCNM-SAN Server version 3.3(0) and later. Launch pad establishes connection with the server using HTTP protocol.

DETAILED STEPS

Step 1 Open your browser and enter the IP address where you installed Cisco DCNM-SAN Server, or enter localhost if you installed Cisco DCNM-SAN Server on your local workstation.

You see the Cisco DCNM-SAN Web Server Login dialog box.

Step 2 Enter your user name and password and click **Login**.

You see the Cisco DCNM-SAN Web Client Summary page.

Step 3 Click the **Download** link in the upper right corner of the page.

You see the Download page for Cisco DCNM-SAN and Device Manager.

Step 4 Click the link for **Cisco DCNM-SAN**.

You see the Cisco DCNM-SAN Server launch pad.

Step 5 Enter the host name of the server or IP address in the **Server URL** drop-down list.

Step 6 Click **Start**.

Note Launch pad retains the history of the server URLs used. You can choose one of the previously user Server URLs from the drop-down list.

Setting Cisco DCNM-SAN Preferences

To set your preferences for the behavior of the Cisco DCNM-SAN, choose **File > Preferences** from the Cisco DCNM-SAN menu bar. You see the Preferences dialog box with the following tabs for setting different components of the application:

- General
- SNMP
- Map

The default General preferences for Cisco DCNM-SAN are as follows:

- **Show Device Name by**—Displays the switches in the Fabric pane by IP address, DNS name, or logical name. The default setting for this value is Logical Name.
- **Show WorldWideName (WWN) Vendor**—Displays the world wide name vendor name in any table or listing displayed by Cisco DCNM-SAN. Check the **Prepend Name** check box to display the name in front of the IP address of the switch. Check the **Replacing Vendor Bytes** check box to display the name instead of the IP address. The default is the Prepend Name option.
- **Show End Device Using**—Displays end devices in the Fabric pane using alias or pWWN alias. The default setting for this value is Alias.
- **Show Shortened iSCSI Names**—Displays the default setting for this value is OFF.
- **Show Timestamps as Date/Time**—Displays timestamps in the date/time format. If this preference is not checked, timestamps are displayed as elapsed time. The default setting is enabled (checked).
- **Telnet Path**—Displays the path for the telnet.exe file on your system. The default is **telnet.exe**, but you need to browse for the correct location.

  Note If you browse for a path or enter a path and you have a space in the pathname (for example, **c:\program files\telnet.exe)**, then the path will not work. To get the path to work, you must manually place quotes around it (for example, **"c:\program files\telnet.exe"**).

- **Use Secure Shell instead of Telnet**—Specifies whether to use SSH or Telnet when using the CLI to communicate with the switch. If enabled, you must specify the path to your SSH application. The default setting is disabled.
- **Confirm Deletion**—Displays a confirmation pop-up window when you delete part of your configuration using Cisco DCNM-SAN. The default setting is enabled (checked).
- **Export Tables with Format**—Specifies the type of file that is created when you export a table using Device Manager. The options are tab-delimited or XML. The default setting is Tab-Delimited.

- Show CFS Warnings—Shows warning messages if CFS is not enabled on all switches for a selected feature.

The default SNMP preferences for Cisco DCNM-SAN are as follows:

- **Retry request 1 time(s) after 5 sec timeout**—You can set the retry value to 0-5, and the timeout value to 3-30.
- **Trace SNMP packets in Log**—The default setting for this value is ON.
- **Enable Audible Alert when Event Received**—The default setting for this value is OFF.

The default Map preferences for Cisco DCNM-SAN are as follows:

- **Display Unselected VSAN Members**—Displays the unselected VSAN members in the Fabric pane. The default setting for this value is ON.
- **Display End Devices**—Displays the fabric's end devices in the Fabric pane. The default setting for this value is ON.
- **Display End Device Labels**—Displays the fabric's end device labels in the Fabric pane. The default setting for this value is OFF.
- **Expand Loops**—Displays the loops in the fabric as individual connections in the Fabric pane. The default setting for this value is OFF.
- **Expand Multiple Links**—Displays multiple links in the Fabric pane as separate lines instead of one thick line. The default setting for this value is OFF.
- **Open New Device Manager Each Time**—Opens a new instance of Device Manager each time that you invoke it from a switch in your fabric. The default value is OFF, which means that only one instance of Device Manager is open at a time.
- **Select Switch or Link from Table**—Allows you to select a switch or link in the Fabric pane by clicking the switch or link in a table in the Information pane. The default setting for this value is disabled (unchecked), which means clicking a switch or link in the table does not change the switch or link selection in the Fabric pane.
- **Layout New Devices Automatically**—Automatically places new devices in the Fabric pane in an optimal configuration. The default setting for this value is OFF. In this mode, when you add a new device, you must manually reposition it if the initial position does not suit your needs.
- **Use Quick Layout when Switch has 30 or more End Devices**—Displays the default setting for this value (30). You can enter any number in this field. Enter **0** to disable Quick Layout.
- **Override Preferences for Non-default Layout**—Displays the default setting for this value (ON).
- **Automatically Save Layout**—If this option is enabled, any changes in the layout are automatically saved. The default setting for this value is ON.
- **Detach Overview Window**—Allows you to easily center the Fabric pane on the area of the fabric that you want to see. (This feature is useful for large fabrics that cannot be displayed entirely within the Fabric pane.) Bring up the overview window by clicking the **Show/Hide Overview Window** button. It overlays the fabric window and remains there until you click the **Show/Hide Overview Window** button again. If you enable this preference, you can detach the overview window and move it to one side while you access the Fabric pane. The default setting for this value is disabled (unchecked).

Network Fabric Discovery

Cisco DCNM-SAN collects information about the fabric topology through SNMP queries to the switches that are connected to Cisco DCNM-SAN. The switch replies after having discovered all devices connected to the fabric by using the information from its FSPF technology database and the Name Server database and collected using the Fabric Configuration Server's request/response mechanisms that are defined by the FC-GS-3/4 standard. When you start Cisco DCNM-SAN, you enter the IP address (or host name) of a seed switch for discovery.

After you start Cisco DCNM-SAN and the discovery completes, Cisco DCNM-SAN presents you with a view of your network fabric, including all discovered switches, hosts, and storage devices.

Network LAN Discovery

Starting from NX-OS Release 4.2(0), you can discover Nexus and Catalyst Ethernet switches using Cisco Discovery Protocol (CDP). DataCenter 3(DC3) switches are displayed under Datacenter and LAN nodes. Cisco DCNM-SAN displays basic information about DC3 switches and its ISLs.

Viewing Ethernet Switches

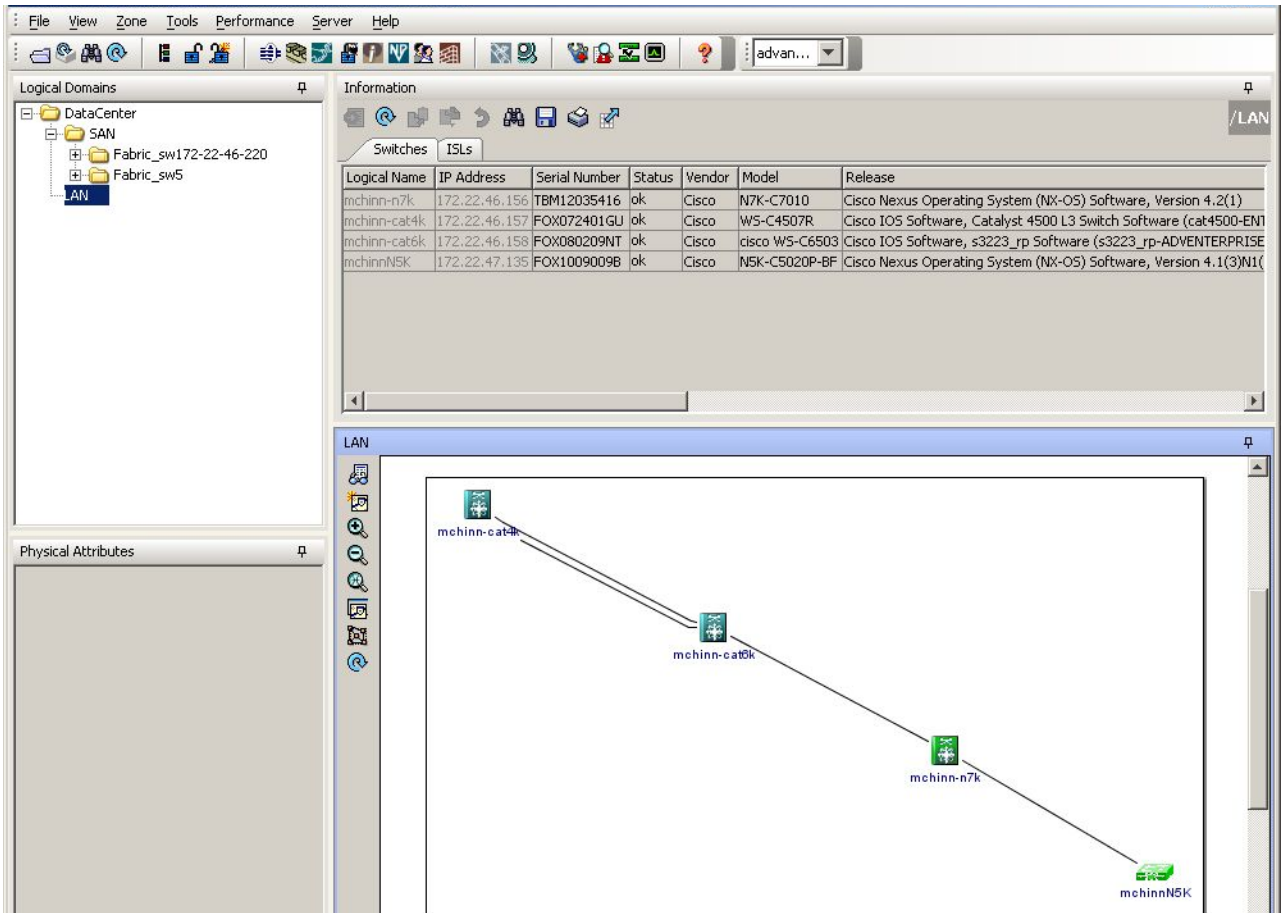
DETAILED STEPS

Step 1 Click the **LAN** node under **Datacenter** node.

Step 2 Click **Switches** tab in the Information pane.

You can see the switch information as shown in Figure 9-6.

Figure 9-6 Ethernet Switch Information



Note Datacenter is the parent node of SAN and LAN nodes. The SAN node remains in the tree as the parent for all the fabrics.

Removing a LAN

DETAILED STEPS

Step 1 Choose **Server > Admin**.

You can see the switch information.

Step 2 Click to select the switch IP of the LAN you want to remove.

Step 3 Click **Remove**.

Modifying the Device Grouping

Because not all devices are capable of responding to FC-GS-3 requests, different ports of a single server or storage subsystem may be displayed as individual end devices on the Cisco DCNM-SAN map.

DETAILED STEPS

Step 1 Expand **End Devices** and then choose **Storage** or **Hosts** in the Physical Attributes pane.

You see the end devices displayed in the Information pane.

Step 2 Click one of the devices in the Fabric pane, or click the **Enclosures** tab of the Information pane, and then click the device name (in the Name field) that you want to include in the enclosure.

Step 3 Enter a name to identify the new enclosure in the Fabric pane map.

Step 4 Click once on the device name in the Name field. To select more than one name, press the **Shift** key and click each of the other names.

Step 5 Press **Ctrl-C** to copy the selected name(s).

Step 6 Press **Ctrl-V** to paste the device name into the Name field.

Note To remove devices from an enclosure, triple click the device name and press **Delete**. To remove an enclosure, repeat this step for each device in the enclosure.

Using Alias Names as Enclosures

DETAILED STEPS

Step 1 Expand End Devices and choose **Hosts** or **Storage** from the Physical Attributes pane.

You see the list of devices in the Information pane. The NxPorts tab is the default.

Step 2 Right-click the enclosure names that you want to convert to alias names and choose **Alias > Enclosure**.

The Ailas > Enclosures window appears. It contains a list of expressions. You can also add expressions to the list and modify expressions in the current list.

Step 3 Click the **Apply Changes** icon to save the changes and then click **Close**.

Note Cisco DCNM-SAN uses the regular expressions to convert multiple alias names into one enclosure. The alias names should be in the same expression pattern rule. You can create enclosure names from selected aliases using the regular expresssions list.

Using Alias Names as Descriptions

DETAILED STEPS

Step 1 Choose **End Devices** and from the Physical Attributes pane.

Step 2 Click the **General** tab.

You see the list of devices in the Information pane.

Step 3 Select the device names that you want to populate the description with alias names and then click **Alias > Enclosure** button.

You see the alias names are copied to corresponding rows in the description column.

Note Cisco DCNM-SAN does not parse or format the alias name while copying.

Controlling Administrator Access with Users and Roles

Cisco MDS 9000 Family switches support role-based management access whether using the CLI or Cisco Cisco DCNM-SAN. This lets you assign specific management privileges to particular roles and then assign one or more users to each role.

The default-role contains the access permissions needed by a user to access the GUI (Cisco DCNM-SAN and Device Manager). These access permissions are automatically granted to all users in order for them to use the GUI.

Cisco Cisco DCNM-SAN uses SNMPv3 to establish role-based management access. After completing the setup routine, a single role, user name, and password are established. The role assigned to this user allows the highest level of privileges, which includes creating users and roles. Use the Cisco Cisco DCNM-SAN to create roles and users and to assign passwords as required for secure management access in your network.

Note Either to create a new SNMPv3 user or modify password of SNMPv3 user, the DCNM login user need to have enabled with DES/AES privacy password. Since the creating and modifying SNMP SET request need to be encrypted, the login user password needs to have the privacy password.

Using Cisco DCNM-SAN Wizards

Cisco DCNM-SAN Client provides the following wizards to facilitate common configuration tasks:

- VSAN—Creates VSANs on multiple switches in the fabric and sets VSAN attributes including interop mode, load balancing, and FICON.
- Zone Edit Tool—Creates zone sets, zones, and aliases. Adds members to zones and edits the zone database.

- IVR Zone—Creates IVR zone sets, zones, and aliases. Enables IVR NAT and auto-topology. Adds members to IVR zones, and edits the IVR zone database.
- FCoE—Creates virtual Fibre Channel (FC) interfaces and VLAN-VSAN mappings, and binds virtual FC interfaces to Ethernet interfaces or PortChannels.
- PortChannel—Creates PortChannels from selected ISLs either manually or automatically. Sets PortChannel attributes such as channel ID and trunking mode.
- FCIP—Creates FCIP links between Gigabit Ethernet ports. Enables Fibre Channel write acceleration and IP compression.
- DPVM—Establishes dynamic port VSAN membership, enables autolearning, and activates the DPVM database.
- Port Security—Prevents unauthorized access to Cisco MDS switches and reports these intrusions to the administrator.
- iSCSI—Creates zones for iSCSI initiators and adds a VSAN to a target-allowed VSAN list.
- NPV—Reduces the number of Fibre Channel domain IDs in SANs.
- QoS—Sets QoS attributes for zones in the selected VSAN.
- IP ACL—Creates ordered IP access control lists and distributes to selected switches in the fabric.
- License Install—Facilitates download and installation of licenses in selected switches in the fabric.
- Software Install—Verifies image compatibility and installs software images on selected switches in the fabric.

Cisco DCNM-SAN Troubleshooting Tools

Cisco DCNM-SAN has several troubleshooting tools available from the toolbar or Tools menu

- **Zone Merge Analysis**—The zone merge analysis tool (available from the Zone menu) enables you to determine if zones will merge successfully when two Cisco MDS switches are interconnected. If the interconnected switch ports allow VSANs with identical names or contain zones with identical names, then Cisco DCNM-SAN verifies that the zones contain identical members. The merge analysis tool can be run before attempting a merge or after fabrics are interconnected to determine zone merge failure causes.
- **End-to-End Connectivity**—Cisco DCNM-SAN's end-to-end connectivity analysis tool uses FC Ping to verify interconnections between Cisco MDS switches and end-device (HBAs and storage devices) in a particular VSAN. In addition to basic connectivity, Cisco DCNM-SAN can optionally verify the following:
  - Paths are redundant.
  - Zones contain at least two members.

