R Commands

This chapter describes the Cisco NX-OS security commands that begin with R.

radius-server deadtime

To configure the dead-time interval for all RADIUS servers on a Cisco Nexus 5000 Series switch, 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.

Command Default

0 minutes

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

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

Note 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:

```
switch(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:

```
switch(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 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.

Command Default

Sends the authentication request to the configured RADIUS server group.

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

You can specify the *username@vrfname*:*hostname* during login, where *vrfname* is the VRF 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:

```
switch(config)# radius-server directed-request
```

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

```
switch(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 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 has a maximum of 63 characters.
pac	(Optional) Enables the generation of Protected Access Credentials on the RADIUS Cisco ACS server for use with Cisco TrustSec.
accounting	(Optional) Configures accounting.
acct-port *port-number*	(Optional) Configures the RADIUS server port for accounting. The range is from 0 to 65535.
auth-port *port-number*	(Optional) Configures the RADIUS server port for authentication. The range is from 0 to 65535.
authentication	(Optional) Configures authentication.
retransmit *count*	(Optional) Configures the number of times that the switch tries to connect to a RADIUS server before reverting to local authentication. 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 *time*	Specifies the time interval (in minutes) for monitoring the server. The range is from 1 to 1440 minutes.
password *password*	Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.

username *name*	Specifies a username in the test packets. The is alphanumeric, not case sensitive, and has a maximum of 32 characters.
timeout *seconds*	Specifies the timeout (in seconds) between retransmissions to the RADIUS server. The default is 1 second and the range is from 1 to 60 seconds.

Command Default

Accounting port: 1813
Authentication port: 1812
Accounting: enabled
Authentication: enabled
Retransmission count: 1
Idle-time: 0
Server monitoring: disabled
Timeout: 5 seconds
Test username: test
Test password: test

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(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:

```
switch(config)# radius-server host 192.168.2.3 key HostKey
switch(config)# radius-server host 192.168.2.3 auth-port 2003
switch(config)# radius-server host 192.168.2.3 acct-port 2004
switch(config)# radius-server host 192.168.2.3 accounting
switch(config)# radius-server host radius2 key 0 abcd
switch(config)# radius-server host radius3 key 7 1234
switch(config)# radius-server host 192.168.2.3 test idle-time 10
switch(config)# radius-server host 192.168.2.3 test username tester
switch(config)# radius-server host 192.168.2.3 test password 2B9ka5
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server key

To configure a 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 has a maximum of 63 characters.

Command Default

Clear text authentication

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

You must configure the RADIUS preshared key to authenticate the switch to the RADIUS server. The length of the key is restricted to 65 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 this global key assignment by using the **key** keyword in the **radius-server host** command.

Examples

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

```
switch(config)# radius-server key AnyWord
switch(config)# radius-server key 0 AnyWord
switch(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 switch should try a request with a 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 switch tries to connect to a RADIUS server before reverting to local authentication. The range is from 1 to 5 times.

Command Default

1 retransmission

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

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

```
switch(config)# radius-server retransmit 3
```

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

```
switch(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 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.

Command Default

1 second

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to configure the timeout interval:

```
switch(config)# radius-server timeout 30
```

This example shows how to revert to the default interval:

```
switch(config)# no radius-server timeout 30
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

remark

To enter a comment into an IPv4 or MAC access control list (ACL), use the **remark** command. To remove a remark command, use the **no** form of this command.

[*sequence-number*] **remark** *remark*

no {*sequence-number* | **remark** *remark*}

Syntax Description

sequence-number	(Optional) Sequence number of the **remark** command, which causes the switch to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the switch adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. Use the **resequence** command to reassign sequence numbers to remarks and rules.
remark	Text of the remark. This argument can be up to 100 characters.

Command Default

No ACL contains a remark by default.

Command Modes

IPv4 ACL configuration mode
MAC ACL configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

The *remark* argument can be up to 100 characters. If you enter more than 100 characters for the *remark* argument, the switch accepts the first 100 characters and drops any additional characters.

Examples

This example shows how to create a remark in an IPv4 ACL and display the results:

```
switch(config)# ip access-list acl-ipv4-01
switch(config-acl)# 100 remark this ACL denies the marketing department access to the lab
switch(config-acl)# show access-list acl-ipv4-01
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
mac access-list	Configures a MAC ACL.
show access-list	Displays all ACLs or one ACL.

resequence

To reassign sequence numbers to all rules in an access control list (ACL) or a time range, use the **resequence** command.

