Hyper-V Host Migrated to Azure_RDP SSH

Last updated by | Kevin Gregoire | Mar 29, 2022 at 11:47 AM PDT

Tags

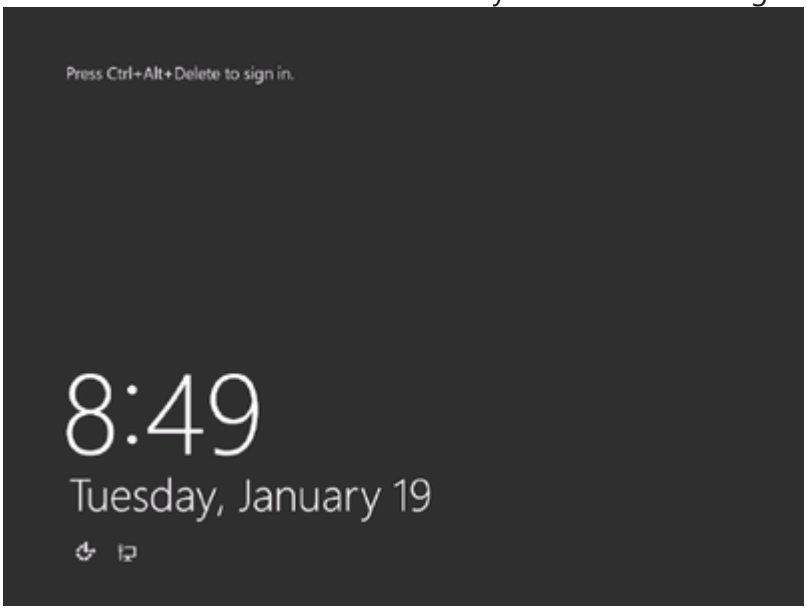
cw.TSG	cw.RDP-SSH

Contents

Symptoms

1. Usually you will find these cases on VMs that are getting migrated from On-Premises either with an upload of an specialized disk or in an automatic way with **Azure Site Recovery**

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



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

4. On the Azure Agent log, you could also see the OS doesn't have a NIC

```
[00000006] [10/17/2017 16:48:24.09] [INFO]  Could not find any network interface that has DHCP enable
[00000006] [10/17/2017 16:48:24.09] [ERROR] Did not discover fabric address on any interface. Dumping
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all: .
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all: Windows IP Configuration.
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all: .
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all:    Host Name . . . . . . . . . . . . :
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all:    Primary Dns Suffix  . . . . . . . :
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all:    Node Type . . . . . . . . . . . . :
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all:    IP Routing Enabled. . . . . . . . :
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all:    WINS Proxy Enabled. . . . . . . . :
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all:    DNS Suffix Search List. . . . . . :
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all: .
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all: Tunnel adapter Teredo Tunneling Pseudo
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all: .
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all:    Media State . . . . . . . . . . . :
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all:    Connection-specific DNS Suffix  . :
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all:    Description . . . . . . . . . . . :
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all:    Physical Address. . . . . . . . . :
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all:    DHCP Enabled. . . . . . . . . . . :
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all:    Autoconfiguration Enabled . . . . :
[00000015] [10/17/2017 16:48:24.10] [INFO]  ipconfig.exe /all: .
[00000003] [10/17/2017 16:48:24.12] [INFO]  route.exe print: ===========================================
[00000003] [10/17/2017 16:48:24.12] [INFO]  route.exe print: Interface List.
```

5. If you pull the Guest OS Logs, on the startup of the VM, you will see several events from HYPER-V starting their services:

```
Time:     10/17/2017 5:11:10 PM
ID:       7036
Level:    Information
Source: Service Control Manager
Machine:  IMALWEB.kipco.net
Message:  The Hyper-V Virtual Machine Management service entered the running state.
```

```
Time:     10/17/2017 5:11:07 PM
ID:       7036
Level:    Information
Source: Service Control Manager
Machine:  IMALWEB.kipco.net
Message:  The Hyper-V Image Management Service service entered the running state.



Time:     10/17/2017 5:11:04 PM
ID:       7036
Level:    Information
Source: Service Control Manager
Machine:  IMALWEB.kipco.net
Message:  The Hyper-V Networking Management Service service entered the running state.



Log Name:      System
Source:        VMSMP
Date:          10/17/2017 9:06:32 AM
Event ID:      5
Task Category: None
Level:         Information
Keywords:      Classic
User:          N/A
Computer:      IMALWEB.kipco.net
Description:
The description for Event ID 5 from source VMSMP cannot be found. Either the component that raises th
If the event originated on another computer, the display information had to be saved with the event.
The following information was included with the event:
0
LOCAL AREA CONNECTION - VIRTUAL NETWORK
SWITCH-SM-947643FA-C1AC-4F78-8A0B-E254E7D9498F-0
SWIT
```

