CHAPTER 25

Users and Common Roles

Fabric Manager provides the capability to configure and manage several different types of security for MDS 9000 switches.

This chapter includes the following sections:

Role-Based Authorization

Switches in the Cisco MDS 9000 Family perform authentication based on roles. Role-based authorization limits access to switch operations by assigning users to roles. This kind of authentication restricts you to management operations based on the roles to which you have been added.

When you execute a command, perform command completion, or obtain context sensitive help, the switch software allows the operation to progress if you have permission to access that command.

Each role can contain multiple users and each user can be part of multiple roles. For example, if role1 users are only allowed access to configuration commands, and role2 users are only allowed access to debug commands, then if Joe belongs to both role1 and role2, he can access configuration as well as debug commands.

Note If you belong to multiple roles, you can execute a union of all the commands permitted by these roles. Roles are cumulative. Access to a command takes priority over being denied access to a command. For example, suppose you belong to a TechDocs group and you were denied access to configuration commands. However, you also belong to the engineering group and have access to configuration commands. In this case, you will have access to configuration commands.

Tip Any role, when created, does not allow access to the required commands immediately. The administrator must configure appropriate rules for each role to allow access to the required commands.

Configuring Common Roles

From Cisco SAN-OS Release 1.2(x), CLI and SNMP in all switches in the Cisco MDS 9000 Family use common roles.

You can use SNMP to modify a role that was created using CLI and vice versa. Each role in SNMP is the same as a role created or modified through the CLI. Common roles allow you to use a set of rules to set the scope of VSAN security. Each role can be restricted to one or more VSANs as required.

To configure common roles from the Device Manager, select **Common Roles** from the Security menu. You can then access the Rules dialog box to configure the set of rules.

To configure common roles from Fabric Manager, select **Security > SNMP** and click the **Roles** tab in the Information pane. Fabric Manager uses a default rules set for roles; therefore, no Rules dialog box is displayed.

Note Most tabs in the Information pane for features using CFS are dimmed until you click the CFS tab. The CFS tab shows which switches have CFS enabled and shows the master switch for this feature. Once the CFS tab is clicked, the other Information pane tabs that use CFS are activated.

Creating Common Roles

To create a common role, follow these steps.

Step 1 In Fabric Manager, choose **Switches > Security > SNMP** from the Physical Attributes , and click the **Roles** tab in the Information pane.
In Device Manager, choose **Common Roles** from the Security menu. You see the Common Roles dialog box.

Step 2 Click the **Create Row** icon to create a new role in Fabric Manager or click **Create** in Device Manager.

You see the Roles - Create dialog box.

Step 3 Select the switches on which you want to configure the role in Fabric Manager.

Step 4 Enter the name of the role in the Name field.

Step 5 Enter the description of the role in the Description field.

Step 6 Check the **Has Config and Exec Permission** check box if you want your role to have read, write, and create permission. If you do not check the **Has Config and Exec Permission** check box, your role will have read-only permission.

Step 7 Optionally, check the **Enable** check box to enable the VSAN scope and enter the list of VSANs in the Scope field that you want to restrict this role to.

Step 8 Click **Create** to create the role, or click **Close** to close the Roles - Create dialog box without creating the common role.

Note Device Manager automatically creates six roles that are required for Device Manager to display a view of a switch. These roles are: **system**, **snmp**, **module**, **interface**, **hardware**, and **environment**.

Editing Rules For Common Roles in Device Manager

Up to 16 rules can be configured for each role. The user-specified rule number determines the order in which the rules are applied. For example, rule 1 is applied before rule 2, which is applied before rule 3, and so on. A user not belonging to the network-admin role cannot perform commands related to roles.

Note The order of rule placement is important. If you place a more permissive policy after a restrictive policy, the permissive policy may have priority over the permissive policy.

To edit the rules for a common role in Device Manager, follow these steps.

Step 1 Choose **Security > Roles**. You see the Common Roles dialog box.

Step 2 Click the common role that you want to edit the rules for.

Step 3 Click **Rules** to view the rules for the role. You see the Rules dialog box. It may take a few minutes to display.

Step 4 Edit the rules you want to enable or disable for the common role.

Step 5 Click **Apply** to apply the new rules and close the Rules dialog, or click **Close** to close the Rules dialog without applying the rules.

