



CHAPTER 2

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 section, page 2-1](#)
- [Licensing Requirements For Cisco DCNM-SAN Server section, page 2-2](#)
- [Installing and Configuring Cisco DCNM-SAN Server section, page 2-2](#)
- [Managing a Cisco DCNM-SAN Server Fabric section, page 2-6](#)
- [Modifying Cisco DCNM-SAN Server section, page 2-8](#)
- [Server Federation section, page 2-10](#)
- [Additional References section, page 2-12](#)

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 install DCNM-SAN, the basic unlicensed version of Cisco DCNM-SAN Server is installed with it. To get the licensed features, such as Performance Manager, remote client support, and continuously monitored fabrics, you need to buy and install the Cisco DCNM-SAN Server package.

However, trial versions of these licensed features 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.

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 2-3.
 - 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 2-6.
 - 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 2-5.

- Step 6** Verify Performance Manager is collecting data. See the “[Verifying Performance Manager Collections](#)” section on page 2-5.
-

Installing Cisco DCNM-SAN Server

When you install DCNM-SAN, 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.

On a Windows PC, you install the Cisco DCNM-SAN Server as a service. This service can then be administered using Services in the Administrative Tools. The default setting for the Cisco DCNM-SAN Server service is that the server is automatically started when the Windows PC is rebooted. You can change this behavior by modifying the properties in Services.

For switches running Cisco MDS 9000 FabricWare, you must install DCNM-SAN from the CD-ROM included with your switch, or you can download DCNM-SAN from Cisco.com.

**Note**

You can have only one instance of Cisco DCNM-SAN Server running on a computer. If you have a DCNM-SAN Standalone version on your computer, you may need to uninstall it before you install Cisco DCNM-SAN Server.

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

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

**Note**

If you are upgrading from an earlier version to 5.0(1a) or later, that is configured with HTTPS to use your own self-provisioned or a third-party issued SSL certificate, make sure that you set the keystore password and then restart the DCNM-SAN Server. To set the keystore password, run **\$INSTALLDIR/dcm/fm/bin encrypter.bat ssl**.

DETAILED STEPS

- Step 1** Click the **Install Management Software** link.
- Step 2** Choose **Management Software > Cisco DCNM-SAN**.
- Step 3** Click the **Installing DCNM-SAN** link.
- Step 4** Click the **FM Installer** link.
- You see the welcome message in the Cisco DCNM-SAN Installer window.
- Step 5** Click the **Custom** radio button, and then click **Next** to begin installation.
- Step 6** Check the **I accept the terms of the License Agreement** check box, and then click **Next**.
- You see the Install Options dialog box.

Step 7 Click the **Cisco DCNM-SAN Server (Licensed)** radio button to install the server components for Cisco DCNM-SAN Server.

Step 8 Click **Add server to an existing server federation** to add the server to a federation.



Note You may need to add the following line in the pg-hba.conf file under **# IPv4 local connections** in order to allow remote hosts to connect to PostgreSQL database:

```
host all all 0.0.0.0/0 md5
```

After adding, save the configuration file, restart the PostgreSQL database before you install the second server node.



Note If you are joining more than three DCNM-SAN Servers in a federation, you need to use an Oracle database with the following settings.

```
C:\Documents and Settings\Administrator>sqlplus /nolog
SQL*Plus: Release 10.2.0.1.0 - Production on Wed Jan 6 17:19:32 2010
Copyright (c) 1982, 2005, Oracle. All rights reserved.
SQL> connect / as sysdba;
Connected.
```

```
SQL> alter system set processes=150 scope=spfile;
System altered.
SQL> alter system set open_cursors=500 scope=spfile;
System altered.
```

```
SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> startup;
ORACLE instance started.
Total System Global Area 805306368 bytes
Fixed Size 1453836 bytes
Variable Size 218714356 bytes
Database Buffers 583008256 bytes
Redo Buffers 2129920 bytes
Database mounted.
Database opened.
SQL> show parameter processes;
```

```
Total System Global Area 805306368 bytes
Fixed Size 1453836 bytes
Variable Size 218714356 bytes
Database Buffers 583008256 bytes
Redo Buffers 2129920 bytes
Database mounted.
Database opened.
SQL> show parameter processes;
```

NAME	TYPE	VALUE
aq_tm_processes	integer	0
db_writer_processes	integer	4
gcs_server_processes	integer	0
job_queue_processes	integer	4
log_archive_max_processes	integer	2

```
processes                               integer      100
```

Step 9 Select an installation folder on your workstation for Cisco DCNM-SAN. On Windows, the default location is C:\Program Files\Cisco Systems.

Step 10 Click **Next**.

You see the Database Options dialog box.

Step 11 Click the radio button for either **Install PostgreSQL** or **Use existing DB** to specify which database you want to use.

If you choose Install PostgreSQL, accept the defaults and enter a password. The PostgreSQL database will be installed.



Note If you choose to install PostgreSQL, you must disable any security software you are running, because PostgreSQL may not install certain folders or users.



Note Before you install PostgreSQL, remove the cygwin/bin from your environment variable path if Cygwin is running on your system.

Step 12 If you select Use existing DB, click the radio button for either PostgreSQL 8.1/8.2 or Oracle10g.

Step 13 Click **Next** in the Database Options dialog box.

You see the Configuration Options dialog box.

Step 14 Click **Install** to install Cisco DCNM-SAN Server.

If you are evaluating one of these Cisco DCNM-SAN Server features and want to stop the evaluation period for that feature, you can do that using Device Manager.

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 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:

- 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

Fabric Manager Release 2.1(2) or later allows you to modify certain Cisco DCNM-SAN Server settings without stopping and starting the server.

- [Adding or Removing Cisco DCNM-SAN Server Users section, page 2-8](#)
- [Changing the Cisco DCNM-SAN Server Username and Password section, page 2-9](#)
- [Changing the DCNM-SAN Server Fabric Discovery Username and Password section, page 2-9](#)
- [Changing the Polling Period and Fabric Rediscovery Time section, page 2-9](#)
- [Using Device Aliases or FC Aliases section, page 2-10](#)

Adding or Removing Cisco DCNM-SAN Server Users

BEFORE YOU BEGIN

You must be a network administrator before you can manage users.

DETAILED STEPS

To add a Cisco DCNM-SAN Server user or to change the password for an existing user using DCNM-SAN, follow these steps:

-
- Step 1** Click the **Local FM Users** tab in the Control Panel dialog box. You see a list of DCNM-SAN users.
 - Step 2** Click **New** to add a user or click the user name and click **Edit** to change the password for an existing user. You see the FM User dialog box.
 - Step 3** Set the username and password for the new user and then click **Apply**.
-

-
- Step 1** Click the **Local FM Users** tab in the Control Panel dialog box. You see a list of DCNM-SAN users.
-

- Step 2** Click the username you want to delete.
 - Step 3** Click **Remove** to delete the user.
 - Step 4** Click **Yes** to confirm the deletion or **No** to cancel it.
-

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 3-3”.
-

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 Server

DETAILED STEPS

- Step 1** Stop the Cisco DCNM-SAN Server.
 - Step 2** Change the following parameter in the \$INSTALLDIR/conf/FMServer.conf.
wrapper.app.parameter.4=127.0.0.1
 - Step 3** Change the following parameter in the \$INSTALLDIR/conf/server.properties.
server.bindaddr = 127.0.0.1
 - Step 4** Enter the following command to assign a new IP address.

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

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

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 the **Device Alias** check box to use global device aliases, or uncheck to use FC aliases.
 - Step 3** Click **Apply** to save these changes.
-

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.
The Control Panel appears.

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*.