

Cannot Connect to Remote Computer_RDP SSH

Last updated by | Kevin Gregoire | Mar 17, 2023 at 9:16 AM PDT

Tags

cw.TSG

cw.RDP-SSH

Contents

- Symptoms
- Refresher / Training Template
- 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
 - Root Cause Analysis 7
 - Root Cause Analysis 8
 - Root Cause Analysis 9
 - Root Cause Analysis 10
- Customer Enablement
- Mitigation
 - Mitigation 1
 - 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 2
 - Mitigation 3
 - Mitigation 4
 - Mitigation 5
 - Mitigation 6
 - Mitigation 7
 - Mitigation 8
 - Mitigation 9
 - Mitigation 10
 - OFFLINE Troubleshooting
 - OFFLINE Approaches
 - Information

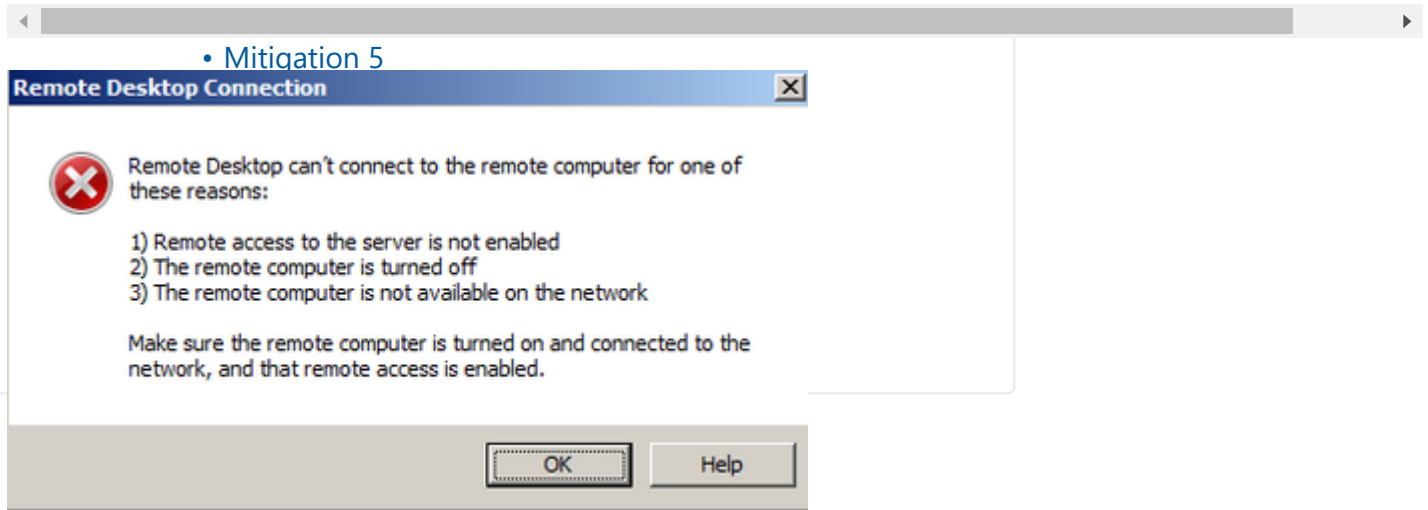
Symptoms

- [Using Recovery Script](#)
 - [For ARM VMs](#)
 - [For Classic VMs](#)
 - [Using OSDisk Swap API](#)
 - [Using VM Recreation scripts](#)
 - [For ARM VMs](#)
1. The VM has connectivity but RDP says the VM is offline.
 2. If you RDP the machine you'll get generic error:

Remote Desktop can't connect to the remote computer for one of these reasons:

- 1) Remote access to the server is not enabled
- 2) The remote Computer is turned off
- 3) The remote computer is not available on the network

Make sure the remote computer is turned on and connected to the network, and that remote access is en



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

Root Cause Analysis 1

The RDP port is not opened or is misconfigured on the Azure Load Balancer.

Root Cause Analysis 2

Remote Desktop is turn OFF.

Root Cause Analysis 3

The *Remote Desktop Services* service is currently not running.

