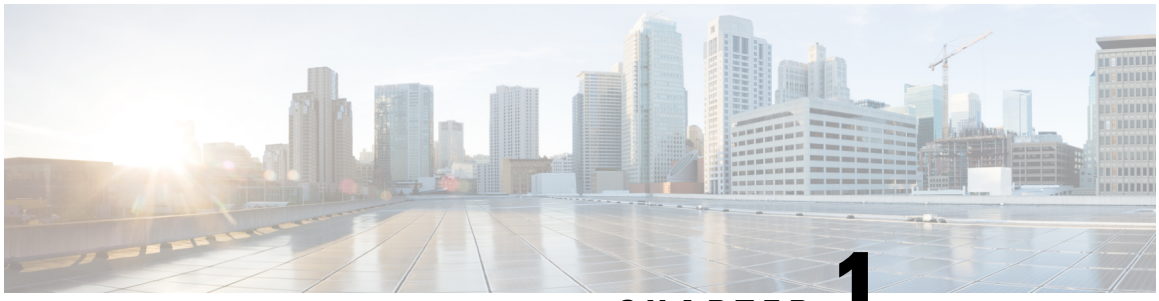
Cisco DCNM Fundamentals Guide, Release 11.x

Last Modified: 2020-07-02

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

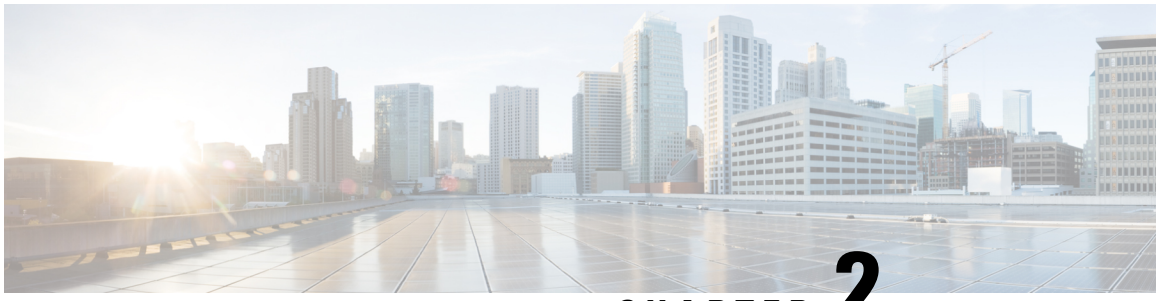
Overview

Overview

Cisco Data Center Network Manager (DCNM) is a management system for the Cisco Unified Fabric. It enables you to provision, monitor, and troubleshoot the data center network infrastructure. It provides visibility and control of the unified data center. 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 install applications related to Unified Fabric only for Unified Fabric-mode installations.

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

Configuring Cisco DCNM-SAN Server

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.

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. The Cisco DCNM-SAN software, including the server components, requires about 60 MB of hard disk space on your workstation. Cisco DCNM-SAN Server runs on Windows 2000, Windows 2003, Windows XP, Solaris 9 and 10, and Red Hat Enterprise Linux AS Release 5.

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.

Step 1 Install Cisco DCNM-SAN Client and Cisco DCNM-SAN Server on your workstation.

See the Installing Cisco DCNM-SAN Server, on page 5.

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, on page 5.

Step 4 Repeat Step 2 and 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, on page 5.

Step 6 Verify Performance Manager is collecting data.

See the Verifying Performance Manager Collections, on page 5.

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

SUMMARY STEPS

1. Choose **Server** > **Admin**.
2. Choose one of the following Admin options:

3. Click **Apply**.

DETAILED STEPS

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

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

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:

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

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

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 9-3 ".

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.

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 and DCNM-SMIS WINDOWS Server

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

- **$INSTALLDIR\wildfly-xx.x.x.Final\bin\service\sanservice.bat**
- **$INSTALLDIR\wildfly-xx.x.x.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 and DCNM-SMIS LINUX Server

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

- **$INSTALLDIR/wildfly-xx.x.x.Final/bin/init.d/sanservice.sh**
- /etc/init.d/FMServer
- **$INSTALLDIR/wildfly-xx.x.x.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.

