T to V Commands

This chapter describes the Cisco NX-OS Security commands that begin with T to V.

tacacs+ abort

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

tacacs+ abort

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Global configuration

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**.**

tacacs+ commit

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration

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

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	Time interval in minutes. The range is from 1 to 1440.

Defaults

0 minutes

Command Modes

Global configuration

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.

Command	Description
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 **tacacs-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

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. To revert to the default setting, 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*] [single-connection]

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*] [single-connection]

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 cleartext (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*	Specifies the time interval (in minutes) for monitoring the server. The time range is 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 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.
single-connection	(Optional) Configures a single connection for the TACACS+ server.

Defaults

Idle time: disabled

Server monitoring: disabled

Timeout: 1 second.

Test username: test

Test password: test

Command Modes

Global configuration

Command History

Release	Modification
6.2(2)	The single-connection keyword was added.
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** | 6 | **7**] *shared-secret*

no tacacs-server key [**0** | 6 | **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.
6	(Optional) Configures a preshared key specified in clear text to authenticate communication between the TACACS+ client and server.
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

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 test

To monitor the availability of all TACACS+ servers without having to configure the test parameters for each server individually, use the **tacacs-server test** command. To disable this configuration, use the **no** form of this command.

tacacs-server test {**idle-time** *time* | **password** *password* | **username** *name*}

no tacacs-server test {**idle-time** *time* | **password** *password* | **username** *name*}

Syntax Description

idle-time *time*	Specifies the time interval (in minutes) for monitoring the server. The range is from 1 to 1440 minutes. **Note** When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.
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 name is alphanumeric, not case sensitive, and has a maximum of 32 characters. **Note** To protect network security, we recommend that you use a username that is not the same as an existing username in the TACACS+ database.

Defaults

Server monitoring: Disabled
Idle time: 0 minutes
Test username: test
Test password: test

Command Modes

Global configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable TACACS+ authentication.

Any servers for which test parameters are not configured are monitored using the global level parameters.

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

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 the parameters for global TACACS+ server monitoring:

```
switch# configure terminal
switch(config)# tacacs-server test username user1 password Ur2Gd2BH idle-time 3
```

Related Commands

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

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

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

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.
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

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.

Send document comments to nexus7k-docfeedback@cisco.com.

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

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.
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

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

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.

Command	Description
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

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.
deny (IPv6)	Configures an IPv6 deny rule.
periodic	Specifies a time range that is active one or more times per week.
permit (IPv4)	Configures an IPv4 permit rule.
permit (IPv6)	Configures an IPv6 permit rule.

trustedCert

To configure the attribute name, search filter, and base-DN for the trusted certificate search operation in order to send a search query to the Lightweight Directory Access Protocol (LDAP) server, use the **trustedCert** command. To disable this configuration, use the **no** form of this command.

trustedCert attribute-name *attribute-name* **search-filter** *filter* **base-DN** *base-DN-name*

no trustedCert

Syntax Description

attribute-name *attribute-name*	Specifies the attribute name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
search-filter *filter*	Specifies the filter for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
base-DN *base-DN-name*	Specifies the base designated name for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Defaults

None

Command Modes

LDAP search map configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure the attribute name, search filter, and base-DN for the trusted certificate search operation in order to send a search query to the LDAP server:

```
switch# conf t
switch(config)# ldap search-map s0
switch(config-ldap-search-map)# trustedCert attribute-name cACertificate search-filter
(&(objectClass=certificationAuthority)) base-DN CN=NTAuthCertificates,CN=Public Key
Services,CN=Services,CN=Configuration,DC=mdsldaptestlab,DC=com
switch(config-ldap-search-map)#
```

Related Commands

Command	Description
feature ldap	Enables LDAP.