End devices are connected to a manageable switch (have a currently active in-band or out-of-band management path.)

- **Switch Health Analysis**—You can run an in-depth switch health analysis with Cisco DCNM-SAN. It verifies the status of all critical Cisco MDS switches, modules, ports, and Fibre Channel services. Over 40 conditions are checked. This tool provides a very fast, simple, and thorough way to assess Cisco MDS switch health.

- **Fabric Configuration Analysis**—Cisco DCNM-SAN includes a fabric configuration analysis tool. It compares the configurations of all Cisco MDS switches in a fabric to a reference switch or a policy file. You can define what functions to check and what type of checks to perform. The analysis can look for mismatched values, and missing or extra values. If all configuration checking is performed for all functions, over 200 checks are performed for each Cisco MDS switch.

After the analysis is run, the results are displayed with details about the issues that were discovered. You can automatically resolve configuration differences by selecting them and clicking the **Resolve** button. Cisco DCNM-SAN automatically changes the configuration to match the reference switch or policy file.

Integrating Cisco DCNM-SAN and Data Center Network Management Software

Cisco DCNM-SAN and Data Center Network Management (DCNM) software are the two major components in the Cisco next-generation data center environment. Cisco DCNM-SAN configures Cisco Nexus 5000 Series switches and Cisco MDS 9000 Series switches. DCNM software configures Cisco Nexus 5000 and Cisco Nexus 7000 Series switches. The Scope of the Cisco DCNM-SAN software is confined to SAN while the scope of the DCNM-LAN software is limited to the LAN network.

In a typical data center environment, the mixture of SAN and LAN topology are becoming increasingly common. Since the two management software are not designed to work across their topology limits, users are not able to navigate to Cisco DCNM-SAN from DCNM-LAN software and vice versa.

Integrating Cisco DCNM-SAN and DCNM-LAN provides a single platform to manage the networks in data center 3.0 and it provides seamless user experience under specific configuration. Starting from Cisco MDS NX-OS Release 4.2, the directory structure has changed to accommodate the integration of Cisco DCNM-SAN with Cisco Nexus 5000 Series products.

Launching a Switch from the Topology Map

DETAILED STEPS

Step 1 In the Cisco DCNM-SAN fabric pane, right-click the Nexus switch in the LAN map that you want to open with DCNM.

You see the pop-up men.

Step 2 In the pop up menu, click **DCNM** and select appropriate context.

Device Manager

This chapter contains descriptions and instructions for using the Device Manager. This chapter contains the following sections:

Information About Device Manager

Device Manager provides a graphical representation of a Cisco MDS 9000 Family switch chassis, a Cisco Nexus 5000 Series switch chassis, or a Cisco Nexus 7000 Series switch chassis including the installed switching modules, the supervisor modules, the status of each port within each module, the power supplies, and the fan assemblies.

Note Device Manager support for Cisco Nexus 7000 Series switches is only for FCoE. Non-FCoE modules appear as Unsupported Card.

The tables in the DCNM-SAN Information pane basically correspond to the dialog boxes that appear in Device Manager. However, while DCNM-SAN tables show values for one or more switches, a Device Manager dialog box shows values for a single switch. Also, Device Manager provides more detailed information for verifying or troubleshooting device-specific configuration than DCNM-SAN.

Device Manager Release 4.2 and later provides enhanced security using multiple perspectives (simple and advanced) allowing role based-access to its features. The Device Manager perspective filters out menu items that are not relevant to the user. Users with server admin role, can only access a subset of the fabric related features. The server admin role will not be able to manage Device Manager users or connected clients.

Device Manager Release 5.0 and later supports all the software features that are offered by Cisco NX-OS for managing Cisco MDS 9148 and 9124 Multilayer Fabric switches. Cisco MDS 9148 Multilayer Fabric Switch is a 48-port (1/2/4/8G) FC 1RU switch based on the Sabre ASIC andCisco MDS 9124 Multilayer Fabric switch is a 1/2/4/8G switch module for HP BladeServer based on the Sabre ASIC. Device Manager and DCNM-SAN allow you to discover, display, configure, monitor and service both these new switches. Device Manager also supports the following Cisco Nexus 2000 Series Fabric Extenders on a Cisco Nexus 5000 Series switch that runs Cisco NX-OS Release 5.0(1):

- Cisco Nexus 2148T Fabric Extender—It has four 10-Gigabit Ethernet fabric interfaces for its uplink connection to the parent Cisco Nexus 5000 Series switch and eight 1-Gigabit Ethernet or 10-Gigabit Ethernet host interfaces for its downlink connection to servers or hosts.
- Cisco Nexus 2232PP Fabric Extender—It has eight 10-Gigabit Ethernet fabric interfaces with SFP+ interface adapters for its uplink connection to the parent Cisco Nexus 5000 Series switch and 32 10-Gigabit Ethernet fabric interfaces with SFP+ interface adapters for its downlink connection to servers or hosts.
- Cisco Nexus 2248TP Fabric Extender—It has four 10-Gigabit Ethernet fabric interfaces with small form-factor pluggable (SFP+) interface adapters for its uplink connection to the parent Cisco Nexus 5000 Series switch and 48 1000BASE-T (1-Gigabit) Ethernet host interfaces for its downlink connection to servers or hosts.

Device Manager allows you to discover and display these Fabric Extenders. Cisco Device Manager and the Cisco DCNM-SAN client support provisioning and monitoring of the 48-port 8-Gbps Advanced Fibre Channel switching module (DS-X9248-256K9) and the 32-port 8-Gbps Advanced Fibre Channel switching module (DS-X9232-256K9).

Device Manager Features

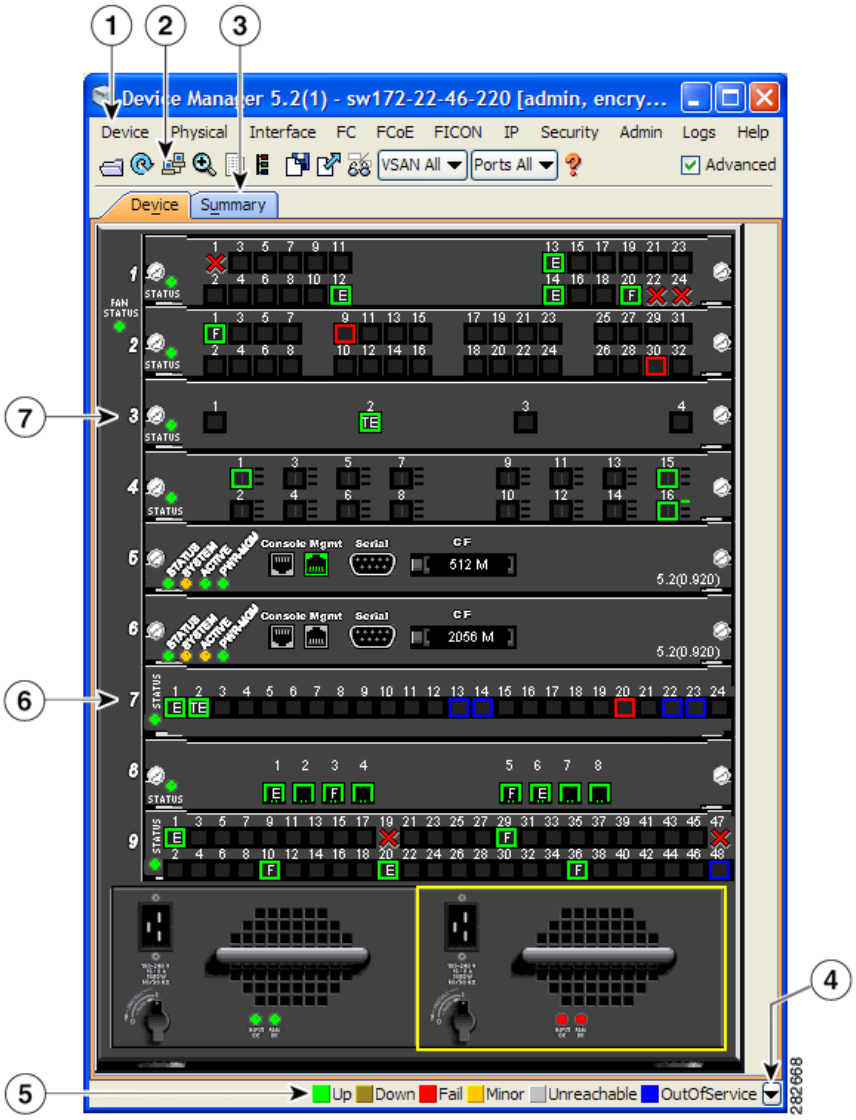
Device Manager provides two views: Device View and Summary View. Use Summary View to monitor interfaces on the switch. Use Device View to perform switch-level configurations including the following:

- Configure virtual Fibre Channel interfaces.
- Configure Fibre Channel over Ethernet (FCoE).
- Configure zones for multiple VSANs.
- Manage ports, PortChannels, and trunking.
- Manage SNMPv3 security access to switches.
- Manage CLI security access to the switch.
- Manage alarms, events, and notifications.
- Save and copy configuration files and software image.
- View hardware configuration.
- View chassis, module, port status, and statistics.

Using Device Manager Interface

This section describes the Device Manager interface as shown in Figure 10-1.

Figure 10-1 Device Manager, Device Tab



1	Menu bar	**5**	Status
2	Toolbar	**6**	Supervisor modules
3	Tabs	**7**	Switching or services modules
4	Legend		

Menu Bar

The menu bar at the top of the Device Manager main window provides options for managing and troubleshooting a single switch. The menu bar provides the following options:

- Device—Opens an instance of Device Manager, sets management preferences, sets the page layout, opens a Telnet/SSH session with the current switch, exports a device image, and closes the Device Manager application.
- Physical—Allows you to view and manage inventory, modules, temperature sensors, power supplies, fans, and the entire system.
- Interface—Allows you to configure and manage PortChannels, as well as Fibre Channel, Ethernet, iSCSI, and FICON ports. Also provides diagnostic, management and monitoring capabilities, as well as SPAN and port tracking.

Note The Interface > Port Channels menu option does not appear if the Cisco Nexus 5000 Series switch is in NPV mode and runs a Cisco NX-OS release prior to 4.2(1).

- FC—Allows you to configure and manage VSAN, domain, and name server characteristics. Also provides advanced configuration capabilities.
- FCoE—Allows you to configure the FCoE parameters and map VSANs to VLANs on a Cisco Nexus 5000 Series switch.

Note The FCoE menu option appears only if the Cisco Nexus 5000 Series switch runs Cisco NX-OS Release 4.0(1a) or later releases.

- FICON—Allows you to configure and manage FICON VSANs, configure RLIR ERL information, swap selected FICON ports, and view FICON port numbers.
- IP—Allows you to configure and manage the following types of information: FCIP, iSCSI, iSNS, routes, VRRP, and CDP.
- Security—Allows you to configure and manage FCSP, port security, iSCSI security, SNMP security, common roles, SSH, AAA, and IP ACLs.
- Admin—Allows you to save, copy, edit, and erase the switch configuration, monitor events, manipulate Flash files, manage licenses, configure NTP, use CFS, and reset the switch. Also enables you to use the **show tech support, show cores**, and **show image** commands.
- Logs—Shows the various logs: message, hardware, events, and accounting. Also displays FICON link incidents, and allows you to configure the syslog setup.
- Help—Displays online help topics for specific dialog boxes in the Information pane.

Toolbar Icons

The Device Manager toolbar provides quick access to many Device Manager features. Once the icon is selected, a dialog box may open that allows configuration of the feature. The toolbar provides the main Device and Summary View icons as shown in Table 10-1.

Table 10-1 Device Manager Main Toolbar

Icon	Description
 Open Device	Opens the Device Manager view for another switch, with the option to open this view in a separate window.
 Refresh Display	Communicates with the switch and displays the information in the Device Manager view.
 Command-Line Interface	Opens a separate CLI command window to the switch.
 Configure Selected	Opens a configuration dialog box for the selected component (line card or port).
 SysLog	Opens a window that lists the latest system messages that occurred on the switch.
 VSANs	Opens the VSAN dialog box that provides VSAN configuration for the switch.
 Save Configuration	Saves the current running configuration to the startup configuration.
 Copy	Copies configuration file between server and switch.
 Toggle FICON/Interface Port Labels	Toggles the FICON and interface port labels.
 Select VSAN	Filters the port display to show only those ports belonging to the selected VSAN.
 Help	Accesses online help for Device Manager.

Dialog Boxes

If a toolbar icon is selected, a dialog box may open that allows configuration of the selected feature. The dialog box may include table manipulation icons. See the "Information Pane" section on page 9-5 for descriptions of these icons.

Tabs

Click the **Device** tab on the Device Manager main window to see a graphical representation of the switch chassis and components.

Note The Device view also shows the switch chassis information of the Cisco Nexus 2000 Series Fabric Extenders (FEXs) that are connected to a Cisco Nexus 5000 Series switch that runs Cisco NX-OS Release 5.0(1).

Click the **Summary** tab on the Device Manager main window to see a summary of active interfaces on a single switch, as well as Fibre Channel and IP neighbor devices. The Summary View also displays port speed, link utilization, and other traffic statistics. There are two buttons in the upper left corner of the Summary View tab used to monitor traffic. To monitor traffic for selected objects, click the **Monitor Selected Interface Traffic Util%** button. To display detailed statistics for selected objects, click the **Monitor Selected Interface Traffic Details** button. You can set the poll interval, the type or Rx/Tx display, and the thresholds.

Note The Summary tab does not display the utilization statistics (Util%) of virtual Fibre Channel interfaces for Cisco Nexus 5000 Series switches that run Cisco NX-OS Release 4.2.

Legend

The legend at the bottom right of the Device Manager indicates port status, as follows:

Colors

- Green—The port is up.
- Brown—The port is administratively down.
- Red cross—The port is down or has failed as a result of either hardware failure, loopback Diagnostic failure, or link failure.
- Red square—The port is down or has failed as a result of failure other than described for red cross.
- Amber—The port has a minor fault condition as a result of either signal loss, synchronization loss, credit loss, LIP F8 receiver failure, non operational sequence receiver, or off-line sequence receiver failure.
- Gray—The port is unreachable.
- Blue—The port is out of service.

Labels

- X—Link failure
- E—ISL
- TE—Multi-VSAN ISL
- F—Host/storage
- FL—F loop
- I— iSCSI
- SD—SPAN destination

- CH—Channel
- CU—Control Unit
- NP—Proxy N-Port (NPV Mode)
- TNP—Trunking NP_Port (NPV Mode)
- TF—Trunking F_Port
- f—vFC Present (Cisco Nexus 5000 Series switches only)

Supervisor and Switching Modules

In the Device View, you can right-click an object and get information on it, or configure it. If you right-click a module, the menu shows the module number and gives you the option to configure or reset the module. If you right-click a port, the menu shows the port number and gives you the option to configure, monitor, enable/disable, set beacon mode, or perform diagnostics on the port.

Tip You can select multiple ports in Device Manager and apply options to all the selected ports at one time. Either select the ports by clicking the mouse and dragging it around them, or hold down the **Control** key and click each port.

To enable or disable a port, right-click the port and click **Enable** or **Disable** from the pop-up menu. To enable or disable multiple ports, drag the mouse to select the ports and then right-click the selected ports. Then click **Enable** or **Disable** from the pop-up menu.

To manage trunking on one or more ports, right-click the ports and click **Configure**. In the dialog box that appears, right-click the current value in the Trunk column and click **nonTrunk**, **trunk**, or **auto** from the pull-down list.

To create PortChannels using Device Manager, click **PortChannels** from the Interface menu.

Note To create a PortChannel, all the ports on both ends of the link must have the same port speed, trunking type, and administrative state.

Context Menus

Context menus are available in both Device Manager views by right-clicking a device or table.

From Device View:

- Device—Right-click a system, module, or power supply to bring up a menu that gives you the option to configure or reset the device.
- Port— Right-click a port to bring up a menu that shows you the number of the port you have clicked, and to give you the option to configure, monitor, enable, disable, set beacon mode, or perform diagnostics on the port.

