Black Screen Due to MTU Size_RDP SSH

Last updated by | Kalyn George | Jun 21, 2022 at 9:02 AM PDT

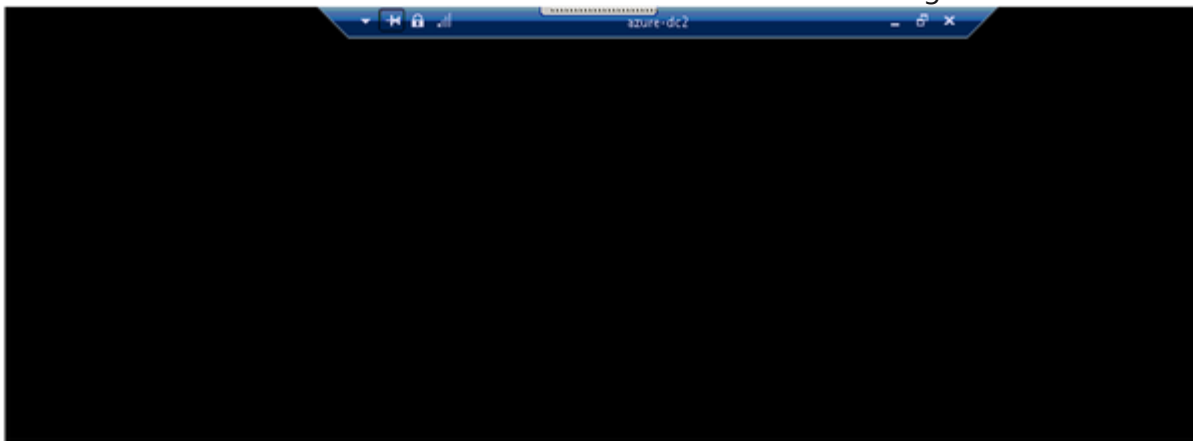## Tags

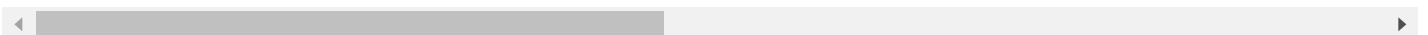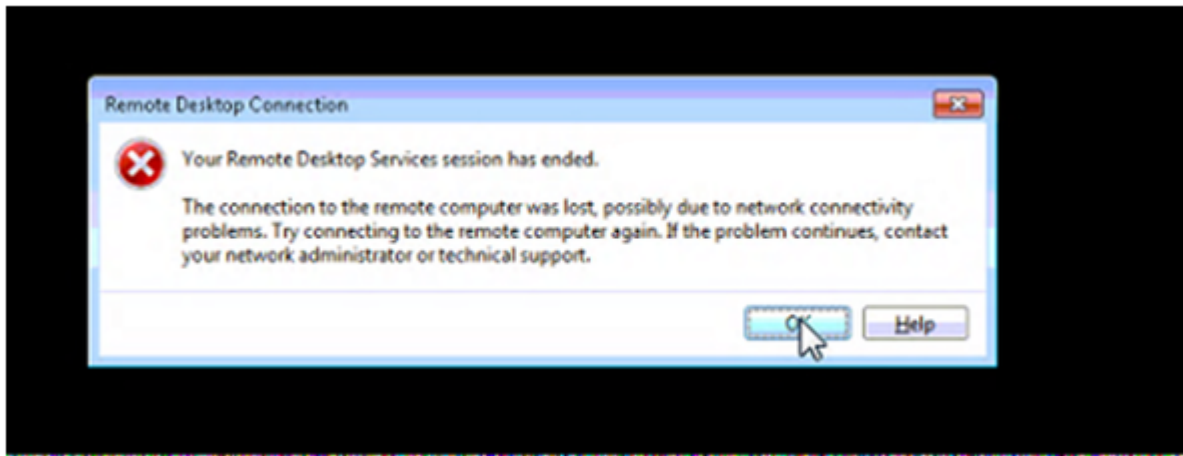|	
cw.TSG	cw.RDP-SSH

Contents

Symptoms

1. If you try to connect from an on-premises machine thru a VNET, after you authenticate you get a black screen and then after 1min the session disconnected with the following error:


```
Your Remote Desktop Service session has ended.
The connection to the remote computer was lost, possible due to network connectivity problems. Try co
```

2. No event 4005 logged on the SYSTEM logs on the target VM.

Root Cause Analysis

MTU size set up on the on premises firewall.

References

- How to check User Defined Route settings on a VM

Tracking close code for this volume

Root Cause	Product	Support Topic	Cause Tracking code	Bug
1	*Azure Virtual Networks*	*Routing Azure Virtual Network V3\Connectivity\Cannot connect to virtual machine using RDP or SSH*	*Root Cause - Windows Azure\Virtual Network\Internet Service Provider/Third Party Network*	

To know how to flag a bug on a case please refer to How to do Proper Case Coding

Customer Enablement

https://docs.microsoft.com/en-us/troubleshoot/windows-server/remote/a-black-screen-appears-while-sign ⧉

Data Collection

On Disconnections cases, you may need to collect some date. For that please refer to the follwoing HowTo's document to achieve this:

- How to collect an RDSTrace

1. Download Netmon ⧉ on both server and client in a location like *c:\temp*
2. Download the RDSTracing ⧉ utility to the client and server machines on a location like *c:\temp*
3. Start both captures and reproduce the RDP attempt a couple of times (3-4 attemps)
4. Stop the network captures and the RDSTracing traces from both ends, client and server

5. Rename the network captures as *CLIENT-netmonCapture.cap* and *SERVER-netmonCapture.cap*

6. Create a [DTM Workspace](#) ⧉ and upload all the traces
   - *c:\temp\netmon\CLIENT-netmonCapture.cap* and *c:\temp\netmon\SERVER-netmonCapture.cap*
   - RDSTracing cab file
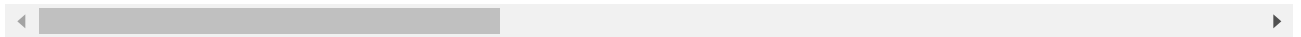   - Compress a copy of the folder *C:\Windows\System32\winevt\Logs*

Mitigation

1. Check to see if you find the following RDSTracing info on the capture:
   1. On the Client:

      - **MAN-RDCLIENT-!FMT.txt:**

        ```
        [0]3788.3298::09/27/16-11:16:27.5379220 [Microsoft-Windows-TerminalServices-RDPClient/Analyt
        The connection to the remote computer was lost, possibly due to network connectivity problem
        ```

      - **RDCLIENT-!FMT.txt:**

        ```
        [1] 3788.3A9C::09/27/16-11:16:27.5301410 [rdpencconlib] rdpencstream_cpp795 CRDPENCCONStrean
        [1] 3788.3A9C::09/27/16-11:16:27.5301470 [rdpencconlib] rdpencstream_cpp405 CRDPENCCONStrean
        [1] 3788.3A9C::09/27/16-11:16:27.5302385 [rdpencconlib] rdpencstream_cpp431 CRDPENCCONStrean
        [1] 3788.3A9C::09/27/16-11:16:27.5302554 [WinTransClntCore] rdpwinstreamtcp_cpp506 CRdpWinSt
        [1] 3788.3A9C::09/27/16-11:16:27.5302569 [RdpXTransClntCore] tstcptransport_cpp1144 CTSTcpTr
        [1] 3788.3A9C::09/27/16-11:16:27.5302675 [RdpXTransClntCore] tstcptransport_cpp1159 CTSTcpTr
        [2] 3788.2F70::09/27/16-11:16:27.5303049 [platformu] thread_cpp1976 CTSThread::internalMsgPu
        [2] 3788.2F70::09/27/16-11:16:27.5303091 [RdpXTransClntCore] tstcptransport_cpp1176 CTSTcpTr

        Error:(-1073741299, c000020d) = STATUS_CONNECTION_RESET = The transport connection has been
        ```
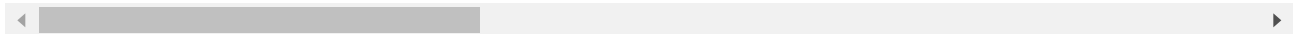
   2. On the server:

      - On the event logs:

        ```
        Log Name:      Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
        Source:        Microsoft-Windows-RemoteDesktopServices-RdpCoreTS
        Date:          9/27/2016 10:15:52 AM
        Event ID:      131
        Task Category: RemoteFX module
        Level:         Information
        Keywords:
        User:          NETWORK SERVICE
        Computer:      azure-adfs1
        Description:
        The server accepted a new TCP connection from client 192.168.219.100:41906.
        ```

```
Log Name:       Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
Source:         Microsoft-Windows-TerminalServices-RemoteConnectionManager
Date:           9/27/2016 10:15:52 AM
Event ID:       1149
Task Category: None
Level:          Information
Keywords:
User:           NETWORK SERVICE
Computer:       azure-adfs1
Description:
Remote Desktop Services: User authentication succeeded:

User: admin
Domain: constoso
Source Network Address: 192.168.219.100
```

