CHAPTER 2

Configuring AAA

This chapter describes how to configure authentication, authorization, and accounting (AAA) on Cisco NX-OS devices.

This chapter includes the following sections:

Information About AAA

This section includes the following topics:

AAA Security Services

The AAA feature allows you to verify the identity of, grant access to, and track the actions of users managing an Cisco NX-OS device. Cisco NX-OS devices support Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control device Plus (TACACS+) protocols.

Based on the user ID and password combination that you provide, Cisco NX-OS devices perform local authentication or authorization using the local database or remote authentication or authorization using one or more AAA servers. A preshared secret key provides security for communication between the Cisco NX-OS device and AAA servers. You can configure a common secret key for all AAA servers or for only a specific AAA server.

AAA security provides the following services:

- Authentication—Identifies users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol that you select, encryption.

  Authentication is the process of verifying the identity of the person or device accessing the Cisco NX-OS device, which is based on the user ID and password combination provided by the entity trying to access the Cisco NX-OS device. Cisco NX-OS devices allow you to perform local authentication (using the local lookup database) or remote authentication (using one or more RADIUS or TACACS+ servers).

- Authorization—Provides access control.

  AAA authorization is the process of assembling a set of attributes that describe what the user is authorized to perform. Authorization in the Cisco NX-OS software is provided by attributes that are downloaded from AAA servers. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user.

- Accounting—Provides the method for collecting information, logging the information locally, and sending the information to the AAA server for billing, auditing, and reporting.

  The accounting feature tracks and maintains a log of every management session used to access the Cisco NX-OS device. You can use this information to generate reports for troubleshooting and auditing purposes. You can store accounting logs locally or send them to remote AAA servers.

Note The Cisco NX-OS software supports authentication, authorization, and accounting independently. For example, you can configure authentication and authorization without configuring accounting.

Benefits of Using AAA

AAA provides the following benefits:

- Increased flexibility and control of access configuration
- Scalability
- Standardized authentication methods, such as RADIUS and TACACS+
- Multiple backup devices

Remote AAA Services

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

- It is easier to manage user password lists for each Cisco NX-OS device in the fabric.
- AAA servers are already deployed widely across enterprises and can be easily used for AAA services.

- You can centrally manage the accounting log for all Cisco NX-OS devices in the fabric.
- It is easier to manage user attributes for each Cisco NX-OS device in the fabric than using the local databases on the Cisco NX-OS devices.

AAA 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 that implement 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 fail to respond, then that server group option is considered a failure. If required, you can specify multiple server groups. If the Cisco NX-OS device 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 NX-OS devices is service based, which means that you can have separate AAA configurations for the following services:

- User Telnet or Secure Shell (SSH) login authentication
- Console login authentication
- 802.1X authentication (see Chapter 6, “Configuring 802.1X”)
- User management session accounting
- 802.1X accounting (see Chapter 6, “Configuring 802.1X”)

You can specify the following authentication methods for the AAA services:

- RADIUS server groups—Uses the global pool of RADIUS servers for authentication.
- Specified server groups—Uses specified RADIUS or TACACS+ server groups for authentication.
- Local—Uses the local username or password database for authentication.
- None—Uses only the username.

Note If the method is all RADIUS servers, rather than a specific server group, the Cisco NX-OS device chooses the RADIUS server from the global pool of configured RADIUS servers, in the order of configuration. Servers from this global pool are the servers that can be selectively configured in a RADIUS server group on the Cisco NX-OS device.

Table 2-1 shows the AAA authentication methods that you can configure for the AAA services.

Table 2-1 AAA Authentication Methods for AAA Services

AAA Service	AAA Methods
Console login authentication	Server groups, local, and none
User login authentication	Server groups, local, and none
802.1X authentication	Server groups only

Table 2-1 AAA Authentication Methods for AAA Services (continued)

AAA Service	AAA Methods
User management session accounting	Server groups and local
802.1X accounting	Server groups and local

