

TermService not Starting_RDP SSH

Last updated by | Heath Rensink | Oct 20, 2022 at 9:01 AM PDT

Tags

cw.TSG

cw.RDP-SSH

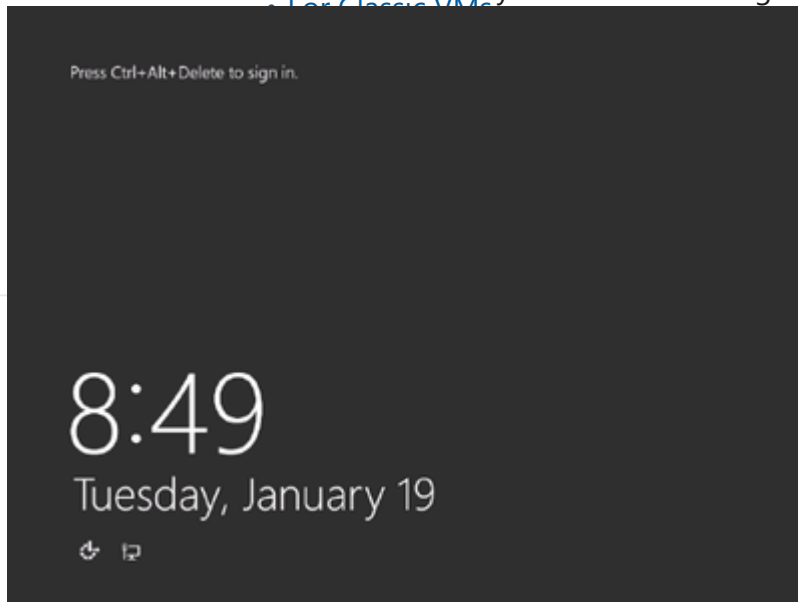
Contents

- Symptoms
- Root Cause Analysis
 - Tracking close code for this volume
- Customer Enablement
- Service Reference
- Refresher / Training Template
- 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
 - TermService service is stopped due to Access Denied error
 - TermService service is crashing/hanging
 - TermService service is disabled
 - TermService service fails due to dependency
 - TermService service fails due to logon failure
 - TermService service different startup account from the shar...
 - 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

- Using OSDisk Swap API
- Using VM Recreation scripts
- For ARM VMs

Symptoms

1. The VM screenshot shows the OS fully loaded and waiting for the credentials



2. In **WinGuestAnalyzer\Health Signal** tab you will see the service is currently in **not Running** state:



3. If you pull the Guest OS Logs, you'll see that Remote Desktop Services (TermServ) is not starting or failing to start. This could be due to a hang or crash of this process.

```

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 Remote Desktop Services service hung on starting.

```

4. It could also be that you don't see any attempt to start this service during the booting time and this would be if the service was indeed disabled.

Root Cause Analysis

The Remote Desktop Service (TermService) is not running on the Virtual Machine. This happen on the following scenarios and the RCA will depend on which of the following:

1. TermService service was set to disabled
2. TermService is crashing, the RCA will depend on the dump from the process.
3. TermService is hanging, , the RCA will depend on the dump from the process.

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\Compute\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

- [Remote Desktop Services is not starting on an Azure VM](#) 

Service Reference

		Windows Server 2008 R2 - Windows 7	Windows Server 2012 - Windows 10
<i>Startup account</i>		NT Authority\NetworkService	NT Authority\NetworkService
<i>Startup Type</i>		Manual (3)	Manual (3)
<i>Service Dependency</i>	<i>Driver - Startup type</i>	TermDD - System (1)	-
	<i>Service - Startup type</i>	RpcSs - Auto (2)	RpcSs - Auto (2)
<i>ImagePath</i>		%SystemRoot%\System32\svchost.exe -k termsvcs	%SystemRoot%\System32\svchost -k termsvcs
<i>Shared Container with</i>		TermService	TermService

Refresher / Training Template

- For the purpose of training or following along with this TSG, you can use the following link or url 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.

