Member Nodes - Task #4141

MNDeployment # 3188 (Deprecated): Kansas University Biodiversity Institute

Task # 4041 (Closed): Review KUBI synchronization results

Verify server SSL server certificate installation

2013-10-29 21:30 - Chris Jones

Status:	Closed	**Start date:**	2013-10-29
Priority:	Normal	**Due date:**	
Assignee:	CJ Grady	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	Operational		
Story Points:			

Description

After CJ and Roger worked on upgrading the GMN stack to the latest version available via PyPI, I reset the harvest date on the CNs, and attempted to re-sync the content. The CN reported SSL errors:

[ERROR] 2013-10-23 06:21:00,293 (ObjectListHarvestTask:retrieve:251) urn:node:TestKUBI-
<?xml version="1.0" encoding="UTF-8"?>

class javax.net.ssl.SSLPeerUnverifiedException: peer not authenticated

I tested the SSL connection manually using openssl, and also got an error. (I had previously written an email that said this worked, but I was wrong. You can get the /mn/v1/node document via fallback, but the SSL connection fails nonetheless)

cjones@cn-stage-ucsb-1:private$ sudo openssl s_client -connect bidataone.nhm.ku.edu:443 -showcerts -CApath /etc/ssl/certs
CONNECTED(00000003)
depth=0 /C=US/ST=Kansas/L=Lawrence/O=University of Kansas/OU=Biodiversity Institute/CN=bidataone.nhm.ku.edu
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 /C=US/ST=Kansas/L=Lawrence/O=University of Kansas/OU=Biodiversity Institute/CN=bidataone.nhm.ku.edu
verify error:num=27:certificate not trusted
verify return:1
depth=0 /C=US/ST=Kansas/L=Lawrence/O=University of Kansas/OU=Biodiversity Institute/CN=bidataone.nhm.ku.edu
verify error:num=21:unable to verify the first certificate

verify return:1

Certificate chain
0 s:/C=US/ST=Kansas/L=Lawrence/O=University of Kansas/OU=Biodiversity Institute/CN=bidataone.nhm.ku.edu
i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert High Assurance CA-3
-----BEGIN CERTIFICATE-----
MIIGzTCCBbWgAwIBAgIQAURtdQewWkpyaenKS0gnNzANBgkqhkiG9w0BAQUFADBm
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSUwIwYDVQQDExxEaWdpQ2VydCBIaWdoIEFzc3VyYW5j
ZSBDQS0zMB4XDTEyMTAxMDAwMDAwMFoXDTE1MTAxNTEyMDAwMFowgZAxCzAJBgNV
BAYTAlVTMQ8wDQYDVQQIEwZLYW5zYXMxETAPBgNVBAcTCExhd3JlbmNlMR0wGwYD
VQQKExRVbml2ZXJzaXR5IG9mIEthbnNhczEfMB0GA1UECxMWQmlvZGl2ZXJzaXR5
IEluc3RpdHV0ZTEdMBsGA1UEAxMUYmlkYXRhb25lLm5obS5rdS5lZHUwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCykMXiEYBhilP56kh14NAX3dS0JG4m
ODfc5YMM15qjc/6NboLTenUQxvJmolCoZJ0Xo14wzvb0ghr7/Nq7ph7lJaZfeAr2
U82q35mSX4Zix0OmsLulubzVhDwCah5Q5mjK/bJPvNl8t1ZaKXk3p93EAUVT8RL5
Vz3OjVjShWw2awjjHWqsuglKjaphZObAXkJZbm5egkROoYyZNVT5G/Jhnci1WVp5
p9bI4ljYDvF57mLsNMhBgsQCsRYCKgb2R/M8NVV6UNvQ4Qfpxc7Djl0zZJ1VUxWG
aLwtCgN1Qlqac8t5AkRoCnp9WQWB4ww3ANEkOGD2EvDW/gLGHme/T8TDAgMBAAGj
ggNKMIIDRjAfBgNVHSMEGDAWgBRQ6nOJ2yn7EI+e5QEg1N55mUiD9zAdBgNVHQ4E
FgQUJXpTCQyXhhvToyf3AR+NS6DPgEYwHwYDVR0RBBgwFoIUYmlkYXRhb25lLm5o
bS5rdS5lZHUwDgYDVR0PAQH/BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggr
BgEFBQcDAjBhBgNVHR8EWjBYMCqgKKAmhiRodHRwOi8vY3JsMy5kaWdpY2VydC5j
b20vY2EzLWcxNS5jcmwwKqAooCaGJGh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9j

