Black Screen on RDP and WinLogon_RDP SSH

Last updated by | Kevin Gregoire | Dec 5, 2022 at 9:01 AM PST

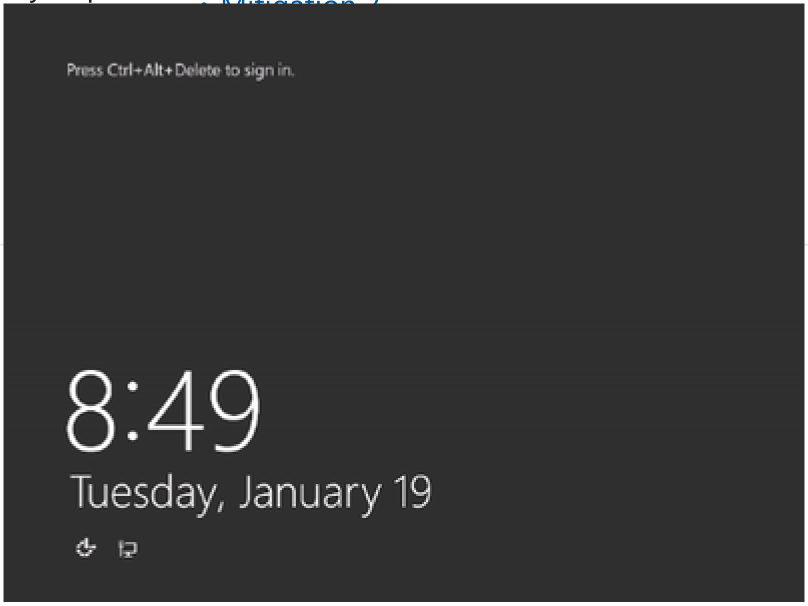
Tags

cw.TSG	cw.RDP-SSH

Contents

Symptoms

1. If you pull the screenshot of the VM, the console screenshot shows the VM is at Ctrl+Alt+Del screen



Press Ctrl+Alt+Delete to sign in.

8:49

Tuesday, January 19

2. When you RDP the server, you get prompted for the credentials and then opens a black screen and after roughly 60 seconds the session closes

3. Rebooting the VM resolves the issue temporally

4. Other type of connections to the machine works just fine:

    1. SMB connections: \\MACHINE\C$
    2. RPC connections like checking the event logs remotely
    3. Remote registry
    4. WinRM connections
    5. Any application running on this VM, like IIS websites or SQL will remain unaffected

5. On the Guest OS logs, you could see the event 4005:

```
Log Name:      Application
Source:        Microsoft-Windows-Winlogon
Date:          9/28/2016 10:45:03 AM
Event ID:      4005
Task Category: None
Level:         Error
Keywords:      Classic
User:          N/A
Computer:      AzureVM
Description:
The Windows logon process has unexpectedly terminated.
```

Symptom 1

1. On the Guest OS logs, you could see the event 36:

```
Log Name:      Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
Source:        Microsoft-Windows-TerminalServices-LocalSessionManager
Date:          9/28/2016 2:20:51 PM
Event ID:      36
Task Category: None
Level:         Error
Keywords:
User:          SYSTEM
Computer:      AzureVM
Description:
An error occurred when transitioning from CsrConnected in response to EvCsrInitialized. (ErrorCode 0x
```

