

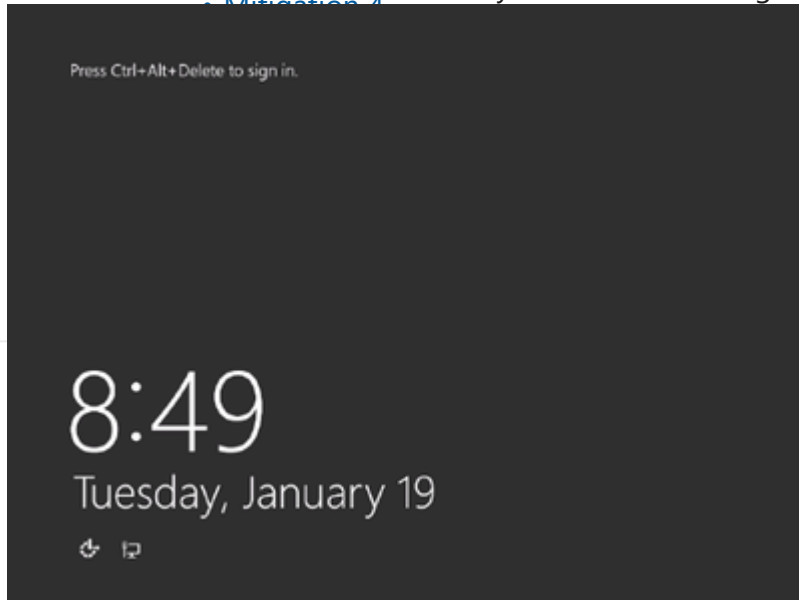
Contents

- Symptoms
- Root Cause Analysis
 - Root Cause Analysis 1
 - Root Cause Analysis 2
 - Root Cause Analysis 3
 - Root Cause Analysis 4
 - Root Cause Analysis 5
 - Root Cause Analysis 6
 - 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
 - ONLINE Mitigations
 - Mitigation 1
 - Mitigation 2
 - Mitigation 3
 - Mitigation 4
 - Mitigation 5
 - Mitigation 6
 - 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

Symptoms

- [Mitigation 1](#)
- [Mitigation 2](#)
- [Mitigation 3](#)
- [Mitigation 4](#)

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



2. There's no connectivity to the virtual machine on its VIP or DIP or its PA verified with [VM Port Scanner](#).
3. If you check over SAC, you will notice that the VM has an APIPA IP

1. In some rare scenarios, you could also have a null IP or not IPv4 listed at all

Root Cause Analysis

The VM run into an DHCP request fail to request for an IP from the Azure Wire DHCP Server. This could be caused by multiple reasons:

Root Cause Analysis 1

The host where this VM is hosted has some issue to provide connectivity via the hyperV platform to the guest. This could happen when:

1. The host OS has some problem or performance issue
2. The TOR device that works on this cluster and provides this connectivity to the host has problems to register new clients

Root Cause Analysis 2

The Guest OS had some issue with the virtual network card which was preventing the VM to have connectivity.

Root Cause Analysis 3

The customer has Custom DNS injected on the VM which overwrites the ones provided by the Azure Platform. If the primary DNS is unresponsive but not enough to give a time out to failover to the secondary DNS, this could bring problems on the availability of this VM.

Root Cause Analysis 4

The customer has custom routes added on the routing table of this VM and based on the network/subnet/gateway and interface written down on the table, could impact the outbound connectivity of this VM to even seek the connectivity from the platform as part of the DHCP discovery process.

Root Cause Analysis 5

The customer has the DHCP Role enabled on the VM which is an unsupported scenario in azure.

Root Cause Analysis 6

The customer is trying to use Custom DHCP entries on the VM which is an unsupported scenario in azure.

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\My vm restarted, paused, or stopped unexpectedly\Help diagnose my VM restart issue	Root Cause - Windows Azure\Virtual Machine\Azure Platform\Unhealthy node	
2	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\No Nic\NIC Disconnected status	
3	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\No Nic\NIC with custom DNS	
4	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\No IP\Persistent routes added	
5	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\No Nic\NIC with custom DHCP	
6	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\No Nic\NIC with custom DHCP	

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

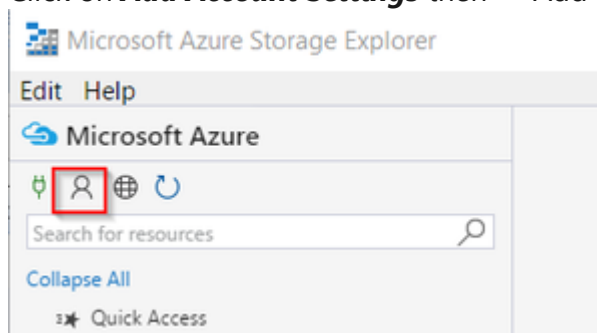
1. Before doing anything, please validate if this is an encrypted VM. On ASC check on the Resource Explorer on the VMCard for the value *OS Disk Encrypted*

OS Disk Lease Id	0db9a55c-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

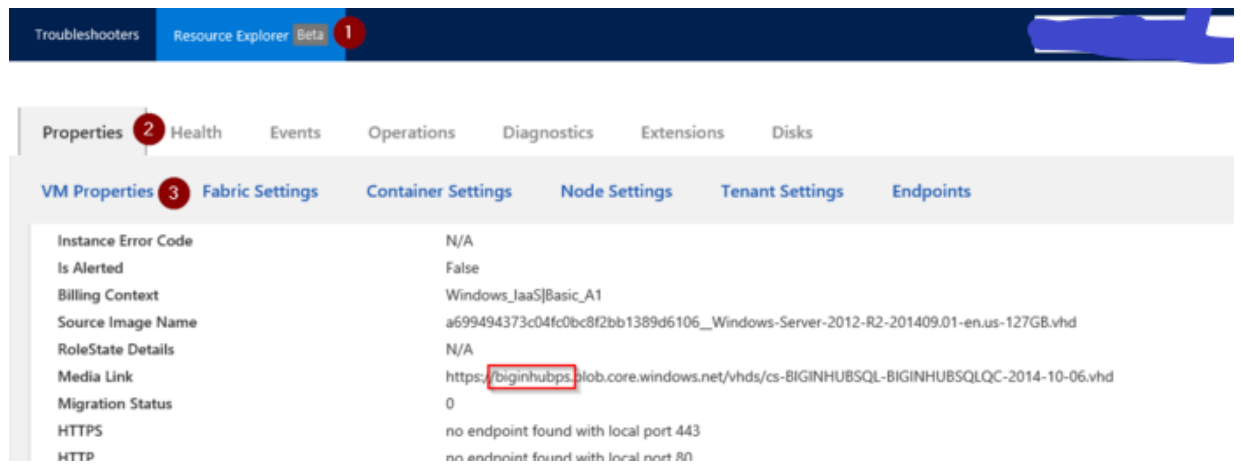
2. If the OS Disk is encrypted, then proceed to [Unlock an encrypted disk](#)
3. Now proceed to do a copy of the OS disk, this will help in case of a rollback for recovery or RCA in a later stage
4. Power the machine down and once it is stopped de-allocated to do the copy.
5. Create a snapshot
 1. If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

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

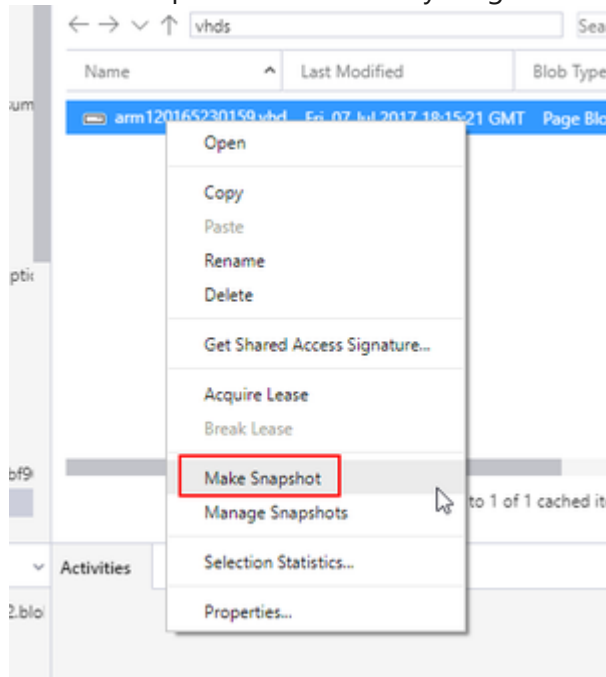
1. Once the customer download the tool, proceed to add the Azure account details so you can access the storage accounts
2. Click on **Add Account Settings** then ***Add an account...***



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

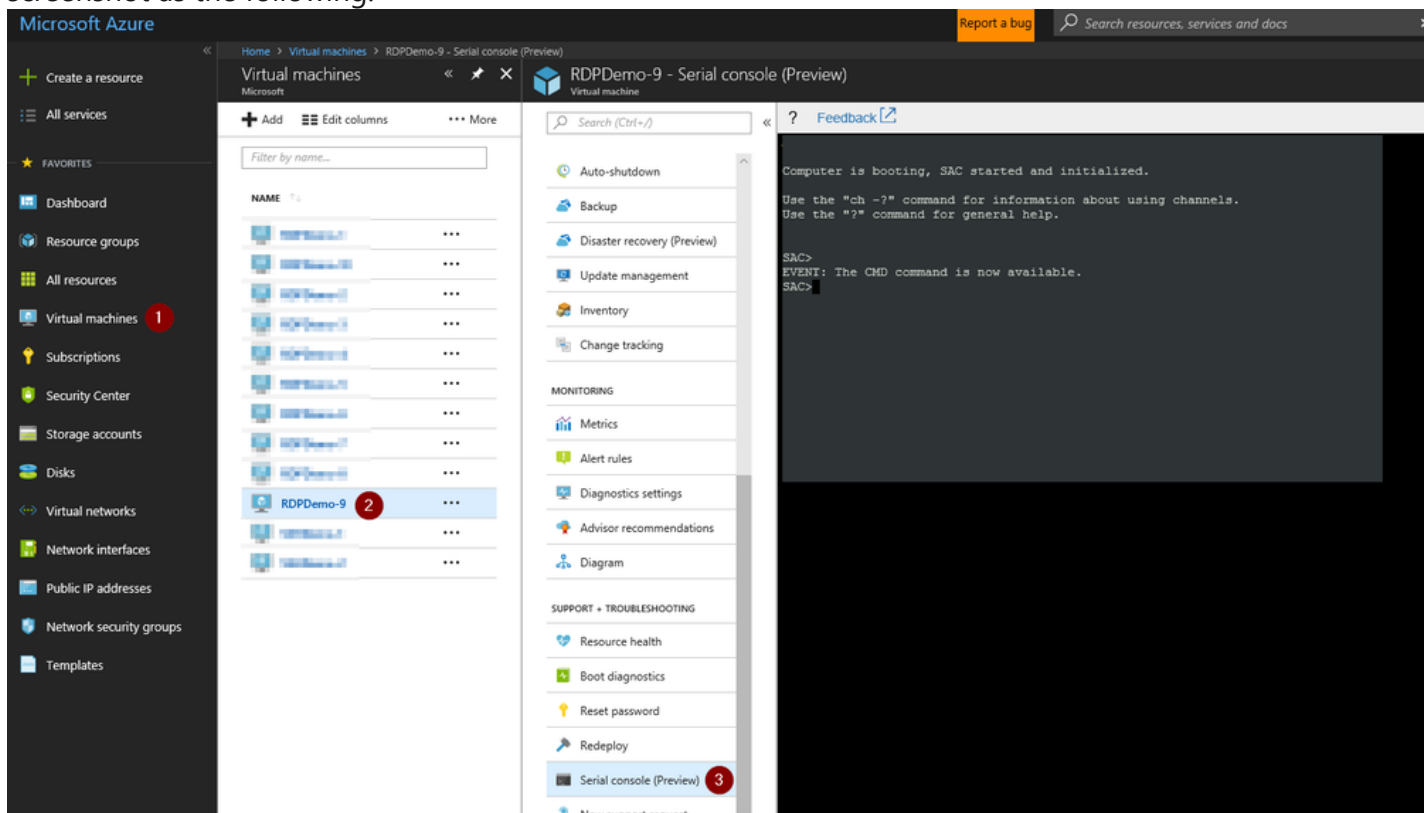
See [How To Access Thru Windows Admin Center](#)

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
```

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

```
? Feedback
Name: Cmd0001
Description: Command
Type: VT-UTF8
Channel GUID:
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:

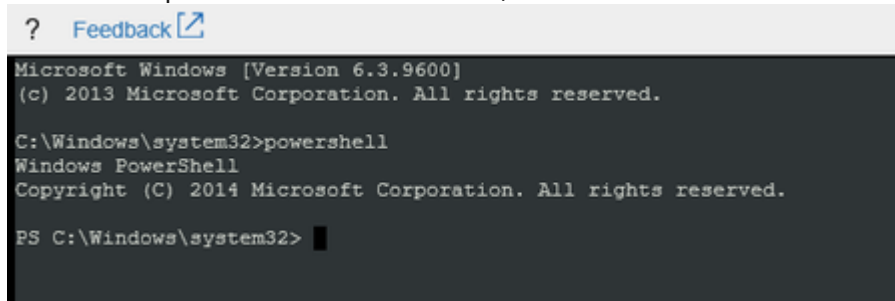
```
? Feedback
Please enter login credentials.
Username:
```

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`

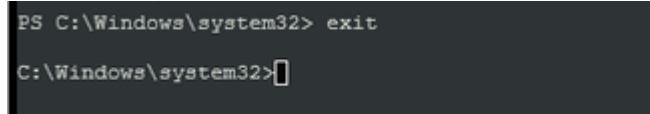


```
? Feedback
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

ONLINE Mitigations

Mitigation 1

- ▼ Click here to expand or collapse this section

1. Redeploy the VM so it is moved to a new host

1. If the issue is fixed, please file a [sev 3 ICM to RDOS EEE](#) so they can investigate further why the connectivity to the VM was not working
2. If the issue is NOT fixed, proceed with the next mitigation

Mitigation 2

- ▼ Click here to expand or collapse this section

1. Proceed to [present a new NIC to a Guest OS](#) and in an attempt to isolate if the problem is on the Guest or in the Host, after to you do this, [validate a NIC was introduced in the Guest OS](#)
 1. If you don't see any new NIC in the guest, then treat this case as a [NoNIC case](#)
 2. If you see evidence of the new NIC

1. Re-run the insights on ASC and see if there's any detection on a new DHCP Request fail, if you do, then proceed with the next mitigation
2. If you don't get any *DHCP Request Fail* insight, then get a new screenshot
 1. If you see a red cross over the NIC, then refer to [Red Cross Bucket](#)
 2. If you don't see a red cross, then proceed with the next mitigation

Mitigation 3

▼ Click here to expand or collapse this section

Check with the customer is he/she is trying to use any custom DNS and check if they added this on the NIC instead of adding them on the VNET/Subnet information on the portal.

1. Using [SAC](#) open an elevated CMD channel and query the IP configuration and look for the *DNS Servers* data under the network card:

```
C:\Users\glimoli>ipconfig /all

Windows IP Configuration.
Host Name . . . . . : OPENTEXT-DBA.
Primary Dns Suffix . . . . . : tec.com.kw.
Node Type . . . . . : Hybrid.
IP Routing Enabled. . . . . : No.
WINS Proxy Enabled. . . . . : No.
DNS Suffix Search List. . . . . : tec.com.kw.

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . : .
Description . . . . . : Microsoft Hyper-V Network Adapter #2.
Physical Address. . . . . : 00-0D-3A-B3-44-8F.
DHCP Enabled. . . . . : No.
Autoconfiguration Enabled . . . : Yes.
IPv4 Address. . . . . : 10.50.10.13(Preferred) .
Subnet Mask . . . . . : 255.255.255.0.
Default Gateway . . . . . : 10.50.10.1.
DNS Servers . . . . . : 8.8.8.8.
                        192.168.150.10.
NetBIOS over Tcpi. . . . . : Enabled.
```

2. Then using ASC, go the Networking tab on the Network and subnet this customer is using on this VM, and check the property *DNS Servers*:

The screenshot shows the Azure portal interface for a virtual network named 'xoi2devsvnet'. The left sidebar displays a tree view of resource groups and providers, with 'Microsoft.Network' expanded and 'virtualNetworks' selected. The main pane shows the 'Properties' tab for the virtual network. The 'DNS Servers' and 'DNS Names' fields are highlighted with a red box, indicating they are set to 'Default (Azure-Provided)' and 'N/A' respectively.

Property	Value
Resource Id	/subscriptions/.../resourceGroups/XOI2DEV.ES.RESOURCE.GROUP/providers/Microsoft.Network/virtualNetworks/XOI2DEVSVNET
Name	xoi2devsvnet
Location	westus2
Resource Group	xoi2dev.es.resource.group
Resource Guid	c8ba307c-...
Full Name	xoi2devsvnet
Created Time	01/09/2017 22:07:54
Last Modified Time	10/23/2018 21:03:50
Last Operation Id	27c3f7aa-...
Last Operation Type	Microsoft.WindowsAzure.Networking.Nrp.Frontend.Operations.Csm.PutVirtualNetworkOperation
Provisioning State	Succeeded
Address Prefixes	10.0.0.0/16
VnetId	c8ba307c-...
VNet Peering	N/A
Contains Accelerated Networking VMs	False
Enable DDoS Protection	False
DDoS Protection Plan	N/A
DNS Servers	Default (Azure-Provided)
DNS Names	N/A
Allocation Committed IPs	N/A
Allocation Goal IPs	N/A
Previous Allocation Goals IPs	N/A

3. If you see the entries on the OS but not on the platform, then it means the customer is setting this manually over the NIC which is not following the best practices on azure. Please educate the customer on how to set these up on the VNET/Subnet configuration in the portal and remove these DNS entries. To remove these entries on the Guest OS please follow the following:

1. List the name of the interface, usually *Ethernet*

```
netsh interface ip show config
```

2. Then to delete all the hardcoded DNS entries, just run the following:

```
netsh dnsclient delete dnsserver "<INTERFACE NAME>" all
```

3. Then by default the hardcoded DNS entry will be deleted and the DNS entry will be replace by an entry obtain from the Wire DHCP server from the azure platform. To check this out, you can again list this entry

```
netsh interface ip show config
```

4. Then to add the custom DNS entries, add these on the VNET/Subnet where this VM belongs in the portal. Once the change is done in the portal, the VM (and any VM in that network), will need to restart to pick up those changes

Mitigation 4

▼ Click here to expand or collapse this section

Validate the customer doesn't have any persistent routes on the internal routing table impacting the outbound traffic of a VM

1. Query the current persistent routes information:

```
REG QUERY "HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes"
```

1. If this branch has **any** property inside with the list of the routes created, then these routes could be impacting the outbound traffic of the VM based on which network/subnet/gateway or interface card is trying to use. You can remove them by:

```
REG DELETE "HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\PersistentRoutes" /va /f
```

2. If it comes up empty, then it means you don't have any Persistent Route pushed to the VM. Proceed with the next mitigation.

Mitigation 5

▼ Click here to expand or collapse this section

1. Check if the VM has [the DHCP Server role](#) enabled on the OS. Using this role in Azure is **unsupported**
2. If this is not your case, then proceed to the next mitigation

Mitigation 6

▼ Click here to expand or collapse this section

Check with the customer if he/she is trying to use any custom DHCP and if he is, **this is not supported in azure**, the machine should use the DHCP wired server from the Azure Platform which is 168.63.129.16 :

1. If they are, just presenting a new NIC to wiped off that configuration. Refer to [Present a new NIC to a Guest OS](#)
2. Then, ensure the *DHCP Client* service in the OS is running. Open a CMD instance and check the current status of the *DHCP Client*:

```
sc query DHCP
```

1. If this is stopped or failing, then proceed with [DHCP Client service is not starting](#).

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

Mitigation 1

1. This applies only to ONLINE troubleshooting.

Mitigation 2

▼ Click here to expand or collapse this section

1. If you are working OFFLINE, the recreation of the VM will take care to present a new NIC to the Guest OS so in an attempt to isolate if the problem is on the Guest or Host refer to [validate a NIC was introduced in the Guest OS](#)
 1. If you don't see any new NIC in the guest, then treat this case as a [NoNIC case](#)
 2. If you see evidence of the new NIC
 1. Re-run the insights on ASC and see if there's any detection on a new DHCP Request fail, if you do, then proceed with the next mitigation
 2. If you don't get any *DHCP Request Fail* insight, then get a new screenshot
 1. If you see a red cross over the NIC, then refer to [Red Cross Bucket](#)
 2. If you don't see a red cross, then proceed with the next mitigation

Mitigation 3

▼ Click here to expand or collapse this section

1. If you are working OFFLINE, the recreation of the VM will take care to present a new NIC to the Guest OS so in an attempt to isolate if the problem is on the Guest or Host refer to [validate a NIC was introduced in the Guest OS](#)

Mitigation 4

▼ Click here to expand or collapse this section

Validate the customer doesn't have any persistent routes on the internal routing table impacting the traffic of a VM

1. Query the current persistent routes information:

```
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 Query the current Persistent Routes data
set key=HKLM\BROKENSYSTEM\ControlSet00%ControlSet%\Services\Tcpip\Parameters\PersistentRoutes
REG QUERY %key%

reg unload HKLM\BROKENSYSTEM
```

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

1. If this branch has any property inside, these would be the list of the routes created. Then these routes could be impacting the outbound traffic of the VM based on which network/subnet/gateway or interface card is trying to use. You can remove them by:

```
reg load HKLM\BROKENSYSTEM f:\windows\system32\config\SYSTEM
REG DELETE %key% /va /f
reg unload HKLM\BROKENSYSTEM
```

2. If it comes up empty, then it means you don't have any Persistent Route pushed to the VM. Proceed with the next mitigation.
2. Reassemble the VM and retry

Mitigation 5

▼ Click here to expand or collapse this section

1. Check if the VM has [the DHCP Server role](#) enabled on the OS. Using this role in Azure is **unsupported**
2. If this is not your case, then proceed to the next mitigation

Mitigation 6

▼ Click here to expand or collapse this section

Check with the customer is he/she is trying to use any custom DHCP and if he is, **this is not supported in azure:**

1. The recreation of the VM will take care of the recreation of the NIC in the guest and that will wipe off that configuration on it
2. Then, ensure the *DHCP Client* service in the OS is running. Open an elevated CMD instance and run the following script:

```

reg load HKLM\BROKENSYSYSTEM 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\BROKENSYSYSTEM\Select /v Current') do set ControlSet=%x
set ControlSet=%ControlSet:~2,1%

REM Query the current Persistent Routes data
set key=HKLM\BROKENSYSYSTEM\ControlSet00\ControlSet%\Services\services\dhcp

REM Set default values back on the broken service
reg add %key% /v start /t REG_DWORD /d 2 /f
reg add %key% /v ImagePath /t REG_EXPAND_SZ /d "%SystemRoot%\system32\svchost.exe -k LocalServiceNetw
reg add %key% /v ObjectName /t REG_SZ /d "NT AUTHORITY\LocalService" /f
reg add %key% /v type /t REG_DWORD /d 16 /f

REM Enable default dependencies from the broken service
set key=HKLM\BROKENSYSYSTEM\ControlSet00\ControlSet%\Services\services\nsi
reg add %key% /v start /t REG_DWORD /d 2 /f

set key=HKLM\BROKENSYSYSTEM\ControlSet00\ControlSet%\Services\services\tdx
reg add %key% /v start /t REG_DWORD /d 1 /f

set key=HKLM\BROKENSYSYSTEM\ControlSet00\ControlSet%\Services\services\afd
reg add %key% /v start /t REG_DWORD /d 1 /f

reg unload HKLM\BROKENSYSYSTEM

```

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

3. Reassemble the VM and retry

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 - RDPFE 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>