```powershell
#Task 1: Exploring PowerShell Commands

#1. Identify available PowerShell commands.
Get-Command

#2. Retrieve detailed help for a specific command.
Get-Help Get-Process

#3. List all properties and methods of an object.
Get-Process
Get-Process ServerManager

#Task 2: Working with Objects

#1. Display process information in table and list formats.
Get-Process | Format-Table -AutoSize
Get-Process | Format-List

#2. Sort processes based on CPU usage.
Get-Process | Sort-Object -Property CPU

#3. Select and filter objects based on specific conditions.
Get-Process | Select-Object -First 5
Get-Process | Select-Object -First 10
Get-Process | Where-Object { $_.CPU -gt 15 }

#4. Loop through system objects and extract specific information.
Get-Service | ForEach-Object { "$($_.Name) is $($_.Status)" }

#Task 3: Managing the File System

#1. Navigate through directories and list files.
Get-ChildItem C:\Users
Get-ChildItem C:\Windows
Set-Location -Path C:\
Get-ChildItem C:\Users\Administrator
Get-ChildItem C:\Users\Administrator\Documents


#2. Create and delete files and folders.
New-Item -Path "C:\TestLab2.txt" -ItemType File
New-Item -ItemType Directory -Path C:\TestLab2Folder
Remove-Item -Path C:\TestLab2Folder
Remove-Item -Path C:\TestLab2.txt


#3. Copy and move files between locations.
New-Item -ItemType Directory -Path C:\Backup
New-Item -Path "C:\TestLab2.txt" -ItemType File
Copy-Item -Path "C:\TestLab2.txt" -Destination "C:\Backup\"
New-Item -Path "C:\Test2Lab2.txt" -ItemType File
Move-Item -Path "C:\Test2Lab2.txt" -Destination "C:\Backup\"

#4. Check available disk space.
Get-PSDrive

#Task 4: Managing System Services and Processes

#1. List all running services on the system.
Get-Service | Where-Object { $_.Status -eq 'Running' }

#2. Start and stop specific services.
Start-Service -Name "Spooler"
Get-Service -Name "Spooler"
Stop-Service -Name "Spooler"
Get-Service -Name "Spooler"
```

```
#3. Retrieve information about active processes.
Get-Process | Where-Object { $_.Responding -eq $true }

#4. Terminate a process.
Stop-Process -Name "notepad"

#Task 5: Monitoring Event Logs and System Information

#1. View the latest system event logs.
Get-EventLog -LogName System -Newest 10

#2. Retrieve security event logs.
Get-WinEvent -LogName Security

#3. Extract operating system details using PowerShell.
Get-WmiObject -Class Win32_OperatingSystem
Get-CimInstance -ClassName Win32_OperatingSystem | Select-Object Caption,Version,BuildNumber,OSArchitecture
```

4/30/2025

Lab 2

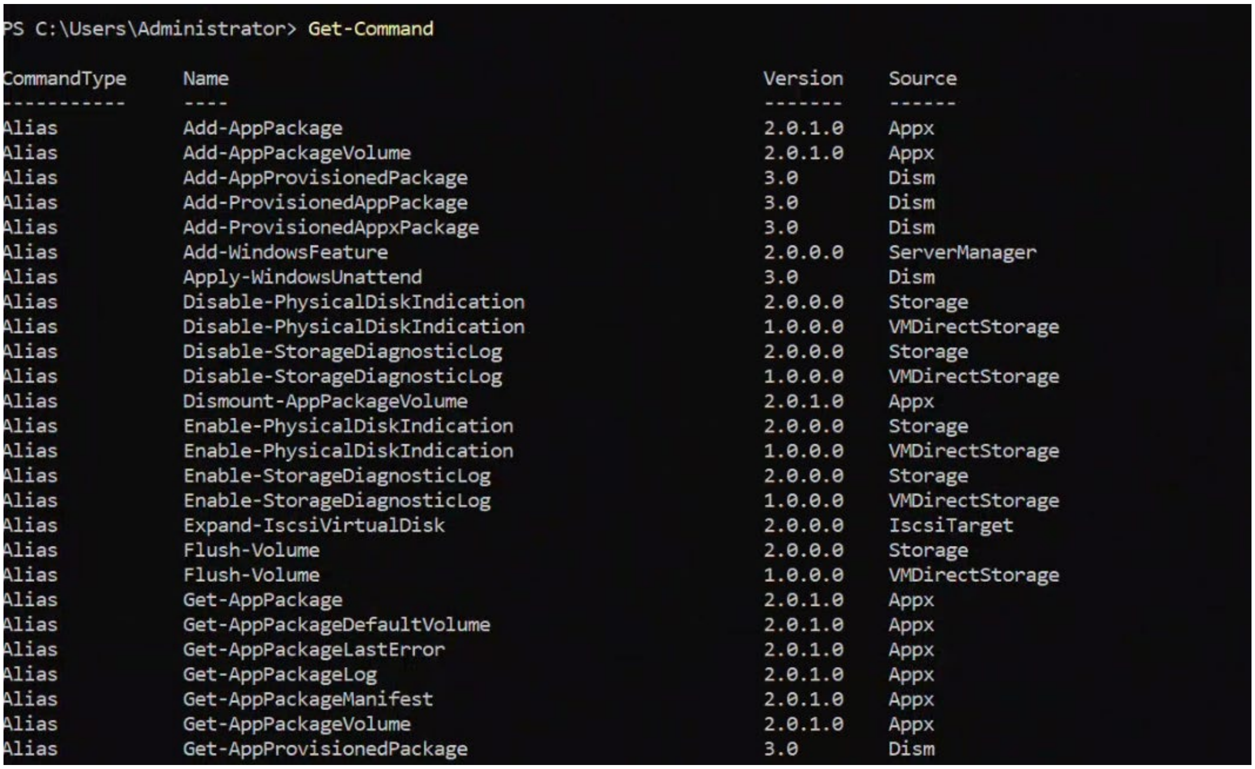
PowerShell Basics & System Administration

Mohammed, Laetitia, 0931512
NETWORK INSTALLATION AND ADMINISTRATION II

Contents

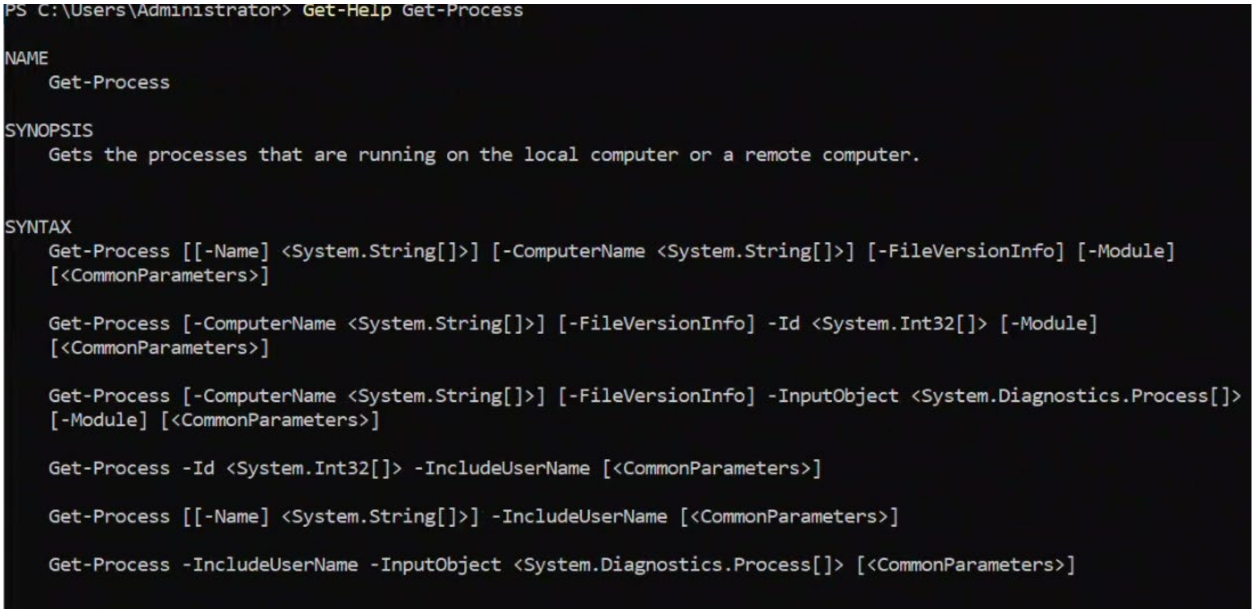
Task 1: Exploring PowerShell Commands

Identify available PowerShell commands

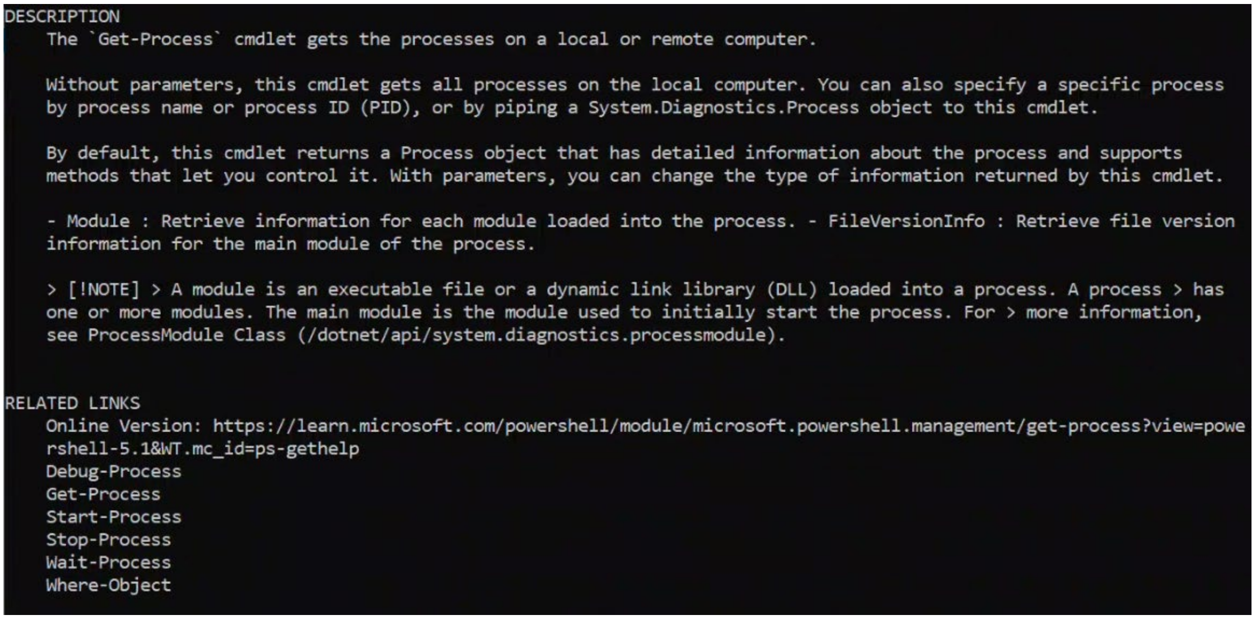


```
PS C:\Users\Administrator> Get-Command

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Alias           Add-AppPackage                                     2.0.1.0    Appx
Alias           Add-AppPackageVolume                               2.0.1.0    Appx
Alias           Add-AppProvisionedPackage                          3.0        Dism
Alias           Add-ProvisionedAppPackage                          3.0        Dism
Alias           Add-ProvisionedAppxPackage                         3.0        Dism
Alias           Add-WindowsFeature                                 2.0.0.0    ServerManager
Alias           Apply-WindowsUnattend                              3.0        Dism
Alias           Disable-PhysicalDiskIndication                     2.0.0.0    Storage
Alias           Disable-PhysicalDiskIndication                     1.0.0.0    VMDirectStorage
Alias           Disable-StorageDiagnosticLog                       2.0.0.0    Storage
Alias           Disable-StorageDiagnosticLog                       1.0.0.0    VMDirectStorage
Alias           Dismount-AppPackageVolume                          2.0.1.0    Appx
Alias           Enable-PhysicalDiskIndication                      2.0.0.0    Storage
Alias           Enable-PhysicalDiskIndication                      1.0.0.0    VMDirectStorage
Alias           Enable-StorageDiagnosticLog                        2.0.0.0    Storage
Alias           Enable-StorageDiagnosticLog                        1.0.0.0    VMDirectStorage
Alias           Expand-IscsiVirtualDisk                            2.0.0.0    IscsiTarget
Alias           Flush-Volume                                       2.0.0.0    Storage
Alias           Flush-Volume                                       1.0.0.0    VMDirectStorage
Alias           Get-AppPackage                                     2.0.1.0    Appx
Alias           Get-AppPackageDefaultVolume                        2.0.1.0    Appx
Alias           Get-AppPackageLastError                            2.0.1.0    Appx
Alias           Get-AppPackageLog                                  2.0.1.0    Appx
Alias           Get-AppPackageManifest                             2.0.1.0    Appx
Alias           Get-AppPackageVolume                               2.0.1.0    Appx
Alias           Get-AppProvisionedPackage                          3.0        Dism
```

