Upgrading a Shibboleth 2.x IdP

Shibboleth IdP 2.x is becoming End-Of-Life on July 31st, 2016. This page now exists only as a historical archive.

Please see the instructions on Upgrading a 2.x IdP to 3.x.

Overview and Plan

This guide for upgrading a Shibboleth IdP is based on the assumption the IdP has been built according to the Tuakiri Installing a Shibboleth 2.x IdP manual.

This guide covers updating to the current release in the 2.4.x branch and versions 2.3.x and 2.4.x are considered for the base install. Adjust accordingly for other version combinations.

Overall, this plan assumes to carry over modifications done to the old installation tree (unpacked zip binary) to the new one, rebuilding the war file and reusing the configuration files.

Upgrade plan:

- Compare existing Shibboleth installation directory (old version) with a vanilla copy of the same version, identify local modifications, which would likely include:
  - Login page
  - uApprove jars
  - Shared token jar
  - web.xml modifications
- Download and extract the new version
  - Update the current environment variables to point to the new version
- Install local modifications into the new version
- Backup /opt/shibboleth-idp
- Run the installer from the new version, answering NO to overwriting files.
  - Update the default environment to point to the new version
  - Restart Tomcat

In a nutshell, this plan assumes the configuration files in `/opt/shibboleth-idp/conf` will be left untouched and only the web application `/opt/shibboleth-idp/war/idp.war` (and files in `/opt/shibboleth-idp/lib/`) will get updated. Among the 2.2.x, 2.3.x, and 2.4.x branches, the configuration files are compatible with new releases without modification.

Upgrade Walkthrough

Examine local modifications

- Create a vanilla copy of the old installation directory

```
cd /root/inst
unzip -d /tmp shibboleth-identityprovider-${IDP_VERSION}-bin.zip
mv /tmp/shibboleth-identityprovider-${IDP_VERSION} shibboleth-identityprovider-${IDP_VERSION}-orig
```

- Run a diff between the vanilla version and the current installation directory, examine the output:

```
diff -r shibboleth-identityprovider-${IDP_VERSION}-orig shibboleth-identityprovider-${IDP_VERSION} | less
```

- Expect to find:
  - Shared token library missing:

```
Only in shibboleth-identityprovider-2.4.0/lib: arcs-shibext-1.5.4.jar
```

  - uApprove IdP plugin libraries missing:

```
Only in shibboleth-identityprovider-2.4.0/lib: jstl-1.2.jar
Only in shibboleth-identityprovider-2.4.0/lib: uApprove-2.5.0.jar
Only in shibboleth-identityprovider-2.4.0/lib: spring-jdbc-2.5.6.SEC03.jar
Only in shibboleth-identityprovider-2.4.0/lib: spring-tx-2.5.6.SEC03.jar
Only in shibboleth-identityprovider-2.4.0/lib: mysql-connector-java-5.1.25.jar
```

- Differences in `src/installer/resources/install.properties` (IGNORE)
- Local branding modifications in `src/main/webapp` (`login.jsp`, the `images` directory, stylesheets, the `uApprove` directory...) - these will need to be backported
- Differences in `src/main/webapp/WEB-INF/web.xml` (uApprove hooks) - these will have to be re-applied to web.xml coming with the new version.

Preparing new version

Set the current environment to point to the new version:

```
IDP_VERSION="2.4.2"
SHIB_INST_HOME=/root/inst/shibboleth-identityprovider-$IDP_VERSION
export IDP_VERSION SHIB_INST_HOME
```

Download and extract the new version

```
wget http://www.shibboleth.net/downloads/identity-provider/latest/shibboleth-identityprovider-${IDP_VERSION}-bin.zip
unzip shibboleth-identityprovider-${IDP_VERSION}-bin.zip
```

Installing local modifications into the new version

- Re-install shared token library:

  ```
  cp arcs-shibext-*.jar $SHIB_INST_HOME/lib
  ```

- Re-install uApprove IdP plugin libraries:

  ```
  cp $UAPPROVE_INST_HOME/lib/*.jar $SHIB_INST_HOME/lib
  cp $UAPPROVE_INST_HOME/lib/jdbc/*.jar $SHIB_INST_HOME/lib
  ```