2. A stack trace analysis of the TermService process shows the following:

```
0: kd> k
  *** Stack trace for last set context - .thread/.cxr resets it
 # Child-SP          RetAddr           Call Site
00 ffffd000`fff898e0 fffff800`1eed79ee nt!KiSwapContext+0x76 [d:\blue\minkernel\ntos\ke\amd64\ctxswap
01 ffffd000`fff89a20 fffff800`1eed7469 nt!KiSwapThread+0x14e [d:\blue\minkernel\ntos\ke\thredsup.c @
02 ffffd000`fff89ac0 fffff800`1ef08523 nt!KiCommitThreadWait+0x129 [d:\blue\minkernel\ntos\ke\waitsup
03 ffffd000`fff89b40 fffff800`1f277042 nt!KeWaitForSingleObject+0x373 [d:\blue\minkernel\ntos\ke\wait
04 ffffd000`fff89bd0 fffff800`1efe2ab3 nt!NtWaitForSingleObject+0xb2 [d:\blue\minkernel\ntos\ob\obwai
05 ffffd000`fff89c40 00007ffc`5ed206fa nt!KiSystemServiceCopyEnd+0x13 [d:\blue\minkernel\ntos\ke\amd6
06 000000f9`375bf6a8 00007ffc`5be91118 ntdll!ZwWaitForSingleObject+0xa [o:\blue.obj.amd64fre\minkerne
07 000000f9`375bf6b0 00007ffc`4d31923e KERNELBASE!WaitForSingleObjectEx+0x94 [d:\blue\minkernel\kerne
08 000000f9`375bf750 00007ffc`4d28d63c rdpcorets!CRdpDynVCMgr::CloseChannel+0x21e [d:\blue\termsrv\rd
09 000000f9`375bf7d0 00007ffc`4d290d3a rdpcorets!CRdpDynVC::OnClose+0x124 [d:\blue\termsrv\rdpplatfor
0a 000000f9`375bf860 00007ffc`4d290a61 rdpcorets!CTSMsg::Invoke+0x46 [d:\blue\termsrv\rdpplatform\com
```

Symptom 2

1. Another variation of this is that when the customer RDP into the VM, gets prompted for credentials and once these are entered, the winlogon services crashes
2. If the machine is restarted, the winlogon services starts normally till you try to login again so on the system log, you will see several events 4005 as shown before.
3. The customer has Citrix Xenapp install on this VM.

Symptom 3

1. On the Guest OS logs, you could see the event 4006:

```
Log Name:      Application
Source:        Microsoft-Windows-Winlogon
Date:          10/1/2019 9:59:40 AM
Event ID:      4006
Task Category: None
Level:         Warning
Keywords:      Classic
User:          N/A
Computer:      AzureVM
Description:
The Windows logon process has failed to spawn a user application. Application name: . Command line pa
```

PowerShell version:

```
$logonEvent = Get-WinEvent -LogName *Application* | where { $_.id -eq 4006}
$logonEvent.Message
```

Root Cause Analysis

Root Cause Analysis 1

- WSD Bug 8777675 on terminal services
- For further details on this bug please refer to this internal Bemis article

This bug was fixed on November 2016 KB3197875 release

```
OS Bug 8777675
```

Root Cause Analysis 2

Citrix has injected the binary *TWI3.dll* within the winlogon processes and has a fault version causing winlogon to crashes.

Root Cause Analysis 3

The account for "Authenticated Users" and "Interactive" have been removed from the Group "Users".

Root Cause Analysis 4

If spawning an event 4006 in Application.evtx, the registry value for `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon -> Userinit` could've been misconfigured.

Refresher / Training Template

- For the purpose of training or following along with this TSG, you can use the following link to deploy a VM with this scenario built-in. You will need to enable JIT for the VM. This lab is not to be shared with customers.

Deploy to Azure

References

- For Root Cause 1: November 2016 Preview of Monthly Quality Rollup for Windows 8.1 and Windows Server 2012 R2

Tracking close code for this volume

Root Cause	Product	Support Topic	Cause Tracking code	Bug
1	*Azure Virtual Machine – Windows*	*Routing Azure Virtual Machine V3\Cannot Connect to my VM\Failure to connect using RDP or SSH port*	*Root Cause - Windows Azure\Virtual Machine\Guest OS - Windows\VM Responding\Black Screen\Winlogon crash*	OS Bug 8777675

Root Cause	Product	Support Topic	Cause Tracking code	Bug
1	*Azure Virtual Machine – Windows*	*Routing Azure Virtual Machine V3\Cannot Connect to my VM\Failure to connect using RDP or SSH port*	*Root Cause - Windows Azure\Root Cause Not Determined	Applicable_Unsupported Scenario*

