T Commands

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

tacacs+ abort

To discard a TACACS+ Cisco Fabric Services (CFS) distribution session in progress, use the **tacacs+ abort** command in configuration mode.

tacacs+ abort

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Global configuration

SupportedUserRoles network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines To use this command, TACACS+ must be enabled using the **feature tacacs+** command.

This command does not require a license.

Examples

This example shows how to discard a TACACS+ CFS distribution session in progress:

```
switch# config terminal
switch(config)# tacacs+ abort
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show tacacs+	Displays TACACS+ CFS distribution status and other details.
tacacs+ distribute	Enables CFS distribution for TACACS+.

tacacs+ commit

To apply the pending configuration pertaining to the TACACS+ Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **tacacs+ commit** command in configuration mode.

tacacs+ commit

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin
VDC user

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

To use this command, TACACS+ must be enabled using the **feature tacacs+** command.

Before committing the TACACS+ configuration to the fabric, all switches in the fabric must have distribution enabled using the **tacacs+ distribute** command.

CFS does not distribute the TACACS+ server group configurations, periodic TACACS+ server testing configurations, or server and global keys. The keys are unique to the Cisco NX-OS device and are not shared with other Cisco NX-OS devices.

This command does not require a license.

Examples

This example shows how to apply a TACACS+ configuration to the switches in the fabric.

```
switch# config terminal
switch(config)# tacacs+ commit
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show tacacs+	Displays TACACS+ CFS distribution status and other details.
tacacs+ distribute	Enables CFS distribution for TACACS+.

tacacs+ distribute

To enable Cisco Fabric Services (CFS) distribution for TACACS+, use the **tacacs+ distribute** command. To disable this feature, use the **no** form of the command.

tacacs+ distribute

no tacacs+ distribute

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin
VDC user

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

To use this command, TACACS+ must be enabled using the **feature tacacs+** command.

CFS does not distribute the TACACS+ server group configurations, periodic TACACS+ server testing configurations, or server and global keys. The keys are unique to the Cisco NX-OS device and are not shared with other Cisco NX-OS devices.

This command does not require a license.

Examples

This example shows how to enable TACACS+ fabric distribution:

```
switch# config terminal
switch(config)# tacacs+ distribute
```

Related Commands

Command	Description
feature tacacs+	Enables TACACS+.
show tacacs+	Displays TACACS+ CFS distribution status and other details.

tacacs-server deadtime

To set a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness, use the **tacacs-server deadtime** command. To disable the monitoring of the nonresponsive TACACS+ server, use the **no** form of this command.

tacacs-server deadtime *minutes*

no tacacs-server deadtime *minutes*

Syntax Description

time	Specifies the time interval in minutes. The range is from 1 to 1440.

Defaults

0 minutes

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Setting the time interval to zero disables the timer. If the dead-time interval for an individual TACACS+ server is greater than zero (0), that value takes precedence over the value set for the server group.

When the dead-time interval is 0 minutes, TACACS+ server monitoring is not performed unless the TACACS+ server is part of a server group and the dead-time interval for the group is greater than 0 minutes.

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

This command does not require a license.

Examples

This example shows how to configure the dead-time interval and enable periodic monitoring:

```
switch# configure terminal
switch(config)# tacacs-server deadtime 10
```

This example shows how to revert to the default dead-time interval and disable periodic monitoring:

```
switch# configure terminal
switch(config)# no tacacs-server deadtime 10
```

Related Commands

Command	Description
deadtime	Sets a dead-time interval for monitoring a nonresponsive TACACS+ server.
show tacacs-server	Displays TACACS+ server information.
feature tacacs+	Enables TACACS+.

tacacs-server directed-request

To allow users to send authentication requests to a specific TACACS+ server when logging in, use the **radius-server directed request** command. To revert to the default, use the **no** form of this command.

tacacs-server directed-request

no tacacs-server directed-request

Syntax Description

This command has no arguments or keywords.

Defaults

Sends the authentication request to the configured TACACS+ server groups

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

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

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.

This command does not require a license.

