FE Connection Issue due to certificate

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

Contents

Issue

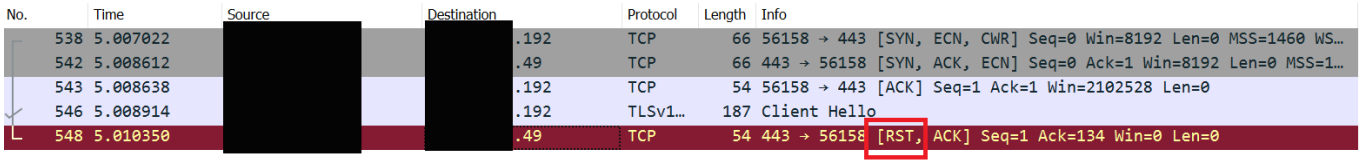
Sometimes, the self-IR could not make connection to FE server and error below:

DEBUG: An error occurred while sending the request. The underlying connection was closed: An unexpected error occurred on a send. Unable to read data from the transport connection: An existing connection was forcibly closed by the remote host. An existing connection was forcibly closed by the remote host Activity ID: 72b258b5-0b06-4e07-b79f-252e4dc04de0 An error occurred while sending the request. The underlying connection was closed: An unexpected error occurred on a send. Unable to read data from the transport connection: An existing connection was forcibly closed by the remote host. An existing connection was forcibly closed by the remote host

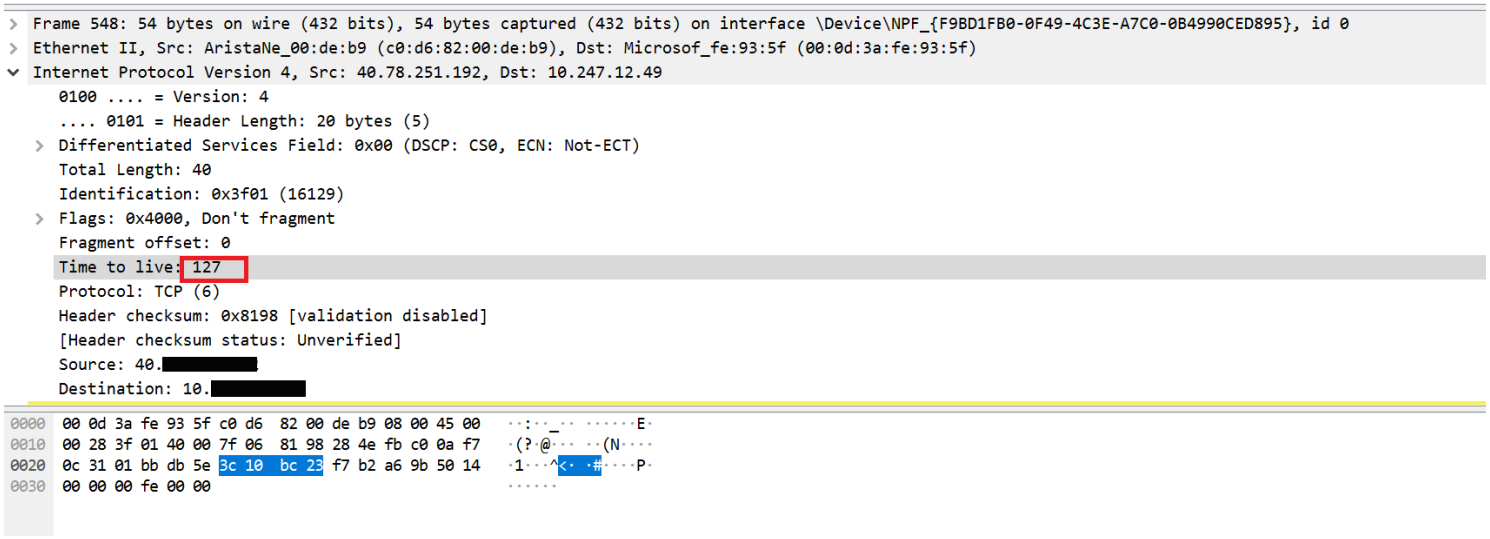
Suggestion

Please take netmon trace to analyze further and refer to the TSG
https://supportability.visualstudio.com/AzureDataFactory/_wiki/wikis/AzureDataFactory/303927/ADLS-TLS-Comunication-Certificate

You suppose can see four handshakes there from netmon trace.



