

The Number Of Connections To This Computer Is Limited_RDP SSH

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

Tags

[cw.TSG](#)[cw.RDP-SSH](#)

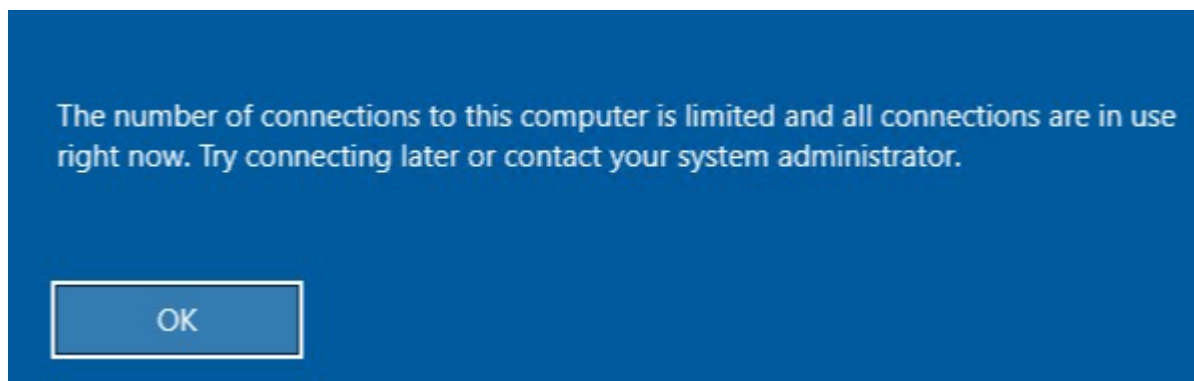
Contents

- [Symptoms](#)
- [Root Cause Analysis](#)
 - [References](#)
- [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](#)
 - [OFFLINE Troubleshooting](#)
 - [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. If you RDP a certain number of concurrent RDP connections, you might get the following client side error:

The number of connections to this computer is limited and all connections are in use right now. Try connecting later or contact your system administrator.



3. You are on this scenario if you have the following ASC Insight <TO BE CREATED>

Root Cause Analysis

There's a quota that was set to the GuestOS that handles on how many RDP sessions can the system run at the same time.

References

- [INTERNAL - More than 2 users cannot logon to the RDS server](#) 

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

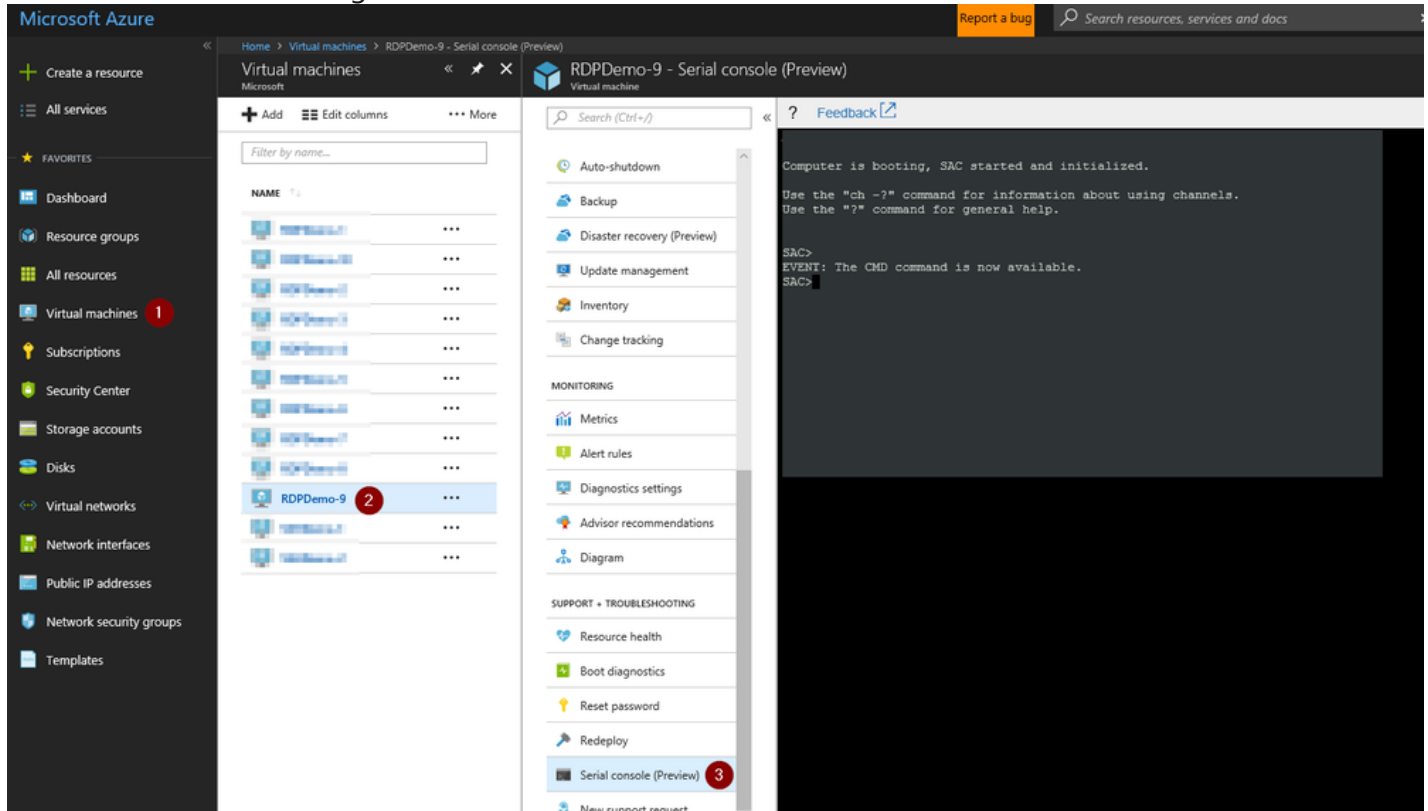
See [How To Access Thru Windows Admin Center](#)

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:



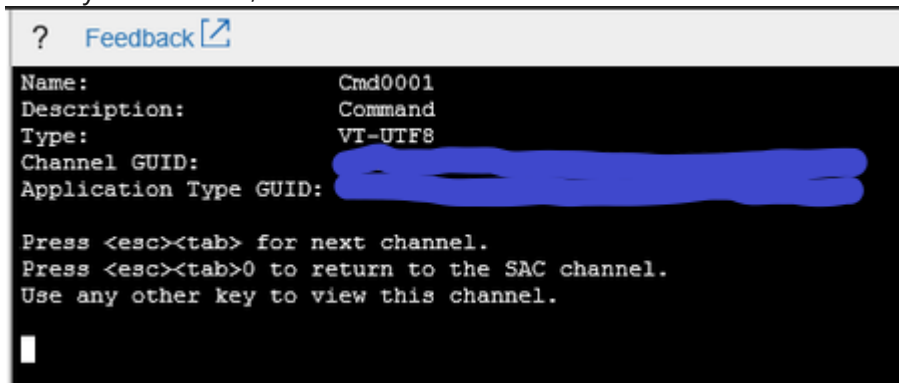
1. If EMS does not connect, it means the Guest OS was not setup to use this feature:
 1. If the issue that you have will repro on a restart and if the customer is OK to enable this feature, you enable this feature. For details refer to [Serial Console](#) on the *How to enable this feature*
 2. If on 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
SAC>
```

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

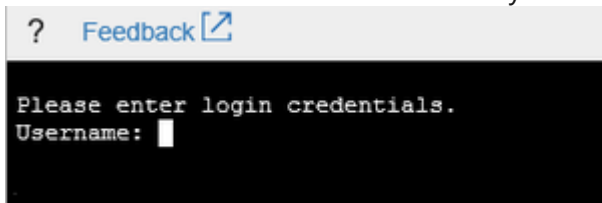


```
? Feedback [link]
Name: Cmd0001
Description: Command
Type: VT-UTF8
Channel GUID: [redacted]
Application Type GUID: [redacted]

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:

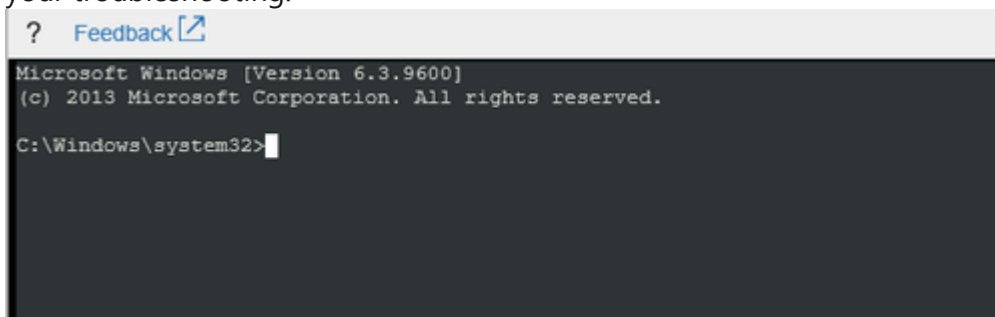


```
? Feedback [link]

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:



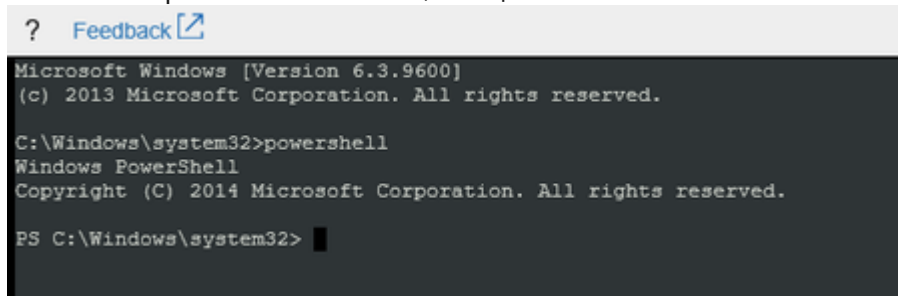
```
? Feedback [link]

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`



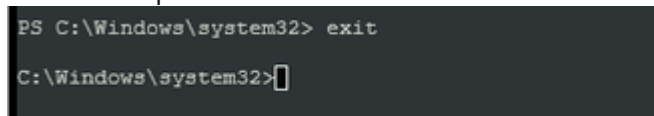
```
? Feedback [link]

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

1. Open a CMD instance and query to see if you have a policy that is being applied to your VM guest OS limiting the number of concurrent connections:

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

1. If the former registry *exist*, it means this is set by an AD policy. If the value of is different from *0xffffffff* then it means that whatever value (in hexadecimal) is specified here is the quota that is applying to this GuestOS to handle connections. **If this is your case, the customer needs to change/remove the policy for a proper quota.** to modify this policy. Once you ask that to the customer, proceed with step 2
2. If the former policy registry and value *doesn't exist* then it means this limitation is setup with a local policy. You can check this by running the following:

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



1. Change the local policy to a unlimited or a higher value

- Option to set the quota to unlimited

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v MaxInstanceCount /t REG_DWORD /d 0xffffffff
```



- Option to set the quota to a higher value. This illustrates how to add a limit to a 100 (64 in hexadecimal) connections

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v MaxInstanceCount /t REG_DWORD /d 0x64
```



2. There's another place where this limitation *could* be setup. This key does not exist by default and doesn't have any GUI nor policy way to set this up. **If this value is set, this means that this was done manually**

by the customer at some point in time by manipulating the registry.

```
reg query "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v UserSessionLimit
```

1. As this value is not a default configuration, the customer can opt out to either remove the quota by deleting this value or increasing the quota to a higher value or unlimited.

- Option to remove the quota

```
reg delete "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v UserSessionLimit
```

- Option to set the quota to unlimited

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v UserSessionLimit /d 0xffffffff
```



- Option to set the quota to a higher value. This illustrates how to add a limit to a 100 (64 in hexadecimal) connections

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v UserSessionLimit /d 0x00000064
```



OFFLINE Troubleshooting

While this change could also be done in OFFLINE mode, we don't recommend this out as will increase the time and effort on the customer by setting a rescue VM to attach the OS disk and modify the registry which is easier to be done using any of the methods explains on the Online approach section.

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 - 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 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>