LDAP Server State

The LDAP Server State feature enables users to capture information about Lightweight Directory Access Protocol (LDAP) server reachability before a request is sent to the server.

LDAP provides applications with a standard method for accessing and modifying the information stored in a directory. LDAP is integrated into the Cisco software as an authentication, authorization, and accounting (AAA) protocol alongside the existing AAA protocols such as RADIUS, TACACS+, Kerberos, and Diameter.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for LDAP Server State

The Lightweight Directory Access Protocol (LDAP) server should be marked as DEAD by default to get the exact state of the server and the server group.

Restrictions for LDAP Server State

When configuring a Lightweight Directory Access Protocol (LDAP) server, we assume that the server is in DEAD state and is not reachable. The correct state of the server is obtained after the deadtime (the period during which new authentication requests are not sent to an LDAP server that has failed to respond to a previous request) expiry is reached. Within this time frame, even if the server is reachable, no requests should be sent to the server.

Information About LDAP Server State

Overview of LDAP Server State

The LDAP Server State feature reduces the load on the network if the servers are not reachable and avoids unnecessary processing of retransmits.

The authentication, authorization, and accounting (AAA) servers are used to validate users or subscribers before they access a network. If one of the servers is not reachable, the next configured server specified in the configuration is contacted.

AAA client components make use of the DEAD and ALIVE states to keep track of each server state to handle protocol transactions effectively. If the state is DEAD, the client component applies a default set of policies to users or subscribers and allows them to access the default web content. If the state is ALIVE, the client component gets the actual policies from the Lightweight Directory Access Protocol (LDAP) server.

If the **automate-tester** command is configured along with the **deadtime** command, after every deadtime expiry, the AAA test APIs send a dummy bind request packet to the LDAP server.

- If a bind response is received, the server state is updated as ALIVE and further dummy bind requests are not sent.
- If a bind response is not received, the server state remains as DEAD and after every deadtime expiry, AAA test APIs send dummy bind request packets to the LDAP server.

If the **deadtime** command is configured when the server is not reachable, the server state remains DEAD until the deadtime expiry is reached, after which the state changes to ALIVE.

Note If one of the servers in a server group is ALIVE, the server group is marked as ALIVE.

How to Configure LDAP Server State

Perform this task to enable the server state notification functionality in a Lightweight Directory Access Protocol (LDAP) server. By default, all servers are marked as DEAD during configuration.

Configuring LDAP Server State

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **username** *user* **password** {**0** | **7**} *password*
4. **aaa new-model**
5. **ldap server** *name*
6. **deadtime** *minutes*
7. **automate-tester username** *name* **probe-on**
8. **end**
9. **show ldap server**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**username** *user* **password** {**0** | **7**} *password* **Example:** `Device(config)# username user1 password 0 pwd1`	Configures an unencrypted password that is automatically picked up by the **automate-tester** command.
Step 4	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables the authentication, authorization, and accounting (AAA) access control system.
Step 5	**ldap server** *name* **Example:** `Device(config)# ldap server server1`	Configures a device to use the LDAP protocol and enters LDAP server configuration mode.
Step 6	**deadtime** *minutes* **Example:** `Device(config-ldap-server)# deadtime 1`	Configures the deadtime expiry value (in minutes) for the LDAP server.

	Command or Action	Purpose
Step 7	**automate-tester username** *name* **probe-on** **Example:** `Device(config-ldap-server)# automate-tester username user1 probe-on`	Assigns the state of the LDAP server as DEAD by default when configured along with the **deadtime** *minutes* command.
Step 8	**end** **Example:** `Device(config-ldap-server)# end`	Exits LDAP server configuration mode and returns to privileged EXEC mode.
Step 9	**show ldap server** **Example:** `Device# show ldap server`	Displays the LDAP server state information and various other counters for the server.

Configuration Examples for LDAP Server State

Example: Configuring LDAP Server State

```
Device# configure terminal
Device(config)# username user1 password 0 pwd1
Device(config)# aaa new-model
Device(config)# ldap server server1
Device(config-ldap-server)# deadtime 1
Device(config-ldap-server)# automate-tester username user1 probe-on
Device(config-ldap-server)# end
```

The following output is displayed on entering the **automate-tester username** *name* **probe-on** command:

```
*Feb 24 09:14:55.139: LDAP_SERVER 192.0.2.10 Server state is UP
```

The following sample output from the **show ldap server** command shows the Lightweight Directory Access Protocol (LDAP) server state information of *server1* server and various other counters for the server.

```
Device# show ldap server server1 summary

Server Information for server1
================================
Server name :server1
Server Address :192.0.2.10
Server listening Port :389
Bind Root-dn :user1
Server mode :Non-Secure
Cipher Suite :0x00
Authentication Seq :Search first. Then Bind/Compare password next
Authentication Procedure:Bind with user password
Request timeout :30
Deadtime in Mins :1
State :ALIVE
No. of active connections :0
---------------------------------
```

Additional References for LDAP Server State

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Security Command Reference: Commands A to C • Security Command Reference: Commands D to L • Security Command Reference: Commands M to R • Security Command Reference: Commands S to Z
LDAP configuration tasks	"Configuring LDAP" chapter in *AAA LDAP Configuration Guide*

Standards and RFCs

Standard/RFC	Title
RFC 4511	*Lightweight Directory Access Protocol (LDAP)*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for LDAP Server State

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for LDAP Server State

Feature Name	Releases	Feature Information
LDAP Server State	15.4(2)T	The LDAP Server State feature enables users to capture information about LDAP server reachability before a request is sent to the server. The following commands were introduced or modified: **automate-tester**, **deadtime**.