Change of Shibboleth SP Configuration from v2 to v3

Martin Haase, DAASI International SSO team, 2021-04-28
Reference: https://wiki.shibboleth.net/confluence/display/SP3/UpgradingFromV2

Why

Shibboleth Service Provider (SP) version 3 is compatible with configuration files from a version 2 installation. However, some features are not available if a v3 SP runs from a v2 configuration file. For example, the April 2021 SP security advisory[1] has a workaround for Ubuntu/Debian SPs which only works if a v3 configuration format is in effect.

Affected Installations

SP v3 installations which were not newly installed but were updated from v2 are affected. One can tell from the XML header of the main configuration file `/etc/shibboleth/shibboleth2.xml`.

If this file contains mentions of `"urn:mace:shibboleth:1.0:native:sp:config"` or `"urn:mace:shibboleth:2.0:native:sp:config"`, DAASI recommends to update the file, following the steps below.

Backup

```
cp -a /etc/shibboleth/shibboleth2.xml /etc/shibboleth/shibboleth2.xml.BAK
```

Now edit shibboleth2.xml.

XML Header

Old XML header:

```
<SPConfig xmlns="urn:mace:shibboleth:1.0or2.0:native:sp:config"
   xmlns:conf="urn:mace:shibboleth:2.0:native:sp:config"
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
   xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
   clockSkew="180">
```

Replace in full with the new XML header:

```
<SPConfig xmlns="urn:mace:shibboleth:3.0:native:sp:config"
   xmlns:conf="urn:mace:shibboleth:3.0:native:sp:config"
   clockSkew="180">
```

1 https://shibboleth.net/community/advisories/secadv_20210426.txt

Keep the clockSkew value from the old configuration.

Metadata Providers

In all <MetadataProvider> elements, replace the following XML attributes

- uri becomes url
- reloadInterval becomes maxRefreshDelay
- file becomes path

For example:

Old:

```
<MetadataProvider type="XML" file="partner-metadata.xml"/>
<MetadataProvider type="XML" validate="true"
     uri="http://example.org/federation-metadata.xml"
     backingFilePath="federation-metadata.xml"
     reloadInterval="7200">
```

New:

```
<MetadataProvider type="XML" path="partner-metadata.xml"/>
<MetadataProvider type="XML" validate="true"
     url="http://federation.org/federation-metadata.xml"
     backingFilePath="federation-metadata.xml"
     maxRefreshDelay="7200">
```

Recommendations

In order to mitigate some open redirect attacks, set redirectLimit="host" in the <Sessions> element (recommendation by SWITCH[2]):

```
<Sessions lifetime="..." ... redirectLimit="host">
```

This step should be repeated for all `<Session>` elements in the file.

SP on Windows

Please refer to https://wiki.shibboleth.net/confluence/display/SP3/Upgrading+Older+ISAPI+Configuration.

2 https://www.switch.ch/aai/guides/sp/migration/#8

Testing the Configuration

Linux

```
sudo shibd -t
```

Windows

```
C:\opt\shibboleth-sp\sbin\shibd.exe -check
```

The last line should output:

```
overall configuration is loadable, check console for non-fatal
problems
```