# System Configuration

## Windows Fundamentals Part 2

Learned:

- Event Viewer helps you investigate problems on a computer, like failed logins or suspicious applications.

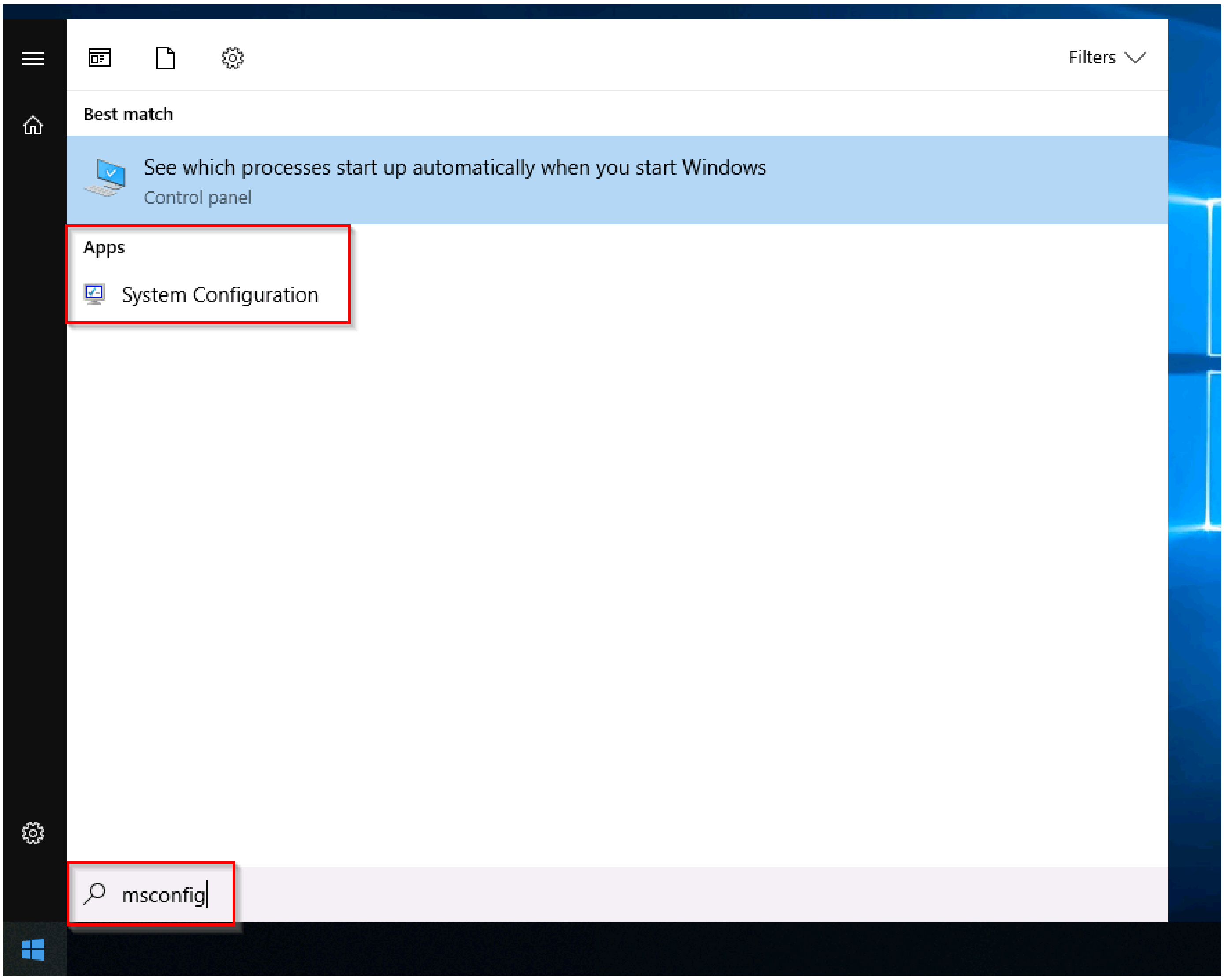
- System tools like MSConfig, Performance Monitor, and Resource Monitor are used for diagnosing startup issues and detecting unusual activity.

- Command line tools such as `ipconfig`, and `netstat` are useful for viewing network configurations, active connections, and managing network resources.

System Configuration

The **System Configuration** utility (`MSConfig`) is for advanced troubleshooting, and its main purpose is to help diagnose startup issues.

There are several methods to launch System Configuration. One method is from the Start Menu.



Best match

See which processes start up automatically when you start Windows
Control panel

Apps

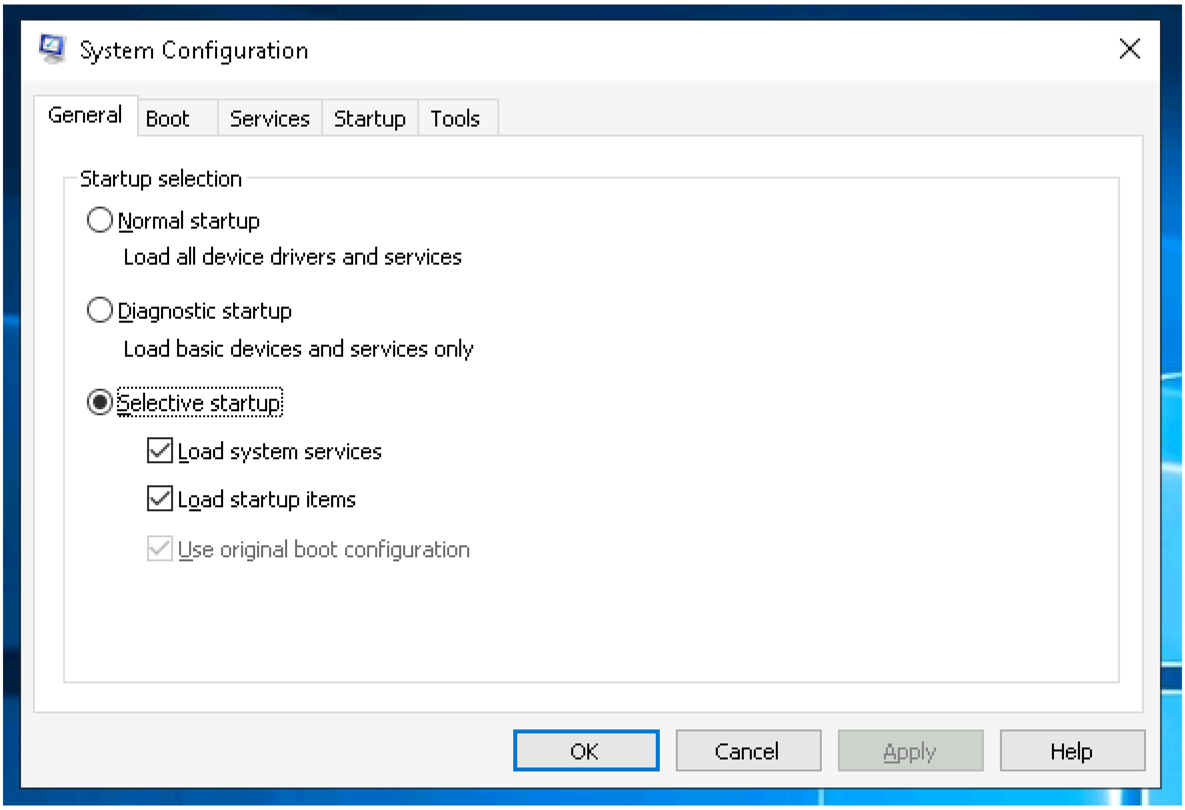
System Configuration

msconfig

**Note**: You need local administrator rights to open this utility.

The utility has five tabs across the top.

1. General
2. Boot
3. Services
4. Startup
5. Tools


System Configuration

Startup selection

○ Normal startup

Load all device drivers and services

○ Diagnostic startup

Load basic devices and services only

● Selective startup

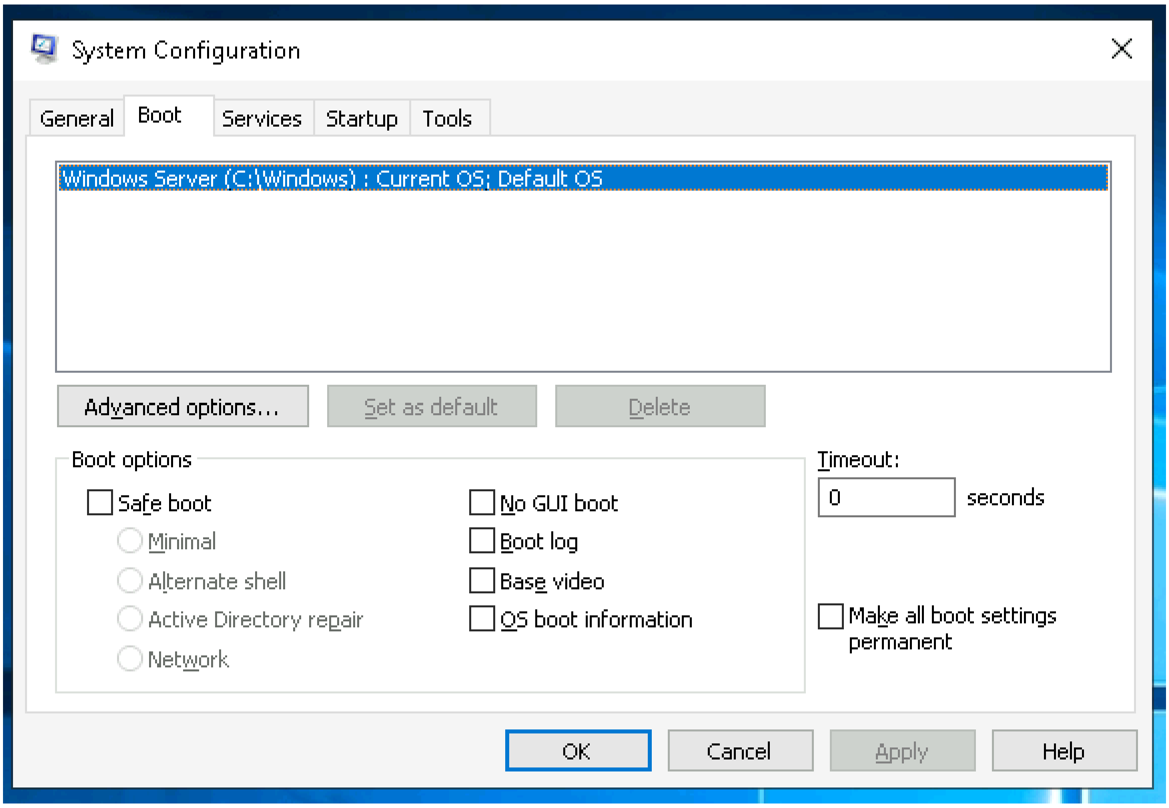
☑ Load system services

☑ Load startup items

☑ Use original boot configuration

In the **General** tab, we can select what devices and services for Windows to load upon boot. The options are: **Normal**, **Diagnostic**, or **Selective**.

In the **Boot** tab, we can define various boot options for the Operating System.


System Configuration

Windows Server (C:\Windows) : Current OS; Default OS

Boot options

□ Safe boot

○ Minimal

○ Alternate shell

○ Active Directory repair

○ Network

□ No GUI boot

□ Boot log

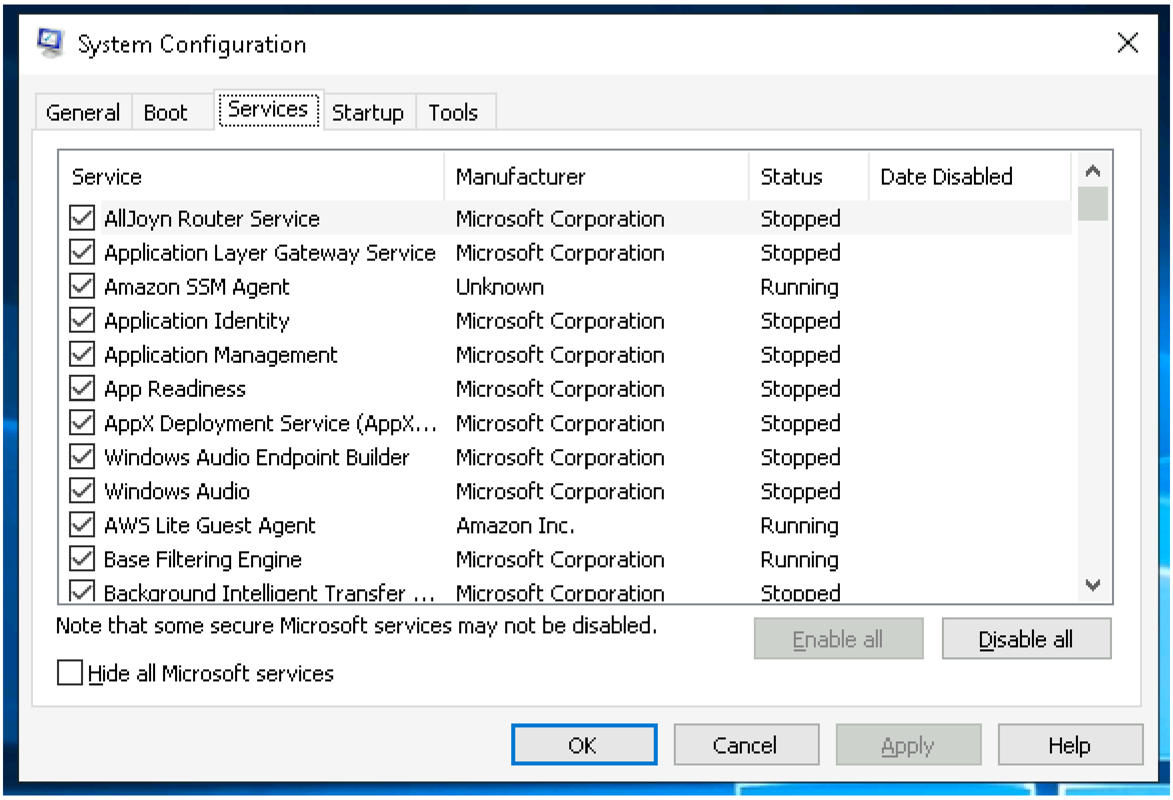
□ Base video

□ OS boot information

Timeout: 0 seconds

□ Make all boot settings permanent

The **Services** tab lists all services configured for the system regardless of their state (running or stopped). A service is a special type of application that runs in the background.

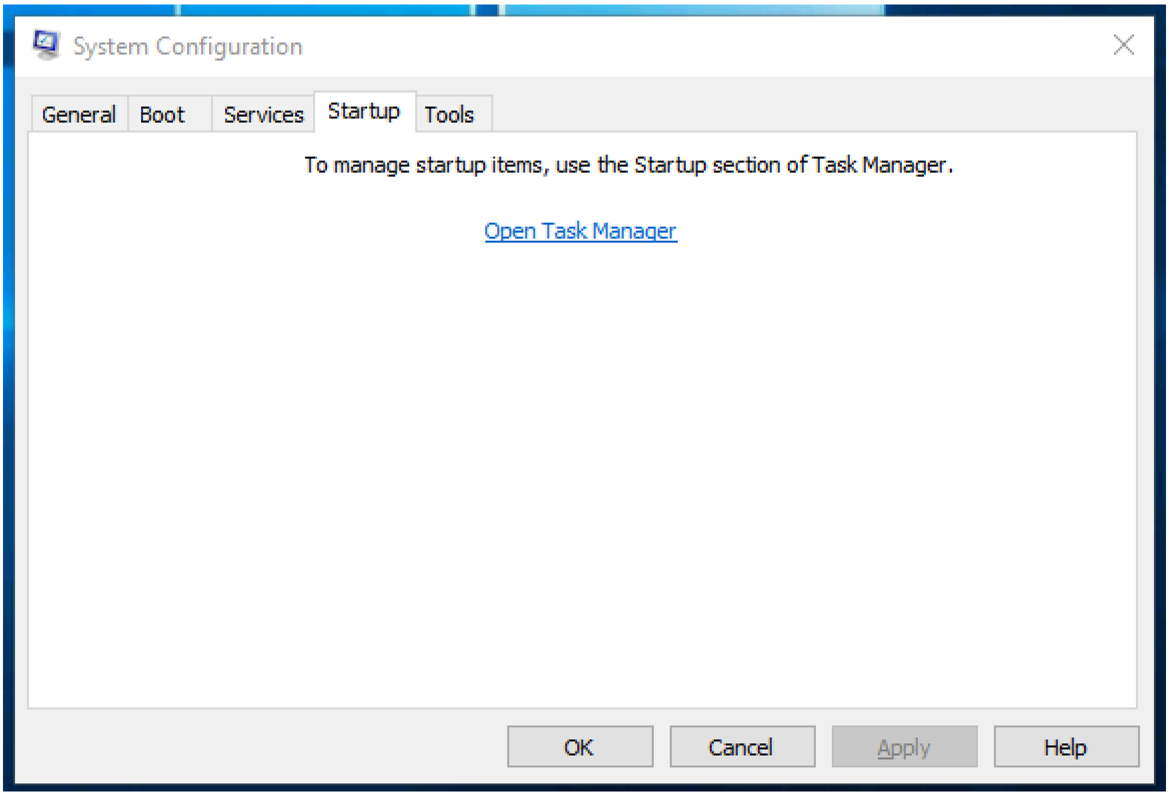


| Service | Manufacturer | Status | Date Disabled |
|---|---|---|---|
| ☑ AllJoyn Router Service | Microsoft Corporation | Stopped | |
| ☑ Application Layer Gateway Service | Microsoft Corporation | Stopped | |
| ☑ Amazon SSM Agent | Unknown | Running | |
| ☑ Application Identity | Microsoft Corporation | Stopped | |
| ☑ Application Management | Microsoft Corporation | Stopped | |
| ☑ App Readiness | Microsoft Corporation | Stopped | |
| ☑ AppX Deployment Service (AppX… | Microsoft Corporation | Stopped | |
| ☑ Windows Audio Endpoint Builder | Microsoft Corporation | Stopped | |
| ☑ Windows Audio | Microsoft Corporation | Stopped | |
| ☑ AWS Lite Guest Agent | Amazon Inc. | Running | |
| ☑ Base Filtering Engine | Microsoft Corporation | Running | |
| ☑ Background Intelligent Transfer … | Microsoft Corporation | Stopped | |

Note that some secure Microsoft services may not be disabled.

□ Hide all Microsoft services

Below is a screenshot of the Startup tab for **MSConfig.**

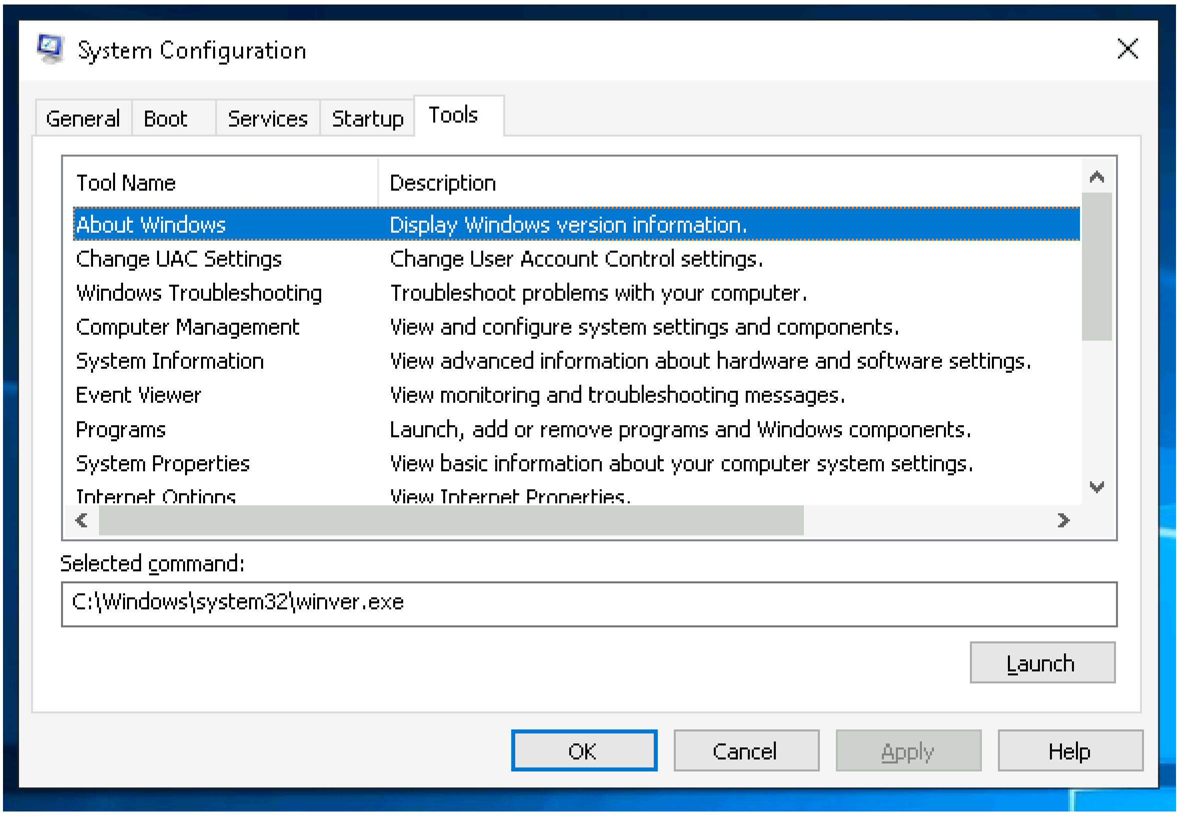


To manage startup items, use the Startup section of Task Manager.

Open Task Manager

Microsoft advises using **Task Manager (`taskmgr`)** to manage (enable/disable) startup items. The System Configuration utility is **NOT** a startup management program.

