IdPJBossTomcatPrepare

Preparing JBoss for the Shibboleth Identity Provider

Version Requirements/Recommendations

- JBoss AS 5 or greater
- Java 6 or greater

Required Configuration Changes

- Edit your the */login-config.xml/* configuration file and comment out the `<application-policy name = "other">` element. This default policy requires that a user authentication source also report a set of roles for the user. Most deployer's will not do this during the authentication step (though they may later on during the attribute resolution step). Therefore, this policy needs to be removed.
- Limit the allowed size of POST submissions to any HTTP or AJP connectors (including the SOAP connector below) by adding the `maxPostSize` attribute. A size of about 100K (100000) is a reasonable choice.

Supporting SOAP Endpoints

Most new deployments without legacy needs will not need to support back-channel SOAP communication. The most common case requiring this feature is support for legacy Shibboleth SPs using SAML 1.1 that perform attribute queries using SOAP.

If you do need this support, these connections require special security properties which are not appropriate for user-facing/browser use. Therefore an additional endpoint must be configured.

Configure Tomcat

1. Download tomcat6-dta-ssl-1.1.0.jar (asc) in to *server/<serviceProfile>/deploy/jboss-web.sar/*
2. Add the following Connector definition into JBoss Tomcat's *server/<serviceProfile>/deploy/jboss-web.sar//server.xml/* (replacing `IDP_HOME` with your IdP's home directory):

```
<Connector port="8443"
           protocol="org.apache.coyote.http11.Http11Protocol"
           SSLImplementation="edu.internet2.middleware.security.tomcat6.
DelegateToApplicationJSSEImplementation"
           scheme="https"
           maxPostSize="100000"
           SSLEnabled="true"
           clientAuth="want"
           keystoreFile="IDP_HOME/credentials/idp.jks"
           keystorePass="PASSWORD" />
```