

Access Is Denied Responding_RDP SSH

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

Tags

cw.TSG

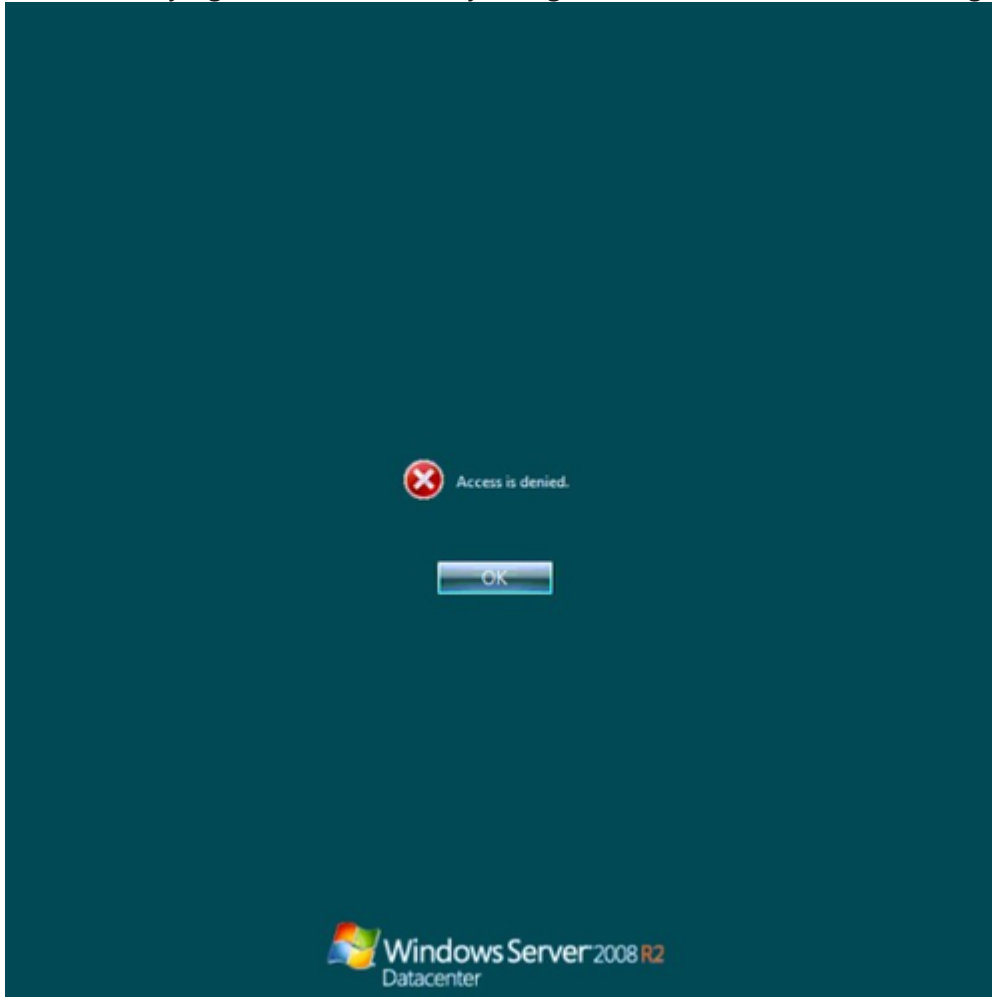
cw.RDP-SSH

Contents

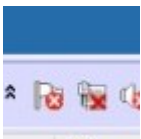
- Symptoms
- Root Cause Analysis
 - Root Cause Analysis 1
 - Root Cause Analysis 2
 - Root Cause Analysis 3
 - Root Cause Analysis 4
 - Tracking close code for this volume
- Customer Enablement
- Mitigation
 - Backup OS disk
 - ONLINE Troubleshooting
 - ONLINE Approaches
 - Using Windows Admin Center (WAC)
 - Using Serial Console Feature
 - Using Remote Powershell
 - Using Remote CMD
 - Using Custom Script Extension or RunCommands Feature
 - Using Remote Registry
 - Using Remote Services Console
 - ONLINE Mitigations
 - Mitigation 1
 - Mitigation 2
 - Mitigation 3
 - Mitigation 4
 - OFFLINE Troubleshooting
 - OFFLINE Approaches
 - Information
 - Using Recovery Script
 - For ARM VMs
 - For Classic VMs
 - Using OSDisk Swap API
 - Using VM Recreation scripts
 - For ARM VMs
 - For Classic VMs
 - OFFLINE Mitigations
 - Escalate
 - After work - Cleanup
- Need additional help or have feedback?

Symptoms

1. The VM screenshot shows the OS fully loaded and waiting for the credentials
2. The OS is a Windows 2008 R2 machine
3. If you try to RDP the VM either internally or externally with either a domain or local ID thru RDP, when the RDP is trying to authentication you'll get the **Access is denied** message



4. If you try to RDP the VM either internally or externally using an administrative session (mstsc /admin), you can successfully connect, however you'll notice there is a network connectivity error icon, under notification area:



5. On the Guest OS logs, you could find that the Remote Desktop Licensing service is crashing with following error message:

Log Name: System
 Source: Service Control Manager
 Date: 19.08.2016 13:28:07
 Event ID: 7024
 Task Category: None
 Level: Error
 Keywords: Classic
 User: N/A
 Computer: <computer name>
 Description:
 The Remote Desktop Licensing service terminated with the following service-specific error:
 A device attached to the system is not functioning.

Root Cause Analysis

This could happen for many reasons, some of them are the following:

Root Cause Analysis 1

Lack of permissions for the users to read the certificate registry entries on terminal services

Root Cause Analysis 2

Login error while loading the profiles. Usually this is due to some user policy causing a conflict on the profile

Root Cause Analysis 3

The size of the Kerberos token is not big enough to hold all the permissions for that user. This happens when the user belongs to many AD groups and nested AD groups

Root Cause Analysis 4

The Terminal Service is not starting with the correct account

Tracking close code for this volume

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

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\Virtual Machine\Guest OS - Windows\VM Responding\Logon failure\User Profile 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\Virtual Machine\Guest OS - Windows\VM Responding\Active Directory issues\GPO preventing RDP	

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\Guest OS - Windows\Isolated\Windows Services not starting/crashing	

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

► 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

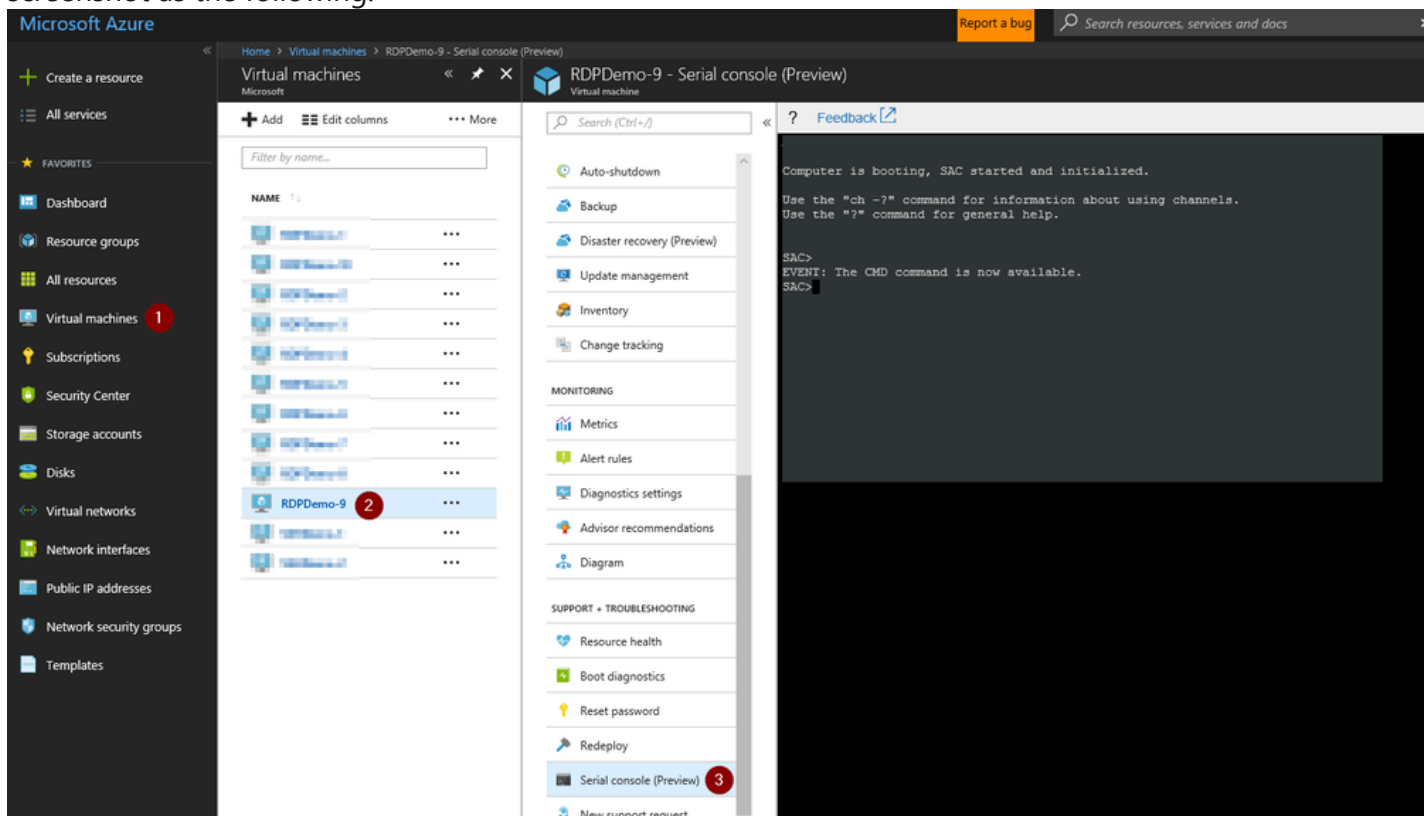
See [How To Access Thru Windows Admin Center](#)

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:
Application Type GUID:
Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.
```

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

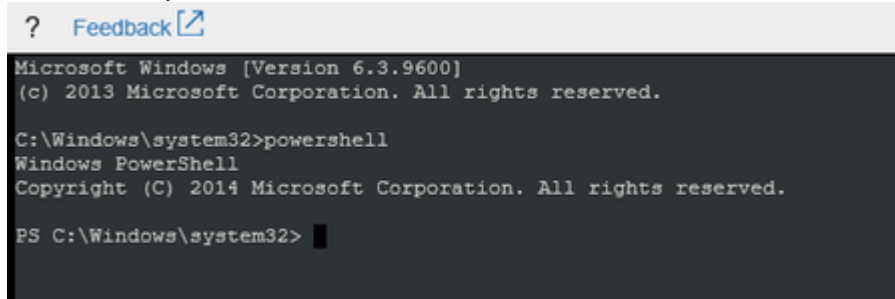
```
? Feedback
Please enter login credentials.
Username:
```

1. If the machine has connectivity, you could use either local or domain IDs. If you want to use a local ID, for domain just add the hostname of the VM
 2. If the machine doesn't have connectivity, you could try to use domains IDs however this will work if only the credentials are cached on the VM. In this scenario, it is suggested to use local IDs instead.
7. Once you add valid credentials, the CMD instance will open and you will have the prompt for you to start your troubleshooting:

```
? Feedback
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Windows\system32>
```

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

1. To launch a powershell instance, run `powershell`

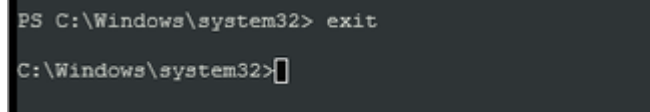


```
? Feedback [link]
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>powershell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>
```

2. To end the powershell instance and return to CMD, just type `exit`



```
PS C:\Windows\system32> exit

C:\Windows\system32>
```

8. <<<<INSERT MITIGATION>>>>

Using [Remote Powershell](#)

- Click here to expand or collapse this section

Using [Remote CMD](#)

- Click here to expand or collapse this section

Using [Custom Script Extension](#) or [RunCommands Feature](#)

- Click here to expand or collapse this section

Using [Remote Registry](#)

- Click here to expand or collapse this section

Using [Remote Services Console](#)

- Click here to expand or collapse this section

ONLINE Mitigations

Mitigation 1

- ▼ Click here to expand or collapse this section

1. Open an elevated Powershell instance and query the following keys to ensure some specific values:
 1. Local group *Remote Desktop Users* has *READ* access over this key

```
Get-Acl -Path "HKLM:\SOFTWARE\Microsoft\SystemCertificates\Remote Desktop\Certificates" | Format
```



2. If you find that this access is not there, please grant it out

3. Retry your access

2. If this is not fixing, continue with the next mitigation

Mitigation 2

▼ Click here to expand or collapse this section

1. Open an elevated CMD instance, and query the following key
 1. By default, this key doesn't exist however it could be setup to ignore all login errors due to profile issues:

```
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server' -name "IgnoreRegl
```

2. Restart the VM and retry your access
3. If this is not fixing, continue with the next mitigation

Mitigation 3

▼ Click here to expand or collapse this section

1. Open an elevated CMD instance, and query the following key
 1. Query the Kerberos size. On legacy system this number will be low and if each domain ID has multiple nested membership, the Kerberos token size could not big enough to create the ticket for that user. On windows Server 2008 R2, this could be increase to the following maximum:

```
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters' -name "M:
```

2. Restart the VM and retry your access
3. If this is not fixing, continue with the next mitigation

Mitigation 4

▼ Click here to expand or collapse this section

1. Open an elevated CMD instance, and query the following key
 1. Ensure the startup account for Terminal Services is the correct one:

```
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\services\termervice' -name "ObjectName"
```

2. Restart the VM and retry your access
3. If this is not fixing your case, continue on the escalation section

OFFLINE Troubleshooting

This scenario can only be investigated in ONLINE mode

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

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

REM Setup to ignore login errors on user policies during logon
REG ADD "HKLM\BROKENSYSTEM\ControlSet001\Control\Terminal Server" /v IgnoreRegUserConfigErrors /t REG_DWORD /d 1
REG ADD "HKLM\BROKENSYSTEM\ControlSet002\Control\Terminal Server" /v IgnoreRegUserConfigErrors /t REG_DWORD /d 1

REM Increase the Kerberos token to its maximum
REG ADD "HKLM\BROKENSYSTEM\ControlSet001\Control\Lsa\Kerberos\Parameters" /v MaxTokenSize /t REG_DWORD /d 0xffffffff
REG ADD "HKLM\BROKENSYSTEM\ControlSet002\Control\Lsa\Kerberos\Parameters" /v MaxTokenSize /t REG_DWORD /d 0xffffffff

REM Ensure that the terminal services is starting with the correct account
REG ADD "HKLM\BROKENSYSTEM\ControlSet001\services\TermService" /v ObjectName /t REG_SZ /d "NT Authority\SYSTEM"
REG ADD "HKLM\BROKENSYSTEM\ControlSet002\services\TermService" /v ObjectName /t REG_SZ /d "NT Authority\SYSTEM"

reg unload HKLM\BROKENSYSTEM
```

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

2. Ensure that the following registry key has READ access to the local group **Remote Desktop Users**

Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\Remote Desktop\Certificates
Access level:	READ
Group:	Remote Desktop Users

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 - RDPE 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>