Metacat - Bug #449

Enable ssl for metacat and morpho

03/26/2002 01:27 PM - Jing Tao

Status:	Resolved	**Start date:**	03/26/2002
Priority:	Immediate	**Due date:**	
Assignee:	Jing Tao	**% Done:**	0%
Category:	marine	**Estimated time:**	0.00 hour
Target version:	1.1	**Spent time:**	0.00 hour
Bugzilla-Id:	449		

Description

Now communication between Metacat and Morpho uses plain text. In order to increase security, we want to enable SSL.

History

#1 - 03/27/2002 10:34 AM - Jing Tao

Just now I read a web site:
http://jakarta.apache.org/tomcat/tomcat-3.3-doc/tomcat-ssl-howto.html
It is said, if Tomcat only serves as a Servlet/JSP container behind another web server (dev has this siuation), the web server (Apache) should be configured as SSL rather than Tomcat.
In my machine, Tocat serves as both web server and ervlet/JSP container. I would like to try configure my local machine first.

#2 - 03/29/2002 01:38 PM - Jing Tao

Here is how we configured Tomcat standalone as both web server and servlet container.

1. Download and install JSSE
Download JSSE package from java.sun.com and unzip it. Copy the three files - jcert.jar, jnet.jar and jsse.jar in Jsse_home/lib to $Java_home/jre/lib/ext

2. Edit file $Java_home/jre/lib/security/java.security
Add a line:
security.provider.3=com.sun.net.ssl.internal.ssl.Provider

3. General public and private keys:
In $Java_home/bin directory, type command:
keytool -genkey -alias tomcat -keyalg RSA
It will create keys and store it in the file ".keystore" in the default directory /home/usr
More information can be gotten form java documentation about keytool.
Please remember the keystore password.

4. Edit file $Tomcat_home/conf/server.xml
Uncomment the part about https and make them look like:

```
<Http10Connector  port="8443"
secure="true"
keystore="/home/tao/.keystore"
keypass="123456"
clientAuth="false"

SSLImplementation="org.apache.tomcat.util.net.JSSEImplementation" />
```

Don't comment the Http10Connector for port 8080. It will be use to catch systle sheet and other things.

4. Edit the build.xml in metacat.
Add a property named systemidserver, its value="http://host.domainname:8080"
Add a token named systemidserver too.
This is for stylesheet. So we can catch sytle without ssl and performance will be better.

5. Edit the knb.xml in metacat/lib
Change every "http://server" in target to "systemidserver". It will look

like that:
<target
publicid="-//W3C//HTML//EN">systemidserver@style-path@/resultset.xsl</target>

6. Edit the loaddtd.sql in metacat/src
Change every "http://server to "systemidserver". It will look like:
INSERT INTO xml_catalog (entry_type, public_id, system_id)
VALUES ('DTD', '-//ecoinformatics.org//eml-software-eml-version//EN',
'systemidserver@html-path@/dtd/eml-software-eml-version.dtd')

7. Install Metacat again from scratch (include "ant dtdsql")

8. Edit the tomcat.sh file in $tomcat_home/bin
Change TOMCAT_OPTS to
TOMCAT_OPTS="-Djava.protocol.handler.pkgs=edu.ucsb.nceas.protocols|com.sun.net.s
sl.internal.www.protocol"

9. Stop and restart Tomcat

10. User keytool to create a file and distribute to users
In $java_home/bin, type the command
keytool -export -alias tomcat -file tomcat.cer
tomcat.cer will be create in the directory $java_home/bin.

#3 - 03/29/2002 01:44 PM - Matt Jones

Great. A note about TOMCAT_OPTS. We should not be editing the tomcat.sh file.
It is not needed. I was able to do the same thing by setting the "TOMCAT_OPTS"
environment variable when running tomcat.sh. Look at /etc/rc.d/init.d/tomcat to
see an example of how this works. This way, when we upgrade TOMCAT stuff will
still work with the new tomcat.sh.

BTW, we need the tomcat startup script to be copied to ecoinfo as well. RIght
now it is manually started.

#4 - 03/29/2002 04:50 PM - Jing Tao

In my local machine, I cancel the changes in tomcat.sh and got an copy the
file tomcat from /etc/rc.d/init.d in dev. I make some changes to in the tomcat
and it worked fine.

I couldn't copy this /etc/rc.d/init.d/tomcat to ecoinfo because some
permission issue. I will do it soon

#5 - 04/01/2002 02:56 PM - Jing Tao

I aked Colby to copy the tomcat file to /etc/rc.d/init.d directory in ecoinfo.

#6 - 04/02/2002 10:43 AM - Jing Tao

When we create the keys by keytool. If it is selfsinged, we should put the
first name and last name as server's name (no port number).
If do this, the style sheet and dtd can be access by ssl (https).

So now metacat can be configured to use ssl or not to access systle sheet and
dtd file.

#7 - 04/02/2002 10:57 AM - Jing Tao

Tomcat standalone was successfully configured to support ssl. But in the dev
and ecoinfo, apache is web server. There is some difference. So we need to add
another bug for configure ssl in dev and ecoinfo.

#8 - 03/27/2013 02:14 PM - Redmine Admin

Original Bugzilla ID was 449