- Re-apply `web.xml` modifications for uApprove: edit the IdP web application descriptor file `$SHIB_INST_HOME/src/main/webapp/WEB-INF/web.xml` and add the `filter` and `filter-mapping` elements just before the closing tag of the top-level `web-app` element (and also apply any other changes done to the web.xml file in your customizations):

  ```
  <web-app>
    ...

    <filter>
      <filter-name>uApprove IdP plugin</filter-name>
      <filter-class>ch.SWITCH.aai.uApprove.idpplugin.Plugin</filter-class>
      <init-param>
        <param-name>Config</param-name>
        <param-value>
          /opt/uApprove/conf/idp-plugin.properties;
          /opt/uApprove/conf/common.properties;
        </param-value>
      </init-param>
    </filter>

    <filter-mapping>
      <filter-name>uApprove IdP plugin</filter-name>
      <url-pattern>/*</url-pattern>
    </filter-mapping>

  </web-app>
  ```

Check and backport login page branding.

- Examine changes made to the login page between the versions: run

```
diff -rwu shibboleth-identityprovider-2.4.0-orig/src/main/webapp/ shibboleth-identityprovider-2.4.2/src
/main/webapp/ | less
```

- In the 2.4.x branch, the login.jsp template has not changed in between versions.
- The 2.4.x branch however introduced a completely new layout over what the 2.3.x branch was using. You may choose to either copy over your existing login page (the branches are API compatible), or you may want to apply your branding to the 2.4.x version as per the IdP Install Manual (Customizing and branding IdP login screen section).
- In the 2.3.x branch, these are just cosmetic (moving the stylesheet link into the HTML `<head>` element) - but reapply them to your login page.

- When upgrading from a 2.2.x version:
  - There have been minor changes to the error-404.jsp and error.jsp pages (back-port these if you have been customizing these pages, otherwise just use the new versions):
    - Adding the `idpui` taglib (in error-404.jsp only)
    - Switching from `error.getMessage()` to `esapiEncoder.encodeForHTML(error.getMessage())`
  - The has been a major overhaul of `login.jsp`, including a switch from direct API to the `idpui` taglib. However, a login page designed for a 2.2.x IdP will work with a 2.3.x IdP. You may either copy the login.jsp over, or you may re-apply the branding steps to the new IdP 2.3.x `login.jsp` file.

- Make a backup copy of any files you'd be modifying (at least login.jsp):

```
cp $SHIB_INST_HOME/src/main/webapp/login.jsp $SHIB_INST_HOME/src/main/webapp/login.jsp.dist
```

- Copy all of the branding files identified earlier from the new version to the new version.
  - This would typically be `src/main/webapp/login.jsp` and any stylesheet and image files

Update configuration files

Shibboleth IdP is designed to run newer versions with configuration files from an older version - so you can keep your existing configuration files as they are and all already existing features should still work.

However, to benefit from the features added in newer releases, it may be worth adding the relevant sections from the configuration templates (in `$SHIB_INST_HOME/src/installer/resources/conf-tmpl`) into your configuration files in `/opt/shibboleth-idp/conf` and the IdP metadata in `/opt/shibboleth-idp/metadata/idp-metadata.xml`.

Notably:

- Shibboleth IdP 2.4.0 introduced the Logout handler (in `conf/handler.xml` and `metadata/idp-metadata.xml`)
- Shibboleth IdP 2.3.0 introduced ECP and UnsolicitedSSO (bth in `conf/handler.xml` and `conf/relying-party.xml`)

You can examine the difference by comparing `src/installer/resources/conf-tmpl` and `src/installer/resources/metadata-tmpl` in the old and new installation tree - e.g.:

```
diff -rwu shibboleth-identityprovider-2.3.8-orig/src/installer/resources shibboleth-identityprovider-2.4.2/src
/installer/resources | less
```

and applying the differences (adding new snippets for the new features like ECP or SLO) to your existing configuration files (and IdP metadata) in `/opt/shibboleth-idp/conf` and `/opt/shibboleth-idp/metadata/idp-metadata.xml`.

Deploy the new version

Important

Backup the `/opt/shibboleth-idp` directory before deploying the upgrade

- Backup the `/opt/shibboleth-idp`directory with:

```
tar czf /root/backup-shibboleth-idp-`date +'%F-%T'`.tar.gz /opt/shibboleth-idp/
```

- Run the installer from the new version, answering NO to overwriting files.

```
cd $SHIB_INST_HOME
sh ./install.sh
```

- Update the default environment to point to the new version: edit `/etc/profile.d/shib.sh` and update the IdP version (**`IDP_VERSION="2.3.3"`**)
    - Reload the environment with:

```
. /etc/profile.d/shib.sh
```

- Restart Tomcat

```
service tomcat6 restart
```