Command	Description
ldap search-map	Configures an LDAP search map.
show ldap-search-map	Displays the configured LDAP search maps.

use-vrf

To specify a virtual routing and forwarding instance (VRF) name for a RADIUS, TACACS+, or LDAP server group, use the **use-vrf** command. To remove the VRF name, use the **no** form of this command.

use-vrf *vrf-name*

no use-vrf *vrf-name*

Syntax Description

vrf-name	VRF name. The name is case sensitive.

Defaults

None

Command Modes

RADIUS server group configuration
TACACS+ server group configuration
LDAP server group configuration

Command History

Release	Modification
5.0(2)	Added support for LDAP server groups.
4.0(1)	This command was introduced.

Usage Guidelines

You can configure only one VRF instance for a server group.

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

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

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

This command does not require a license.

Examples

This example shows how to specify a VRF name for a RADIUS server group:

```
switch# config t
switch(config)# aaa group server radius RadServer
switch(config-radius)# use-vrf vrf1
```

This example shows how to specify a VRF name for a TACACS+ server group:

```
switch# config t
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# use-vrf vrf2
```

This example shows how to remove the VRF name from a TACACS+ server group:

```
switch# config t
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no use-vrf vrf2
```

This example shows how to specify a VRF name for an LDAP server group:

```
switch# config t
switch(config)# feature ldap
switch(config)# aaa group server ldap LdapServer
switch(config-tacacs+)# use-vrf vrf3
```

This example shows how to remove the VRF name from an LDAP server group:

```
switch# config t
switch(config)# feature ldap
switch(config)# aaa group server ldap LdapServer
switch(config-tacacs+)# no use-vrf vrf3
```

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
radius-server host	Configures a RADIUS server.
show ldap-server groups	Displays LDAP server information.
show radius-server groups	Displays RADIUS server information.
show tacacs-server groups	Displays TACACS+ server information.
feature ldap	Enables LDAP.
feature tacacs+	Enables TACACS+.
ldap-server host	Configures an LDAP server.
tacacs-server host	Configures a TACACS+ server.
vrf	Configures a VRF instance.

user-certdn-match

To configure the attribute name, search filter, and base-DN for the certificate DN match search operation in order to send a search query to the Lightweight Directory Access Protocol (LDAP) server, use the **user-certdn-match** command. To disable this configuration, use the **no** form of this command.

user-certdn-match attribute-name *attribute-name* **search-filter** *filter* **base-DN** *base-DN-name*

no user-certdn-match

Syntax Description

attribute-name *attribute-name*	Specifies the attribute name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
search-filter *filter*	Specifies the filter for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
base-DN *base-DN-name*	Specifies the base designated name for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Defaults

None

Command Modes

LDAP search map configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure the attribute name, search filter, and base-DN for the certificate DN match search operation in order to send a search query to the LDAP server:

```
switch# conf t
switch(config)# ldap search-map s0
switch(config-ldap-search-map)# user-certdn-match attribute-name certificateDN
search-filter (&(objectClass=inetOrgPerson)(cn=$userid)) base-DN dc=acme,dc=com
switch(config-ldap-search-map)#
```

Related Commands

Command	Description
feature ldap	Enables LDAP.

Command	Description
ldap search-map	Configures an LDAP search map.
show ldap-search-map	Displays the configured LDAP search maps.

user-pubkey-match

To configure the attribute name, search filter, and base-DN for the public key match search operation in order to send a search query to the Lightweight Directory Access Protocol (LDAP) server, use the **user-pubkey-match** command. To disable this configuration, use the **no** form of this command.

user-pubkey-match attribute-name *attribute-name* **search-filter** *filter* **base-DN** *base-DN-name*

no user-pubkey-match

Syntax Description

attribute-name *attribute-name*	Specifies the attribute name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
search-filter *filter*	Specifies the filter for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
base-DN *base-DN-name*	Specifies the base designated name for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Defaults

None

Command Modes

LDAP search map configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure the attribute name, search filter, and base-DN for the public key match search operation in order to send a search query to the LDAP server:

```
switch# conf t
switch(config)# ldap search-map s0
switch(config-ldap-search-map)# user-pubkey-match attribute-name sshPublicKey
search-filter (&(objectClass=inetOrgPerson)(cn=$userid)) base-DN dc=acme,dc=com
switch(config-ldap-search-map)#
```

Related Commands

Command	Description
feature ldap	Enables LDAP.

