Computer Can't Connect to the Remote Computer Error_RDP SSH

Last updated by | Yuri Ohno | Jan 18, 2023 at 11:11 PM PST

Tags

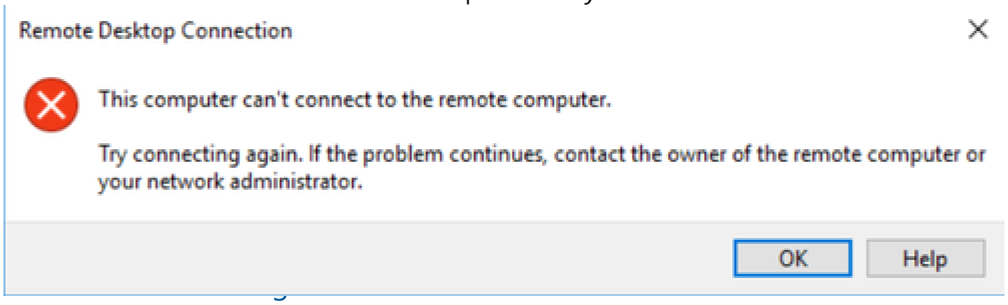
cw.TSG	cw.RDP-SSH

Contents

Symptoms

1. The VM has connectivity and even RDP responds asking for credentials
2. When you try to connect thru RDP do the VM, as soon as you add your credentials, the connections is aborted with the following error:

```
 This computer can't connect to the remote computer. Try connecting again, if the problem continues,
contact the owner of the remote computer or your network administrator.
```



Remote Desktop Connection

This computer can't connect to the remote computer.

Try connecting again. If the problem continues, contact the owner of the remote computer or your network administrator.

Symptoms 1

If you have any of these events go to *Root Cause Analysis 1* & *Mitigation 1* directly:

1. On the Guest OS logs you could find:
   1. In ***System*** you could find events 1058 and/or 1057 as the following:

```
Log Name:      System
Source:        Microsoft-Windows-TerminalServices-RemoteConnectionManager
Date:          6/12/2016 12:53:55 PM
Event ID:      1058
Task Category: None
Level:         Error
Keywords:      Classic
User:          N/A
Computer:      contoso
Description:
The RD Session Host Server has failed to replace the expired self signed certificate used for RD
```

```
Log Name:      System
Source:        Microsoft-Windows-TerminalServices-RemoteConnectionManager
Date:          6/12/2016 12:53:55 PM
Event ID:      1058
Task Category: None
Level:         Error
Keywords:      Classic
User:          N/A
Computer:      contoso
Description:
RD Session host server has failed to create a new self-signed certificate to be used for RD Sess:
```

```
Time:     7/18/2019 8:08:07 PM
ID:       1057
Level:    Error
Source: Microsoft-Windows-TerminalServices-RemoteConnectionManager
Machine:  contoso.local
Message:  The RD Session Host Server has failed to create a new self signed certificate to be use
```

2. In ***System*** you will also find events 36870 with error codes *0x8009030D* or *-2146893043* which stands for *SEC_E_UNKNOWN_CREDENTIALS* as the following:

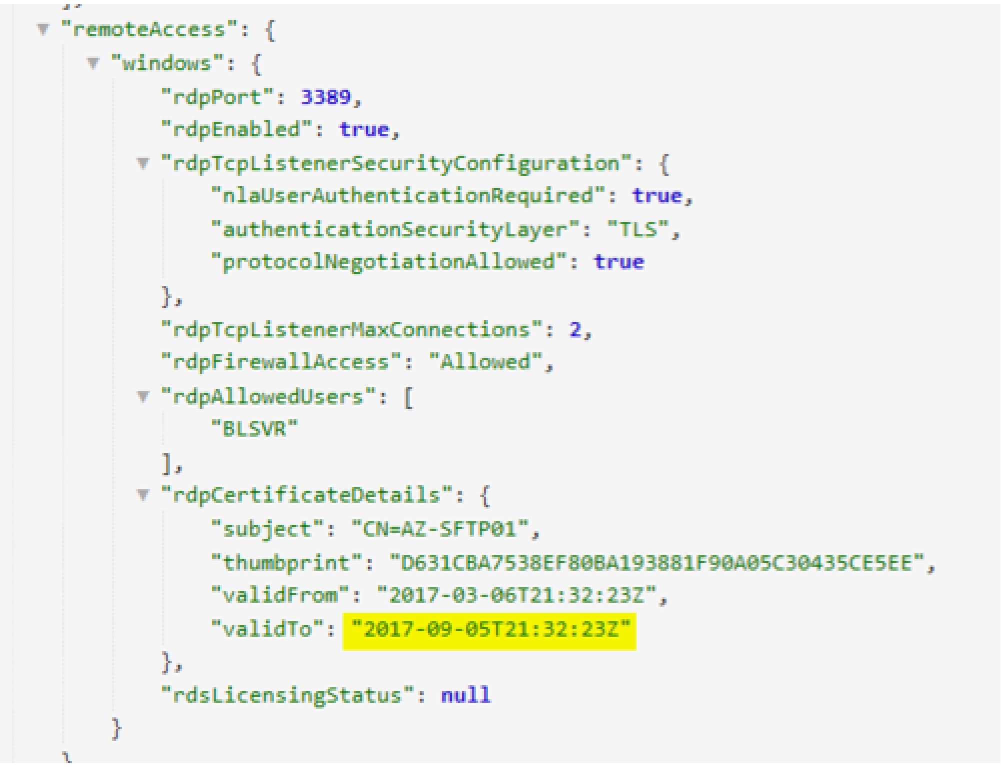
```
Log Name:      System
Source:        Schannel
Date:          10/31/2016 9:37:55 AM
Event ID:      36870
Task Category: None
Level:         Error
Keywords:
User:          SYSTEM
Computer:      contoso.local
Description:
A fatal error occurred when attempting to access the TLS server credential private key. The error
```

```
Time:     7/28/2019 5:49:19 AM
ID:       36870
Level:    Error
Source: Schannel
Machine:  contoso.local
Message:  A fatal error occurred when attempting to access the SSL server credential private key
```

3. In ***Windows Remote Desktop Services*** you could also find event 226:

```
Log Name:      Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
Source:        Microsoft-Windows-RemoteDesktopServices-RdpCoreTS
Date:          17/10/2016 09:36:52 p.m.
Event ID:      226
Task Category: RemoteFX module
Level:         Warning
Keywords:
User:          NETWORK SERVICE
Computer:      contoso.local
Description:
RDP_TCP: An error was encountered when transitioning from StatePreparingX224CC in response to Eve
```

2. In ***WinGuestAnalyzer\Health Signal*** tab you can see the thumbsprint of the certificate tied to the RDP listener and you could tell is expired by looking at the expiration date:



```
  },
  "remoteAccess": {
    "windows": {
      "rdpPort": 3389,
      "rdpEnabled": true,
      "rdpTcpListenerSecurityConfiguration": {
        "nlaUserAuthenticationRequired": true,
        "authenticationSecurityLayer": "TLS",
        "protocolNegotiationAllowed": true
      },
      "rdpTcpListenerMaxConnections": 2,
      "rdpFirewallAccess": "Allowed",
      "rdpAllowedUsers": [
        "BLSVR"
      ],
      "rdpCertificateDetails": {
        "subject": "CN=AZ-SFTP01",
        "thumbprint": "D631CBA7538EF80BA193881F90A05C30435CE5EE",
        "validFrom": "2017-03-06T21:32:23Z",
        "validTo": "2017-09-05T21:32:23Z"
      },
      "rdsLicensingStatus": null
    }
  }
```

Symptoms 2

If you have these events, go to *Root Cause Analysis 2* & *Migitation 2* directly:

1. On the Guest OS logs
    1. in ***System*** you donnot find events 1058 nor 1057

    2. in ***System*** you find events 36870 or 36871 as the following:

```
Log Name:      System
Source:        Schannel
Date:          10/31/2016 9:37:55 AM
Event ID:      36870
Task Category: None
Level:         Error
Keywords:
User:          SYSTEM
Computer:      contoso.local
Description:
A fatal error occurred when attempting to access the TLS server credential private key. The erro
```

```
Log Name:      System
Source:        Schannel
Date:          —
Event ID:      36871
Task Category: None
Level:         Error
Keywords:
User:          SYSTEM
Computer:      contoso.local
Description:
A fatal error occurred while creating a TLS server credential. The internal error state is 10013
```

Symptoms 3

If you have these events, go to *Root Cause Analysis 3* & *Migitation 3* directly:

1. The VM will be having the ***Remote Desktop Connection Broker*** role installed
2. On the GuestOS logs, you will find the following events:
   1. In ***Microsoft-Windows-TerminalServices-SessionBroker/Operational*** the event 2056:

```
Log Name:      Microsoft-Windows-TerminalServices-SessionBroker/Operational
Source:        Microsoft-Windows-TerminalServices-SessionBroker
Date:          6/22/2016 10:23:28 AM
Event ID:      2056
Task Category: (109)
Level:         Error
Keywords:
User:          NETWORK SERVICE
Computer:      contoso.local
Description:
Logon to the database failed.
```

