Black Screen Generic_RDP SSH

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

Tags

cw.TSG cw.RDP-SSH

Contents

Symptoms

Customer reports that after he's entering the credentials on RDP, the GUI is not loaded on the RDP Session and the customer gets only a Black window.

- The VM has connectivity

- RDP is responding
- After you enter the credentials, the profile does not complete to load getting a black screen

Root Cause Analysis

What the black screen tells us is that RDS was able to connect to the server but was unable to transition to the Blue background of the logon and policy processing functions of Winlogon.

This is usually an indication the server is in a bad state were something on the box is deadlocked on some resource and the only way to determine the root cause is to dump the machine when in the problem state to see who/what is creating a blocking lock on some resource on the Server.

References

N/A

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*	Check with the RDP SME since this will depend on the analysis from GES and also, this is a new scenario.	

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

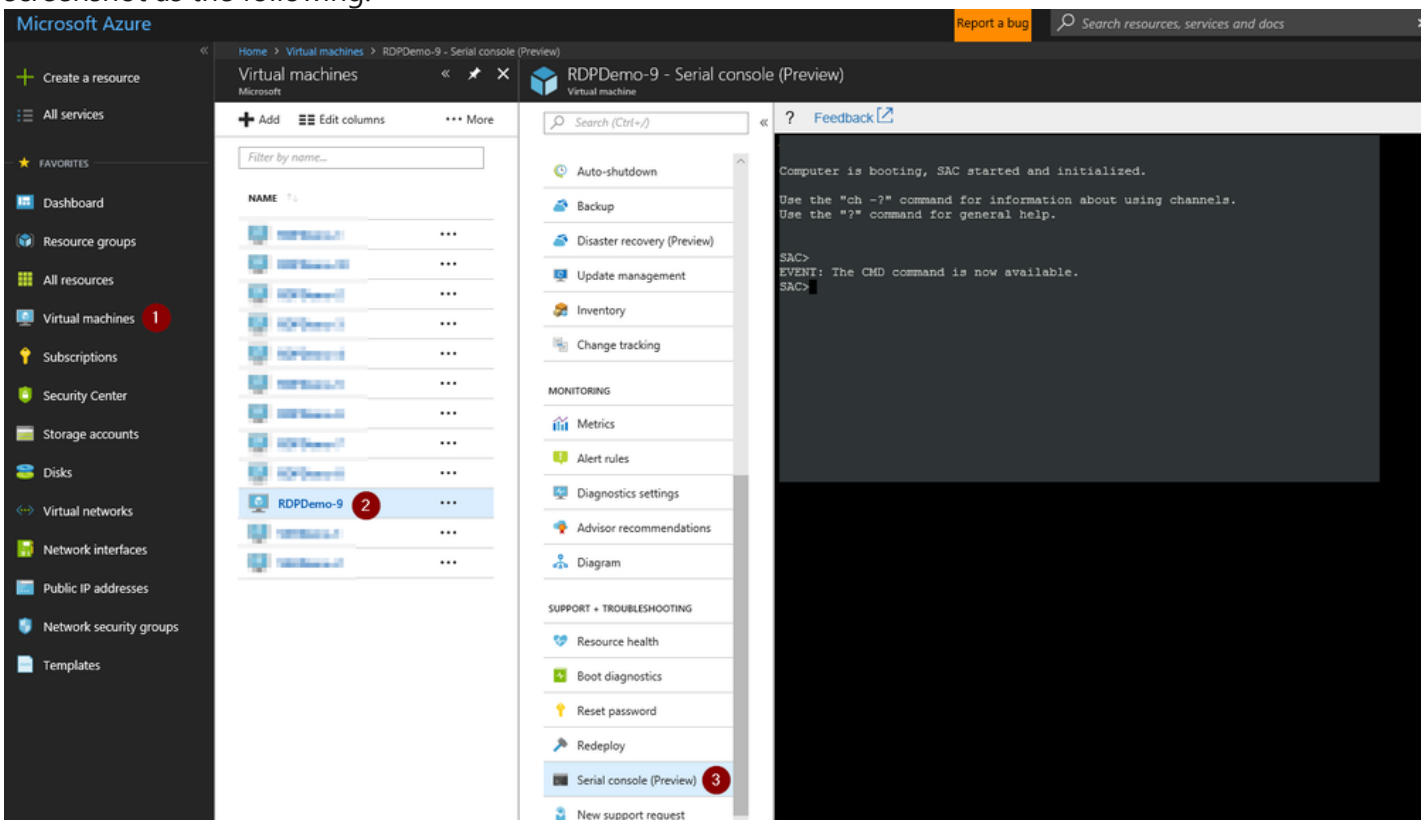
WAC is supported on ARM VMs running Windows Server 2016 or later (not Win10 or any other Windows client version, and not 2012R2/2012/2008R2 versions of Windows Server