Command	Description
ldap search-map	Configures an LDAP search map.
show ldap-search-map	Displays the configured LDAP search maps.

user-switch-bind

To configure the attribute name, search filter, and base-DN for the user-switchgroup search operation in order to send a search query to the Lightweight Directory Access Protocol (LDAP) server, use the **user-switch-bind** command. To disable this configuration, use the **no** form of this command.

user-switch-bind attribute-name *attribute-name* **search-filter** *filter* **base-DN** *base-DN-name*

no user-switch-bind

Syntax Description

attribute-name *attribute-name*	Specifies the attribute name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
search-filter *filter*	Specifies the filter for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
base-DN *base-DN-name*	Specifies the base designated name for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Defaults

None

Command Modes

LDAP search map configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure the attribute name, search filter, and base-DN for the user-switchgroup search operation in order to send a search query to the LDAP server:

```
switch# conf t
switch(config)# ldap search-map s0
switch(config-ldap-search-map)# user-switch-bind attribute-name memberuid search-filter
(&(objectClass=posixGroup)(cn=dcgroup)) base-DN dc=acme,dc=com
switch(config-ldap-search-map)#
```

Related Commands

Command	Description
feature ldap	Enables LDAP.

Command	Description
ldap search-map	Configures an LDAP search map.
show ldap-search-map	Displays the configured LDAP search maps.

Send document comments to nexus7k-docfeedback@cisco.com.

username

To create and configure a user account in a virtual device context (VDC), use the **username** command. To remove a user account, use the **no** form of this command.

username *user-id* [**expire** *date*] [**password** [**0** | **5**] *password*] [**role** *role-name*]

username *user-id* [**sshkey** {*key* | **file** *filename*}]

username *user-id* [**keypair generate** {**rsa** [*bits* **[force]] | dsa [force]}]**

username *user-id [***keypair** {**export** | **import**} {**bootflash:***filename* | **volatile:***filename*} {**rsa** | **dsa**} [**force**]]

username *user-id [***priv-lvl** *n]* [**expire** *date*] [**password** [**0** | **5**] *password*]

no username *user-id*

Syntax Description

user-id	User identifier for the user account. The *user-id* argument is a case-sensitive, alphanumeric character string with a maximum length of 28 characters. For more information, see the usage guidelines section below. **Note** The Cisco NX-OS software allows these special characters in the *user-id* argument text string: (_ . + = \ -).
expire *date*	(Optional) Specifies the expire date for the user account. The format for the *date* argument is YYYY-MM-DD.
password	(Optional) Specifies a password for the account. The default is no password.
0	(Optional) Specifies that the password is in clear text. Clear text passwords are encrypted before they are saved to the running configuration.
5	(Optional) Specifies that the password is in encrypted format. Encrypted passwords are not changed before they are saved to the running configuration.
password	Password string. The password is alphanumeric, case sensitive, and has a maximum of 64 characters. **Note** All printable ASCII characters are supported in the password string if they are enclosed in quotation marks.
role *role-name*	(Optional) Specifies the user role. The *role-name* argument is case sensitive.
sshkey	(Optional) Specifies an SSH key for the user account.
key	SSH key string.
file *filename*	Specifies the name of a file that contains the SSH key string.
keypair	Generates SSH user keys.
generate	Generates SSH key-pairs.
rsa	Generates Rivest, Shamir, and Adelman (RSA) keys.
bits	Number of bits used to generate the key. The range is from 1024 to 2048, and the default value is 1024.
force	Forces the generation of keys even if previous ones are present.
dsa	Generates Digital System Algorithm (DSA) keys.

export	Exports key-pairs to the bootflash or volatile directory.
import	Imports key-pairs from the bootflash or volatile directory.
bootflash:*filename*	Specifies the bootflash filename.
volatile:*filename*	Specifies the remote filename.
priv-lvl *n*	Specifies the privilege level to which the user is assigned. The range is from 0 to 15.

