CHAPTER 27

RADIUS and TACACS+

Fabric Manager provides the capability to authenticate users with RADIUS or TACACS+.

This chapter includes the following sections:

Authentication, Authorization, and Accounting

The authentication, authorization, and accounting (AAA) mechanism verifies the identity of, grants access to, and tracks the actions of users managing a switch. All Cisco MDS 9000 Family switches use Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) protocols to provide solutions using remote AAA servers.

Based on the user ID and password combination provided, switches perform local authentication or authorization using the local database or remote authentication or authorization using AAA server(s). A preshared secret key provides security for communication between the switch and AAA servers. This secret key can be configured for all AAA server or for only a specific AAA server. This security mechanism provides a central management capability for AAA servers.

CLI Security Options

You can access the CLI using the console (serial connection), Telnet, or Secure Shell (SSH). For each management path (console or Telnet and SSH), you can configure one or more of the following security control options: local, remote (RADIUS or TACACS+), or none.

- Remote security control
  - Using Remote Authentication Dial-In User Services (RADIUS). See the "Configuring RADIUS" section on page 27-5.
  - Using Terminal Access Controller Access Control System plus (TACACS+). See the "Configuring TACACS+" section on page 27-8.
- Local security control. See the "Local AAA Services" section on page 27-12.

These security mechanisms can also be configured for the following scenarios:

- iSCSI authentication (see the "iSCSI User Authentication" section on page 20-17).
- Fibre Channel Security Protocol (FC-SP) authentication (see the "Fibre Channel Security Protocol" section on page 30-1)

SNMP Security Options

The SNMP agent supports security features for SNMPv1,SNMPv 2c, and SNMPv3. Normal SNMP security mechanisms apply to all applications that use SNMP (for example, Cisco MDS 9000 Fabric Manager).

Fabric Manager and Device Manager security options also apply to the CLI.

See the "SNMP Version 3" section on page 26-2.

Switch AAA Functionalities

Using Fabric Manager, you can configure authentication, authorization, and accounting (AAA) switch functionalities on any switch in the Cisco MDS 9000 Family.

Authentication

Authentication is the process of verifying the identity of the person managing the switch. This identity verification is based on the user ID and password combination provided by the person trying to manage the switch. Cisco MDS 9000 Family switches allow you to perform local authentication (using the local lookup database) or remote authentication (using one or more RADIUS or TACACS+ servers).

Note When Fabric Manager logs into a Cisco MDS SAN-OS switch successfully through Telnet or SSH and if that switch is configured for AAA server-based authentication, a temporary SNMP user entry is automatically created with an expiry time of one day. The SNMP v3 protocol data units (PDUs) with your Telnet/SSH login name as the SNMPv3 user are authenticated by the switch. Fabric Manager can temporarily use the Telnet/SSH login name as the SNMP v3 `auth` and `priv` passphrase. This temporary SNMP login is only allowed if you have one or more active MDS Shell sessions. If you do not have an active session at any given time, your login is deleted and you will not be allowed to perform SNMP v3 operations.

Note Fabric Manager does not support AAA passwords with trailing whitespace, for example "passwordA ".

Authorization

By default, two roles exist in all Cisco MDS switches:

- Network operator—Has permission to view the configuration only. The operator cannot make any configuration changes.
- Network administrator— Has permission to execute all commands and make configuration changes. The administrator can also create and customize up to 64 additional roles.

If you use a SAN Volume Controller (SVC) setup, two more roles exist in all Cisco MDS switches:

- SVC administrator— Has permission to view the entire configuration and make SVC-specific configuration changes within the `switch(svc)` prompt.
- SVC operator—Has permission to view the entire configuration. The operator cannot make any configuration changes.

Note Refer to the *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide* for more information on SVC.

These four default roles cannot be changed or deleted. You can create additional roles and configure the following options:

- Configure role-based authorization by assigning user roles locally or using remote AAA servers.
- Configure user profiles on a remote AAA server to contain role information. This role information is automatically downloaded and used when the user is authenticated through the remote AAA server.

Note If a user only belongs to one of the newly-created roles and that role is subsequently deleted, then the user immediately defaults to the network-operator role.

Accounting

The accounting feature tracks and maintains a log of every management session used to access the switch. This information can be used to generate reports for troubleshooting and auditing purposes. Accounting logs can be stored locally or sent to remote AAA servers.

Tip The Cisco MDS 9000 Family switch uses interim-update RADIUS accounting-request packets to communicate accounting log information to the RADIUS server. The RADIUS server must be appropriately configured to log the information communicated in these packets. Several servers typically have log update/watchdog packet flags in the AAA client configuration. Turn on this flag to ensure proper RADIUS accounting.

Note Configuration operations are automatically recorded in the accounting log if they are performed in configuration mode. Additionally, important system events (for example, configuration save and system switchover) are also recorded in the accounting log.

Remote AAA Services

Remote AAA services provided through RADIUS and TACACS+ protocols have the following advantages over AAA servers:

- It is easier to manage user password lists for each switch in the fabric.
- AAA servers are already deployed widely across enterprises and can be easily adopted.
- Easier to manage.
- Accounting log for all switches in the fabric can be centrally managed.
- Easier to manage user role mapping for each switch in the fabric.

Remote Authentication Guidelines

When you prefer using remote AAA servers, follow these guidelines:

- A minimum of one AAA server should be IP reachable.
- Be sure to configure a desired local AAA policy as this policy is used if all AAA servers are not reachable.
- AAA servers are easily reachable if an overlay Ethernet LAN is attached to the switch. This is the recommended method.
- SAN networks connected to the switch should have at least one gateway switch connected to the Ethernet LAN reaching the AAA servers.

Server Groups

You can specify remote AAA servers for authentication, authorization, and accounting using server groups. A server group is a set of remote AAA servers implementing the same AAA protocol. The purpose of a server group is to provide for fail-over servers in case a remote AAA server fails to respond. If the first remote server in the group fails to respond, the next remote server in the group is tried until one of the servers sends a response. If all the AAA servers in the server group fails to respond, then that server group option is considered a failure. If required, you can specify multiple server groups. If the Cisco MDS switch encounters errors from the servers in the first group, it tries the servers in the next server group.

AAA Service Configuration Options

AAA configuration in Cisco MDS 9000 Family switches is service based. You can have separate AAA configurations for the following services

- Telnet or SSH login (Cisco MDS Fabric Manager and Device Manager login).
- Console login.
- iSCSI authentication (see the "iSCSI User Authentication" section on page 20-17).
- FC-SP authentication (see "Fibre Channel Security Protocol" section on page 30-1).
- Accounting.

In general, server group, local, and none are the three options that can be specified for any service in an AAA configuration. Each option is tried in the order specified. If all the methods fail, local is tried.

Note Even if local is not specified as one of the options, it is tried when all other configured options fail.

When RADIUS times out, local login is always attempted. For this local login to be successfull, a local account for the user with the same password should exist and the RADIUS timeout and retries should take less than 40 seconds. The user is authenticated if the username and password exists in the local authentication configuration.

Configuring RADIUS

Cisco MDS 9000 Family switches can use the RADIUS protocol to communicate with remote AAA servers. You can configure multiple RADIUS servers and server groups and set timeout and retry counts.

This section defines the RADIUS operation, identifies its network environments, and describes its configuration possibilities.

RADIUS is a distributed client/server protocol that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco MDS 9000 Family switches and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

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 click, the other Information pane tabs that use CFS are activated.

Setting the RADIUS Server for Authentication and Accounting

You can add up to 64 RADIUS servers in Cisco MDS SAN-OS or up to five RADIUS servers in Cisco FabricWare. RADIUS keys are always stored in encrypted form in persistent storage. The running configuration also displays encrypted keys.

By default, a switch retries a RADIUS server only once. This number can be configured. The maximum is five retries per server.

To add a RADIUS server, follow these steps:

Step 1 Choose **Switches > Security > AAA** in Fabric Manager or choose **Security > AAA** in Device Manager.

Step 2 Choose the **Servers** tab. You see the RADIUS or TACACS+ servers configured.

Step 3 Click **Create Row** in Fabric Manager or **Create** in Device Manager. You see the Create Server dialog box.

Step 4 Select the **radius** radio button to add a RADIUS server.

Step 5 Set the IP address, authentication port and accounting port values.

Step 6 Select whether the shared key is plain or encrypted in the KeyType field and set the key in the Key field.

Step 7 Set the timeout and retry values for authentication attempts.

Step 8 Click **Create** to create this RADIUS server or click **Close** to exit the dialog box without creating the new server.

Setting the Global Preshared Key

You need to configure the RADIUS preshared key to authenticate the switch to the RADIUS server. The length of the key is restricted to 64 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all RADIUS server configurations on the switch.

You can override this global key assignment by explicitly using the **key** option when you create a new server.

To set the global preshared key, follow these steps:

Step 1 Choose **Switches > Security > AAA** in Fabric Manager or choose **Security > AAA** in Device Manager.

Step 2 Choose the **Defaults** tab. You see the RADIUS and TACACS+ default settings.

Step 3 Select whether the shared key is plain or encrypted in the KeyType field and set the key in the Key field.

Step 4 Set the timeout and retry values for authentication attempts.

Step 5 Click **Apply Changes** in Fabric Manager or **Apply** in Device Manager to save the global preshared key or click **Close** discard any unsaved changes.

Defining Vendor-Specific Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific attributes (VSAs) between the network access server and the RADIUS server. The IETF uses attribute 26. VSAs allow vendors to support their own extended attributes that are not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor ID is 9, and the supported option is vendor type 1, which is named `cisco-avpair`. The value is a string with the following format:

```
protocol : attribute sep value *
```

Where `protocol` is a Cisco attribute for a particular type of authorization, and `sep` is `=` for mandatory attributes, and `*` is for optional attributes.

When you use RADIUS servers to authenticate yourself to a Cisco MDS 9000 Family switch, the RADIUS protocol directs the RADIUS server to return user attributes, like authorization information, along with authentication results. This authorization information is specified through VSAs.

VSA Format

The following VSA protocol options are supported:

- `Shell` protocol—used in access-accept packets to provide user profile information.
- `Accounting` protocol—used in accounting-request packets. If a value contains any white spaces, it should be put within double quotation marks.

The following attributes are supported:

- `roles`–This attribute lists all the roles to which the user belongs. The value field is a string storing the list of group names delimited by white space. For example, if you belong to roles `vsan-admin` and `storage-admin`, the value field would be "`vsan-admin storage-admin`." This subattribute is sent in the VSA portion of the Access-Accept frames from the RADIUS server, and it can only be used with the shell protocol value. These are two examples using the roles attribute:

  ```
  shell:roles="network-admin vsan-admin"
  shell:roles*"network-admin vsan-admin"
  ```

  When an VSA is specified as `shell:roles*"network-admin vsan-admin"`, this VSA is flagged as an optional attribute, and other Cisco devices ignore this attribute.

- `accountinginfo`—This attribute stores additional accounting information besides the attributes covered by a standard RADIUS accounting protocol. This attribute is only sent in the VSA portion of the Account-Request frames from the RADIUS client on the switch, and it can only be used with the accounting protocol-related PDUs.

Specifying SNMPv3 on AAA Servers

The vendor/custom attribute `cisco-av-pair` can be used to specify user's role mapping using the format:

```
shell:roles="roleA roleB …"
```

As of Cisco MDS SAN-OS Release 2.0, the VSA format is enhanced to optionally specify your SNMPv3 authentication and privacy protocol attributes as follows:

```
shell:roles="roleA roleB..." snmpv3:auth=SHA priv=AES-128
```

The SNMPv3 authentication protocol options are SHA and MD5. The privacy protocol options are AES-128 and DES. If these options are not specified in the `cisco-av-pair` attribute on the ACS server, MD5 and DES are used by default.

Note Only administrators can view the RADIUS preshared key.

