ExLibris
Aleph

ALEPH VERSION 19.01 and Later

How to Configure ALEPH with LDAP

ExLibris The bridge to knowledge

Last Update: December 30, 2009
Document Version 1.2

CONFIDENTIAL INFORMATION

The information herein is the property of Ex Libris Ltd. or its affiliates and any misuse or abuse will result in economic loss. DO NOT COPY UNLESS YOU HAVE BEEN GIVEN SPECIFIC WRITTEN AUTHORIZATION FROM EX LIBRIS LTD.

This document is provided for limited and restricted purposes in accordance with a binding contract with Ex Libris Ltd. or an affiliate. The information herein includes trade secrets and is confidential.

DISCLAIMER

The information in this document will be subject to periodic change and updating. Please confirm that you have the most current documentation. There are no warranties of any kind, express or implied, provided in this documentation, other than those expressly agreed upon in the applicable Ex Libris contract.

Any references in this document to non-Ex Libris Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Ex Libris product and Ex Libris has no liability for materials on those Web sites.

Documentation first produced August 2004.
Document version 1.2

Web address: http://www.exlibrisgroup.com

Table of Contents

Introduction

LDAP (Lightweight Directory Access Protocol) is a client-server protocol for accessing a directory service. Directories are repositories of network name information, essential for navigating loosely structured data like the Web. One type of directory common on TCP/IP networks is the Domain Name System, or DNS, which is a globally accessible table of domain names and their corresponding IP addresses.

Although DNS works well, it requires users to know the domain name they want. Applications like e-mail and network management can benefit from more natural directory entries that include, for instance, people's names, type of service, or geographic locale.

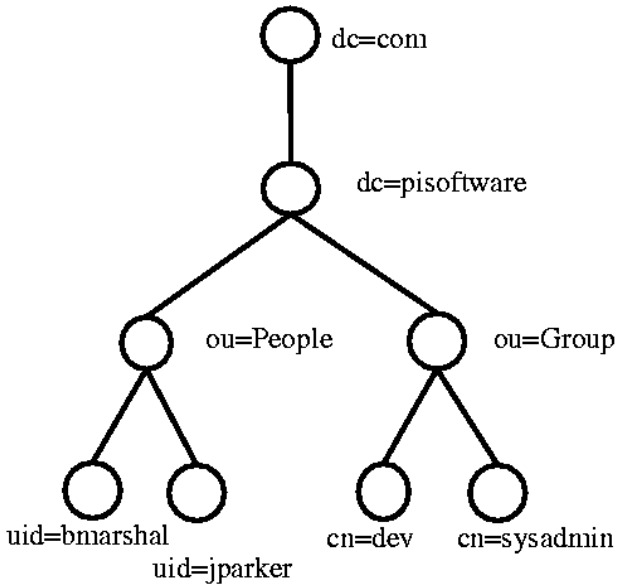
LDAP enables corporate directory entries to be arranged in a hierarchical structure that reflects geographic and organizational boundaries. Using LDAP, companies can map their corporate directories to actual business processes, rather than arbitrary codes.

LDAP directory servers store their data hierarchically. If you have seen top-down representations of DNS trees or UNIX file directories, an LDAP directory structure will be familiar ground. As with DNS host names, an LDAP directory record's Distinguished Name (DN for short) is read from the individual entry upwards through the tree to the topmost level.

An example of LDAP tree organization in XML might look like this:

```
dc=foobar, dc=com
        ou=customers
            ou=asia
            ou=europe
            ou=usa
        ou=employees
        ou=rooms
        ou=groups
        ou=assets-mgmt
        ou=nisgroups
        ou=recipes
```

Here is a graphic representation of an LDAP hierarchy:



The following is a typical example of the DN of an LDAP record:

```
cn=Oatmeal Deluxe,ou=recipes,dc=foobar,dc=com
```

or

```
uid=jparker,ou=People,dc=pisoftware,dc=com
```

A typical search command in an LDAP tree includes the search base (which is the tree branch to start a search from) and a search filter (the criteria to narrow down the number of records to be retrieved). Usually, the criteria is on one or few of the record attributes.

Let us assume that the search base is "**ou=People,dc=pisoftware,dc=com**" and the search filter is **"tel=972*"**. This search command retrieves all records under the tree branch "**ou=People,dc=pisoftware,dc=com"** with a phone number beginning with 972.

LDAP and ALEPH

ALEPH uses LDAP to authenticate patrons attempting to log in to the Web OPAC. To enable LDAP authentication, you must first set up the following two system components correctly:

- Ldap.conf
- Z308

ldap.conf

A simple ALEPH configuration file, `ldap.conf`, controls the following:

- LDAP server name and port
- Communication type (regular or secured)
- The search base the patron is under
- The search filter (which is the user name the patron types in and which should identify him/her uniquely.
- Initial binding setting (relevant only for LDAP servers that do not allow anonymous searches).

`ldap.conf`, should be located under the `$usr00_dev/usr00/tab` directory. From version 17.01 and above, the LDAP configuration file is only under `$usr00_dev/usr00/tab` for the demo libraries. For the customer libraries, it should be placed under the patron library's `$data_tab`, for example: `$miu50_dev/miu50/tab` (the default however stays `usr00`)
Example of the ldaf.conf file:

```
[general]
        host_name = exchange01
        port      = 389

        search_base = o=ExLibris
        search_filter = (uid=USERNAME)
```

This configuration file instructs ALEPH to connect to the exchange01 host through the 389 port, search the o=ExLibris subtree and retrieve all records with the uid attribute that match the username the patron typed in.

The following is an explanation for each of the configuration file variables:

host_name The host name to which to connect.

port The port to which to connect (the default is 389 for regular communication and 636 for secured communication.

secure_ldap Y/N flag for secure communication. The default is N.

init_bind_dn The full DN of the user for whom ALEPH performs the search. (Relevant only for a server that disallows anonymous searches.)

init_bind_password The password of the user for whom ALEPH performs the search. (Relevant only for a server that disallows anonymous searches.)

timeout A search times out after the defined number of seconds have elapsed. The default is 120.

search_base The subtree where the search starts.

search_filter A list that specifies criteria to filter records under the search_base subtree. The *USERNAME* reserved keyword is replaced with the username the patron typed in.

Note
The search_base and search_filter are repeatable. This means that you can search several subtrees (in order of appearance) in the event that one subtree fails to find a patron record.

Setting Up Z308 – Patron's ID

The Z308 table needs to be set up correctly in order to instruct the system to perform the authentication in LDAP and not in ALEPH. In the regular verification process, the password typed in is compared with the verification (password) field, which is Z308-VERIFICATION-DATA. However, in LDAP mode, the Z308-VERIFICATION-TYPE field must be set to 02, directing ALEPH to perform an LDAP search and to compare the password typed in with the LDAP record and not with ALEPH's.

This configuration has two implications:

- Z308 records must exist for the usernames the patron can type in. Those records must contain 02 in their Z308-VERIFICATION-TYPE field.
- If the Z308-VERIFICATION-TYPE field is set to 02, the Z308-VERIFICATION-DATA field (usually the patron's password) is not consulted. It might contain spaces, but Ex Libris recommends this field to be populated with the username.

Authentication Workflow

The following is the authentication workflow:

1. Patron types in a username and password on the ALEPH Web OPAC login page.
2. ALEPH looks for the username in the Z308 table. If the verification-type is 02, ALEPH redirects the request to the LDAP authentication script.
3. The LDAP script (named `authen_ldap.pl`) reads the configuration file, `ldap.conf`.

4 ALEPH connects to the given LDAP hostname and establishes a secure or non-secure communication (depending on the `secure_ldap` flag).

5 ALEPH uses `init_bind_dn` and `init_bind_password` (provided both are present) in order to perform the LDAP search as privileged patron, as oppose to an anonymous search.

