

NIC Disabled_RDP SSH

Last updated by | Heath Rensink | Nov 29, 2022 at 9:08 AM PST

Tags

cw.TSG

cw.RDP-SSH

Contents

- Symptoms
- Root Cause Analysis
 - References
 - Refresher / Training Template
 - Tracking close code for this volume
- Customer Enablement
- 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
 - ONLINE Mitigations
 - Mitigation 1
 - Mitigation 2
 - Mitigation 3
 - Mitigation 4
 - 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
 - OFFLINE Mitigations
 - Mitigation 1
 - Mitigation 2
 - Mitigation 3
 - Mitigation 4
- Escalate
- After work - Cleanup

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

Symptoms

- You cannot RDP to a Virtual Machine after performing any of the actions below from within Windows OS:

1. Disabled the Network Card Interface (NIC), if so you will find the following event on the Guest OS logs describing the *NIC is in hailing state*:

```

Log Name:      System
Source:        Microsoft-Windows-Hyper-V-Netvsc
Date:          7/18/2016 1:02:34 AM
Event ID:      6
Task Category: (1003)
Level:         Information
Keywords:
User:          SYSTEM
Computer:      MACPreserv01
Description:
Miniport NIC 'Microsoft Hyper-V Network Adapter #2' is halting

```

2. Once the NIC is disable, the Guest OS will not see this interface anymore:

1. On the Guest OS WaAppAgent.log, you'll see there's no active network card:

```

[00000006] [02/12/2016 01:51:33.09] [ERROR] Failed to obtain fabric URI. ControlSystem not initi
[00000006] [02/12/2016 01:51:38.28] [INFO]   Initializing ControlSystem.
[00000006] [02/12/2016 01:51:38.28] [ERROR] Did not discover fabric address on any interface. Dur
[00000038] [02/12/2016 01:51:38.34] [INFO]   ipconfig.exe /all: .
[00000038] [02/12/2016 01:51:38.34] [INFO]   ipconfig.exe /all: Windows IP Configuration.
[00000038] [02/12/2016 01:51:38.34] [INFO]   ipconfig.exe /all: .
[00000038] [02/12/2016 01:51:38.34] [INFO]   ipconfig.exe /all:   Host Name . . . . .
[00000038] [02/12/2016 01:51:38.34] [INFO]   ipconfig.exe /all:   Primary Dns Suffix . . . . .
[00000038] [02/12/2016 01:51:38.34] [INFO]   ipconfig.exe /all:   Node Type . . . . .
[00000038] [02/12/2016 01:51:38.34] [INFO]   ipconfig.exe /all:   IP Routing Enabled. . . . .
[00000038] [02/12/2016 01:51:38.34] [INFO]   ipconfig.exe /all:   WINS Proxy Enabled. . . . .
[00000038] [02/12/2016 01:51:38.34] [INFO]   ipconfig.exe /all:   DNS Suffix Search List. . . .
[00000038] [02/12/2016 01:51:38.34] [INFO]   ipconfig.exe /all: .
[00000038] [02/12/2016 01:51:38.35] [INFO]   ipconfig.exe /all: .
[00000036] [02/12/2016 01:51:38.42] [INFO]   route.exe print: =====
[00000036] [02/12/2016 01:51:38.42] [INFO]   route.exe print: Interface List.
[00000036] [02/12/2016 01:51:38.42] [INFO]   route.exe print: 1.....Softw
[00000036] [02/12/2016 01:51:38.42] [INFO]   route.exe print: =====
[00000036] [02/12/2016 01:51:38.42] [INFO]   route.exe print: .

```

2. In **WinGuestAnalyzer\Health Signal** tab on the *NetworkAdapters* section, you will not see any active network card:



Root Cause Analysis

If the NIC is disabled on the Guest OS, the VM will not have any connectivity and that is by design. On the other hand all the NIC configuration, Static IP/DNS/WINS, should be managed from the Azure Portal and this is also by design. The NIC configuration on the Guest OS should remain empty and in DHCP mode.