No.	Time	Source	Destination	Protocol	Length	Info
538	5.007022	[redacted]	.192	TCP	66	56158 → 443 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS…
542	5.008612		.49	TCP	66	443 → 56158 [SYN, ACK, ECN] Seq=0 Ack=1 Win=8192 Len=0 MSS=1…
543	5.008638		.192	TCP	54	56158 → 443 [ACK] Seq=1 Ack=1 Win=2102528 Len=0
546	5.008914		.192	TLSv1…	187	Client Hello
548	5.010350		.49	TCP	54	443 → 56158 [RST, ACK] Seq=1 Ack=134 Win=0 Len=0

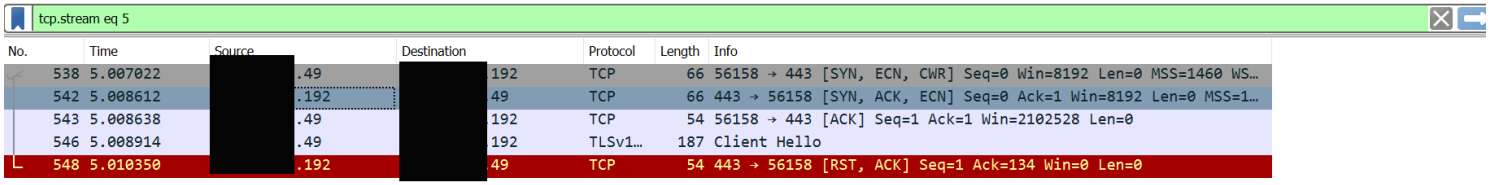


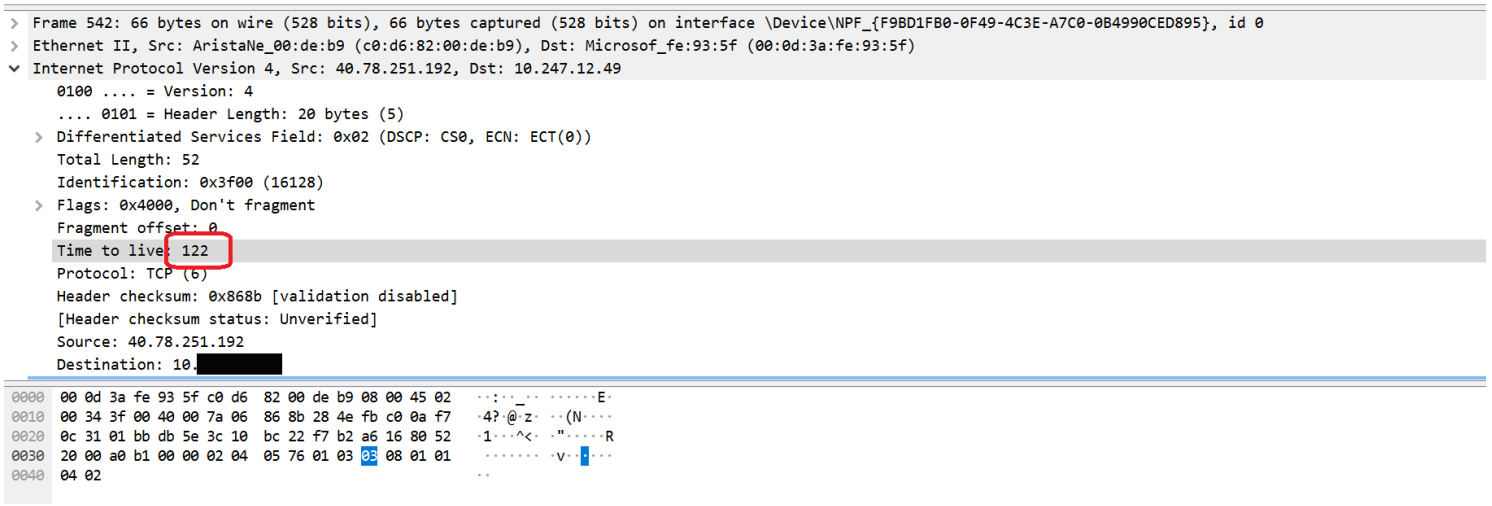
```
> Frame 548: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{F9BD1FB0-0F49-4C3E-A7C0-0B4990CED895}, id 0
> Ethernet II, Src: AristaNe_00:de:b9 (c0:d6:82:00:de:b9), Dst: Microsof_fe:93:5f (00:0d:3a:fe:93:5f)
v Internet Protocol Version 4, Src: 40.78.251.192, Dst: 10.247.12.49
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x3f01 (16129)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 127
    Protocol: TCP (6)
    Header checksum: 0x8198 [validation disabled]
    [Header checksum status: Unverified]
    Source: 40.[redacted]
    Destination: 10.[redacted]
```

```
0000  00 0d 3a fe 93 5f c0 d6  82 00 de b9 08 00 45 00   ··:··_·· ······E·
0010  00 28 3f 01 40 00 7f 06  81 98 28 4e fb c0 0a f7   ·(?·@··· ··(N····
0020  0c 31 01 bb db 5e bc 10  bc 23 f7 b2 a6 9b 50 14   ·1···^·· ·#····P·
0030  00 00 00 fe 00 00                                  ·····
```

However, after first handshake, it is reset by the destination, based on the TTL value, we can see 127 which means the second hop reset the package from client when certificate handshakes.

