

# TCP Port Exhaustion\_RDP SSH

Last updated by | Kevin Gregoire | Mar 2, 2023 at 6:38 AM PST

## Tags

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

## Contents

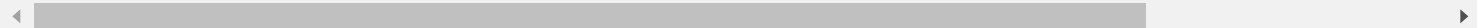
- [Symptoms](#)
  - [Symptom 1](#)
  - [Symptom 2](#)
- [Root Cause Analysis](#)
  - [Root Cause Analysis 1](#)
  - [Root Cause Analysis 2](#)
- [MS Internal Article](#)
- [MS Public Articles](#)
- [Refresher / Training Template](#)
- [Training / Brownbag](#)
- [Mitigation 1](#)
- [Mitigation 2](#)
- [Escalate](#)
- [Need additional help or have feedback?](#)

## Symptoms

You may experience an Event ID 4227 and 4231 in SYSTEM Event log, when all of the TCP dynamic ports are exhausted:

Log Name:	System
Source:	Tcpip
Event ID:	4227
Task Category:	None
Level:	Warning
Keywords:	Classic
User:	N/A
Computer:	TestMachine
Description:	TCP/IP failed to establish an outgoing connection because the selected local endpoint was recent

Log Name: System  
Source: Tcpip  
Event ID: 4231  
Task Category: None  
Level: Warning  
Keywords: Classic  
User: N/A  
Computer: TestMachine  
Description: A request to allocate an ephemeral port number from the global TCP port space has failed due to



## Symptom 1

1. After migrating a 2008SP2 VM from a Hyper-V 2012r2 host to a Hyper-V 2019 host, sockets in the 2008SP2 VM get stuck in TIME\_WAIT status indefinitely.
2. The VM is a Windows Server 2008 SP2 (Not R2).
3. The VM was moved from On-Prem to Azure.
4. An application that continuously opens and closes sockets will reproduce this faster.
5. This issue may or may not impact RDP connectivity directly.

## Symptom 2

1. You are unable to RDP with a domain account due to a domain connectivity issue such as
  - o The trust relationship between this workstation and the primary domain failed. OR
  - o The remote computer that you are trying to connect to requires Network Level Authentication (NLA), but your Windows domain controller cannot be contacted to perform NLA. If you are an administrator on the remote computer, you can disable NLA by using the options on the Remote tab of the System Properties dialog box.
2. Connecting with a local admin account or a domain account with cached credentials may still succeed.
3. Other outgoing connections may start failing such as Group Policy processing, file shares, etc.
4. If you run `netstat -anob` via CMD or PowerShell and/or collect a PerfInsights you may notice an application using several ports. You may also experience increased CPU utilization as a result of this application overworking.

## Root Cause Analysis

Possibilities include:









### Root Cause Analysis 1

- TCPIP gets into a state where it stops processing timer DPCs. These timer DPCs handle changing the state of these ports which results in them being stuck in TIME\_WAIT and eventually exhausting all ephemeral ports.
- It is random for TCPIP to get in this state and there is no known indication of being in state other than increasing number of ports in TIME\_WAIT.






### Root Cause Analysis 2

- An application is flooding outgoing ephemeral connections, preventing more from being made.

## MS Internal Article

- [KB4597363](#) 
- [Server stops processing Group policies after a few days](#) 
- [Error: IPC\\$ is returned with 53 | Unable to join a server to the domain](#) 
- [TCP connection leaks on connection between svchost.exe \(IPSECSVC\) <-> wmiprvse.exe after SCEP installed](#) 
- <https://internal.evergreen.microsoft.com/en-us/topic/b014b436-d31c-bcab-5458-112bcd1318e> 
- [NET: Problem connecting to server as of Ephemeral Port Exhaustion issues](#) 
- [Ephemeral port exhaustion due to FITTradingServer.exe process](#) 
- [ADPERF: Tools: Win8 events that identify port exhaustion](#) 
- [Windows Networking - Port Exhaustion](#)
- [Azure Networking - How to detect port exhaustion in Windows](#)

## MS Public Articles

- [Troubleshoot port exhaustion issues](#) 
- [Port Exhaustion and You!](#) 
- [Detecting ephemeral port exhaustion](#) 
- [Dynamic Ports in Windows Server 2008 and Windows Vista \(or: How I learned to stop worrying and love the IANA\)](#) 
- [Netstat](#) 

## Refresher / Training Template

- For the purpose of training or following along with this TSG, you can use the following link or url 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: After deployment, wait ~20 minutes for the ports to be exhausted, then attempt to login to the APP1 server using the domain account `User1` to experience the issue (you will receive an NLA error). `User1` will share the same password entered for your admin user. Your account should follow this syntax depending on the variables you enter for the template deployment: `Domain Name\User1`. E.G. if you leave the Domain Name as `corp.contoso.com`, you should attempt to login via `mstsc.exe` with the username `corp.contoso.com\User1`.

## Training / Brownbag

[TCP Port Exhaustion in Windows VMs](#) 

## Mitigation 1

1. Windows Server 2008 SP2 is out of support, customers need to upgrade to a supported version of Windows.

1. To work around the issue until OS can be upgraded

## 2. Schedule periodic reboots of servers prior to port exhaustion such as when you see a few thousand ports in use

1. If that cannot be done, increase number of ephemeral ports:

```
netsh int ipv4 set dynamicport tcp start=1025 num=64500
```

2. Periodically execute *netstat -ano* and monitor for increasing numbers of ports in TIME\_WAIT, when you see a few thousand trigger a notification or a reboot
3. Here is how to count the instances

```
netstat -ano | findstr TIME_WAIT | find /c "TIME_WAIT".
```

## Mitigation 2

1. If increasing the number of ephemeral ports (Mitigation 1) did not help, determine the application causing the ports to be exhausted:

- using CMD (admin):

```
netstat -anob
```

- using PowerShell (admin):

```
Get-NetTCPConnection
```

2. There may be one process using several ephemeral ports. You can either safely stop this program from an mstsc.exe session or forcefully by grabbing the PID and running one of the following:

- using Serial Console (without logging in):

```
t                                     # Running t
Enter                                # Press enter
k <processIdentifier>                # Replace <p
```

- using CMD (admin):

```
tasklist | more                      REM run this
Enter                                REM press En
taskkill /PID <processIdentifier>    REM Replace
```

- using PowerShell (admin):

Get-Process | Sort-Object -Property HandleCount -Descending | Format-Table \* | more # Get all pro  
 Stop-Process -Id <processIdentifier> -Force # Replace <pr

## 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 engage 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**

## 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>