Send documentation comments to fm-docfeedback@cisco.com

CHAPTER 4

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, page 4-1
- Best Practices for Discovering a Fabric, page 4-3
- Performance Manager Authentication, page 4-4
- Fabric Manager Web Server Authentication, page 4-4

Fabric Manager Authentication Overview

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

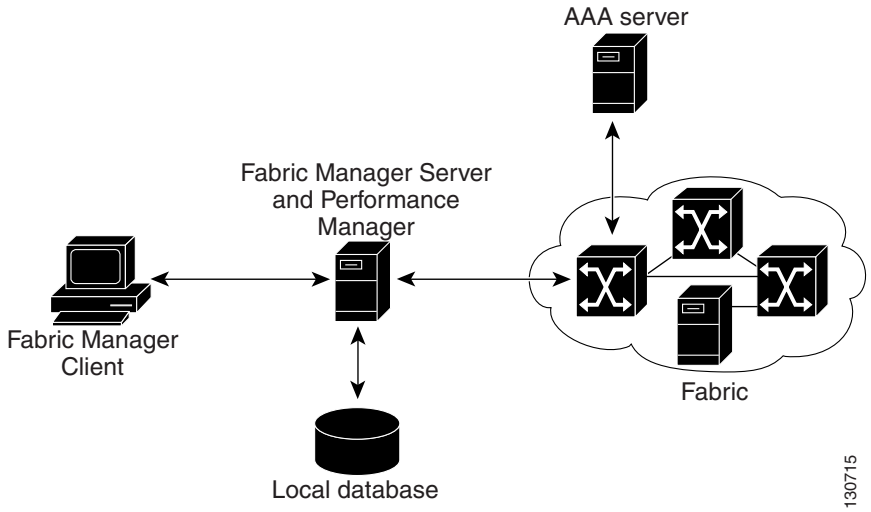
These components include:

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

Figure 4-1 shows an example configuration for these components.

Send documentation comments to fm-docfeedback@cisco.com

Figure 4-1 Fabric Manager Authentication Example



Administrators launch Fabric Manager Client and select the seed switch that is used to discover the fabric. The user name and password used are passed to Fabric Manager 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 Fabric Manager Client or Fabric Manager 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 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 2-42.

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.

Send documentation comments to fm-docfeedback@cisco.com

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.

Caution If the Fabric Manager Server's CPU usage exceeds 50 percent, it is recommended that you switch to a higher CPU-class system. For more information on recommended hardware, see the "Before You Install" section on page 2-19.

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.

Note Fabric Manager 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. For more information on Fabric Manager Server fabric monitoring, see the "Managing a Fabric Manager Server Fabric" section on page 3-7.

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 user name in each switch on your fabric with network administrator or network operator roles. Or, create a special Fabric Manager 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 Fabric Manager administrative user name 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 "Managing a Fabric Manager Server Fabric" section on page 3-7.

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

Send documentation comments to fm-docfeedback@cisco.com

Performance Manager Authentication

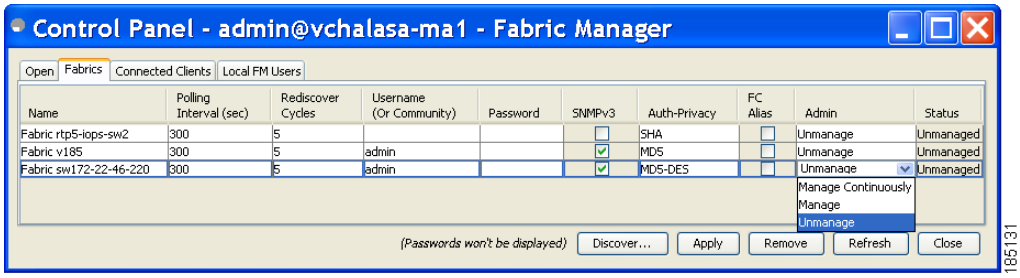
Performance Manager uses the user name and password information stored in the Fabric Manager Server database. If this information changes on the switches in your fabric while Performance Manager is running, you need to update the Fabric Manager Server database and restart Performance Manager. Updating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

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

Step 1 Click **Server > Admin** in Fabric Manager.

You see the Control Panel dialog box with the Fabrics tab open (see Figure 4-2).

Figure 4-2 Fabrics Tab in Control Panel Dialog Box



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.**

Step 5 From the Admin listbox, select **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. Fabric Manager 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.

Fabric Manager Web Server Authentication

Fabric Manager Web Server does not communicate directly with any switches in the fabric. Fabric Manager 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 Fabric Manager Web Server.

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

Send documentation comments to fm-docfeedback@cisco.com

Step 1 Launch Fabric Manager Web Server.

See the "Launching Fabric Manager Web Client" section on page 7-7.

Step 2 Click the **Admin** tab **> Configure** to update the authentication used by Fabric Manager Web Server.

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 Server to use TACACS+ authentication, follow these steps:

Step 1 Launch Fabric Manager Web Server.

See the "Launching Fabric Manager Web Client" section on page 7-7.

Step 2 Click **Admin > Configure** to update the authentication used by Fabric Manager Web Server.

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.

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

Send documentation comments to fm-docfeedback@cisco.com