



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:

- [About RADIUS, on page 1](#)
- [Licensing Requirements for RADIUS, on page 4](#)
- [Prerequisites for RADIUS, on page 4](#)
- [Guidelines and Limitations for RADIUS, on page 4](#)
- [Default Settings for RADIUS, on page 5](#)
- [Configuring RADIUS Servers, on page 5](#)
- [Verifying the RADIUS Configuration, on page 24](#)
- [Monitoring RADIUS Servers, on page 24](#)
- [Clearing RADIUS Server Statistics, on page 25](#)
- [Configuration Example for RADIUS, on page 25](#)
- [Where to Go Next , on page 26](#)
- [Additional References for RADIUS, on page 26](#)

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:

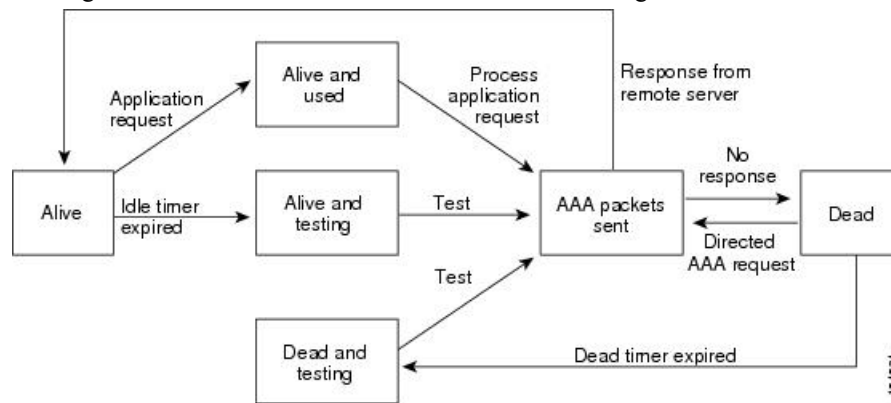
- Services that the user can access, including Telnet, rlogin, or local-area transport (LAT) connections, and Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services.
- Connection parameters, including the host or client IPv4 or IPv6 address, access list, and user timeouts.

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.

Figure 1: RADIUS Server States

This figure shows the states for RADIUS server monitoring.



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 `network-admin`, the value field would be `network-operator network-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 network-admin
shell:roles*"network-operator network-admin
```

The following examples show the roles attribute that is supported by FreeRADIUS:

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



Note When you specify a VSA as `shell:roles*"network-operator network-admin"` or `"shell:roles*\network-operator network-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 NX-OS	RADIUS requires no license. Any feature not included in a license package is bundled with the nx-os image and is provided at no extra charge to you. For an explanation of the Cisco NX-OS licensing scheme, see the <i>Cisco NX-OS Licensing Guide</i> .

Prerequisites for RADIUS

RADIUS has the following prerequisites:

- Obtain IPv4 or IPv6 addresses or hostnames for the RADIUS servers.
- Obtain keys from the RADIUS servers.
- Ensure that the Cisco NX-OS device is configured as a RADIUS client of the AAA servers.

Guidelines and Limitations for RADIUS

RADIUS has the following guidelines and limitations:

- You can configure a maximum of 64 RADIUS servers on the Cisco NX-OS device.
- 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.
- Only the RADIUS protocol supports one-time passwords.
- Cisco Nexus 9K Series switches support the CLI command, `aaa authentication login ascii-authentication`, only for TACAAS+, but not for RADIUS. Ensure that you have disabled `aaa authentication login ascii-authentication switch` so that the default authentication, PAP, is enabled. Otherwise, you will see syslog errors.

Default Settings for RADIUS

This table lists the default settings for RADIUS parameters.

Table 1: Default RADIUS Parameter Settings

Parameters	Default
Server roles	Authentication and accounting
Dead timer interval	0 minutes
Retransmission count	1
Retransmission timer interval	5 seconds
Authentication port	1812
Accounting port	1813
Idle timer interval	0 minutes
Periodic server monitoring username	test
Periodic server monitoring password	test

Configuring RADIUS Servers

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



Note 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.



Note Cisco Nexus 9K Series switches support the CLI command, `aaa authentication login ascii-authentication`, only for TACAAS+, but not for RADIUS. Ensure that you have disabled `aaa authentication login ascii-authentication` switch so that the default authentication, PAP, is enabled. Otherwise, you will see syslog errors.