Root Cause Analysis 4

Misconfiguration on the RDP listener.

Root Cause Analysis 5

Either a certificate tied up to the TCP listener is preventing the access or the security level of the VM was changed to a more restrictive one. If the access is locked out due to a TCP-Listener SSL certificate, the client machine is unable to authenticate the access. This usually happened when:

1. A certificate was push to the tcp listener to secure RDP connections with the wrong hash
2. The certificate is corrupted or expired
3. The certificate is missing
4. The CA to authenticate the certificate is unreachable

Root Cause Analysis 6

For Citrix VMs

The installation of XenApp 6.x or 7x RDS VDA modifies the RDP connection in the registry which tells the listener which DLL needs to be loaded. In the RDP Listener the data from the registry key *LoadableProtocol_Object* is modified to *RPM.CtxRdpProtocolManager*. The original value are stored in *CitrixBackupRdpTcpLoadableProtocolObject*.

When uninstalling XenApp 6.x or 7x VDA, this original value must be copied back to ***LoadableProtocol_Object***, but sometimes the original settings are not restored.

Root Cause Analysis 7

The machine is having a brute force RDP attack over the internet, the customer needs to provide more security on his environment.

Root Cause Analysis 8

A misconfigured User Defined Route is blocking RDP connectivity (and possibly network access altogether).



Root Cause Analysis 9

The server is in an unhealthy state, causing RDP to be inaccessible.

Root Cause Analysis 10

The antivirus installed on the server is blocking RDP connectivity.

Customer Enablement

- [Troubleshoot an RDP general error in Azure VM](#) 
- [General Remote Desktop connection troubleshooting](#) 

Mitigation

Mitigation 1

Check if the routing tables are allowing the network traffic to the VM using the **Test Traffic** feature on *Azure Support Center*

1. If the traffic is blocked then
 1. For Classic (V1), verify if the VM has setup
 1. any ACL blocking the access to the Endpoint then [Incorrect Endpoint configuration](#)
 2. any NSG Rule that is blocking the access. Follow instructions at [Incorrect NSG Configuration?](#) to verify that the NSGs
 2. For ARM (V2) Verify if the VM has any NSGs. Follow instructions at [Incorrect NSG Configuration?](#) to verify that the NSGs are correctly configured.
2. If the traffic is not blocked, then proceed with the following mitigations.

