Identifying Application Attack Indicators

Scenario

You are concerned about discovering application layer attacks against your Windows servers. You have decided to simulate some attacks that might consume processor or memory resources, making the server sluggish or unresponsive. First, you will use CPU Stress to simulate a heavy processor load on the server. Second, you will use testlimit to simulate a similar heavy memory load. In both cases, you will monitor the output by using CPU Explorer, Task Manager, and Performance Monitor.

Objectives

This activity is designed to test your understanding of and ability to apply content examples in the following CompTIA Security+ objectives:

- 1.2 Given a scenario, analyze potential indicators associated with application attacks.

Lab

- DC1 VM

Task 1

Display Process Explorer and Performance Monitor

To prepare for application attack detection, you will use Process Explorer and Performance Monitor to display current resource utilization information. You will create a custom Data Collector Set in Performance Monitor to observe a simulated deviation from the baseline.

1. On the **DC1** VM, send **CTRL+ALT+DEL**, and then sign on as **CONTOSO\Administrator** using **Pa$$w0rd** as the password.

2. In **Server Manager**, select **Tools > Performance Monitor**.

3. Expand the **Data Collector Sets > User Defined** node. Right-click the **User Defined** node and then select **New > Data Collector Set**.

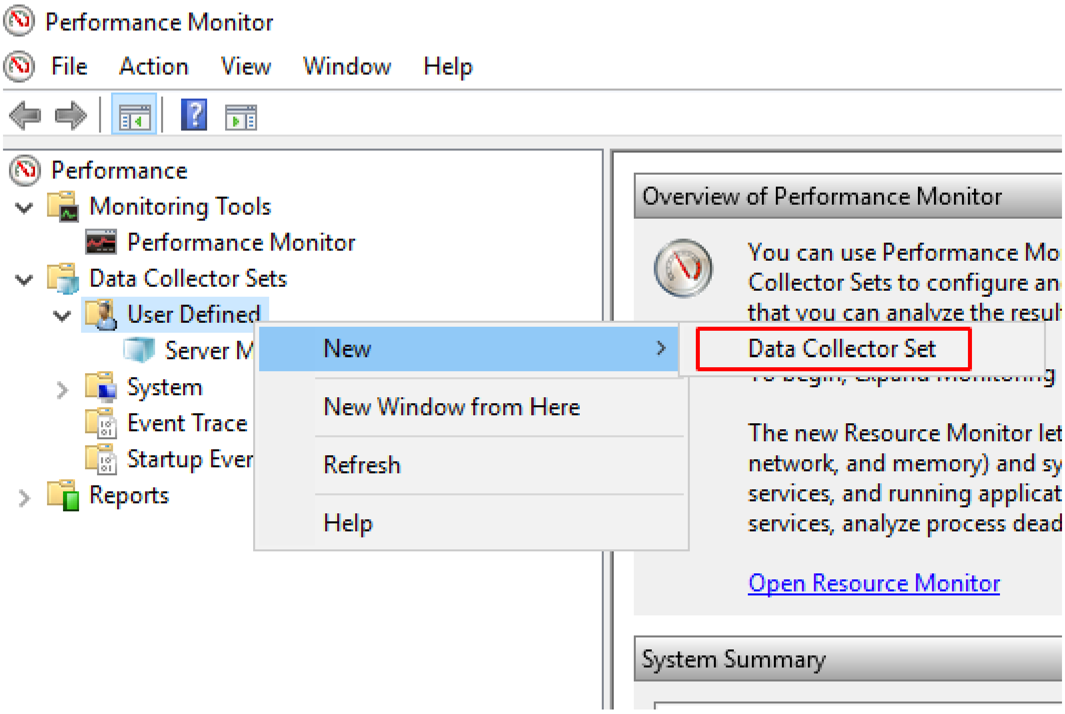
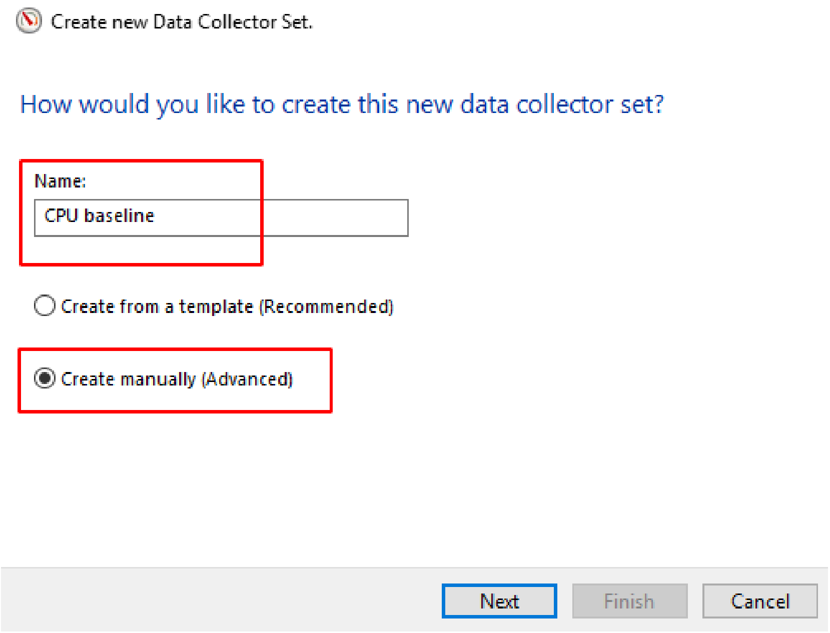

Performance Monitor
File Action View Window Help
Performance
Monitoring Tools
Performance Monitor
Data Collector Sets
User Defined
Server M
System
Event Trace
Startup Ever
Reports
New
New Window from Here
Refresh
Help
Data Collector Set
Overview of Performance Monitor
You can use Performance Mo
Collector Sets to configure an
that you can analyze the resul
The new Resource Monitor let
network, and memory) and sy
services, and running applicat
services, analyze process dead
Open Resource Monitor
System Summary

Figure 1.1 – Data Collector Sets > User Defined > New > Data Collector Set.

4. Use **CPU baseline** as the Name, select the radio button for **Create manually (advanced)**, and then select **Next**.



Create new Data Collector Set.

How would you like to create this new data collector set?

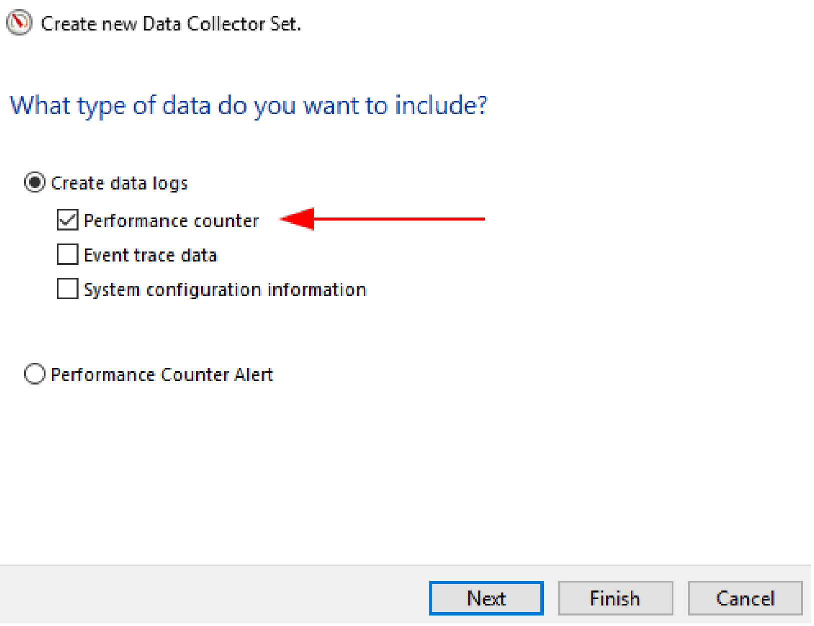
Name:
CPU baseline

○ Create from a template (Recommended)

● Create manually (Advanced)

Figure 1.2 – Create a new Data Collector Set.

5. With **Create data logs** selected, check the box for **Performance Counter**, and then select **Next**.



Create new Data Collector Set.

What type of data do you want to include?

