Metacat - Bug #468

TLS between ldap server and metacat

04/11/2002 11:25 AM - Jing Tao

Status:	Resolved	**Start date:**	04/11/2002
Priority:	Immediate	**Due date:**	
Assignee:	Jing Tao	**% Done:**	0%
Category:	metacat	**Estimated time:**	0.00 hour
Target version:	1.6	**Spent time:**	0.00 hour
Bugzilla-Id:	468		

Description

We already figured out hwo connect metacat with client. But we still need
metacat connect ldap server throught TSL. We will use startTls to handle this.

History

#1 - 10/14/2002 12:28 PM - Matt Jones

Fixed typo in bug simmary: TSL should have been TLS

#2 - 04/30/2003 06:10 PM - Jing Tao

Postphone it to next release

#3 - 09/21/2004 04:10 AM - Matt Jones

We need to implement TLS as soon as possible, as its a real problem we're passing so many passwords around in cleartext. Maybe fold this into the redesign for PKI certificates as part of the EcoGrid work.

#4 - 10/06/2005 04:49 PM - Saurabh Garg

I was able to setup secure connection between ldap and metacat without any changes in the code. There might be a need to change to the code to use ldapsUrl when it is specified in metacat.properties. I dont think any change is required in classes being used by current code.
So if ldaps url is specified in the ldapurl in metacat.properties then TLS is started by the current classes being used. A point that verifies this is that if I follow the instructions from this page:
http://java.sun.com/products/jndi/tutorial/ldap/ext/starttls.html
and include following code
StartTlsResponse tls =
(StartTlsResponse) ctx.extendedOperation(new StartTlsRequest());
SSLSession sess = tls.negotiate();

I get the following error:
LDAP: error code 1 - TLS already started

It would be helpful to know why we have ldapUrl and ldapsUrl in metacat.properties. e.g.
ldapurl=ldap://machination.msi.ucsb.edu:386/
ldapsurl=ldaps://machination.msi.ucsb.edu:636/

If we just have the ldapUrl and specify ldapsUrl in it if we want to use ldaps.
e.g.
ldapurl=ldaps://machination.msi.ucsb.edu:636/

#5 - 01/19/2006 11:40 AM - Saurabh Garg

Closing the bug. I was able to run TLS (see my last comment)

Making a note in bug# 2175 for this bug as the new setup should have TLS between metacat and ldap. So if there is a problem in that, then this bug can be reopened.

#6 - 05/16/2006 09:43 AM - Saurabh Garg

Have to modify current code in AuthLdap.java and integrate new code from Matt into AuthLdap.

#7 - 08/02/2006 12:23 PM - Saurabh Garg

The code change was working on my machine but was not working on KNB. The testing was done with the PISCO certificate provided by Jordan. My machine has jdk 1.5 on it and KNB had 1.4. So that might be a problem.

I tried running jdk 1.4 on my machine and I ran into the same problem as I have seen on KNB. So I will have to install Java 1.5 on KNB to be able to use the PISCO certificate. Will close the bug after doing that and verifying that the code works on KNB.

#8 - 08/16/2006 10:22 AM - Saurabh Garg

Verified the code on KNB. There was some problem in running tomcat 5.0 with jdk1.5 and using xml jars that come with tomcat 5.0. But after removal of the jars, everything seems to be running.

The code run fine on KNB. Now TLS is used while passing the username and password information to KNB ldap. TLS is also used while passing the username passwd info to PISCO ldap. The certificates are missing for LTER-ldap - hence that is not setup yet.

Closing the bug.

#9 - 03/27/2013 02:14 PM - Redmine Admin

Original Bugzilla ID was 468