1. Lab 1



2. Lab 2



Mitigation

For sections where you need to troubleshoot the problematic process, execute its troubleshooting for the <PROCESS NAME> with **TermService**

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

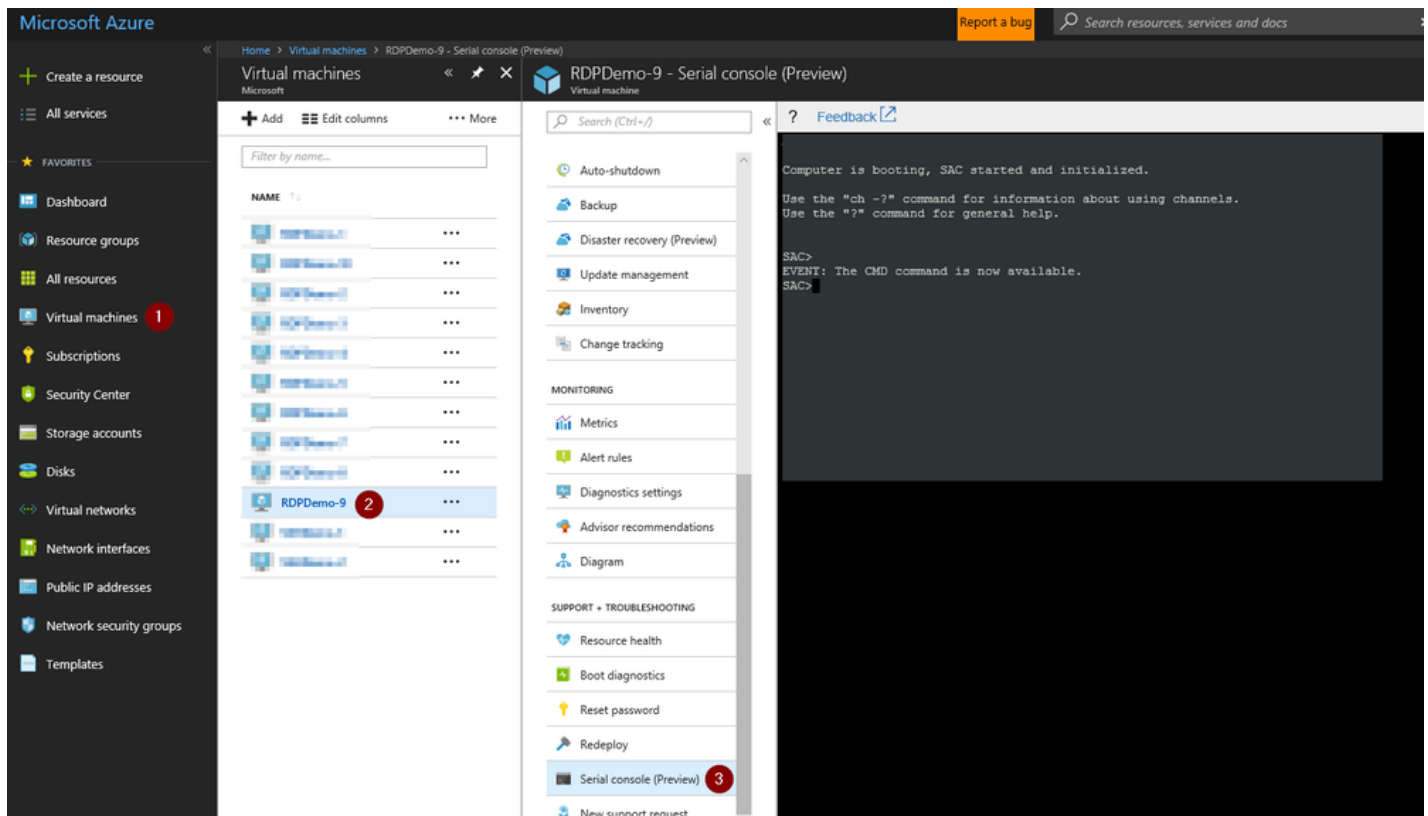
See [How To Access Thru Windows Admin Center](#)

