Self-IR HA Certificate Related Issues

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

WCF HA Certificate Related Issues

Friday, April 24, 2020
1:12 PM

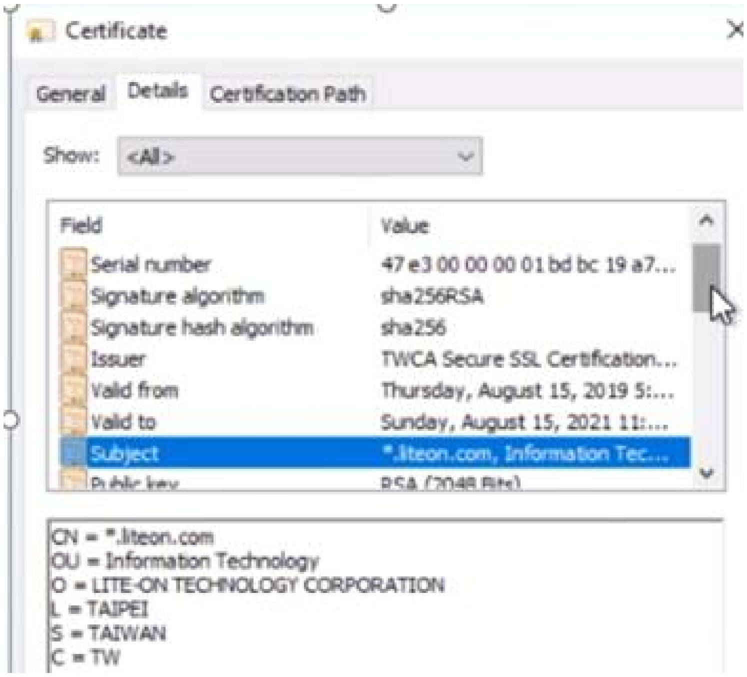
- **Issue 1:**

Customer tried to enable TLS/SSL certificate(Advanced) from SHIR Configuration Manager -> Remote access from intranet.
After selecting TLS/SSL certificate, error shows up:
Remote access settings is invalid.
Identity check failed for outgoing message. The expected DNS identity of the remote endpoint was 'ddb001.liteon.com' but the remote endpoint provided DNS claim 'liteon.com'. If this is a legitimate remote endpoint, you can fix the problem by explicitly specifying DNS identity 'liteon.com' as the Identity property of EndpointAddress when creating channel proxy.

We already have an TSG for this type of issue: "200113 - Identity check failed for outgoing message. The expected DNS identity of the remote endpoint was". I'd like to add some details here.
In this case scenario, customer is using wildcard Cert (*.liteon.com) because their organization has multiple sites.

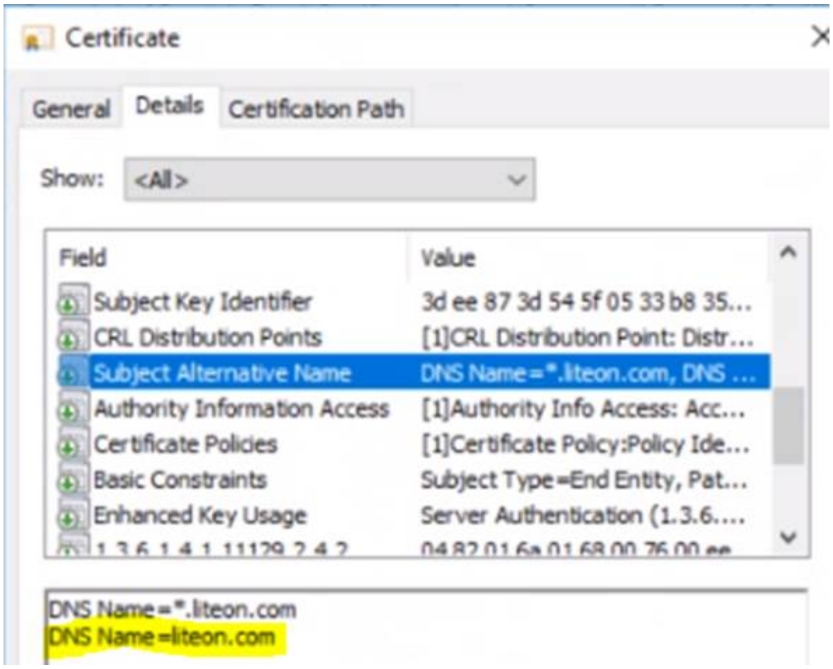
>> **Cause:** known issue in WCF: WCF TLS/SSL validate only check last DNSName in SAN.

