Send comments to nexus5k-docfeedback@cisco.com

S Commands

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

Send comments to nexus5k-docfeedback@cisco.com

server

To add a server to a RADIUS or TACACS+ server group, use the **server** command. To delete a server from a server group, use the **no** form of this command.

server {*ipv4-address* | *ipv6-address* | *hostname*}

no server {*ipv4-address* | *ipv6-address* | *hostname*}

Syntax Description

ipv4-address	Server IPv4 address in the *A.B.C.D* format.
ipv6-address	Server IPv6 address in the *X:X:X::X* format.
hostname	Server name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.

Command Default

None

Command Modes

RADIUS server group configuration mode
TACACS+ server group configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

You can configure up to 64 servers in a server group.

Use the **aaa group server radius** command to enter RADIUS server group configuration mode or **aaa group server tacacs+** command to enter TACACS+ server group configuration mode.

If the server is not found, use the **radius-server host** command or **tacacs-server host** command to configure the server.

Note You must use the **feature tacacs+** command before you configure TACACS+.

Examples

This example shows how to add a server to a RADIUS server group:

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 192.168.1.1
```

This example shows how to delete a server from a RADIUS server group:

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# no server 192.168.1.1
```

This example shows how to add a server to a TACACS+ server group:

```
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
```

Send comments to nexus5k-docfeedback@cisco.com

```
switch(config-tacacs+)# server 192.168.2.2
```

This example shows how to delete a server from a TACACS+ server group:

```
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no server 192.168.2.2
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
feature tacacs+	Enables TACACS+.
radius-server host	Configures a RADIUS server.
show radius-server groups	Displays RADIUS server group information.
show tacacs-server groups	Displays TACACS+ server group information.
tacacs-server host	Configures a TACACS+ server.

Send comments to nexus5k-docfeedback@cisco.com

ssh

To create a Secure Shell (SSH) session using IPv4, use the **ssh** command.

ssh [*username*@]{*ipv4-address* | *hostname*} [**vrf** {*vrf-name* | **default** | **management**}]

Syntax Description

username	(Optional) Username for the SSH session. The username is not case sensitive and has a maximum of 64 characters.
ipv4-address	IPv4 address of the remote host.
hostname	Hostname of the remote host. The hostname is case sensitive and has a maximum of 64 characters.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the SSH session. The name can be a maximum of 32 alphanumeric characters.
default	Specifies the default VRF.
management	Specifies the management VRF.

Command Default

Default VRF

Command Modes

EXEC mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The switch supports SSH version 2.

Examples

This example shows how to start an SSH session using IPv4:

```
switch# ssh 192.168.1.1 vrf management
```

Related Commands

Command	Description
clear ssh session	Clears SSH sessions.
ssh server enable	Enables the SSH server.
ssh6	Starts an SSH session using IPv6 addressing.

Send comments to nexus5k-docfeedback@cisco.com

ssh6

To create a Secure Shell (SSH) session using IPv6, use the **ssh6** command.

ssh6 [*username*@]{*ipv6-address* | *hostname*} [**vrf** {*vrf-name* | **default** | **management**}]

Syntax Description

username	(Optional) Username for the SSH session. The username is not case sensitive and has a maximum of 64 characters.
ipv6-address	IPv6 address of the remote host.
hostname	Hostname of the remote host. The hostname is case sensitive and has a maximum of 64 characters.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the SSH IPv6 session. The name can be a maximum of 32 alphanumeric characters.
default	Specifies the default VRF.
management	Specifies the management VRF.

Command Default

Default VRF

Command Modes

EXEC mode

Command History

Release	Modification
4.0(1a)N1(1)	This command was introduced.

Usage Guidelines

The switch supports SSH version 2.

Examples

This example shows how to start an SSH session using IPv6:

```
switch# ssh6 2001:0DB8::200C:417A vrf management
```

Related Commands

Command	Description
clear ssh session	Clears SSH sessions.
ssh	Starts an SSH session using IPv4 addressing.
ssh server enable	Enables the SSH server.

Send comments to nexus5k-docfeedback@cisco.com

ssh key

To create a Secure Shell (SSH) server key, use the **ssh key** command. To remove the SSH server key, use the **no** form of this command.

ssh key {**dsa** [**force**] | **rsa** [*length* [**force**]]}

no ssh key [**dsa** | **rsa**]

Syntax Description

dsa	Specifies the Digital System Algorithm (DSA) SSH server key.
force	(Optional) Forces the generation of a DSA SSH key even if previous ones are present.
rsa	Specifies the Rivest, Shamir, and Adelman (RSA) public-key cryptography SSH server key.
length	(Optional) Number of bits to use when creating the SSH server key. The range is from 768 to 2048.

Command Default

1024-bit length

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software supports SSH version 2.

If you want to remove or replace an SSH server key, you must first disable the SSH server using the **no ssh server enable** command.

Examples

This example shows how to create an SSH server key using RSA with the default key length:

```
switch(config)# ssh key rsa
```

This example shows how to create an SSH server key using RSA with a specified key length:

```
switch(config)# ssh key rsa 768
```

This example shows how to replace an SSH server key using DSA with the force option:

```
switch(config)# no ssh server enable
switch(config)# ssh key dsa force
switch(config)# ssh server enable
```

This example shows how to remove the DSA SSH server key:

```
switch(config)# no ssh server enable
switch(config)# no ssh key dsa
```

Send comments to nexus5k-docfeedback@cisco.com

```
switch(config)# ssh server enable
```

This example shows how to remove all SSH server keys:

```
switch(config)# no ssh server enable
switch(config)# no ssh key
switch(config)# ssh server enable
```

Related Commands

Command	Description
show ssh key	Displays the SSH server key information.
ssh server enable	Enables the SSH server.

Send comments to nexus5k-docfeedback@cisco.com

ssh login-attempts

To configure the maximum number of times that a user can attempt to log in to a Secure Shell (SSH) session, use the **ssh login-attempts** command. To disable the configuration, use the **no** form of this command.

ssh login-attempts *number*

no ssh login-attempts *number*

Syntax Description

number	Maximum number of login attempts. The range is from 1 to 10.

Command Default

3

Command Modes

Global configuration

SupportedUserRoles

network-admin

vdc-admin

Command History

Release	Modification
5.0(2)	This command was introduced

Usage Guidelines

The total number of login attempts includes attempts through public-key authentication, certificate-based authentication, and password-based authentication.

This command does not require a license.

If the user exceeds the maximum number of permitted login attempts, the session disconnects.

Examples

This example shows how to configure the maximum number of times that a user can attempt to log in to an SSH session:

```
switch# configure terminal
switch(config)# ssh login-attempts 5
```

This example shows how to disable the SSH login attempt configuration:

```
switch# configure terminal
switch(config)# no ssh login-attempts
```

Related Commands

Command	Description
show running-config security all	Displays the configured maximum number of SSH login attempts.

Send comments to nexus5k-docfeedback@cisco.com

ssh server enable

To enable the Secure Shell (SSH) server, use the **ssh server enable** command. To disable the SSH server, use the **no** form of this command.

ssh server enable

no ssh server enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

The switch supports SSH version 2.

Examples

This example shows how to enable the SSH server:

```
switch(config)# ssh server enable
```

This example shows how to disable the SSH server:

```
switch(config)# no ssh server enable
```

Related Commands

Command	Description
show ssh server	Displays the SSH server key information.

Send comments to nexus5k-docfeedback@cisco.com

storm-control level

To set the suppression level for traffic storm control, use the **storm-control level** command. To turn off the suppression mode or revert to the default, use the **no** form of this command.

storm-control {**broadcast** | **multicast** | **unicast**} **level** *percentage*[.*fraction*]

no storm-control {**broadcast** | **multicast** | **unicast**} **level**

Syntax Description

broadcast	Specifies the broadcast traffic.
multicast	Specifies the multicast traffic.
unicast	Specifies the unicast traffic.
level *percentage*	Specifies the percentage of the suppression level. The range is from 0 to 100 percent.
fraction	(Optional) Fraction of the suppression level. The range is from 0 to 99.

Command Default

All packets are passed.

Command Modes

Interface configuration mode

Command History

Release	Modification
4.0(0)N1(1a)	This command was introduced.

Usage Guidelines

Enter the **storm-control level** command to enable traffic storm control on the interface, configure the traffic storm-control level, and apply the traffic storm-control level to all traffic storm-control modes that are enabled on the interface.

The period (.) is required when you enter the fractional-suppression level.

The suppression level is a percentage of the total bandwidth. A threshold value of 100 percent means that no limit is placed on traffic. A threshold value of 0 or 0.0 (fractional) percent means that all specified traffic is blocked on a port.

Use the **show interfaces counters storm-control** command to display the discard count.

Use one of the following methods to turn off suppression for the specified traffic type:

- Set the level to 100 percent for the specified traffic type.
- Use the **no** form of this command.

Examples

This example shows how to enable suppression of broadcast traffic and set the suppression threshold level:

```
switch(config-if)# storm-control broadcast level 30
```

Send comments to nexus5k-docfeedback@cisco.com

This example shows how to disable the suppression mode for multicast traffic:

```
switch(config-if)# no storm-control multicast level
```

Related Commands

Command	Description
show interface	Displays the storm-control suppression counters for an interface.
show running-config	Displays the configuration of the interface.

Send comments to nexus5k-docfeedback@cisco.com