References

- [Network interfaces](#) ☐
- [New-AzureNetworkInterface](#) ☐
- [Add-AzureRmVMNetworkInterface](#) ☐
- [Multiple VM NICs and Network Virtual Appliances in Azure](#) ☐
- [Create or update a network interface card](#) ☐
- [Create Azure VM with Multiple Network Interfaces](#) ☐

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.



Tracking close code for this volume

Root Cause	Product	Support Topic	Cause Tracking code	Bug
1	Azure Virtual Machine – Windows	For existing VMs: <i>Routing Azure Virtual Machine V3\Cannot Connect to my VM\Failure to connect using RDP or SSH port</i>	<i>Root Cause - Windows Azure\Virtual Machine\Guest OS - Windows\Isolated\No Nic\NIC Disabled</i>	
	Azure Virtual Machine – Windows	For new migrated VMs: <i>Routing Azure Virtual Machine V3\Cannot create a VM\I need guidance preparing an image</i>	<i>Root Cause - Windows Azure\Virtual Machine\Guest OS - Windows\Isolated\Firewall misconfigured\Lack of preparation prior migration - Firewall not setup</i>	

Customer Enablement

- [Cannot remote desktop to a VM because the network interface is disabled](#) 




Mitigation

Backup OS disk

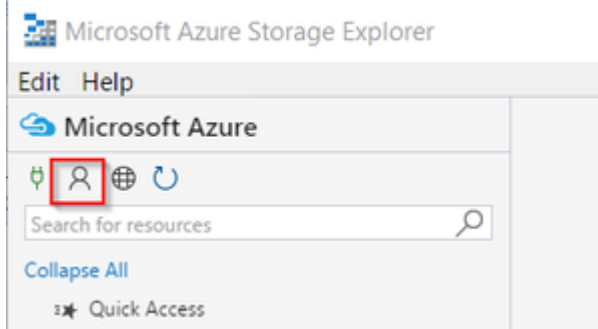
▼ Click here to expand or collapse this section

1. Before doing anything, please validate if this is an encrypted VM. On ASC check on the Resource Explorer on the VMCard for the value *OS Disk Encrypted*

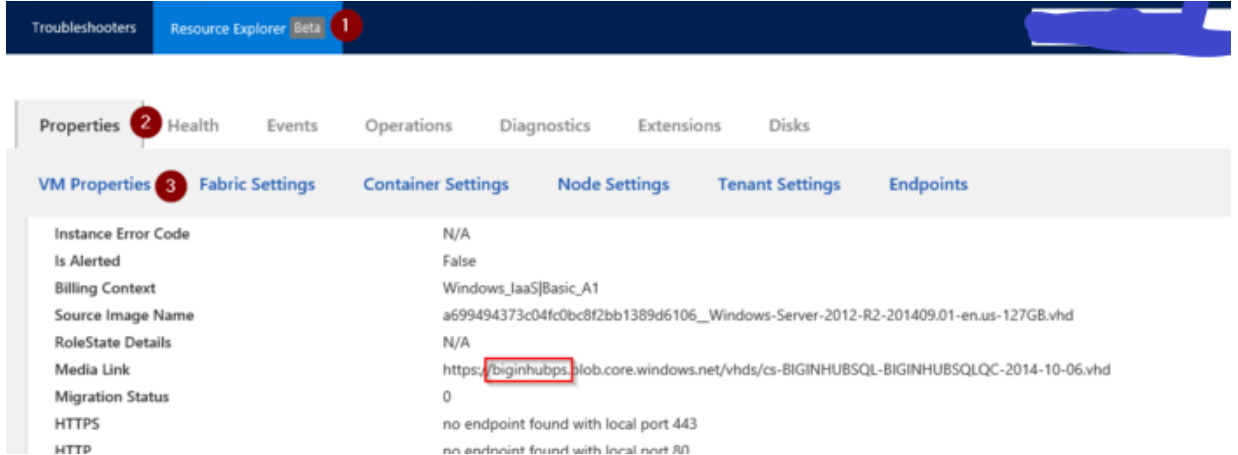
OS Disk Lease Id	Udb9a55c-0317-40fa-a032-b1f3550f3775
OS Disk Lease Acquired	True
OS Disk Billing Validated	True
OS Disk Encrypted	False
Billing Code	Windows_IaaS
Billing is Created from Marketplace Image	N/A
Billing Tag GUID	00000000-0000-0000-0000-000000000000