Backup OS disk

► Details

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

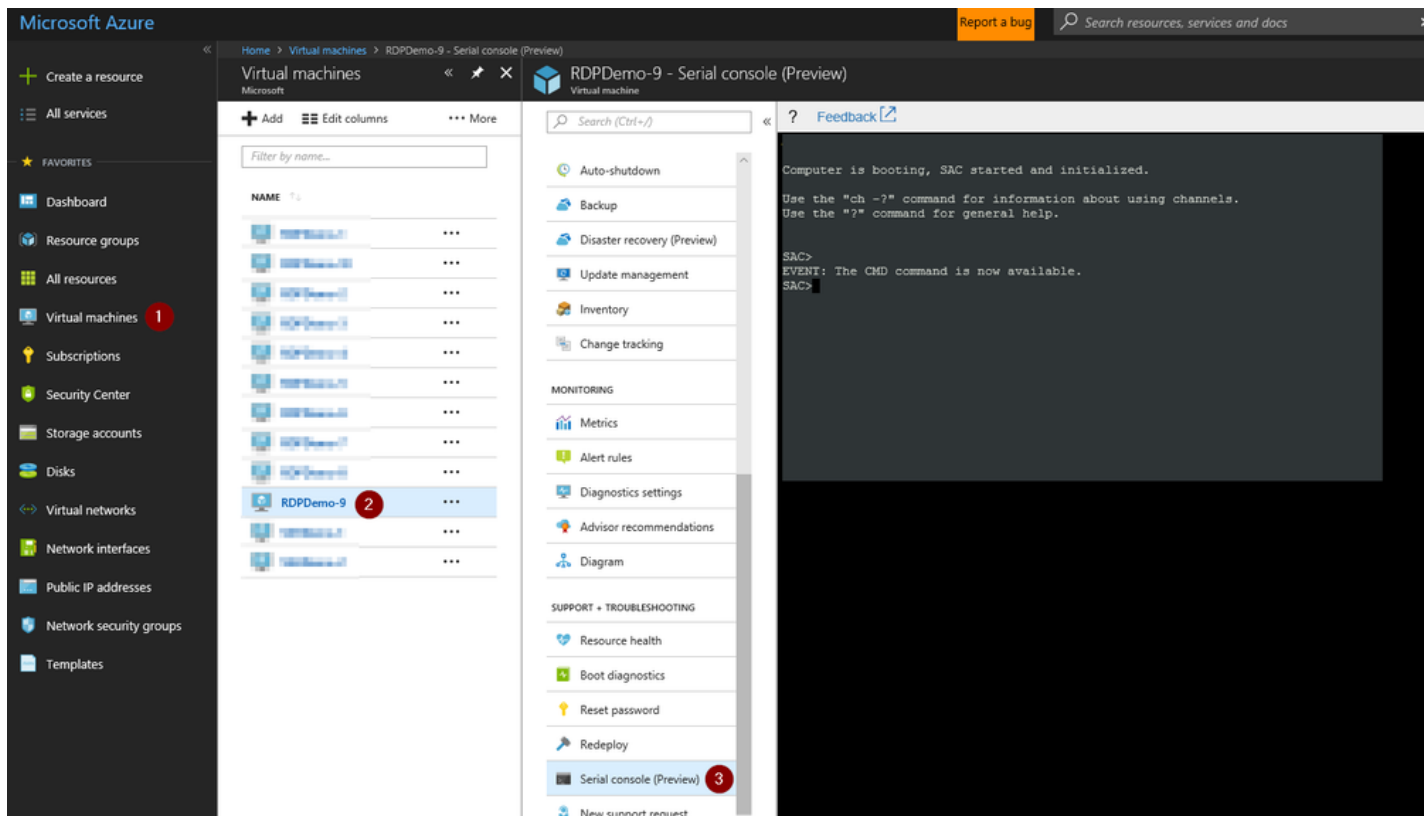
See [How To Access Thru Windows Admin Center](#)

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
```

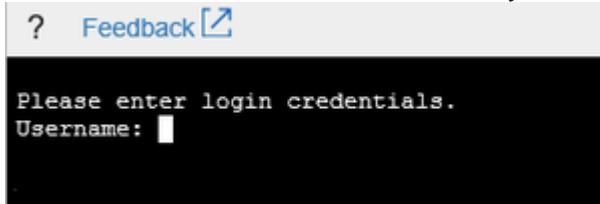
```
SAC>ch -si 1
```

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

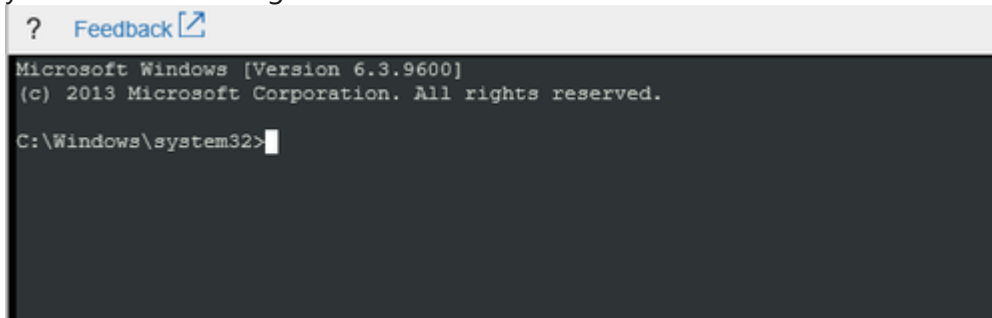
```
? Feedback
Name: Cmd0001
Description: Command
Type: VT-UTF8
Channel GUID: [REDACTED]
Application Type GUID: [REDACTED]

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:

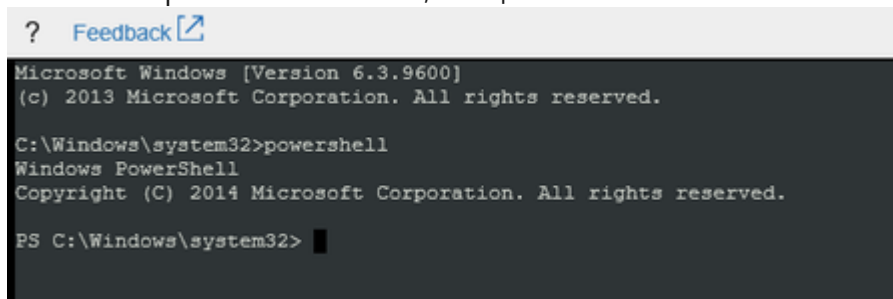


1. If the machine has connectivity, you could use either local or domain IDs. If you want to use a local ID, for domain just add the hostname of the VM
 2. If the machine doesn't have connectivity, you could try to use domains IDs however this will work if only the credentials are cached on the VM. In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

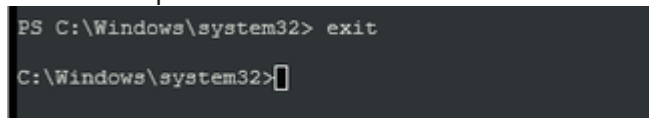


1. At this point, you can do your troubleshooting in bash (CMD) or else, you could start a powershell instance:

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

Mitigation 2

▼ Click here to expand or collapse this section

RDP needs to be turned on:

Step 1

1. Open an administrative CMD instance and check which is the current configuration of RDP

1. Check the current remote connection configuration:

```
REM Get the local remote connection setting
reg query "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections
```

If the command returns 0x1, the VM is not allowing remote connection. Then, allow remote connection using the following command:

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0
```

2. Check if the RDP is disabled by group policies (Local or Domain policies):

```
REM Get the group policy :
reg query "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v fDenyTSConnections
```

If the group policy states that RDP is disabled (fDenyTSConnections value is 0x1), run the following command to enable the TermService service. If the registry key is not found, there is no group policy configured to disabled the RDP. You can move to the next step.

```
REM update the fDenyTSConnections value to enable TermService service:
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v fDenyTSConnections /t REG_DWORD /d 0
```

To enable RDP via policy, the customer needs to change the following GPO policy:

Computer Configuration\Policies\Administrative Templates: Policy definitions\Windows Components\Remote De

Note: If RDP is blocked by policies, check the resultant set of policies [gpresult /H] to understand if RDP is blocked by local or domain policy and modify that policy. If the policy which is blocking RDP connection is

not updated, the registry values will be reset after reboot or group policy refresh and you will not be able to RDP once again.

And If this registry doesn't exist it means this property is not controlled via policy however if it does, then there's a policy in place which will overwrite whatever setup is on the local policy.

Step 2

1. Other things that could turn down RDP are the following keys. Open an administrative CMD instance and run the following:

1. At Terminal Service level

1. TS is disabled

```
reg query "HKLM\SYSTEM\CurrentControlSet\control\Terminal Server" /v TSEnabled
```

1. To enable TS:

```
reg add "HKLM\SYSTEM\CurrentControlSet\control\Terminal Server" /v TSEnabled /t REG_DWORD /d 1
```

2. TS was set to drain mode. Usually this happens if the server is on a terminal server farm (RDS or citrix) and this is a command that is set from the farm:

```
reg query "HKLM\SYSTEM\CurrentControlSet\control\Terminal Server" /v TSServerDrainMode
```

1. To set the server back to working mode:

```
reg add "HKLM\SYSTEM\CurrentControlSet\control\Terminal Server" /v TSServerDrainMode /t REG_DWORD /d 0
```

3. TS was set to disable logon

```
reg query "HKLM\SYSTEM\CurrentControlSet\control\Terminal Server" /v TSUserEnabled
```

1. To enable TS logon:

```
reg add "HKLM\SYSTEM\CurrentControlSet\control\Terminal Server" /v TSUserEnabled /t REG_DWORD /d 1
```

2. At the listener level

1. The listener was set to disabled