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

Customer Enablement

N/A

Mitigation

Backup OS disk

▶ Details

ONLINE Troubleshooting

ONLINE Approaches

Please be aware that the Serial Console Feature option will be today possible in:

1. Azure Resource Management VMs (ARM)

2. Public cloud

Whenever you are in a middle of a troubleshooting and you find the step **<<<<<INSERT MITIGATION>>>>>**, proceed to replace that steps with the mitigation section that you need referred below

Using Windows Admin Center (WAC)

▼ Click here to expand or collapse this section

WAC is supported on ARM VMs running Windows Server 2016 or later (not Win10 or any other Windows client version, and not 2012R2/2012/2008R2 versions of Windows Server

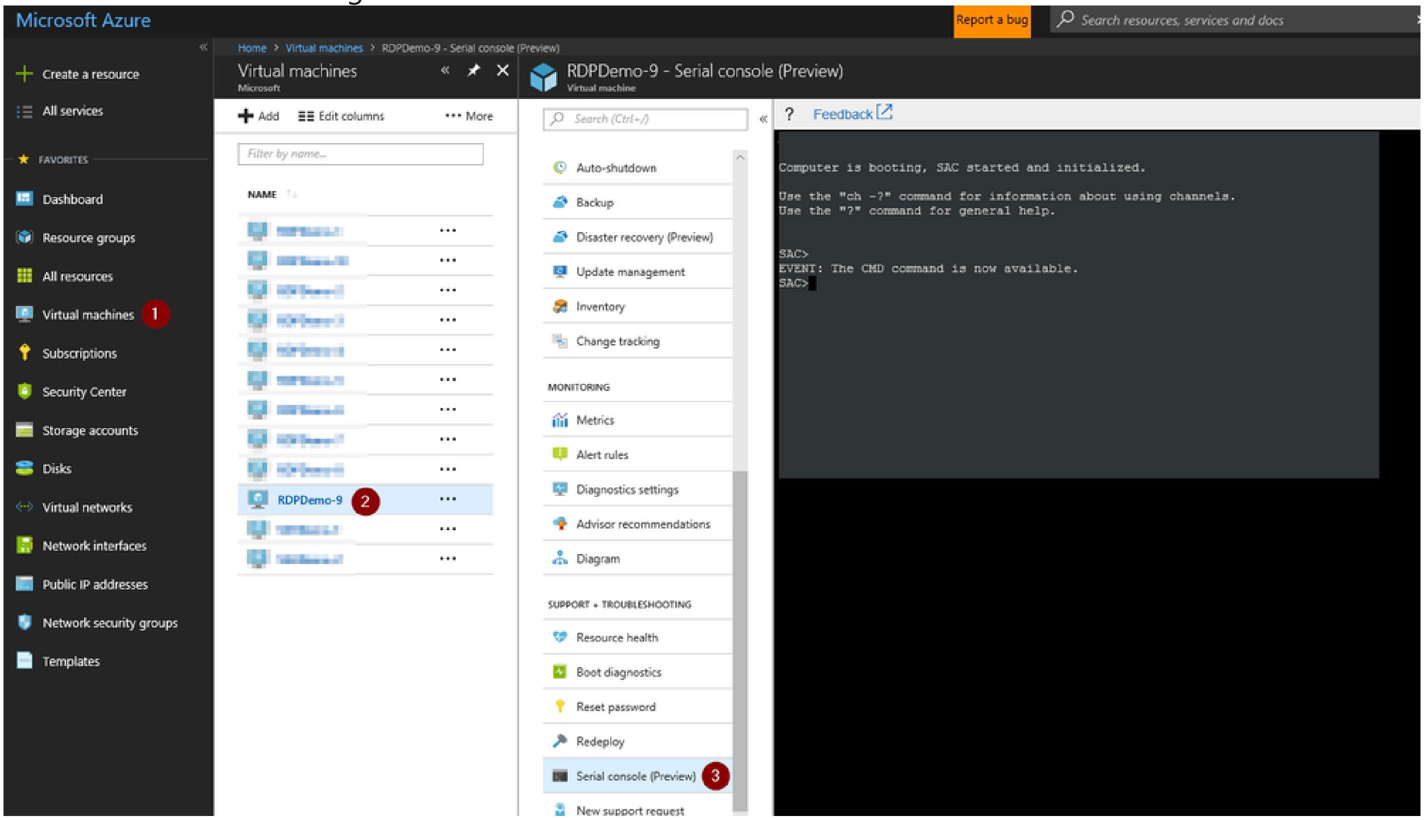
See How To Access Thru Windows Admin Center

