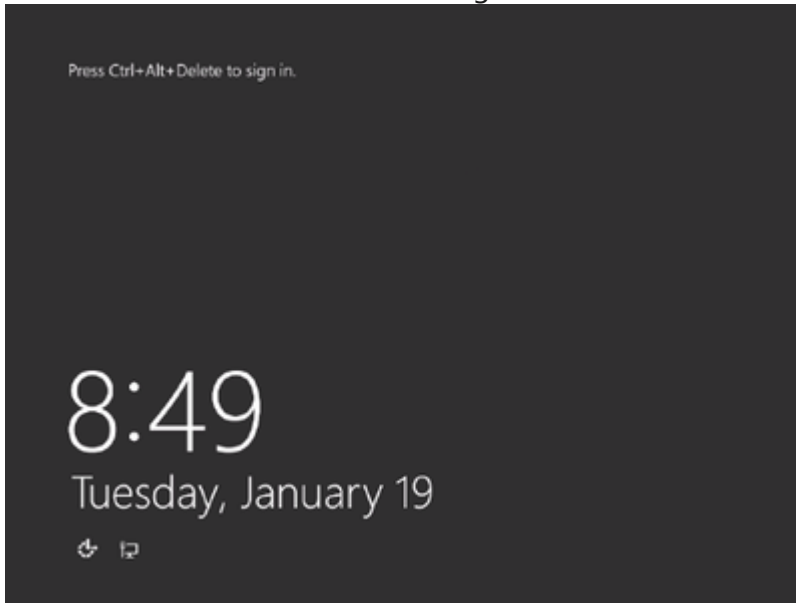


Contents

- Symptoms
- Root Cause Analysis
 - Tracking close code for this volume
- Refresher / Training Template
- Service Reference
- 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
 - ONLINE Mitigations
 - BFE service is stopped due to Access Denied error
 - BFE service is crashing/hanging
 - BFE service is disabled
 - BFE service fails due to dependency
 - BFE service fails due to logon failure
 - BFE service different startup account from the shared cont...
- 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
 - OFFLINE Mitigations
- Escalate
- After work - Cleanup
- Need additional help or have feedback?

Symptoms

1. As a VM screenshot that is in waiting for credentials:



2. There's no connectivity to the virtual machine on its VIP or DIP or its PA after verifying with [VM Port Scanner](#).
3. In **WinGuestAnalyzer\Health Signal** tab you will see the service is currently in **Stopped** state:



4. In the GuestOS log, you could either not see the event, meaning that was disabled, or see it crashing/hanging abruptly or just getting stopped:


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.

Root Cause Analysis

The Base Filtering Engine service is not running on the Virtual Machine. This happen on the following scenarios and the RCA will depend on which of the following:

1. service was set to disabled
2. is crashing, the RCA will depend on the dump from the process.
3. is hanging, the RCA will depend on the dump from the process.
4. Another required service is not running, the RCA will depend on why the other service was not starting

Tracking close code for this volume

Root Cause	Product	Support Topic	Cause Tracking code	Bug
1	Azure Virtual Machine  Windows	<i>Routing Azure Virtual Machine V3\Cannot Connect to my VM\Failure to connect using RDP or SSH port</i>	<i>Root Cause - Windows Azure\Virtual Machine\Guest OS - Windows\Isolated\Windows Services not starting/crashing</i>	

To know how to flag a bug on a case please refer to [How to do Proper Case Coding](#)

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.



Service Reference

		Windows Server 2008 R2 - Windows 7	Windows Server 2012 - Windows 8
<i>Startup account</i>		NT AUTHORITY\LocalService	NT AUTHORITY\LocalService
<i>Startup Type</i>		Automatic (2)	Automatic (2)
<i>Service Dependency</i>	<i>Driver - Startup type</i>	-	WfpLwfs - Boot (0)
	<i>Service - Startup type</i>	RpcSs - Auto (2)	RpcSs - Auto (2)
<i>ImagePath</i>		%systemroot%\system32\svchost.exe -k LocalServiceNoNetwork -p	%systemroot%\system32\svchost.exe -k LocalServiceNoNetwork -p
<i>Shared Container with</i>		DPS PLA BFE mpssvc	DPS PLA BFE mpssvc