>> **Resolution:** Wildcard Cert is supported in ADF v2 SHIR. This issue is normally due to SSL cert is not correct. The last DNSName in SAN should be valid.
How to verify: Open Management Console, double check both Subject and Subject Alternative Name from Certificate Details. In this case for example, the last item in Subject Alternative Name is not legitimate, which is DNS Name=liteon.com. Next ask customer to contact cert issue company to remove this wrong DNS Name.



Field	Value
Serial number	47 e3 00 00 00 01 bd bc 19 a7...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	TWCA Secure SSL Certification...
Valid from	Thursday, August 15, 2019 5:...
Valid to	Sunday, August 15, 2021 11:...
Subject	*.liteon.com, Information Tec...
Public key	RSA (2048 Bits)

CN = *.liteon.com
OU = Information Technology
O = LITE-ON TECHNOLOGY CORPORATION
L = TAIPEI
S = TAIWAN
C = TW



Certificate

Show: <All>

Field	Value
Subject Key Identifier	3d ee 87 3d 54 5f 05 33 b8 35...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Subject Alternative Name	DNS Name=*.liteon.com, DNS ...
Authority Information Access	[1]Authority Info Access: Acc...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Basic Constraints	Subject Type=End Entity, Pat...
Enhanced Key Usage	Server Authentication (1.3.6....
1.3.6.1.4.1.11129.2.4.2	04 82 01 6a 01 68 00 76 00 ee

DNS Name=*.liteon.com
DNS Name=liteon.com

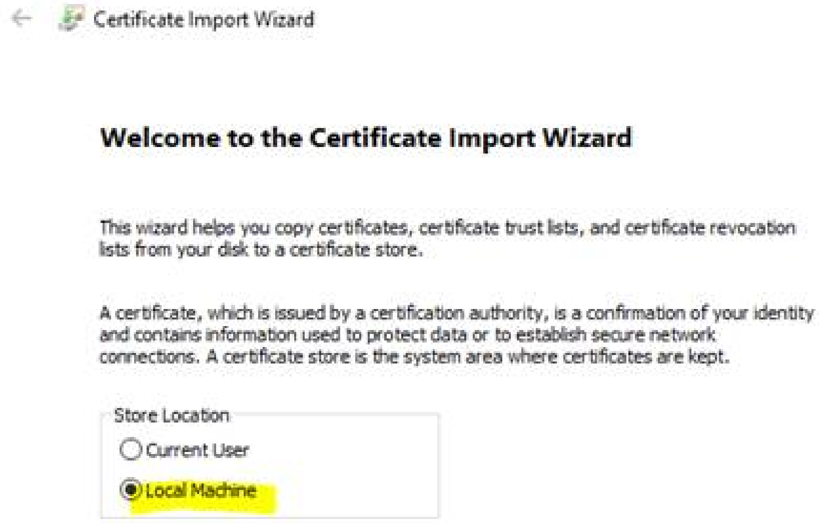
- **Issue 2:**

When selecting default Data Management Gateway SSL certificate in SHIR Remote access from intranet, got the following error:

Remote access settings is invalid.
The X.509 certificate CN=DDB001.liteon.com chain building failed. The certificate that was used has a trust chain that cannot be verified. Replace the certificate or change the certificateValidationMode. A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.

>> **Cause:** As the error message suggests, this CA root certificate is not in the Trusted Root Certification Authorities store.

>> **Resolution:** Install the cert in Local Machine -> Trusted Root Certification Authorities store.
Step 1: Click on this certificate and Install it.
Step 2: Select “Local Machine”, and “Place all certificates in the Trusted Root Certification Authorities”. If you cannot find “Local Machine” perform Step 3. Otherwise, go to Step 4.