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

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\wildfly-xx.x.x.Final\bin\service\sanservice.bat**.

Step 3 Change the old IP Address with the new IP Address in the file **$INSTALLDIR\wildfly-xx.x.x.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\wildfly-xx.x.x.Final\bin\service\sanservice.bat**.

Step 3 Change the old IP Address with the new IP Address in the file **$INSTALLDIR\wildfly-xx.x.x.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\wildfly-xx.x.x.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 for Federated Linux Setup

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

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/wildfly-xx.x.x./bin/service/sanservice.sh`

Step 3 Change the old IP Address with the new IP Address in the file `$INSTALLDIR/wildfly-xx.x.x./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.sh -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/wildfly-xx.x.x./bin/service/sanservice.sh`.

Step 3 Change the old IP Address with the new IP Address in the file `$INSTALLDIR/wildfly-xx.x.x./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 IP Address change in primary server.

postgresql.cfg.xml\ oracle.cfg.xml can be found under `$INSTALLDIR/wildfly-xx.x.x./standalone/ conf/` directory.

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

run $INSTALLDIR/fm/bin/PLMapping.sh -p newipaddress 1.

Note ServerID can be got by run **$INSTALLDIR/fm/bin/PLMapping.sh -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.

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.

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 are 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. You can move a fabric

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.

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

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

Step 1 Choose Server > Admin.

Step 2 Click the Connected Clients tab.

You see the Control Panel.

Discover Devices Managed by SVI

SUMMARY STEPS

1. Log on to the DCNM Web Client.
2. Select Admin>Server Properties.
3. Scroll down to the GENERAL->DATA SOURCE FABRIC section.
4. Set the fabric.managementIpOverwrite property to false.
5. Click Apply.
6. Restart the DCNM service.
7. Delete any previously discovered switch that incorrectly shows the mgmt0 IP address.
8. Retry the discovery.

DETAILED STEPS

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.

Changing the Authentication Type from Remote to Local

To change the authentication from Remote to Local, perform the following.

Step 1 Log on to the DCNM Server via SSH.

Step 2 Navigate to the `server.properties.xml` file locate at: `C:\Program Files\Cisco Systems \dcm\fm\conf`.

```
cd C:\Program Files\Cisco Systems \dcm\fm\conf
```

Step 3 Edit the authentication mode in the `server.properties.xml` file.

```
authentication.mode = tacacs|radius|ldap
```

To

```
authentication.mode = local
```

Step 4 Save and close the `server.properties.xml` file.

Step 5 Navigate to the DCNM Postgres database server properties table.

```
cd C:\Program Files\Cisco Systems\dcm\db
```

Step 6 Execute the following command: **pg_env.bat**

Step 7 Navigate to the bin folder.

```
cd bin
```

Step 8 Log on to the DCNM Postgres database by using the following command:

psql.exe -U<*db username*>**-d dcmdb**

Step 9 At the prompt, enter the password for the database user.

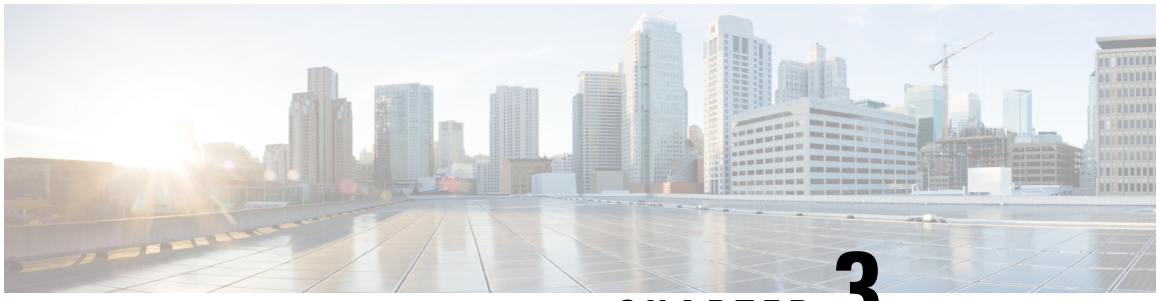
```
dcnmdb=> Password for dcnmuser: database_password
```