Retrieve detailed help for a specific command

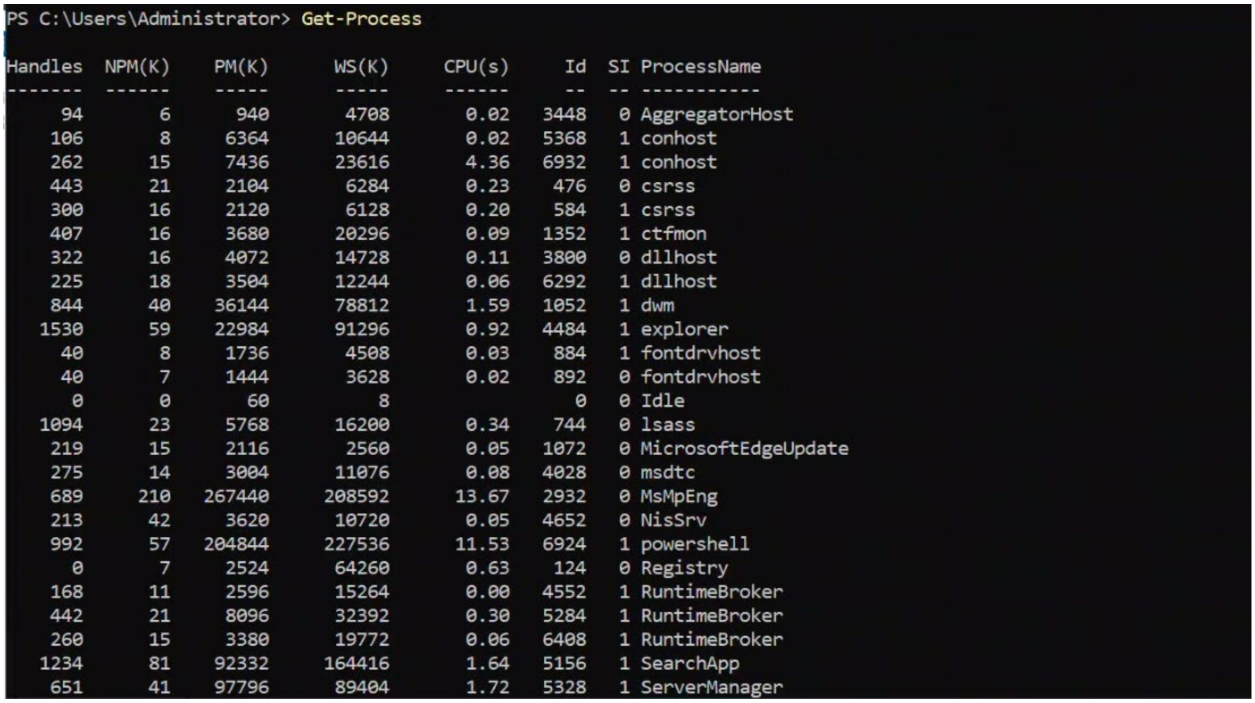


```
PS C:\Users\Administrator> Get-Help Get-Process

NAME
    Get-Process

SYNOPSIS
    Gets the processes that are running on the local computer or a remote computer.


SYNTAX
    Get-Process [[-Name] <System.String[]>] [-ComputerName <System.String[]>] [-FileVersionInfo] [-Module]
    [<CommonParameters>]

    Get-Process [-ComputerName <System.String[]>] [-FileVersionInfo] -Id <System.Int32[]> [-Module]
    [<CommonParameters>]

    Get-Process [-ComputerName <System.String[]>] [-FileVersionInfo] -InputObject <System.Diagnostics.Process[]>
    [-Module] [<CommonParameters>]

    Get-Process -Id <System.Int32[]> -IncludeUserName [<CommonParameters>]

    Get-Process [[-Name] <System.String[]>] -IncludeUserName [<CommonParameters>]

    Get-Process -IncludeUserName -InputObject <System.Diagnostics.Process[]> [<CommonParameters>]
```

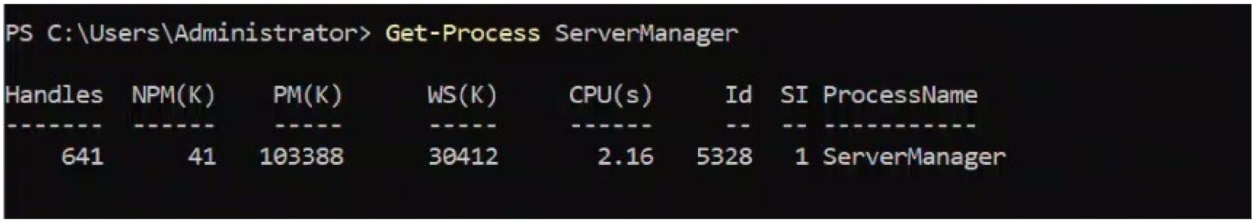


```
DESCRIPTION
    The `Get-Process` cmdlet gets the processes on a local or remote computer.

    Without parameters, this cmdlet gets all processes on the local computer. You can also specify a specific process
    by process name or process ID (PID), or by piping a System.Diagnostics.Process object to this cmdlet.

    By default, this cmdlet returns a Process object that has detailed information about the process and supports
    methods that let you control it. With parameters, you can change the type of information returned by this cmdlet.

    - Module : Retrieve information for each module loaded into the process. - FileVersionInfo : Retrieve file version
    information for the main module of the process.

    > [!NOTE] > A module is an executable file or a dynamic link library (DLL) loaded into a process. A process > has
    one or more modules. The main module is the module used to initially start the process. For > more information,
    see ProcessModule Class (/dotnet/api/system.diagnostics.processmodule).


RELATED LINKS
    Online Version: https://learn.microsoft.com/powershell/module/microsoft.powershell.management/get-process?view=powe
    rshell-5.1&WT.mc_id=ps-gethelp
    Debug-Process
    Get-Process
    Start-Process
    Stop-Process
    Wait-Process
    Where-Object
```

List all properties and methods of an object.



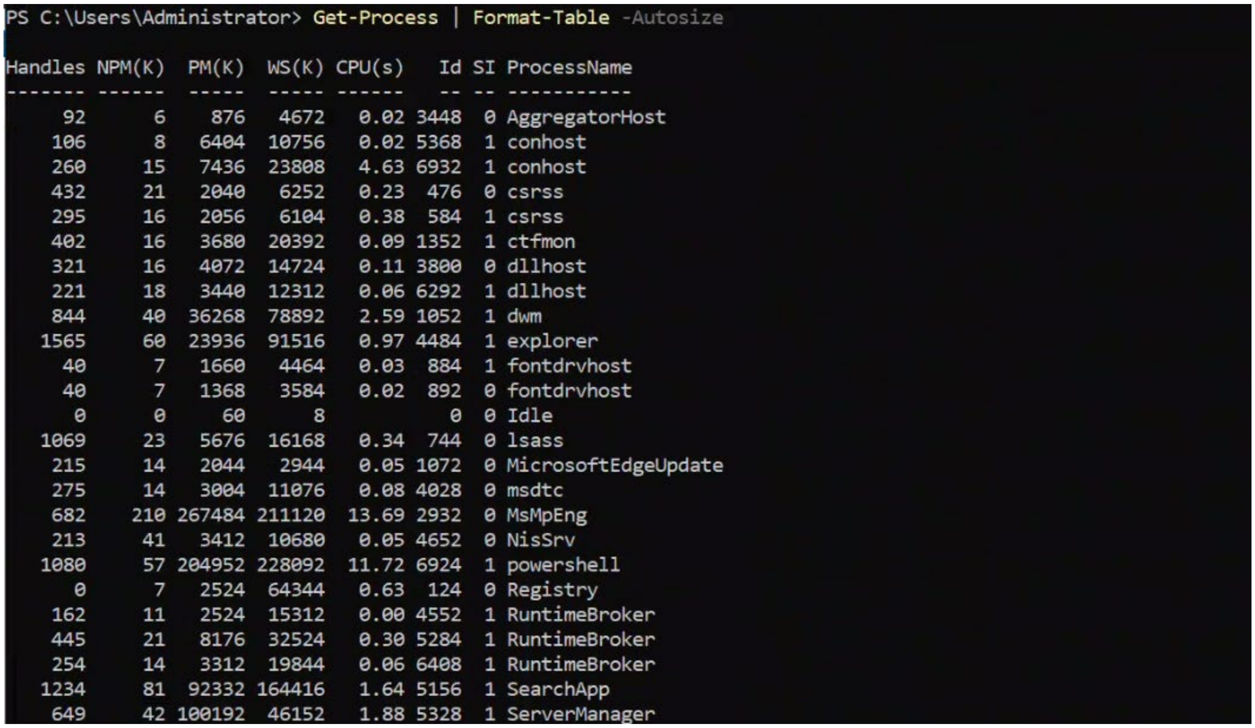
```
PS C:\Users\Administrator> Get-Process

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
     94       6      940       4708       0.02   3448   0 AggregatorHost
    106       8     6364      10644       0.02   5368   1 conhost
    262      15     7436      23616       4.36   6932   1 conhost
    443      21     2104       6284       0.23    476   0 csrss
    300      16     2120       6128       0.20    584   1 csrss
    407      16     3680      20296       0.09   1352   1 ctfmon
    322      16     4072      14728       0.11   3800   0 dllhost
    225      18     3504      12244       0.06   6292   1 dllhost
    844      40    36144      78812       1.59   1052   1 dwm
   1530      59    22984      91296       0.92   4484   1 explorer
     40       8     1736       4508       0.03    884   1 fontdrvhost
     40       7     1444       3628       0.02    892   0 fontdrvhost
      0       0       60          8                 0   0 Idle
   1094      23     5768      16200       0.34    744   0 lsass
    219      15     2116       2560       0.05   1072   0 MicrosoftEdgeUpdate
    275      14     3004      11076       0.08   4028   0 msdtc
    689     210   267440     208592      13.67   2932   0 MsMpEng
    213      42     3620      10720       0.05   4652   0 NisSrv
    992      57   204844     227536      11.53   6924   1 powershell
      0       7     2524      64260       0.63    124   0 Registry
    168      11     2596      15264       0.00   4552   1 RuntimeBroker
    442      21     8096      32392       0.30   5284   1 RuntimeBroker
    260      15     3380      19772       0.06   6408   1 RuntimeBroker
   1234      81    92332     164416       1.64   5156   1 SearchApp
    651      41    97796      89404       1.72   5328   1 ServerManager
```



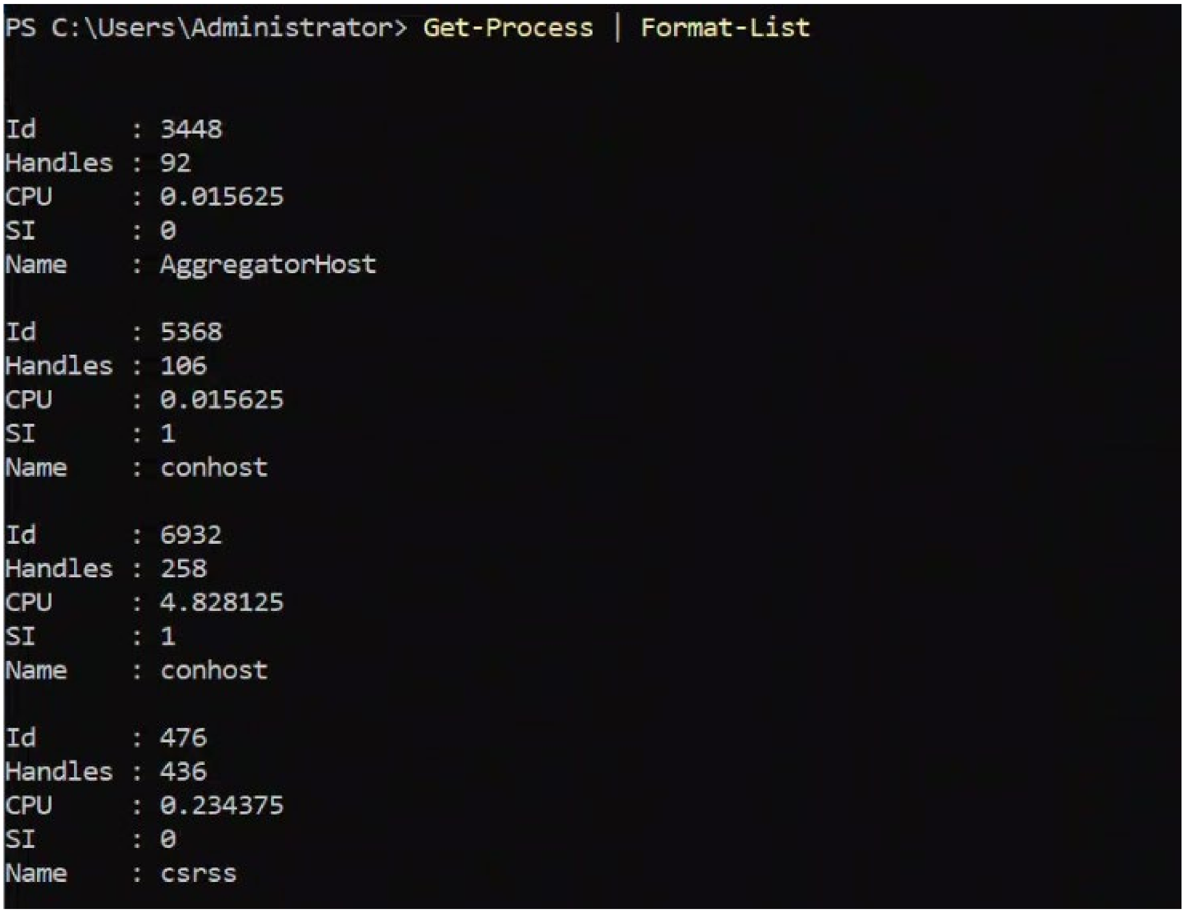
```
PS C:\Users\Administrator> Get-Process ServerManager

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    641      41   103388      30412       2.16   5328   1 ServerManager
```

