

# Symantec Blocking Incoming Traffic\_RDP SSH

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

---

Tags

cw.TSG

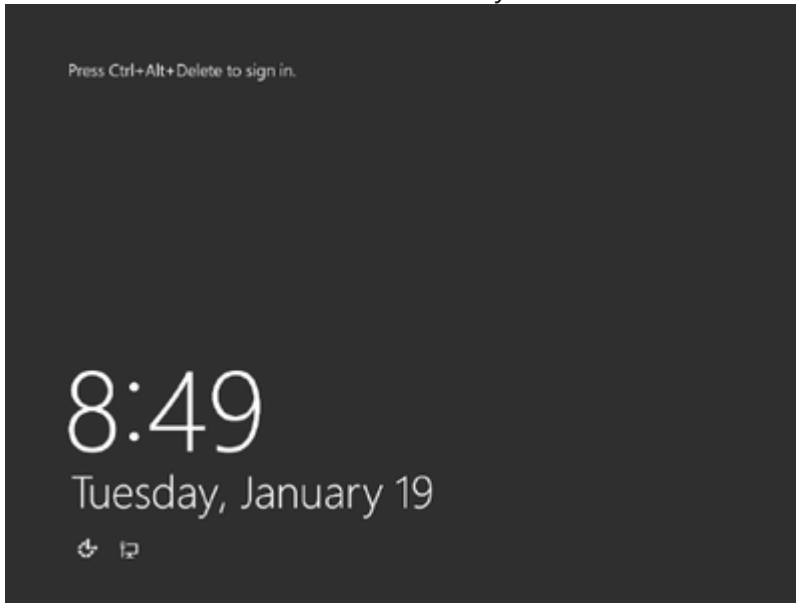
cw.RDP-SSH

## Contents

- Symptoms
  - Software version tried with this article
- Root Cause Analysis
  - 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
  - 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
      - Mitigation 1
      - Mitigation 2
      - Mitigation 3
  - Escalate
  - After work - Cleanup
- Need additional help or have feedback?

## Symptoms

- The VM screenshot shows the OS fully loaded at CAD screen (Ctrl+Alt+Del)



- On the Guest OS logs you will not find connections being made
- WaAppAgent logs shows the machine is doing heartbeat normally.
- As soon as the VM is restarted, ***you could have connectivity for almost a minute*** and then you are kicked out and the machine reject inbound traffic
- The software *Symantec Endpoint Protection* is installed on the VM

## Software version tried with this article





- Symantec Endpoint Protection 12.1

**Note:** If your case is solved by this very same action plan and you have a different version than the ones described in this section, please provide your feedback at the end of this page so we can add your version in this article. Thanks.

## Root Cause Analysis

Symantec Endpoint Protection firewall is blocking the network inbound traffic.

## References

- [Uninstall the Endpoint Protection client using the command prompt](#) 
- [How to manually stop and start the Symantec Endpoint Protection service](#) 
- [The SMC -stop command does not work from a CMD window](#) 
- [Commands for the Windows client service smc in Symantec Endpoint Protection and Symantec Endpoint Security](#) 

## 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> <i>Routing Azure Virtual Machine V3\Cannot Connect to my VM\Failure to connect using RDP or SSH port</i>	<i>Root Cause - Windows Azure\Virtual Machine\Third Party Issues/Questions</i>	
	Azure Virtual Machine – Windows	<b>For new migrated machines:</b> <i>Routing Azure Virtual Machine V3\Cannot create a VM\I need guidance preparing an image</i>	<i>Root Cause - Windows Azure\Compute\Migration\On-prem to Azure - ASR\Third Party filter/driver</i>	

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

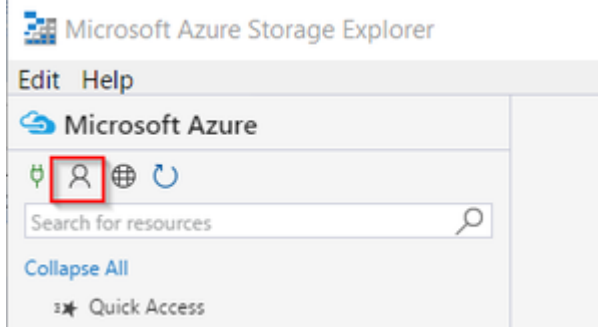
▼ Click here to expand or collapse this section

