CHAPTER 26

Configuring Users and Common Roles

The CLI and SNMP use common roles in all switches in the Cisco MDS 9000 Family. You can use CLI to modify a role that was created using SNMP and vice versa.

Users, passwords, and roles for all CLI and SNMP users are the same.

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

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 Roles and Profiles

	Command	Purpose
Step 1	`switch# `**`config t`**	

Step 2	`switch(config)# `**`role name techdocs`**
	`switch(config-role)#`	

	`switch(config)#`	

Step 3	`switch(config-role)# `**`description`**
	`Entire Tech. Docs. group`	

	`no description`	

Configuring Rules and Features for Each Role

show

show role

rule

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).

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

Modifying Profiles

`config t`	
`role name sangroup`	

	rule 1 permit config rule 2 deny config feature fspf rule 3 permit debug feature zone rule 4 permit exec feature fcping	**zone debug** **fcping**
Step 4		Deletes rule 4, which no longer permits the sangroup to perform the command.

fspf

deny config

feature fspf **permit config**

Configuring the VSAN Policy

Configuring the VSAN policy requires the ENTERPRISE_PKG license (see Chapter 3, “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 policy for any role is permit, which allows tasks to be performed for all VSANs. You can configure a role that only allows tasks to be performed for a selected set of VSANs. To selectively allow VSANs for a role, set the VSAN policy to deny, and then set the configuration to permit or the appropriate VSANs.

Users configured in roles where the VSAN policy is set to deny 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.

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 policy is set to deny are referred to as VSAN-restricted users. These users cannot perform commands that require the startup configuration to be viewed or modified.

These commands include the **copy running-config startup-config**, **show startup-config**, **show running-config diff**, and **copy startup-config running-config** commands. For information on these commands, see Chapter 2, “Before You Begin.”

Modifying the VSAN Policy

	Command	Purpose
Step 1		
Step 2		
Step 3	**vsan policy deny** switch(config-role-vsan)	
	switch(config-role)#	
	switch(config-role-vsan)# **10-30**	
	no permit **vsan 15-20**	

Distributing Role-Based Configurations

Chapter 5, "Using the CFS Infrastructure").

The following configurations are distributed:

- Role names and descriptions
- List of rules for the roles
- VSAN policy and the list of permitted VSANs

Database Implementation

- Configuration database—The database currently enforced by the fabric.
- Pending database—Your subsequent configuration changes are stored in the pending database. If you modify the configuration, you need to commit or discard the pending database changes to the configuration database. The fabric remains locked during this period. Changes to the pending database are not reflected in the configuration database until you commit the changes.

Locking The Fabric

-
-

Committing the Changes

	Command	Purpose
Step 1		
Step 2		

If you discard (abort) the changes made to the pending database, the configuration database remains unaffected and the lock is released.

To discard role-based configuration changes, follow these steps:

	Command	Purpose
Step 1		
Step 2		

Enabling Distribution

	Command	Purpose
Step 1		
Step 2		

Clearing Sessions

Caution

Database Merge Guidelines

-
-

Displaying Role-Based Information

Example 26-1 Displays Information for All Roles

```
        show role
Role: network-admin
Description: Predefined Network Admin group. This role cannot be modified
Access to all the switch commands

Role: network-operator
Description: Predefined Network Operator group. This role cannot be modified
Access to Show commands and selected Exec commands

Role: svc-admin
Description: Predefined SVC Admin group. This role cannot be modified
Access to all SAN Volume Controller commands

Role: svc-operator
Description: Predefined SVC Operator group. This role cannot be modified
Access to selected SAN Volume Controller commands

Role: TechDocs
  vsan policy: permit (default)

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
```

Displaying Role-Based When Distribution is Enabled

Displays the Role Status Information

```
Session State: Locked

Last operation (initiated from this switch): Distribution enable
Last operation status: Success
```

```
myrole
```