Defaults

Unless specified, usernames have no expire date, password, or SSH key.

In the default VDC, the default role is network-operator if the creating user has the network-admin role, or the default role is vdc-operator if the creating user has the vdc-admin role.

In nondefault VDCs, the default user role is vdc-operator.

You cannot delete the default admin user role. Also, you cannot change the expire date or remove the network-admin role for the default admin user role.

To specify privilege levels, you must enable the cumulative privilege of roles for command authorization on TACACS+ servers using the **feature privilege** command. There is no default privilege level.

This command does not require a license.

Command Modes

Global configuration

Command History

Release	Modification
5.1(1)	Removed support for RSA keys less than 1024 bits.
5.0(2)	Added the **keypair** keyword option.
5.0(2)	Added the **priv-lvl** keyword option.
4.1(2)	Added the **sshkey** keyword option.
4.0(1)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software creates two default user accounts in the VDC: admin and adminbackup. The nondefault VDCs have one default user account: admin. You cannot remove a default user account.

User accounts are local to the VDCs. You can create user accounts with the same user identifiers in different VDCs.

⚠ **Caution** The Cisco NX-OS software does not support all numeric usernames, whether created with TACACS+ or RADIUS, or created locally. Local users with all numeric names cannot be created. If an all numeric user name exists on an AAA server and is entered during login, the user is not logged in.

The Cisco NX-OS software accepts only strong passwords when you have password-strength checking enabled using the **password strength-check** command. The characteristics of a strong password include the following:

- At least eight characters long

- Does not contain many consecutive characters (such as “abcd”)
- Does not contain many repeating characters (such as “aaabbb”)
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

Caution If you do not specify a password for the user account, the user might not be able to log in to the account.

To use this command, you must enable the cumulative privilege of roles using the **feature privilege** command.

A passphrase is required when you export or import the key-pair. The passphrase encrypts the exported private key for the user and decrypts it during import.

This command does not require a license.

Examples

This example shows how to create a user account with a password and a user role:

```
switch# config t
switch(config)# username user1 password Ci5co321 role vdc-admin
```

This example shows how to configure the SSH key for a user account:

```
switch# config t
switch(config)# username user1 sshkey file bootflash:key_file
```

This example shows how to generate the SSH public and private keys and store them in the home directory of the Cisco NX-OS device for the user:

```
switch# config t
switch(config)# username user1 keypair generate rsa
generating rsa key(2048 bits)......
generated rsa key
```

This example shows how to export the public and private keys from the home directory of the Cisco NX-OS device to the bootflash directory:

```
switch# config t
switch(config)# username user1 keypair export bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# dir
.
.
.
951 Jul 09 11:13:59 2009 key_rsa
221 Jul 09 11:14:00 2009 key_rsa.pub
.
.
```

The private key is exported as the file that you specify, and the public key is exported with the same filename followed by a .pub extension.

This example shows how to import the exported public and private keys from the bootflash directory to the home directory of the Cisco NX-OS device:

```
switch# config t
switch(config)# username user1 keypair import bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# show username user1 keypair
**************************************
rsa Keys generated: Thu Jul 9 11:10:29 2009
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZElTfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TBypYDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=
bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
**************************************
could not retrieve dsa key information
**************************************
switch(config)#
```

The private key is imported as the file that you specify, and the public key is imported with the same filename followed by a .pub extension.