Examples

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

```
switch# configure terminal
switch(config)# tacacs-server directed-request
```

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

```
switch# configure terminal
switch(config)# no tacacs-server directed-request
```

Related Commands

Command	Description
show tacacs-server directed request	Displays a directed request TACACS+ server configuration.
feature tacacs+	Enables TACACS+.

tacacs-server host

To configure TACACS+ server host parameters, use the **tacacs-server host** command in configuration mode. To revert to the defaults, use the **no** form of this command.

tacacs-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret*] [**port** *port-number*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds*]

no tacacs-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret*] [**port** *port-number*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds*]

Syntax Description

hostname	TACACS+ server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
ipv4-address	TACACS+ server IPv4 address in the *A.B.C.D* format.
ipv6-address	TACACS+ server IPv6 address in the *X*:*X*:*X*::*X* format.
key	(Optional) Configures the TACACS+ server's shared secret key.
0	(Optional) Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the TACACS+ 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 TACACS+ client and server.
shared-secret	Preshared key to authenticate communication between the TACACS+ client and server. The preshared key is alphanumeric, case sensitive, and has a maximum of 63 characters.
port *port-number*	(Optional) Configures a TACACS+ server port for authentication. The range is from 1 to 65535.
test	(Optional) Configures parameters to send test packets to the TACACS+ server.
idle-time *time*	(Optional) Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.
password *password*	(Optional) Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.
username *name*	(Optional) Specifies a user name in the test packets. The username is alphanumeric, case sensitive, and has a maximum of 32 characters.
timeout *seconds*	(Optional) Configures a TACACS+ server timeout period (in seconds) between retransmissions to the TACACS+ server. The range is from 1 to 60 seconds.

Defaults

Idle time: disabled

Server monitoring: disabled

Timeout: 1 second.

Test username: test

Test password: test

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

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

This command does not require a license.

Examples

This example shows how to configure TACACS+ server host parameters:

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.2.3 key HostKey
switch(config)# tacacs-server host tacacs2 key 0 abcd
switch(config)# tacacs-server host tacacs3 key 7 1234
switch(config)# tacacs-server host 10.10.2.3 test idle-time 10
switch(config)# tacacs-server host 10.10.2.3 test username tester
switch(config)# tacacs-server host 10.10.2.3 test password 2B9ka5
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
feature tacacs+	Enables TACACS+.

tacacs-server key

To configure a global TACACS+ shared secret key, use the **tacacs-server key** command. To removed a configured shared secret, use the **no** form of this command.

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

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

Syntax Description

0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the TACACS+ client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text to authenticate communication between the TACACS+ client and server.
shared-secret	Preshared key to authenticate communication between the TACACS+ client and server. The preshared key is alphanumeric, case sensitive, and has a maximum of 63 characters.

Defaults

None

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must configure the TACACS+ preshared key to authenticate the device to the TACACS+ 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 TACACS+ server configurations on the device. You can override this global key assignment by using the **key** keyword in the **tacacs-server host** command.

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

This command does not require a license.

Examples

The following example shows how to configure TACACS+ server shared keys:

```
switch# configure terminal
switch(config)# tacacs-server key AnyWord
switch(config)# tacacs-server key 0 AnyWord
switch(config)# tacacs-server key 7 public
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
feature tacacs+	Enables TACACS+.

tacacs-server timeout

To specify the time between retransmissions to the TACACS+ servers, use the **tacacs-server timeout** command. To revert to the default, use the **no** form of this command.

tacacs-server timeout *seconds*

no tacacs-server timeout *seconds*

Syntax Description

seconds	Seconds between retransmissions to the TACACS+ server. The range is from 1 to 60 seconds.

Defaults

1 second

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

This command does not require a license.

Examples

This example shows how to configure the TACACS+ server timeout value:

```
switch# configure terminal
switch(config)# tacacs-server timeout 3
```

This example shows how to revert to the default TACACS+ server timeout value:

```
switch# configure terminal
switch(config)# no tacacs-server timeout 3
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
feature tacacs+	Enables TACACS+.

telnet

To create a Telnet session using IPv4 on the Cisco NX-OS device, use the **telnet** command.

telnet {*ipv4-address* | *hostname*} [*port-number*] [**vrf** *vrf-name*]

Syntax Description

ipv4-address	IPv4 address of the remote device.
hostname	Hostname of the remote device. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
port-number	(Optional) Port number for the Telnet session. The range is from 1 to 65535.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the Telnet session. The name is case sensitive.

Defaults

Port 23

Default VRF

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Telnet server using the **feature telnet** command.

To create a Telnet session with IPv6 addressing, use the **telnet6** command.

The Cisco NX-OS software supports a maximum of 60 concurrent SSH and Telnet sessions.

This command does not require a license.

Examples

This example shows how to start a Telnet session using an IPv4 address:

```
switch# telnet 10.10.1.1 vrf management
```

Related Commands

Command	Description
clear line	Clears Telnet sessions.