2. If the OS Disk is encrypted, then proceed to [Unlock an encrypted disk](#)
3. Now proceed to do a copy of the OS disk, this will help in case of a rollback for recovery or RCA in a later stage
4. Power the machine down and once it is stopped de-allocated to do the copy.
5. Create a snapshot
 1. If the **disk is unmanaged**, this could be done by using [Microsoft Azure Storage Explorer](#)  or [Azure Powershell](#) 
 1. Using [Microsoft Azure Storage Explorer](#) 
 1. Once the customer download the tool, proceed to add the Azure account details so you can access the storage accounts

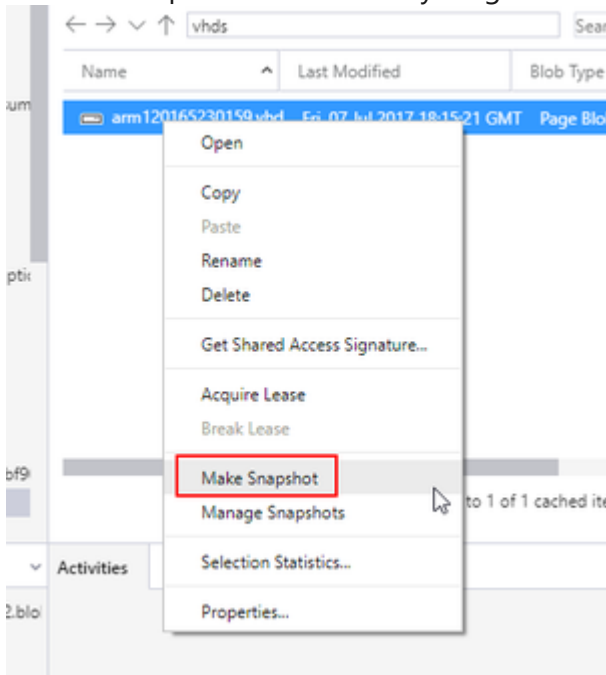
2. Click on **Add Account Settings** then ***Add an account...***



3. Go to the storage account where the OS disk is, you can see this on ASC under *Resource Explorer* on *Properties* in the *VM Properties* card



4. Create a snapshot of this disk by a right click over the disk and select *Make Snapshot*



2. Using [Azure Powershell](#)

1. You can follow [How to Clone a disk using Powershell](#)

2. If the **disk is managed**, use Azure portal to take a snapshot
1. Sign in to the Azure portal.
 2. Starting in the upper-left, click New and search for snapshot.
 3. In the Snapshot blade, click Create.

4. Enter a Name for the snapshot.
5. Select an existing Resource group or type the name for a new one.
6. Select an Azure datacenter Location.
7. For Source disk, select the Managed Disk to snapshot.
8. Select the Account type to use to store the snapshot. We recommend Standard_LRS unless you need it stored on a high performing disk.
9. Click Create.