This example shows how to assign privilege level 15 to the user:

```
switch# config t
switch(config)# feature privilege
switch(config)# enable secret 5 def456 priv-lvl 15
switch(config)# username user2 priv-lvl 15
```

Related Commands

Command	Description
enable *level*	Enables a user to move to a higher privilege level.
enable secret priv-lvl	Enables a secret password for a specific privilege level.
feature privilege	Enables the cumulative privilege of roles for command authorization on TACACS+ servers.
password strength-check	Checks the password security strength.
show privilege	Displays the current privilege level, username, and status of cumulative privilege support.
show user-account	Displays the user account configuration.
show username	Displays the public key for the specified user.

userprofile

To configure the attribute name, search filter, and base-DN for the user profile search operation in order to send a search query to the Lightweight Directory Access Protocol (LDAP) server, use the **userprofile** command. To disable this configuration, use the **no** form of this command.

userprofile attribute-name *attribute-name* **search-filter** *filter* **base-DN** *base-DN-name*

no userprofile

Syntax Description

attribute-name *attribute-name*	Specifies the attribute name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
search-filter *filter*	Specifies the filter for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
base-DN *base-DN-name*	Specifies the base designated name for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Defaults

None

Command Modes

LDAP search map configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure the attribute name, search filter, and base-DN for the user profile search operation in order to send a search query to the LDAP server:

```
switch# conf t
switch(config)# ldap search-map s0
switch(config-ldap-search-map)# userprofile attribute-name description search-filter
(&(objectClass=inetOrgPerson)(cn=$userid)) base-DN dc=acme,dc=com
switch(config-ldap-search-map)#
```

Related Commands

Command	Description
feature ldap	Enables LDAP.

Command	Description
ldap search-map	Configures an LDAP search map.
show ldap-search-map	Displays the configured LDAP search maps.

Send document comments to nexus7k-docfeedback@cisco.com.

vlan access-map

spec indicates that there are sequence numbers for access maps and each seq number can have an action and match command. no seq numbers on CLI.

To create a new VLAN access-map entry or to configure an existing VLAN access-map entry, use the **vlan access-map** command. To remove a VLAN access-map entry, use the **no** form of this command.

vlan access-map *map-name* [*sequence-number*]

no vlan access-map *map-name* [*sequence-number*]

Syntax Description

sequence-number	(Optional) Sequence number of the VLAN access-map entry that you are creating or editing. A sequence number can be any integer between 1 and 4294967295. By default, the first entry in a VLAN access map has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the VLAN access map and assigns a sequence number that is 10 greater than the sequence number of the preceding entry. When you use the **no** form of the command, use the *sequence-number* argument to specify an entry that you want to remove. Omit the *sequence-number* argument if you want to remove the entire VLAN access map.
map-name	Name of the VLAN access map that you want to create or configure. The *map-name* argument can be up to 64 alphanumeric, case-sensitive characters.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Each VLAN access-map entry can include one **action** command and one or more **match** command.

Use the **statistics per-entry** command to configure the device to record statistics for a VLAN access-map entry.

This command does not require a license.

Examples

This example shows how to create a VLAN access map named vlan-map-01, add two entries that each have two **match** commands and one **action** command, and enable statistics for the packets matched by the second entry:

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# match mac address mac-acl-00f

switch(config-access-map)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-320
switch(config-access-map)# match mac address mac-acl-00e
switch(config-access-map)# action drop
switch(config-access-map)# statistics per-entry

switch(config-access-map)# show vlan access-map

Vlan access-map vlan-map-01 10
        match ip: ip-acl-01
        match mac: mac-acl-00f
        action: forward
Vlan access-map vlan-map-01 20
        match ip: ip-acl-320
        match mac: mac-acl-00e
        action: drop
        statistics per-entry
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
statistics per-entry	Enables collection of statistics for each entry in an ACL.
vlan filter	Applies a VLAN access map to one or more VLANs.

vlan filter

To apply a VLAN access map to one or more VLANs, use the **vlan filter** command. To unapply a VLAN access map, use the **no** form of this command.

