Infrastructure - Support #3573

Ornithology Avian Knowledge Network node misconfigured

2013-02-14 03:35 - Robert Waltz

Status:	Closed	**Start date:**	2013-02-14
Priority:	High	**Due date:**	2014-04-12
Assignee:	Robert Waltz	**% Done:**	100%
Category:	Support Operations	**Estimated time:**	0.00 hour
Target version:	2014.14-Block.2.3		
Milestone:	CCI-1.2	**Story Points:**	
Product Version:	1.2		

Description

When attempting to retrieve log records on Ornithology Avian Knowledge Network MN from cn-unm-1.dataone.org, I receive the following response:

Only the CN or admin is allowed to harvest logs from this node

The initial problem is documented above. I have since attempted

curl --trace curl.out --cert /etc/dataone/client/private/urn_node_CNUCSB1.pem --capath /home/waltz/cloakn "https://dataone.ornith.cornell.edu/knb/d1/mn/v1/log?count=10"

curl: (35) error:14094418:SSL routines:SSL3_READ_BYTES:tlsv1 alert unknown ca

waltz@cn-ucsb-1:~$ sudo openssl s_client -connect dataone.ornith.cornell.edu:443 -cert /etc/dataone/client/private/urn_node_CNUCSB1.pem -CApath /home/waltz/cloakn -showcerts -state -verify 3
(note that the openssl command is passing a client certificate)
verify depth is 3
CONNECTED(00000003)
SSL_connect:before/connect initialization
SSL_connect:SSLv2/v3 write client hello A
SSL_connect:SSLv3 read server hello A
depth=3 /C=US/ST=UT/L=Salt Lake City/O=The USERTRUST Network/OU=http://www.usertrust.com/CN=UTN - DATACorp SGC
verify return:1
depth=2 /C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root
verify return:1
depth=1 /C=US/O=Internet2/OU=InCommon/CN=InCommon Server CA
verify return:1
depth=0 /C=US/postalCode=14853/ST=NY/L=Ithaca/streetAddress=no street/O=Cornell University/OU=Lab of Ornithology/CN=dataone.ornith.cornell.edu
verify return:1
SSL_connect:SSLv3 read server certificate A
SSL_connect:SSLv3 read server key exchange A
SSL_connect:SSLv3 read server certificate request A
SSL_connect:SSLv3 read server done A
SSL_connect:SSLv3 write client certificate A
SSL_connect:SSLv3 write client key exchange A
SSL_connect:SSLv3 write certificate verify A
SSL_connect:SSLv3 write change cipher spec A
SSL_connect:SSLv3 write finished A
SSL_connect:SSLv3 flush data
SSL3 alert read:fatal:unknown CA
SSL_connect:failed in SSLv3 read finished A
14203:error:14094418:SSL routines:SSL3_READ_BYTES:tlsv1 alert unknown ca:s3_pkt.c:1099:SSL alert number 48
14203:error:140790E5:SSL routines:SSL23_WRITE:ssl handshake failure:s23_lib.c:188:

Below is what I can gather is the certificate chain:

1) openssl s_client -CApath /home/waltz/cloakn -verify 3 -msg -debug -connect dataone.ornith.cornell.edu:443
(note that the openssl command is not passing a client certificate)
...
depth=3 /C=US/ST=UT/L=Salt Lake City/O=The USERTRUST Network/OU=http://www.usertrust.com/CN=UTN - DATACorp SGC
verify return:1
depth=2 /C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root
verify return:1
depth=1 /C=US/O=Internet2/OU=InCommon/CN=InCommon Server CA
verify return:1
depth=0 /C=US/postalCode=14853/ST=NY/L=Ithaca/streetAddress=no street/O=Cornell University/OU=Lab of Ornithology/CN=dataone.ornith.cornell.edu
...
Verify return code: 0 (ok)

2) The certificate chain:

From CLOAKN Server Certificate PEM
Subject: C=US/postalCode=14853, ST=NY, L=Ithaca/streetAddress=no street, O=Cornell University, OU=Lab of Ornithology, CN=dataone.ornith.cornell.edu

Issuer: C=US, O=Internet2, OU=InCommon, CN=InCommon Server CA
X509v3 Authority Key Identifier:
keyid:48:4F:5A:FA:2F:4A:9A:5E:E0:50:F3:6B:7B:55:A5:DE:F5:BE:34:5D

From InCommon Server Cerficate Authority PEM
Subject: C=US, O=Internet2, OU=InCommon, CN=InCommon Server CA

Issuer: C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External CA Root

```
        X509v3 Authority Key Identifier:
            keyid:AD:BD:98:7A:34:B4:26:F7:FA:C4:26:54:EF:03:BD:E0:24:CB:54:1A

        X509v3 Subject Key Identifier:
            48:4F:5A:FA:2F:4A:9A:5E:E0:50:F3:6B:7B:55:A5:DE:F5:BE:34:5D
```

From AddTrust External CA Root PEM
Subject: C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External CA Root

Issuer: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN - DATACorp SGC
X509v3 Authority Key Identifier:
keyid:53:32:D1:B3:CF:7F:FA:E0:F1:A0:5D:85:4E:92:D2:9E:45:1D:B4:4F

```
        X509v3 Subject Key Identifier:
            AD:BD:98:7A:34:B4:26:F7:FA:C4:26:54:EF:03:BD:E0:24:CB:54:1A
```

From The USERTRUST Network PEM
Subject: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN - DATACorp SGC

Issuer: C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN - DATACorp SGC

```
        X509v3 Subject Key Identifier:
            53:32:D1:B3:CF:7F:FA:E0:F1:A0:5D:85:4E:92:D2:9E:45:1D:B4:4F
```

The certificates are attached in a zipfile cloakn.tar.gz tar xvfz cloakn.tar.gz should provide the cloakn directory I have been using to test with.