There is a list of various utilities (tools) in the Tools tab that we can run to configure the operating system further. There is a brief description of each tool.



| Tool Name | Description |
|---|---|
| About Windows | Display Windows version information. |
| Change UAC Settings | Change User Account Control settings. |
| Windows Troubleshooting | Troubleshoot problems with your computer. |
| Computer Management | View and configure system settings and components. |
| System Information | View advanced information about hardware and software settings. |
| Event Viewer | View monitoring and troubleshooting messages. |
| Programs | Launch, add or remove programs and Windows components. |
| System Properties | View basic information about your computer system settings. |
| Internet Options | View Internet Properties. |

Selected command:

```
C:\Windows\system32\winver.exe
```

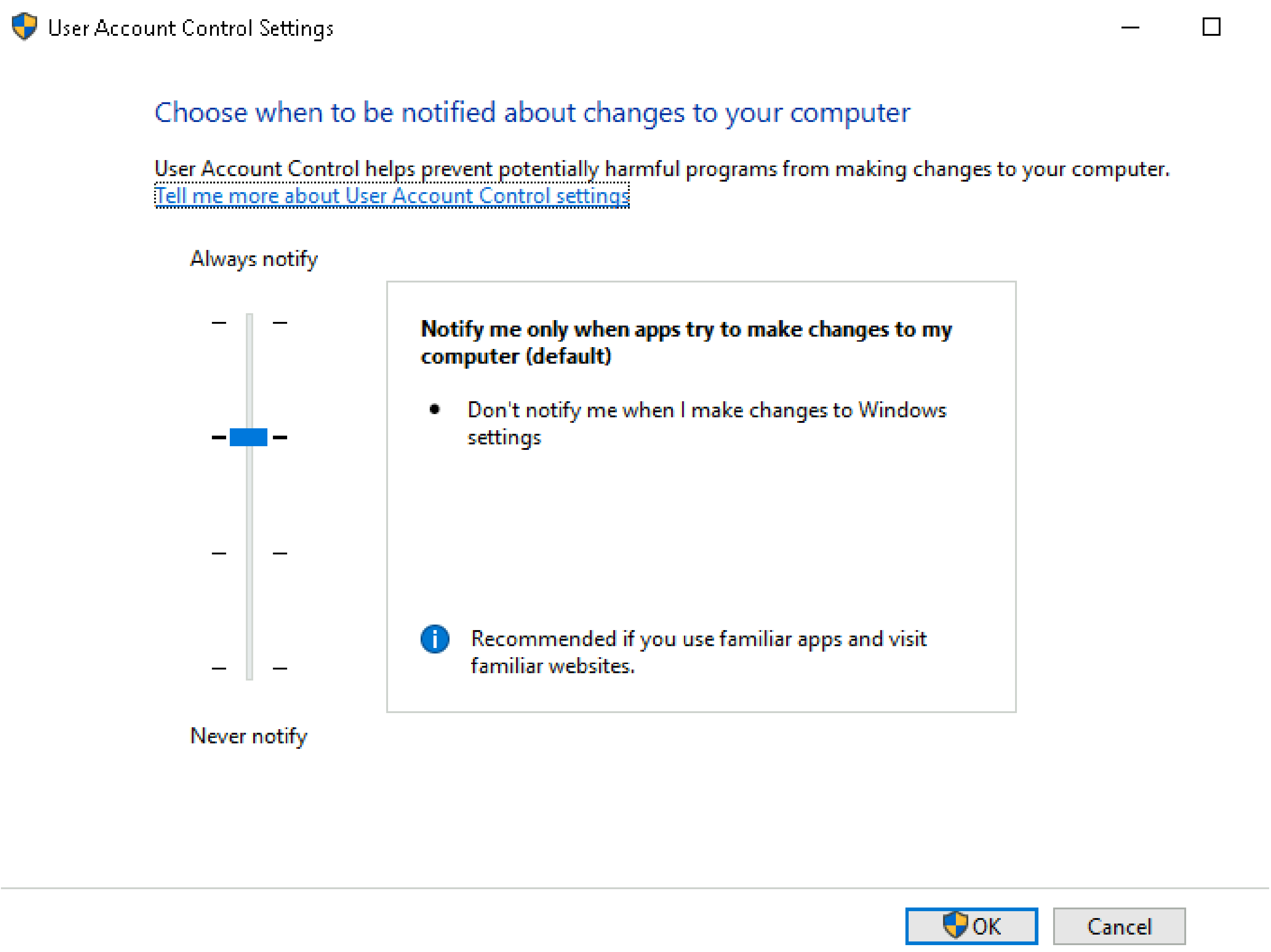
**In the Selected command** section. The information in this textbox will change per tool.

To run a tool, we can use the command to launch the tool via the run prompt, command prompt, or by clicking the `Launch` button.

## Change UAC Settings (User Account Control)

The UAC settings can be changed or even turned off (not recommended).

You can move the slider to see how the setting will change the UAC settings and Microsoft's stance on the setting.



Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

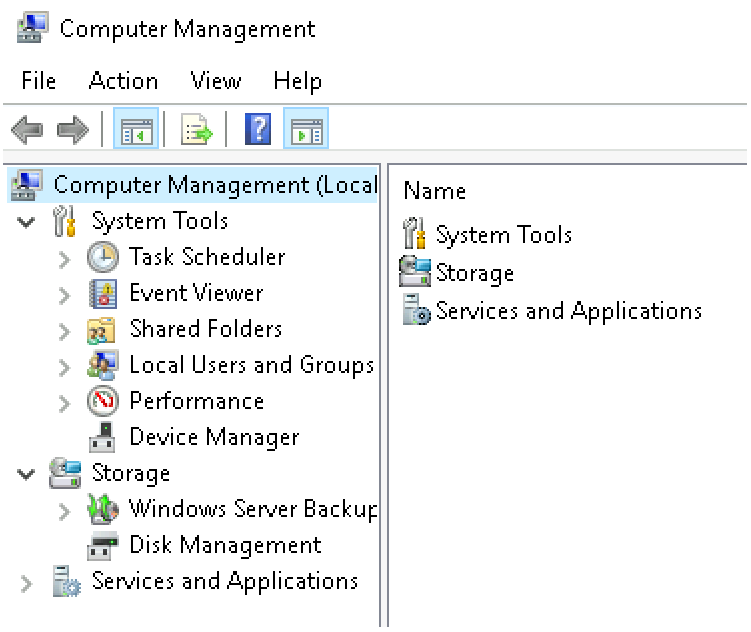
**Notify me only when apps try to make changes to my computer (default)**

- Don't notify me when I make changes to Windows settings

Recommended if you use familiar apps and visit familiar websites.

## Computer Management

The **Computer Management** (`compmgmt`) utility has three primary sections: System Tools, Storage, and Services and Applications.

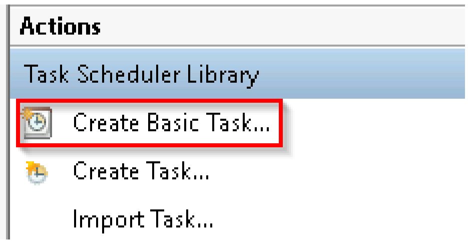


### System Tools

with Task Scheduler, we can create and manage common tasks that our computer will carry out automatically at the times we specify.

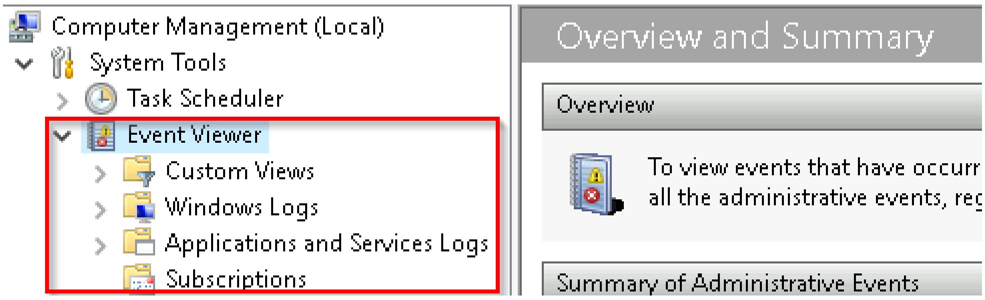
A task can run an application, a script, etc., and tasks can be configured to run at any point. A task can run at log in or at log off. Tasks can also be configured to run on a specific schedule, for example, every five mins.

To create a basic task, click on `Create Basic Task` under **Actions** (right pane).



Next is **Event Viewer**.

Event Viewer allows us to view events that have occurred on the computer. These records of events can be seen as an audit trail that can be used to understand the activity of the computer system. This information is often used to diagnose problems and investigate actions executed on the system.

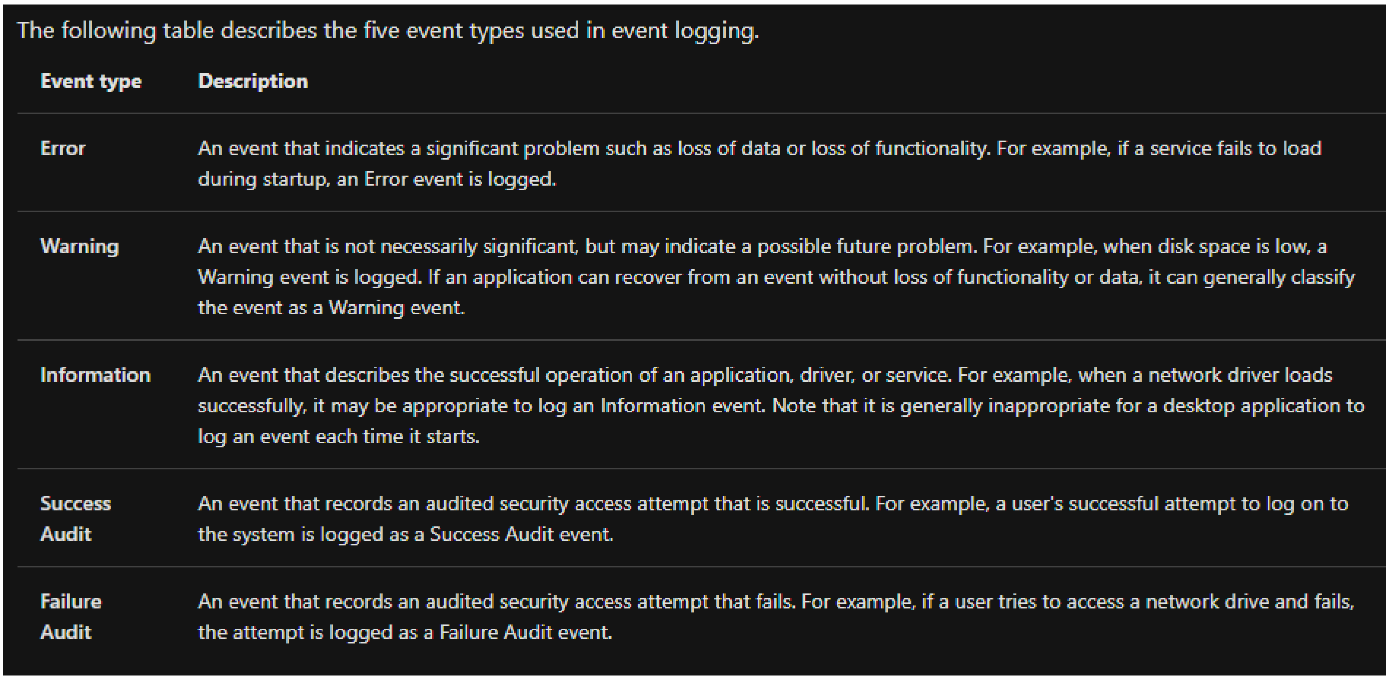


To view events that have occurr
all the administrative events, reg

Event Viewer has three panes.

