Grouper web services - authentication - Tomcat authentication

If you want to use tomcat authentication, you can do that. Generally you should not use the tomcat-users.xml file (use grouper built-in authn instead), if you use LDAP or something else it could be useful.

Note that in v2.5+ the container uses tomee which is essentially tomcat (same authn config)

Manage users

If you are using tomcat ldap authn, manage users in your ldap. This is an example using tomcat-users.xml file which is not convenient in container, but as an example

```
<user username="THE_PRINCIPAL" password="THE_PASSWORD" roles="grouper,grouper_user"/>
```

Configure

Note the file locations in the container are listed in the v2.5 container documentation

File	Value	Description
grouper.hibernate.properties	grouper.is.ws.basicAuthn=false	This is the default provided with container, do not overlay

<table>
<tr><td>web.xml</td><td>Make sure the appropriate security configs are there, this is an example in the v2.5 container

<pre>
<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns:j2ee="http://java.sun.com/xml/ns/j2ee" xmlns:
xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee
http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd"
  version="2.4">

  <security-constraint>
    <web-resource-collection>
      <web-resource-name>Web services</web-resource-name>
      <url-pattern>/services/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
      <role-name>grouper_user</role-name>
    </auth-constraint>
  </security-constraint>

  <security-constraint>
    <web-resource-collection>
      <web-resource-name>Web services</web-resource-name>
      <url-pattern>/servicesRest/*</url-pattern>
    </web-resource-collection>
    <auth-constraint>
      <!-- NOTE: This role is not present in the default
users file -->
      <role-name>grouper_user</role-name>
    </auth-constraint>
  </security-constraint>

  <!-- Define the Login Configuration for this Application -->
  <login-config>
    <auth-method>BASIC</auth-method>
    <realm-name>Grouper Application</realm-name>
  </login-config>

  <!-- Security roles referenced by this web application -->
  <security-role>
    <description>
      The role that is required to log in to web service
    </description>
    <role-name>grouper_user</role-name>
  </security-role>

</web-app>
</pre></td><td>Overlay this, and do not include any servlet mappings etc</td></tr>
<tr><td>server.xml</td><td>ajp 8009 connector element: tomcatAuthentication="true"</td><td>Tomcat is doing authn so that attribute needs to be true</td></tr>
<tr><td>server.xml</td><td>add in any other configs, e.g. for ldap authn

<pre>
<Realm className="org.apache.catalina.realm.JNDIRealm"
connectionURL="ldaps://ldap.ad.ufl.edu:636"
connectionName="CN=something-grouper,OU=Grouper,OU=Service
Accounts,OU=somead,DC=ad,DC=school,DC=edu"
connectionPassword="XXXXX"
userBase="OU=users,DC=ad,DC=ufl,DC=edu"
userSubtree="true"
userSearch="(userPrincipalName={0})"
adCompat="true"
allRolesMode="authOnly"
/>
</Realm>
</pre></td><td>See the tomcat documentation for correct location</td></tr>
</table>

grouper-ws.properties	ws.security.non-rampart.authentication.class =	This should be blank (get remote_user) This is the default provided with container, do not overlay
grouper-www.conf	Has no auth directives	This is the default provided with container, do not overlay for authn reasons