ShibAuth Plugin
Installation Guide

A Shibboleth 2 Service Provider Plugin for Vitro developed by CTRIP at the University of Florida.

CTRIP

UF Clinical & Translational Research Informatics Program

Table of Contents

1 Introduction

The Shibboleth System is a standard based, open source software package for web single sign-on across or within organizational boundaries. It allows sites to make informed authorization decisions for individual access of protected online resources in a privacy-preserving manner. The following is the procedure that was used to install a Shibboleth Service Provider within the University of Florida environment. UF is a Shibboleth Identity Provider (IDP). In this example, we use our IDP to authenticate users accessing Vitro.

2 Intended Audience

This document is intended for the system administrator that will be installing and maintaining a Shibboleth 2 Service Provider. The following basic skills are expected of the reader, and are beyond the scope of what this document attempts to cover:

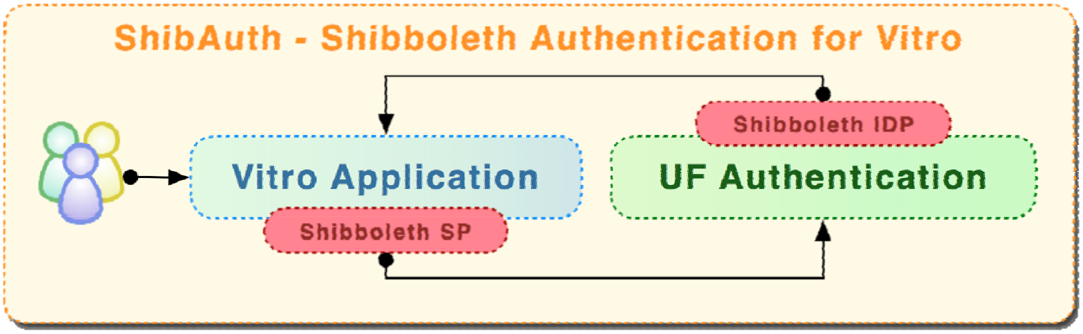
- Familiarity with the local operating system, including how to install software (On some UNIX systems, this may mean compiling packages from source code or using the ITS-provided package)
- Configuring the local web server (Apache, IIS, etc.)
- Basic understanding of SSL, including how to generate a key and CSR
- Basic understanding of XML documents

3 System/Plugin Overview

This procedure is an example installation of a Shibboleth 2 Service Provider on a Linux (Debian Lenny) system. All commands were executed as the root user. In this example, the following applications have already been installed and configured:

- OpenSSL
- Apache 2
- Tomcat 6
- Vitro

The ShibAuth plugin allows a Vitro system administrator to authenticate using the Shibboleth Service Provider. It is assumed that the user already has an account in the "Users" table of the database where the username matches the username provided by the IDP.



4 Installation Procedure

4.1 Install Shibboleth 2 Service Provider

Install Shibboleth Packages

```
apt-get update
apt-get install shibboleth-sp2-schemas libshibsp-dev
apt-get install libshibsp-doc libapache2-mod-shib2 opensam12-tools
```

Enter the sbin directory

```
cd /usr/sbin/
```

Generate a key/certificate for Shibboleth

```
./shib-keygen –h shib.your.domain.edu
```

Make an SSL directory to store the certificates

```
mkdir /etc/shibboleth/ssl
```

Copy certificates and rename with your hostname

```
cp -rp /etc/shibboleth/sp-cert.pem /etc.shibboleth/ssl/YOUR.DOMAIN.EDU.cert
cp -rp /etc/shibboleth.sp-key.pem /etc/shibboleth/ssl.YOUR.DOMAIN.EDU.pem
```

Rename the default XML file to store as a backup

```
cd /etc/shibboleth
mv shibboleth2.xml shibboleth2.xml.bak
```

Download the Linux XML config file from the Identity Provider (IDP) or modify per your IDP’s recommendations.

```
wget http://YOUR.IDENTITYPROVIDER.EDU/linux.shibboleth2.xml
```

Rename the XML config file

```
mv linux.shibboleth2.xml. shibboleth2.xml
```

Configure your XML file per your organizations Identity Provider recommendations. You will need to obtain a URN from your IDP.

Restart the Shibboleth Process

```
/etc/init.d/shibd restart
```

4.2 Enable Shibboleth Authentication In Apache 2

Add a line to your Apache configuration on the proper virtual host, such as in httpd.conf, to trigger Shibboleth session initiation and authentication for your application. The use of ShibUseHeaders On is important.

Edit your virtual host

```
nano /etc/apache2/sites-available/default-ssl
```

Add the following to your virtual host. You can enter anything to replace "shibauth". For example, you could use "/secure" or just "/" to secure the entire virtual host.

```
# Path to invoke authentication
<Location /shibauth>
AuthType shibboleth
ShibRequireSession On
ShibUseHeaders On
require valid-user
</Location>


# Make Shibboleth variables available to entire webapp
<Location />
AuthType shibboleth
ShibRequireSession Off
require valid-user
ShibUseHeaders On
require shibboleth
</Location>
```

Restart Apache 2

```
/etc/init.d/apache2 restart
```

Test for Metadata File

https://your.domain.edu/Shibboleth.sso/Metadata

If your Metadata file is accessible, you can then contact your IDP and ask them to fetch your metadata file. Once this has occurred, a trust is established between the IDP and the SP.

Test by accessing the authentication path in your browser

https://your.domain.edu/Shibboleth.sso/Metadata

4.3 University of Florida ShibAuth Plugin Example

The following files contain UF-Specific source code. For your implementation, you will need to change data in the following files:

- shibauth_admin_login.jsp
- shibauth_admin_login_process.jsp
- loginForm.jsp

Add a ShibAuth class (single command)

```
mv ShibauthAdminAuthenticate.class /usr/local/tomcat/webapps/vitro/WEB-INF/classes/edu/cornell/mannlib/vitro/webapp/controller/edit/
```

Add ShibAuth files

```
mv shibauth_admin_login.jsp /usr/local/tomcat/webapps/vitro/
mv shibauth_admin_login_process.jsp /usr/local/tomcat/webapps/vitro/
```

Backup existing login form (single command)

```
mv /usr/local/tomcat/webapps/vitro/siteAdmin/loginForm.jsp /usr/local/tomcat/webapps/vitro/siteAdmin/loginForm.jsp.BAK
```

Replace the login form with our new page, which has a link sending the user to the IDP authentication page.

```
mv loginForm.jsp /usr/local/tomcat/webapps/vitro/siteAdmin/
```

Backup existing web.xml

```
mv /usr/local/tomcat/webapps/vitro/WEB-INF/web.xml /usr/local/tomcat/webapps/vitro/WEB-INF/web.xml.BAK
```

Replace the web.xml with our new file.

```
mv web.xml /usr/local/tomcat/webapps/vitro/WEB-INF/
```

Add image files

```
mv ajax-loader.gif  /usr/local/tomcat/webapps/vitro/images/
mv transbg50.png  /usr/local/tomcat/webapps/vitro/images/
```

Restart Apache/Tomcat

```
/etc/init.d/apache2 stop
/etc/init.d/tomcat stop
/etc/init.d/tomcat start
/etc/init.d/apache2 start
```

Test Shibboleth Login

https://your.domain.edu/vitro/siteAdmin?home=1&login=block