Configuring IPv6 Support for LDAP

Restrictions for Configuring IPv6 Support for LDAP

- Only bind, search, and compare operations are supported.
- The Lightweight Directory Access Protocol (LDAP) referrals are not supported.
- Unsolicited messages or notifications from LDAP server are not handled.

Information About Configuring IPv6 Support for LDAP

IPv6 Support for LDAP

To support Lightweight Directory Access Protocol (LDAP) over IPv6, changes are made to authentication, authorization and accounting (AAA) transactions in terms of authentication and authorization while communicating over an IPv6 network. In order to support LDAP over an IPv6 network, transport calls have been modified to support both IPv4 and IPv6 based on the server configuration.

Transport Layer Security

Transport Layer Security (TLS) is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. It relies upon certificates, public keys, and private keys for clients to prove the identity. Certificates are issued by Certificate Authorities (CAs). Each certificate includes the name of the authority that issued it, the name of the entity to which the certificate was issued, the entity's public key, and time stamps that indicate the certificate's expiration date. TLS support for LDAP is mentioned in RFC 2830 as an extension to the LDAP protocol.

LDAP Operations

Bind

The bind operation is used to authenticate a user to the server. It is used to start a connection with the LDAP server. LDAP is a connection-oriented protocol. The client specifies the protocol version and the client authentication information. LDAP supports the following binds:

- Authenticated bind
- Anonymous bind

An authenticated bind is performed when a root distinguished name (DN) and password are available. In the absence of a root DN and password, an anonymous bind is performed. In LDAP deployments, the search operation is performed first and the bind operation later. This is because, if a password attribute is returned as part of the search operation, the password verification can be done locally on an LDAP client. Thus, there is no need to perform an extra bind operation. If a password attribute is not returned, the bind operation can be performed later. Another advantage of performing a search operation first and a bind operation later is that the DN received in the search result can be used as the user DN instead of forming a DN by prefixing the username (cn attribute) with the base DN. All entries stored in an LDAP server have a unique DN. The DN consists of two parts: the Relative Distinguished Name (RDN) and the location within the LDAP server where the record resides.

Most of the entries that you store in an LDAP server will have a name, and the name is frequently stored in the Common Name (cn) attribute. Because every object has a name, most objects you store in an LDAP will use their cn value as the basis for their RDN.

Compare

The compare operation is used to replace a bind request with a compare request for an authentication. The compare operation helps to maintain the initial bind parameters for the connection.

Search

A search operation is used to search the LDAP server. The client specifies the starting point (base DN) of the search, the search scope (either the object, its children, or the subtree rooted at the object), and a search filter.

For authorization requests, the search operation is directly performed without a bind operation. The LDAP server can be configured with certain privileges for the search operation to succeed. This privilege level is established with the bind operation.

An LDAP search operation can return multiple user entries for a specific user. In such cases, the LDAP client returns an appropriate error code to AAA. To avoid these errors, appropriate search filters that help to match a single entry must be configured.

How to Configure IPv6 Support for LDAP

Configuring Device-to-LDAP Server Communication

The Lightweight Directory Access Protocol (LDAP) host is a multiuser system running LDAP server software, such as Active Directory (Microsoft) and OpenLDAP. Configuring device-to-LDAP server communication can have several components:

- Hostname or IP address
- Port number
- Timeout period
- Base distinguished name (DN)

To configuring Device-to-LDAP server communication, perform this procedure:

Procedure

	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	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**ldap server** *name* **Example:** `Device(config)# ldap server server1`	Configures a device as an LDAP protocol and enters LDAP server configuration mode.
Step 5	**ipv6** *ipv6-address* **Example:** `Device(config-ldap-server)# ipv6 2001:DB8:0:0:8:800`	Specifies an IPv6 address to the LDAP server.

	Command or Action	Purpose
Step 6	**transport port** *port-number* **Example:** `Device(config-ldap-server)# transport port 200`	Configures the transport protocol for connecting to the LDAP server.
Step 7	**timeout retransmit** *seconds* **Example:** `Device(config-ldap-server)# timeout retransmit 20`	Specifies the number of seconds a device waits for a reply to an LDAP request before retransmitting the request.
Step 8	**exit** **Example:** `Device(config-ldap-server)# exit`	Exits the LDAP server configuration mode and enters global configuration mode.

Configuring LDAP Protocol Parameters

To configure LDAP protocol parameters, perform this procedure:

Procedure

	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	**aaa** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**ldap server** *name* **Example:** `Device(config)# ldap server server1`	Defines a Lightweight Directory Access Protocol (LDAP) server and enters LDAP server configuration mode.
Step 5	**bind authenticate root-dn password** [**0** *string* | **7** *string*] *string*	Specifies a shared secret text string used between the device and an LDAP server. Use

	Command or Action	Purpose
	Example: `Device(config-ldap-server)# bind authenticate root-dn "cn=administrator,cn=users,dc=nac-blr2,dc=example,dc=com password"`	the **0** line option to configure an unencrypted shared secret. Use the **7** line option to configure an encrypted shared secret.
Step 6	**search-filter user-object-type** *string* **Example:** `Device(config-ldap-server)# search-filter user-object-type string1`	Specifies the search filter to be used in the search requests.
Step 7	**base-dn** *string* **Example:** `Device(config-ldap-server)# base-dn "dc=sns,dc=example,dc=com"`	Specifies the base distinguished name (DN) of the search.
Step 8	**mode secure** [**no-negotiation**] **Example:** `Device(config-ldap-server)# mode secure no-negotiation`	Configures LDAP to initiate the transport layer security (TLS) connection and specifies the secure mode.
Step 9	**secure cipher 3des-ede-cbc-sha** **Example:** `Device(config-ldap-server)# secure cipher 3des-ede-cbc-sha`	Specifies the ciphersuite in the case of a secure connection.
Step 10	**exit** **Example:** `Device(config-ldap-server)# exit`	Exits LDAP server configuration mode and enters global configuration mode.

