Metacat - Bug #235

ssl support for metacat (https)

06/05/2001 03:40 PM - Matt Jones

Status:	Resolved	**Start date:**	06/05/2001
Priority:	Normal	**Due date:**	
Assignee:	Jivka Bojilova	**% Done:**	0%
Category:	metacat	**Estimated time:**	0.00 hour
Target version:	Beta2	**Spent time:**	0.00 hour
Bugzilla-Id:	235		

Description

Need support for clients to connect to metacat using ssl. Need to determine a reasonable way of generating and assigning certificates (probably we generate them and provide a central registry of metacat servers where clients can get the public keys).

Need support for metacat to contact LDAP over SSL to make this a secure connection.

Related issues:

Blocked by Morpho - Bug #201: add https support to client framework	**Resolved**	**04/09/2001**
Blocked by Metacat - Bug #185: replication security hole	**Resolved**	**04/09/2001**

History

#1 - 06/19/2001 04:26 PM - Jivka Bojilova

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

1. in $TOMCAT_HOME/conf/server.xml uncomment this part for SSL suport:

<Connector className="org.apache.tomcat.service.PoolTcpConnector">
<Parameter name="handler"
value="org.apache.tomcat.service.http.HttpConnectionHandler"/>
<Parameter name="port"
value="8443"/>
<Parameter name="socketFactory"
value="org.apache.tomcat.net.SSLSocketFactory" />
</Connector>

but comment the part for the normal HTTP.

2. Download JSSE and install JSSE jars by coping jart.jar, jnet.jar, jsse.jar to $JAVA_HOME/jre/lib/ext.

3. Edit $JAVA_HOME/jre/lib/security/java.security by adding one line for Sun's CSProvider "SunJSSE":
security.provider.2=com.sun.net.ssl.internal.ssl.Provider

4. Do: keytool -genkey -alias tomcat -keyalg RSA -keystore /opt/httpd/.keystore
RSA is essential to work with Netscape and IIS. Use "changeit" as password. (or add keypass attribute to change it.) You don't need to sign the certificate.

This generates key pair with self-signed certificate holding the public key. You don't need to sign the certificate. Check with:
keytool -list -alias tomcat

5. vi $TOMCAT_HOME/bin/tomcat.sh. In there add the HTTPS handler by:
TOMCAT_OPTS="-Djava.protocol.handler.pkgs=edu.ucsb.nceas.protocols|com.sun.net.ssl.internal.www.protocol"

6. Restart Tomcat to take effects.

7. In order for the client to trust that certificate you should export it in a file. Send that file to the client who then should import it as a trusted certificate.
keytool -export -alias tomcat -file dev.cer -keystore /opt/httpd/.keystore

dev.cer is the file to be sent to the client.

#2 - 06/19/2001 04:56 PM - Jivka Bojilova

2. Download JSSE and install JSSE jars by coping jart.jar, jnet.jar, jsse.jar to $JAVA_HOME/jre/lib/ext and to $TOMCAT_HOME/lib.

#3 - 07/13/2001 03:35 PM - Jivka Bojilova

DONE

#4 - 03/27/2013 02:13 PM - Redmine Admin

Original Bugzilla ID was 235