```
reg query "HKLM\SYSTEM\CurrentControlSet\control\Terminal Server\WinStations\RDP-Tcp" /v fErv
```

1. To enable the listener:

```
reg add "HKLM\SYSTEM\CurrentControlSet\control\Terminal Server\Winstations\RDP-Tcp" /v
```

2. The listener was set to disable logon

```
reg query "HKLM\SYSTEM\CurrentControlSet\control\Terminal Server\Winstations\RDP-Tcp" /v fLc
```

1. To enable the listener logon:

```
reg add "HKLM\SYSTEM\CurrentControlSet\control\Terminal Server\Winstations\RDP-Tcp" /v
```

3. Ensure RDP component is enabled. Get the current status:

```
REM Get the local policy
reg query "HKLM\SYSTEM\CurrentControlSet\control\Terminal Server\Winstations\RDP-Tcp" /v fDenyTSConnections

REM Get the domain policy if any
reg query "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v fDenyTSConnections
```

1. If the domain policy key exist, then that one goes and the local policy is overwritten
 1. If the policy states that RDP is disabled (value = 1), the customer will need to update his AD policy
 2. If the policy states that RDP is enabled (value = 0), then no change is needed
2. If the domain policy key doesn't exist, then the local policy goes
 1. If the local policy states that RDP is disabled (value = 1) you can enable it by running the following:

```
reg add "HKLM\SYSTEM\CurrentControlSet\control\Terminal Server\Winstations\RDP-Tcp
```

Step 3

1. Restart the VM
 1. Exit from the CMD instance by typing `exit` then hit the Enter key twice to go back to EMS
 2. Now restart from EMS by typing `restart`

Mitigation 3

▼ Click here to expand or collapse this section

1. If the core remote desktop services is not running, please follow [TermService service is not starting](#)

Mitigation 4

▼ Click here to expand or collapse this section

1. Please check that the RDP listener is properly setup, check this VM configuration against the following checklist [RDP Listener Misconfigured](#)
2. If the server belongs to an RDS farm, check if the [connection were disabled from the RDSession Host console](#)
3. Restart the VM
 1. Exist from the CMD instance by typing `exit` then twice Enter key to go back to EMS
 2. Now restart from EMS by typing `restart`

Mitigation 5

▼ Click here to expand or collapse this section

1. If the server is setup to use an SSL certificate, then the rdp-listener key will have an extra entry as the following. Open an elevated CMD instance and run the following:

```
reg query "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v SSLCertificateSHA1Hash
```



1. Validate with the customer he is using an SSL certificate and if so, if the thumbsprint (value of the SSLCertificateSHA1Hash key) is the same
 1. If it is not, then change the thumbsprint

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v SSLCertificateSHA1Hash /t REG_SZ /d [thumbsprint]
```



2. If the customer is not aware of using any certificate, delete that key so the RDP will use the selfsign certificate for RDP

```
reg delete "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v SSLCertificateSHA1Hash
```



2. Ask the customer which type of clients are trying to connect to the machine and write it down in the case for documentation before you proceed to the next step. Collect the following:

Client OS

RDP Client version

Is this a device like a phone or tablet? if so has the latest RDP client?

Is this a thin client? if so which is the brand and model?

1. If the customer is then using legacy RDP clients to connect to the VM, there's a couple of properties on the listener on the server that could prevent your access:
 1. *MinLevelEncryption* could prevent these connections. To change these to their default values, on an elevated CMD instance and run the following:
 1. To query which is your current setting:

```
reg query "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v Mi
```



2. Then you can lower its encryption level to the lowest encryption the server can handle

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v MinE
```



2. *SecurityLevel* could also prevent these connections. This property could be handle in two places:

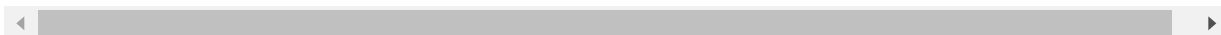
1. Local policy:

```
reg query "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v Se
```



2. If the machine is domain joined, this property could be handle at policy level. To validate if this is your case, check the following key:

```
reg query "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v SecurityLayer
```



1. If this registry doesn't exist it means this property is not controlled via policy however if it does, then there's a policy in place which will overwrite whatever setup is on the local policy

3. To change this property to its default value which is **RDP Security Layer**:

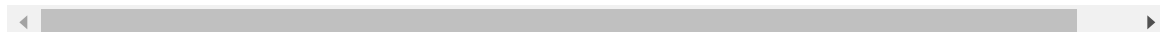
1. For the local policy:

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v
```



2. For the domain policy, the customer needs to change the following GPO policy:

```
Computer\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Securi
```



3. Restart the VM

1. Exist from the CMD instance by typing `exit` then twice Enter key to go back to EMS
2. Now restart from EMS by typing `restart`

Mitigation 6

- ▼ Click here to expand or collapse this section

1. Refer to *Mitigation 1* on [Fail RDP connection on a Citrix VM](#)

Mitigation 7

▼ Click here to expand or collapse this section

1. Follow the [RDP Brute force attack](#) TSG

Mitigation 8

▼ Click here to expand or collapse this section

1. Follow the [UDR](#) TSG.

Mitigation 9

▼ Click here to expand or collapse this section

1. Follow the [Basic Workflow](#) to further isolate if it's a hang, perf issue, etc.
2. If it's a hang, consider getting an [OS dump](#).

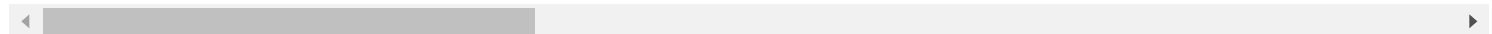
Mitigation 10

▼ Click here to expand or collapse this section

1. Confirm from WGA what antivirus is installed (if any).
2. If there is one installed, snapshot the OS disk to have a backup and uninstall the AV:
 - [Kaspersky](#)
 - [McAfee](#)
 - [Symantec](#)

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 2

▼ Click here to expand or collapse this section

RDP needs to be turn on:

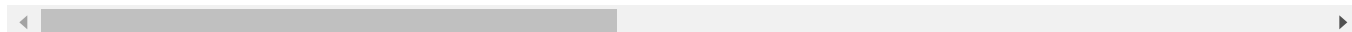
1. If the machine is domain joined, RDP could be disabled at a policy level. To validate if this is your case, check the following key:

```
reg load HKLM\BROKENSOFTWARE f:\windows\system32\config\SOFTWARE
reg query "HKLM\BROKENSOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v fDenyTSConnections
reg unload HKLM\BROKENSOFTWARE
```

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

1. If this key is set to 1, this is pushed thru policy
2. To enable RDP via policy, the customer needs to change the following GPO policy:

Computer Configuration\Policies\Administrative Templates: Policy definitions\Windows Components\Remot



2. If the key doesn't exist or has value 0, then just push the following script:

```
reg load HKLM\BROKENSYSTEM f:\windows\system32\config\SYSTEM
reg load HKLM\BROKENSOFTWARE f:\windows\system32\config\SOFTWARE

reg add "HKLM\BROKENSYSTEM\ControlSet001\control\Terminal Server\WinStations\RDP-Tcp" /v fDenyTSConnectio
reg add "HKLM\BROKENSYSTEM\ControlSet001\control\Terminal Server" /v TSEnabled /t REG_DWORD /d 1 /f
reg add "HKLM\BROKENSYSTEM\ControlSet001\control\Terminal Server" /v TSServerDrainMode /t REG_DWORD /d 0
reg add "HKLM\BROKENSYSTEM\ControlSet001\control\Terminal Server" /v TSUserEnabled /t REG_DWORD /d 0 /f
reg add "HKLM\BROKENSYSTEM\ControlSet001\control\Terminal Server\WinStations\RDP-Tcp" /v fEnableWinStatio
reg add "HKLM\BROKENSYSTEM\ControlSet001\control\Terminal Server\WinStations\RDP-Tcp" /v fLogonDisabled /

reg add "HKLM\BROKENSYSTEM\ControlSet002\control\Terminal Server\WinStations\RDP-Tcp" /v fDenyTSConnectio
reg add "HKLM\BROKENSYSTEM\ControlSet002\control\Terminal Server" /v TSEnabled /t REG_DWORD /d 1 /f
reg add "HKLM\BROKENSYSTEM\ControlSet002\control\Terminal Server" /v TSServerDrainMode /t REG_DWORD /d 0
reg add "HKLM\BROKENSYSTEM\ControlSet002\control\Terminal Server" /v TSUserEnabled /t REG_DWORD /d 0 /f
reg add "HKLM\BROKENSYSTEM\ControlSet002\control\Terminal Server\WinStations\RDP-Tcp" /v fEnableWinStatio
reg add "HKLM\BROKENSYSTEM\ControlSet002\control\Terminal Server\WinStations\RDP-Tcp" /v fLogonDisabled /

reg unload HKLM\BROKENSYSTEM
reg unload HKLM\BROKENSOFTWARE
```