Customer Enablement

N/A

Mitigation

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

Backup OS disk

▼ Click here to expand or collapse this section

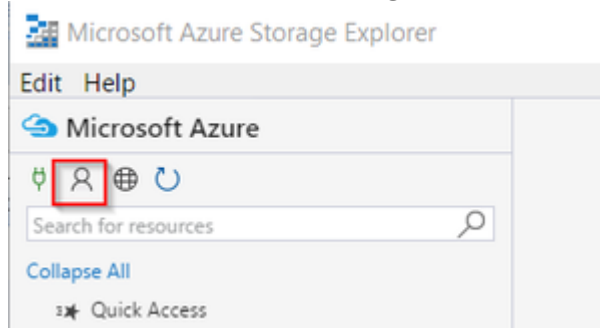
1. Before doing anything, please validate if this is an encrypted VM. On ASC check on the Resource Explorer on the VMCARD for the value *OS Disk Encrypted*

OS Disk Lease Id	0d69a55c-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

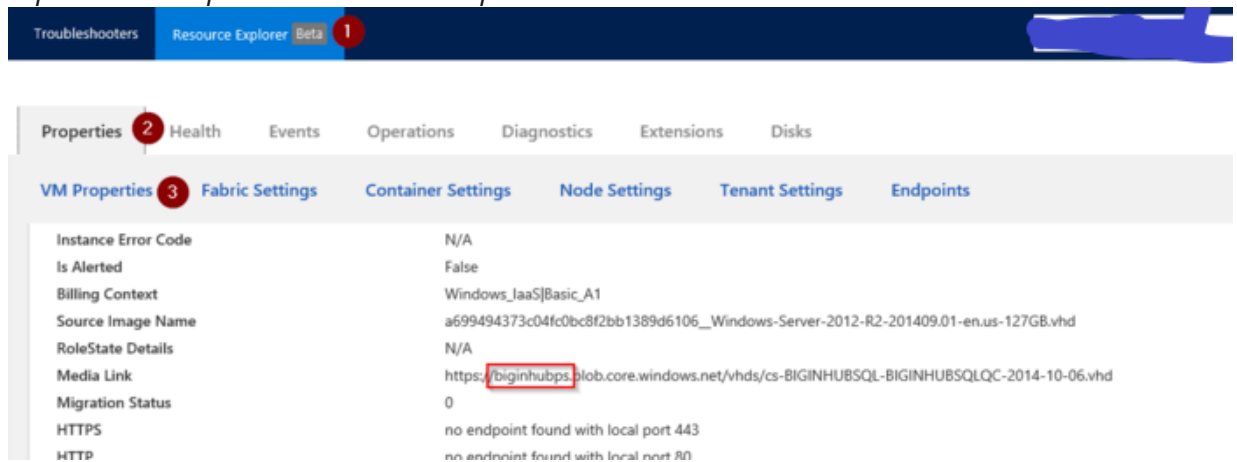
- If the OS Disk is encrypted, then proceed to [Unlock an encrypted disk](#)
- Now proceed to do a copy of the OS disk, this will help in case of a rollback for recovery or RCA in a later stage
- Power the machine down and once it is stopped de-allocated to do the copy.
- Create a snapshot
 - If the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

- Using [Microsoft Azure Storage Explorer](#)

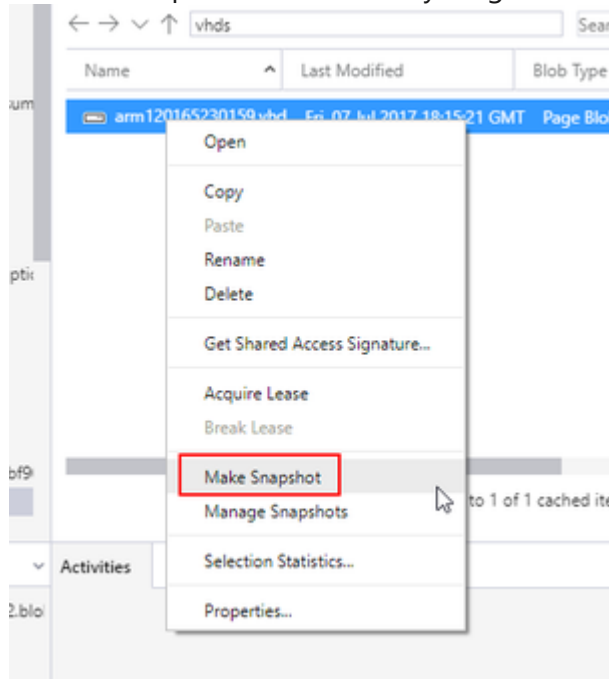
- Once the customer download the tool, proceed to add the Azure account details so you can access the storage accounts
- Click on **Add Account Settings** then ***Add an account...***



- 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)