Configuring TACACS+

A Cisco MDS switch uses the Terminal Access Controller Access Control System Plus (TACACS+) protocol to communicate with remote AAA servers. You can configure multiple TACACS+ servers and set timeout values.

About TACACS+

TACACS+ is a client/server protocol that uses TCP (TCP port 49) for transport requirements. All switches in the Cisco MDS 9000 Family provide centralized authentication using the TACACS+ protocol. The addition of TACACS+ support in Cisco MDS SAN-OS Release1.3(x) enables the following advantages over RADIUS authentication:

- Provides independent, modular AAA facilities. Authorization can be done without authentication.
- TCP transport protocol to send data between the AAA client and server, using reliable transfers with a connection-oriented protocol.
- Encrypts the entire protocol payload between the switch and the AAA server to ensure higher data confidentiality. The RADIUS protocol only encrypts passwords.

Enabling TACACS+

By default, the TACACS+ feature is disabled in all switches in the Cisco MDS 9000 Family. You must explicitly enable the TACACS+ feature to access the configuration and verification commands for fabric authentication. When you disable this feature, all related configurations are automatically discarded.

Setting the TACACS+ Server

If a secret key is not configured for a configured server, a warning message is issued if a global key is not configured. If a server key is not configured, the global key (if configured) is used for that server (see the "Setting the Global Preshared Key" section on page 27-7).

To add a TACACS+ server, follow these steps:

Step 1 Choose **Switches > Security > AAA** in Fabric Manager or choose **Security > AAA** in Device Manager.

Step 2 Choose the **Servers** tab. You see the RADIUS or TACACS+ servers configured.

Step 3 Click **Create Row** in Fabric Manager or **Create** in Device Manager. You see the Create Server dialog box.

Step 4 Select the **tacacs+** radio button to add a RADIUS server.

Step 5 Set the IP address, authentication port and accounting port values.

Step 6 Select whether the shared key is plain or encrypted in the KeyType field and set the key in the Key field.

Step 7 Set the timeout and retry values for authentication attempts.

Step 8 Click **Create** to create this TACACS+ server or click **Close** to exit the dialog box without creating the new server.

Defining Custom Attributes for Roles

Cisco MDS 9000 Family switches use the TACACS+ custom attribute for service shells to configure roles to which a user belongs. TACACS+ attributes are specified in `name=value` format. The attribute name for this custom attribute is `cisco-av-pair`. The following example illustrates how to specify roles using this attribute:

```
cisco-av-pair=shell:roles="network-admin vsan-admin"
```

You can also configure optional custom attributes to avoid conflicts with non-MDS Cisco switches using the same AAA servers.

```
cisco-av-pair*shell:roles="network-admin vsan-admin"
```

Additional custom attribute shell:roles are also supported:

```
shell:roles="network-admin vsan-admin"
```

or

```
shell:roles*"network-admin vsan-admin"
```

Note TACACS+ custom attributes can be defined on an Access Control Server (ACS) for various services (for example, shell). Cisco MDS 9000 Family switches require the TACACS+ custom attribute for the service shell to be used for defining roles.

Supported TACACS+ Servers

The Cisco MDS SAN-OS software currently supports the following parameters for the listed TACACS+ servers:

- TACACS:

  ```
  cisco-av-pair=shell:roles="network-admin"
  ```

- Cisco ACS TACACS

  ```
  shell:roles="network-admin"
  shell:roles*"network-admin"
  cisco-av-pair*shell:roles="network-admin"
  cisco-av-pair*shell:roles*"network-admin"
  cisco-av-pair=shell:roles*"network-admin"
  ```

- Open TACACS

  ```
  cisco-av-pair*shell:roles="network-admin"
  cisco-av-pair=shell:roles*"network-admin"
  ```

Configuring Server Groups

You can specify one or more remote AAA servers to authenticate users using server groups. All members of a group must belong to the same protocol: either RADIUS or TACACS+. The servers are tried in the same order in which you configure them.

You can configure these server groups at any time but they only take effect when you apply them to an AAA service.

To configure a RADIUS or TACACS+ server group, follow these steps:

Step 1 Choose **Switches > Security > AAA** in Fabric Manager or choose **Security > AAA** in Device Manager.

