Configuring RADIUS

This chapter describes how to configure the Remote Access Dial-In User Service (RADIUS) protocol on Cisco NX-OS devices.

This chapter includes the following sections:

Information About RADIUS

The RADIUS distributed client/server system allows you to secure networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco NX-OS devices and send authentication and accounting requests to a central RADIUS server that contains all user authentication and network service access information.

RADIUS Network Environments

RADIUS can be implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

You can use RADIUS in the following network environments that require access security:

- Networks with multiple-vendor network devices, each supporting RADIUS. For example, network devices from several vendors can use a single RADIUS server-based security database.

- Networks already using RADIUS. You can add a Cisco NX-OS device with RADIUS to the network. This action might be the first step when you make a transition to a AAA server.
- Networks that require resource accounting. You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider (ISP) might use a freeware-based version of the RADIUS access control and accounting software to meet special security and billing needs.
- Networks that support authentication profiles. Using the RADIUS server in your network, you can configure AAA authentication and set up per-user profiles. Per-user profiles enable the Cisco NX-OS device to better manage ports using their existing RADIUS solutions and to efficiently manage shared resources to offer different service-level agreements.

RADIUS Operation

When a user attempts to log in and authenticate to a Cisco NX-OS device using RADIUS, the following process occurs:

- The user is prompted for and enters a username and password.
- The username and encrypted password are sent over the network to the RADIUS server.
- The user receives one of the following responses from the RADIUS server:

ACCEPT	The user is authenticated.
REJECT	The user is not authenticated and is prompted to reenter the username and password, or access is denied.
CHALLENGE	A challenge is issued by the RADIUS server. The challenge collects additional data from the user.
CHANGE PASSWORD	A request is issued by the RADIUS server, asking the user to select a new password.

The ACCEPT or REJECT response is bundled with additional data that is used for EXEC or network authorization. You must first complete RADIUS authentication before using RADIUS authorization. The additional data included with the ACCEPT or REJECT packets consists of the following:

- Services that the user can access, including Telnet, rlogin, or local-area transport (LAT) connections, and Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services.
- Connection parameters, including the host or client IPv4 or IPv6 address, access list, and user timeouts.

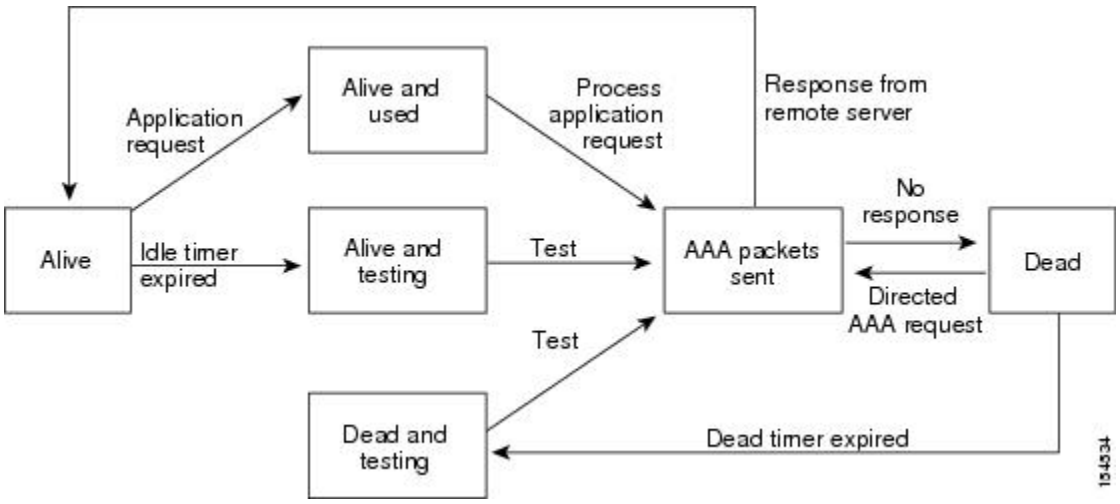
RADIUS Server Monitoring

An unresponsive RADIUS server can cause a delay in processing AAA requests. You can configure the Cisco NX-OS device to periodically monitor a RADIUS server to check whether it is responding (or alive) to save time in processing AAA requests. The Cisco NX-OS device marks unresponsive RADIUS servers as dead and does not send AAA requests to any dead RADIUS servers. The Cisco NX-OS device periodically monitors the dead RADIUS servers and brings them to the alive state once they respond. This monitoring process verifies that a RADIUS server is in a working state before real AAA requests are sent its way. Whenever a

