Infrastructure - Task #6751

GLEON Node does not accept CN certificate

2015-01-09 16:31 - Skye Roseboom

Status:	Closed	**Start date:**	2015-01-09
Priority:	Normal	**Due date:**	
Assignee:	Mark Servilla	**% Done:**	100%
Category:	Support Operations	**Estimated time:**	0.00 hour
Target version:			
Milestone:	None	**Story Points:**	
Product Version:	*		

Description

In production, GLEON node is generating an 'unknown ca' error when the CN attempts to synchonize it.

Attached file of ssl handshake debug. Appears to indicate the GLEON certificate chain does not recognize the DataONE root CA.

Related issues:

Related to Member Nodes - MNDeployment #3422: GLEON	**Deprecated**	**2013-10-15**	**2015-03-31**

History

#1 - 2015-01-09 16:34 - Dave Vieglais

Might be worth checking using a test CN cert - it maybe that they have test installed instead of production.

#2 - 2015-01-09 16:43 - Skye Roseboom

Dave Vieglais wrote:

> Might be worth checking using a test CN cert - it maybe that they have test installed instead of production.

Good call - tried same request from cn-stage-ucsb-1.test.dataone (using test cert) and the request succeeds.

#3 - 2015-01-14 21:59 - Mark Servilla

- % Done changed from 0 to 80

- Status changed from New to In Progress

Mark Gahler of GLEON performed the following upgrade of their system:

> I've done these steps:
>
> 1. /etc/ssl/certs contains DataONECAChain.crt
> 2. Lines inside file /etc/apache2/site-enabled/metacat-site-ssl: SSLCertificateFile /etc/ssl/certs/poseidon_limnology_wisc_edu_cert.crt SSLCertificateKeyFile /etc/ssl/private/poseidon.key SSLCertificateChainFile /etc/ssl/certs/poseidon_limnology_wisc_edu_interm.crt SSLCACertificatePath /etc/ssl/certs/ SSLCACertificateFile /etc/ssl/certs/DataONECAChain.crt
>
> Should any of this be changed (I don't really understand the cert stuff)?
>
> 1. /etc/ssl/certs/c_rehash .
> 2. service apache2 restart

I was now able to confirm that the production DataONE cert performs as expected:

curl -E ./cnode.pem -v -X GET https://poseidon.limnology.wisc.edu/metacat/d1/mn/v1/node
* Hostname was NOT found in DNS cache
*   Trying 144.92.62.198...
* Connected to poseidon.limnology.wisc.edu (144.92.62.198) port 443 (#0)
* successfully set certificate verify locations:
*   CAfile: none
CApath: /etc/ssl/certs
* SSLv3, TLS handshake, Client hello (1):
* SSLv3, TLS handshake, Server hello (2):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Server key exchange (12):
* SSLv3, TLS handshake, Request CERT (13):
* SSLv3, TLS handshake, Server finished (14):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Client key exchange (16):
* SSLv3, TLS handshake, CERT verify (15):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSL connection using DHE-RSA-AES256-GCM-SHA384
* Server certificate:
*   subject: C=US; postalCode=53706; ST=WI; L=Madison; street=1210 West Dayton Street; O=University of Wisconsin-Madison; OU=OCIS; CN=poseidon.limnology.wisc.edu
*   start date: 2014-02-06 00:00:00 GMT
*   expire date: 2017-02-05 23:59:59 GMT
*   subjectAltName: poseidon.limnology.wisc.edu matched
*   issuer: C=US; O=Internet2; OU=InCommon; CN=InCommon Server CA
*   SSL certificate verify ok.

    GET /metacat/d1/mn/v1/node HTTP/1.1
    User-Agent: curl/7.35.0
    Host: poseidon.limnology.wisc.edu
    Accept: /

This ticket will remain open until final verification can be made during CN synchronization.

#4 - 2015-03-10 18:06 - Laura Moyers

- Status changed from In Progress to Closed

- % Done changed from 80 to 100

- translation missing: en.field_remaining_hours set to 0.0

Issue resolved.

Files

GLEON-ssl-handshake-error.log	162 KB	2015-01-09	Skye Roseboom