Deleting Common Roles

To delete a common role, follow these steps:

Step 1 In Fabric Manager, choose **Switches > Security > SNMP** from the Physical Attributes pane and click the **Roles** tab in the Information pane.
In Device Manager, choose **Security > Common Roles**. You see the Common Roles dialog box i

Step 2 Click the common role you want to delete.

Step 3 Click the **Delete Row** icon in Fabric Manager or **Delete** in Device Manager to delete the common role.

Configuring the VSAN Policy

Configuring the VSAN policy or VSAN scope requires the ENTERPRISE_PKG license . See Chapter 9, “Obtaining and Installing Licenses.”

You can configure a role so that it only allows tasks to be performed for a selected set of VSANs. By default, the VSAN scope for any role is disabled. That is, the roles allow tasks to be performed in all VSANs. To configure a role to selectively allow tasks in a subset of VSANs, you must enable the VSAN scope and then list the appropriate VSANs in the VSAN list.

Note Users configured in roles where the VSAN scope is enabled cannot modify the configuration for E ports. They can only modify the configuration for F or FL ports (depending on whether the configured rules allow such configuration to be made). This is to prevent such users from modifying configurations that may impact the core topology of the fabric.

Tip Roles can be used to create VSAN administrators. Depending on the configured rules, these VSAN administrators can configure MDS features (for example, zone, fcdomain, or VSAN properties) for their VSANs without affecting other VSANs. Also, if the role permits operations in multiple VSANs, then the VSAN administrators can change VSAN membership of F or FL ports among these VSANs.

Users belonging to roles in which the VSAN scope is enabled are referred to as VSAN-restricted users. These users cannot perform tasks that require the startup configuration to be viewed or modified.

Modifying the VSAN Policy

To modify the VSAN policy or VSAN scope for an existing common role, follow these steps.

Step 1 In Fabric Manager, choose **Switches > Security > SNMP** from the Physical Attributes , and click the **Roles** tab in the Information pane.
In Device Manager, choose **Common Roles** from the Security menu. You see the Common Roles dialog box.

Step 2 Check the **enable** check box if you want to enable the VSAN scope and restrict this role to a subset of VSANs.

Step 3 Enter the list of VSANs in the VSAN Scope > List field that you want to restrict this role to.

Step 4 Click **Apply Changes** in Fabric Manager or click **Apply** in Device Manager to save these changes. Click **Undo Changes** in Fabric Manager or click **Close** in Device Manager to discard any unsaved changes.

Configuring User Accounts

Every Cisco MDS 9000 Family switch user has the account information stored by the system. Your authentication information, user name, user password, password expiration date, and role membership are stored in your user profile.

The tasks explained in this section enable you to create users and modify the profile of an existing user.These tasks are restricted to privileged users as determined by your administrator.

Note Cisco SAN-OS does not support all numeric usernames, whether created with TACACS+ or RADIUS, or created locally. Local users with all numeric names cannot be created. If an all numeric username exists on an AAA server and is entered during login, the user is not logged in.

Creating or Updating Users

As of Cisco MDS SAN-OS Release 2.x and later, the passphrase specified in the **snmp-server user** option and the password specified in the **username** option are synchronized.

By default, the user account does not expire unless you explicitly configure it to expire. The **expire** CLI option determines the date on which the user account is disabled. The date is specified in the YYYY-MM-DD format.

Tip The following words are reserved and cannot be used to configure users: bin, daemon, adm, lp, sync, shutdown, halt, mail, news, uucp, operator, games, gopher, ftp, nobody, nscd, mailnull, rpc, rpcuser, xfs, gdm, mtsuser, ftpuser, man, and sys.

Note User passwords are not displayed in the switch configuration file.

Creating Strong Passwords

If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password as shown in the sample configuration. Passwords are case-sensitive. As of Cisco MDS SAN-OS Release 2.x and later, admin is not the default password for any switch in the Cisco MDS 9000 Family. You must explicitly configure a password that meets the following requirements:

- Is at least eight characters in length
- Does not have multiple consecutive characters (such as abcd or jklm)
- Does not have multiple repeat characters (such as fff or qqdd)
- Does not contain words found in a dictionary
- Contains both upper and lower case characters
- Contais numbers.