Configuring Search and Bind Operations for an Authentication Request

To configure search and bind operations for an authentication request, perform this procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**ldap server** *name* **Example:** `Device(config)# ldap server server1`	Defines a Lightweight Directory Access Protocol (LDAP) server and enter LDAP server configuration mode.
Step 5	**authentication bind-first** **Example:** `Device(config-ldap-server)# authentication bind-first`	Configures the sequence of search and bind operations for an authentication request.
Step 6	**authentication compare** **Example:** `Device(config-ldap-server)# authentication compare`	Replaces the bind request with the compare request for authentication.
Step 7	**exit** **Example:** `Device(config-ldap-server)# exit`	Exits LDAP server configuration mode.

Monitoring and Maintaining LDAP Scalability Enhancements

The following **show** and **debug** commands can be entered in any order.

Procedure

Step 1 **enable**

Example:

```
> enable
```

Enables privileged EXEC mode.

Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
# configure terminal
```

Enters global configuration mode.

Step 3 **clear ldap server**

Clears the Lightweight Directory Access Protocol (LDAP) server of the TCP connection.

Example:

```
# clear ldap server
```

Step 4 **debug ldap**

Displays information associated with LDAP.

Example:

```
# debug ldap
```

Step 5 **show ldap server**

Displays the LDAP server state information and various other counters for the server.

Example:

```
# show ldap server
```

Step 6 **show ldap attributes**

Displays information about default LDAP attribute mapping.

Example:

```
Device# show ldap attributes

LDAP Attribute                  Format      AAA Attribute
==============                  ======      =============
airespaceBwDataBurstContract    Ulong       bsn-data-bandwidth-burst-contr
userPassword                    String      password
airespaceBwRealBurstContract    Ulong       bsn-realtime-bandwidth-burst-c
employeeType                    String      employee-type
airespaceServiceType            Ulong       service-type
airespaceACLName                String      bsn-acl-name
priv-lvl                        Ulong       priv-lvl
memberOf                        String DN   supplicant-group
cn                              String      username
airespaceDSCP                   Ulong       bsn-dscp
policyTag                       String      tag-name
airespaceQOSLevel               Ulong       bsn-qos-level
airespace8021PType              Ulong       bsn-8021p-type
airespaceBwRealAveContract      Ulong       bsn-realtime-bandwidth-average
airespaceVlanInterfaceName      String      bsn-vlan-interface-name
airespaceVapId                  Ulong       bsn-wlan-id
airespaceBwDataAveContract      Ulong       bsn-data-bandwidth-average-con
sAMAccountName                  String      sam-account-name
meetingContactInfo              String      contact-info
```

```
telephoneNumber                 String      telephone-number
Map: att_map_1
department                      String DN   element-req-qos
```

Configuration Examples of IPv6 Support for LDAP

Example: Device-to-LDAP Server Communication

The following example shows how to create server group server1 and specify the IP address, transport port 200, and retransmit values:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# ldap server server1
Device(config-ldap-server)# ipv6 2001:DB8:0:0:8:800
Device(config-ldap-server)# transport port 200
Device(config-ldap-server)# timeout retransmit 20
Device(config-ldap-server)# exit
```

Example: LDAP Protocol Parameters

The following example shows how to configure Lightweight Directory Access Protocol (LDAP) parameters:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# ldap server server1
Device(config-ldap-server)# bind authenticate root-dn
"cn=administrator,cn=users,dc=nac-blr2,dc=example,dc=com password"
Device(config-ldap-server)# base-dn "dc=sns,dc=example,dc=com"
Device(config-ldap-server)# mode secure no-negotiation
Device(config-ldap-server)# secure cipher 3des-ede-cbc-sha
Device(config-ldap-server)# exit
```

Example: Search and Bind Operations for an Authentication Request

The following example shows how to configure the sequence of search and bind operations for an authentication request:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# ldap server server1
Device(config-ldap-server)# authentication bind-first
Device(config-ldap-server)# authentication compare
Device(config-ldap-server)# exit
```

Example: Server Information from an LDAP Server

The following is sample output from an LDAP server:

```
Device# show ldap server all

Server Information for server1
============================================
 Server name              :server1
 Server IP                :2001:DB8:0:0:8:800
 Server listening Port    :389
 Connection status        :DOWN
 Root Bind status         :No Bind
 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
 ----------------------------------------
 * LDAP STATISTICS *
 Total messages  [Sent:0, Received:0]
 Response delay(ms) [Average:0, Maximum:0]
 Total search    [Request:0, ResultEntry:0, ResultDone:0]
 Total bind      [Request:0, Response:0]
 Total extended  [Request:0, Response:0]
 Total compare   [Request:0, Response:0]
 Search [Success:0, Failures:0]
 Bind   [Success:0, Failures:0]
 Missing attrs in Entry [0]
----------------------------------------
```

Additional References

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	*Command Reference (Catalyst 9500 Series Switches)*

Standards and RFCs

Standard/RFC	Title
RFC 4511	*Lightweight Directory Access Protocol (LDAP)*
RFC 4513	*Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms*

Feature History for IPv6 Support for LDAP

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Fuji 16.8.1a	IPv6 Support for LDAP	The IPv6 Support for LDAP feature describes IPv6 transport support for the LDAP protocol by introducing changes in authentication, authorization, and accounting (AAA) transactions. Support for this feature was introduced on the C9500-32C, C9500-32QC, C9500-48Y4C, and C9500-24Y4C models of the Cisco Catalyst 9500 Series Switches.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.