Step 2 Choose the **Server Group** tab. You see the RADIUS or TACACS+ servers configured.

Step 3 Click **Create Row** in Fabric Manager or **Create** in Device Manager. You see the Create Server dialog box.

Step 4 Select the **radius** radio button to add a RADIUS server group or select **tacacs+** to add a TACACS+ server group.

Step 5 Check the servers from the ServerIdList for the servers you want to be part of this server group.

Step 6 Click **Create** to create this RADIUS server or click **Close** to exit the dialog box without creating the new server.

Distributing AAA server Configuration

Configuration for RADIUS and TACACS+ AAA on a switch running Cisco MDS SAN-OS can be distributed using the Cisco Fabric Services (CFS). The distribution is disabled by default.

After enabling the distribution, the first server or global configuration starts an implicit session. All server configuration commands entered there after are stored in a temporary database and applied to all switches in the fabric (including the originating one) when you explicitly commit the database. The various server and global parameters are distributed, except the server and global keys. These keys are unique secrets to a switch and should not be shared with other switches.

Note Server group configurations are not distributed.

Enabling the distribution

Only switches where distribution is enabled can participate in the distribution activity.

To enable a RADIUS or TACACS+ CFS distribution using Fabric Manager, follow these steps:

Step 1 Choose **Switches > Security > AAA > RADIUS** or choose **Switches > Security > AAA > TACACS+**. You see the RADIUS or TACACS+ configuration in the Information pane.

Step 2 Choose the **CFS** tab. You see the RADIUS or TACACS+ CFS configuration.

Step 3 Choose **enable** from the Enable > Admin drop-down list for all switches that you want to enable CFS on for RADIUS or TACACS+.

Step 4 Click **Apply Changes** to distribute these changes through the fabric.

Starting a Distribution Session on a Switch

A distribution session starts the moment you begin a AAA configuration. For example, the following tasks start an implicit session:

- Specifying the global timeout for RADIUS servers.
- Specifying the global timeout for TACACS+ servers.

Note After you issue the first configuration command related to AAA servers, all server and global configuration made (including the configuration that caused the distribution session start) are stored in a temporary buffer—not in the running configuration.

Committing the Distribution

The RADIUS or TACACS global and/or server configuration stored in the temporary buffer can be applied to the running configuration across all switches in the fabric (including the originating switch).

To distribute a RADIUS or TACACS+ configuration using Fabric Manager, follow these steps:

Step 1 Choose **Switches > Security > AAA > RADIUS** or choose **Switches > Security > AAA > TACACS+**. You see the RADIUS or TACACS+ configuration in the Information pane.

Step 2 Choose the **CFS** tab. You see the RADIUS or TACACS+ CFS configuration

Step 3 Choose **commit** in the Config Changes > Action drop-down list for all switches that you want to enable CFS on for RADIUS or TACACS+.

Step 4 Click **Apply Changes** to distribute these changes through the fabric.

Discarding the Distribution Session

Discarding the distribution of a session-in-progress causes the configuration in the temporary buffer to be dropped. The distribution is no applied.

To discard a RADIUS or TACACS+ distribution using Fabric Manager, follow these steps:

Step 1 Choose **Switches > Security > AAA > RADIUS** or choose **Switches > Security > AAA > TACACS+**. You see the RADIUS or TACACS+ configuration in the Information pane.

Step 2 Choose the **CFS** tab. You see the RADIUS or TACACS+ CFS configuration

Step 3 Choose **clear** from the Config Changes > Action drop-down list for all switches that you want to enable CFS on for RADIUS or TACACS+.

Step 4 Click **Apply Changes** to cancel the distribution.

Local AAA Services

The system maintains the user name and password locally and stores the password information in encrypted form. You are authenticated based on the locally stored user information.

Disabling AAA Authentication

You can turn off password verification. If you configure this option, users will be able to log in without giving a valid password. But the user should at least exist locally on the Cisco MDS 9000 Family switch.

Use this option cautiously. If configured, any user can to access the switch at any time.