History

#1 - 2013-03-01 19:22 - Robert Waltz

- Assignee changed from Robert Waltz to Ben Leinfelder

#2 - 2013-03-01 19:23 - Robert Waltz

- Due date changed from 2013-02-14 to 2013-03-16

- Milestone changed from CCI-1.1.1 to CCI-1.1.2

- Target version changed from 2013.6-Block.1.3 to 2013.10-Block.2.1

#3 - 2013-03-02 06:08 - Ben Leinfelder

- Status changed from New to In Progress

- Due date changed from 2013-03-16 to 2013-02-14

- Milestone changed from CCI-1.1.2 to CCI-1.1.1

- Target version changed from 2013.10-Block.2.1 to 2013.6-Block.1.3

- Assignee changed from Ben Leinfelder to Robert Waltz

Something is not quite right:

leinfelder@cn-ucsb-1:~$ sudo curl -v --cert /etc/dataone/client/private/urn_node_CNUCSB1.pem "https://dataone.ornith.cornell.edu/knb/d1/mn/v1/log"

returns

curl: (35) error:0B07C065:x509 certificate routines:X509_STORE_add_cert:cert already in hash table

While the same command works for, say, the SANParks MN.

#4 - 2013-06-05 04:37 - Robert Waltz

- Target version changed from 2013.6-Block.1.3 to 2013.22-Block.3.3

- Due date changed from 2013-02-14 to 2013-06-08

#5 - 2013-08-02 18:25 - Robert Waltz

- Due date changed from 2013-06-08 to 2013-08-03

- Target version changed from 2013.22-Block.3.3 to 2013.30-Block.4.3

#6 - 2013-08-14 14:30 - Dave Vieglais

- Target version changed from 2013.30-Block.4.3 to 2013.33-Block.4.4

- Due date changed from 2013-08-03 to 2013-08-24

#7 - 2013-08-14 20:23 - Robert Waltz

removed a couple nasty links in /etc/ssl/certs that were causing the problems for Ben on ucsb. Still having the same issues.

#8 - 2013-08-15 17:56 - Robert Waltz

- File cloakn.tar.gz added

- Description updated

#9 - 2013-08-15 17:57 - Robert Waltz

- Assignee changed from Robert Waltz to Chris Jones

- Milestone changed from CCI-1.1.1 to None

#10 - 2013-08-15 17:57 - Robert Waltz

- Priority changed from Normal to High

#11 - 2013-08-16 17:13 - Ben Leinfelder

Sent to Kevin Webb but got an error from the mail server:

Hi Kevin,
There's been some difficulty harvesting the log records from your MN:
https://redmine.dataone.org/issues/3573
I looked through my email to see if we'd previously gotten SSL client certificates working with AKN but I think perhaps that never got fully resolved. My guess is that your Apache server is still not trusting the DataONE (and perhaps the CILogon) Certificate Authority which would explain the "unknown ca" messages we receive.
Could you take a look at your Apache configuration and update the redmine ticket with your findings?
Thank you!
-ben

kfw4@cornell.edu: host ASPMX.L.GOOGLE.COM[173.194.79.26] said: 550-5.1.1 The
email account that you tried to reach does not exist. Please try 550-5.1.1
double-checking the recipient's email address for typos or 550-5.1.1
unnecessary spaces. Learn more at 550 5.1.1
http://support.google.com/mail/bin/answer.py?answer=6596 x6si2413577pab.107
- gsmtp (in reply to RCPT TO command)

#12 - 2013-08-22 16:02 - Chris Jones

- Assignee changed from Chris Jones to Ben Leinfelder

Assigning to Ben, since he's been working with Kevin.

#13 - 2013-10-15 22:53 - Ben Leinfelder

- Product Version set to 1.2

Curl command is now returning log records from this node - hope the same is true for CN log aggregation process.

#14 - 2013-10-16 15:51 - Ben Leinfelder

- Assignee changed from Ben Leinfelder to Robert Waltz

#15 - 2013-10-16 17:01 - Ben Leinfelder

Emailed Kevin to update nodeId on his end - will let you know when safe to reharvest log records.

#16 - 2013-10-28 20:04 - Robert Waltz

- Target version changed from 2013.33-Block.4.4 to 2013.44-Block.6.1

- Due date changed from 2013-08-24 to 2013-11-09

- Milestone changed from None to CCI-1.2

#17 - 2014-01-06 18:37 - Dave Vieglais

- Due date changed from 2013-11-09 to 2014-02-01

- Target version changed from 2013.44-Block.6.1 to 2014.4-Block.1.2

#18 - 2014-03-14 17:48 - Robert Waltz

- Due date changed from 2014-02-01 to 2014-04-12

- Target version changed from 2014.4-Block.1.2 to 2014.14-Block.2.3

#19 - 2014-07-30 04:16 - Robert Waltz

- Status changed from In Progress to Closed

Files

cloakn.tar.gz	4.5 KB	2013-08-15	Robert Waltz