Adding ESGF-Security to THREDDS

Before publishing test datasets, it is necessary to install some security components and filters to support ESGF-Security.

Enable Tomcat SSL security

To enable ssl we need a valid certificate from a Certificate Authority such as Verisign. We can create one although the browser will not recognize as trusted. We will need two files: keystore and truststore. A keystore is a file which contains private keys and certificates. The certificates are sent to the remote server in a SSLConnection. A truststore contains the CA certificates you are willing to trust when a remote party presents its certificate.

Install and configure SSL support on Tomcat 6

Create a keystore file to store the server's private key and self-signed certificate by executing the following:

Important: set your hostname as CN. (See error "Target is not trusted" ?http://esgf.org/wiki/Security/FAQ. For example, if you are deploying tomcat for testing in your own machine use CN=localhost.

```
keytool -genkey -alias tomcat -keyalg RSA
password: changeit
```

This command will create a file in your user home directory named ".keystore". This keystore contains the server certificate whose alias is *localhost*.

Download the ESGF Truststore which contains the trusted CA's and add your localhost certificate:

1. You can download the ESGF truststore from here ?https://rainbow.llnl.gov/dist/certs/esg-truststore.ts and add your tomcat certificate by yourself or download the esg-truststore.ts? which contains the tomcat pem. You can also download the .keystore?

   Uncomment the *SSL HTTP/1.1 Connector* entry in *$CATALINA_HOME/conf/server.xml* and add the following:

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"  SSLEnabled="true" maxThreads="150" scheme="ht
  clientAuth="want" keystoreFile="C:\apache-tomcat-6.0.36\config_files\esg-orp\.keystore" keystorePassword="changeit"
  truststoreFile="C:\apache-tomcat-6.0.36\config_files\esg-orp\esg-truststore.ts" truststorePass="changeit" sslProtocol=
```

1. Add the truststore to the classpath (it will be required by Java)

Edit $CATALINA_HOME/bin/setclasspath.bat (windows) or $CATALINA_HOME/bin/setclasspath.sh (Linux) and add the following:

```
 rem Windows
set "JAVA_OPTS=-Xmx2560m -Xms2560m -Ddebug=true -Djavax.net.ssl.trustStore=C:/apache-tomcat-6.0.36/config_files/esg-orp/es
echo %JAVA_OPTS%
```

Deploy and configure ESG-ORP

1. Start tomcat server. Run **$CATALINA_HOME/bin/startup.bat on windows** or **$CATALINA_HOME/bin/startup.sh** on Linux
2. Download esg-orp.war? and move it to **$CATALINA_HOME/webapps**. A new directory called 'esg-orp' will be created by Tomcat.

Edit WEB-INF/classes/esg-orp.properties to configure ESG-ORP to sign the cookies:

```
#location of keystore used to sign the authentication cookie
keystoreFile=$CATALINA_HOME/config_files/esg-orp/.keystore

#password used to read the keystore
keystorePassword=changeit

#alias of keystore entry used to sign the authentication cookie
keystoreAlias=localhost
```

ESG-ORP manages a list that is used to allow the idp's. It is called whitelist. The idp's are entities which provide an openid login and return a valid cookie. We will need two lists and you can download them from here esgf_idp.xml? esgf_idp_static.xml?. If your idp is not contained by *esgf_idp_static.xml* just add your idp to the file. It is recommended to save these files in **WEB-INF/classes/esg/config** to work properly in all environments because Windows paths are not considered by the momment.

The file which reads the lists is located in WEB-INF/classes/esg/orp/orp/config/security-context-auth.xml Go to the line 84 and replace it with this line:

```
<property name="idpWhiteListFile" value="esg/config/esgf_idp.xml, esg/config/esgf_idp_static.xml" />
```

Test ESG-ORP

Open your browser and type this url: ?http://localhost:8080/OpenidRelyingParty . You should be redirected to an HTTPS page where you are prompted to enter your openid.

TDS Configuration

Firstable, copy the following jars onto the TDS WEB-INF/lib directory thredds_esg_security_libraries.zip?.

Then edit the file $CATALINA_HOME/webapps/thredds/WEB-INF/web.xml and

Then edit the file $CATALINA_HOME/webapps/thredds/WEB-INF/web.xml and insert the XML snippet that configures the ESG access control filters to intercepts all requests sent to the TDS (see example below). You must configure the filter parameters to values that are specific to your system, specifically:

```
  <!-- web.xml entry for the esg node  access Control Filter chain -->

<filter>
  <filter-name>authenticationFilter</filter-name>
  <filter-class>esg.orp.app.AuthenticationFilter</filter-class>
  <init-param>
    <param-name>policyServiceClass</param-name>
    <param-value>esg.orp.app.CompositePolicyService</param-value>
  </init-param>
      <init-param>
    <param-name>policyServiceClasses</param-name>
    <param-value>esg.orp.app.RegexPolicyService, esg.orp.app.LocalXmlPolicyService</param-value>
  </init-param>
      <init-param>
    <param-name>authenticationNotRequiredPatterns</param-name>
    <param-value>"[^?]*(/|(/admin/)(.*)|(/remoteCatalogService\?.*)|(?&lt;=\.(html|xml|css|gif|pdf))(\?.*)?)"</param-valu
  </init-param>
       <init-param>
    <param-name>policyFiles</param-name>
    <param-value>thredds/config/esgf_policies_local.xml, thredds/config/esgf_policies_common.xml</param-value>
  </init-param>
  <init-param>
    <param-name>openidRelyingPartyUrl</param-name>
    <param-value>https://localhost:8443/esg-orp/home.htm</param-value>
  </init-param>
  <init-param>
    <param-name>trustoreFile</param-name>
    <param-value>C:/apache-tomcat-6.0.36/config_files/esg-orp/esg-truststore.ts</param-value>
  </init-param>
      <init-param>
    <param-name>trimURIRegEx</param-name>
    <param-value>\.ascii.*,\.dods.*,\.dds.*,\.das.*</param-value>
  </init-param>
  <init-param>
    <param-name>trustorePassword</param-name>
    <param-value>changeit</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>authenticationFilter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

```
 <!-- web.xml entry for the esg node authorization Control Filter chain -->

<filter>
  <filter-name>authorizationFilter</filter-name>
  <filter-class>esg.orp.app.AuthorizationFilter</filter-class>
  <init-param>
    <param-name>authorizationServiceClass</param-name>
    <param-value>esg.orp.app.SAMLAuthorizationServiceFilterCollaborator</param-value>
  </init-param>
  <init-param>
    <param-name>urlTransformer</param-name>
    <param-value>esg.orp.app.RegexReplaceAuthorizationFilterUrlTransformer</param-value>
  </init-param>
  <init-param>
    <param-name>urlTransformerReplacements</param-name>
    <param-value>"\?.*":"", "/dodsC/":"/fileServer/", "\.(asc|ascii|das|dds|dods|html)\Z":""</param-value>
  </init-param>
  <init-param>
    <param-name>authorizationServiceUrl</param-name>
    <param-value>
      https://localhost:8443/esg-orp/saml/soap/secure/authorizationService.htm
    </param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>authorizationFilter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

References

Tomcat configuration - ?http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html#Configuration

Esg-orp configuration - ?https://oodt.jpl.nasa.gov/wiki/display/CLIMATE/Part+2+-+Deploy+an+ESG+Openid+Relying+Party

Idps information - ?http://esgf.org/wiki/ESGF_IdPs

Manage openssl command - ?http://www.madboa.com/geek/openssl/#verify-standard

Esg-truststore - ?http://esgf.org/esg-certs/#ESG_Federation_Trust_Roots

Keystore and truststore - ?http://www.techbrainwave.com/?p=953

keytool commands - ?https://www.sslshopper.com/article-most-common-java-keytool-keystore-commands.html