resequence [**ip** | **ipv6** | **mac**] **access-list** *access-list-name starting-number increment*

resequence time-range *time-range-name starting-number increment*

Syntax Description

ip **ipv6** **mac**	Type of the ACL.
access-list *access-list-name*	Specifies the name of the ACL.
time-range *time-range-name*	Specifies the name of the time range.
starting-number	Sequence number for the first rule in the ACL or time range.
increment	Number that the switch adds to each subsequent sequence number.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

The **resequence** command allows you to reassign sequence numbers to the rules of an ACL or time range. The new sequence number for the first rule is determined by the *starting-number* argument. Each additional rule receives a new sequence number determined by the *increment* argument. If the highest sequence number would exceed the maximum possible sequence number, then no sequencing occurs and the following message appears:

```
ERROR: Exceeded maximum sequence number.
```

The maximum sequence number is 4294967295.

Examples

This example shows how to resequence an IPv4 ACL named ip-acl-01 with a starting sequence number of 100 and an increment of 10, using the **show ip access-lists** command to verify sequence numbering before and after the use of the **resequence** command:

```
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
```

```
        7 permit tcp 128.0.0/16 any eq www
        10 permit udp 128.0.0/16 any
        13 permit icmp 128.0.0/16 any eq echo
        17 deny igmp any any
switch(config)# resequence ip access-list ip-acl-01 100 10
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
        100 permit tcp 128.0.0/16 any eq www
        110 permit udp 128.0.0/16 any
        120 permit icmp 128.0.0/16 any eq echo
        130 deny igmp any any
switch(config)#
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
ipv6 access-list	Configures an IPv6 ACL.
mac access-list	Configures a MAC ACL.
show access-lists	Displays all ACLs or a specific ACL.

role feature-group name

To create or specify a user role feature group and enter user role feature group configuration mode, use the **role feature-group name** command. To delete a user role feature group, use the **no** form of this command.

role feature-group name *group-name*

no role feature-group name *group-name*

Syntax Description

group-name	User role feature group name. The *group-name* has a maximum length of 32 characters and is a case-sensitive, alphanumeric character string.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Examples

This example shows how to create a user role feature group and enter user role feature group configuration mode:

```
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)#
```

This example shows how to remove a user role feature group:

```
switch(config)# no role feature-group name MyGroup
switch(config)#
```

Related Commands

Command	Description
feature-group name	Specifies or creates a user role feature group and enters user role feature group configuration mode.
show role feature-group	Displays the user role feature groups.

role name

To create or specify a user role and enter user role configuration mode, use the **role name** command. To delete a user role, use the **no** form of this command.

role name {*role-name* | **default-role** | *privilege-role*}

no role name {*role-name* | **default-role** | *privilege-role*}

Syntax Description

role-name	User role name. The *role-name* has a maximum length of 16 characters and is a case-sensitive, alphanumeric character string.
default-role	Specifies the default user role name.
privilege-role	Privilege user role, which can be one of the following: • priv-0 • priv-1 • priv-2 • priv-3 • priv-4 • priv-5 • priv-6 • priv-7 • priv-8 • priv-9 • priv-10 • priv-11 • priv-12 • priv-13

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

A Cisco Nexus 5000 Series switch provides the following default user roles:

- Network Administrator—Complete read-and-write access to the entire switch
- Complete read access to the entire switch

You cannot change or remove the default user roles.

To view the privilege level roles, you must enable the cumulative privilege of roles for command authorization on TACACS+ servers using the **feature privilege** command. Privilege roles inherit the permissions of lower level privilege roles.

Examples

This example shows how to create a user role and enter user role configuration mode:

```
switch(config)# role name MyRole
switch(config-role)#
```

This example shows how to create a privilege 1 user role and enter user role configuration mode:

```
switch(config)# role name priv-1
switch(config-role)#
```

This example shows how to remove a user role:

```
switch(config)# no role name MyRole
```

Related Commands

Command	Description
feature privilege	Enables cumulative privilege of roles for command authorization on TACACS+ servers.
rule	Configures rules for user roles.
show role	Displays the user roles.

rollback running-config

To rollback a running configuration, use the **rollback running-config** command.

rollback running-config {**checkpoint** *checkpoint-name* | **file** {**bootflash:** | **volatile:**}[*//server*][*directory/*][*filename*] [**atomic**] [**verbose**]}

Syntax Description

checkpoint	Specifies that the running configuration be rolled back to the checkpoint.
checkpoint-name	Checkpoint name. The name can be a maximum of 32 characters.
file	Specifies that the running configuration be rolled back to the configuration file.
bootflash:	Specifies the bootflash local writable storage file system.
volatile:	Specifies the volatile local writable storage file system.
//server	Name of the server. Valid values are **///**, **//module-1/**, **//sup-1/**, **//sup-active/**, or **//sup-local/**. The double slash (//) is required.
directory/	Name of a directory. The directory name is case sensitive.
filename	Name of the checkpoint configuration file. The filename is case sensitive.
atomic	(Optional) Specifies that the rollback execution is to stop when the first failure occurs while applying the patch. This is the default mode.
verbose	(Optional) Specifies that the roll back execution steps be displayed during a rollback operation.

Note There can be no spaces in the *filesystem*://*server*/*directory*/*filename* string. Individual elements of this string are separated by colons (:) and slashes (/).

Command Default

Atomic rollback

Command Modes

EXEC mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

You can roll back to a checkpoint name or file. Before you roll back, you can view the differences between the source and destination checkpoints that reference the current or saved configurations using the **show diff rollback-patch** command.

A rollback to a specified checkpoint restores the active configuration of the system to the checkpointed configuration.

A rollback to files on bootflash is supported only on files that are created using the **checkpoint** *checkpoint_name* command and not on any other type of ASCII file.

Note If you make a configuration change during an atomic rollback, the rollback will fail. You must manually correct the error and then run the **rollback** command.

Examples

This example shows how to roll back the running configuration to a checkpoint, named chkpnt-1, in verbose mode:

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration--->
switch# checkpoint chkpnt-2
<-- modify configuration in running configuration--->
switch# rollback running-config chkpnt-1 verbose
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
Generating Rollback patch for switch profile
Rollback Patch is Empty
Collecting Running-Config
#Generating Rollback Patch
Rollback Patch is Empty

Rollback completed successfully.

switch#
```

This example shows how to roll back the running configuration to a checkpoint configuration file named chkpnt_configSep9-1.txt in the bootflash storage system:

```
switch# checkpoint chkpnt-1
<-- modify configuration in running configuration--->
switch# checkpoint file bootflash:///chkpnt_configSep9-1.txt
<-- modify configuration in running configuration--->
switch# checkpoint file bootflash:///chkpnt_configSep9-2.txt
<-- modify configuration in running configuration--->
switch# checkpoint chkpnt-2
switch# rollback running-config file bootflash:///chkpnt_configSep9-1.txt
switch#
```

Related Commands

Command	Description
rollback	Rolls back the switch to any of the saved checkpoints.
show checkpoint	Displays checkpoint information.
show diff rollback-patch checkpoint	Displays the differences between current checkpoint and saved configuration.
show diff rollback-patch file	Displays the differences between the current checkpoint file and the saved configuration.
show diff rollback-patch running-config	Displays the differences between the current running configuration and the saved checkpoint configuration.

rule

To configure rules for a user role, use the **rule** command. To delete a rule, use the **no** form of this command.

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

no rule *number*

Syntax Description

number	Sequence number for the rule. The switch applies the rule with the highest value first and then the rest in descending order.
deny	Denies access to commands or features.
permit	Permits access to commands or features.
command *command-string*	Specifies a command string. The command string can be a maximum of 128 characters and can contain spaces.
read	Specifies read access.
read-write	Specifies read and write access.
feature *feature-name*	(Optional) Specifies a feature name. Use the **show role feature** command to list the switch feature names.
feature-group *group-name*	(Optional) Specifies a feature group.

Command Default

None

Command Modes

User role configuration mode

Command History

Release	Modification
5.2(1)N1(1)	This command was introduced.

Usage Guidelines

You can configure up to 256 rules for each role.

The rule number that you specify determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.

Deny rules cannot be added to any privilege roles, except the privilege 0 (priv-0) role.

Examples

This example shows how to add rules to a user role:

```
switch(config)# role name MyRole
switch(config-role)# rule 1 deny command clear users
switch(config-role)# rule 1 permit read-write feature-group L3
```

This example shows how to add rules to a user role with privilege 0:

```
switch(config)# role name priv-0
switch(config-role)# rule 1 deny command clear users
switch(config-role)#
```

This example shows how to remove a rule from a user role:

```
switch(config)# role MyRole
switch(config-role)# no rule 10
```

Related Commands

Command	Description
role name	Creates or specifies a user role name and enters user role configuration mode.
show role	Displays the user roles.