Configuring LDAP

Lightweight Directory Access Protocol (LDAP) is integrated into Cisco software as an authentication, authorization, and accounting (AAA) protocol alongside the existing AAA protocols such as RADIUS, TACACS+, Kerberos, and Diameter. The AAA framework provides tools and mechanisms such as method lists, server groups, and generic attribute lists that enable an abstract and uniform interface to AAA clients irrespective of the actual protocol used for communication with the AAA server. LDAP supports authentication and authorization functions for AAA.

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 Configuring LDAP

If you are using a secure Transport Layer Security (TLS) secure connection, you must configure X.509 certificates.

Restrictions for Configuring LDAP

- LDAP referrals are not supported.
- Unsolicited messages or notifications from the LDAP server are not handled.
- LDAP authentication is not supported for interactive (terminal) sessions.

Information About LDAP

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.

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.

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.

LDAP Dynamic Attribute Mapping

Lightweight Directory Access Protocol (LDAP) is a powerful and flexible protocol for communication with AAA servers. LDAP attribute maps provide a method to cross-reference the attributes retrieved from a server to Cisco attributes supported by the security appliances.

When a user authenticates a security appliance, the security appliance, in turn, authenticates to the server and uses the LDAP protocol to retrieve the record for that user. The record consists of LDAP attributes associated with fields displayed on the user interface of the server. Each attribute retrieved includes a value that was entered by the administrator who updates the user records.

How to Configure LDAP

Configuring Router-to-LDAP Server Communication

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

- Hostname or IP address
- Port number
- Timeout period
- Base DN

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ldap server** *name*
4. **ipv4** *ipv4-address*
5. **transport port** *port-number*
6. **timeout retransmit** *seconds*
7. **exit**

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	**ldap server** *name* **Example:** `Device(config)# ldap server server1`	Configures a device to use the LDAP protocol and enters LDAP server configuration mode.
Step 4	**ipv4** *ipv4-address* **Example:** `Device(config-ldap-server)# ipv4 192.0.2.1`	Specifies the LDAP server IP address using IPv4.
Step 5	**transport port** *port-number* **Example:** `Device(config-ldap-server)# transport port 200`	Configures the transport protocol for connecting to the LDAP peer.
Step 6	**timeout retransmit** *seconds* **Example:** `Device(config-ldap-server)# timeout retransmit 20`	Specifies the number of seconds a router waits for a reply to an LDAP request before retransmitting the request.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Device(config-ldap-server)# exit`	Exits LDAP server configuration mode.

Configuring LDAP Protocol Parameters

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa**
4. **ldap server** *name*
5. **bind authenticate root-dn password** [**0** *string* | **7** *string*] *string*
6. **search-filter user-object-type** *string*
7. **base-dn** *string*
8. **mode secure** [**no-negotiation**]
9. **secure cipher 3des-ede-cbc-sha**
10. **exit**

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	**aaa** **Example:** `Device(config)# aaa new-model`	Enables AAA.

	Command or Action	Purpose
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* **Example:** `Device(config-ldap-server)# bind authenticate root-dn "cn=administrator,cn=users,dc=nac-blr2,dc=example,dc=com password"`	Specifies a shared secret text string used between the device and an LDAP server. Use 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 a AAA Server Group

Configuring the router to use AAA server groups enables you to group existing servers. You need to select a subset of the configured server hosts and use them for a particular service. A server group is used in conjunction with a global server-host list. The server group lists the IP addresses of the selected server hosts. Server groups can also include multiple host entries for the same server, as long as each entry has a unique identifier.

If two different host entries on the same LDAP server are configured for the same service (for example, accounting) the second host entry configured acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The LDAP host entries will be tried in the order in which they are configured.) To define a server host with a server group name, enter the following commands. The listed server must exist in global configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server ldap** *group-name*
5. **server** *name*
6. **exit**

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	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**aaa group server ldap** *group-name* **Example:** `Device(config)# aaa group server ldap name1`	Defines the AAA server group with a group name and enters LDAP server group configuration mode. All members of a group must be the of same type, that is, RADIUS, LDAP, or TACACS+.

	Command or Action	Purpose
Step 5	**server** *name* **Example:** `Device(config-ldap-sg)# server server1`	Associates a particular LDAP server with the defined server group. Each security server is identified by its IP address and UDP port number.
Step 6	**exit** **Example:** `Device(config-ldap-sg)# exit`	Exits LDAP server group configuration mode.

Configuring Search and Bind Operations for an Authentication Request

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **ldap server** *name*
5. **authentication bind-first**
6. **authentication compare**
7. **exit**

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.

	Command or Action	Purpose
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.

Configuring a Dynamic Attribute Map on an LDAP Server

You must create LDAP attribute maps that map your existing user-defined attribute names and values to Cisco attribute names and values that are compatible with the security appliance. You can then bind these attribute maps to LDAP servers or remove them as required. For more information about user-based firewalls, see the "User-Based Firewall Support" chapter in *Security Configuration Guide: Zone-Based Policy Firewall*.

Note To use the attribute mapping features correctly, you need to understand the Cisco LDAP attribute names and values as well as the user-defined attribute names and values.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ldap attribute map** *map-name*
4. **map type** *ldap-attr-type aaa-attr-type*
5. **exit**
6. **ldap server** *name*
7. **ipv4** *ipv4-address*
8. **bind authenticate root-dn** *user-name* **password** [**0 string** | **7** *string*] *string*
9. **base-dn** *string*
10. **attribute map** *map-name*
11. **exit**

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	**ldap attribute map** *map-name* **Example:** `Device(config)# ldap attribute-map map1`	Configures a dynamic LDAP attribute map and enters attribute-map configuration mode.
Step 4	**map type** *ldap-attr-type aaa-attr-type* **Example:** `Device(config-attr-map)# map type department supplicant-group`	Defines an attribute map.
Step 5	**exit** **Example:** `Device(config-attr-map)# exit`	Exits attribute-map configuration mode.

	Command or Action	Purpose
Step 6	**ldap server** *name* **Example:** `Device(config)# ldap server ldap_dir_1`	Specifies the LDAP server name and enters LDAP server configuration mode.
Step 7	**ipv4** *ipv4-address* **Example:** `Device(config-ldap-server)# ipv4 192.0.2.1`	Specifies the IP address of the LDAP server.
Step 8	**bind authenticate root-dn** *user-name* **password** [**0 string** | **7** *string*] *string* **Example:** `Device(config-ldap-server)# bind authenticate root-dn "cn=user1,cn=users,dc=sns,dc=example,dc=com" password example123`	Binds the attribute testmap to the LDAP server.
Step 9	**base-dn** *string* **Example:** `Device(config-ldap-server)# base-dn "dc=sns,dc=example,dc=com"`	(Optional) Configures the base DN that you want to use to perform search operations in the LDAP server.
Step 10	**attribute map** *map-name* **Example:** `Device(config-ldap-server)# attribute map map1`	Attaches the attribute map to a particular LDAP server.
Step 11	**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.

SUMMARY STEPS

1. **enable**
2. **clear ldap server**
3. **debug ldap**
4. **show ldap server**
5. **show ldap attributes**

DETAILED STEPS

Step 1 **enable**
Enables privileged EXEC mode.

- Enter your password if prompted.

Example:

```
Device> enable
```

Step 2 **clear ldap server**
Clears the Lightweight Directory Access Protocol (LDAP) server of the TCP connection.

Example:

```
Device# clear ldap server
```

Step 3 **debug ldap**
Displays information associated with LDAP.

Example:

```
Device# debug ldap
```

Step 4 **show ldap server**
Displays the LDAP server state information and various other counters for the server.

Example:

```
Device# show ldap server
```

Step 5 **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 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 the LDAP parameters:

```
ldap server server1
 bind authenticate root-dn “cn=administrator,cn=users,dc=nac-blr2,dc=cisco,dc=com password
 123”
 search-filter user-object-type objectclass
 base-dn "dc=sns,dc=example,dc=com"
 mode secure no-negotiation
 secure cipher 3des-ede-cbc-sha
```

Example: AAA Server Group

The following example shows how to configure the AAA server group:

```
aaa new-model
 aaa group server ldap server1
```

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: Dynamic LDAP Attribute Map and LDAP Server

The following example shows how to attach the attribute map to a particular LDAP server:

```
ldap attribute-map map1
 map type department element-req-qos
exit
ldap server ldap_dir_1
ipv4 192.0.2.1
 bind authenticate root-dn "cn=administrator,cn=users,dc=nac-blr2,dc=example,dc=com" password
 example123
 base-dn "dc=sns,dc=example,dc=com"
 attribute map map1
```

The following example shows how to attach the attribute map to an LDAP host running Active Directory (Microsoft) server software for successful user authentication:

```
ldap attribute-map map1
 map type sAMAccountName username
exit
ldap server ldap_dir_1
ipv4 192.0.2.1
 bind authenticate root-dn "cn=administrator,cn=users,dc=nac-blr2,dc=example,dc=com" password
 example123
 base-dn "dc=sns,dc=example,dc=com"
 attribute map map1
```

Additional References for Configuring LDAP

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
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
AAA	"Configuring Authentication" module

RFCs

RFC	Title
RFC 2830	*Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security*
RFC 4511	*Lightweight Directory Access Protocol (LDAP)*
RFC 4513	*Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms*
RFC 4514	*Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names*
RFC 4515	*Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters*
RFC 4517	*Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules*
RFC 4519	*Lightweight Directory Access Protocol (LDAP): Schema for User Applications*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring LDAP

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 Configuring LDAP

Feature Name	Releases	Feature Information
LDAP Integration with Active Directory	Cisco IOS 15.0(1)EX	Lightweight Directory Access Protocol (LDAP) is a standard-based protocol used to access directories. It is based on the client server model similar to RADIUS. LDAP is deployed on Cisco devices to send authentication requests to a central LDAP server that contains all user authentication and network service access information. The LDAP Integration with Active Directory feature provides authentication and authorization support for authentication, authorization, and accounting (AAA). The following commands were introduced or modified: **aaa group server ldap**, **authentication bind-first**, **authentication compare**, **bind authenticate**, **base-dn**, **clear ldap server**, **debug ldap**, **ipv4, mode secure**, **ldap server**, **search-filter**, **secure cipher**, **show ldap server**, **transport port**, **timeout**, **retransmit**.