- 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*

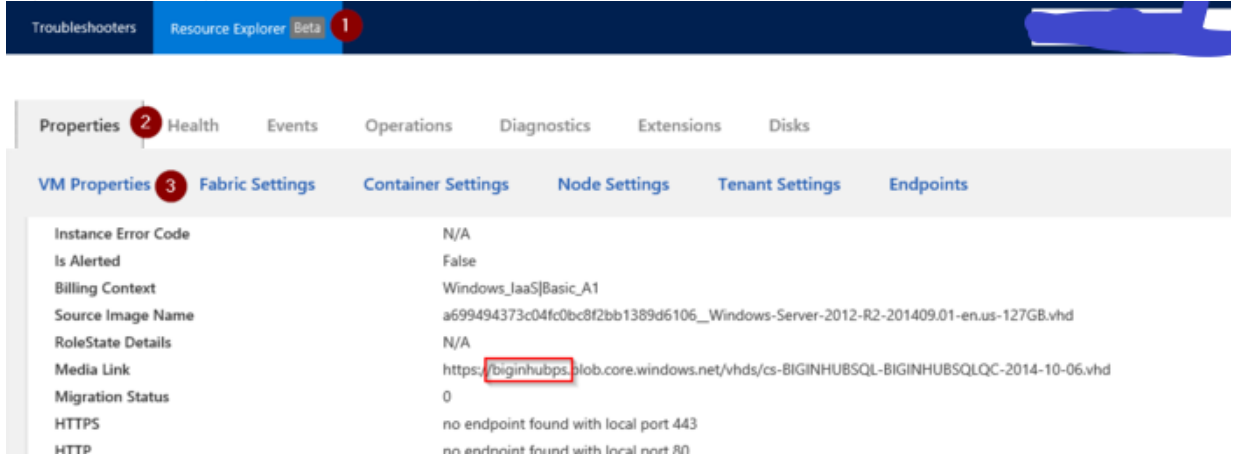
OS Disk Lease Id	0d69a55c-0317-40fa-a032-b1f3550f3775
OS Disk Lease Acquired	True
OS Disk Billing Validated	True
OS Disk Encrypted	False
Billing Code	Windows_IaaS
Billing is Created from Marketplace Image	N/A
Billing Tag GUID	00000000-0000-0000-0000-000000000000

- If the OS Disk is encrypted, then proceed to [Unlock an encrypted disk](#)
- 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
- Power the machine down and once it is stopped de-allocated to do the copy.
- Create a snapshot
  - If the **disk is unmanaged**, this could be done by using [Microsoft Azure Storage Explorer](#) or [Azure Powershell](#)
    - Using [Microsoft Azure Storage Explorer](#)
      - Once the customer download the tool, proceed to add the Azure account details so you can access the storage accounts

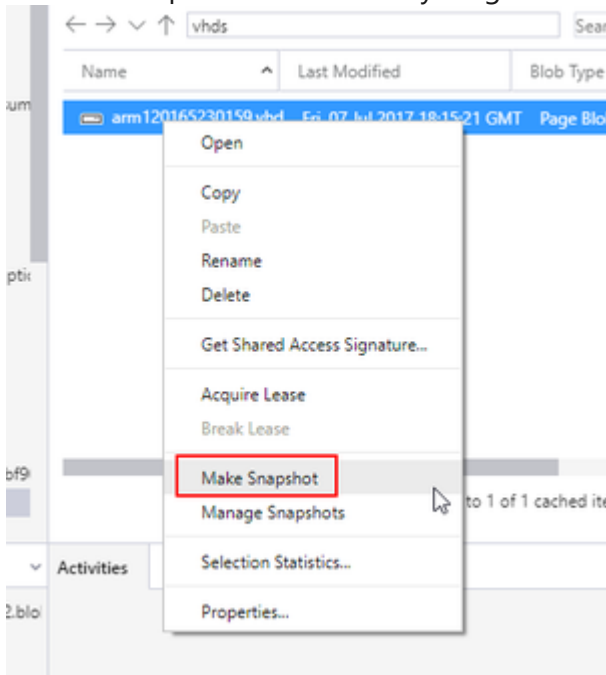
2. Click on **Add Account Settings** then \*\*\*Add an account...\*\*\*



