

Morpho - Bug #201

add https support to client framework

04/09/2001 02:31 PM - Matt Jones

Status:	Resolved	Start date:	04/09/2001
Priority:	Normal	Due date:	
Assignee:	Dan Higgins	% Done:	0%
Category:	morpho - general	Estimated time:	0.00 hour
Target version:	1.7	Spent time:	0.00 hour
Bugzilla-Id:	201		
Description			
Need to enable HTTPS in Morpho, via the client framework. Right now it is enabled in each component, sometimes resulting in redundancy. Need to streamline to one http/https implementation in the framework that can be called from the plugins. Need corresponding support on the Metacat side.			
Related issues:			
Blocks Metacat - Bug #235: ssl support for metacat (https)		Resolved	06/05/2001

History

#1 - 06/13/2001 01:24 PM - Matt Jones

All metacat communication is now handled through methods in ClientFramework. Need to add https (SSL) support. Reassigned to bojilova to work on this.

#2 - 06/19/2001 03:45 PM - Jivka Bojilova

These are the things that should be done on the client for Morpho to communicate with Metacat through HTTPS:

1. Put JSSE jars as an extension on the clients machine: jart.jar, jnet.jar, jsse.jar to \$JAVA_HOME\lib\ext.

This won't be necessary with the next JSDK v1.4, because JSSE is no longer extension and comes as part of the core API.

2. In ClientFramework.getMetacatInputStream() set a System property as:
System.setProperty("java.protocol.handler.pkgs",
"com.sun.net.ssl.internal.www.protocol");
before the URL object of metacat_url to be established.

3. Add in \$JAVA_HOME\lib\security\java.security one line for the Sun's CSPProvider: SunJSSE.
security.provider.2=com.sun.net.ssl.internal.ssl.Provider
or again dynamically in Morpho by:
Security.addProvider(new com.sun.net.ssl.internal.ssl.Provider());

4. Use the keytool to import the certificate received from the server (Metacat) to the local keystore as:
keytool -import -alias dev -file dev.cer -keystore
\$JAVA_HOME\lib\security\cacerts

(In order to do this the server should have already generated the public/private key (the public key is initially in self-signed certificate) by:
keytool -genkey
and of course configured to communicate through https.
The same certificate can then be exported to a file as dev.cer by:
keytool -export -file dev.cer
which can be sent to the client for use. Client needs to import it on its end as a trusted certificate as shown above.)

5. Have in lib\config.xml <metacat_url> specified to:
<https://dev.nceas.ucsb.edu:8443/jones/servlet/metacat>

#3 - 07/12/2001 05:11 PM - Matt Jones

Changed milestone for a number of morpho features that will not be able to be

completed by Beta 1 (ESA). Delaying these features to Beta 2.

#4 - 03/12/2002 11:31 AM - Dan Higgins

Various requirements for HTTPS on the client side have been added to Morpho, but not tested. Need to get an HTTPS version of Metacat running in order to test.

#5 - 04/02/2002 10:12 AM - Dan Higgins

https support has been added to Morpho code.

This consisted of patching the HttpClient code to use jsse package from Sun. Then using ssl is the same as standard URL calls used in Morpho to communicate with Metacat.

Interestingly, if a self-signed certificate is used on Tomcat (for the Metacat servlet), one MUST set the NAME in the certificate to the server name (e.g. epsilon.nceas.ucsb.edu) and a trust certificate with the public key must be available to Morpho. See code in 'main' method of ClientFramework class to see how various properties are set to use ssl.

On a 700 MHz PC, the use of SSL adds about 10 sec to the startup time of Morpho.

#6 - 04/02/2002 10:13 AM - Dan Higgins

https support has been added to Morpho code.

This consisted of patching the HttpClient code to use jsse package from Sun. Then using ssl is the same as standard URL calls used in Morpho to communicate with Metacat.

Interestingly, if a self-signed certificate is used on Tomcat (for the Metacat servlet), one MUST set the NAME in the certificate to the server name (e.g. epsilon.nceas.ucsb.edu) and a trust certificate with the public key must be available to Morpho. See code in 'main' method of ClientFramework class to see how various properties are set to use ssl.

On a 700 MHz PC, the use of SSL adds about 10 sec to the startup time of Morpho.

#7 - 04/05/2002 09:00 PM - Dan Higgins

Currently, HTTPS support is included in Morpho code. Use of a self-signed certificate, however, requires that a copy of that self-signed certificate be included in the Morpho /lib directory and be named "morphocacerts".

Web browsers, however, give users the choice of accepting certificates that are not in the trust chain; ie they can connect without having a local copy of the certificate. Default jsse operation (ie https use of URL) just throws an error however.

We need to eventually fix code not to fail, but to let user choose to use a self signed certificate without having a local copy.

#8 - 04/09/2002 01:29 PM - Dan Higgins

https support that has been added to version 1.1.0 of Morpho does NOT work on older Macintosh OSs (i.e. pre OS X). This is because the Sun JSSE classes needed were written to work with Java 1.3 and greater, while pre OS-X versions of Java on the Mac only run Java 1.1.8

As a result, the https code that is in Morpho 1.1.0 has been removed from the Mac OS9 version of Morpho. This includes using an older version of the HttpClient library.

#9 - 11/11/2010 12:18 PM - ben leinfelder

we have been using https for KNB communication since Morpho 1.7.0

#10 - 03/27/2013 02:13 PM - Redmine Admin

Original Bugzilla ID was 201