Tomcat Shibboleth Config

Overview

This document explains how to use Shibboleth with Tomcat and the Apache web server. You should already have Apache working with Shibboleth before you proceed. If not, refer to Install and Configure SAML Service Provider (SP) Software.

Shibboleth Configuration

For Apache to pass Shibboleth attributes to Tomcat, the attributes must be stored in environment variables with a special prefix. Edit the shibboleth2.xml file and find the ApplicationDefaults element. Add the attribute attributePrefix with a value of "AJP_". For example, your ApplicationDefaults element might look like this:

```
<ApplicationDefaults entityID="https://your-server.ucsf.edu/shibboleth"
    REMOTE_USER="eppn persistent-id targeted-id" attributePrefix="AJP_">
```

Restart shibd to load the new configuration.

Apache Configuration

You can make the following changes either in the main httpd.conf file or in a file under the conf.d directory. For example, the proxy_ajp.conf and shib.conf files usually exist in conf.d on RedHat systems and are good places to make the changes.

Configure Apache to pass requests for the path to your web application on to Tomcat. Add the following line, replacing "my-application" with the path to your application.

```
ProxyPass /my-application ajp://localhost:8009/my-application
```

If you are not serving any content directly from Apache, but only from Tomcat, you can pass all traffic instead:

```
ProxyPass / ajp://localhost:8009/
```

Configure Apache to require Shibboleth authentication for the path to your web application. Add the following lines, again replacing "my-application" with the path to your application. If you wish to require Shibboleth for all content, replace "/my-application" with "/".

```
<Location /my-application>
  AuthType shibboleth
  ShibRequestSetting requireSession 1
  require valid-user
</Location>
```

Restart Apache to load the new configuration.

Tomcat Configuration

Edit the server.xml file, and find the AJP Connector element on port 8009. It should look something like this:

```
<Connector port="8009" protocol="AJP/1.3" />
```

This line may be "commented out," with <!-- on a line before and --> on a line after. If so, remove those lines. If you cannot find the AJP connector element, simply create it from the code above.

In order to receive authentication information from Shibboleth, you must disable Tomcat's native authentication. Set the tomcatAuthentication attribute to "false" - see below for an example.

If your Apache web server is using SSL/HTTPS (and it should be), you need to tell Tomcat about that fact so that it can construct internal URLs correctly. Set the scheme attribute to "https" and the proxyPort attribute to "443" - see below for an example.

For increased security, disable access to the connector from anywhere but the local system. Set the address attribute to "127.0.0.1" - see below for an example.

When you are finished making changes, your connector should look something like this:

```
<Connector port="8009" protocol="AJP/1.3" tomcatAuthentication="false" scheme="https" redirectPort="443"
address="127.0.0.1" />
```

Restart Tomcat to load the new configuration. Now your Tomcat web applications should see all of the Shibboleth attributes. To retrieve them, use request.getRemoteUser() or request.getAttribute("ATTRIBUTE NAME"). Note that request.getAttributeNames() will not list Shibboleth attributes – you must request each attribute individually by name.