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
5. (Optional) If RADIUS distribution is enabled, commit the RADIUS configuration to the fabric.

Related Topics

[Configuring RADIUS Server Hosts](#), on page 6

[Configuring Global RADIUS Keys](#), on page 8

Configuring RADIUS Server Hosts

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 of 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.

SUMMARY STEPS

1. **configure terminal**

2. **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*}
3. (Optional) **show radius** {**pending** | **pending-diff**}
4. (Optional) **radius commit**
5. **exit**
6. (Optional) **show radius-server**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } Example: <pre>switch(config)# radius-server host 10.10.1.1</pre>	Specifies the IPv4 or IPv6 address or hostname for a RADIUS server to use for authentication.
Step 3	(Optional) show radius { pending pending-diff } Example: <pre>switch(config)# show radius pending</pre>	Displays the RADIUS configuration pending for distribution.
Step 4	(Optional) radius commit Example: <pre>switch(config)# radius commit</pre>	Applies the RADIUS configuration changes in the temporary database to the running configuration.
Step 5	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 6	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	Displays the RADIUS server configuration.
Step 7	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Related Topics

[Configuring a Key for a Specific RADIUS Server](#), on page 9

Configuring Global RADIUS Keys

You can configure RADIUS keys 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.

Before you begin

Obtain the RADIUS key values for the remote RADIUS servers.

Configure the RADIUS key on the remote RADIUS servers.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server key [0 | 6 | 7] key-value**
3. **exit**
4. (Optional) **show radius-server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	radius-server key [0 6 7] key-value Example: <pre>switch(config)# radius-server key 0 QsEfThUkO</pre>	Specifies a RADIUS key for all RADIUS servers. You can specify that the <i>key-value</i> is in clear text format (0), is type-6 encrypted (6), or is type-7 encrypted (7). The Cisco NX-OS software encrypts a clear text key before saving it to the running configuration. The default format is clear text. The maximum length is 63 characters. By default, no RADIUS key is configured.
Step 3	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 4	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	Displays the RADIUS server configuration. Note The RADIUS keys are saved in encrypted form in the running configuration. Use the show running-config command to display the encrypted RADIUS keys.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Related Topics

[Configuring RADIUS Server Groups](#), on page 10

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.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **key** [**0** | **6** | **7**] *key-value*
3. **exit**
4. (Optional) **show radius-server**
5. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } key [0 6 7] <i>key-value</i> Example: <pre>switch(config)# radius-server host 10.10.1.1 key 0 P1IjUhYg</pre>	Specifies a RADIUS key for a specific RADIUS server. You can specify that the <i>key-value</i> is in clear text format (0), is type-6 encrypted (6), or is type-7 encrypted (7). The Cisco NX-OS software encrypts a clear text key before saving it to the running configuration. The default format is clear text. The maximum length is 63 characters. This RADIUS key is used instead of the global RADIUS key.
Step 3	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 4	(Optional) show radius-server Example:	Displays the RADIUS server configuration.

	Command or Action	Purpose
	<code>switch# show radius-server</code>	Note The RADIUS keys are saved in encrypted form in the running configuration. Use the show running-config command to display the encrypted RADIUS keys.
Step 5	(Optional) copy running-config startup-config Example: <code>switch# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

Related Topics

[Configuring RADIUS Server Hosts](#), on page 6

Configuring RADIUS Server Groups

You can specify one or more remote AAA servers for authentication 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

Ensure that all servers in the group are RADIUS servers.

SUMMARY STEPS

1. **configure terminal**
2. **aaa group server radius** *group-name*
3. **server** {*ipv4-address* | *ipv6-address* | *hostname*}
4. (Optional) **deadtime** *minutes*
5. (Optional) **server** {*ipv4-address* | *ipv6-address* | *hostname*}
6. (Optional) **use-vrf** *vrf-name*
7. **exit**
8. (Optional) **show radius-server groups** [*group-name*]
9. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <code>switch# configure terminal</code> <code>switch(config)#</code>	Enters global configuration mode.

	Command or Action	Purpose
Step 2	aaa group server radius <i>group-name</i> Example: <pre>switch(config)# aaa group server radius RadServer switch(config-radius)#</pre>	Creates a RADIUS server group and enters the RADIUS server group configuration submode for that group. The <i>group-name</i> argument is a case-sensitive alphanumeric string with a maximum length of 127 characters.
