Modifying a Quick Install IdP to Authenticate Against LDAP

Richard Turpin
Swindon College

These guides have been prepared by organisations who participated in the JANET Shibboleth on Windows project. These guides are provided for general information purposes and are not intended to be definitive or exhaustive guides to the configuration, installation and implementation of Shibboleth On Windows.

Modifying a Quick Install IdP to authenticate against LDAP

By default the Quick Install IdP authenticates using Kerberos. This document describes how you might want to change this to using LDAP authentication.

Why would you want to do this?

In the situation we ran into, the Active Directory was a forest with separate domains for staff and students. Using Kerberos meant that the user had to specify the domain when logging in (rod@staff.coll.ac.uk or 37940@student.coll.ac.uk). This was considered cumbersome and, since the login names were unique across both domains, we decided to authenticate against the global catalogue of the forest.

Preparing the install

It is a good idea to get the install working in all other aspect before starting this. In particular you should get attribute resolution working.

It should be noted that only a very small part of this job is to do with configuring Shibboleth, the rest is to do with configuring Tomcat.

1. Download the latest version of the Virginia Tech LDAP authorization module as described at http://www.middleware.vt.edu/doku.php?id=middleware:opensource:ldap. Place the download war file into

   ```
   c:\program files\Internet2\CaptiveTomcat5.5\Server\Lib
   ```

2. Modify the Tomcat's <Realm>, in the file

   ```
   c:\program files\Internet2\CaptiveTomcat5.5\Conf\Server.xml
   ```

   to read:

   ```
   <Realm
       className="org.apache.catalina.realm.JAASRealm
       appName="Tomcat"
       userClassNames="edu.vt.middleware.ldap.jaas.LdapPrincipal"
       roleClassNames="edu.vt.middleware.ldap.jaas.LdapRole" />
   ```

3. You now need to instruct JAAS to use the VT LDAP library and to give it a few parameters. You do this by editing the file

   ```
   c:\program files\Internet2\CaptiveTomcat5.5\Conf\jaas.conf
   ```

   Here is the example we used:

   ```
   Tomcat {
       edu.vt.middleware.ldap.jaas.LdapLoginModule required
         host="gcserver.int.coll.ac.uk"
         base="DC=int,DC=coll,DC=ac,DC=uk"
         port="3268"
         serviceUser="username@int. coll.ac.uk"
         serviceCredential="password"
         userField="sAMAccountName"
         userRoleAttribute="objectClass"
         subtreeSearch="true";
   };
   ```

   To note:
   - Host has to point to a root AD server, and one with the Global Catalogue
   - The port has to be 3280 (which is the Global catalogue)
   - serviceUser and serviceCredential should not be required. If you supply them, use the same username password that you use in resolver.xml.
   - userRoleAttribute is used to supply a role to JAAS, which Tomcat will then use to police which users can access the IdP (we'll see how to do this below). In the example I used "objectClass", so I could test in Tomcat against "user". You might want to experiment with "memberOf" if you want finer granularity of control.

4. We now need to set up Tomcat to listen to these new roles we have defined. To protect the root of the service (we'll use this to test) edit this file

   ```
   C:\Program Files\Internet2\CaptiveTomcat5.5\webapps\ROOT\WEB-INF\web.xml
   ```

   In two places you will see a line like this

   ```
     <role-name>idpuser</role-name>
   ```

   In both places add another line like this

   ```
     <role-name>user</role-name>
   ```

5. Start and stop Tomcat and try to browse to

   ```
   https:\\localhost:8442\
   ```

   You will be prompted for a BasicAuth username & password (a dialogue box will pop up). Enter the username and password from a user inside the forest. You should get to the Tomcat home page.

6. We now need to declare these roles to the Shibboleth application. To do make a similar edit as you did in step 4 (defining the new <role-name> "user") to the file

   ```
   C:\Program Files\Internet2\IdPInstall\webAppConfig\dist.idp.tomcat2k3.xml
   ```

7. Stop Tomcat and redeploy the war file. Do this by going to

   ```
   C:\Program Files\Internet2\IdPInstall
   ```

   from a command line and typing "ant", and accepting (<CR>) all the defaults. You may find that you get an error when running ant, in which case you will have to edit the file build.properties to set up values for "tomcat.password" and "tomcat.url". These can be set to any value – they are not actually used during or after the installation.

   There are some issues with deploying into Tomcat like this so I usually delete the old war file and directory from the webapps directory before I run ant.

8. You should then be ready to test again.