Normal handshake TTL is 122 which is the normal hops between self-IR and FE.

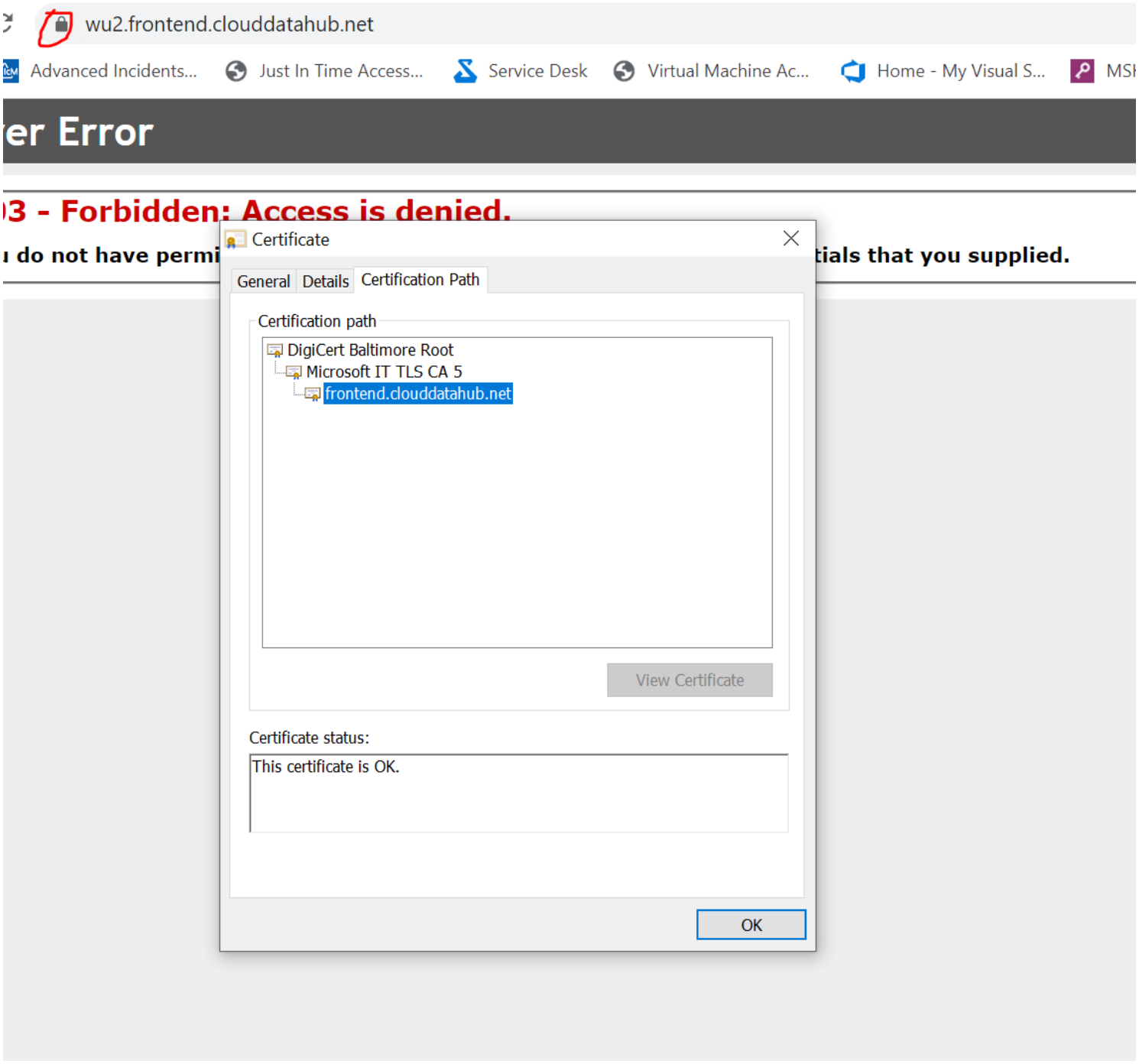




Action Plan

Please make sure your proxy trust the certificate from FE.

You can access https://wu2.frontend.clouddatahub.net to get the certificate:



SimilarICM:

https://portal.microsofticm.com/imp/v3/incidents/details/193600211/home

How good have you found this content?