# Black Screen on RDP and Console_RDP SSH

Last updated by | Kevin Gregoire | Mar 29, 2022 at 11:47 AM PDT

Tags

| | |
|---|---|
| cw.TSG | cw.RDP-SSH |

**Contents**

## Symptoms

1. If you pull the screenshot of the VM, the console screenshot shows a black screen

2. When you RDP the server, you get prompted for the credentials and then opens a black screen

3. 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
4. The black screen on console is even on cleanmode or safe mode in case you downloaded this VHD to on premise and create a VM from it on a HyperV

5. On the Guest OS logs, you may find that the *Desktop Windows Manager* (dwm.exe) is crashing

```
Log Name:      System
Source:        Application Popup
Date:          6/23/2016 1:44:52 PM
Event ID:      26
Task Category: None
Level:         Information
Keywords:
User:          SYSTEM
Computer:      AZSOCE01.widex.org
Description:
Application popup: dwm.exe - Application Error : The application was unable to start correctly (0xc00
```

```
Log Name:      Application
Source:        Application Error
Date:          6/23/2016 1:54:38 PM
Event ID:      1000
Task Category: Application Crashing Events
Level:         Error
Keywords:      Classic
User:          N/A
Computer:      AZSOCE01.widex.org
Description:
Faulting application name: dwm.exe, version: 6.3.9600.17415, time stamp: 0x54503cd6
Faulting module name: ntdll.dll, version: 6.3.9600.18233, time stamp: 0x56bb4ebb
Exception code: 0xc000007b
Fault offset: 0x00000000000ecdd0
Faulting process id: 0x310
Faulting application start time: 0x01d1cd346b8ce7ef
Faulting application path: C:\Windows\system32\dwm.exe
Faulting module path: C:\Windows\SYSTEM32\ntdll.dll
Report Id: 7f382d78-3928-11e6-80cf-000d3ab0976f
Faulting package full name:
Faulting package-relative application ID:
```

## Root Cause Analysis

### Root Cause Analysis 2

File corruption that affects the GUI. Issue described on KB3137061

```
OS corruption due to LSI15536267 -  RDBug5688740
```

### Root Cause Analysis 1 & 3

File corruption that affects the GUI.

### References

- Windows Azure VMs don't recover from a network outage and data corruption issues occur

### 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\Non-Boot\File System Corruption* | |
| 2 | *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\Non-Boot\File System Corruption* | RDBug5688740 |
| 3 | *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\Non-Boot\File System Corruption* | |

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

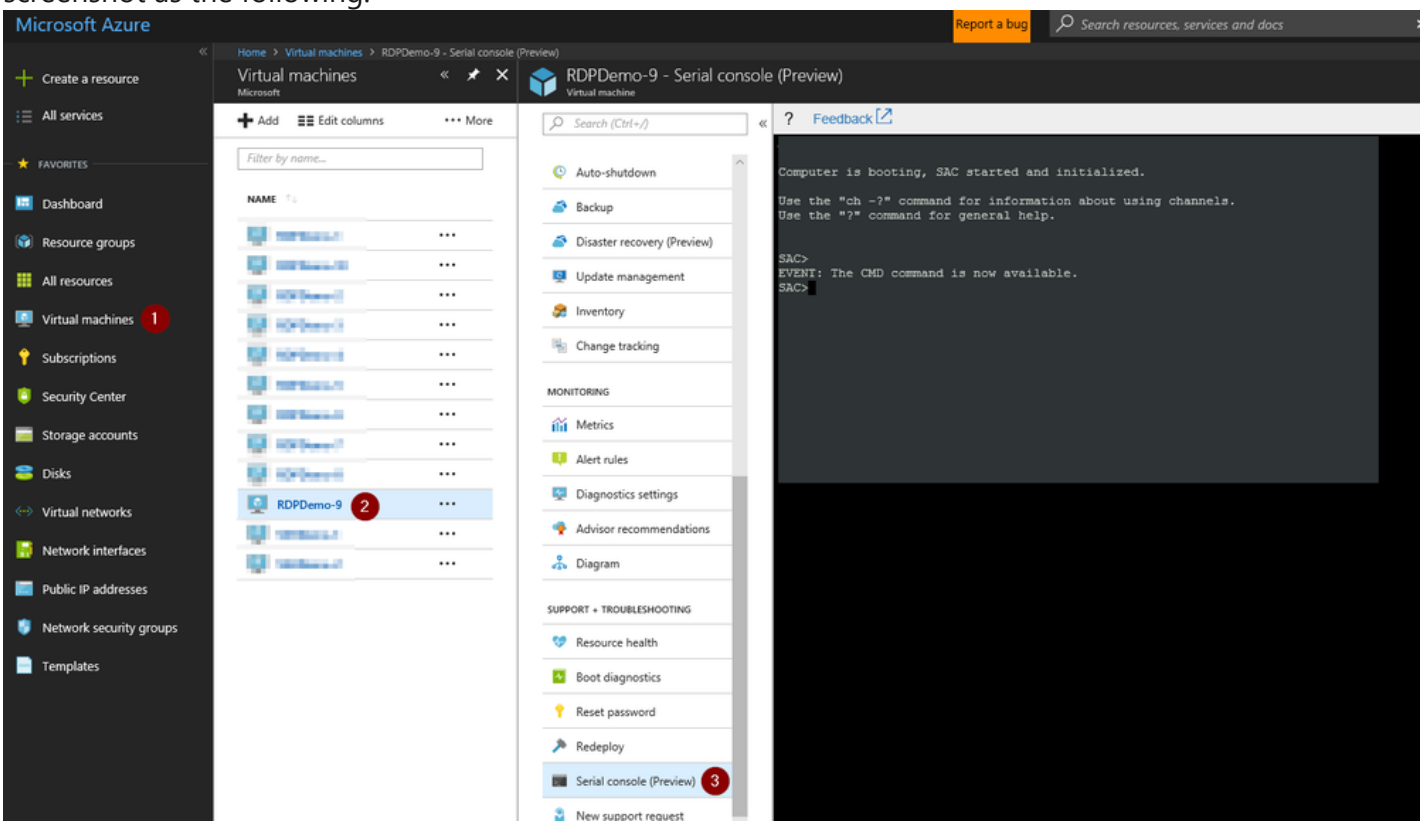
WAC is supported on ARM VMs running Windows Server 2016 or later (not Win10 or any other Windows client version, and not 2012R2/2012/2008R2 versions of Windows Server

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:




   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

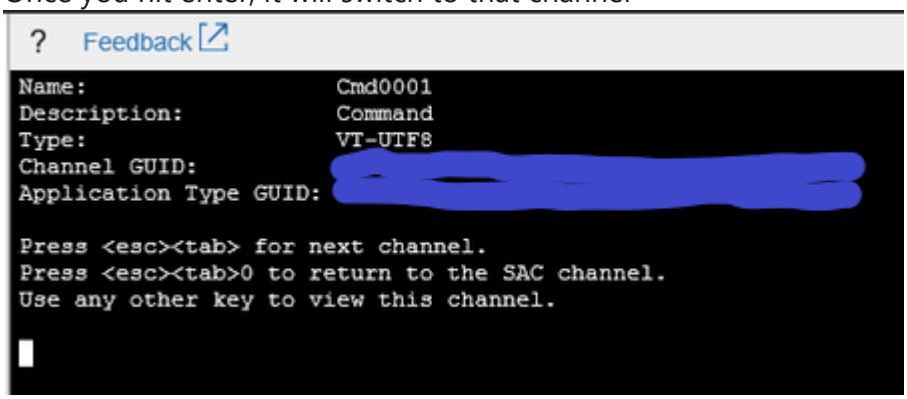
```
SAC>cmd
The Command Prompt session was successfully launched.
SAC>
EVENT:   A new channel has been created.  Use "ch -?" for channel help.
Channel: Cmd0001
SAC>
```

