CHAPTER 18

Troubleshooting Users and Roles

This chapter describes procedures used to troubleshoot users and roles created and maintained in the Cisco MDS 9000 Family Switch products. It includes the following sections:

Overview

The CLI and SNMP use common roles in all switches in the Cisco MDS 9000 Family. You can use the CLI to modify a role that was created using SNMP and vice versa. A user configured through the CLI can access the switch using SNMP (for example, Fabric Manager or Device Manager) and vice versa.

User Accounts

Every Cisco MDS 9000 Family switch user has the account information stored by the system. You can add up to 256 users to a switch. The authentication information, user name, user password, password expiration date, and role membership are stored in the user profile.

The most important aspect of a user is creating a strong password. Weak passwords are not accepted by Cisco SAN-OS, whether you try to configure them locally or attempt authentication using an AAA server.

A strong password has the following characteristics:

- Contains at least eight characters.
- Does not contain many consecutive characters (such as “abcd”).
- Does not contain many repeating characters (such as “aaabbb”).
- Does not contain dictionary words.
- Does not contain proper names.
- Contains both uppercase and lowercase characters.
- Contains numbers.

The following examples show strong passwords:

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Passwords are case-sensitive. The default password for any Cisco MDS 9000 Family switch is no longer “admin”. You must explicitly configure a strong password.

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

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.

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

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 users to management operations based on the roles to which they have been assigned the user.

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 switch operation.

Each role can be assigned to multiple users and each user can be part of multiple roles. If a user has multiple roles, the user has access to a combination of 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 a user belongs to multiple roles, the user can execute a union of all the commands permitted by these roles. 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 user access to the required commands immediately. The administrator must configure appropriate rules for each role to allow user access to the required commands.

Rules and Features for Each Role

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.

For example, if user A is permitted to perform all **show** commands, user A cannot view the output of the **show role** command if user A does not belong to the network-admin role

The **rule** command specifies operations that can be performed by a specific role. Each rule consists of a rule number, a rule type (permit or deny), a command type (for example, **config**, **clear**, **show**, **exec**, **debug**), and an optional feature name (for example, FSPF, zone, VSAN, fcping, or interface).

Note In this case, **exec** commands refer to all commands in the EXEC mode that do not fall in the **show**, **debug**, and **clear** categories.

The order of rule placement is important. For example, the first rule permits user access to all **config** commands. and the next rule denies FSPF configuration to the user. As a result, the user can perform all **config** commands except **fspf** configuration commands.

Note If you had swapped these two rules and issued the **deny config feature fspf** rule first and issued the **permit config** rule next, you would be allowing the user to perform all configuration commands because the second rule globally overrode the first rule.

Initial Troubleshooting Checklist

Begin troubleshooting user and role issues by checking the following issues:

Checklist	Check off
Verify licensing requirements. See *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.	❑
Verify that the passwords for all users follow the guidelines for strong passwords.	❑
Verify that no usernames are reserved words or all numeric.	❑
Verify that users with multiple roles are not assigned more access than planned.	❑
Verify that you have not assigned any empty roles to users.	❑
Verify the order of the rules in each role.	❑

Common Troubleshooting Tools in Fabric Manager

In Fabric Manager, choose **Switches > Security > Users and Roles** to access user and role configuration.

In Device Manager, use the following procedures to access user, role, and rule configurations:

- Choose **Security > Users** to access user configuration.
- Choose **Security > Roles** to access user configuration.
- Select a role from the Roles dialog box and click **Rules** to access the rules for this role.

Note Rules can only be configured from Device Manager.

Common Troubleshooting Commands in the CLI

Use the following CLI commands to troubleshoot user and role issues:

- **show users**
- **show user-account**
- **show role**
- **show role status**
- **show role session status**

User and Role Issues

This section describes troubleshooting user and role issues and includes the following topics:

User Cannot Log into Switch

Symptom User cannot log into the switch.

Table 18-1 User Cannot Log into Switch

Symptom	Possible Cause	Solution
User cannot log into the switch.	Weak password configured at the AAA server.	Create a stronger password. See the "User Accounts" section on page 18-1 for guidelines on strong passwords.
	User name is a restricted word or all numeric.	Change your user name. See the "User Accounts" section on page 18-1 for guidelines on allowed user names.
	User account has expired.	Choose **Switches > Security > Users** in Fabric Manager to view the user account expiration date. Or use the **show user-account** CLI command to verify the account expiration. Recreate the user if necessary.

Verifying User Login with System Messages Using Device Manager

To configure the switch logging to capture system messages when a user attempts to log into a switch, follow these messages:

Step 1 Choose **Logs > Syslog > Setup** and select the **Severity Levels** tab.

Step 2 Select **debug** from the Severity Level drop-down menu for auth, authPriv, and aaad. Click **Apply**.

This sets the switch to log debug information for these facilities.

Step 3 Select the **Switch Logging** tab, select **debug** from the LogFileMsgSeverity radio buttons, and click **Apply**,

This sets the switch to save system messages at the debug level or above in the switch log file. At this point, all future login attempts are tracked in the log file.

Step 4 After a login attempt, choose **Logs > Switch Resident > Syslogs > Since Reboot, and** click **Last Page** to view the most recent messages. You should see messages such as:

```
2006 Mar  2 22:08:44 v_190 %AUTHPRIV-6-SYSTEM_MSG: START: telnet pid=10654 from=
::ffff:161.44.67.125
2006 Mar  3 03:08:49 v_190 %AUTHPRIV-7-SYSTEM_MSG: Got user name <testUser>
2006 Mar  3 03:08:53 v_190 %AUTHPRIV-7-SYSTEM_MSG: user testUser authenticated
2006 Mar  3 03:08:53 v_190 %AUTHPRIV-7-SYSTEM_MSG: PAM login: updating snmpv3 US
M for user testUser
2006 Mar  3 03:08:53 v_190 %AUTHPRIV-7-SYSTEM_MSG: PAM login: snmpv3 attribute v
alue (null)
2006 Mar  3 03:08:53 v_190 %AUTHPRIV-7-SYSTEM_MSG: PAM login: updating snmpv3 US
M success for user testUser
2006 Mar  3 03:08:53 v_190 %AUTH-6-SYSTEM_MSG: (login) session opened for user t
estFoo by (uid=0)
2006 Mar  3 03:08:53 v_190 %AAA-6-AAA_ACCOUNTING_MESSAGE: start:/dev/pts/1_161.4
4.67.125:testUser:
```

Verifying User Login with System Messages Using the CLI

To configure the switch logging to capture system messages when a user attempts to log into a switch, follow these messages:

Step 1 Use the **logging leve**l command to change the level to 7 (debug) for auth, authPriv, and aaad.

```
switch(config)# logging level aaa 7
```

This sets the switch to log debug information for these facilities.

Step 2 Use the **logging logfile** command to set the logging level to 7 (debug) for system messages saved to the named log file.

```
switch(config)# logging logfile TestFile 7
```

This sets the switch to save system messages at the debug level or above in the TestFile log file. At this point, all future login attempts are tracked in the log file.

Step 3 After a login attempt, use the **show logging logfile | last** command to view the most recent messages. You should see messages such as:

```
2006 Mar  2 22:08:44 v_190 %AUTHPRIV-6-SYSTEM_MSG: START: telnet pid=10654 from=
::ffff:161.44.67.125
2006 Mar  3 03:08:49 v_190 %AUTHPRIV-7-SYSTEM_MSG: Got user name <testUser>
2006 Mar  3 03:08:53 v_190 %AUTHPRIV-7-SYSTEM_MSG: user testUser authenticated
2006 Mar  3 03:08:53 v_190 %AUTHPRIV-7-SYSTEM_MSG: PAM login: updating snmpv3 US
M for user testUser
2006 Mar  3 03:08:53 v_190 %AUTHPRIV-7-SYSTEM_MSG: PAM login: snmpv3 attribute v
alue (null)
2006 Mar  3 03:08:53 v_190 %AUTHPRIV-7-SYSTEM_MSG: PAM login: updating snmpv3 US
M success for user testUser
2006 Mar  3 03:08:53 v_190 %AUTH-6-SYSTEM_MSG: (login) session opened for user t
estFoo by (uid=0)
2006 Mar  3 03:08:53 v_190 %AAA-6-AAA_ACCOUNTING_MESSAGE: start:/dev/pts/1_161.4
4.67.125:testUser:
```

User Cannot Create Roles

Symptom User cannot create roles.

Table 18-2 User Cannot Create Roles

Symptom	Possible Cause	Solution
User cannot create roles.	User not assigned network-admin role.	Assign network-admin role to the user. See the "Verifying Roles Using Device Manager" section on page 18-8 or the "Verifying Roles Using the CLI" section on page 18-9.

User Cannot Create Other Users With Fabric Manager or Device Manager

Symptom User cannot create other users with Fabric Manager or Device Manager.

Table 18-3 User Cannot Create Other Users with Fabric Manager or Device Manager

Symptom	Possible Cause	Solution
User cannot create other users.	User is not logged into Fabric Manager or Device Manager with a privacy password.	Log into Fabric Manager or Device Manager with a password and a privacy password. A privacy password is required to manage users via the GUI. **Note** If you have logged in as a network-admin using MDS authentication, Device Manager and Fabric Manager automatically provide the appropriate encryption for this task, even if you did not specify a specific privacy password.

User Cannot Access Certain Features

Symptom User cannot access certain features.

Table 18-4 User Cannot Access Certain Features

Symptom	Possible Cause	Solution
User cannot access certain features.	User is assigned incorrect role.	For RADIUS, configure the vendor-specific attributes on the server for the role using `Cisco-AVPair = "shell: roles = "<rolename>" "`. For TACACS+, configure the attribute and value pair on the server for the role using `roles="vsan-admin storage-admin"`. See the "Verifying Roles Using Device Manager" section on page 18-8 or the "Verifying Roles Using the CLI" section on page 18-9.
	Role is not configured for appropriate access.	See the "Verifying Roles Using Device Manager" section on page 18-8 or the "Verifying Roles Using the CLI" section on page 18-9.

Verifying Roles Using Device Manager

To verify user role-based access using Device Manager, follow these steps:

Step 1 Choose **Security > Users...** to view the roles assigned to the user.

Step 2 Right-click a user and click **Delete** to delete the user.

Step 3 Click **Create** to create a user. You see the Create User dialog box.

Step 4 Set the username and password fields.

Step 5 Check the **role** check boxes for each role that you want to assign to the user and click **Create** to create the user.

Step 6 Choose **Security > Roles...** to view the roles.

Step 7 Right-click a role and select **Rules** to view or modify the rules assigned to a role.

Step 8 Check the **feature** check boxes for the features that you want this role to access and click **Apply** to save these changes.

Verifying Roles Using the CLI

To verify user role-based access using the CLI, follow these steps:

Step 1 Use the **show user-account** command to view the roles assigned to the user.

```
switch# show user-account user1
user:user1
        this user account has no expiry date
        roles:sangroup vsan-admin
no password set. local login not allowed
Remote login through RADIUS is possible
```

Step 2 Use the **username** command to modify the roles assigned to a user.

```
switch# no username user1 role vsan-admin
```

Step 3 Use the **show role** command to view the rules assigned to the role.

```
switch# show role sangroup
Role: sangroup
  Description: SAN management group
  vsan policy: permit

  ----------------------------------------------
  Rule    Type    Command-type      Feature
  ----------------------------------------------
    1.   permit    config                  *
    2.     deny    config                fspf
    3.   permit     debug                zone
    4.   permit      exec              fcping
```

Step 4 Use the **role** command to modify the rules assigned to a role.

```
switch# role name sangroup
switch(config-role)# no rule 4
switch(config-role)# rule 4 deny exec feature fcping
```

User Has Too Much Access

Symptom User has too much access.

Table 18-5 User Has Too Much Access

Symptom	Possible Cause	Solution
User has too much access.	User is assigned incorrect role or overlapping roles.	For RADIUS, configure the vendor-specific attributes on the server for the role using `Cisco-AVPair = "shell: roles = "<rolename>" "`. For TACACS+, configure the attribute and value pair on the server for the role using `roles="vsan-admin storage-admin"`. See the "Verifying Roles Using Device Manager" section on page 18-8 or the "Verifying Roles Using the CLI" section on page 18-9.
	Role is not configured for appropriate access.	See the "Verifying Roles Using Device Manager" section on page 18-8 or the "Verifying Roles Using the CLI" section on page 18-9.

User Cannot Configure Some VSANs

Symptom User cannot configure some VSANs.

Table 18-6 User Cannot Configure Some VSANs

Symptom	Possible Cause	Solution
User cannot configure some VSANs.	User is assigned a VSAN-restricted role.	See the "Verifying VSAN-Restricted Roles Using Fabric Manager" section on page 18-10 or the "Verifying VSAN-Restricted Roles Using the CLI" section on page 18-11.

Verifying VSAN-Restricted Roles Using Fabric Manager

To verify user role-based access using Fabric Manager, follow these steps:

Step 1 Choose **Switches > Security > Users and Roles** and select the **Roles** tab to view the roles.

Step 2 Check the **Scope Enable** check box to make the role VSAN-restricted.

Step 3 Add the range of VSANs that you want to allow this role to configure in the Scope VSAN Id List field.

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

Step 5 Select the **Roles CFS** tab and select **commit** from the Config Action drop-down menu.

Step 6 Click **Apply Changes** to distribute these changes through the fabric.

Verifying VSAN-Restricted Roles Using the CLI

To verify user role-based access using the CLI, follow these steps:

Step 1 Use the **show user-account** command to view the roles assigned to the user.

```
switch# show user-account user1
user:user1
        this user account has no expiry date
        roles:sangroup vsan-admin
no password set. local login not allowed
Remote login through RADIUS is possible
```

Step 2 Use the **show role** command to view the rules assigned to the role.

```
switch# show role sangroup
Role: sangroup
  Description: SAN management group
  vsan policy: deny
  Permitted vsans: 10-30

  ----------------------------------------------
  Rule    Type    Command-type      Feature
  ----------------------------------------------
    1.   permit    config                  *
    2.     deny    config               fspf
    3.   permit     debug               zone
    4.   permit      exec             fcping
```

Step 3 Use the **role** command to modify the VSAN policy for a role.

```
switch# role name sangroup
switch(config-role)# vsan policy deny
switch(config-role)# permit vsan 1 - 30
```

User Cannot Configure E Ports

Symptom User cannot configure E ports.

Table 18-7 User Cannot Configure E Ports

Symptom	Possible Cause	Solution
User cannot configure E ports.	User is assigned a VSAN-restricted role.	See the "Verifying VSAN-Restricted Roles Using Fabric Manager" section on page 18-10 or the "Verifying VSAN-Restricted Roles Using the CLI" section on page 18-11.

Unexpected User Displayed in Logs

Symptom Unexpected user displayed in logs.

Table 18-8 Unexpected User Displayed in Logs

Symptom	Possible Cause	Solution
Unexpected user displayed in logs.	Temporary user created by SNMP, Fabric Manager, or Device Manager.	Temporary users are created by Fabric Manager, Device Manager, or other applications using SNMP. This is normal behavior. These temporary users have a one hour expiration time. If you have an unexpected user with different characteristics, you should investigate that user or use the **clear user** CLI command to terminate that user session.

Troubleshooting Users and Roles with Cisco ACS

To troubleshoot user and role issues with Cisco ACS, follow these steps:

Step 1 Choose **Network Configuration** using Cisco ACS and view the AAA Clients table to verify that the Cisco SAN-OS switch is configured as an AAA client on Cisco ACS.

Step 2 Choose **User Setup > User Data Configuration** to verify that the user is configured.

Step 3 View the Cisco IOS/PIX RADIUS Attributes setting for a user. Verify that the user is assigned the correct roles in the AV-pairs. For example, `shell:roles="network-admin"`.

Note The Cisco IOS/PIX RADIUS Attributes field is case-sensitive. Verify that the role listed in the AV-pair exists on the Cisco SAN-OS switch.

Step 4 If the Cisco IOS/PIX RADIUS Attributes field is not present, follow these steps:

a. Choose **Interface > RADIUS (Cisco IOS/PIX).**

b. Check the **User** and **Group** check boxes for the cisco-av-pair option and click **Submit**.

c. Choose **User Setup > User Data Configuration** and add the AV-pair to assign the correct role to each user.

Step 5 Choose **System Configuration > Logging** to activate logs to look for reasons for failed authentication attempts.

Step 6 Choose **Reports and Activity** to view the resulting logs.

Step 7 On the Cisco SAN-OS switch, use the **show radius-server** command to verify that the RADIUS server timeout value is set to 5 seconds or greater.

Refer to the *User guide for Cisco Secure ACS* at the following website for more information:

http://cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_list.html