Configuring Authentication in Cisco DCNM-SAN

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

This chapter contains the following sections:

Information About Cisco DCNM-SAN Authentication

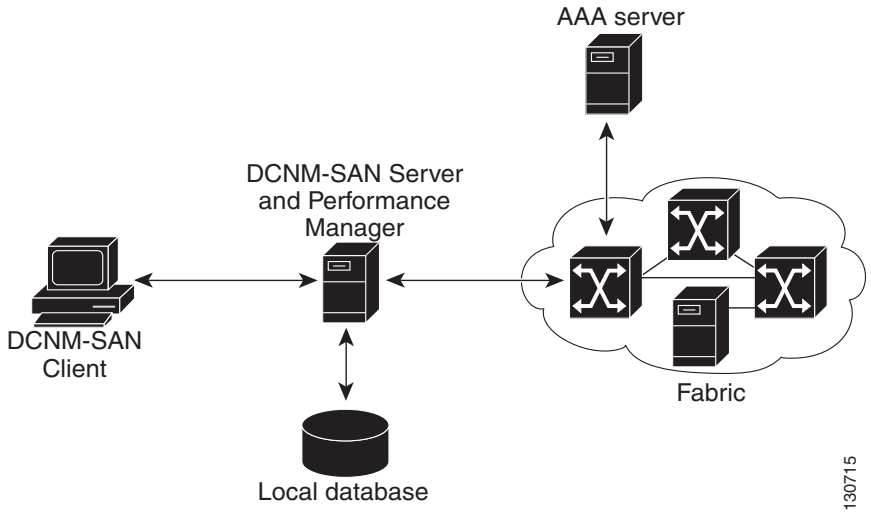
Cisco DCNM-SAN contains multiple components that interact to manage a fabric.

These components include:

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

Figure 9-1 shows an example configuration for these components.

Figure 9-1 Cisco DCNM-SAN Authentication Example



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

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

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

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

Best Practices for Discovering a Fabric

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

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

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

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

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

Setting Up Discovery for a Fabric

DETAILED STEPS

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

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

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

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

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

Performance Manager Authentication

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

DETAILED STEPS

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

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

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

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

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

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

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

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

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

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

Cisco DCNM-SAN Web Client Authentication

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

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

DETAILED STEPS

Step 1 Launch Cisco DCNM-SAN Web Client.

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

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

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

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

Step 1 Launch Cisco DCNM-SAN Web Client.

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

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

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

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

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