

Service Failing Service Account_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
 - Tracking close code for this volume
- Customer Enablement
- Mitigation
 - Backup OS disk
 - 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
 - Using Remote Powershell
 - Using Remote CMD
 - Using Custom Script Extension or RunCommands Feature
 - Using Remote Registry
 - Using Remote Services Console
 - ONLINE Mitigations
 - OFFLINE Troubleshooting
 - OFFLINE Approaches
 - Information
 - Using Recovery Script
 - For ARM VMs
 - For Classic VMs
 - Using OSDisk Swap API
 - Using VM Recreation scripts
 - For ARM VMs
 - For Classic VMs
 - For Classic VMs
 - Using OSDisk Swap API
 - Using VM Recreation scripts
 - For ARM VMs
 - For Classic VMs
 - OFFLINE Mitigations
- Escalate

- [After work - Cleanup](#)

Symptoms [Need additional help or have feedback?](#)

1. The VM screenshot shows the OS fully loaded and waiting for the credentials
2. There's no connectivity to the virtual machine on its VIP or DIP or its PA verified with [VM Port Scanner](#).
3. If you pull the Guest OS Logs, you'll see that some of the network relative services are unable to start. This could be the Network Store Interface Service (or any of the other network related services or services that have dependencies on network services).
4. On the  Guest OS logs, you could find an event stating that the service is unable to start due to The account specified for this service is different from the account specified for other services running in the same process:

```
Log Name:  System
Source:  Service Control Manager
Date:  12.08.2016 15:35:22
Event ID:  7000
Task Category: None
Level:  Error
Keywords:  Classic
User:  N/A
Computer:  RDPDemo.contoso.net
Description:
The Network Store Interface Service service failed to start due to the following error:
The account specified for this service is different from the account specified for other services run
```

5. Depending on the service that is failing to start, if any of those service belongs to the network stack like BFE, Windows Firewall, DHCP, etc, you could find that service failing to start and this also list in **WinGuestAnalyzer\Health Signal** tab on the *services* section:




```
{
  "services": [
    {
      "name": "TermService",
      "state": "Running",
      "startMode": "Manual"
    },
    {
      "name": "BFE",
      "state": "Stopped",
      "startMode": "Auto"
    }
  ]
}
```

Root Cause Analysis

The service is running in a shared process having the same PID and there's a mismatch between the startup account between those components.