From Summary View:

- Table— Right-click the table header to show a list of which columns to display in that table: Interface, Description, VSANs, Mode, Connected To, Speed (Gb), Rx, Tx, Errors, Discards, and Log. Click the Description field to bring up the appropriate configuration dialog box for the port type.

Launching Device Manager

To launch Device Manager from your desktop, double-click the **Device Manager** icon and follow the instructions described in the *Cisco DCNM Installation and Licensing Guide*.

DETAILED STEPS

Step 1 You can choose one of the following three steps

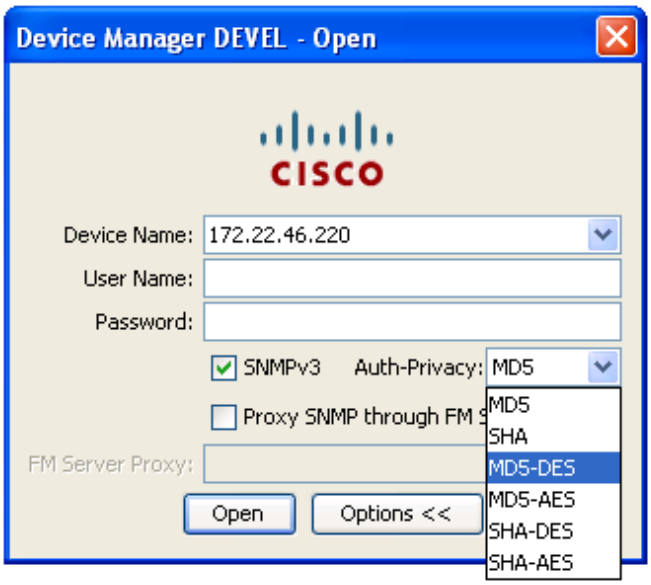
a. Right-click the switch you want to manage on the Fabric pane map and choose **Device Manager** from the menu that appears.

b. Double-click a switch in the Fabric pane map.

c. Select a switch in the Fabric pane map and choose **Tools > Device Manager**.

You see the Device Manager open dialog box as shown in Figure 10-2

Figure 10-2 Device Manager: Open Dialog Box



Step 2 Enter the IP adress of the device.

Step 3 Enter the user name and password.

Step 4 Check the Proxy SNMP through FMS check box if you want Device Manager Client to use a TCP-based proxy server.

Step 5 Choose the Auth-Privacy option according to the privacy protocol you have configured on your switch:

a. If you have not configured the switch with a privacy protocol, then choose Auth-Privacy option MD5 (no privacy).

b. If you have configured the switch with your privacy protocol, choose your Auth-Privacy choice.

Step 6 Click **Open** to open the Device Manager.

Setting Device Manager Preferences

To set your preferences for the behavior of the Device Manager application, choose **Device > Preferences** from the Device menu. You can set the following preferences:

- **Retry Requests x Time(s) After x sec Timeout**—Allows you to set the retry request values. The default settings are 1 time after a 5-second timeout.
- **Enable Status Polling Every x secs**—Allows you to set the status polling value. The default setting is enabled (checked) with a time of 40 seconds.
- **Trace SNMP Packets in Message Log**—Allows you to set whether Device Manager traces SNMP packets and logs the trace. The default setting is disabled (unchecked).
- **Register for Events After Open, Listen on Port 1163**—Allows you to register this switch so that events are logged once you open Device Manager. The default setting is enabled (checked).
- **Show WorldWideName (WWN) Vendor**—Displays the world wide name vendor name in any table or listing displayed by Device Manager. If **Prepend** is checked, the name is displayed in front of the IP address of the switch. If **Replace** is checked, the name is displayed instead of the IP address. The default setting is enabled (checked) with the **Prepend** option.
- **Show Timestamps as Date/Time**—Displays timestamps in the date/time format. If this preference is not checked, timestamps are displayed as elapsed time. The default setting is enabled (checked).
- **Telnet Path**—Sets the path for the telnet.exe file on your system. The default is **telnet.exe**, but you need to browse for the correct location.

  Note If you browse for a path or enter a path and you have a space in the pathname (for example, **c:\program files\telnet.exe**, then the path will not work. To get the path to work, manually place quotes around it (for example, **"c:\program files\telnet.exe"**).

- **Use Secure Shell Instead of Telnet**—Specifies whether to use SSH or Telnet when using the CLI to communicate with the switch. If enabled, you must specify the path to your SSH application. The default setting is disabled.
- **CLI Session Timeout x secs (0= disable)**—Specifies the timeout interval for a CLI session. Enter 0 to disable (no timeout value). The default setting is 30 seconds.
- **Show Tooltips in Physical View**—Determines whether tooltips are displayed in Physical (Device) View. The default setting is enabled (checked).
- **Label Physical View Ports With:**—Specifies the type of label to assign to the ports when you are in Physical (Device) View. The options are FICON and Interface. The default setting is Interface.
- **Export Table**—Specifies the type of file that is created when you export a table using Device Manager. The options are Tab-Delimited or XML. The default setting is Tab-Delimited.

Configuring Performance Manager

This chapter describes how DCNM-SAN is used to monitor and manage a network. This chapter includes the following topics:

Information About Performance Manager

This section includes the following topics:

Performance Manager gathers network device statistics historically and provides this information graphically using a web browser. It presents recent statistics in detail and older statistics in summary. Performance Manager also integrates with external tools such as Cisco Traffic Analyzer.

The Performance Manager has three operational stages:

- Definition—The Flow Wizard sets up flows in the switches.
- Collection—The Web Server Performance Collection screen collects information on desired fabrics.
- Presentation—Generates web pages to present the collected data through DCNM-SAN Web Server.

Performance Manager can collect statistics for ISLs, hosts, storage elements, and configured flows. Flows are defined based on a host-to-storage (or storage-to-host) link. Performance Manager gathers statistics from across the fabric based on collection configuration files. These files determine which SAN elements and SAN links Performance Manager gathers statistics for. Based on this configuration, Performance Manager communicates with the appropriate devices (switches, hosts, or storage elements) and collects the appropriate information at fixed five-minute intervals.

Performance Manager uses a round-robin database to hold the statistical data collected from the fabric. This data is stored based on the configured parameters in the collection configuration file. At each polling interval, Performance Manager gathers the relevant statistics and stores them in the round-robin database. This database is a fixed size and will not grow beyond its preset limits.

Performance Manager creates a series of archived data to hold summarized information present in the real-time round-robin database. This archived data is used to generate daily, weekly, monthly, and yearly consolidated reports. In this way, Performance Manager maintains significant historical data without the cost of an ever-increasing database size.

Note You must restart Performance Manager if you change the user credentials on DCNM-SAN Server.

Data Interpolation

One of the unique features of Performance Manager is its ability to interpolate data when statistical polling results are missing or delayed. Other performance tools may store the missing data point as zero, but this can distort historical trending. Performance Manager interpolates the missing data point by comparing the data point that preceded the missing data and the data point stored in the polling interval after the missing data. This maintains the continuity of the performance information.

Data Collection

One year's worth of data for two variables (Rx and Tx bytes) requires a round-robin database (rrd) file size of 76 K. If errors and discards are also collected, the rrd file size becomes 110 K. The default internal values are as follows:

- 600 samples of 5 minutes (2 days and 2 hours)
- 700 samples of 30 minutes (14 days)
- 775 samples of 2 hours (64 days)
- 300 samples of 1 day

A 1000-port SAN requires 110 MB for a year's worth of historical data that includes errors and discards. If there were 20 switches in this SAN with equal distribution of fabric ports, about two to three SNMP packets per switch would be sent every 5 minutes for a total of about 100 request or response SNMP packets required to monitor the data.

Because of their variable counter requests, flows are more difficult to predict storage space requirements for. But in general you can expect that, each extra flow adds another 76 KB.

Note Performance Manager does not collect statistics on non-manageable and non-MDS switches. Loop devices (FL/NL) are not collected.

To setup a shared RRD path to collect PM data, perform these steps:

Step 1 Locate the server.properties file.

For Windows setup, location is: `C:\Program Files\Cisco Systems\dcm\fm\conf`

For Linux setup, locatio is: `/usr/local/cisco/dcm/fm/conf`.

Step 2 Add **pm.rrdpath** property file information to the server.properties file.

For example:

Add server location accessible from the DCNM server in the format:

```
pm.rrdpath=\\server_ip\\public\\cisco\\data
```

Step 3 Save the **server.properties** file.

Step 4 Restart the Cisco DCNM server.

Note After the Performance Manager server is ready, the new updated location will be used to save the RRD files. Performance Manager creates a new directory `pm\db` under the specified location. Ensure that RRD files are not altered, as the Performance Manager server is actively writing into the rrd files.

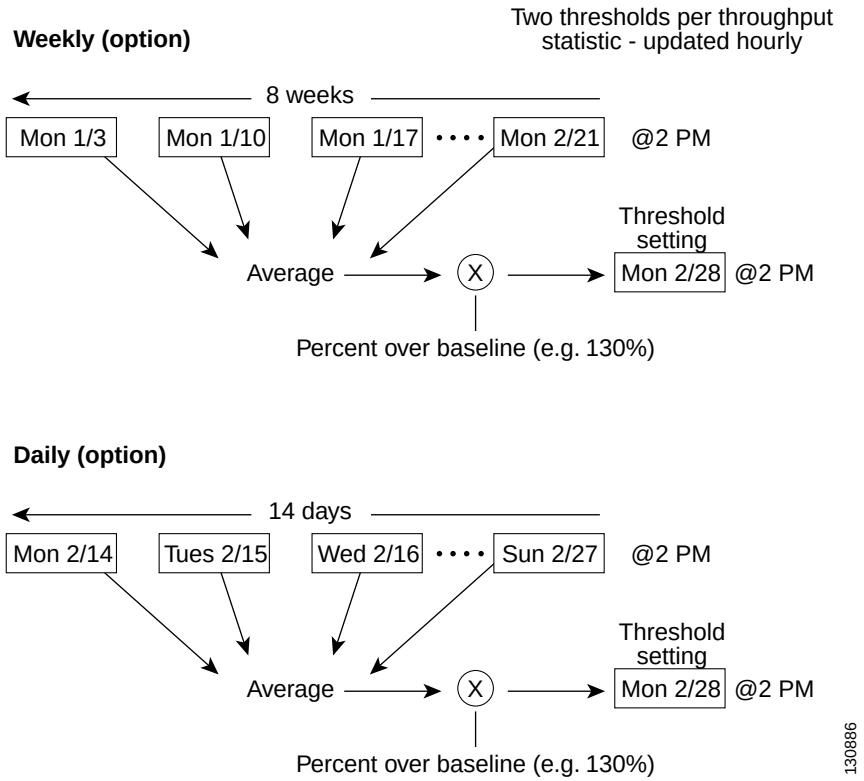
Using Performance Thresholds

The Performance Manager Configuration Wizard allows you to set up two thresholds that will trigger events when the monitored traffic exceeds the percent utilization configured. These event triggers can be set as either Critical or Warning events that are reported on the DCNM-SAN web client Events browser page.

Absolute value thresholds apply directly to the statistics gathered. These statistics, as a percent of the total link capacity, are compared to the percent utilization configured for the threshold type. If the statistics exceed either configured threshold, an event is shown on the DCNM-SAN web client Events tab.

Baseline thresholds create a threshold that adapts to the typical traffic pattern for each link for the same time window each day, week, or every two weeks. Baseline thresholds are set as a percent of the average (110% to 500%), where 100% equals the calculated weighted average. Figure 11-1 shows an example of setting a baseline threshold for a weekly or daily option.

Figure 11-1 Baseline Threshold Example



The threshold is set for Monday at 2 p.m. The baseline threshold is set at 130% of the average for that statistic. The average is calculated from the statistics value that occurred at 2 p.m. on Monday, for every prior Monday (for the weekly option) or the statistics value that occurred at 2 p.m. on each day, for every prior day (for the daily option).

Flow Statistics

Flow statistics count the ingress traffic in the aggregated statistics table. You can collect two kinds of statistics:

- Aggregated flow statistics to count the traffic for a VSAN.
- Flow statistics to count the traffic for a source and destination ID pair in a VSAN.

If you enable flow counters, you can enable a maximum of 1 K entries for aggregate flow and flow statistics. Be sure to assign an unused flow index to a module for each new flow. Flow indexes can be repeated across modules. The number space for flow index is shared between the aggregate flow statistics and the flow statistics.

Generation 1 modules allow a maximum of 1024 flow statements per module. Generation 2 modules allow a maximum of 2048-128 flow statements per module.

Table 11-1 explains the Flow Type radio button that defines the type of traffic monitored.

Table 11-1 Performance Manager Flow Types

Flow type	Description
Host->Storage	Unidirectional flow, monitoring data from the host to the storage element
Storage->Host	Unidirectional flow, monitoring data from the storage element to the host
Both	Bidirectional flow, monitoring data to and from the host and storage elements

Flow Setup Wizards

The Performance Manager Flow and Performance Manager Setup wizards greatly simplify configuration. All you need to do is select the categories of statistics to capture and the wizards provide a list of flows and links to monitor. You can remove entries if desired, or just accept the provided list and start data collection. Statistics for host and storage links are not associated with a specific port on a switch, so you do not lose long term statistics if a connection is moved to a different port.

Creating a Flow Using Performance Manager Flow Wizard

DETAILED STEPS

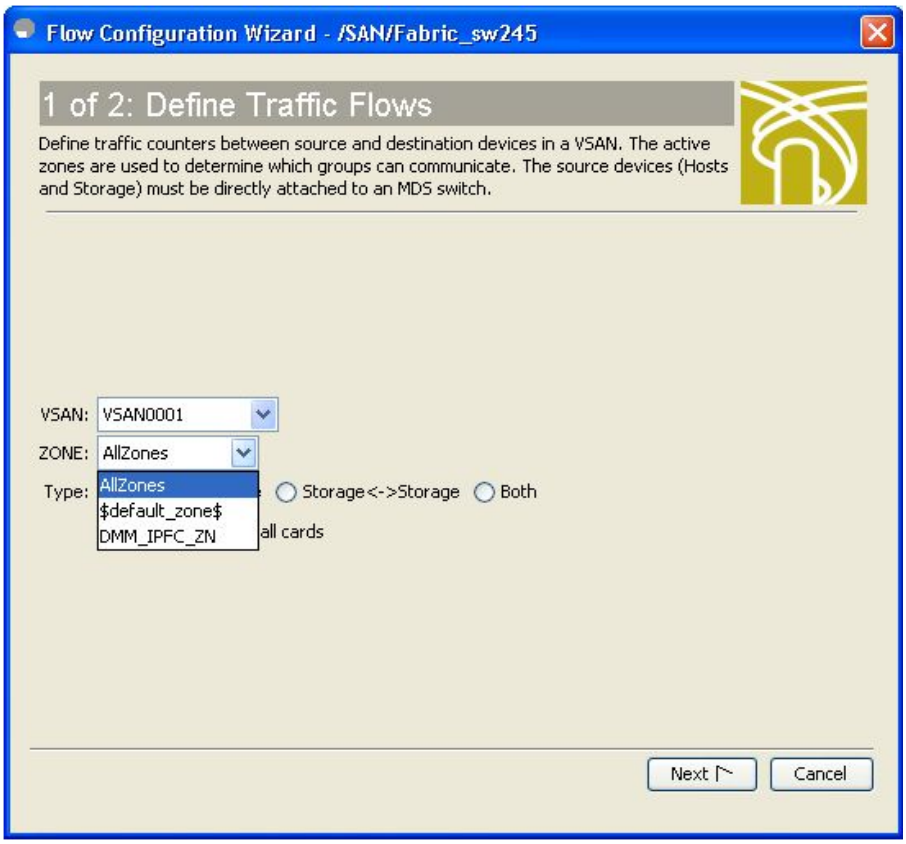
Step 1 Choose **Performance > Create Flows**.

Specify how you want to determine and add new flows as shown in Figure 11-2. For this, you have to define traffic counters between source and destination devices, via one of these options:

- In a VSAN - For this option, click **VSAN**.
- Based on high traffic devices - For this option, click **Device Traffic**. Note that PM collections must already be turned on in order to use this option. If PM collection is not turned on for the selected fabric, then an error message will appear and you cannot continue.

