CN REST - Task #8617

Fix CN to CN replication in Stage

2018-06-17 01:30 - Chris Jones

Status:	Closed	**Start date:**	2018-06-17
Priority:	Normal	**Due date:**	
Assignee:	Chris Jones	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:			
Story Points:			

Description

While working on on-boarding ESS-DIVE in the Stage environment, we found that DATA objects were both sync'ing fine (their sysmeta) to the CNs, and they were indexing fine on the CNs. However, METADATA and RESOURCE object types were only sync'ing fine. They were failing to index. Looking at the indexer log files on cn-stage-orc-1, I saw errors where the indexer could not find the object (science metadata and resource map documents) on disk because there was no path to the object in the hzObjectPaths map.

I confirmed that:

1) There was no pid-to-docid entry in the PostgreSQL identifier table
2) There was no file on disk for these objects in /var/metacat/{data,documents}
3) That the system metadata for each document *did* exist in the PostgreSQL systemmetadata table

Since sysmeta replicates via Hazelcast and is persisted on all CNs, this didn't surprise me. But science metadata nad resource maps get replicated via the CN-to-CN Metacat replication service.

Looking at the replication.log files, the CNs were unable to create SSL connections among themselves, and replication wasn't working since May 18th, 2018. After trying this manually, I confirmed this didn't work.

After looking at the certificate key and cert files on each CN in /etc/dsataone/client/{certs,private}, I saw that the cn-stage-{orc,ucsb,unm}-1.test.dataone.org.{pem,key} files had the wrong subject in them. For instance:

```
subject= /DC=org/DC=dataone/CN=urn:node:cnStageORC1
notBefore=May 14 16:52:20 2018 GMT
notAfter=May 13 16:52:20 2021 GMT
```

This is the subject for the client certificate, not for the server certificate that is signed by the DataONE Test Intermediate CA, whic for instance is:

```
subject= /DC=org/DC=dataone/CN=cn-stage-orc-1.test.dataone.org
notBefore=Oct 13 22:12:57 2015 GMT
notAfter=Oct 12 22:12:57 2018 GMT
```

This file was updated in May on all three CNs, and the old certificate was moved to a .bak version. The .bak version still contained the un-expired certificate (expires in Oct 2018), which has the correct subject string in the certificate (the FQDN of the hostname).

I moved the .bak certificates back to the current active name. After forcing CN-to-CN replication via the Metacat Admin interface, all three CNs are now replicating to each other again, and are making their way through the backlog.

I think someone mistakenly copied the client certificate file to the server cert files used for Metacat, LDAP, and PostgreSQL replication when the client certificates were updated in may. This is likely just a procedure documentation issue. We'll have to look out for this as the certificates expire in the next few months.

History

#1 - 2018-06-17 01:30 - Chris Jones

- % Done changed from 0 to 100

- Status changed from New to Closed

#2 - 2018-06-17 16:33 - Chris Jones

- Description updated