SHRINE 4.0.0 Appendix A.3 - More Details : Shibboleth Configuration

Shibboleth consists of a daemon plus an Apache module. These must be configured for Shibboleth to intercept certain requests (see Apache Configuration in SHRINE 4.0.0 Appendix A.4 - More Details: Apache Configuration). When a request is intercepted, Shibboleth will decide whether the user (1) needs to login at the configured IdP (which will present a login form to the user), or (2) is already logged in (and Shibboleth will let the request be served as if it wasn't there to intercept it).

While the user is logged in, upon each HTTP request, Shibboleth will provide to the Apache and Tomcat servers information about the user from the idP, such as the username with which the user logged in at the idP.

Shibboleth Configuration is documented in full at https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2063695920/Configuration

`/etc/shibboleth/shibboleth2.xml`

`<ApplicationDefaults> element:`

> **`entityID`**: the ID of our Service Provider (SP)
>
> **`attributePrefix`** must be set to "`AJP_`" so that the attributes from the "**`attribute-map.xml`**" file (see below) are passed to Tomcat as request attributes (as opposed to request headers). See also SHRINE 4.0.0 Appendix A.5 - More Details: Tomcat Configuration on the same topic.
>
> The **`REMOTE_USER`** xml attribute of **`<ApplicationDefaults>`** should be populated, in the form of a list of at least one attribute name; the first of which should normally be "**`userId`**", which is defined in `attribute-map.xml`.
>
> See: https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2067400159/JavaHowTo
>
> See: https://stackoverflow.com/questions/63505670/apache-cant-connect-to-new-tomcat-9-ajp

```
<ApplicationDefaults
  entityID="https://[your hostname]" <!-- should match the entityID in sp-metadata.xml -->
  signing="true"
  REMOTE_USER="userId"
  attributePrefix="AJP_"
>
```

`<Sessions>` configuration documentation is available at https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2065334342/Sessions

```
<!--
Controls session lifetimes, address checks, cookie handling, and the protocol handlers.
You MUST supply an effectively unique handlerURL value for each of your applications.
The value defaults to /Shibboleth.sso, and should be a relative path, with the SP computing
a relative value based on the virtual host. Using handlerSSL="true", the default, will force
the protocol to be https. You should also set cookieProps to "https" for SSL-only sites.
Note that while we default checkAddress to "false", this has a negative impact on the
security of your site. Stealing sessions via cookie theft is much easier with this disabled.
-->
<Sessions lifetime="28800" timeout="3600" relayState="ss:mem"
checkAddress="true" handlerSSL="true" cookieProps="https">
```

The following specifies the **`entityID`** of the idP to use for authentication. Get it from the idP metadata. We also specify that we speak only **`SAML2`** protocol:

```
<SSO entityID="[your idP's entityID, a URI] e.g. http://sso.med.harvard.edu/adfs/services/trust">
    SAML2
</SSO>
```

When logging out, only log out of the local Shibboleth session:

```
<Logout>Local</Logout>
```

Setting the status-reporting-service URL (relative to the hostname) to "/Shibboleth.sso/Status":

```
<Handler type="Status" Location="/Status"/>
```

Setting the session diagnostic service to "/Shibboleth.sso/Session":

```
<Handler type="Session" Location="/Session" showAttributeValues="true"
contentType="application/json"
/>
```

The IdP's metadata should be stored in a file called **`idp-metadata.xml`**. It should be obtained from the IdP admin(s):

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

You can customize the error pages, at least with an email

```
        <!--
        <Errors supportContact="<your contact email address>"> tag allows overriding of error template
information/filenames. You can
        also add attributes with values that can be plugged into the templates.
        See https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2065334361/Errors
        -->
        <Errors supportContact="<your contact email address>" />
```

The **`attribute-map.xml`** file (as set by the "**path**" xml attribute) will specify which attributes are extracted from the IdP's response and the name of the request headers or attributes they will be available to the Servlet code. More on this file below:

```
<AttributeExtractor type="XML" validate="true" reloadChanges="false" path="attribute-map.xml"/>
```

We left the following elements and the file `<AttributeFilter>` it points to unchanged:

```
<AttributeResolver type="Query" subjectMatch="true"/>
<AttributeFilter type="XML" validate="true" path="attribute-policy.xml"/>
```

This points to the key pair we created above:

```
<CredentialResolver type="File" key="/etc/shibboleth/sp-key.pem" certificate="/etc/shibboleth/sp-cert.pem"
password="<only if needed>" />
```

We left the following elements and the files they point to unchanged. See https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2065334523/SecurityPolicyProvider, "*By default, it's supplied in a separate file (security-policy.xml) because the settings are rarely altered*" and https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2065335163/ProtocolProvider, "*This is not a part of the configuration that requires changes, it's a point of extensibility.*")

```
<SecurityPolicyProvider type="XML" validate="true" path="security-policy.xml"/>
<ProtocolProvider type="XML" validate="true" reloadChanges="false" path="protocols.xml"/>
```

If needed, refer to `shibboleth2.xml.dist`

`/etc/shibboleth/idp-metadata.xml`

Get it from your IdP.

`/etc/shibboleth/attribute-map.xml`

The path of this file is specified in the `<AttributeExtractor>` element in `shibboleth2.xml`. This file specifies the SAML content that your SP turns into "attributes". These will be made available to the `ServletRequest` running on Tomcat. For Shrine SSO, the only attribute needed here is the user id returned by the idP, mapped to the "**`userId`**" id so it matches the `REMOTE_USER` attribute in `shibboleth2.xml`.

IMPORTANT: you must specify exactly one attribute whose **id** is "**`userId`**". The Shrine SP code will look for a request attribute of that **`id`** to populate the username in the code (which appears in the user account "badge" at the top-right corner of the UI).

```
<Attributes xmlns="urn:mace:shibboleth:2.0:attribute-map" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<!-- The 'name' attributes need to match exactly what your IdP sends in
its response to your (successful) AuthnRequest
-->
<Attribute name="[idP's name for the user id]" id="userId"/></Attributes>
```

Next Step:

SHRINE 4.0.0 Appendix A.4 - More Details: Apache Configuration