Shibboleth Install Checklist

ORIGIN

A. ___Deploy surrounding infrastructure;
   ____attribute source (Campus-based LDAP, Internet2 provided LDAP, JDBC or RDBMS, echo responder provided for testing only)
   ____Mechanism for web-based authentication of users to Apache or Tomcat

B. ___Install various components; (SODG 3.a)
   ____tomcat version _____
   ____mod_jk or mod_jk2
   ____apache version _____

C. Apply for membership in Inqueue; fill out submit the form available here:
   http://inqueue.internet2.edu/join.html

D. ___Install Shibboleth (SODG 3.b)

1. Ensure you have already obtained the proper tarball.

   curl -L -o shibboleth-origin-1.2.tar.gz
   http://wayf.internet2.edu/shibboleth/shibboleth-origin-1.2.tar.gz

   wget http://wayf.internet2.edu/shibboleth/shibboleth-origin-1.2.tar.gz

2. Expand the archive into a shibboleth-origin-1.2/ directory /opt/local recommended).

3. Run the following command to move the Java files into Tomcat's tree:
   $ cp /opt/shibboleth-origin-1.2/dist/shibboleth.war /usr/local/tomcat/webapps/

4. Both Tomcat 4.1.x and 5.x require that several Java jarfiles used by Shibboleth be located in a special "endorsed" folder to override obsolete classes that Sun includes with their JVM. To deal with this problem use the following command, adjusting paths as needed:
   $ cp /opt/shibboleth-origin-1.2/endorsed/*.jar /usr/local/tomcat/common/endorsed
   Other Java servers may have other locations in which to place these files or deal with this problem. Refer to your application server's documentation to find out how to properly endorse classes, if necessary.

5. Restart Tomcat, which will automatically detect that there has been a new .war file added. This file will by default be expanded into /usr/local/tomcat/webapps/shibboleth. After a few minutes, stop Tomcat (when the files in Tomcat's logs directory stop growing).

E. Configure Tomcat

By default, the Coyote/JK2 connector will not permit the REMOTE_USER value set by Apache to pass into Tomcat, and thus into Shibboleth. If user authentication will be handled in this fashion, then the /conf/jk2.properties file must include the following line:

request.tomcatAuthentication=false

F. Configure mod_jk/mod_jk2 into Apache, and map the Shibboleth URL tree into Tomcat

1. Apache must be told to load the JK or JK2 module. This can be done directly in httpd.conf, or in a separate file using the Include command:

For mod_jk (this also maps the */shibboleth* URL tree to the webapp in Tomcat):

```
--------- begin ---------
<IfModule !mod_jk.c>
LoadModule jk_module libexec/mod_jk.so
</IfModule>

JkWorkersFile "/usr/local/tomcat/conf/jk/workers.properties"
JkLogFile "/usr/local/apache/logs/mod_jk.log"
JkLogLevel emerg

JkMount /shibboleth/* ajp13
--------- end ---------
```

For mod_jk2:

```
--------- begin ---------
<IfModule !mod_jk2.c>
LoadModule jk2_module libexec/mod_jk2.so
</IfModule>
--------- end ---------
```

To map the URL tree for mod_jk2, modify the /conf/workers2.properties file in the Apache tree and add these lines. It may also be necessary to modify the references in the file to the socket port and make sure it matches the port set in the Coyote connector.

```
--------- begin ---------
[uri:/shibboleth/*]
group=lb
--------- end ---------
```

G. Configure Apache

1. It is required that the AA be SSL-protected to enable authentication of attribute requests. To do so, add an appropriate location block to httpd.conf:

```
<Location /shibboleth/AA>
SSLVerifyClient optional
SSLOptions +StdEnvVars +ExportCertData
</Location>
```

H. ___Control access to the HS with the web authentication system (SODG 4.c)
___ Local authentication system _____
(e.g., Basic, LDAP, SSO, Kerberos)

This is usually done by inserting a Location Block similar to this one:

```
<Location /shibboleth/HS>
AuthType Basic
AuthName "Internet2 Handle Service"
AuthUserFile /usr/local/apache/conf/user.db
require valid-user
</Location>
```

I. ____Generate keys, obtain a cert from bossie configure the trust information. This process is described in detail in SODG Section 4.b.

