IdP Installation

1. Requirement for Shibboleth IdP (Version 2.4 or later)

Required packages to be installed:

- Apache HTTP Server 2.2 or later, with mod_ssl
- Apache Tomcat 6.0.17 or later (NOT 7.x.x. There are limitations on use of Tomcat 7.)
- Java 6 or later
    - Use Shibboleth IdP 2.4.0 or later in case you use Java 7
    - GNU Java included in CentOS does not seem to be work. Use Oracle Java or OpenJDK instead.

If these softwares are installed with RPM, you can check installed versions with "rpm -qa"

Please check latest information on the site of original Shibboleth:
Installation, Jetty 7, Apache Tomcat, JBoss Tomcat

---

2. Installation of Operating System

2.1. Configuration at OS installation

- Packages required to be installed at OS installation (CentOS 6 assumed):
    - Apache Web Server (httpd)
    - OpenLDAP (openldap-servers, openldap-clients)
    - and others you need.

  Java Development Kit (JDK) and Tomcat will be installed in this document later.
  SELinux is not supported with this document. Please confirm it is disabled with:

  ```
  $ /usr/sbin/getenforce
  Disabled
  ```

- hostname
  Determine a hostname for IdP: idp.example.asia
  Hostname is defined as follows in /etc/sysconfig/network

  ```
  HOSTNAME=idp.example.asia
  ```

2.2. Register to DNS server in your domain

In local testing environment, registering to /etc/hosts may be enough.

2.3. Configuration on time synchronization

Use of NTP is recommended. Configure ntpd to refer nearby NTP servers.

(It may be configured already at installation to refer default NTP servers provided by pool.ntp.org project, though)

Shibboleth IdP and SP must work within 5min difference of clock.

---

3. Installation of jdk6 and tomcat6

WS Participants

You can skip 3.1 through 3.4, and go to 3.5 for the workshop.

We have already installed the following yum packages into WS IdP VM: java-1.6.0-openjdk, tomcat6

3.1. confirm version of tomcat if installed

Uninstall tomcat if version of installed tomcat is tomcat5-5.5.25 or older.

3.2. Installation of jdk 6

If required jdk6 has not been installed yet, download jdk-6u??-linux-x64-rpm.bin from http://java.sun.com/javase/downloads/index.jsp and do as follows:

```
# chmod a+x jdk-6u??-linux-x64-rpm.bin
# ./jdk-6u??-linux-x64-rpm.bin
```

3.3. Installation of tomcat 6

If required tomcat6 has not been installed yet, download apache-tomcat-6.?.??.tar.gz from http://tomcat.apache.org/download-60.cgi in /usr /java, and do as follows:

```
# tar zxv -C /usr/java f apachetomcat-6.?.??.tar.gz
# ln -s /usr/java/apache-tomcat-6.?.?? /usr/java/tomcat
```

In addition, it is useful to use automatic start-up script. If it is not enclosed in the package, you can get from here

```
# unzip tomcat6.zip
# chmod a+x tomcat6
# cp tomcat6 /etc/rc.d/init.d/
```

Configure as follows to enable start-up script:

```
# chkconfig --add tomcat6
# chkconfig --level 345 tomcat6 on
# service tomcat6 start
```

3.4. Configure system wide environment

If you have newly installed tomcat and jdk, you may required to add following descriptions for environment variables in /etc/profile or create a file with suffix .sh in /etc/profile.d/:

```
# /etc/profile
JAVA_HOME=/usr/java/default
MANPATH=$MANPATH:$JAVA_HOME/man
CATALINA_HOME=/usr/java/tomcat
TOMCAT_HOME=$CATALINA_HOME
PATH=$JAVA_HOME/bin:$CATALINA_HOME/bin:$PATH
export PATH JAVA_HOME CATALINA_HOME

# System wide environment and startup programs, for login setup
```

Apply the configured environment variables for current shell after modifying /etc/profile or some files in /etc/profile.d/

```
source /etc/profile
```

Finally, heck whether tomcat is working properly by accessing URL: http://idp.example.asia:8080 (change hostname as you building)

It works if you see default screen of tomcat.

3.5. Configuration of httpd

Modify /etc/httpd/conf/httpd.conf on hostname

```
(omitted)

ServerName idp.example.asia:80 (your hostname)

(omitted)
```

Modify /etc/httpd/conf.d/ssl.conf

```
(omitted)

<VirtualHost _default_:443>

(omitted)

ServerName idp.example.asia:443 (your hostname)
ProxyPass /idp/ ajp://localhost:8009/idp/ (new)

(omitted)
```

3.6. Modification of tomcat configuration

Edit /usr/share/tomcat6/conf/server.xml as follows:

a. Comment out the following block if you do not have any plan to use the server other than IdP

```
<!--
    <Connector port="8080" protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="8443" />
-->
```

b. Add the following description:

```
<Connector port="8009"
    protocol="AJP/1.3"  redirectPort="8443"  enableLookups="false"
 tomcatAuthentication="false" address="127.0.0.1" />
```

---

4. Installation of Shibboleth IdP

File names and locations in the following description is based on IdP Version 2.3.6.

