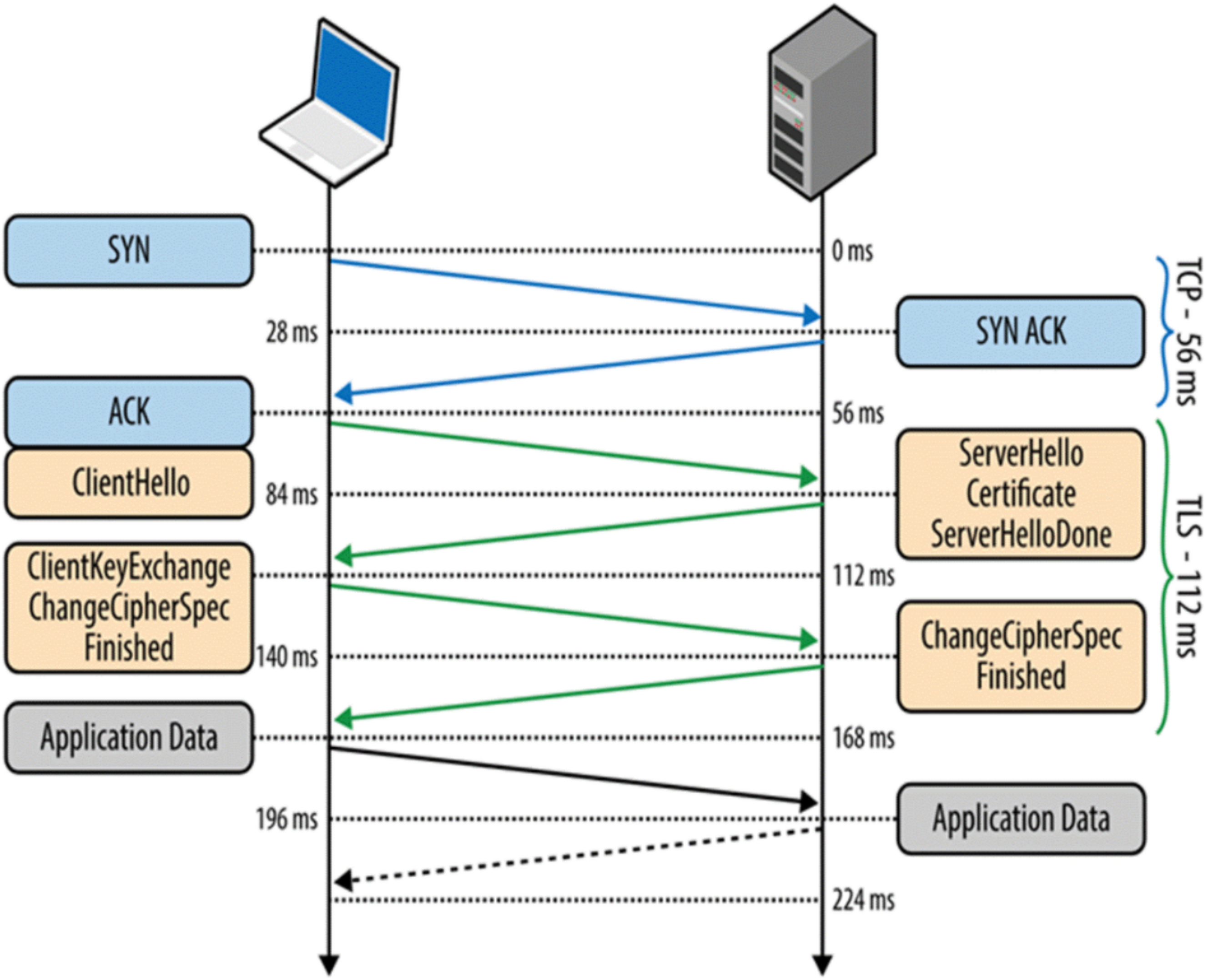
[Certificate]Troubleshooting Tips

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

Contents

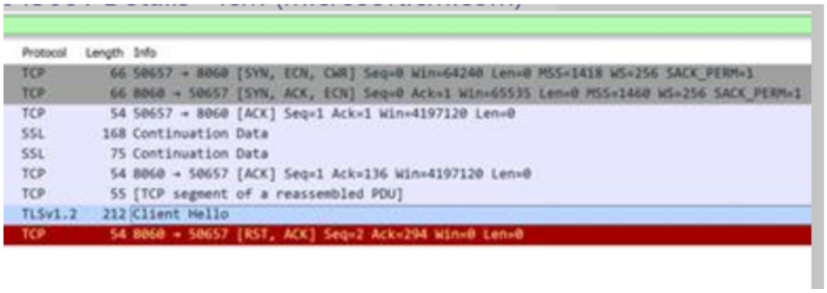
Certificate handshake

Please refer to the following pic on how certificate handshake will be.



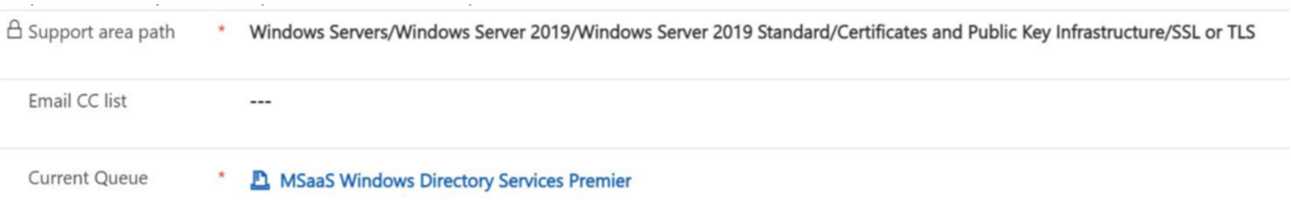
Troubleshooting Suggestion

If you handle any ticket with the following reset during certificate handshake, please involve certificate expert to help you.



```
Protocol  Length Info
TCP           66 50657 → 8060 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1418 WS=256 SACK_PERM=1
TCP           66 8060 → 50657 [SYN, ACK, ECN] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP           54 50657 → 8060 [ACK] Seq=1 Ack=1 Win=4197120 Len=0
SSL          168 Continuation Data
SSL           75 Continuation Data
TCP           54 8060 → 50657 [ACK] Seq=1 Ack=136 Win=4197120 Len=0
TCP           55 [TCP segment of a reassembled PDU]
TLSv1.2      212 Client Hello
TCP           54 8060 → 50657 [RST, ACK] Seq=2 Ack=294 Win=0 Len=0
```

How to engage the Directory team



Support area path	*	Windows Servers/Windows Server 2019/Windows Server 2019 Standard/Certificates and Public Key Infrastructure/SSL or TLS
Email CC list		---
Current Queue	*	MSaaS Windows Directory Services Premier

Note: You need to get trace to confirm the certificate handshake. However, please confirm with the DS team before reaching customer for it.

To collect trace, you can follow these steps:

1. Download https://dsisupportdebugtools.blob.core.windows.net/iis-etw/start.bat onto the impacted ADF Dispatcher server. Save it in a newly created folder, eg: C:\temp
2. Launch the downloaded .bat file as administrator
3. Reproduce the issue, record the time when the issue happened
4. Stop .bat by pressing enter in the console Collect all the .etl files in C:\temp and upload onto Workspace for the further analysis

How good have you found this content?