   2. In ***Microsoft-Windows-TerminalServices-SessionBroker/Operational*** the event 1296:

```
Log Name:      Microsoft-Windows-TerminalServices-SessionBroker-Client/Operational
Source:        Microsoft-Windows-TerminalServices-SessionBroker-Client
Date:          6/23/2016 9:19:56 AM
Event ID:      1296
Task Category: (104)
Level:         Error
Keywords:
User:          NETWORK SERVICE
Computer:      contoso.local
Description:
Remote Desktop Connection Broker is not ready for RPC communication.
```

Root Cause Analysis

Root Cause Analysis 1

Something is preventing the RDP Application to access the local RSAs keys under the **MachineKeys** folder on the VM. Usually this happened when:

- Wrong set of ACLs over the Machinekeys folder and/or the RSAs files

- Corrupted/missing RSA key
- RSA certificate expired

Root Cause Analysis 2

A change was done on the TLSs protocols installed on this VM. This would happen when:

1. A new TLS protocol was introduced on the VM and the compatibility with other TLSs versions was not properly set.
2. Some of the protocols TLS 1.0, 1.1 or 1.2 (server) were disabled on the VM. In particular if TLS 1.0 is disabled, this is the protocol that RDP uses

Root Cause Analysis 3

Changing the Hostname of an RDS Connection Broker server isn’t supported since its hostname has entries and dependancies on the Internal Database that the RDS farm needs to work. Changing this hostname once the RDS farm was already built, will cause many errors and the broker server will not work.

References

Public References

- Schannel Events
- Schannel SSP Technical Overview
- RDP Fails with Event ID 1058 & Event 36870 with Remote Desktop Session Host Certificate & SSL Communication
- Schannel 36872 or Schannel 36870 on a Domain Controller
- Event ID 1058 — Remote Desktop Services Authentication and Encryption

Internal References

- What is Transport Layer Security (TLS)
- Windows - TLS

Tracking close code for this volume

Root Cause	Product	Support Topic	Cause Tracking code	Bug
1	*Azure Virtual Machine – Windows*	*Routing Azure Virtual Machine V3\Cannot Connect to my VM\Failure to connect using RDP or SSH port*	*Root Cause - Windows Azure\Compute\Virtual Machine\Guest OS - Windows\VM Responding\RDS - Misconfiguration/issues\RDBroker issues*	

Root Cause	Product	Support Topic	Cause Tracking code	Bug
1	*Azure Virtual Machine – Windows*	*Routing Azure Virtual Machine V3\Cannot Connect to my VM\My problem is not listed above*	*Root Cause - Windows Azure\Compute\Virtual Machine\Guest OS - Windows\VM Responding\Certificates\Unable to renew RDP Certificate*	

Root Cause	Product	Support Topic	Cause Tracking code	Bug
1	*Azure Virtual Machine – Windows*	*Routing Azure Virtual Machine V3\Cannot Connect to my VM\Failure to connect using RDP or SSH port*	*Root Cause - Windows Azure\Virtual Machine\OS Hardening*	

