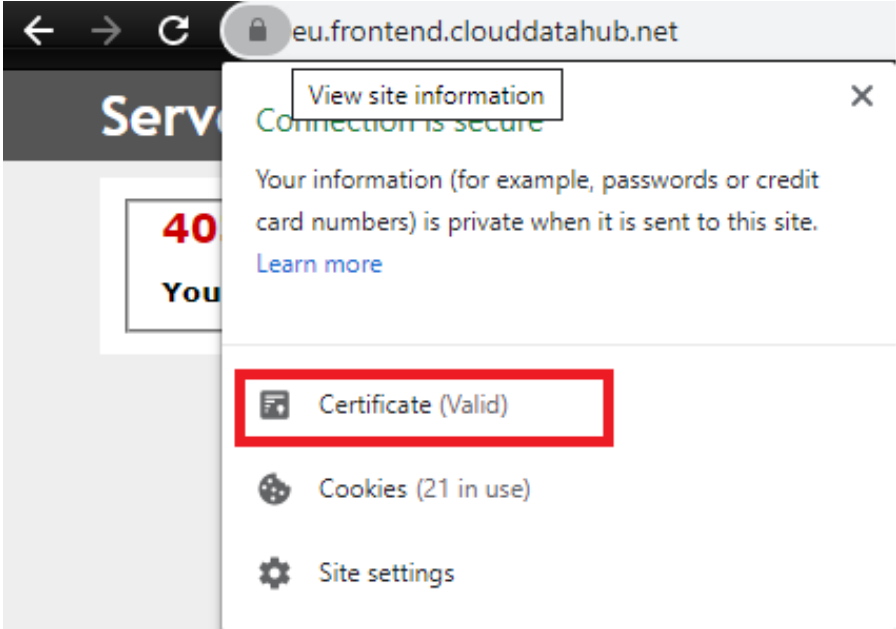


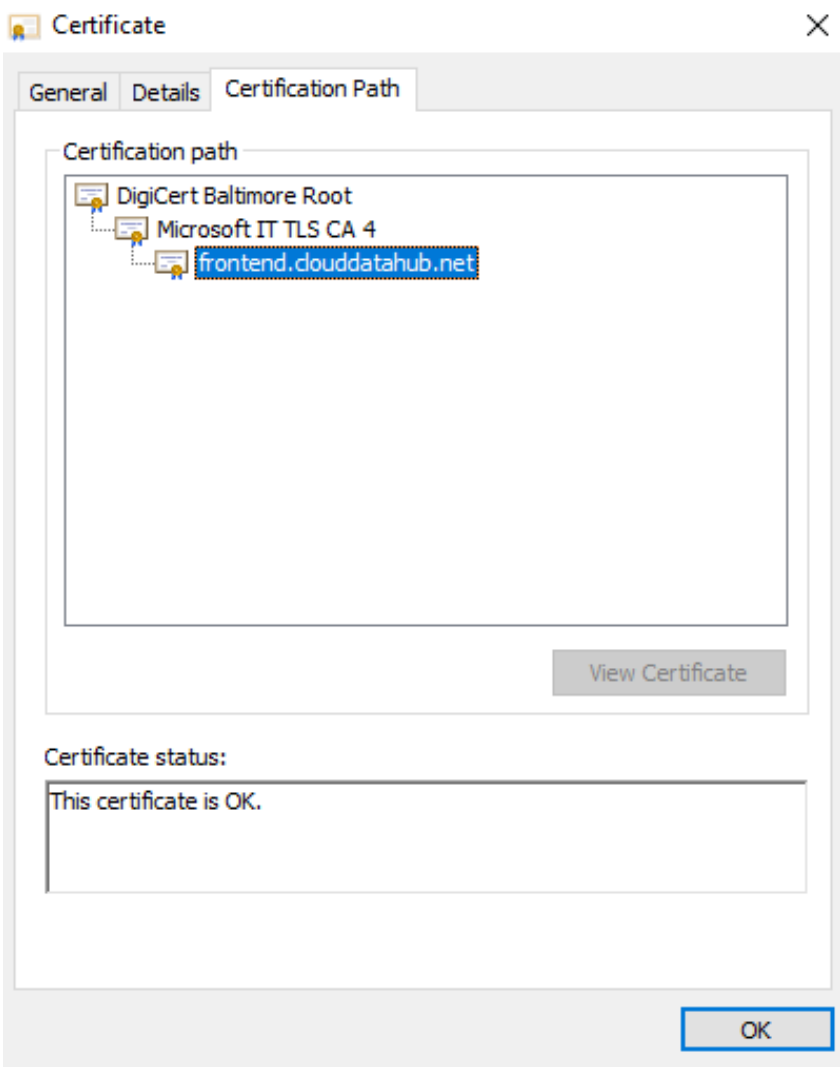
Could not establish trust relationship for the SSLTLS secure channel

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

Could not establish trust relationship for the SSL/TLS secure channel. The remote certificate is invalid according to the validation procedure

Sunday, December 22, 2019
4:17 PM

SME	
Symptoms	<div><p>The self-hosted IR couldn't connect to ADF service.</p><p>By checking SHIR event log, or client notification logs in CustomLogEvent table, the following error message will be found:</p><p>The underlying connection was closed: Could not establish trust relationship for the SSL/TLS secure channel.</p><p>The remote certificate is invalid according to the validation procedure.</p><p>How to check the server certificate of ADF service</p><p>1. The simplest way is to open ADF service URL in browser, e.g., open https://eu.frontend.clouddatahub.net/ on the machine where SHIR is installed, then view the server certificate information:</p><div></div><p>The right certificate path is like this:</p></div>



2. Follow the instruction [Enabling and Saving the CAPI2 Log](#)

Cause	<p>Two possible reasons for this issue:</p> <ol style="list-style-type: none">1. The Root CA of ADF service server certificate is not trusted on the machine where the SHIR is installed. Here is the Root CA of the server certificate of ADF service: [Thumbprint] D4DE20D05E66FC53FE1A50882C78DB2852CAE474 [subjectName] Baltimore CyberTrust Root [Issuer] CN Baltimore CyberTrust Root OU CyberTrust O Baltimore C IE [SerialNumber] 020000B9 [NotBefore] 2000-05-12T18:46:00Z [NotAfter] 2025-05-12T23:59:00Z2. Customer is using proxy in their environment and the server certificate of ADF service is replaced by the proxy, while the replaced server certificate is not trusted by the machine where the SHIR is installed.
Resolution	<p>The current ADF server certificate is:</p>

- Certificate

[**fileRef**] 439C70E27C743DE55A39CA83281D5F57E6ED49DF.cer
 [**subjectName**] frontend.clouddatahub.net

- Subject

CN frontend.clouddatahub.net

- SubjectKeyID

[**computed**] false

[**hash**] 1BDC8B711CAB6EC8F4608E5541904047AD116946

- SignatureAlgorithm

[**oid**] 1.2.840.113549.1.1.11

[**hashName**] SHA256

[**publicKeyName**] RSA

- PublicKeyAlgorithm

[**oid**] 1.2.840.113549.1.1.1

[**publicKeyName**] RSA

[**publicKeyLength**] 2048

- Issuer

CN Microsoft IT TLS CA 4

OU Microsoft IT

O Microsoft Corporation

L Redmond

S Washington

C US

SerialNumber 16000554D6D6CA5AD7EBF7D9250000000554D6

NotBefore 2019-06-15T08:04:02Z

NotAfter 2021-06-15T08:04:02Z

1. For case 1, make sure the ADF server certificate and its certificate chain is trusted by the machine where the SHIR is installed.
2. For case 2, either trust the replaced root CA on SHIR machine, or configure the proxy not to replace ADF server certificate.

Here is the link for how to trust a certificate on Windows:

<https://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-the-trusted-root-certificate>

More Information