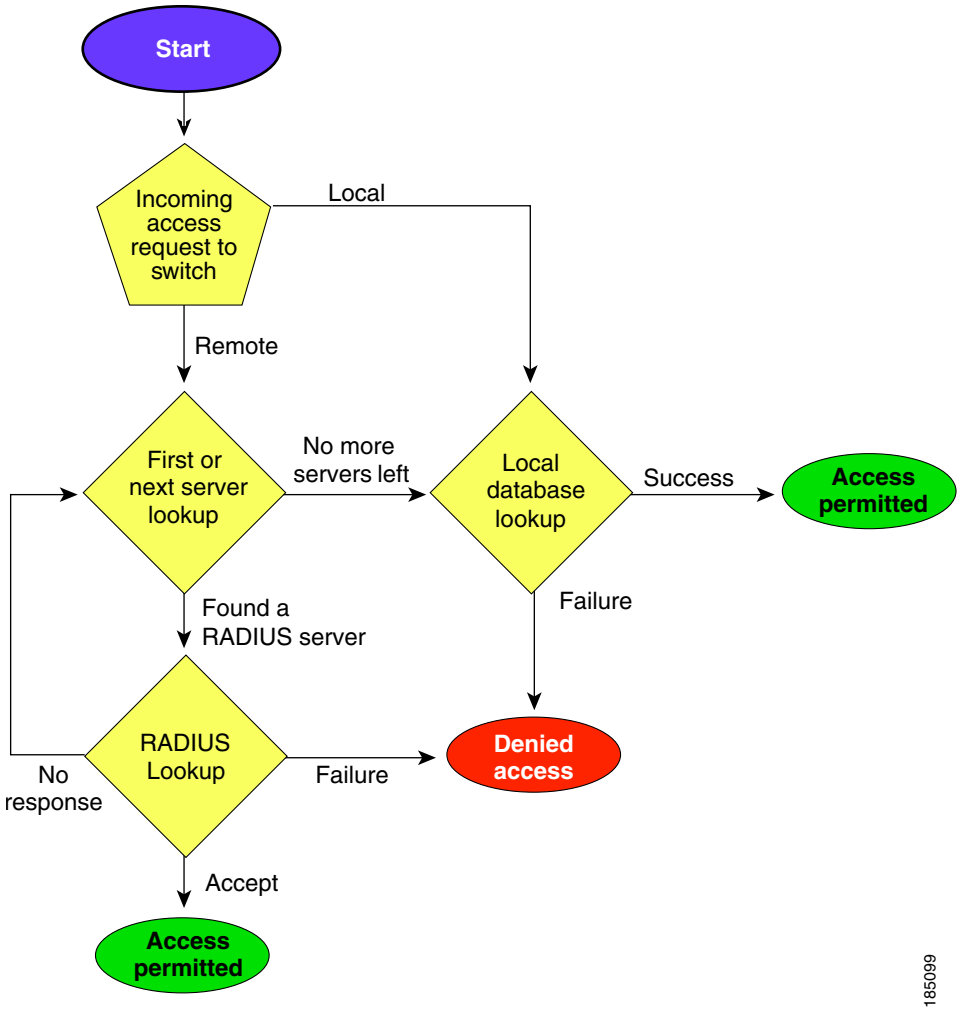
Note For console login authentication and user login authentication, and user management session accounting, the Cisco NX-OS device tries each option in the order specified. The local option is the default method when other configured options fail.

Authentication and Authorization Process for User Login

Figure 2-1 shows a flow chart of the authentication and authorization process for user login. The following list explain the process:

1. When you log in to the required Cisco NX-OS device, you can use the Telnet, SSH, or console login options.
2. When you have configured the AAA server groups using the server group authentication method, the Cisco NX-OS device sends an authentication request to the first AAA server in the group as follows:
   - If the AAA server fails to respond, then the next AAA server is tried and so on until the remote server responds to the authentication request.
   - If all AAA servers in the server group fail to respond, then the servers in the next server group are tried.
   - If all configured methods fail, then the local database is used for authentication.
3. If the Cisco NX-OS device successfully authenticates you through a remote AAA server, then the following possibilities apply:
   - If the AAA server protocol is RADIUS, then user roles specified in the cisco-av-pair attribute are downloaded with an authentication response.
   - If the AAA server protocol is TACACS+, then another request is sent to the same server to get the user roles specified as custom attributes for the shell.
   - If the user roles are not successfully retrieved from the remote AAA server, then the user is assigned with the vdc-operator role.
4. If your username and password are successfully authenticated locally, the Cisco NX-OS device logs you in and assigns you the roles configured in the local database.

Figure 2-1 Authorization and Authentication Flow for User Login



Note "No more server groups left" means that there is no response from any server in all server groups. "No more servers left" means that there is no response from any server within this server group.

Virtualization Support

All AAA configuration and operations are local to the VDC, except the default console methods and the AAA accounting log. The configuration and operation of the AAA authentication methods for the console login apply only to the default VDC. The AAA accounting log is only in the default VDC. You can display the contents from any VDC but you must clear it in the default VDC.