Task 2: Working with Objects

Display process information in table and list formats

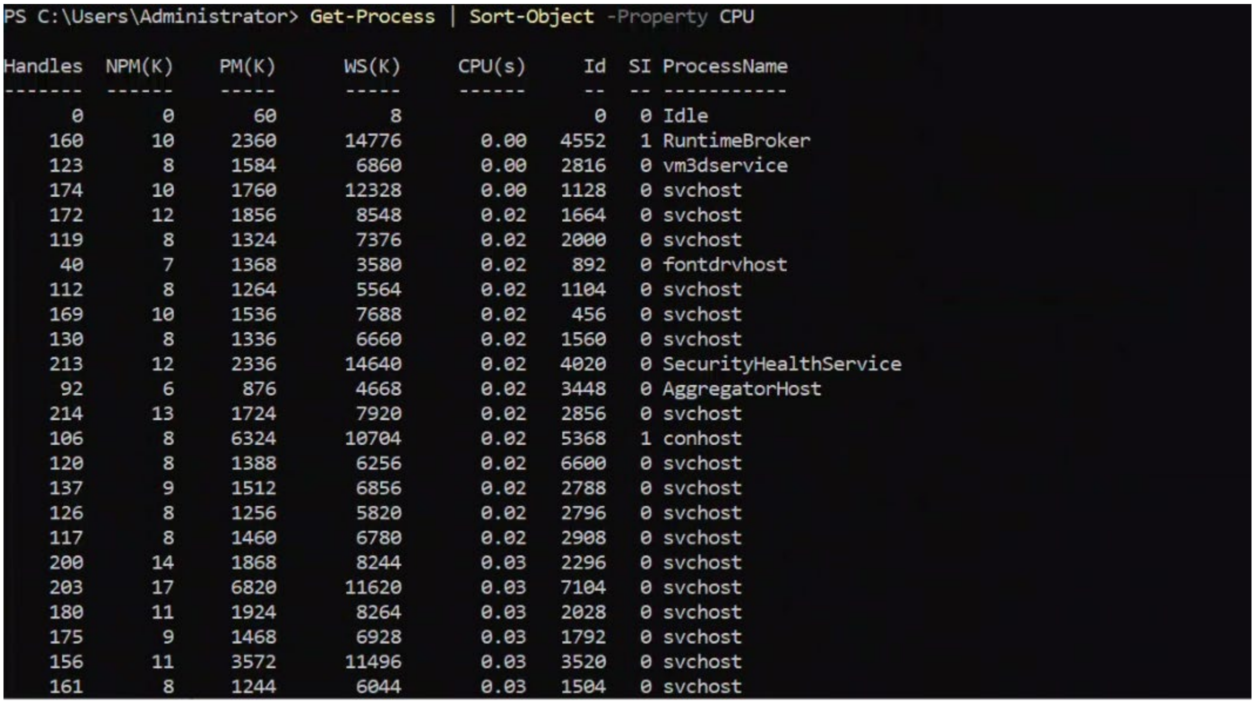


```
PS C:\Users\Administrator> Get-Process | Format-Table -Autosize

Handles NPM(K)  PM(K)  WS(K) CPU(s)   Id SI ProcessName
------- ------  -----  ----- ------   -- -- -----------
     92      6    876   4672   0.02 3448  0 AggregatorHost
    106      8   6404  10756   0.02 5368  1 conhost
    260     15   7436  23808   4.63 6932  1 conhost
    432     21   2040   6252   0.23  476  0 csrss
    295     16   2056   6104   0.38  584  1 csrss
    402     16   3680  20392   0.09 1352  1 ctfmon
    321     16   4072  14724   0.11 3800  0 dllhost
    221     18   3440  12312   0.06 6292  1 dllhost
    844     40  36268  78892   2.59 1052  1 dwm
   1565     60  23936  91516   0.97 4484  1 explorer
     40      7   1660   4464   0.03  884  1 fontdrvhost
     40      7   1368   3584   0.02  892  0 fontdrvhost
      0      0     60      8           0  0 Idle
   1069     23   5676  16168   0.34  744  0 lsass
    215     14   2044   2944   0.05 1072  0 MicrosoftEdgeUpdate
    275     14   3004  11076   0.08 4028  0 msdtc
    682    210 267484 211120  13.69 2932  0 MsMpEng
    213     41   3412  10680   0.05 4652  0 NisSrv
   1080     57 204952 228092  11.72 6924  1 powershell
      0      7   2524  64344   0.63  124  0 Registry
    162     11   2524  15312   0.00 4552  1 RuntimeBroker
    445     21   8176  32524   0.30 5284  1 RuntimeBroker
    254     14   3312  19844   0.06 6408  1 RuntimeBroker
   1234     81  92332 164416   1.64 5156  1 SearchApp
    649     42 100192  46152   1.88 5328  1 ServerManager
```



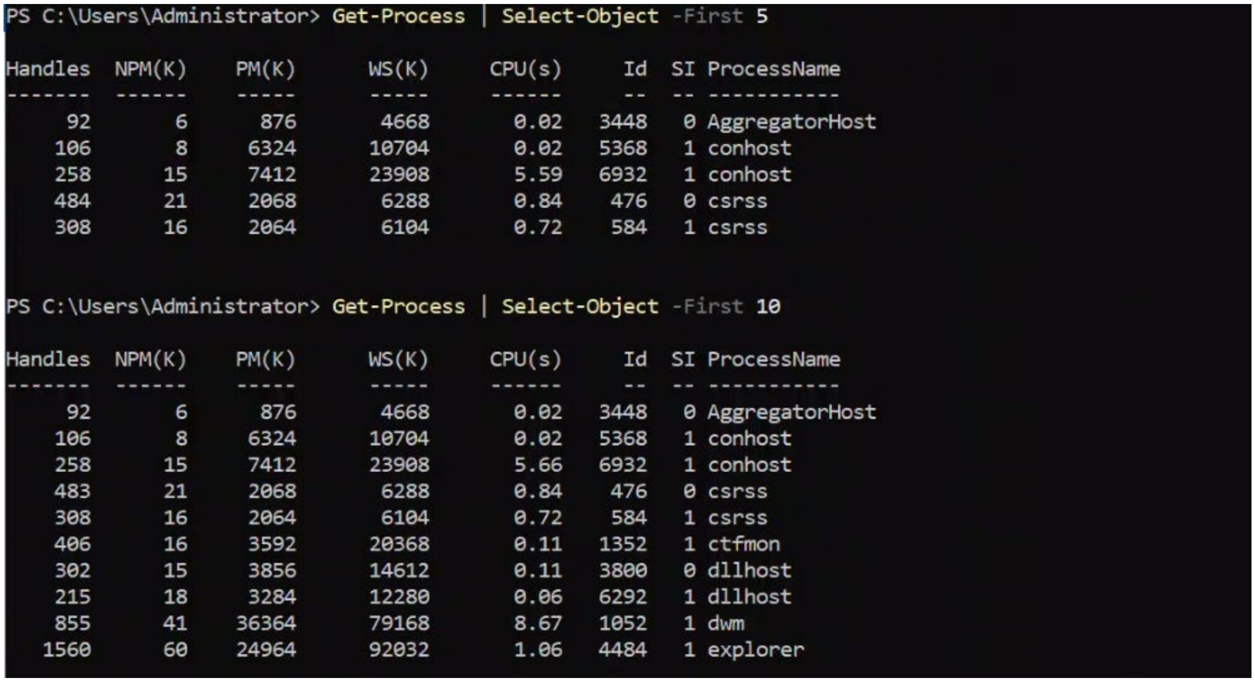
```
PS C:\Users\Administrator> Get-Process | Format-List


Id      : 3448
Handles : 92
CPU     : 0.015625
SI      : 0
Name    : AggregatorHost

Id      : 5368
Handles : 106
CPU     : 0.015625
SI      : 1
Name    : conhost

Id      : 6932
Handles : 258
CPU     : 4.828125
SI      : 1
Name    : conhost

Id      : 476
Handles : 436
CPU     : 0.234375
SI      : 0
Name    : csrss
```

Sort processes based on CPU usage

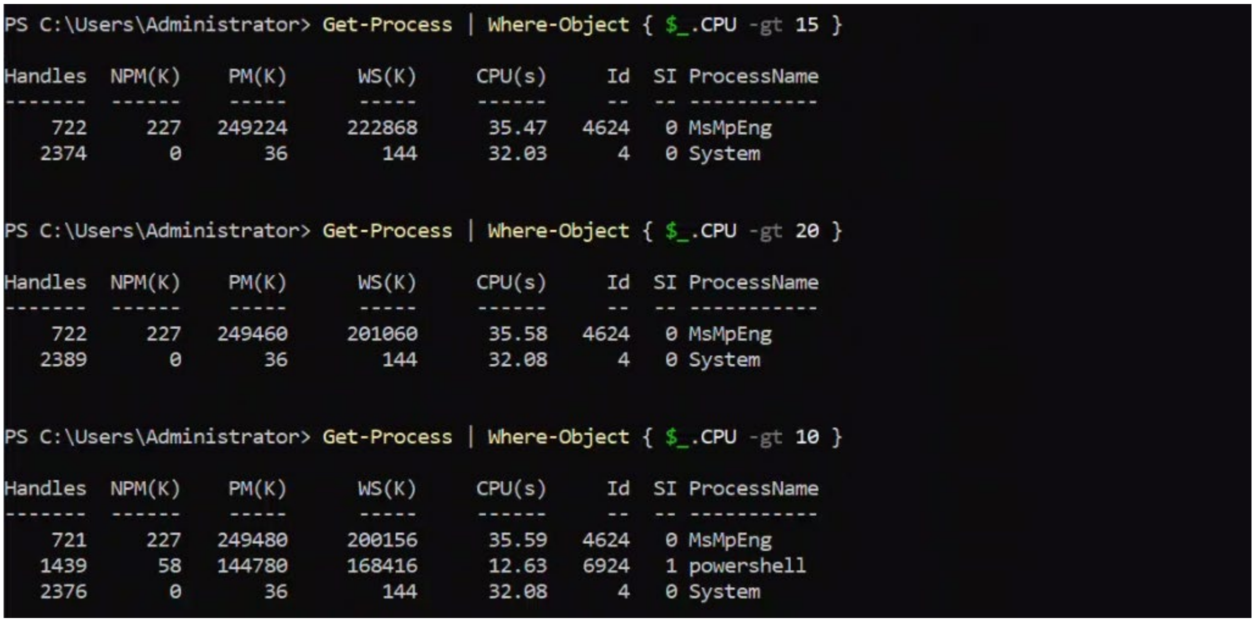


```
PS C:\Users\Administrator> Get-Process | Sort-Object -Property CPU

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
      0       0       60          8                 0   0 Idle
    160      10     2360      14776       0.00   4552   1 RuntimeBroker
    123       8     1584       6860       0.00   2816   0 vm3dservice
    174      10     1760      12328       0.00   1128   0 svchost
    172      12     1856       8548       0.02   1664   0 svchost
    119       8     1324       7376       0.02   2000   0 svchost
     40       7     1368       3580       0.02    892   0 fontdrvhost
    112       8     1264       5564       0.02   1104   0 svchost
    169      10     1536       7688       0.02    456   0 svchost
    130       8     1336       6660       0.02   1560   0 svchost
    213      12     2336      14640       0.02   4020   0 SecurityHealthService
     92       6      876       4668       0.02   3448   0 AggregatorHost
    214      13     1724       7920       0.02   2856   0 svchost
    106       8     6324      10704       0.02   5368   1 conhost
    120       8     1388       6256       0.02   6600   0 svchost
    137       9     1512       6856       0.02   2788   0 svchost
    126       8     1256       5820       0.02   2796   0 svchost
    117       8     1460       6780       0.02   2908   0 svchost
    200      14     1868       8244       0.03   2296   0 svchost
    203      17     6820      11620       0.03   7104   0 svchost
    180      11     1924       8264       0.03   2028   0 svchost
    175       9     1468       6928       0.03   1792   0 svchost
    156      11     3572      11496       0.03   3520   0 svchost
    161       8     1244       6044       0.03   1504   0 svchost
```

