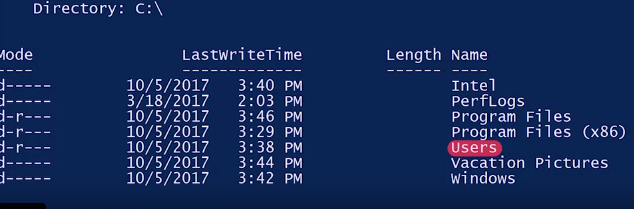
POWERSHELL

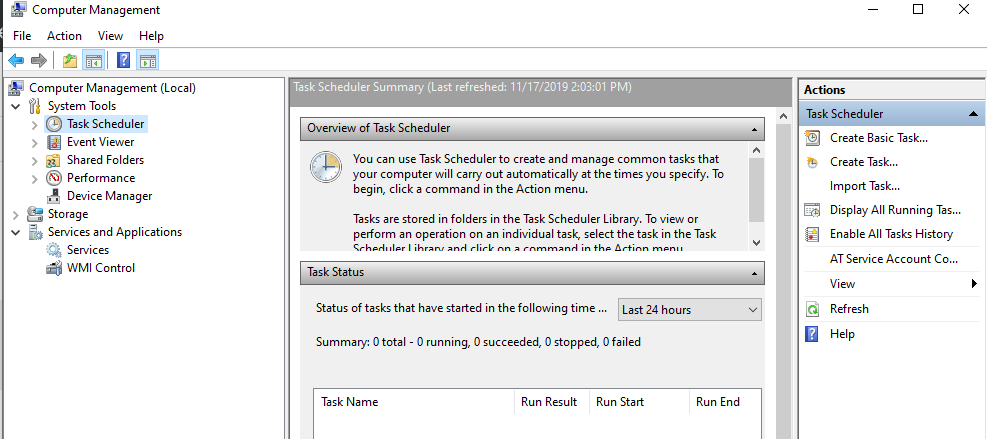
1. List directories
2. Ls c:\ , c is the

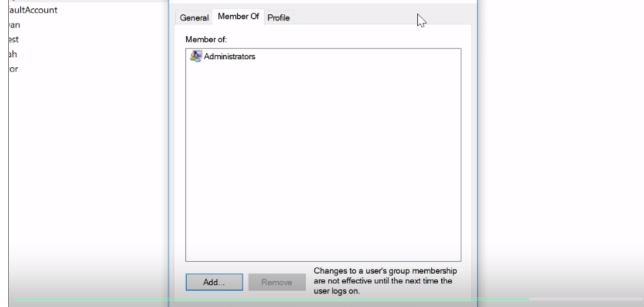


1. Programfiles (x86) is where applications installed, Users list, windows where os is installed
2. C:\ is the root and parent directory and inside its contents child directory
3. Ls -Force c:\ (Hidden files)

Windows user and group information

1. Computer management
2. Local

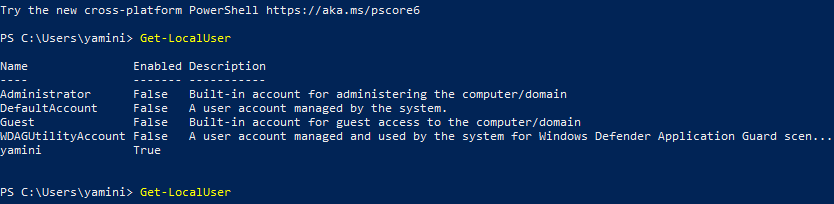




Member of which groups under local users tab in computer management

Using CLI:

1. Get-LocalUser



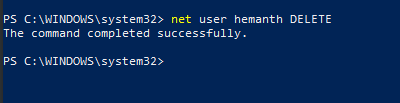
1. Get-LocalGroup
2. Get-LocalGroupMember Adminstrators (to check for who has access to admin)

Windows Passwords:

1. Net user yamini \* (\* for hiding)



1. To delete



1. Net user hemanth logonpasswordchg:yes

( to have the password change in next time)

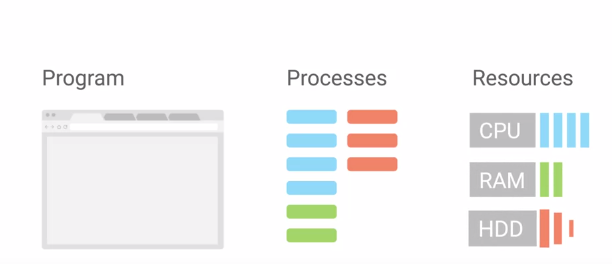
Software and Package management:

1. .exe for software management
2. .msi

Windows archives

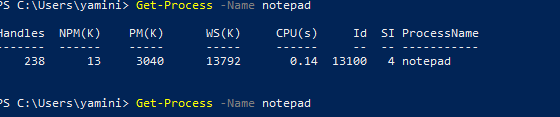
1. Compress-archive in power shell or use 7 zip

WINDOWS OS:



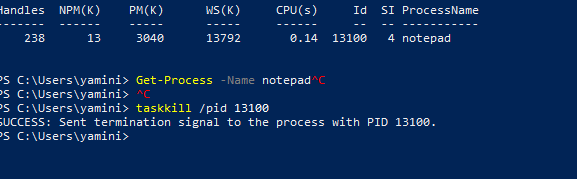
1. PID

Get-Process -Name notepad

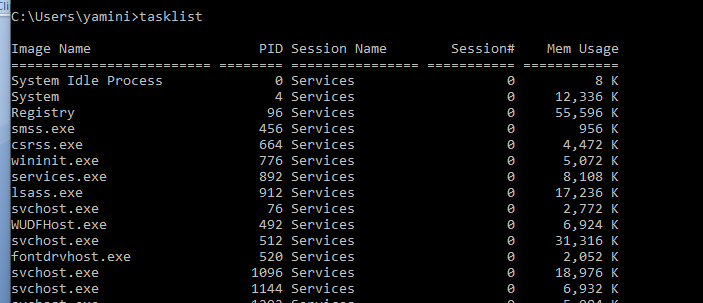


Get-Process for all the processes

1. Kill the process using taskkill /pid 13100



1. Tasklist in cmd



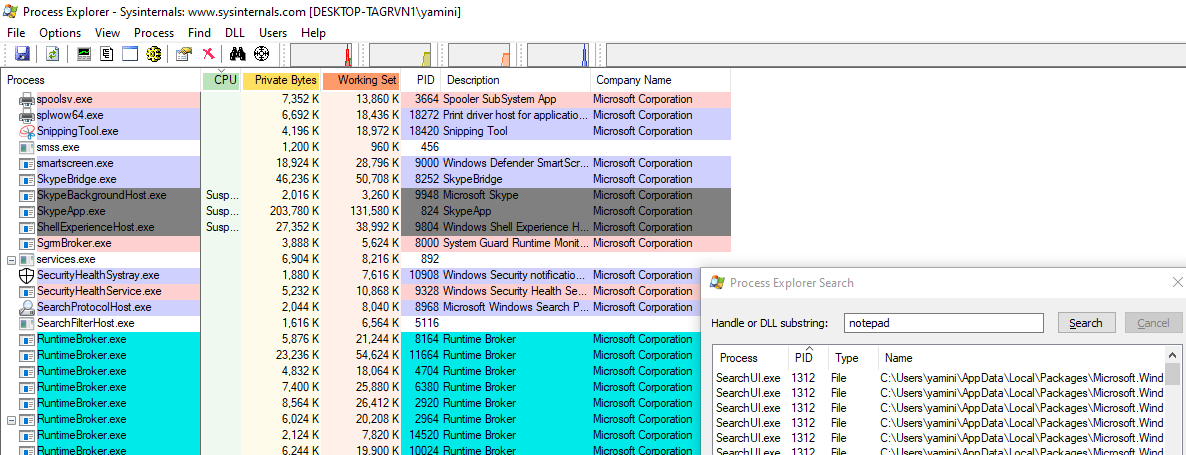
1. Windows signals:

<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/get-process?view=powershell-5.1#outputs>

provides information for all the windows related process

WINDOWS Process Management:

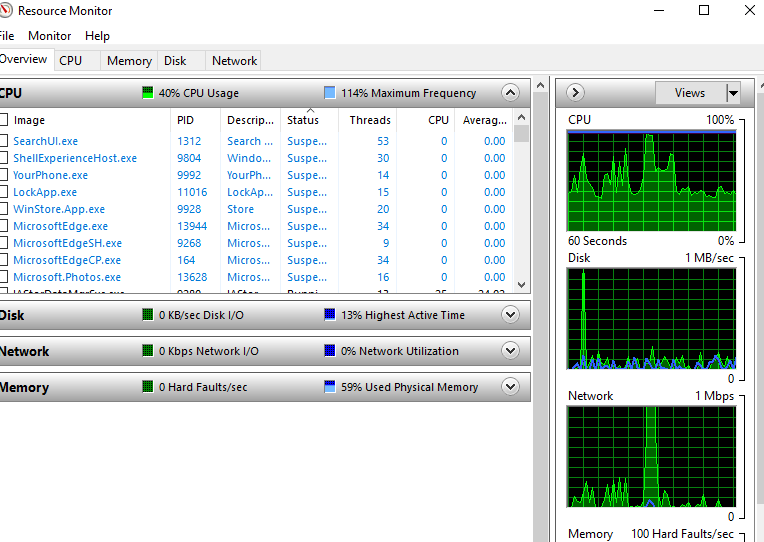
1. We can use process explorer to manage
2. Ctl + f to search



Windows resource monitoring

<https://social.technet.microsoft.com/Forums/ie/en-US/56960c10-e754-41e1-b888-9f2c32e4626a/what-is-paged-pool-non-paged-pool-physical-memoryvirtual-memory?forum=winservergen#:~:targetText=The%20nonpaged%20pool%20consists%20of,and%20out%20of%20the%20system.>

* Resource monitor: Handles: The number of handles that the process has opened.
* NPM(K): The amount of non-paged memory that the process is using, in kilobytes.
* PM(K): The amount of page able memory that the process is using, in kilobytes.
* WS(K): The size of the working set of the process, in kilobytes. The working set consists of the pages of memory that were recently referenced by the process.
* VM(M): The amount of virtual memory that the process is using, in megabytes. Virtual memory includes storage in the paging files on disk.
* CPU(s): The amount of processor time that the process has used on all processors, in seconds.
* ID: The process ID (PID) of the process.
* Process Name: The name of the process. For explanations of the concepts related to processes, see the Glossary in Help and Support Center and the Help for Task Manager.



IMP NOTE: Private bytes means memory

To select few columns: get-process | sort cpu -descending | select -first 3 -Property ID, ProcessName, CPU