4. Switch to the channel running the CMD instance

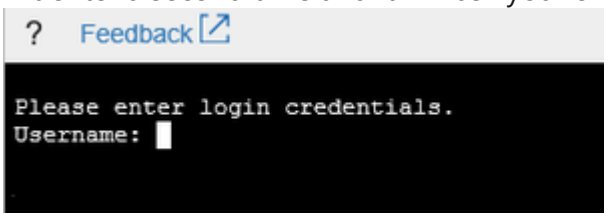
```
ch -si 1
```

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

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



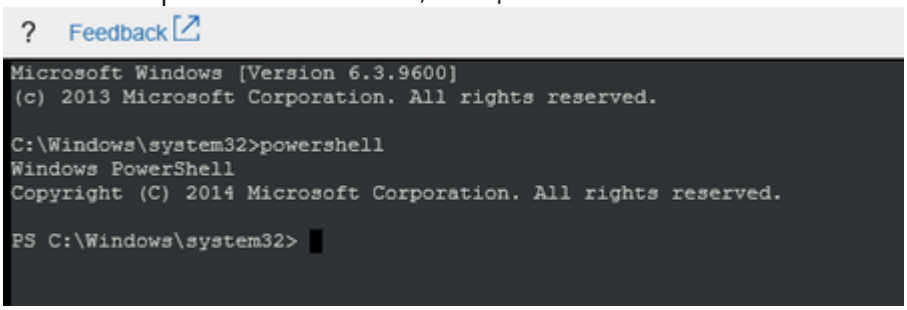

6. Hit enter a second time and it will ask you for user, domain and password:



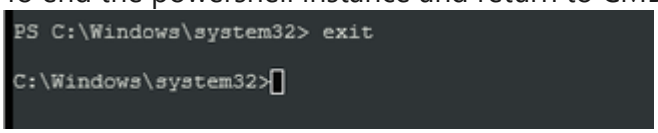

   1. If the machine has connectivity, you could use either local or domain IDs. If you want to use a local ID, for domain just add the hostname of the VM
   2. If the machine doesn't have connectivity, you could try to se domains IDs however this will work if only the credentials are cached on the VM.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


   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`




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




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

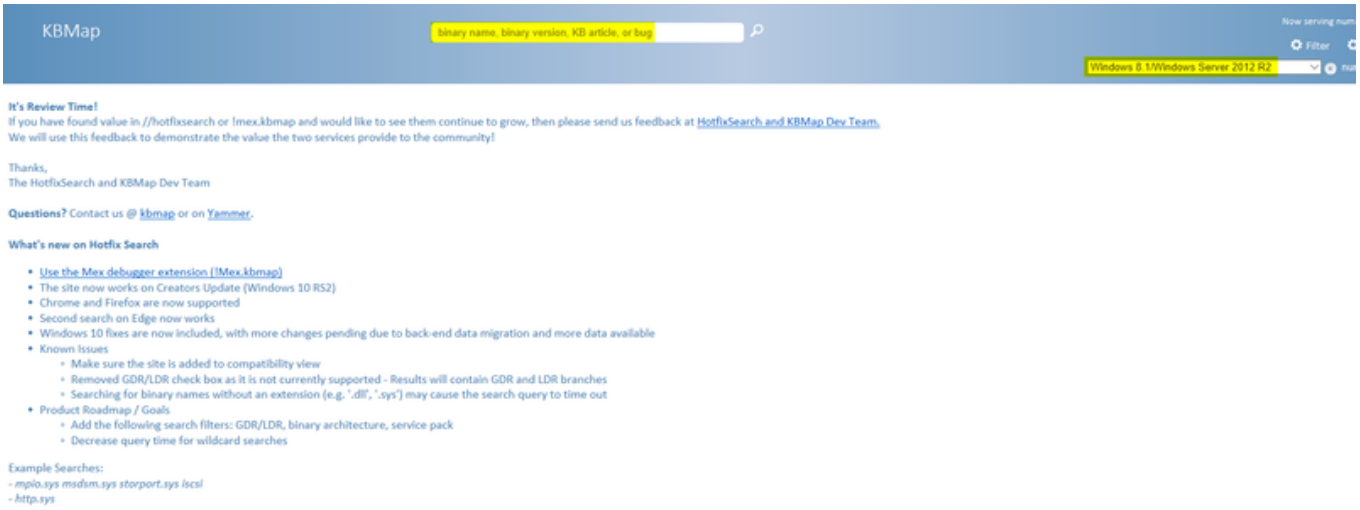
1. Open an elevated CMD instance and run a system consistency check:

```
dism /online /cleanup-image /restorehealth
```

2. If the outcome says that corruption was find and fixed, rerun `dism` till it says that server is corruption free
3. If the outcome says that corruption is found but couldn't fix it, then collect the following logs to see where the corruption is:

```
C:\Windows\Logs\DISM\dism.log
C:\Windows\Logs\CBS\cbs.log
```

4. If you need assistance on how to read these logs, reach out to the SME RDP channel on teams
5. Once you identify where the corruption is, then you can install the latest KB that introduce this file and all the related to its subsystem:
    1. Get the OS version of the VM
    2. Browse up to KBMAP and select the OS and the binary that you are looking for and click search. This will give you the KB history of that component so you could install the latest KB on the image.




**Note:** If the query comes with an empty query, it means that the file you look for is not OS related so you may want to skip from the following way to fix this

3. Download the KB that performs the upgrade on the troubleshooting VM on a folder like `c:\temp`
4. Install the KB on that OS disk

```
dism /online /add-package /packagepath:c:\temp\<<KB .msu or .cab>>
```

6. Restart the VM and retry

#### Mitigation 2

This mitigation applies in OFFLINE mode only

#### Mitigation 3

This mitigation applies in OFFLINE mode only

### 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**

This mitigation applies in ONLINE mode only

**Mitigation 2**

▼ Click here to expand or collapse this section

1. Open an elevated CMD instance
2. Take the ownership of the file ***\windows\system32\DWRITE.DLL*** and rename it as ***DWRITE.OLD***. Copy the file from a working machine with the same OS and patch level and recreate the VM
3. Once the VM is boot back normally, run SFC to repair any other corruption (this operation could last up to 1hs and even more depending on the level of corruption)

```
sfc /scannow
```

4. Once the SFC it is over, check if the corruption was detected and repaired. Ask the customer for a screenshot of the SFC outcome.
5. If he corruption was identified and not repair, then refer to the file ***C:\Windows\Logs\CBS\CBS.log*** to find the path of the corrupted files that needs to be copied from a working machine

```
2016-02-24 20:55:21, Info                  CSI    000008e3 [SR] Beginning Verify and Repair transacti
2016-02-24 20:55:21, Info                  CSI    000008e4 Hashes for file member \SystemRoot\WinSxS\
Found: {l:32 b:Uvaw/kcydXsS1y/ik8x8xCJBakNOAdzebd48zmMv7l0=} Expected: {l:32 b:cEvBiGttek+Lyy2m5p0CY1
2016-02-24 20:55:21, Info                  CSI    000008e5 [SR] Cannot repair member file [l:20{10}]"
2016-02-24 20:55:21, Info                  CSI    000008e6 Hashes for file member \SystemRoot\WinSxS\
Found: {l:32 b:Uvaw/kcydXsS1y/ik8x8xCJBakNOAdzebd48zmMv7l0=} Expected: {l:32 b:cEvBiGttek+Lyy2m5p0CY1
2016-02-24 20:55:21, Info                  CSI    000008e7 [SR] Cannot repair member file [l:20{10}]"
2016-02-24 20:55:21, Info                  CSI    000008e8 [SR] This component was referenced by [l:1
2016-02-24 20:55:21, Info                  CSI    000008e9 Hashes for file member \??\C:\Windows\SysW
Found: {l:32 b:Uvaw/kcydXsS1y/ik8x8xCJBakNOAdzebd48zmMv7l0=} Expected: {l:32 b:cEvBiGttek+Lyy2m5p0CY1
2016-02-24 20:55:21, Info                  CSI    000008ea Hashes for file member \SystemRoot\WinSxS\
Found: {l:32 b:Uvaw/kcydXsS1y/ik8x8xCJBakNOAdzebd48zmMv7l0=} Expected: {l:32 b:cEvBiGttek+Lyy2m5p0CY1
2016-02-24 20:55:21, Info                  CSI    000008eb [SR] Could not reproject corrupted file [m
```

6. If you had to copy some healthy binaries, rerun the SFC till it come up that the OS is corruption free
7. If it keeps on saying that the corruption cannot be identified, keep on checking the CBS log to see which file is still corrupted
8. Collect `C:\Windows\Logs\CBS\CBS.log` for documentation purposes

**Mitigation 3**

▼ Click here to expand or collapse this section

1. Open an elevated CMD

2. If you see ***DWM.EXE crashing***, then proceed to take the ownership and renaming the following files and get a copy from a working machine with the same OS and patch level

   *\windows\system32\dwmcore.dll to \windows\system32\dwmcore.dll.OLD*

   *\windows\system32\imm32.dll to \windows\system32\imm32.dll.OLD*

3. Just to prepare the VM in case that the issue is not fix with this and taking the advantage that you already have access to the disk, setup the VM to create user mode dumps in case of a service crash. Follow Setup a machine for a User-Mode Dump

4. Recreate the VM

5. If the issue remains, then

   1. Delete the VM again, attach the OS disk on a troubleshooting VM and collect the user mode dumps on *c:\CrashDumps* and upload those to a DTM Workspace.
   2. Cut a problem to engage GES and follow the action plan from GES
      - Product: ***Windows Svr 2012 R2 Datacenter*** or ***Windows Svr 2016 Datacenter*** as appropriate
      - Support topic: ***Routing Windows V3\System Performance\Issue in which an application or process is unresponsive or crashes***
      - These routing will route you to a Windows team however since we need to engage GES, override the routing to
        - For Premier cases: ***Windows EE Premier*** queue. Check radius on how to contact this team.
        - For Professional cases: ***Windows EE Pro*** queue. Check radius on how to contact this team.

6. Otherwise, if the VM boots normally then run SFC to repair any other corruption (this operation could last **up to 1hs** (and could last even longer depending on the level of corruption and disk size)

```
sfc /scannow
```

7. Once the SFC it is over, check if the corruption was detected and repaired. Ask the customer for a screenshot of the SFC outcome and documented this on the case

8. If he corruption was identified and not repair, then refer to the file *C:\Windows\Logs\CBS\CBS.log* to find the path of the corrupted files that needs to be copied from a working machine

```
2016-02-24 20:55:21, Info                  CSI    000008e3 [SR] Beginning Verify and Repair transacti
2016-02-24 20:55:21, Info                  CSI    000008e4 Hashes for file member \SystemRoot\WinSxS\
  Found: {l:32 b:Uvaw/kcydXsS1y/ik8x8xCJBakNOAdzebd48zmMv7l0=} Expected: {l:32 b:cEvBiGttek+Lyy2m5p0C
2016-02-24 20:55:21, Info                  CSI    000008e5 [SR] Cannot repair member file [l:20{10}]"
2016-02-24 20:55:21, Info                  CSI    000008e6 Hashes for file member \SystemRoot\WinSxS\
  Found: {l:32 b:Uvaw/kcydXsS1y/ik8x8xCJBakNOAdzebd48zmMv7l0=} Expected: {l:32 b:cEvBiGttek+Lyy2m5p0C
2016-02-24 20:55:21, Info                  CSI    000008e7 [SR] Cannot repair member file [l:20{10}]"
2016-02-24 20:55:21, Info                  CSI    000008e8 [SR] This component was referenced by [l:1
2016-02-24 20:55:21, Info                  CSI    000008e9 Hashes for file member \??\C:\Windows\SysW
  Found: {l:32 b:Uvaw/kcydXsS1y/ik8x8xCJBakNOAdzebd48zmMv7l0=} Expected: {l:32 b:cEvBiGttek+Lyy2m5p0C
2016-02-24 20:55:21, Info                  CSI    000008ea Hashes for file member \SystemRoot\WinSxS\
  Found: {l:32 b:Uvaw/kcydXsS1y/ik8x8xCJBakNOAdzebd48zmMv7l0=} Expected: {l:32 b:cEvBiGttek+Lyy2m5p0C
2016-02-24 20:55:21, Info                  CSI    000008eb [SR] Could not reproject corrupted file [m
```

9. If you had to copy some healthy binaries, rerun the SFC till it come up that the OS is corruption free

10. If it keeps on saying that the corruption cannot be identified, keep on checking the CBS log to see which file is still corrupted

11. Collect *C:\Windows\Logs\CBS\CBS.log* for documentation purposes

### 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.<br><br>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.<br><br>***Please note*** the link to the page is required when submitting feedback on existing pages!<br>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!<br><br>***Please note*** the link to the page is required when submitting kudos! |