For more information on VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.1*.

Licensing Requirements for AAA

The following table shows the licensing requirements for this feature:

Product	License Requirement
DCNM	AAA requires no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For a complete explanation of the DCNM licensing scheme, see the *Cisco DCNM Fundamentals Configuration Guide, Release 4.1*.
Cisco NX-OS	AAA requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the *Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.1*.

Prerequisites for AAA

Remote AAA servers have the following prerequisites:

- Ensure that at least one RADIUS or TACACS+ server is IP reachable (see the "Adding a RADIUS Server Host" section on page 3-8 and the "Adding a TACACS+ Server Host" section on page 4-9).
- Ensure that the Cisco NX-OS device is configured as a client of the AAA servers.
- Ensure that the preshared secret key is configured on the Cisco NX-OS device and the remote AAA servers.
- Ensure that the logging level for AAA in the Cisco NX-OS software is set to 5 using the command-line interface (CLI).

```
switch# configure terminal
switch(config)# logging level aaa 5
```

AAA Guidelines and Limitations

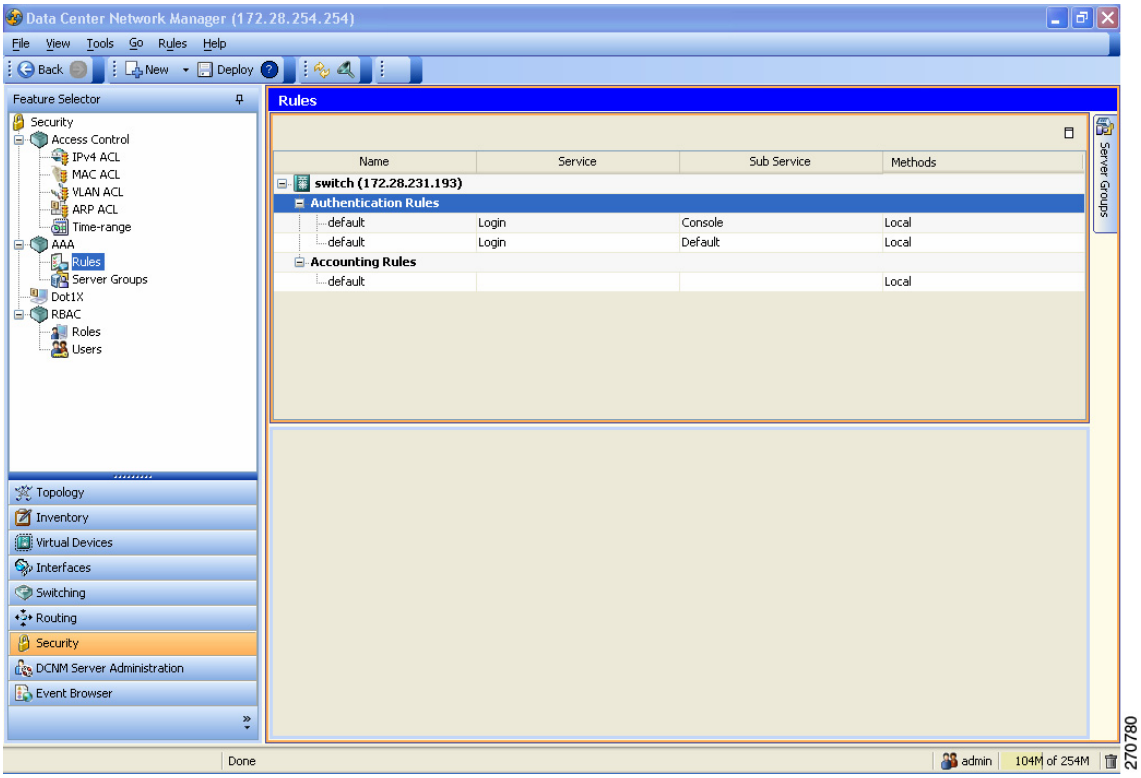
RADIUS has the following guidelines and limitations:

- The Cisco NX-OS software does not support all numeric usernames, whether created with TACACS+ or RADIUS, or created locally, and does not create local users with all numeric names. If an all numeric username exists on an AAA server and is entered during login, the Cisco NX-OS device does log in the user.
- If you have a user account configured on the local Cisco NX-OS device that has the same name as a remote user account on an AAA server, the Cisco NX-OS software applies the user roles for the local user account to the remote user, not the user roles configured on the AAA server.