Step 10 At further prompts, enter the following to update the authentication mode.

```
dcmdb=> select * from svr_prop where key = 'authentication.mode';
dcmdb=> update svr_prop set value = 'local' where key = 'authentication.mode';
dcmdb=> select * from svr_prop where key = 'authentication.mode';
dcmdb=> commit
dcmdb=> \q
```

Step 11 Restart the DCNM services.

The authentication type is changed to Local.



CHAPTER 3

Cisco DCNM User Roles

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.

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.

This chapter contains following sections:

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 doesn't allow you to reset the password using adduser script. Log on to Cisco DCNM Web UI to reset the password. Use the adduser script 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 doesn't 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.

The table below lists the roles supported by Cisco DCNM:

Role	Description
global-admin	Introduced in Cisco Nexus 5000 series switches and FCoE, a role to administrate LAN and SAN features.
network-admin	General role to administrate LAN features.
lan-network-admin	General role to administrate LAN features.
san-network-admin	General role to administrate SAN features.
san-admin	Introduced in Cisco Nexus 5000 series switches and FCoE, a role to administrate SAN features.
server-admin	Introduced in the FlexAttach feature, a role that administrates FC server host feature.
sme-admin	Introduced in the Storage Media Encryption (SME) feature, a role that administrates SME feature.
sme-stg-admin	Introduced in the Storage Media Encryption (SME)) feature, a role that administrates SME storage.
sme-kmc-admin	Introduced in the Storage Media Encryption (SME) feature, a role that administrates SME Key Management.
sme-recovery	Introduced in the Storage Media Encryption (SME) feature, a role that administrates SME recovery.
network-operator	General network operator role.
device-upg-admin	This role is added to perform operations only in Image Management window.
access-admin	This role is introduced to perform operations in Interface Manager window for all fabrics.

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.

User Role Assignment by RADIUS and TACACS+

Cisco DCNM supports the assignment of a user role by the RADIUS or TACACS+ server that grants a user access to the Cisco DCNM client. The user role assigned to a user is in effect for the current session in the Cisco DCNM client only.

To assign a Cisco DCNM user role by RADIUS, configure the RADIUS server to return the RADIUS vendor-specific attribute 26/9/1, which is the Cisco-AV-Pair attribute. To assign a Cisco DCNM user role by TACACS+, the TACACS+ server must return a cisco-av-pair attribute-value pair. If an authentication response doesn't assign the user role, Cisco DCNM assigns the User role. Table 1: Cisco DCNM User Role Assignment Values , on page 19 shows the supported attribute-value pair values for each Cisco DCNM user role.

Table 1: Cisco DCNM User Role Assignment Values

Cisco DCNM Role	RADIUS Cisco-AV-Pair Value	TACACS+ Shell cisco-av-pair Value
User	`shell:roles = "network-operator"`	`cisco-av-pair=shell:roles="network-operator"`
Administrator	`shell:roles = "network-admin"`	`cisco-av-pair=shell:roles="network-admin"`

