Configuring LDAP for the Cisco Secure Access Control Server

Abstract

This document outlines deployment concepts for the Cisco Secure Access Control Server (ACS) when authenticating users of a Lightweight Directory Access Protocol (LDAP) directory server, and describes how to configure the Cisco Secure ACS using these concepts.

Introduction

If an authentication attempt fails against its internal list of users, the Cisco Secure ACS will try the selected databases configured in the Unknown User Policy. The external databases are attempted sequentially, in the configured order. Upon a successful attempt, the user is added to the Cisco Secure ACS internal database but marked for authentication by the appropriate database. For subsequent authentication attempts, ACS will try the supplied credentials directly against the previously successful external database.

One of the external databases supported is Generic LDAP, using standard LDAP to attempt to validate the users. This document describes how to configure the Generic LDAP authenticator in the Cisco Secure ACS.

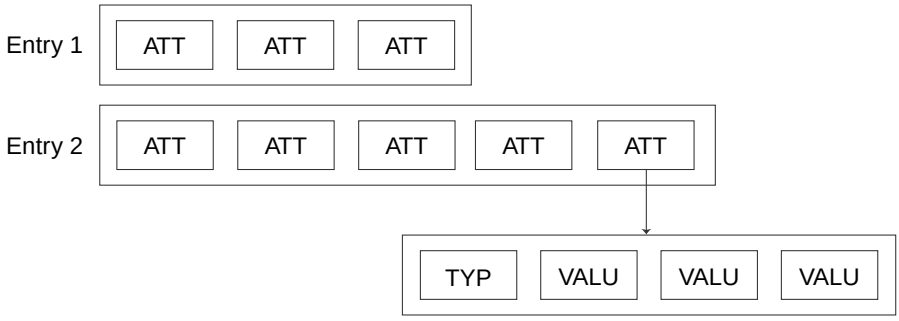
LDAP Concepts

This section outlines a minimal set of LDAP concepts necessary for configuration derivation. If you are well-versed in LDAP you might want to skip this section.

LDAP Entries and Attributes

The objects or concepts that are represented in the LDAP information model are contained in entries. These can represent users, groups, printers, and so forth. Each entry is constructed entirely from a list of attributes. Each attribute has a type and one or more values (see Figure 1).

Figure 1 Entries Composed of Attributes with Type and Values



The directory server handles the special attributes objectClass, DistinguishedName, and passwords differently.

Each entry has an objectClass attribute. The LDAP directory server uses this attribute to determine the entry types (an entry can be of more than one type). The entry types, in turn, define which attributes are required and which are optional. This information, often embedded elsewhere in the directory, is generally referred to as the *schema.*