6 ALEPH searches LDAP tree to find the patrons record according to the given `search_base` and `search_filter`.

7 If the results are not unique (or zero size result), repeat step 5 for the next given base/filter.

8 If the results comprised of one single record, ALEPH uses the "bind" operation to verify that the password is correct. If "bind" fails, repeat step 5 for the next given base/filter.

LDAP Authentication Method for GUI Staff Users

It is possible to allow server-side staff authentication via an LDAP server. The local (Z66) record does not have a password.

Authentication takes place using an external program named authen_staff_ldap.pl that resides in the `$aleph_authen` directory.

Note that although LDAP enables using username/passwords in lowercase, the staff user allows only uppercase IDs (Z66-USER-NAME).

The `$alephe_root/authen/ldap.conf` should be as follows:

```
[XML_SETTING]
xml_root_node   =       bor_authentication
[END]

[GENERAL]
host_name       =       il-dc02
port    =       389
ldap_version    =       3
secure_ldap     =       N
init_bind_dn              =                          CN=test    ldap,OU=Unknown
Mailboxes,OU=Users,OU=Israel,DC=Corp,DC=Exlibrisgroup,DC=com
init_bind_password      =       testldap123

search_base     =       OU=Users,OU=Israel,DC=Corp,DC=ExlibrisGroup,DC=Com
search_filter   =       sAMAccountName=USERNAME
[END]

[DEFAULTS]
expiry-date,today +200d
user_group,STAFF
[END]

[ATTRIBUTES_MAPPING]
cn      =       user_name
sn      =       profile-id
mail    =       email_address
[END]
```

The following is a description of some of the parameters:

secure_ldap Y/N flag, defaults to N. If the flag is set to Y, the SSL protocol is used to communicate with the LDAP server.

init_bind_dn Enter the full ~Sdn~T (distinguished name) for the initial bind.

init_bind_password: Enter the password of the DN for the initial bind.

search_base Enter the full path search in the LDAP directory tree of the user.

search_filter Enter the parameter to filter the results to return only one object.

The `search_base` and `search_filter` parameters can be repeated to search in more then one tree. `ldap_version` is not a mandatory field. If it is not present or if it is empty, `ldap.pl` attempts a bind with the default version, which is 2. If the LDAP server is a version 3 server, the `ldap_version` in the conf. table must be set to 3 for the bind to be successful.

Make sure that the following parameters exist in your files:

`In v500_18.01\Alephcom\Tab\ Alephcom.ini:`

```
Version=LDAP
Encryption=4
```

In /alephe/tab/ tab_version

```
!  1      2    3 4     5          6
!!!!!!-!!!!!-!-!-!!!!!!!!-!!!!!!!!!!
SER1.0 ALEPH Y 0
505XXX ALEPH Y 0 12345678
LDAP   ALEPH Y 4
BNCHMK ALEPH N 0
```

Troubleshooting Tips

- Examine the Web log file for an error messages regarding the LDAP script. It is possible that the Perl script is not executable. If this is the case, consult the Ex Libris support team.
- Verify `ldap.conf` is set up correctly and that the correct `ldap.conf` is being read (by viewing the Web log file).
- Verify that the patron Z308 record verification type is 02.
- Verify the patron Z308 record key type is defined in `tab_bor_id.lng`.
- Verify that `$alephe_root/aleph_start` contains a definition for `aleph_authen`, for example:

  ```
  setenv     aleph_authen $alephm_dev/alephm/source/authen
  ```

  and that the `authen_ldap.pl` script resides under the directory defined.

Debug Mode

You can activate the script in debug mode. This mode should only be used for initial testing and must not left activated in production since it reveals the patrons' passwords.

To activate debug mode:

Before restarting the www_server, type the following from the command line:

```
M505>> setenv AUTHEN_LDAP_DEBUG Y
```

Once debug mode is on, additional information is logged, such as the input parameter (username, password, etc.), the search command performed, and the results.

To deactivate debug mode:

Before restarting the www_server, type:

```
M505>> setenv AUTHEN_LDAP_DEBUG N
```