How to Configure Servlet Container Authentication

Fedora relies on its servlet container to provide authentication. User credentials are configured in your web application container, usually in a properties file or XML file. This document describes how to set up Fedora and either Tomcat or Jetty to enable HTTP Basic Authentication, using simple user files. Consult your web application server documentation for other ways to configure and manage users. Fedora can handle any user principal passed to it by the servlet container, as provisioned by any of the container's supported authentication mechanisms.

- Container Roles
- Configure your repo.xml file
- Configure your repository.json file
- Configure your web.xml
- Configure your web application container
    - Jetty
    - Tomcat

Container Roles

Fedora uses two container roles to determine its authorization behavior. The superuser role is **fedoraAdmin**. Users with this role are not subject to any further authorization checks, and thus can perform any operations on the repository. This is comparable to the **fedoraAdmin** superuser role in Fedora 3, used for Fedora 3 API-M operations. The regular user role is **fedoraUser**. Users with this role *are* subject to authorization checks by the Web Access Control system. The exact permissions any regular user has are determined per request by looking at the effective ACL of the requested resource, the requesting user's security principals, and the nature of the request (HTTP method, content-type, etc.).

Configure your repo.xml file

See the sample Spring configuration for setting up a repo.xml to use servlet container authentication.

To specify a local repo.xml configuration, provide the system property as follows:

```
JAVA_OPTS="... -Dfcrepo.spring.repo.configuration=file:/local/repo.xml"
```

Configure your repository.json file

Modify the security section to enable both authenticated (via authentication provider) and internal sessions between Fedora and ModeShape.

It should contain a "security" element that matches this block:

repository.json security

```
"security" : {
        "anonymous" : {
            "roles" : ["readonly","readwrite","admin"],
            "useOnFailedLogin" : false
        },
        "providers" : [
            { "classname" : "org.fcrepo.auth.common.ShiroAuthenticationProvider" }
        ]
    },
```

To specify a local repository.json configuration, provide the system property as follows:

```
JAVA_OPTS="... -Dfcrepo.modeshape.configuration=file:/local/repository.json"
```

Configure your web.xml

Configure your **web.xml**. Modify fcrepo-webapp/src/main/webapp/WEB-INF/web.xml by uncommenting the security configuration:

```
<!--Uncomment section below to enable Basic-Authentication-->
<security-constraint>
  <web-resource-collection>
    <web-resource-name>Fedora4</web-resource-name>
    <url-pattern>/*</url-pattern>
    <http-method>DELETE</http-method>
    <http-method>PUT</http-method>
    <http-method>HEAD</http-method>
    <http-method>OPTIONS</http-method>
    <http-method>PATCH</http-method>
    <http-method>GET</http-method>
    <http-method>POST</http-method>
  </web-resource-collection>
  <auth-constraint>
    <role-name>fedoraUser</role-name>
    <role-name>fedoraAdmin</role-name>
  </auth-constraint>
  <user-data-constraint>
    <transport-guarantee>NONE</transport-guarantee>
  </user-data-constraint>
</security-constraint>
<login-config>
  <auth-method>BASIC</auth-method>
  <realm-name>fcrepo</realm-name>
</login-config>
```

The "auth-constraint" element must contain the roles defined as your users (see below for jetty and tomcat).

Configure your web application container

Jetty

- Create your **jetty-users.properties** file. This file contains entries in the format *username: password [, role, ...]*, where
  - *username* is the user's login id (the principal)
  - *password* is the user's password
  - *role* is the servlet role they are assigned upon login; jetty allows you to specify any number of roles (or no role at all).
- Sample **jetty-users.properties** file that contains three users, two of whom are regular users, and the third of whom (fedoraAdmin) is a Fedora superuser:

jetty-users.properties

```
testuser: password1,fedoraUser
adminuser: password2,fedoraUser
fedoraAdmin: secret3,fedoraAdmin
```

- Configure your Jetty login realm.
  - **Standalone**: Modify your **jetty.xml** file to configure the login realm and include the jetty-users.properties file:

jetty.xml login service

```
<Configure class="org.eclipse.jetty.webapp.WebAppContext">

  <!-- Set this to the webapp root of your Fedora 4 repository -->
  <Set name="contextPath">/</Set>
  <!-- Set this to the path of of fcrepo4 WAR file -->
  <Set name="war"><SystemProperty name="jetty.home" default="."/>/webapps/fcrepo4</Set>

  <Get name="securityHandler">
    <Set name="loginService">
      <New class="org.eclipse.jetty.security.HashLoginService">
        <Set name="name">fcrepo4</Set>
        <!-- Set this to the path to your jetty-users.properties file -->
        <Set name="config"><SystemProperty name="jetty.home" default="."/>/path/to/jetty-users.
properties</Set>
      </New>
    </Set>
  </Get>

</Configure>
```

- **Embedded in Maven:** The fcrepo-webapp Maven project includes jetty-maven-plugin. The property *jetty.users.file* sets the location of the **jetty-users.properties** file. Run the fcrepo-webapp server with the following system property:

```
-Djetty.users.file=/path/to/jetty-users.properties
```

- See the Jetty Authentication documentation for more details.

Tomcat

- Create or edit your `$CATALINA_HOME/conf/tomcat-users.xml` file. It has entries of the form

```
<user name="principal" password="password" roles="role1, role2, ..." />
```

where:

- *name* is the user's login id (the principal)
- *password* is the user's password
- *roles* are the servlet roles they are assigned upon login; tomcat allows you to specify any number of roles (or no role at all).

Sample **tomcat-users.xml** file that contains three users, two of whom are regular users, and the third of whom (fedoraAdmin) is a Fedora superuser:

tomcat-users.xml

```
<tomcat-users>
  <role rolename="fedoraUser" />
  <role rolename="fedoraAdmin" />
  <user name="testuser" password="password1" roles="fedoraUser" />
  <user name="adminuser" password="password2" roles="fedoraUser" />
  <user name="fedoraAdmin" password="secret3" roles="fedoraAdmin" />
</tomcat-users>
```

- Configure your Tomcat login realm. Modify your file `$CATALINA_HOME/conf/server.xml` file to configure the login realm with the Fedora webapp context:

server.xml

```
<Context>
  ...
  <Realm className="org.apache.catalina.realm.UserDatabaseRealm" resourceName="UserDatabase" />
  ...
</Context>
```

- See the Tomcat Realms documentation for more details.