1. The pane on the left provides a hierarchical tree listing of the event log providers. (as shown in the image above)
2. The pane in the middle will display a general overview and summary of the events specific to a selected provider.
3. The pane on the right is the actions pane.

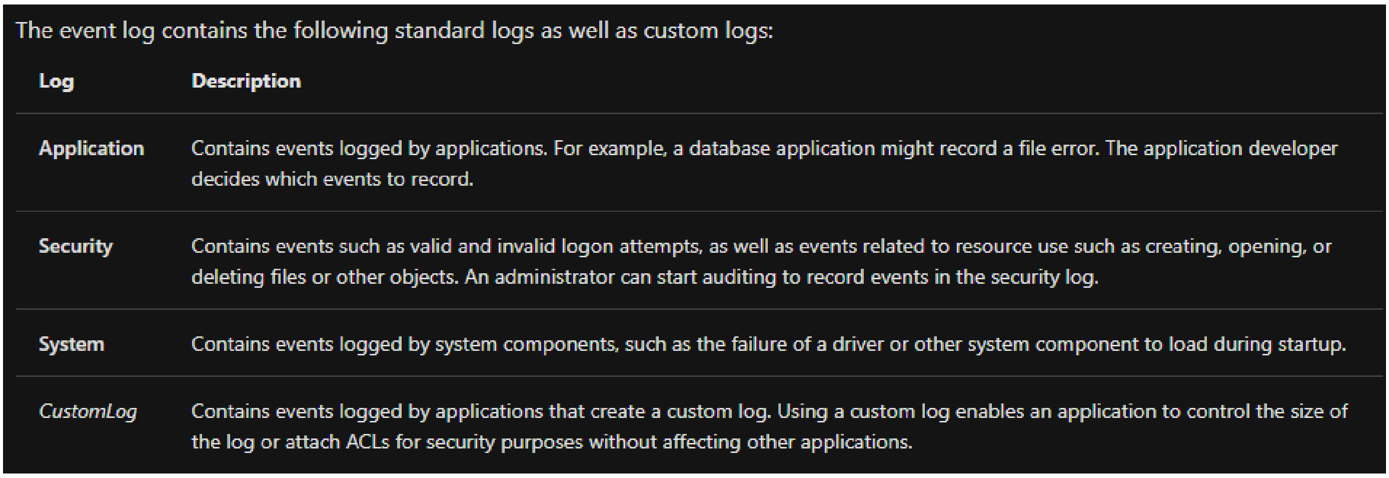
There are five types of events that can be logged.



The following table describes the five event types used in event logging.

| Event type | Description |
|---|---|
| Error | An event that indicates a significant problem such as loss of data or loss of functionality. For example, if a service fails to load during startup, an Error event is logged. |
| Warning | An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a Warning event is logged. If an application can recover from an event without loss of functionality or data, it can generally classify the event as a Warning event. |
| Information | An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, it may be appropriate to log an Information event. Note that it is generally inappropriate for a desktop application to log an event each time it starts. |
| Success Audit | An event that records an audited security access attempt that is successful. For example, a user's successful attempt to log on to the system is logged as a Success Audit event. |
| Failure Audit | An event that records an audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt is logged as a Failure Audit event. |

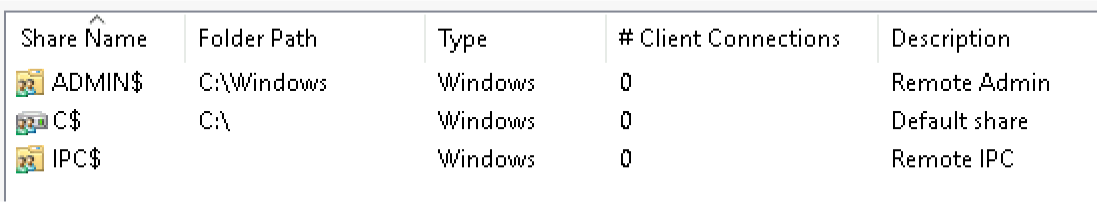
The standard logs are visible under Windows Logs.



The event log contains the following standard logs as well as custom logs:

| Log | Description |
|---|---|
| Application | Contains events logged by applications. For example, a database application might record a file error. The application developer decides which events to record. |
| Security | Contains events such as valid and invalid logon attempts, as well as events related to resource use such as creating, opening, or deleting files or other objects. An administrator can start auditing to record events in the security log. |
| System | Contains events logged by system components, such as the failure of a driver or other system component to load during startup. |
| *CustomLog* | Contains events logged by applications that create a custom log. Using a custom log enables an application to control the size of the log or attach ACLs for security purposes without affecting other applications. |

**Shared Folders** is where you will see a complete list of shares and folders shared that others can connect to.



| Share Name | Folder Path | Type | # Client Connections | Description |
|---|---|---|---|---|
| ADMIN$ | C:\Windows | Windows | 0 | Remote Admin |
| C$ | C:\ | Windows | 0 | Default share |
| IPC$ | | Windows | 0 | Remote IPC |

In the above image, under Shares, are the default share of Windows, C$, and default remote administration shares created by Windows, such as ADMIN$.

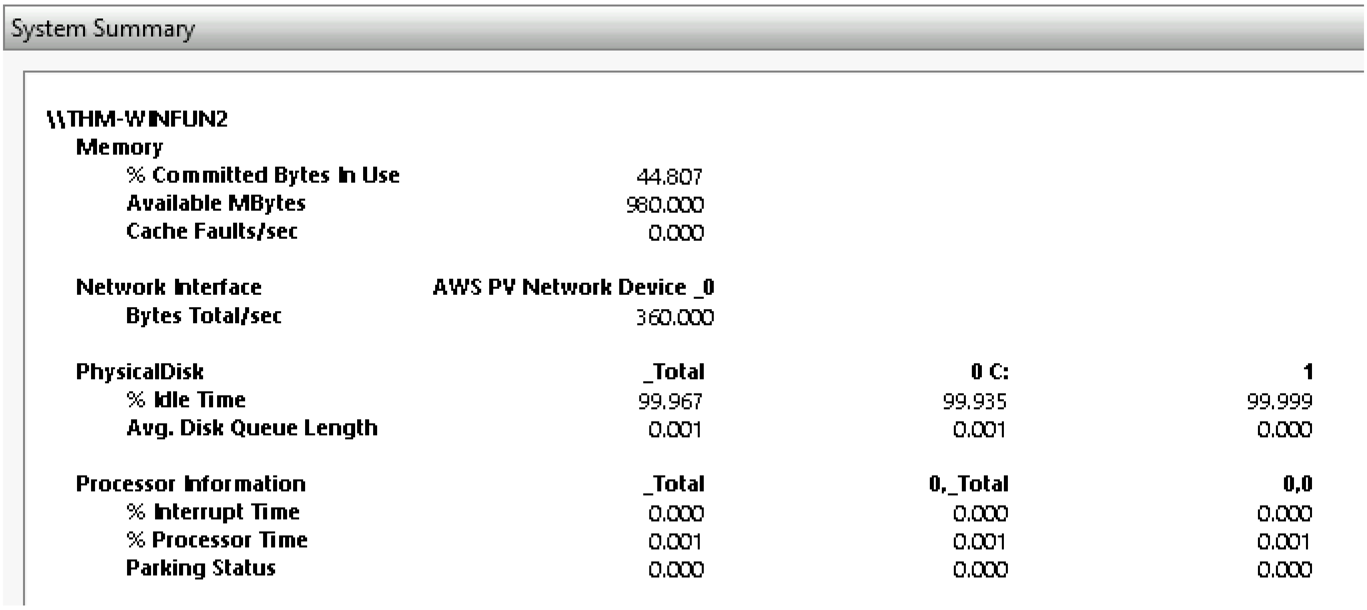
As with any object in Windows, you can right-click on a folder to view its properties, such as Permissions (who can access the shared resource).

Under **Sessions**, you will see a list of users who are currently connected to the shares.

All the folders and/or files that the connected users access will list under **Open Files**.

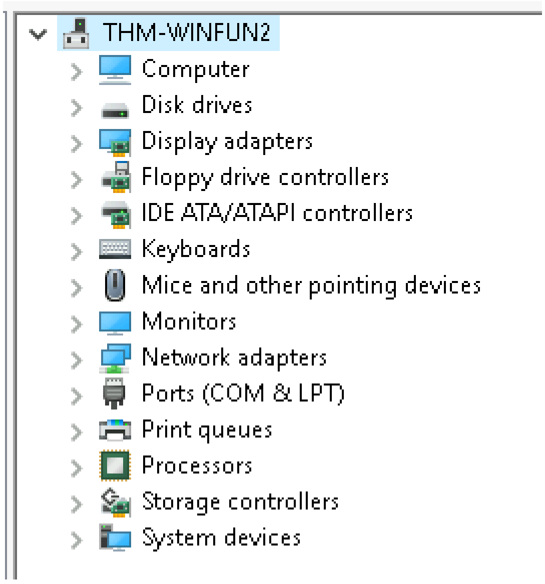
In **Performance**, you'll see a utility called **Performance Monitor** (`perfmon`).

Perfmon is used to view performance data either in real-time or from a log file. This is useful for troubleshooting performance issues on a computer system, whether local or remote.



```
System Summary

\\THM-WINFUN2
  Memory
      % Committed Bytes In Use                44.807
      Available MBytes                       980.000
      Cache Faults/sec                         0.000

  Network Interface             AWS PV Network Device _0
      Bytes Total/sec                        360.000

  PhysicalDisk                               _Total                0 C:                  1
      % Idle Time                             99.967              99.935             99.999
      Avg. Disk Queue Length                   0.001               0.001              0.000

  Processor Information                      _Total             0,_Total                0,0
      % Interrupt Time                         0.000               0.000              0.000
      % Processor Time                         0.001               0.001              0.001
      Parking Status                           0.000               0.000              0.000
```

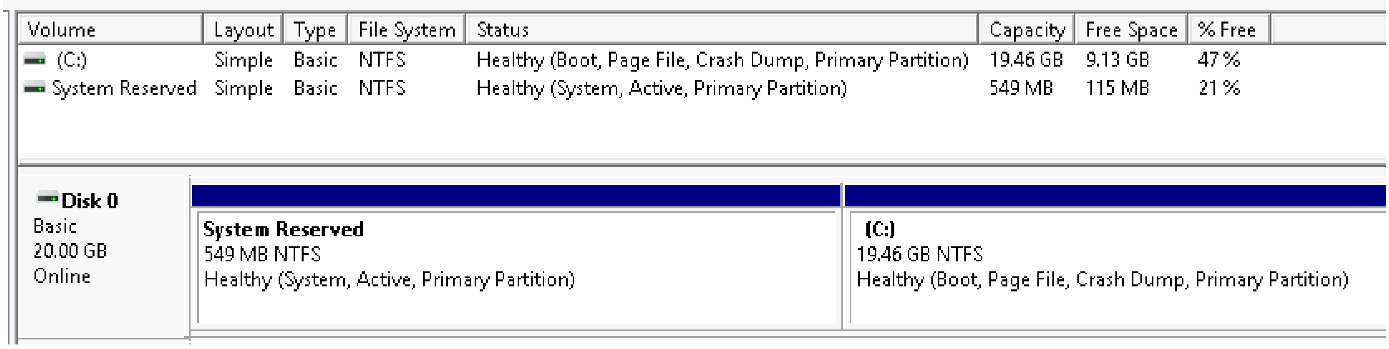
**Device Manager** allows us to view and configure the hardware, such as disabling any hardware attached to the computer.



```
THM-WINFUN2
  > Computer
  > Disk drives
  > Display adapters
  > Floppy drive controllers
  > IDE ATA/ATAPI controllers
  > Keyboards
  > Mice and other pointing devices
  > Monitors
  > Network adapters
  > Ports (COM & LPT)
  > Print queues
  > Processors
  > Storage controllers
  > System devices
```

## Storage

Under Storage is **Windows Server Backup** and **Disk Management**. We'll only look at Disk Management in this room.



| Volume | Layout | Type | File System | Status | Capacity | Free Space | % Free |
|---|---|---|---|---|---|---|---|
| (C:) | Simple | Basic | NTFS | Healthy (Boot, Page File, Crash Dump, Primary Partition) | 19.46 GB | 9.13 GB | 47 % |
| System Reserved | Simple | Basic | NTFS | Healthy (System, Active, Primary Partition) | 549 MB | 115 MB | 21 % |

**Disk 0**
Basic
20.00 GB
Online

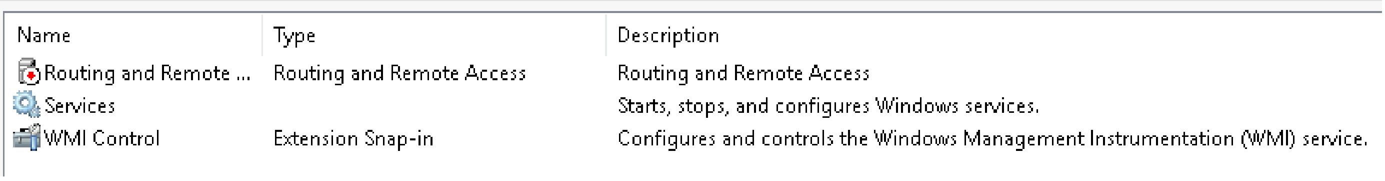
**System Reserved**
549 MB NTFS
Healthy (System, Active, Primary Partition)

**(C:)**
19.46 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

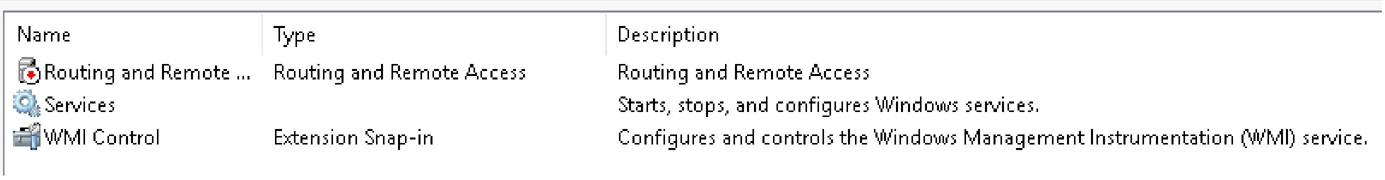
Disk Management is a system utility in Windows that enables you to perform advanced storage tasks. Some tasks are:

- Set up a new drive
- Extend a partition
- Shrink a partition
- Assign or change a drive letter (ex. E:)

## Services and Applications

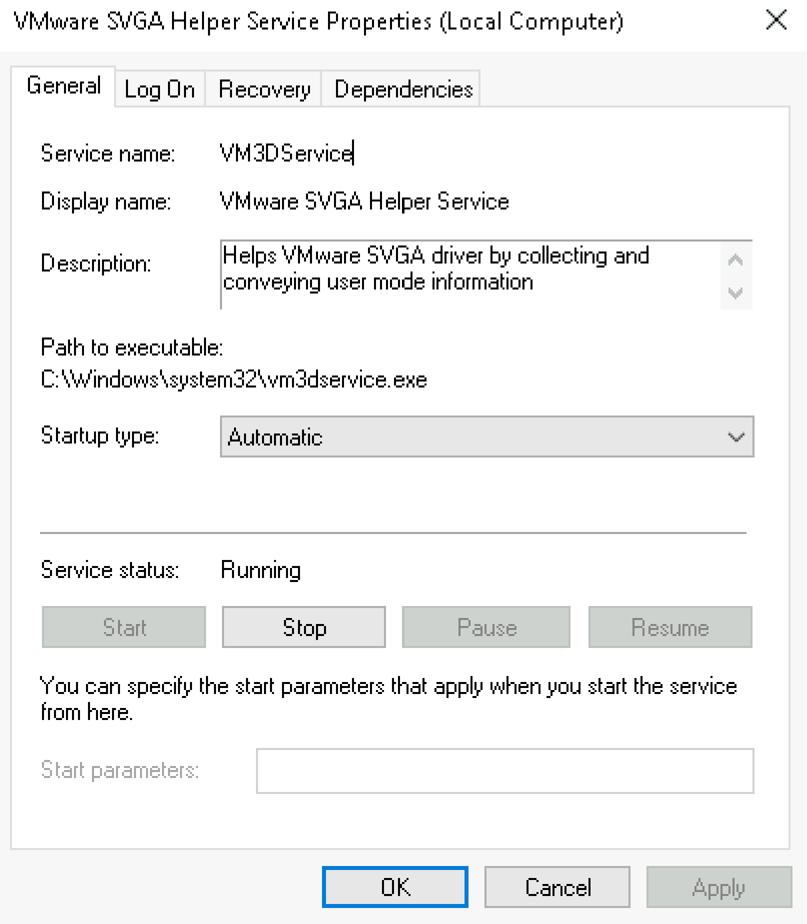


| Name | Type | Description |
|---|---|---|
| Routing and Remote ... | Routing and Remote Access | Routing and Remote Access |
| Services | | Starts, stops, and configures Windows services. |
| WMI Control | Extension Snap-in | Configures and controls the Windows Management Instrumentation (WMI) service. |



| Name | Type | Description |
|---|---|---|
| Routing and Remote ... | Routing and Remote Access | Routing and Remote Access |
| Services | | Starts, stops, and configures Windows services. |
| WMI Control | Extension Snap-in | Configures and controls the Windows Management Instrumentation (WMI) service. |

Recall from the previous task; a service is a special type of application that runs in the background. Here you can do more than enable and disable a service, such as view the Properties for the service.



VMware SVGA Helper Service Properties (Local Computer)

Service name: VM3DService

Display name: VMware SVGA Helper Service

Description: Helps VMware SVGA driver by collecting and conveying user mode information

Path to executable:
C:\Windows\system32\vm3dservice.exe

Startup type: Automatic

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

WMI Control configures and controls the **Windows Management Instrumentation** (WMI) service.

## System Information

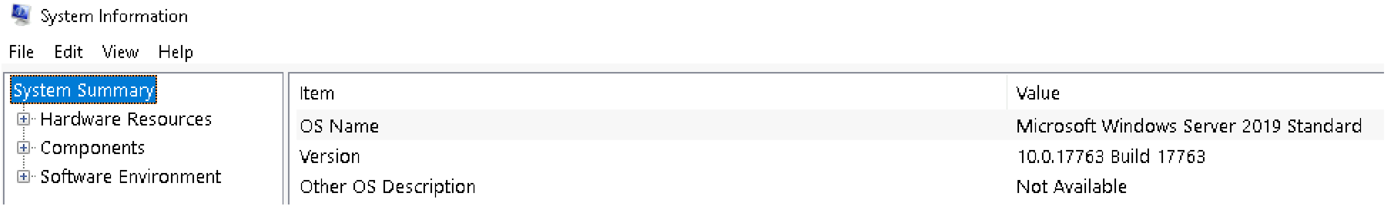
What is the **System Information** (`msinfo32`) tool?

"*Windows includes a tool called Microsoft System Information (Msinfo32.exe). This tool gathers information about your computer and displays a comprehensive view of your hardware, system components, and software environment, which you can use to diagnose computer issues.*"

The information in **System Summary** is divided into three sections:

- **Hardware Resources**
- **Components**
- **Software Environment**

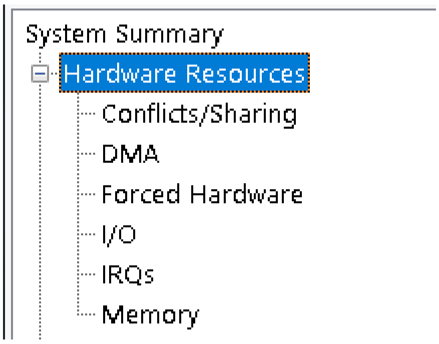
System Summary will display general technical specifications for the computer, such as processor brand and model.



System Information

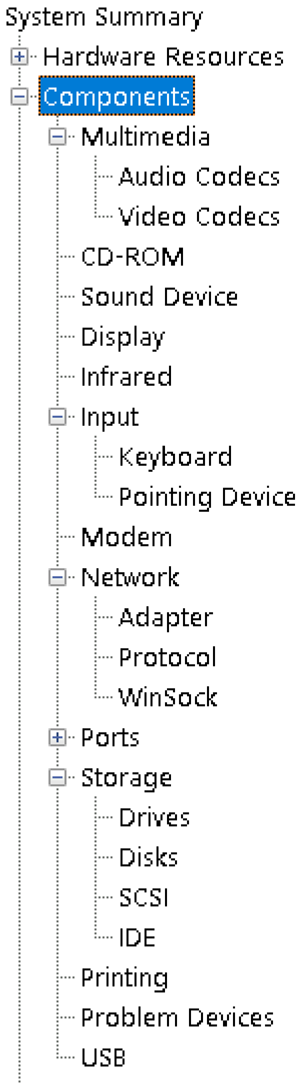
| Item | Value |
|---|---|
| OS Name | Microsoft Windows Server 2019 Standard |
| Version | 10.0.17763 Build 17763 |
| Other OS Description | Not Available |

The information displayed in **Hardware Resources** is not for the average computer user.



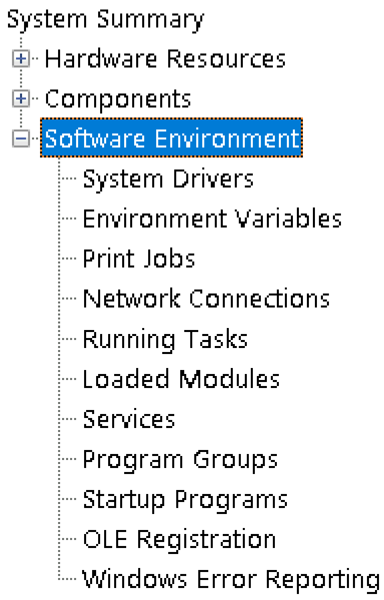
- System Summary
- Hardware Resources
  - Conflicts/Sharing
  - DMA
  - Forced Hardware
  - I/O
  - IRQs
  - Memory

Under **Components**, you can see specific information about the hardware devices installed on the computer. Some sections don't show any information, but some sections do, such as **Display** and **Input**.