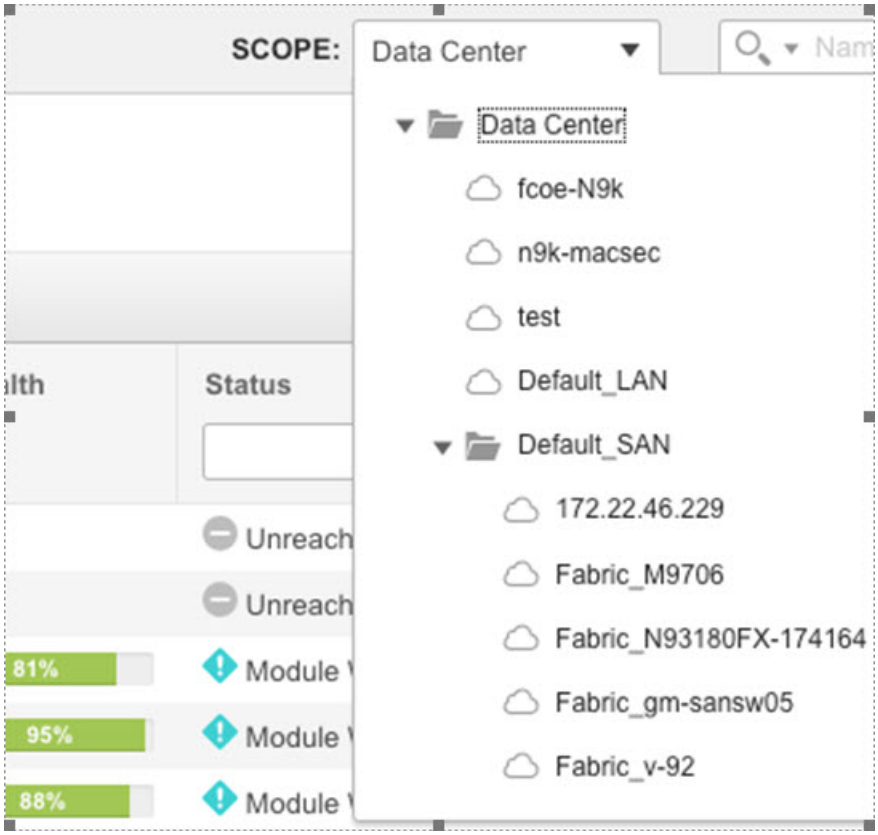
DCNM-Scope Mapping

Cisco DCNM allows you to add fabric names in TACACS using cisco-av-pairs. You can enable different AV pairs for any supported attribute value.

Cisco-av-pair=shell:roles="network-admin": **dcnm-access**="n9k-macsec fcoe-N9k"

Cisco-av-pair=shell:roles="network-admin": **dcnm-access**="fabric_M9706 Fabric_v-92"

These av-pairs appear on the Cisco DCNM **Web UI** > **Scope** drop-down list, based on the user access.



Roles from Cisco DCNM Perspective

Cisco DCNM perspective defines the operations that you 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 whereas **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:

Table 2: DCNM Roles and Perspectives Mapping Table, on page 20 describes how DCNM roles are mapped to client perspectives.

Table 2: 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 Client)	
access-admin	
device-upg-admin	

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 have full control of Cisco DCNM authentication settings.

SAN Client Admin Perspective

SAN 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 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 have full control of Cisco DCNM authentication settings.

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 is categorized to five different sme admin perspective according to the roles:

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 can’t 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 can’t 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 can’t 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 can’t perform the storage and key management features.

SAN Client SME Perspective

SAN 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, and operator perspective.

Operator Perspective

Operator perspective is designed for device-upg-admin, access-admin, network-operator and lan-network-admin role users, and lan-network-admin role only has SAN 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 can’t be used. All the other features can be used.

SAN Client Operator Perspective

SAN client operator perspective has no access to Discover button, Fabrics and License Files tabs, and wouldn’t be able to manage Fabric Manager users or connected clients.

User Access for Cisco DCNM

From Release 11.3(1), Cisco DCNM offers the user access based on your network security requirements. The following user roles allow access to DCNM via SSH or console that is introduced with Release 11.3(1).

- **sysadmin user**

  This DCNM OS user role is considered as the system administrator.

  sysadmin user role allows you to run **appmgr** and other system commands for managing and debugging the system such as **reboot**, **tcpdump**, etc. However, the user can function as a **root** user by using the **su** command.