- **MAN-RDSH-!FMT.txt:**

```
[0]0838.09A8::09/27/16-11:16:11.8179237 [Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/(
[0]0838.09A8::09/27/16-11:16:11.8180285 [Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/[
[0]0838.09A8::09/27/16-11:16:11.8180740 [Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/[
[0]024C.0DAC::09/27/16-11:16:11.8191274 [Microsoft-Windows-TerminalServices-LocalSessionMana
[0]0838.10DC::09/27/16-11:16:11.8399396 [Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/[
[0]0838.10DC::09/27/16-11:16:11.8399571 [Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/(
[0]024C.0DAC::09/27/16-11:16:11.8414905 [Microsoft-Windows-TerminalServices-LocalSessionMana
[0]024C.0908::09/27/16-11:16:11.9422906 [Microsoft-Windows-TerminalServices-LocalSessionMana
[0]0838.0AF8::09/27/16-11:16:11.9426027 [Microsoft-Windows-TerminalServices-RemoteConnection
[0]024C.0908::09/27/16-11:16:12.1356512 [Microsoft-Windows-TerminalServices-LocalSessionMana
[0]024C.1004::09/27/16-11:16:12.1362072 [Microsoft-Windows-TerminalServices-LocalSessionMana
```

- **USRLOGON-!FMT.txt:**

```
[0] 0210.0F90::09/27/16-11:16:11.8221673 [winnt5] userapi_cxx292 SpDeleteUserModeContext() -
[0] 0210.0F90::09/27/16-11:16:11.8221767 [winnt5] userapi_cxx321 SpDeleteUserModeContext() -
[0] 0210.0F90::09/27/16-11:16:11.8221812 [winnt5] ctxtapi_cxx121 SpDeleteContext() - SpDelet
[0] 0210.0F90::09/27/16-11:16:11.8222403 [winnt5] ctxtapi_cxx184 SpDeleteContext() - SpDelet
[0] 0210.0F90::09/27/16-11:16:11.8222407 [winnt5] ctxtapi_cxx186 SpDeleteContext() - SpDelet
[0] 0210.0F90::09/27/16-11:16:11.8226133 [winnt5] logonapi_cxx8844 LsaApLogonTerminated() -
[0] 0210.0F90::09/27/16-11:16:11.8226156 [winnt5] logonapi_cxx8849 LsaApLogonTerminated() -
[0] 0210.0F90::09/27/16-11:16:11.8226170 [winnt5] logonses_cxx584 KerbFreeLogonSession() - F
[0] 0210.0F90::09/27/16-11:16:11.8226234 [winnt5] kerbs4u_cxx297 KerbAgeS4U2ProxyCache() - F
[0] 0BB8.1118::09/27/16-11:16:11.8418874 [logon] accesspage_cpp1950 CAccessPage::Destroy() -
[0] 0BB8.1118::09/27/16-11:16:11.8418885 [logon] accesspage_cpp2766 CAccessPage::v_WndProc()
[0] 0C78.0864::09/27/16-11:16:11.8476270 [server] wmsgsrv_c164 IsRpcCallerLocalSystem() - Ch
[0] 0C78.0864::09/27/16-11:16:11.8476383 [core] wmsgclnt_cxx224 WMsgMessageHandler() -
[0] 0C78.0864::09/27/16-11:16:11.8476391 [statemachine] sigmgr_c291 SignalManagerSetSignal()
[0] 0C78.0DD0::09/27/16-11:16:11.8476436 [statemachine] sigmgr_c601 SignalManagerWaitForSign
[0] 0C78.0DD0::09/27/16-11:16:11.8476442 [statemachine] sigmgr_c552 SignalManagerWaitForSign
[0] 0C78.0864::09/27/16-11:16:11.8476461 [statemachine] sigmgr_c357 SignalManagerSetSignal()
[0] 0C78.0DD0::09/27/16-11:16:11.8476471 [statemachine] sigmgr_c576 SignalManagerWaitForSign
[0] 0C78.0DD0::09/27/16-11:16:11.8476477 [statemachine] stmach_c859 StateMachineRun() - Stat
[0] 0C78.0DD0::09/27/16-11:16:11.8476479 [statemachine] stmach_c905 StateMachineRun() - Stat
[0] 0C78.0DD0::09/27/16-11:16:11.8476488 [core] welcome_cxx1208 WLGeneric_DisplayLegalNotice
[0] 0C78.0864::09/27/16-11:16:11.8476504 [core] wmsgclnt_cxx314 WMsgMessageHandler() - WMsgM
[0] 0C78.0DD0::09/27/16-11:16:11.9468228 [core] wlutil_cxx2760 AbortBlockedThread() - AbortB
[0] 0BB8.131C::09/27/16-11:16:11.9468664 [logon] server_cpp40 _ServerCallback_Abort() -  <IM
[0] 0BB8.131C::09/27/16-11:16:11.9468747 [logon] server_cpp44 _ServerCallback_Abort() -  <IM
[0] 0BB8.1118::09/27/16-11:16:11.9469042 [animationhelpers] animationhelpers_h178 CAnimation
[0] 0BB8.1118::09/27/16-11:16:11.9469205 [logon] duidialog_cpp2489 CLogonFrame::OnQIDisplayS
[0] 0BB8.1118::09/27/16-11:16:11.9472512 [logon] duidialog_cpp8403 CLogonFrame::_SetOptions(
[0] 0BB8.1118::09/27/16-11:16:11.9473645 [animationhelpers] animationhelpers_cpp1460 CAutoAn
[0] 0BB8.1118::09/27/16-11:16:11.9473651 [animationhelpers] animationhelpers_cpp1470 CAutoAn
[0] 0BB8.1118::09/27/16-11:16:11.9473677 [logon] duidialog_cpp3885 CLogonFrame::_OnQICallbac
[0] 0BB8.1118::09/27/16-11:16:11.9474908 [logon] duidialog_cpp2316 CLogonFrame::_OnQIDisplay
[0] 0BB8.1118::09/27/16-11:16:11.9474915 [logon] duidialog_cpp9297 CLogonFrame::_LogonDialog
[0] 0BB8.1118::09/27/16-11:16:11.9474918 [logon] duidialog_cpp8709 CLogonFrame::_OnCancel()
[0] 0BB8.0378::09/27/16-11:16:11.9480566 [logon] server_cpp182 _ServerCallback_DisplayMessag
```

