Client Code 0x1104_RDP SSH

Last updated by | Heath Rensink | Feb 7, 2023 at 9:52 AM PST

Tags

cw.TSG	cw.RDP-SSH

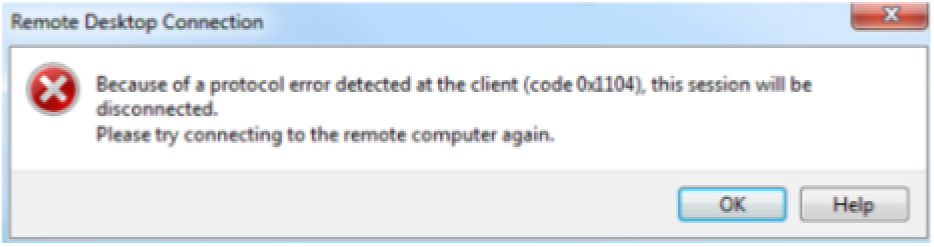
Contents

Symptoms

1. When you try to RDP to an azure VM, the below error is immediately shown without even prompting for creds.� But other means of communication to the VM like SMB, RPC etc will be working, provided the firewall rules are in place.

```
Because of a protocol error detected at the client (code 0x1104), this session will be disconnected.
```

```
Please try connecting to the remote computer again.
```



Because of a protocol error detected at the client (code 0x1104), this session will be disconnected.
Please try connecting to the remote computer again.

Root Cause Analysis

Another application is installed and listener on the RDP Port 3389.

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\My problem is not listed above*	*Root Cause - Windows Azure\Virtual Machine\Guest OS - Windows\VM Responding\RDP Listener misconfiguration/issues\RDP Port changed*	

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

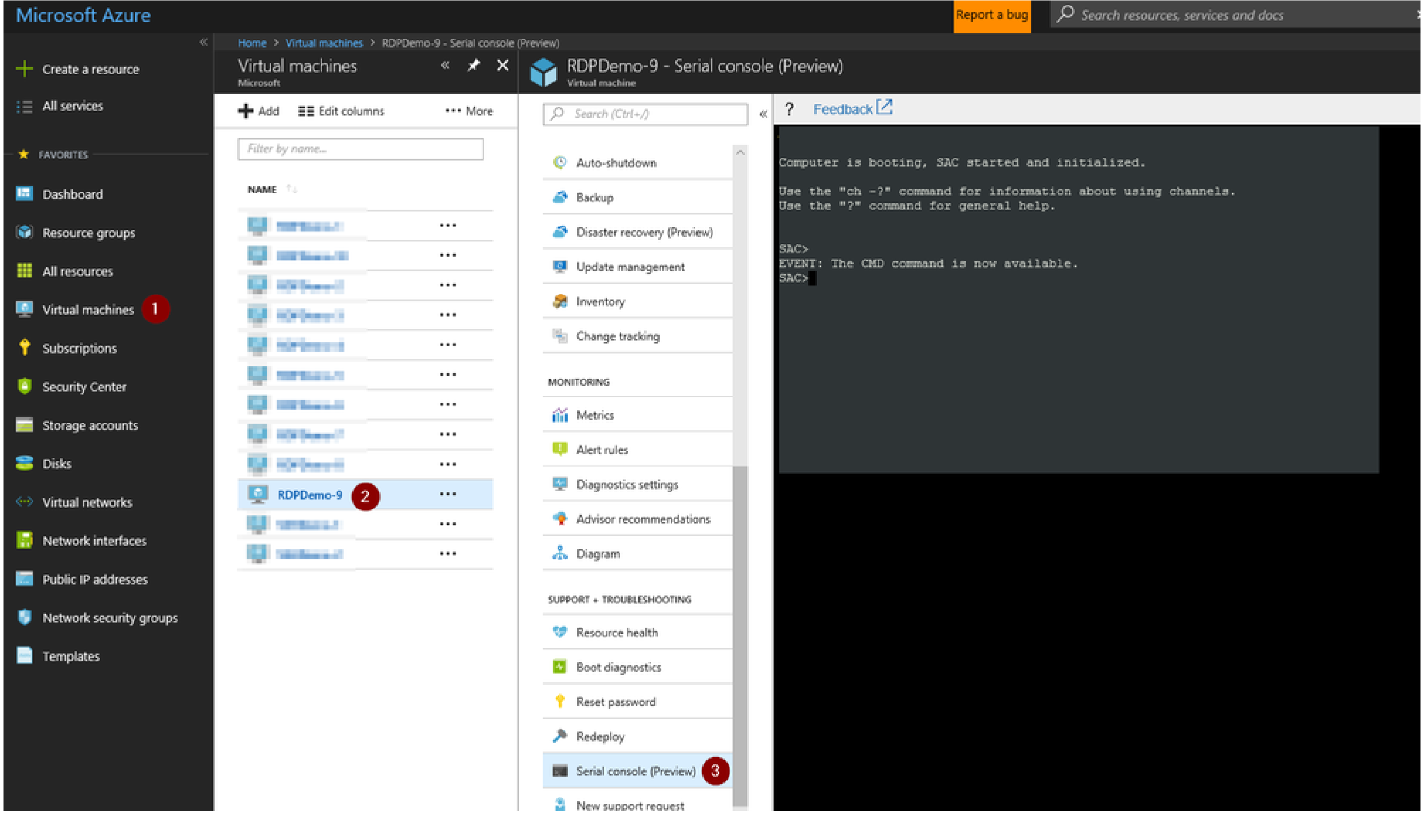
See [How To Access Thru Windows Admin Center]

