Shibboleth SP V3 install

16.02.25

Pegasi Knowledge
https://ghost.pegasi.fi/wiki/

Table of Contents

Shibboleth SP V3 install

A simple guide on how to set up federated / single Shibboleth service provider version 3 to Linux. Based on Sami's excellent instructions published in HAKA pages.

Download packages

Go to Shibboleth SP download page, select platform and click Generate. This will create a text that is ready to be copy-pasted as repository for your package management software.

So now paste the output from your browser as your shibboleth repository data. With CentOS 7 do a yum repository /etc/yum.repos.d/shibboleth.repo and the contents should be something like this :

```
[security_shibboleth]
# If the mirrors stop working, change download to downloadcontent...
name=Shibboleth (CentOS_7)
type=rpm-md
baseurl=http://download.opensuse.org/repositories/security:/shibboleth/CentOS_7/
gpgcheck=1
gpgkey=http://download.opensuse.org/repositories/security:/shibboleth/CentOS_7/repodata/repomd.xml.key
enabled=1
```

After that install shibboleth, with yum compatible systems do :

```
yum install shibboleth
```

And deb compatible systems something like :

```
apt-get install shibboleth
```

Set shibd to start on boot :

```
systemctl enable shibd
```

Configure basics

Open file /etc/shibboleth/shibboleth2.xml .

Configure entity id and signing :

```
<ApplicationDefaults entityID="https://myserver.domain.com/testsp"
       REMOTE_USER="eppn persistent-id targeted-id"
       signing="front">
```

Configure a single IDP or (HAKA) federation :

```
<!--
<SSO discoveryProtocol="SAMLDS"
discoveryURL="https://testsp.funet.fi/shibboleth/WAYF"> SAML2 </SSO>
<SSO discoveryProtocol="SAMLDS"
discoveryURL="https://haka.funet.fi/shibboleth/WAYF"> SAML2 </SSO>
-->
<SSO entityID="https://idp.domain.com/shibboleth"> SAML2 </SSO>
```

Configure contact data to error messages :

```
<Errors supportContact="helpdesk@domain.com"
       helpLocation="/about.html"
       styleSheet="/shibboleth-sp/main.css"/>
```

Configure metadata

Open file /etc/shibboleth/shibboleth2.xml .

If using single IDP (test SP in same server with IDP) :

```
<MetadataProvider type="XML" validate="true" file="/opt/shibboleth-
idp/metadata/idp-metadata.xml"/>
```

If using test federation :

```
<MetadataProvider type="XML"
uri="https://haka.funet.fi/metadata/haka_test_metadata_signed.xml"
backingFilePath="haka_test_metadata_signed.xml" reloadInterval="3600">
        <SignatureMetadataFilter certificate="/opt/shibboleth-
idp/credentials/haka_testi_2015_sha2.crt"/>
        <MetadataFilter type="Whitelist">
        </MetadataFilter>
        <MetadataFilter type="RequireValidUntil"
maxValidityInterval="2592000"/>
</MetadataProvider>
```

If using production federation :

```
<MetadataProvider type="XML"
uri="https://haka.funet.fi/metadata/haka-metadata.xml"
backingFilePath="haka-metadata.xml" reloadInterval="3600">
        <SignatureMetadataFilter certificate="/opt/shibboleth-
idp/credentials/haka-sign-v3.pem"/>
        <MetadataFilter type="Whitelist">
        </MetadataFilter>
        <MetadataFilter type="RequireValidUntil"
maxValidityInterval="2592000"/>
</MetadataProvider>
```

Set up Apache SP

As en easy example try SP with Apache. With rpm installation you get a working example in /etc/httpd/conf.d/shib.conf but in case it is missing here are the contents of the file :

```
LoadModule mod_shib /usr/lib64/shibboleth/mod_shib_24.so
ShibCompatValidUser Off
<Location /Shibboleth.sso>
  AuthType None
  Require all granted
</Location>
<IfModule mod_alias.c>
  <Location /shibboleth-sp>
    AuthType None
    Require all granted
  </Location>
  Alias /shibboleth-sp/main.css /usr/share/shibboleth/main.css
</IfModule>
<Location /testlocation>
  AuthType shibboleth
  ShibRequestSetting requireSession 1
  require shib-session
</Location>
```

To prevent errors after successful authentication you need to create HTML content in file /var/www/html/secure/index.html , such as :

```
<html>
Hello world!
</html>
```

Finally restart shibd and Apache.

```
systemctl restart shibd
```

```
systemctl restart httpd
```

Deliver metadata to IDP

Log in to IDP and download metadata with :

```
wget https://idp.domain.com/Shibboleth.sso/Metadata
```

And append to file/opt/shibboleth-idp/metadata/local-metadata.xml . Restart IDP or let metadata refresh.

Test Apache SP

Surf to https://your-sp/secure and observe.

Comments and suggestions

If you find bugs above please comment below. Also feel free to rate.