- System Summary
- Hardware Resources
- Components
  - Multimedia
    - Audio Codecs
    - Video Codecs
  - CD-ROM
  - Sound Device
  - Display
  - Infrared
  - Input
    - Keyboard
    - Pointing Device
  - Modem
  - Network
    - Adapter
    - Protocol
    - WinSock
  - Ports
  - Storage
    - Drives
    - Disks
    - SCSI
    - IDE
  - Printing
  - Problem Devices
  - USB

In the **Software Environmen**t section, you can see information about software baked into the operating system and software you have installed. Other details are visible in this section as well, such as the **Environment Variables** and **Network Connections**.


System Summary
- Hardware Resources
- Components
- Software Environment
  - System Drivers
  - Environment Variables
  - Print Jobs
  - Network Connections
  - Running Tasks
  - Loaded Modules
  - Services
  - Program Groups
  - Startup Programs
  - OLE Registration
  - Windows Error Reporting

*The environment variables store data that is used by the operating system and other programs. For example, the WINDIR environment variable contains the location of the Windows installation directory. Programs can query the value of this variable to determine where Windows operating system files are located*".

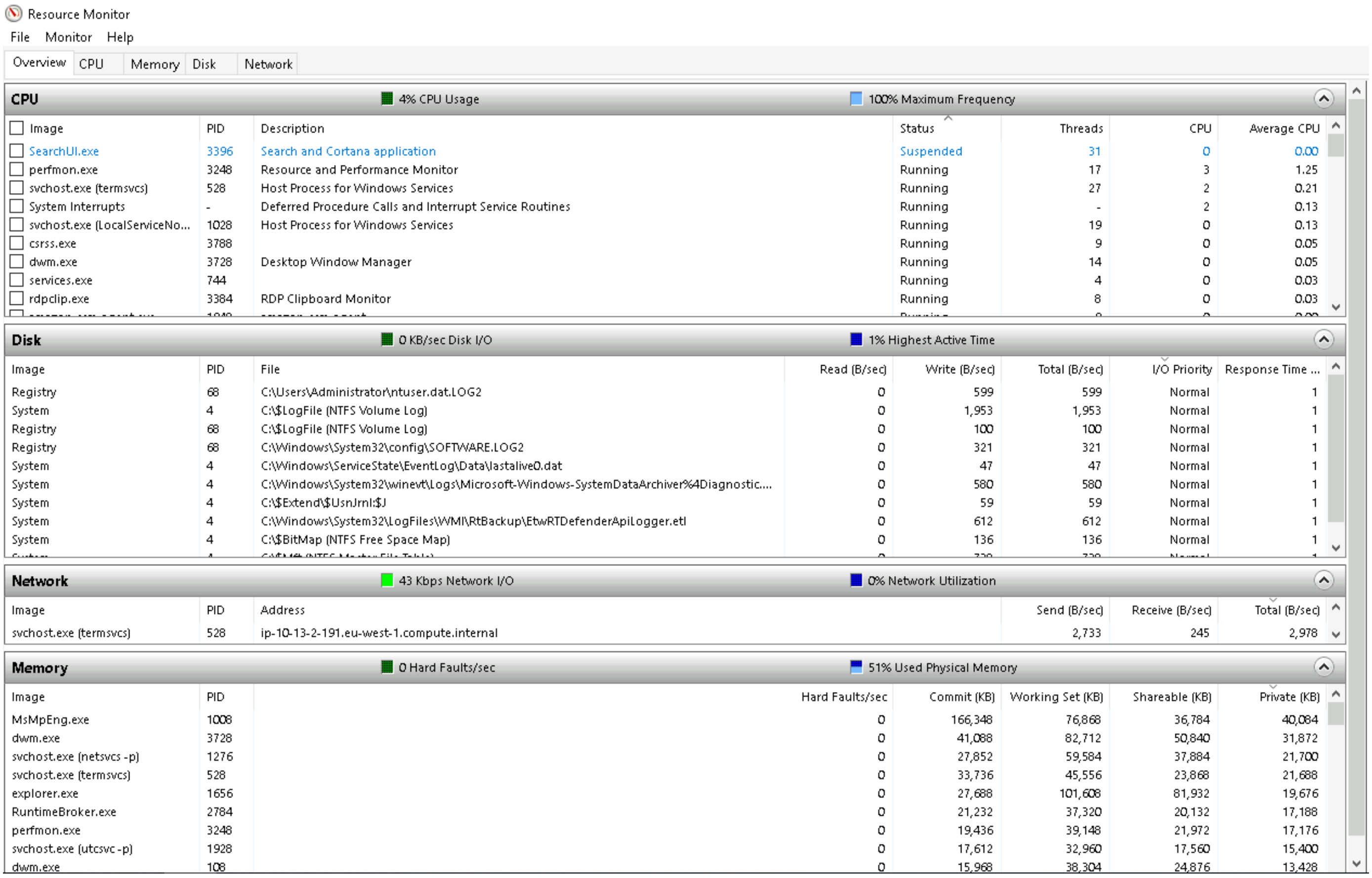
## Resource Monitor

What is **Resource Monitor** (`resmon`)?

Per Microsoft, "*Resource Monitor displays per-process and aggregate CPU, memory, disk, and network usage information, in addition to providing details about which processes are using individual file handles and modules.*

In the Overview tab, Resmon has four sections:

- **CPU**
- **Disk**
- **Network**
- **Memory**



**CPU** 🟩 4% CPU Usage 🟦 100% Maximum Frequency

| □ Image | PID | Description | Status | Threads | CPU | Average CPU |
|---|---|---|---|---|---|---|
| □ SearchUI.exe | 3396 | Search and Cortana application | Suspended | 31 | 0 | 0.00 |
| □ perfmon.exe | 3248 | Resource and Performance Monitor | Running | 17 | 3 | 1.25 |
| □ svchost.exe (termsvcs) | 528 | Host Process for Windows Services | Running | 27 | 2 | 0.21 |
| □ System Interrupts | - | Deferred Procedure Calls and Interrupt Service Routines | Running | - | 2 | 0.13 |
| □ svchost.exe (LocalServiceNo... | 1028 | Host Process for Windows Services | Running | 19 | 0 | 0.13 |
| □ csrss.exe | 3788 | | Running | 9 | 0 | 0.05 |
| □ dwm.exe | 3728 | Desktop Window Manager | Running | 14 | 0 | 0.05 |
| □ services.exe | 744 | | Running | 4 | 0 | 0.03 |
| □ rdpclip.exe | 3384 | RDP Clipboard Monitor | Running | 8 | 0 | 0.03 |

**Disk** 🟩 0 KB/sec Disk I/O 🟦 1% Highest Active Time

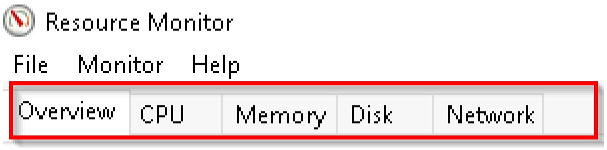
| Image | PID | File | Read (B/sec) | Write (B/sec) | Total (B/sec) | I/O Priority | Response Time ... |
|---|---|---|---|---|---|---|---|
| Registry | 68 | C:\Users\Administrator\ntuser.dat.LOG2 | 0 | 599 | 599 | Normal | 1 |
| System | 4 | C:\$LogFile (NTFS Volume Log) | 0 | 1,953 | 1,953 | Normal | 1 |
| Registry | 68 | C:\$LogFile (NTFS Volume Log) | 0 | 100 | 100 | Normal | 1 |
| Registry | 68 | C:\Windows\System32\config\SOFTWARE.LOG2 | 0 | 321 | 321 | Normal | 1 |
| System | 4 | C:\Windows\ServiceState\EventLog\Data\lastalive0.dat | 0 | 47 | 47 | Normal | 1 |
| System | 4 | C:\Windows\System32\winevt\Logs\Microsoft-Windows-SystemDataArchiver%4Diagnostic.... | 0 | 580 | 580 | Normal | 1 |
| System | 4 | C:\$Extend\$UsnJrnl:$J | 0 | 59 | 59 | Normal | 1 |
| System | 4 | C:\Windows\System32\LogFiles\WMI\RtBackup\EtwRTDefenderApiLogger.etl | 0 | 612 | 612 | Normal | 1 |
| System | 4 | C:\$BitMap (NTFS Free Space Map) | 0 | 136 | 136 | Normal | 1 |

**Network** 🟩 43 Kbps Network I/O 🟦 0% Network Utilization

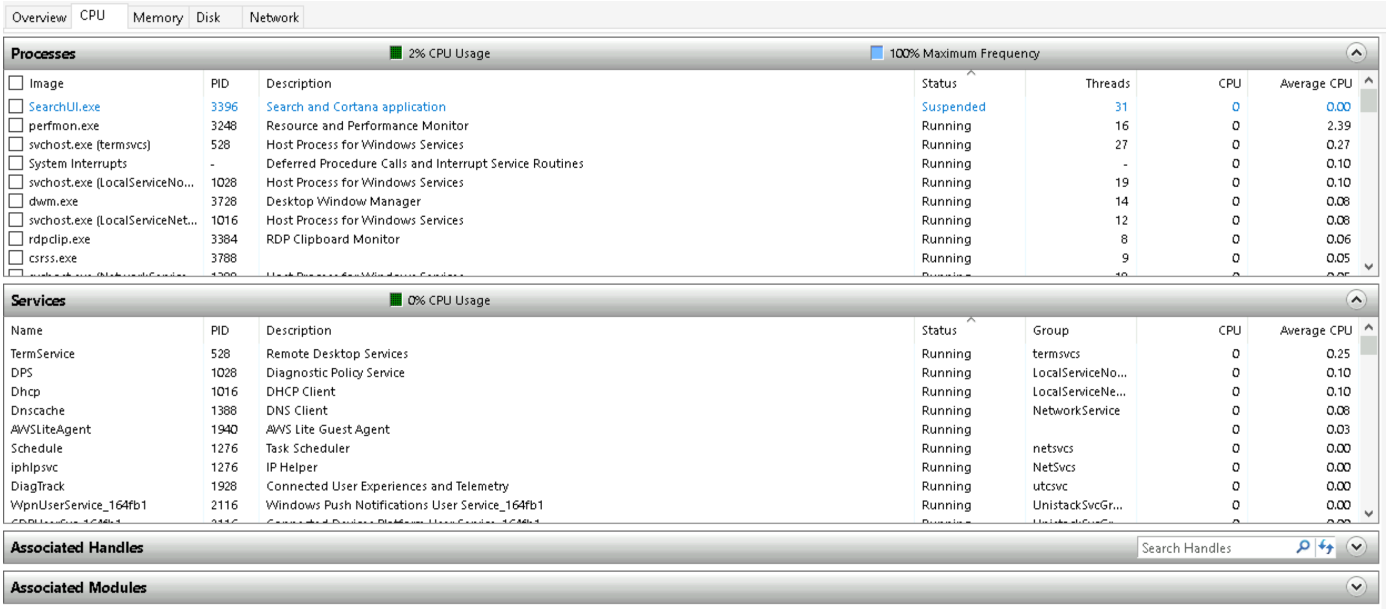
| Image | PID | Address | Send (B/sec) | Receive (B/sec) | Total (B/sec) |
|---|---|---|---|---|---|
| svchost.exe (termsvcs) | 528 | ip-10-13-2-191.eu-west-1.compute.internal | 2,733 | 245 | 2,978 |

**Memory** 🟩 0 Hard Faults/sec 🟦 51% Used Physical Memory

| Image | PID | Hard Faults/sec | Commit (KB) | Working Set (KB) | Shareable (KB) | Private (KB) |
|---|---|---|---|---|---|---|
| MsMpEng.exe | 1008 | 0 | 166,348 | 76,868 | 36,784 | 40,084 |
| dwm.exe | 3728 | 0 | 41,088 | 82,712 | 50,840 | 31,872 |
| svchost.exe (netsvcs -p) | 1276 | 0 | 27,852 | 59,584 | 37,884 | 21,700 |
| svchost.exe (termsvcs) | 528 | 0 | 33,736 | 45,556 | 23,868 | 21,688 |
| explorer.exe | 1656 | 0 | 27,688 | 101,608 | 81,932 | 19,676 |
| RuntimeBroker.exe | 2784 | 0 | 21,232 | 37,320 | 20,132 | 17,188 |
| perfmon.exe | 3248 | 0 | 19,436 | 39,148 | 21,972 | 17,176 |
| svchost.exe (utcsvc -p) | 1928 | 0 | 17,612 | 32,960 | 17,560 | 15,400 |
| dwm.exe | 108 | 0 | 15,968 | 38,304 | 24,876 | 13,428 |



## CPU



**Processes** 🟩 2% CPU Usage 🟦 100% Maximum Frequency

| □ Image | PID | Description | Status | Threads | CPU | Average CPU |
|---|---|---|---|---|---|---|
| □ SearchUI.exe | 3396 | Search and Cortana application | Suspended | 31 | 0 | 0.00 |
| □ perfmon.exe | 3248 | Resource and Performance Monitor | Running | 16 | 0 | 2.39 |
| □ svchost.exe (termsvcs) | 528 | Host Process for Windows Services | Running | 27 | 0 | 0.27 |
| □ System Interrupts | - | Deferred Procedure Calls and Interrupt Service Routines | Running | - | 0 | 0.10 |
| □ svchost.exe (LocalServiceNo... | 1028 | Host Process for Windows Services | Running | 19 | 0 | 0.10 |
| □ dwm.exe | 3728 | Desktop Window Manager | Running | 14 | 0 | 0.08 |
| □ svchost.exe (LocalServiceNet... | 1016 | Host Process for Windows Services | Running | 12 | 0 | 0.08 |
| □ rdpclip.exe | 3384 | RDP Clipboard Monitor | Running | 8 | 0 | 0.06 |
| □ csrss.exe | 3788 | | Running | 9 | 0 | 0.05 |

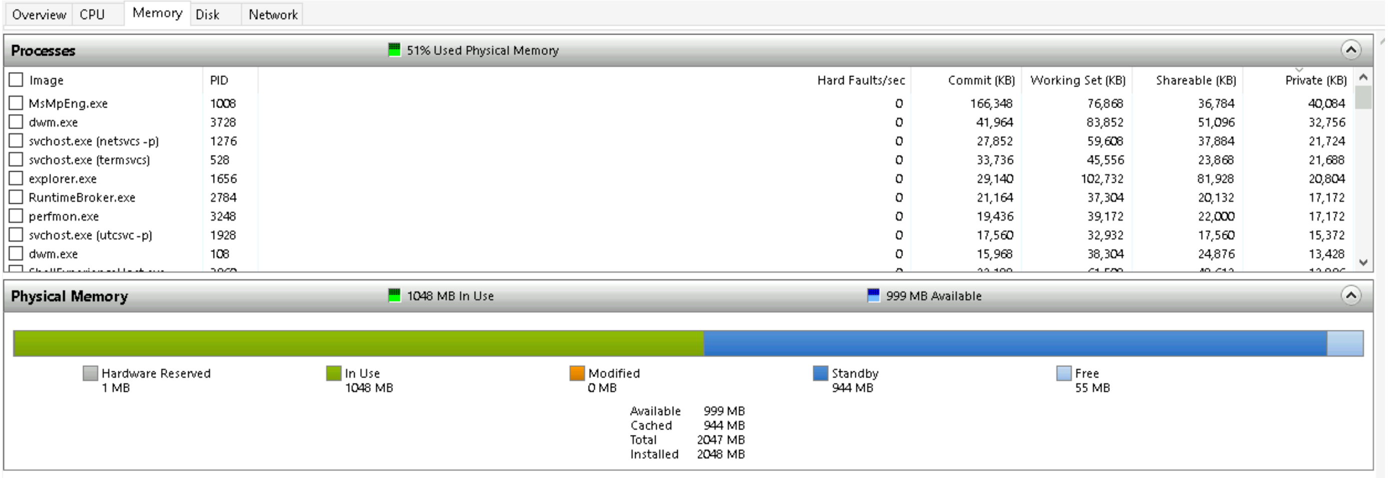
**Services** 🟩 0% CPU Usage

| Name | PID | Description | Status | Group | CPU | Average CPU |
|---|---|---|---|---|---|---|
| TermService | 528 | Remote Desktop Services | Running | termsvcs | 0 | 0.25 |
| DPS | 1028 | Diagnostic Policy Service | Running | LocalServiceNo... | 0 | 0.10 |
| Dhcp | 1016 | DHCP Client | Running | LocalServiceNe... | 0 | 0.10 |
| Dnscache | 1388 | DNS Client | Running | NetworkService | 0 | 0.08 |
| AWSLiteAgent | 1940 | AWS Lite Guest Agent | Running | | 0 | 0.03 |
| Schedule | 1276 | Task Scheduler | Running | netsvcs | 0 | 0.00 |
| iphlpsvc | 1276 | IP Helper | Running | NetSvcs | 0 | 0.00 |
| DiagTrack | 1928 | Connected User Experiences and Telemetry | Running | utcsvc | 0 | 0.00 |
| WpnUserService_164fb1 | 2116 | Windows Push Notifications User Service_164fb1 | Running | UnistackSvcGr... | 0 | 0.00 |

**Associated Handles**

**Associated Modules**

## Memory



**Processes** 🟩 51% Used Physical Memory

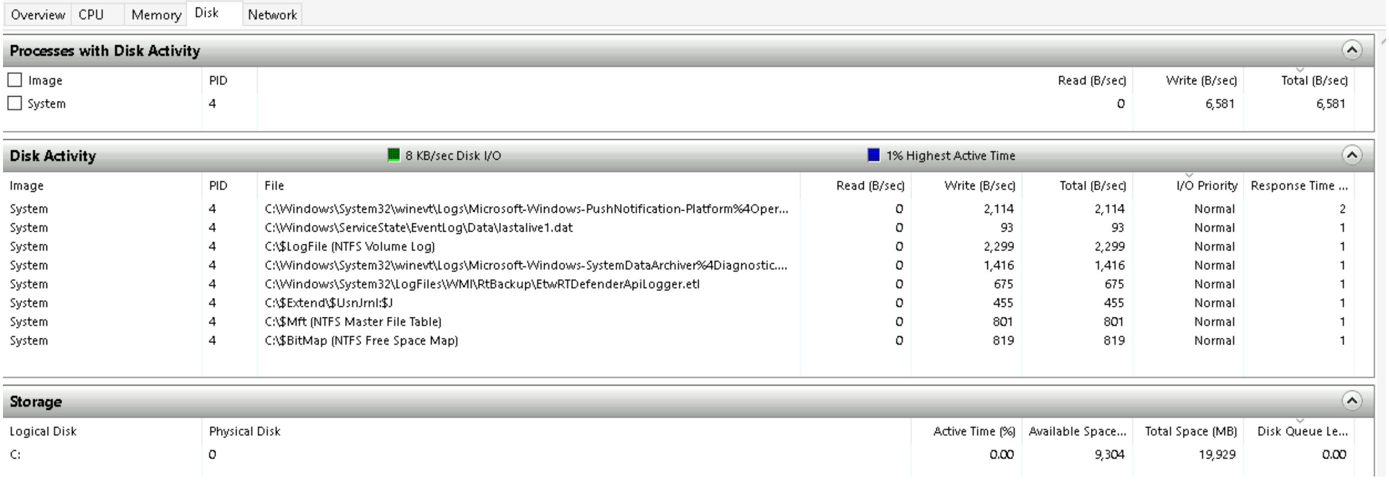
| □ Image | PID | Hard Faults/sec | Commit (KB) | Working Set (KB) | Shareable (KB) | Private (KB) |
|---|---|---|---|---|---|---|
| □ MsMpEng.exe | 1008 | 0 | 166,348 | 76,868 | 36,784 | 40,084 |
| □ dwm.exe | 3728 | 0 | 41,964 | 83,852 | 51,096 | 32,756 |
| □ svchost.exe (netsvcs -p) | 1276 | 0 | 27,852 | 59,608 | 37,884 | 21,724 |
| □ svchost.exe (termsvcs) | 528 | 0 | 33,736 | 45,556 | 23,868 | 21,688 |
| □ explorer.exe | 1656 | 0 | 29,140 | 102,732 | 81,928 | 20,804 |
| □ RuntimeBroker.exe | 2784 | 0 | 21,164 | 37,304 | 20,132 | 17,172 |
| □ perfmon.exe | 3248 | 0 | 19,436 | 39,172 | 22,000 | 17,172 |
| □ svchost.exe (utcsvc -p) | 1928 | 0 | 17,560 | 32,932 | 17,560 | 15,372 |
| □ dwm.exe | 108 | 0 | 15,968 | 38,304 | 24,876 | 13,428 |

**Physical Memory** 🟩 1048 MB In Use 🟦 999 MB Available

| Hardware Reserved | In Use | Modified | Standby | Free |
|---|---|---|---|---|
| 1 MB | 1048 MB | 0 MB | 944 MB | 55 MB |

```
Available    999 MB
Cached       944 MB
Total       2047 MB
Installed   2048 MB
```

## Disk



**Processes with Disk Activity**

| □ Image | PID | Read (B/sec) | Write (B/sec) | Total (B/sec) |
|---|---|---|---|---|
| □ System | 4 | 0 | 6,581 | 6,581 |