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

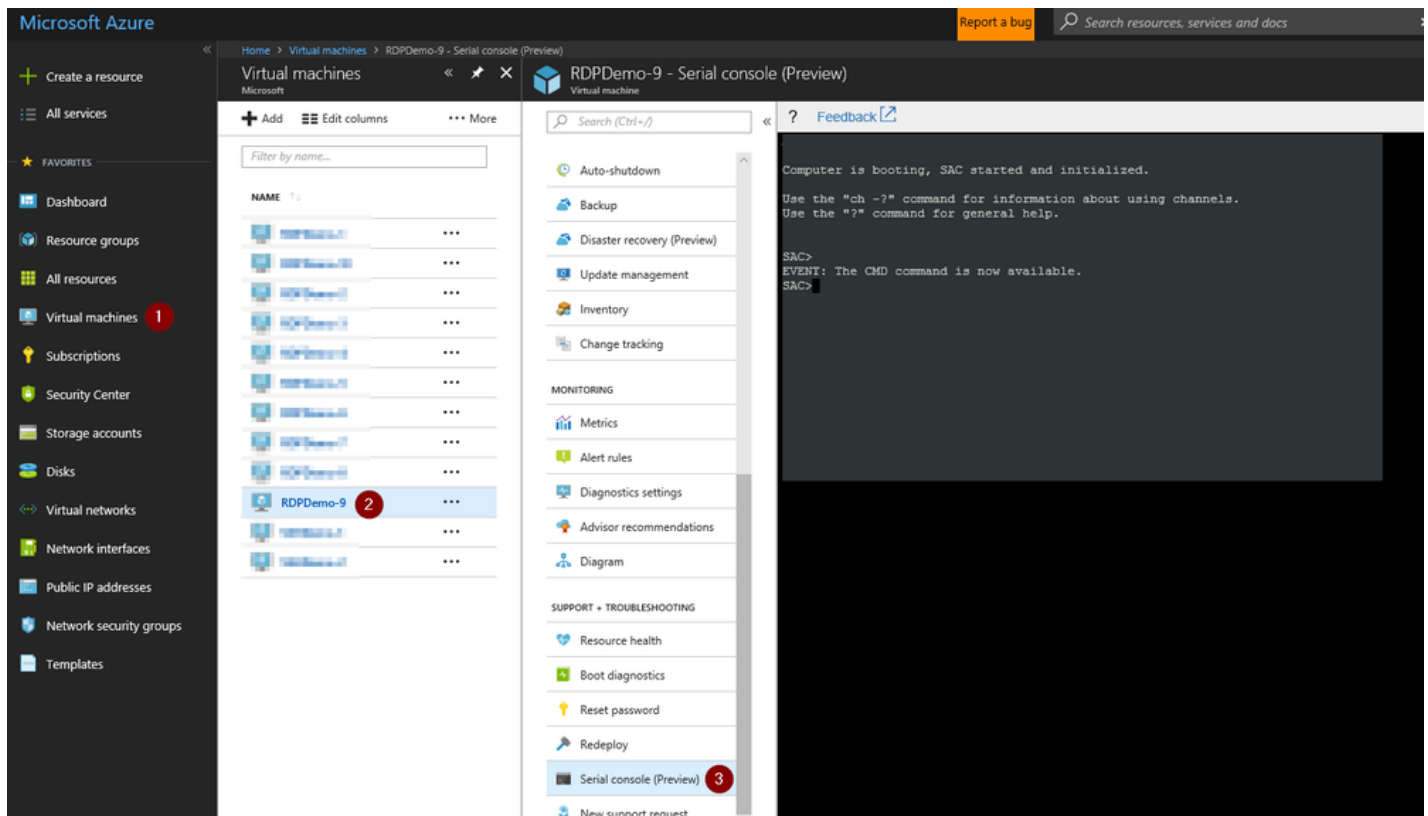
See [How To Access Thru Windows Admin Center](#)