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

Customer Enablement

- Troubleshoot Azure VM RDP connection issues by Event ID

Mitigation

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

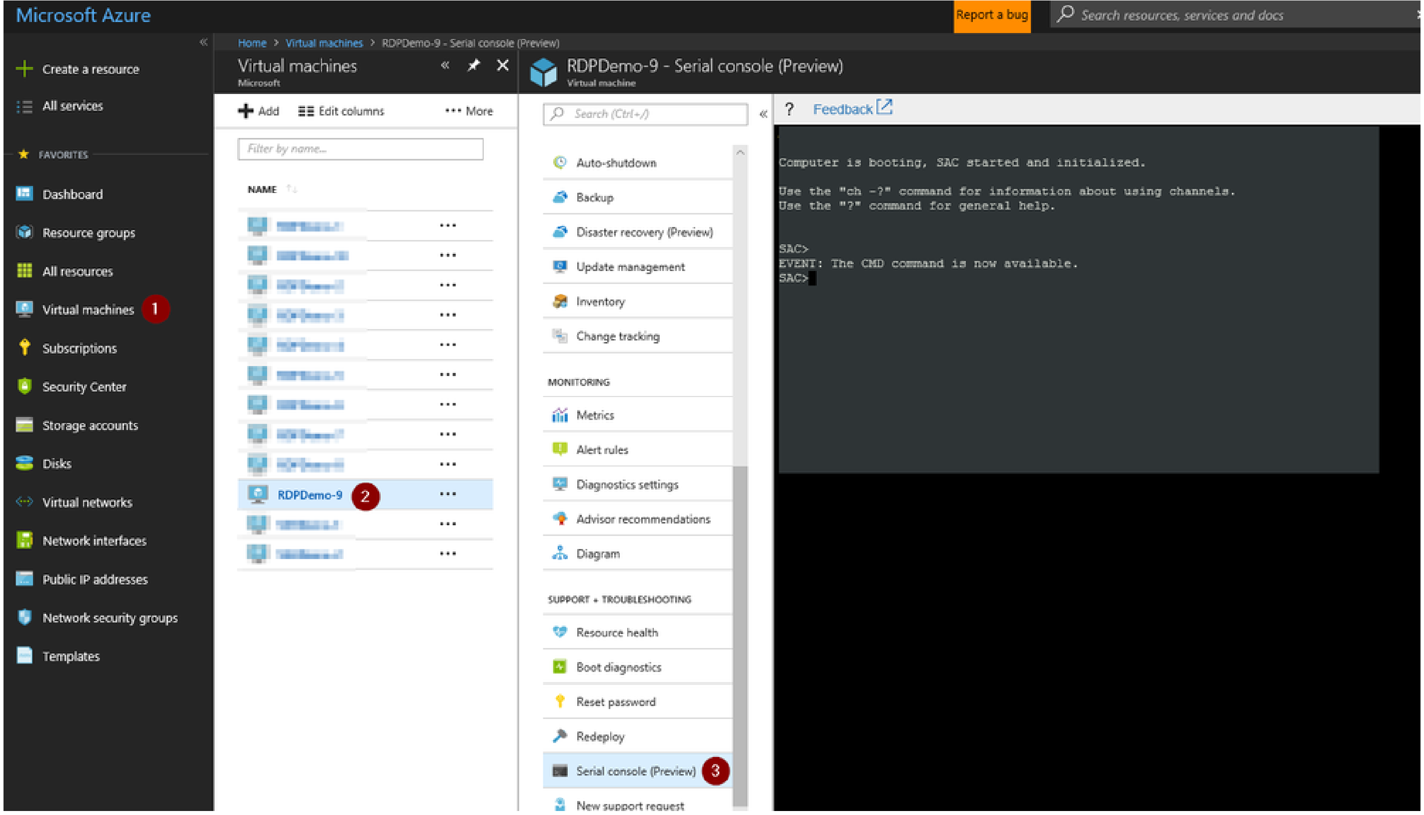
WAC is supported on ARM VMs running Windows Server 2016 or later (not Win10 or any other Windows client

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:



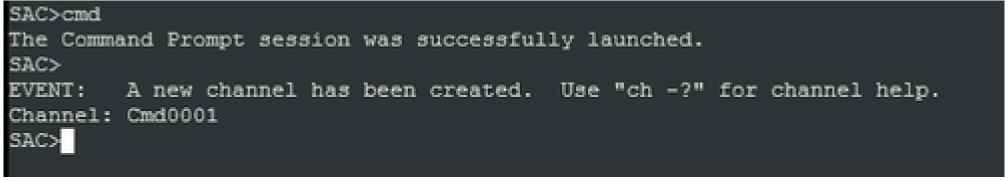
```
Computer is booting, SAC started and initialized.

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

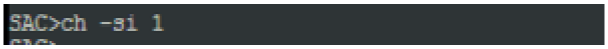
3. Create a channel with a CMD instance. Type `cmd` to start the channel, you will get the name of the channel



```
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>
```

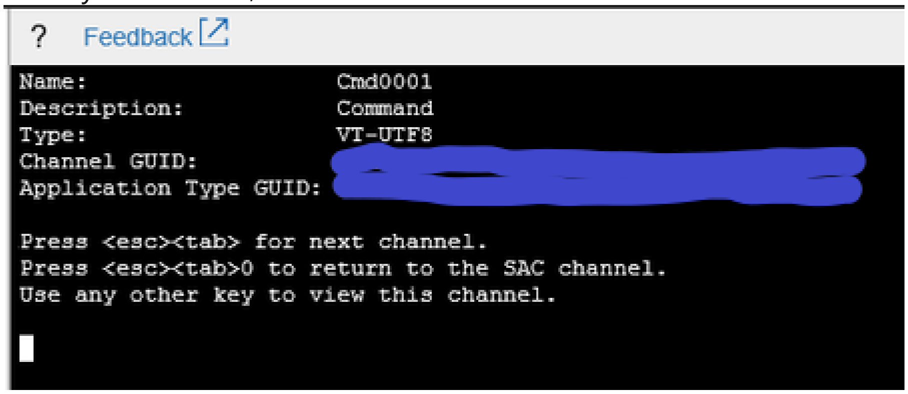
4. Switch to the channel running the CMD instance