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

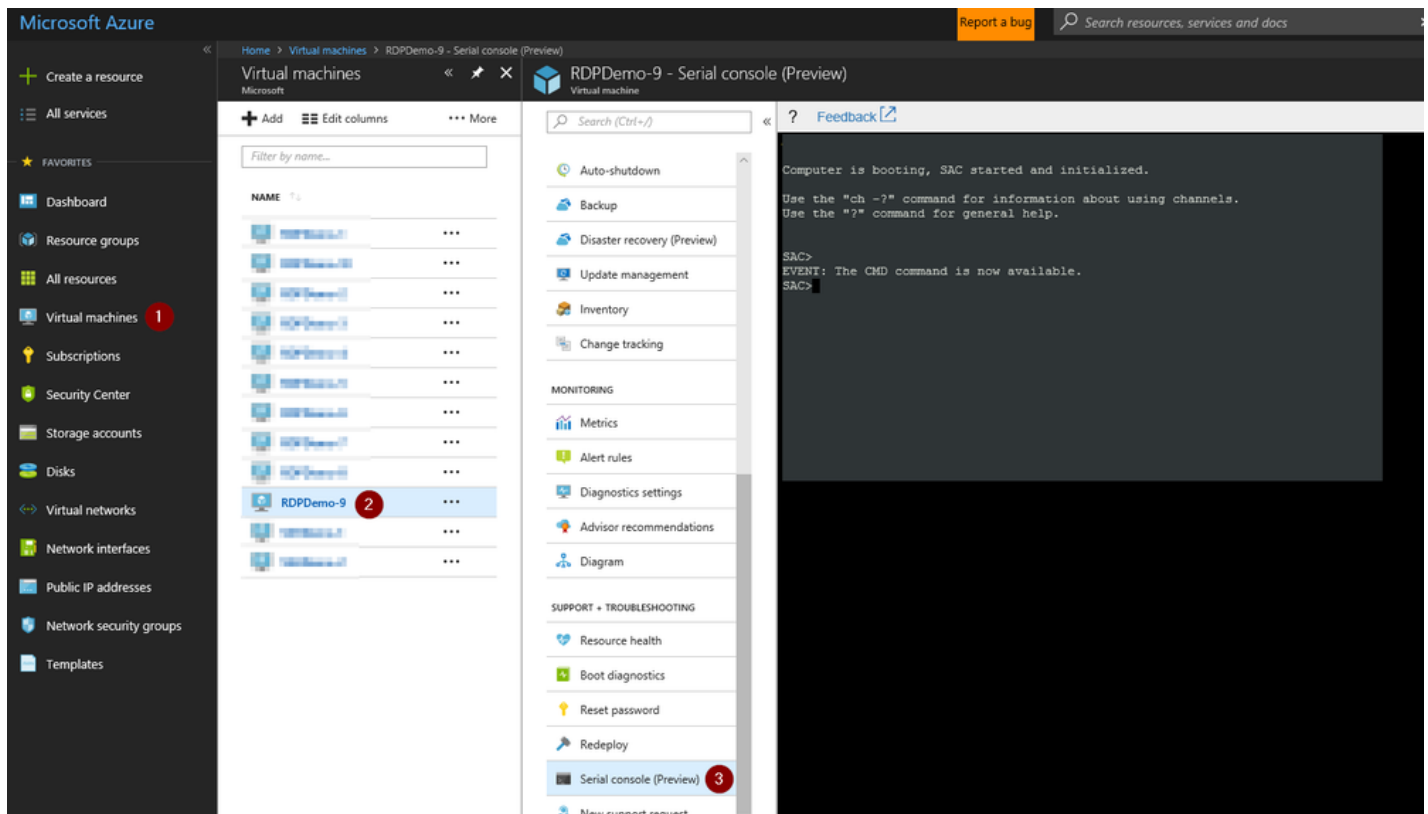
See [How To Access Thru Windows Admin Center](#)

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
```

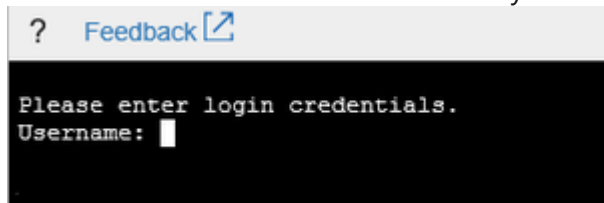
```
SAC>ch -si 1
```

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

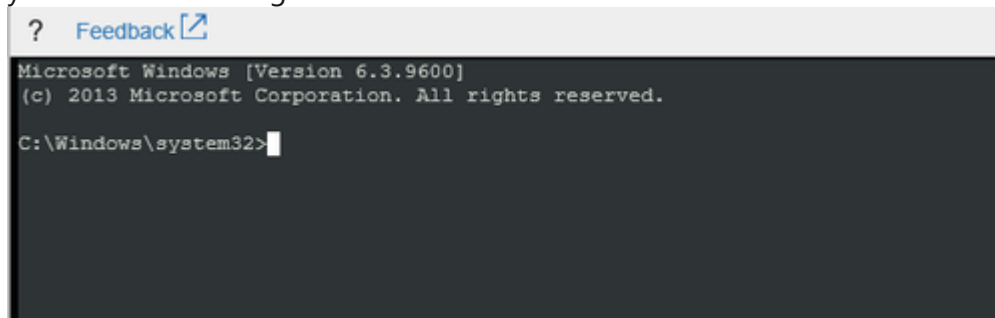
```
? Feedback
Name: Cmd0001
Description: Command
Type: VT-UTF8
Channel GUID: [REDACTED]
Application Type GUID: [REDACTED]