#### 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
```

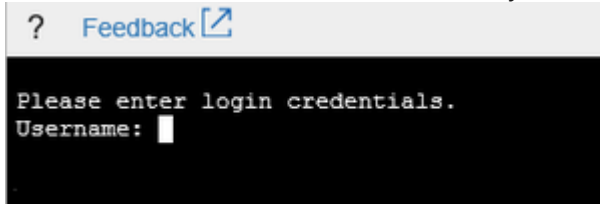
```
SAC>ch -si 1
```

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

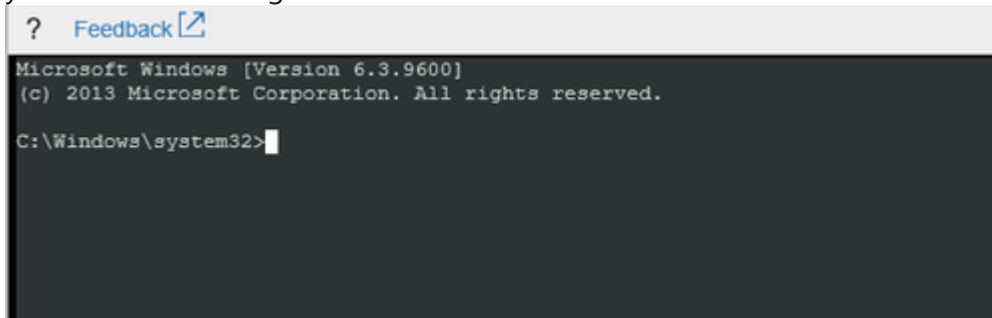
```
? Feedback
Name: Cmd0001
Description: Command
Type: VT-UTF8
Channel GUID: [REDACTED]
Application Type GUID: [REDACTED]

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:

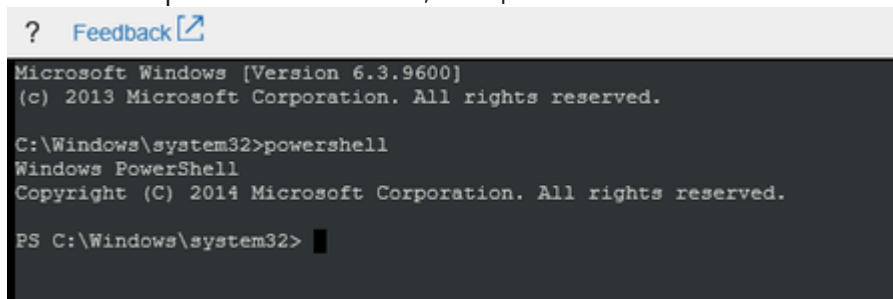


1. If the machine has connectivity, you could use either local or domain IDs. If you want to use a local ID, for domain just add the hostname of the VM
  2. If the machine doesn't have connectivity, you could try to use domains IDs however this will work if only the credentials are cached on the VM.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

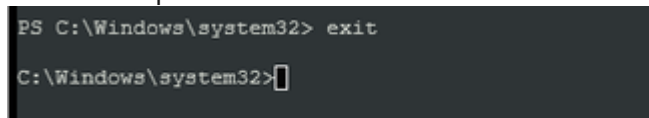


1. At this point, you can do your troubleshooting in bash (CMD) or else, you could start a powershell instance:

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

1. Get the ***list of the services*** you need to disable the *WinGuestAnalyzer* report

### Mitigation 1

▼ Click here to expand or collapse this section

Try to stop/disable the main services only:

1. Open a CMD instance and check the current state of the services:

```
sc query SepMasterService
sc query SmcService
sc query SNAC
```

2. Try stopping the services:

```
sc stop SepMasterService
sc stop SmcService
sc stop SNAC
```

3. See if you can RDP back into the VM. If you run into issues or it hangs on stopping, then just disable the services:

```
sc config SepMasterService start=disabled
sc config SmcService start=disabled
sc config SNAC start=disabled
```

Then Reboot the VM.

4. If the above fails, try one of the following smc commands:

```
start smc -stop OR smc -stop
```

If Symantec is password protected, the cx will need to add the -p paramater and add the password as well:

```
start smc -p PASSWORD -stop OR smc -p PASSWORD -stop
```

### Mitigation 2

▼ Click here to expand or collapse this section

Try removing the software:

1. Open a Powershell instance and run the following to remove the software:


```
(Get-WmiObject -Class Win32_Product -Filter "Name='Symantec Endpoint Protection'" -ComputerName .).Unins
```

A successful uninstall will return a message that ends with "ReturnValue: 0"

2. If the name of the particular version of Symantec is not exactly 'Symantec Endpoint Protection', you can get the exact name of the Symantec-based AV, then remove that application:

```
Get-WmiObject -Class Win32_Product | where {$_.Name -like "*symantec*"}
# get the name of the app from the above command then enter it in $name below
$name = 'ENTER_NAME_HERE'
(Get-WmiObject -Class Win32_Product -Filter "Name='$name'" -ComputerName .).Uninstall()
```

Note: If Symantec is password protected, the cx should disable it first:



<https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/managing-groups-clients-and-administrators/managing-client-computers-v55115300-d19e131/password-protecting-the-client-v9722139-d19e3958.html> 

3. Reboot the VM and if this is still not fixed, then proceed with the following mitigation.

#### Mitigation 3

- ▼ Click here to expand or collapse this section

1. A memory dump from the VM needs to be collected **while the VM is on state**.

1. Confirm if customer has already granted permission in DfM "Product details" section: Customer permission granted: Yes If No, ask the customer to go to their case in the Portal and grant us permission to look at OS logs. An example email can be found at: <https://aka.ms/azdataperm/> 
2. Refer to [How to Get an OS Dump from an Azure Virtual Machine](#)
3. Once the memory dump was collected, then engage the [GES team](#)  (Windows EEs) for a dump analysis. Cut a problem with the following details:
  - Product: **Windows Svr 2008 R2** or **Windows Svr 2012 R2 Datacenter** or **Windows Svr 2016 Datacenter** or **Windows Svr 2019 Datacenter** as appropriate
  - Support topic: **Routing Windows V3\System Performance\System Hangs**
  - Problem Description:

```
===== <start copy> =====
Customer-facing error (RDP client error):
Symptoms description:

SR#
VM name
ICM#          <--- Only if the dump was collected from the Host
Datacenter    <--- Only if the dump was collected from the Host
Jumpbox       <--- Only if the dump was collected from the Host
Path in the jumpbox <--- Only if the dump was collected from the Host
===== <end copy> =====
```

- These routing will route you to a Windows team however since we need to engage GES, override the routing to

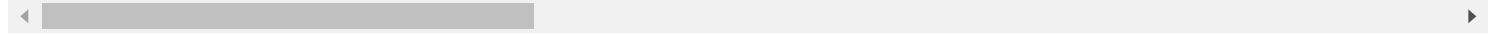
- For Premier cases: **Windows EE Premier** queue
- For Professional cases: **Windows EE Pro** queue

2. Proceed with the action plan provided by the Windows EE

## 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

1. Get the **list of the services** you need to disable the *WinGuestAnalyzer* report

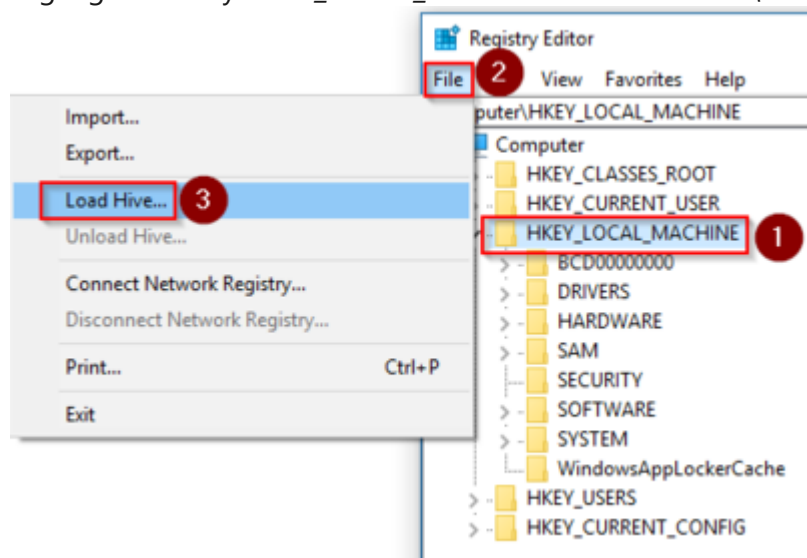
#### Mitigation 1

▼ Click here to expand or collapse this section

This mitigation will attempt to disable the software.

1. Before doing any change please create a copy of the folder `\windows\system32\config` in case a rollback on the changes is needed
2. On the troubleshooting machine, open the registry editor *REGEDIT*

- Highlight the key *HKEY\_LOCAL\_MACHINE* and select *File\Load Hive* from the menu