Command	Description
telnet6	Creates a Telnet session using IPv6 addressing.
feature telnet	Enables the Telnet server.

telnet server enable

To enable the Telnet server for a virtual device context (VDC), use the **telnet server enable** command. To disable the Telnet server, use the **no** form of this command.

telnet server enable

no telnet server enable

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.1(2)	This command was deprecated and replaced with the **feature telnet** command.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable the Telnet server:

```
switch# configure terminal
switch(config)# telnet server enable
```

This example shows how to disable the Telnet server:

```
switch# configure terminal
switch(config)# no telnet server enable
XML interface to system may become unavailable since ssh is disabled
```

Related Commands

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

telnet6

To create a Telnet session using IPv6 on the Cisco NX-OS device, use the **telnet6** command.

telnet6 {*ipv6-address* | *hostname*} [*port-number*] [**vrf** *vrf-name*]

Syntax Description

ipv6-address	IPv6 address of the remote device.
hostname	Hostname of the remote device. The name is alphanumeric, case sensitive, and has a maximum of 64 characters.
port-number	(Optional) Port number for the Telnet session. The range is from 1 to 65535.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) name to use for the Telnet session. The name is case sensitive.

Defaults

Port 23

Default VRF

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable the Telnet server using the **feature telnet** command.

To create a Telnet session with IPv4 addressing, use the **telnet** command.

The Cisco NX-OS software supports a maximum of 60 concurrent SSH and Telnet sessions.

This command does not require a license.

Examples

This example shows how to start a Telnet session using an IPv6 address:

```
switch# telnet6 2001:0DB8:0:0:E000::F vrf management
```

Related Commands

Command	Description
clear line	Clears Telnet sessions.

Command	Description
telnet	Creates a Telnet session using IPv4 addressing.
feature telnet	Enables the Telnet server.

terminal verify-only

To enable command authorization verification on the command-line interface (CLI), use the **terminal verify-only** command. To disable this feature, use the **no** form of this command.

terminal verify-only [**username** *username*]

terminal no verify-only [**username** *username*]

Syntax Description

username *username*	(Optional) Specifies the username for which to verify command authorization.

Defaults

Disabled

The default for the **username** keyword is the current user session.

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

When you enable command authorization verification, the CLI indicates if the command is successfully authorized for the user but does not execute the command.

The command authorization verification uses the methods configured in the **aaa authorization commands default** command and the **aaa authorization config-commands default** command.

This command does not require a license.

Examples

This example shows how to enable command authorization verification:

```
switch# terminal verify-only
```

This example shows how to disable command authorization verification:

```
switch# terminal no verify-only
```

Related Commands

Command	Description
aaa authorization commands default	Configures authorization for EXEC commands.
aaa authorization config-commands default	Configures authorization for configuration commands.

test aaa authorization command-type

To test the TACACS+ command authorization for a username, use the **test aaa authorization command-type** command.

test aaa authorization command-type {**commands** | **config-commands**} **user** *username* **command** *command-string*

Syntax Description

commands	Tests EXEC commands.
config-commands	Tests configuration commands.
user *username*	Specifies the user name for TACACS+ command authorization testing.
command *command-string*	Specifies the command for authorization testing. Put double quotes around the *command-string* argument if the command contains spaces.

Defaults

None

Command Modes

Any command mode

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

To use the **test aaa authorization command-type** command, you must enable the TACACS+ feature using the **feature tacacs+** command.

You must configure a TACACS+ group on the Cisco NX-OS device using the **aaa server group** command before you can test the command authorization.

This command does not require a license.

Examples

This example shows how to test the TACACS+ command authorization for a username:

```
switch# test aaa authorization command-type commands user testuser command "configure terminal"
```

Related Commands

Command	Description
aaa authorization commands default	Configures authorization for EXEC commands.
aaa authorization config-commands default	Configures authorization for configuration commands.
aaa group server	Configures AAA server groups.

time-range

To configure a time range, use the **time-range** command. To remove a time range, use the **no** form of this command.

time-range *time-range-name*

no time-range *time-range-name*

Syntax Description

time-range-name	Name of the time range, which can be up to 64 alphanumeric, case-sensitive characters.

Defaults

None

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

You can use a time range in **permit** and **deny** commands for IPv4 and IPv6 ACLs.

Examples

This example shows how to use the **time-range** command and enter time range configuration mode:

```
switch# configure terminal
switch(config)# time-range workweek-vpn-access
switch(config-time-range)#
```

Related Commands

Command	Description
absolute	Specifies a time range that has a specific start date and time.
deny (IPv4)	Configures an IPv4 deny rule.
periodic	Specifies a time range that is active one or more times per week.
permit (IPv4)	Configures an IPv4 permit rule.