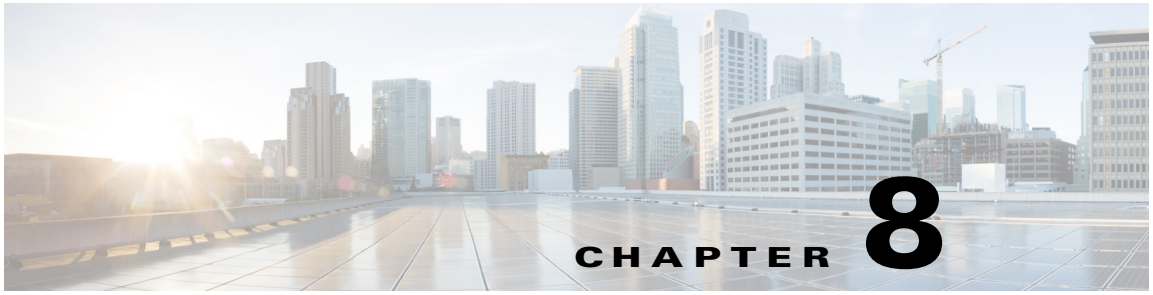

Configuring Cisco DCNM-SAN Server

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

This chapter contains the following sections:

Information About Cisco DCNM-SAN Server

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

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 8-3.

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 8-4.

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

Step 5 Install DCNM-SAN Web Server. See the "Verifying Performance Manager Collections" section on page 8-3.

Step 6 Verify Performance Manager is collecting data. See the "Verifying Performance Manager Collections" section on page 8-3.

Installing Cisco DCNM-SAN Server

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

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

- DCNM Web Client
- DCNM SAN + LAN Client

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

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

For detailed Cisco DCNM installation steps, please refer to

Cisco DCNM Installation Guide, Release 10.0(x).

Data Migration in Cisco DCNM-SAN Server

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

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

Verifying Performance Manager Collections

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

Managing a Cisco DCNM-SAN Server Fabric

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

Selecting a Fabric to Manage Continuously

DETAILED STEPS

Step 1 Choose **Server > Admin**.

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

Note The Fabrics tab is only accessible to network administrators.

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

Step 2 Choose one of the following Admin options:

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

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

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

Step 3 Click **Apply**.

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

Cisco DCNM-SAN Server Properties File

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

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

The server properties file contains these nine general sections:

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

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

SNMP Specific

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

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

Performance Chart

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

EMC Call Home

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

Event Forwarding

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

Deactivation

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

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

Modifying Cisco DCNM-SAN Server

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

Changing the Cisco DCNM-SAN Server Username and Password

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

DETAILED STEPS

Step 1 Choose **Server > Admin**.

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

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

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

Changing the DCNM-SAN Server Fabric Discovery Username and Password

DETAILED STEPS

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

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

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

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

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

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

DETAILED STEPS

Step 1 Choose **Server > Admin**.

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

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

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

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

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

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

Detailed Steps

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

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

- *$INSTALLDIR\jboss-as-7.2.0.Final\bin\service\sanservice.bat*

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

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

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

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

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

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

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

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

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

Changing the IP address of primary server

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

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

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

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

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

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

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

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

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

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

Changing the IP address of secondary server

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Detailed Steps

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

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

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

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

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

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

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

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

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

Using Device Aliases or FC Aliases

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

DETAILED STEPS

Step 1 Choose **Server > Admin**.

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

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

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

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

Configuring Security Manager

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

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

You see the control panel.

Server Federation

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

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

Restrictions

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

Mapping Fabric ID to Server ID

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

DETAILED STEPS

Step 1 Choose **Server > Admin**.

You see the Control Panel.

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

You see the Move Fabric dialog box.

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

Step 4 Click **Move**.

Opening the Fabric on a Different Server

DETAILED STEPS

Step 1 Choose **Server > Admin**.

You see the Control Panel.

Step 2 Click **Discover**.

You see the Discover New Fabric dialog box.

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

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

Step 5 In the password field, enter the password.

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

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

Step 8 Click **Discover**.

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

Viewing the Sessions in a Federation

DETAILED STEPS

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

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

You see the Control Panel.

Viewing the Servers in a Federation

DETAILED STEPS

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

Step 2 Click the **Servers** tab.

You see the Control Panel.

Discover Devices Managed by SVI

Step 1 Log on to the DCNM Web Client.

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

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

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

Step 5 Click **Apply**.

Step 6 Restart the DCNM service.

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

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

Step 8 Retry the discovery.

Note Each SVI switch must be discovered separately.

Additional References

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