Self IR HA SSL Certificate issue troubleshooting

Last updated by | Veena Pachauri | Mar 8, 2023 at 11:10 PM PST

Self-IR HA SSL Certificate issue troubleshooting

Monday, March 23, 2020
9:46 AM

SME	Bohan Zhan; Brian Wang

Symptoms

Self-IR work node has reported the error below:

Failed to pull shared states from primary node net.tcp://b2bdp-pprd-ir02.cloud.corp.telstra.com:8060/ExternalService.svc/.
Activity ID: 1cba7381-8eda-498f-afe9-8590d870505b
The X.509 certificate CN=b2bdp-pprd-ir02.cloud.corp.telstra.com, OU=Customer Product and Data, O=Telstra Corporation Limited, L=Melbourne, S=VIC, C=AU chain building failed. **The certificate that was used has a trust chain that cannot be verified. Replace the certificate or change the certificateValidationMode. The revocation function was unable to check revocation because the revocation server was offline.**

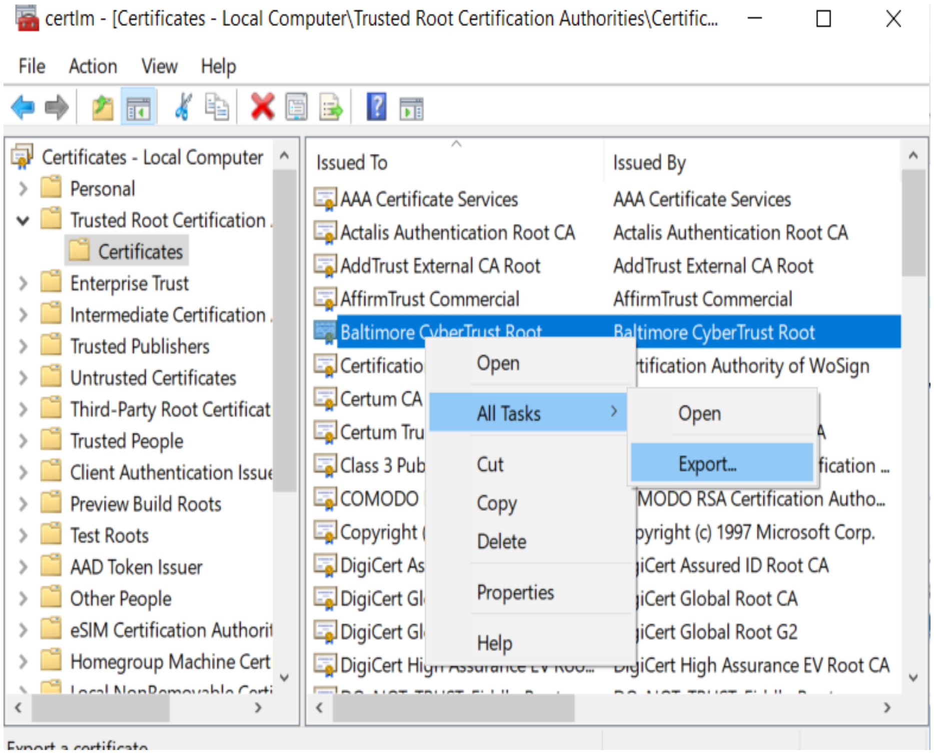
The X.509 certificate CN=b2bdp-pprd-ir02.cloud.corp.telstra.com, OU=Customer Product and Data, O=Telstra Corporation Limited, L=Melbourne, S=VIC, C=AU chain building failed. The certificate that was used has a trust chain that cannot be verified. Replace the certificate or change the certificateValidationMode. The revocation function was unable to check revocation because the revocation server was offline.

Cause

When we handle cases related to SSL/TLS handshake, we might encounter some issues related to certificate chain verification.
Here I provided a quick and intuitive way to troubleshoot X.509 certificate chain build failure .

Export certificate which need to be verified.

1.Go to manage computer certificate and find the cert which you want to check and right click All task -> Export


certlm - [Certificates - Local Computer\Trusted Root Certification Authorities\Certific...
File
Action
View
Help
Certificates - Local Computer
Personal
Trusted Root Certification
Certificates
Enterprise Trust
Intermediate Certification
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificat
Trusted People
Client Authentication Issue
Preview Build Roots
Test Roots
AAD Token Issuer
Other People
eSIM Certification Authorit
Homegroup Machine Cert
Issued To
Issued By
AAA Certificate Services
AAA Certificate Services
Actalis Authentication Root CA
Actalis Authentication Root CA
AddTrust External CA Root
AddTrust External CA Root
AffirmTrust Commercial
AffirmTrust Commercial
Baltimore CyberTrust Root
Baltimore CyberTrust Root
Certificatio
rtification Authority of WoSign
Certum CA
Certum Tru
Class 3 Pub
fication ...
COMODO
MODO RSA Certification Autho...
Copyright (
pyright (c) 1997 Microsoft Corp.
DigiCert As
iCert Assured ID Root CA
DigiCert Gl
iCert Global Root CA
DigiCert Gl
iCert Global Root G2
DigiCert High Assurance EV Roo...
DigiCert High Assurance EV Root CA
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Export...
Export a certificate

2. Copy the exported certificate to the client machine.
3. Run below command in CMD in client side, please replace the highlight part with the path to the cert and path to the output log file

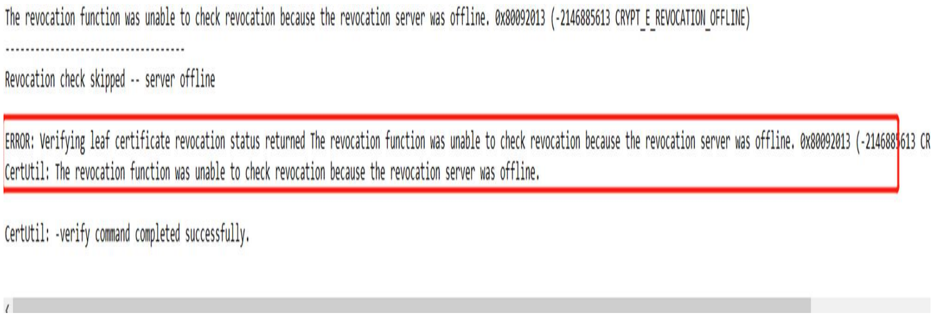
```
Certutil -verify -urlfetch   <certificate path>  >   <output txt file path>
```

Sample:

```
Certutil -verify -urlfetch c:\users\bohzhan\desktop\servercert02.cer > c:\users\bohzhan\desktop\Certinfo.txt
```

4. Check if there is any error in the output txt file.
   The error summary will be in the end of the txt file.

   For example:

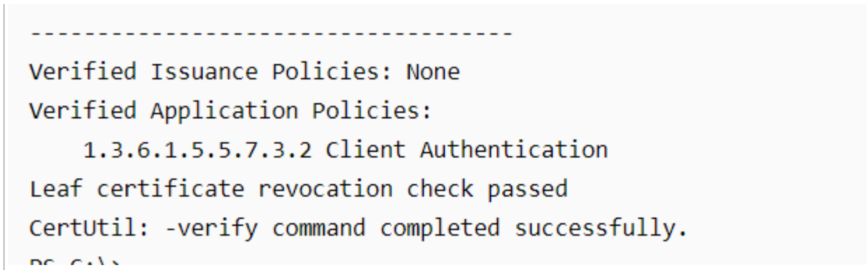


```
The revocation function was unable to check revocation because the revocation server was offline. 0x80092013 (-2146885613 CRYPT_E_REVOCATION_OFFLINE)
------------------------------------
Revocation check skipped -- server offline

ERROR: Verifying leaf certificate revocation status returned The revocation function was unable to check revocation because the revocation server was offline. 0x80092013 (-2146885613 CR
CertUtil: The revocation function was unable to check revocation because the revocation server was offline.

CertUtil: -verify command completed successfully.
```

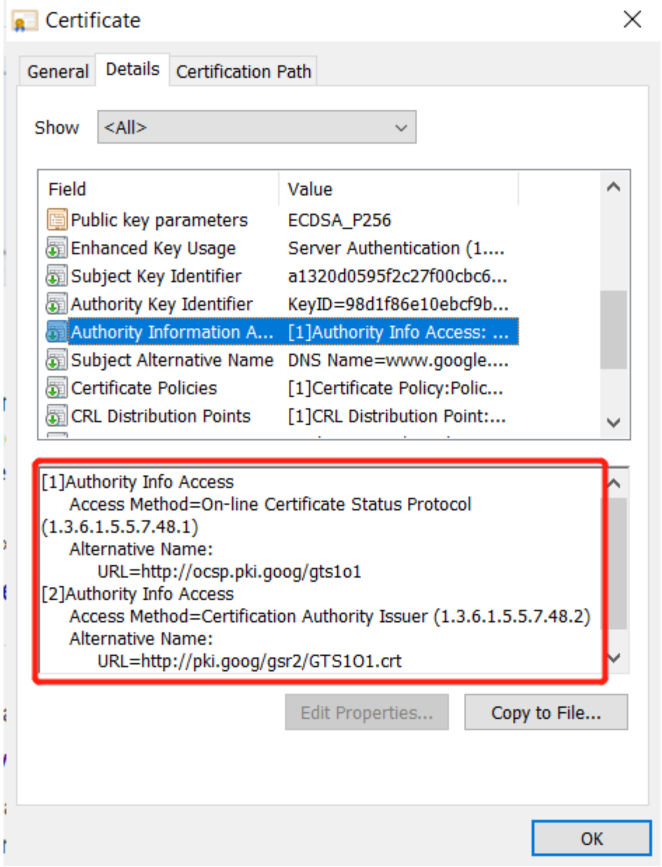
If you do not see any error and the end of the log file show as below, you can consider the certificate chain able to build up successfully in the client machine:



```
------------------------------------
Verified Issuance Policies: None
Verified Application Policies:
    1.3.6.1.5.5.7.3.2 Client Authentication
Leaf certificate revocation check passed
CertUtil: -verify command completed successfully.
PS C:\>
```

Resolution

If there are AIA,CDP and OCSP configured in the certificate file. We can check it in a more intuitive way.
You can get these info by checking the details of a certificate.



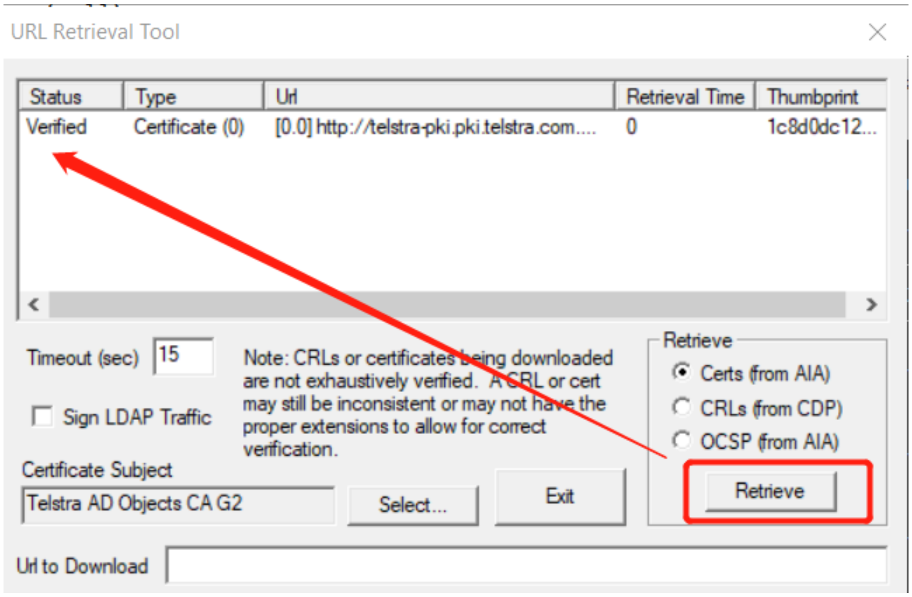
Show <All>

Field	Value
Public key parameters	ECDSA_P256
Enhanced Key Usage	Server Authentication (1....
Subject Key Identifier	a1320d0595f2c27f00cbc6...
Authority Key Identifier	KeyID=98d1f86e10ebcf9b...
Authority Information A...	[1]Authority Info Access: ...
Subject Alternative Name	DNS Name=www.google....
Certificate Policies	[1]Certificate Policy:Polic...
CRL Distribution Points	[1]CRL Distribution Point:...

```
[1]Authority Info Access
     Access Method=On-line Certificate Status Protocol
(1.3.6.1.5.5.7.48.1)
     Alternative Name:
          URL=http://ocsp.pki.goog/gts1o1
[2]Authority Info Access
     Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
     Alternative Name:
          URL=http://pki.goog/gsr2/GTS1O1.crt
```

Run below command:
Certutil -URL <certificate path>

Then the "URL Retriveal tool" will be opened.
You can verify the Certs from AIA,CDP and OCSP one by one by clicking the "Retrieve" button



Status	Type	Url	Retrieval Time	Thumbprint
Verified	Certificate (0)	[0.0] http://telstra-pki.pki.telstra.com....	0	1c8d0dc12...

Timeout (sec) 15

Note: CRLs or certificates being downloaded are not exhaustively verified. A CRL or cert may still be inconsistent or may not have the proper extensions to allow for correct verification.

☐ Sign LDAP Traffic

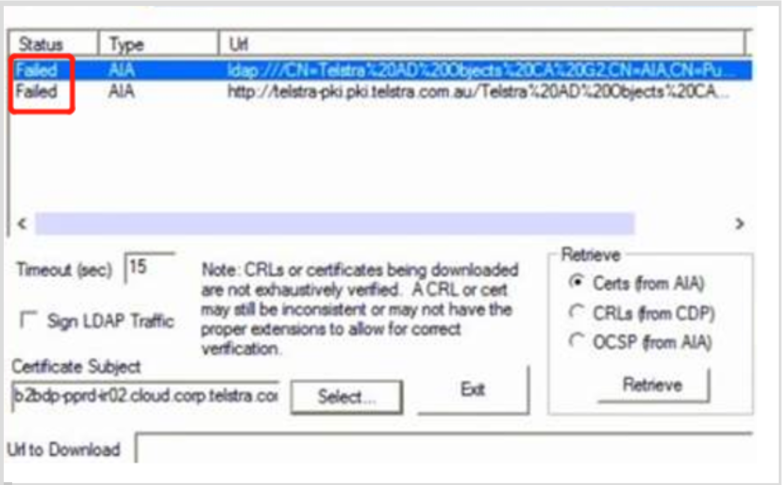
Certificate Subject: Telstra AD Objects CA G2

Retrieve
● Certs (from AIA)
○ CRLs (from CDP)
○ OCSP (from AIA)

Url to Download

The certificate chain can be built up successfully if Certs from AIA is "Verified" and either CDP or OCSP is "Verified"

If you see failure like below when retrieving AIA, CDP



Status	Type	Url
Failed	AIA	ldap:///CN=Telstra%20AD%20Objects%20CA%20G2,CN=AIA,CN=Pu...
Failed	AIA	http://telstra-pki.pki.telstra.com.au/Telstra%20AD%20Objects%20CA...

Timeout (sec) 15

☐ Sign LDAP Traffic

Note: CRLs or certificates being downloaded are not exhaustively verified. A CRL or cert may still be inconsistent or may not have the proper extensions to allow for correct verification.

Retrieve
● Certs (from AIA)
○ CRLs (from CDP)
○ OCSP (from AIA)

Certificate Subject: b2bdp-pprd-ir02.cloud.corp.telstra.co

Url to Download:

Please further capture Netmon trace and work with network team to let the client machine able connect to target URL (Please note, one of the http path and ldap path able to be verified will be enough)

More Information	https://portal.microsofticm.com/imp/v3/incidents/details/178562266/home
Tags	Provide some tags that may help search

Created with Microsoft OneNote 2016.

How good have you found this content?