DSpace 7 Shibboleth Configuration

OBSOLETE PAGE

These old notes are now OBSOLETE. The official documentation for DSpace 7 + Shibboleth is now at Authentication Plugins#ShibbolethAuthentication

Problem

Based on the work done on https://github.com/DSpace/dspace-angular/pull/568 and https://github.com/DSpace/DSpace/pull/2651 , it isn't been possible for all to accomplish authentication using shibboleth. We agree to share workable configurations.

Solution

In DSpace configuration, local.cfg file, ensure these lines are uncommented:

```
# Shibboleth authentication/authorization. See authentication-shibboleth.cfg for default configuration.
plugin.sequence.org.dspace.authenticate.AuthenticationMethod = org.dspace.authenticate.ShibAuthentication

# Enabled by default in authentication.cfg
plugin.sequence.org.dspace.authenticate.AuthenticationMethod = org.dspace.authenticate.PasswordAuthentication
```

we also use default attributes that are mapped in my Shibboleth (version 3.0.4) attribute map (this may differ accordingly with the IdP).

In my local setup (Paulo Graça), I'm using Apache/2.4.6 (CentOS) with Proxypass with this settings. This is also tested (Ben Bosman) with Apache/2.4.41 (Amazon Linux 2) and (Andrea Bollini (4Science)) in the offical demo with Apache 2 (Ubuntu 18.04LTS):

```
<VirtualHost *:443>
#(...)
        <Proxy *>
                AddDefaultCharset Off
                Order deny,allow
                Allow from all
        </Proxy>

        # The Shibboleth handler shall process all HTTPS requests on this location...
    <Location /server/api/authn/shibboleth>
        Order deny,allow
        Allow from all
                AuthType shibboleth
        # this must be on
        ShibRequireSession On
                ShibUseHeaders On
                Require shibboleth
    </Location>
        # The Shibboleth handler shall process all HTTPS requests on this location...
    <Location /server/api/authn/login>
        Order deny,allow
        Allow from all
                AuthType shibboleth
                # this require to be off otherwise the available auth methods will be not visible
        ShibRequireSession Off
                ShibUseHeaders On
                Require shibboleth
    </Location>

    #Adding SSL Proxy Engine On
    SSLProxyEngine on
        ProxyRequests off
    ProxyPreserveHost On

        # A specific configuration for shibboleth proxypass
        ProxyPass /Shibboleth.sso !

        # A specific proxypass configuration for DSpace server (both server and angular on the same machine)
        ProxyPass /server ajp://localhost:8009/server
        ProxyPassReverse /server ajp://localhost:8009/server

        # A specific proxypass configuration for Angular
        ProxyPass / http://localhost:3000/
        ProxyPassReverse / http://localhost:3000/
#(...)
</VirtualHost>
```

The AJP proxy only works (Ben Bosman) if shibboleth2.xml **doesn't** contain the attribute *attributePrefix="AJP_"* in the ApplicationDefaults.

I'm (Paulo Graça) also using Tomcat v9 (apache-tomcat-9.0.30) and java-11-openjdk.x86_64, with a almost default tomcat server.xml file. Ben Bosman has created the setup with apache-tomcat-9.0.31 and OpenJDK Runtime Environment Corretto-11.0.6.10.1:

```
<?xml version="1.0" encoding="UTF-8"?>
<Server port="8005" shutdown="SHUTDOWN">
  <!-- (...) -->
    <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
    <Engine name="Catalina" defaultHost="localhost">
  <!-- (...) -->
      <Host name="localhost"  appBase="/dspace/webapps" unpackWARs="true" autoDeploy="true" xmlNamespaceAware="
false" xmlValidation="false">
                <Context allowLinking="true" path="" docBase="server" />
        <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs" prefix="access_log"
suffix=".log" pattern="%h %l %u %t "%r" %s %b" />
      </Host>
    </Engine>
  <!-- (...) -->
  </Service>
</Server>
```

Separate REST and Angular hostname

When using separate hostnames for REST and Angular, more configuration is required on the REST Apache to make sure you allow requests from the given hostname. The configuration below allows access from localhost:4000 and dspace7-demo.atmire.com as used in the official DSpace 7 Demo where the REST API is hosted at a different domain dspace7.4science.it

Apache config

```
  Header set Access-Control-Expose-Headers: "Authorization, expires, Location, Content-Disposition, WWW-
Authenticate, Set-Cookie, X-Requested-With"
```

Also make sure you don't have a Proxy for http://localhost:3000/ if you're testing from http://localhost:3000/

This setup currently causes warnings:

A cookie associated with a cross-site resource at http://dspace7-rest.atmire.com/ was set without the `SameSite` attribute. A future release of Chrome will only deliver cookies with cross-site requests if they are set with `SameSite=None` and `Secure`. You can review cookies in developer tools under Application>Storage>Cookies and see more details at https://www.chromestatus.com/feature/5088147346030592 and https://www.chromestatus.com/feature/5633521622188032.

A custom context.xml is currently needed for tomcat to allow cookie to full work across domain, this is the current configuration on the official DSpace7 demo

```
<?xml version="1.0" encoding="UTF-8"?>
<Context>
 ...
    <CookieProcessor sameSiteCookies="none" />
 ...
</Context>
```

Finally, shibboleth seems to require to be configured to manage the SameSite=None property in its cookies to work properly with DSpace. Please note that this is not what the shibboleth community recommend but it is the result of our current investigation according to the dspace source code at the time of writing, see https://wiki.shibboleth.net/confluence/display/SP3/SameSite

Moreover, on the demo, as the shibboleth daemon version doesn't support the specific attribute **sameSiteSession** (see https://wiki.shibboleth.net/confluence/display/SP3/Sessions)

we have applied a workaround settings cookieProps as follow

shibboleth2.xml

```
...
<Sessions lifetime="28800" timeout="3600" relayState="ss:mem"
                checkAddress="false" handlerSSL="false" cookieProps="; path=/; SameSite=None; Secure; HttpOnly">
...
```

Related resources

- DSpace 7 Shibboleth Configuration