R Commands

This chapter describes the Cisco Nexus 1000V commands that begin with the letter R.

radius-server deadtime

To configure the dead-time interval for all Remote Access Dial-In User Service (RADIUS) servers used by a device, use the **radius-server deadtime** command. To revert to the default, use the **no** form of this command.

radius-server deadtime *minutes*

no radius-server deadtime *minutes*

Syntax Description

minutes	Number of minutes for the dead-time interval. The range is from 1 to 1440 minutes.

Defaults

0 minutes

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Usage Guidelines

The dead-time interval is the number of minutes before the device checks a RADIUS server that was previously unresponsive.

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

Examples

This example shows how to configure the global dead-time interval for all RADIUS servers to perform periodic monitoring:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# radius-server deadtime 5
```

This example shows how to revert to the default for the global dead-time interval for all RADIUS servers and disable periodic server monitoring:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# no radius-server deadtime 5
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server directed-request

To allow users to send authentication requests to a specific Remote Access Dial-In User Service (RADIUS) server when logging in, use the **radius-server directed request** command. To revert to the default, use the **no** form of this command.

radius-server directed-request

no radius-server directed-request

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Usage Guidelines

You can specify the *username@vrfname:hostname* during login, where *vrfname* is the virtual routing and forwarding (VRF) instance to use and *hostname* is the name of a configured RADIUS server. The username is sent to the RADIUS server for authentication.

Examples

This example shows how to allow users to send authentication requests to a specific RADIUS server when logging in:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# radius-server directed-request
```