Configuring AAA

Figure 2-2 shows the AAA Rules pane.

Figure 2-2 AAA Rules Pane



This section includes the following topics:

- Changing an AAA Authentication Rule Method, page 2-8
- Adding an AAA Authentication Rule Method, page 2-8
- Rearranging an AAA Authentication Rule Method, page 2-9
- Deleting an AAA Authentication Rule Method, page 2-10
- Changing an AAA Accounting Rule Method, page 2-10
- Adding an AAA Accounting Rule Method, page 2-11
- Rearranging an AAA Accounting Rule Method, page 2-12
- Deleting an AAA Accounting Rule Method, page 2-13
- Using AAA Server VSAs with Cisco NX-OS Devices, page 2-13

Note To configure authentication methods for 802.1X, see the "Configuring an AAA Authentication Method for 802.1X" section on page 6-11.

Changing an AAA Authentication Rule Method

You can change an AAA authentication rule method.

The methods include the following:

- Group—RADIUS server groups
- Local—Local database on the device
- None—Username only

The default method is local.

The rules are applied in the sequence order. If all methods fail, the device uses the default local method.

Note The configuration and operation of the AAA for the console login apply to the default VDC.

BEFORE YOU BEGIN

Configure RADIUS or TACACS+ server groups, as needed.

DETAILED STEPS

To change an authentication rule method, follow these steps:

Step 1 From the Feature Selector pane, choose **Security > AAA > Rules**.

Step 2 Double-click **Authentication Rules** to display the list of accounting rules.

Step 3 Click the rule to which to add a method.

Step 4 Click the rule to change.

The Authentication Rules tab appears in the Details pane.

Step 5 From the Authentication Rules tab, click the method to change.

Step 6 Double-click the method cell under Type and choose the method type from the drop-down list.

Step 7 If you chose the Group method type, double-click the method cell under Server Group Name and choose a server group name from the drop-down list. Click **OK**.

Step 8 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Adding an AAA Authentication Rule Method

You can change an AAA authentication rule method.

The methods include the following:

- Group—RADIUS server groups
- Local—Local database on the Cisco NX-OS device
- None—Username only

The default method is local.

The rules are applied in the sequence order. If all methods fail, the Cisco NX-OS device uses the default local method.

Note The configuration and operation of the AAA for the console login only apply to the default VDC.

BEFORE YOU BEGIN

Configure RADIUS or TACACS+ server groups, as needed.

DETAILED STEPS

To add an authentication rule method, follow these steps:

Step 1 From the Feature Selector pane, choose **Security > AAA > Rules**.

Step 2 From the Summary pane, double-click the device.

Step 3 Double-click **Authentication Rules** to display the list of accounting rules.

Step 4 Click the rule to which to add a method.

The Authentication Rules tab appears in the Details pane.

Step 5 Right-click on a method and click **Add Method** from the pop-up menu.

A new rule displays at the end of the list with a sequence number and blank fields.

Step 6 Double-click the cell under Type in the new method and choose the method type from the drop-down list.

Note If you chose None for the method type, it must always be the last method in the list.

Step 7 If you chose the Group method type, double-click the method cell under Server Group Name and choose a server group name from the drop-down list. Click **OK**.

Step 8 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Rearranging an AAA Authentication Rule Method

You can rearrange the sequence of the methods for an AAA authentication rule.

Note The None method must always be the last method in the list.

DETAILED STEPS

To rearrange an AAA authentication rule method, follow these steps:

Step 1 From the Feature Selector pane, choose **Security > AAA > Rules**.

Step 2 From the Summary pane, double-click the device.

Step 3 Double-click **Authentication Rules** to display the list of accounting rules.

Step 4 Click the rule which has the method that you want to rearrange.

The Authentication Rules tab appears in the Details pane with the list of methods.

Step 5 Click the methodthat you want to rearrange.

Step 6 Right-click and click **Move Up** or **Move Up** from the pop-up menu.

Step 7 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Deleting an AAA Authentication Rule Method

You can delete an AAA authentication rule method.

Note An AAA authentication rule must have at least one method. You can only delete a method when the rule had more than one method.

DETAILED STEPS

To delete an authentication rule method, follow these steps:

Step 1 From the Feature Selector pane, choose **Security > AAA > Rules**.

Step 2 From the Summary pane, double-click the device.

Step 3 Double-click **Authentication Rules** to display the list of accounting rules.

Step 4 Click the rule from which to delete a method.