Using *Serial Console Feature*

▼ Click here to expand or collapse this section

Applies only for ARM VMs

1. In the portal on the VM blade you will have an extra option called *Serial Console* click there
2. If EMS was enabled on the Guest OS, SAC will be able to connect successfully and then you will have a screenshot as the following:



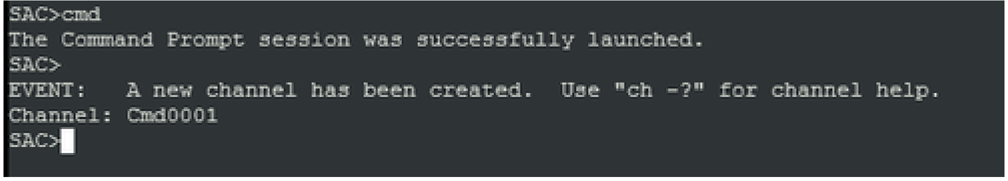
```
Computer is booting, SAC started and initialized.

Use the "ch -?" command for information about using channels.
Use the "?" command for general help.


SAC>
EVENT: The CMD command is now available.
SAC>
```

   1. If EMS does not connect, it means the Guest OS was not setup to use this feature:
      1. If the issue that you have will repro on a restart and if the customer is OK to enable this feature, you enable this feature. For details refer to Serial Console on the *How to enable this feature*
      2. If on the other hand, the issue will not repro on a restart, then you will need to skip this section and go on normally with the **OFFLINE troubleshooting** section

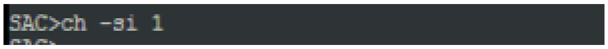
3. Create a channel with a CMD instance. Type `cmd` to start the channel, you will get the name of the channel



```
SAC>cmd
The Command Prompt session was successfully launched.
SAC>
EVENT:   A new channel has been created.  Use "ch -?" for channel help.
Channel: Cmd0001
SAC>
```

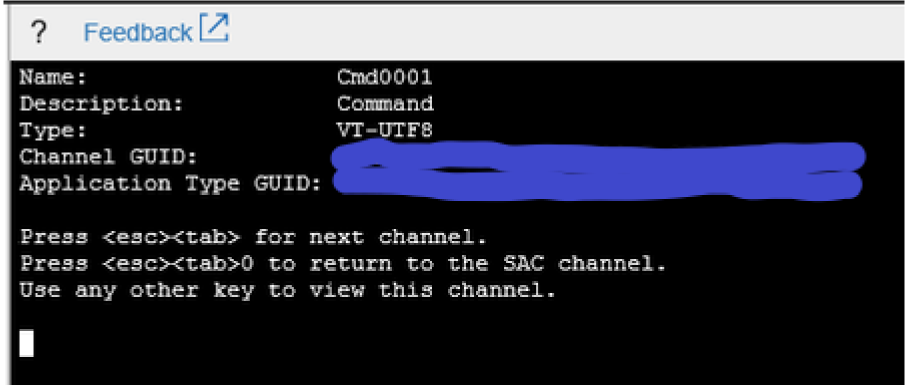
4. Switch to the channel running the CMD instance

```
ch -si 1
```



```
SAC>ch -si 1
```

