Infrastructure - Bug #3627

inconsistent SSL peer not auth exceptions with KNB content (godaddy CA)

2013-02-28 00:12 - Rob Nahf

Status:	Rejected	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Rob Nahf	**% Done:**	0%
Category:	d1_client_r	**Estimated time:**	0.00 hour
Target version:			
Milestone:	None	**Story Points:**	
Product Version:	*		

Description

Some objects can be downloaded with the getD1Object D1Client method (in R), while others give the SSL peer not authorized exception from the same MN (knb.informatics.org). but the problem cannot be duplicated outside the R client.

Test conditions:
1) no client cert
2) no GoDaddy cert in the libclient shipped certs / using default shipped certs to extend the truststore
3) Rob's laptop, updated R client

Behavior:
the following can be downloaded:
doi:10.5063/AA/bowdish.217.3
resourceMap_bowdish.217.3
resourceMap_sharrer.6.1

these cannot
doi:10.5063/AA/bowdish.220.1
doi:10.5063/AA/bowdish.218.1
doi:10.5063/AA/bowdish.219.1
doi:10.5063/AA/sharrer.7.1

laptop was physically restarted to try to unstick any cache and the sharrer items were never seen before the tests, so could not be in libclient LocalCache....

Testing other setups gives consistent results:
1) curl, Rob, no client cert, laptop - both bowdish.220.1, and 217.3 can be downloaded
2) chrome, Rob, can get all objects
3) Robert, from cn, no client cert, gets consistent SSL peer not auth exceptions
4) Rob, via JUnit, no client cert, gets consistent SSL peer not auth exceptions

Testing on desktop R Client duplicates results on laptop

need to try to libclient trunk with laptop.

Related issues:

Related to Member Nodes - Task #3583: Production KNB node should return inter...	**Closed**	**2013-02-17**

History

#1 - 2013-02-28 00:15 - Rob Nahf

- Description updated

#2 - 2013-02-28 00:24 - Rob Nahf

info from R Client shows fewer CA certificates...

20130227-17:23:02: [INFO]: creating custom TrustManager [org.dataone.client.auth.CertificateManager]
20130227-17:23:02: [INFO]: loading into client truststore: [org.dataone.client.auth.CertificateManager]
20130227-17:23:02: [INFO]: 0 alias CN=DataONE Root CA,DC=dataone,DC=org [org.dataone.client.auth.CertificateManager]
20130227-17:23:02: [INFO]: 1 alias CN=DataONE Production CA,DC=dataone,DC=org [org.dataone.client.auth.CertificateManager]

20130227-17:23:02: [INFO]: 2 alias CN=CILogon Basic CA 1,O=CILogon,C=US,DC=cilogon,DC=org [org.dataone.client.auth.CertificateManager]
20130227-17:23:02: [INFO]: 3 alias CN=CILogon OpenID CA 1,O=CILogon,C=US,DC=cilogon,DC=org [org.dataone.client.auth.CertificateManager]
20130227-17:23:02: [INFO]: 4 alias CN=CILogon Silver CA 1,O=CILogon,C=US,DC=cilogon,DC=org [org.dataone.client.auth.CertificateManager]
20130227-17:23:02: [INFO]: 5 alias CN=RapidSSL CA,O=GeoTrust\, Inc.,C=US [org.dataone.client.auth.CertificateManager]
20130227-17:23:02: [INFO]: using allow-all hostname verifier [org.dataone.client.auth.CertificateManager]
checkServerTrusted - RSA

#3 - 2013-02-28 22:39 - Rob Nahf

- Status changed from New to Rejected

d1_libclient_java doesn't ship with the godaddy cert that KNB is sending out without the full CA chain. So, by that measure, the R Client should not be able to retrieve any content from that member node.

However, the R Client can gets around this limitation for science metadata and resourceMaps because it gets them from the CN after unsuccessful connect to KNB.

As there is already a ticket related to the missing intermediate certificate in the CA chain sent by KNB, ticket #3583, I'm simply rejecting the ticket.