RADIUS server changes to the dead or alive state, a Simple Network Management Protocol (SNMP) trap is generated and the Cisco NX-OS device displays an error message that a failure is taking place.

This figure shows the states for RADIUS server monitoring.

Figure 1: RADIUS Server States



Note The monitoring interval for alive servers and dead servers are different and can be configured by the user. The RADIUS server monitoring is performed by sending a test authentication request to the RADIUS server.

Vendor-Specific Attributes

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 separator 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, with authentication results. This authorization information is specified through VSAs.

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, you should enclose the value within double quotation marks.

The Cisco NX-OS software supports the following attributes:

roles Lists all the roles to which the user belongs. The value field is a string that lists the role names delimited by white space. For example, if the user belongs to roles network-operator and vdc-admin, the value field would be network-operator vdc-admin. This subattribute, which the RADIUS server sends in the VSA portion of the Access-Accept frames, can only be used with the shell protocol value. The following examples show the roles attribute that is supported by the Cisco Access Control Server (ACS):

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

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

The following examples show the roles attribute that is 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. It can be used only with the accounting protocol data units (PDUs).

Licensing Requirements for RADIUS

This table shows the licensing requirements for this feature.

Product	License Requirement
Cisco DCNM	RADIUS 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 an explanation of the Cisco DCNM licensing scheme, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.
Cisco NX-OS	RADIUS 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 an explanation of the Cisco NX-OS licensing scheme for your platform, see the licensing guide for your platform.

Prerequisites for RADIUS

The following prerequisites are required for using this feature on Cisco DCNM. For a full list of feature-specific prerequisites, see the platform-specific documentation.

- System-message logging levels for RADIUS must meet or exceed Cisco DCNM requirements. During device discovery, Cisco DCNM detects inadequate logging levels and raises them to the minimum requirements. Cisco Nexus 7000 Series switches that run Cisco NX-OS Release 4.0 are an exception. For Cisco NX-OS Release 4.0, prior to device discovery, use the command-line interface to configure logging levels to meet or exceed Cisco DCNM requirements. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Platform Support for RADIUS

The following platforms support this feature but may implement it differently. For platform-specific information, including guidelines and limitations, system defaults, and configuration limits, see the corresponding documentation.

Platform	Documentation
Cisco Nexus 1000V Series Switches	Cisco Nexus 1000V Series Switches Documentation
Cisco Nexus 3000 Series Switches	Cisco Nexus 3000 Series Switches Documentation
Cisco Nexus 4000 Series Switches	Cisco Nexus 4000 Series Switches Documentation
Cisco Nexus 5000 Series Switches	Cisco Nexus 5000 Series Switches Documentation
Cisco Nexus 7000 Series Switches	Cisco Nexus 7000 Series Switches Documentation

Configuring RADIUS Servers

This section describes how to configure RADIUS servers on a Cisco NX-OS device.

RADIUS Server Configuration Process

1. Establish the RADIUS server connections to the Cisco NX-OS device.
2. Configure the RADIUS secret keys for the RADIUS servers.
3. If needed, configure RADIUS server groups with subsets of the RADIUS servers for AAA authentication methods.
4. If needed, configure any of the following optional parameters:
   - Dead-time interval
   - RADIUS server specification allowed at user login
   - Timeout interval
   - TCP port

Related Topics

- Adding a RADIUS Server Host, page 6
- Configuring a Global RADIUS Key, page 8

Adding a RADIUS Server Host

To access a remote RADIUS server, you must configure the IP address or hostname of a RADIUS server. You can configure up to 64 RADIUS servers.

