Contents

Symptoms

1. The OS is Windows Server 2016 Datacenter or Windows 10

2. There's no connectivity to the virtual machine on its VIP or DIP or its PA verified with VM Port Scanner.

3. The VM screenshot shows that the OS is fully loaded but there's no network.

4. In ***WinGuestAnalyzer\Health Signal*** tab on the *NetworkAdapter* section, you will find the interface disconnected:


```
[
  {
    "reportTime": "2017-09-21T14:54:53.3972862Z",
    "networkAdapters": [
      {
        "name": "Microsoft Hyper-V Network Adapter #3",
        "status": "Media Disconnected",
        "macAddress": "00-0D-3A-19-D0-16",
        "ipProperties": [
          {
            "protocolVersion": 4,
            "address": "0.0.0.0",
            "isDhcpEnabled": true
          },
          {
            "protocolVersion": 6,
            "address": "0.0.0.0",
            "isDhcpEnabled": true
          }
        ]
      },
```


5. If the OS is Build ***14393*** (RS1) you may on the system logs an event as the following:

```
Time:     3/14/2017 6:09:25 PM
ID:       19
Level:    Information
Source: Microsoft-Windows-WindowsUpdateClient
Machine:  AlfaServer
Message:  Installation Successful: Windows successfully installed the following update: Cumulative Up
```

Note: Or the same type of events from KB3209835 or KB3216755

6. There's no event to track if the image is a Windows Creator version which is build **15063** (RS2) so ask the customer directly if they have upgraded to or installed a Windows Creator image.

Root Cause Analysis

The driver **netvsc.sys** on the guest is on a version that brings a condition where the Guest OS (Windows 10 or Windows Server 2016) cannot interact with a Hyper-V 2016 Host. This could happen in two scenarios:

1. RS1: If the image was an RTM version, then any of the updates **KB3213986**, **KB3209835** or **KB3216755** was installed on the VM bringing that upgrading to that specific version
2. RS2: For Windows 10 VM's, either VM was upgraded or was deployed from an image with the **Windows Creator update** or was directly a **Windows Creator** image

Internal RCA

The following file versions of the file **c:\windows\system32\drivers\netvsc.sys** is either version ***10.0.14393.594*** or ***10.0.15063.0*** requires a feature on the Hyper-V 2016 host to use the Media Sense feature which in Azure, that is disabled to then be able to use VMPHU.

If the driver **c:\windows\system32\drivers\netvsc.sys** is version

- In Build 14393 - RS1: ***10.0.14393.594***, then the bug associated with this is

```
OS Bug 10564224
```

- In Build 15063 - RS2: ***10.0.15063.0***, then the bug is

```
OS Bug 10887629
```

References

- Further details are described in Compatibility update for upgrading to and recovering Windows 10 Version 1703: April 25, 2017
- Leverage DISM on Azure VM troubleshooting

Tracking close code for this volume

Root Cause	Product	Support Topic	Cause Tracking code	Bug
Build 14393 - RS1	*Azure Virtual Machine – Windows*	**For existing VMs:** *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\No Nic\NIC Disconnected status*	*OS 10564224*
	Azure Virtual Machine – Windows	**For new migrated machines:** *Routing Azure Virtual Machine V3\Cannot create a VM\I need guidance preparing an image*	*Root Cause - Windows Azure\Virtual Machine\Guest OS - Windows\Non-Boot\Windows Update Issues\Lack of preparation prior migration - Missing required Patch level*	*OS 10564224*
Build 15063 - RS2	*Azure Virtual Machine – Windows*	**For existing VMs:** *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\No Nic\NIC Disconnected status*	*OS 10887629*
	Azure Virtual Machine – Windows	**For new migrated machines:** *Routing Azure Virtual Machine V3\Cannot create a VM\I need guidance preparing an image*	*Root Cause - Windows Azure\Virtual Machine\Guest OS - Windows\Non-Boot\Windows Update Issues\Lack of preparation prior migration - Missing required Patch level*	*OS 10887629*

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

Customer Enablement

- Cannot connect remotely to a Windows 10 or Windows Server 2016 VM in Azure because of netvsc.sys

