CHAPTER 7

Authentication in Fabric Manager

Fabric Manager contains interdependent software components that communicate with the switches in your fabric. These components use varying methods to authenticate to other components and switches. This chapter describes these authentication steps and the best practices for setting up your fabric and components for authentication.

This chapter contains the following sections:

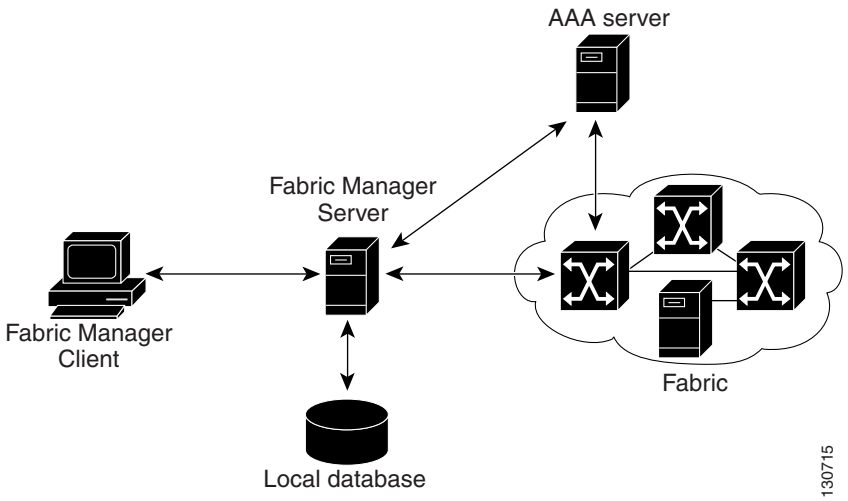
Fabric Manager Authentication Overview

Fabric Manager contains multiple components that interact to manage a fabric. These components include:

- Fabric Manager client
- Fabric Manager server
- Performance Manager
- Interconnected fabric of Cisco MDS 9000 switches and storage devices
- AAA server (optional)

Figure 7-1 shows an example configuration for these components.

Figure 7-1 Fabric Manager Authentication Example



Administrators launch Fabric Manager client and select the seed switch that is used to discover the fabric. The username and password used are passed to Fabric Manager server and used to authenticate to the seed switch. If this username and password are not a recognized SNMP username and password, either Fabric Manager client or Fabric Manager server opens a CLI session to the switch (SSH or Telnet) and retries the username/password pair. If the username 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 username that is used by Fabric Manager client and server.

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

Note You must allow CLI sessions to pass through any firewall that exists between Fabric Manager client and Fabric Manager server. See the "Running Fabric Manager Behind a Firewall" section on page 1-12.

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

Best Practices for Discovering a Fabric

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

We recommend you use these best practices for discovering your network and setting up Performance Manager. This ensures that Fabric Manager server has a complete view of the fabric. Subsequent Fabric Manager 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 Fabric Manager server using a network administrator or network operator role so that Fabric Manager server has a view of all the VSANs in the fabric. When a VSAN-limited user launches Fabric Manager client, that user sees only the VSANs they are allowed to manage.

We recommend you use these best practices for discovering your network and setting up Performance Manager.

Setting up Discovery for a Fabric

To ensure that Fabric Manager server discovers your complete fabric, follow these steps:

Step 1 Create a special Fabric Manager administrative username in each switch on your fabric with network administrator or network operator roles. Or, create a special Fabric Manager administrative username 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 Fabric Manager administrative username are the same on all switches in the fabric and that this role has access to all VSANs.

Step 3 Launch Fabric Manager client using the Fabric Manager administrative user. This ensures that your fabric discovery includes all VSANs.

Step 4 Set Fabric Manager Server to continuously monitor the fabric. See the "Fabric Manager Server Fabric Monitoring and Removal" section on page 2-7.

Step 5 Repeat Step 4 for each fabric that you want to manage through Fabric Manager server.

Performance Manager Authentication

Performance Manager uses the username and password information stored in the Fabric Manager server database. If this information changes on the switches in your fabric while Performance Manager is running, you need to update the Fabric Manager server database and restart Performance Manager. Updating the Fabric Manager server database requires removing the fabric from Fabric Manager server and rediscovering the fabric.

To update the username and password information used by Performance Manager, follow these steps:

Step 1 Choose **Server > Admin** in Fabric Manager. You see the Admin dialog box.

Step 2 Click the **Fabrics** tab to view the fabrics currently monitored by Fabric Manager server.

Step 3 Right-click the fabrics that have updated username and password information.

Step 4 Click **Remove** to remove these fabrics from Fabric Manager server.

Step 5 Choose **File > Open Fabric.** You see the Open Fabric dialog box.

Step 6 Set the seed switch and the appropriate username and password to rediscover the fabric.

Step 7 Click **Open** to rediscover the fabric. Fabric Manager server updates its username and password information.

Step 8 Repeat Step 5 through Step 7 for any fabric that you need to rediscover.

Step 9 Click **Performance > Collector > Restart** to restart Performance Manager and use the new username and password.

Fabric Manager Web Services Authentication

Fabric Manager Web Services does not communicate directly with any switches in the fabric. Fabric Manager Web Services uses its own username 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 Fabric Manager Web Services.

To configure Fabric Manager Web Services to use RADIUS authentication, follow these steps:

Step 1 Launch Fabric Manager Web Services. See the "Launching and Using Fabric Manager Web Services" section on page 5-7.

Step 2 Choose **Admin > Web Users** to update the authentication used by Fabric Manager Web Services.

Step 3 Click **AAA**.

Step 4 Set the authentication.mode attribute to **radius**.

Step 5 Set the RADIUS server name, shared secret, authentication method, and ports used for up to three RADIUS servers.

Step 6 Click **Modify** to save this information.

To configure Fabric Manager Web Services to use TACACS+ authentication, follow these steps:

Step 1 Launch Fabric Manager Web Services. See the "Launching and Using Fabric Manager Web Services" section on page 5-7.

Step 2 Choose **Admin > Web Users** to update the authentication used by Fabric Manager Web Services.

Step 3 Click **AAA**.

Step 4 Set the authentication.mode attribute to **tacacs**.

Step 5 Set the TACACS+ server name, shared secret, authentication method, and port used for up to three TACACS+ servers.

Step 6 Click **Modify** to save this information.