Service Provider Installation (Red Hat, Fedora, CentOS, Ubuntu)

The information provided here is primarily for Red Hat Linux as it is the most common Linux distro on UBC campus and also one of the Virtual Server operating systems offered by UBC-IT.

If you use a different linux distro, you can still use the information provided here, and make the modifications as necessary based on requirements of your operating systems.

Installation Steps

Assumptions: You have a Red Hat linux server available and have system administrator access. You understand the firewall rules for the server. The skill sets required for installation and management of the Service Provider are listed by Internet2. This tutorial assumes that the installer has the skill-sets outlined by Internet2.

1. OpenSSL (required for SSL transactions)

- Download OpenSSL
- Unpack the downloaded OpenSSL tar file (i.e. 'gunzip' and 'tar -xvf')
- Change directory to the OpenSSL folder and enter following command:
    - ./config --prefix=/usr/openssl
    - make
    - sudo make install

2. Apache Web Server

- Download Apache web server
- Unpack the downloaded Apache file
- Change directory to the Apache folder and enter the following command (installs in '/opt' folder; change accordingly if you would like different installation destination):
    - ./configure --prefix=/opt/apache --enable-proxy --enable-proxy-ajp --enable-rewrite --enable-ssl --with-ssl=/usr/openssl/ssl --enable-so
    - make
    - sudo make install
- Configure your Apache web server to listen for a virtual host (usual Apache configuration)
- Connect the Apache server to the Shibboleth Service Provider installed in Step 3 below.

3. Shibboleth Service Provider

- Red Hat 5: Download the yum configuration file 'shib.repo', and place it in '/etc/yum.repos.d'
- Red Hat 6: Download the yum configuration file 'shib-6.repo', and place it in '/etc/yum.repos.d'
- If 32-bit OS enter 'sudo yum install shibboleth'
- If (64-bit OS) enter 'sudo yum install shibboleth.x86_64'
- Create directory: 'mkdir /opt/shibboleth-sp' (to facilitate management of the Service Provider, the relevants components will be placed here via symbolic links)
- Create symbolic link to Shibboleth configuration files:'ln -s /etc/shibboleth /opt/shibboleth-sp/etc'
- Create symbolic link to the Shibboleth log files: 'ln -s /var/log/shibboleth/ /opt/shibboleth-sp/log'
- Create directory for the Shibboleth Start and Stop scripts: 'mkdir /opt/shibboleth-sp/bin'
- Download the Shibboleth Service Provider start-up and shut-down scripts and place it in '/opt/shibboleth-sp/bin'
- Enable execution on the above scripts:
    - chmod uog+x start-shib.sh
    - chmod uog+x stop-shib.sh

4. iptables (Linux's kernel firewall)

- Enable port 443 on iptables (example below allows access from anywhere – restrict as per your requirements):
    - sudo /sbin/iptables -I INPUT -p tcp -m tcp --dport 443 -j ACCEPT

- Save iptables update (otherwise the rule will be lost when your server next reboots):
    - sudo /etc/init.d/iptables save

5. If your server is behind an external firewall, ensure appropriate access have been given by the firewall administrator

6. Create SSL certificated for the Apache web server

- Steps outlined below are for <u>self-signed certificate</u>, for production service, a certificate from a recognized Certificate Authority may be required.
    - openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout www.mysitename.key -out www.mysitename.crt
    - Fill out details as requested and place the 'key' and 'crt' files in /opt/apche/conf/ssl'
- If applying for <u>certificate from a Certificate Authority (CA)</u>, you will be required to send a 'csr' file to the CA to purchase the certificate (follow the CA's installation instructions upon receipt of the certificate)
    - openssl genrsa -out www.mysitename.key 2048
    - openssl req -new -key www.mysitename.key -out www.mysitename.csr (send the 'csr' file generated to a recognized CA; e.g. Thawte)

7. Install or Write a HTTP Header (optional)

   Attributes, forwarded by the Shibboleth Identity Provider, are sent via HTTP headers to the Shibboleth Service Provider; this is an optional step if you would like to view the headers via a browser with a HTTP reader. You can choose to write your own HTTP reader or download the one written by Internet2 (modified by UBC-IT to reflect UBC requirements).

- Get the latest stable PHP tar ball from www.php.net
- ./configure --prefix=/opt/apache --with-apxs2=/opt/apache/bin/apxs (change relative paths as necessary)
- 'make' & 'make install' as per usual Linux installation process
- Place the HTTP reader's PHP file you downloaded to the Apache document folder (if you are using this tutorial's path name convention, place file in 'opt/apache/htdocs/secure'; create the folder 'secure' if it does not already exist)
- Or if you are configuring a Java application server, download the shibboleth.jsp file and place it in the root of your webapp.

8. You are now ready to configure your Shibboleth Service Provider.