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

Mitigation 3

▼ Click here to expand or collapse this section

1. If the core remote desktop services is not running, please follow [TermService service is not starting](#)

Mitigation 4

▼ Click here to expand or collapse this section

1. Please check that the RDP listener is properly setup, check this VM configuration against the following checklist [RDP Listener Misconfigured](#)

Mitigation 5

▼ Click here to expand or collapse this section

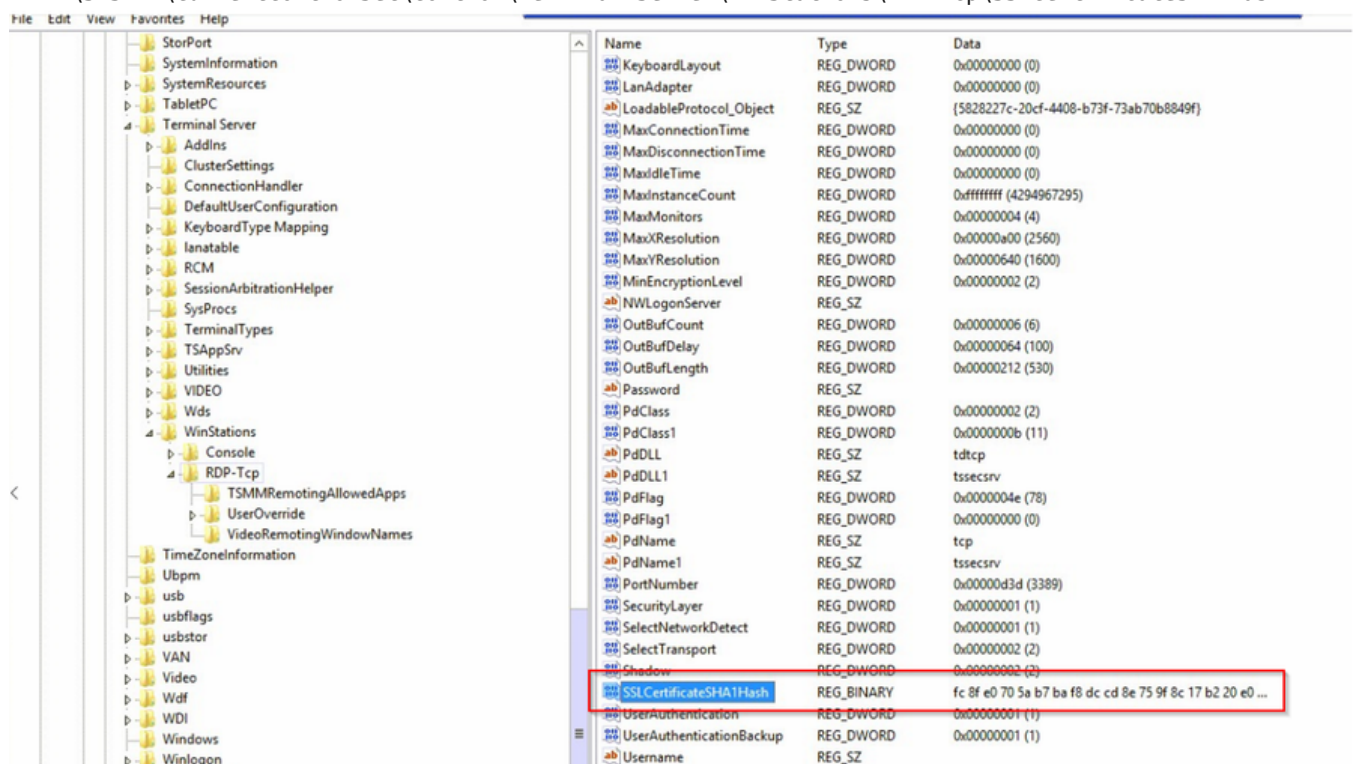
1. Before proceeding any further, do a safe copy of the registry of the affected VM in case a rollback is needed
2. If a certificate was pushed to the RDP listener and is preventing the access, you can remove it