Mitigation

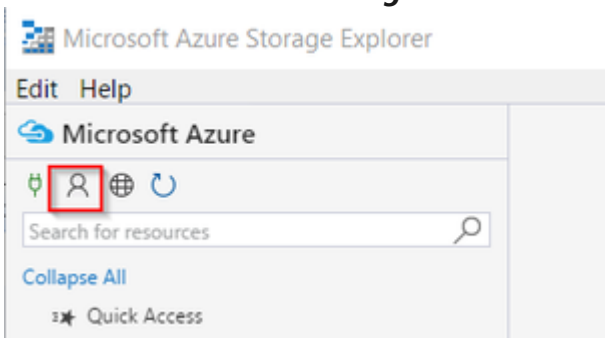
Backup OS disk

▼ Click here to expand or collapse this section

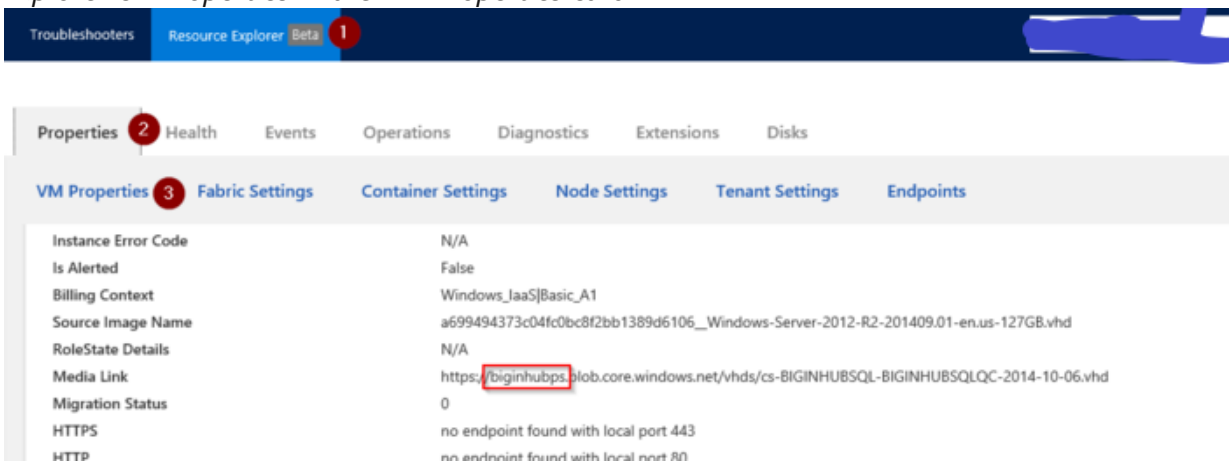
1. Before doing anything, please validate if this is an encrypted VM. On ASC check on the Resource Explorer on the VMCard for the value *OS Disk Encrypted*

OS Disk Lease Id	0db9a55c-0317-40fa-a032-61f3550f3775
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

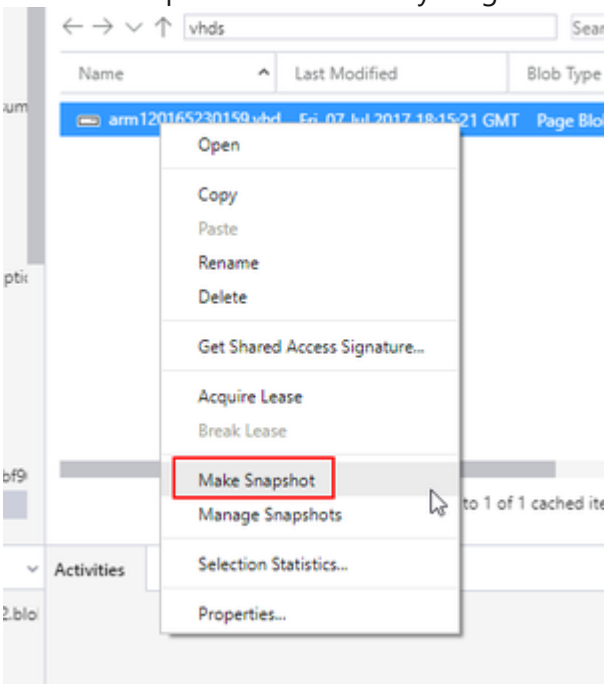
2. If the OS Disk is encrypted, then proceed to Unlock an encrypted disk
3. Now proceed to do a copy of the OS disk, this will help in case of a rollback for recovery or RCA in a later stage
4. Power the machine down and once it is stopped de-allocated to do the copy.
5. Create a snapshot
    1. If the **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