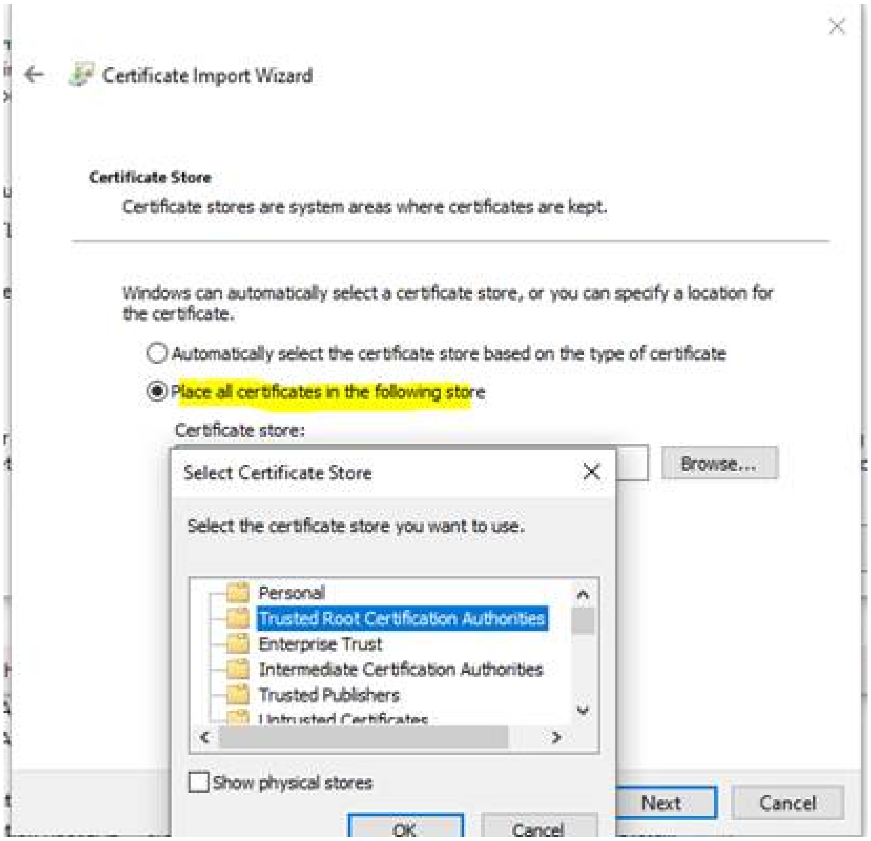
Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Select Certificate Store

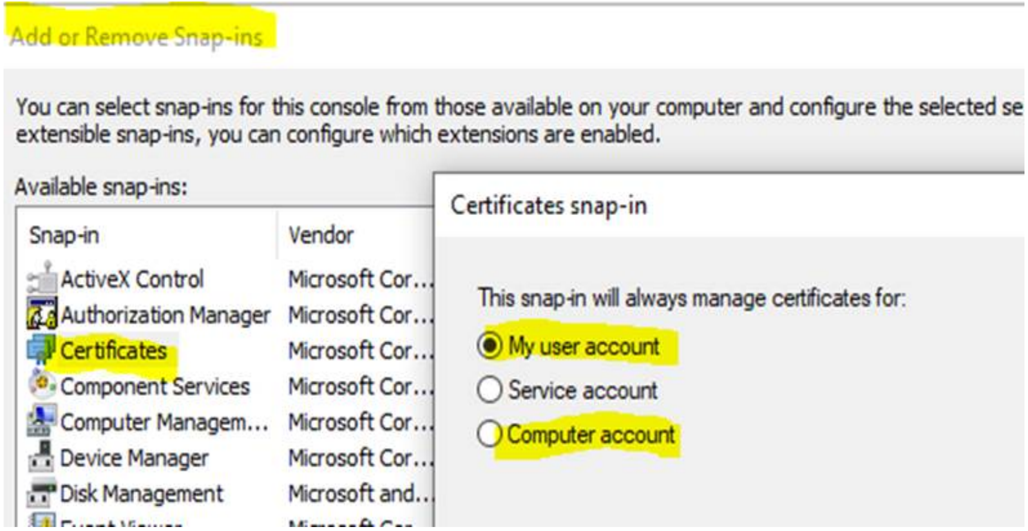
Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

☐ Show physical stores

Step 3: a. Instead, install the certificate in “Current User”.

b. Run “mmc” to open Management Console, add “My user account” and “Computer account”-> Local computer Snap-ins. Then copy the certificate from “Current User” to “Local Computer” -> Trusted Root Certification Authorities.


Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected se extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...

Certificates snap-in

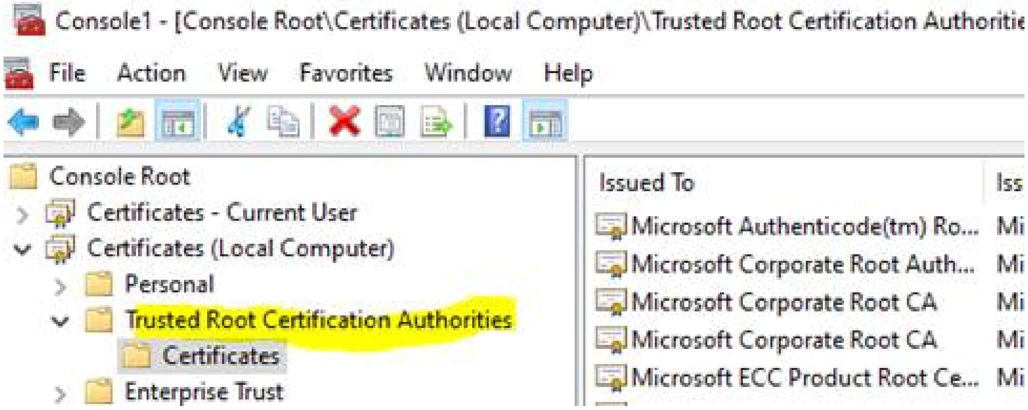
This snap-in will always manage certificates for:

● My user account

○ Service account

○ Computer account

Step 4: Verify the certificate exists in the target store.

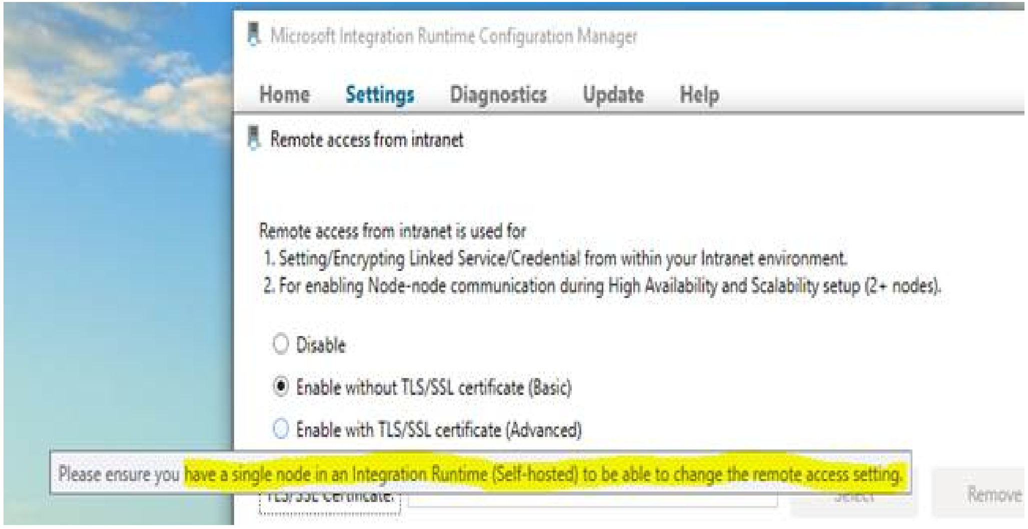

Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authoritie
File
Action
View
Favorites
Window
Help

Console Root
Certificates - Current User
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust

Issued To	Iss
Microsoft Authenticode(tm) Ro...	Mi
Microsoft Corporate Root Auth...	Mi
Microsoft Corporate Root CA	Mi
Microsoft Corporate Root CA	Mi
Microsoft ECC Product Root Ce...	Mi

- **Issue 3:**

SHIR HA mode: after VM nodes' SHIR installations are finished, unable to change Remote access from intranet option to enable TLS/SSL certificate(Advanced) .