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	

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

▼ Click here to expand or collapse this section

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

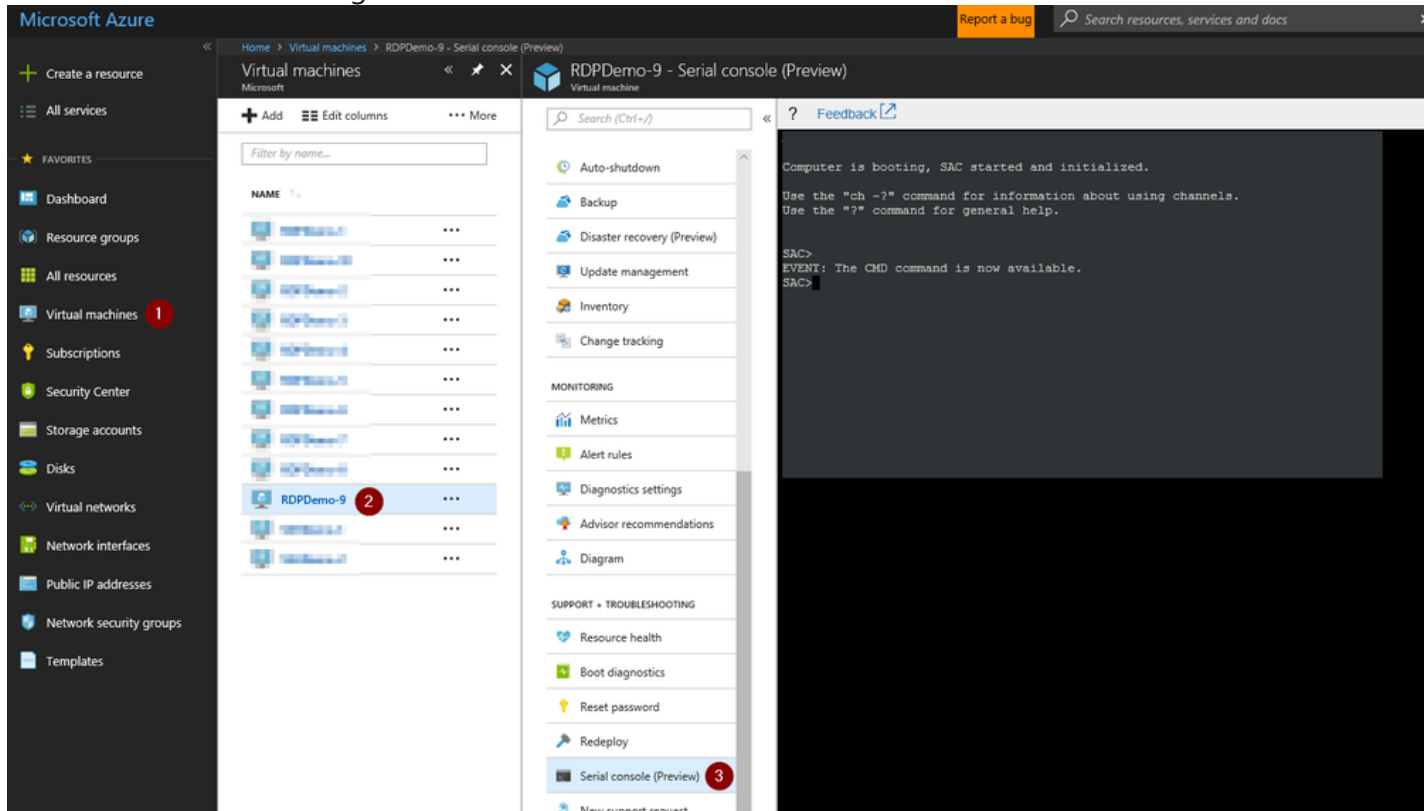
See [How To Access Thru Windows Admin Center](#)

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
```

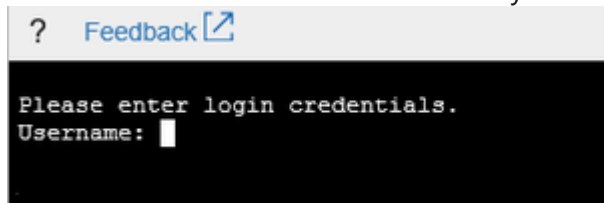
```
SAC>ch -si 1
```

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

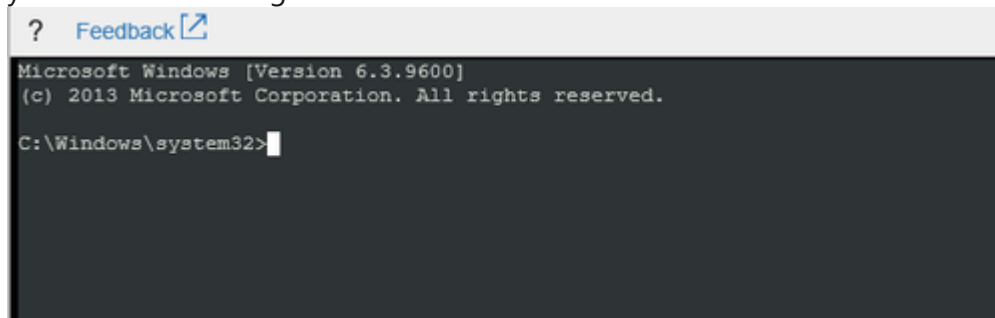
```
? Feedback
Name: Cmd0001
Description: Command
Type: VT-UTF8
Channel GUID: [REDACTED]
Application Type GUID: [REDACTED]

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:

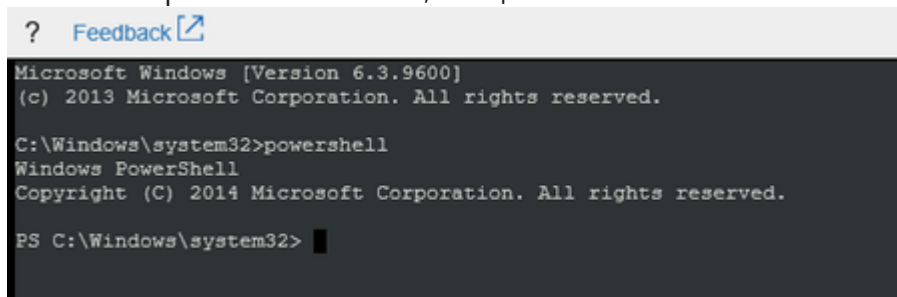


1. If the machine has connectivity, you could use either local or domain IDs. If you want to use a local ID, for domain just add the hostname of the VM
 2. If the machine doesn't have connectivity, you could try to use domains IDs however this will work if only the credentials are cached on the VM. In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

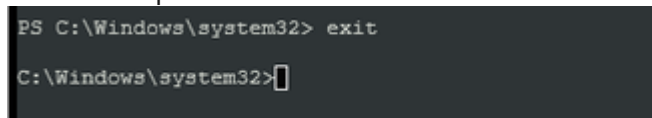


1. At this point, you can do your troubleshooting in bash (CMD) or else, you could start a powershell instance:

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

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

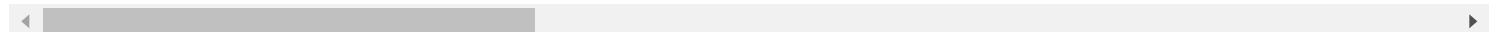
1. If you have a service failing to start with the error **due to service account error** means that:
 - That binary is sharing a process with other components under any of the *Svchost* processes
 - There's a mismatch between the startup account use on the failing component and the others components sharing the process container
2. First you need to identify what is the correct startup account to use and the best way to know which is the correct one is by checking on a working machine and then update yours:
 1. Open a CMD instance and query which is the account that the service is using currently using, that is **SERVICE_START_NAME**

```
sc qc <SERVICE NAME>
```
 2. Now compare this account with this service running in another working machine and then to change it to the correct value:


```
sc config <SERVICE NAME> obj= <SERVICE ACCOUNT>
```
3. You don't need to restart your VM, just go ahead and start your service

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

For Classic VMs

1. Use Phase 1 to mount the OS disk on your rescue VM
2. **PREMITIGATION STEPS TO ENABLE SAC AND CONFIGURE THE DUMP SETUP** Now open an elevated CMD instance and run the following script:

```
REM Load hive
reg load HKLM\BROKENSYSTEM f:\windows\system32\config\SYSTEM

REM Get the current ControlSet from where the OS is booting
for /f "tokens=3" %x in ('REG QUERY HKLM\BROKENSYSTEM\Select /v Current') do set ControlSet=%x
set ControlSet=%ControlSet:~2,1%

REM Suggested configuration to enable OS Dump
set key=HKLM\BROKENSYSTEM\ControlSet00%ControlSet%\Control\CrashControl
REG ADD %key% /v CrashDumpEnabled /t REG_DWORD /d 2 /f
REG ADD %key% /v DumpFile /t REG_EXPAND_SZ /d "%SystemRoot%\MEMORY.DMP" /f
REG ADD %key% /v NMICrashDump /t REG_DWORD /d 1 /f

REM Unload the hive
reg unload HKLM\BROKENSYSTEM
```

Note: This will assume that the disk is drive F; if this is not your case, update the letter assignment

3. <<<<<<INSERT MITIGATION>>>>>>

4. Use Phase 2 to reassemble the original VM with the now modified disk

Using [OSDisk Swap API](#)

