Infrastructure - Task #6742

KUBI member node not accepting cn certificate

2015-01-07 19:25 - Dave Vieglais

Status:	Closed	**Start date:**	2015-01-07
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

Looks like the KUBI MN is not accepting the CN certificate (this is using a copy of the CN client certificate to identify the requester as a CN). Task is to verify behavior and correct.

e.g.

curl -v -k --cert ../.dataone/cnode.pem "https://bidataone.nhm.ku.edu/mn/v1/object?count=0"
* About to connect() to bidataone.nhm.ku.edu port 443 (#0)
* Trying 129.237.201.57... connected
* 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 alert, Server hello (2):
* error:14094418:SSL routines:SSL3_READ_BYTES:tlsv1 alert unknown ca
* Closing connection #0
curl: (35) error:14094418:SSL routines:SSL3_READ_BYTES:tlsv1 alert unknown ca

Related issues:

Related to Member Nodes - MNDeployment #3188: Kansas University Biodiversity ...	**Deprecated**	**2012-09-05**	**2013-10-10**

History

#1 - 2015-01-07 20:28 - Mark Servilla

- Status changed from New to In Progress

#2 - 2015-01-07 22:19 - Mark Servilla

The following email was sent to CJ Grady at KUBI, along with the DataONECAChain.crt file:

MIME-Version: 1.0
Received: by 10.140.29.166 with HTTP; Wed, 7 Jan 2015 14:16:06 -0800 (PST)
Date: Wed, 7 Jan 2015 15:16:06 -0700
Delivered-To: mark.servilla@gmail.com
Message-ID:
Subject: DataONE certificate failure...
From: Mark Servilla mark.servilla@gmail.com
To: cjgrady@ku.edu
Cc: Laura Moyers lmoyers1@utk.edu
Content-Type: multipart/mixed; boundary=047d7bdcadbc19e880050c1745c8

--047d7bdcadbc19e880050c1745c8
Content-Type: multipart/alternative; boundary=047d7bdcadbc19e87c050c1745c6

--047d7bdcadbc19e87c050c1745c6
Content-Type: text/plain; charset=UTF-8

Hi CJ,

My name is Mark Servilla and I work with DataONE supporting general operations and Member Node issues. There is an issue (below; lines 20-22) when the DataONE Coordinating Node attempts to communicate with your MN server at https://bidataone.nhm.ku.edu when using the CN certificate. Since the CN certificate is signed by a DataONE specific CA, the DataONE CA chain file (attached) must be available to your web server for TLS negotiating and certificate verification. Judging from the diagnostic information in the curl snippet, your Apache configuration is using the default /etc/ssl/certs directory (line 7) for CA certificates. I am wondering if the DataONE CA chain file is missing from this directory or may have been modified, thus making it invalid? Note that this is in reference to DataONE Redmine ticket #6742 (https://redmine.dataone.org/issues/6742).

```
1 curl -v -k --cert cnode.pem "
https://bidataone.nhm.ku.edu/mn/v1/object?count=0"
2 * Hostname was NOT found in DNS cache
3 *   Trying 129.237.201.57...
4 * Connected to bidataone.nhm.ku.edu (129.237.201.57) port 443 (#0)
5 * successfully set certificate verify locations:
6 *   CAfile: none
7 CApath: /etc/ssl/certs
8 * SSLv3, TLS handshake, Client hello (1):
9 * SSLv3, TLS handshake, Server hello (2):
10 * SSLv3, TLS handshake, CERT (11):
11 * SSLv3, TLS handshake, Server key exchange (12):
12 * SSLv3, TLS handshake, Request CERT (13):
13 * SSLv3, TLS handshake, Server finished (14):
14 * SSLv3, TLS handshake, CERT (11):
15 * SSLv3, TLS handshake, Client key exchange (16):
16 * SSLv3, TLS handshake, CERT verify (15):
17 * SSLv3, TLS change cipher, Client hello (1):
18 * SSLv3, TLS handshake, Finished (20):
19 * SSLv3, TLS alert, Server hello (2):
20 * error:14094418:SSL routines:SSL3_READ_BYTES:tlsv1 alert unknown ca
21 * Closing connection 0
22 curl: (35) error:14094418:SSL routines:SSL3_READ_BYTES:tlsv1 alert
unknown ca
```

If you have any further questions or would like to discuss this via a video conference (Google Hangout or GoToMeeting), please let me know at your convenience.