● Create data logs

☑ Performance counter

☐ Event trace data

☐ System configuration information

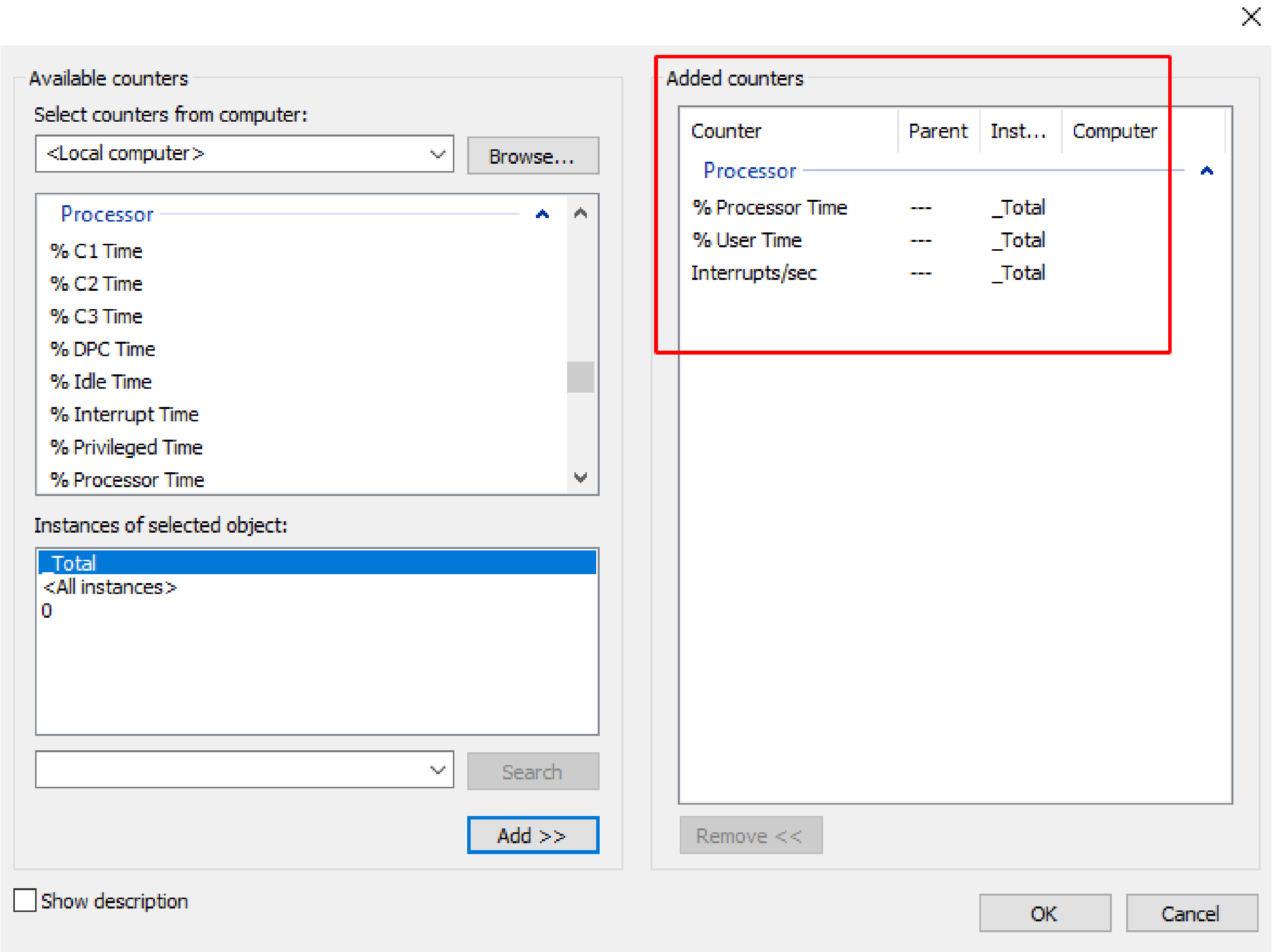
○ Performance Counter Alert

Figure 1.3 – Create data logs > Performance counter.

6. On Which performance counters would you like to log? page, select **Add**.

7. On the available counters page, expand the **Processor** node (it is already highlighted for you). Select the following three counters, and **Add** them to the **Added Counters** column:

- % Processor Time (this counter is a good general indicator of the processor’s overall activity level).
- % User Time (this counter provides data on time spent by the processor managing user applications)
- Interrupt/Sec (this counter measures interrupts that the processor must handle immediately)



<Local computer>

Processor
% C1 Time
% C2 Time
% C3 Time
% DPC Time
% Idle Time
% Interrupt Time
% Privileged Time
% Processor Time

_Total
<All instances>
0

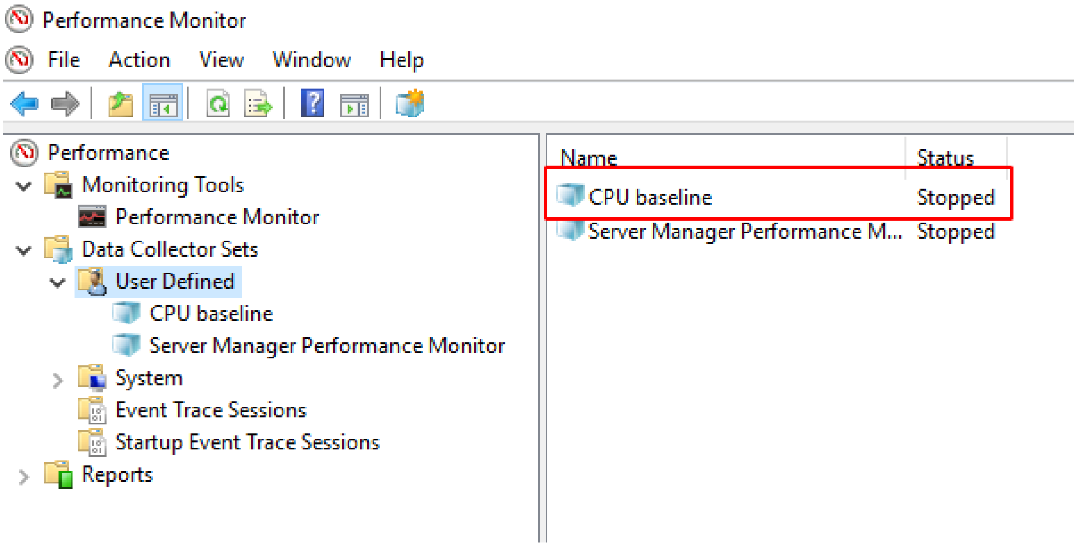
Counter	Parent	Inst...	Computer
Processor			
% Processor Time	---	_Total	
% User Time	---	_Total	
Interrupts/sec	---	_Total	

Figure 1.4 – Selecting Processor counters.

8. Select **OK** to complete the **Available counters** dialog box.

9. Select **Next**.

10. Select **Finish** to complete the Data Collector Set configuration.



Name	Status
CPU baseline	Stopped
Server Manager Performance M...	Stopped

Figure 1.5 – User defined Data Collector – CPU baseline.

You will start the Data Collector Set in a later step.

11. Minimize Performance Monitor. You will use it in later tasks.

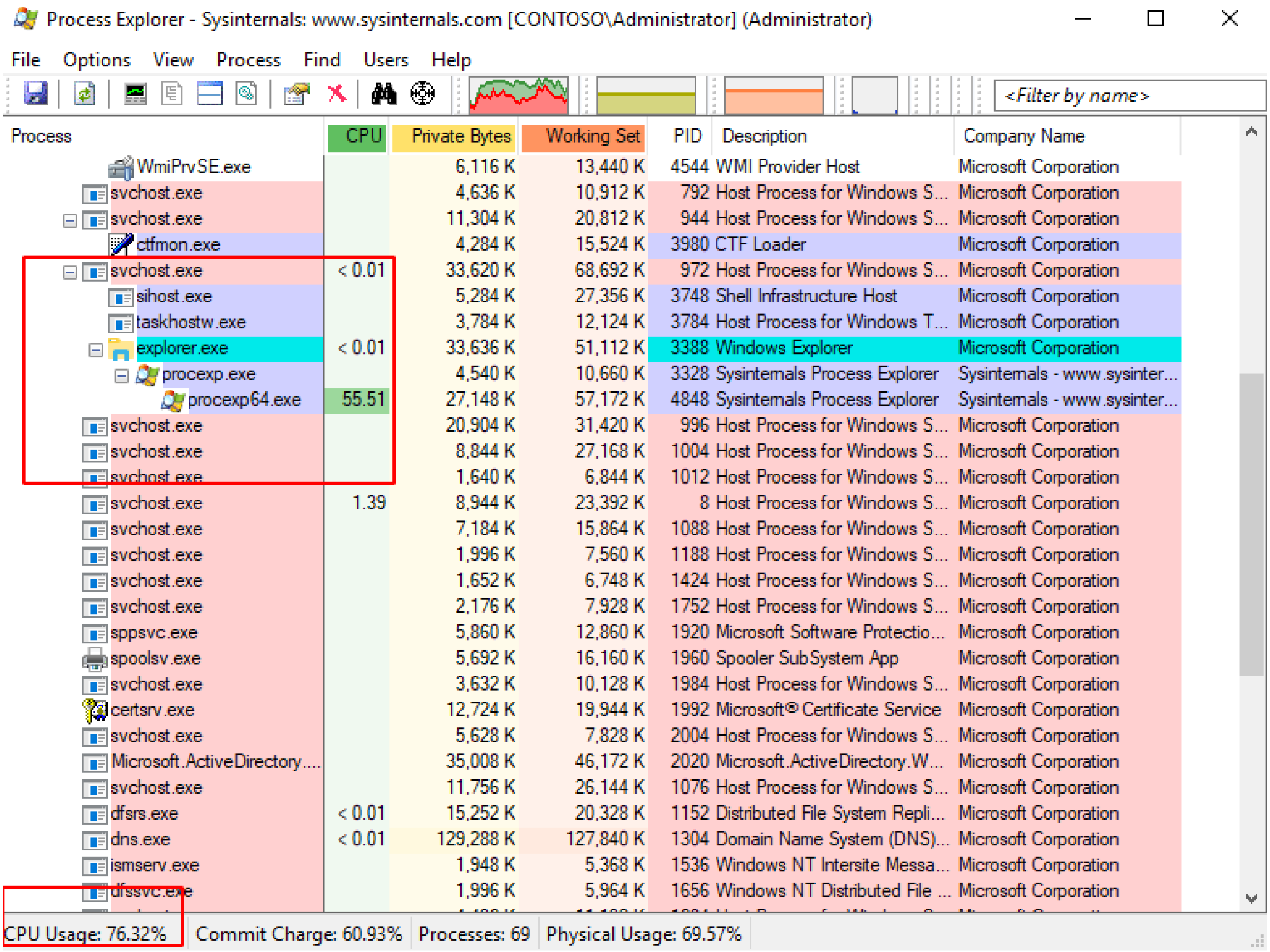
12. From the Desktop, open the **LABFILES** folder, and then launch **procexp**.

