

Metacat - Bug #502

Security issues in replication

05/10/2002 01:02 PM - Jing Tao

Status:	Resolved	Start date:	05/10/2002
Priority:	Normal	Due date:	
Assignee:	Jing Tao	% Done:	0%
Category:	metacat	Estimated time:	0.00 hour
Target version:	1.2	Spent time:	0.00 hour
Bugzilla-Id:	502		
Description			
During the replication, security is a issue too. At least, we need some authentication for control server list.			
We maybe set a table name xml_replicationadmin in database and store some administrative users and their password there. So we can check the authentication for it.			

History

#1 - 05/20/2002 03:30 PM - Jing Tao

public key couldn't control the replication.

If in NCEAS keystore, it didn't contain LTER's public key. But LTER is still in the replication table in NCEAS. NCEAS couldn't replicate a document to LTER by Force Replication because untrust chain. This is good.

But, LTER can use delta T replication to get the documents from NCEAS easily (LTER is easy to install NCEAS public key in its keystore).

So the installation of public key in key store can control Force replication, but couldn't control delta T replication.

#2 - 05/21/2002 10:15 AM - Jing Tao

Now code was changed and public key can be a control for replication. Even a server is the replication server list, but if its public key is NOT in the metacat default keystore, replication couldn't be carried out by either force or delta T replication.

A very simple action "test" was added into MetacatReplication class. It only send back a successful message.

In handleUpdateRequest, handleGetDocumentRequest and handleGetDataFileRequest, the test action will be executed by sending request through "https" at first. So if LTER send a getDocument request to NCEAS, NCEAS should send back a test action to LTER by https. If public key of LTER was not installed in the default keystore in NCEAS, this will cause an exception. So NCEAS would not send the document to LTER. If LTER's public key was installed, the document will be sent. Same thing will happen to handleUpdateRequest and handleGetDataFileRequest too.

The installation of public key into keystore will control the replication happen or not. So it becomes an authentication for replication. Administrator of MetaCat can control it.

#3 - 03/27/2013 02:14 PM - Redmine Admin

Original Bugzilla ID was 502