Single Sign On - Jetty HashSSORealm

Single Sign On - Jetty HashSSORealm

There are very many single sign on technologies available, but on this page we discuss a very simple implementation provided in the standard distro, the HashSSORealm.

The HashSSORealm permits a user to authenticate with one web application, and then have that authentication and authorization shared by other web applications deployed in the same instance.

Configuration

The key is to configure a single instance of the HashSSORealm for all web applications that wish to share authentication and authorization information, and then plug that instance into each UserRealm configured for each web application.

Here's the definition of a HashSSORealm instance:

```
<New id="sso"
class="org.mortbay.jetty.security.HashSSORea
lm">
</New>
```

Now, if we have web applications A and B, we would plug the instance we defined above into the configurations for both:

Web App A

```
<Configure
class="org.mortbay.jetty.webapp.WebAppContex
t">
  <Set name="contextPath">/A</Set>
  <Set name="war"><SystemProperty
name="jetty.home"
default="."/>/webapps/A</Set>
  <Get name="securityHandler">
    <Set name="userRealm">
      <New
class="org.mortbay.jetty.security.HashUserRe
alm">
            <Set name="name">My Realm</Set>
            <Set
name="config"><SystemProperty
name="jetty.home"
default="."/>/etc/realm.properties</Set>
            <Set name="sSORealm"><Ref
id="sso"/></Set>
      </New>
    </Set>
  </Get>
</Configure>
```

Web App B

```
<Configure
class="org.mortbay.jetty.webapp.WebAppContex
t">
  <Set name="contextPath">/B</Set>
  <Set name="war"><SystemProperty
name="jetty.home"
default="."/>/webapps/B</Set>
  <Get name="securityHandler">
    <Set name="userRealm">
      <New
class="org.mortbay.jetty.security.HashUserRe
alm">
            <Set name="name">My Realm</Set>
            <Set
name="config"><SystemProperty
name="jetty.home"
default="."/>/etc/realm.properties</Set>
            <Set name="sSORealm"><Ref
id="sso"/></Set>
      </New>
    </Set>
  </Get>
</Configure>
```

Don't Forget!

You probably need to set up your Session cookie configuration to allow a session id established by one web app to be shared by another. By default, the Session cookie path is that of the context path of the related page. So, if you have web app A at /A and web app B at /B, a session id established by /A would not be able to be used by /B, making single sign-on impossible.

So, you need to configure a path that is valid for all the webapps that wish to share the session. In the example above, the only common path is "/". However, if you have 2 webapps, one at "/one" and the other at "/one/two", you could configure the common path as "/one".

Check the wiki page Session Configuration for information on how to configure Session cookies.