1. OpenSSL commands to generate a new keypair and a certificate request are shown here, assuming 2048 bit RSA keys are to be used:

```
$ openssl genrsa -out ssl.key 2048
$ openssl req -new -key ssl.key -out ssl.csr
```

2. Obtain a cert from bossie; (password: 4304538),
https://bossie.doit.wisc.edu:3443/cert/i2server/csr

3. The default configuration file informs Shibboleth to load its key and certificate from flat files. The Key element specifies a key in DER format located at /conf/shib2.key, while the Certificate element specifies the corresponding certificate in PEM format located at /conf/shib2.crt. If any of these values is inconsistent with your deployment, change it accordingly. Note that keys are supported in a variety of formats: DER, PEM, encrypted PEM, PKCS8, and encrypted PKCS8. If a keystore must be used instead, consult SODG Section 5.a for appropriate structure and details on population.

J. Configure origin.xml for membership within InQueue,

1. Follow the config steps described by InQueue
(http://inqueue.internet2.edu/configure.html)

The following steps must be undertaken to configure a standard Shibboleth origin configuration to use InQueue. Some steps may vary or may be completed already depending on how origin.xml has already been modified.

a. ShibbolethOriginConfig must be modified as follows:
* providerId must be populated with a URI that will be assigned by InQueue when you are accepted into the federation.
* defaultRelyingParty should be changed to urn:mace:inqueue.

* Ensure that AAUrl has been changed to reflect the value sent in with the application.

b. Uncomment the InQueue RelyingParty element. If the default providerId as specified in ShibbolethOriginConfig is not the one supplied by InQueue, modify the providerId to match the value assigned by InQueue to this origin.

c. A new KeyStoreResolver or FileResolver element must be added pointing to the private key and certificate for use by this origin. See section 4.b of the origin deploy guide for further information.

d. Uncomment the FederationProvider element for InQueue.

e. Apache/mod_ssl must also be configured to use the appropriate set of trusted roots for the validation of SSL client certificates. For InQueue, this list may be obtained from http://wayf.internet2.edu/InQueue/ca-bundle.crt. This list should then be copied for mod_ssl, which will typically need to be to /conf/ssl.crt/ca-bundle.crt. This list of CA's is not rigorous nor secure and contains CA's which have little or no level of assurance.

2. Other changes to the origin's origin.xml file (decribed in detail in SODG 4.a, steps 1, 2, 3)

____:

3. Although not explicitly necessary, it's highly recommended for initial installation and testing that logging be activated at the DEBUG level by uncommenting the second Logging element and ensuring that the pathnames for TransactionLog and ErrorLog are appropriate. However, in production, this will slow the operation of the origin considerably.

K. Test and validate your new Origin, using the InQueue sample target
https://wayf.internet2.edu/InQueue/sample.jsp

____InQueue test (http://inqueue.internet2.edu/test.html)

L. Configure the new origin to use your attribute repository.
____Point at a (LDAP) directory, configure attribute resolver (SODG 4.a.i)

M. ___Test using sample targets with various access control policies:

____Other tests

1) http://wayf.internet2.edu/InQueue/installfest/employee,jsp

http://wayf.internet2.edu/InQueue/installfest/student,jsp

http://wayf.internet2.edu/InQueue/installfest/member.jsp

These will check for either affiliation or scoped affiliation.

2) http://wayf.internet2.edu/InQueue/installfest/iknowyou.jsp requires an EPPN.

3) http://wayf.internet2.edu/InQueue/installfest/incommon.jsp requires urn:mace:incommon:entitlement:common:1

SODG – Shibboleth Origin Deployment Guide
(http://shibboleth.internet2.edu/guides/deploy-guide-origin1.2.html)