

# Guest OS Firewall Blocking Inbound Traffic\_RDP SSH

Last updated by | Maria Radu | Feb 7, 2023 at 7:52 AM PST

Tags

cw.TSG

cw.RDP-SSH

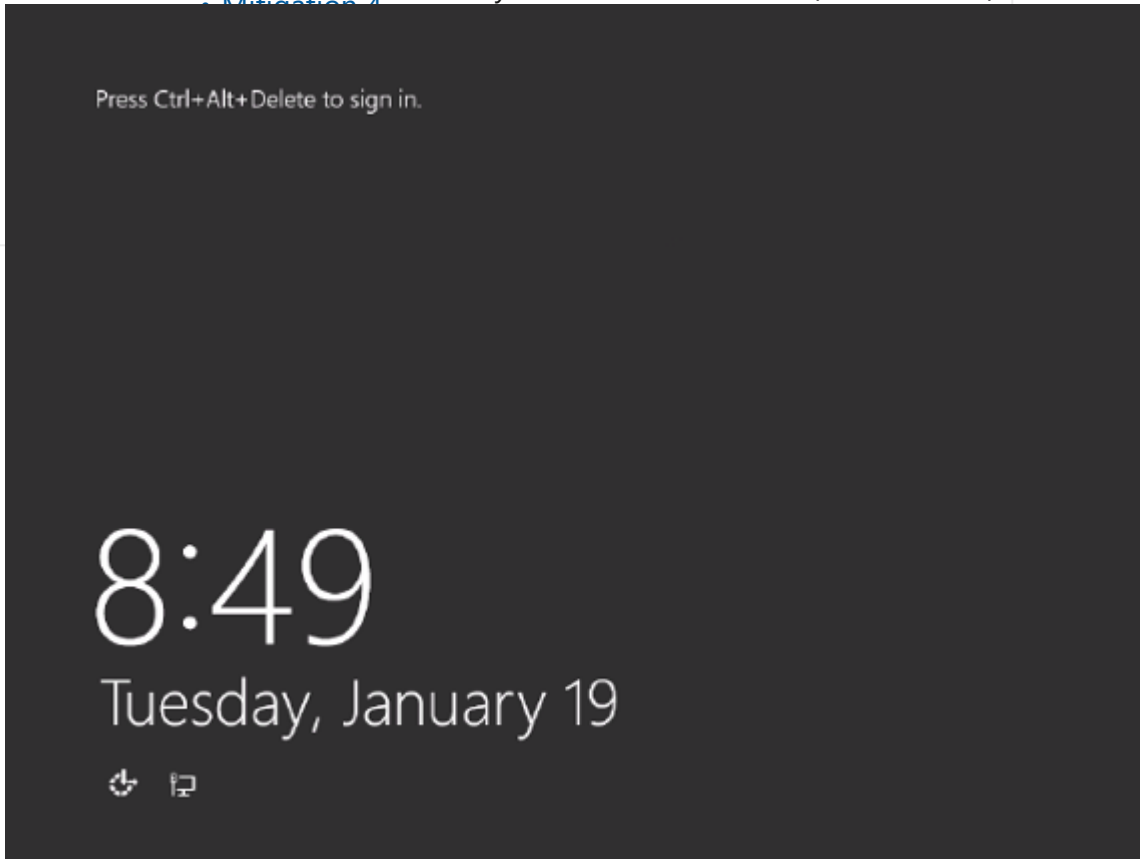
## Contents

- Symptoms
  - Brownbag Video
- Root Cause Analysis
  - Root Cause Analysis 1
    - Refresher / Training Template
  - Root Cause Analysis 2
    - Refresher / Training Template
  - Root Cause Analysis 3
  - Root Cause Analysis 4
  - References
  - 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
  - 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 at CAD screen (Ctrl+Alt+Del)



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 will not find connections being made.
4. WaAppAgent logs shows the machine is doing hear beat normally.
5. By default the Guest OS firewall logging is disabled so you will not have any evidence of it there either
6. In **WinGuestAnalyzer\Health Signal** tab on the *remoteaccess* section, RDP traffic could be shown as denied:



## Brownbag Video

- [Azure VM RDP issue - GuestOS firewall blocking inbound traffic](#) 

## Root Cause Analysis

### Root Cause Analysis 1

The RDP rule is not setup to allow the RDP traffic.

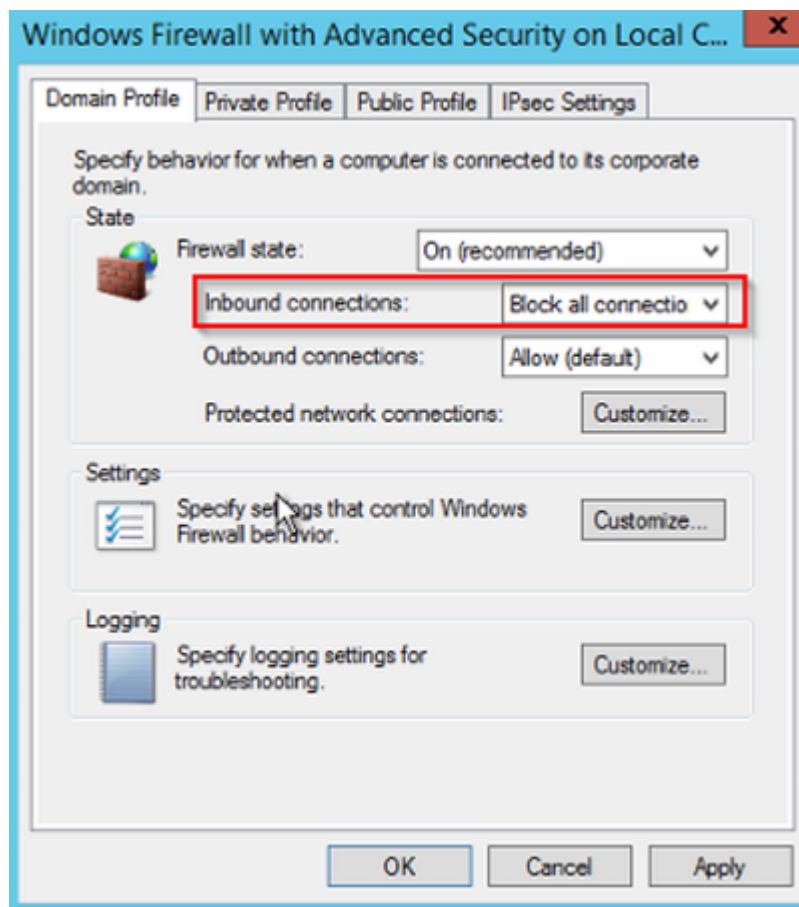
#### Refresher / Training Template

- 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.



### Root Cause Analysis 2

The any of the Guest OS firewall profiles was setup to block all inbound connections and this includes the RDP traffic:



#### 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.



### Root Cause Analysis 3

This applies **only** for Microsoft corp domain machines.

This machine could be set up to be of a restrictive access and setup only to be reachable:

1. From a SAW device only
2. From a specific network segment

Usually this is achieved by placing the VM on an OU that has linked an AD policy that is blocking every connection that is not from one specific network segment and detecting if the connection is coming from a SAW devices.

*If you confirm this scenario but the customer still wants to use this machine from a non SAW device and/or from his network, he will need to file a case with MSIT and this case can then be closed out as this out of our support.*

If this is your case, refer to the *Mitigation 1* on [Microsoft Corp domain joined machines](#)

### Root Cause Analysis 4

This applies **only** for Microsoft corp domain machines.

This machine could be set up to be of a restrictive access and setup only to be reachable:

1. From a specific network segment

Usually this is setup at a network level to avoid traffic between network segments.

*If you confirm this scenario but the customer still wants to use this machine from his network, he will need to file a case with MSIT and this case can then be closed out as this out of our support.*

If this is your case, refer to the *Mitigation 2* on [Microsoft Corp domain joined machines](#)

### References

N/A

Tracking close code for this volume

Root Cause	Product	Support Topic	Cause Tracking code	Bug
1	Azure Virtual Machine ❖ Windows	<b>For existing VMs:</b> Routing Azure Virtual Machine V3\Cannot Connect to my VM\Troubleshoot my network security group (NSG)	Root Cause - Windows Azure\Virtual Machine\Guest OS - Windows\Isolated\Firewall misconfigured\Rule not enabled	
	Azure Virtual Machine ❖ Windows	<b>For new migrated VMs:</b> Routing Azure Virtual Machine V3\Cannot create a VM\I need guidance preparing an image	Root Cause - Windows Azure\Virtual Machine\Guest OS - Windows\Isolated\Firewall misconfigured\Lack of preparation prior migration - Firewall not setup	
2	Azure Virtual Machine ❖ Windows	<b>For existing VMs:</b> Routing Azure Virtual Machine V3\Cannot Connect to my VM\Troubleshoot my network security group (NSG)	Root Cause - Windows Azure\Virtual Machine\Guest OS - Windows\Isolated\Firewall misconfigured\BlockAllInboundTraffic	
	Azure Virtual Machine ❖ Windows	<b>For new migrated VMs:</b> Routing Azure Virtual Machine V3\Cannot create a VM\I need guidance preparing an image	Root Cause - Windows Azure\Virtual Machine\Guest OS - Windows\Isolated\Firewall misconfigured\Lack of preparation prior migration - Firewall not setup	
3	Azure Virtual Machine ❖ Windows	Routing Azure Virtual Machine V3\Cannot Connect to my VM\Troubleshoot my network security group (NSG)	Root Cause - Windows Azure\Virtual Machine\Guest OS - Windows\VM Responding\Activity Directory issues\GPO preventing RDP	
4	Azure Virtual Networks	Routing Azure Virtual Network V3\Connectivity\Cannot connect to virtual machine using RDP or SSH	Root Cause - Windows Azure\Virtual Network\Internet Service Provider/Third Party Network	

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

## Customer Enablement

- [Azure VM Guest OS firewall is blocking inbound traffic](#) 

## Mitigation

Depending on the type of traffic blocking the firewall is doing, CSE may work however bear in mind that if the network stack is fully blocked, CSE will *NOT* work at all.



### 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*

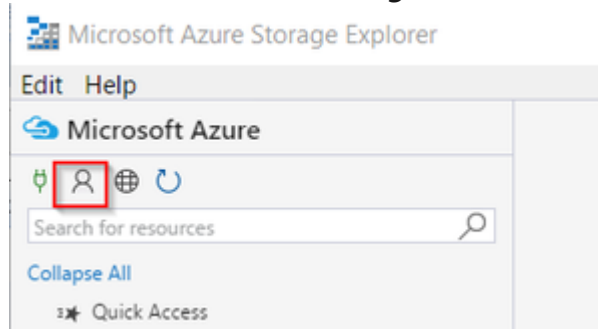
OS Disk Lease Id	Udb9a55c-0317-40fa-a032-b1f3550f3775
OS Disk Lease Acquired	True
OS Disk Billing Validated	True
OS Disk Encrypted	False
Billing Code	Windows_IaaS
Billing is Created from Marketplace Image	N/A
Billing Tag GUID	00000000-0000-0000-0000-000000000000

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

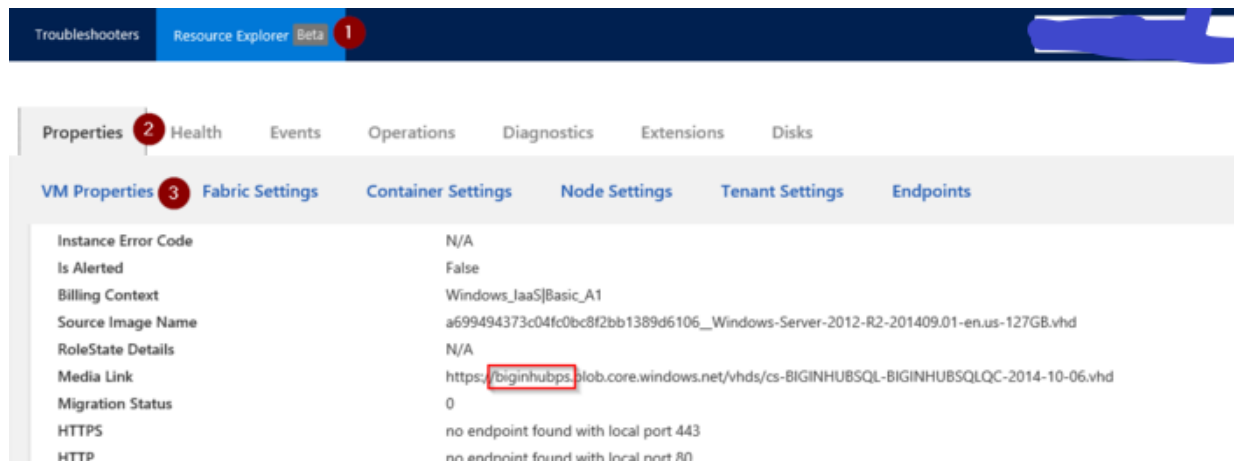
1. If the **disk is unmanaged**, this could be done by using [Microsoft Azure Storage Explorer](#)  or [Azure Powershell](#) 

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

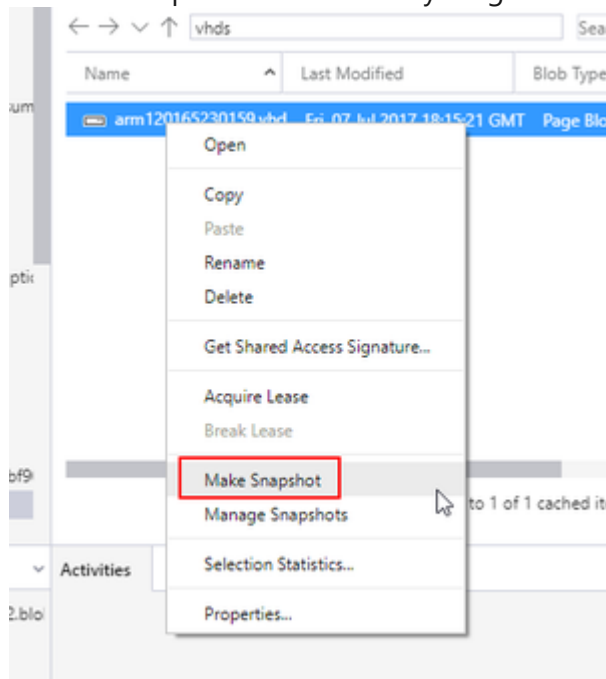
1. Once the customer download the tool, proceed to add the Azure account details so you can access the storage accounts
2. Click on **Add Account Settings** then \*\*\*Add an account...\*\*\*



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

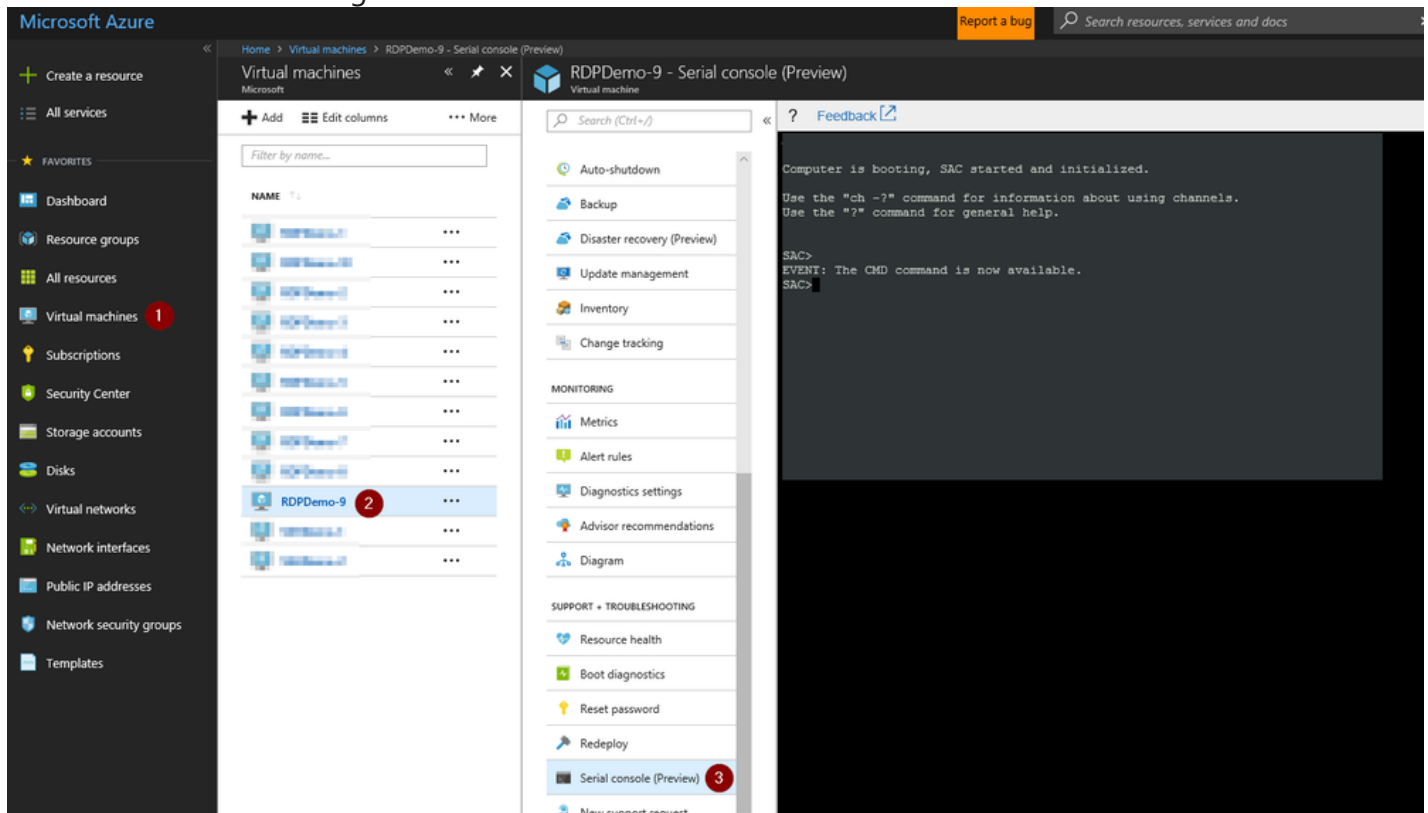
See [How To Access Thru Windows Admin Center](#)

### 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:

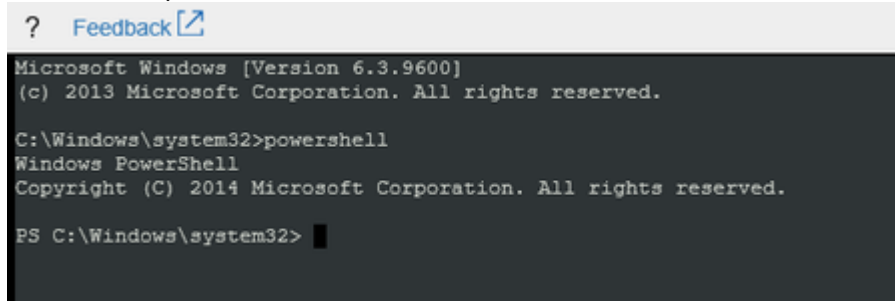
```
? Feedback
Please enter login credentials.
Username:
```

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`

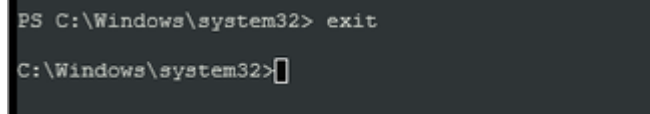


```
? Feedback
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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. Open a PowerShell instance and query to see which how is setup the *Remote Desktop*' rules:

Disclaimer: If you plan on running the following PowerShell commands from the Serial Console, make sure you run **Remove-Module PSReadline** first, to avoid having duplicated characters when pasting them.

1. To query all the rules with the names *Remote Desktop*:

```
#PowerShell
netsh advfirewall firewall show rule dir=in name=all | select-string -pattern "(Name.*Remote Desktop
```



or

#PowerShell

Get-NetFirewallRule -DisplayGroup "Remote Desktop" | Get-NetFirewallAddressFilter

```

? Feedback [Feedback icon] [Settings icon]

Grouping: Core Networking
LocalIP: Any
RemoteIP: Any
Protocol: ICMPv6
Type: 1
Code: Any
Edge traversal: Yes
Action: Allow

> Rule Name: Remote Desktop - Shadow (TCP-In)
-----
Enabled: Yes
Direction: In
Profiles: Domain, Private, Public
Grouping: Remote Desktop
LocalIP: Any
RemoteIP: Any
Protocol: TCP
LocalPort: Any
RemotePort: Any
Edge traversal: Defer to application
Action: Allow
-- More --

? Feedback [Feedback icon] [Settings icon]

> Rule Name: Remote Desktop - User Mode (UDP-In)
-----
Enabled: Yes
Direction: In
Profiles: Domain, Private, Public
Grouping: Remote Desktop
LocalIP: Any
RemoteIP: Any
Protocol: UDP
LocalPort: 3389
RemotePort: Any
Edge traversal: No
Action: Allow

> Rule Name: Remote Desktop - User Mode (TCP-In)
-----
Enabled: Yes
Direction: In
Profiles: Domain, Private, Public

PS C:\Windows\system32>

```

2. In the case where the RDP port was set to any other than 3389, you need to get which is the custom rule created if any with that port. To query the custom RDP port:

#PowerShell

Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\RDP-Tcp'



3. To query for all the inbound rules with a custom port:

#PowerShell

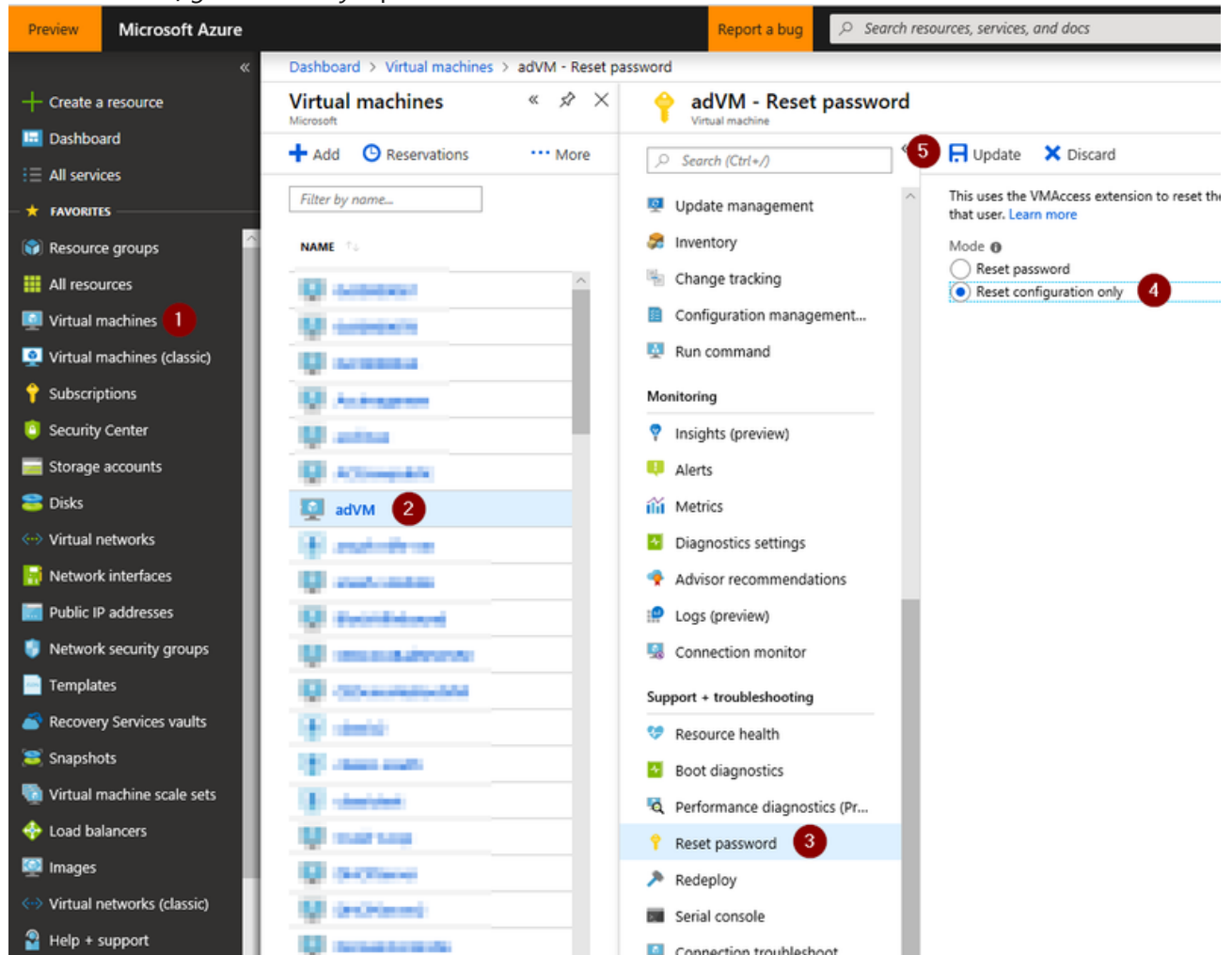
netsh advfirewall firewall show rule dir=in name=all | select-string -pattern "(LocalPort.\*&lt;CUSTOM P



2. If you see the rule is disabled, then open it:

1. In case that the VM has a healthy *Azure Agent* installed, then you can leverage the *VMAccess* extension

1. Use *Reset configuration only* option from the *Password reset* menu:



2. This will

1. Enable RDP component in case it is disabled
2. Enable all windows firewall profiles
3. Ensure the RDP Rule is turned on in the Windows Firewall

2. In case this fails, you can use SAC

1. To open a whole group like the builtin group *Remote Desktop*:

REM CMD

```
netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes
```

or

#PowerShell

```
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
Set-NetFirewallRule -DisplayGroup "Remote Desktop" -Profile "Private,Domain,Public"
Get-NetFirewallrule -Name "RemoteDesktop-UserMode-In-TCP" | Get-NetFirewallAddressFilter | Set-I
```

1. Otherwise, to open the rule *Remote Desktop (TCP-In)* is enough for RDP access
2. To open a custom rule which you know is opening the custom rdp port:

REM CMD

```
netsh advfirewall firewall set rule name="<CUSTOM RULE NAME>" new enable=yes
```

3. If for troubleshooting purposes you need to turn the firewall profiles OFF:

REM CMD

```
netsh advfirewall set allprofiles state off
```

1. If you went this route, after you finish your troubleshooting setting the firewall correctly, enable the firewall back.
4. You don't need to restart the VM, the VM will be back reachable on that network card

#### Mitigation 2

▼ Click here to expand or collapse this section

1. Open a CMD instance and query the firewall profiles and you will see that the inbound firewall policy is set to *Block inbound* the traffic always:

REM CMD

```
netsh advfirewall show allprofiles | more
```

```

? Feedback [link] [gear] [grid] fn

Domain Profile Settings:
-----
State                                ON
Firewall Policy                      BlockInboundAlways,AllowOutbound
LocalFirewallRules                  N/A (GPO-store only)
LocalConSecRules                    N/A (GPO-store only)
InboundUserNotification              Disable
RemoteManagement                    Disable
UnicastResponseToMulticast           Enable

Logging:
LogAllowedConnections                Disable
LogDroppedConnections                Disable
FileName                             %systemroot%\system32\LogFiles\Firewall\pf
firewall.log
MaxFileSize                          4096

Private Profile Settings:
-----
State                                ON
Firewall Policy                      BlockInboundAlways,AllowOutbound
-- More --

? Feedback [link] [gear] [grid] fn

LocalFirewallRules                  N/A (GPO-store only)
LocalConSecRules                    N/A (GPO-store only)
InboundUserNotification              Disable
RemoteManagement                    Disable
UnicastResponseToMulticast           Enable

Logging:
LogAllowedConnections                Disable
LogDroppedConnections                Disable
FileName                             %systemroot%\system32\LogFiles\Firewall\pf
firewall.log
MaxFileSize                          4096

Public Profile Settings:
-----
State                                ON
Firewall Policy                      BlockInboundAlways,AllowOutbound
LocalFirewallRules                  N/A (GPO-store only)
LocalConSecRules                    N/A (GPO-store only)
InboundUserNotification              Disable
RemoteManagement                    Disable
UnicastResponseToMulticast           Enable
-- More --

? Feedback [link] [gear] [grid] fn

Public Profile Settings:
-----
State                                ON
Firewall Policy                      BlockInboundAlways,AllowOutbound
LocalFirewallRules                  N/A (GPO-store only)
LocalConSecRules                    N/A (GPO-store only)
InboundUserNotification              Disable
RemoteManagement                    Disable
UnicastResponseToMulticast           Enable

Logging:
LogAllowedConnections                Disable
LogDroppedConnections                Disable
FileName                             %systemroot%\system32\LogFiles\Firewall\pf
firewall.log
MaxFileSize                          4096

Ok.

C:\Windows\system32>

```

**Note:** If the Firewall Policy is setup to:

- *BlockInbound*: Means that all inbound traffic will be block except you have a rule allowing that traffic

- *BlockInboundAlways*: Means that all the firewall rules will be ignored and all traffic will be blocked
2. Modify the *DefaultInboundAction* for these profiles to *Allow* the traffic:

REM CMD

```
netsh advfirewall set allprofiles firewallpolicy allowinbound,allowoutbound
```

3. If for troubleshooting purposes you need to turn off all the firewall profiles

REM CMD

```
netsh advfirewall set allprofiles state off
```

1. If you went this route, after you finish your troubleshooting setting the firewall correctly, enable the firewall back.
4. Query the profiles again to ensure your change was done successfully:

REM CMD

```
netsh advfirewall show allprofiles | more
```

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

### Mitigation 3

▼ Click here to expand or collapse this section

This applies **only** for Microsoft corp domain machines.

1. Please refer to the *Mitigation 1* from [Microsoft Corp domain joined machines](#)

### Mitigation 4

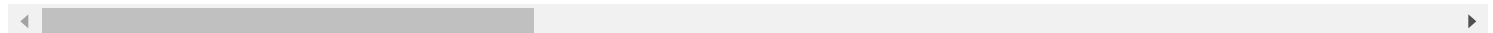
▼ Click here to expand or collapse this section

This applies **only** for Microsoft corp domain machines.

1. Please refer to the *Mitigation 2* from [Microsoft Corp domain joined machines](#)

## 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

▼ Click here to expand or collapse this section

1. Refer [How to Enable-Disable a Firewall rule on a Guest OS](#)

### Mitigation 2

▼ Click here to expand or collapse this section

1. Now open an elevated CMD instance and run the following script:

```
REM CMD
reg load HKLM\BROKENSYSTEM f:\windows\system32\config\SYSTEM

REM Delete the keys to block all inbound connection scenario
REG DELETE "HKLM\BROKENSYSTEM\ControlSet001\services\SharedAccess\Parameters\FirewallPolicy\DomainProfile
REG DELETE "HKLM\BROKENSYSTEM\ControlSet001\services\SharedAccess\Parameters\FirewallPolicy\PublicProfile
REG DELETE "HKLM\BROKENSYSTEM\ControlSet001\services\SharedAccess\Parameters\FirewallPolicy\StandardProfi

REG DELETE "HKLM\BROKENSYSTEM\ControlSet002\services\SharedAccess\Parameters\FirewallPolicy\DomainProfile
REG DELETE "HKLM\BROKENSYSTEM\ControlSet002\services\SharedAccess\Parameters\FirewallPolicy\PublicProfile
REG DELETE "HKLM\BROKENSYSTEM\ControlSet002\services\SharedAccess\Parameters\FirewallPolicy\StandardProfi

reg unload HKLM\BROKENSYSTEM
```

### Mitigation 3

▼ Click here to expand or collapse this section

This applies **only** for Microsoft corp domain machines.

1. Please refer to the *Mitigation 1* from [Microsoft Corp domain joined machines](#)

### Mitigation 4

▼ Click here to expand or collapse this section

This applies **only** for Microsoft corp domain machines.

1. Please refer to the *Mitigation 2* from [Microsoft Corp domain joined machines](#)

## 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 - RDP 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 <a href="#">RDP-SSH SMEs</a> ☑ for faster assistance.</p> <p>Make sure to use the <a href="#">Ava process</a> for faster assistance.</p>	<p>Use the <a href="#">RDP-SSH Feedback</a> form to submit detailed feedback on improvements or new content ideas for RDP-SSH.</p> <p><b>Please note</b> 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 <a href="#">RDP-SSH Kudos</a> form to submit kudos on the page. Kudos will help us improve our wiki content overall!</p> <p><b>Please note</b> the link to the page is required when submitting kudos!</p>