Hardware Performance Counter

The system used and the rest of the HPC manual

İ.Yusuf Cosgun /180101012

12 January 2024

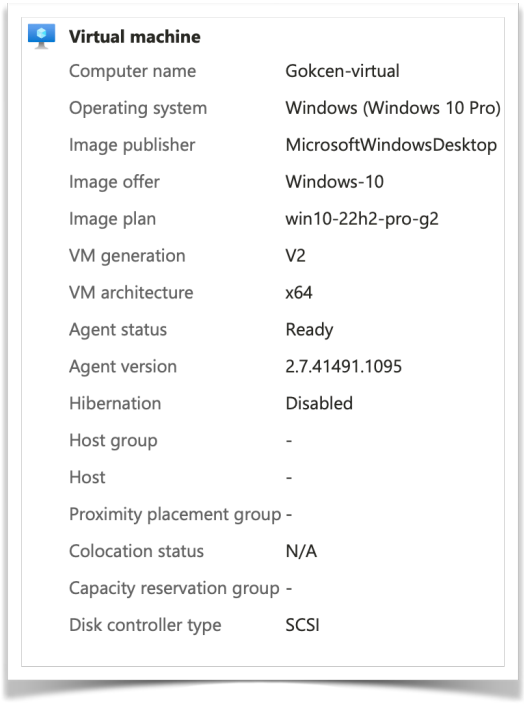
System Used For This research

Observations were made on 3 virtual machines and it should be known that similar architectures and configurations were selected in these 3 machines. For showing the reference ,explain and show one system.

*This configuration is available on all operating systems ***

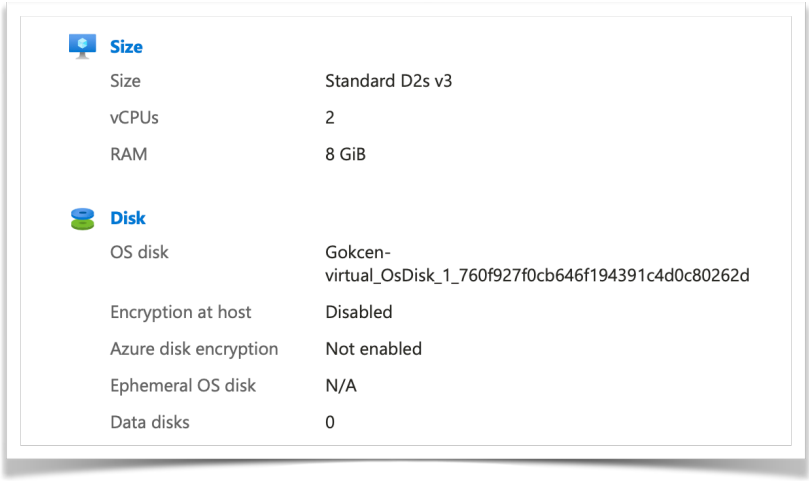
I used Microsoft's virtual machine through the 'Azure portal'.

https://portal.azure.com/#home



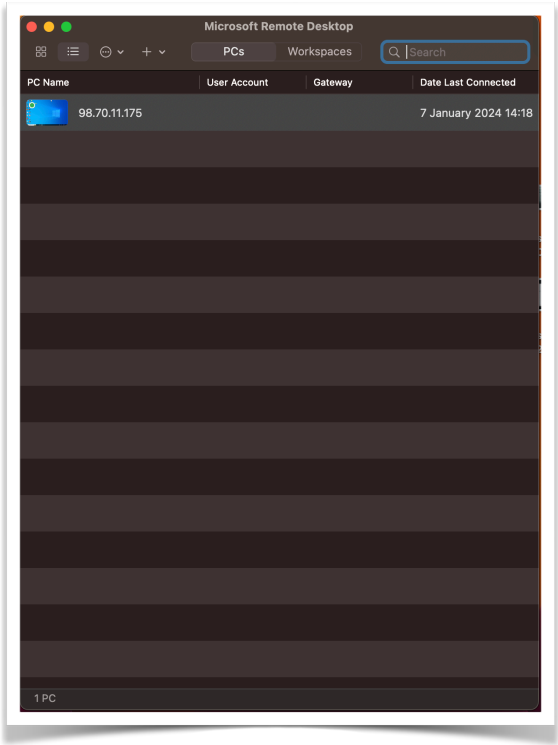
Virtual machine	
Computer name	Gokcen-virtual
Operating system	Windows (Windows 10 Pro)
Image publisher	MicrosoftWindowsDesktop
Image offer	Windows-10
Image plan	win10-22h2-pro-g2
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.7.41491.1095
Hibernation	Disabled
Host group	-
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-
Disk controller type	SCSI

1.Virtual Machine Informations



2.Configurations

For connecting to the Remote Virtual Machine Microsoft have to “Microsoft Remote Desktop” applications



Preferred Apps for HPC Observing

In Virtual machine Windows , we chose one main program (Performance Monitor) and one program for helping (Process explorer) process name chose. I will explain step by step in this point.