Step 2 If you have clicked **VSAN**, then:

Figure 11-2 Create Flows Dialog Box



a. Click the drop-down menu in the VSAN field.

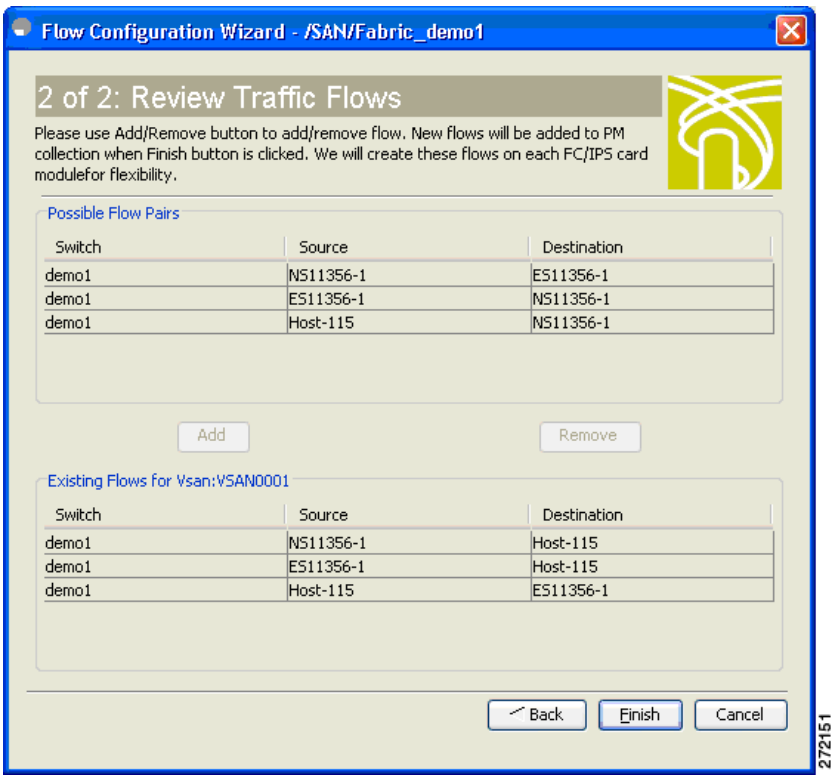
b. Choose the list of VSANs provided by the flow configuration wizard.

c. Click the drop-down menu in the Zone field.

d. Choose the list of zones provided by the flow configuration wizard.

e. Click **Next** to continue to the next windowas shown in Figure 11-3).

Figure 11-3 Review Traffic Flows Dialog Box



f. Choose items in the Possible Flow Pairs area.

g. The Review Traffic Flows window displays all VSAN flow pairs in the Exisitng Flows for Vsan area.

h. Click **Add** to create the selected flow.

i. Choose items in the Existing Flows for Vsan area.

j. Click **Remove** to remove the selected flow.

Step 3 If you have clicked **Device Traffic**, then:

a. Click **Next**.

You see the Define Traffic Flows page.

b. Specify a traffic utilization percentage threshold vlaue in the Show device ports with traffic > text box.

c. Specify whether you want to look at the peak or average traffic values, over the last day or last week, for the traffic types:

- Host<->Storage
- Storage<->Storage
- Both

d. Click **Next**.

If new flow pairs are found, you will see the Review Traffic Flows page, where possible flow pairs are shown in a table, along with the traffic parameters used to identify them.

e. To see only rows having a specific source or destination device, specify the name of the device in the **Filter** text box.

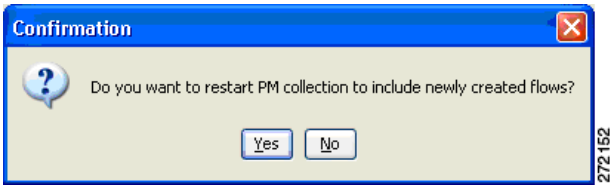
f. To create a flow, click the corresponding row in the Possible Flow Pairs table, and then click **Add**.

To remove an existing flow, click the corresponding row in the Existing Flow Pairs table, and then click **Remove**.

Step 4 Click **Finish** to restart the Performance Manager collection.

You see the Confirmation dialog box as shown in Figure 11-4.

Figure 11-4 Confirmation Dialog Box



To verify the newly created flow, choose **Physical Attributes > End Devices > Flow Statistics.** The newly created flows are displayed.

Note Performance Manager Collection can be enabled for LAN devices and traffice counters are collected periodically.

Monitoring the Network

This chapter describes how the DCNM-SAN manages the network. In particular, SAN discovery and network monitoring are two of its key network management capabilities.

This chapter contains the following sections:

Information About Network Monitoring

DCNM-SAN provides extensive SAN discovery, topology mapping, and information viewing capabilities. DCNM-SAN collects information on the fabric topology through SNMP queries to the switches connected to it. DCNM-SAN recreates a fabric topology, presents it in a customizable map, and provides inventory and configuration information in multiple viewing options such as fabric view, device view, summary view, and operation view.

Once DCNM-SAN is invoked, a SAN discovery process begins. Using information polled from a seed Cisco MDS 9000 Family switch, including Name Server registrations, Fibre Channel Generic Services (FC-GS), Fabric Shortest Path First (FSPF), and SCSI-3, DCNM-SAN automatically discovers all devices and interconnects on one or more fabrics. All available switches, host bus adapters (HBAs), and storage devices are discovered. The Cisco MDS 9000 Family switches use Fabric-Device Management Interface (FMDI) to retrieve the HBA model, serial number and firmware version, and host operating-system type and version discovery without host agents. DCNM-SAN gathers this information through SNMP queries to each switch. The device information discovered includes device names, software revision levels, vendor, ISLs, PortChannels, and VSANs.

Monitoring Health and Events

DCNM-SAN works with the Cisco MDS 9000 Family switches to show the health and status of the fabric and switches. Information about the fabric and its components is gathered from multiple sources, including Online System Health Management, Call Home, system messages, and SNMP notifications. This information is then made available from multiple menus on DCNM-SAN or Device Manager.

DCNM-SAN Events Tab

The DCNM-SAN Events tab, available from the topology window, displays the events DCNM-SAN received from sources within the fabric. These sources include SNMP events, RMON events, system messages, and system health messages. The Events tab shows a table of events, including the event name, the source and time of the event, a severity level, and a description of the event. The table is sortable by any of these column headings.

Note Cisco DCNM SAN client displays events that are created after the client session is started. Any event created before the current user login session will not be retrieved and displayed.

Event Information in DCNM-SAN Web Server Reports

The DCNM-SAN web server client displays collections of information gathered by the Performance Manager. This information includes events sent to the DCNM-SAN Server from the fabric. To open these reports, choose **Performance Manager > Reports**. This opens the web client in a web browser and displays a summary of all fabrics monitored by the DCNM-SAN Server. Choose a fabric and then click the **Events** tab to see a summary or detailed report of the events that have occurred in the selected fabric. The summary view shows how many switches, ISLs, hosts, or storage elements are down on the fabric and how many warnings have been logged for that SAN entity. The detailed view shows a list of all events that have been logged from the fabric and can be filtered by severity, time period, or type.

Events in Device Manager

Device Manager displays the events when you choose **Logs > Events**. Device Manager can display the current list of events or an older list of events that has been stored on the DCNM-SAN host. The event table shows details on each event, including time, source, severity, and a brief description of the event.

SAN Discovery and Topology Mapping

DCNM-SAN provides extensive SAN discovery, topology mapping, and information viewing capabilities. DCNM-SAN collects information on the fabric topology through SNMP queries to the switches connected to it. DCNM-SAN recreates a fabric topology, presents it in a customizable map, and provides inventory and configuration information in multiple viewing options.

Device Discovery

Once DCNM-SAN is invoked, a SAN discovery process begins. Using information polled from a seed Cisco MDS 9000 Family switch, including Name Server registrations, Fibre Channel Generic Services (FC-GS), Fabric Shortest Path First (FSPF), and SCSI-3, DCNM-SAN automatically discovers all devices and interconnects on one or more fabrics. All available switches, host bus adapters (HBAs), and storage devices are discovered. The Cisco MDS 9000 Family switches use Fabric-Device Management Interface (FMDI) to retrieve HBA model, serial number and firmware version, and host operating-system type and version discovery without host agents. DCNM-SAN gathers this information through SNMP queries to each switch. The device information discovered includes device names, software revision levels, vendor, ISLs, PortChannels, and VSANs.

For a VSAN change involving a third-party switch, DCNM-SAN will need a second discovery to show the correct topology due to the discovery dependency when there is any change in a mixed VSAN. The first discovery finds the third-party switch and the subsequent discovery will show the information on which VSAN it is going to join and can discover the end devices connected to it. You can wait for the subsequent discovery or trigger a manual discovery.

Topology Mapping

DCNM-SAN is built upon a topology representation of the fabric. DCNM-SAN provides an accurate view of multiple fabrics in a single window by displaying topology maps based on device discovery information. You can modify the topology map icon layout with an easy-to-use, drag-and-drop interface. The topology map visualizes device interconnections, highlights configuration information such as zones, VSANs, and ISLs exceeding utilization thresholds. The topology map also provides a visual context for launching command-line interface (CLI) sessions, configuring PortChannels, and opening device managers.

Using the Topology Map

The DCNM-SAN topology map can be customized to provide a view into the fabric that varies from showing all switches, end devices, and links, to showing only the core switches with single bold lines for any multiple links between switches. Use the icons along the left side of the topology map to control these views or right-click anywhere in the topology map to access the map controls.

You can zoom in or out on the topology map to see an overview of the SAN or focus on an area of importance. You can also open an overview window that shows the entire fabric. From this window, you can right-click and draw a box around the area you want to view in the main topology map view.

Another way to limit the scope of the topology display is to select a fabric or VSAN from the Logical Domains pane. The topology map displays only that fabric or VSAN.

Moving the mouse pointer over a link or switch provides a simple summary of that SAN component, along with a status indication. Right-clicking on the component brings up a pop-up menu. You can view the component in detail or access configuration or test features for that component.

Double-click a link to bring link status and configuration information to the information pane. Double-click a switch to bring up Device Manager for that switch.

Saving a Customized Topology Map Layout

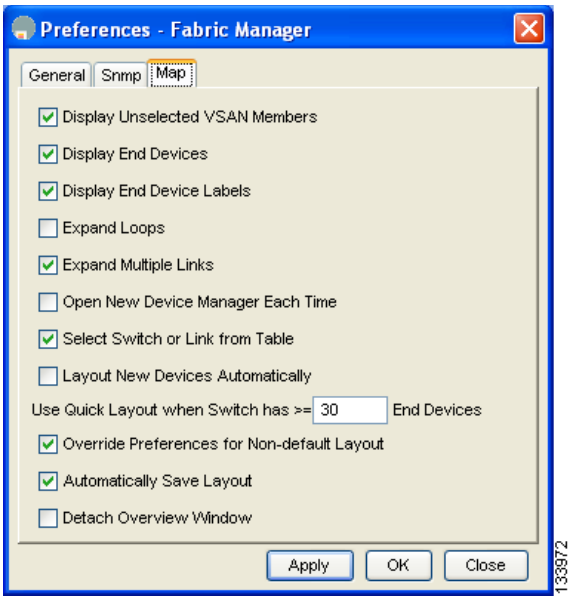
Changes made to the topology map can be saved so that the customized view is available any time you open the DCNM-SAN Client for that fabric.

DETAILED STEPS

Step 1 Click **File > Preferences** to open the DCNM-SAN preferences dialog box.

Step 2 Click the **Map** tab and check the **Automatically Save Layout** check box to save any changes to the topology map as shown in Figure 12-1.

Figure 12-1 DCNM-SAN Preferences



Step 3 Click **Apply,** and then click **OK** to save this change.

Using Enclosures with DCNM-SAN Topology Maps

Because not all devices are capable of responding to FC-GS-3 requests, different ports of a single server or storage subsystem may be displayed as individual end devices on the topology map. See the "Modifying the Device Grouping" section on page 9-33 to group these ports into a single enclosure for DCNM-SAN.

Clicking **Alias->Enclosure** displays hosts and storage elements in the Information pane. This is a shortcut to naming enclosures. To use this shortcut, highlight each row in the host or storage table that you want grouped in an enclosure then click **Alias -> Enclosure**. This automatically sets the enclosure names of each selected row with the first token of the alias.

Mapping Multiple Fabrics

To log into multiple fabrics, the same username and password must be used. The information for both fabrics is displayed, with no need to select a seed switch. To see details of a fabric, click the tab for that fabric at the bottom of the Fabric pane, or double-click the fabric's cloud icon. To continuously manage a fabric using DCNM-SAN, follow the instructions in the "Managing a Cisco DCNM-SAN Server Fabric" section on page 7-4.

Inventory Management

The Information pane in DCNM-SAN shows inventory, configuration, and status information for all switches, links, and hosts in the fabric. Inventory management includes vendor name and model, and software or firmware versions. Select a fabric or VSAN from the Logical Domains pane, and then select the **Summary** tab in the Information pane to get a count of the number of VSANS, switches, hosts, and

storage elements in the fabric. See the "Cisco DCNM-SAN Client Quick Tour: Admin Perspective" section on page 9-6 for more information on the DCNM-SANDCNM-SAN user interface.

Using the Inventory Tab from DCNM-SAN Web Server

If you have configured DCNM-SAN Web Server, you can launch this application and access the Inventory tab to see a summary of the fabrics managed by the DCNM-SAN Server. The Inventory tab shows an inventory of the selected SAN, fabric, or switch. See Chapter 4, "Cisco DCNM Web Client" for more information on how to configure and use DCNM-SAN Web Server.

DETAILED STEPS

Step 1 Point your browser at the DCNM-SAN Web Server.

Step 2 Click the **Events** tab and then the **Details** tab to view the system messages. The columns in the events table are sortable. In addition, you can use the Filter button to limit the scope of messages within the table.

Viewing Logs from Device Manager

You can view system messages from Device Manager if Device Manager is running from the same workstation as the DCNM-SAN Server. Choose **Logs > Events > current** to view the system messages on Device Manager. The columns in the events table are sortable. In addition, you can use the Find button to locate text within the table.

You can view switch-resident logs even if you have not set up your local syslog server or your local PC is not in the switch's syslog server list. Due to memory constraints, these logs will wrap when they reach a certain size. The switch syslog has two logs: an NVRAM log that holds a limited number of critical and greater messages and a nonpersistent log that contains notice or greater severity messages. Hardware messages are part of these logs.

Note To view syslog local logs, you need to configure the IP address of the DCNM-SAN Server in the syslog host.

Monitoring Performance

This chapter describes how to configure Performance Monitoring tools for Cisco DCNM-SAN and Device Manager. These tools provide real-time statistics as well as historical performance monitoring.

This chapter contains the following sections:

Information About Performance Monitoring

Device Manager provides an easy tool for monitoring ports on the Cisco MDS 9000 Family switches. This tool gathers statistics at a configurable interval and displays the results in tables or charts. Real-time performance statistics are useful for dynamic troubleshooting and fault isolation within the fabric. Real-time statistics gather data on parts of the fabric in user-configurable intervals and display these results in DCNM-SAN and Device Manager. For a selected port, you can monitor any of a number of statistics including traffic in and out, errors, class 2 traffic, and FICON data.

Real-Time Performance Monitoring

Device Manager provides an easy tool for monitoring ports on the Cisco MDS 9000 Family switches. This tool gathers statistics at a configurable interval and displays the results in tables or charts. These statistics show the performance of the selected port in real-time and can be used for performance monitoring and troubleshooting. For a selected port, you can monitor any of a number of statistics including traffic in and out, errors, class 2 traffic, and FICON data. You can set the polling interval from ten seconds to one hour, and display the results based on a number of selectable options including absolute value, value per second, and minimum or maximum value per second.

Device Manager checking for oversubscription on the host-optimized four-port groups on relevant modules. Right-click the port group on a module and choose **Check Oversubscription** from the pop-up menu.

Device manager provides two performance views: the Summary View tab and the configurable monitor option per port.

Historical Performance Monitoring

Performance Manager gathers network device statistics historically and provides this information using DCNM-SAN client and web browser. It presents recent statistics in detail and older statistics in summary. Performance Manager also integrates with external tools such as Cisco Traffic Analyzer. See the "Information About Performance Manager" section on page 11-1 for an overview of Performance Manager.

Configuring Performance Manager

This section includes the following topics:

Creating a Flow with Performance Manager

With the Flow Configuration Wizard you can create host-to-storage, storage-to-host, or bidirectional flows. Once defined, you can add these flows to a collection configuration file to monitor the traffic between a host/storage element pair. The flows created become part of the collection options in the Performance Manager Configuration Wizard.

Creating a Collection with Performance Manager

The Performance Manager Configuration Wizard steps you through the process of creating collections using configuration files. Collections are defined for one or all VSANs in the fabric. Collections can include statistics from the SAN element types described in Table 13-1.

Table 13-1 Performance Manager Collection Types

Collection Type	Description
ISLs	Collects link statistics for ISLs.
Host	Collects link statistics for SAN hosts.
Storage	Collects link statistics for a storage elements.
Flows	Collects flow statistics defined by the Flow Configuration Wizard.

Using Performance Thresholds

The Performance Manager Configuration Wizard allows you to set up two thresholds that trigger events when the monitored traffic exceeds the percent utilization configured. These event triggers can be set as either Critical or Warning events that are reported on the DCNM-SAN web client Events browser page.

You must choose either absolute value thresholds or baseline thresholds that apply to all transmit or receive traffic defined in the collection. Click the **Use absolute values** radio button on the last screen of the Performance Manager Configuration Wizard to configure thresholds that apply directly to the statistics gathered. These statistics, as a percent of the total link capacity, are compared to the percent utilization configured for the threshold type. If the statistics exceed either configured threshold, an event is shown on the DCNM-SAN web client Events tab.

As an example, the collection has absolute value thresholds set for 60% utilization (for warning) and 80% utilization (for critical). If Performance Manager detects that the traffic on a 1-Gigabit link in its collection exceeds 600 Mbps, a warning event is triggered. If the traffic exceeds 800 Mbps, a critical event is triggered.

Baseline thresholds are defined for a configured time of day or week (1 day, 1 week, or 2 weeks). The baseline is created by calculating the average of the statistical results for the configured time each day, week, or every 2 weeks. Table 13-2 shows an example of the statistics used to create the baseline value for a collection defined at 4 pm on a Wednesday.

Table 13-2 Baseline Time Periods for a Collection Started on Wednesday at 4pm

Baseline Time Window	Statistics Used in Average Calculation
1 day	Every prior day at 4 pm
1 week	Every prior Wednesday at 4 pm
2 weeks	Every other prior Wednesday at 4 pm

Baseline thresholds create a threshold that adapts to the typical traffic pattern for each link for the same time window each day, week, or every 2 weeks. Baseline thresholds are set as a percent of the average (110% to 500%), where 100% equals the calculated average.

As an example, a collection is created at 4 pm on Wednesday, with baseline thresholds set for 1 week, at 150% of the average (warning) and 200% of the average (critical). Performance Manager recalculates the average for each link at 4 pm every Wednesday by taking the statistics gathered at that time each Wednesday since the collection started. Using this as the new average, Performance Manager compares each received traffic statistic against this value and sends a warning or critical event if the traffic on a link exceeds this average by 150% or 200% respectively.

Table 13-3 shows two examples of 1-Gigabit links with different averages in our example collection and at what traffic measurements the Warning and Critical events are sent.

Table 13-3 Example of Events Generated for 1-Gigabit Links

Average	Warning Event Sent at 150%	Critical Event Sent at 200%
400 Mbps	600 Mbps	800 Mbps
200 Mbps	300 Mbps	400 Mbps

Set these thresholds on the last screen of the Collections Configuration Wizard by checking the **Send events if traffic exceeds threshold** check box.

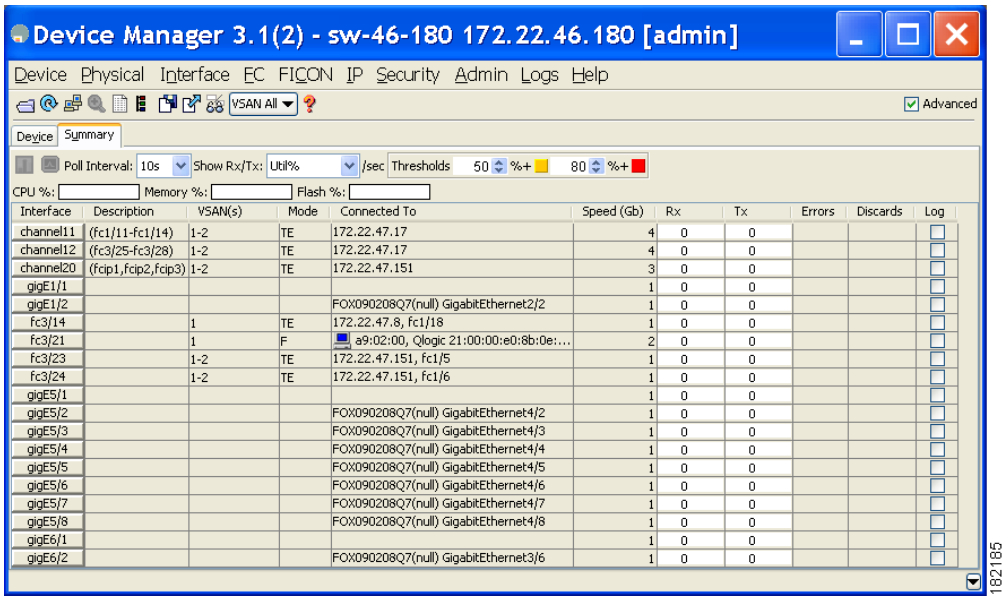
Configuring the Summary View in Device Manager

DETAILED STEPS

Step 1 Click the **Summary** tab on the main display.

You see all of the active ports on the switch, as well as the configuration options available from the Summary view shown in Figure 13-1.

Figure 13-1 Device Manager Summary Tab



Step 2 Choose a value from the Poll Interval drop-down list.

Step 3 Decide how you want your data to be interpreted by looking at the Show Rx/Tx drop-down menu. The table updates each polling interval to show an overview of the receive and transmit data for each active port on the switch.

Step 4 Select a value from the **Show Rx/Tx** drop-down list. If you select **Util%**, you need to also select values from the two **Show Rx/Tx > %Util/sec** drop-down lists. The first value is the warning level and the second value is the critical threshold level for event reporting.

Note that you can also display percent utilization for a single port by selecting the port and clicking the **Monitor Selected Interface Traffic Util %** icon.

Configuring Per Port Monitoring using Device Manager

The configurable monitor per port option gives statistics for in and out traffic on that port, errors, class 2 traffic and other data that can be graphed over a period of time to give a real-time view into the performance of the port.

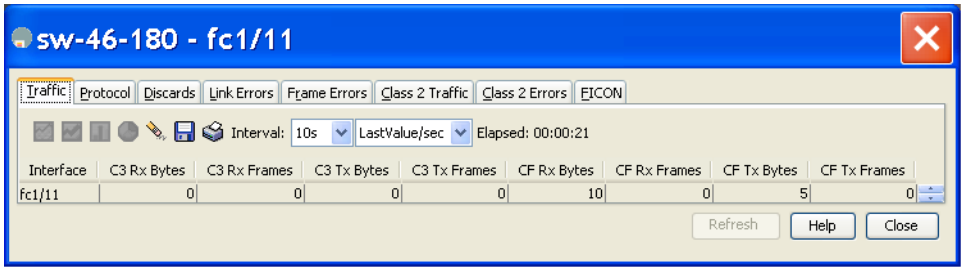
DETAILED STEPS

Step 1 Click the **Device** tab.

Step 2 Right-click the port you are interested in and choose **Monitor** from the drop-down menu.

You see the port real-time monitor dialog box shown in Figure 13-2.

Figure 13-2 Device Manager Monitor Dialog Box



Step 3 Select a value from the Interval drop-down list to determine how often data is updated in the table shown here.

Step 4 Click a statistical value in the table then click one of the graphing icons to display a running graph of that statistic over time. You see a graph window that contains options to change the graph type.

Tip You can open multiple graphs for statistics on any of the active ports on the switch.

Displaying DCNM-SAN Real-Time ISL Statistics

This section includes the following topics:

- "Viewing Performance Statics Using DCNM-SAN" section on page 13-6

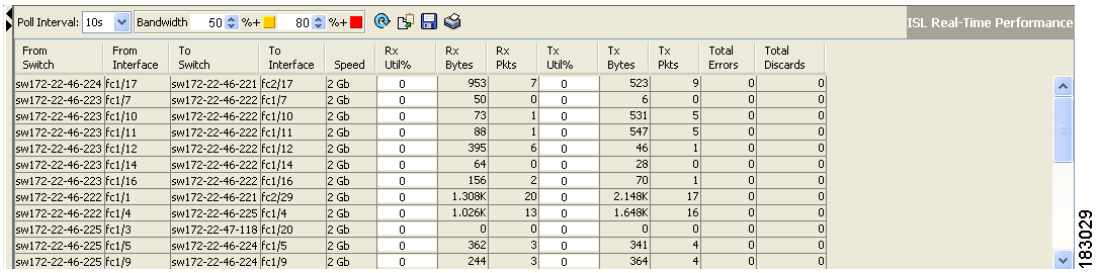
You can configure DCNM-SAN to gather ISL statistics in real time. These ISL statistics include receive and transmit utilization, bytes per second, as well as errors and discards per ISL.

DETAILED STEPS

Step 1 Choose **Performance > ISLs in Real-Time**.

You see any ISL statistics in the Information pane as shown in Figure 13-3.

Figure 13-3 ISL Performance in Real Time



From Switch	From Interface	To Switch	To Interface	Speed	Rx Util%	Rx Bytes	Rx Pkts	Tx Util%	Tx Bytes	Tx Pkts	Total Errors	Total Discards
sw172-22-46-224	fc1/17	sw172-22-46-221	fc2/17	2 Gb	0	953	7	0	523	9	0	0
sw172-22-46-223	fc1/7	sw172-22-46-222	fc1/7	2 Gb	0	50	0	0	6	0	0	0
sw172-22-46-223	fc1/10	sw172-22-46-222	fc1/10	2 Gb	0	73	1	0	531	5	0	0
sw172-22-46-223	fc1/11	sw172-22-46-222	fc1/11	2 Gb	0	88	1	0	547	5	0	0
sw172-22-46-223	fc1/12	sw172-22-46-222	fc1/12	2 Gb	0	395	6	0	46	1	0	0
sw172-22-46-223	fc1/14	sw172-22-46-222	fc1/14	2 Gb	0	64	0	0	28	0	0	0
sw172-22-46-223	fc1/16	sw172-22-46-222	fc1/16	2 Gb	0	156	2	0	70	1	0	0
sw172-22-46-222	fc1/1	sw172-22-46-221	fc2/29	2 Gb	0	1.308K	20	0	2.148K	17	0	0
sw172-22-46-222	fc1/4	sw172-22-46-225	fc1/4	2 Gb	0	1.026K	13	0	1.648K	16	0	0
sw172-22-46-225	fc1/3	sw172-22-47-118	fc1/20	2 Gb	0	0	0	0	0	0	0	0
sw172-22-46-225	fc1/5	sw172-22-46-224	fc1/5	2 Gb	0	362	3	0	341	4	0	0
sw172-22-46-225	fc1/9	sw172-22-46-224	fc1/9	2 Gb	0	244	3	0	364	4	0	0

Step 2 Select a value from the **Poll Interval** drop-down list.

Step 3 Select two values from the **Bandwidth** utilization thresholds drop-down lists, one value for the minor threshold and one value for the major threshold.

The table shown updates each polling interval to show the statistics for all configured ISLs in the fabric.

Step 4 Select a row in the table to highlight that ISL in blue in the Topology map.

Viewing Performance Statics Using DCNM-SAN

You can configure DCNM-SAN to gather historic and real time statistics of ISLs or End devices. These statistics include receive and transmit utilization, bytes per second, as well as errors and discards per ISL or end device.

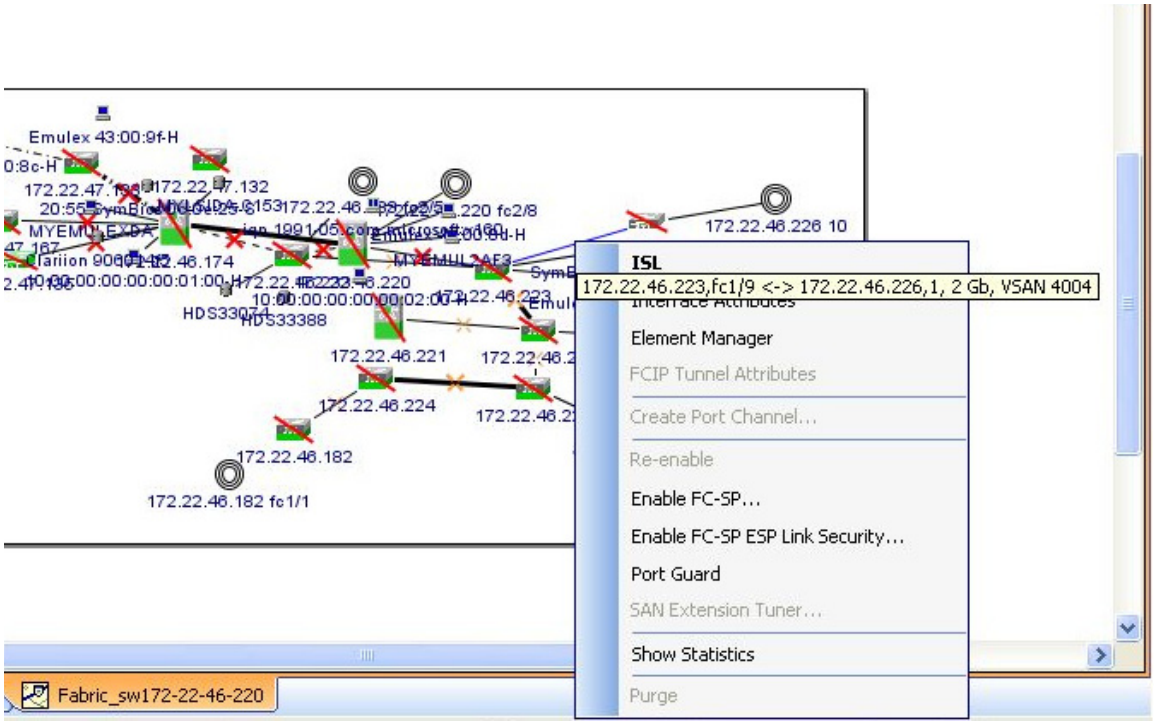
DETAILED STEPS

Step 1 Right-click the ISL or end device in the Fabric pane.

You see a context menu as shown in the Figure 13-4.

Step 2 Select **Show Statics**.

Figure 13-4 Show Statics Menu



Note Show Statics menu will be enabled only if you add the fabric to the Performance Manager collection.

Displaying Performance Manager Reports

This section includes the following topics:

You can view Performance Manager statistical data using preconfigured reports that are built on demand and displayed in a web browser. These reports provide summary information as well as detailed statistics that can be viewed for daily, weekly, monthly, or yearly results.

DETAILED STEPS

Step 1 Choose **Performance > Reports** to access Performance Manager reports from DCNM-SAN.

This opens a web browser window showing the default DCNM-SAN web client event summary report.

Step 2 Click the **Performance** tab to view the Performance Manager reports.

Performance Manager begins reporting data ten minutes after the collection is started.

Note DCNM-SAN Web Server must be running for reports to work.

Displaying Performance Summary

The Performance Summary page presents a dashboard display of the throughput and link utilization for hosts, ISLs, storage, and flows for the last 24-hour period. The summary provides a quick overview of the fabric's bandwidth consumption and highlights any hotspots.

The report includes network throughput pie charts and link utilization pie charts. Use the navigation tree on the left to show summary reports for monitored fabrics or VSANs. The summary displays charts for all hosts, storage elements, ISLs, and flows. Each pie chart shows the percent of entities (links, hosts, storage, ISLs, or flows) that measure throughput or link utilization on each of six predefined ranges. Move the mouse over a pie chart section to see how many entities exhibit that range of statistics. Double-click any pie chart to bring up a table of statistics for those hosts, storage elements, ISLs, or flows.

Displaying Performance Tables and Details Graphs

Click **Host, Storage, ISL**, or **Flow** to view traffic over the past day for all hosts, storage, ISLs, or flows respectively. A table lists all of the selected entities, showing transmit and receive traffic and errors and discards, if appropriate. The table can be sorted by any column heading. The table can also be filtered by day, week, month, or year. Tables for each category of statistics display average and peak throughput values and provide hot-links to more detailed information.

Clicking a link in any of the tables opens a details page that shows graphs for traffic by day, week, month, and year. If flows exist for that port, you can see which storage ports sent data. The details page also displays graphs for errors and discards if they are part of the statistics gathered and are not zero.

If you double-click a graph on a Detail report, it will launch the Cisco Traffic Analyzer for Fibre Channel, if configured. The aliases associated with hosts, storage devices, and VSANs in the fabric are passed to the Cisco Traffic Analyzer to provide consistent, easy identification.

Displaying Performance of Host-Optimized Port Groups

You can monitor the performance of host-optimized port groups by selecting **Performance > End Devices** and selecting **Port Groups** from the Type drop-down list.

Displaying Performance Manager Events

Performance Manager events are viewed through DCNM-SAN Web Server. To view problems and events in DCNM-SAN Web Server, choose a fabric and then click the **Events** tab to see a summary or detailed report of the problems and events that have occurred in the selected fabric.

Generating Performance Manager Reports

Generating Top10 Reports in Performance Manager

You can generate historical Top10 reports that can be saved for later review. These reports list the entities from the data collection, with the most active entities appearing first. This is a static, one-time only report that generates averages and graphs of the data collection as a snapshot at the time the report is generated. These Top10 reports differ from the other monitoring tables and graphs in Performance Manager in that the other data is continuously monitored and is sortable on any table column. The Top10 reports are a snapshot view at the time the report was generated and are static. These are one-time reports that generate averages and graphs of the data collection as a snapshot at the time the report is generated.

Tip Name the reports with a timestamp so that you can easily find the report for a given day or week.

These Top10 reports differ from the other monitoring tables and graphs in Performance Manager in that the other data is continuously monitored and is sortable on any table column. The Top10 reports are a snapshot view at the time the report was generated.

Note Top10 reports require analyzing the existing data over an extended period of time and can take hours or more to generate on large fabrics.

Generating Top10 Reports Using Scripts

You can generate Top10 reports manually by issuing the following commands:

- On UNIX, run the script:

  ```
  "/<user_directory>/.cisco_mds9000/bin/pm.sh display pm/pm.xml <output_directory>"
  ```

- On Windows, run the script:

  ```
  "c:\Program Files\Cisco Systems\MDS 9000\bin\pm.bat display pm\pm.xml
  <output_directory>"
  ```

On UNIX, you can automate the generation of the Top10 reports on your DCNM-SANDCNM-SAN Server host by adding the following cron entry to generate the reports once an hour:

```
0 * * * * /<user_directory>/.cisco_mds9000/bin/pm.sh display pm/pm.xml <output_directory>
```

If your crontab does not run automatically or Java complains about an exception similar to Example 13-1, you need to add "-Djava.awt.headless=true" to the JVMARGS command in /<user_directory>/.cisco_mds9000/bin/pm.sh.

Example 13-1 Example Java Exception

```
in thread "main" java.lang.InternalError Can't connect to X11 window server using '0.0' as
the value of the DISPLAY variable.
```

Configuring Performance Manager for Use with Cisco Traffic Analyzer

Performance Manager works in conjunction with the Cisco Traffic Analyzer to allow you to monitor and manage the traffic on your fabric. Using Cisco Traffic Analyzer with Performance Manager requires the following components:

- A configured Fibre Channel Switched Port Analyzer (SPAN) destination (SD) port to forward Fibre Channel traffic.
- A Port Analyzer Adapter 2 (PAA-2) to convert the Fibre Channel traffic to Ethernet traffic.
- Cisco Traffic Analyzer software to analyze the traffic from the PAA-2.

DETAILED STEPS

Step 1 Set up the Cisco Traffic Analyzer according to the instructions in the *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note.*

Step 2 Get the following three items of information:

- The IP address of the management workstation on which you are running Performance Manager and Cisco Traffic Analyzer.
- The path to the directory where Cisco Traffic Analyzer is installed.
- The port that is used by Cisco Traffic Analyzer (the default is 3000).

Step 3 Start the Cisco Traffic Analyzer.

a. Choose **Performance > Traffic Analyzer > Open**.

b. Enter the URL for the Cisco Traffic Analyzer, in the format:

`http://<ip address>:<port number>`

ip address is the address of the management workstation on which you have installed the Cisco Traffic Analyzer

:*port number* is the port that is used by Cisco Traffic Analyzer (the default is :3000).

c. Click **OK**.

d. Choose **Performance > Traffic Analyzer > Start**.

e. Enter the location of the Cisco Traffic Analyzer, in the format:

`D:\<directory>\ntop.bat`

D: is the drive letter for the disk drive where the Cisco Traffic Analyzer is installed.

directory is the directory containing the ntop.bat file.

f. Click **OK**.

Step 4 Create the flows you want Performance Manager to monitor, using the Flow Configuration Wizard. See the "Creating a Flow with Performance Manager" section on page 13-2

Step 5 Define the data collection you want Performance Manager to gather, using the Performance Manager Configuration Wizard. See the "Creating a Collection with Performance Manager" section on page 13-2.

a. Choose the VSAN you want to collect information for or choose **All VSANs**.

b. Check the types of items you want to collect information for (Hosts, ISLs, Storage Devices, and Flows).

c. Enter the URL for the Cisco Traffic Analyzer in the format:

`http://<ip address>/<directory>`

where:

ip address is the address of the management workstation on which you have installed the Cisco Traffic Analyzer, and *directory* is the path to the directory where the Cisco Traffic Analyzer is installed.

d. Click **Next**.

e. Review the data collection on this and the next section to make sure this is the data you want to collect.

f. Click **Finish** to begin collecting data.

Note Data is not collected for JBOD or for virtual ports. If you change the data collection configuration parameters during a data collection, you must stop and restart the collection process for your changes to take effect.

Step 6 Choose **Performance > Reports** to generate a report. Performance Manager Web Server must be running. You see Web Services; click **Custom** then select a report template.

Note It takes at least five minutes to start collecting data for a report. Do not attempt to generate a report in Performance Manager during the first five minutes of collection.

Step 7 Click **Cisco Traffic Analyzer** at the top of the Host or Storage detail pages to view the Cisco Traffic Analyzer information, or choose **Performance > Traffic Analyzer > Open**. The Cisco Traffic Analyzer page will not open unless ntop has been started already.

Note For information on capturing a SPAN session and starting a Cisco Traffic Analyzer session to view it, refer to the *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note.*

Note For information on viewing and interpreting your Performance Manager data, see the "Creating a Flow with Performance Manager" section on page 13-2.

For information on viewing and interpreting your Cisco Traffic Analyzer data, refer to the *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*.

For performance drill-down, DCNM-SAN Server can launch the Cisco Traffic Analyzer in-context from the Performance Manager graphs. The aliases associated with hosts, storage devices, and VSANs are passed to the Cisco Traffic Analyzer to provide consistent, easy identification.

Exporting Data Collections

This section includes the following topics:

• "Exporting Data Collections in Readable Format" section on page 13-12

Exporting Data Collections to XML Files

The RRD files used by Performance Manager can be exported to a freeware tool called rrdtool. The rrd files are located in pm/db on the DCNM-SAN Server. To export the collection to an XML file, enter the following command at the operating system command-line prompt:

```
/bin/pm.bat xport xxx yyy
```

In this command, *xxx* is the RRD file and *yyy* is the XML file that is generated. This XML file is in a format that rrdtool is capable of reading with the command:

```
rrdtool restore filename.xml filename.rrd
```

You can import an XML file with the command:

```
bin/pm.bat pm restore <xmlFile> <rrdFile>
```

This reads the XML export format that rrdtool is capable of writing with the command:

```
rrdtool xport filename.xml filename.rrd.
```

The **pm xport** and **pm restore** commands can be found on your DCNM-SAN Server at bin\PM.bat for Windows platforms or bin/PM.sh on UNIX platforms. For more information on the rrdtool, refer to the following website: http://www.rrdtool.org.

Exporting Data Collections in Readable Format

You can export the RRD files used by Performance Manager to a freeware tool called rrdtool and export the collection to an XML file. Cisco MDS SAN-OS Release 2.1(1a) introduces the inability to export data collections in comma-separated format (CSV). This format can be imported to various tools, including Microsoft Excel. You can export these readable data collections either from the DCNM-SAN Web Services menus or in batch mode from the command line on Windows or UNIX. Using DCNM-SAN Web Services, you can export one file. Using batch mode, you can export all collections in the pm.xml file.

Note DCNM-SAN Web Server must be running for this to work.

You can export data collections to Microsoft Excel using DCNM-SAN Web Server.

DETAILED STEPS

Step 1 Click the **Performance** tab on the main page.

You see the overview table.

Step 2 Click the **Flows** sub-tab.

Step 3 Right-click the name of the entity you want to export and select **Export to Microsoft Excel**.

You see the Excel chart for that entity in a pop-up window.

You can export data collections using command-line batch mode.

DETAILED STEPS

Step 1 Go to the installation directory on your workstation and then go to the bin directory.

Step 2 On Windows, enter **.\pm.bat export C:\Program Files\Cisco Systems\MDS 9000\pm\pm.xml** <*export directory*>**.** This creates the csv file (export.csv) in the *export directory* on your workstation.

Step 3 On UNIX, enter **./pm.sh export /usr/local/cisco_mds9000/pm/pm.xml** <*export directory*>. This creates the csv file (export.csv) in the *export directory* on your workstation.

When you open this exported file in Microsoft Excel, the following information displays:

- Title of the entity you exported and the address of the switch the information came from.
- The maximum speed seen on the link to or from this entity.
- The VSAN ID and maximum speed.
- The timestamp, followed by the receive and transmit data rates in bytes per second.

Analyzing SAN Health

The SAN Health Advisor tool is a utility that used to monitor the performance and collect the statistics. You can perform the following tasks with this tool:

- Run Performance Monitor to collect I/O statistics
- Collect fabric inventory (switches and other devices)
- Create a graphical layout of fabric topology
- Create reports of error conditions and statistical data

You can install this tool at any SAN environment to collect I/O statistics for the specified time (usually 24 hours), generate health reports and automatically send reports to the designated system administrator for review at regular intervals.

When you start SAN Health Advisor tool, it runs in wizard mode, and prompts for inputs such as seed switch credentials, IP address of the server to which the data to be sent and all the necessary information for the software setup. As soon as the fabric is discovered, the tool starts capturing performance data, I/O statistics and error conditions.

The reports generated from the collection is stored in the **$INSTALLDIR/dcm/fm/reports** directory. These reports are automatically sent to the designated SAN administrator for review. In a situation where the tool fails to collect the data, it generates a report with an error message or exception. After sending the reports the tool automatically uninstalls itself and terminates all the processes that it established on the host machine.

The report that SAN Health Advisor tool generates will have the following details:

- Events
- System messages
- Analysis of connectivity
- Zone discrepancy

- System configuration
- Interface status
- Domain information
- Security settings

Installing the SAN Health Advisor Tool

SAN Health Advisor tool can be installed and run on Windows, UNIX, and Solaris platforms. Install the package that contains the .jar file with JRE version 6.0.

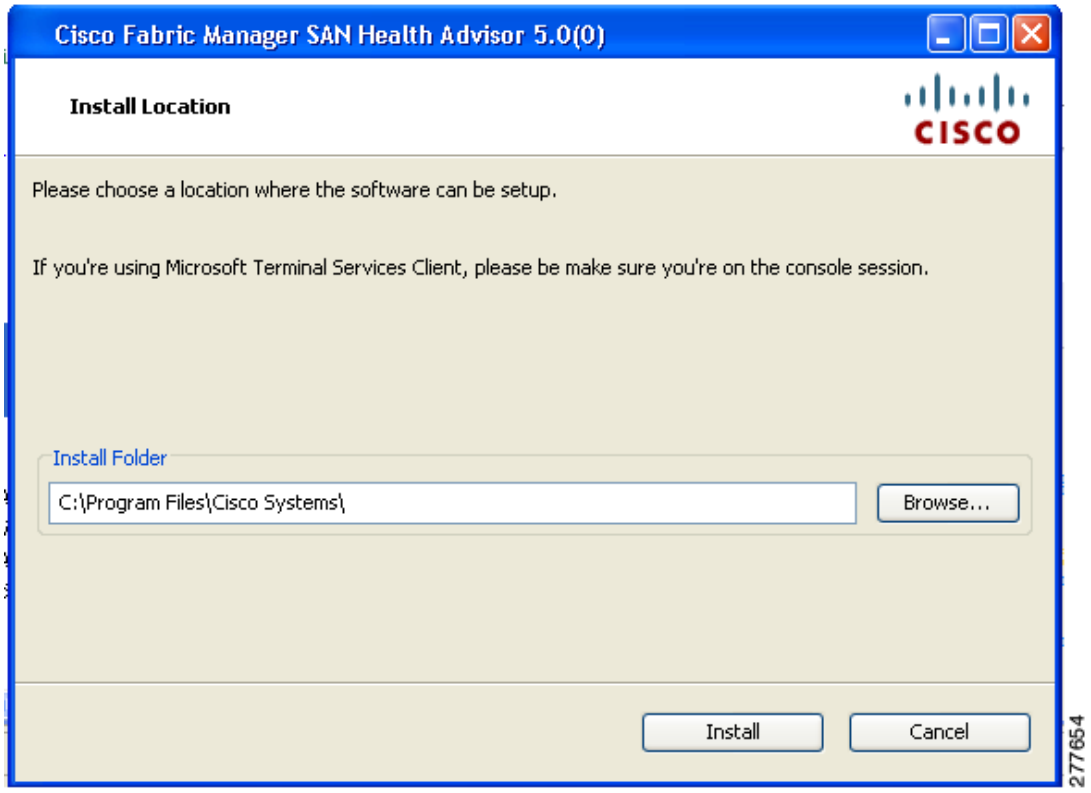
Note The SAN Health tool is not installed by default when you install DCNM-SAN software.

DETAILED STEPS

Step 1 Double-click the San Health Advisor tool installer.

You see the San Health Advisor tool Installer window as shown in Figure 13-5.

Figure 13-5 SAN Health Advisor: Installer



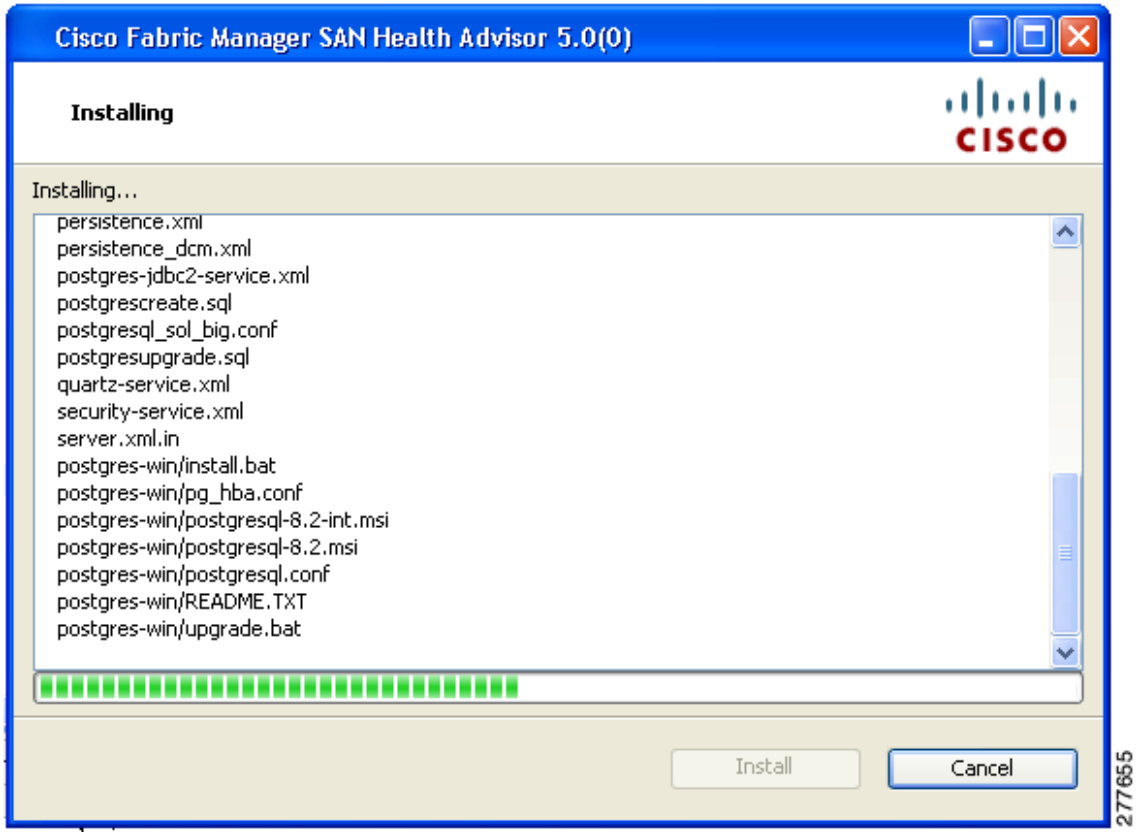
Step 2 Select an installation folder on your workstation for SAN Health Advisor.

On Windows, the default location is **C:\Program Files\Cisco Systems**.

Step 3 Click **Install** to start the installation.

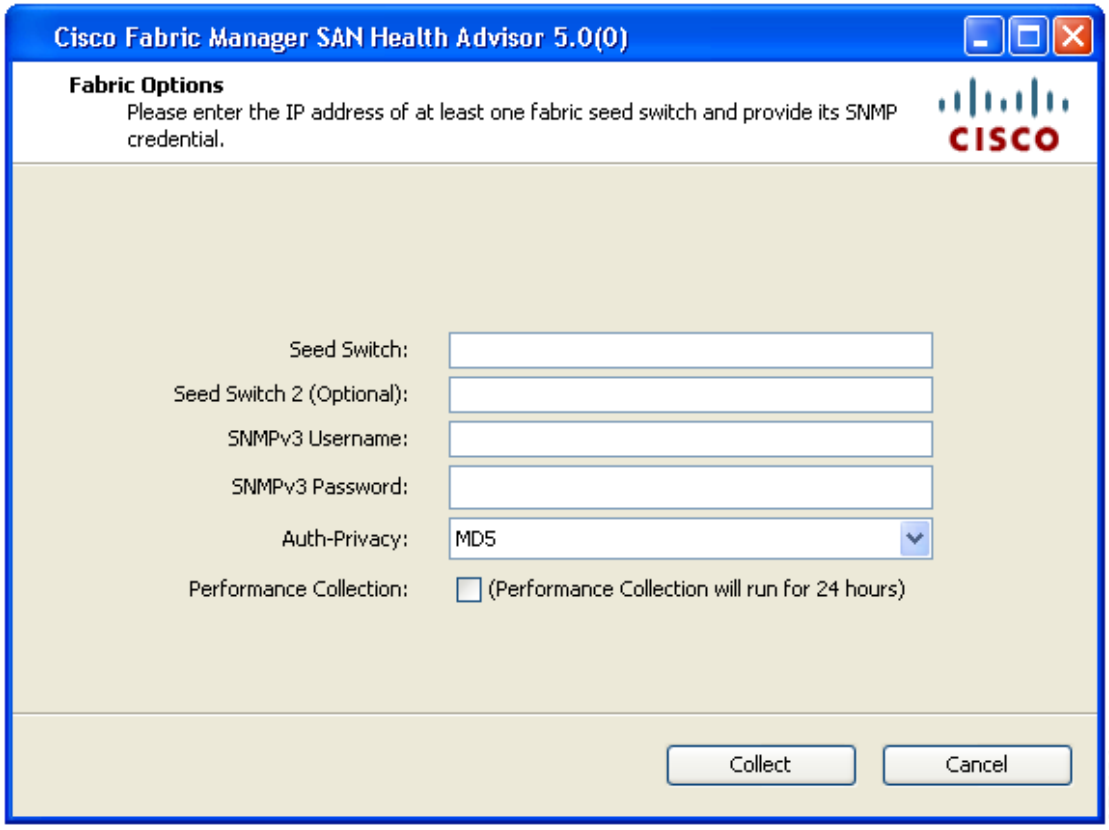
You see the installation progressing as shown in Figure 13-6.

Figure 13-6 SAN Health Advisor: Installation in Progress



You see the Fabric Options dialog box as shown in Figure 13-7

Figure 13-7 SAN Health Advisor: Fabric Options



Step 4 In the Seed Switch text box, enter the IP address of the seed switch.

Step 5 Enter the user name and password for the switch.

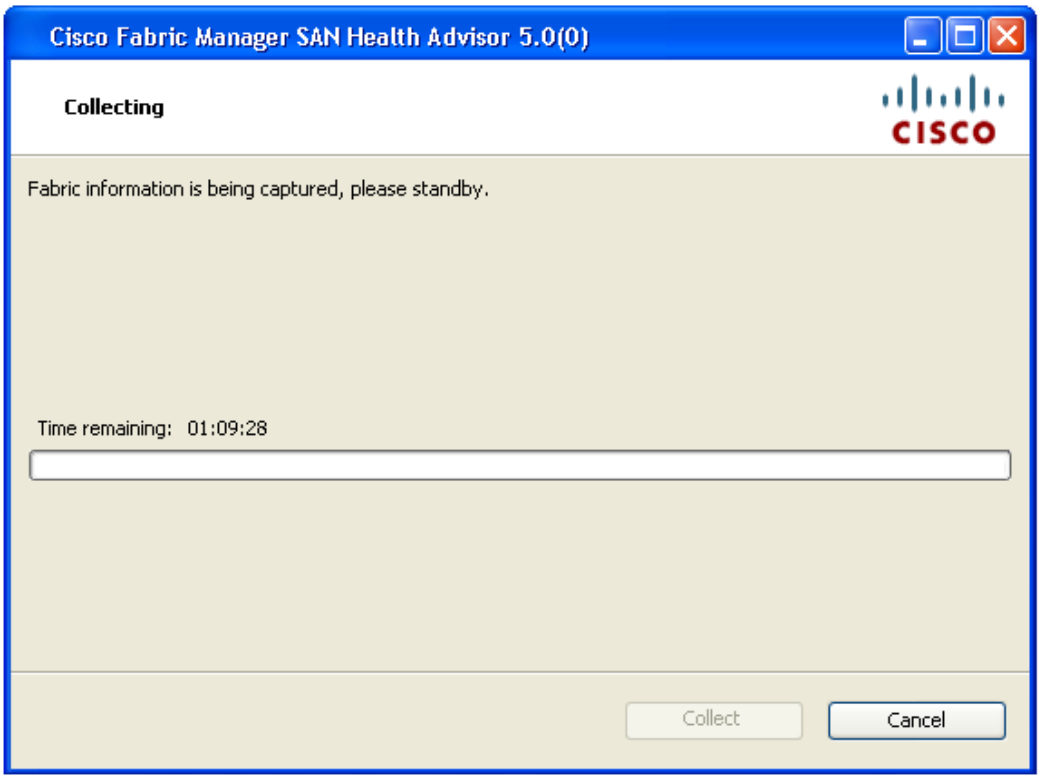
Step 6 Select the authentication privacy option from the Auth-Privacy drop-down list box.

Step 7 Click the **Performance Collection** check box to enable the process to run for 24 hours.

Step 8 Click **Collect** to start gathering performance information.

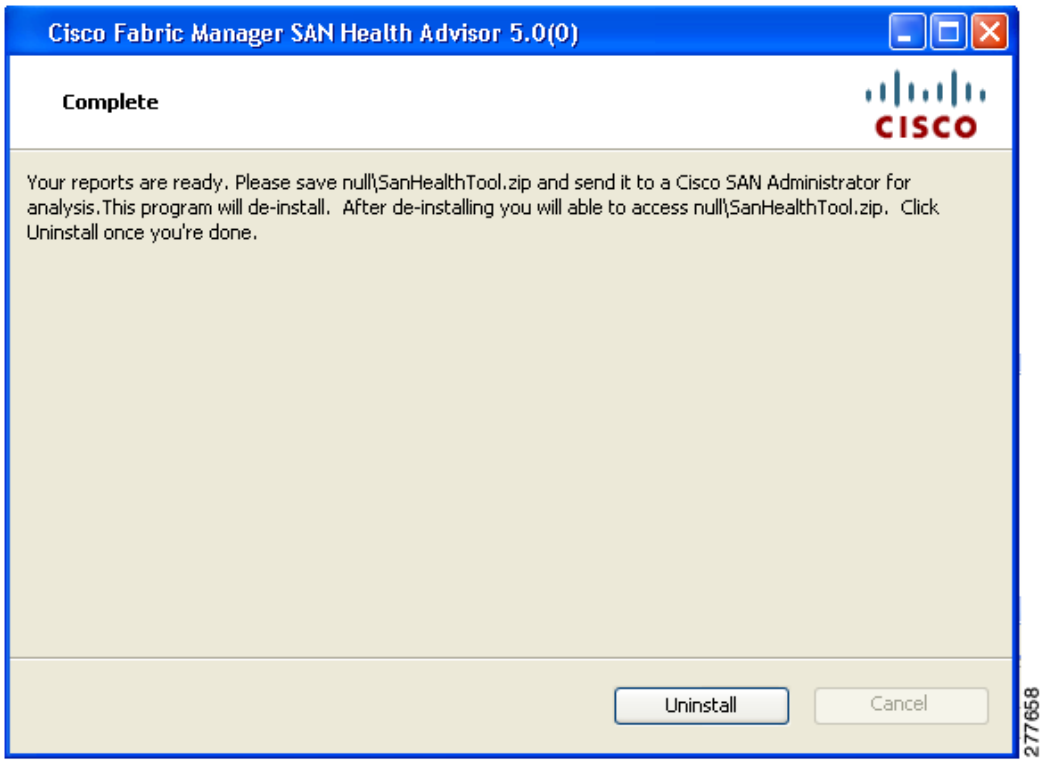
You see the collecting dialog box as shown in Figure 13-8.

Figure 13-8 SAN Health Advisor: Collecting



If you want to stop gathering information in the middle of the process, click Cancel. You see the message indicating performance collection is complete as shown in Figure 13-9.

Figure 13-9 SAN Health Advisor: Performance Collection Complete



Step 9 Click **Uninstall** to remove the SAN Health Advisor software.

CHAPTER A

DCNM Vacuum and Autovacuum Postgres Databases

This chapter describes how to vacuum the postgres database in Microsoft Windows and Linux.

This chapter includes the following sections:

Background Information

It is absolutely critical to vacuum postgres databases in order for the databases to properly function. Through the life of the database, new entries are added and current entries are updated. By design, postgres does not immediately remove the iterations of a record as it gets updated. Therefore, postgres databases can contain a large number of stale, unused records. These old records should be removed at least every two weeks with the vacuum function in order to reduce disk usage and improve the speed of database queries. It is even more effective if you configure postgres to automatically vacuum the database without the need to stop the Data Center Network Manager (DCNM) services.

Note $INSTALLDIR throughout this article refers to "**C:\Program Files\Cisco Systems**" or "**/usr/local/cisco/**" based on the operating system, Microsoft Windows or Linux respectively. The install path could be changed from these defaults during installation.

Vacuum DCNM's Postgresql Database in Windows

Step 1 Stop the DCNM services by clicking **Stop DCNM Servers** button, or enter the command as below:

$INSTALLDIR/dcm/dcnm/bin/stopLANSANserver.bat

Step 2 Obtain the database name, username, and password. Locate the **postgresql.cfg.xml** file on the DCNM server.

- In DCNM Version 6.2.x, enter:

  $INSTALLDIR/dcm/jboss-4.2.2.GA/server/dcnm/conf/database/postgresql.cfg.xml

- In DCNM Version 6.3.x, enter:

  $INSTALLDIR/dcm/Jboss-as-7.2.0.Final/standalone/conf/postgresql.cfg.xml

Step 3 Open **PgAdmin III.exe**, which is a helpful GUI for the postgres database. Then, right-click the object in the list and connect to the database. Enter the password from Step 2 here.

Step 4 Navigate through the drop-down menus to the dcmdb database.

Step 5 Right-click dcmdb and select Maintenance. Select the **Vacuum**, **Full**, **Analyze**, and **Verbose** options in the Maintain Database dcmdb dialog box.

Note The vacuum operation usually completes within an hour, but can take much longer for larger databases. Remember to restart the DCNM services.

Vacuum DCNM's Postgresql Database in Linux

Step 1 Stop dcnm by using the **appmgr stop dcnm** command.

Step 2 Open the psql prompt:

./usr/local/cisco/dcm/db/bin/psql -U <*dbUsername*> dcmdb

Step 3 Run the database vacuum and quit:

dcmdb=> VACUUM FULL ANALYZE VERBOSE;

Many pages of output pass on the screen. The vacuum is finished when you see a message similar to this one:

Current limits are: 532000 page slots, 1000 relations, using 3182 kB.

VACUUM

dcmdb=>

dcmdb=> \q

The previous command exits the sql prompt.

Step 4 Start DCNM services by using the **appmgr start dcnm** command.

DCNM-SAN Event Management

DCNM Event Management tool (EMAN) offers event management capability directly in Cisco MDS, Nexus 7000 and 5000 series switches to monitor events and take informational or corrective action as events occur, or when a threshold is reached. EMAN captures the state of the switches during critical situations helping to take immediate recovery actions and gather information to perform root-cause analysis.

An event is generated when the object matches specified values or crosses specified thresholds. When it detects an event, EMAN will parse the event for the host name, severity and then determine the host-to-application dependency by comparing the event in the host table. EMAN monitors these events to detect the severity type such as warning, critical and emergency of the events. It will also list the impacted components such as a host, ISL or a storage port. Switch health and performance threshold are the two event types that the EMAN monitor.

This Appendix contains the following sections:

Benefits of the Event Management Tool

EMAN tracks resource utilization and resource depletion by monitoring events in 45000 ports and 240 switches. It also provides a mechanism to send notifications whenever the specified threshold values are exceeded by any of the components. This notification helps network administrators diagnose resource utilization issues and prioritize resources making it more scalable.

EMAN helps in addressing component issues real time by performing the following functions:

- Monitoring resource usage.
- Using resource threshold pre-sets.
- Generating alerts when resource utilization reaches the specified level.
- Provides dependency path mapping.

DCNM-SAN Event Management

This section describes how DCNM handles asynchronous transfer events from the managed switches and contains the following topics:

Events

The following are the three primary methods by which DCNM detects events:

- SNMP—The Simple Network Management Protocol v1 (SNMPv1) event detector allows an event to be generated when the object matches specified values or crosses specified thresholds. The Cisco MDS 9000 switch can contain up to 10 trap destinations. The unmanaged fabrics or switches are removed from the list of traps destinations.
- Syslog—DCNM-SAN receives syslog messages and are logged in the events table in the database and archived on each switch.
- Fabric Model—DCNM-SAN can function even without receiving SNMP traps from the managed switches. DCNM-SAN polls for traps every 5 minutes and does a deeper discovery every 30 minutes by default.

Purpose

Asynchronous event handling serves the following purposes:

- Model Update—DCNM-SAN design the model of the physical and logical connectivity of each fabric. Asynchronous events enables real time synchronization with the fabric. In cases such as a linkdown, this model quickly updates the event without polling the fabric. However, for major changes such as an ISL link change, this model polls the fabric to synchronize.
- Log—All the events are logged into a database. The number of events that can be logged is set to 10,000 by default. You can view this log in the Cisco DCNM-SAN Client and in Cisco DCNM Web Client. The Cisco DCNM Web Client stores all events in the database unless you do not apply any filteres. The Cisco DCNM-SAN Client log is restricted to the fabric(s) that are opened in the client's interface. TheCisco DCNM-SAN Client automatically updates the table as new events appear.
- Map—The Cisco DCNM-SAN Client's updates the map automatically when topology changes.

Forwarding

Events are forwarded in three ways:

- Cisco Call Home—The Cisco MDS 9000 series switches generates an email at the event of a critical event such as a module down etc. You can customize this email to include additional information. You can use Cisco DCNM-SAN client to configure Cisco call home feature and it has no operational dependency on Cisco DCNM.
- EMC Call Home—If you enable this feature, the Cisco DCNM server generates an EMC call home email at the event of a critical event such as a linkDown event etc. This email is created in XML format.
- Event Forwarding—You can optionally choose to send an email or SNMP traps from Cisco DCNM for any or all events that are logged into the database.

DCNM-SAN Event Classification

Port Events

Port events provides real-time information about the operational status of the host ports, storage ports, ISLs, NPV etc in your network. At the event of a fault, the Cisco DCNM EMAN generates an event or events that are rolled up into an alert. The port events are broadly classified into two as follows:

- Service Impacting—Indicates the severity of the event that impacts the service. Examples are PMON, RMON and SFP events.
- Outage—Indicates the severity of the event that impacts the functioning of the device. Exampls are link up/down and threshold events.

Event Log Format

Events log consists of parseable information that is available to higher level management applications in the following format:

```
<fabric>/<switch> <localTime> <severity> <type> <description>
```

- Fabric/Switch—The name of the fabric or the switch.
- LocalTime—The date and time of the event occurred. The time is in the following format: hh:mm:ss.ttt. The date is in the following format: MM/DD/YYYY.
- Severity—Event severity level, combination of single events, or a range of event severity levels. The severity contains one of the following.
  - Emergencies
  - Alert
  - Critical
  - Error
  - Warning
  - Notice
  - Informational
  - Debugging
- Type—Type of events.
  - Fabric
  - FICON
  - IVR
  - License
  - Other
  - Port Alarm
  - Port Up and Port Down
  - Security

  - Switch Hardware
  - Switch Manageability
  - Threshold
  - VSAN
  - Zone
- Description—Description of the event in the following format:

```
<portType>: <name>, Port: <interface>, VSAN: <vsanId(s)>, <condition>
```

Event Types

IVR

Table B-1 IVR Events

Event Name	Description
civrDomainConflictNotify	
civrZoneActivationDoneNotify	
civrZoneCompactNotify	
civrZoneDeactivationDoneNotify	
civrDomainConflictNotify	
civrAfidConfigNotify	

License

Table B-2 Licence Events

Event Name	Description
clmLicenseExpiryNotify	
clmLicenseExpiryWarningNotify	
clmLicenseFileMissingNotify	
clmNoLicenseForFeatureNotify	

Port Alarm

Any RMON event that relates to an interface object.

Table B-3 Port Alarm Event

Event Name	Description
cIfXcvrMonStatusChangeNotif	

Port Up and Port Down

Model-generated events relating to Host, Storage, ISL, NP_Links

Table B-4 IVR Events

Event Name	Description
linkup	
linkDown	
cieLinkUp	
cieLinkDown	
connUnitPortStatusChange	
fcNameServerEntryAdd	
fcNameServerEntryDelete	
fcTrunkIfDownNotify	
fcTrunkIfUpNotify	
cieDelayedLinkUpDownNotif	

Note Port Moved events will not be logged.

Security

Table B-5 Security Event Types

Event Name	Description
casServerStateChange	
cfcspAuthFailTrap	
ciscoPsmFabricBindDenyNotifyNew	
ciscoEnhIpsecFlowBadSa	
ciscoEnhIpsecFlowSetupFail	
ciscoEnhIpsecFlowSysFailure	
ciscoEnhIpsecFlowTunnelStart	
ciscoEnhIpsecFlowTunnelStop	
ciscoIPsecProvCryptomapAdded	

Event Name	Description
ciscoIPsecProvCryptomapAttached	
ciscoIPsecProvCryptomapDeleted	
ciscoIPsecProvCryptomapDetached	
ciscoIkeConfigOperStateChanged	
ciscoIkeConfigPolicyAdded	
ciscoIkeConfigPolicyDeleted	
ciscoIkeConfigPskAdded	
ciscoIkeConfigPskDeleted	
ciscoIkeFlowInNewGrpRejected	
ciscoIkeFlowOutNewGrpRejected	
ciscoIpsSgCertCrlFailure	
ciscoIpsSgSysFailure	
ciscoIpsSgTunnelStart	
ciscoIpsSgTunnelStop	

Switch Hardware

Table B-6 Switch Hardware Events

Event Name	Description
cefcFRUInserted	
cefcFRURemoved	
cefcPowerStatusChange	
cefcPowerSupplyOutputChange	
cefcFanTrapStatusChange	
cefcUnrecognizedFRU	
cefcFRUInserted	
cefcFRURemoved	
cefcUnrecognizedFRU	
entPhysicalVendorType	
entPhysicalName	
entPhysicalModelName	
cefcPhysicalStatus	
cefcPowerStatusChange	
cefcFRUPowerOperStatus	
cefcFRUPowerAdminStatus	
cefcFanTrapStatusChange	

Switch Managability

Table B-7 Switch Event Types

Event Name	Description
Switch Discovered	
Switch Rebooted	
Switch Unreachable	
Switch Manageable	
Switch Unmanageable	
Switch IP Changed	
warmStart	
coldStart	
ciscoRFProgressionNotif	
ciscoRFSwactNotif	

Threshold

Table B-8 Threshold Events

Event Name	Description
cHcRisingAlarm	
cHcFallingAlarm	
hcRisingAlarm	
hcFallingAlarm	
risingAlarm	
FallingAlarm	

VSAN

Table B-9 VSAN Events

Event Name	Description
vsanPortMembershipChange	
vsanStatusChange	

Zone

Table B-10 Zone Events

Event Name	Description
zoneActivateNotify	
zoneCompactNotify	

Event Name	Description
zoneDefZoneBehaviourChngNotify	
zoneMergeFailureNotify	
zoneMergeSuccessNotify	
zoneServiceReqRejNotify	
zoneUnsuppMemInIntOpModeNotify	

Others

This table contains all other trap types such as ISCSI, VRRP, Cisco callhome, flex attach, FDMI, FICON, CFS, PMON config, SVC, SCSI, SNE, Core, Domain Manager, FCNS, FCOT, and UCS.

Table B-11 Other Events

Event Name	Description
cIsnsClientInitalRegistration	
cIsnsClientLostConnection	
cIsnsClientNoServerDiscovered	
cIsnsClientStart	
cIsnsServerShutdown	
cIsnsServerStart	
cVrrpNotificationNewMaster	
cVrrpNotificationProtoError	
casServerStateChange	
ccCopyCompletion	
ccmAlertGroupTypeAddedNotif	
ccmAlertGroupTypeDeletedNotif	
ccmCLIRunningConfigChanged	
ccmCTIDRolledOver	
ccmEventNotif	
ccmSmtpMsgSendFailNotif	
ccmSmtpServerFailNotif	
cfaIfVirtualWwnChangeNotify	
cfaVirtualWwnMapChangeNotify	
cfdmiRejectRegNotify	
cficonPortInfoChange	
ciscoCFSDiscoveryCompleteNotif	
ciscoCFSFeatureActionNotif	
ciscoCFSMergeFailNotif	

Event Name	Description
ciscoCFSStatPeerStatusChngNotif	
ciscoConfigManEvent	
ciscoEnhIpsecFlowBadSa	
ciscoEnhIpsecFlowSetupFail	
ciscoEnhIpsecFlowSysFailure	
ciscoEnhIpsecFlowTunnelStart	
ciscoEnhIpsecFlowTunnelStop	
ciscoExtScsiLunDiscDoneNotify	
ciscoFCCCongestionRateLimitEnd	
ciscoFCCCongestionRateLimitStart	
ciscoFCCCongestionStateChange	
ciscoFeatOpStatusChange	
ciscoFeatureOpStatusChange	
ciscoFeatureSetOpStatusChange	
ciscoFlashCopyCompletionTrap	
ciscoFlashDeviceChangeTrap	
ciscoFlashDeviceInsertedNotif	
ciscoFlashDeviceInsertedNotifRev1	
ciscoFlashDeviceRemovedNotif	
ciscoFlashDeviceRemovedNotifRev1	
ciscoFlashMiscOpCompletionTrap	
ciscoFlashPartitioningCompletionTrap	
ciscoIPsecProvCryptomapAdded	
ciscoIPsecProvCryptomapAttached	
ciscoIPsecProvCryptomapDeleted	
ciscoIPsecProvCryptomapDetached	
ciscoIkeConfigOperStateChanged	
ciscoIkeConfigPolicyAdded	
ciscoIkeConfigPolicyDeleted	
ciscoIkeConfigPskAdded	
ciscoIkeConfigPskDeleted	
ciscoIkeFlowInNewGrpRejected	
ciscoIkeFlowOutNewGrpRejected	
ciscoIpsSgCertCrlFailure	
ciscoIpsSgSysFailure	
ciscoIpsSgTunnelStart	
ciscoIpsSgTunnelStop	

Event Name	Description
ciscoPmonPolicyChangeNotify	
ciscoPrefPathHWFailureNotify	
ciscoPsmFabricBindDenyNotify	
ciscoPsmFabricBindDenyNotifyNew	
ciscoPsmPortBindEPortDenyNotify	
ciscoPsmPortBindFPortDenyNotify	
ciscoSanBaseSvcClusterNewMaster	
ciscoSanBaseSvcInterfaceCreate	
ciscoSanBaseSvcInterfaceDelete	
ciscoScsiFlowStatsNotify	
ciscoScsiFlowVerifyNotify	
ciscoScsiFlowWrAccNotify	
ciscoSmeClusterNewMaster	
ciscoSmeInterfaceCreate	
ciscoSmeInterfaceDelete	
ciscoSystemClockChanged	
ciscoVshaStateChngNotify	
ciuUpgradeJobStatusNotify	
ciuUpgradeOpCompletionNotify	
cseFailSwCoreNotify	
cseFailSwCoreNotifyExtended	
cseHaRestartNotify	
cseShutDownNotify	
csiErrorTrap	
csiInformationTrap	
csiWarningTrap	
dmDomainIdNotAssignedNotify	
dmFabricChangeNotify	
dmNewPrincipalSwitchNotify	
fcNameServerDatabaseFull	
fcNameServerRejectRegNotify	
fcPingCompletionNotify	
fcTraceRouteCompletionNotify	
fcotInserted	
fcotRemoved	
fcsDiscoveryCompleteNotify	
fcsMgmtAddrChangeNotify	

Event Name	Description
fcsReqRejNotify	
fspfNbrStateChangeNotify	
ptopoConfigChange	
qlSB2PortLinkDown	
qlSB2PortLinkUp	
rscnElsRejectReqNotify	
rscnElsRxRejectReqNotify	
rscnIlsRejectReqNotify	
rscnIlsRxRejectReqNotify	
virtualNwIfCreateEntryNotify	
virtualNwIfDeleteEntryNotify	
vlanTrunkPortDynamicStatusChange	
vrrpTrapAuthFailure	
vrrpTrapNewMaster	
vtpConfigDigestError	
vtpConfigRevNumberError	
vtpLocalModeChanged	
vtpMtuTooBig	
vtpPruningStateOperChange	
vtpServerDisabled	
vtpVersionInUseChanged	
vtpVersionOneDeviceDetected	
vtpVlanCreated	
vtpVlanDeleted	
vtpVlanRingNumberConflict	
wwnmType1WwnAvailableNotify	
wwnmType1WwnShortageNotify	
wwnmTypeOtherWwnAvailableNotify	
wwnmTypeOtherWwnShortageNotify	

Vcenter Plugin

VMware Vcenter plugin allows you to monitor the Cisco Unified Computing System™ (Cisco UCS®), Cisco Nexus, and Cisco MDS 9000 Family platforms through Cisco DCNM.

The Cisco DCNM plug-in for VMware Vcenter adds a multihop view and monitoring of Ethernet and Fibre Channel Cisco Nexus and Cisco MDS 9000 Family topologies. The increased visibility into virtualized infrastructure helps network administrators locate performance anomalies that may cause service degradation. It also aids to eliminate virtual computing and networking as a root cause of the problem.

This Appendix contains the following sections:

Associating Vcenter with the Datasource

To associate the Vcenter with the datasource, Cisco DCNM must discover the LAN and SAN devices.

Navigate to **Inventory > Discovery > LAN Switches** or **Inventory > Discovery > SAN Switches** to check if the LAN or SAN devices are discovered on the Cisco DCNM Web Client. In the **Inventory->Discovery->Virtual Machine Manager** block, click + to add the Vcenter to the datasource.

Registering Vcenter plugin

To register the Vcenter plugin, run the RegisterPlugin script. Enter the Vcenter IP address, Vcenter username, Vcenter password, and complete URL of the DCNM server. The plugin configuration file is stored in the DCNM server.

```
Example:
RegisterPlugin.bat -add 172.22.29.87 admin nbv123 https://dcnm-san-001:443
```

Triggering the plugin

When user clicks on the menu, it will show the login page first, and then will launch an internal browser which will show the host dashboard.

Removing the plugin

To remove the Vcenter plugin, run the RegisterPlugin script. Enter the Vcenter IP address, Vcenter username, Vcenter password, and complete URL of the DCNM server. The plugin configuration file is located in the DCNM server.

Interface Nonoperational Reason Codes

If the administrative state for an interface is up and the operational state is down, the reason code differs based on the nonoperational reason code as described in Table D-1.

Table D-1 Reason Codes for Nonoperational States

Reason Code	Description	Applicable Modes
Link failure or not connected	Physical layer link is not operational.	All
SFP not present	The small form-factor pluggable (SFP) hardware is not plugged in.	
Initializing	The physical layer link is operational and the protocol initialization is in progress.	
Reconfigure fabric in progress	The fabric is currently being reconfigured.	
Offline	Cisco MDS SAN-OS waits for the specified R_A_TOV time before retrying initialization.	
Inactive	The interface VSAN is deleted or is in a suspended state. To make the interface operational, assign that port to a configured and active VSAN.	
Hardware failure	A hardware failure is detected.	
Error disabled	Error conditions require administrative attention. Interfaces may be error-disabled for various reasons. For example: • Configuration failure. • Incompatible buffer-to-buffer credit configuration. To make the interface operational, you must first fix the error conditions causing this state; and next, administratively shut down or enable the interface.	

Table D-1 Reason Codes for Nonoperational States (continued)

Reason Code	Description	Applicable Modes
Isolation due to ELP failure	Port negotiation failed.	Only E ports and TE ports
Isolation due to ESC failure	Port negotiation failed.	
Isolation due to domain overlap	The Fibre Channel domains (fcdomain) overlap.	
Isolation due to domain ID assignment failure	The assigned domain ID is not valid.	
Isolation due to other side E port isolated	The E port at the other end of the link is isolated.	
Isolation due to invalid fabric reconfiguration	The port is isolated due to fabric reconfiguration.	
Isolation due to domain manager disabled	The fcdomain feature is disabled.	
Isolation due to zone merge failure	The zone merge operation failed.	
Isolation due to VSAN mismatch	The VSANs at both ends of an ISL are 2different.	
Nonparticipating	FL ports cannot participate in loop operations. It may happen if more than one FL port exists in the same loop, in which case all but one FL port in that loop automatically enters nonparticipating mode.	Only FL ports and TL ports
PortChannel administratively down	The interfaces belonging to the PortChannel are down.	Only PortChannel interfaces
Suspended due to incompatible speed	The interfaces belonging to the PortChannel have incompatible speeds.	
Suspended due to incompatible mode	The interfaces belonging to the PortChannel have incompatible modes.	
Suspended due to incompatible remote switch WWN	An improper connection is detected. All interfaces in a PortChannel must be connected to the same pair of switches.	