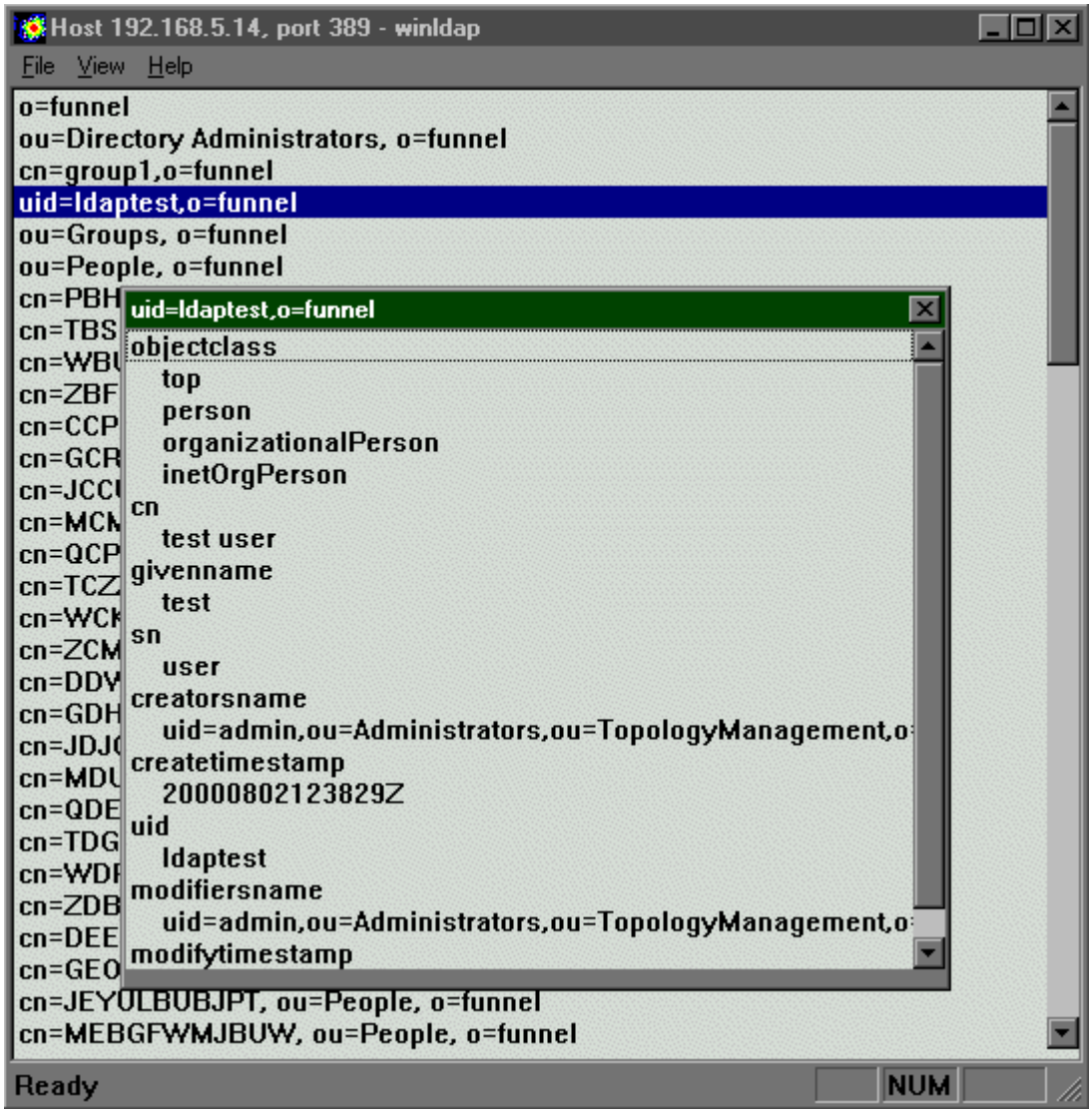
Figure 2 shows the results of examining a real entry in an LDAP server using a browser from the Netscape LDAP Software Development Kit (SDK). Most of the attributes are single values, but the objectClass attribute contains four values.

One important attribute not shown in the list displayed in Figure 2 is the ”Distinguished Name” or *dn.* The dn uniquely identifies the entry among all entries in the directory. In fact, the dn is not always stored as a single attribute, but can be synthesized, at least partly, from other attributes. Therefore, in the sample screenshot, for instance, the uid identifier is used as part of the dn.

The dn can be constructed under a generous set of rules, and this permits great flexibility for the directory layout. Normally, however, a tree structure is imposed using a hierarchy of component elements within the dn. These elements are called Relative Distinguished Names and are formatted as a little endian set of attributes. For example:

dn = uid = Fred, ou = QA Department, ou = Access Products, o = cisco

Figure 2 Directory Entry



Attributes containing passwords are normally hidden for security reasons. These are covered in more detail in the next section, “LDAP Binding.”

LDAP Binding

You typically configure LDAP directory servers so that passwords are not exposed. However, to validate that a user’s credentials are correct, you can use a bind to authenticate a user against a directory. This mechanism, which you use to validate Cisco Secure ACS users, is effectively a logon to the directory.

Simple LDAP Search Filters

Knowledge of search filters is useful in understanding the configuration information required to correctly set up the Cisco Secure ACS. You use a search filter to specify which records are returned by the LDAP directory server. In the case of the Cisco Secure ACS, the search filter can be represented as a string whose format is defined in RFC 1960[1] . The Cisco Secure ACS uses a restricted subset of this RFC.