Note By default, when you configure a RADIUS server IP address or hostname the Cisco NX-OS device, the RADIUS server is added to the default RADIUS server group. You can also add the RADIUS server to another RADIUS server group.

Before You Begin

Ensure that the server is already configured as a member of the server group.

Ensure that the server is configured to authenticate RADIUS traffic.

Ensure that the Cisco NX-OS device is configured as a RADIUS client of the AAA servers.

Procedure

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

Step 2 From the Summary pane, double-click the device to display the server groups.

Step 3 Click **Default RADIUS Server Group**.

Step 4 From the menu bar, choose **Server Groups > Add Server**.
The Server Details appear in the Details pane.

Step 5 In the Server field, enter the RADIUS server IPv4 address, IPv6 address, or hostname in the Server field.

Step 6 From the Server drop-down list, choose either the IPv4 address, IPv6 address, or hostname as the correct server identifier type.

Note If the server identifier format matches the identifier type selected, Cisco DCNM outlines the Server field in yellow to indicate that it is correct. If the server identifier format does not match the identifier type, Cisco DCNM outlines the Server field in red to indicate an error. Change the address or the address type to correct this problem.

Step 7 (Optional) In the Authentication Port field, enter a new UDP port number or clear the field to disable authentication.
The default authentication UDP port is 1812.

Step 8 (Optional) In the Accounting Port field, enter a new UDP port number or clear the field to disable accounting.
The default accounting UDP port is 1813.

Step 9 (Optional) In the Test area, you can enter a username, password, and idle time interval in minutes for periodic server host monitoring.
The default username is test, the default password is test, and the default idle time interval is 0 minutes, which disables periodic monitoring.

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

Related Topics

- Adding a RADIUS Server Group, page 9

Copying a RADIUS Server Host

You can copy the configuration of a RADIUS server host from one RADIUS server to another server group, either on the same Cisco NX-OS device or on another Cisco NX-OS device.

Before You Begin

Ensure that you have configured the server in the default RADIUS server group.

Ensure that you have created the target RADIUS server group.

Procedure

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

Step 2 From the Summary pane, double-click the device to display the server groups.

Step 3 Double-click **Default RADIUS Server Group**.
The list of RADIUS server hosts appears.

Step 4 Click the RADIUS server host you want to copy.

Step 5 From the menu bar, choose **Actions > Copy**.
The RADIUS server host appears in the list of servers for the server group.

Step 6 Click the destination RADIUS server group.

Note You can copy the server host configuration to a server group within the same device or in another device.

Step 7 From the menu bar, choose **Actions > Paste**.

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

Related Topics

- Adding a RADIUS Server Host, page 6
- Adding a RADIUS Server Group, page 9

Deleting a RADIUS Server Host

You can delete a RADIUS server host from a RADIUS server group.

Before You Begin

Add one or more RADIUS server hosts.

Procedure

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

Step 2 From the Summary pane, double-click the device to display the server groups.

Step 3 Click **Default RADIUS Server Group**.

Step 4 Click the desired RADIUS server.

Step 5 From the menu bar, choose **Server Groups > Delete Server**.
The RADIUS server disappears from the list of servers.

Step 6 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Related Topics

- Adding a RADIUS Server Host, page 6

Configuring a Global RADIUS Key

You can configure a RADIUS key for all servers used by the Cisco NX-OS device. A RADIUS key is a shared secret text string between the Cisco NX-OS device and the RADIUS server hosts. You can also configure a RADIUS key specific to a RADIUS server.

Before You Begin

Obtain the RADIUS key values for the remote RADIUS servers.

Configure the RADIUS key on the remote RADIUS servers.

Procedure

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

Step 2 From the Summary pane, double-click the device to display the server groups.

Step 3 Click **Default RADIUS Server Group**.

Step 4 From the Details pane, click the **Global Settings** tab.

Step 5 In the Key field, enter the RADIUS key.

Step 6 (Optional) Check **Encrypt** if the key is in an encrypted format.
The default is clear text. The Cisco NX-OS software encrypts a clear text key before saving it to the running configuration.