Select and filter objects based on specific conditions

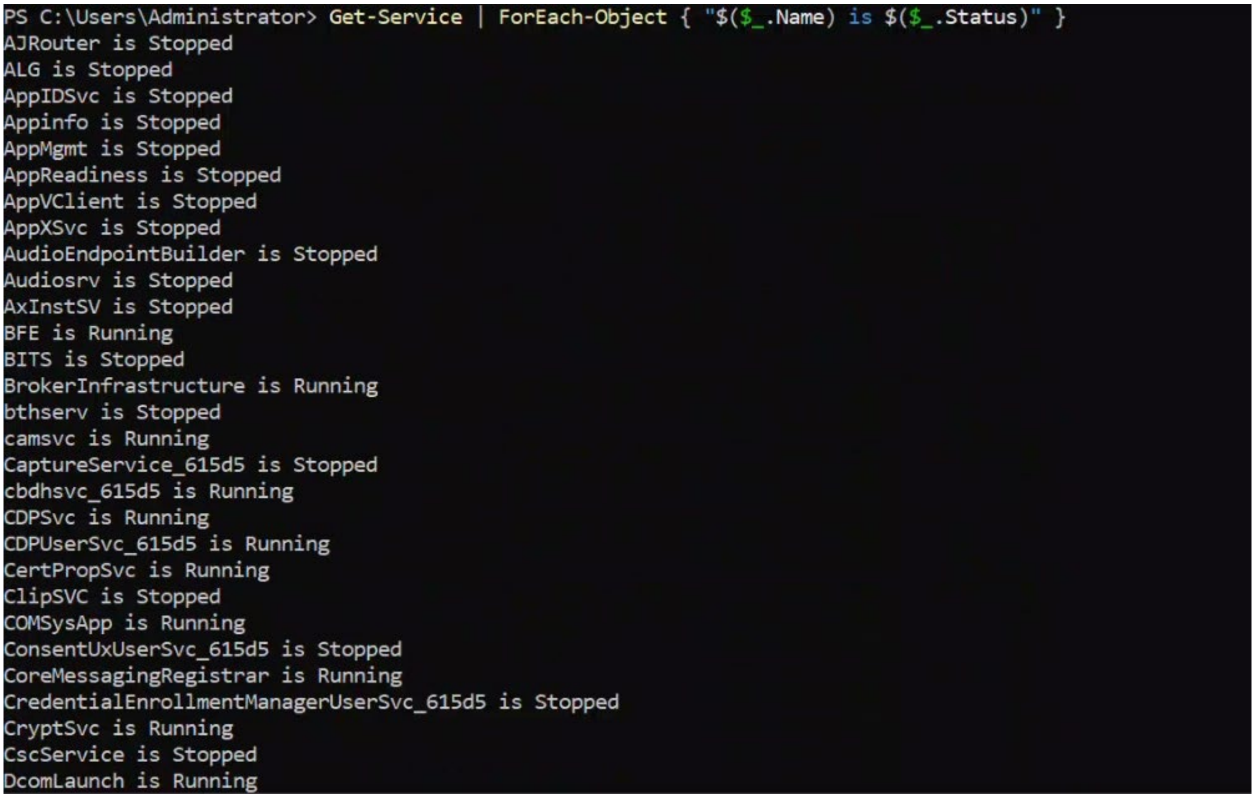


```
PS C:\Users\Administrator> Get-Process | Select-Object -First 5

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
     92       6      876       4668       0.02   3448   0 AggregatorHost
    106       8     6324      10704       0.02   5368   1 conhost
    258      15     7412      23908       5.59   6932   1 conhost
    484      21     2068       6288       0.84    476   0 csrss
    308      16     2064       6104       0.72    584   1 csrss


PS C:\Users\Administrator> Get-Process | Select-Object -First 10

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
     92       6      876       4668       0.02   3448   0 AggregatorHost
    106       8     6324      10704       0.02   5368   1 conhost
    258      15     7412      23908       5.66   6932   1 conhost
    483      21     2068       6288       0.84    476   0 csrss
    308      16     2064       6104       0.72    584   1 csrss
    406      16     3592      20368       0.11   1352   1 ctfmon
    302      15     3856      14612       0.11   3800   0 dllhost
    215      18     3284      12280       0.06   6292   1 dllhost
    855      41    36364      79168       8.67   1052   1 dwm
   1560      60    24964      92032       1.06   4484   1 explorer
```



```
PS C:\Users\Administrator> Get-Process | Where-Object { $_.CPU -gt 15 }

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    722     227   249224     222868      35.47   4624   0 MsMpEng
   2374       0       36        144      32.03      4   0 System


PS C:\Users\Administrator> Get-Process | Where-Object { $_.CPU -gt 20 }

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    722     227   249460     201060      35.58   4624   0 MsMpEng
   2389       0       36        144      32.08      4   0 System


PS C:\Users\Administrator> Get-Process | Where-Object { $_.CPU -gt 10 }

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
    721     227   249480     200156      35.59   4624   0 MsMpEng
   1439      58   144780     168416      12.63   6924   1 powershell
   2376       0       36        144      32.08      4   0 System
```

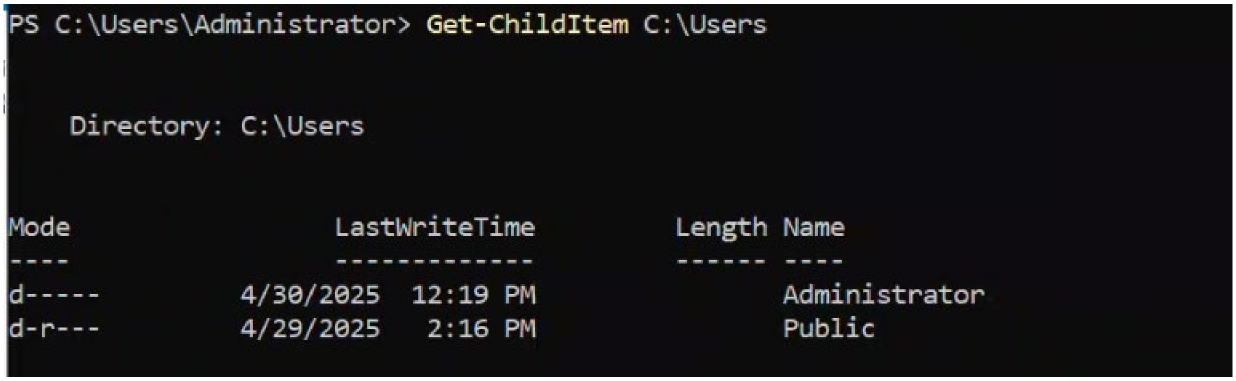
Loop through system objects and extract specific information



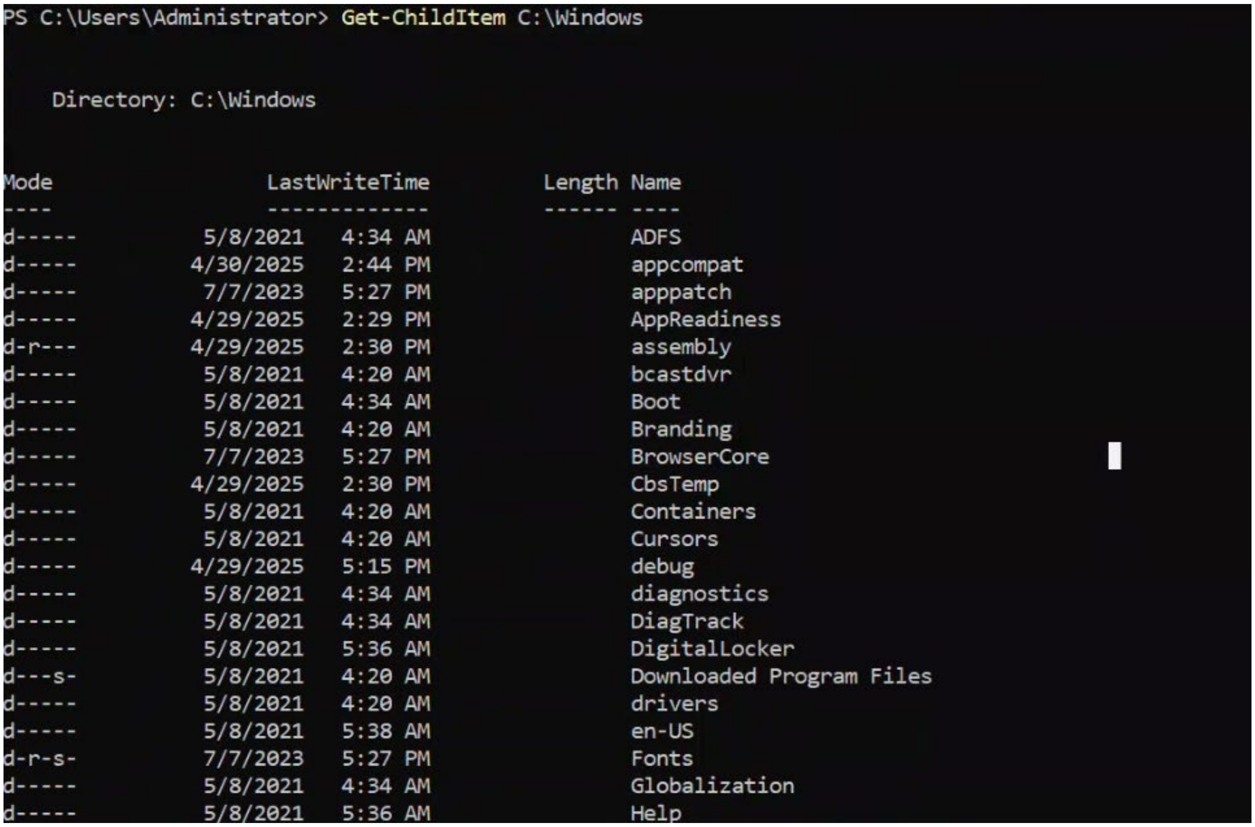
```
PS C:\Users\Administrator> Get-Service | ForEach-Object { "$($_.Name) is $($_.Status)" }
AJRouter is Stopped
ALG is Stopped
AppIDSvc is Stopped
Appinfo is Stopped
AppMgmt is Stopped
AppReadiness is Stopped
AppVClient is Stopped
AppXSvc is Stopped
AudioEndpointBuilder is Stopped
Audiosrv is Stopped
AxInstSV is Stopped
BFE is Running
BITS is Stopped
BrokerInfrastructure is Running
bthserv is Stopped
camsvc is Running
CaptureService_615d5 is Stopped
cbdhsvc_615d5 is Running
CDPSvc is Running
CDPUserSvc_615d5 is Running
CertPropSvc is Running
ClipSVC is Stopped
COMSysApp is Running
ConsentUxUserSvc_615d5 is Stopped
CoreMessagingRegistrar is Running
CredentialEnrollmentManagerUserSvc_615d5 is Stopped
CryptSvc is Running
CscService is Stopped
DcomLaunch is Running
```

Task 3: Managing the File System

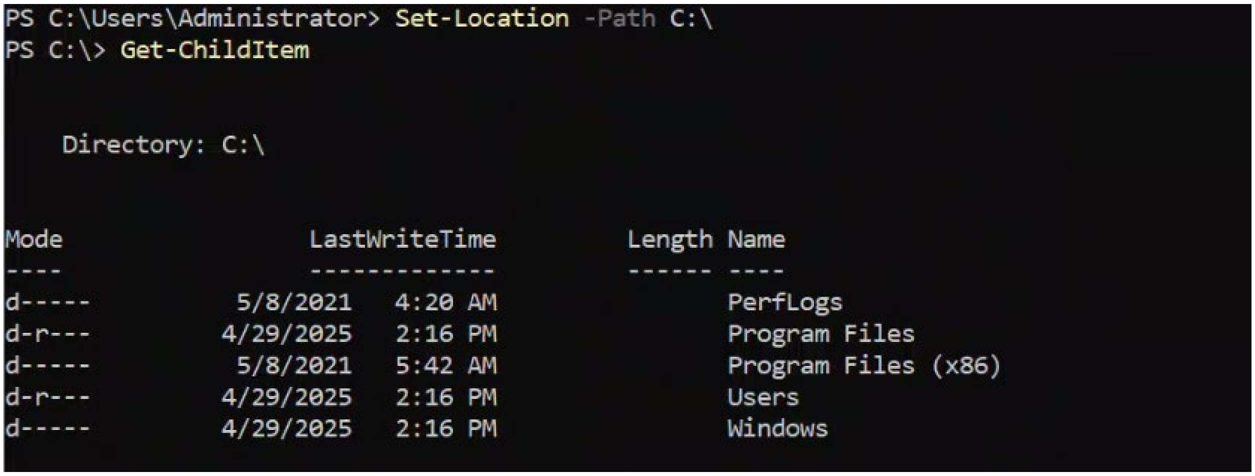
Navigate through directories and list files



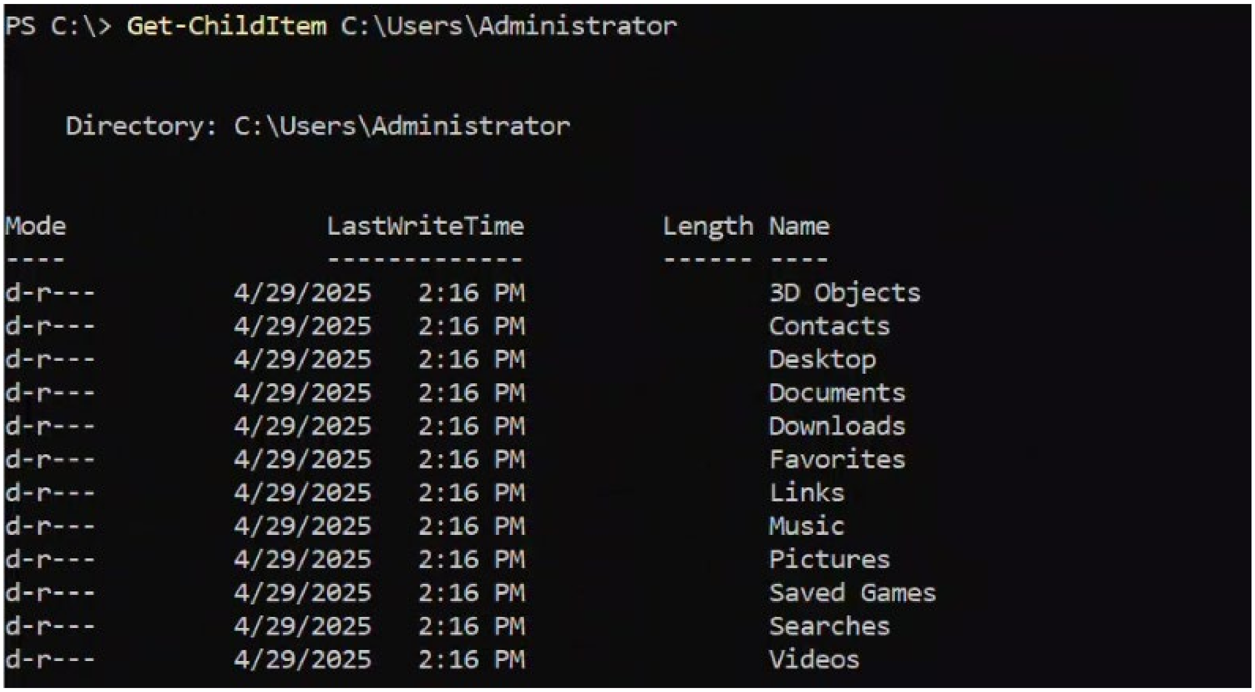
```
PS C:\Users\Administrator> Get-ChildItem C:\Users


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         4/30/2025  12:19 PM                Administrator
d-r---         4/29/2025   2:16 PM                Public
```



