Ghost NIC_RDP SSH

Last updated by | Kalyn George | Jun 21, 2022 at 9:02 AM PDT

Tags

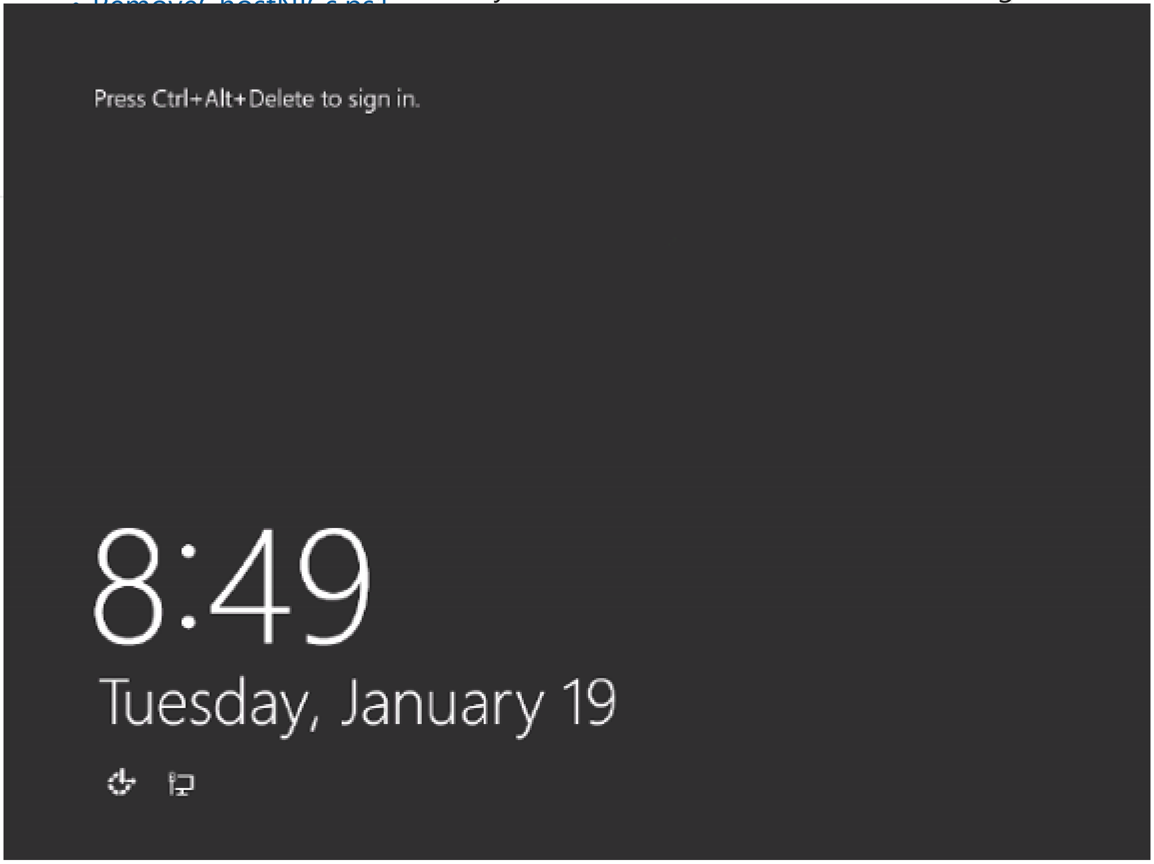
cw.TSG	cw.RDP-SSH

Contents

- FixAzureVM-RemoveNICs.ps1
- DeviceManagement.psd1
- FixAzureVM.cmd
- RemoveGhostNICs.ps1

Symptoms

1. The VM screenshot shows the OS fully loaded at Ctrl+Alt+Del screen waiting for credentials



Press Ctrl+Alt+Delete to sign in.