- **RDPCORE-!FMT.txt:**

```
[0] 0838.0AD0::09/27/16-11:16:11.8114306 [rdpencconlib] rdpencstream_cpp795 CRDPENCCONStream
[0] 0838.0AD0::09/27/16-11:16:11.8114337 [rdpencconlib] rdpencstream_cpp405 CRDPENCCONStream
[0] 0838.0AD0::09/27/16-11:16:11.8114516 [rdpencconlib] rdpencstream_cpp431 CRDPENCCONStream
[0] 0838.0AD0::09/27/16-11:16:11.8114638 [rdpencconlib] rdpencstream_cpp771 CRDPENCCONStream
[0] 0838.0AD0::09/27/16-11:16:11.8114658 [rdpencconlib] rdpencstream_cpp795 CRDPENCCONStream
[0] 0838.0AD0::09/27/16-11:16:11.8114677 [rdpencconlib] rdpencstream_cpp405 CRDPENCCONStream
[0] 0838.0AD0::09/27/16-11:16:11.8114719 [rdpwdumxlib] rdpwdumximpl_cpp1898 CRDPWDUMXStack:
[0] 0838.0AD0::09/27/16-11:16:11.8114743 [rdpnetdetect] networkdetector_cpp713 CRDPNetworkDe

Error:(-1073741643, c00000b5) = STATUS_IO_TIMEOUT = {Device Timeout} The specified I/O opera
```