YTMtZzE1LmNybDCCAcQGA1UdIASCAbswggG3MIIBswYJYIZIAYb9bAEBMIIBpDA6
BggrBgEFBQcCARYuaHR0cDovL3d3dy5kaWdpY2VydC5jb20vc3NsLWNwcy1yZXBv
c2l0b3J5Lmh0bTCCAWQGCCsGAQUFBwICMIIBVh6CAVIAQQBuAHkAIAB1AHMAZQAg
AG8AZgAgAHQAaABpAHMAIABDAGUAcgB0AGkAZgBpAGMAYQB0AGUAIABjAG8AbgBz
AHQAaQB0AHUAdABlAHMAIABhAGMAYwBlAHAAdABhAG4AYwBlACAAbwBmACAAdABo
AGUAIABEAGkAZwBpAEMAZQByAHQAIABDAFAALwBDAFAAUwAgAGEAbgBkACAAdABo
AGUAIABSAGUAbAB5AGkAbgBnACAAUABhAHIAdAB5ACAAQQBnAHIAZQBlAG0AZQBu
AHQAIAB3AGgAaQBjAGgAIABsAGkAbQBpAHQAIABsAGkAYQBiAGkAbABpAHQAeQAg
AGEAbgBkACAAYQByAGUAIABpAG4AYwBvAHIAcABvAHIAYQB0AGUAZAAgAGgAZQBy
AGUAaQBuACAAYgB5ACAAcgBlAGYAZQByAGUAbgBjAGUALjB7BggrBgEFBQcBAQRv
MG0wJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0LmNvbTBFBggrBgEF
BQcwAoY5aHR0cDovL2NhY2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0SGlnaEFz
c3VyYW5jZUNBLTMuY3J0MAwGA1UdEwEB/wQCMAAwDQYJKoZIhvcNAQEFBQADggEB
AB3kl3o0AHbvaZRvB0ynyx4RnzKz+UBzf/Kg9xGA/bZjhYQFD5b9ZpyYud/tiSFd
Z8h9SEeuirGnzhjlsz2t7cxbjqrWYbsq+LvJ4vrRVnJgInSzeaS2noDlnoVIVk/d
m/Gv6sIuOt0lGd7PNuMjwktyDnRt15DTbt2wURtAXOs9nkqlj+blJouQIyTd5AGc
5fjcyfcf5hxYOONRmB+AE23f6jon7Qax5JfId1oW2ID2XHnc7a4fo39PmD0o71Ug
dha04+XnOEKaNWCatkeMrzBso0+pn4MPzpSXgMpeGVw7LTbaO89X9Ff3rsz0IIq9
rFI+PG3VYbUb1GSNZkkpHhc=

-----END CERTIFICATE-----

Server certificate
subject=/C=US/ST=Kansas/L=Lawrence/O=University of Kansas/OU=Biodiversity Institute/CN=bidataone.nhm.ku.edu

issuer=/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert High Assurance CA-3

Acceptable client certificate CA names
/DC=org/DC=dataone/CN=DataONE Test CA
/DC=org/DC=dataone/CN=DataONE Test Intermediate CA
/DC=org/DC=cilogon/C=US/O=CILogon/CN=CILogon Basic CA 1
/DC=org/DC=cilogon/C=US/O=CILogon/CN=CILogon OpenID CA 1

/DC=org/DC=cilogon/C=US/O=CILogon/CN=CILogon Silver CA 1

SSL handshake has read 2953 bytes and written 331 bytes

New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
Protocol : TLSv1
Cipher : DHE-RSA-AES256-SHA
Session-ID: B842DE534668398C02BD2C1E368F60C94884320733BA5E33AD9B4173E304D0A8
Session-ID-ctx:
Master-Key:
DB1AAE4156FBEC687C51AF860BCFBD07EC133EC5A3F0A894A84978EDEAF88C41455ABAC9C625399666482E9B2543E8DB
Key-Arg : None
Start Time: 1383081118
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)

I'm thinking this may have to do with the certificate chain of trust being presented from the KUBI Apache configuration. The KUBI certificate is not being trusted, and as a first guess, I would assume that the '/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert High Assurance CA-3' issuer of the KUBI cert is an intermediate CA from DigiCert. If so, the Apache configuration needs to present the entire certificate chain from that intermediate CA up to the Root CA for Digicert. This is usually done with the SSLCertificateChainFile directive.

See http://www.digicert.com/ssl-certificate-installation-apache.htm

If this is not the issue, we'll need to test more, but as it is now, a simple SSL handshake cannot verify the server certificate.

History

#1 - 2013-10-29 21:35 - Chris Jones

Note that the -showcerts param in the SSL command is only showing a single certificate. If Apache is configured properly, I'd expect multiple certificates to be returned, one for each intermediate CA up to the root CA for Digicert.

#2 - 2013-11-13 18:36 - Bruce Wilson

- Target version changed from 315 to Deploy by end of Y5Q2

#3 - 2014-01-13 16:39 - Roger Dahl

- Status changed from New to Closed

- translation missing: en.field_remaining_hours set to 0.0

#4 - 2014-02-03 16:04 - Laura Moyers

- Target version changed from Deploy by end of Y5Q2 to Deploy by end of Y5Q3

#5 - 2014-02-20 21:21 - Laura Moyers

- Target version changed from Deploy by end of Y5Q3 to Operational