Guest OS Firewall Misconfigured_RDP SSH

Last updated by | Heath Rensink | Sep 28, 2022 at 9:02 AM PDT

Tags

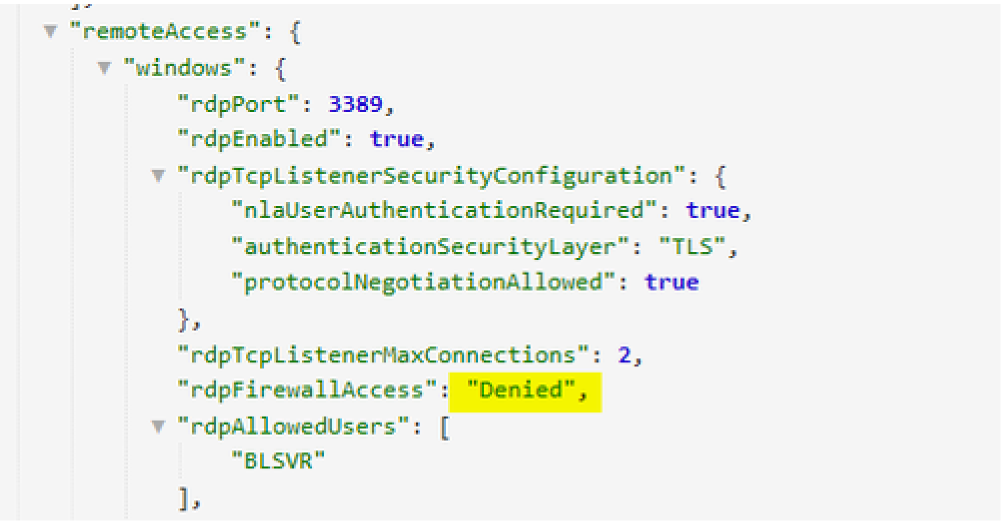
cw.TSG	cw.RDP-SSH

Contents

Symptoms

1. You find the Virtual Machine screenshot showing that the VM is fully up on the logon screen
2. There's no connectivity to the virtual machine on its VIP or DIP, verified with VM Port Scanner.

3. In ***WinGuestAnalyzer\Health Signal*** tab in the *remoteaccess* section, you can see if RDP is allowed or not in the firewall:



```
▼ "remoteAccess": {
    ▼ "windows": {
          "rdpPort": 3389,
          "rdpEnabled": true,
        ▼ "rdpTcpListenerSecurityConfiguration": {
              "nlaUserAuthenticationRequired": true,
              "authenticationSecurityLayer": "TLS",
              "protocolNegotiationAllowed": true
          },
          "rdpTcpListenerMaxConnections": 2,
          "rdpFirewallAccess": "Denied",
        ▼ "rdpAllowedUsers": [
              "BLSVR"
          ],
```

Root Cause Analysis

Misconfiguration of the Guest OS Firewall could block some or all type of network traffic to the VM. Azure Virtual machines, the only type of access is thru RDP so if this traffic is not enable, this machine will not be reachable over the network.

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.

Deploy to Azure

References

N/A

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\Firewall misconfigured\Rule not enabled*	
	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\Guest OS - Windows\Isolated\Firewall misconfigured\Lack of preparation prior migration - Firewall not setup*	

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 misconfigured

Mitigation

Ideally, all the firewall profiles should be enable and then the rules needs to be setup properly. However if your customer wants to have a combination of profiles ON/OFF, if the firewall rules are not properly setup, you will have scenarios where when the OS switch to another firewall profile, either if the customer wants that to be or not, your traffic will be impacted in some way and you will have disconnections. This is the reason why Microsoft suggest to have all the profiles ON and then with the proper rules.

An example on this would be migration cases from onprem to Azure using ASR that the moment the machine is deployed in azure. Imagine a customer that in onprem have the Domain profile OFF since he was not using that but then didn't change any configuration on the Public profile which by default is going to be ON. Then the moment the machine is created in azure, if there's any problem to contact the domain controller, your firewall profile will switch to public so all the rules which includes the public profile will work on the VM only.

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.

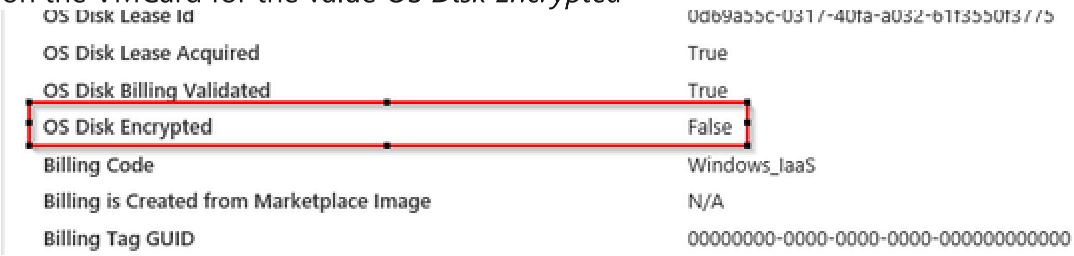
1. These are the following rules that you may be interested on changing to either enable access to the VM (RDP) or to have an easier troubleshooting experience:
   1. *Remote Desktop (TCP-In)* rule, this allows the RDP access to the VM, in azure this is a must to have and the primary access to the VM.
   2. *Windows Remote Management (HTTP-In)* rule, to enable connect to the machine using powershell, in azure this type of access is nice to have to then leverage the scripting aspect of remote scripting/troubleshooting

    3. *File and Printer Sharing (SMB-In)* rule, to enable network share type of access, this also depends on the customer however for troubleshooting aspects, you may want to consider opening this during your troubleshooting.
    4. *File and Printer Sharing (Echo Request - ICMPv4-In)* rule, in case the customer wants to be able to ping the machine. This will depend on the customer.

Backup OS disk

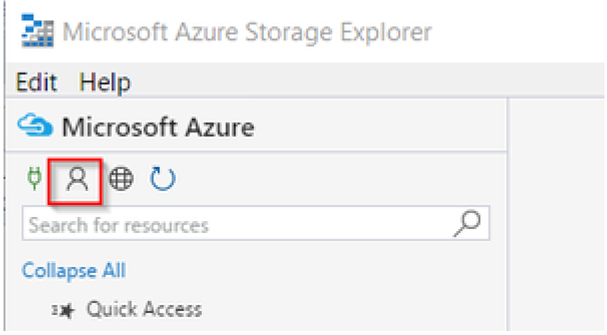
▼ Click here to expand or collapse this section

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*

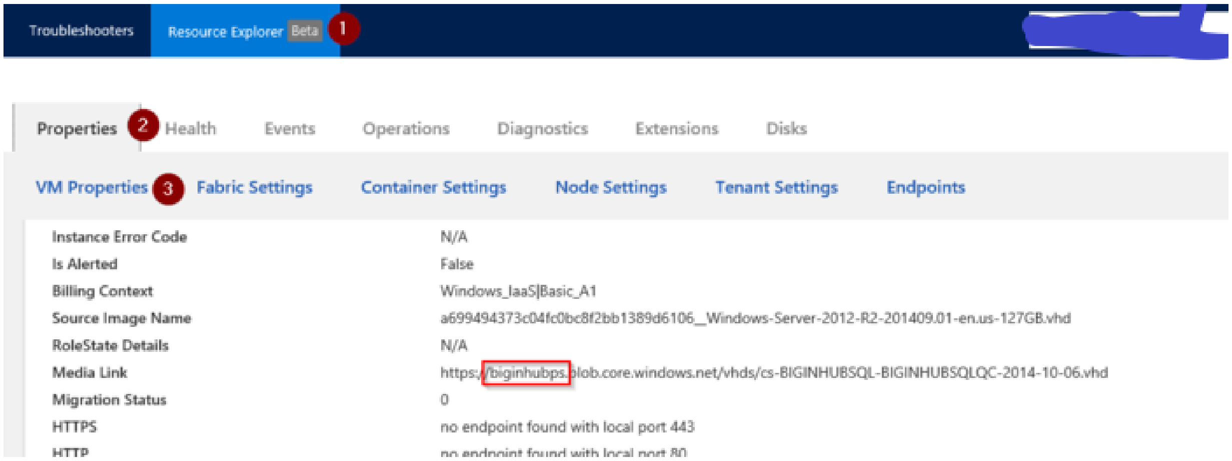


OS Disk Lease Id	0d69a55c-0317-40fa-a032-61f3550f3775
OS Disk Lease Acquired	True
OS Disk Billing Validated	True
OS Disk Encrypted	False
Billing Code	Windows_IaaS
Billing is Created from Marketplace Image	N/A
Billing Tag GUID	00000000-0000-0000-0000-000000000000

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...***

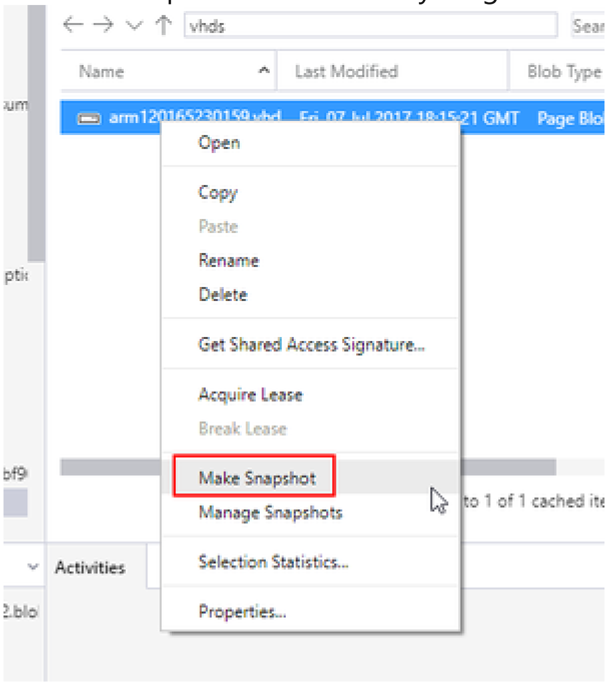


            3. Go to the storage account where the OS disk is, you can see this on ASC under *Resource Explorer* on *Properties* in the *VM Properties* card



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

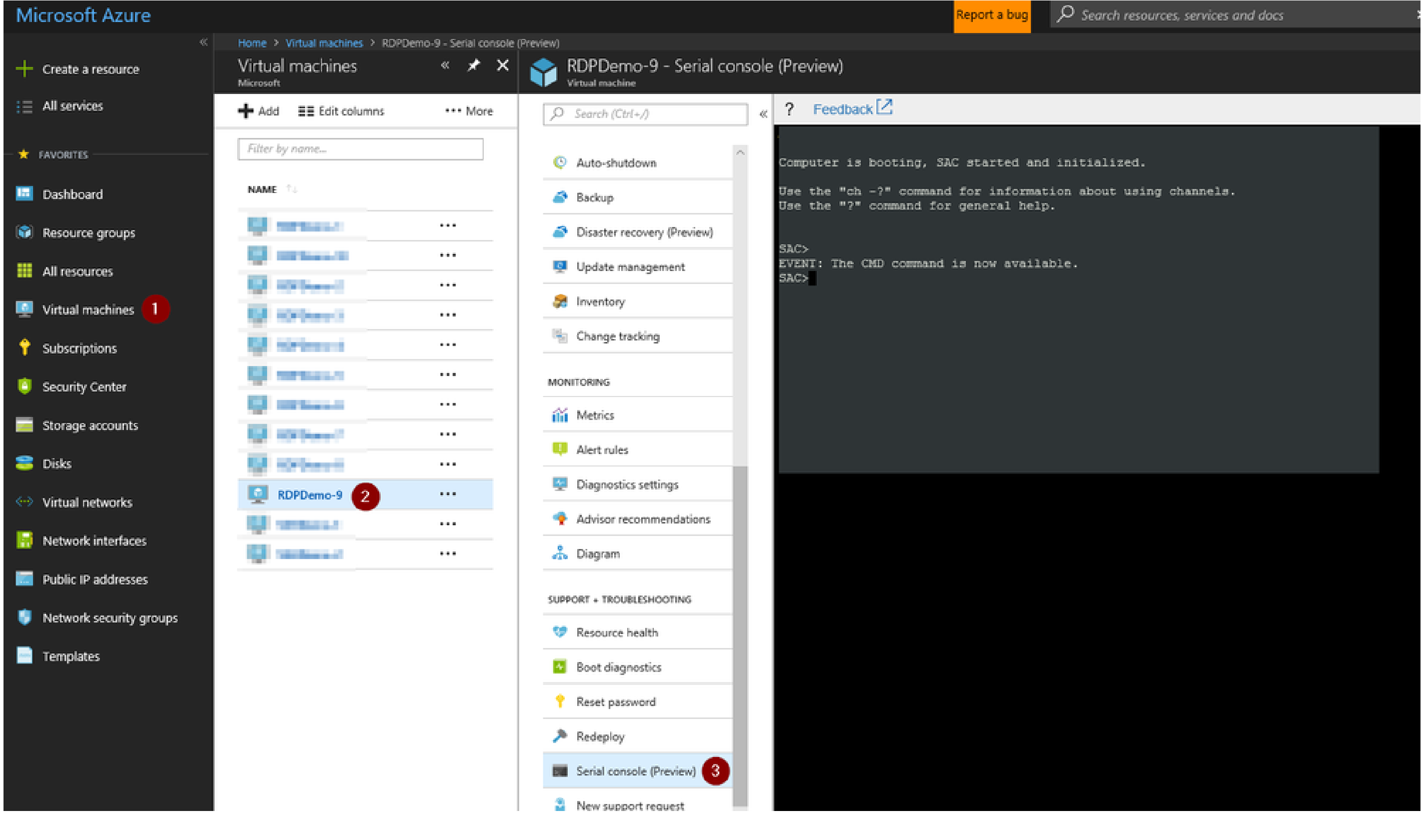
WAC is supported on ARM VMs running Windows Server 2016 or later (not Win10 or any other Windows client version, and not 2012R2/2012/2008R2 versions of Windows Server

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:

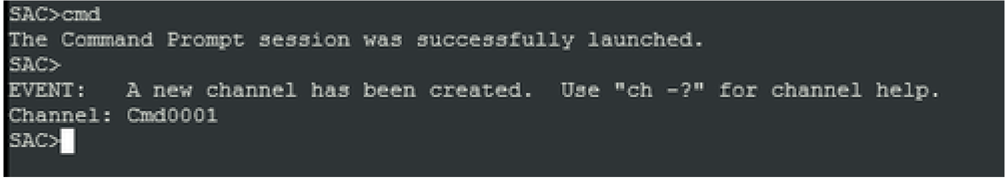


```
Computer is booting, SAC started and initialized.

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

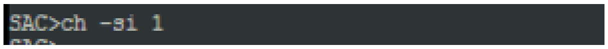
3. Create a channel with a CMD instance. Type `cmd` to start the channel, you will get the name of the channel



```
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>
```

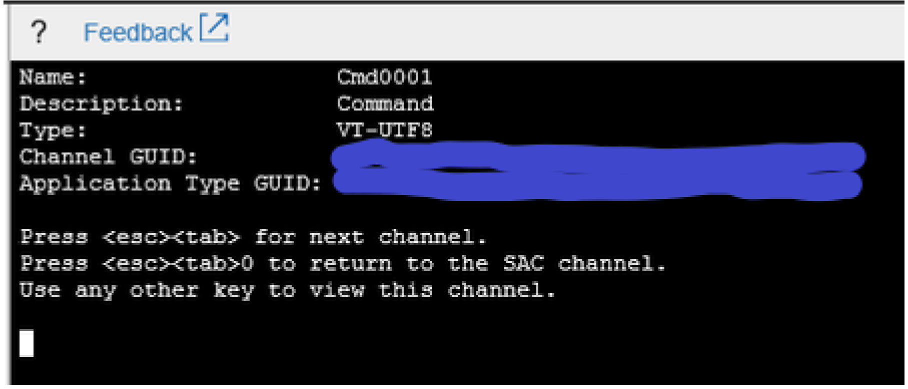
4. Switch to the channel running the CMD instance

```
ch -si 1
```



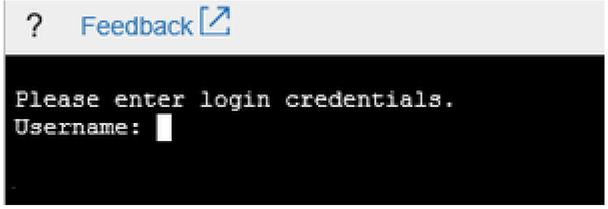
```
SAC>ch -si 1
```

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.
```

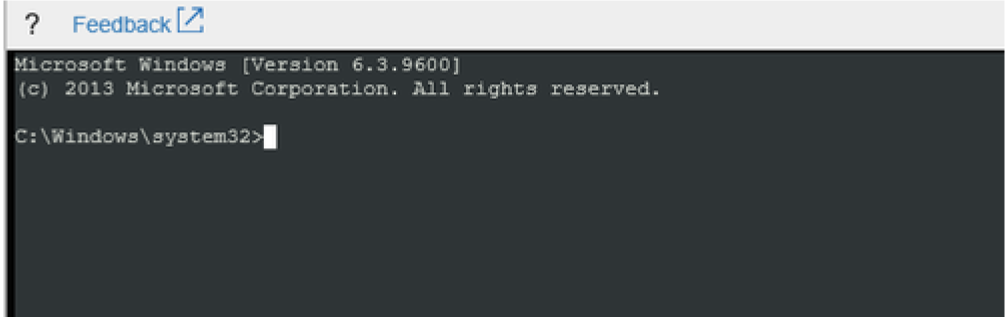
6. Hit enter a second time and it will ask you for user, domain and password:



```
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.

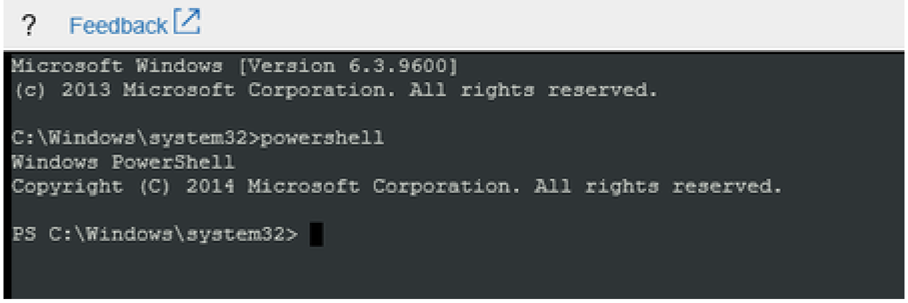
7. Once you add valid credentials, the CMD instance will open and you will have the prompt for you to start your troubleshooting:



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

C:\Windows\system32>
```

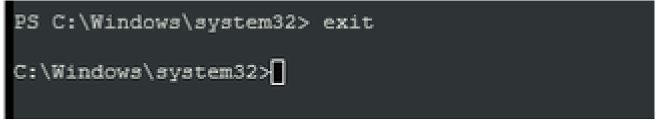
   1. At this point, you can do your troubleshooting in bash (CMD) or else, you could start a powershell instance:

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

▼ Click here to expand or collapse this section

1. This is the generic way to handle a firewall rule on the VM. Open a CMD instance and query the current status of the rule:

   1. How to query using the *Display Name* as a parameter:

      ```
      netsh advfirewall firewall show rule dir=in name=all | select-string -pattern "(DisplayName.*<FI
      ```

   2. How to query using the *Local Port* the application is using:

      ```
      netsh advfirewall firewall show rule dir=in name=all | select-string -pattern "(LocalPort.*<APPL
      ```

   3. How to query using the *Local IP* the application is using:

      ```
      netsh advfirewall firewall show rule dir=in name=all | select-string -pattern "(LocalIP.*<CUSTOM
      ```

2. If you see the rule disabled, then you can enable it as the following:

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

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

   ```
   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 for this change to kick in

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. To enable/disable Firewall rules please refer to Enable-Disable a Firewall rule on a Guest OS

2. You can also check if you are in the GuestOS firewall blocking inbound traffic scenario
3. Furthermore, if you are still in doubt if the firewall is blocking your access, as a troubleshooting step you can proceed to Disable the Guest OS Firewall on Windows however then the best practices are to enable the GuestOS firewall back with the correct rules.

Escalate

1. If this doesn't work out, please reach out to the Unable to RDP-SSH SME channel on teams for advise providing the case number, issue description and your question

After work - Cleanup

If you are uncertain that we may need this snapshot by the end of this case for RCA purposes, then just leave it.

1. If the issue is already fix and no further RCA analysis is needed, then proceed to remove the OS Disk backup we created at the beginning of the case
   1. If the **disk is managed** using the portal so the snapshot section and select the snapshot you created previously as a backup.
   2. If the **disk is unmanaged** then
      1. If this is an CRP Machine - ARM, then no further action is required
      2. If this is an Classic - RDFE machine, then
         1. Check the storage account where the OS disk of this machine is hosted using Microsoft Azure Storage Explorer right click over the disk and select *Managed Snapshots*
         2. Proceed to delete the snapshot of the broken machine

Need additional help or have feedback?

To engage the Azure RDP-SSH SMEs...	*To provide feedback on this page...*	*To provide kudos on this page...*
Please reach out to the **RDP-SSH SMEs** for faster assistance. Make sure to use the **Ava process** for faster assistance.	Use the **RDP-SSH Feedback** form to submit detailed feedback on improvements or new content ideas for RDP-SSH. ***Please note*** the link to the page is required when submitting feedback on existing pages! If it is a new content idea, please put N/A in the Wiki Page Link.	Use the **RDP-SSH Kudos** form to submit kudos on the page. Kudos will help us improve our wiki content overall! ***Please note*** the link to the page is required when submitting kudos!