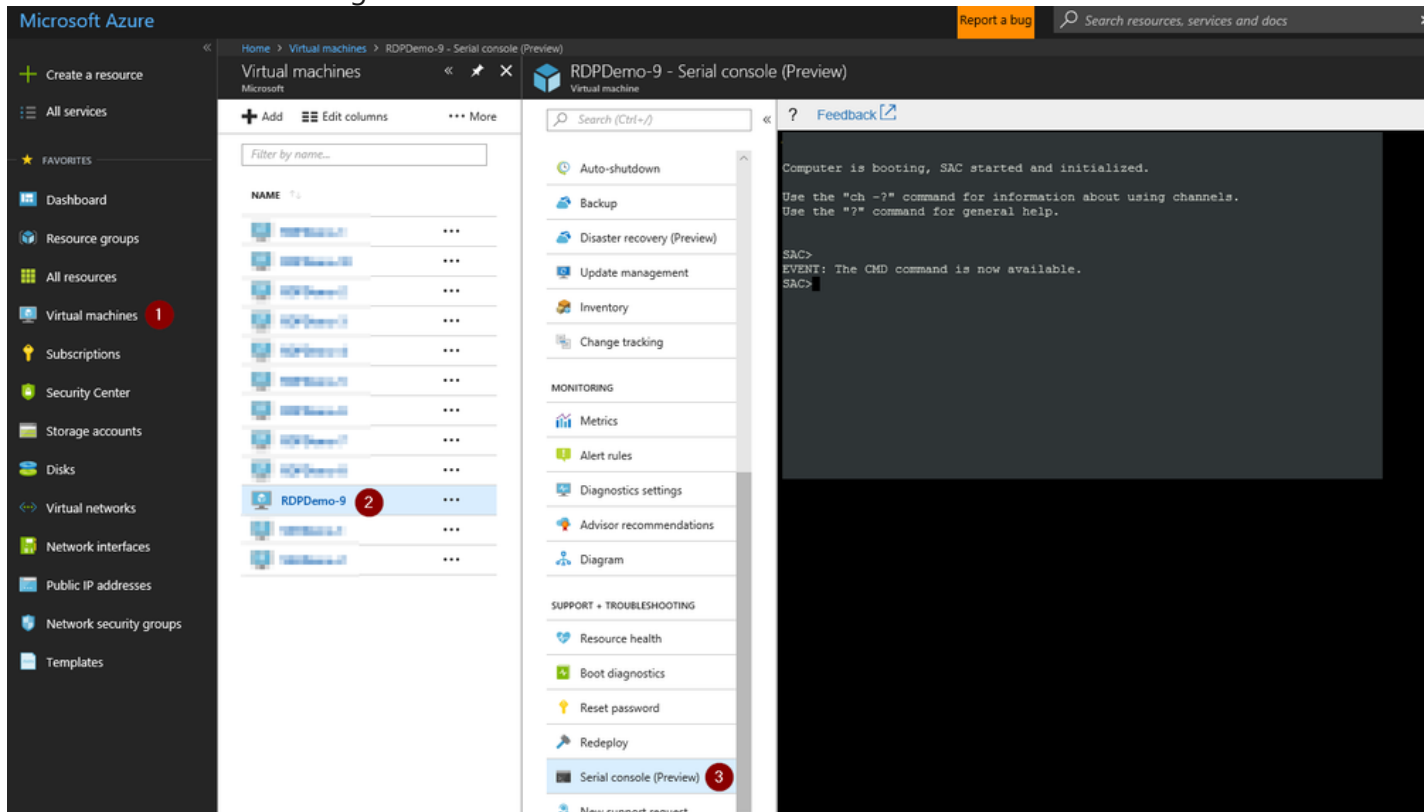
See [How To Access Thru Windows Admin Center](#)

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:



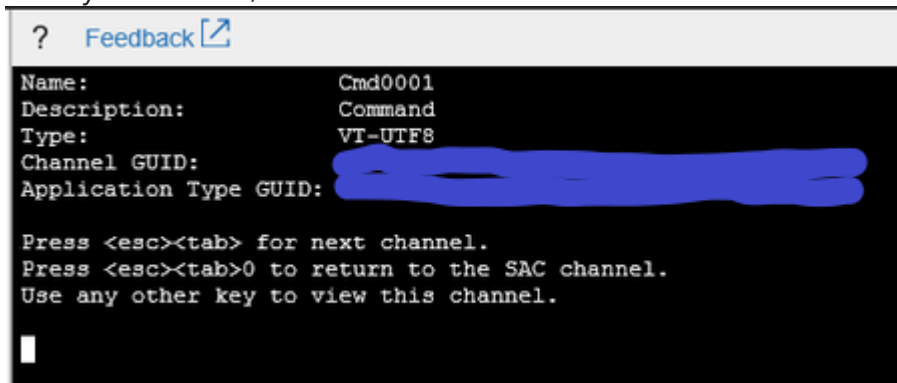
1. If EMS does not connect, it means the Guest OS was not setup to use this feature:
 1. If the issue that you have will repro on a restart and if the customer is OK to enable this feature, you enable this feature. For details refer to [Serial Console](#) on the *How to enable this feature*
 2. If on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

