CHAPTER 2

Configuring AAA

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

This chapter includes the following sections:

Information About AAA

AAA Security Services

The AAA feature allows you to verify the identity of, grant access to, and track the actions of users managing an 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 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 NX-OS device, which is based on the user ID and password combination provided by the entity trying to access the 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 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 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 NX-OS software supports authentication, authorization, and accounting independently. For example, you can configure authentication and authorization without configuring accounting.

Benefits of Using AAA

-
-
-
- Multiple backup devices

Remote AAA Services

-
-
-
-

AAA Server Groups

AAA Service Configuration Options

- User Telnet or Secure Shell (SSH) login authentication
- Console login authentication
- Cisco TrustSec authentication (see Chapter 9, “Configuring Cisco TrustSec”)

  802.1X authentication (see Chapter 7, “Configuring 802.1X”)

  Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) authentication for Network Admission Control (NAC) (see Chapter 8, “Configuring NAC”)

  User management session accounting

  802.1X accounting (see Chapter 7, “Configuring 802.1X”)

Table 2-1 provides the related CLI command for each AAA service configuration option.

Table 2-1 AAA Service Configuration Commands

AAA Service Configuration Option	Related Command
	aaa authentication login default
	aaa authentication login console
	aaa authentication cts default
	aaa authentication dot1x default
	aaa authentication eou default

AAA Service Configuration Commands (continued)

User session accounting	
802.1X accounting	

Table 2-2 AAA Authentication Methods for AAA Services

	AAA Methods
Cisco TrustSec authentication	Server groups only
802.1X authentication	Server groups only
EAPoUDP authentication	Server groups only
User management session accounting	Server groups and local
802.1X accounting	Server groups and local

Authentication and Authorization Process for User Login

1. When you log in to the required Cisco NX-OS device, you can use the Telnet, SSH, or console login options.

2.

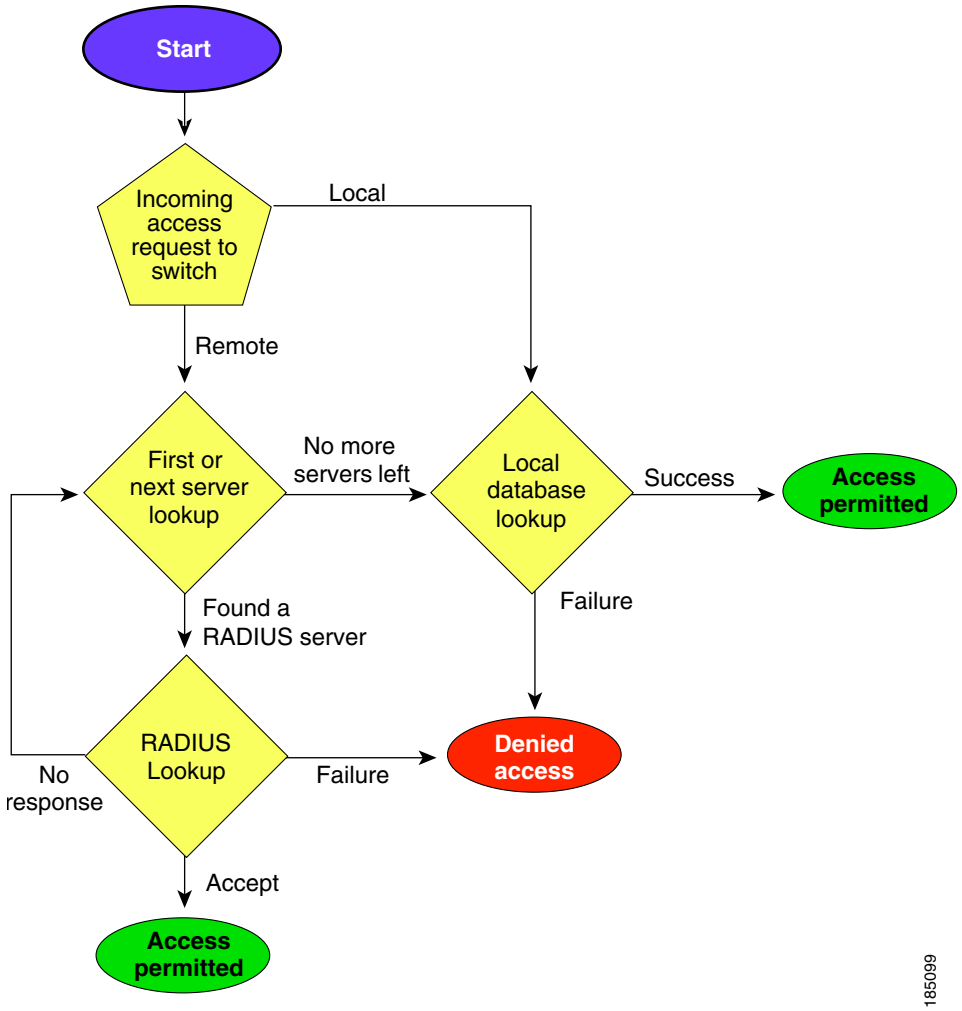
-
-
-

3.

-
-
-

4.

Figure 2-1 Authorization and Authentication Flow for User Login



Virtualization Support

Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.0

Licensing Requirements for AAA

Product	License Requirement
	Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.0

Prerequisites for AAA

-
-
-
-

AAA Guidelines and Limitations

-
-

Configuring AAA

-
-
-
-
-

, page 2-15

Using AAA Server VSAs with Cisco NX-OS Devices, page 2-16

If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Follow these steps to configure AAA authentication and accounting:

Step 1

Step 2

Step 3

Step 4

Note

Configuring Console Login Authentication Methods

-
-
-
-

Note

Note **group radius** **group** *server-name* **aaa authentication** **radius server-host** **aaa group server radius**

BEFORE YOU BEGIN

SUMMARY STEPS

1.
2. { *group-list* [ ] | | }

show aaa authentication

5. **copy running-config start-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t switch(config)#	
	aaa authentication login console {**group** *group-list* [ ] | | }	
	switch(config)# aaa authentication login console group radius	
	switch(config)# exit switch#	

Step 4	**show aaa authentication** **Example:**	
	copy running-config startup-config **Example:** switch# copy running-config startup-config	

Configuring Default Login Authentication Methods

-
-
-
-

BEFORE YOU BEGIN

SUMMARY STEPS

1.
2. }
3. **exit**
4. **show aaa authentication**
5. **copy running-config start-config**

	Command	Purpose
Step 1		
Step 2	`aaa authentication login default group none local none` **Example:**	• •
Step 3	`exit` **Example:**	
Step 4	`show aaa authentication` **Example:**	
Step 5	`copy running-config startup-config` **Example:**	

Enabling the Default User Role for AAA Authentication

BEFORE YOU BEGIN

SUMMARY STEPS

1.
2.
3.
4.
5.

DETAILED STEPS

`switch# config t` `switch(config)#`	
`switch(config)# aaa user default-role`	
`switch(config)# exit` `switch#`	
`switch# show aaa user default-role`	
`switch# copy running-config startup-config`	

Enabling Login Authentication Failure Messages

servers do not respond. In such cases, the following message is displayed on the user's terminal—if you have enabled displaying login failure messages:

```
Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.
```

aaa authentication login error-enable

exit

show aaa authentication

copy running-config start-config

	Command	Purpose
Step 1		
Step 2	`aaa authentication login error-enable` **Example:**	
	`exit` **Example:**	
	`show aaa authentication` **Example:**	
	`copy running-config startup-config` **Example:**	

Enabling MSCHAP Authentication

Table 2-3 MSCHAP RADIUS VSAs

Vendor-ID Number	Vendor-Type Number	VSA	Description

aaa authentication login mschap enable

exit

show aaa authentication login mschap

copy running-config start-config

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		

Configuring AAA Accounting Default Methods

-
-
-

Note

BEFORE YOU BEGIN

SUMMARY STEPS

1.
2.
3.
4.
5.

DETAILED STEPS

	Command	Purpose
Step 1		
Step 2		• • local,
Step 3		
Step 4		
Step 5		

Using AAA Server VSAs with Cisco NX-OS Devices

-
-
-

About VSAs

```
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

-
-
-

```
shell:roles="network-operator vdc-admin"
shell:roles*"network-operator vdc-admin"
```

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

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

```
shell:roles="roleA roleB …"
```

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

Displaying and Clearing the Local AAA Accounting Log

Note

BEFORE YOU BEGIN

SUMMARY STEPS

1. *size* *year month day hh*:*mm*:*ss*

   clear accounting log

size *year month day hh mm ss*	

Verifying AAA Configuration

Command	Purpose
all]	
show startup-config aaa	

Example AAA Configuration

Default Settings

Table 2-4 Default AAA Parameters

	250 KB

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

Related Documents, page 2-20

Standards, page 2-20

MIBs, page 2-20

Related Topic	Document Title
NX-OS Licensing	
Command reference	
RADIUS security protocol	Chapter 3, “Configuring RADIUS”
TACACS+ Security protocol	Chapter 4, “Configuring TACACS+”

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
• •	http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml