Connect using MSTSC or MSRDC Fails_RDP SSH

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

Tags

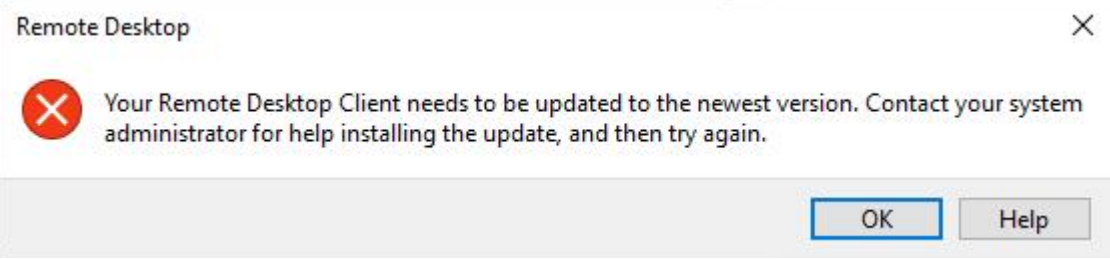
cw.TSG cw.RDP-SSH

Contents

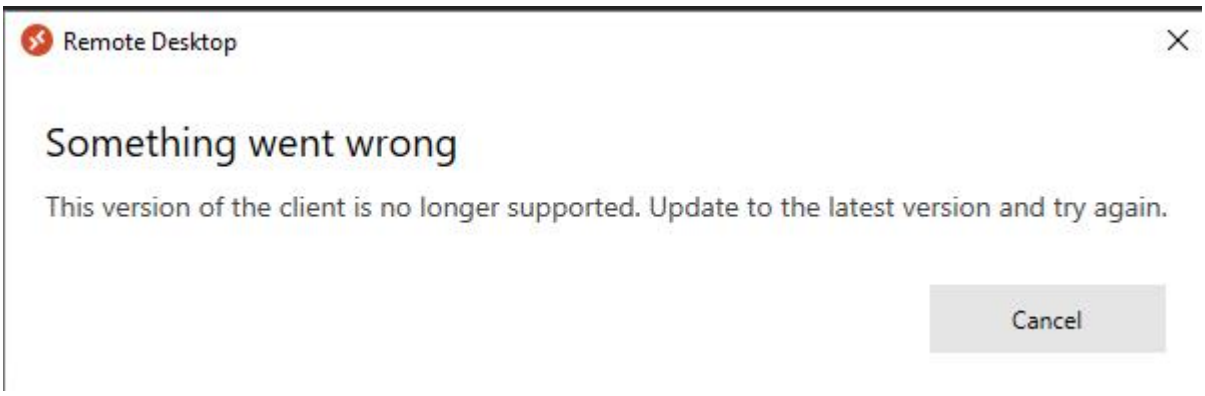
Symptoms

1. When users are trying to connect to thier into VMs using MSTSC or from MSRDC older than 1.2.675, that may result in either of the errors below:

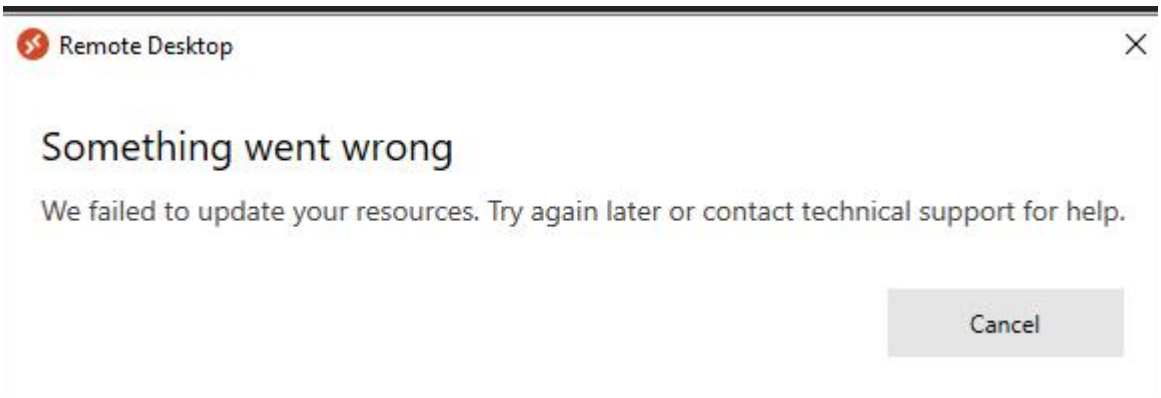
    1. Connection Block on Windows Desktop (MSRDC) client version 1.2.247 and above



2. Subscription Block on Windows Desktop (MSRDC) client version 1.2.247 to 1.2.428 and 1.2.1672+



3. Subscription Block on Windows Desktop (MSRDC) client version 1.2.605 to 1.2.1525



Root Cause Analysis

- All connections from old legacy RDP clients (MSTSC and MSRDC) older than 1.2.675 are currently blocked because they are not secure enough.
- This mostly applies to Windows 10, Windows 8, Window 8.1 and Windows 7.

References

- What's new in the Windows Desktop client
- MSTSC
- Windows Desktop client for admins
- MSTSC vs RDMan

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*		

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

Customer Enablement

Windows Desktop client

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

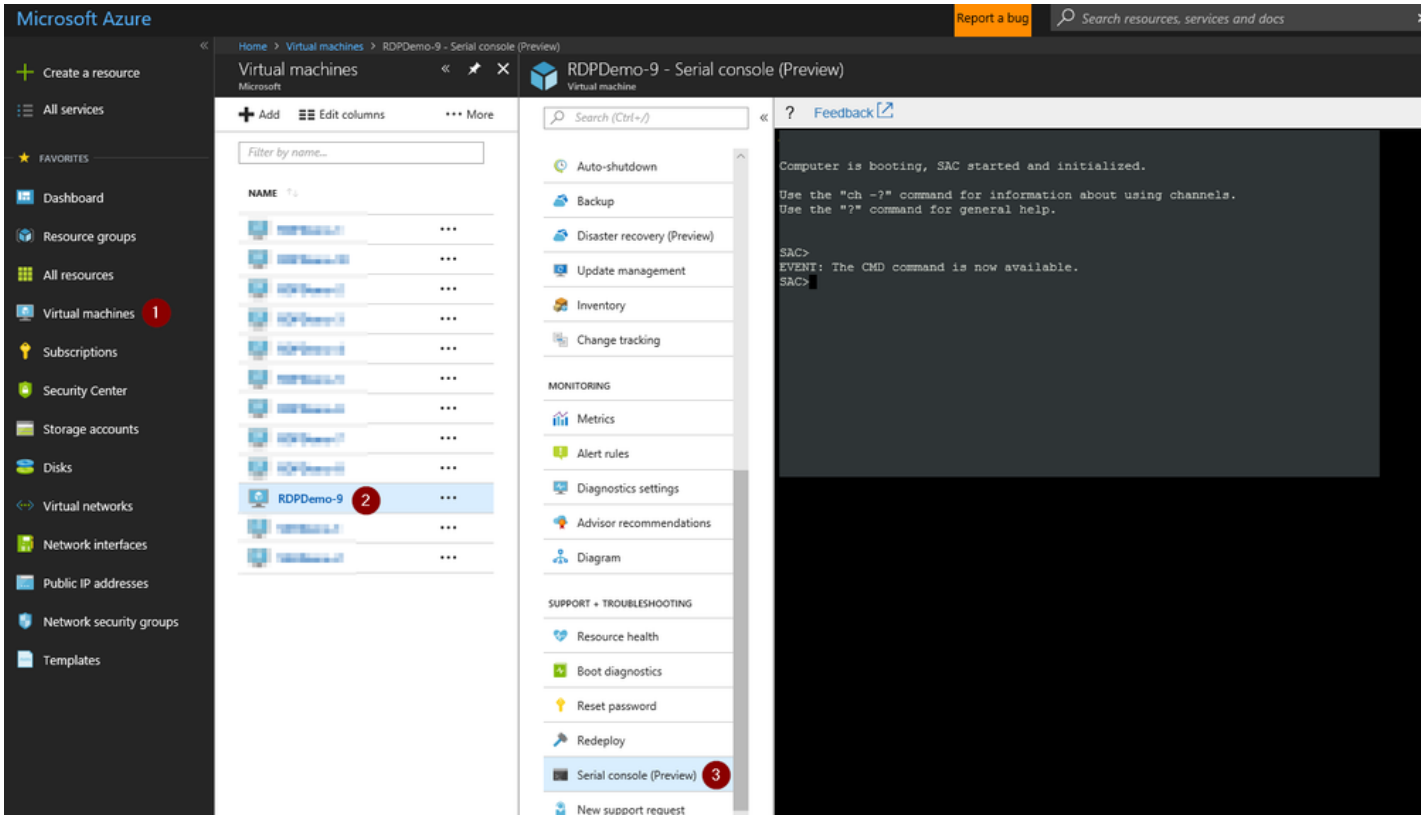
WAC is supported on ARM VMs running Windows Server 2016 or later (not Win10 or any other Windows client version, and not 2012R2/2012/2008R2 versions of Windows Server

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
```

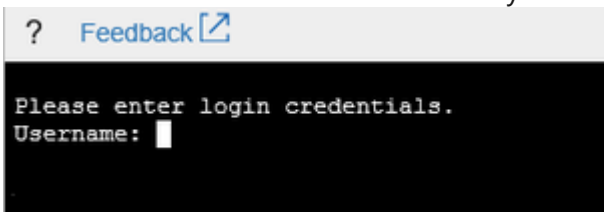
```
SAC>ch -si 1
```

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

```
? Feedback
Name:                   Cmd0001
Description:            Command
Type:                   VT-UTF8
Channel GUID:           [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.
```

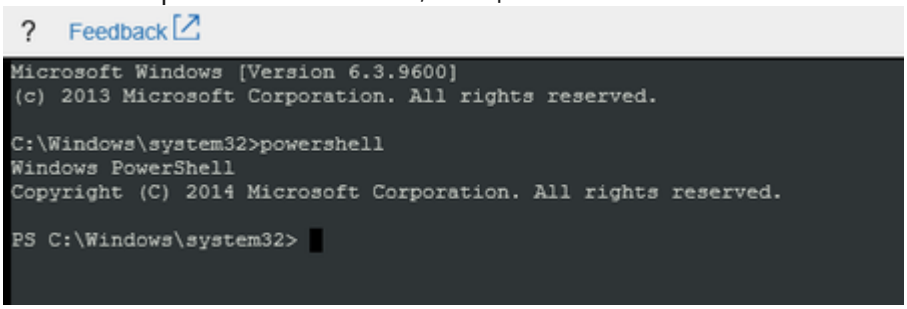
6. Hit enter a second time and it will ask you for user, domain and password:



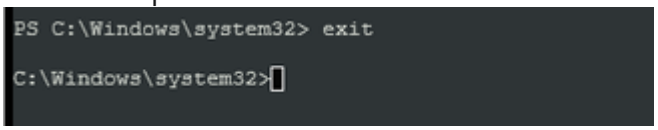
    1. If the machine has connectivity, you could use either local or domain IDs. If you want to use a local ID, for domain just add the hostname of the VM
    2. If the machine doesn't have connectivity, you could try to se domains IDs however this will work if only the credentials are cached on the VM.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

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



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



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

Using *Remote Powershell*

▶ Click here to expand or collapse this section

Using *Remote CMD*

▶ Click here to expand or collapse this section

Using *Custom Script Extension* or *RunCommands Feature*

▶ Click here to expand or collapse this section

Using *Remote Registry*

▶ Click here to expand or collapse this section

Using *Remote Services Console*

▶ Click here to expand or collapse this section

ONLINE Mitigations

1. You can use the Remote Desktop client for Windows Desktop to access Windows apps and desktops remotely from a different Windows device.

2. Choose the client that matches the version of Windows. The new Remote Desktop client (MSRDC) supports Windows 10, Windows 10 IoT Enterprise, and Windows 7 client devices.

- Windows 64-bit
- Windows 32-bit
- Windows ARM64

3. You can install the client for the current user, which doesn't require admin rights, or your admin can install and configure the client so that all users on the device can access it.

4. Once you've installed the client, you can launch it from the Start menu by searching for Remote Desktop.

Note: You might need the client logs when investigating a problem.

1. To retrieve the client logs:

    1. Ensure no sessions are active and the client process isn't running in the background by right-clicking on the Remote Desktop icon in the system tray and selecting Disconnect all sessions.
    2. Open File Explorer.
    3. Navigate to the %temp%\DiagOutputDir\RdClientAutoTrace folder.

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***

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!