Step 3	server { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } Example: <pre>switch(config-radius)# server 10.10.1.1</pre>	Configures the RADIUS server as a member of the RADIUS server group. If the specified RADIUS server is not found, configure it using the radius-server host command and retry this command.
Step 4	(Optional) deadtime <i>minutes</i> Example: <pre>switch(config-radius)# deadtime 30</pre>	Configures the monitoring dead time. The default is 0 minutes. The range is from 1 through 1440. Note If the dead-time interval for a RADIUS server group is greater than zero (0), that value takes precedence over the global dead-time value.
Step 5	(Optional) server { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } Example: <pre>switch(config-radius)# server 10.10.1.1</pre>	Configures the RADIUS server as a member of the RADIUS server group. Tip If the specified RADIUS server is not found, configure it using the radius-server host command and retry this command.
Step 6	(Optional) use-vrf <i>vrf-name</i> Example: <pre>switch(config-radius)# use-vrf vrf1</pre>	Specifies the VRF to use to contact the servers in the server group.
Step 7	exit Example: <pre>switch(config-radius)# exit switch(config)#</pre>	Exits configuration mode.
Step 8	(Optional) show radius-server groups [<i>group-name</i>] Example: <pre>switch(config)# show radius-server groups</pre>	Displays the RADIUS server group configuration.
Step 9	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Related Topics

[Configuring the RADIUS Dead-Time Interval](#), on page 21

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. You can also configure a different source interface for a specific RADIUS server group. By default, the Cisco NX-OS software uses any available interface.

SUMMARY STEPS

1. **configure terminal**
2. **ip radius source-interface *interface***
3. **exit**
4. (Optional) **show radius-server**
5. (Optional) **copy running-config startup config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)	Enters global configuration mode.
Step 2	ip radius source-interface <i>interface</i> Example: switch(config)# ip radius source-interface mgmt 0	Configures the global source interface for all RADIUS server groups configured on the device.
Step 3	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 4	(Optional) show radius-server Example: switch# show radius-server	Displays the RADIUS server configuration information.
Step 5	(Optional) copy running-config startup config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Related Topics

[Configuring RADIUS Server Groups](#), on page 10

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 Cisco NX-OS device uses only the RADIUS method for authentication and not the default local method.



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

SUMMARY STEPS

1. **configure terminal**
2. **radius-server directed-request**
3. (Optional) **show radius {pending | pending-diff}**
4. (Optional) **radius commit**
5. **exit**
6. (Optional) **show radius-server directed-request**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	radius-server directed-request Example: switch(config)# radius-server directed-request	Allows users to specify a RADIUS server to send the authentication request when logging in. The default is disabled.
Step 3	(Optional) show radius {pending pending-diff} Example: switch(config)# show radius pending	Displays the RADIUS configuration pending for distribution.
Step 4	(Optional) radius commit Example: switch(config)# radius commit	Applies the RADIUS configuration changes in the temporary database to the running configuration.
Step 5	exit Example: switch(config)# exit switch#	Exits configuration mode.

	Command or Action	Purpose
Step 6	(Optional) show radius-server directed-request Example: switch# show radius-server directed-request	Displays the directed request configuration.
Step 7	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

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.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server retransmit** *count*
3. **radius-server timeout** *seconds*
4. (Optional) **show radius** {*pending* | *pending-diff*}
5. (Optional) **radius commit**
6. **exit**
7. (Optional) **show radius-server**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	radius-server retransmit <i>count</i> Example: switch(config)# radius-server retransmit 3	Specifies the retransmission count for all RADIUS servers. The default retransmission count is 1 and the range is from 0 to 5.
Step 3	radius-server timeout <i>seconds</i> Example: switch(config)# radius-server timeout 10	Specifies the transmission timeout interval for RADIUS servers. The default timeout interval is 5 seconds and the range is from 1 to 60 seconds.

	Command or Action	Purpose
Step 4	(Optional) show radius {pending pending-diff} Example: switch(config)# show radius pending	Displays the RADIUS configuration pending for distribution.
Step 5	(Optional) radius commit Example: switch(config)# radius commit	Applies the RADIUS configuration changes in the temporary database to the running configuration.
Step 6	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 7	(Optional) show radius-server Example: switch# show radius-server	Displays the RADIUS server configuration.