8:49

Tuesday, January 19

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

3. On the Guest OS logs, you find events like the following

```
Time:     3/17/2016 1:56:28 PM
ID:       11
Level:    Information
Source: Microsoft-Windows-Hyper-V-Netvsc
Machine:  medm-build-2
Message:  Miniport NIC 'Microsoft Hyper-V Network Adapter #4' restarted
```

```
Time:     3/17/2016 1:56:28 PM
ID:       3
Level:    Information
Source: Microsoft-Windows-Hyper-V-Netvsc
Machine:  medm-build-2
Message:  The miniport 'Microsoft Hyper-V Network Adapter #4' was successfully initialized
```

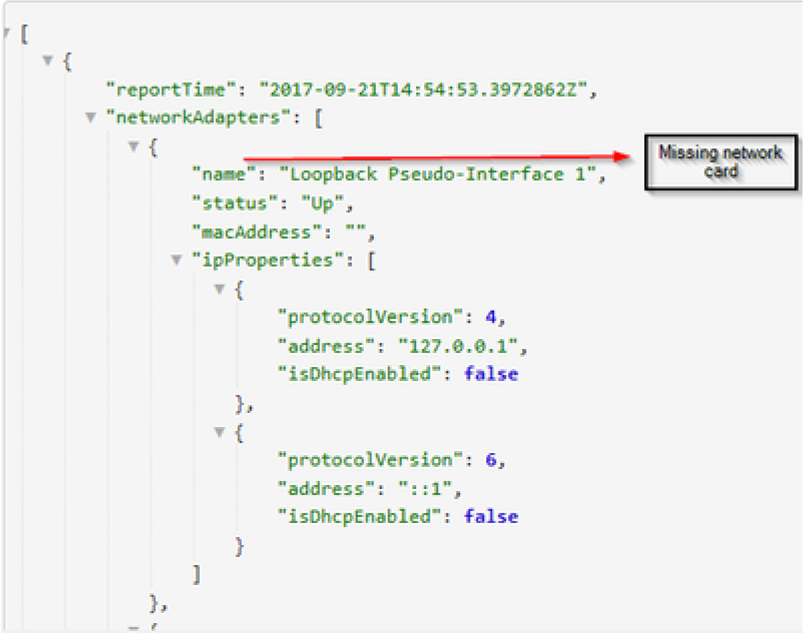
4. You see **UserPnp** event **20001** with **0x5AA**, then vNIC install failure is caused by having **>1,204** ghosted NICs

```
UserPnp Event 20001 0x5AA Log Name: System Source: Microsoft-Windows-UserPnp Date: 3/23/2016 3:32:12
wnetvsc.inf_amd64_59543c94591217e6\wnetvsc.inf for Device Instance ID VMBUS\{F8615163-DF3E-46C5-913F-
```

5. On the Guest OS WaAppAgent.log, you'll see there's no active network card:

```
[00000006] [02/12/2016 01:51:33.09] [ERROR] Failed to obtain fabric URI. ControlSystem not initialize
[00000006] [02/12/2016 01:51:38.28] [INFO]  Initializing ControlSystem.
[00000006] [02/12/2016 01:51:38.28] [ERROR] Did not discover fabric address on any interface. Dumping
[00000038] [02/12/2016 01:51:38.34] [INFO]  ipconfig.exe /all: .
[00000038] [02/12/2016 01:51:38.34] [INFO]  ipconfig.exe /all: Windows IP Configuration.
[00000038] [02/12/2016 01:51:38.34] [INFO]  ipconfig.exe /all: .
[00000038] [02/12/2016 01:51:38.34] [INFO]  ipconfig.exe /all:    Host Name . . . . . . . . . . . . :
[00000038] [02/12/2016 01:51:38.34] [INFO]  ipconfig.exe /all:    Primary Dns Suffix  . . . . . . . :
[00000038] [02/12/2016 01:51:38.34] [INFO]  ipconfig.exe /all:    Node Type . . . . . . . . . . . . :
[00000038] [02/12/2016 01:51:38.34] [INFO]  ipconfig.exe /all:    IP Routing Enabled. . . . . . . . :
[00000038] [02/12/2016 01:51:38.34] [INFO]  ipconfig.exe /all:    WINS Proxy Enabled. . . . . . . . :
[00000038] [02/12/2016 01:51:38.34] [INFO]  ipconfig.exe /all:    DNS Suffix Search List. . . . . . :
[00000038] [02/12/2016 01:51:38.34] [INFO]  ipconfig.exe /all:
[00000038] [02/12/2016 01:51:38.35] [INFO]  ipconfig.exe /all: .
[00000036] [02/12/2016 01:51:38.42] [INFO]  route.exe print: ========================================
[00000036] [02/12/2016 01:51:38.42] [INFO]  route.exe print: Interface List.
[00000036] [02/12/2016 01:51:38.42] [INFO]  route.exe print:   1...........................Software L
[00000036] [02/12/2016 01:51:38.42] [INFO]  route.exe print: ========================================
[00000036] [02/12/2016 01:51:38.42] [INFO]  route.exe print: .
```

