

# There are Currently no Logon Servers Available\_RDP SSH

Last updated by | Subbu Konathala | Nov 18, 2022 at 9:21 AM PST

---

## Tags

[cw.TSG](#)[cw.RDP-SSH](#)

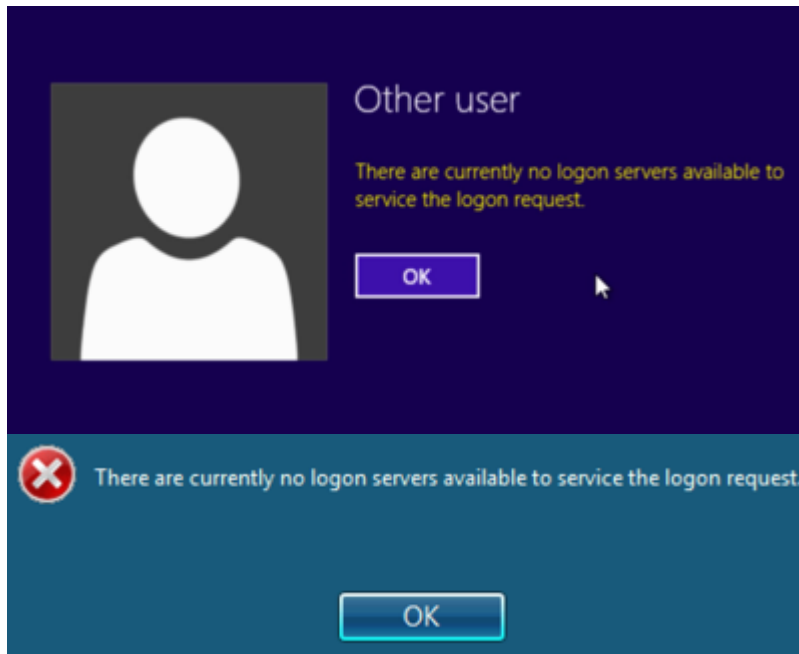
## Contents

- Symptoms
- Root Cause Analysis
  - Root Cause Analysis 1
  - Root Cause Analysis 2
  - Tracking close code for this volume
- Customer Enablement
- Refresher / Training Template
- Mitigation
  - 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
      - Mitigation 1
      - Mitigation 2
  - OFFLINE Troubleshooting
  - Escalate
  - After work - Cleanup
- Need additional help or have feedback?

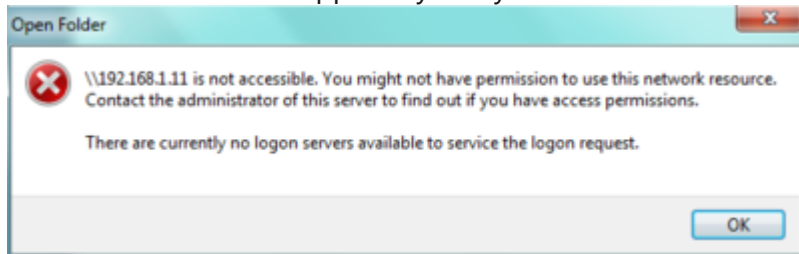
## Symptoms

1. The VM screenshot shows the OS fully loaded and waiting for the credentials however, when you try to logon, you get the following error:

There are currently no logon servers available to service the logon request.



2. This error could also happen if you try to access the VM using SMB:



3. On the Guest OS logs, you could find the event 4625 under *Security.evtx*:

Time: 6/17/2019 6:46:13 PM  
 ID: 4625  
 Level: Information  
 Source: Microsoft-Windows-Security-Auditing  
 Machine: contoso.local  
 Message: An account failed to log on.

Subject:  
 Security ID: \*No String Type\*  
 Account Name: -  
 Account Domain: -  
 Logon ID: 0

Logon Type: 3

Account For Which Logon Failed:  
 Security ID: \*No String Type\*  
 Account Name: tonyadmin  
 Account Domain: CONTOSO

Failure Information:  
 Failure Reason: %%2304  
 Status: -1073741730  
 Sub Status: 0

Process Information:  
 Caller Process ID: 0  
 Caller Process Name: -

Network Information:  
 Workstation Name: PS-B05  
 Source Network Address: -  
 Source Port: -



Detailed Authentication Information:  
 Logon Process: NtLmSsp  
 Authentication Package: NTLM  
 Transited Services: -  
 Package Name (NTLM only): -  
 Key Length: 0

This event is generated when a logon request fails. It is generated on the computer where access was  
 The Subject fields indicate the account on the local system which requested the logon. This is most c  
 The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (int  
 The Process Information fields indicate which account and process on the system requested the logon.  
 The Network Information fields indicate where a remote logon request originated. Workstation name is  
 The authentication information fields provide detailed information about this specific logon request.  
 - Transited services indicate which intermediate services have participated in this logon request  
 - Package name indicates which sub-protocol was used among the NTLM protocols.  
 - Key length indicates the length of the generated session key. This will be 0 if no session key is



Where the error code -1073741730 means:

```
# for decimal -1073741730 / hex 0xc000005e
STATUS_NO_LOGON_SERVERS                                ntstatus.h
# There are currently no logon servers available to service
```

- o <https://aka.ms/errors>  link: <https://windowsinternalservices.azurewebsites.net/Static/Errors/?-1073741730> 

## Root Cause Analysis

### Root Cause Analysis 1

The Virtual Machine is unable to communicate with the domain. Inability to communicate with a Domain Controller could prevent RDP access to the VM with Domain Credentials. However, you would still be able to login using the Local Administrator credentials.

### Root Cause Analysis 2

The Active Directory Secure Channel between this Virtual Machine and the domain is broken.

### Tracking close code for this volume

Root Cause	Product	Support Topic	Cause Tracking code	Bug
1	Azure Virtual Networks	Routing Azure Virtual Network V3\Connectivity\Cannot connect to virtual machine using RDP or SSH	This will depend on the investigation from the Azure Network engineer	

Root Cause	Product	Support Topic	Cause Tracking code	Bug
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\Guest OS - Windows\VM Responding\Active Directory issues\Broken trusted channel - Rejoin	

To know how to flag a bug on a case please refer to [How to do Proper Case Coding](#)

## Customer Enablement

N/A

## Refresher / Training Template

- For the purpose of training or following along with this TSG, you can use the following link to deploy a VM with this scenario built-in. You will need to enable JIT for the VM. This lab is not to be shared with customers.



- Note: Login to the APP1 server using your domain account to experience the issue. Your account should follow this syntax depending on the variables you enter for the template deployment: Domain Name\Domain Account Username . E.G. if you leave the Domain Name as corp.contoso.com and the Domain Account Username is AzureAdmin , you should attempt to login via mstsc.exe with the username corp.contoso.com\AzureAdmin .

