L Commands

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

ldap-server deadtime

To configure the deadtime interval for all Lightweight Directory Access Protocol (LDAP) servers, use the **ldap-server deadtime** command. The deadtime interval specifies the time that the Cisco NX-OS device waits, after declaring that an LDAP server is dead, before sending out a test packet to determine if the server is now alive. To remove the global deadtime interval configuration, use the **no** form of this command.

ldap-server deadtime *minutes*

no ldap-server deadtime *minutes*

Syntax Description

minutes	Global deadtime interval for LDAP servers. The range is from 1 to 60 minutes.

Defaults

0 minutes

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

When the dead-time interval is 0 minutes, LDAP servers are not marked as dead even if they are not responding.

This command does not require a license.

Examples

This example shows how to configure the global deadtime interval for LDAP servers:

```
switch# config t
switch(config)# ldap-server deadtime 5
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
show ldap-server	Displays the LDAP server configuration.

ldap-server host

To configure Lightweight Directory Access Protocol (LDAP) server host parameters, use the **ldap-server host** command. To revert to the defaults, use the **no** form of this command.

ldap-server host {*ipv4-address* | *ipv6-address* | *host-name*}
[**enable-ssl**]
[**port** *tcp-port* [**timeout** *seconds*]]
[**rootDN** *root-name* [**password** *password*] [**port** *tcp-port* [**timeout** *seconds*] | [**timeout** *seconds*]]]
[**test rootDN** *root-name* [**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]]]
[**timeout** *seconds*]

no ldap-server host {*ipv4-address* | *ipv6-address* | *host-name*}
[**enable-ssl**]
[**port** *tcp-port* [**timeout** *seconds*]]
[**rootDN** *root-name* [**password** *password*] [**port** *tcp-port* [**timeout** *seconds*] | [**timeout** *seconds*]]]
[**test rootDN** *root-name* [**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]]]
[**timeout** *seconds*]

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.
host-name	Server name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
enable-ssl	(Optional) Ensures the integrity and confidentiality of the transferred data by causing the LDAP client to establish a Secure Sockets Layer (SSL) session before sending the bind or search request.
port *tcp-port*	(Optional) Specifies the TCP port to use for LDAP messages to the server. The range is from 1 to 65535.
timeout *seconds*	(Optional) Specifies the timeout interval for the server. The range is from 1 to 60 seconds.
rootDN *root-name*	(Optional) Specifies the root designated name (DN) for the LDAP server database. You can enter up to 128 alphanumeric characters for the root name.
password *password*	(Optional) Specifies the bind password for the root.
test	(Optional) Configures parameters to send test packets to the LDAP server.
idle-time *minutes*	Specifies the time interval (in minutes) for monitoring the server. The range is from 1 to 1440 minutes.
username *name*	Specifies a username in the test packets. The username is alphanumeric, 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 LDAP database.

Defaults

Server monitoring: Disabled
TCP port: The global value or 389 if a global value is not configured
Timeout: The global value or 5 seconds if a global value is not configured
Idle time: 60 minutes
Test username: test
Test password: Cisco

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP and obtain the IPv4 or IPv6 address or hostname for the remote LDAP server.

If you plan to enable the SSL protocol, make sure that the LDAP server certificate is manually configured on the Cisco NX-OS device.

By default, when you configure an LDAP server IP address or hostname on the Cisco NX-OS device, the LDAP server is added to the default LDAP server group. You can also add the LDAP server to another LDAP server group.

The timeout interval value specified for an LDAP server overrides the global timeout interval value specified for all LDAP servers.

This command does not require a license.

Examples

This example shows how to configure the IPv6 address for an LDAP server:

```
switch# config t
switch(config)# ldap-server host 10.10.2.2 timeout 20
```

This example shows how to configure the parameters for LDAP server monitoring:

```
switch# config t
switch(config)# ldap-server host 10.10.1.1 test rootDN root1 username user1 password
Ur2Gd2BH idle-time 3
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
show ldap-server	Displays the LDAP server configuration.

ldap-server port

To configure a global Lightweight Directory Access Protocol (LDAP) server port through which clients initiate TCP connections, use the **ldap-server port** command. To remove the LDAP server port configuration, use the **no** form of this command.

ldap-server port *tcp-port*

no ldap-server port *tcp-port*

Syntax Description

tcp-port	Global TCP port to use for LDAP messages to the server. The range is from 1 to 65535.