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

Related Topics

- Configuring a Key for a Specific RADIUS Server, page 9

Configuring a Key for a Specific RADIUS Server

You can configure a key on the Cisco NX-OS device for a specific RADIUS server. A RADIUS key is a secret text string shared between the Cisco NX-OS device and a specific RADIUS server.

Before You Begin

Configure one or more RADIUS server hosts.

Obtain the key value for the remote RADIUS server.

Configure the key on the RADIUS server.

Procedure

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

Step 2 From the Summary pane, double-click the device to display the server groups.

Step 3 Double-click **Default RADIUS Server Group** to display the list of RADIUS servers.

Step 4 Click the desired RADIUS server.

Step 5 From the Details pane, click the **Server Details** tab.

Step 6 Check **Override Defaults**.

Step 7 In the Key field, enter the RADIUS key.

Step 8 The default is the global RADIUS key.

Step 9 (Optional) Check **Encrypt** to encrypt the key.

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

Related Topics

- Adding a RADIUS Server Host, page 6
- Configuring a Global RADIUS Key, page 8

Adding a RADIUS Server Group

You can reference one or more remote AAA servers to authenticate users using server groups. All members of a group must belong to the RADIUS protocol. 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.

Before You Begin

Configure one or more RADIUS server hosts.

Procedure

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

Step 2 From the Summary pane, click the device.

Step 3 From the menu bar, choose **Server Groups > RADIUS Server Group**.
A new line appears at the end of the server group list for the device and the Details tab appears in the Details pane.

Step 4 In the Server Group Name field, enter the name and press the **Enter** key.
The server group name is a case-sensitive alphanumeric string with a maximum length of 127 characters.

Step 5 (Optional) In the Dead time(mins) field, enter the number of minutes for the dead-time interval.
The default dead-time interval is 0 minutes.

Step 6 In the VRF Name field, click the down arrow to display the VRF Name dialog and click a VRF. Click **OK**.

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

Adding a RADIUS Server Host to a RADIUS Server Group

You can add a RADIUS server host to a RADIUS server group.

Before You Begin

Ensure that you have added the RADIUS server host to the Default RADIUS Server Group.

Procedure

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

Step 2 From the Summary pane, double-click the device to display the server groups.

Step 3 Click a RADIUS server group.

Step 4 From the menu bar, choose **Server Groups > Add Server**.
The Server Details appear in the Details pane.

Step 5 In the Server field, enter the RADIUS server IPv4 address, IPv6 address, or hostname in the Server field.

Step 6 From the Server drop-down list, choose either the IPv4 address, IPv6 address, or hostname as the correct server identifier type.

Note If the server identifier format matches the identifier type selected, Cisco DCNM outlines the Server field in yellow to indicate that it is correct. If the server identifier format does not match the identifier type, Cisco DCNM outlines the Server field in red to indicate an error. Change the address or the address type to correct this problem.

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

Related Topics

- Adding a RADIUS Server Host, page 6

Deleting a RADIUS Server Host from a RADIUS Server Group

You can delete a RADIUS server host from a RADIUS server group.

Procedure

Step 1 From the Feature Selector pane, choose **Security > AAA > Server Groups**.
Step 2 From the Summary pane, double-click the device to display the server groups.
Step 3 Double-click the server group to display the list of server hosts.
Step 4 Click the RADIUS server host to delete.
Step 5 From the menu bar, choose **Server Groups > Delete Server** and click **Yes** on the confirmation dialog.
Step 6 The RADIUS server host disappears from the list.
Step 7 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Related Topics

- Adding a RADIUS Server Host to a RADIUS Server Group, page 10

Deleting a RADIUS Server Group

You can delete a RADIUS server group.

Before You Begin

Ensure that all servers in the group are RADIUS servers.

Procedure

Step 1 From the Feature Selector pane, choose **Security > AAA > Server Groups**.
Step 2 From the Summary pane, double-click the device to display the list of server groups.
Step 3 Click the RADIUS server group to delete.
Step 4 From the menu bar, choose **Server Groups > Delete Server Group** and click **Yes** in the confirmation dialog. The server group disappears from the server group list.
Step 5 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Configuring the Global Source Interface for RADIUS Server Groups

You can configure a global source interface for RADIUS server groups to use when accessing RADIUS servers. This configuration forces the RADIUS servers to use the IP address of the source interface for all outgoing RADIUS packets. By default, the Cisco NX-OS software uses any available interface.

