LDAP Hierarchical Authentication with Active Directory

Files:

- *dspace*/config/dspace.cfg

Instructions:

These instructions involve setting up DSpace 1.5.2 to use LDAP Hierarchical Authentication with Microsoft's Active Directory (but these instructions should help anyone looking to set this up for an LDAP server that doesn't allow anonymous binds). The LDAP Hierarchical Authentication method is particularly useful when you have users in separate LDAP containers and need to to have users in different containers log in. For example, you may have students in one container and faculty/staff in another container, with both containers at the same level in the hierarchy of your organization's LDAP server.

Please note that these instructions assume that ePerson accounts are created, in advance, for the LDAP users that will log in. I haven't tested for auto account generation upon login.

The LDAP Hierarchical Authentication method uses some of the standard LDAP authentication method's configuration settings in the dspace.cfg file.

Before beginning, make sure that you have a generic account configured on your LDAP server that can be used for searching for users. Active Directory does not allow anonymous binds for searches, so you will need a user account to do the bind and find the DSpace user in the correct LDAP container, wherever that is. For this example, I will assume that we are connecting to ldap.example.com as the LDAP server using ldapuser as the LDAP search user and ldappassword as the LDAP search user password.

Edit your dspace.cfg file so that it has the following lines:

```
plugin.sequence.org.dspace.authenticate.AuthenticationMethod = org.dspace.authenticate.
LDAPHierarchicalAuthentication
```

```
ldap.enable = true
```

```
ldap.provider_url = ldap://ldap.example.com:389/
```

```
ldap.id_field = cn
```

```
ldap.object_context = cn=Users,dc=example,dc=com
```

```
ldap.search_context = dc=example,dc=com
```

```
ldap.email_field = mail
```

```
ldap.surname_field = sn
```

```
ldap.givenname_field = givenName
```

```
ldap.phone_field = telephoneNumber
```

```
ldap.search_scope = 2
```

```
ldap.search.user = cn=ldapuser,cn=Users,dc=example,dc=com
ldap.search.password = ldappassword
```

```
ldap.netid_email_domain = @example.com
```

Restart Tomcat and try to log in. Any errors will be logged in the *dspace*/logs/dspace.log file.

Notes:

- These settings, of course, assume that you created the ldapuser account and left it in the default Users container in Active Directory. If your ldapuser is in a different place, change the

  ```
  ldap.search.user
  ```

  to reflect the actual location;

  ```
  ldap.search.user
  ```

  must have the full, correct string of your search user in order to log in.