Newcastle University - Protecting UI With Shib

At Newcastle University we currently protect access to the Grouper User Interfaces with Shibboleth. Any users trying to access the UI will need to create a valid session with Shibboleth, before being granted or denied access to the Grouper application.

The following page will explain how we have achieved this, there maybe some difference in configurations required depending on server set up.

1. The first step is to configure Shib so that it will protect any content that lives under the main Grouper install directory, to do this we use the following location block in our Shib conf file;

```
<Location /grouper>
Authtype shibboleth
ShibRequireSession On
require valid-user
</Location>
```

2. We configure our Tomcat server to take the headers from Apache, in the server.xml configuration file in our<TOMCAT-HOME>/conf directory, we define the AJP(8009) connector not to use tomcat Authentication;

```
<Connector port="8009" protocol="AJP/1.3" tomcatAuthentication="false" redirectPort="8443" />
```

3. We currently use mod_proxy to forward requests for /grouper to our Tomcat install

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

On the install of Grouper 1.5 and the new Lite UI, we encountered problems when accessing the lite UI, when browsing to https://<server-name>/grouper /grouperUi/appHtml/grouper.html?operation=SimpleMembershipUpdate.index, we encountered an HTTP 403 error. This subsequently highlighted problems when trying to access the admin UI using the link from the grouper holding page, https://<server-name>/grouper/callLogin.do, which also gave us a HTTP 403 error.

With the help of the Grouper user mailing list, solutions to solve these problems were pointed out which we have implemented in our install successfully.

The main way to overcome the authentication problems was to make use of the CAS contribution, more details of which can be found on the Yale CAS auth page.

Gary pointed out the key areas from the CAS contribution that would solve the problems we were having with the 403 errors, these changes are documented below;

NOTE: By adding in the CAS contribution to the build of the UI solved the problems, below highlights the configurations that are specific to what we were wanting to achieve.

Grouper Admin UI

When accessing the admin UI through https://<server-name>/grouper/callLogin.do, this will call the default authentication method for Grouper, when protected by Shib it needs to bypass this page and go straight to the Grouper home page. This can be done by amending the action path for callLogin in the struts-config.xml, amend this so that it forwards the request to home.do rather than login.do;

```
<action path="/callLogin" scope="request"
type="edu.internet2.middleware.grouper.ui.actions.CallLoginAction"
unknown="false" validate="false">
<forward name="callLogin" path="/home.do" redirect="true"/>
</action>
```

Once this change has been put in place, when the callLogin action is called it will forward the user straight through to the home page as they have already identified themselves through Shib.

web.xml

To tell the grouper webapp not to authenticate (leave it to the web server), take out this section (all security stuff):

```
<security-constraint>
    <web-resource-collection>
      <web-resource-name>UI</web-resource-name>
      <url-pattern>/grouperUi/app/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
      <role-name>*</role-name>
    </auth-constraint>
  </security-constraint>
<!--Inserting tag from base file. Merge file was file:/C:/mchyzer/grouper/trunk/grouper-ui/temp/99.web.core-
filters.xml-->
<security-constraint>
    <web-resource-collection>
      <web-resource-name>UI</web-resource-name>
      <url-pattern>/grouperUi/appHtml/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
      <role-name>*</role-name>
    </auth-constraint>
  </security-constraint>
<!--Inserting tag from base file. Merge file was file:/C:/mchyzer/grouper/trunk/grouper-ui/temp/99.web.core-
filters.xml-->
<security-constraint>
    <web-resource-collection>
      <web-resource-name>UI</web-resource-name>
      <url-pattern>/grouperExternal/app/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
      <role-name>*</role-name>
    </auth-constraint>
  </security-constraint>
<!--Inserting tag from base file. Merge file was file:/C:/mchyzer/grouper/trunk/grouper-ui/temp/99.web.core-
filters.xml-->
<security-constraint>
    <web-resource-collection>
      <web-resource-name>UI</web-resource-name>
      <url-pattern>/grouperExternal/appHtml/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
      <role-name>*</role-name>
    </auth-constraint>
  </security-constraint>
<!--Inserting tag from base file. Merge file was file:/C:/mchyzer/grouper/trunk/grouper-ui/temp/99.web.core-
filters.xml-->
<security-constraint>
    <web-resource-collection>
      <web-resource-name>Tomcat login</web-resource-name>
      <url-pattern>/login.do</url-pattern>
    </web-resource-collection>
    <auth-constraint>
       <!-- NOTE:  This role is not present in the default users file -->
       <role-name>*</role-name>
    </auth-constraint>
  </security-constraint>
<login-config>
    <auth-method>BASIC</auth-method>
    <realm-name>Grouper Application</realm-name>
  </login-config>
<!--Processing security-role-->
<!--Inserting tag from base file. Merge file was file:/C:/mchyzer/grouper/trunk/grouper-ui/temp/99.web.core-
filters.xml-->
<security-role>
    <description>
      The role that is required to log in to the Grouper UI
    </description>
    <role-name>*</role-name>
  </security-role>
```

This change will now allow users to access through to the lite Ui through the login link or the admin ui when the user has a valid Shib Session, if they do not have a session they are directed to the Shib login page.

The configurations shown above maybe slightly different for other environments, though hopefully it will be of some help.

See Also

For an overview of authenticating to Grouper using Shib, see also the Grouper UI Training Video, around minute 7.30.