Before You Begin

Make sure that you are in the correct VDC.

Procedure

Step 1 From the Feature Selector pane, choose **Security > AAA > Server Groups**.
The available devices appear in the Summary pane.

Step 2 From the Summary pane, double-click the device to display the server groups.

Step 3 Click **Default RADIUS Server Group**.

Step 4 From the Details pane, click the **Global Settings** tab.

Step 5 From the Source Interface drop-down list, choose an Ethernet interface, a loopback interface, a port-channel interface, a tunnel interface, a VLAN interface, or the management interface (mgmt 0).

Step 6 Click **OK**.

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

Related Topics

- Configuring a Source Interface for a Specific RADIUS Server Group, page 12

Configuring a Source Interface for a Specific RADIUS Server Group

You can configure a source interface for a specific RADIUS server group to use when accessing RADIUS servers. This configuration forces the RADIUS servers to use the IP address of the source interface for all outgoing RADIUS packets.

Note This configuration overrides the global source interface for this server group.

Before You Begin

Make sure that you are in the correct VDC.

Procedure

Step 1 From the Feature Selector pane, choose **Security > AAA > Server Groups**.
The available devices appear in the Summary pane.

Step 2 From the Summary pane, double-click the device to display the server groups.

Step 3 Click the desired RADIUS server group.

Step 4 From the Details pane, click the **Details** tab.

Step 5 From the Source Interface drop-down list, choose an Ethernet interface, a loopback interface, a port-channel interface, a tunnel interface, a VLAN interface, or the management interface (mgmt 0).

Step 6 Click **OK**.

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

Related Topics

- Configuring the Global Source Interface for RADIUS Server Groups, page 11

Allowing Users to Specify a RADIUS Server at Login

By default, the Cisco NX-OS device forwards an authentication request based on the default AAA authentication method. You can configure the Cisco NX-OS device to allow the user to specify a VRF and RADIUS server to send the authentication request by enabling the directed-request option. If you enable this option, the user can log in as *username@vrfname*:*hostname*, where *vrfname* is the VRF to use and *hostname* is the name of a configured RADIUS server.

Note If you enable the directed-request option, the device uses only the RADIUS method for authentication and not the default local method.

Note User-specified logins are supported only for Telnet sessions.

Procedure

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

Step 2 From the Summary pane, double-click the device to display the server groups.

Step 3 Click **Default RADIUS Server Group**.

Step 4 From the Details pane, click the **Global Settings** tab.

Step 5 Click **Direct Req**.

Step 6 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Configuring the Global RADIUS Transmission Retry Count and Timeout Interval

You can configure a global retransmission retry count and timeout interval for all RADIUS servers. By default, a Cisco NX-OS device retries transmission to a RADIUS server only once before reverting to local authentication. You can increase this number up to a maximum of five retries per server. The timeout interval determines how long the Cisco NX-OS device waits for responses from RADIUS servers before declaring a timeout failure.

Procedure

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

Step 2 From the Summary pane, double-click the device to display the server groups.

Step 3 Click **Default RADIUS Server Group**.

Step 4 From the Details pane, click the **Global Settings** tab.

Step 5 In the Retransmit field, enter a number of retransmit attempts.
The default is 1.

Step 6 In the Time out(secs) field, enter the number of seconds for the timeout interval.
The default is 1.

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

Related Topics

- Configuring the RADIUS Transmission Retry Count and Timeout Interval for a Server, page 14

Configuring the RADIUS Transmission Retry Count and Timeout Interval for a Server

By default, a Cisco NX-OS device retries a transmission to a RADIUS server only once before reverting to local authentication. You can increase this number up to a maximum of five retries per server. You can also set a timeout interval that the Cisco NX-OS device waits for responses from RADIUS servers before declaring a timeout failure.

Before You Begin

Configure one or more RADIUS server hosts.

