Configuring JavaEE App Client Security

Overview

Application client security starts with specifying the CallbackHandler you want to use in the app client dd (in Geronimo) or in a similar element in the Geronimo deployment plan. In Geronimo, this callback handler is run as soon as the client is activated and before the main class main method is called.

For a CallbackHandler to work, a security realm must be configured. This must be defined on the client. You can configure this in any plugin that will be started before the client application itself (due to being an ancestor of the client application) or in the client plan itself. The security realm configuration is exactly the same on the client and server, using the GenericSecurityRealm GBean.

Logging "in" to OpenEjb.

One common use of application clients is as ejb clients. In this case, you will want to provide who the client is run by to the openejb so that the openejb can apply the authentication rules properly. You do this by using the OpenejbRemoteLoginModule which uses the openejb protocol to log into the server and provide a token used in subsequent calls to the openejb. Note that by default, ejbd communication is unsecure and this token may be eavesdropped and used by others.

Here's a typical configuration for this scenario:

```
    <gbean name="remote-openejb-realm"
        class="org.apache.geronimo.security.realm.GenericSecurityRealm">
        <attribute name="realmName">remote-openejb-realm</attribute>
        <xml-reference name="LoginModuleConfiguration">
            <lc:login-config xmlns:lc="http://geronimo.apache.org/xml/ns/loginconfig-1.2">
                <lc:login-module control-flag="REQUIRED">
                    <lc:login-domain-name>remote-openejb-realm</lc:login-domain-name>
                    <lc:login-module-class>org.apache.geronimo.openejb.OpenejbRemoteLoginModule</lc:login-
module-class>
                    <lc:option name="RemoteSecurityRealm">test-realm</lc:option>
                    <lc:option name="ServerURI">ejbd://localhost:4201</lc:option>
                </lc:login-module>
            </lc:login-config>
        </xml-reference>
        <reference name="ServerInfo">
            <name>ServerInfo</name>
        </reference>
    </gbean>
```

Note that there are two options: the server side security realm name to log into server-side, and the URI for the openejb listener.

By providing an appropriate CallbackHandler and security realm such as this on the client, when the client is started the callback handler will obtain the required user name and password and this login module will log in to Geronimo over the openejb ejbd protocol. The resulting token is stored in the client side Subject for use in subsequent ejb related calls to openejb.