  Note The **root** user role is required to read log files.

- **SSH access by user root**

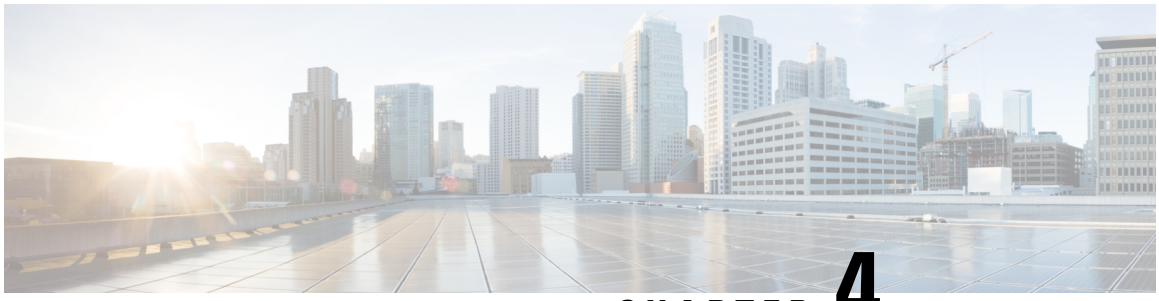
  On a Native HA setup using DCNM Management IPv4 VIP, SSH access with **root** user is allowed from DCNM to DCNM Computes. SSH access with **root** user is always allowed between HA peers. When adding a second node to a Standalone system or to a Native-HA setup (while restoring the secondary node), SSH access must be permitted for the installation to complete successfully.

  By default, SSH access with **root** user is disabled. Alternatively, you can use the **sysadmin** user.

  You can change the SSH access with **root** user by using the following command:

  appmgr root-access {permit|deny|without-password}

Note The DCNM GUI root user is no longer created. Alternatively, use the Admin user role to log on to the DCNM Web UI.



CHAPTER 4

Monitoring the Network

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 a fabric view, device view, summary view, and operation view.

Once DCNM-SAN is invoked, a SAN discovery process begins. Using information that is 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 that is 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 that is gathered by the Performance Manager. This information includes events that are sent to the DCNM-SAN Server from the fabric. To open these reports, choose **Performance Manager > Reports**. A summary of all the fabrics that are monitored by the DCNM-SAN Server is displayed. Choose a fabric and 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 the 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 the 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 the 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.

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.

Step 3 Click **Apply**, and 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 10-33 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

Use the same username and password to log on to multiple fabrics. 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. You can also double-click the cloud icon of the fabric.

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.

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. The summary of fabrics that are managed by the DCNM-SAN Server is displayed. The Inventory tab shows an inventory of the selected SAN, fabric, or switch.

Step 1 Point your browser at the DCNM-SAN Web Server.

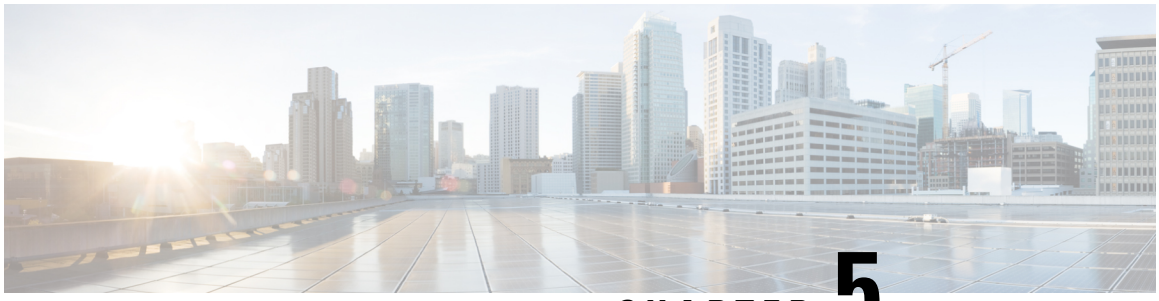
Step 2 Click the **Events** tab and click **Details** tab to view the system messages. The columns in the events table are sortable. In addition, you can use the **Filter** to limit the scope of messages within the table.