Procedure

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

Step 2 From the Summary pane, double-click the device to display the server groups.

Step 3 Double-click **Default RADIUS Server Group** to display the list of RADIUS servers.

Step 4 Click the desired RADIUS server.

Step 5 From the Details pane, click the **Server Details** tab.

Step 6 Check **Override Defaults**.

Step 7 In the Retransmit field, enter the number of retransmit attempts.
The default is 1.

Step 8 In the Timeout(secs) field, enter the number of seconds for the retransmission interval.
The default is 5 seconds.

Step 9 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Related Topics

- Configuring the Global RADIUS Transmission Retry Count and Timeout Interval, page 13

Configuring Accounting and Authentication Attributes for RADIUS Servers

You can specify that a RADIUS server is to be used only for accounting purposes or only for authentication purposes. By default, RADIUS servers are used for both accounting and authentication. You can also specify the destination UDP port numbers where RADIUS accounting and authentication messages should be sent if there is a conflict with the default port.

Before You Begin

Configure one or more RADIUS server hosts.

Procedure

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

Step 2 From the Summary pane, double-click the device to display the server groups.

Step 3 Double-click **Default RADIUS Server Group** to display the list of RADIUS servers.

Step 4 Click the desired RADIUS server.

Step 5 From the Details pane, click the **Server Details** tab.

Step 6 (Optional) In the Authentication Port field, enter a new UDP port number or clear the field to disable authentication.
The default authentication UDP port is 1812.

Step 7 (Optional) In the Accounting Port field, enter a new UDP port number or clear the field to disable accounting.
The default accounting UDP port is 1813.

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

Related Topics

- Adding a RADIUS Server Host, page 6

Configuring Periodic RADIUS Server Monitoring

You can monitor the availability of RADIUS servers. These parameters include the username and password to use for the server and an idle timer. The idle timer specifies the interval during which a RADIUS server receives no requests before the Cisco NX-OS device sends out a test packet. You can configure this option to test servers periodically.

Note For security reasons, we recommend that you do not configure a test username that is the same as an existing user in the RADIUS database.

The test idle timer specifies the interval during which a RADIUS server receives no requests before the Cisco NX-OS device sends out a test packet.

Note The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, the Cisco NX-OS device does not perform periodic RADIUS server monitoring.

Before You Begin

Add one or more RADIUS server hosts.

Procedure

Step 1 From the Feature Selector pane, choose **Security > AAA > Server Groups**.
Step 2 From the Summary pane, double-click the device to display the server groups.
Step 3 Double-click **Default RADIUS Server Group** to display the list of RADIUS servers.
Step 4 Click the desired RADIUS server.
Step 5 From the Details pane, click the **Server Details** tab.
Step 6 In the User Name field, enter a username.
Step 7 In the Password field, enter a password.
Step 8 In the Idle Time field, enter the number of minutes for periodic monitoring.
Step 9 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Related Topics

- Adding a RADIUS Server Host, page 6

Configuring the RADIUS Dead-Time Interval

You can configure the dead-time interval for all RADIUS servers. The dead-time interval specifies the time that the Cisco NX-OS device waits after declaring a RADIUS server is dead, before sending out a test packet to determine if the server is now alive. The default value is 0 minutes.

Note When the dead-time interval is 0 minutes, RADIUS servers are not marked as dead even if they are not responding. You can configure the dead-time interval for a RADIUS server group.

Procedure

Step 1 From the Feature Selector pane, choose **Security > AAA > Server Groups**.
Step 2 From the Summary pane, double-click the device to display the server groups.
Step 3 Click **Default RADIUS Server Group**.
Step 4 From the Details pane, click the **Global Settings** tab.
Step 5 In the Dead time(mins) field, enter the number of minutes.
The default is 0 minutes.
Step 6 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Related Topics

- Adding a RADIUS Server Group, page 9

Displaying RADIUS Server Statistics

You can display the statistics that the Cisco NX-OS device maintains for the RADIUS servers.

Before You Begin

Configure one or more RADIUS server hosts.