6. In ***WinGuestAnalyzer\Health Signal*** tab on the *NetworkAdapters* section, you will not see any active network card:



```
[
  {
    "reportTime": "2017-09-21T14:54:53.3972862Z",
    "networkAdapters": [
      {
        "name": "Loopback Pseudo-Interface 1",
        "status": "Up",
        "macAddress": "",
        "ipProperties": [
          {
            "protocolVersion": 4,
            "address": "127.0.0.1",
            "isDhcpEnabled": false
          },
          {
            "protocolVersion": 6,
            "address": "::1",
            "isDhcpEnabled": false
          }
        ]
      },
```

7. Psping and ping to that VM are timing out

8. No further crashing can be seen on the Guest OS logs

9. On the Azure Portal you find that there's no inbound/outbound network traffic

Root Cause Analysis

The issue is seen because every time a new MAC address is presented to the OS, Windows recognizes this as a new network adapter or the motherboard as a new device. This causes the network adapter or motherboard device to generate a different serial number than the previous network adapter or motherboard device and left former entries on the registry. These can cause different problems, to name some a few of them:

1. Slow startup
2. Different components have different threshold on code that one is reached, the component start to have trouble to work. Some of those components are 'File Share' and network.
3. You could also have problems with the AD communication, etc.

References

- Ghost NIC seen on Windows 7/Windows 2008 R2 machines built from VMWare Templates when the Template uses a Synthetic NIC (VMXNET3)
- Ghost/Hidden Network Interfaces
- Error message when you try to set an IP address on a network adapter

Tracking close code for this volume

Root Cause	Product	Support Topic	Cause Tracking code	Bug
1	*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\Not Valid NIC*	
	Azure Virtual Machine – Windows	**For new migrated VMs:** *Routing Azure Virtual Machine V3\Cannot create a VM\I need guidance preparing an image*	*Azure Virtual Machine - Windows\Compute\Migration\On-prem to azure - ASR*	

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

Customer Enablement

https://docs.microsoft.com/en-us/troubleshoot/windows-server/virtualization/ghost-nic-built-vmware-templates

Prerequisites

- Devcon.zip (x64 & x86) **Note:** If you need to get a newer version you will need to install the Windows Driver Kit

- FixAzureVM-RemoveNICs.ps1
- FixAzureVM.cmd
- RemoveGhostNICs.ps1
- RemoveGhostNICs-Devcon.ps1
    - Information on DeviceManagement.psd1 (incorporated as a module, run `Install-Module -Name DeviceManagement`)
    - If you are seeing encoding errors or "Â" text characters within the script files, please open them in Notepad to copy and paste (or copy and paste from the Scripts section below).

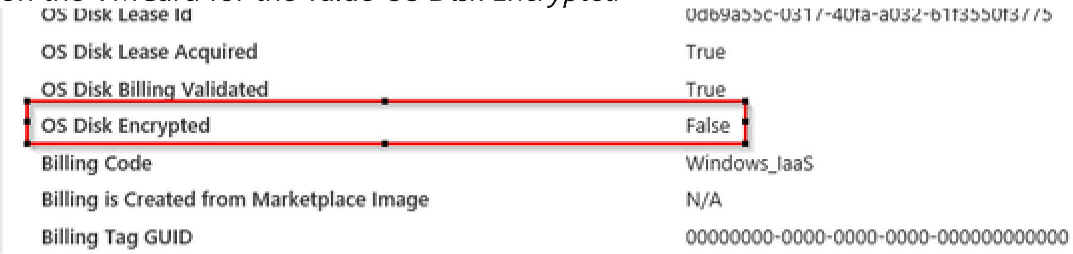
Note: If links are dead, the content of the scripts are in the Scripts section below.

Mitigation

Backup OS disk

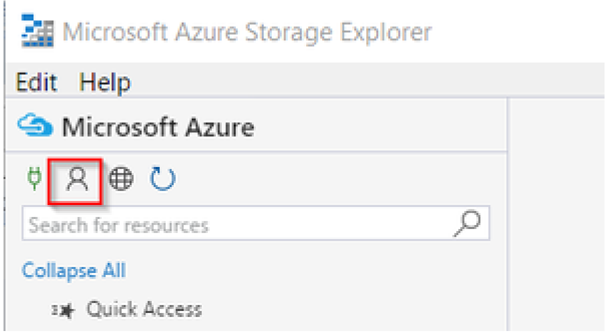
▼ Click here to expand or collapse this section

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*

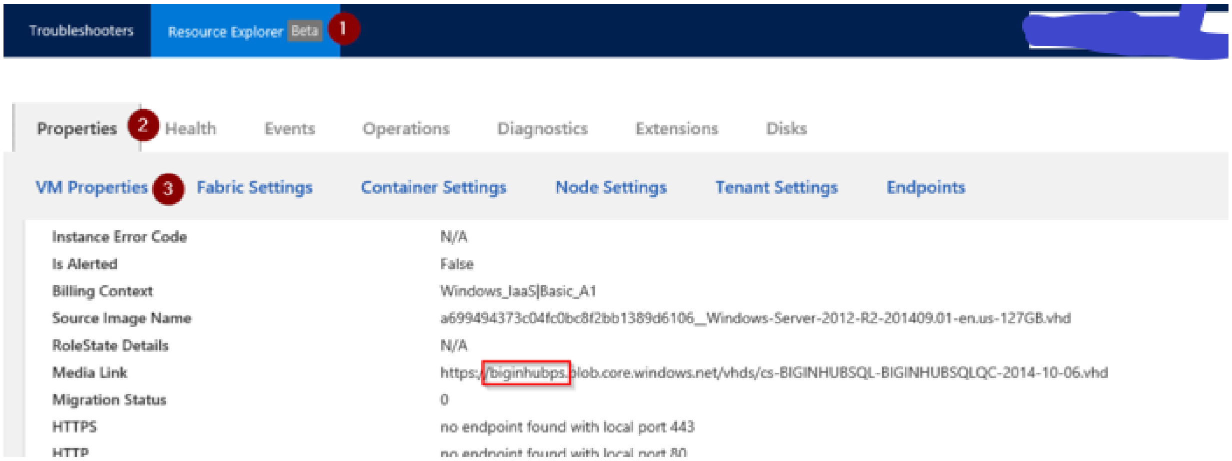
    

OS Disk Lease Id	0d69a55c-0317-40fa-a032-61f3550f3775
OS Disk Lease Acquired	True
OS Disk Billing Validated	True
OS Disk Encrypted	False
Billing Code	Windows_IaaS
Billing is Created from Marketplace Image	N/A
Billing Tag GUID	00000000-0000-0000-0000-000000000000

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...***

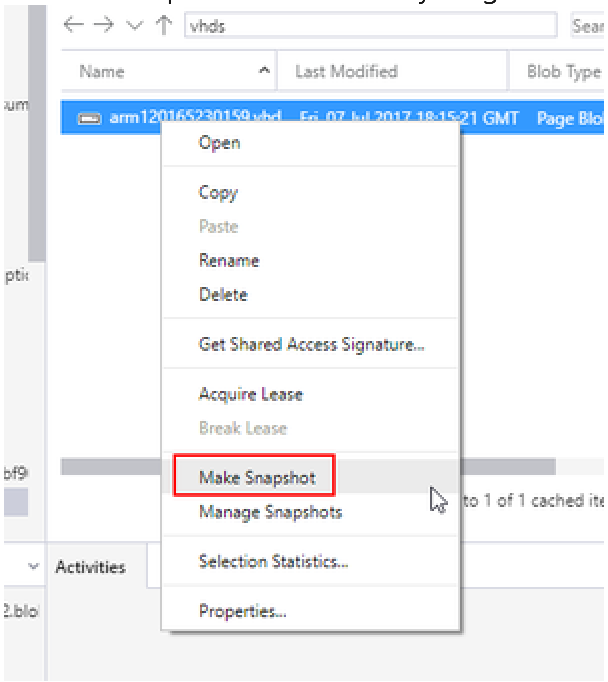
            3. Go to the storage account where the OS disk is, you can see this on ASC under *Resource Explorer* on *Properties* in the *VM Properties* card



[redacted]

Instance Error Code	N/A
Is Alerted	False
Billing Context	Windows_IaaS|Basic_A1
Source Image Name	a699494373c04fc0bc8f2bb1389d6106__Windows-Server-2012-R2-201409.01-en.us-127GB.vhd
RoleState Details	N/A
Media Link	https://biginhubps.blob.core.windows.net/vhds/cs-BIGINHUBSQL-BIGINHUBSQLQC-2014-10-06.vhd
Migration Status	0
HTTPS	no endpoint found with local port 443
HTTP	no endpoint found with local port 80

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

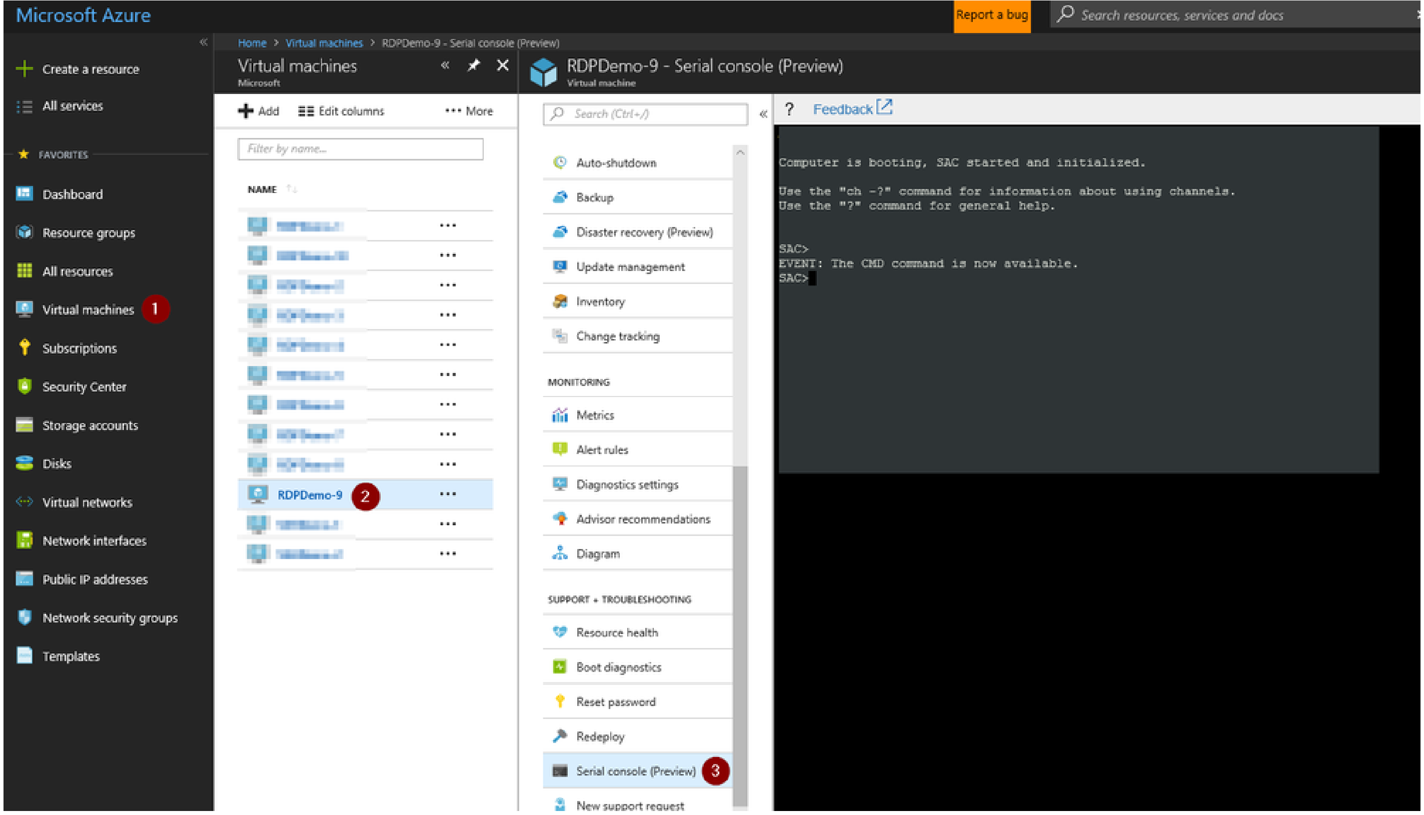
WAC is supported on ARM VMs running Windows Server 2016 or later (not Win10 or any other Windows client version, and not 2012R2/2012/2008R2 versions of Windows Server

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:

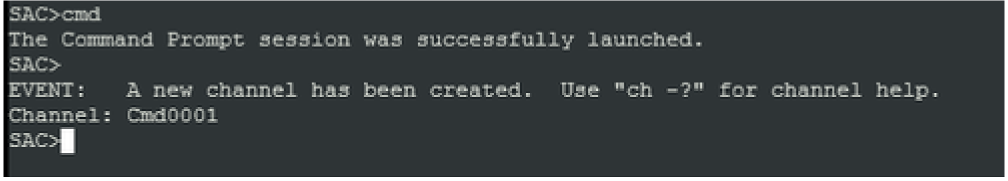


```
Computer is booting, SAC started and initialized.

Use the "ch -?" command for information about using channels.
Use the "?" command for general help.


SAC>
EVENT: The CMD command is now available.
SAC>
```

   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

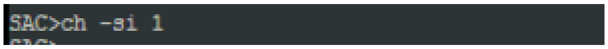
3. Create a channel with a CMD instance. Type `cmd` to start the channel, you will get the name of the channel



```
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>
```

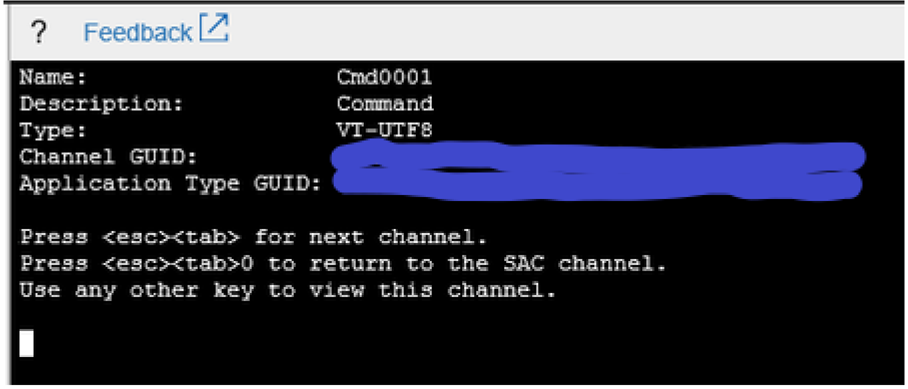
4. Switch to the channel running the CMD instance

```
ch -si 1
```



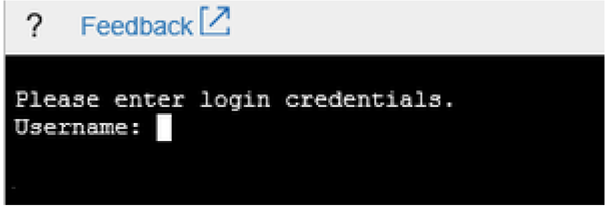
```
SAC>ch -si 1
```

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



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

Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.
```

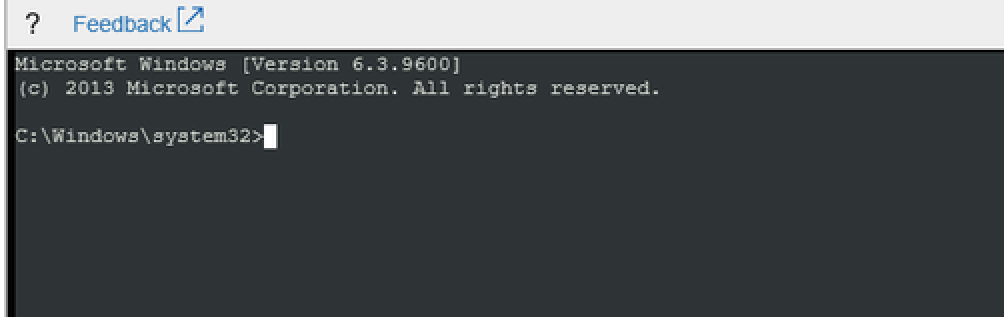
6. Hit enter a second time and it will ask you for user, domain and password:



```
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 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.

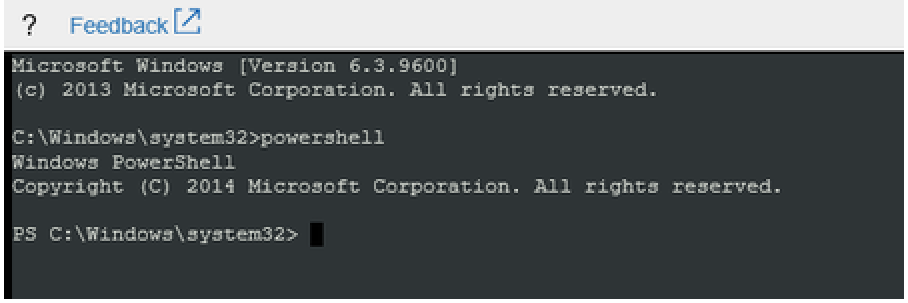
7. Once you add valid credentials, the CMD instance will open and you will have the prompt for you to start your troubleshooting:



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

C:\Windows\system32>
```

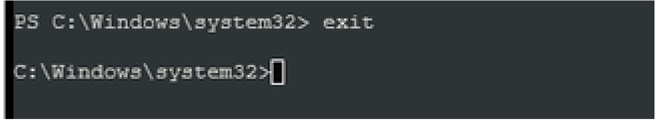
   1. At this point, you can do your troubleshooting in bash (CMD) or else, you could start a powershell instance:

1. To launch a powershell instance, run `powershell`



```
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

Mitigation 1

▼ Click here to expand or collapse this section

This only works for Windows 2012 R2 and above

1. Open a Powershell instance and run the following to perform a cleanup on the PNP internal database:

```
Invoke-Command {C:\windows\system32\RUNDLL32.exe c:\windows\system32\pnpclean.dll,RunDLL_PnpClean /Device
```

2. Restart the VM

Mitigation 2

▼ Click here to expand or collapse this section

1. Download the following files on a new or existing data disk which is attached to a working VM from the same region.
    1. Devcon (More info)
    2. RemoveGhostNICs-Devcon.ps1
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. Open an administrative Powershell instance in the same location and run the script *RemoveGhostNICs-Devcon.ps1*
4. Restart the VM