4.1. Download of Shibboleth IdP

> WS Participants
>
> The following instruction requires the Internet connection. If you don't have the Internet connection, all required files are stored under /root/source directory.

Download latest IdP shibboleth-identityprovider-2.?.?-bin.tar.gz from http://www.shibboleth.net/downloads/identity-provider/latest/

4.2. Installation

Do as follows:

```
# tar zxvf shibboleth-identityprovider-2.?.?-bin.tar.gz
# cd shibboleth-identityprovider-2.?.?
# ./install.sh
```

Supply parameters during execution of the install.sh as follows:

```
Buildfile: src/installer/resources/build.xml

install:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Be sure you have read the installation/upgrade instructions on the Shibboleth website before proceeding.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Where should the Shibboleth Identity Provider software be installed? [/opt/shibboleth-idp]
[Enter]    (just an enter)
What is the fully qualified hostname of the Shibboleth Identity Provider server? [idp.example.org]
idp.example.asia[Enter] (hostname of your IdP)
A keystore is about to be generated for you. Please enter a password that will be used to protect it.
keystore[Enter] (any password which will be used later)
Updating property file: /root/PKG/shibboleth-identityprovider-2.3.6/src/installer/resources/install.properties

(omitted)

BUILD SUCCESSFUL
Total time: 54 seconds
```

4.3. Configuration of Java for Back-channel request support

> WS Participants
>
> The following instruction requires the Internet connection. If you don't have the Internet connection, all required files are stored under /root/source directory.

Download tomcat6-dta-ssl-1.0.0.jar from https://build.shibboleth.net/nexus/content/repositories/releases/edu/internet2/middleware/security/tomcat6/tomcat6-dta-ssl/1.0.0/tomcat6-dta-ssl-1.0.0.jar and copy it into /usr/share/tomcat6/lib ($CATALINA_HOME is assumed to be /usr/share/tomcat6 here).

```
# cp tomcat6-dta-ssl-1.0.0.jar /usr/share/tomcat6/lib
```

After copying, edit /usr/share/tomcat6/conf/server.xml to add the following description:

```
<Connector port="8443"
   protocol="org.apache.coyote.http11.Http11Protocol"
   SSLImplementation="edu.internet2.middleware.security.tomcat6.DelegateToApplicationJSSEImplementation"
   scheme="https"
   SSLEnabled="true"
   clientAuth="want"
   keystoreFile="/opt/shibboleth-idp/credentials/idp.jks"
   keystorePass="keystore" /> (password)

                    ↑ change it with your keystore password
```

4.4. Configuration of Tomcat

Create /usr/share/tomcat6/endorsed and copy all (five) jar files in /opt/shibboleth-idp/lib/endorsed/ into it.

```
# mkdir /usr/share/tomcat6/endorsed
# cp /opt/shibboleth-idp/lib/endorsed/*.jar /usr/share/tomcat6/endorsed
```

Following files are included in IdP 2.4.0

- serializer-2.10.0.jar
- xalan-2.7.1.jar
- xercesImpl-2.10.0.jar
- xml-apis-2.10.0.jar
- xml-resolver-1.2.jar

To enable these jar files in start-up script of tomcat, add following line in /etc/tomcat6/tomcat6.conf:

```
JAVA_ENDORSED_DIRS="${CATALINA_HOME}/endorsed"
```

If you run tomcat with an user "tomcat", change ownership of directories as follows:

```
# chown -R tomcat: /opt/shibboleth-idp/logs
# chown -R tomcat: /opt/shibboleth-idp/metadata
```

4.5. Deployment of idp.war

Copy /opt/shibboleth-idp/war/idp.war into ${CATALINA_HOME}/webapps

```
# cp /opt/shibboleth-idp/war/idp.war /usr/share/tomcat6/webapps/
```

Restart httpd and tomcat.

```
# service tomcat6 stop
# service httpd restart
# service tomcat6 start
```

Be sure that any error messages are logged in /usr/share/tomcat6/logs/catalina.out after restarting tomcat.

Ignore messages as follows logged at restarting (terminating) tomcat:

```
SEVERE: A web application appears to have started a TimerThread named [Timer-0] via the java.util.Timer API but has failed to stop it. To prevent a memory leak, the timer (and hence the associated thread) has been forcibly cancelled.
```

```
SEVERE: A web application created a ThreadLocal with key of type [null] (value [ch.qos.logback.core.
UnsynchronizedAppenderBase$1@XXXXXXXX]) and a value of type [java.lang.Boolean] (value [false]) but failed to remove it when the web application was stopped. To prevent a memory leak, the ThreadLocal has been forcibly removed.
```

(other related bug reports)

---

5. Basic operation of IdP

5.1. Start up

httpd:

```
service httpd start
```

tomcat:

```
service tomcat6 start

 or

sh /usr/java/tomcat/bin/startup.sh (in case start-up script is unavailable)
```

5.2. Termination

httpd:

```
service httpd stop
```

tomcat:

```
service tomcat6 stop

 or

sh /usr/java/tomcat/bin/shutdown.sh (in case start-up script is unavailable)
```

Proceed to next step for configuration of IdP