## 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

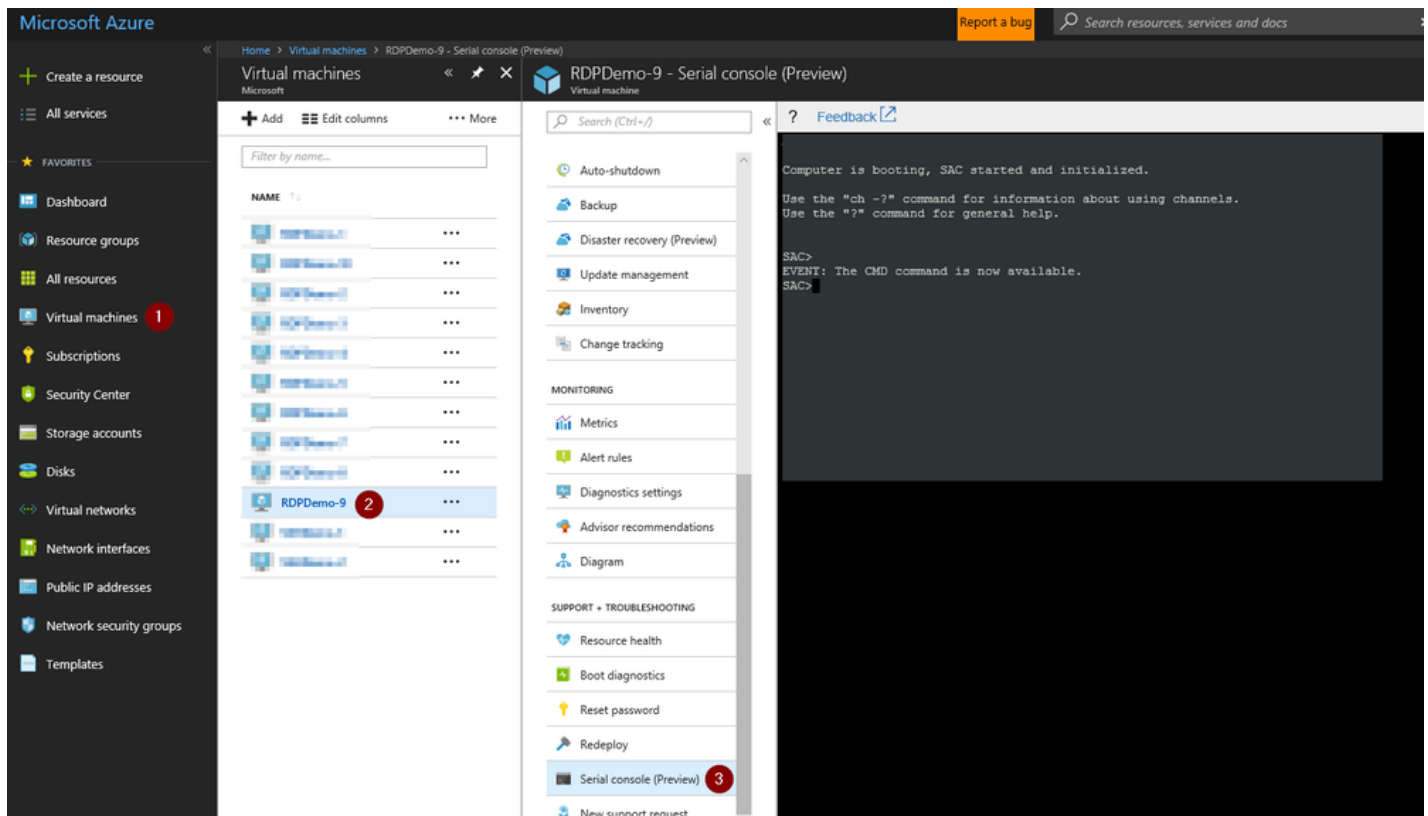
See [How To Access Thru Windows Admin Center](#)

#### 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
```

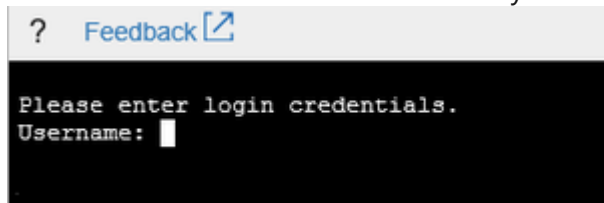
```
SAC>ch -si 1
```

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

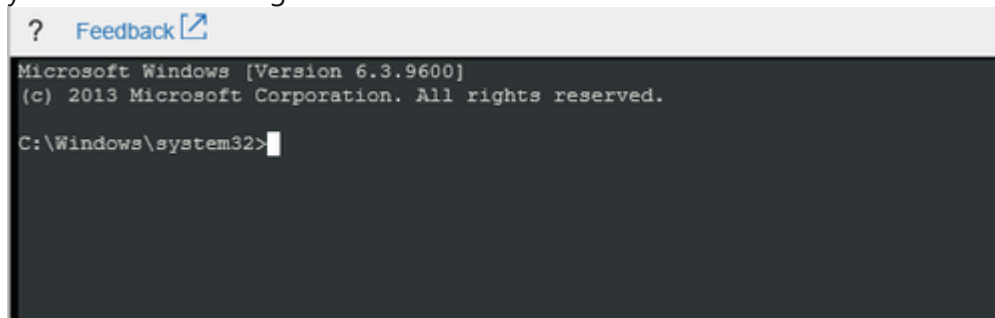
```
? Feedback
Name: Cmd0001
Description: Command
Type: VT-UTF8
Channel GUID: [REDACTED]
Application Type GUID: [REDACTED]

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:

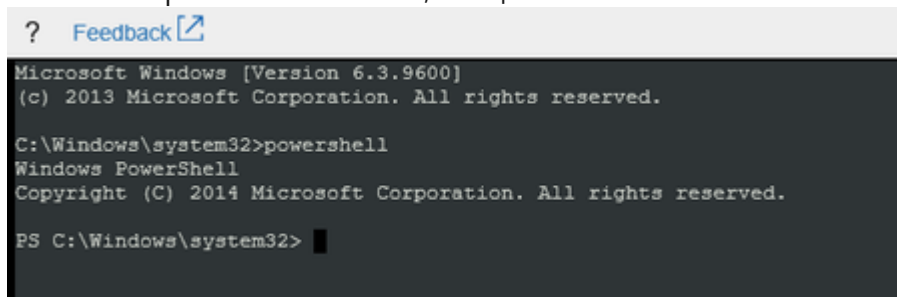


1. If the machine has connectivity, you could use either local or domain IDs. If you want to use a local ID, for domain just add the hostname of the VM
  2. If the machine doesn't have connectivity, you could try to use domains IDs however this will work if only the credentials are cached on the VM.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

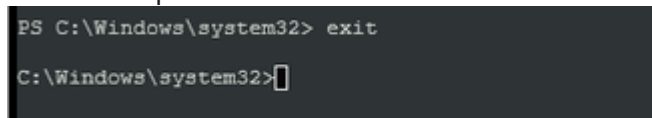


1. At this point, you can do your troubleshooting in bash (CMD) or else, you could start a powershell instance:

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

### Mitigation 1

▼ Click here to expand or collapse this section

**Note:** Applies only for domain joined machines, if you have a standalone server please continue with the next Mitigation plan.

1. Double check that the member machine has connectivity to a domain controller and also that the domain controller is healthy enough to pick up the request from the member machine. One way to tell is pick up another machine on the same VNET and Subnet who shares the same logon server.
  1. To compare who is the domain controller the machine is using, you could run the following on an CMD instance

```
set | find /i "LOGONSERVER"
```
2. If there's no communication between your server and the domain controller you are reporting to, engage *Azure Networking* with a problem with the following details:
  - Product: **Azure Virtual Networks**
  - Support Topic: **Routing Azure Virtual Networks V3\Connectivity\Network connectivity problems**

### Mitigation 2

▼ Click here to expand or collapse this section

**Note:** Applies only for domain joined machines, if you have a standalone server please continue with the next Mitigation plan.

1. Test how healthy is the secure channel of this machine against the Domain Controller. The following command will give you a Boolean flag if the secure channel is alive. Run the following on an elevated

powershell instance:

```
Test-ComputerSecureChannel -verbose
```

1. If the channel is **broken**, then try to fix it with the following:

```
Test-ComputerSecureChannel -repair
```

2. Ensure that the computer account password on active directly is in sync between your machine and the domain:

```
Reset-ComputerMachinePassword -Server "<COMPUTERNAME>" -Credential <DOMAIN CREDENTIAL WITH DOMAIN ADM
```



3. If the communication with the domain controller is OK but the Domain Controller is not healthy enough to even open an RDP session, then you could try to restart the domain controller.
4. If the above commands don't *fix* your communication to the domain, you could then rejoin this VM to the domain using CSE or RunCommands, please refer to [Rejoin a VM to an Active Directory Domain using CSE](#)
5. If any of the above is fixing your case or if with get an error when trying to join to the domain, then you could engage *Directory Services*
  - o Product: **Windows Server 2008 R2** or **Windows Svr 2012 R2 Datacenter** or **Windows Svr 2016 Datacenter** as appropriate
  - o Support Topic: **Routing Windows V3\Active Directory**
  - o Override the queue to **Windows Directory Services T2**
6. If the AD channel is *healthy*, the computer password is in sync and the domain controller is working as expected then just proceed with the following mitigation procedure.

## OFFLINE Troubleshooting

This troubleshooting cannot be done in OFFLINE 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

## 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 - RDPFE 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 <a href="#">RDP-SSH SMEs</a> ☑ for faster assistance.</p> <p>Make sure to use the <a href="#">Ava process</a> for faster assistance.</p>	<p>Use the <a href="#">RDP-SSH Feedback</a> form to submit detailed feedback on improvements or new content ideas for RDP-SSH.</p> <p><b>Please note</b> 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 <a href="#">RDP-SSH Kudos</a> form to submit kudos on the page. Kudos will help us improve our wiki content overall!</p> <p><b>Please note</b> the link to the page is required when submitting kudos!</p>