NOTE: If you have a **SmartScreen** window click **Run**.

Agree to the license from Sysinternals if prompted.

13. Observe some of the key information reported by Process Explorer, including:

- CPU Usage in the lower left corner – a percentage of processor utilization
- The tree format of the processes and their relationships to each other
- Reorganize data by selecting the column headers. The CPU column can be organized to display processes that are consuming the most resources, for example.


Process Explorer - Sysinternals: www.sysinternals.com [CONTOSO\Administrator] (Administrator)
File
Options
View
Process
Find
Users
Help
<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
WmiPrvSE.exe		6,116 K	13,440 K	4544	WMI Provider Host	Microsoft Corporation
svchost.exe		4,636 K	10,912 K	792	Host Process for Windows S...	Microsoft Corporation
svchost.exe		11,304 K	20,812 K	944	Host Process for Windows S...	Microsoft Corporation
ctfmon.exe		4,284 K	15,524 K	3980	CTF Loader	Microsoft Corporation
svchost.exe	< 0.01	33,620 K	68,692 K	972	Host Process for Windows S...	Microsoft Corporation
sihost.exe		5,284 K	27,356 K	3748	Shell Infrastructure Host	Microsoft Corporation
taskhostw.exe		3,784 K	12,124 K	3784	Host Process for Windows T...	Microsoft Corporation
explorer.exe	< 0.01	33,636 K	51,112 K	3388	Windows Explorer	Microsoft Corporation
procexp.exe		4,540 K	10,660 K	3328	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	55.51	27,148 K	57,172 K	4848	Sysinternals Process Explorer	Sysinternals - www.sysinter...
svchost.exe		20,904 K	31,420 K	996	Host Process for Windows S...	Microsoft Corporation
svchost.exe		8,844 K	27,168 K	1004	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,640 K	6,844 K	1012	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1.39	8,944 K	23,392 K	8	Host Process for Windows S...	Microsoft Corporation
svchost.exe		7,184 K	15,864 K	1088	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,996 K	7,560 K	1188	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,652 K	6,748 K	1424	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,176 K	7,928 K	1752	Host Process for Windows S...	Microsoft Corporation
sppsvc.exe		5,860 K	12,860 K	1920	Microsoft Software Protectio...	Microsoft Corporation
spoolsv.exe		5,692 K	16,160 K	1960	Spooler SubSystem App	Microsoft Corporation
svchost.exe		3,632 K	10,128 K	1984	Host Process for Windows S...	Microsoft Corporation
certsrv.exe		12,724 K	19,944 K	1992	Microsoft® Certificate Service	Microsoft Corporation
svchost.exe		5,628 K	7,828 K	2004	Host Process for Windows S...	Microsoft Corporation
Microsoft.ActiveDirectory....		35,008 K	46,172 K	2020	Microsoft.ActiveDirectory.W...	Microsoft Corporation
svchost.exe		11,756 K	26,144 K	1076	Host Process for Windows S...	Microsoft Corporation
dfsrs.exe	< 0.01	15,252 K	20,328 K	1152	Distributed File System Repli...	Microsoft Corporation
dns.exe	< 0.01	129,288 K	127,840 K	1304	Domain Name System (DNS)...	Microsoft Corporation
ismserv.exe		1,948 K	5,368 K	1536	Windows NT Intersite Messa...	Microsoft Corporation
dfssvc.exe		1,996 K	5,964 K	1656	Windows NT Distributed File ...	Microsoft Corporation

CPU Usage: 76.32% | Commit Charge: 60.93% | Processes: 69 | Physical Usage: 69.57%

Figure 1.6 – Process Explorer.

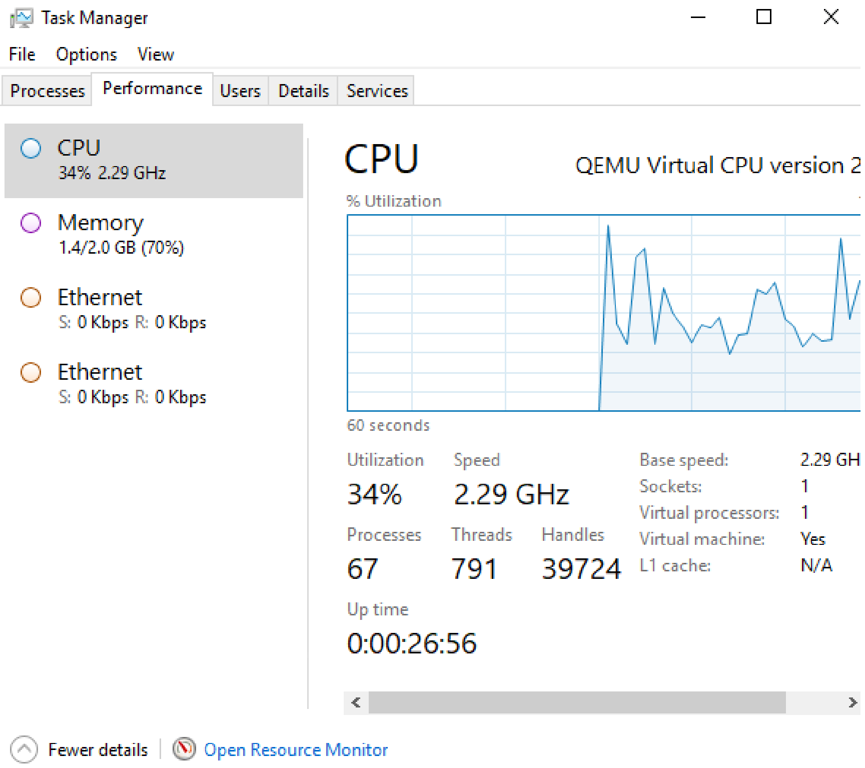
14. Leave Process Explorer open. You will use it in later tasks.

15. Right-click the **Taskbar**, and then select **Task Manager**.

16. Select the **Performance** tab.

17. Select each of the following three categories to observe the relevant performance information:

- CPU
- Memory
- Ethernet



CPU
34% 2.29 GHz

Memory
1.4/2.0 GB (70%)

Ethernet
S: 0 Kbps R: 0 Kbps

Ethernet
S: 0 Kbps R: 0 Kbps

CPU QEMU Virtual CPU version 2
% Utilization
60 seconds

Utilization 34%
Speed 2.29 GHz
Processes 67
Threads 791
Handles 39724
Up time 0:00:26:56

Base speed: 2.29 GH
Sockets: 1
Virtual processors: 1
Virtual machine: Yes
L1 cache: N/A

Figure 1.7 – Task Manager.

18. Leave **CPU** selected.

19. Leave Task Manager open. You will use it in the later tasks.

Task 2

Create stress on the CPU

You will use CPU Stress to place false load on the VM’s processors. You’ll use Performance Monitor, Task Manager, and Process Explorer to monitor the workload.

1. Select Performance Monitor, Under **Data Collector Sets** > **User Defined**, right-click the **CPU baseline** set, and then select **Start**.