Note Clear test passwords can only contain alphanumeirc characters. Special characters, such as the dollar sign ($) or the percent sign (%) are not allowed.

Adding a User

To add a user, follow these steps:

Step 1 In Fabric Manager, choose **Switches > Security > SNMP** from the Physical Attributes pane and click the **Users** tab in the Information pane.

In Device Manager, choose **Security > SNMP** and click the **Users** tab.

Step 2 Click the **Create Row** icon in Fabric Manager or click **Create** in Device Manager. You see the Create Users dialog box.

The dialog box from Fabric Manager also provides check boxes to specify one or more switches.

Step 3 Enter the user name in the **New User** field.

Step 4 Select the role from the drop-down menu in Fabric Manager or the check boxes in Device Manager. In Fabric Manager, you can enter a new role name in the field if you do not want to select one from the drop-down menu. If you do this, you must go back and configure this role appropriately (see the "Configuring Common Roles" section on page 25-2).

Step 5 Enter the password for the user twice in the New Password and Confirm Password fields.

Step 6 Check the **Privacy** check box and complete the password fields to encrypt management traffic.

Enter the same new password in the New Password and Confirm Password fields.

Step 7 Click **Create** to create the new entry or click **Close** to discard any unsaved changes and close the dialog box.

Deleting a User

To delete a user, follow these steps:

Step 1 In Fabric Manager, choose **Switches > Security > SNMP** from the Physical Attributes pane and click the **Users** tab in the Information pane.

In Device Manager, choose **Security > SNMP** and click the **Users** tab.

Step 2 Click the name of the user you want to delete.

Step 3 Click the **Delete Row** icon in Fabric Manager or **Delete** in Device Manager to delete the selected user.

Viewing User Information

To view information about users, follow these steps:

Step 1 In Fabric Manager, choose **Security > SNMP** from the Physical Attributes pane.
In Device Manager, choose **Security > SNMP**. You see the

Step 2 Click the **Users** tab in Fabric Manager. You see the list of SNMP users in the Information pane.

Configuring SSH Services

The Telnet service is enabled by default on all Cisco MDS 9000 Family switches. Before enabling the SSH service, generate a server key pair.

Generating the SSH Server Key Pair and Enabling SSH

Be sure to have an SSH server key pair with the appropriate version before enabling the SSH service. Generate the SSH server key pair according to the SSH client version used. The number of bits specified for each key pair ranges from 768 to 2048.

The SSH service accepts three types of key pairs for use by SSH versions 1 and 2.

- TheSSH1 option generates the RSA1 key pair for the SSH version 1 protocol.
- TheSSH2(dsa) option generates the DSA key pair for the SSH version 2 protocol.
- The SSH2(rsa) option generates the RSA key pair for the SSH version 2 protocol.

Caution If you delete all of the SSH keys, you cannot start a new SSH session.

To generate an SSH server key pair and enable SSH, follow these steps:

Step 1 In Fabric Manager, choose **Switches > Security > SSH**. You see the SSH configuration in the Information pane.
In Device Manager, choose **Security > SSH**. You see the SSH dialog box.

Step 2 Click the **Create Row** icon in Fabric Manager or click **Create** in Device Manager. You see the SSH Key Create dialog box.

Step 3 Optionally, check the switches you want this SSH key pair for in Fabric Manager.

Step 4 Choose the **Control** tab in Fabric Manager check the **enable** check box to enable SSH on the selected switches.
Check the **enable** check box in Device Manager to enable SSH.

Step 5 Choose the key pair option type from the Protocols radio buttons.

Step 6 Set the number of bits that will be used to generate the key pairs in the NumBits drop-down menu.

Step 7 Click **Create** to generate these keys or click **Close** to discard any unsaved changes.

Deleting a Generated Key Pair

If the SSH key pair option is already generated for the required SSH protocol version, you must delete the previously generated key pair before you can a new key pair for that SSH protocol version.

Recovering Administrator Password

An administrator can recover a password from a local console connection. The password recovery procedure must be performed on the supervisor module that becomes the active supervisor module after the recovery procedure is completed.

Note To recover a n administrator's password, refer to the *Cisco MDS 9000 Family Configuration Guide*.