

Service Hang or Crash_RDP SSH

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

Tags

cw.TSG

cw.RDP-SSH

Contents

- Symptoms
- Root Cause Analysis
 - Tracking close code for this volume
- Customer Enablement
- Mitigation
 - Backup OS disk
 - ONLINE Troubleshooting
 - ONLINE Approaches
 - Using Windows Admin Center (WAC)
 - Using Serial Console Feature
 - Using Remote Powershell
 - Using Remote CMD
 - Using Custom Script Extension or RunCommands Feature
 - Using Remote Registry
 - Using Remote Services Console
 - Using Remote Powershell
 - Using Remote CMD
 - Using Custom Script Extension or RunCommands Feature
 - Using Remote Registry
 - Using Remote Services Console
 - ONLINE Mitigations
 - Service is in a hung state
 - Service is stopped
 - OFFLINE Troubleshooting
 - OFFLINE Approaches
 - Information
 - Using Recovery Script
 - For ARM VMs
 - For Classic VMs
 - Using OSDisk Swap API
 - Using VM Recreation scripts
 - For ARM VMs
 - For Classic VMs
 - For Classic VMs
 - Using OSDisk Swap API
 - Using VM Recreation scripts
 - For ARM VMs
 - For Classic VMs
 - OFFLINE Mitigations

- [Escalate](#)

- [After work - Cleanup](#)

Symptoms

1. The screenshot of the VM could be anything, from Ctrl+Alt+Del, open sessions, black/blue screen, the booting process that is stuck
[Need addition of the VM have feedback?](#)
2. There's no connectivity to the virtual machine on its VIP or DIP or its PA verified with [VM Port Scanner](#).
3. On the GuestOS logs we could see event 7022 for hanging services:

```
Log Name:      System
Source:        Service Control Manager
Date:          12/16/2015 11:19:36 AM
Event ID:      7022
Task Category: None
Level:         Error
Keywords:      Classic
User:          N/A
Computer:      RcnSharePoint.rcnradio.net
Description:   The Base Filtering Engine service hung on starting.
```

4. Or events 1000 for services crashing:

```
Log Name:      Application
Source:         Application Error
Date:           10/27/2014 4:01:40 PM
Event ID:       1000
Task Category: Application Crashing Events
Level:          Error
Keywords:       Classic
User:           N/A
Computer:       DJSMXL2500120.pemex.pmx.com
Description:
Faulting application name: explorer.EXE, version: 14.0.7125.5000, time stamp: 0x53745315
Faulting module name: eS4px3ui.dll, version: 5.15.96.1, time stamp: 0x4c7f551c
Exception code: 0xc0000005
Fault offset: 0x000024da
Faulting process id: 0x19b4
Faulting application start time: 0x01cfff2030d494474
Faulting application path: C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Faulting module path: C:\Windows\system32\spool\DRIVERS\W32X86\3\eS4px3ui.dll
Report Id: d3bed295-5e24-11e4-83e6-10604b6346c2
Faulting package full name: %14
Faulting package-relative application ID: %15
```

5. Depending on the service crashing/hanging and its dependent services
 1. We could or could not have connectivity of the VM or any other symptom.
 2. If any of those service belongs to the network stack like BFE, Windows Firewall, DHCP, etc, is the one hanging or crashing, in **WinGuestAnalyzer\Health Signal** tab on the *services* section you will see

status as **Starting**, **Stopping** or directly **Stopped**:

```
},
  "services": [
    {
      "name": "TermService",
      "state": "Running",
      "startMode": "Manual"
    },
    {
      "name": "BFE",
      "state": "Stopped",
      "startMode": "Auto"
    }
  ]
}
```

Root Cause Analysis

The root cause analysis will depend on the scenario and the outcome of the dump analysis.

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\Isolated\Windows Services not starting/crashing | |

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

- ▼ Click here to expand or collapse this section
1. Before doing anything, please validate if this is an encrypted VM. On ASC check on the Resource Explorer on the VMCard for the value *OS Disk Encrypted*

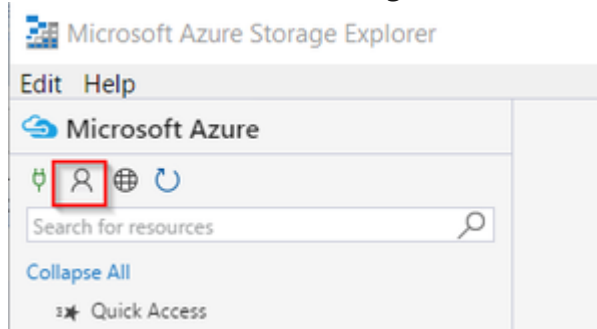
| | |
|---|--------------------------------------|
| OS Disk Lease Id | Udb9a55c-0317-40fa-a032-b1f3550f3775 |
| OS Disk Lease Acquired | True |
| OS Disk Billing Validated | True |
| OS Disk Encrypted | False |
| Billing Code | Windows_IaaS |
| Billing is Created from Marketplace Image | N/A |
| Billing Tag GUID | 00000000-0000-0000-0000-000000000000 |

2. If the OS Disk is encrypted, then proceed to [Unlock an encrypted disk](#)

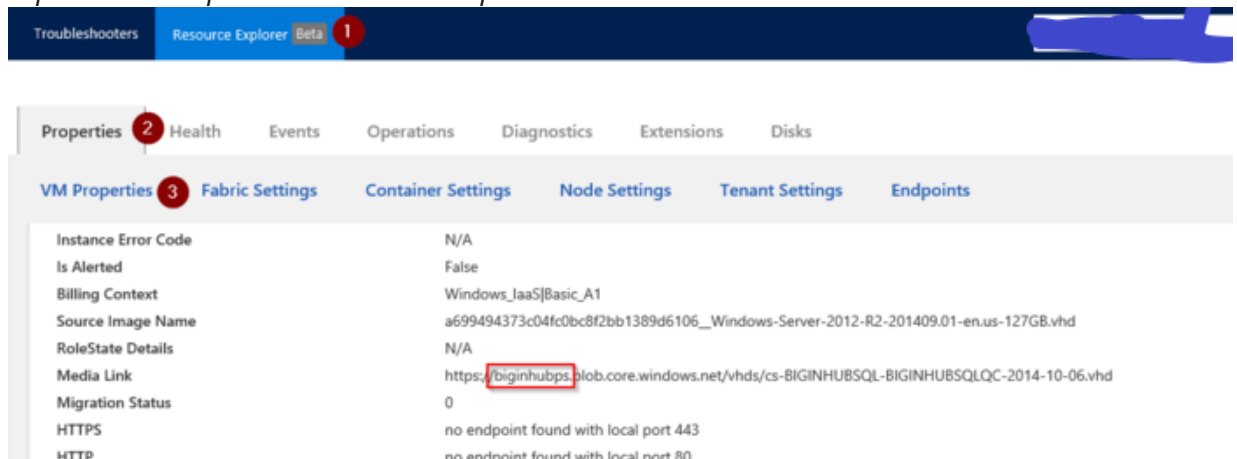
3. Now proceed to do a copy of the OS disk, this will help in case of a rollback for recovery or RCA in a later stage
4. Power the machine down and once it is stopped de-allocated to do the copy.
5. Create a snapshot
 1. If the **disk is unmanaged**, this could be done by using [Microsoft Azure Storage Explorer](#) or [Azure Powershell](#)

1. Using [Microsoft Azure Storage Explorer](#)

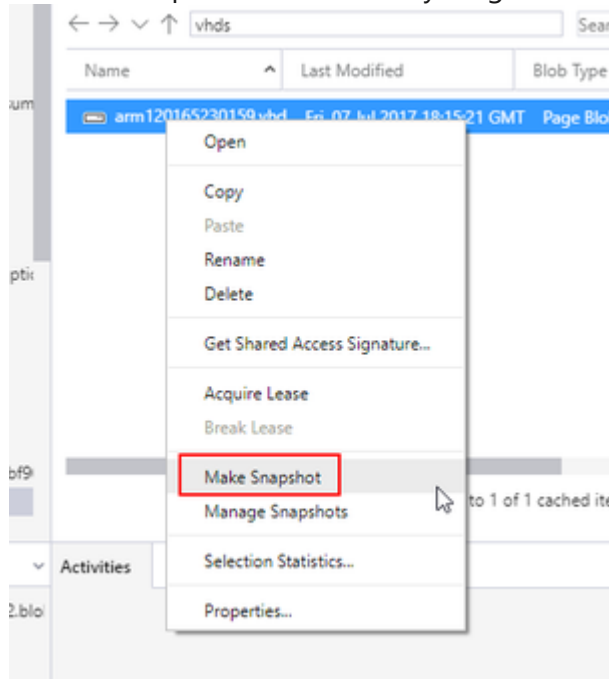
1. Once the customer download the tool, proceed to add the Azure account details so you can access the storage accounts
2. Click on **Add Account Settings** then ***Add an account...***



3. Go to the storage account where the OS disk is, you can see this on ASC under *Resource Explorer* on *Properties* in the *VM Properties* card



4. Create a snapshot of this disk by a right click over the disk and select *Make Snapshot*



2. Using [Azure Powershell](#)

1. You can follow [How to Clone a disk using Powershell](#)

2. If the **disk is managed**, use Azure portal to take a snapshot

1. Sign in to the Azure portal.
2. Starting in the upper-left, click New and search for snapshot.
3. In the Snapshot blade, click Create.
4. Enter a Name for the snapshot.
5. Select an existing Resource group or type the name for a new one.
6. Select an Azure datacenter Location.
7. For Source disk, select the Managed Disk to snapshot.
8. Select the Account type to use to store the snapshot. We recommend Standard_LRS unless you need it stored on a high performing disk.
9. Click Create.

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)

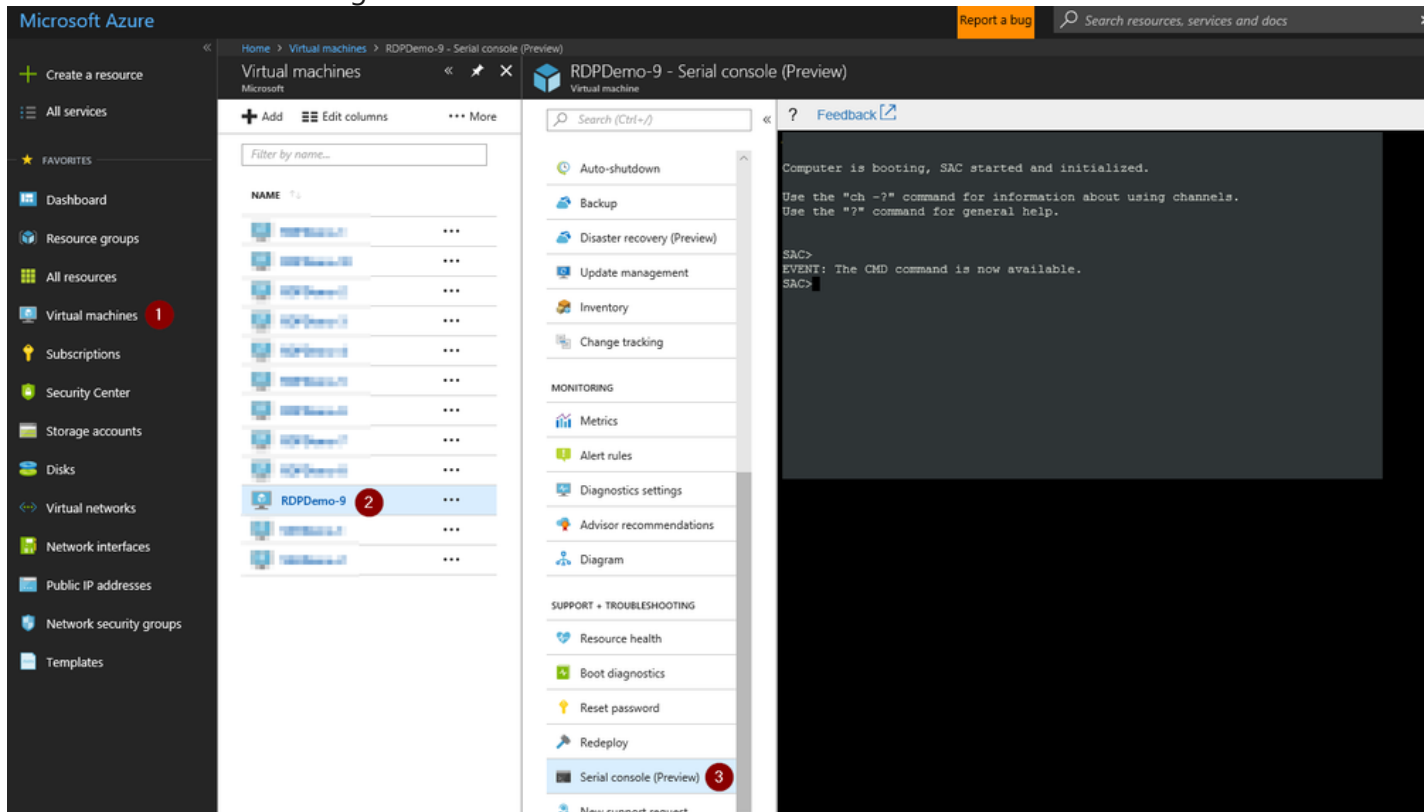
See [How To Access Thru Windows Admin Center](#)

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:



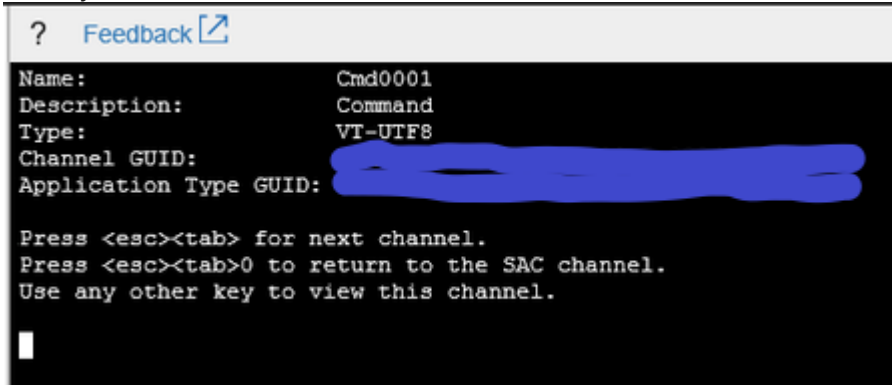
1. If EMS does not connect, it means the Guest OS was not setup to use this feature:
 1. If the issue that you have will repro on a restart and if the customer is OK to enable this feature, you enable this feature. For details refer to [Serial Console](#) on the *How to enable this feature*
 2. If on 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
SAC>
```

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



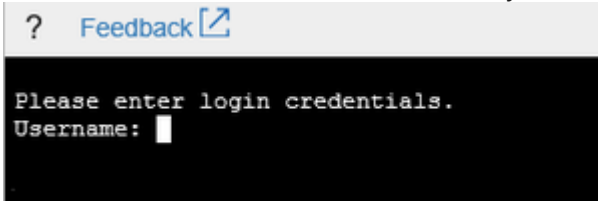
```

? Feedback
Name: Cmd0001
Description: Command
Type: VT-UTF8
Channel GUID: [REDACTED]
Application Type GUID: [REDACTED]

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:



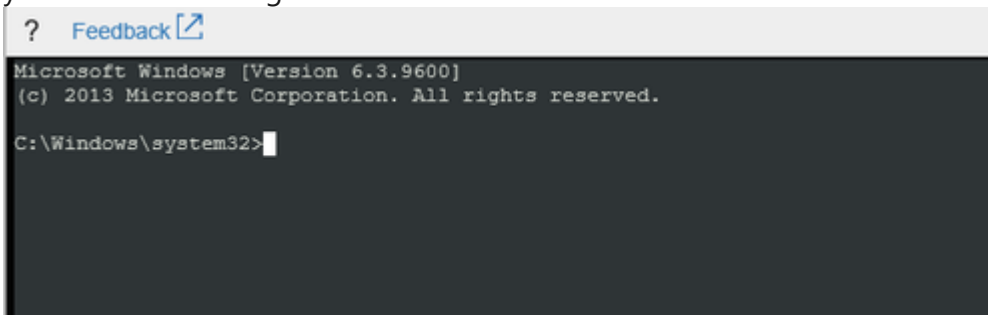
```

? Feedback
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 use domains IDs however this will work if only the credentials are cached on the VM. In this scenario, it 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:



```

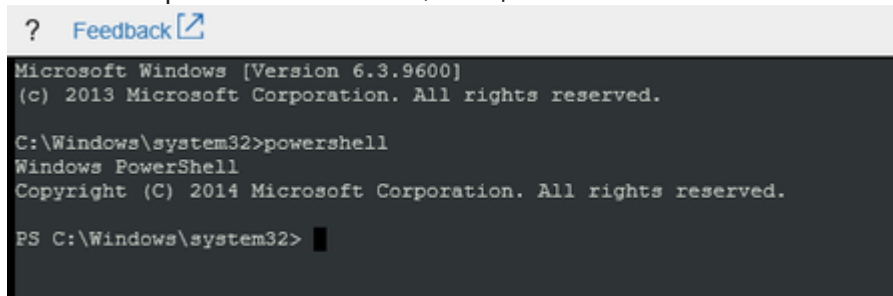
? Feedback
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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`



```

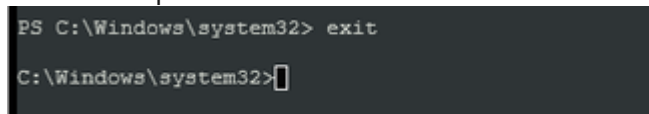
? Feedback
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

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

1. Open a CMD instance and based on the status of the service you are troubleshooting, you will act differently. Start by getting the current state of your service:


```
sc query <SERVICE NAME>
```

1. If the service status shows *Starting* or *Stopping*, then refer to *Service is in a hung state* section
2. If the service is *stopped*, then refer to the *Service is stopped* section

Service is in a hung state

1. If the service is hung on *starting/stopping* then try to stop the service first:

```
sc stop <SERVICE NAME>
```


1. If you can do it successfully, see if you can start it again normally. If you can then there may be a timing issue with other services.
2. If it repro, then go ahead and collect a dump of the process in that state:
 1. Download [Procdump tool](#)  in a new or existing data disk which is attached to a working VM from the same region.
 2. Detach the disk containing the files needed from the working VM and attach to your broken VM. We are calling this disk the *Utility disk*
 3. Then the CMD instance proceed to take a sample of this hang process:

```
procdump.exe -s ''<<Number of seconds apart>>'' -n ''<<Numbers of dumps>>'' -ma ''<<Process
```



- On the example below, we are taking 3 dumps 5sec apart from the nsi

```
procdump.exe -s 5 -n 3 -ma nsi
```

3. Create a [DTM Workspace](#)  and upload these dump files
2. Now engage GES for a dump analysis:

1. Cutting a problem with the following details:

- Product: **Windows Svr 2008 R2 Datacenter** or **Windows Svr 2012 R2 Datacenter** or **Windows Svr 2016 Datacenter** as appropriate
- Support topic: **Routing Windows V3\System Performance\An application or process hangs or crashes**
- Problem Description:

```
===== <start copy> =====
The OS cannot come all the way up due to hanging services
Symptoms description:

SR#
VM name
Service affected
Files uploaded into a DTM workspace
===== <end copy> =====
```

- 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
 - For Professional cases: **Windows EE Pro** queue

2. Follow the Windows EE action plan

Service is stopped

If the service is *stopped* then check if it is because if it is disabled or if it is being stopped gracefully (just stop) or ungracefully (crash).

1. Query which is the configuration of the service

```
sc qc <SERVICE NAME>
```

2. If the *START TYPE* is disabled, then change this to its default value. Check on the *Service Reference* section to know which is the default startup mode.

1. If you want to set the service to *Automatic*, then:

```
sc config <SERVICE NAME> start= auto
```

2. If you want to set the service to *Manual*, then:

```
sc config <SERVICE NAME> start= demand
```

3. If the startup is not *disabled*, then see if the service is crashing or if it was gracefully stopped:

1. Try to start the service

```
sc start <SERVICE NAME>
```

2. If you start it with no issues, then you may want to recheck all the other binaries/services in charge of the network stack

3. If the service fails with error 5 or access denied error, go to the section where the ***service is stopped due to Access Denied error***

4. If you cannot start and you get an error message that it cannot start due to some required service/driver not started, then:

1. If the service is failing due to a required driver, then at this point it is best to run an SFC to the disk to restore the OS health

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

2. If the service is failing to start due to another service sharing its container is failing then you will need to troubleshoot that other process. To see which is the services dependencies:

```
reg query "HKLM\SYSTEM\CurrentControlSet\services\<SERVICE NAME>" /v DependOnService
```

3. Then you just need to query for the startup of those services/driver and go from there:

```
sc query <SERVICE NAME>
```

4. If the service runs into a shared SVCHOST container and is failing to start with the error **due to service account error**, then it means that this service startup account is not the same as the other binaries running in the same container. Just check which is the correct account to set it up on a working machine and then update this in your service as the following:

```
reg add "HKLM\SYSTEM\CurrentControlSet\services\<SERVICE NAME>" /v ObjectName /t REG_SZ /d '
```

5. Enable memory dump

- If after you start it the services crashes, then you'll need to collect a memory dump of that crash:
 1. Ensure that *Windows Error Reporting* service is properly setup and if not, set it up:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\LocalDumps" /v DumpFolder /t REG_M
reg add "HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\LocalDumps" /v DumpCount /t REG_DW
reg add "HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\LocalDumps" /v DumpType /t REG_DW
sc config WerSvc start= demand
sc stop WerSvc
sc start WerSvc
```

2. Now that WER is properly set up, go ahead and repro to collect the user mode dump

3. Upload this file into a [DTM Workspace](#) 

4. Engage GES for a dump analysis:

1. Cutting a problem with the following details:

- Product: **Windows Svr 2008 R2 Datacenter** or **Windows Svr 2012 R2 Datacenter** or **Windows Svr 2016 Datacenter** as appropriate
- Support topic: **Routing Windows V3\System Performance\An application or process hangs or crashes**
- Problem Description:

```
===== <start copy> =====
The OS cannot come all the way up due to services that hangs
Symptoms description:

SR#
VM name
Service affected
Files uploaded into a DTM workspace
===== <end copy> =====
```

- 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
- For Professional cases: **Windows EE Pro** queue

2. Follow the Windows EE action plan

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

For Classic VMs

1. Use Phase 1 to mount the OS disk on your rescue VM
2. **PREMITIGATION STEPS TO ENABLE SAC AND CONFIGURE THE DUMP SETUP** Now open an elevated CMD instance and run the following script:

```
REM Load hive
reg load HKLM\BROKENSYSTEM f:\windows\system32\config\SYSTEM

REM Get the current ControlSet from where the OS is booting
for /f "tokens=3" %x in ('REG QUERY HKLM\BROKENSYSTEM\Select /v Current') do set ControlSet=%x
set ControlSet=%ControlSet:~2,1%

REM Suggested configuration to enable OS Dump
set key=HKLM\BROKENSYSTEM\ControlSet00%ControlSet%\Control\CrashControl
REG ADD %key% /v CrashDumpEnabled /t REG_DWORD /d 2 /f
REG ADD %key% /v DumpFile /t REG_EXPAND_SZ /d "%SystemRoot%\MEMORY.DMP" /f
REG ADD %key% /v NMICrashDump /t REG_DWORD /d 1 /f

REM Unload the hive
reg unload HKLM\BROKENSYSTEM
```

Note: This will assume that the disk is drive F; if this is not your case, update the letter assignment

3. <<<<<<INSERT MITIGATION>>>>>>

4. Use Phase 2 to reassemble the original VM with the now modified disk

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

1. If the service is hanging [Get a user Mode dump of a hanging process](#)
2. If the service is crashing [Setup a machine for a User-Mode Dump](#)
3. Once you collect the user-mode dump then cut a problem to engage a GES for analysis and follow the action plan from the GES engineer:
 - Product: **Windows Svr 2008 R2** or **Windows Svr 2012 R2 Datacenter** or **Windows Svr 2016 Datacenter** as appropriate
 - Support topic: **Routing Windows V3\System Performance\An application or process hangs or crashes**
 - Problem Description:

```
===== <start copy> =====
The network stack of the VM cannot come all the way up due to a service hang/crashes services up
Symptoms description:

SR#
VM name
Service hanging
===== <end copy> =====
```



- 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
 - For Professional cases: **Windows EE Pro** queue
- 4. Follow the action plan from the GES engineer and reassemble the VM

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

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?

| <i>To engage the Azure RDP-SSH SMEs...</i> | <i>To provide feedback on this page...</i> | <i>To provide kudos on this page...</i> |
|---|--|---|
| <p>Please reach out to the RDP-SSH SMEs ☑ for faster assistance.</p> <p>Make sure to use the Ava process for faster assistance.</p> | <p>Use the RDP-SSH Feedback form to submit detailed feedback on improvements or new content ideas for RDP-SSH.</p> <p>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.</p> | <p>Use the RDP-SSH Kudos form to submit kudos on the page. Kudos will help us improve our wiki content overall!</p> <p>Please note the link to the page is required when submitting kudos!</p> |