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

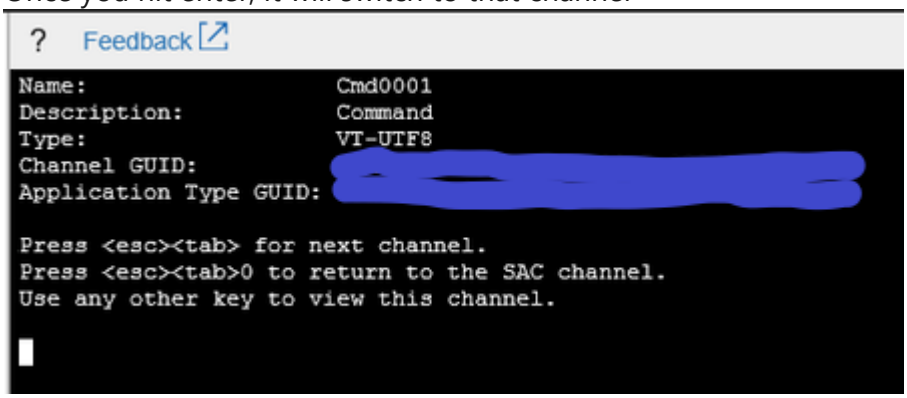
```
SAC>cmd
The Command Prompt session was successfully launched.
SAC>
EVENT:   A new channel has been created.  Use "ch -?" for channel help.
Channel: Cmd0001
SAC>
```

4. Switch to the channel running the CMD instance

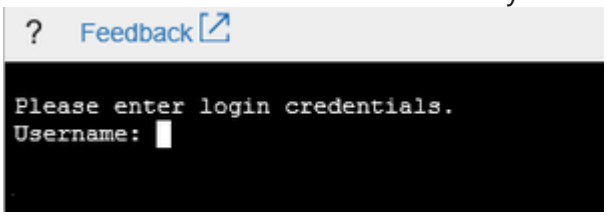
```
ch -si 1
```

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

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



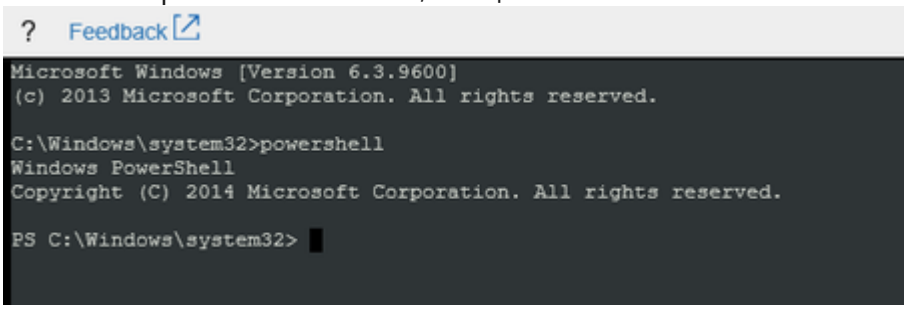
6. Hit enter a second time and it will ask you for user, domain and password:



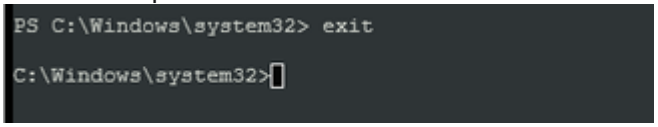
    1. If the machine has connectivity, you could use either local or domain IDs. If you want to use a local ID, for domain just add the hostname of the VM
    2. If the machine doesn't have connectivity, you could try to se domains IDs however this will work if only the credentials are cached on the VM.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

Mitigation 1

▼ Click here to expand or collapse this section

1. Open an elevated CMD instance and run a system consistency check:

```
dism /online /cleanup-image /restorehealth
```

2. If the outcome says that corruption was find and fixed, rerun `dism` till it says that server is corruption free

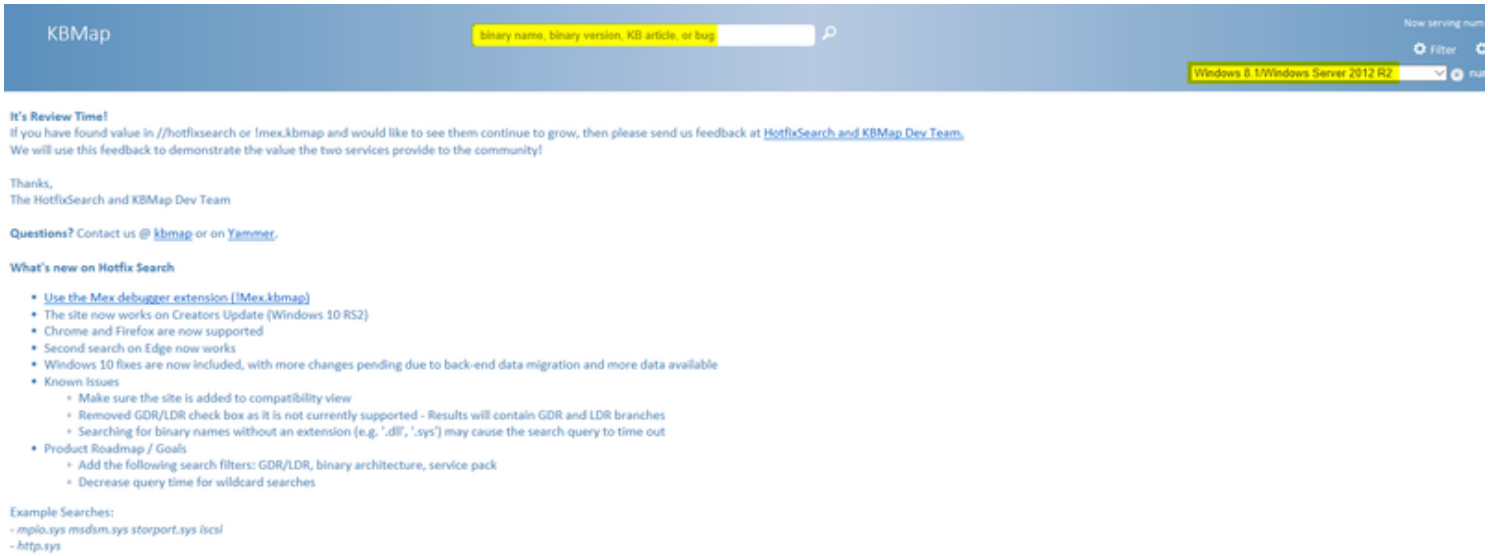
3. If the outcome says that corruption is found but couldn't fix it, then collect the following logs to see where the corruption is, you can do this by running Inspect IAAS Disk mode *WindowsUpdate*:

```
C:\Windows\Logs\DISM\dism.log
C:\Windows\Logs\CBS\cbs.log
```

4. If you need assistance on how to read these logs, reach out to the SME RDP channel on teams

5. Once you identify where the corruption is, then you can install the latest KB that introduce this file and all the related to its subsystem:

    1. Get the OS version of the VM
    2. Browse up to KBMAP and select the OS and the binary that you are looking for and click search. This will give you the KB history of that component so you could install the latest KB on the image.



Note: If the query comes with an empty query, it means that the file you look for is not OS related so you may want to skip from the following way to fix this 3. Download the KB that performs the upgrade on the troubleshooting VM on a folder like `c:\temp` 4. Install the KB on that OS disk

```
dism /online /add-package /packagepath:c:\temp\<<KB .msu or .cab>>
```

6. Restart the VM and retry

Mitigation 2

▼ Click here to expand or collapse this section

1. A memory dump from the VM needs to be collected **while the VM is on state**.
    1. Confirm if customer has already granted permission in DfM "Product details" section: `Customer permission granted: Yes` If No, ask the customer to go to their case in the Portal and grant us permission to look at OS logs. An example email can be found at: https://aka.ms/azdataperm/
    2. Refer to How to Get an OS Dump from an Azure Virtual Machine
    3. Once the memory dump was collected, then engage the GES team (Windows EEs) for a dump analysis. Cut a problem with the following details:
        - Product: ***Windows Svr 2008 R2*** or ***Windows Svr 2012 R2 Datacenter*** or ***Windows Svr 2016 Datacenter*** or ***Windows Svr 2019 Datacenter*** as appropiate
        - Support topic: ***Routing Windows V3\System Performance\System Hangs***
        - Problem Description:

```
================== <start copy> =====================================
Customer-facing error (RDP client error):
Symptoms description:

SR#
VM name
ICM#                  <--- Only if the dump was collected from the Host
Datacenter            <--- Only if the dump was collected from the Host
Jumpbox               <--- Only if the dump was collected from the Host
Path in the jumpbox   <--- Only if the dump was collected from the Host
================== <end copy> =======================================
```

- These routing will route you to a Windows team however since we need to engage GES, override the routing to
  - For Premier cases: ***Windows EE Premier*** queue
  - For Professional cases: ***Windows EE Pro*** queue

2. Proceed with the action plan provided by the Windows EE

OFFLINE Troubleshooting

This scenario can only be investigated in ONLINE mode

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!