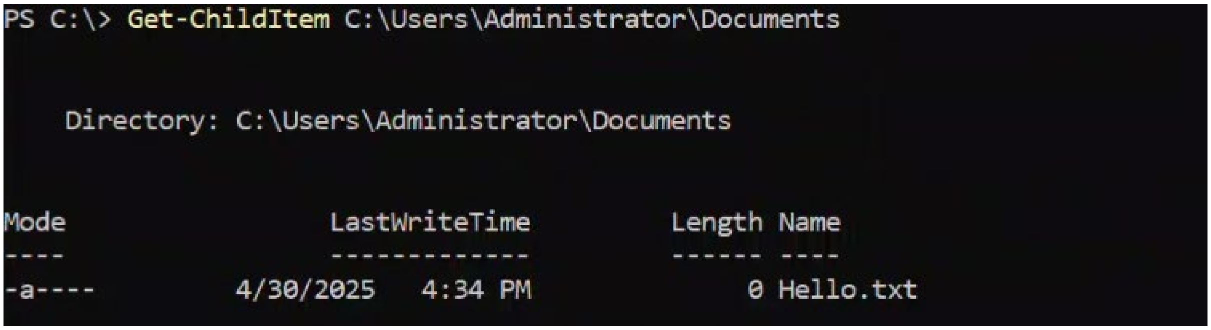
```
PS C:\Users\Administrator> Get-ChildItem C:\Windows


    Directory: C:\Windows


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          5/8/2021   4:34 AM                ADFS
d-----         4/30/2025   2:44 PM                appcompat
d-----          7/7/2023   5:27 PM                apppatch
d-----         4/29/2025   2:29 PM                AppReadiness
d-r---         4/29/2025   2:30 PM                assembly
d-----          5/8/2021   4:20 AM                bcastdvr
d-----          5/8/2021   4:34 AM                Boot
d-----          5/8/2021   4:20 AM                Branding
d-----          7/7/2023   5:27 PM                BrowserCore
d-----         4/29/2025   2:30 PM                CbsTemp
d-----          5/8/2021   4:20 AM                Containers
d-----          5/8/2021   4:20 AM                Cursors
d-----         4/29/2025   5:15 PM                debug
d-----          5/8/2021   4:34 AM                diagnostics
d-----          5/8/2021   4:34 AM                DiagTrack
d-----          5/8/2021   5:36 AM                DigitalLocker
d---s-          5/8/2021   4:20 AM                Downloaded Program Files
d-----          5/8/2021   4:20 AM                drivers
d-----          5/8/2021   5:38 AM                en-US
d-r-s-          7/7/2023   5:27 PM                Fonts
d-----          5/8/2021   4:34 AM                Globalization
d-----          5/8/2021   5:36 AM                Help
```



```
PS C:\Users\Administrator> Set-Location -Path C:\
PS C:\> Get-ChildItem


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          5/8/2021   4:20 AM                PerfLogs
d-r---         4/29/2025   2:16 PM                Program Files
d-----          5/8/2021   5:42 AM                Program Files (x86)
d-r---         4/29/2025   2:16 PM                Users
d-----         4/29/2025   2:16 PM                Windows
```

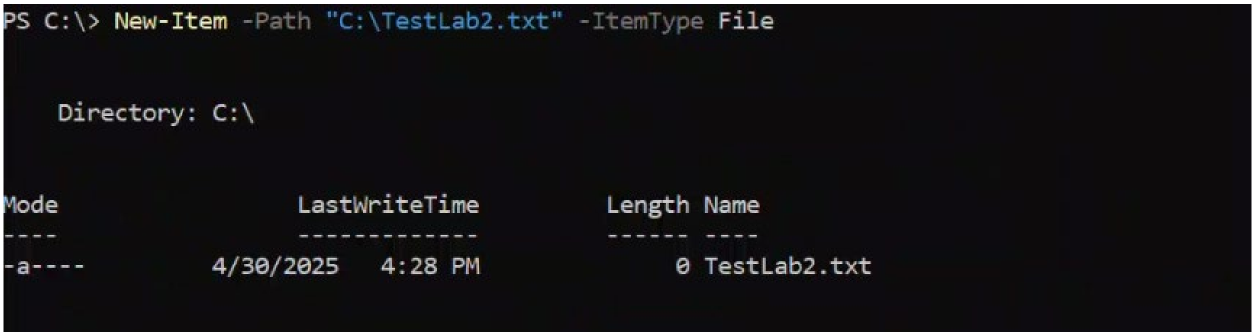


```
PS C:\> Get-ChildItem C:\Users\Administrator


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         4/29/2025   2:16 PM                3D Objects
d-r---         4/29/2025   2:16 PM                Contacts
d-r---         4/29/2025   2:16 PM                Desktop
d-r---         4/29/2025   2:16 PM                Documents
d-r---         4/29/2025   2:16 PM                Downloads
d-r---         4/29/2025   2:16 PM                Favorites
d-r---         4/29/2025   2:16 PM                Links
d-r---         4/29/2025   2:16 PM                Music
d-r---         4/29/2025   2:16 PM                Pictures
d-r---         4/29/2025   2:16 PM                Saved Games
d-r---         4/29/2025   2:16 PM                Searches
d-r---         4/29/2025   2:16 PM                Videos
```

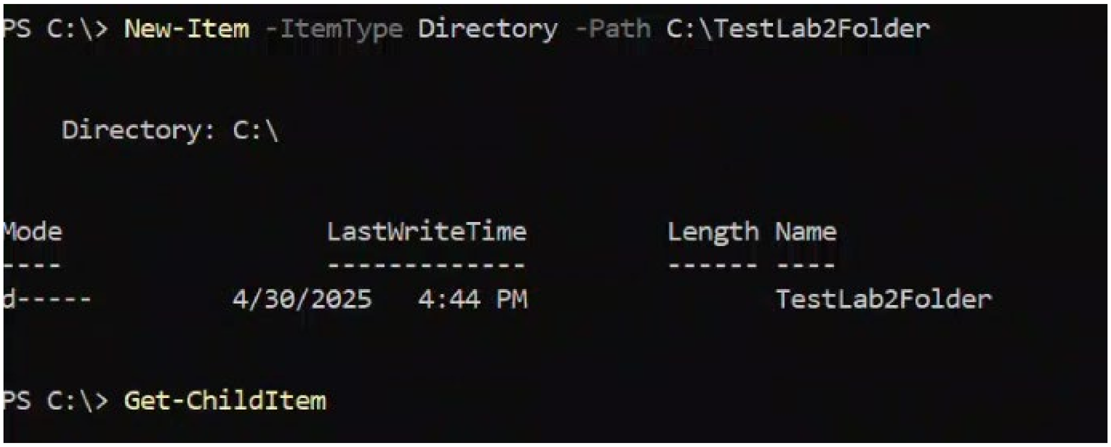


```
PS C:\> Get-ChildItem C:\Users\Administrator\Documents


    Directory: C:\Users\Administrator\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/30/2025   4:34 PM              0 Hello.txt
```

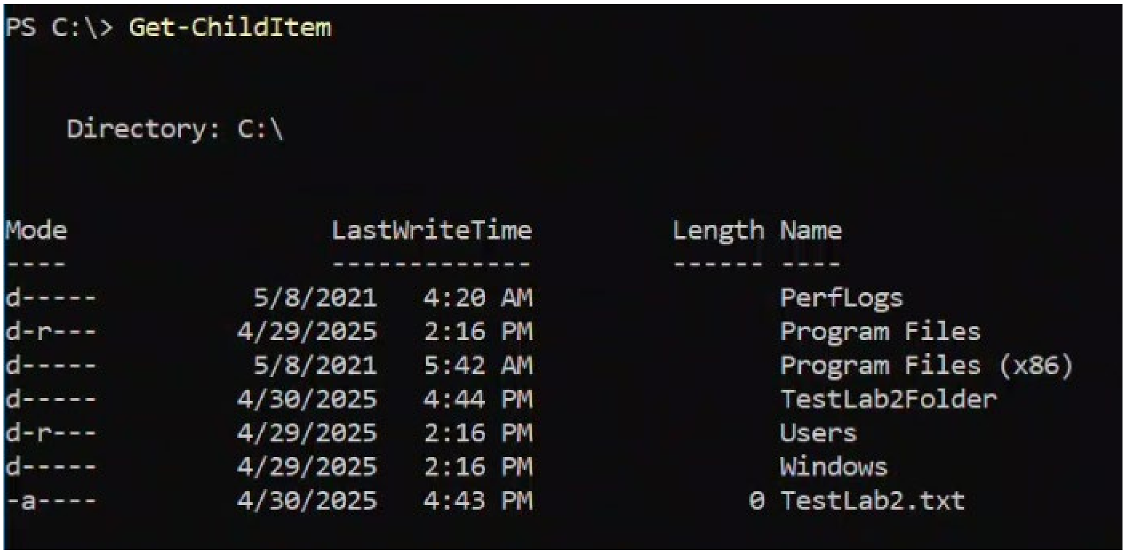
Create and delete files and folders



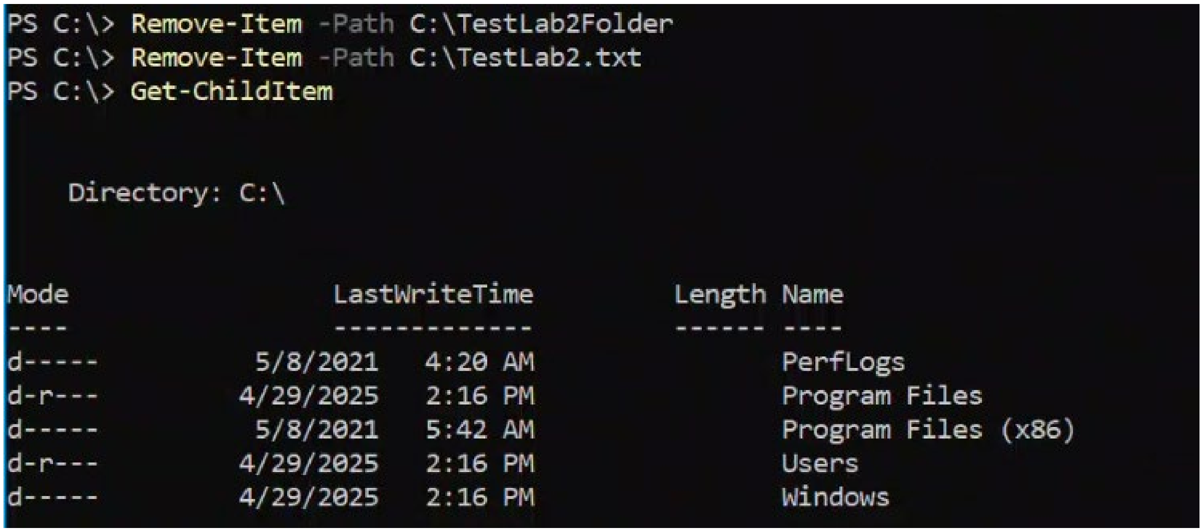
```
PS C:\> New-Item -Path "C:\TestLab2.txt" -ItemType File


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/30/2025   4:28 PM              0 TestLab2.txt
```



```
PS C:\> New-Item -ItemType Directory -Path C:\TestLab2Folder


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         4/30/2025   4:44 PM                TestLab2Folder


PS C:\> Get-ChildItem
```

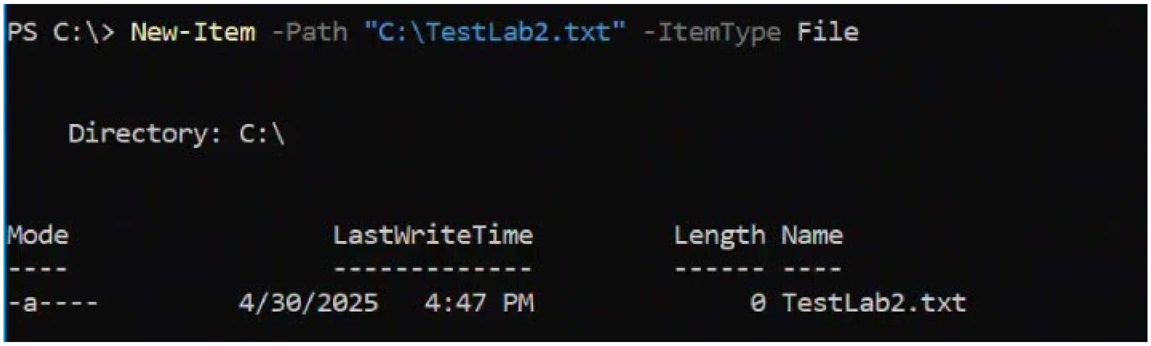


```
PS C:\> Get-ChildItem


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          5/8/2021   4:20 AM                PerfLogs
d-r---         4/29/2025   2:16 PM                Program Files
d-----          5/8/2021   5:42 AM                Program Files (x86)
d-----         4/30/2025   4:44 PM                TestLab2Folder
d-r---         4/29/2025   2:16 PM                Users
d-----         4/29/2025   2:16 PM                Windows
-a----         4/30/2025   4:43 PM              0 TestLab2.txt
```