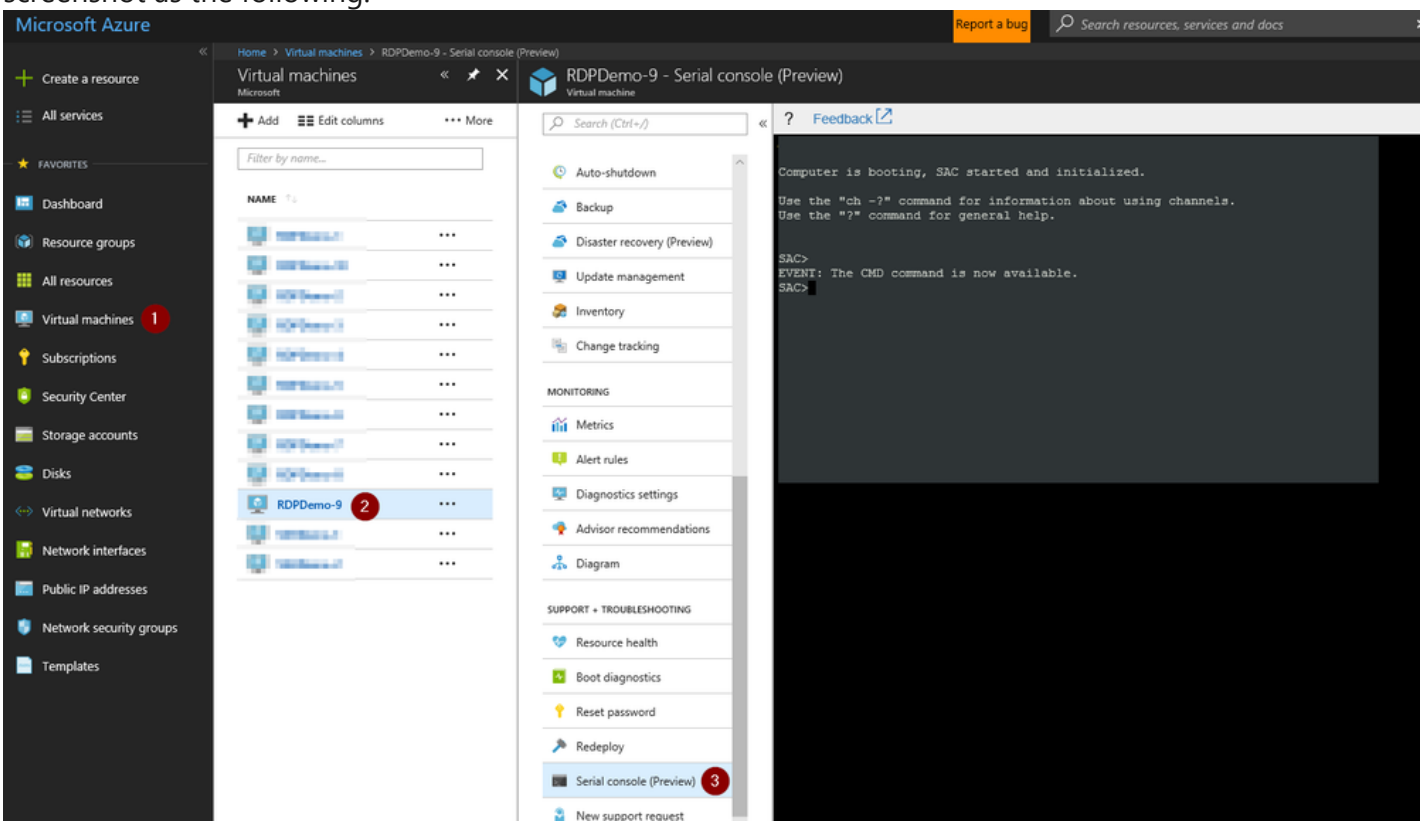
WAC is supported on ARM VMs running Windows Server 2016 or later (not Win10 or any other Windows client version, and not 2012R2/2012/2008R2 versions of Windows Server

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

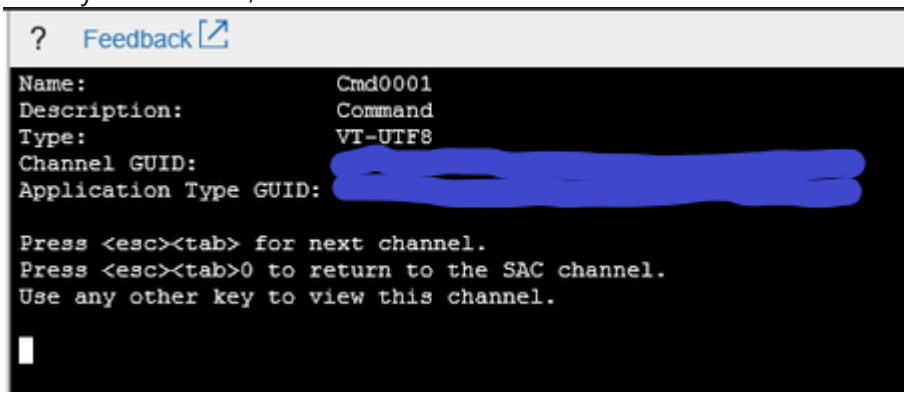
```
SAC>cmd
The Command Prompt session was successfully launched.
SAC>
EVENT:   A new channel has been created.  Use "ch -?" for channel help.
Channel: Cmd0001
SAC>
```