rule 1 permit config feature fspf

show role pending

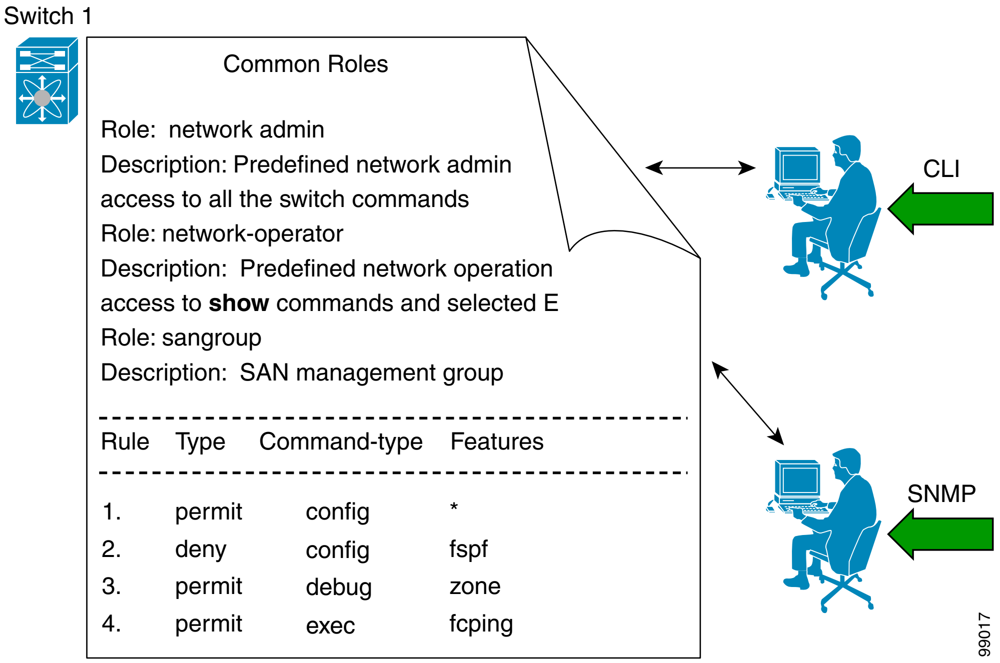
Example 26-3 Displays Information on the Pending Roles Database

Example 26-4 Displays the Differences between the Two Databases

```
+Role: myrole
+  vsan policy: permit (default)
+  ---------------------------------------------
+  Rule    Type    Command-type      Feature
+  ---------------------------------------------
+    1.   permit    config                fspf
```

Configuring Common Roles

Figure 26-1 Common Roles



Common Roles

Role: network admin
Description: Predefined network admin
access to all the switch commands
Role: network-operator
Description: Predefined network operation
access to **show** commands and selected E
Role: sangroup
Description: SAN management group

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

Mapping of CLI operations to SNMP

Note

CLI Operation to SNMP Operation Mapping

CLI Operation	SNMP Operation

Example

```
        show role name my_role
Role:my_role
  vsan policy:permit (default)
  ---------------------------------------------
  Rule    Type    Command-type      Feature
  ---------------------------------------------
    1.   permit     clear                  *
    2.     deny     clear                ntp
    3.   permit    config                  *
    4.     deny    config                ntp
    5.   permit     debug                  *
    6.     deny     debug                ntp
    7.   permit      show                  *
    8.     deny      show                ntp
    9.   permit      exec                  *
```

Although CONFIG is denied for NTP in rule 4, rule 9 allows the SET to NTP MIB objects because EXEC also maps to the SNMP SET operation.

Configuring User Accounts

Characteristics of Strong Passwords

-
-
-
-

-
-
-

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

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

Creating or Updating Users

The passphrase specified in the **snmp-server user** **username**

expire

Cisco MDS 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.

To issue commands with the keyword for troubleshooting purposes, you must have an account that is a member of the network-admin group.

To configure a new user or to modify the profile of an existing user, follow these steps:

	Enters configuration mode.
username usam password abcd123AAA expire 2003-05-31	
username msam password 0 abcd12AAA role network-operator	
username user1 password 5 !@*asdsfsdfjh!@df	password (!@*asdsfsdfjh!@df) for the user account (user1).
	Adds the specified user (usam) to the network-admin role.
	Deletes the specified user (usam) from the vsan-admin role.
AAAAB3NzaC1yc2EAAAABIwAAAIEAtjIHrIt/3dDeohix6JcRSIYZ0EOdJ3l5RONWcwSgAuTUSrLk 3a9hdYkzY94fhHmNGQGCjVg+8cbOxyH4Z1jcVFcrDogtQT+Q8dveqts/8XQhqkNAFeGy4u8TJ2Us oreCU6DlibwkpzDafzKTpA5vB6FmHd2TI6Gnse9FUgKD5fs=	
no username admin sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAtjIHrIt/3dDeohix6JcRSIYZ0EOdJ3l5RONWcwSgAuTUSrLk 3a9hdYkzY94fhHmNGQGCjVg+8cbOxyH4Z1jcVFcrDogtQT+Q8dveqts/8XQhqkNAFeGy4u8TJ2Us oreCU6DlibwkpzDafzKTpA5vB6FmHd2TI6Gnse9FUgKD5fs=	

To log out another user on the switch, use the command.

In the following example, the user named vsam is logged out from the switch.

Use the command to view a list of the logged in users (see Example 26-5).

