LDAP Authentication

Introduction

This article will walk you through configuring LDAP for Sakai (Using the Unboundid SDK).

> **This article applies to Sakai 19.x and greater versions. If you're using Sakai 12.x or prior versions try these instructions:**
>
> LDAP in Sakai 2.5

Stop your Tomcat instance and edit this file:

Edit this file in your Tomcat folder:

```
$TOMCAT_HOME/components/sakai-provider-pack/WEB-INF/components.xml
```

Uncomment the unbound-id provider

```
 <!--  import resource="unboundid-ldap.xml" / -->
```

Edit the ldap properties in the Unboundid LDAP provider:

Edit this file in your Tomcat folder:

```
$TOMCAT_HOME/components/sakai-provider-pack/WEB-INF/unboundid-ldap.xml
```

Edit the most important properties, at a minimum you will need to setup:

- the ldapHost (Host name or address of your LDAP server):

```
<property name="ldapHost">
    <value>ldap.server.ac.uk</value>
</property>
```

- the basePath (Base DN for directory searches):

```
<property name="basePath">
    <value>ou=users,ou=university,dc=something,dc=somethingelse</value>
</property>
```

If you require an authenticated bind to your LDAP server, you will also need the following properties setup:

- the ldapUser (DN to which to bind for directory searches):

```
<property name="ldapUser">
    <value>cn=username,ou=staff,ou=users,ou=university,dc=something,dc=somethingelse</value>
</property>
```

- the ldapPassword (Password for ldapUser defined above):

```
<property name="ldapPassword">
    <value>somepassword</value>
</property>
```

- autoBind (Indicate if connection allocation should implicitly bind as the ldapUser above):

```
<property name="autoBind">
       <value>true</value>
</property>
```

You will also need to uncomment and review some of the settings that map LDAP attributes to Sakai attributes:

```
<property name="attributeMappings">
<map>
<!--
<entry key="aid"><value>krb5PrincipalName</value></entry>
-->
<entry key="login"><value>uid</value></entry>
<entry key="firstName"><value>givenName</value></entry>
<entry key="preferredFirstName"><value>preferredName</value></entry>
<entry key="lastName"><value>sn</value></entry>
<entry key="email"><value>mail</value></entry>
<entry key="groupMembership"><value>groupMembership</value></entry>
<entry key="jpegPhoto"><value>jpegPhoto</value></entry>
</map>
```

Start your Tomcat instance and test!

Restart Tomcat and see if you can login using a username and password combination that would come from LDAP. Especially try using a username and password that has NEVER logged into Sakai to test it really is working.Also try a user account that exists only in Sakai, ie create a user 'testuser1' and try to login with that. It should also work (as Sakai will fall through LDAP to its internal database if no user is found in LDAP that matches) .

You should also test the User membership tool in the Administration Workspace, try searching for LDAP users.

Troubleshooting

Subscribe and post a message in sakai-dev[at]apereo.org.