- **RDSH-!FMT.txt:**
```

```
[0] 0838.09A8::09/27/16-11:16:11.8209874 [termsrv] termsrv_cpp1128 DoWppTrace() - [00001191
[0] 0838.09A8::09/27/16-11:16:11.8209910 [termsrv] termsrv_cpp1128 DoWppTrace() - [00001191
[0] 024C.1004::09/27/16-11:16:11.8211399 [lsm] service_cpp3003 DoWppTrace() - [00003789]:CTS
[0] 024C.1004::09/27/16-11:16:11.8211420 [lsm] service_cpp3003 DoWppTrace() - [00003789]:Ses
[0] 024C.1004::09/27/16-11:16:11.8211527 [lsm] service_cpp3003 DoWppTrace() - [00003789]:CTS
[0] 0838.09A8::09/27/16-11:16:11.8211618 [termsrv] termsrv_cpp1128 DoWppTrace() - [00001191
[0] 024C.0DAC::09/27/16-11:16:11.8223776 [lsm] service_cpp3003 DoWppTrace() - [0000378a]:CTS
[0] 0838.10DC::09/27/16-11:16:11.8224734 [termsrv] termsrv_cpp1128 DoWppTrace() - [00001192
[0] 0838.10DC::09/27/16-11:16:11.8225690 [termsrv] termsrv_cpp1132 DoWppTrace() - [00001192
[0] 0838.10DC::09/27/16-11:16:11.8226444 [termsrv] termsrv_cpp1128 DoWppTrace() - [00001192
[0] 024C.1004::09/27/16-11:16:11.8387354 [lsm] service_cpp3007 DoWppTrace() - INF::OnGetSMCc
[0] 024C.1004::09/27/16-11:16:11.8387380 [lsm] service_cpp3007 DoWppTrace() - INF::OnGetSMCc
[0] 024C.1004::09/27/16-11:16:11.8387428 [lsm] service_cpp3007 DoWppTrace() - INF::OnGetSMCc
[0] 024C.1004::09/27/16-11:16:11.8387454 [lsm] service_cpp3007 DoWppTrace() - INF::OnGetSMCc
[0] 024C.0DAC::09/27/16-11:16:11.8393271 [lsm] service_cpp3053 DoWppTrace() - [0000378a]PERF
[0] 0838.10DC::09/27/16-11:16:11.8394330 [termsrv] termsrv_cpp1128 DoWppTrace() - [00001193
[0] 0838.10DC::09/27/16-11:16:11.8443116 [termsrv] termsrv_cpp1128 DoWppTrace() - [00001193
[0] 024C.0DAC::09/27/16-11:16:11.8443345 [lsm] service_cpp3007 DoWppTrace() - [0000378a]INF
[0] 0838.10DC::09/27/16-11:16:11.8447252 [termsrv] termsrv_cpp1128 DoWppTrace() - [00001194
[0] 0838.10DC::09/27/16-11:16:11.8447305 [termsrv] termsrv_cpp1128 DoWppTrace() - [00001194
[0] 024C.0DAC::09/27/16-11:16:11.8447478 [lsm] service_cpp3003 DoWppTrace() - [0000378a]:Ses
```

- **Network traces:**

  1. You can find lots of retransmits:

     ```
     615      11:15:52 AM 9/27/2016   192.168.219.100 10.169.3.4       TCP      TCP:[Request F
     616      11:15:52 AM 9/27/2016   10.169.3.4      192.168.219.100 TCP      TCP:[ReTransmi
     ```

  2. And eventually we see the connection is being reset by the server:

     ```
     1016     11:16:11 AM 9/27/2016   192.168.219.100 10.169.3.4       TCP      TCP:[Segment L
     1017     11:16:11 AM 9/27/2016   10.169.3.4      192.168.219.100 TCP      TCP: [Bad Chec
     ```

3. Back to the client we could we check the MTU size:

   ```
   ping azure-adfs1 -f -l 1420
   Pinging azure-adfs1.decaresystems.ie [10.169.3.4] with 1420 bytes of data:
   Packet needs to be fragmented but DF set.
   ```

4. So we see there is a problem with if the packet size is more then 1420. We then tried to reduce send a packet with a smaller MTU:

   ```
   ping azure-adfs1 -f -l 1410
   Pinging azure-adfs1.decaresystems.ie [10.169.3.4] with 1410 bytes of data:
   Reply from 10.169.3.4: bytes=1410 time=9ms TTL=125
   ```

5. And the packet passed through with MTU size of 1410. This usually indicates an issue with the firewall in between the on-premises network and the Azure vNET.

2. If this is true and this is your case, then the customer needs to update the MTU size on his network. If he prefers to change the MTU size over this VM only, he can do it locally by running the following:

```
netsh interface ipv4 set subinterface "Local Area Connection" mtu=1420 store=persistent
```

3. Once you changed the MTU, to test and validate its size run the following:

```
netsh int ipv4 show subint
```

Need additional help or have feedback?

To engage the Azure RDP-SSH SMEs...	To provide feedback on this page...	To provide kudos on this page...
Please reach out to the **RDP-SSH SMEs** ◲ for faster assistance. Make sure to use the **Ava process** for faster assistance.	Use the **RDP-SSH Feedback** form to submit detailed feedback on improvements or new content ideas for RDP-SSH. ***Please note*** the link to the page is required when submitting feedback on existing pages! If it is a new content idea, please put N/A in the Wiki Page Link.	Use the **RDP-SSH Kudos** form to submit kudos on the page. Kudos will help us improve our wiki content overall! ***Please note*** the link to the page is required when submitting kudos!