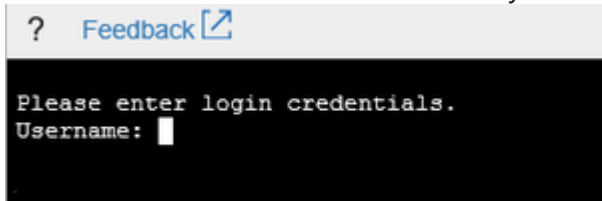


```
? Feedback [link]
Name: Cmd0001
Description: Command
Type: VT-UTF8
Channel GUID: [redacted]
Application Type GUID: [redacted]

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:

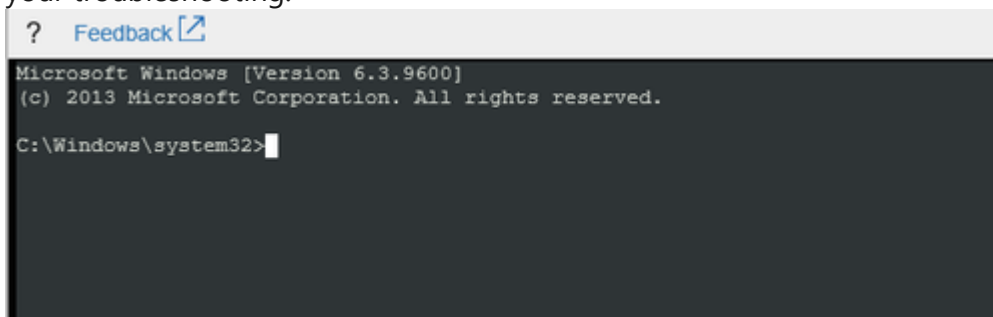


```
? Feedback [link]

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:



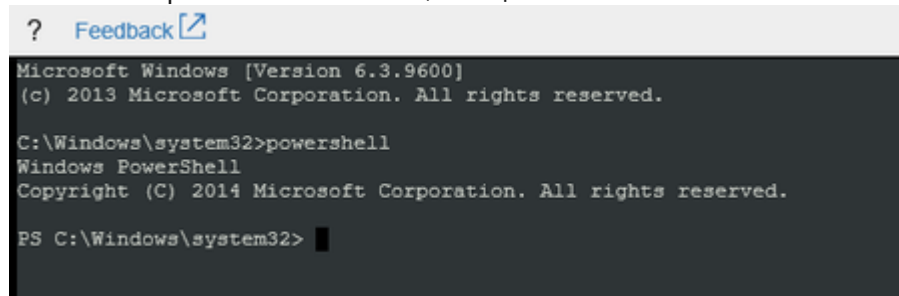
```
? Feedback [link]

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`



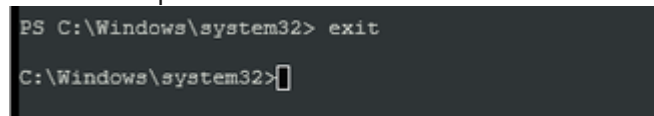
```
? Feedback [link]

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

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 bfe
```

2. If the service is shown as:

1. *Starting/Stopping*, then refer to the *BFE 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 bfe
```

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 *BFE service fails due to Access Denied* section
 2. 1053 - *ERROR_SERVICE_REQUEST_TIMEOUT*. Refer to the *BFE service is crashing/hanging* section
 3. 1058 - *ERROR_SERVICE_DISABLED*. Refer to the *BFE service is disabled* section
 4. 1059 - *ERROR_CIRCULAR_DEPENDENCY*. Refer to the *BFE service fails due to dependency* section
 5. 1067 - *ERROR_PROCESS_ABORTED*. Refer to the *BFE service is crashing/hanging* section
 6. 1068 - *ERROR_SERVICE_DEPENDENCY_FAIL*. Refer to the *BFE service fails due to dependency* section
 7. 1069 - *ERROR_SERVICE_LOGON_FAILED*. Refer to the *BFE service fails due to logon failure* section