Search filters are composed of attribute match requirements. For example, to construct a search filter to return all the entries in a directory that contain an attribute called *uid* with one value equal to *testuser*, the filter would be:

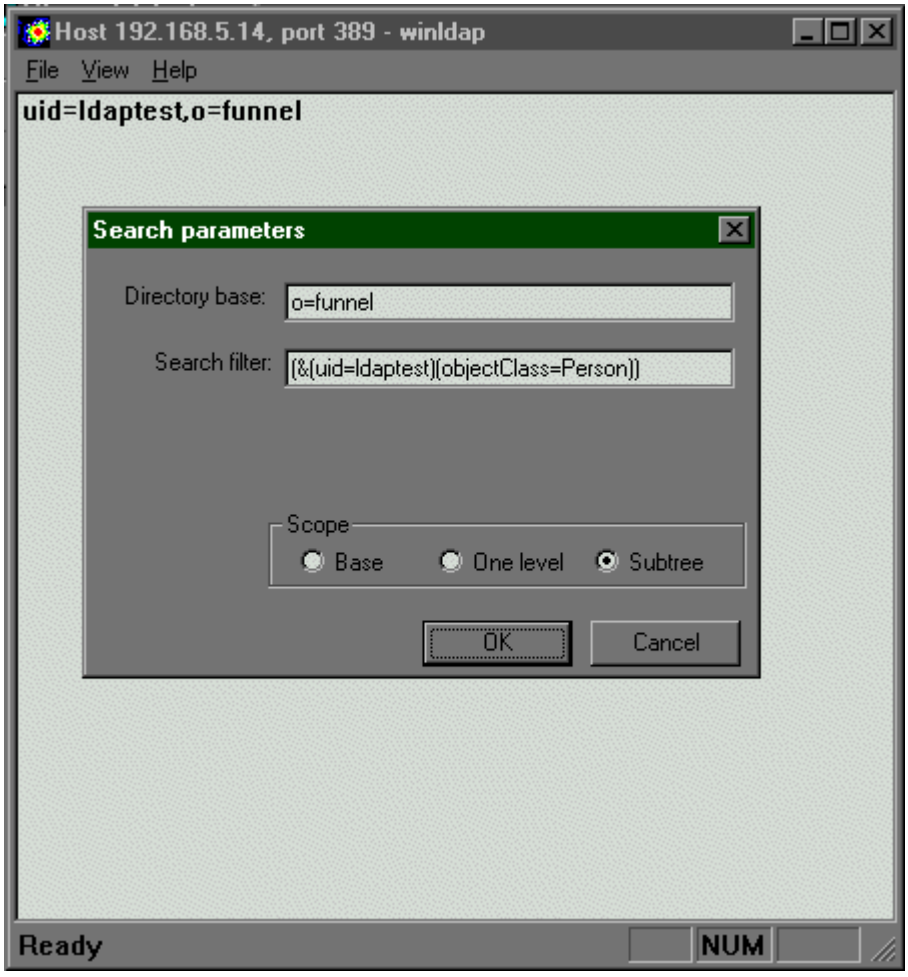
(uid = testuser)

Filters can be logically conjoined; so to add a further qualification to the above filter that the objectClass of the entries to be returned is "Person," we have:

(&(uid = ldaptest)(objectClass = Person))

Figure 3 shows the results of applying this search filter against a test directory.

Figure 3 Using a Search Filter



1. RFC 1960 "A String Representation of LDAP Search Filters." June 1996

Configuration

This section describes how the values required by the Cisco Secure ACS LDAP Database Configuration page are derived from the particular details of the target LDAP server. The configuration has been broken into two sections: information about the server and information about the schema.

LDAP Directory Server Information

The Connection

The first two fields on the LDAP Database configuration page, Hostname and Port, specify where the LDAP requests are sent. Hostname is either an IP address or a DNS. The port box contains the TCP/IP port the LDAP server is listening on.

LDAP Version

The Cisco Secure ACS negotiates with the server for a supported version. If this check box is unchecked, ACS does not try to negotiate using LDAP version 3. By default, this check box is selected.

Security Settings

LDAP communicates in plain text between the ACS server and the LDAP directory. You can configure this connection to use Secure Socket Layer (SSL) if a certificate has been obtained. If the Security check box is selected, you must provide the path to a certificate database. For further details on setting up SSL, see the section “Setting Up SSL.”

Administrator Credentials

To provide the authority necessary when obtaining group mapping information, you must provide a username and a password for an administrative entry that has permissions to search and retrieve the list of groups under a specified group subtree.

The admin dn must be fully qualified. You can obtain an admin user who has permissions over the standard directory namespace for a Netscape directory from the Netscape console under the Users and Groups tab, under the Directory button in the field Bind DN. For a default installation, this is normally:

‘uid = admin, ou = Administrators, ou = TopologyManagement, o = NetscapeRoot’

This entry is space sensitive.

Subtrees

There are two locations used as the root of the hierarchy for searching for users and groups, respectively. These must be fully specified in conventional distinguished name format. These are configured when the LDAP directory server is set up. Often these are left at the root level of the directory, that is:

‘o = cisco’

Schema

Retrieving the Groups for a Specified Subtree Root

This search uses a filter (described in the section “Simple LDAP Search Filters”). The filter specifies that objects are returned only if their objectclass indicates that they are a group:

(objectclass = groupObjectClass)

For example, using the default Netscape schema where:

groupObjectClass = GroupOfUniqueNames

(objectClass = GroupOfUniqueNames)

the value of the groupObjectClass field in the GUI must be equal to the value of the objectClass attribute in the target directory server that uniquely characterizes this entry as a group.

Logon

This search enables you to find users when given a login ID. It is performed during authentication so that we can perform a bind to validate the credentials, without the user needing to supply their complete, fully qualified name. The filter used for this search is as follows:

(&(objectclass = userObjectClass)(userObjectType = <<username>>))

For example, authenticating user ‘testuser’ and using the default Netscape schema where:

userObjectType = uid

userObjectClass = Person

these values are substituted into the filter. So, the following filter would be constructed for this search:

(&(objectclass = Person)(uid = testuser))

Consequently, the value of the userObjectClass field in the GUI must be equal to the value of the objectClass attribute in the target directory server, which uniquely characterizes this entry as a user. Furthermore, the value of userObjectType must be the name of attribute whose value is the login name for the user object.

Retrieving Groups for a User

This search is performed after authentication to find groups that contain a membership attribute equal to the user being authenticated. The syntax of the filter is:

(&(objectclass = groupObjectClass)(groupAttribute = <<username>>))

For example, authenticating user *testuser* and using the default Netscape schema where:

GroupObjectClass = GroupOfUniqueNames

GroupAttribute = UniqueMember

These values are substituted into the filter. Therefore, the following filter is constructed for this search:

(&(objectclass = GroupOfUniqueNames)(UniqueMember = testuser))

The value of the userObjectClass field in the GUI is described above. The GroupAttribute name must be the name of the attribute in a group that contains the list of members of the group as its values.

Summary of Schema Section

This section has shown how the values put into the Cisco Secure ACS in the schema section fit into LDAP searches. In summary:

UserObjectType	The name of attribute in a user entry object whose value is the login name for that user object.
UserObjectClass	The value of the objectClass attribute in the target Directory Server that uniquely characterizes this entry as a user.
GroupObjectType	The name of attribute in a group entry object whose value is the name for that group object.
GroupObjectClass	The value of the objectClass attribute in the target Directory Server that uniquely characterizes this entry as a group.
Group Attribute Name	The name of the attribute in a group that contains the list of members of the group as its values.

Setting Up SSL

This section describes how to set up Secure Socket Layer (SSL) when using the Netscape LDAP Directory Server and Certificate Management Server (CMS). This assumes that the LDAP Directory Server has already been set up for SSL using a certificate from the CMS. You can obtain externally verified certificates and use those instead.

Fundamentally, this method uses a Netscape browser pointed at a specific SSL port on the directory server to obtain the certificate and install it in the certificate database (cert7.db).

Step 1. Point the browser at the certificate server from which to get the CA certificate.