Step 8	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

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.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server host {ipv4-address | ipv6-address | hostname} retransmit count**
3. **radius-server host {ipv4-address | ipv6-address | hostname} timeout seconds**
4. (Optional) **show radius {pending | pending-diff}**
5. (Optional) **radius commit**
6. **exit**
7. (Optional) **show radius-server**
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } retransmit <i>count</i> Example: switch(config)# radius-server host server1 retransmit 3	Specifies the retransmission count for a specific server. The default is the global value. Note The retransmission count value specified for a RADIUS server overrides the count specified for all RADIUS servers.
Step 3	radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } timeout <i>seconds</i> Example: switch(config)# radius-server host server1 timeout 10	Specifies the transmission timeout interval for a specific server. The default is the global value. Note The timeout interval value specified for a RADIUS server overrides the interval value specified for all RADIUS servers.
Step 4	(Optional) show radius { pending pending-diff } Example: switch(config)# show radius pending	Displays the RADIUS configuration pending for distribution.
Step 5	(Optional) radius commit Example: switch(config)# radius commit	Applies the RADIUS configuration changes in the temporary database to the running configuration and distributes RADIUS configuration to other Cisco NX-OS devices if you have enabled CFS configuration distribution for the user role feature.
Step 6	exit Example: switch(config)# exit switch#	Exits configuration mode.
Step 7	(Optional) show radius-server Example: switch# show radius-server	Displays the RADIUS server configuration.
Step 8	(Optional) copy running-config startup-config Example: switch# copy running-config startup-config	Copies the running configuration to the startup configuration.

Related Topics

[Configuring RADIUS Server Hosts](#), on page 6

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.

SUMMARY STEPS

1. **configure terminal**
2. (Optional) **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **acct-port** *udp-port*
3. (Optional) **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **accounting**
4. (Optional) **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **auth-port** *udp-port*
5. (Optional) **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **authentication**
6. (Optional) **show radius** {**pending** | **pending-diff**}
7. (Optional) **radius commit**
8. **exit**
9. (Optional) **show radius-server**
10. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	(Optional) radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } acct-port <i>udp-port</i> Example: <pre>switch(config)# radius-server host 10.10.1.1 acct-port 2004</pre>	Specifies a UDP port to use for RADIUS accounting messages. The default UDP port is 1813. The range is from 0 to 65535.
Step 3	(Optional) radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } accounting Example: <pre>switch(config)# radius-server host 10.10.1.1 accounting</pre>	Specifies to use the RADIUS server only for accounting purposes. The default is both accounting and authentication.
Step 4	(Optional) radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } auth-port <i>udp-port</i> Example:	Specifies a UDP port to use for RADIUS authentication messages. The default UDP port is 1812. The range is from 0 to 65535.

	Command or Action	Purpose
	<code>switch(config)# radius-server host 10.10.2.2 auth-port 2005</code>	
Step 5	(Optional) radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } authentication Example: <code>switch(config)# radius-server host 10.10.2.2 authentication</code>	Specifies to use the RADIUS server only for authentication purposes. The default is both accounting and authentication.
Step 6	(Optional) show radius { <i>pending</i> <i>pending-diff</i> } Example: <code>switch(config)# show radius pending</code>	Displays the RADIUS configuration pending for distribution.
Step 7	(Optional) radius commit Example: <code>switch(config)# radius commit</code>	Applies the RADIUS configuration changes in the temporary database to the running configuration.
Step 8	exit Example: <code>switch(config)# exit switch#</code>	Exits configuration mode.
Step 9	(Optional) show radius-server Example: <code>switch(config)# show radius-server</code>	Displays the RADIUS server configuration.
Step 10	(Optional) copy running-config startup-config Example: <code>switch# copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

Related Topics

[Configuring RADIUS Server Hosts](#), on page 6

Configuring Global Periodic RADIUS Server Monitoring

You can monitor the availability of all RADIUS servers without having to configure the test parameters for each server individually. Any servers for which test parameters are not configured are monitored using the global level parameters.



Note Test parameters that are configured for individual servers take precedence over global test parameters.

The global configuration parameters include the username and password to use for the servers and an idle timer. The idle timer specifies the interval in 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, or you can run a one-time only test.



Note To protect network security, we recommend that you use a username that is not the same as an existing username in the RADIUS database.