8. 1070 - *ERROR_SERVICE_START_HANG*. Refer to the *BFE service is crashing/hanging* section
9. 1077 - *ERROR_SERVICE_NEVER_STARTED*. Refer to the *BFE service is disabled* section
10. 1079 - *ERROR_DIFFERENCE_SERVICE_ACCOUNT*. Refer to the *BFE service different startup account from the shared container* section
11. 1753 . Refer to the *BFE service fails due to dependency* section

BFE 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
```

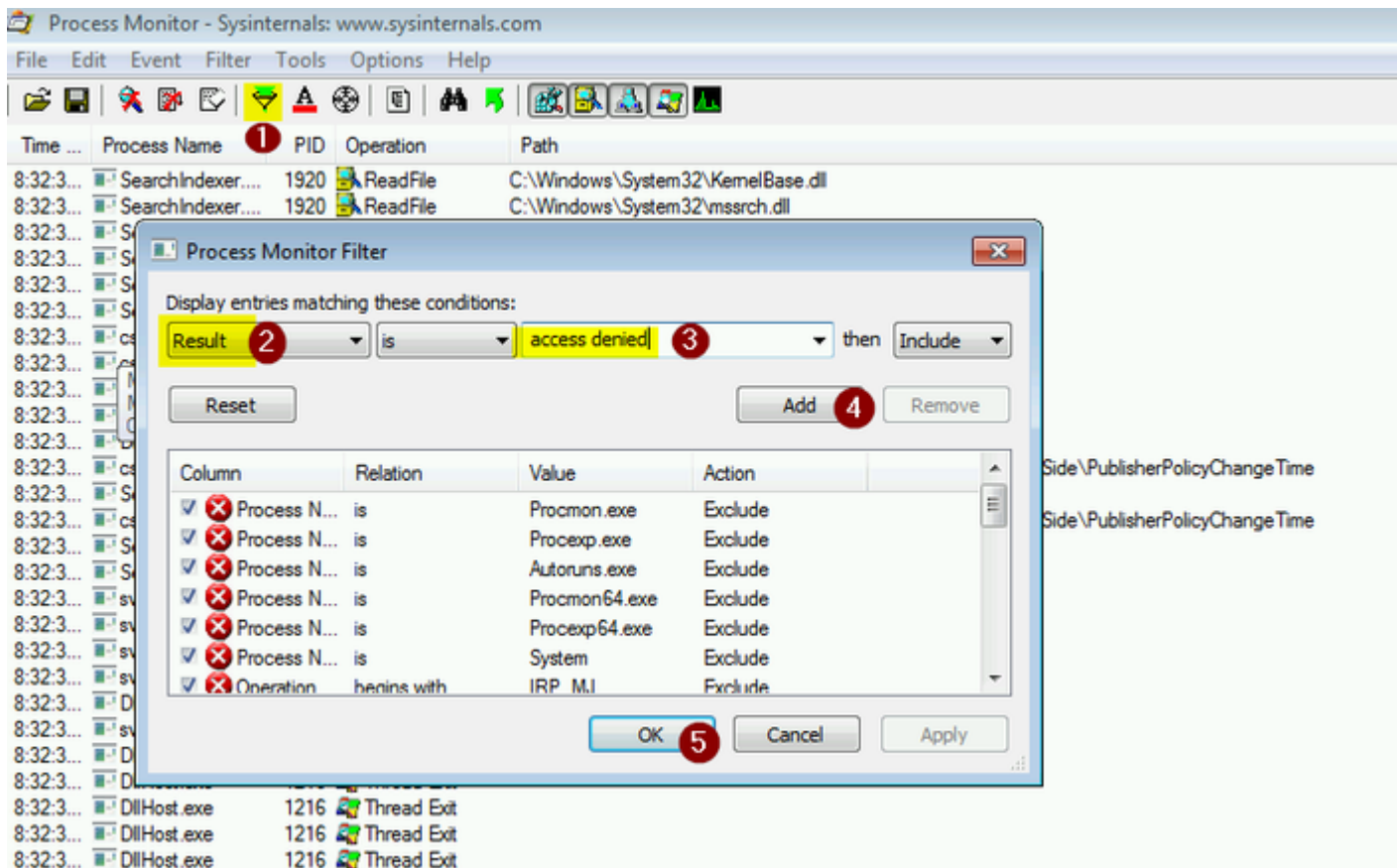
3. Now reproduce the issue which in this case is try to start the service that is giving access deny:

```
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 account

#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","Allow")

#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

BFE 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: