Black Screen on RDP_RDP SSH

Last updated by | Yuri Ohno | Jun 2, 2022 at 5:39 PM PDT

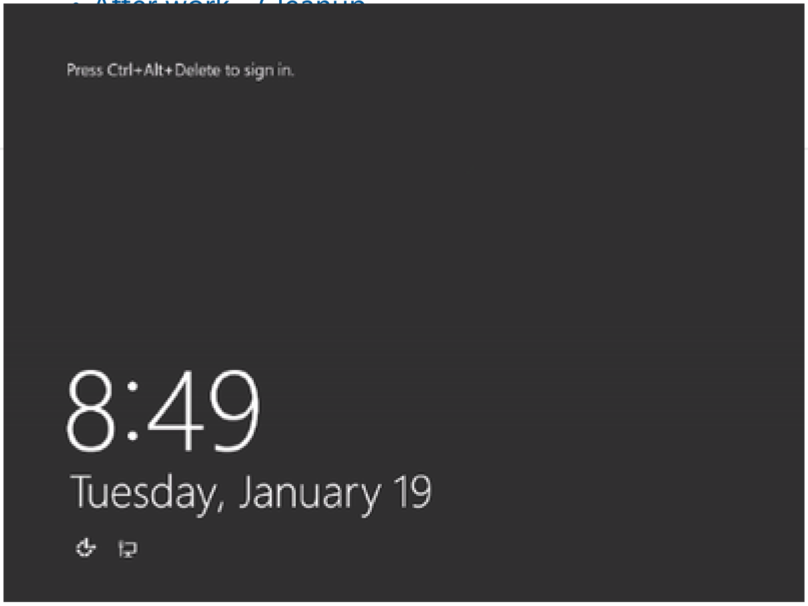
Tags

cw.TSG	cw.RDP-SSH

Contents

Symptoms

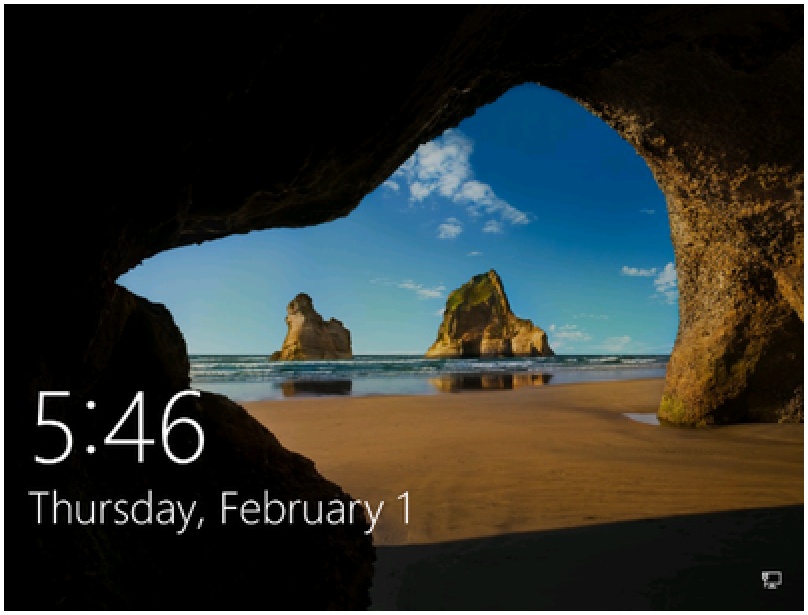
1. The screenshot shows no issues and is on CTRL+ALT+DEL



Press Ctrl+Alt+Delete to sign in.

8:49

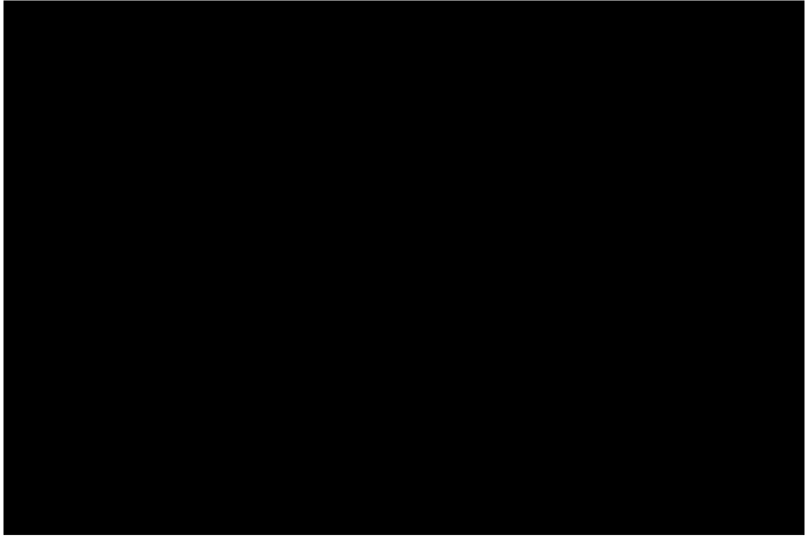
Tuesday, January 19



5:46

Thursday, February 1

2. When you RDP a machine, you'll get prompted for the credentials and then you get a black screen:



3. Ping will respond just fine
4. All the other services/apps/PS/SMB on the VM may or maynot work since the VM is in a partial hang state.
5. For Windows Server 2012 R2 VMs, if there's any running application like SQL, it may run but slow, if the machine is restarted, the issue is temporarily fix
6. For Windows 10 RS3 VMs, if you resize to any size with more than 1 CPU, the issue is mitigated.

Root Cause Analysis

Root Cause Analysis 1

This only applies for Windows Server 2012 R2 VMs

The OS is running into a known issue where a deadlock can occur when the service ***WinHttpAutoProxySvc*** is disabled and the system was under significant stress and RPCSS is having multiple threads trying to get information from WinHttpAutoProxy.

Root Cause Analysis 2

This only applies for Windows 10 RS3 VMs only

The image ***MicrosoftWindowsDesktop.Windows-10.RS3-Pro.latest*** currently has an issue that if it is deploy with only 1 CPU, the OS will not complete its initialization hanging while trying to initialize the Azure Agent Service. If this is resize to any size with 2 CPUs, the OS will come up but very slow till this initialization is complete. With 2 CPU you can at least complete the RDP Session but its performance will be bad. The more the CPUs are added on the first boot, the faster this initialization is completed and once is complete the VM could be resize back to 1 CPU if needed.

This issue is currently under investigation by the image owner and *this image is being removed from the Marketplace till this issue is resolved*.

```
OS Bug 15849068
```

Root Cause Analysis 3

This applies to *Citrix Xenapp servers*

Under certain circumstances, Citrix Profile Management deletes some registry keys after session logoff. As a result, the session can appear as a black screen after the VDA restarts.

For further information on this issue, please refer to the following articles from Citrix:

- 7.15 LTSR CU2 Session Launches as a Black Screen with Profile Management Enabled
- Server 2016 black screen

Root Cause Analysis 4

File system corruption.

Root Cause Analysis 5

This applies to *Windows Virtual Desktop (Windows 10 Version 2004)*

known issue on Windows virtual desktop machines. This issue was fixed on September 2020 KB4571744 release. https://support.microsoft.com/en-us/help/4571744/windows-10-update-kb4571744

This KB Addresses an issue that displays a black screen to Windows Virtual Desktop (WVD) users when they attempt to sign in.

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\Virtual Machine\Guest OS - Windows\Isolated\Windows Services not starting/crashing*	
2	*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\Administration\HowTo:Size Family Issues - Not possible due to hardware limitations*	OS Bug 15849068
3	*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\Non-Boot\File System Corruption*	

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\Root Cause Not Determined	Applicable_Unsupported 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

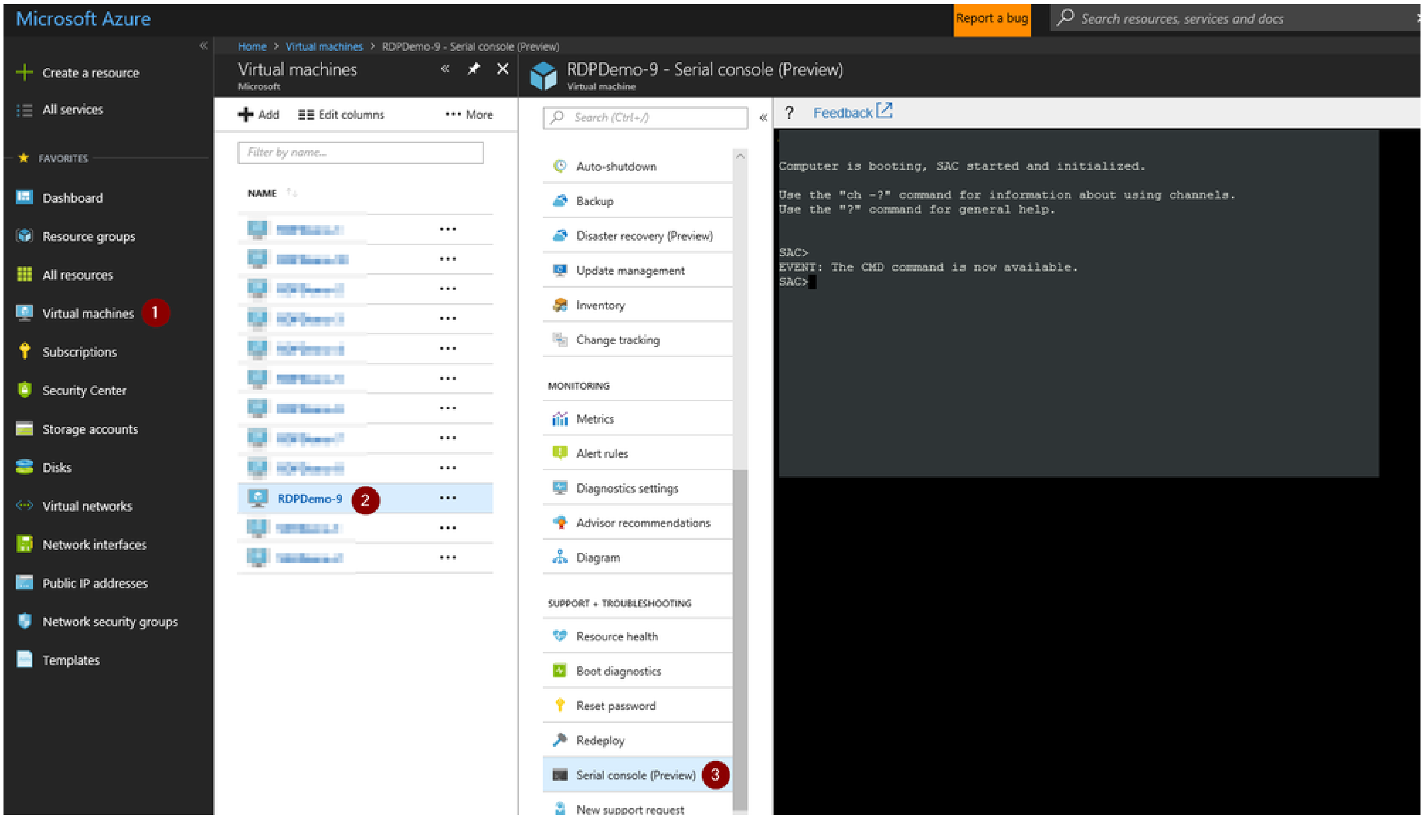
WAC is supported on ARM VMs running Windows Server 2016 or later (not Win10 or any other Windows client version, and not 2012R2/2012/2008R2 versions of Windows Server

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

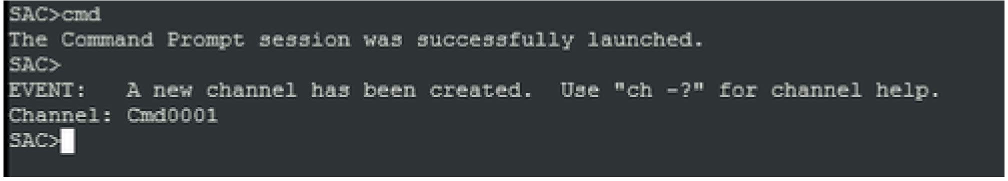
1. In the portal on the VM blade you will have an extra option called *Serial Console* click there
2. If EMS was enabled on the Guest OS, SAC will be able to connect successfully and then you will have a screenshot as the following:



```
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



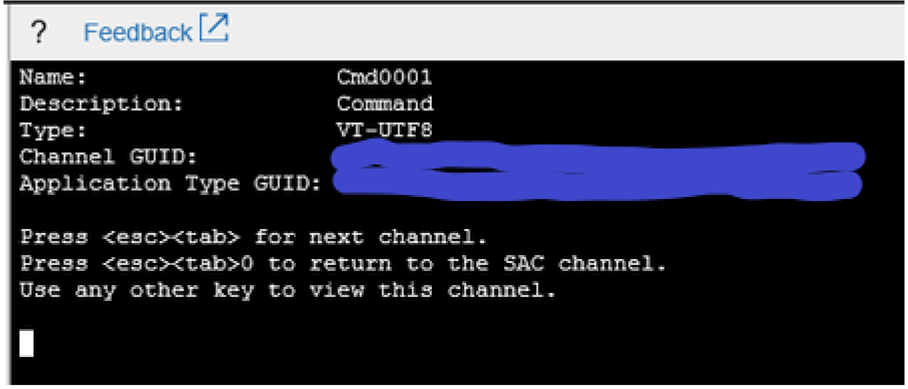
```
SAC>cmd
The Command Prompt session was successfully launched.
SAC>
EVENT:   A new channel has been created.  Use "ch -?" for channel help.
Channel: Cmd0001
SAC>
```

4. Switch to the channel running the CMD instance

```
ch -si 1
```

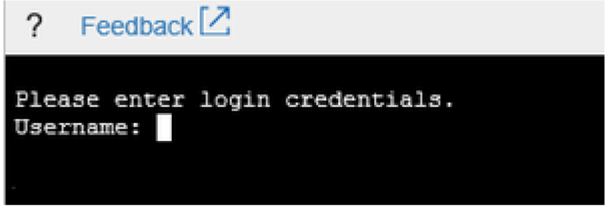
```
SAC>ch -si 1
```

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



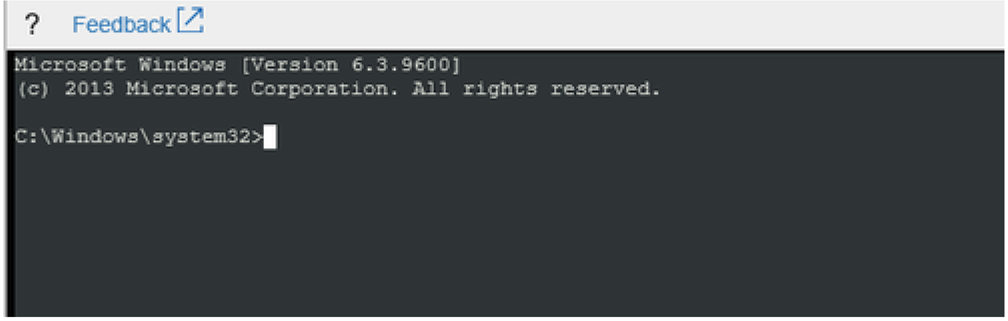
```
Name:                   Cmd0001
Description:            Command
Type:                   VT-UTF8
Channel GUID:           [redacted]
Application Type GUID:  [redacted]

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:

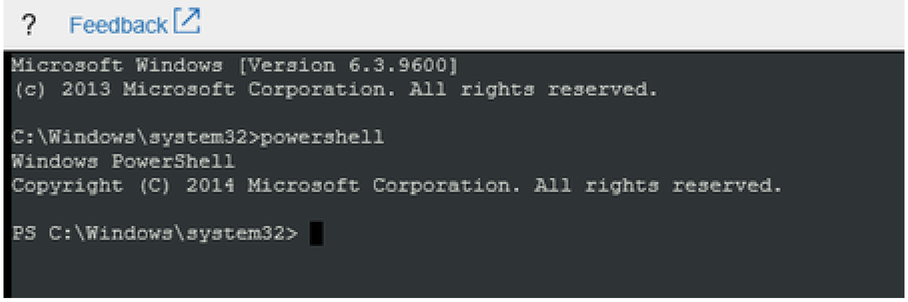
   ```
   Please enter login credentials.
   Username: █
   ```

   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:

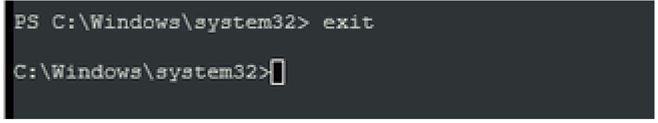
   ```
   Microsoft Windows [Version 6.3.9600]
   (c) 2013 Microsoft Corporation. All rights reserved.

   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

ONLINE Mitigations

Mitigation 1

▼ Click here to expand or collapse this section

Applies only for Windows Server 2012 R2 VMs

1. Restore the service *WinHttpAutoProxySvc* to its default startup value. Open an elevated CMD and run the following:

```
sc config WinHttpAutoProxySvc start= demand
```

2. Restart the VM and retry

Mitigation 2

▼ Click here to expand or collapse this section

Applies only for Windows 10 RS3

As a temporary fix, resize this VM to a minimum of 3vCPUs so the OS could complete its initialization.

1. Once the VM is started with the 3 vCPU, ask the customer to login to RDP so the whole profile is completed and the VM could initialized the components in the OS.
2. Once it is done, if the customer prefers to, he could resize back to 1 vCPU

This issue was already reported and is under investigation by the image owner who will replace this image as soon as possible but currently is retiring this image from the Marketplace.

Mitigation 3

▼ Click here to expand or collapse this section

1. Refer to *Mitigation 4* on Fail RDP connection on a Citrix VM

Mitigation 4

▼ 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

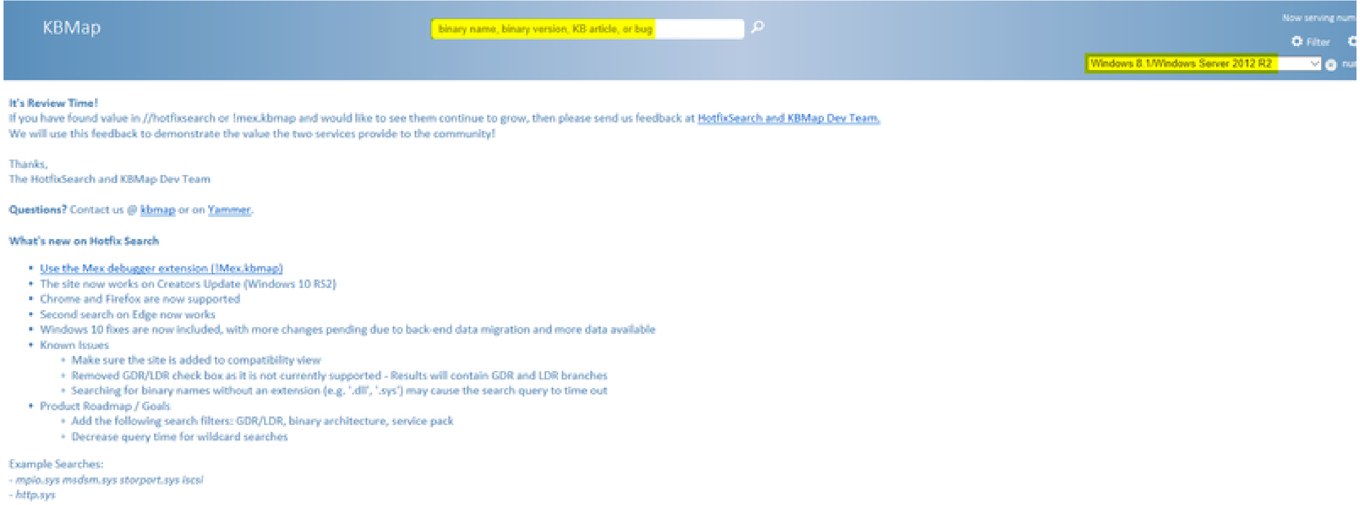
3. If the outcome says that corruption is found but couldn't fix it, then collect the following logs to see where the corruption is:

```
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.

       
       KBMap
binary name, binary version, KB article, or bug
Now serving num
Filter
Windows 8.1/Windows Server 2012 R2

       It's Review Time!
       If you have found value in //hotfixsearch or !mex.kbmap and would like to see them continue to grow, then please send us feedback at HotfixSearch and KBMap Dev Team.
       We will use this feedback to demonstrate the value the two services provide to the community!

       Thanks,
       The HotfixSearch and KBMap Dev Team

       Questions? Contact us @ kbmap or on Yammer.

       What's new on Hotfix Search

       - Use the Mex debugger extension (!Mex.kbmap)
       - The site now works on Creators Update (Windows 10 RS2)
       - Chrome and Firefox are now supported
       - Second search on Edge now works
       - Windows 10 fixes are now included, with more changes pending due to back-end data migration and more data available
       - Known Issues
         - Make sure the site is added to compatibility view
         - Removed GDR/LDR check box as it is not currently supported - Results will contain GDR and LDR branches
         - Searching for binary names without an extension (e.g. '.dll', '.sys') may cause the search query to time out
       - Product Roadmap / Goals
         - Add the following search filters: GDR/LDR, binary architecture, service pack
         - Decrease query time for wildcard searches

       Example Searches:
       - *mpio.sys msdsm.sys storport.sys iscsi*
       - *http.sys*

       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 5

▼ Click here to expand or collapse this section

Check if the Machine has the KB4571744 installed, if not proceed to install it, you could see the patch level of the server in WinGuestAnalyzer report.

If it is not installed, open an elevated Powershell instance and run the following script:

```
## Create a download location
md c:\temp

## Download the KB File
remove-module psreadline
$source = "http://download.windowsupdate.com/d/msdownload/update/software/updt/2020/09/windows10.0-kb457174
$destination = "c:\temp\windows8.1-kb3197875-x64_979273db494c9f70d0a6cfbffb2d033f30ddf01b.msu"
$wc = New-Object System.Net.WebClient
$wc.DownloadFile($source,$destination)

## Install the KB
expand -F:* $destination C:\temp\
dism /ONLINE /add-package /packagepath:"c:\temp\Windows10.0-KB4571744-x64_PSFX.cab"

## Restart the VM to complete the installatioin/settings
shutdown /r /t 0 /f
```

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

OFFLINE Mitigations

Mitigation 1

▼ Click here to expand or collapse this section
Applies only for Windows Server 2012 R2 VMs

1. Restore the service *WinHttpAutoProxySvc* to its default startup value. Open an elevated CMD and run the following:

```
REG ADD "HKLM\BROKENSYSTEM\ControlSet001\Services\WinHttpAutoProxySvc" /v Start /t REG_DWORD /d 3 /f
REG ADD "HKLM\BROKENSYSTEM\ControlSet002\Services\WinHttpAutoProxySvc" /v Start /t REG_DWORD /d 3 /f
```

1. Restart the VM

Mitigation 2

▼ Click here to expand or collapse this section

Applies only for Windows 10 RS3

As a temporary fix, resize this VM to a minimum of 3vCPUs so the OS could complete its initialization.

1. Once the VM is started with the 3 vCPU, ask the customer to login to RDP so the whole profile is completed and the VM could initialized the components in the OS.
2. Once it is done, if the customer prefers to, he could resize back to 1 vCPU

This issue was already reported and is under investigation by the image owner who will replace this image as soon as possible but currently is retiring this image from the Marketplace.

Mitigation 3

▼ Click here to expand or collapse this section

1. Refer to *Mitigation 4* on Fail RDP connection on a Citrix VM

Mitigation 4

▼ Click here to expand or collapse this section

1. Open an elevated CMD

```
dism /image:<OS Disk letter>:\ /cleanup-image /restorehealth
```

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!