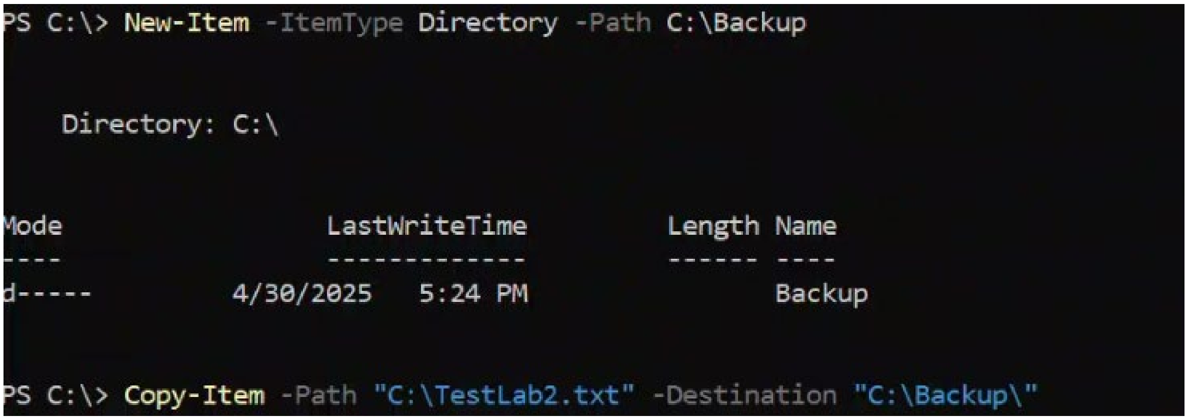


```
PS C:\> Remove-Item -Path C:\TestLab2Folder
PS C:\> Remove-Item -Path C:\TestLab2.txt
PS C:\> Get-ChildItem


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          5/8/2021   4:20 AM                PerfLogs
d-r---         4/29/2025   2:16 PM                Program Files
d-----          5/8/2021   5:42 AM                Program Files (x86)
d-r---         4/29/2025   2:16 PM                Users
d-----         4/29/2025   2:16 PM                Windows
```

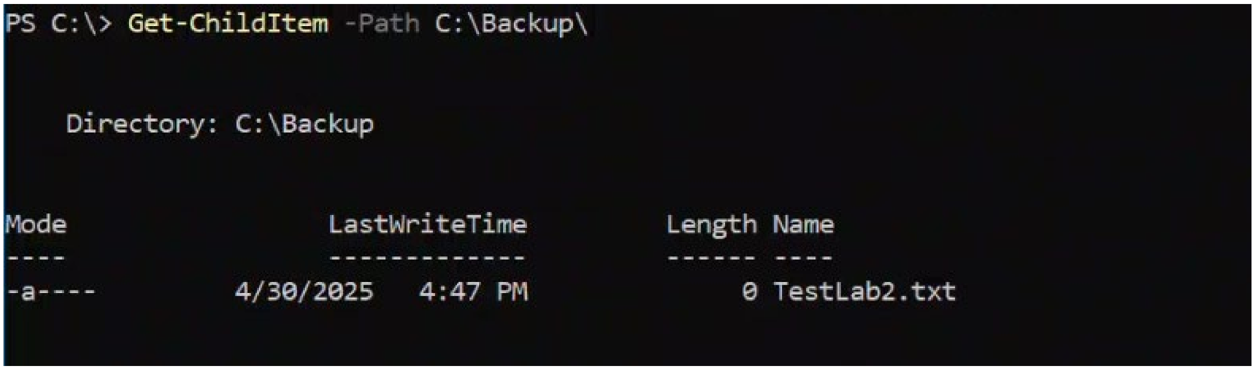
Copy and move files between locations



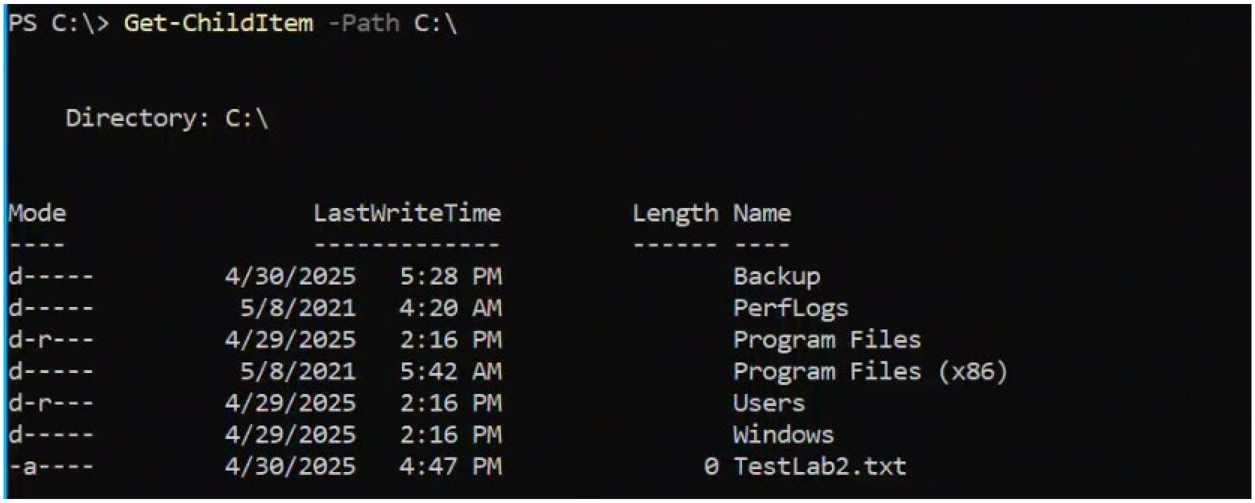
```
PS C:\> New-Item -Path "C:\TestLab2.txt" -ItemType File


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/30/2025   4:47 PM              0 TestLab2.txt
```



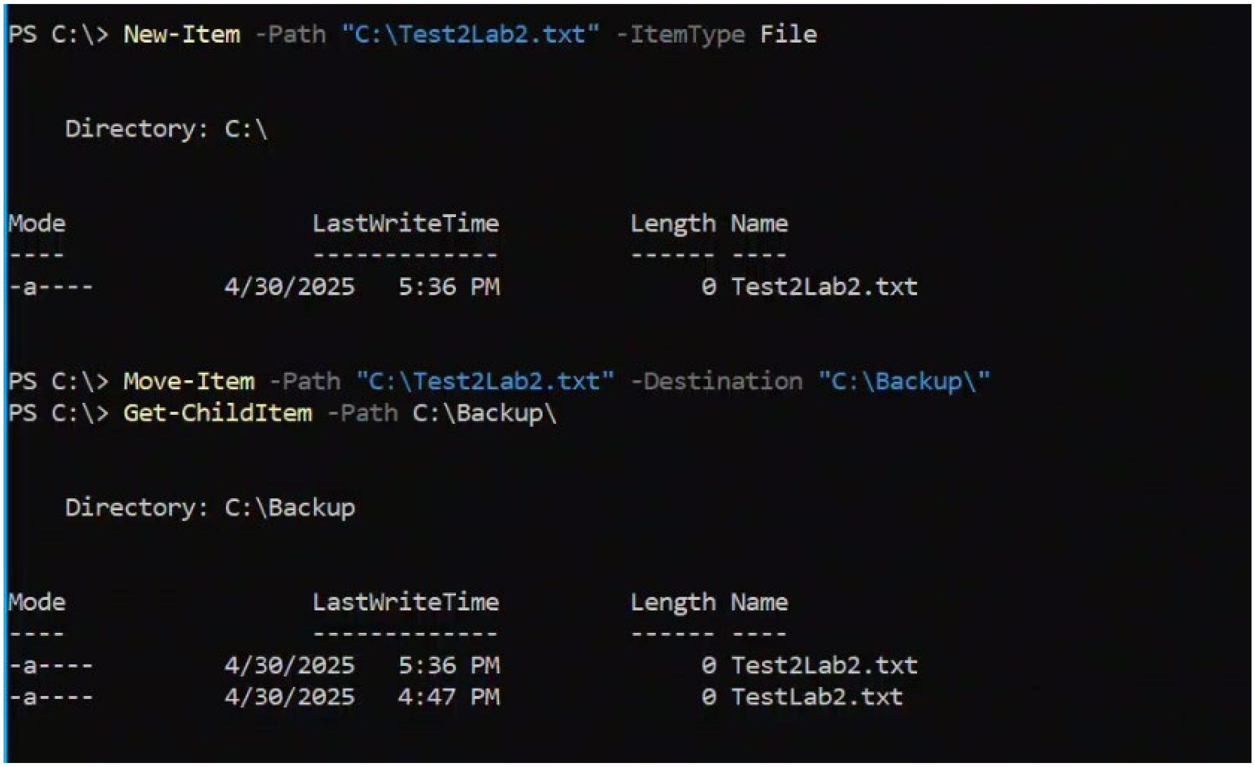
```
PS C:\> New-Item -ItemType Directory -Path C:\Backup


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         4/30/2025   5:24 PM                Backup


PS C:\> Copy-Item -Path "C:\TestLab2.txt" -Destination "C:\Backup\"
```



```
PS C:\> Get-ChildItem -Path C:\Backup\


    Directory: C:\Backup


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/30/2025   4:47 PM              0 TestLab2.txt
```

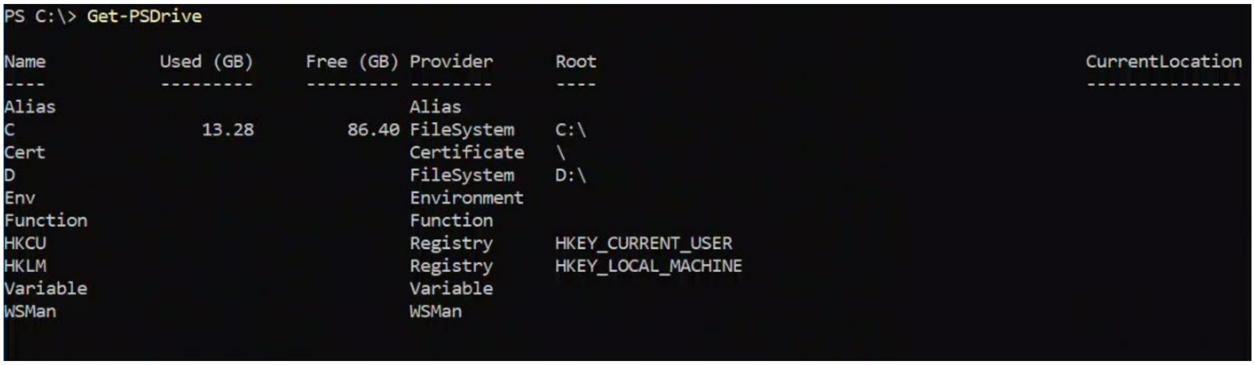


```
PS C:\> Get-ChildItem -Path C:\


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         4/30/2025   5:28 PM                Backup
d-----          5/8/2021   4:20 AM                PerfLogs
d-r---         4/29/2025   2:16 PM                Program Files
d-----          5/8/2021   5:42 AM                Program Files (x86)
d-r---         4/29/2025   2:16 PM                Users
d-----         4/29/2025   2:16 PM                Windows
-a----         4/30/2025   4:47 PM              0 TestLab2.txt
```



```
PS C:\> New-Item -Path "C:\Test2Lab2.txt" -ItemType File


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/30/2025   5:36 PM              0 Test2Lab2.txt


PS C:\> Move-Item -Path "C:\Test2Lab2.txt" -Destination "C:\Backup\"
PS C:\> Get-ChildItem -Path C:\Backup\


    Directory: C:\Backup


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/30/2025   5:36 PM              0 Test2Lab2.txt
-a----         4/30/2025   4:47 PM              0 TestLab2.txt
```

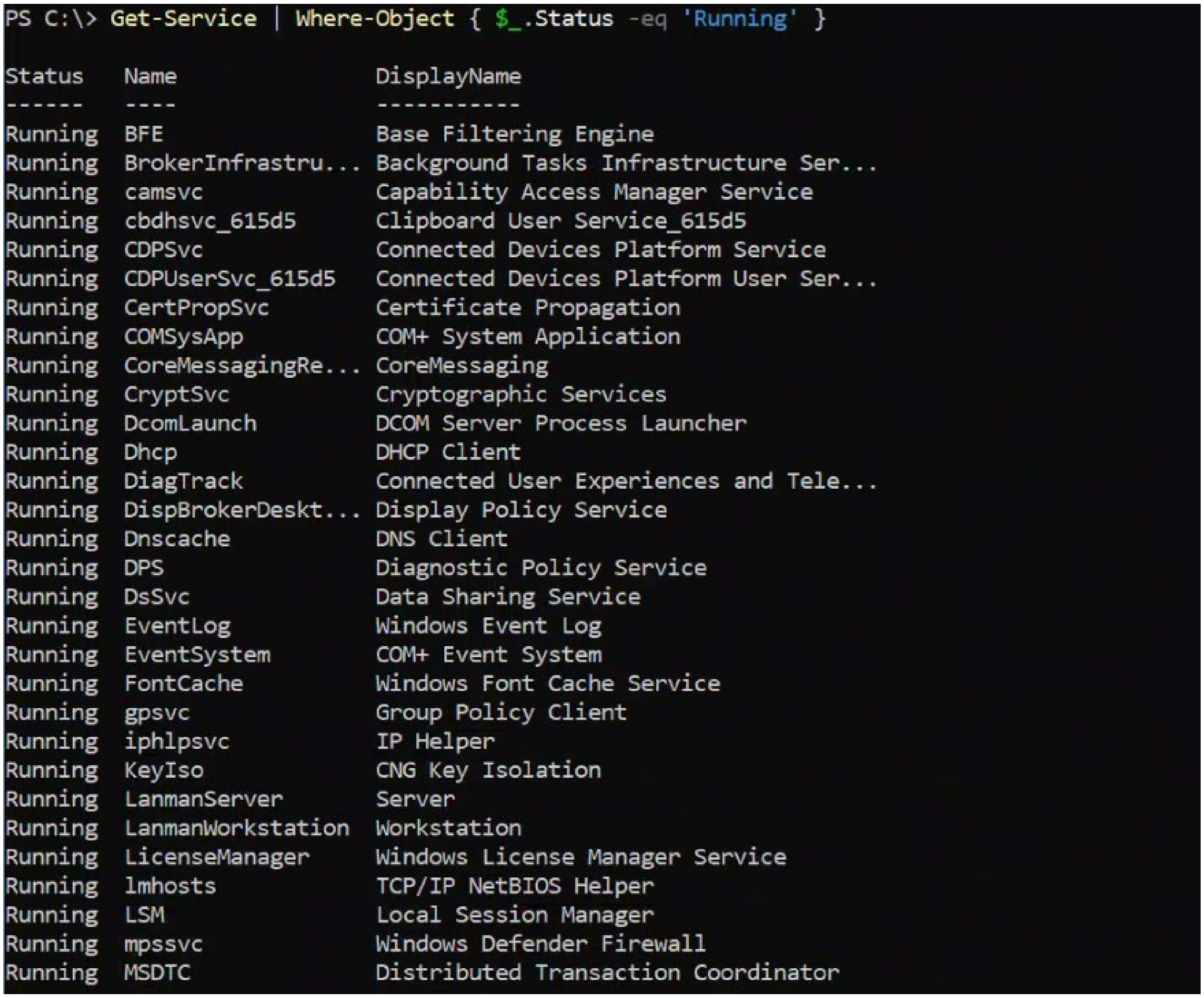
Check available disk space



```
PS C:\> Get-PSDrive

Name           Used (GB)     Free (GB) Provider      Root                                               CurrentLocation
----           ---------     --------- --------      ----                                               ---------------
Alias                                  Alias
C                  13.28         86.40 FileSystem    C:\
Cert                                   Certificate   \
D                                      FileSystem    D:\
Env                                    Environment
Function                               Function
HKCU                                   Registry      HKEY_CURRENT_USER
HKLM                                   Registry      HKEY_LOCAL_MACHINE
Variable                               Variable
WSMan                                  WSMan
```

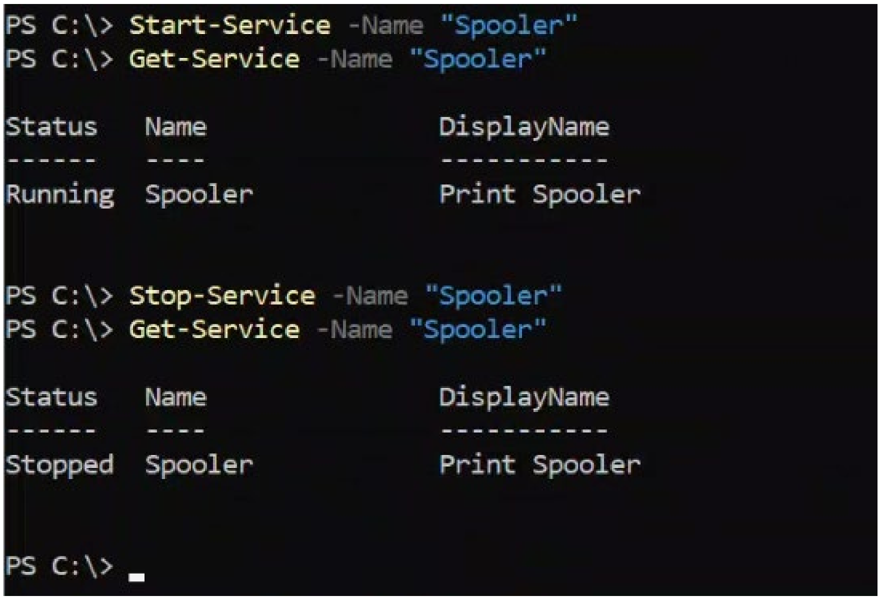
Task 4: Managing System Services and Processes

List all running services on the system



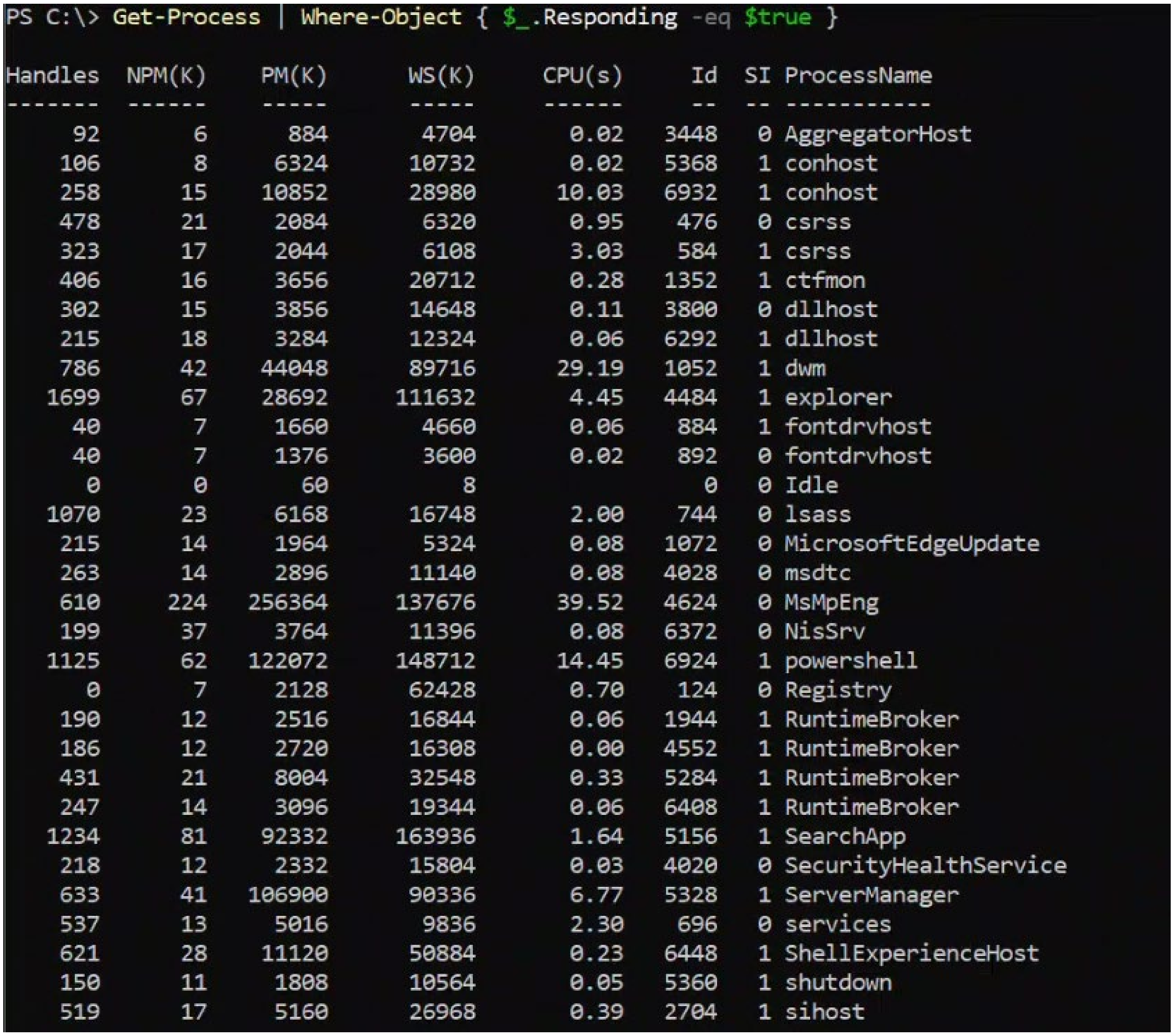
```
PS C:\> Get-Service | Where-Object { $_.Status -eq 'Running' }

Status   Name               DisplayName
------   ----               -----------
Running  BFE                Base Filtering Engine
Running  BrokerInfrastru... Background Tasks Infrastructure Ser...
Running  camsvc             Capability Access Manager Service
Running  cbdhsvc_615d5      Clipboard User Service_615d5
Running  CDPSvc             Connected Devices Platform Service
Running  CDPUserSvc_615d5   Connected Devices Platform User Ser...
Running  CertPropSvc        Certificate Propagation
Running  COMSysApp          COM+ System Application
Running  CoreMessagingRe... CoreMessaging
Running  CryptSvc           Cryptographic Services
Running  DcomLaunch         DCOM Server Process Launcher
Running  Dhcp               DHCP Client
Running  DiagTrack          Connected User Experiences and Tele...
Running  DispBrokerDeskt... Display Policy Service
Running  Dnscache           DNS Client
Running  DPS                Diagnostic Policy Service
Running  DsSvc              Data Sharing Service
Running  EventLog           Windows Event Log
Running  EventSystem        COM+ Event System
Running  FontCache          Windows Font Cache Service
Running  gpsvc              Group Policy Client
Running  iphlpsvc           IP Helper
Running  KeyIso             CNG Key Isolation
Running  LanmanServer       Server
Running  LanmanWorkstation  Workstation
Running  LicenseManager     Windows License Manager Service
Running  lmhosts            TCP/IP NetBIOS Helper
Running  LSM                Local Session Manager
Running  mpssvc             Windows Defender Firewall
Running  MSDTC              Distributed Transaction Coordinator
```

Start and stop specific services

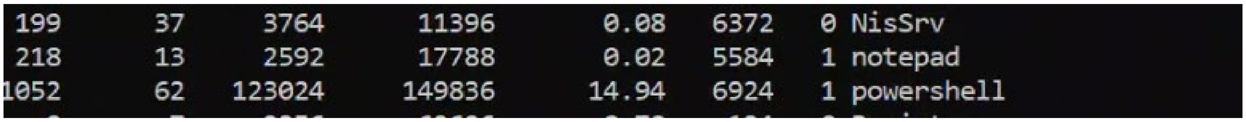


```
PS C:\> Start-Service -Name "Spooler"
PS C:\> Get-Service -Name "Spooler"

Status   Name               DisplayName
------   ----               -----------
Running  Spooler            Print Spooler


PS C:\> Stop-Service -Name "Spooler"
PS C:\> Get-Service -Name "Spooler"

Status   Name               DisplayName
------   ----               -----------
Stopped  Spooler            Print Spooler


PS C:\> _
```

Retrieve information about active processes.

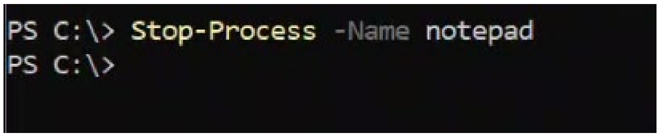


```
PS C:\> Get-Process | Where-Object { $_.Responding -eq $true }

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)     Id  SI ProcessName
-------  ------    -----      -----     ------     --  -- -----------
     92       6      884       4704       0.02   3448   0 AggregatorHost
    106       8     6324      10732       0.02   5368   1 conhost
    258      15    10852      28980      10.03   6932   1 conhost
    478      21     2084       6320       0.95    476   0 csrss
    323      17     2044       6108       3.03    584   1 csrss
    406      16     3656      20712       0.28   1352   1 ctfmon
    302      15     3856      14648       0.11   3800   0 dllhost
    215      18     3284      12324       0.06   6292   1 dllhost
    786      42    44048      89716      29.19   1052   1 dwm
   1699      67    28692     111632       4.45   4484   1 explorer
     40       7     1660       4660       0.06    884   1 fontdrvhost
     40       7     1376       3600       0.02    892   0 fontdrvhost
      0       0       60          8                 0   0 Idle
   1070      23     6168      16748       2.00    744   0 lsass
    215      14     1964       5324       0.08   1072   0 MicrosoftEdgeUpdate
    263      14     2896      11140       0.08   4028   0 msdtc
    610     224   256364     137676      39.52   4624   0 MsMpEng
    199      37     3764      11396       0.08   6372   0 NisSrv
   1125      62   122072     148712      14.45   6924   1 powershell
      0       7     2128      62428       0.70    124   0 Registry
    190      12     2516      16844       0.06   1944   1 RuntimeBroker
    186      12     2720      16308       0.00   4552   1 RuntimeBroker
    431      21     8004      32548       0.33   5284   1 RuntimeBroker
    247      14     3096      19344       0.06   6408   1 RuntimeBroker
   1234      81    92332     163936       1.64   5156   1 SearchApp
    218      12     2332      15804       0.03   4020   0 SecurityHealthService
    633      41   106900      90336       6.77   5328   1 ServerManager
    537      13     5016       9836       2.30    696   0 services
    621      28    11120      50884       0.23   6448   1 ShellExperienceHost
    150      11     1808      10564       0.05   5360   1 shutdown
    519      17     5160      26968       0.39   2704   1 sihost
```

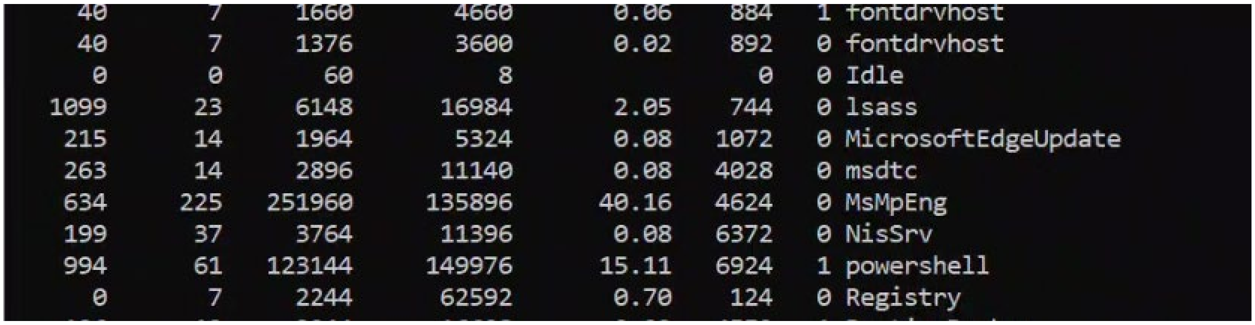


```
 199      37      3764      11396       0.08    6372   0 NisSrv
 218      13      2592      17788       0.02    5584   1 notepad
1052      62    123024     149836      14.94    6924   1 powershell
```

Terminate a process



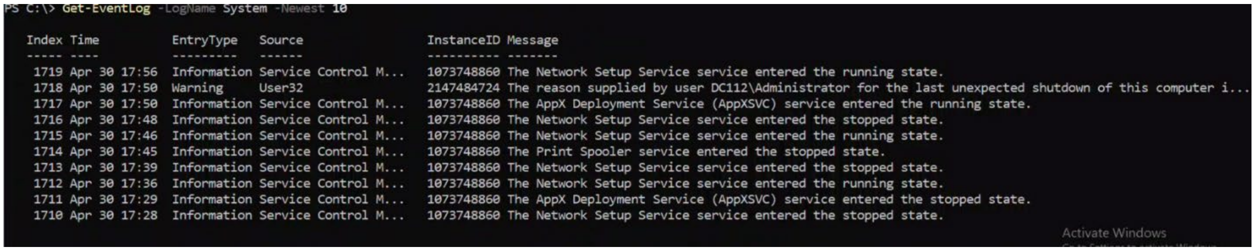
```
PS C:\> Stop-Process -Name notepad
PS C:\>
```



```
     40       7     1660      4660       0.06    884   1 fontdrvhost
     40       7     1376      3600       0.02    892   0 fontdrvhost
      0       0       60         8                 0   0 Idle
   1099      23     6148     16984       2.05    744   0 lsass
    215      14     1964      5324       0.08   1072   0 MicrosoftEdgeUpdate
    263      14     2896     11140       0.08   4028   0 msdtc
    634     225   251960    135896      40.16   4624   0 MsMpEng
    199      37     3764     11396       0.08   6372   0 NisSrv
    994      61   123144    149976      15.11   6924   1 powershell
      0       7     2244     62592       0.70    124   0 Registry
```

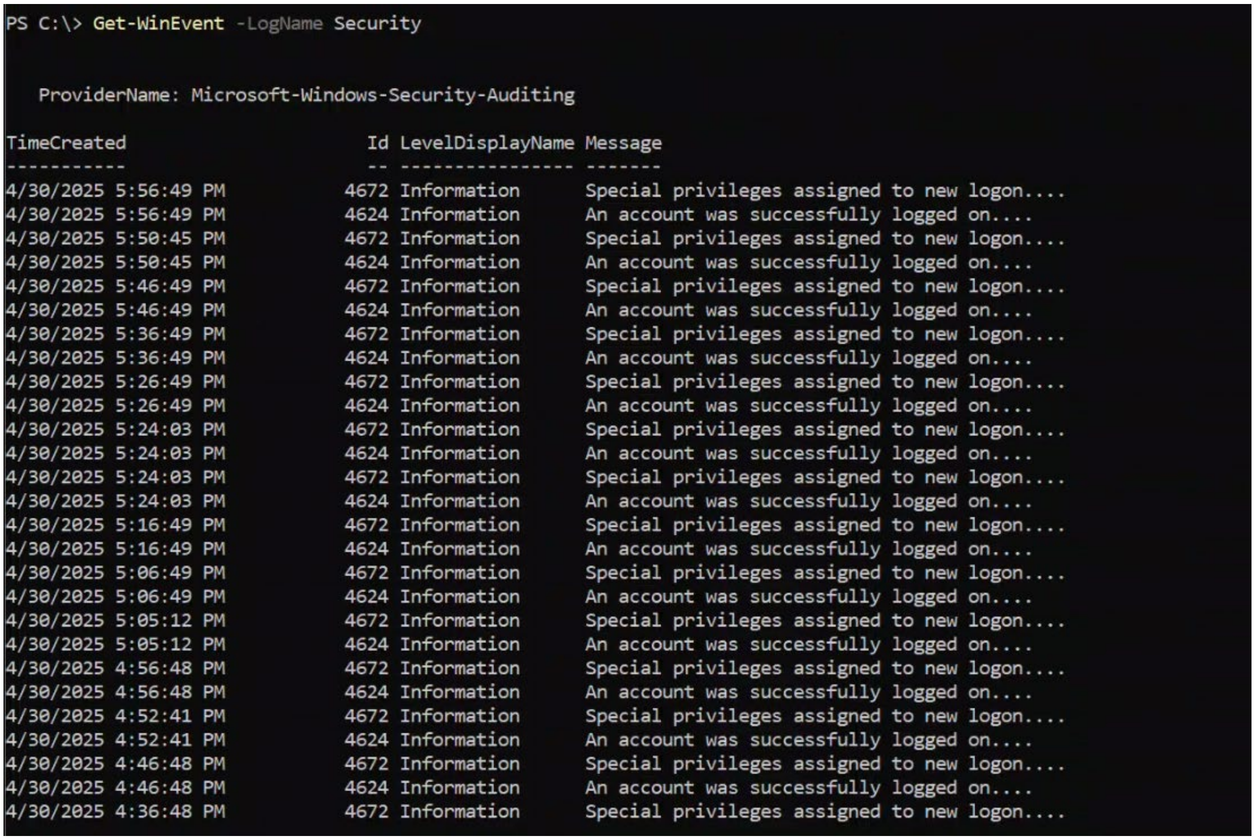
Task 5: Monitoring Event Logs and System Information

View the latest system event logs



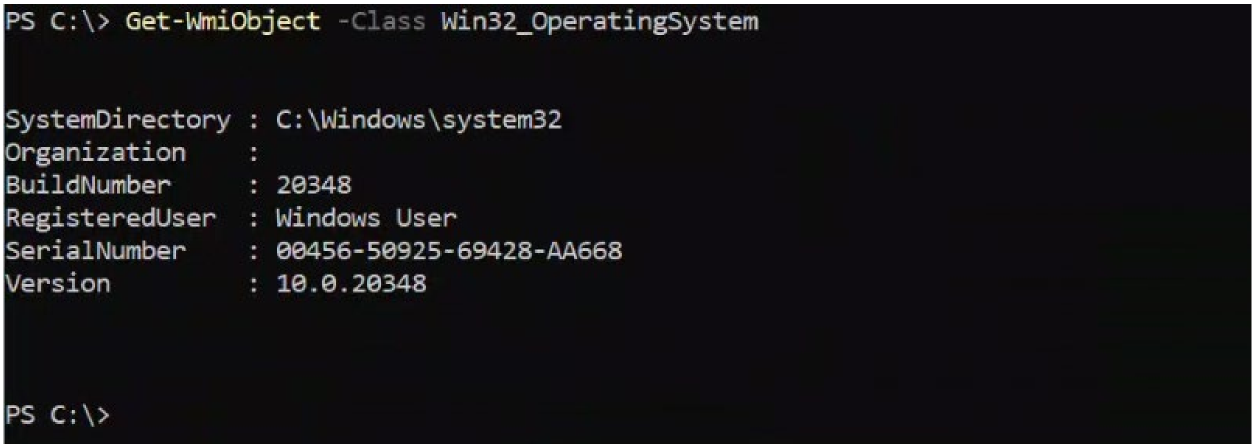
```
PS C:\> Get-EventLog -LogName System -Newest 10

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
    1719 Apr 30 17:56  Information Service Control M...   1073748860 The Network Setup Service service entered the running state.
    1718 Apr 30 17:50  Warning     User32                 2147484724 The reason supplied by user DC112\Administrator for the last unexpected shutdown of this computer i...
    1717 Apr 30 17:50  Information Service Control M...   1073748860 The AppX Deployment Service (AppXSVC) service entered the running state.
    1716 Apr 30 17:48  Information Service Control M...   1073748860 The Network Setup Service service entered the stopped state.
    1715 Apr 30 17:46  Information Service Control M...   1073748860 The Network Setup Service service entered the running state.
    1714 Apr 30 17:45  Information Service Control M...   1073748860 The Print Spooler service entered the stopped state.
    1713 Apr 30 17:39  Information Service Control M...   1073748860 The Network Setup Service service entered the stopped state.
    1712 Apr 30 17:36  Information Service Control M...   1073748860 The Network Setup Service service entered the running state.
    1711 Apr 30 17:29  Information Service Control M...   1073748860 The AppX Deployment Service (AppXSVC) service entered the stopped state.
    1710 Apr 30 17:28  Information Service Control M...   1073748860 The Network Setup Service service entered the stopped state.
```

Retrieve security event logs

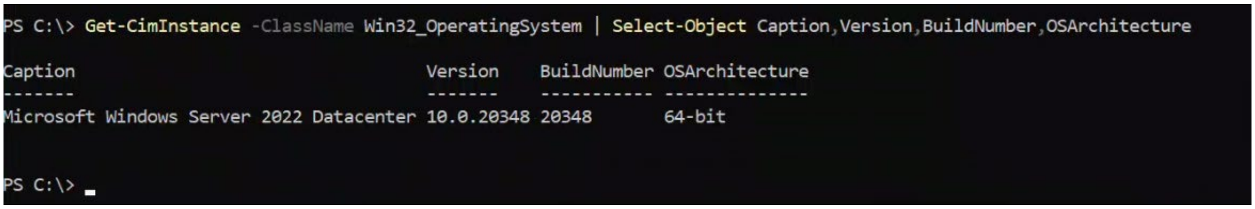


```
PS C:\> Get-WinEvent -LogName Security


   ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated                      Id LevelDisplayName Message
-----------                      -- ---------------- -------
4/30/2025 5:56:49 PM           4672 Information      Special privileges assigned to new logon....
4/30/2025 5:56:49 PM           4624 Information      An account was successfully logged on....
4/30/2025 5:50:45 PM           4672 Information      Special privileges assigned to new logon....
4/30/2025 5:50:45 PM           4624 Information      An account was successfully logged on....
4/30/2025 5:46:49 PM           4672 Information      Special privileges assigned to new logon....
4/30/2025 5:46:49 PM           4624 Information      An account was successfully logged on....
4/30/2025 5:36:49 PM           4672 Information      Special privileges assigned to new logon....
4/30/2025 5:36:49 PM           4624 Information      An account was successfully logged on....
4/30/2025 5:26:49 PM           4672 Information      Special privileges assigned to new logon....
4/30/2025 5:26:49 PM           4624 Information      An account was successfully logged on....
4/30/2025 5:24:03 PM           4672 Information      Special privileges assigned to new logon....
4/30/2025 5:24:03 PM           4624 Information      An account was successfully logged on....
4/30/2025 5:24:03 PM           4672 Information      Special privileges assigned to new logon....
4/30/2025 5:24:03 PM           4624 Information      An account was successfully logged on....
4/30/2025 5:16:49 PM           4672 Information      Special privileges assigned to new logon....
4/30/2025 5:16:49 PM           4624 Information      An account was successfully logged on....
4/30/2025 5:06:49 PM           4672 Information      Special privileges assigned to new logon....
4/30/2025 5:06:49 PM           4624 Information      An account was successfully logged on....
4/30/2025 5:05:12 PM           4672 Information      Special privileges assigned to new logon....
4/30/2025 5:05:12 PM           4624 Information      An account was successfully logged on....
4/30/2025 4:56:48 PM           4672 Information      Special privileges assigned to new logon....
4/30/2025 4:56:48 PM           4624 Information      An account was successfully logged on....
4/30/2025 4:52:41 PM           4672 Information      Special privileges assigned to new logon....
4/30/2025 4:52:41 PM           4624 Information      An account was successfully logged on....
4/30/2025 4:46:48 PM           4672 Information      Special privileges assigned to new logon....
4/30/2025 4:46:48 PM           4624 Information      An account was successfully logged on....
4/30/2025 4:36:48 PM           4672 Information      Special privileges assigned to new logon....
```

Extract operating system details using PowerShell



```
PS C:\> Get-WmiObject -Class Win32_OperatingSystem


SystemDirectory : C:\Windows\system32
Organization    :
BuildNumber     : 20348
RegisteredUser  : Windows User
SerialNumber    : 00456-50925-69428-AA668
Version         : 10.0.20348



PS C:\>
```



```
PS C:\> Get-CimInstance -ClassName Win32_OperatingSystem | Select-Object Caption,Version,BuildNumber,OSArchitecture

Caption                                  Version    BuildNumber OSArchitecture
-------                                  -------    ----------- --------------
Microsoft Windows Server 2022 Datacenter 10.0.20348 20348       64-bit


PS C:\>
```