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:

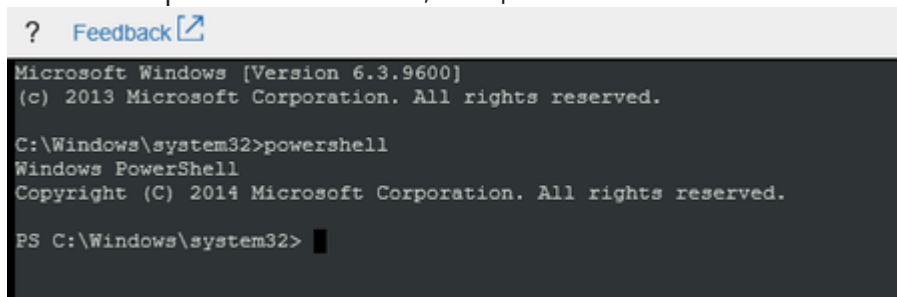


1. If the machine has connectivity, you could use either local or domain IDs. If you want to use a local ID, for domain just add the hostname of the VM
 2. If the machine doesn't have connectivity, you could try to use domains IDs however this will work if only the credentials are cached on the VM. In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

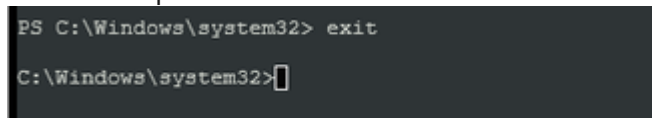


1. At this point, you can do your troubleshooting in bash (CMD) or else, you could start a powershell instance:

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

ONLINE Mitigations

Mitigation 1

▼ Click here to expand or collapse this section

1. Open a CMD instance and query the network cards available on the OS

```
netsh interface show interface
```

2. You will see that the network card showing the admin state of *Disabled*

```
C:\Windows\system32>netsh interface show interface
```

Admin State	State	Type	Interface Name
Disabled	Disconnected	Dedicated	Ethernet 2

3. Enable this network card using its name as a parameter. You can do this as the following:

```
netsh interface set interface name=<NIC Name> admin=enabled
```

1. In this case the network card is called *Ethernet 2*

```
C:\Windows\system32>netsh interface set interface name="Ethernet 2" admin=enabled
```

```
C:\Windows\system32>netsh interface show interface
```

Admin State	State	Type	Interface Name
Enabled	Connected	Dedicated	Ethernet 2

4. You don't need to restart the VM, the VM will be back reachable on that network card

Mitigation 2

▼ Click here to expand or collapse this section

1. Follow the steps described on the article [Present a new NIC to a Guest OS](#)

Mitigation 3

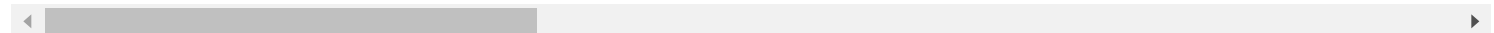
This mitigation can only be done in OFFLINE mode

Mitigation 4

This mitigation can only be done in OFFLINE mode

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

This mitigation can only be done in ONLINE mode

Mitigation 2

▼ Click here to expand or collapse this section

1. Follow the steps described on the article [Present a new NIC to a Guest OS](#)

Mitigation 3

▼ Click here to expand or collapse this section

1. Just proceed to recreate the VM, this operation will introduce a new MAC address which will trigger the PlugNPlay service on the OS to create a new virtual network card inside the Guest OS

Mitigation 4

▼ Click here to expand or collapse this section

This applies only for ARM machines.

1. Create a new NIC object in the portal
2. Edit the JSON file from VM configuration taken earlier and change the NIC card name

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 - RDP 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>