4. Switch to the channel running the CMD instance

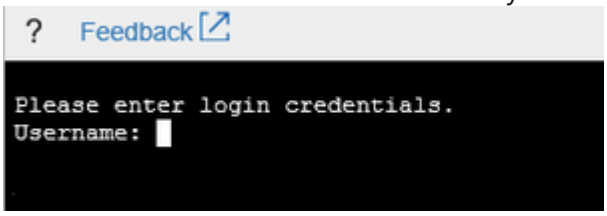
   `ch -si 1`

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

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



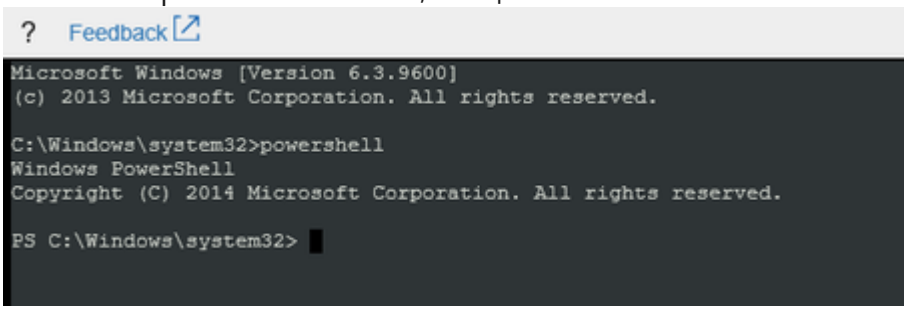
6. Hit enter a second time and it will ask you for user, domain and password:



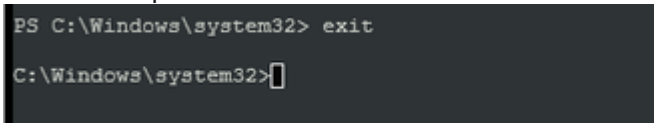
    1. If the machine has connectivity, you could use either local or domain IDs. If you want to use a local ID, for domain just add the hostname of the VM
    2. If the machine doesn't have connectivity, you could try to se domains IDs however this will work if only the credentials are cached on the VM.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

▼ Click here to expand or collapse this section

1. Get the version of the file **c:\windows\system32\drivers\netvsc.sys**
    1. On a *Powershell* instance run:

```
(get-childitem "$env:systemroot\system32\drivers\netvsc.sys").VersionInfo.FileVersion
```

2. Now base on the driver version, we see which KB needs to be download:
    1. For version ***10.0.14393.594*** then
        1. The KB4073562 was released to fix this issue so you could install this one or a newer.
        2. Download either Download KB4073562 or a newer KB on the machine. If you prefer install the latest KB on that driver check Query for KB or a driver history
    2. For version ***10.0.15063.0*** then
        1. This version has a bug so this binary needs to be updated with a *newer version*. To know the latest KB on that driver check Query for KB or a driver history
3. Download this KB in a new or existing data disk which is attached to a working VM from the same region.
4. 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*
5. Then on a CMD instance proceed to install the KB you need on the machine:

```
dism /ONLINE /add-package /packagepath:<<UTILITY DISK LETTER>>:\<<KB .msu or .cab>>
```

6. Restart your VM

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

▼ Click here to expand or collapse this section

1. Get the version of the file **c:\windows\system32\drivers\netvsc.sys**
    1. Pull a diagnostics inspect IAAS disk from Azure Support Center
    2. Mount the SYSTEM hive as BROKENSYSTEM and browse to the following location:

        ```
        HKLM\BROKENSYSTEM\ControlSet001\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}
        ```

    3. Now look in every subkey which will have the form ***00x*** and inside each of them you look for the ***DriverDesc*** and displayed the name of your network card as *Microsoft HYPER-V Network Adapter*
    4. Once you identify that, check the property ***DriverVersion*** and this will be the driver version of the network card that the machine is running.
2. Now base on the driver version, we see which KB needs to be download:
    1. For version ***10.0.14393.594*** then
        1. The KB4073562 was released to fix this issue so you could install this one or a newer.
        2. Download either Download KB4073562 or a newer KB on the machine. If you prefer install the latest KB on that driver check Query for KB or a driver history
    2. For version ***10.0.15063.0*** then

    1. This version has a bug so this binary needs to be updated with a *newer version*. To know the latest KB on that driver check Query for KB or a driver history
3. Attach your OS disk as a data disk on a rescue VM where you can download the KB locally
4. Once the disk is attached, install the KB on that OS disk

```
dism /image:<OS Disk letter>:\ /add-package /packagepath:c:\temp\<<KB .msu or .cab>>
```

5. Unmount the hives
6. Detach the disk and reassemble the original 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?

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!