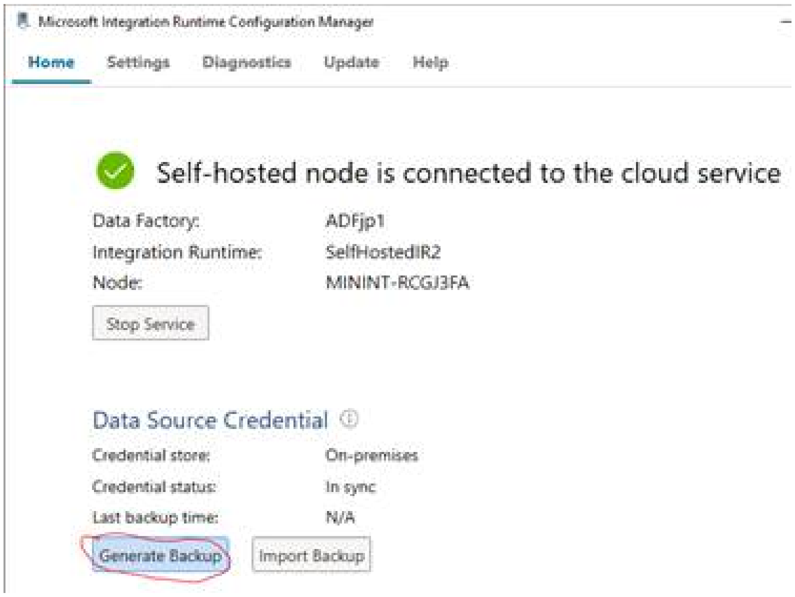
Remote access from intranet

Remote access from intranet is used for
1. Setting/Encrypting Linked Service/Credential from within your Intranet environment.
2. For enabling Node-node communication during High Availability and Scalability setup (2+ nodes).

○ Disable
● Enable without TLS/SSL certificate (Basic)
○ Enable with TLS/SSL certificate (Advanced)

Please ensure you have a single node in an Integration Runtime (Self-hosted) to be able to change the remote access setting.

>> **Cause:** This is by design. Ensure you have a single node in an SHIR to be able to change the remote access settings.
>> **Resolution:** Re-installation and re-register SHIR nodes is needed.
Step 1. Remove other nodes from ADF Portal -> SHIR settings and leave only one node.
Step 2. Uninstall SHIR from these VM nodes. Noted: Generate Data Source Credential Backup before uninstallation. Select "Yes" to delete all user data.

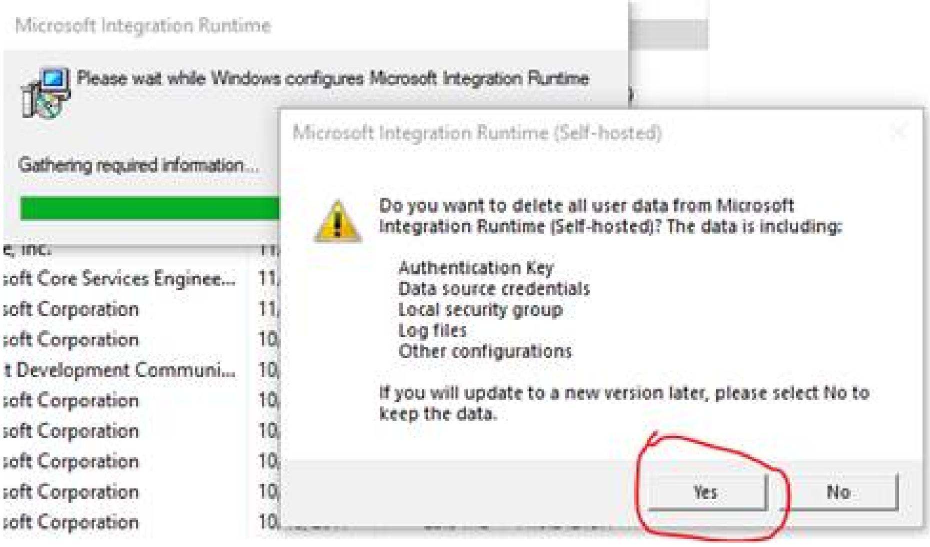


Self-hosted node is connected to the cloud service

Data Factory:	ADFjp1
Integration Runtime:	SelfHostedIR2
Node:	MININT-RCGJ3FA

Data Source Credential

Credential store:	On-premises
Credential status:	In sync
Last backup time:	N/A



Microsoft Integration Runtime

Please wait while Windows configures Microsoft Integration Runtime

Gathering required information...

Microsoft Integration Runtime (Self-hosted)

Do you want to delete all user data from Microsoft Integration Runtime (Self-hosted)? The data is including:

Authentication Key
Data source credentials
Local security group
Log files
Other configurations

If you will update to a new version later, please select No to keep the data.

Step 3. Go the remaining node, restart SHIR service. Now it should be able to set Remote access from intranet -> enable TLS/SSL certificate(Advanced).
Step 4. Install and register SHIR in other VM nodes, and configure Remote access from intranet during this installation.
Step 5. After these settings are completed, customer will be able to update their certificate from SHIR Configuration Manager.

Created with Microsoft OneNote 2016.

How good have you found this content?