Sincerely,
Mark

Mark Servilla
mark.servilla@gmail.com

#3 - 2015-01-08 18:23 - Mark Servilla

Additional email traffic on this issue revealed that the appropriate chain file (DataONECAChain.crt) was not in the expected /etc/ssl/certs directory:

MIME-Version: 1.0
Received: by 10.140.29.166 with HTTP; Wed, 7 Jan 2015 15:37:48 -0800 (PST)
In-Reply-To: CC2C04145913A34BA69782682A953D8772070B6A@EXCH10-MBX-02.home.ku.edu
References:
CC2C04145913A34BA69782682A953D8772070B6A@EXCH10-MBX-02.home.ku.edu
Date: Wed, 7 Jan 2015 16:37:48 -0700
Delivered-To: mark.servilla@gmail.com
Message-ID:
Subject: Re: DataONE certificate failure...
From: Mark Servilla mark.servilla@gmail.com
To: "Grady, C J" cjgrady@ku.edu
Cc: Laura Moyers lmoyers1@utk.edu, "Smith, Gregory D." gsmith@ku.edu
Content-Type: multipart/alternative; boundary=001a11c1e566422127050c1869b6

--001a11c1e566422127050c1869b6
Content-Type: text/plain; charset=UTF-8

Hi CJ,

The location is defined by your Apache site configuration file
(/etc/apache2/sites-enabled/gmn-ssl.conf for default GMN deployments); for
GMN, the default location of the certificates and chain files may be either
/var/local/dataone/certs/ca or /var/local/dataone/certs/server, but again,
it depends on your Apache config. Note that this issue is really between
the client (in this case, my local curl client) and the Apache web server,
so placing the chain file in /etc/ssl/certs should
work - I'm pretty sure that GMN doesn't come into play during
the negotiation/certificate verification at this point.

I really don't know when this issue first occurred, sorry.

Here's a direct link to the chain file:
https://repository.dataone.org/software/tools/trunk/ca/DataONECAChain.crt

Sincerely,
Mark

Mark Servilla
mark.servilla@gmail.com

On Wed, Jan 7, 2015 at 3:56 PM, Grady, C J cjgrady@ku.edu wrote:

> Hi Mark,
>
> You are correct that the chain file is not present in that location. I
> thought that it was configured to use a different location
> (/var/local/dataone/gmn_certs). Did this just start happening or has this
> never worked?
>
> The attachment was blocked, is there another way you can send it to me?
>
> Thanks,
>
> CJ

#4 - 2015-01-14 16:13 - Mark Servilla

As of this date (09:00 14 Jan 2015), the KUBI MN is still not accepting the CN certificate due to an "tlsv1 alert unknown ca" error.

#5 - 2015-01-28 18:27 - Mark Servilla

- Status changed from In Progress to Closed

- translation missing: en.field_remaining_hours set to 0

- % Done changed from 0 to 100

The following was performed by CJ as requested:

> Hi CJ,
>
> It's a shot in the dark, but here is something we can try:
>
> 1. Copy the following file into /var/local/dataone/certs/ca - https://repository.dataone.org/software/tools/trunk/ca/DataONECAChain.crt
> 2. Change ownership of the new DataONECAChain.crt file to gmn:www-data: chown gmn:www-data DataONECAChain.crt
> 3. Change permissions of the new DataONECAChain.crt to read/write owner and read group/world: chmod 644 DataONECAChain.crt
> 4. Make a backup copy of the GMN apache config file (gmn-ssl) for safe keeping and easy restore
> 5. Edit the GMN apache config file (gmn-ssl) and change the SSLCACertificateFile directive from "../cilogon_dataone_ca_chain.crt" to "../DataONECAChain.crt"
> 6. Restart apache: service apache2 restart
>
> Sincerely,
> Mark

Testing with the production D1 CN certificate now resolves correctly:

```
curl -v -k --cert cnode.pem "https://bidataone.nhm.ku.edu/mn/v1/object?count=0"
* Hostname was NOT found in DNS cache
*   Trying 129.237.201.57...
* Connected to bidataone.nhm.ku.edu (129.237.201.57) 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; ST=Kansas; L=Lawrence; O=University of Kansas; OU=Biodiversity Institute; CN=bidataone.nhm.ku.edu
*    start date: 2012-10-10 00:00:00 GMT
*    expire date: 2015-10-15 12:00:00 GMT
*    issuer: C=US; O=DigiCert Inc; OU=www.digicert.com; CN=DigiCert High Assurance CA-3
*    SSL certificate verify ok.

    GET /mn/v1/object?count=0 HTTP/1.1
    User-Agent: curl/7.35.0
    Host: bidataone.nhm.ku.edu
    Accept: /

    < HTTP/1.1 200 OK
    < Date: Wed, 28 Jan 2015 18:12:44 GMT
    * Server Apache/2.2.22 (Ubuntu) is not blacklisted
    < Server: Apache/2.2.22 (Ubuntu)
    < Last-Modified: Mon, 21 Oct 2013 17:32:09 GMT
    < Content-Length: 122
    < Content-Type: application/xml
    <
```

* Connection #0 to host bidataone.nhm.ku.edu left intact
<?xml version="1.0" ?>