The Authentication Rules tab appears in the Details pane.

Step 5 Click the method that you want to delete.

Note You can only delete a method with sequence number 2 or greater. To delete the rule with sequence number 1, you must first rearrange the methods (see the "Rearranging an AAA Authentication Rule Method" section on page 2-9).

Step 6 Right-click and click **Delete Method** from the pop-up menu.

The rule disappears from the list and the sequence numbers are updated.

Step 7 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Changing an AAA Accounting Rule Method

You can change an AAA accounting rule method. The device supports TACACS+ and RADIUS methods for accounting, which report user activity to TACACS+ or RADIUS security servers in the form of accounting records.

You can specify the following accounting methods:

- Server group—Uses a specified RADIUS or TACACS+ server group for accounting.

- Local—Uses the local username or password database for accounting.

The default method is local.

Note If you have configured server groups and the server groups do not respond, by default, the local database is used for authentication.

BEFORE YOU BEGIN

Configure RADIUS or TACACS+ server groups, as needed.

DETAILED STEPS

To change an accounting rule method, follow these steps:

Step 1 From the Feature Selector pane, choose **Security > AAA > Rules**.

Step 2 From the Summary pane, double-click the device.

Step 3 Double-click **Accounting Rules** to display the list of accounting rules.

Step 4 Click the rule to change.

The Accounting Rules tab appears in the Details pane.

Step 5 From the Accounting Rules tab, click the method to change.

Step 6 Double-click the method cell under Type and choose the method type from the drop-down list.

Step 7 If you chose the Group method type, double-click the method cell under Server Group Name and choose a server group name from the drop-down list. Click **OK**.

Step 8 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Adding an AAA Accounting Rule Method

You can add an AAA accounting rule method.

The methods include the following:

- Group—RADIUS server groups
- Local—Local database on the Cisco NX-OS device

The default method is local.

The rules are applied in the sequence order. If all methods fail, the device uses the default local method.

BEFORE YOU BEGIN

Configure RADIUS or TACACS+ server groups, as needed.

DETAILED STEPS

To add accounting rule methods, follow these steps:

Step 1 From the Feature Selector pane, choose **Security > AAA > Rules**.

Step 2 From the Summary pane, double-click the device.

Step 3 Double-click **Accounting Rules** to display the list of accounting rules.

Step 4 Click the rule to which to add a method.

The Accounting Rules tab appears in the Details pane.

Step 5 Right-click a method to add the new method after and click **Add Method** from the pop-up menu.

A new method displays at the end of the list with a sequence number and blank fields.

Step 6 If the new method is after a method with type Local, right-click the new method and click **Move Up** from the pop-up menu.

Note You cannot add methods after a method with type Local.

Step 7 Double-click the cell under Type in the new method and click **Group** from the drop-down list.

Step 8 Double-click the new method cell under Server Group Name.

Step 9 Enter the server group name or choose a server group name from the drop-down list and click **OK**.

Step 10 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Rearranging an AAA Accounting Rule Method

You can rearrange the sequence of the methods for an AAA accounting rule.

DETAILED STEPS

To rearrange an AAA accounting rule method, follow these steps:

Step 1 From the Feature Selector pane, choose **Security > AAA > Rules**.

Step 2 From the Summary pane, double-click the device.

Step 3 Double-click **Accounting Rules** to display the list of accounting rules.

Step 4 Click the rule which has the method that you want to rearrange.

The Accounting Rules tab appears in the Details pane with the list of methods.

Step 5 Click the method that you want to rearrange.

Step 6 Right-click and click **Move Up** or **Move Up** from the pop-up menu.

Step 7 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Deleting an AAA Accounting Rule Method

You can delete an AAA accounting rule method.

Note An AAA accounting rule must have at least one method. You can only a delete method when the rule has more than one method.

DETAILED STEPS

To delete an accounting rule method, follow these steps:

Step 1 From the Feature Selector pane, choose **Security > AAA > Rules**.

Step 2 From the Summary pane, double-click the device.

Step 3 Double-click **Accounting Rules** to display the list of accounting rules.

Step 4 Click the rule from which to delete a method.

The Accounting Rules tab appears in the Details pane.

Step 5 Click the method that you want to delete.

Note You can only delete a method with sequence number 2 or greater. To delete the rule with sequence number 1, you must first rearrange the methods (see the "Rearranging an AAA Accounting Rule Method" section on page 2-12).

Step 6 Right-click and click **Delete Method** from the pop-up menu.