Defaults

TCP port 389

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.2(1)	This command was deprecated.
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 a global TCP port for LDAP messages:

```
switch# config t
switch(config)# ldap-server port 2
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
show ldap-server	Displays the LDAP server configuration.

ldap-server timeout

To configure a global timeout interval that determines how long the Cisco NX-OS device waits for responses from all Lightweight Directory Access Protocol (LDAP) servers before declaring a timeout failure, use the **ldap-server timeout** command. To remove the global timeout configuration, use the **no** form of this command.

ldap-server timeout *seconds*

no ldap-server timeout *seconds*

Syntax Description

seconds	Timeout interval for LDAP servers. The range is from 1 to 60 seconds.

Defaults

5 seconds

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

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 global timeout interval for LDAP servers:

```
switch# config t
switch(config)# ldap-server timeout 10
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
show ldap-server	Displays the LDAP server configuration.

ldap search-map

To configure a Lightweight Directory Access Protocol (LDAP) search map to send a search query to the LDAP server, use the **ldap search-map** command. To disable the search map, use the **no** form of this command.

ldap search-map *map-name*

no ldap search-map *map-name*

Syntax Description

map-name	Name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Defaults

Disabled

Command Modes

Global configuration

SupportedUserRoles

network-admin
vdc-admin

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 an LDAP search map:

```
switch# config t
switch(config)# ldap search-map map1
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
show ldap-search-map	Displays the configured LDAP search maps.
CRLLookup	Configures the attribute name, search filter, and base-DN for the CRL search operation in order to send a search query to the LDAP server.

Command	Description
trustedCert	Configures 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.
user-certdn-match	Configures 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.
user-pubkey-match	Configures 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.
user-switch-bind	Configures 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.
userprofile	Configures 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.

logging drop threshold

To configure the threshold value for dropped packets and generate a syslog if the drop count exceeds the configured threshold in a policy map for Control Plane Policing (CoPP), use the **logging drop threshold** command.

logging drop threshold [*drop-count* [**level** *syslog-level*]]

Syntax Description

drop-count	Drop count. The range is from 1 to 80000000000.
level	(Optional) Specifies the syslog level.
syslog-level	Syslog level. The range is from 1 to 7.

Defaults

Syslog level 4

Command Modes

config-pmap-c

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

Ensure that you are in the default VDC.

Ensure that you have configured the IP ACLs if you want to use ACE hit counters in the class maps.

This command does not require a license.

Examples

This example shows how to configure the threshold value for dropped packets and generate a syslog if the drop count exceeds the configured threshold in a policy map for CoPP:

```
switch# config t
switch(config)# policy-map type control-plane ClassMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# police cir 52000
switch(config-pmap-c)# police cir 52000 bc 2000
switch(config-pmap-c)# police cir 5000 conform transmit exceed drop violate set1 dscp3
dscp4 table1 pir-markdown-map
switch(config-pmap-c)# police cir 52000 pir 78000 be 2000
switch(config-pmap-c)# logging drop threshold 1800 level 2
switch(config-pmap-c)#
```

Related Commands

Command	Description
policy-map type control-plane	Configures a control plane policy map and enters policy map configuration mode.

lt

To specify a less-than group member for an IP port object group, use the **lt** command. A less-than group member matches port numbers that are less than (and not equal to) the port number specified in the entry. To remove a greater-than group member from port object group, use the **no** form of this command.

[*sequence-number*] **lt** *port-number*

no {*sequence-number* | **lt** *port-number*}

Syntax Description

sequence-number	(Optional) Sequence number for this group member. Sequence numbers maintain the order of group members within an object group. Valid sequence numbers are from 1 to 4294967295. If you do not specify a sequence number, the device assigns a number that is 10 greater than the largest sequence number in the current object group.
port-number	Port number that traffic matching this group member does not exceed or equal. Valid values are from 0 to 65535.

Defaults

None

Command Modes

IP port object group configuration

SupportedUserRoles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

IP port object groups are not directional. Whether a **lt** command matches a source or destination port or whether it applies to inbound or outbound traffic depends upon how you use the object group in an ACL.

This command does not require a license.

Examples

This example shows how to configure an IP port object group named port-group-05 with a group member that matches traffic sent to or from port 1 through port 49151:

```
switch# config t
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# lt 49152
```

Related Commands

Command	Description
eq	Specifies an equal-to group member in an IP port object group.
gt	Specifies a greater-than group member in an IP port object group.
neq	Specifies a not-equal-to group member in an IP port object group.
object-group ip port	Configures an IP port object group.
range	Specifies a port range group member in an IP port object group.
show object-group	Displays object groups.