Note The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

Before you begin

Enable RADIUS.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server test** {*idle-time minutes* | **password** *password* [*idle-time minutes*] | **username** *name* [**password** *password* [*idle-time minutes*]]}
3. **radius-server deadtime** *minutes*
4. **exit**
5. (Optional) **show radius-server**
6. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	radius-server test { <i>idle-time minutes</i> password <i>password</i> [<i>idle-time minutes</i>] username <i>name</i> [password <i>password</i> [<i>idle-time minutes</i>]]} Example: <pre>switch(config)# radius-server test username user1 password Ur2Gd2BH idle-time 3</pre>	Specifies parameters for global server monitoring. The default username is test, and the default password is test. The default value for the idle timer is 0 minutes, and the valid range is from 0 to 1440 minutes. Note For periodic RADIUS server monitoring, the idle timer value must be greater than 0.
Step 3	radius-server deadtime <i>minutes</i> Example: <pre>switch(config)# radius-server deadtime 5</pre>	Specifies the number of minutes before the Cisco NX-OS device checks a RADIUS server that was previously unresponsive. The default value is 0 minutes, and the valid range is from 0 to 1440 minutes.
Step 4	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.

	Command or Action	Purpose
Step 5	(Optional) <code>show radius-server</code> Example: switch# <code>show radius-server</code>	Displays the RADIUS server configuration.
Step 6	(Optional) <code>copy running-config startup-config</code> Example: switch# <code>copy running-config startup-config</code>	Copies the running configuration to the startup configuration.

Related Topics

[Configuring Periodic RADIUS Server Monitoring on Individual Servers](#), on page 20

Configuring Periodic RADIUS Server Monitoring on Individual Servers

You can monitor the availability of individual RADIUS servers. The configuration 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, or you can run a one-time only test.



Note Test parameters that are configured for individual servers take precedence over global test parameters.



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.



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

Enable RADIUS.

Add one or more RADIUS server hosts.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **test** {*idle-time minutes* | **password** *password* [*idle-time minutes*] | **username** *name* [**password** *password* [*idle-time minutes*]]}
3. **radius-server deadtime** *minutes*
4. **exit**
5. (Optional) **show radius-server**

6. (Optional) copy running-config startup-config

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	radius-server host { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } test [idle-time <i>minutes</i>] [password <i>password</i>] [username <i>name</i>] [password <i>password</i>] [idle-time <i>minutes</i>]; Example: <pre>switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3</pre>	Specifies parameters for individual server monitoring. The default username is test, and the default password is test. The default value for the idle timer is 0 minutes, and the valid range is from 0 to 1440 minutes. Note For periodic RADIUS server monitoring, you must set the idle timer to a value greater than 0.
Step 3	radius-server deadtime <i>minutes</i> Example: <pre>switch(config)# radius-server deadtime 5</pre>	Specifies the number of minutes before the Cisco NX-OS device checks a RADIUS server that was previously unresponsive. The default value is 0 minutes, and the valid range is from 1 to 1440 minutes.
Step 4	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 5	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	Displays the RADIUS server configuration.
Step 6	(Optional) copy running-config startup-config Example: <pre>switch# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Related Topics

[Configuring RADIUS Server Hosts](#), on page 6

[Configuring Global Periodic RADIUS Server Monitoring](#), on page 18

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.

SUMMARY STEPS

1. **configure terminal**
2. **radius-server deadtime** *minutes*
3. (Optional) **show radius** {**pending** | **pending-diff**}
4. (Optional) **radius commit**
5. **exit**
6. (Optional) **show radius-server**
7. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	radius-server deadtime <i>minutes</i> Example: <pre>switch(config)# radius-server deadtime 5</pre>	Configures the dead-time interval. The default value is 0 minutes. The range is from 1 to 1440 minutes.
Step 3	(Optional) show radius { pending pending-diff } Example: <pre>switch(config)# show radius pending</pre>	Displays the RADIUS configuration pending for distribution.
Step 4	(Optional) radius commit Example: <pre>switch(config)# radius commit</pre>	Applies the RADIUS configuration changes in the temporary database to the running configuration.
Step 5	exit Example: <pre>switch(config)# exit switch#</pre>	Exits configuration mode.
Step 6	(Optional) show radius-server Example: <pre>switch# show radius-server</pre>	Displays the RADIUS server configuration.
Step 7	(Optional) copy running-config startup-config Example:	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	switch# <code>copy running-config startup-config</code>	

Related Topics

[Configuring RADIUS Server Groups](#), on page 10

Configuring One-Time Passwords

One-time password (OTP) support is available for Cisco NX-OS devices through the use of RSA SecurID token servers. With this feature, users authenticate to a Cisco NX-OS device by entering both a personal identification number (or one-time password) and the token code being displayed at that moment on their RSA SecurID token.