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
```

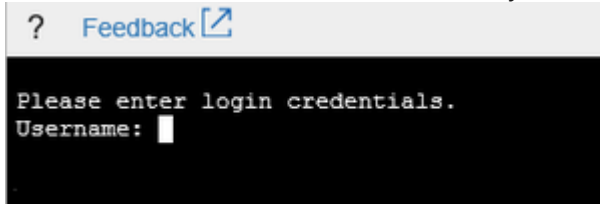
```
SAC>ch -si 1
```

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

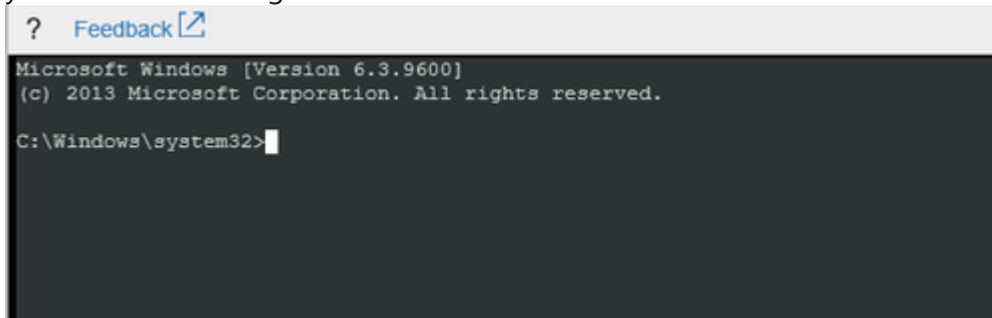
```
? Feedback
Name: Cmd0001
Description: Command
Type: VT-UTF8
Channel GUID: [REDACTED]
Application Type GUID: [REDACTED]

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:

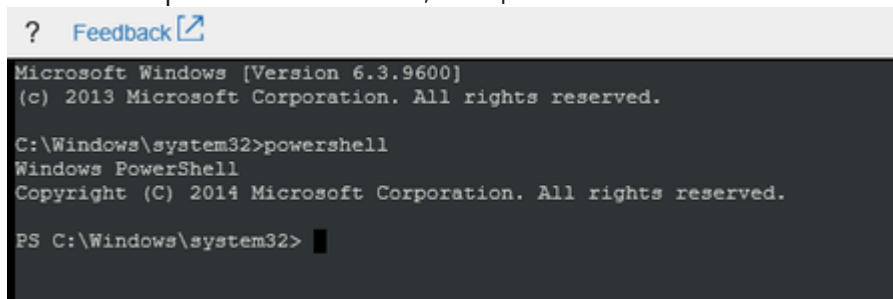


1. If the machine has connectivity, you could use either local or domain IDs. If you want to use a local ID, for domain just add the hostname of the VM
 2. If the machine doesn't have connectivity, you could try to use domains IDs however this will work if only the credentials are cached on the VM. In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

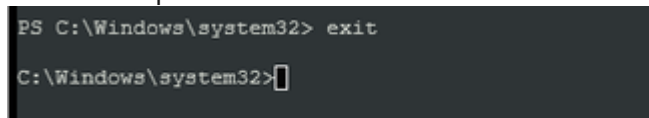


1. At this point, you can do your troubleshooting in bash (CMD) or else, you could start a powershell instance:

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

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 what you see in health signal you are going to act differently. Start by confirming the current state of the service:

```
sc query TermService
```

2. If the service is shown as:

1. *Starting/Stopping*, then refer to the *TermService service is crashing/hanging* section
2. *Stopped*, check if the service was disabled or if it is crashing or getting stopped by some other process
 1. Try to start the service

```
sc start TermService
```

1. If you start it with no issues, then the service was just stopped by some other process before but right now your access was restored
2. If the service fails with error:
 1. *5 - ACCESS DENIED*. Refer to the *TermService service fails due to Access Denied* section
 2. *1053 - ERROR_SERVICE_REQUEST_TIMEOUT*. Refer to the *TermService service is crashing/hanging* section
 3. *1058 - ERROR_SERVICE_DISABLED*. Refer to the *TermService service is disabled* section
 4. *1059 - ERROR_CIRCULAR_DEPENDENCY*. Refer to the *TermService service fails due to dependency* section

5. 1067 - *ERROR_PROCESS_ABORTED*. Refer to the *TermService service is crashing/hanging* section
6. 1068 - *ERROR_SERVICE_DEPENDENCY_FAIL*. Refer to the *TermService service fails due to dependency* section
7. 1069 - *ERROR_SERVICE_LOGON_FAILED*. Refer to the *TermService service fails due to logon failure* section
8. 1070 - *ERROR_SERVICE_START_HANG*. Refer to the *TermService service is crashing/hanging* section
9. 1077 - *ERROR_SERVICE_NEVER_STARTED*. Refer to the *TermService service is disabled* section
10. 1079 - *ERROR_DIFFERENCE_SERVICE_ACCOUNT*. Refer to the *TermService service different startup account from the shared container* section
11. 1753 . Refer to the *TermService service fails due to dependency* section

TermService service is stopped due to Access Denied error

▼ Click here to expand or collapse this section

1. Download the [Process Monitor tool](#) ☐ on this VM by

1. Attaching a remote shared folder as the volume Z:

```
net use z: "<REMOTE_SHARED_FOLDER>" /persistent:no
```

2. Downloading the tool directly from the SAC console. Open a powershell instance and then run:

```
md c:\temp
remove-module psreadline
$source = "https://download.sysinternals.com/files/ProcessMonitor.zip"
$destination = "c:\temp\ProcessMonitor.zip"
$wc = New-Object System.Net.WebClient
$wc.DownloadFile($source,$destination)
```

3. Or attaching an utility disk

2. Now start a procmon trace

```
procmon /Quiet /Minimized /BackingFile c:\temp\ProcMonTrace.PML
```

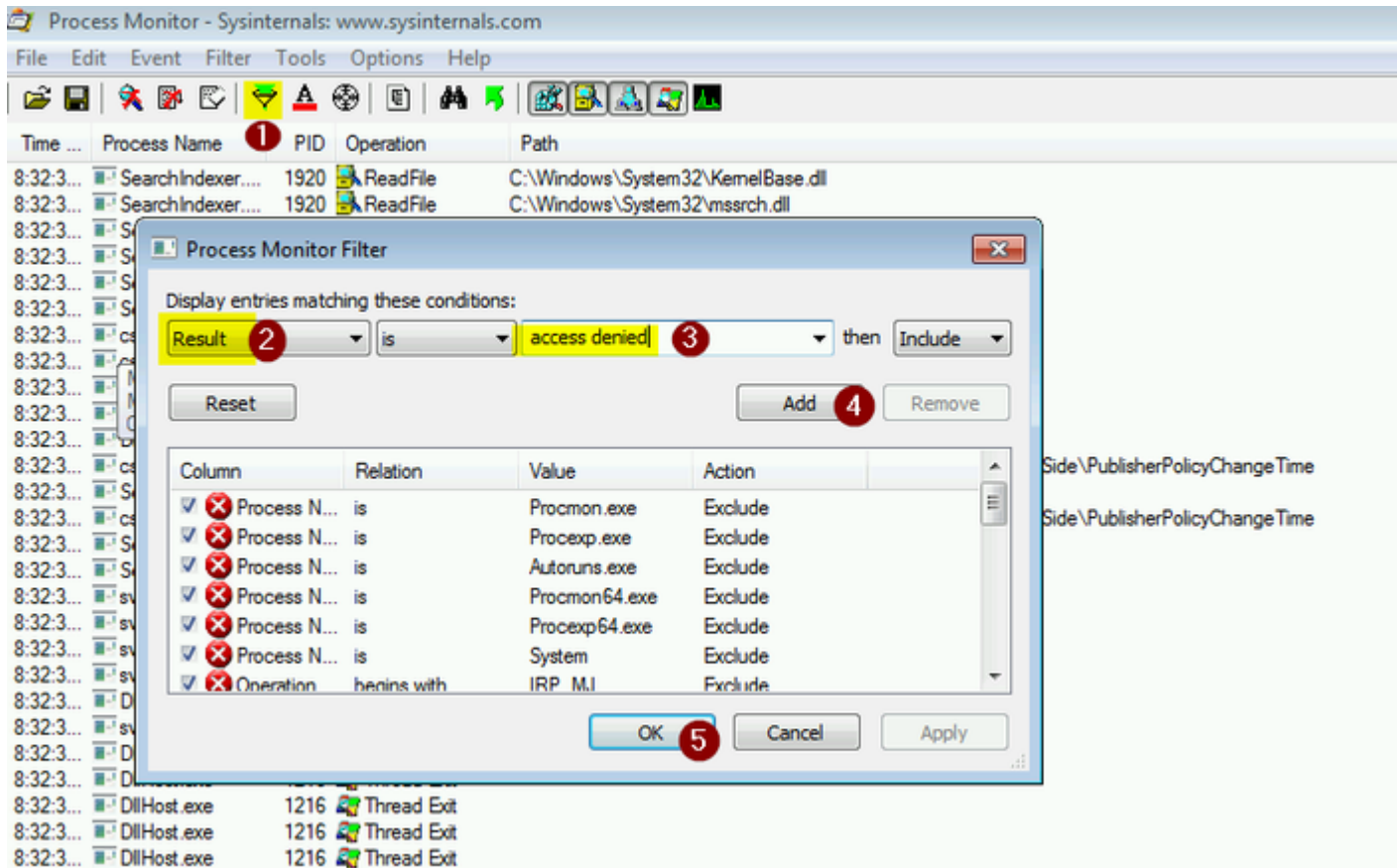
3. Now reproduce the issue which in this case is try to start the service that is giving access deny:

```
sc start <PROCESS NAME>
```

4. When it failed, go ahead and terminate the Process Monitor trace

```
procmon /Terminate
```

5. Collect the file `c:\temp\ProcMonTrace.PML` and open it up on procmon and filter by *Result is ACCESS DENIED*



6. Now fix the registry or folder/files that is on the output. Usually this is a lack of access from the logon account used on the service for those entries. To know which is the correct ACL you can check on a healthy machine.

1. For folder/files you can use SAC to change this by working with the `takeown` and `icacls` commands
2. For registry, you can use SAC as well to modify this permissions on an elevated powershell instance:
 1. Run the following script:

```
$registry = "HKLM:\"+<SPECIFY THE REST OF THE REGISTRY PATH>
$id = "<MISSING ID>" #This could be like "NT AUTHORITY\SYSTEM" for the built-in SYSTEM accou

#Load the current ACL object of your registry
$acl = Get-Acl $registry

#Create the new ACL with the missing access
$rule = New-Object System.Security.AccessControl.RegistryAccessRule ($id,"FullControl","Allc

#Modify the ACL object and update the registry with the new ACL object
$acl.SetAccessRule($rule)
$acl | Set-Acl -Path $registry
```

2. If you get the error *Requested registry access is not allowed*, then it means that you will also need to update the ownership of the registry. Doing this on SAC is a bit complicated so it is better to work in offline:

1. Shutdown the VM


2. Get a copy of the VHD (snapshot)
3. Attach this copy on a rescue VM
4. Mount the hive on regedit (like BROKENSYSYSTEM/BROKENSOFTWARE)
5. Then use the registry editor GUI by doing right click over the registry and selecting *Permissions*
6. Then proceed normally as if you are working with File/Folders
7. Once this is complete, unload the hive and detach the disk
8. Swap your modified disk with the original disk
9. Turn on the VM

TermService service is crashing/hanging

▼ Click here to expand or collapse this section

1. If the service status is stuck in *Starting/Stopping*, then try to stop the service:

```
sc stop <PROCESS 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 but for now the issue is mitigated. Monitor this service to see if it crashes again over time.
2. Collect a user mode dump from this process:
 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 NAME>''
```

- 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

4. 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 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

TermService service is disabled

▼ Click here to expand or collapse this section

1. Change the service configuration to its default value. Check on the *Service Reference* section to know which is the default startup type:

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

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

or

```
Set-Service "PROCESS NAME" -StartupType Automatic
```

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

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

or

```
Set-Service "PROCESS NAME" -StartupType Manual
```

2. Now just start the service

```
sc start <PROCESS NAME>
```

or

```
Start-Service "PROCESS NAME"
(Get-Service "PROCESS NAME").DependentServices | Restart-Service -Force
```

3. Now query its status once again to ensure the service is running:

```
sc query <PROCESS NAME>
```

or

```
Get-Service "PROCESS NAME"
```

4. Retry your access

TermService service fails due to dependency

▼ Click here to expand or collapse this section

Check on the *Service Reference* section which are the services/drivers that you have as dependency, then you will need to troubleshoot ***each of them*** following this logic:

1. Query which is the current state of the process:

```
sc query <PROCESS NAME>
```

2. If the process is stop then:

1. Validate the process was not disabled:

1. Get the process configuration:

```
sc qc <PROCESS NAME>
```

2. If *START_TYPE* is shown as disabled, then just change this settings to its default. Refer to the *Service Reference* section to know which is the default startup value:

```
sc config <PROCESS NAME> start= <DEFAULT VALUE>
```

3. Restart your VM so the every service dependent to this process, will start now in the proper order

4. Retry your access

2. If you ruled out if the process was disabled, then checking from the *Service Reference* section:

1. If the process that is not starting is a driver then, it is best to run SFC to ensure the OS is healthy

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

1. If you cannot restore its health, refer to the *Escalation* section

2. If the process is a service, then:

1. Query which are the current service dependency for our process:

```
sc query <PROCESS NAME>
```

2. Now compare this with the Service Reference section to know which are the default service dependencies for this service:

1. If the services listed on *DependOnService* key are the same as the default values as per the chart above, you will need to troubleshoot that separately follow the same logic that you performed in here with every service listed on *DependOnService* key
2. However if you notice some extra service listed on the dependencies from your VM outside of the default values, you could update this with the default value:

```
sc config <PROCESS NAME> depend= "<DEPENDENCIES SEPARATED BY />"
```

3. Restart your VM so the every service dependent to this process, will start now in the proper order
4. Retry your access

3. If you cannot restore its health, refer to the *Escalation* section

TermService service fails due to logon failure

▼ Click here to expand or collapse this section

Check on the *Service Reference* section to get which is the Startup account this service should have.

1. This means that the startup account of this service was changed. Changed this back to its default:

```
sc config <PROCESS NAME> obj= "<DEFAULT VALUE>"
```

or

```
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\<PROCESS NAME>' -name "ObjectName" -value
```



2. Now start the service

```
sc start <PROCESS NAME>
```

or

```
Start-Service "PROCESS NAME"
(Get-Service "PROCESS NAME").DependentServices | Restart-Service -Force
```

3. Retry your access

TermService service different startup account from the shared container

▼ Click here to expand or collapse this section

Refer to the *Service Reference* section to get which is the Startup account and ImagePath key value this service should have.

1. This means that the startup account and/or the container environment from the service was changed.
Changed this back to its default values:

```
sc config <PROCESS NAME> obj= <STARTUP ACCOUNT>
sc config <PROCESS NAME> binPath= "<IMAGEPATH VALUE>"
```

2. Now start the service

```
sc start <PROCESS NAME>
```

3. Retry your access

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

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. Now open an elevated CMD and run the following script:

1. Please refer to the *Service Reference* section to get the following details to complete these on the script below:

- `<STARTUP TYPE>` (Note: use the number only, not the whole string. Use 2, not Automatic (2))
- `<IMAGE PATH>`
- `<STARTUP ACCOUNT>`
- `<DRIVER/SERVICE NAME>` if applies

2. For `<PROCESS NAME>`, this is referred right under the *Mitigation* section

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

```
REM Set default values back on the broken service
```

```
reg add "HKLM\BROKENSYSTEM\ControlSet001\services\<PROCESS NAME>" /v start /t REG_DWORD /d <STARTUP TYPE>
reg add "HKLM\BROKENSYSTEM\ControlSet001\services\<PROCESS NAME>" /v ImagePath /t REG_EXPAND_SZ /d "<IMAG
reg add "HKLM\BROKENSYSTEM\ControlSet001\services\<PROCESS NAME>" /v ObjectName /t REG_SZ /d "<STARTUP AC
reg add "HKLM\BROKENSYSTEM\ControlSet001\services\<PROCESS NAME>" /v type /t REG_DWORD /d 16 /f
```

```
reg add "HKLM\BROKENSYSTEM\ControlSet002\services\<PROCESS NAME>" /v start /t REG_DWORD /d <STARTUP TYPE>
reg add "HKLM\BROKENSYSTEM\ControlSet002\services\<PROCESS NAME>" /v ImagePath /t REG_EXPAND_SZ /d "<IMAG
reg add "HKLM\BROKENSYSTEM\ControlSet002\services\<PROCESS NAME>" /v ObjectName /t REG_SZ /d "<STARTUP AC
reg add "HKLM\BROKENSYSTEM\ControlSet002\services\<PROCESS NAME>" /v type /t REG_DWORD /d 16 /f
```

```
REM Enable default dependencies from the broken service
```

```
reg add "HKLM\BROKENSYSTEM\ControlSet001\services\<DRIVER/SERVICE NAME>" /v start /t REG_DWORD /d <STARTU
reg add "HKLM\BROKENSYSTEM\ControlSet002\services\<DRIVER/SERVICE NAME>" /v start /t REG_DWORD /d <STARTU
```

```
reg unload HKLM\BROKENSYSTEM
```

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

After starting the server, you can run `sc qc <PROCESS NAME>` to verify the settings:

[https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc742055\(v=ws.11\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc742055(v=ws.11)) ☐

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 - RDP 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>