First of downloading “Process Explorer”

https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer

Second program Performance Monitor (updated version here but we are not used)

https://techcommunity.microsoft.com/t5/windows-admin-center-blog/introducing-the-new-performance-monitor-for-windows/ba-p/957991

In this example we’ll observing “Winamp” application.

Step -1-

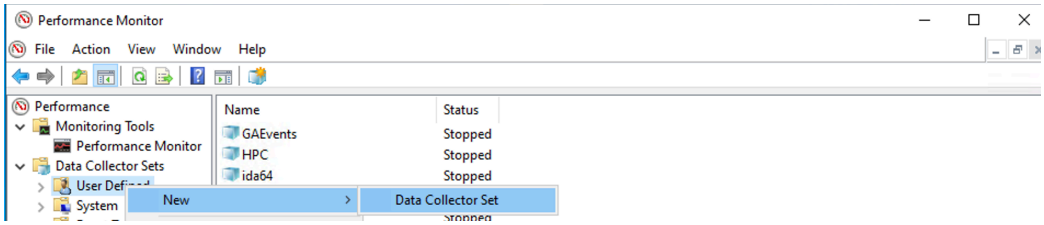
First we detect the process name with Process explorer

Step-2-

After open the Performance Monitor.

In the window that opens, click Data Collector Sets

The 'User Defined' folder will appear at the bottom. Right-click the 'User Defined' Folder and select 'Data Collector Set' from the 'New' sect.



After Chose the name then click NEXT

At this point, we saved an xml file on the desktop to improve performance and to perform the listening of a certain program, we updated the process_name section in the file and increased our observation speed..

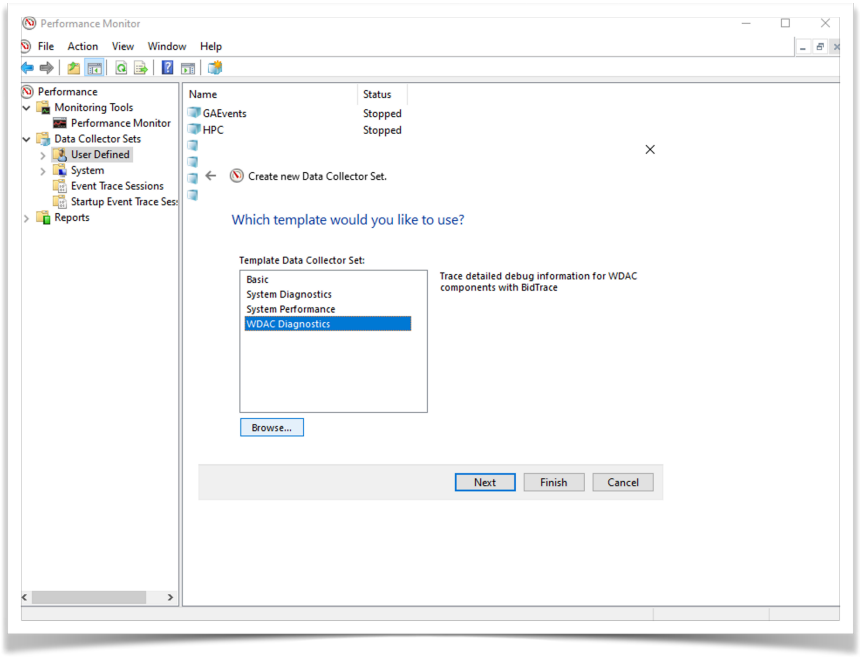
notepad++ -> control+f and replace method giving more speed for procedure

Process.xml {<?xml version="1.0" encoding="UTF-16"?>

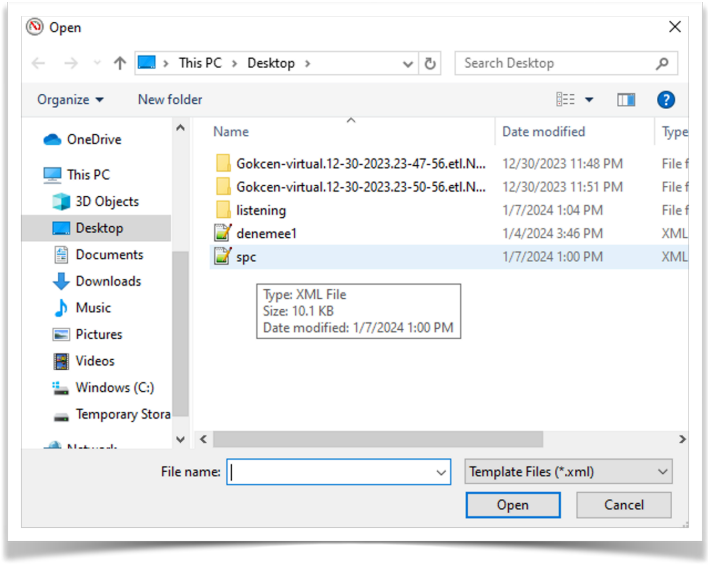
<DataCollectorSet>
<Status>0</Status>
<Duration>0</Duration>
<Description>
</Description>
<DescriptionUnresolved>
</DescriptionUnresolved>
<DisplayName>
</DisplayName>
<DisplayNameUnresolved>
</DisplayNameUnresolved>
<SchedulesEnabled>-1</SchedulesEnabled>
<LatestOutputLocation>C:\PerfLogs\Admin\OSPC Values\DESKTOP-DLOIPN7_20240107-000003</LatestOutputLocation>
<Name>OSPC Values</Name>
<OutputLocation>C:\PerfLogs\Admin\OSPC Values\DESKTOP-DLOIPN7_20240107-000004</OutputLocation>
<RootPath>%systemdrive%\PerfLogs\Admin\OSPC Values</RootPath>
0
<SegmentMaxDuration>60</SegmentMaxDuration>
<SegmentMaxSize>0</SegmentMaxSize>
<SerialNumber>4</SerialNumber>
<Server>
</Server>
<Subdirectory>
</Subdirectory>
<SubdirectoryFormat>3</SubdirectoryFormat>
<SubdirectoryFormatPattern>yyyyMMdd\-NNNNNN</SubdirectoryFormatPattern>
<Task>
</Task>
<TaskRunAsSelf>0</TaskRunAsSelf>
<TaskArguments>

```
        </TaskArguments>
        <TaskUserTextArguments>
        </TaskUserTextArguments>
        <UserAccount>SYSTEM</UserAccount>
        <Security>O:BAG:S-1-5-21-187289043-3473897721-2699178721-513D:AI(A;;FA;;;SY)(A;;FA;;;BA)(A;;0x1200a9;;;LU)
(A;;0x1301ff;;;S-1-5-80-2661322625-712705077-2999183737-3043590567-590698655)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)
(A;ID;FR;;;NS)(A;ID;FA;;;BA)</Security>
        <StopOnCompletion>0</StopOnCompletion>
        <PerformanceCounterDataCollector>
            <DataCollectorType>0</DataCollectorType>
            <Name>SPC</Name>
            <FileName>SPC</FileName>
            <FileNameFormat>1</FileNameFormat>
            <FileNameFormatPattern>
            </FileNameFormatPattern>
            <LogAppend>0</LogAppend>
            <LogCircular>0</LogCircular>
            <LogOverwrite>0</LogOverwrite>
            <LatestOutputLocation>C:\PerfLogs\Admin\OSPC Values\DESKTOP-DLOIPN7_20240107-000003\SPC.csv</
LatestOutputLocation>
            <DataSourceName>
            </DataSourceName>
            <SampleInterval>1</SampleInterval>
            <SegmentMaxRecords>0</SegmentMaxRecords>
            <LogFileFormat>0</LogFileFormat>
            <Counter>\Process({process_name})\% Privileged Time</Counter>
            <Counter>\Process({process_name})\Handle Count</Counter>
            <Counter>\Process({process_name})\IO Data Bytes/sec</Counter>
            <Counter>\Process({process_name})\IO Data Operations/sec</Counter>
            <Counter>\Process({process_name})\IO Other Bytes/sec</Counter>
            <Counter>\Process({process_name})\IO Other Operations/sec</Counter>
            <Counter>\Process({process_name})\IO Read Bytes/sec</Counter>
            <Counter>\Process({process_name})\IO Read Operations/sec</Counter>
            <Counter>\Process({process_name})\IO Write Bytes/sec</Counter>
            <Counter>\Process({process_name})\IO Write Operations/sec</Counter>
            <Counter>\Process({process_name})\Page Faults/sec</Counter>
            <Counter>\Process({process_name})\Page File Bytes</Counter>
            <Counter>\Process({process_name})\Page File Bytes Peak</Counter>
            <Counter>\Process({process_name})\Pool Nonpaged Bytes</Counter>
            <Counter>\Process({process_name})\Pool Paged Bytes</Counter>
            <Counter>\Process(process_name)\Priority Base</Counter>
            <Counter>\Process(process_name)\Private Bytes</Counter>
            <Counter>\Process(process_name)\Thread Count</Counter>
            <Counter>\Process(process_name)\Virtual Bytes</Counter>
            <Counter>\Process(process_name)\Virtual Bytes Peak</Counter>
            <Counter>\Process(process_name)\Working Set</Counter>
            <Counter>\Process(process_name)\Working Set - Private</Counter>
            <Counter>\Process(process_name)\Working Set Peak</Counter>
            <CounterDisplayName>% Privileged Time</CounterDisplayName>
            <CounterDisplayName>Handle Count</CounterDisplayName>
            <CounterDisplayName>IO Data Bytes/sec</CounterDisplayName>
            <CounterDisplayName>IO Data Operations/sec</CounterDisplayName>
            <CounterDisplayName>IO Other Bytes/sec</CounterDisplayName>
            <CounterDisplayName>IO Other Operations/sec</CounterDisplayName>
            <CounterDisplayName>IO Read Bytes/sec</CounterDisplayName>
            <CounterDisplayName>IO Read Operations/sec</CounterDisplayName>
            <CounterDisplayName>IO Write Bytes/sec</CounterDisplayName>
            <CounterDisplayName>IO Write Operations/sec</CounterDisplayName>
```

```
                <CounterDisplayName>Page Faults/sec</CounterDisplayName>
                <CounterDisplayName>Page File Bytes</CounterDisplayName>
                <CounterDisplayName>Page File Bytes Peak</CounterDisplayName>
                <CounterDisplayName>Pool Nonpaged Bytes</CounterDisplayName>
                <CounterDisplayName>Pool Paged Bytes</CounterDisplayName>
                <CounterDisplayName>Priority Base</CounterDisplayName>
                <CounterDisplayName>Private Bytes</CounterDisplayName>
                <CounterDisplayName>Thread Count</CounterDisplayName>
                <CounterDisplayName>Virtual Bytes</CounterDisplayName>
                <CounterDisplayName>Virtual Bytes Peak</CounterDisplayName>
                <CounterDisplayName>Working Set</CounterDisplayName>
                <CounterDisplayName>Working Set - Private</CounterDisplayName>
                <CounterDisplayName>Working Set Peak</CounterDisplayName>
        </PerformanceCounterDataCollector>
        <DataManager>
                <Enabled>0</Enabled>
                <CheckBeforeRunning>0</CheckBeforeRunning>
                <MinFreeDisk>0</MinFreeDisk>
                <MaxSize>0</MaxSize>
                <MaxFolderCount>0</MaxFolderCount>
                <ResourcePolicy>0</ResourcePolicy>
                <ReportFileName>report.html</ReportFileName>
                <RuleTargetFileName>report.xml</RuleTargetFileName>
                <EventsFileName>
                </EventsFileName>
        </DataManager>
</DataCollectorSet>
}
```

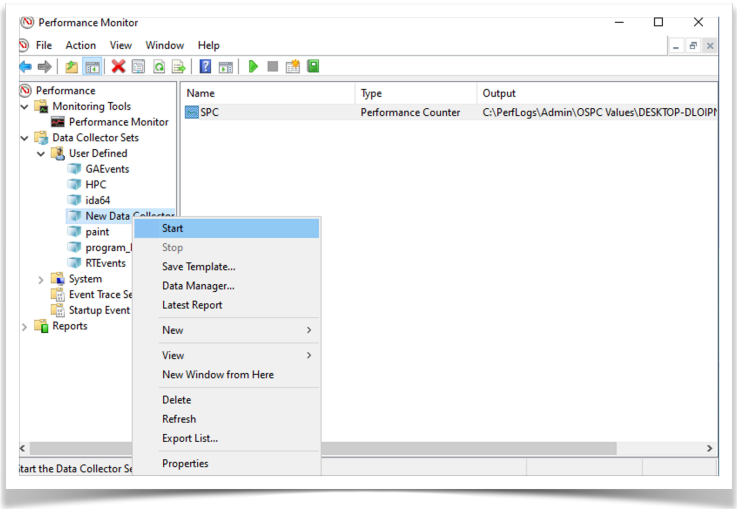


To do this, the 'Browse' option is clicked in the window after the name is selected.

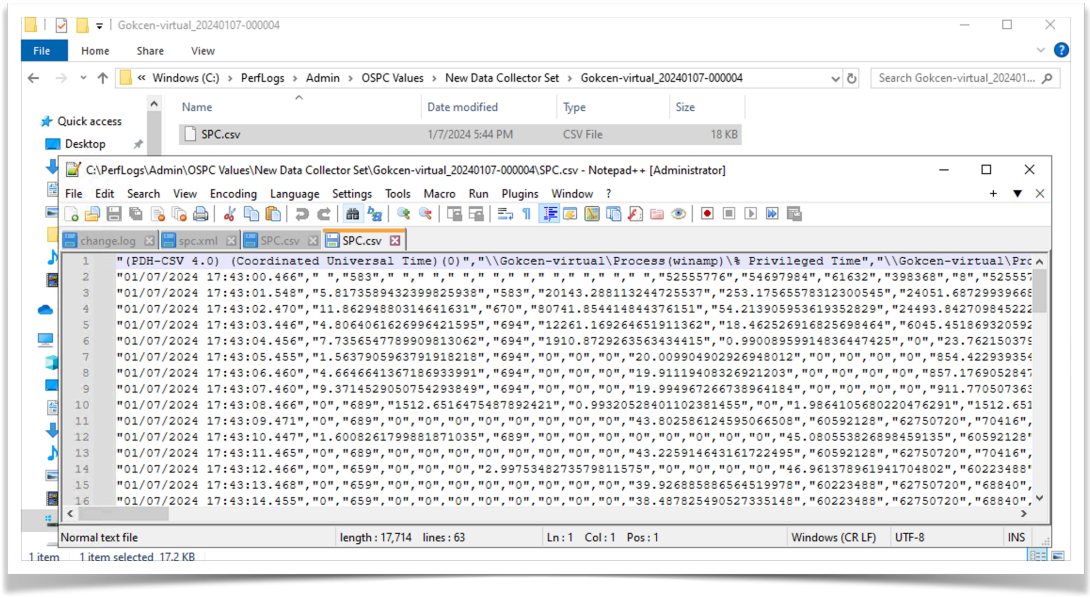


Then clicking xml file for Observing settings. Then clicking FINISH

First of all, whichever program to be observed should be opened. In our example, we mentioned Winamp.



After click to Start button. This method observing 60 sec to Winamp HPC'S.



Here the our observed HPC’s for Winamp (for 60 sec)

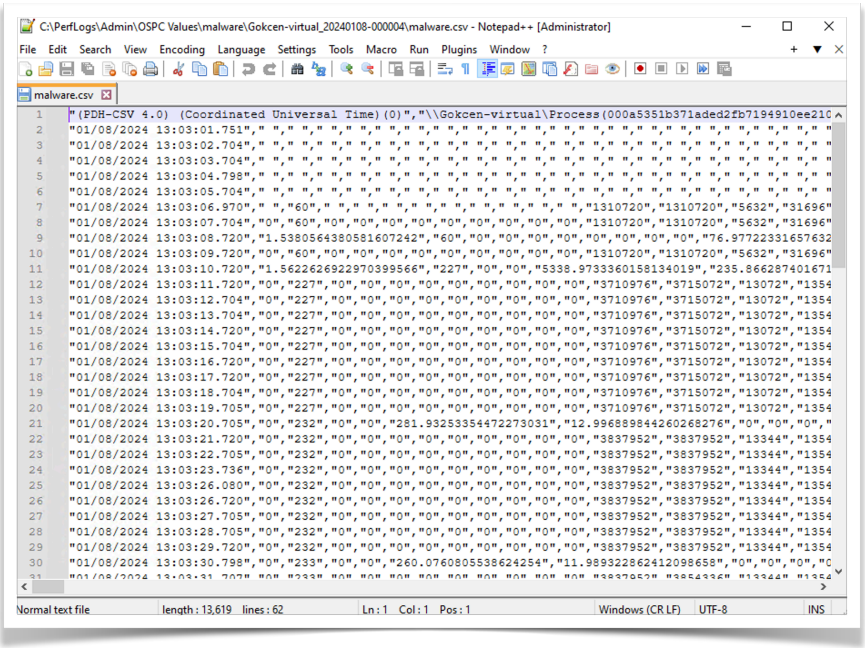
SAME METHOD FOR MALWARE

At this point Same Procedure is performed for

”

000a5351b371aded2fb7194910ee210cb029199eb65a4f755f23a4f904117607”

malware name example. In this example, it is natural that the first lines are empty because the observation is started first and the records are taken later.



Consulation

With this guide, we have achieved our goal to guide researchers who want to observe a malware or benign program. If the researcher is a student, he can use a 1-month desktop via Azure or consider installing a VM on his own computer. The created CSV files are kept in a file and ready to use for machine learning research.