

Infrastructure - Bug #4178

SSLException during metacat replicate cause hung replication requests

2013-11-14 18:06 - Skye Roseboom

<b>Status:</b>	Closed	<b>Start date:</b>	
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	Jing Tao	<b>% Done:</b>	100%
<b>Category:</b>	Metacat	<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>		<b>Story Points:</b>	
<b>Milestone:</b>	None		
<b>Product Version:</b>	*		
<b>Description</b>			
When an SSLException is thrown during MNodeService.replicate -- object = mn.getReplica(thisNodeSession, pid); -- the replication request failure is not communicated back to the CN, resulting in 'hung' requests.			
Example of exception log message:			
knb 20131114-08:36:02: [DEBUG]: Connecting to data.esa.org/128.111.54.82:443 [org.apache.http.impl.conn.DefaultClientConnectionOperator] checkServerTrusted - RSA CertMan Custom TrustManager: checking JVM trusted certs CertMan Custom TrustManager: server cert chain subjectDNs: CertMan Custom TrustManager: subjDN: CN=data.esa.org, OU=Domain Control Validated, O=data.esa.org / issuerDN: SERIALNUMBER=07969287, CN=Go Daddy Secure Certification Authority, OU= <a href="http://certificates.godaddy.com/repository">http://certificates.godaddy.com/repository</a> , O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US knb 20131114-08:36:02: [DEBUG]: Connection closed [org.apache.http.impl.conn.DefaultClientConnection] knb 20131114-08:36:02: [DEBUG]: Connection shut down [org.apache.http.impl.conn.DefaultClientConnection] knb 20131114-08:36:02: [DEBUG]: Releasing connection org.apache.http.impl.conn.SingleClientConnManager\$ConnAdapter@74904497 [org.apache.http.impl.conn.SingleClientConnManager] knb 20131114-08:36:02: [INFO]: rest call info: GET <a href="https://data.esa.org/esa/d1/mn/v1/replica/esa.67.3">https://data.esa.org/esa/d1/mn/v1/replica/esa.67.3</a> [org.dataone.client.RestClient] knb 20131114-08:36:02: [ERROR]: Error running replication: class javax.net.ssl.SSLPeerUnverifiedException: peer not authenticated [edu.ucsb.nceas.metacat.restservice.D1ResourceHandler] org.dataone.service.exceptions.ServiceFailure: class javax.net.ssl.SSLPeerUnverifiedException: peer not authenticated at com.sun.net.ssl.internal.ssl.SSLSessionImpl.getPeerCertificates(SSLSessionImpl.java:352)			
Chris - not sure who to assign this bug too, please assign as appropriate.			
<b>Subtasks:</b>			
Task # 4187: Confirm GMN handles SSL exceptions from source nodes appropriately			Closed
<b>Related issues:</b>			
Related to Infrastructure - Story #4193: Release CCI 1.2.4 Features			Closed 2013-12-11 2013-12-14

History

#1 - 2013-11-22 16:54 - Chris Jones

- Assignee changed from Chris Jones to Jing Tao

Assigning to Jing.

Jing, please investigate edu.ucsb.nceas.metacat.dataone.MNodeService.replicate(). When Metacat gets the request to replicate content, it should call getReplica() on the source MN. If this call fails, we should be calling back to the CN with CN.setReplicationStatus(FAILED). It looks like this is causing replica requests to remain in the REQUESTED state.

#2 - 2013-12-03 23:53 - Jing Tao

- Status changed from New to Closed

In the `edu.ucsb.nceas.metacat.dataone.MNodeService.replicate()` method, the exceptions were carefully checked and caught. In the caught clause, `CN.setReplicationStatus(FAILED)` is caught.

I tested the fixed code on the dev env:

1. Install the new metacat on mn-7 and mn-8.
2. It is hard to break the ca trust chain since mn-7 and mn-8 were signed by DataONE CA. So i created a self-signed key/certificate on mn-8.
3. Concatenate the mn-8 certificate to the `DataONETestCACHain.crt` on `cn-dev-ucsb-1` and `cn-dev-unm-1`.
4. Add the mn-8 certificate to the `cacert` of java on `cn-dev-ucsb-1` and `cn-dev-unm-1`.
5. Add the mn-8 certificate to the `cacert` of java of my local machine (morpho will use it).
6. Use morpho to insert a new document to the mn-8 and specify it to be replicated to mn-7.

I can see the ssl exception on tomcat log of mn-7 and status of replication of the package for mn-7 kept changing from queued to requested, failed:  
<https://cn-dev.test.dataone.org/cn/v1/meta/urn:uuid:8e132a5c-7c54-4dd4-bed3-61f65f5dbf17>

After i switched the key/certificate signed by DataONE CA on mn-8, the replication completed.