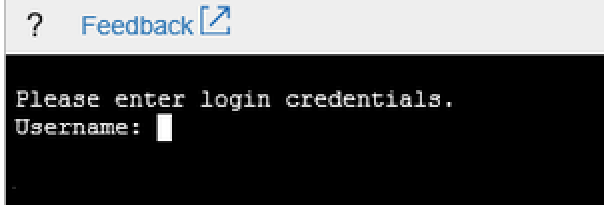
5. Once you hit enter, it will switch to that channel



```
Name:                    Cmd0001
Description:             Command
Type:                    VT-UTF8
Channel GUID:            [redacted]
Application Type GUID:

Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.
```

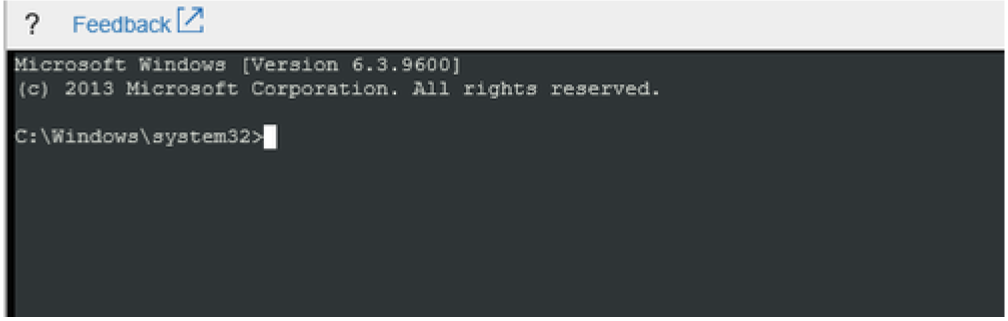
6. Hit enter a second time and it will ask you for user, domain and password:



```
Please enter login credentials.
Username:
```

   1. If the machine has connectivity, you could use either local or domain IDs. If you want to use a local ID, for domain just add the hostname of the VM
   2. If the machine doesn't have connectivity, you could try to se domains IDs however this will work if only the credentials are cached on the VM. In this scenario, is suggested to use local IDs instead.

7. Once you add valid credentials, the CMD instance will open and you will have the prompt for you to start your troubleshooting:

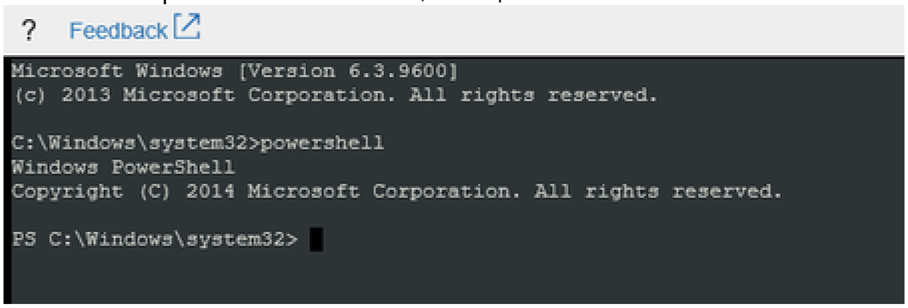


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

   1. At this point, you can do your troubleshooting in bash (CMD) or else, you could start a powershell instance:

1. To launch a powershell instance, run `powershell`

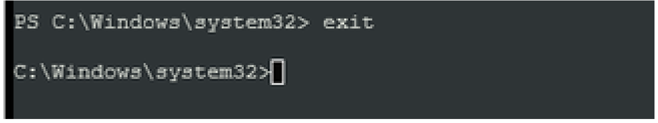


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>powershell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>
```

2. To end the powershell instance and return to CMD, just type `exit`