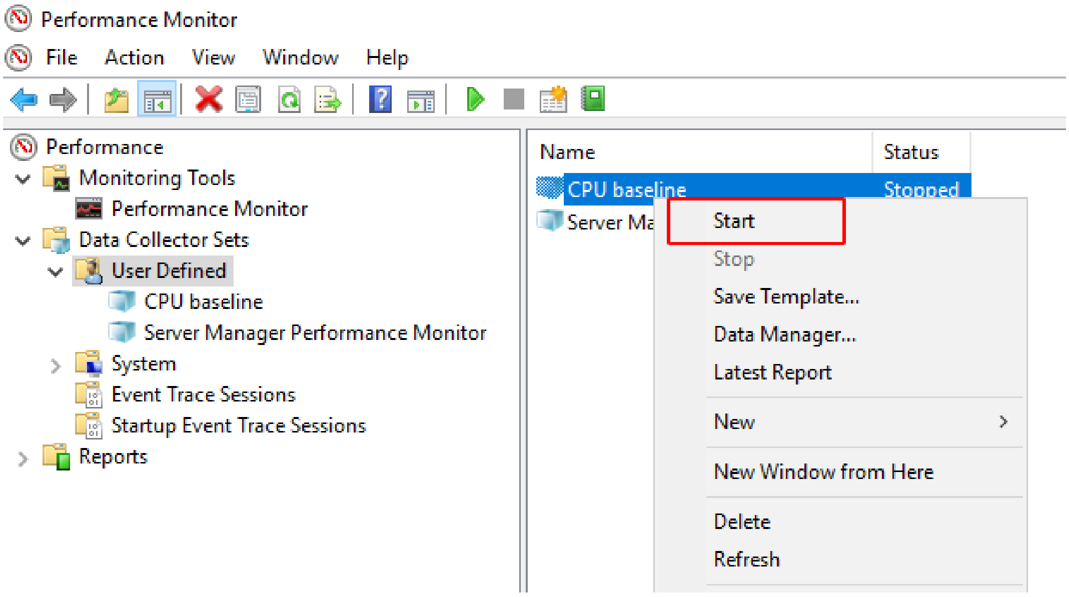


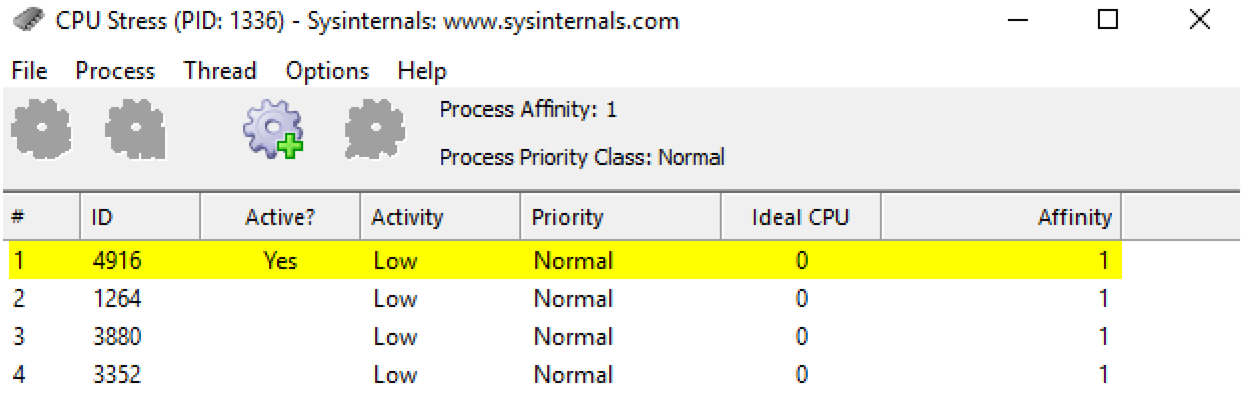
Figure 2.1 – Staring the CPU baseline.

You will leave the Data Collector Set running through the next several tasks. It gathers information as you accomplish activity steps.

2. From the **C:\LABFILES\** folder, open **CPUSTRESS64**.

NOTE: If you have a **SmartScreen** window click **Run**.

Agree to the license from Sysinternals if prompted.


CPU Stress (PID: 1336) - Sysinternals: www.sysinternals.com
File Process Thread Options Help

Process Affinity: 1

Process Priority Class: Normal

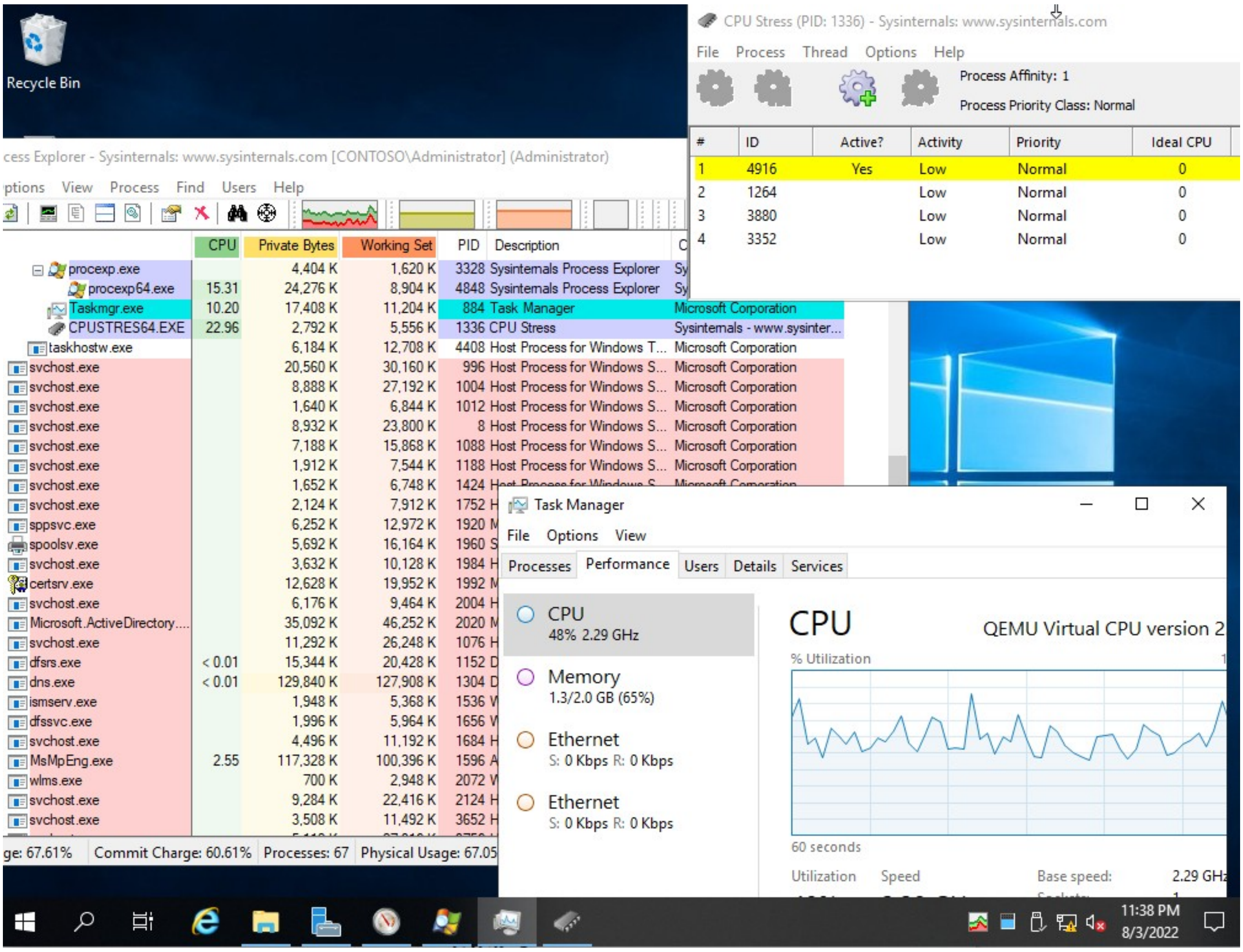
#	ID	Active?	Activity	Priority	Ideal CPU	Affinity
1	4916	Yes	Low	Normal	0	1
2	1264		Low	Normal	0	1
3	3880		Low	Normal	0	1
4	3352		Low	Normal	0	1

Figure 2.2 – CPU Stress.

You will see a dashboard with your four pre-created threads available. The menu allows you to start and stop threads, as well as to create new threads. Right-click threads to manage their priority level. You will create and execute threads in a later step.

NOTE: CPUStres is a performance management utility that applies a workload to the processor by creating one or more threads. Each thread can be given a priority level (low, medium, high, maximum). This tool is part of the Windows Sysinternals suite.

3. Resize and reposition the Task Manager, Process Explorer, and CPU Stress window so that you can observe them simultaneously.



CPU Stress (PID: 1336) - Sysinternals: www.sysinternals.com

Process Affinity: 1

Process Priority Class: Normal

#	ID	Active?	Activity	Priority	Ideal CPU
1	4916	Yes	Low	Normal	0
2	1264		Low	Normal	0
3	3880		Low	Normal	0
4	3352		Low	Normal	0

cess Explorer - Sysinternals: www.sysinternals.com [CONTOSO\Administrator] (Administrator)

	CPU	Private Bytes	Working Set	PID	Description	C
procexp.exe		4,404 K	1,620 K	3328	Sysinternals Process Explorer	Sy
procexp64.exe	15.31	24,276 K	8,904 K	4848	Sysinternals Process Explorer	Sy
Taskmgr.exe	10.20	17,408 K	11,204 K	884	Task Manager	Microsoft Corporation
CPUSTRES64.EXE	22.96	2,792 K	5,556 K	1336	CPU Stress	Sysinternals - www.sysinter...
taskhostw.exe		6,184 K	12,708 K	4408	Host Process for Windows T...	Microsoft Corporation
svchost.exe		20,560 K	30,160 K	996	Host Process for Windows S...	Microsoft Corporation
svchost.exe		8,888 K	27,192 K	1004	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,640 K	6,844 K	1012	Host Process for Windows S...	Microsoft Corporation
svchost.exe		8,932 K	23,800 K	8	Host Process for Windows S...	Microsoft Corporation
svchost.exe		7,188 K	15,868 K	1088	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,912 K	7,544 K	1188	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,652 K	6,748 K	1424	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,124 K	7,912 K	1752	H	
sppsvc.exe		6,252 K	12,972 K	1920	M	
spoolsv.exe		5,692 K	16,164 K	1960	S	
svchost.exe		3,632 K	10,128 K	1984	H	
certsrv.exe		12,628 K	19,952 K	1992	M	
svchost.exe		6,176 K	9,464 K	2004	H	
Microsoft.ActiveDirectory....		35,092 K	46,252 K	2020	M	
svchost.exe		11,292 K	26,248 K	1076	H	
dfsrs.exe	< 0.01	15,344 K	20,428 K	1152	D	
dns.exe	< 0.01	129,840 K	127,908 K	1304	D	
ismserv.exe		1,948 K	5,368 K	1536	W	
dfssvc.exe		1,996 K	5,964 K	1656	W	
svchost.exe		4,496 K	11,192 K	1684	H	
MsMpEng.exe	2.55	117,328 K	100,396 K	1596	A	
wlms.exe		700 K	2,948 K	2072	W	
svchost.exe		9,284 K	22,416 K	2124	H	
svchost.exe		3,508 K	11,492 K	3652	H	

ge: 67.61% Commit Charge: 60.61% Processes: 67 Physical Usage: 67.05

Task Manager

CPU
48% 2.29 GHz

Memory
1.3/2.0 GB (65%)

Ethernet
S: 0 Kbps R: 0 Kbps

Ethernet
S: 0 Kbps R: 0 Kbps

CPU QEMU Virtual CPU version 2

Utilization Speed Base speed: 2.29 GHz

Figure 2.3 – Repositioning the tools on Windows Server.

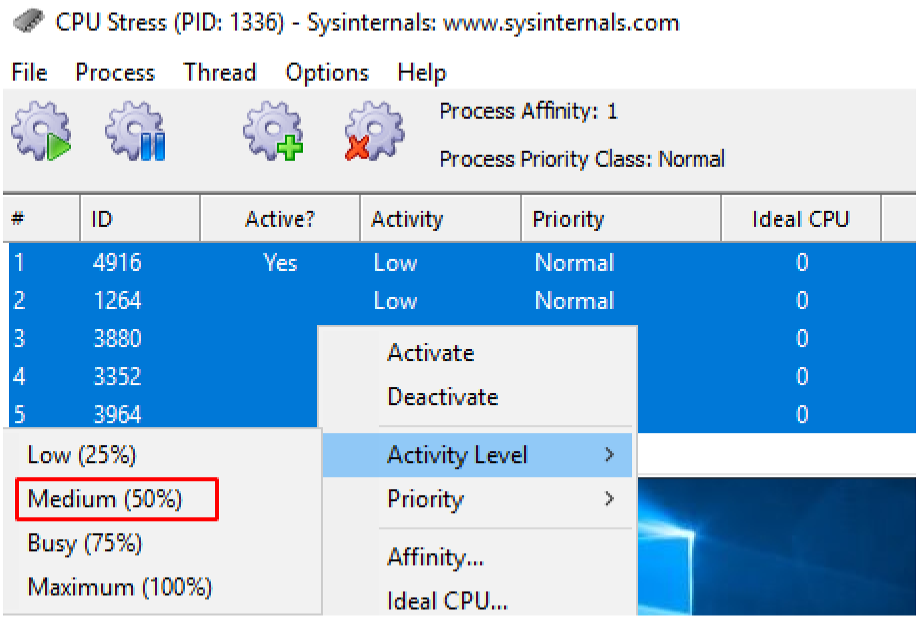
The goal is to view the effect of staring CPU Stress in Task Manager and Process Explorer.

4. In the CPU Stress console, select **Create Threads** button. A thread is generated in the window.

The new thread is currently inactive. You can select additional values, such as workload, affinity, and priority.

There should now be five threads created. Four were created by default, and you created the fifth.

5. Select all five threads, right-click them, and then select **Activity Level** > **Medium (50%).**



CPU Stress (PID: 1336) - Sysinternals: www.sysinternals.com

Process Affinity: 1

Process Priority Class: Normal

#	ID	Active?	Activity	Priority	Ideal CPU
1	4916	Yes	Low	Normal	0
2	1264		Low	Normal	0
3	3880				0
4	3352				0
5	3964				0

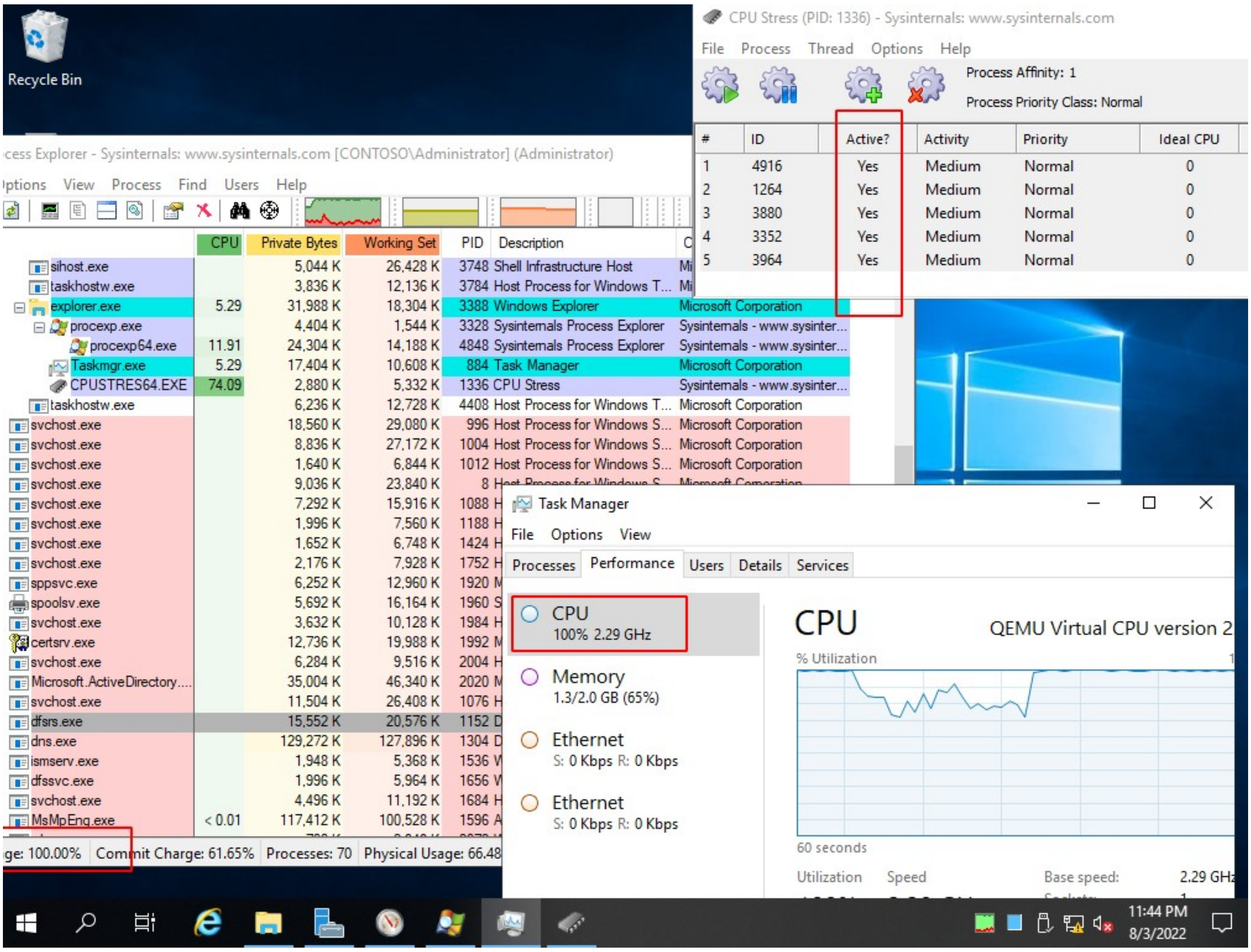
Figure 2.4 – Selecting threads and Activity Level from CPU Stress.

6. In CPU Stress, select the five threads, right-click the selection, and then select **Activate**.

WARNING: The system will become very slow!

7. Switch to Task Manager. CPU Utilization should be nearly 100%.

8. Switch to Process Explorer. In the lower left corner, CPU Usage should also be nearly 100%.


Recycle Bin
cess Explorer - Sysinternals: www.sysinternals.com [CONTOSO\Administrator] (Administrator)
ptions View Process Find Users Help
CPU Stress (PID: 1336) - Sysinternals: www.sysinternals.com
File Process Thread Options Help
Task Manager
File Options View
Processes Performance Users Details Services
11:44 PM
8/3/2022

	CPU	Private Bytes	Working Set	PID	Description	C
sihost.exe		5,044 K	26,428 K	3748	Shell Infrastructure Host	Mi
taskhostw.exe		3,836 K	12,136 K	3784	Host Process for Windows T...	Mi
explorer.exe	5.29	31,988 K	18,304 K	3388	Windows Explorer	Microsoft Corporation
procexp.exe		4,404 K	1,544 K	3328	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	11.91	24,304 K	14,188 K	4848	Sysinternals Process Explorer	Sysinternals - www.sysinter...
Taskmgr.exe	5.29	17,404 K	10,608 K	884	Task Manager	Microsoft Corporation
CPUSTRES64.EXE	74.09	2,880 K	5,332 K	1336	CPU Stress	Sysinternals - www.sysinter...
taskhostw.exe		6,236 K	12,728 K	4408	Host Process for Windows T...	Microsoft Corporation
svchost.exe		18,560 K	29,080 K	996	Host Process for Windows S...	Microsoft Corporation
svchost.exe		8,836 K	27,172 K	1004	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,640 K	6,844 K	1012	Host Process for Windows S...	Microsoft Corporation
svchost.exe		9,036 K	23,840 K	8	Host Process for Windows S...	Microsoft Corporation
svchost.exe		7,292 K	15,916 K	1088	H	
svchost.exe		1,996 K	7,560 K	1188	H	
svchost.exe		1,652 K	6,748 K	1424	H	
svchost.exe		2,176 K	7,928 K	1752	H	
sppsvc.exe		6,252 K	12,960 K	1920	M	
spoolsv.exe		5,692 K	16,164 K	1960	S	
svchost.exe		3,632 K	10,128 K	1984	H	
certsrv.exe		12,736 K	19,988 K	1992	M	
svchost.exe		6,284 K	9,516 K	2004	H	
Microsoft.ActiveDirectory....		35,004 K	46,340 K	2020	M	
svchost.exe		11,504 K	26,408 K	1076	H	
dfsrs.exe		15,552 K	20,576 K	1152	D	
dns.exe		129,272 K	127,896 K	1304	D	
ismserv.exe		1,948 K	5,368 K	1536	W	
dfssvc.exe		1,996 K	5,964 K	1656	W	
svchost.exe		4,496 K	11,192 K	1684	H	
MsMpEng.exe	< 0.01	117,412 K	100,528 K	1596	A	

ge: 100.00% | Commit Charge: 61.65% | Processes: 70 | Physical Usage: 66.48

Process Affinity: 1

Process Priority Class: Normal

#	ID	Active?	Activity	Priority	Ideal CPU
1	4916	Yes	Medium	Normal	0
2	1264	Yes	Medium	Normal	0
3	3880	Yes	Medium	Normal	0
4	3352	Yes	Medium	Normal	0
5	3964	Yes	Medium	Normal	0

CPU
100% 2.29 GHz

Memory
1.3/2.0 GB (65%)

Ethernet
S: 0 Kbps R: 0 Kbps

Ethernet
S: 0 Kbps R: 0 Kbps

CPU QEMU Virtual CPU version 2

% Utilization 1

60 seconds

Utilization Speed Base speed: 2.29 GHz

Figure 2.5 – Checking CPU performance on the different tools.

9. In Process Explorer, open the **CPUSTRES64.exe** process to display detailed data. Select Cancel when you have browsed each tab.

Task 3

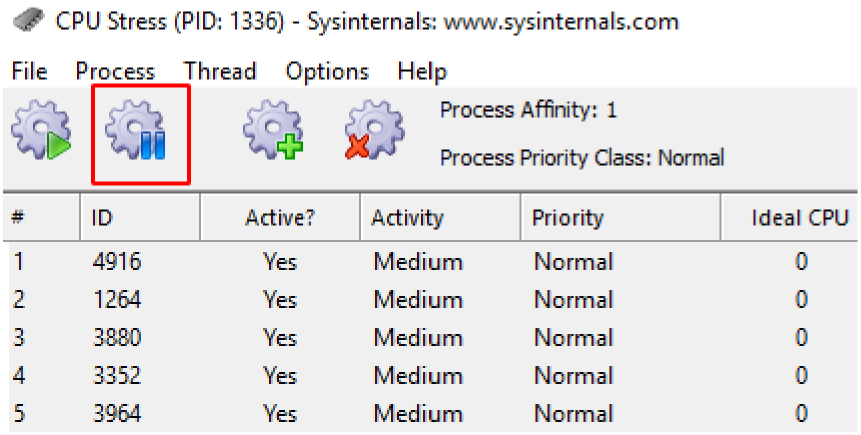
End the CPU Stress threads

You have now completed the stress test, so you will end the threads.

1. In the CPU Stress console, right-click each thread, and then select **Deactivate**.

You can select several or all of the threads by holding down the **SHIFT** or **CTRL** keys.

Or, in **CPU Stress** click the **Deactivate Threads** button to stop it.



Process Affinity: 1

Process Priority Class: Normal

#	ID	Active?	Activity	Priority	Ideal CPU
1	4916	Yes	Medium	Normal	0
2	1264	Yes	Medium	Normal	0
3	3880	Yes	Medium	Normal	0
4	3352	Yes	Medium	Normal	0
5	3964	Yes	Medium	Normal	0

Figure 3.1 – Stopping the Thread in CPU Stress.

2. Display Process Explorer and Task Manager, CPU utilization should be well below 100%.

3. Close Process Explorer, Task Manager, and CPU Stress.

4. Switch to Performance Monitor, right-click the **CPU baseline** data collector set, and select **Stop**.

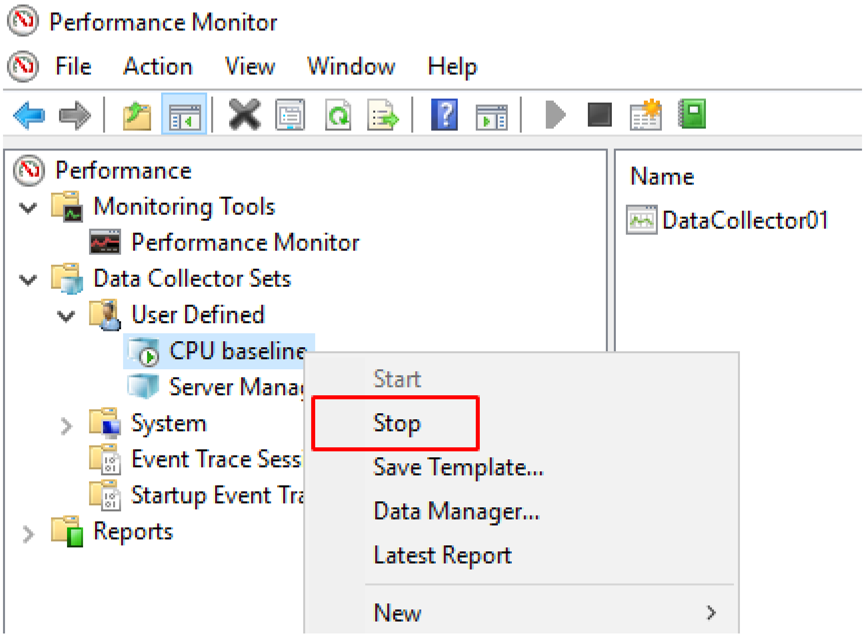
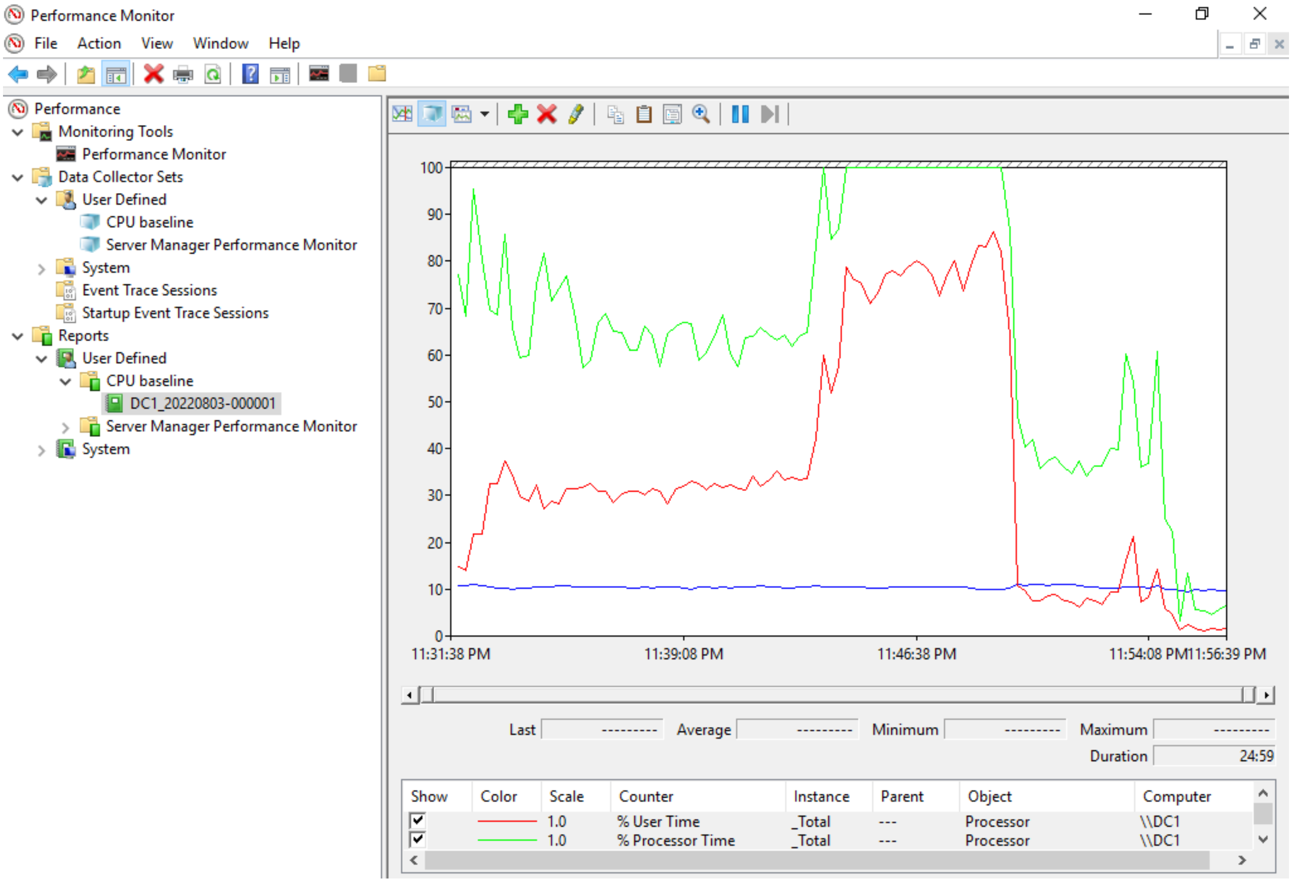


Figure 3.2 – Stopping the Data Collector.

5. Right-click **CPU baseline** and select **Latest Report**.



Last --------- Average --------- Minimum --------- Maximum ---------

Duration 24:59

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑	🟥	1.0	% User Time	_Total	---	Processor	\\DC1
☑	🟩	1.0	% Processor Time	_Total	---	Processor	\\DC1

Figure 3.3 – Analyzing the report.

6. Analyze the report.

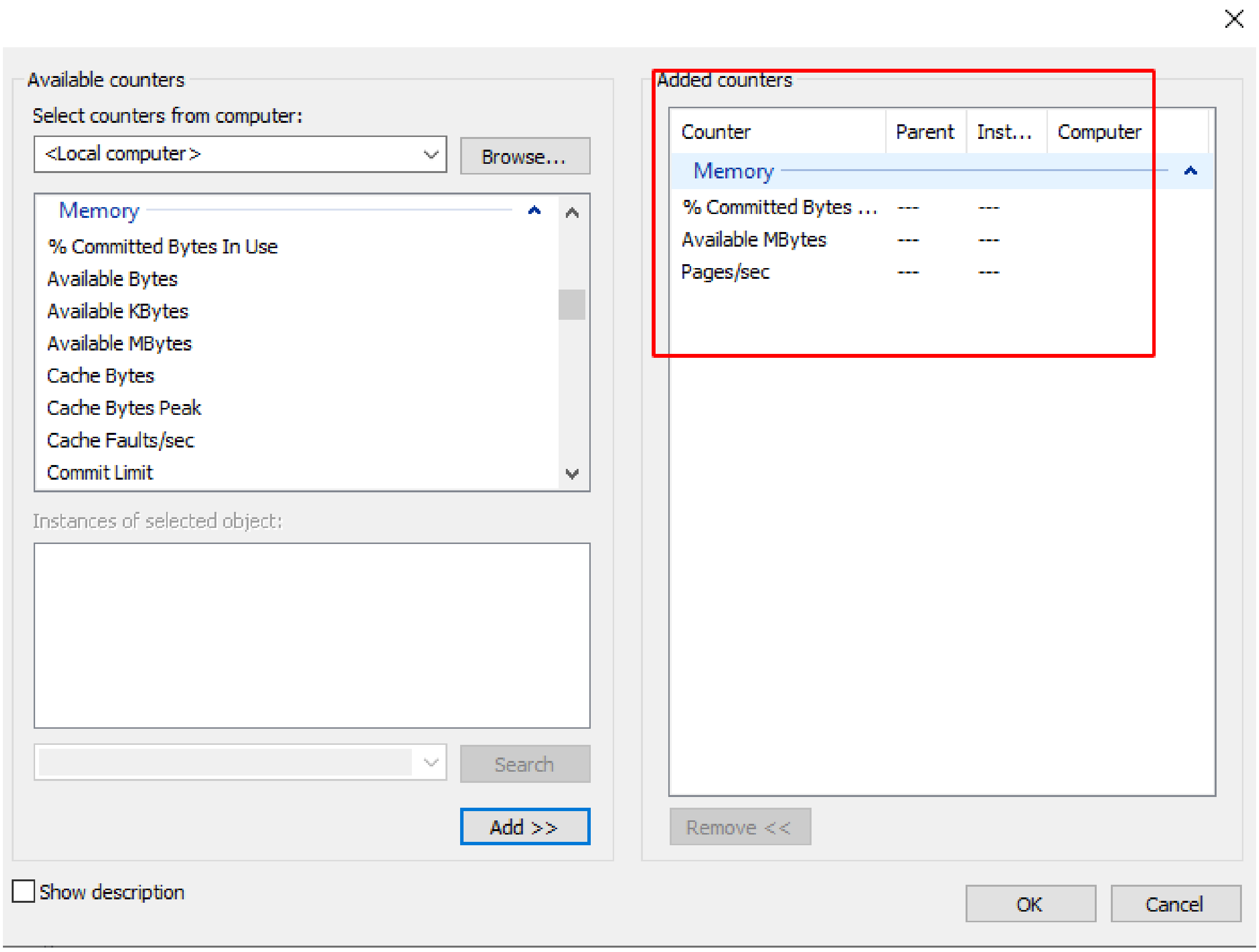
Task 4

Create stress on the Memory

You will use the testlimit utility to create a false workload that stresses the system’s memory. Simulating an application attack that attempts to consume RAM. You’ll use Performance Monitor and Task Manager to observe the results.

1. Select **Performance Monitor**, and then create a **new Data Collector Set** named **Memory baseline** with the following counters from the **Memory** category:

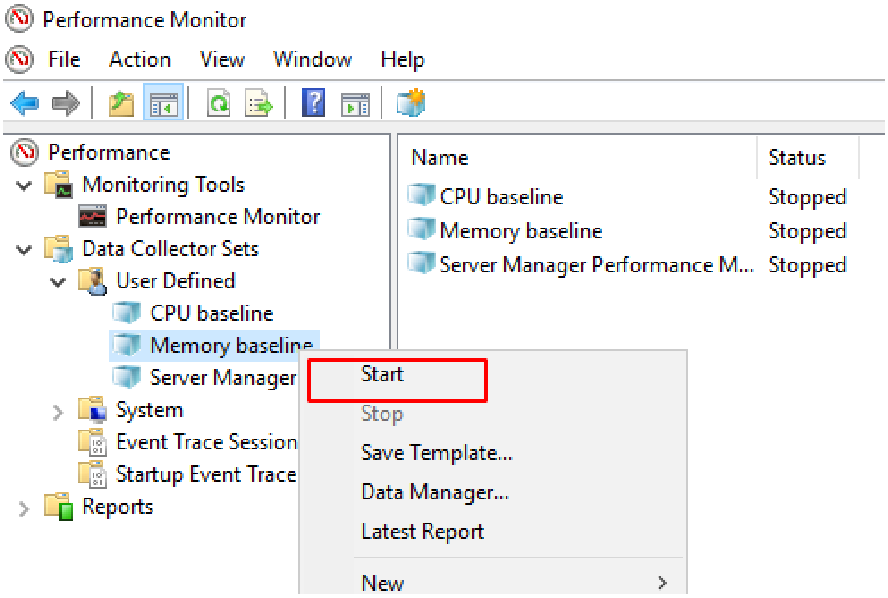
- % Committed Bytes In Use (this counter compares committed memory bytes to the byte commit level, indicating paging utilization that may be due to memory leaks or too many open applications)
- Available MBytes (this counter reports the quantity of memory available for new application to startup)
- Pages/sec (this counter reports the rate at which memory pages are written to or from the pagefile on the hard disk drive)



Counter	Parent	Inst...	Computer
Memory			
% Committed Bytes ...	---	---	
Available MBytes	---	---	
Pages/sec	---	---	

Figure 4.1 - Adding Memory counters.

2. Right-click the **Memory baseline** data collector set, and then select **Start**.



Name	Status
CPU baseline	Stopped
Memory baseline	Stopped
Server Manager Performance M...	Stopped

Figure 4.2 – Starting the Memory baseline.

You will leave the Data Collector Set running through the next several tasks. It gathers information as you accomplish activity steps.

3. Select Windows **Start** menu, right-click **Windows PowerShell (admin)**.

4. In the **Windows PowerShell** console, **ENTER**:

```
cd C:\LABFILES
```

5. In the **Task Manager** console, select the **Memory** node.

6. Resize the Windows PowerShell console and the task Manager console so that you can observe them simultaneously.

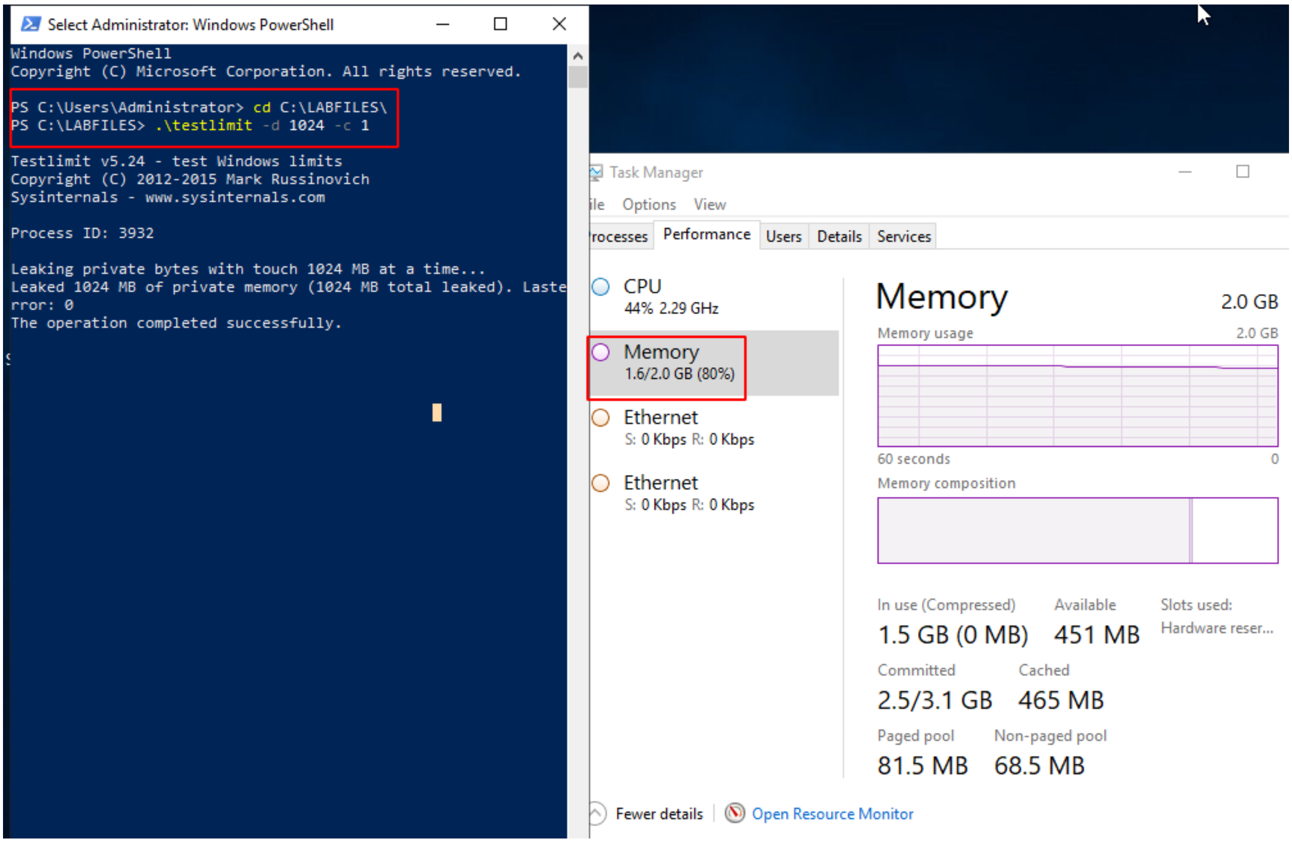
The goal is to view the effect of starting the testlimit utility in Task Manager.

7. Run the following command in Windows PowerShell to simulate the consumption of memory, selecting Agree when prompted to accept the license agreement:

```
.\testlimit -d 1024 -c 1
```

8. Switch to **Task Manager**, and then view the **Memory** category.

Memory utilization should be high.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd C:\LABFILES\
PS C:\LABFILES> .\testlimit -d 1024 -c 1

Testlimit v5.24 - test Windows limits
Copyright (C) 2012-2015 Mark Russinovich
Sysinternals - www.sysinternals.com

Process ID: 3932

Leaking private bytes with touch 1024 MB at a time...
Leaked 1024 MB of private memory (1024 MB total leaked). Laste
rror: 0
The operation completed successfully.
```

CPU
44% 2.29 GHz

Memory
1.6/2.0 GB (80%)

Ethernet
S: 0 Kbps R: 0 Kbps

Ethernet
S: 0 Kbps R: 0 Kbps

Memory 2.0 GB

Memory usage 2.0 GB

60 seconds 0

Memory composition

In use (Compressed): 1.5 GB (0 MB)
Available: 451 MB
Slots used:
Hardware reser...
Committed: 2.5/3.1 GB
Cached: 465 MB
Paged pool: 81.5 MB
Non-paged pool: 68.5 MB

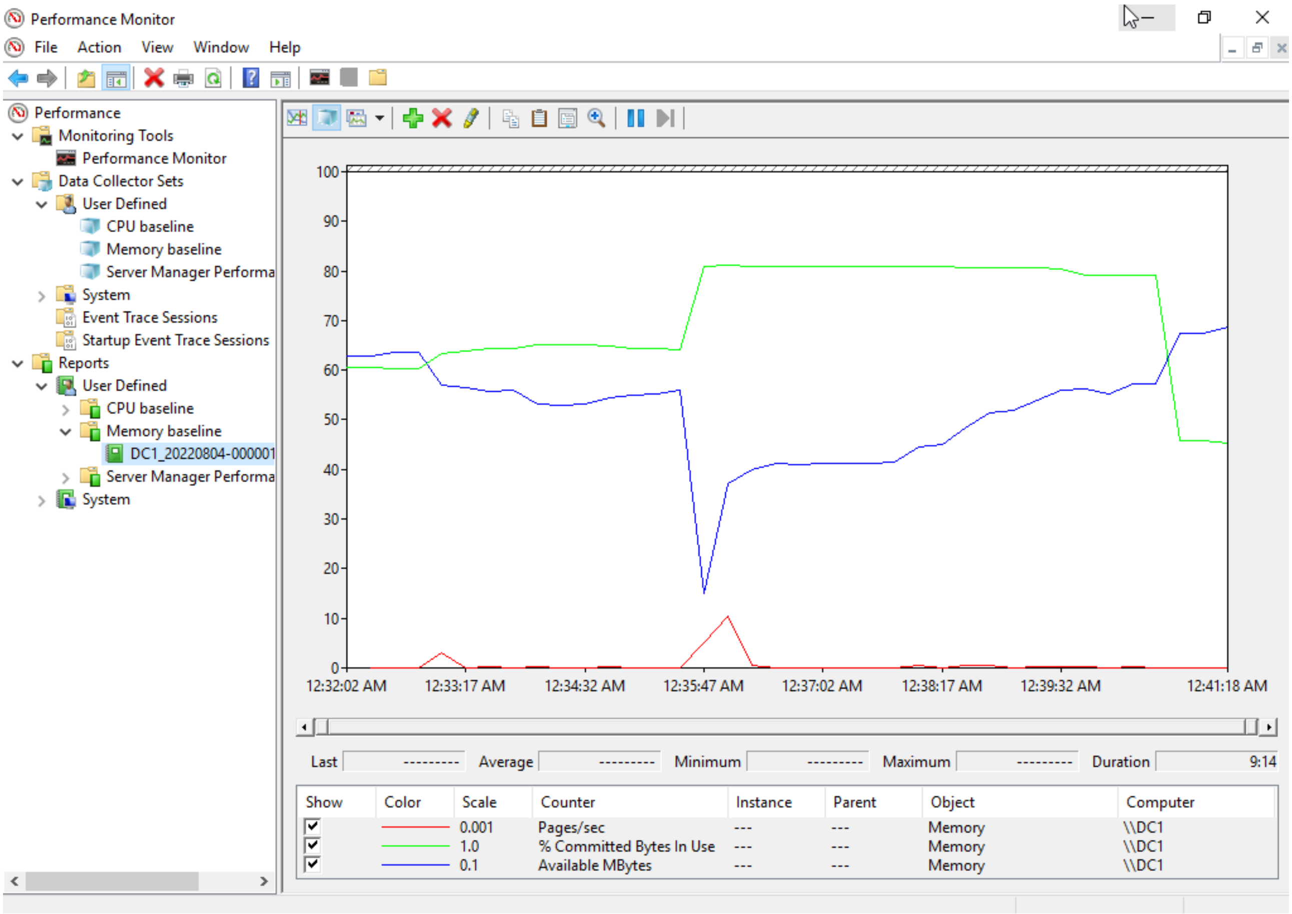
Figure 4.3 – Executing testlimit and checking task manager.

9. In Task Manager, select **Processes** tab.

10. Scroll down to the B**ackground Processes** section, right-click **Test Windows Limits**, and then select **End Task**.

11. Select **Performance Monitor**, and then stop the **Memory baseline** Data Collector Set.

12. Right-click **Memory baseline** and then select **Latest Report**.



Last --------- Average --------- Minimum --------- Maximum --------- Duration 9:14

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑	🟥	0.001	Pages/sec	---	---	Memory	\\DC1
☑	🟩	1.0	% Committed Bytes In Use	---	---	Memory	\\DC1
☑	🟦	0.1	Available MBytes	---	---	Memory	\\DC1

Figure 4.4 – Analyzing the report.

13. Analyze the **Report**.