Grouper WS REST user configuration

Suggestion for Configuring Grouper WS Rest User

The COmanage Registry Grouper Provisioner provisions groups and membership from Registry to Grouper by invoking Grouper web services (WS) calls, specifically the Grouper REST WS functionality. It does this by authenticating to Grouper WS using basic authentication (a login and password combination). The authenticated user as known by Grouper WS must have the necessary privileges to create folders (stems), groups, and memberships in the stem used for the CO (since provisioner instances are configured per-CO).

There are many different ways one might configure a Grouper WS deployment to support basic authentication for a user with the required privileges. Here we outline an approach often used.

First, we suggest that you proxy the Java servlet container (eg. Tomcat) being used for Grouper WS with Apache HTTP Server (Apache). We recommend this approach because Apache offers so many choices for "basic" authentication that are easy to configure "out of the box". The details of how to proxy the container with Apache is out of scope for this wiki page but it is not hard to find examples (Google for 'apache tomcat ajp example').

With Apache proxying for the container using AJP, one can configure simple basic authentication that uses a login and password. For example your Apache configuration might include

```
<Location /grouper-ws>
  AuthType Basic
  AuthName "Grouper WS"
  AuthUserFile /etc/apache2/passwords
  Require valid-user
</Location>
```

You can then create the password file and set a password for the WS user. For example to create a password for the GrouperSystem user one might do

```
htpasswd -c /etc/apache2/passwords GrouperSystem
```

and then enter the password (twice) when prompted. Of course it is strongly recommended that the Grouper WS only be available by HTTPS so that the password is protected by the TLS secure channel.

An alternative to using a password file is to use a module like mod_authnz_ldap that would test the password against an LDAP directory server instead of a password file.

At this time only authentication methods that use basic authentication are supported by the COmanage Registry Grouper Provisioner. The provisioner cannot, for example, follow redirects or fill out a form or use an X.509 certificate for authentication.