AAD - Netmon Trace for Advanced Troubleshoot

Last updated by | Vitor Tomaz | Feb 18, 2021 at 2:30 AM PST

Contents

AAD - Netmon Trace for Advanced Troubleshoot

Issue :

On scenarios where TSG failed or do not help resolve the problem, please request customer to try logging in via Universal authentication and grab a Fiddler trace for further analysis.

Steps :

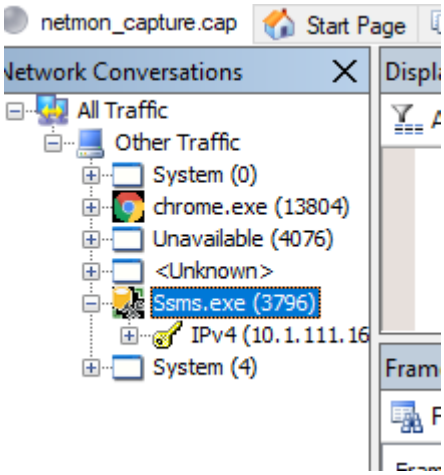
Grab NetMon Trace:

Download and install NetMon from here https://www.microsoft.com/en-us/download/details.aspx?id=4865

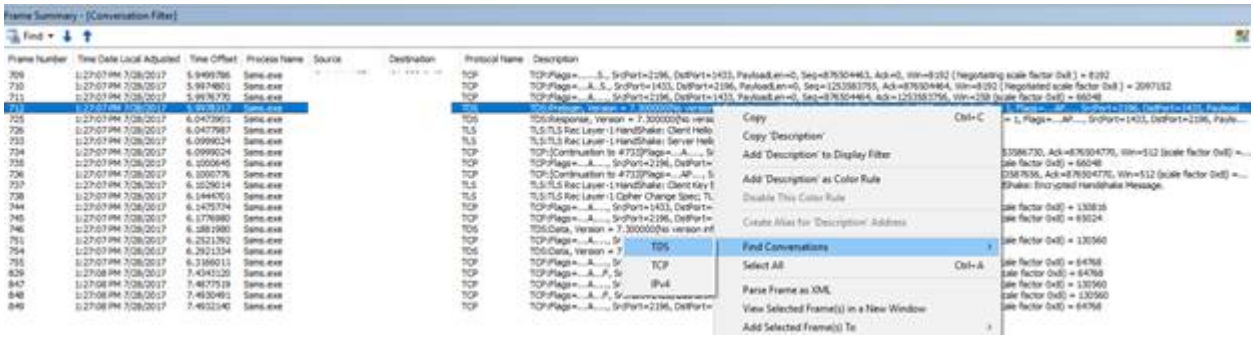
a. New Capture -> Start
b. Launch SSMS
c. Try to login with AAD
d. Stop Capture
e. Save the trace

Debug using NetMon Trace

1. Open the trace in Netmon
2. Select the process from left pane “Network conversations” which was trying to connect to SQL Server. (in our example SSMS)



3. In the frame summary panel, look for TDS under “Protocol Name” Column, Right click -> Find Conversations->TDS This will filter all the frames for TDS protocol and now you can view all changes



4. Validate the filtered Packets 1 by one (for each message sent from client, there should be a response from server. You can determine whether the client or server has the issue by looking at the party which stopped the flow of requests)
    1. TDS:Prelogin, TDS:response
    2. TLS Handshake should look something like this:

```
TLS:TLS Rec Layer-1 HandShake: Client Hello.
TLS:TLS Rec Layer-1 HandShake: Server Hello. Certificate.
TLS:TLS Rec Layer-1 HandShake: Client Key Exchange.; TLS Rec Layer-2 Cipher Change Spec; TLS Rec Layer-3 HandShake: Encrypted Handshake Message.
TLS:TLS Rec Layer-1 Cipher Change Spec; TLS Rec Layer-2 HandShake: Encrypted Handshake Message.
```

    3. Next there should be a TDS:Login exchange.
    4. In case of AAD Integrated or Password auth, there should be a client message pushing FedAuth Token to the server.

How good have you found this content?