```
ch -si 1
```



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

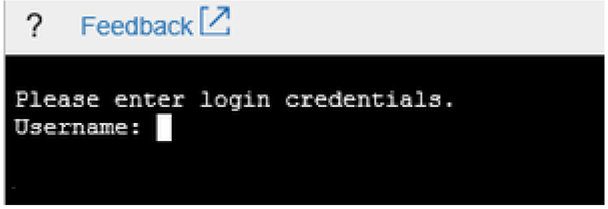
5. Once you hit enter, it will switch to that channel



```
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.
```

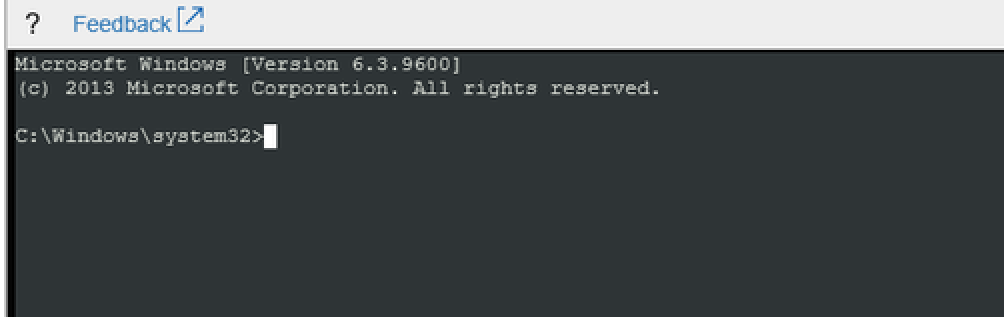
6. Hit enter a second time and it will ask you for user, domain and password:



```
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.

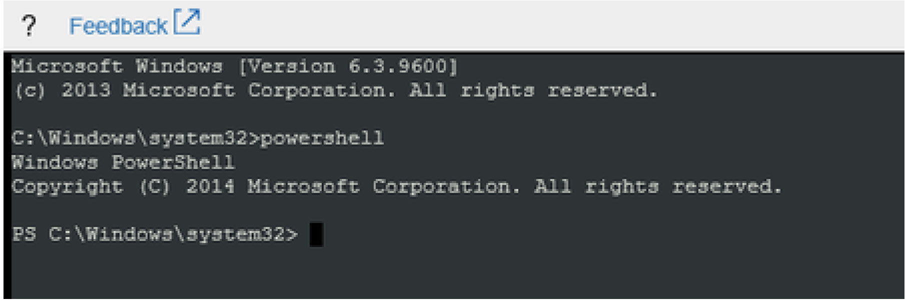
7. Once you add valid credentials, the CMD instance will open and you will have the prompt for you to start your troubleshooting:



```
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`

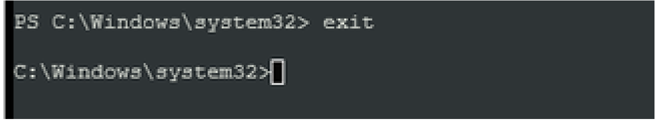


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

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. You will need to setup the correct permissions on the **RDP Certificate**:

    1. Open a Powershell instance and create the script named *Restore_RSA_MachineKeys_Folder_Access.ps1* with the following content:

```
#RESTORE MACHINEKEYS ACL
remove-module psreadline

$folder = "C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys"
$pairkey = "C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\f686*"

#Take ownership of the folder and its child objects
# Takeown /f $folder /a /r
takeown /f $folder /a /r /d:Y

#Take a backup of the current access levels
md c:\temp
icacls $folder /t /c > c:\temp\machinekeys_before.txt

#disable inheritance on folder
icacls $folder /inheritance:d

#Correct perms to the MachineKeys folder
icacls $folder /c /grant "BUILTIN\Administrators:(F)"
icacls $folder /c /grant "Everyone:(R,W)"

#Correct perms to the f686 pair key
icacls $pairkey /c /grant "NT AUTHORITY\System:(F)"
icacls $pairkey /c /grant "NT AUTHORITY\NETWORK SERVICE:(R)"
icacls $pairkey /c /grant "NT Service\SessionEnv:(F)"

#enable inheritance on pair key
icacls $pairkey /inheritance:e

#Get ACL after change
icacls $folder /t /c > c:\temp\machinekeys_after.txt

#Give ownership back to SYSTEM for folder & contents
icacls $folder /setowner "NT Authority\SYSTEM" /T

#Restart the Terminal Service
Restart-Service TermService -Force
```

2. Now run this script to reset the permissions to default on the MachineKey folder and the RSA files inside.

3. Retry RDP access.

   NOTE: Alternatively, try running the commands in Serial Console one line at a time to view and acknowledge the prompts.

2. If RDP still fails (you can confirm the failure via system logs *Event 1058/1057*), then use the script below to ensure that the existing RDP Self Sign certificate is removed and then renewed:

```
remove-module psreadline
Import-Module PKI
Set-Location Cert:\LocalMachine
$RdpCertThumbprint = 'Cert:\LocalMachine\Remote Desktop\'+((Get-ChildItem -Path 'Cert:\LocalMachine\Remot
Remove-Item -Path $RdpCertThumbprint
Stop-Service -Name "SessionEnv"
Start-Service -Name "SessionEnv"
```

3. If you still cannot renew the certificate this way, you could attempt ensuring the certificate is deleted using the MMC console: Renew the RDP Self sign certificate remotely.

4. For the RCA on why the certificate was unable to renew by itself, check the following files to see the permission(s) missing on these folder/files and provide that to the customer:
    - *c:\temp\machinekeys_before.txt*
    - *c:\temp\machinekeys_after.txt*
5. In case you need to rollback the ACLs that you've changed on this TSG, the step to do so is:

    ```
    icacls c:\programdata\microsoft\crypto\rsa\machinekeys\ /restore c:\temp\machinekeys_before.txt
    ```

    However this will also mean that you would be reinjecting the problem, so the next time the certificate needs to renew it will not have access and the issue will reoccur. To avoid this, you will need to redo the step adding the default system permissions.

6. If these methods fail as well, force the MachineKeys folder to regenerate at startup:
    1. Snapshot the OS disk to have a backup.
    2. Disable NLA from the Run Command options or Serial Console, then restart: https://supportability.visualstudio.com/AzureIaaSVM/_wiki/wikis/AzureIaaSVM/495352/Network-Level-Authentication_RDP-SSH?anchor=workaround
    3. Can the customer now RDP? If so, RDP into the VM and rename `C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys` to `C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys_old`.
    4. Re-enable NLA as dictated by this mitigation and restart the machine: https://supportability.visualstudio.com/AzureIaaSVM/_wiki/wikis/AzureIaaSVM/495352/Network-Level-Authentication_RDP-SSH?anchor=mitigation-7
    5. Then see if the customer can now log in successfully with the MachineKeys folder automatically regenerated and NLA re-enabled.
        - If the customer still cannot log in with NLA disabled, add a copy of the OS disk drive to a Rescue VM and rename `\ProgramData\Microsoft\Crypto\RSA\MachineKeys` to `\ProgramData\Microsoft\Crypto\RSA\MachineKeys_old` there (make sure you select the correct attached disk, not the C: volume of the Rescue VM). Swap the disks and retry RDP.

    ⚠ **Important** ⚠ If this method is successful, please proceed now to restore the other customer's keys.

    ```
    WARNING
    Please make sure to restore all the files. If this step is skipped, some other applications or services c
    ```

    Please copy the older Machine Keys files to the newer folder again. Copy all files from `C:\Windows\ProgramData\Microsoft\Crypto\RSA\MachineKeys_old` To `C:\Windows\ProgramData\Microsoft\Crypto\RSA\MachineKeys` **WITHOUT overwriting any file**. This will help not reinject the previous ones that weren't working.

If the customer is requesting a deep dive RCA, please reach out to Windows UEX for further assistance, SAP: `Windows Servers/Windows Server 20##/Windows Server 20## [VERSION HERE]/Remote Desktop Services and Terminal Services/Certificate management`.

Mitigation 2

▶ Click here to expand or collapse this section

Mitigation 3

▼ Click here to expand or collapse this section

Generally if this issue happens, everything works on the VM so you are going to have access to remote registry. For RDP, this uses TLS 1.0 as the default protocol. However, this could be then changed to TLS 1.1 which became the new standard.

1. So open a CMD instance and query how is TLS 1.0, 1.1 and 1.2 set up on the machine:

```
reg query "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server" /v
reg query "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server" /v
reg query "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server" /v
```

   1. If the values are different than *1*, it means that the protocol is disabled. Enable these protocols back:

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server"
reg add "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server"
reg add "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server"
```

      1. For other types of protocols:

```
REM View any additional protocols
reg query "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\"

REM If there are entries beside TLS 1.0, TLS 1.1 and TLS 1.2, query the "Enabled" value for that
reg query "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS x.x\Se
reg query "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS x.x\Se

REM If the values are different from 1, enable the protocols back (replace x.x)
reg add "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS x.x\Serv
reg add "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS x.x\Serv
```

      Note: Get the SSL/TLS version x.x from the Guest OS Logs on the *SCHANNEL* errors

   2. On top of the changes above and just for troubleshooting purposes and to avoid any AD Policy to overwrite the changes that we've done so far, disable the ability of this machine to retrieve the domain to get the latest AD Policies:

```
REM Disable the member server to retrieve the latest GPO from the domain upon start
REG add "HKLM\SYSTEM\CurrentControlSet\Services\gpsvc" /v Start /t REG_DWORD /d 4 /f
```

   3. Restart the VM so the changes on the registry take place.

2. If this fixed your case, then reinstate the ability of this machine to be able to contact the domain to retrieve the latest GPO from the domain. Run the following on an elevated CMD:

```
sc config gpsvc start= auto
sc start gpsvc
```

3. Now ensure that the change that we've done on this mitigation is not reverted by an AD GPO by running `gpupdate /force`.
4. If the change is reverted, it means that there's an AD policy that the customer need to change that to avoid this from happening again.

Mitigation 4

▼ Click here to expand or collapse this section

Applies only for Remote Desktop Connection Broker servers

The Remote Desktop Connection Broker role and the Windows Internal Database needs to be uninstalled as well as additional cleanup needs to be done as to redeploy the TCP-Listener due to a certificate mismatch.

1. Engate the RDS team for assistance on this. Cut a problem to the RDS team.
    - Product: ***Azure Virtual Machine - Windows***
    - Support topic: ***Issue with Remote Desktop Service (RDS) on Azure\Issue with connectivity using RDS***

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

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. Setup the correct permissions on the **RDP Certificate** and its folder. You could do this in multiple ways:
    1. If you have a working Azure Agent, you can use CSE pushing the Restore_RSA_MachineKeys_Folder_Access.ps1 script (also pasted below if this link fails for whatever reason). **Note:** The script will:
        1. Take ownership of the MachineKeys folder
        2. Reset the Permissions of this folder and all the files within
        3. Create two logs file, one before the script (*c:\temp\BeforeScript_permissions.txt*) and another after the script (*c:\temp\AfterScript_permissions.txt*).

            ▶ Restore_RSA_MachineKeys_Folder_Access.ps1
    2. If you do not have a working Guest Agent, you cannot use CSE so you will need to do the following from a Rescue VM:
        1. Perform the above steps offline while the broken VM's OS disk is attached to the Rescue VM:

            ▶ Restore_RSA_MachineKeys_Folder_Access_Rescue_VM.ps1
        2. Set the disk to offline in Disk Management and swap the disk back. Test RDP connectivity. I recommend that we do not remove the Repair VM until we confirm RDP connectivity is working in case the cx requires the `*_permission.txt` files.
2. if the problem is still not resolved, you could force the OS to renew the RDP certificate.
    1. This requires connectivity to the VM (e.g. from a VM in the same VNET). Please refer to How to renew the RDP Self sign certificate remotely
    2. If you do not have connectivity to the VM, you cannot use the above method so you will need to do the following from a Rescue VM:
        1. Perform the above steps offline while the broken VM's OS disk is attached to the Rescue VM:

            ▶ Renew_MachineKey_Certs_Rescue_VM.ps1
        2. Set the disk to offline in Disk Management and swap the disk back. The `MachineKeys` folder should have been regenerated with default settings on OS startup. Test RDP connectivity. If working, we should snapshot the disk and inform the cx to compare both `MachineKeys` and `MachineKeys_old` as `MachineKeys_old` may have some ACLs the require for their environment:

            ▶ Compare_MachineKey_Certs.ps1

3. If the server is setup to use an SSL certificate, then the rdp-listener key will have an extra entry as the following:

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

REG QUERY "HKLM\BROKENSYSTEM\ControlSet001\Control\Terminal Server\WinStations\RDP-Tcp" /v SSLCertifi
REG QUERY "HKLM\BROKENSYSTEM\ControlSet002\Control\Terminal Server\WinStations\RDP-Tcp" /v SSLCertifi
```

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

   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\BROKENSYSTEM\ControlSet001\Control\Terminal Server\WinStations\RDP-Tcp" /v SSl
REG ADD "HKLM\BROKENSYSTEM\ControlSet002\Control\Terminal Server\WinStations\RDP-Tcp" /v SSl

reg unload HKLM\BROKENSYSTEM
```

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

```
REG DELETE "HKLM\BROKENSYSTEM\ControlSet001\Control\Terminal Server\WinStations\RDP-Tcp" /v
REG DELETE "HKLM\BROKENSYSTEM\ControlSet002\Control\Terminal Server\WinStations\RDP-Tcp" /v

reg unload HKLM\BROKENSYSTEM
```

Mitigation 2

▼ Click here to expand or collapse this section

1. If the regular options for repair are not working, use a Rescue VM with the broken VM's cloned OS disk attached. For RDP, we usually use TLS 1.0 by default; however, and depending on the OS, these could be 1.1 or 1.2 as well.

   1. Check which TLS is enabled in the OS (**Note:** this will assume that the attached OS disk is drive `F:` but if this is not your case, update the letter assignment):

```
REM Load the registry hive from the broken VM's registry
reg load HKLM\BROKENSYSTEM F:\windows\system32\config\SYSTEM

REM Check the 'Enabled' value of TLS 1.0, TLS 1.1 and TLS 1.2
reg QUERY "HKLM\BROKENSYSTEM\ControlSet001\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Serv
reg QUERY "HKLM\BROKENSYSTEM\ControlSet001\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Serv
reg QUERY "HKLM\BROKENSYSTEM\ControlSet001\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Serv

reg QUERY "HKLM\BROKENSYSTEM\ControlSet002\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Serv
reg QUERY "HKLM\BROKENSYSTEM\ControlSet002\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Serv
reg QUERY "HKLM\BROKENSYSTEM\ControlSet002\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Serv

REM View any additional protocols
reg query "HKLM\BROKENSYSTEM\ControlSet001\Control\SecurityProviders\SCHANNEL\Protocols\"
reg query "HKLM\BROKENSYSTEM\ControlSet002\Control\SecurityProviders\SCHANNEL\Protocols\"

REM If there are entries beside TLS 1.0, TLS 1.1 and TLS 1.2, query the "Enabled" value for that entr
reg query "HKLM\BROKENSYSTEM\ControlSet001\Control\SecurityProviders\SCHANNEL\Protocols\TLS x.x\Serve
reg query "HKLM\BROKENSYSTEM\ControlSet002\Control\SecurityProviders\SCHANNEL\Protocols\TLS x.x\Serve
```

2. If any of these are disabled, either because the key doesn't exist or its value is 0, enable the protocol:

```
REM Enable TLS 1.0, TLS 1.1 and TLS 1.2
reg ADD "HKLM\BROKENSYSTEM\ControlSet001\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server
reg ADD "HKLM\BROKENSYSTEM\ControlSet001\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server
reg ADD "HKLM\BROKENSYSTEM\ControlSet001\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server

reg ADD "HKLM\BROKENSYSTEM\ControlSet002\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server
reg ADD "HKLM\BROKENSYSTEM\ControlSet002\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server
reg ADD "HKLM\BROKENSYSTEM\ControlSet002\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server

REM Enable any additional protocols found above (replace x.x)
reg ADD "HKLM\BROKENSYSTEM\ControlSet001\Control\SecurityProviders\SCHANNEL\Protocols\TLS x.x\Server
reg ADD "HKLM\BROKENSYSTEM\ControlSet002\Control\SecurityProviders\SCHANNEL\Protocols\TLS x.x\Server
```

2. Once you perform the change, enable NLA and unload the repaired hive:

```
REM Make sure NLA is enabled
reg ADD "HKLM\BROKENSYSTEM\ControlSet001\Control\Terminal Server\WinStations\RDP-Tcp" /v UserAuthenticati
reg ADD "HKLM\BROKENSYSTEM\ControlSet002\Control\Terminal Server\WinStations\RDP-Tcp" /v UserAuthenticati

REM unload the repaired registry hive from the repair VM's registry
reg unload HKLM\BROKENSYSTEM
```

3. Swap the repaired OS disk back to the broken VM (or recreate the VM if using a classic) and check if this works. If so, then run a `gpupdate /force` and ensure that the access is still possible. If it is not, it means that these changes are pushed through AD policy and the customer needs to change that to avoid this from happening again.

Mitigation 3

▼ Click here to expand or collapse this section

Applies only for Remote Desktop Connection Broker servers

The Remote Desktop Connection Broker role and the Windows Internal Database needs to be uninstalled as well as additional cleanup needs to be done as to redeploy the TCP-Listener due to a certificate mismatch.

1. Engate the RDS team for assistance on this. Cut a problem to the RDS team.
   - Product: ***Azure Virtual Machine - Windows***
   - Support topic: ***Issue with Remote Desktop Service (RDS) on Azure\Issue with connectivity using RDS***

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 engate 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 - 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!