Note The token code used for logging into the Cisco NX-OS device changes every 60 seconds. To prevent problems with device discovery, we recommend using different usernames that are present on the Cisco Secure ACS internal database.

Before you begin

On the Cisco NX-OS device, configure a RADIUS server host and remote default login authentication.

Ensure that the following are installed:

- Cisco Secure Access Control Server (ACS) version 4.2
- RSA Authentication Manager version 7.1 (the RSA SecurID token server)
- RSA ACE Agent/Client

No configuration (other than a RADIUS server host and remote authentication) is required on the Cisco NX-OS device to support one-time passwords. However, you must configure the Cisco Secure ACS as follows:

1. Enable RSA SecurID token server authentication.
2. Add the RSA SecurID token server to the Unknown User Policy database.

Manually Monitoring RADIUS Servers or Groups

You can manually issue a test message to a RADIUS server or to a server group.

SUMMARY STEPS

1. `test aaa server radius {ipv4-address | ipv6-address | hostname} [vrf vrf-name] username password`
2. `test aaa group group-name username password`

DETAILED STEPS

	Command or Action	Purpose
Step 1	test aaa server radius { <i>ipv4-address</i> <i>ipv6-address</i> <i>hostname</i> } [vrf <i>vrf-name</i>] <i>username password</i> Example: <pre>switch# test aaa server radius 10.10.1.1 user1 Ur2Gd2BH</pre>	Sends a test message to a RADIUS server to confirm availability.
Step 2	test aaa group <i>group-name username password</i> Example: <pre>switch# test aaa group RadGroup user2 As3He3CI</pre>	Sends a test message to a RADIUS server group to confirm availability.

Verifying the RADIUS Configuration

To display RADIUS configuration information, perform one of the following tasks:

Command	Purpose
show radius { status pending pending-diff }	Displays the RADIUS Cisco Fabric Services distribution status and other details.
show running-config radius [all]	Displays the RADIUS configuration in the running configuration.
show startup-config radius	Displays the RADIUS configuration in the startup configuration.
show radius-server [<i>hostname</i> <i>ipv4-address</i> <i>ipv6-address</i>] [directed-request groups sorted statistics]	Displays all configured RADIUS server parameters.

Monitoring RADIUS Servers

You can monitor the statistics that the Cisco NX-OS device maintains for RADIUS server activity.

Before you begin

Configure one or more RADIUS server hosts.

SUMMARY STEPS

1. **show radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>show radius-server statistics <i>{hostname ipv4-address ipv6-address}</i></p> <p>Example:</p> <pre>switch# show radius-server statistics 10.10.1.1</pre>	Displays the RADIUS statistics.

Related Topics

[Configuring RADIUS Server Hosts](#), on page 6

[Clearing RADIUS Server Statistics](#), on page 25

Clearing RADIUS Server Statistics

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

Before you begin

Configure RADIUS servers on the Cisco NX-OS device.

SUMMARY STEPS

1. (Optional) **show radius-server statistics** *{hostname | ipv4-address | ipv6-address}*
2. **clear radius-server statistics** *{hostname | ipv4-address | ipv6-address}*

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>(Optional) show radius-server statistics <i>{hostname ipv4-address ipv6-address}</i></p> <p>Example:</p> <pre>switch# show radius-server statistics 10.10.1.1</pre>	Displays the RADIUS server statistics on the Cisco NX-OS device.
Step 2	<p>clear radius-server statistics <i>{hostname ipv4-address ipv6-address}</i></p> <p>Example:</p> <pre>switch# clear radius-server statistics 10.10.1.1</pre>	Clears the RADIUS server statistics.

Related Topics

[Configuring RADIUS Server Hosts](#), on page 6

Configuration Example for RADIUS

The following example shows how to configure RADIUS:

```
radius-server key 7 "ToIkLhPpG"
radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
aaa group server radius RadServer
    server 10.10.1.1
```

Where to Go Next

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

Additional References for RADIUS

This section describes additional information related to implementing RADIUS.

Related Documents

Related Topic	Document Title
Cisco NX-OS Licensing	<i>Cisco NX-OS Licensing Guide</i>
VRF configuration	<i>Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide</i>

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
MIBs related to RADIUS	To locate and download supported MIBs, go to the following URL: ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html