Root Cause Analysis

The machine migrated in azure is a HYPER-V Host and this does not fulfill the requirements:

1. The Guest should only be Windows Server 2016 or Windows 10
2. The HYPER-V Switch between the Guest and the Host needs to have a virtual NAT switch created in between to connect both Hypervisors

If the customer wants to have a HYPER-V host in Azure, this needs to be created in only the supported regions and work with supported GuestOS versions (2016/10) and enable these roles within azure so the virtual NAT switch is created with no issues.

Also, as the machine was migrated into Azure, most likely this was not prepared successfully. The following article needs to be shared with the customer so he could prepared the VMs before they are uploaded into Azure.

- Prepare a Windows VHD or VHDX to upload to Azure

Note: Please be aware that Azure Site Recovery is not doing this on the customer behalf, these are extra steps the customer needs to do to prepare for the migration.

References

- Nested Virtualization in Azure
- Run Hyper-V in a Virtual Machine with Nested Virtualization
- Microsoft server software support for Microsoft Azure virtual machines

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\VM Deployment, Start, Stop, Resize, Delete failures\Custom Image incorrectly prepared*	
	Azure Virtual Machine ⧼ Windows	**For new migrated VMs:** *Routing Azure Virtual Machine V3\Cannot create a VM\I need guidance preparing an image*	*Root Cause - Windows Azure\Virtual Machine\VM Deployment, Start, Stop, Resize, Delete failures\Custom Image incorrectly prepared*	

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

Customer Enablement

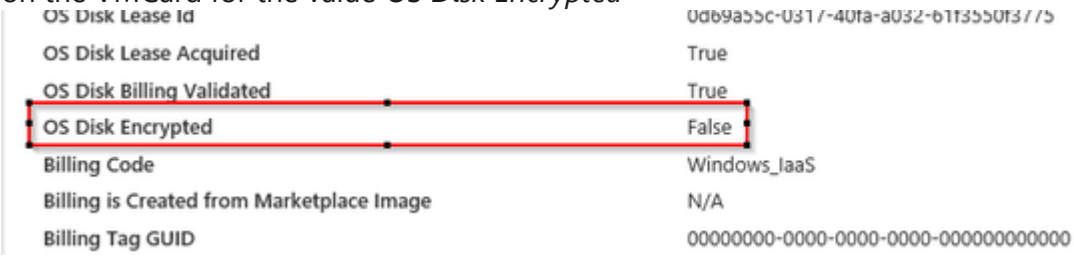
N/A

Mitigation

Backup OS disk

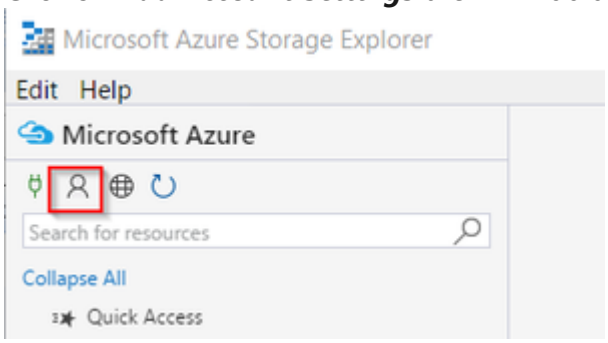
▼ Click here to expand or collapse this section

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*

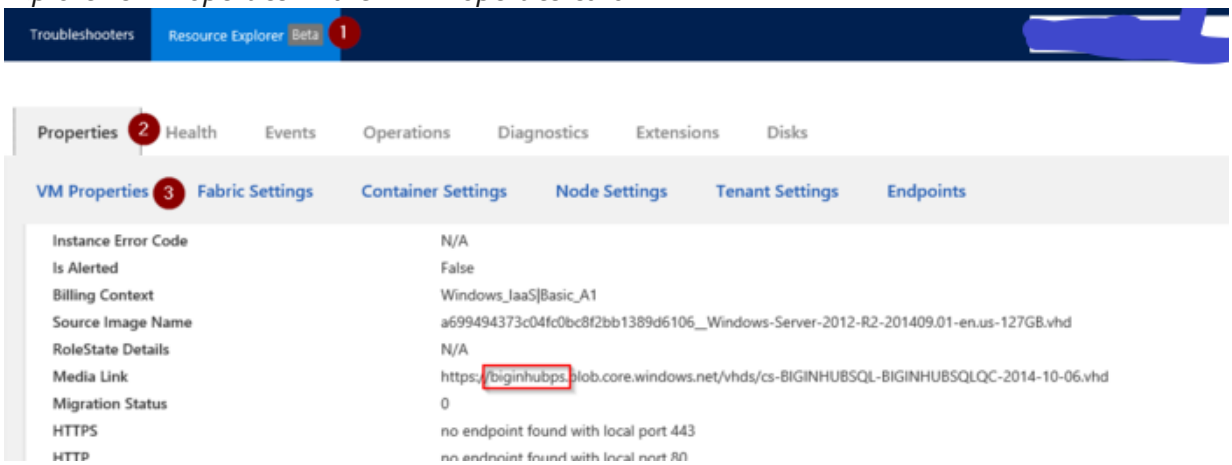


2. If the OS Disk is encrypted, then proceed to Unlock an encrypted disk
3. Now proceed to do a copy of the OS disk, this will help in case of a rollback for recovery or RCA in a later stage
4. Power the machine down and once it is stopped de-allocated to do the copy.
5. Create a snapshot

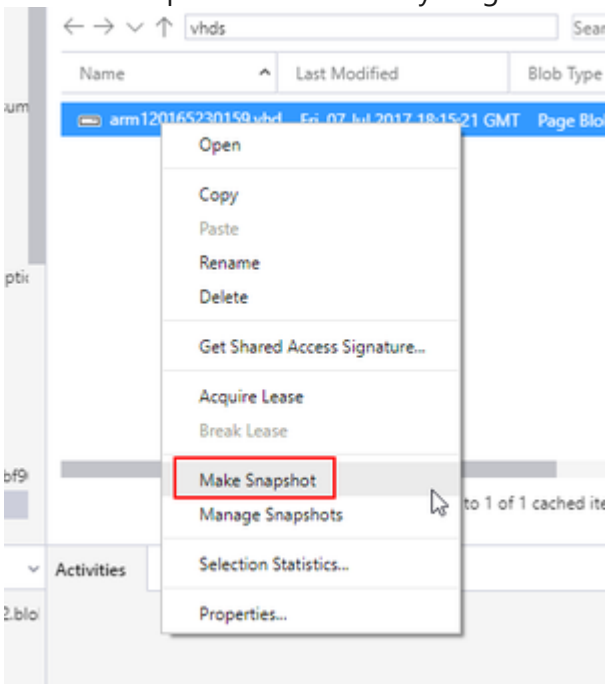
1. If the **disk is unmanaged**, this could be done by using Microsoft Azure Storage Explorer or Azure Powershell
    1. Using Microsoft Azure Storage Explorer
        1. Once the customer download the tool, proceed to add the Azure account details so you can access the storage accounts
        2. Click 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

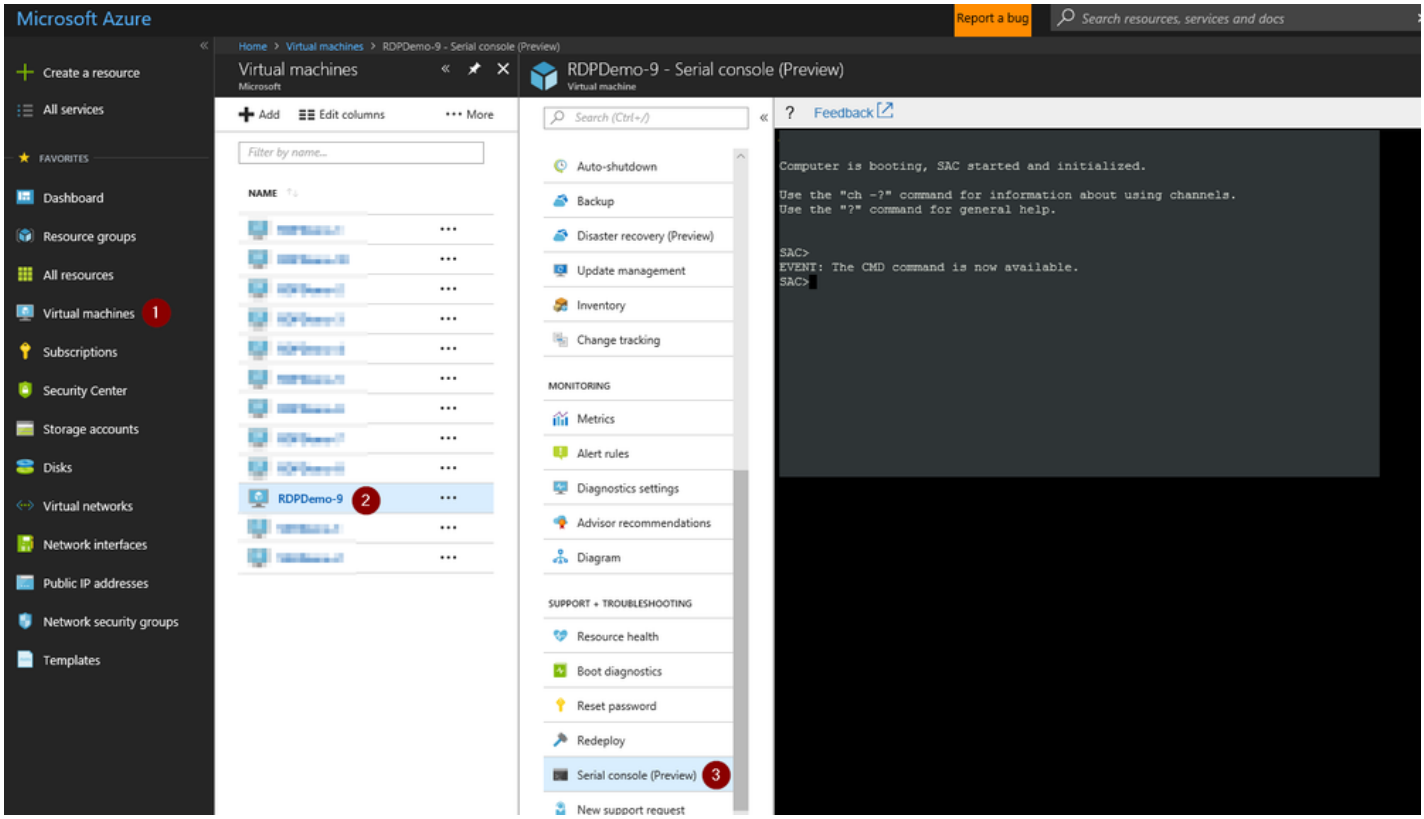
WAC is supported on ARM VMs running Windows Server 2016 or later (not Win10 or any other Windows client version, and not 2012R2/2012/2008R2 versions of Windows Server

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
```

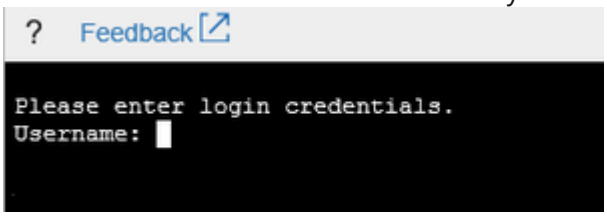
```
SAC>ch -si 1
```

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

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

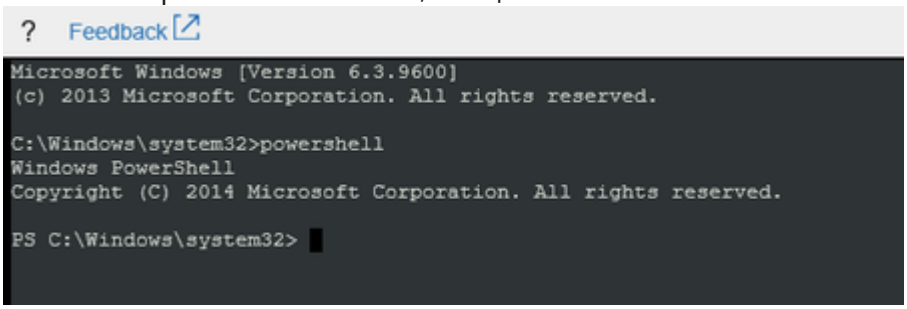
6. Hit enter a second time and it will ask you for user, domain and password:



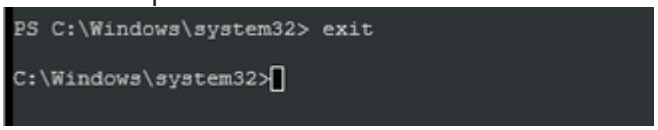
    1. If the machine has connectivity, you could use either local or domain IDs. If you want to use a local ID, for domain just add the hostname of the VM
    2. If the machine doesn't have connectivity, you could try to se domains IDs however this will work if only the credentials are cached on the VM.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

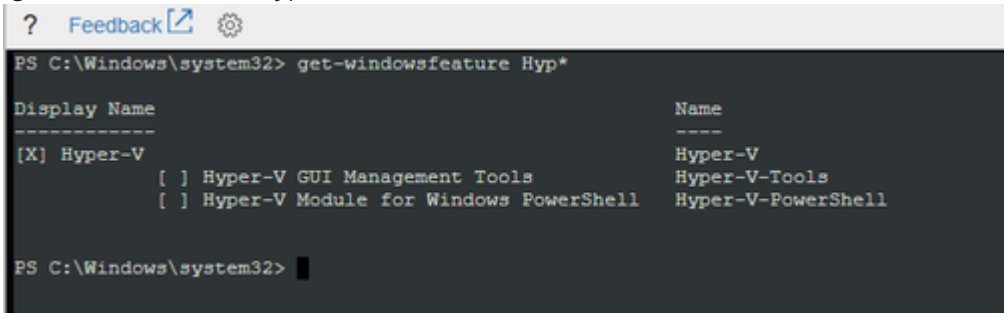
ONLINE Mitigations

▼ Click here to expand or collapse this section

If the customer is doing a migration or Disaster Recovery using Azure Site Recovery, you may want to explain the customer that HYPER-V host cannot be migrated in azure, the HYPER-V Roles needs to be removed. If they later on wants to have these roles back, they can enable back on in Azure since this will ensure that the NAT Switch between hypervisors is taken care in that moment.

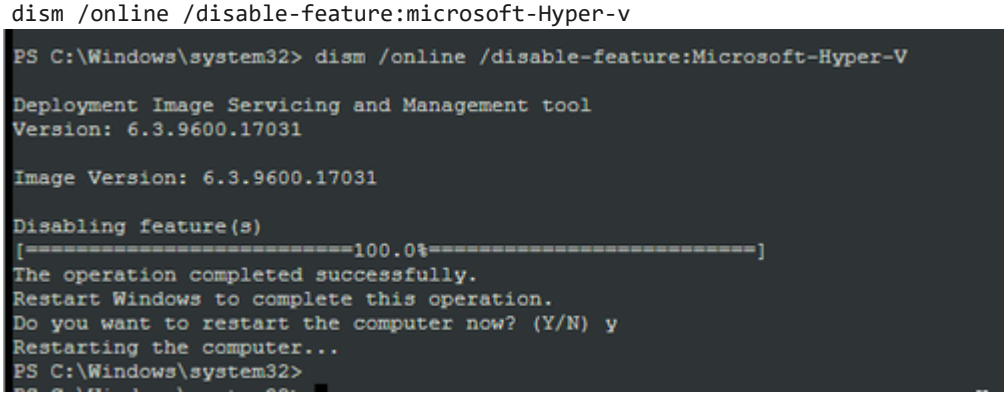
1. Open a Powershell instance and query the roles of the machine and you will see that the HYPER-V role is enabled

```
get-windowsfeature Hyp*
```



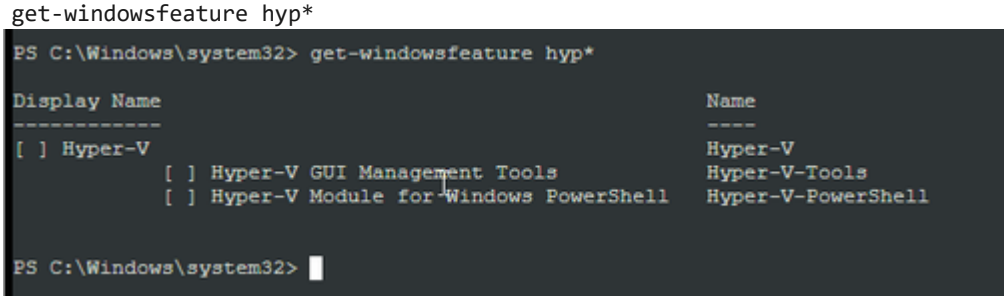
2. Remove the HYPER-V role and complete the removal with a restart:

```
dism /online /disable-feature:microsoft-Hyper-v
```



3. Once the machine is back online, query for the roles to ensure the HYPER-V role was removed successfully:

```
get-windowsfeature hyp*
```



4. You don't need to restart the VM, the VM will be back reachable on that network card

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. Open an elevated CMD and remove the HYPER-V Role

```
Dism /Image:<OS Disk letter>:\ /Disable-Feature /FeatureName:Microsoft-Hyper-V
```

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

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!