Procedure

Step 1 From the Feature Selector pane, choose **Security > AAA > Server Groups**.
Step 2 From the Summary pane, double-click the device to display the server groups.
Step 3 Double-click **Default RADIUS Server Group** to display the list of RADIUS servers.
Step 4 Click the desired RADIUS server.
Step 5 From the Details pane, click the **Statistics** tab.

Where to Go Next

You can now configure AAA authentication methods to include the server groups.

Field Descriptions for RADIUS Server Groups and Servers

This section includes field descriptions for RADIUS server groups and servers.

Security: AAA: Server Groups: Summary Pane

Table 1: Security: AAA: Server Groups: Summary Pane

Fields	Description
Authentication Port	UDP port number for authentication traffic for the servers. The default is 49.
Accounting Port	UDP port used for accounting for the servers.
Timeout	Number of seconds for the timeout interval for the servers. The default is 5 seconds.
Status	Status of the servers.

Security: AAA: Server Groups: device: Default RADIUS Server Group: Global Settings Tab

Table 2: Security: AAA: Server Groups: device: Default RADIUS Server Group: Global Settings Tab

Field	Description
Server Group Type	Server group type.
Time out(secs)	Number of seconds for the timeout interval. The default is 5 seconds.
Key	Global RADIUS key.
Source Interface	Source interface for a specific RADIUS server group to use when accessing RADIUS servers. The options are an Ethernet interface, a loopback interface, or the management interface (mgmt 0).
Retransmit	Number of retransmissions when the server does not respond.
Dead time(mins)	Number of minutes for the dead time interval. The default is 0 minutes.
Direct Req	Users can specify a RADIUS server at login.

Security: AAA: Server Groups: device: Default RADIUS Server Group: server: Server Details Tab

Table 3: Security: AAA: Server Groups: device: Default RADIUS Server Group: Server: Server Details Tab

Fields	Description
General	
Server Type	Server type.
Server	Server IPv4 address, IPv6 address, or alphanumeric name and the server name type.
Authentication Port	UDP port number for authentication traffic. The default is 1812.
Accounting Port	UDP port number for accounting traffic. The default is 1813.
Test	
User Name	Username for periodic monitoring of the RADIUS server.
Password	Password for periodic monitoring of the RADIUS server.
Idle Time	Number of minutes for the idle time interval for periodic monitoring of the RADIUS server. The default is 0, which disables periodic monitoring.
Override Default	Global values that you can override and configure for the RADIUS server. The default is to use the global values.
Key	Secret key for the RADIUS server.
Encrypt	RADIUS server key encryption status. The default is clear text.
Timeout(secs)	Number of seconds for the timeout interval. The default is 5 seconds.

Fields	Description
Retransmit	Number of retransmissions when the server does not respond. The default is 3.

Security: AAA: Server Groups: device: server group: Details Tab

Table 4: Security: AAA: Server Groups: device: server group : Details Tab

Fields	Description
Type	Displays RADIUS for the server group type.
Server Group Name	Displays the server group name.
Dead time(mins)	Number of minutes for the dead-time interval for the server group. The default is 0 minutes.
VRF Name	VRF name.
Source Interface	Source interface for a specific RADIUS server group to use when accessing RADIUS servers. The options are an Ethernet interface, a loopback interface, or the management interface (mgmt 0).

Additional References for RADIUS

This section describes additional information related to implementing RADIUS.

Related Documents

Related Topic	Document Title
Cisco NX-OS Licensing	*Cisco NX-OS Licensing Guide*
Cisco DCNM Licensing	*Cisco DCNM Installation and Licensing Guide, Release 5.x*
VRF configuration	*Unicast Configuration Guide, Cisco DCNM for LAN, Release 5.x*

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 RADIUS

This table lists the release history for this feature.

Table 5: Feature History for RADIUS

Feature Name	Releases	Feature Information
RADIUS	5.2(1)	Added support for the Cisco Nexus 3000 Series Switches.
RADIUS	5.1(1)	No change from Release 5.0.
RADIUS server groups	5.0(2)	Added support for configuring the global source interface for all RADIUS server groups.
RADIUS server groups	5.0(2)	Added support for configuring a source interface for a specific RADIUS server group.