Example 26-5 Displays All Logged in Users

```
admin    pts/7        Jan 12 20:56 (10.77.202.149)
admin    pts/9        Jan 12 23:29 (modena.cisco.com)
admin    pts/10       Jan 13 03:05 (dhcp-171-71-58-120.cisco.com)
admin    pts/11       Jan 13 01:53 (dhcp-171-71-49-49.cisco.com)
```

```
switch#
user:user1
        this user account has no expiry date
        roles:network-operator
no password set. Local login not allowed
Remote login through RADIUS is possible
```

Example 26-7 Displays Information for All Users

```
switch#
show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:usam
        expires on Sat May 31 00:00:00 2003
        roles:network-admin network-operator
user:msam
        this user account has no expiry date
        roles:network-operator
user:user1
        this user account has no expiry date
        roles:network-operator
no password set. local login not allowed
Remote login through RADIUS is possible
```

Configuring SSH Services

ssh key

Enabling SSH Service

	Command	Purpose
Step 1		
Step 2		

Caution

Enter

Specifying the SSH Key

	Command	Purpose
Step 1		
Step 2		

Generating the SSH Server Key Pair

-
-
-

Caution

	Command	Purpose
Step 1		Enters configuration mode.
Step 2		Generates the RSA1 server key pair.
		Generates the DSA server key pair.
		Generates the RSA server key pair.
		Clears the RSA server key pair configuration.

Overwriting a Generated Key Pair

	Command	Purpose
Step 1		Enters configuration mode.

Step 2	**ssh key dsa 768**
	`dsa keys already present, use force option to overwrite them`
	`switch(config)#`
	`deleting old dsa key.....`
	`generating dsa key.....`
	`generated dsa key`	

Clearing SSH Hosts

SCP/SFTP along with command for particular hosts.

Example 26-8 Using SCP/SFTP to Copy Files

```
        copy scp://abcd@171.71.48.223/users/abcd/abc
bootflash:abc The authenticity of host '171.71.48.223 (171.71.48.223)'
can't be established.
RSA1 key fingerprint is 01:29:62:16:33:ff:f7:dc:cc:af:aa:20:f8:20:a2:db.
Are you sure you want to continue connecting (yes/no)? yes
Added the host to the list of known hosts
(/var/home/admin/.ssh/known_hosts). [SSH key information about the host is
stored on the switch]
abcd@171.71.48.223's password:
switch#
```

If a host's SSH key changes before you use SCP/SFTP along with the command, you will receive an error (see Example 26-9).

Example 26-9 Using SCP/SFTP to Copy Files—Error Caused by SSH Key Change

```
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA1 host key has just been changed.
The fingerprint for the RSA1 key sent by the remote host is
36:96:ca:d7:29:99:79:74:aa:4d:97:49:81:fb:23:2f.
Please contact your system administrator.
Add correct host key in /mnt/pss/.ssh/known_hosts to get rid of this
message.
Offending key in /mnt/pss/.ssh/known_hosts:2
RSA1 host key for 171.69.16.46 has changed and you have requested strict
checking.
```

Example 26-10 Displays SSH Protocol Status

```
switch#
ssh is enabled
version 1 enabled
version 2 enabled
```

Displays Server Key Pair Details

```
rsa1 Keys generated:Sun Jan 13 07:16:26 1980
1024 35
fingerprint:
1024 67:76:02:bd:3e:8d:f5:ad:59:5a:1e:c4:5e:44:03:07
could not retrieve rsa key information
dsa Keys generated:Sun Jan 13 07:40:08 1980
ssh-dss
AAAAB3NzaC1kc3MAAABBAJTCRQOydNRel2v7uiO6Fix+OTn8eGdnnDVxw5eJs5OcOEXOyjaWcMMYsEgxc9ada1NElp
8Wy7GPMWGOQYj9CU0AAAAVAMCcWhNN18zFNOIPo7cU3t7d0iEbAAAAQBdQ8UAOi/Cti84qFb3kTqXlS9mEhdQUo0lH
cH5bw5PKfj2Y/dLR437zCBKXetPj4p7mhQ6Fq5os8RZtJEyOsNsAAABAA0oxZbPyWeR5NHATXiyXdPI7j9i8fgyn9F
NipMkOF2Mn75Mi/lqQ4NIq0gQNvQOx27uCeQlRts/QwI4q68/eaw=
fingerprint:
512 f7:cc:90:3d:f5:8a:a9:ca:48:76:9f:f8:6e:71:d4:ae
```

Recovering the Administrator Password

-
-

Using the CLI With Network-Admin Privilege

Step 1

Step 2

<new password>

Ctrl-]

```
Ctrl-]
```

config terminal

Step 5

< >

Step 6

```
switch(boot-config)#
switch(boot)#
```

Step 7

Step 8

```
switch login:
Password: <              >
```

Step 9

Step 10

Step 11

Default Settings

Parameters	Default