1. Connecting to its certificate repository and remove it from there:

run --> mmc --> file --> add/remove snap-in --> certificates --> add --> computer account --> next --> another computer --> internal forms then go into *personal store* --> right clicked on cert --> delete

2. Manual remove on the registry. Connect to the registry by using remote registry and delete the following entries:

HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\SSLCertificateSHA1Hash



3. If the security level was changed, then change the following keys back to its default values

HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\MinEncryptionLevel From 2
 HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\SecurityLayer From 1

4. Restart the VM

5. If this doesn't work out, please reach out to the Teams Channel *Azure VM POD\Ask a SME -- Unable to RDP SSH* for advise providing the case number, issue description and your question

1. If the Can't RDP SMEs are not available, engage the RDS team to recheck the listener's configuration:

- Product: **Azure Virtual Machine - Windows**
- Support Topic: **Routing Azure Virtual Machine V3\Management\Manage or use RDS in Azure**

Mitigation 6

▼ Click here to expand or collapse this section

1. Refer to *Mitigation 1* on [Fail RDP connection on a Citrix VM](#)

Mitigation 7

▼ Click here to expand or collapse this section

1. Follow the [RDP Brute force attack](#) TSG

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
 2. If the RDP SMEs are not available to answer you, you could engage the RDS team for assistance on this.
 1. Ensure you collect the Windows Performance SDP package from the VM and upload that into the DTM workspace.
1. This would be easily done by running the following script on Serial Console on a powershell instance:

```
#Create a download location and setup the console to prioritize TLS1.2 connections
remove-module psreadline
[Net.ServicePointManager]::SecurityProtocol = "tls12, tls11, tls"
md c:\temp

#Download the Windows SDP file
$source = "https://aka.ms/getTSSv2"
$destination = "c:\temp\TSSv2.zip"
$wc = New-Object System.Net.WebClient
$wc.DownloadFile($source,$destination)

#Expand and run the SDP package for Setup, Network and Performance
Expand-Archive -LiteralPath $destination -DestinationPath C:\temp

#recommended to run the new packages:
C:\temp\TSSv2.ps1 -SDP Setup
C:\temp\TSSv2.ps1 -SDP NET
C:\temp\TSSv2.ps1 -SDP Perf

#Note: you still can run old SDP packages, in case is required:
C:\temp\psSDP\Get-psSDP.ps1 Setup
C:\temp\psSDP\Get-psSDP.ps1 Net
C:\temp\psSDP\Get-psSDP.ps1 Perf
```

2. Collect the following files to the DTM workspace of this case:

1. C:\MS_DATA\SDP_Setup\tss_DATETIME_COMPUTERNAME_psSDP_SETUP.zip
2. C:\MS_DATA\SDP_NET\tss_DATETIME_COMPUTERNAME_psSDP_NET.zip
3. C:\MS_DATA\SDP_Perf\tss_DATETIME_COMPUTERNAME_psSDP_PERF.zip

2. Cut a problem with the following details:

- Product: **Azure\Virtual Machine running Windows**
- Support topic: **Routing Issue with Remote Desktop Service (RDS) on Azure\Issue with connectivity using RDS**

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 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>