Mitigation 3

▼ Click here to expand or collapse this section

1. Download the following files RemoveGhostNICs.ps1 on 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. Open a Powershell instance and run the script RemoveGhostNICs.ps1 **
4. Restart the 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

Removing the subkeys **tcpip\parameters\adapters** and **tcpip\parameters\interfaces** is **IS NOT** will not achieve removing the Ghosted NICs since there's a lot of other devices that will be impacted with lingering entries referring to these and you could leave the VM in a worst state which most of the time cannot be fixed. ****

You should always avoid doing that.

Mitigation 1

This mitigation applies only in ONLINE mode

Mitigation 2

▼ Click here to expand or collapse this section

1. Create **gpt.ini** in **\Windows\System32\GroupPolicy** on the affected VM's drive (if gpt.ini exists, rename to gpt.ini.bak). If the affected VM's VHD is the only data disk attached to the troubleshooting VM, it should be the F: drive, but make sure before continuing. Paste the following text into the gpt.ini file you created:

```
[General]
gPCFunctionalityVersion=2
gPCMachineExtensionNames=[{42B5FAAE-6536-11D2-AE5A-0000F87571E3}{40B6664F-4972-11D1-A7CA-0000F87571E3}]
Version=1
```

2. Create **scripts.ini** in **\Windows\System32\GroupPolicy\Machine\Scripts** (make sure hidden folders are shown, and the Scripts folder may need to be created) and paste the following text into the scripts.ini file you created:

```
[Startup]
0CmdLine=c:\Windows\System32\FixAzureVM.cmd
0Parameters=
```

3. Copy **DevCon.exe** to **\Windows\System32**

4. Copy FixAzureVM-RemoveNICs.ps1 to **\Windows\System32**

5. Copy FixAzureVM.cmd to **\Windows\System32**

6. In Azure Management Portal, detach the disk from the troubleshooting VM

7. Reassemble the VM

8. After the VM is running, reboot the VM from Azure Management Portal. If you do not do an additional reboot the connection will fail since we expect the startup script to have removed all NICs from the system

9. After the VM is running, attempt to RDP to it, and check **%windir%\System32\FixAzureVM-RemoveNICs.log** to check the results

10. Gather the FixAzureVM-RemoveNICs.log file and send it to Microsoft for review

11. From within your remote session, remove the following in order to clean up:

    1. From **%windir%\System32**, remove *DevCon.exe*, *FixAzureVM-RemoveNICs.ps1*, and *FixAzureVM.cmd*
    2. From **%windir%\System32\GroupPolicy\Machine\** remove *scripts.ini*
    3. From **%windir%\System32\GroupPolicy** remove *gpt.ini* (if gpt.ini existed before, and you renamed it to gpt.ini.bak, rename the .bak file back to gpt.ini)

Mitigation 3

▼ Click here to expand or collapse this section

1. You can redo the same steps as in mitigation 2 but with the RemoveGhostNICs.ps1 script

Actions to Avoid Reocurrence

Since MAC preservation was already enable, the reocurrence of having lingering NIC entries on the registry will reduce greatly however if as part of any troubleshooting a new NIC needs to be presented, you will also create a leftover registry entry for the former key and for that, the customer needs some plan to remove lingering entries as part of any other maintenance task to perform this cleanup either Manunally following the KB269155 or by any schedule task running a script.

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

Scripts

If the above files are no longer available or have been moved, please copy the ones available here.

FixAzureVM-RemoveNICs.ps1

▶ Click here to expand or collapse this section

DeviceManagement.psd1

▶ Click here to expand or collapse this section

FixAzureVM.cmd

▶ Click here to expand or collapse this section

RemoveGhostNICs.ps1

▶ Click here to expand or collapse this section

RemoveGhostNICs-Devcon.ps1

▶ Click here to expand or collapse this section

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!