ADLS | TLS Communication AdlsGen2TimeoutError

Last updated by | Veena Pachauri | Mar 8, 2023 at 11:59 PM PST

Contents

Issue

Customer got error saying:

"Message": "ErrorCode=AdlsGen2TimeoutError,'Type=Microsoft.DataTransfer.Common.Shared.HybridDeliveryException,Message=Request to ADLS Gen2 account 'XXXXXX' met timeout error. It is mostly caused by the poor network between the Self-hosted IR machine and the ADLS Gen2 account. Check the network to resolve such error.,Source=Microsoft.DataTransfer.ClientLibrary

The topology of the network is as below:

ADF client(Self-hosted IR machine)--(Intranet)----->customer's proxy server-----(WAN/Internet)-->ADLS Gen2 server

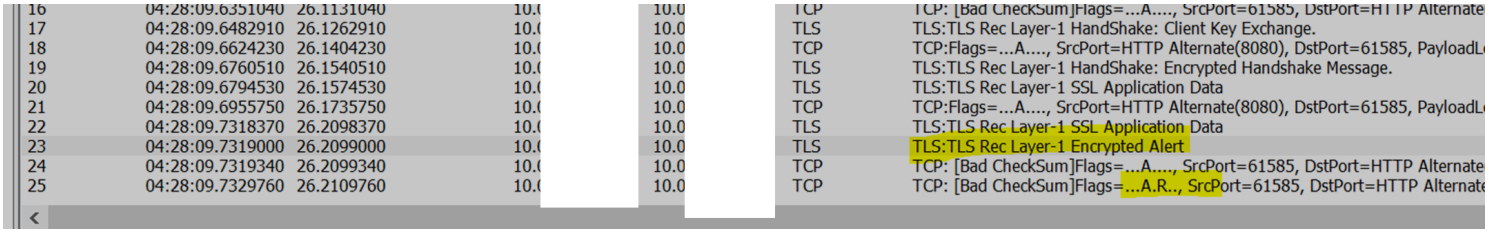
Suggestion

Please take the netmon trace from the Self-hosted IR machine

Analysis

By looking to the trace in more detail,before the client reset, we can see - TLS: TLS Rec Layer-1 Encrypted Alert, we need to figure out why it is happening at the first stage by decrypting the data, why the proxy server sent client Encrypted Alert, so you need the CSS expert for network SSL side to help you further.

https://stackoverflow.com/questions/15416624/unclear-tls-rec-layer-1-encrypted-alert



16	04:28:09.6351040	26.1131040	10.(	10.0	TCP	TCP: [Bad CheckSum]Flags=...A...., SrcPort=61585, DstPort=HTTP Alternate
17	04:28:09.6482910	26.1262910	10.(	10.0	TLS	TLS:TLS Rec Layer-1 HandShake: Client Key Exchange.
18	04:28:09.6624230	26.1404230	10.(	10.0	TCP	TCP:Flags=...A...., SrcPort=HTTP Alternate(8080), DstPort=61585, PayloadL
19	04:28:09.6760510	26.1540510	10.(	10.0	TLS	TLS:TLS Rec Layer-1 HandShake: Encrypted Handshake Message.
20	04:28:09.6794530	26.1574530	10.(	10.0	TLS	TLS:TLS Rec Layer-1 SSL Application Data
21	04:28:09.6955750	26.1735750	10.(	10.0	TCP	TCP:Flags=...A...., SrcPort=HTTP Alternate(8080), DstPort=61585, PayloadL
22	04:28:09.7318370	26.2098370	10.(	10.0	TLS	TLS:TLS Rec Layer-1 SSL Application Data
23	04:28:09.7319000	26.2099000	10.(	10.0	TLS	TLS:TLS Rec Layer-1 Encrypted Alert
24	04:28:09.7319340	26.2099340	10.(	10.0	TCP	TCP: [Bad CheckSum]Flags=...A...., SrcPort=61585, DstPort=HTTP Alternate
25	04:28:09.7329760	26.2109760	10.(	10.0	TCP	TCP: [Bad CheckSum]Flags=...A.R.., SrcPort=61585, DstPort=HTTP Alternate

Solution

Changed another proxy server and resolved the issue.

Addtional information

As it might be IR upgrading with .net which changed the TLS behavior, so the proxy server could not handle it well enough. You can try following for troubleshooting purpose as well.

```
SchUseStrongCrypto
The HKEY_LOCAL_MACHINE\SOFTWARE\[Wow6432Node\]Microsoft\.NETFramework\<VERSION>: SchUseStrongCrypto registry key has a value of type DWORD. A value of 1 cause
If your app targets .NET Framework 4.6 or later versions, this key defaults to a value of 1. That's a secure default that we recommend. If your app targets .N
This key should only have a value of 0 if you need to connect to legacy services that don't support strong cryptography and can't be upgraded.
```

Reference

ICM: 221609396

How good have you found this content?