vlan filter *map-name* **vlan-list** *VLAN-list*

no vlan filter *map-name* **vlan-list** *VLAN-list*

Syntax Description

map-name	Name of the VLAN access map that you want to create or configure.
vlan-list *VLAN-list*	Specifies the ID of one or more VLANs that the VLAN access map filters. Valid VLAN IDs are from 1 to 4096. Use a hyphen (-) to separate the beginning and ending IDs of a range of VLAN IDs; for example, use 70-100. Use a comma (,) to separate individual VLAN IDs and ranges of VLAN IDs; for example, use 20,70-100,142. **Note** When you use the **no** form of this command, the *VLAN-list* argument is optional. If you omit this argument, the device removes the access map from all VLANs where the access map is applied.

Defaults

None

Command Modes

Global configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can apply a VLAN access map to one or more VLANs.

You can apply only one VLAN access map to a VLAN.

The **no** form of this command enables you to unapply a VLAN access map from all or part of the VLAN list that you specified when you applied the access map. To unapply an access map from all VLANs where it is applied, you can omit the *VLAN-list* argument. To unapply an access map from a subset of the VLANs where it is currently applied, use the *VLAN-list* argument to specify the VLANs where the access map should be removed.

This command does not require a license.

Examples

This example shows how to apply a VLAN access map named vlan-map-01 to VLANs 20 through 45:

```
switch# config t
switch(config)# vlan filter vlan-map-01 20-45
```

This example show how to use the **no** form of the command to unapply the VLAN access map named vlan-map-01 from VLANs 30 through 32, which leaves the access map applied to VLANs 20 through 29 and 33 through 45:

```
switch# show vlan filter

vlan map vlan-map-01:
        Configured on VLANs:    20-45
switch(config)# no vlan filter vlan-map-01 30-32
switch# show vlan filter

vlan map vlan-map-01:
        Configured on VLANs:    20-29,33-45
```

Related Commands

Command	Description
action	Specifies an action for traffic filtering in a VLAN access map.
match	Specifies an ACL for traffic filtering in a VLAN access map.
show vlan access-map	Displays all VLAN access maps or a VLAN access map.
show vlan filter	Displays information about how a VLAN access map is applied.
vlan access-map	Configures a VLAN access map.

vlan policy deny

To enter VLAN policy configuration mode for a user role, use the **vlan policy deny** command. To revert to the default VLAN policy for a user role, use the **no** form of this command.

vlan policy deny

no vlan policy deny

Syntax Description

This command has no arguments or keywords.

Defaults

All VLANs

Command Modes

User role configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command denies all VLANs to the user role except for those that you allow using the **permit vlan** command in user role VLAN policy configuration mode.

This command does not require a license.

Examples

This example shows how to enter user role VLAN policy configuration mode for a user role:

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)#
```

This example shows how to revert to the default VLAN policy for a user role:

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# no vlan policy deny
```

Related Commands

Command	Description
permit vlan	Allows a VLAN in a user role VLAN policy.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.

vrf policy deny

To enter virtual forwarding and routing instance (VRF) policy configuration mode for a user role, use the **vrf policy deny** command. To revert to the default VRF policy for a user role, use the **no** form of this command.

vrf policy deny

no vrf policy deny

Syntax Description

This command has no arguments or keywords.

Defaults

All VRFs

Command Modes

User role configuration

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command denies all VRFs to the user role except for those that you allow using the **permit vrf** command in user role VRF policy configuration mode.

This command does not require a license.

Examples

This example shows how to enter VRF policy configuration mode for a user role:

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)#
```

This example shows how to revert to the default VRF policy for a user role:

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# no vrf policy deny
```

Related Commands

Command	Description
vrf permit	Permits VRFs in a user role VRF policy.
role name	Creates or specifies a user role and enters user role configuration mode.
show role	Displays user role information.