- Browse up to the file `\windows\system32\config\SYSTEM`
- When you hit open it's going to ask for a name, put *BROKENSYSTEM* and then expand *HKEY\_LOCAL\_MACHINE* and you will see an extra key called *BROKENSYSTEM*. For this troubleshooting, we are mounting these trouble hives as *BROKENSYSTEM*
- Check which ControlSet is the machine booting from. You will see its key number in `HKLM\BROKENSYSTEM\Select\Current`
- Disable the Symantec Endpoint Protection services

```
Set-ItemProperty -Path 'HKLM:\BROKENSYSTEM\ControlSet00x\Services\SepMasterService' -name 'Start' -Value 4
Set-ItemProperty -Path 'HKLM:\BROKENSYSTEM\ControlSet00x\Services\Smcinst' -name 'Start' -Value 4
Set-ItemProperty -Path 'HKLM:\BROKENSYSTEM\ControlSet00x\Services\SmcService' -name 'Start' -Value 4
Set-ItemProperty -Path 'HKLM:\BROKENSYSTEM\ControlSet00x\Services\SNAC' -name 'Start' -Value 4
```

- Disable the Symantec driver, this may not exist but if it does, you need to disable it:

1. Remove the filter

1. Browse up to the following registry entry  
`HKLM\BROKENSYSTEM\ControlSet00x\Control\Network\{4D36E974-E325-11CE-BFC1-08002BE10318}`
2. Find the keys that have a value of **ComponentId** that is set to **symc\_teefer2**, and update the value of Characteristics to **40000**
3. Browse up to the network section  
`HKLM\BROKENSYSTEM\ControlSet00x\Control\Network`
4. Delete the value named **Config**

- Now uninstall the Symantec driver

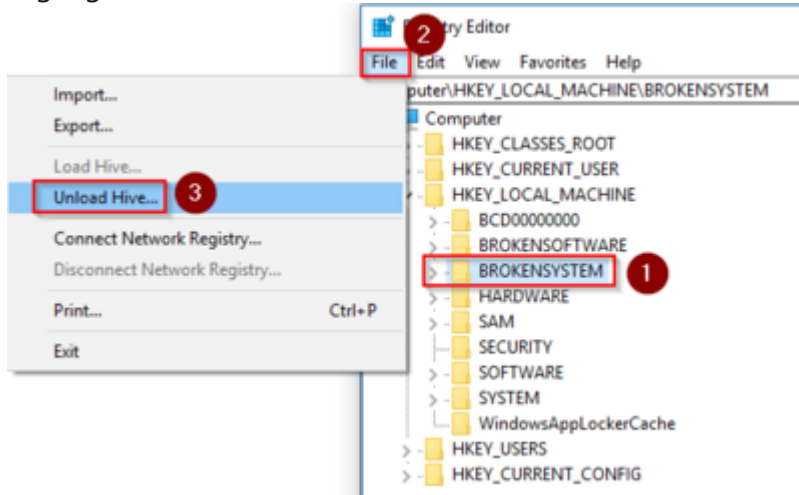
1. Query for all the 3rd party drivers installed on the disk. The system will rename and show these drivers as *OEMxx.inf*. Look in the list and identify the one that matches **Teefer** driver and how it was renamed in its OEMxx form:

```
dism /image:<OS Disk letter>:\ /get-drivers
```

2. Now remove this driver using its OEMxx name

`Dism /Image:<OS Disk letter>:\ /Remove-Driver /Driver:<<OEM1.inf>>`

10. Highlight **BROKENSYSTEM** and select **File\Unload Hive** from the menu



### Mitigation 2

▼ Click here to expand or collapse this section

1. If after all this the issue remains, you need more access to troubleshoot this VM:

1. Depending if this VM is hosted on a datacenter where [Nested virtualization](#) is an option and if the customer agrees, then you can build this environment and the VM in this environment where you are going to have full access to the VM's console screen.
2. If the VM is not hosted in a datacenter where nested environment is an option, you can ask the customer to download the VHD in onprem for further troubleshooting
3. At any point and whenever you have full access to the VM, if you require more help, you can engage **Windows Devices and Deployment** team for further troubleshooting. If that's what you need, then cut a problem with the following values:

- Product: **Windows Svr 2008 R2** or **Windows Svr 2012 R2 Datacenter** or **Windows Svr 2016 Datacenter** as appropriate
- Support topic: **Routing Windows V3\Network Connectivity and File Sharing\TCP/IP Communications**
- Override the routing to engage Tier 2 directly **Note:** Be aware that to engage this team you need to provide them a way of access to the machine they need to troubleshoot so you may want to cut the problem to engage them but by the time the engineer is engaged the VHD needs to be already downloaded or the nested environment created so they can work on the machine.

2. Once the VM is created on nested environment, you could remove this software normally as any other machine using the console access to this VM.

### Mitigation 3

This mitigation only applies in ONLINE mode

### 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?

<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>