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.



CHAPTER 5

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.

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 3: Performance Manager Collection Types, on page 28.

Table 3: 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 4: Baseline Time Periods for a Collection Started on Wednesday at 4pm, on page 29 shows an example of the statistics used to create the baseline value for a collection defined at 4 pm on a Wednesday.

Table 4: 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 5: Example of Events Generated for 1-Gigabit Links, on page 29 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 5: 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

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.

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.

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.

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.

Viewing Performance Statistics 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.

SUMMARY STEPS

1. Right-click the ISL or end device in the Fabric pane.
2. Select Show Statics.

DETAILED STEPS

Step 1 Right-click the ISL or end device in the Fabric pane.

You see a context menu.

Step 2 Select Show Statics.

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.

SUMMARY STEPS

1. Choose Performance > Reports to access Performance Manager reports from DCNM-SAN.
2. Click the Performance tab to view the Performance Manager reports.

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.

What to do next

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:

Note Cisco DCNM on Linux (RHEL), and Cisco DCNM for SAN OVA/ISO display the Top10 reports on **Web UI > Dashboard > Summary**.

- 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-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 that is similar to the exception shown in the example below, you need to add "-Djava.awt.headless=true" to the JVMARGS command in /<user_directory>/.cisco_mds9000/bin/pm.sh.

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.

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:

Example:

```
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:

Example:

```
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.

Step 5 Define the data collection you want Performance Manager to gather, using the Performance Manager Configuration Wizard.

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:

Example:

```
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. 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* .

What to do next

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 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.

SUMMARY STEPS

1. Click the Performance tab on the main page.
2. Click the **Flows** sub-tab.
3. Right-click the name of the entity you want to export and select **Export to Microsoft Excel**.

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.

Exporting Data Collections in Readable Format

You can export data collections using command-line batch mode.

SUMMARY STEPS

1. Go to the installation directory on your workstation and then go to the bin directory.
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.
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.

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.

What to do next

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.

Step 1 Double-click the San Health Advisor tool installer.

You see the San Health Advisor tool Installer window.

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 will see the installation progressing.

You will see the Fabric Options dialog box.

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.

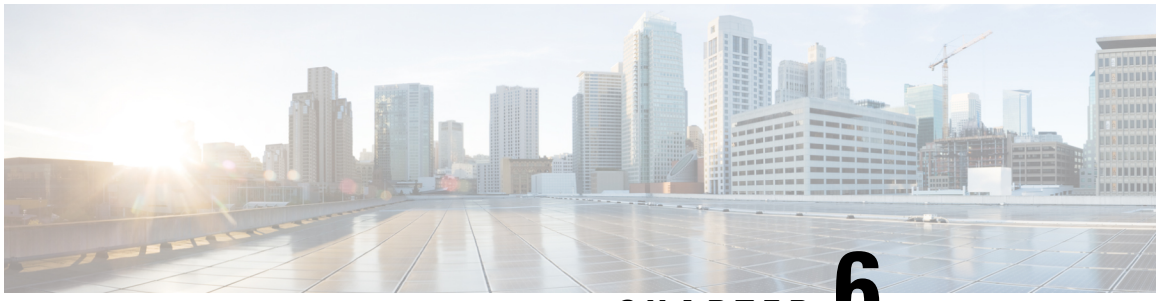
If you want to stop gathering information in the middle of the process, click Cancel.

Step 9 Click Uninstall to remove the SAN Health Advisor software.

Monitoring the LAN Switch Performance Counters

DCNM allows you to monitor LAN switch performance counters. The following counters can be monitored:

- Performance monitoring of interfaces (RX/TX traffic statistics, errors/discards, average/peak statistics etc.)
- Monitor VPC member Rx/Tx counters.
- Monitor CPU/Memory statistics.
- Monitor switch traffic.
- Monitor Health Scores.
- Monitor Events.



CHAPTER 6

Vacuum and Autovacuum Postgres Databases

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 critical to vacuum postgres databases in order for the databases to function properly. Through the life of the database, new entries are added and current entries are updated. By design, the postgres database does not remove the iterations of a record immediately as it gets updated. Therefore, postgres databases can contain many stale, unused records. These old records must 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 automatically to vacuum the database without the need to stop the 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 PostgreSQL Database in Windows

To vacuum the PostgresSQL database in Windows, perform the following steps:

Step 1 Stop the DCNM services by clicking Stop DCNM Servers button, or enter the followinng command:
$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.
$INSTALLDIR/dcm/wildfly-10.1.0.Final/server/dcnm/conf/database/postgresql.cfg.xml

Step 3 Open `PgAdmin III.exe`, which is a helpful GUI for the postgres database. Right-click the object in the list and connect to the database. Enter the password from Step 2.

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 PostgreSQL Database in Linux

To vacuum the PostgresSQL database in Linux, perform the following steps:

Step 1 Stop the applications 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.

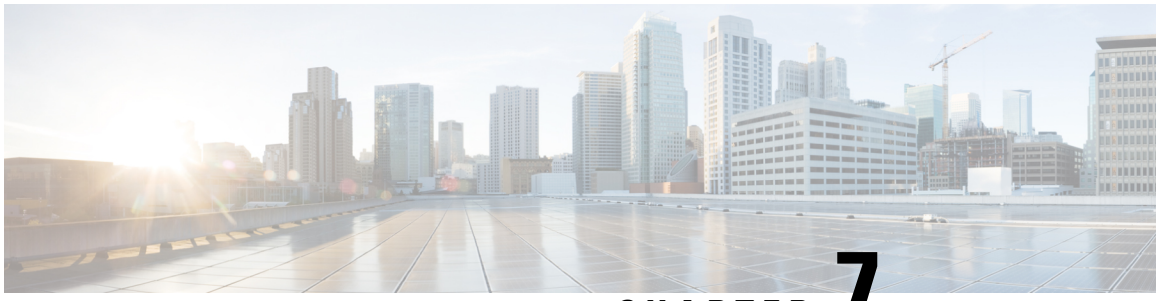
VACUUM

dcmdb=>

dcmdb=> \q

The previous command exits the SQL prompt.

Step 4 Start DCNM services by using the **appmgr start dcnm** command.



CHAPTER 7

Vcenter Plugin

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.

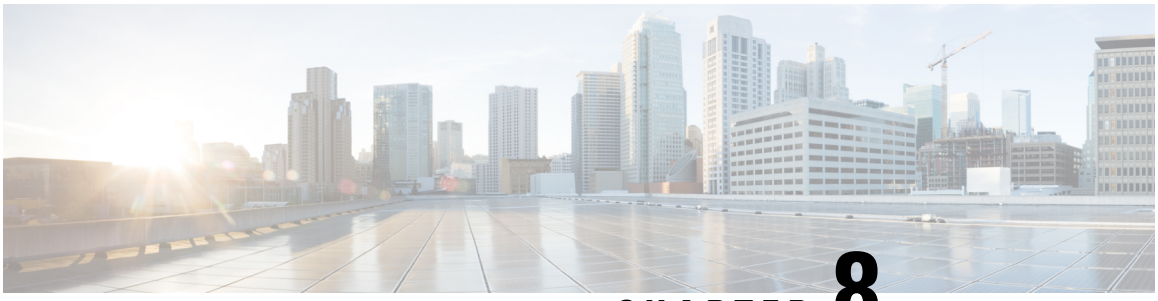
```
Example:
RegisterPlugin.bat -add 172.22.29.87 admin nbv123 https://dcnm-san-001:443
```

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.



CHAPTER 8

Interface Nonoperational Reason Codes

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 following table.

Table 6: 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.	

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 different.	
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.	

Interface Nonoperational Reason Codes