Java Client - Story #6570

libclient should give better indication of expired certificates

2014-11-15 18:41 - Jing Tao

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Rob Nahf	**% Done:**	100%
Category:	d1_libclient_java	**Estimated time:**	0.00 hour
Target version:	CLJ		
Story Points:			

Description

A user with an expired cilogon certificate should be treated as the user public in D1Client:

The day before yesterday I downloaded a user cilogon certificate - /tmp/x509up_u502. It expired after 24 (or 12) hours but wasn't deleted.

Yesterday When I ran a junit class of Matecat and got a "peer not authenticated" error. The is error was caused by the line - NodeList nodeList = D1Client.getCN().listNodes(); Eventually I figured out the expired certificate /tmp/x509up_u502 caused the issue. After I removed it, the junit test worked.

The listNodes() method can be called by the user public. So a user with an expired cilogon certificate calling it wouldn't hurt anything. I think the D1Client maybe examines the user certificate first: if it expires, don't send it to the server, just treats it as the user public.

Related issues:

Related to Infrastructure - Bug #2411: knb MNs and CNs allow self-signed cert...	**In Progress**	**2014-10-01**	**2014-10-01**
Related to Infrastructure - Story #2548: recasting untrusted certs to public ...	**New**	**2012-03-27**	

Associated revisions

Revision 18501 - 2016-12-08 20:45 - Rob Nahf

refs: #6570, #7830: Refactored D1Client behavior under situations where it can't get a NodeList from CN_URL. Improved error messages, cleaned up some unnecessary complexity. Harmonized v1 and v2 implementaiton classes (NodeListNodeLocator, SettingsContextNL, D1Client). Added NodeLocator expiration to be able to pick up new MN BaseUrls periodically (5 minutes).

Revision 18501 - 2016-12-08 20:45 - Rob Nahf

refs: #6570, #7830: Refactored D1Client behavior under situations where it can't get a NodeList from CN_URL. Improved error messages, cleaned up some unnecessary complexity. Harmonized v1 and v2 implementaiton classes (NodeListNodeLocator, SettingsContextNL, D1Client). Added NodeLocator expiration to be able to pick up new MN BaseUrls periodically (5 minutes).

Revision 19054 - 2018-01-17 00:56 - Rob Nahf

refs #6570, #7830: Manual merge of refactoring found in trunk: Refactored D1Client behavior under situations where it can't get a NodeList from CN_URL. Improved error messages, cleaned up some unnecessary complexity. Harmonized v1 and v2 implementaiton classes (NodeListNodeLocator, SettingsContextNL, D1Client). Added NodeLocator expiration to be able to pick up new MN BaseUrls periodically (5 minutes).

Revision 19054 - 2018-01-17 00:56 - Rob Nahf

refs #6570, #7830: Manual merge of refactoring found in trunk: Refactored D1Client behavior under situations where it can't get a NodeList from CN_URL. Improved error messages, cleaned up some unnecessary complexity. Harmonized v1 and v2 implementaiton classes (NodeListNodeLocator, SettingsContextNL, D1Client). Added NodeLocator expiration to be able to pick up new MN BaseUrls periodically (5 minutes).

History

#1 - 2014-11-17 19:50 - Rob Nahf

*- Product Version changed from * to 2*

- translation missing: en.field_remaining_hours set to 0.0

- Start date deleted (2014-11-15)

- Tracker changed from Task to Story

This is an interesting situation where the response from the CN would be the same whether or not the user is authenticated or not. The current design of DataONE is to not allow expired certificates to be recast as public, because that would be confusing for users to suddenly have 'downgraded' access to content if their session expires in the middle of working with an application, and have no warning of the change in identity from the server's perspective. This is mostly a service configuration made a few years ago, but further development of libclient with respect to configuring libclient's trust-store away from "all-trusting" is in line with the notion of trust / authentication before information exchange.

From conversation in stand-up, the major frustration was the lack of diagnostic power with the PeerNotAuthenticated exception in determining where the problem was. Currently, this exception is wrapped as a ServiceFailure in order to comply with DataONE API, and the "Peer not authenticated" only appears as text, not an exception type.

It would be good to do something to help this situation, but the solution needs to be able to differentiate between different causes for the PeerNotAuthenticated exception expired client certificate vs. server not trusted vs. other client-not-trusted situations). Certificate handling is managed differently between v1 and v2 libclient, and so developing a solution for v2 would not be able to be merged back to v1.

Agreed in standup to discuss in full coredev meeting as a feature to be considered.

#2 - 2014-11-17 20:43 - Rob Nahf

- Subject changed from A user with an expired cilogon certificate should be treated as the user public in D1Client to libclient should give better indication of expired certificates

- Description updated

#3 - 2015-01-19 22:24 - Dave Vieglais

- Category deleted (d1_libclient_java)

- Project changed from Infrastructure to Java Client

#4 - 2015-02-11 20:45 - Rob Nahf

- % Done changed from 0 to 30

- Status changed from New to In Progress

- Category set to d1_libclient_java

- Target version set to CLJ-2.0.0

#5 - 2015-02-11 20:49 - Rob Nahf

- Status changed from In Progress to Testing

- % Done changed from 30 to 50

refctored CertificateManager and HttpMultipartRestClient (the class handling connections and calls) so that the certificate used by the connection manager is available for examination. The abstract base class for MNodes and CNodes now has a getRestClient() method that API calls utilize, and that method does the certificate expiration check before making the api call.

Now you should get a more immediately understandable exception message.

#6 - 2015-08-04 18:25 - Rob Nahf

- Target version changed from CLJ-2.0.0 to CLJ

not essential for v2.0

#7 - 2016-12-02 21:12 - Rob Nahf

When D1Client is used by servers, expired certificates cause warnings to be generated in the log files. These messages can get lost in the weeds when debugging, especially since it is only generated once at startup, then an empty NodeList is generated for the NodeLocator. (requested behavior to allow environment-less usage of libclient in metacat and other tools.

It was suggested that when an expired certificate is encountered, a more prominent exception (not ServiceFailure) and logging statement (ERROR or SEVERE?) be generated.

Maybe a RuntimeException should be thrown?

MultipartD1Node.getRestClient does check the validity of the certificate, but converts the CertificateExpiredException to ServiceFailure. This is the method that is called by every API method, so therein lies the rub.

#8 - 2016-12-08 21:05 - Rob Nahf

Initialization of D1Client's NodeLocator is more transparent, and failures to initialize due to communication errors will trigger re-initialization and continued warnings. Now, expired certificates are specifically checked for and return ExpiredCertificateException as the cause of the ServiceFailure.

#9 - 2018-01-17 19:44 - Dave Vieglais

- % Done changed from 50 to 100

- Status changed from Testing to Closed