```
PS C:\Windows\system32> exit

C:\Windows\system32>
```

8. **<<<<<INSERT MITIGATION>>>>>**

Using *Remote Powershell*

▶ Click here to expand or collapse this section

Using *Remote CMD*

▶ Click here to expand or collapse this section

Using *Custom Script Extension* or *RunCommands Feature*

▶ Click here to expand or collapse this section

Using *Remote Registry*

▶ Click here to expand or collapse this section

Using *Remote Services Console*

▶ Click here to expand or collapse this section

ONLINE Mitigations

Mitigation 1

▼ Click here to expand or collapse this section

Applies to Windows Server 2012 R2

1. Get the running services to get the PID of the **svchost** where **TermService** is running

   ```
   tasklist /svc
   ```

2. Once you identify the correct process and its PID you kill it

   ```
   taskkill /PID <<PID>> /F
   ```

3. Now check if the service is getting automatically started, this will be done within 1min

4. At this point the RDP connections will be restore however the issue is not fix

5. Check if the server has the [KB3197875](#) or a newer installed, if not proceed to install it, you could see the patch level of the server in WinGuestAnalyzer report.

6. If it is not installed, open an elevated Powershell instance and run the following script:

```
#Create a download location
md c:\temp

##Download the KB file
remove-module psreadline
$source = "http://download.windowsupdate.com/c/msdownload/update/software/updt/2016/11/windows8.1-kb31978
$destination = "c:\temp\windows8.1-kb3197875-x64_979273db494c9f70d0a6cfbffb2d033f30ddf01b.msu"
$wc = New-Object System.Net.WebClient
$wc.DownloadFile($source,$destination)

#Install the KB
expand -F:* $destination C:\temp\
dism /ONLINE /add-package /packagepath:"c:\temp\Windows8.1-KB3197875-x64.cab"

#Restart the VM to complete the installations/settings
shutdown /r /t 0 /f
```

Mitigation 2

▼ Click here to expand or collapse this section

This applies to Citrix Xenapp VMs

1. Refer to *Mitigation 3* on [Fail RDP connection on a Citrix VM](#)

Mitigation 3

▼ Click here to expand or collapse this section

1. Check to see if "Interactive" and "Authenticated Users" are missing from the Group "Users".

2. To check what members are part of the Group "Users" run the below command in CMD.

```
Net localgroup Users
```

3. Run the below command to add "Interactive" and "Authenticated Users" back to the Group "Users".

```
Net localgroup Users Interactive /add
Net localgroup Users "Authenticated Users" /add
```

Mitigation 4

▼ Click here to expand or collapse this section

1. Check if the Winlogon value for userinit.exe has been modified:

```
reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v Userinit
```

2. The resulting value should be `C:\Windows\system32\userinit.exe` . If not, update the registry value to match:

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v Userinit /t REG_SZ
```

Restart the computer and see if the black screen persists on RDP attempts.

OFFLINE Troubleshooting

```
For CRP machines, at any point that you follow end to end any of the OFFLINE mitigation and that doesn't work
```

OFFLINE Approaches

Whenever you are in a middle of a troubleshooting and you find the step **<<<<<<INSERT MITIGATION>>>>>**, proceed to replace that steps with the mitigation section that you need referred below.

Information

For more in-depth information on these operations, please review: Windows Partitions in Non-Boot Scenarios_RDP-SSH.

Using *Recovery Script*

▶ Click here to expand or collapse this section

Using *OSDisk Swap API*

▶ Click here to expand or collapse this section

Using *VM Recreation scripts*

▶ Click here to expand or collapse this section

OFFLINE Mitigations

Mitigation 1

▼ Click here to expand or collapse this section
Applies to Windows Server 2012 R2

1. Check if the server has the KB3197875? or a newer installed, if not proceed to install it, you could see the patch level of the server in WinGuestAnalyzer report.
2. If it is not installed, open an elevated CMD instance and run the following script:

```
#Create a download location
md c:\temp

##Download the KB file
remove-module psreadline
$source = "http://download.windowsupdate.com/c/msdownload/update/software/updt/2016/11/windows8.1-kb31978
$destination = "c:\temp\windows8.1-kb3197875-x64_979273db494c9f70d0a6cfbffb2d033f30ddf01b.msu"
$wc = New-Object System.Net.WebClient
$wc.DownloadFile($source,$destination)

#Install the KB
expand -F:* $destination C:\temp\
dism /image:<OS Disk letter>:\ /add-package /packagepath:"c:\temp\Windows8.1-KB3197875-x64.cab"
```

Mitigation 2

▼ Click here to expand or collapse this section

This applies to Citrix Xenapp VMs

1. Refer to *Mitigation 3* on Fail RDP connection on a Citrix VM

Mitigation 3

▼ Click here to expand or collapse this section

1. Check if the Winlogon value for userinit.exe has been modified by mounting the OS disk to a rescue VM, importing the broken VM's SOFTWARE registry hive, and checking the value for `\Microsoft\Windows NT\CurrentVersion\Winlogon -> Userinit` .
2. The resulting value should be `C:\Windows\system32\userinit.exe` . If not, update the registry value to match.
3. Boot the disk in Hyper-V or swap the disks and see if the issue persists.

Escalate

1. If this doesn't work out, please reach out to the Unable to RDP-SSH SME channel on teams for advise providing the case number, issue description and your question
2. If the RDP SMEs are not available to answer you, you could engate the RDS team for assistance on this.
    1. Ensure you collect the Windows Performance SDP package from the VM and upload that into the DTM workspace.

        1. This would be easily done by running the following script on Serial Console on a powershell instance:

```
#Create a download location and setup the console to prioritize TLS1.2 connections
remove-module psreadline
[Net.ServicePointManager]::SecurityProtocol = "tls12, tls11, tls"
md c:\temp

#Download the Windows SDP file
$source = "https://aka.ms/getTSSv2"
$destination = "c:\temp\TSSv2.zip"
$wc = New-Object System.Net.WebClient
$wc.DownloadFile($source,$destination)

#Expand and run the SDP package for Setup, Network and Performance
Expand-Archive -LiteralPath $destination -DestinationPath C:\temp

#recommended to run the new packages:
C:\temp\TSSv2.ps1 -SDP Setup
C:\temp\TSSv2.ps1 -SDP NET
C:\temp\TSSv2.ps1 -SDP Perf

#Note: you still can run old SDP packages, in case is required:
C:\temp\psSDP\Get-psSDP.ps1 Setup
C:\temp\psSDP\Get-psSDP.ps1 Net
C:\temp\psSDP\Get-psSDP.ps1 Perf
```

    2. Collect the following files to the DTM workspace of this case:
        1. `C:\MS_DATA\SDP_Setup\tss_DATETIME_COMPUTERNAME_psSDP_SETUP.zip`
        2. `C:\MS_DATA\SDP_NET\tss_DATETIME_COMPUTERNAME_psSDP_NET.zip`
        3. `C:\MS_DATA\SDP_Perf\tss_DATETIME_COMPUTERNAME_psSDP_PERF.zip`
2. Cut a problem with the following details:
    - Product: ***Azure\Virtual Machine running Windows***
    - Support topic: ***Routing Issue with Remote Desktop Service (RDS) on Azure\Issue with connectivity using RDS***

After work - Cleanup

If you are uncertain that we may need this snapshot by the end of this case for RCA purposes, then just leave it.

1. If the issue is already fix and no further RCA analysis is needed, then proceed to remove the OS Disk backup we created at the beginning of the case
    1. If the **disk is managed** using the portal so the snapshot section and select the snapshot you created previously as a backup.
    2. If the **disk is unmanaged** then
        1. If this is an CRP Machine - ARM, then no further action is required
        2. If this is an Classic - RDFE machine, then
            1. Check the storage account where the OS disk of this machine is hosted using Microsoft Azure Storage Explorer right click over the disk and select *Managed Snapshots*
            2. Proceed to delete the snapshot of the broken machine

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!