Step 2. Make a request for a personal certificate. For Netscape CMS:

Step 3. Point the browser at the certificate server port 444 to get a manual enrollment form. Fill in the details then send off the request.

Step 4. On the certificate server, verify this certificate request.

Step 5. On the intended SSL client, point the server back to the certificate server on the agent port. (This is very installation dependent, but the test CMS used port 8100). This imports the newly verified personal certificate.

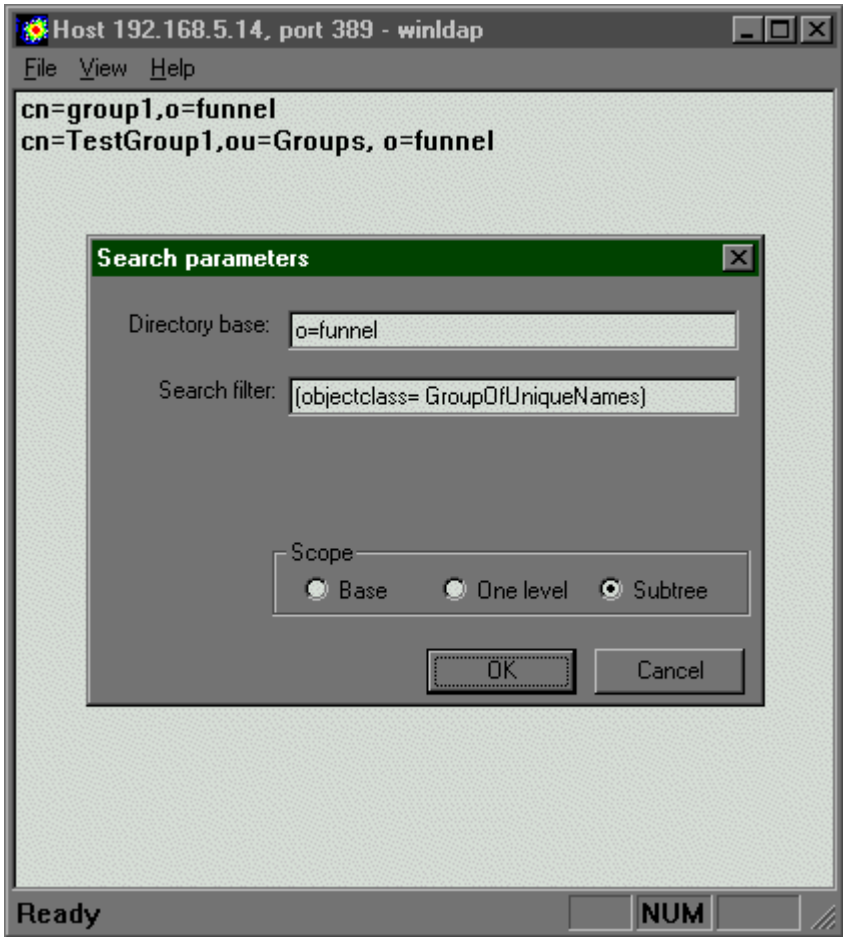
Step 6. Point the browser back at the LDAP SSL port, and accept the certificate. Locate the certificate database file (cert7.db) used by the browser, and enter the full path (including filename) into the Certificate Database Path field in the Cisco Secure ACS GUI.

Appendix A: The LDAP Browser

The screenshots in this document are from the sample browser in the Netscape LDAP Software Developer's Kit for Windows. The LDAP browser is a useful tool for validating that the schema information is correct for the directory server to be used. The schema entries can be substituted into search filters as described in the section "Schema."

For example, assuming that the groupObjectClass has been determined to be *GroupOfUniqueNames*, you can construct the search filter to mirror the search filter actually used in the Cisco Secure ACS (objectclass = GroupOfUniqueNames). The directory base is, in this case, the *Group Directory Subtree* value selected for ACS in the GUI.

Figure 4 Testing a Search Filter



The scope for searches within the Cisco Secure ACS is always set at *Subtree*, that is, a recursive search.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux Cedex 9
France
www.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia
Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

SPS / 05/2001