The rule disappears from the list and the sequence numbers are updated.

Step 7 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Using AAA Server VSAs with Cisco NX-OS Devices

You can use vendor-specific attributes (VSAs) to specify Cisco NX-OS user roles and SNMPv3 parameters on AAA servers.

This section includes the following topics:

About VSAs

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating 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-av-pair. The value is a string with the following format:

```
protocol : attribute seperator value *
```

The protocol is a Cisco attribute for a particular type of authorization, the separator is = (equal sign) for mandatory attributes, and * (asterisk) indicates optional attributes.

When you use RADIUS servers for authentication on a Cisco NX-OS device, the RADIUS protocol directs the RADIUS server to return user attributes, such as authorization information, along with authentication results. This authorization information is specified through VSAs.

VSA Format

The following VSA protocol options are supported by the Cisco NX-OS software:

- 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, put it within double quotation marks.

The following attributes are supported by the Cisco NX-OS software:

- roles—Lists all the roles assigned to the user. The value field is a string that stores the list of group names delimited by white space. For example, if you belong to roles network-operator and vdc-admin, the value field would be “network-operator vdc-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 examples use the roles attribute:

  ```
  shell:roles=“network-operator vdc-admin”
  shell:roles*“network-operator vdc-admin”
  ```

  The following examples show the roles attribute as supported by FreeRADIUS:

  ```
  Cisco-AVPair = ”shell:roles=\“network-operator vdc-admin\”“
  Cisco-AVPair = “shell:roles*\“network-operator vdc-admin\”“
  ```

Note When you specify a VSA as shell:roles*"network-operator vdc-admin" or "shell:roles*\"network-operator vdc-admin\"", this VSA is flagged as an optional attribute and other Cisco devices ignore this attribute.

- accountinginfo—Stores accounting information in addition to the attributes covered by a standard RADIUS accounting protocol. This attribute is sent only 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 Cisco NX-OS User Roles and SMNPv3 Parameters on AAA Servers

You can use the VSA cisco-av-pair on AAA servers to specify user role mapping for the Cisco NX-OS device using this format:

```
shell:roles="roleA roleB …"
```

If you do not specify the role option in the cisco-av-pair attribute, the default user role is network-operator.

You can also 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 you do not specify these options in the cisco-av-pair attribute, MD5 and DES are the default authentication protocols.

For more information on user roles, see Chapter 5, "Configuring RBAC."

Field Descriptions for AAA

This section includes the following topics:

Security: AAA: Rules: Summary Pane

Table 2-3 Security: AAA: Rules: Summary Pane

Field	Description
Name	Rule name. The name for all rules is default.
Service	Service type.
Sub Service	Subservice type.
Methods	Methods for the rule.

Security: AAA: Rules: device: Authentication Rules: Rule: Authentication Rules Tab

Table 2-4 Security: AAA: Rules: Device: Authentication Rules: Rule: Authentication Rules Tab

Field	Description
Rule name	Rule name. The name for all rules is default.
Service Type	Service type.
Sub Service Type	Subservice type.
Methods	
Sequence	Sequence number that determines the order in which the methods are executed.
Type	Method type.
Server Group Name	Server group name

Security: AAA: Rules: device: Accounting Rules: Rule: Accounting Rules Tab

This tab allows you to configure an AAA accounting rule.

Table 2-5 Security: AAA: Rules: Device: Accounting Rules: Rule: Accounting Rules Tab

Field	Description
Rule name	Name of rule. The name for all rules is default.
Service Type	Type of service.
Notify	Unused.
BroadCast	Unused.
Methods	
Sequence	Sequence number that determines the order in which the methods are executed.
Type	Type of method.
Server Group Name	Name of the server group.

Additional References

For additional information related to implementing AAA, see the following sections:

- Related Documents, page 2-16
- Standards, page 2-16
- MIBs, page 2-17

Related Documents

Related Topic	Document Title
Cisco NX-OS Licensing	*Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.1*
DCNM Licensing	*Cisco DCNM Fundamentals Configuration Guide, Release 4.1*
RADIUS security protocol	Chapter 3, “Configuring RADIUS”
TACACS+ Security protocol	Chapter 4, “Configuring TACACS+”

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
• CISCO-AAA-SERVER-MIB • CISCO-AAA-SERVER-EXT-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for AAA

Table 2-6 lists the release history for this feature.

Table 2-6 Feature History for AAA

Feature Name	Releases	Feature Information
AAA	4.0(1)	This feature was introduced.