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:

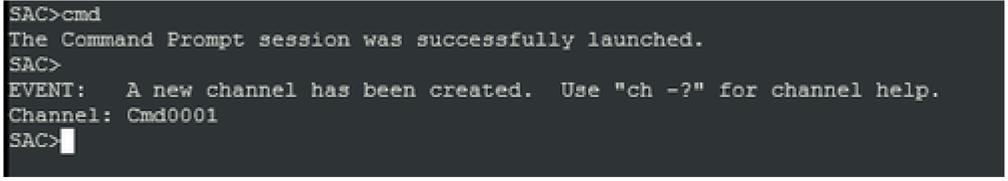


```
Computer is booting, SAC started and initialized.

Use the "ch -?" command for information about using channels.
Use the "?" command for general help.

SAC>
EVENT: The CMD command is now available.
SAC>
```

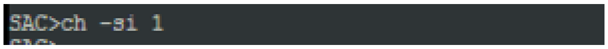
   1. If EMS does not connect, it means the Guest OS was not setup to use this feature:
      1. If the issue that you have will repro on a restart and if the customer is OK to enable this feature, you enable this feature. For details refer to [Serial Console] on the *How to enable this feature*
      2.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

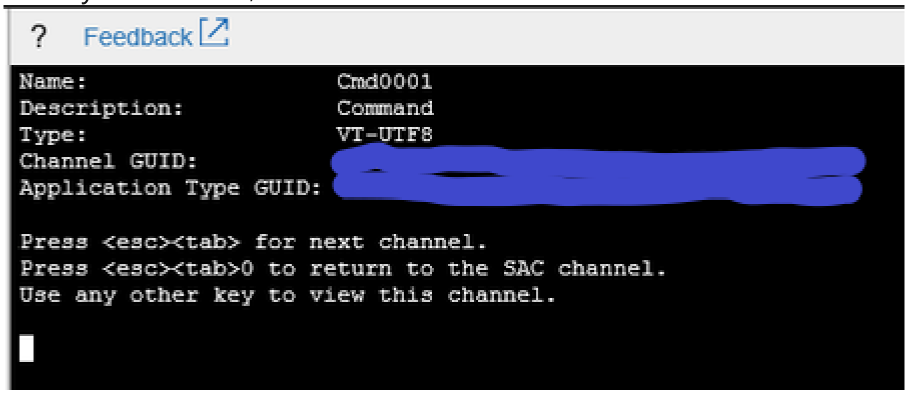
4. Switch to the channel running the CMD instance

```
ch -si 1
```



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

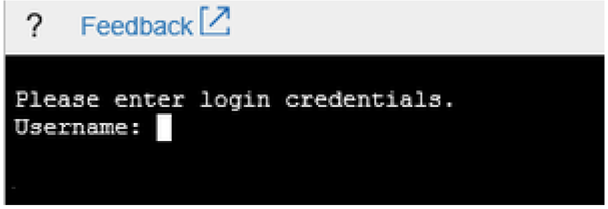
5. Once you hit enter, it will switch to that channel



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

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

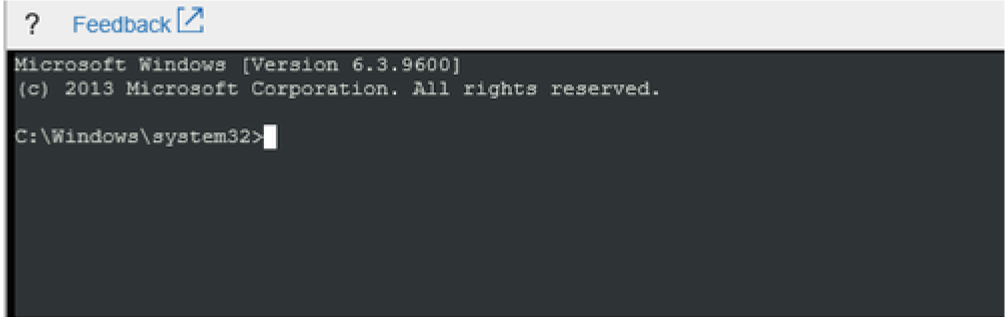
6. Hit enter a second time and it will ask you for user, domain and password:



```
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.

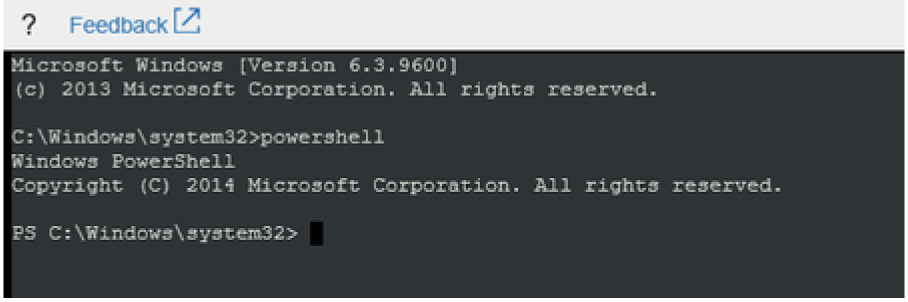
7. Once you add valid credentials, the CMD instance will open and you will have the prompt for you to start your troubleshooting:



```
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`

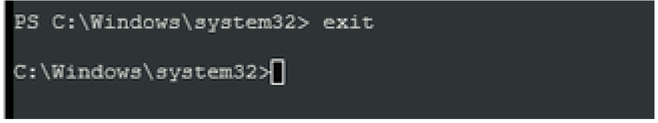


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

▼ Click here to expand or collapse this section

1. Open an elevated Powershell session
2. Use the NETSTAT tool to get the list of application running on the OS and which port are using:

   ```
   Netstat -anob
   ```

3. You will notice that some other process like probably system process is listening on port 3389 but not the termservice.exe. On a working machine, termservice.exe is listening on 3389 not the system process.
4. Now we need to either change the port of the RDP to something else to get the RDP working or stop the application which is currently listening on port 3389
5. If the customer wants to use the default RDP port, he may need to move his application to some other port but to do so he needs to stop the application to do so and then restart the VM to take the changes
   1. Stop the service for the application that is using the 3389 service (customer should be aware of the service name in this case).

      ```
      Stop-Service -Name <<ServiceName>>
      ```

   2. Start the terminal services service

      ```
      Start-Service -Name Termservice
      ```

   3. At this point the customer needs to change the port of the application to avoid for the issue to reoccurrence

6. If the customer is unable to stop the application since this will impact in his production, we could change the RDP port

    1. From the PowerShell console you can change the default RDP port. You will need to know the Hexadecimal equivalent of the custom port.

        ```
        Set-ItemProperty -Path 'HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -
        ```

    2. Restart the terminal services service

        ```
        Stop-Service -Name Termservice
        Start-Service -Name Termservice
        ```

    3. You will still not have RDP access till the following changes are done

        1. The Windows Firewall needs to be updated with the new port information:
            1. You could update the *Remote Desktop Rule* with the new port:

                ```
                Set-NetFirewallRule -Name "RemoteDesktop-UserMode-In-TCP" -LocalPort <NEW PORT (decimal)>
                ```

            2. Another approach will be to disable the firewall temporarily till you update the rule

                ```
                netsh advfirewall set allprofiles state off
                ```

        2. The NSG needs to be updated with this new port

7. In case you disabled the Windows Firewall, suggest the customer that after he regain access, to enable the firewall back

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

▼ Click here to expand or collapse this section

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

```
REM This will assume that the disk is drive F:, if this is not your case, update the letter assignment
reg load HKLM\BROKENSYSTEM F:\windows\system32\config\SYSTEM

REM Update the RDP Port to <CUSTOM PORT>. On the lines below, translate the custom port to hexadecimal (e
REG ADD "HKLM\BROKENSYSTEM\ControlSet001\Control\Terminal Server\WinStations\RDP-Tcp" /v PortNumber /t RE
REG ADD "HKLM\BROKENSYSTEM\ControlSet002\Control\Terminal Server\WinStations\RDP-Tcp" /v PortNumber /t RE

REM Enable the RDP rules on the firewall. On the lines below, the custom port is on decimal
REG ADD "HKLM\BROKENSYSTEM\ControlSet001\Services\SharedAccess\Defaults\FirewallPolicy\FirewallRules" /v
REG ADD "HKLM\BROKENSYSTEM\ControlSet002\Services\SharedAccess\Defaults\FirewallPolicy\FirewallRules" /v

reg unload HKLM\BROKENSYSTEM
```

2. While the VM is rebooting, change the destination port in the azure portal
   - For V1 machine, recreate the RDP Endpoint updating the internal port
   - For V2 machine, in the Inbound rule of the associated NSG to reflect the new port number
3. Now, once the VM is rebooted, retry

Note: Bear in mind that in case you change the default RDP port for the VM, the customer may need to update his on premise firewalls to allow that traffic to that port. An easy way to test if the customer has any setting preventing this access on their environment is to try to RDP from your machine and see if it works and if it does, then the customer may need to do further settings on his on premise environment.

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!