This example shows how to disallow users to send authentication requests to a specific RADIUS server when logging in:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# no radius-server directed-request
```

Related Commands

Command	Description
show radius-server directed-request	Displays the directed request RADIUS server configuration.

radius-server host

To configure Remote Access Dial-In User Service (RADIUS) server parameters, use the **radius-server host** command. To revert to the default, use the **no** form of this command.

radius-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

no radius-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

Syntax Description

hostname	RADIUS server Domain Name Server (DNS) name. The name is alphanumeric, case-sensitive, and has a maximum of 256 characters.
ipv4-address	RADIUS server IPv4 address in the *A.B.C.D* format.
ipv6-address	RADIUS server IPv6 address in the *X:X:X::X* format.
key	(Optional) Configures the RADIUS server preshared secret key.
0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the RADIUS client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the RADIUS client and server.
shared-secret	Preshared key to authenticate communication between the RADIUS client and server. The preshared key can include any printable ASCII characters (white spaces are not allowed), is case-sensitive and can be up to 28 characters.
pac	(Optional) Enables the generation of Protected Access Credentials (PAC) on the RADIUS Cisco Access Control Server (ACS).
accounting	(Optional) Configures accounting.
acct-port	(Optional) Configures the RADIUS server port for accounting.
port-number	Port number. The range is from 0 to 65535.
auth-port	(Optional) Configures the RADIUS server port for authentication.
authentication	(Optional) Configures authentication.
retransmit	(Optional) Configures the number of times that the device tries to connect to a RADIUS server(s) before reverting to local authentication.
count	Number of times a device tries to connect to a RADIUS server. The range is from 1 to 5 times and the default is 1 time.
test	(Optional) Configures parameters to send test packets to the RADIUS server.
idle-time	Specifies the time interval (in minutes) for monitoring the server.
time	Time interval (in minutes) for monitoring the server. The range is from 1 to 1440 minutes.

password	Specifies a user password in the test packets.
password	User *password* in the test packets. The *password* is alphanumeric, case-sensitive, and has a maximum of 32 characters.
username	Specifies a username in the test packets.
name	Username in the test packets. The *name* is alphanumeric, not case-sensitive and can be up to 28 characters.
timeout	Specifies the timeout (in seconds) between retransmissions to the RADIUS server. The default is 5 seconds and the range is from 1 to 60 seconds.
seconds	Timeout (in seconds) between retransmissions to the RADIUS server. The default is 5 seconds and the range is from 1 to 60 seconds.

Defaults

Parameter	Default
Accounting port	1813
Authentication port	1812
Accounting	Enabled
Authentication	Enabled
Retransmission count	1
Idle-time	None
Server monitoring	Disabled
Timeout	5 seconds
Test username	test
Test password	test

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Usage Guidelines

When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

Examples

This example shows how to configure RADIUS server authentication and accounting parameters:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# radius-server host 10.10.2.3 key HostKey
n1000v(config)# radius-server host 10.10.2.3 auth-port 2003
n1000v(config)# radius-server host 10.10.2.3 acct-port 2004
```

```
n1000v(config)# radius-server host 10.10.2.3 accounting
n1000v(config)# radius-server host radius2 key 0 abcd
n1000v(config)# radius-server host radius3 key 7 1234
n1000v(config)# radius-server host 10.10.2.3 test idle-time 10
n1000v(config)# radius-server host 10.10.2.3 test username tester
n1000v(config)# radius-server host 10.10.2.3 test password 2B9ka5
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server key

To configure a Remote Access Dial-In User Service (RADIUS) shared secret key, use the **radius-server key** command. To remove a configured shared secret, use the **no** form of this command.

radius-server key [**0** | **7**] *shared-secret*

no radius-server key [**0** | **7**] *shared-secret*

Syntax Description

0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the RADIUS client and server.
7	(Optional) Configures a preshared key specified in encrypted text to authenticate communication between the RADIUS client and server.
shared-secret	Preshared key used to authenticate communication between the RADIUS client and server. The preshared key can include any printable ASCII characters (white spaces are not allowed), is case-sensitive and can be up to 28 characters.

Defaults

Clear text

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Usage Guidelines

You must configure the RADIUS preshared key to authenticate the switch on the RADIUS server. The length of the key is restricted to 63 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all RADIUS server configurations on the switch. You can override a global key assignment for an individual host by using the **key** keyword in the **radius-server host** command.

Examples

This example shows how to provide various scenarios to configure RADIUS authentication:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# radius-server key AnyWord
n1000v(config)# radius-server key 0 AnyWord
n1000v(config)# radius-server key 7 public pac
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server retransmit

To specify the number of times that the device should try a request with a Remote Access Dial-In User Service (RADIUS) server, use the **radius-server retransmit** command. To revert to the default, use the **no** form of this command.

radius-server retransmit *count*

no radius-server retransmit *count*

Syntax Description

count	Number of times that the device tries to connect to a RADIUS server(s) before reverting to local authentication. The range is from 1 to 5 times.

Defaults

1 retransmission

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Examples

This example shows how to configure the number of retransmissions to RADIUS servers:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# radius-server retransmit 3
```

This example shows how to revert to the default number of retransmissions to RADIUS servers:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# no radius-server retransmit 3
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server timeout

To specify the time between retransmissions to the Remote Access Dial-In User Service (RADIUS) servers, use the **radius-server timeout** command. To revert to the default, use the **no** form of this command.

radius-server timeout *seconds*

no radius-server timeout *seconds*

Syntax Description

seconds	Number of seconds between retransmissions to the RADIUS server. The range is from 1 to 60 seconds.

Defaults

5 seconds

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Examples

This example shows how to configure the timeout interval:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# radius-server timeout 30
```

This example shows how to revert to the default interval:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# no radius-server timeout 30
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

record

To configure a NetFlow flow record, use the **record** command. To remove the flow record configuration, use the **no** form of this command.

record {*name* | **netflow ipv4** {**original-input** | **original-output** | **netflow protocol-port**} | **netflow-original**}

no record {*name* | **netflow ipv4** {**original-input** | **original-output** | **netflow protocol-port**} | **netflow-original**}

Syntax Description

name	NetFlow flow record name. The name is alphanumeric, case-sensitive, and has a maximum of 63 characters.
netflow ipv4	Specifies a predefined NetFlow flow record that uses traditional IPv4 NetFlow collection schemes.
original-input	Specifies a predefined NetFlow flow record that uses traditional IPv4 input.
original-output	Specifies a predefined NetFlow flow record that uses traditional IPv4 output.
netflow protocol-port	Specifies the NetFlow flow record that uses the protocol and ports aggregation scheme.
netflow-original	Specifies a NetFlow flow record that uses traditional IPv4 input with origin ASs.

Defaults

None

Command Modes

Flow monitor configuration (config-flow-monitor)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Usage Guidelines

A flow record defines the information that NetFlow gathers, such as packets in the flow and the types of counters gathered per flow. You can define new flow records or use the predefined flow record.

Examples

This example shows how to configure a flow record to use the predefined traditional IPv4 input NetFlow record:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# flow monitor testmon
```

```
n1000v(config-flow-monitor)# record netflow ipv4 original-input
n1000v(config-flow-monitor)#
```

This example shows how to remove the predefined traditional IPv4 input NetFlow flow record configuration:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# flow monitor testmon
n1000v(config-flow-monitor)# no record netflow ipv4 original-input
n1000v(config-flow-monitor)#
```

Related Commands

Command	Description
show flow monitor	Displays NetFlow monitor configuration information.
show flow record	Displays NetFlow record configuration information.

reload

To reboot both the primary and secondary Virtual Supervisor Modules (VSMs) in a redundant pair, use the **reload** command.

reload

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Usage Guidelines

To reboot only one of the VSMs in a redundant pair, use the **reload module** command instead.

Before reloading, use the **copy running-configuration to startup-configuration** command to preserve any configuration changes made since the previous reboot or restart.

After reloading it, you must manually restart the VSM.

Examples

This example shows how to reload both the primary and secondary VSM:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# reload
!!!WARNING! there is unsaved configuration!!!
This command will reboot the system. (y/n)?  [n] y
2010 Sep  3 11:33:35 bl-n1000v %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from
command-line interface
```

Related Commands

Command	Description
reload module	Reloads the specified VSM (1 or 2) in a redundant pair.

reload module

To reload one of the Virtual Supervisor Modules (VSMs) in a redundant pair, use the **reload module** command.

reload module *module* [**force-dnld**]

Syntax Description

module	Module number: • 1 (primary VSM) • 2 (secondary VSM)
force-dnld	(Optional) Reboots the specified module to force NetBoot and image download.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Usage Guidelines

To reboot both the VSMs in a redundant pair, use the **reload** command instead.

Before reloading, use the **copy running-configuration to startup-configuration** command to preserve any configuration changes made since the previous reboot or restart.

After reloading it, you must manually restart the VSM.

Examples

This example shows how to reload VSM 2, the secondary VSM in a redundant pair:

```
n1000v# reload module 2
!!!WARNING! there is unsaved configuration!!!
This command will reboot the system. (y/n)?  [n] y
2010 Sep  3 11:33:35 bl-n1000v %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from
command-line interface
```

Related Commands

Command	Description
reload	Reboots both the primary and secondary VSM.
show version	Displays information about the software version.

resequence

To resequence a list with sequence numbers, use the **resequence** command.

resequence {{{**ip** | **mac**} **access-list**} | **time-range**} [*name number increment*]

Syntax Description

ip	Specifies resequencing of an IP access list.
mac	Specifies resequencing of a MAC access list.
access-list	Specifies resequencing of an access list.
time-range	Specifies resequencing of a time range.
name	(Optional) List name. The name is alphanumeric, case-sensitive and can be up to 28 characters.
number	(Optional) Starting sequence number. The range is from 1 to 4294967295.
increment	(Optional) Step to increment the sequence number. The range is from 1 to 4294967295.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Examples

This example shows how to resequence the first entry in the MAC ACL named aclOne:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# resequence mac access-list aclOne 1 2
n1000v(config)#
```

Related Commands

Command	Description
show access-list	Displays ACLs.

rmdir

To remove a directory, use the **rmdir** command.

rmdir [*filesystem***:** [*//module/*]] *directory*

Syntax Description

*filesystem***:**	(Optional) File system name. The name is case-sensitive and can be up to 28 characters.
//module/	(Optional) Supervisor module identifier. Values are **sup-active**, **sup-local**, **sup-remote**, or **sup-standby**. The identifiers are case-sensitive and can be up to 28 characters.
directory	Directory name. The name is case-sensitive and can be up to 28 characters.

Defaults

Removes the directory from the current working directory.

Command Modes

Any

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Examples

This example shows how to remove the my_files directory:

```
n1000v# rmdir my_files
```

Related Commands

Command	Description
cd	Changes the current working directory.
dir	Displays the directory contents.
pwd	Displays the name of the current working directory.

role

To create a feature group or user role, use the **role** command. To remove the role, use the **no** form of this command.

role {**feature-group** *group-name* | **name** *name*}

no role {**feature-group** *group-name* | **name** *name*}

Syntax Description

feature-group	Configures the feature group role.
group-name	Feature group name. The name is alphanumeric, case-sensitive, and has a maximum of 32 characters.
name	Specifies a ole name.
name	User role. The name is alphanumeric, case-sensitive, and has a maximum of 16 characters.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Examples

This example shows how to create a role named UserA:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# role name UserA
```

This example shows how to remove the UserA role:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# no role UserA
```

Related Commands

Command	Description
interface policy	Denies users assigned to this role access to all interfaces unless specifically permitted.
permit interface	Specifies the interface(s) that users assigned to this role can access.

Command	Description
permit vlan	Specifies the VLAN(s) that users assigned to this role can access.
show role	Displays the available user roles and their rules.
vlan policy	Denies users assigned to this role access to all VLANs unless specifically permitted.

rule

To create a rule that defines criteria for a user role, use the **rule** command. To remove a rule, use the **no** form of this command.

rule *number* {**deny** | **permit**} {**read** | **read-write** [**feature** *feature-name* | **feature-group** *group-name*] | **command** *command-name*}

no rule *number*

Syntax Description

number	Rule number. The range is from 1 to 256.
deny	Indicates that the user is denied the ability to perform a function.
permit	Indicates that the user is permitted to perform a function.
read	Specifies whether the assigned user has read access.
read-write	Specifies whether the assigned user has read-write access.
feature	(Optional) Specifies a feature for the rule.
feature-name	Feature name, such as syslog or TACACS+, whose access can be defined in this rule.
feature-group	(Optional) Specifies a feature type.
group-name	Group of features whose access can be defined in a rule.
command	Specifies a command for this rule.
command-name	Command, or group of commands collected in a regular expression, whose access can be defined in a rule.

Defaults

None

Command Modes

Role configuration (config-role)

SupportedUserRoles

network-admin

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Usage Guidelines

The *rule number* specifies the order in which the rule is applied, in descending order. For example, if a role has three rules, rule 3 is applied first, rule 2 is applied next, and rule 1 is applied last. You can configure up to 256 rules for each role.

Examples

This example shows how to create a rule that denies access to the **clear users** command:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# role name UserA
n1000v(config-role)# rule 1 deny command clear users
n1000v(config-role)#
```

This example shows how to remove the rule 1 configuration:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# role name UserA
n1000v(config-role)# no rule 1
```

Related Commands

Command	Description
show role	Displays the user role configuration.
username	Configures information about the user.

run-script

To run a command script that is saved in a file, use the **run-script** command.

run-script {**bootflash:** | **volatile:**} *filename*

Syntax Description

bootflash:	Indicates that the file that contains the command script is located in the Bootflash file system.
volatile:	Indicates that the file that contains the command script is located in the Volatile file system.
filename	Filename that contains the command script. The filename is alphanumeric, case-sensitive and can be up to 28 characters.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin
network-operator

Command History

Release	Modification
5.2(1)SK1(1.1)	This command was introduced.

Examples

This example shows how to run a command script that is saved in the Sample file on the Volatile file system:

```
n1000v# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
n1000v(config)# run-script volatile:Sample
n1000v(config)#
```

Related Commands

Command	Description
cd	Changes the current working directory.
copy	Copies files.
dir	Displays the contents of the working directory.
pwd	Displays the name of the present working directory (pwd).