The DSpace Course - Configuring LDAP

Lewis, Stuart

http://hdl.handle.net/10673/57

Downloaded from DSpace Repository, DSpace Institution's institutional repository
Module: Configuring LDAP

Module overview:
This module follows on from the module ‘User management and authentication options’ which introduced the concepts of authentication and LDAP.

This module will cover the process of configuring DSpace to authenticate users with an LDAP server. Troubleshooting tools will be introduced to assist with the integration.

Module objectives:
By the end of this module you will:

1. Understand how DSpace uses LDAP for authentication
2. Be able to configure a DSpace instance to authenticate against an LDAP server
3. Know which tools to use and how to use them in order to test LDAP connection issues

Note
For the practical exercise, please refer to your sheet ‘Local instructions’ for details of the following:

- How to launch a terminal window and a web browser
- What the path to [dspace] and [dspace-src] is
- How to restart Tomcat
- What the URL of your DSpace installation is
- Where example files are located
An Introduction to LDAP

- Tree structure:
  - DC = domain component
  - OU = organisational unit
  - CN = common name
  - DN = distinguished name
    - My DN is:
      - CN=stuart,OU=users,DC=testathon,DC=net

An introduction to LDAP

LDAP is the Lightweight Directory Access Protocol. It is basically a directory of users whose accounts are built up in a hierarchy.

The DN (distinguished name) of a user is a unique name that identifies a single user in the tree. It is made up of several parts including their CN (common name), any OUs (organisational units) that they are in, and the DC (domain component).

A typical DN for a user in an LDAP tree with one OU could be:

CN=stuart,OU=users,DC=testathon,DC=net
How does DSpace use LDAP?

DSpace goes through 3 steps to authenticate a user against an LDAP server:

1. Collect username and password
   a. DSpace must first collect the username (netid) and password of the user from the web interface.
2. Bind to the LDAP server
   a. Using the user’s netid and password, it connects (binds) to the LDAP server. This allows it to make queries to the LDAP server.
   b. If DSpace can not bind to the LDAP server then the username and password must be incorrect, or the LDAP settings in the DSpace configuration file are incorrect.
3. Use the connection
   a. If the user already has an account in DSpace then they will be logged in.
   b. If the user does not already have an account then a new account will be created for them, using the details (name, email, telephone number) stored for that user in the LDAP server.
Stackable Authentication

- Stackable authentication
  - Stacks different authentication mechanisms on top of each other
  - Each is tried until one succeeds, or none succeed

Stackable authentication

DSpace makes use of a stackable authentication mechanism. This means that several authentication systems can be used, and when a user attempts to log in, their credentials are tried in each system. If none of the systems will authenticate the users then they are disallowed from logging in.

Often installations just use one mechanism, but you may wish to have several. For example you might wish to enable IP authentication so that users can login without a username, just because they are on campus. People off-campus can use LDAP, and administrators could use accounts in the built-in DSpace user database.
LDAP Settings

- LDAP settings:
  - ldap.provider_url = ldap://ldap.testathon.net:389/
  - ldap.id_field = cn
  - ldap.object_context = OU=users,DC=testathon,DC=net
  - ldap.search_context = OU=users,DC=testathon,DC=net
  - ldap.email_field = mail
  - ldap.surname_field = sn
  - ldap.givenname_field = givenName
  - ldap.phone_field = telephoneNumber

LDAP Settings

LDAP authentication is configured by setting 8 parameters. The following is taken from the main DSpace configuration file [dspace]/config/dspace.cfg:

```plaintext
# This setting will enable or disable LDAP authentication in DSpace.
# With the setting off, users will be required to register and login with
# their email address. With this setting on, users will be able to login
# and register with their LDAP user ids and passwords.
# This setting is only used by the JSPUI.
ldap.enable = false

# This is the url to the institution's ldap server. The /o=myu.edu
# may or may not be required depending on the LDAP server setup.
# A server may also require the ldaps:// protocol.
#ldap.provider_url = ldap://ldap.myu.edu/o=myu.edu

# This is the unique identifier field in the LDAP directory
# where the username is stored.
#ldap.id_field = uid
```
# This is the object context used when authenticating the user. It is appended to the ldap.id_field and username. For example uid=username,ou=people,o=myu.edu. This must match the LDAP server configuration.
#ldap.object_context = ou=people,o=myu.edu

# This is the search context used when looking up a user’s LDAP object to retrieve their data for autoregistering. With ldap.autoregister turned on, when a user authenticates without an EPerson object, a search on the LDAP directory to get their name and email address is initiated so that DSpace can create an EPerson object for them. So after we have authenticated against uid=username,ou=people,o=byu.edu we now search in ou=people for filtering on [uid=username]. Often the #ldap.search_context is the same as the ldap.object_context parameter. But again this depends on each individual LDAP server configuration.
#ldap.search_context = ou=people

# This is the LDAP object field where the user's email address is stored. "mail" is the default and the most common for LDAP servers. If the mail field is not found the username will be used as the email address when creating the eperson object.
#ldap.email_field = mail

# This is the LDAP object field where the user's last name is stored. "sn" is the default and is the most common for LDAP servers. If the field is not found the field will be left blank in the new eperson object.
#ldap.surname_field = sn

# This is the LDAP object field where the user's given names are stored. This may not be used or set in all LDAP instances. If the field is not found the field will be left blank in the new eperson object.
#ldap.givenname_field = givenName

# This is the field where the user's phone number is stored in the LDAP directory. If the field is not found the field will be left blank in the new eperson object.
#ldap.phone_field = telephoneNumber
Enabling LDAP

LDAP is enabled using the stackable authentication system used by DSpace. LDAP is handled by the authentication class:

```
org.dspace.authenticate.LDAPAuthentication
```

This class must be added to the list of authentication methods used in dspace.cfg under the `plugin.sequence.org.dspace.authenticate.AuthenticationMethod` key.

In order to enable LDAP in the JSP user interface, the key `ldap.enable` must also be set to true. This is not required for the XML interface or SWORD.
Testing LDAP settings

- Use an LDAP client
  - LDAP Browser:
    - Allows you to use the settings in dspace.cfg to log in to an LDAP server and view the output visually.

LDAP client

An LDAP client can be used to log in to an LDAP server and get a visual representation of the contents. If the settings work in the LDAP client, then they should work in DSpace.

An LDAP browser can be downloaded from:

http://www-unix.mcs.anl.gov/~gawor/ldap/

Use your LDAP settings to log in, and look at the results.
Enter settings in the LDAP browser by using the quick connect option:

Once you have connected you can browse the LDAP tree:
Practical – enable LDAP

- LDAP settings:
  - ldap.provider_url = ldap://ldap.testathon.net:389/
  - ldap.id_field = cn
  - ldap.object_context = OU=users,DC=testathon,DC=net
  - ldap.search_context = OU=users,DC=testathon,DC=net
  - ldap.email_field = mail
  - ldap.surname_field = sn
  - ldap.givenname_field = givenName
  - ldap.phone_field = telephoneNumber
- Users are: stuart, john and carol.
- Passwords are the same as the usernames

Enabling LDAP

On your test DSpace instance, enable LDAP using the following settings:
- ldap.provider_url = ldap://ldap.testathon.net:389/
- ldap.id_field = cn
- ldap.object_context = OU=users,DC=testathon,DC=net
- ldap.search_context = OU=users,DC=testathon,DC=net
- ldap.email_field = mail
- ldap.surname_field = sn
- ldap.givenname_field = givenName
- ldap.phone_field = telephoneNumber

There are three users:
1. Username: stuart  Password: stuart
2. Username: john  Password: john
3. Username: carol  Password: carol
Credits

- These notes have been produced by:
  - Stuart Lewis & Chris Yates
  - Repository Support Project
    - http://www.rsp.ac.uk/
  - Part of the RepositoryNet
  - Funded by JISC
    - http://www.jisc.ac.uk/