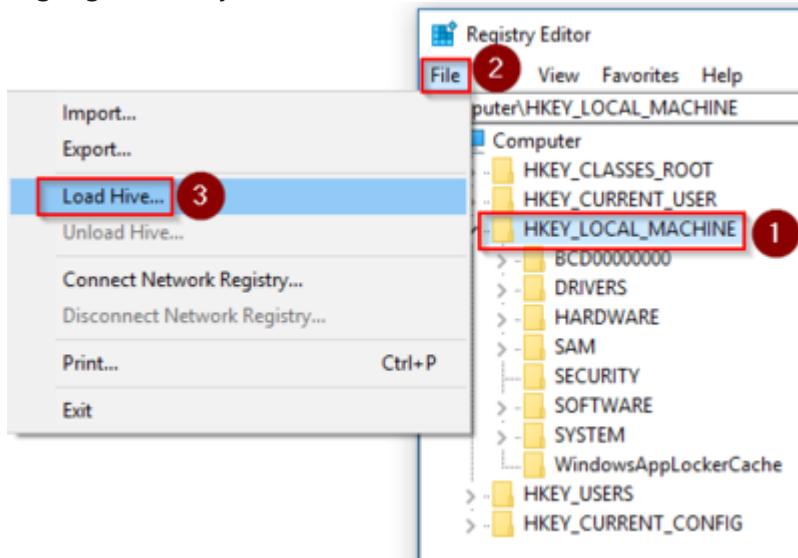
► Click here to expand or collapse this section

Using *VM Recreation scripts*

► Click here to expand or collapse this section

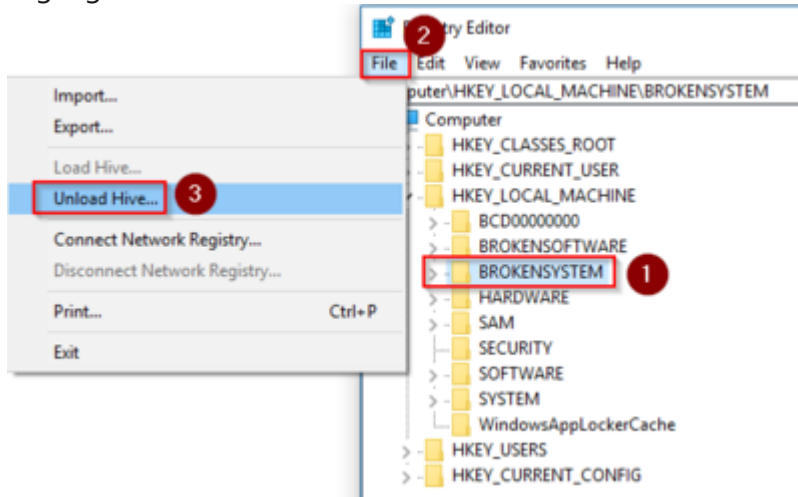
OFFLINE Mitigations

1. Before doing any change please create a copy of the folder `\windows\system32\config` in case a rollback on the changes is needed
2. On the troubleshooting machine, open up registry editor *REGEDIT*
3. Highlight the key *HKEY_LOCAL_MACHINE* and select *File\Load Hive* from the menu



4. Browse up to the file `\windows\system32\config\SYSTEM`
5. When you hit open it's going to ask for a name, put *BROKENSYSTEM* and then expand *HKEY_LOCAL_MACHINE* and you will see an extra key called *BROKENSYSTEM*
6. Browse up to the file `\windows\system32\config\SOFTWARE`
7. When you hit open it's going to ask for a name, put *BROKENSOFTWARE* and then expand *HKEY_LOCAL_MACHINE* and you will see an extra key called *BROKENSOFTWARE*
8. For this troubleshooting, we are mounting these trouble hives as *BROKENSYSTEM* and *BROKENSOFTWARE*
9. Now if you have that a particular service is failing **due to service account error** means that:
 - o That binary is sharing a process with other components under any of the *Svchost* processes
 - o There's a mismatch between the startup account use on the failing component and the others components sharing the process container
10. First you need to identify what is the correct startup account to use and the best way to know which is the correct one is by checking on a working machine and then update yours:
 1. Once you know the account, then check from which ControlSet is the machine booting:
`HKLM\BROKENSYSTEM\Select\Current` This is the number of the controlSet key to use
 2. Now update your failing service:
`HKLM\BROKENSYSTEM\ControlSet00x\services\<<Failing component>>\ObjectName`
11. Unmount Registry Hives
 1. Highlight *BROKENSYSTEM* and select *File\Unload Hive* from the menu

2. Highlight *BROKENSOFTWARE* and select *File\Unload Hive* from the menu



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

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>