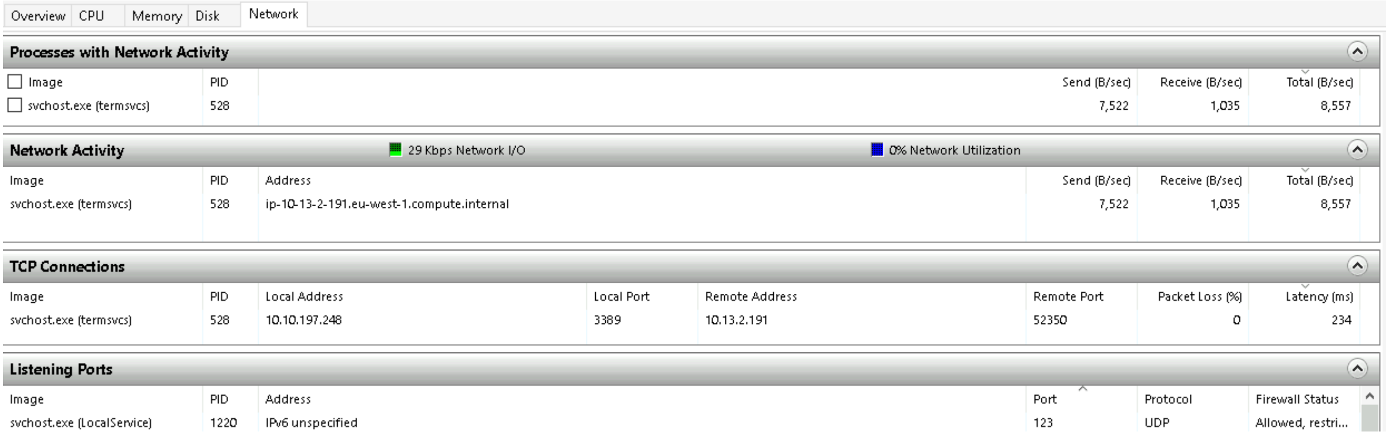
**Disk Activity** 🟩 8 KB/sec Disk I/O 🟦 1% Highest Active Time

| Image | PID | File | Read (B/sec) | Write (B/sec) | Total (B/sec) | I/O Priority | Response Time ... |
|---|---|---|---|---|---|---|---|
| System | 4 | C:\Windows\System32\winevt\Logs\Microsoft-Windows-PushNotification-Platform%4Oper... | 0 | 2,114 | 2,114 | Normal | 2 |
| System | 4 | C:\Windows\ServiceState\EventLog\Data\lastalive1.dat | 0 | 93 | 93 | Normal | 1 |
| System | 4 | C:\$LogFile (NTFS Volume Log) | 0 | 2,299 | 2,299 | Normal | 1 |
| System | 4 | C:\Windows\System32\winevt\Logs\Microsoft-Windows-SystemDataArchiver%4Diagnostic.... | 0 | 1,416 | 1,416 | Normal | 1 |
| System | 4 | C:\Windows\System32\LogFiles\WMI\RtBackup\EtwRTDefenderApiLogger.etl | 0 | 675 | 675 | Normal | 1 |
| System | 4 | C:\$Extend\$UsnJrnl:$J | 0 | 455 | 455 | Normal | 1 |
| System | 4 | C:\$Mft (NTFS Master File Table) | 0 | 801 | 801 | Normal | 1 |
| System | 4 | C:\$BitMap (NTFS Free Space Map) | 0 | 819 | 819 | Normal | 1 |

**Storage**

| Logical Disk | Physical Disk | Active Time (%) | Available Space... | Total Space (MB) | Disk Queue Le... |
|---|---|---|---|---|---|
| C: | 0 | 0.00 | 9,304 | 19,929 | 0.00 |

## Network



**Processes with Network Activity**

| □ Image | PID | Send (B/sec) | Receive (B/sec) | Total (B/sec) |
|---|---|---|---|---|
| □ svchost.exe (termsvcs) | 528 | 7,522 | 1,035 | 8,557 |

**Network Activity** 🟩 29 Kbps Network I/O 🟦 0% Network Utilization

| Image | PID | Address | Send (B/sec) | Receive (B/sec) | Total (B/sec) |
|---|---|---|---|---|---|
| svchost.exe (termsvcs) | 528 | ip-10-13-2-191.eu-west-1.compute.internal | 7,522 | 1,035 | 8,557 |

**TCP Connections**

| Image | PID | Local Address | Local Port | Remote Address | Remote Port | Packet Loss (%) | Latency (ms) |
|---|---|---|---|---|---|---|---|
| svchost.exe (termsvcs) | 528 | 10.10.197.248 | 3389 | 10.13.2.191 | 52350 | 0 | 234 |

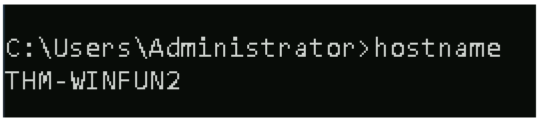
**Listening Ports**

| Image | PID | Address | Port | Protocol | Firewall Status |
|---|---|---|---|---|---|
| svchost.exe (LocalService) | 1220 | IPv6 unspecified | 123 | UDP | Allowed, restri... |

Resource Monitor has a pane at the far right which shows a graphical view in real-time for each section.

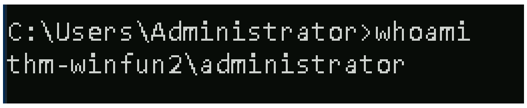
# Command Prompt

The command **hostname** will output the computer name.



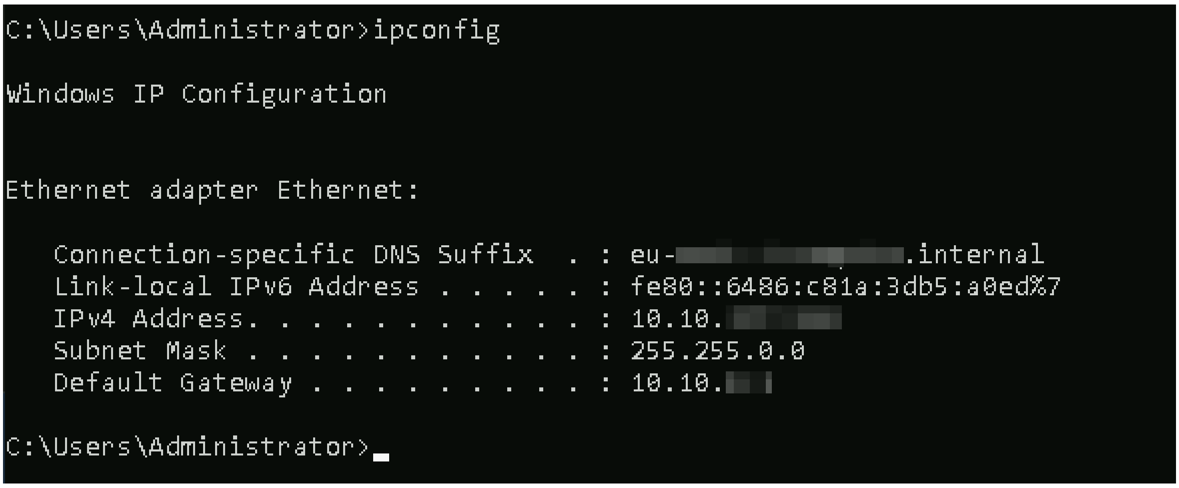
```
C:\Users\Administrator>hostname
THM-WINFUN2
```

The command **whoami** will output the name of the logged-in user.



```
C:\Users\Administrator>whoami
thm-winfun2\administrator
```

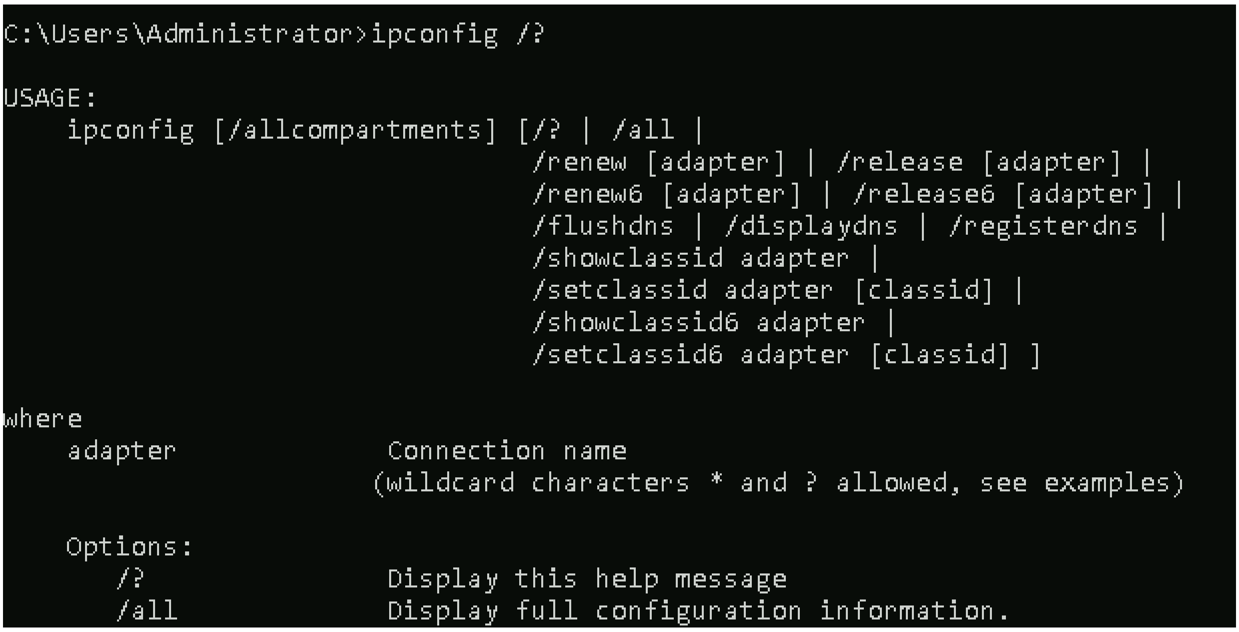
A command used often is `ipconfig`. This command will show the network address settings for the computer.



```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : eu-[redacted].internal
   Link-local IPv6 Address . . . . . : fe80::6486:c81a:3db5:a0ed%7
   IPv4 Address. . . . . . . . . . . : 10.10.[redacted]
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.10.[redacted]

C:\Users\Administrator>_
```

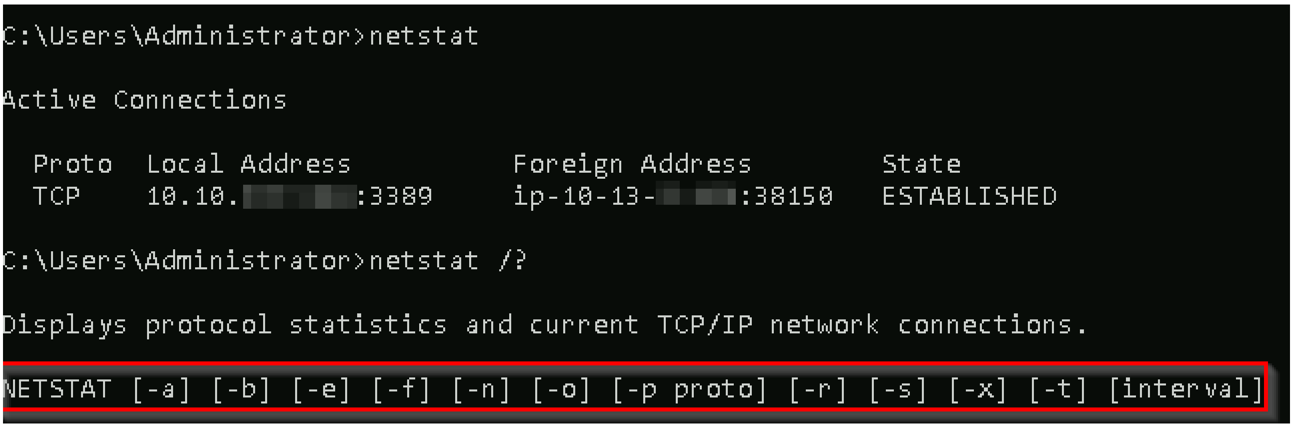
A command to retrieve the help manual for a command is `/?`.

For example, to see the help manual for **ipconfig**, you can use the following command: `ipconfig /?`



```
C:\Users\Administrator>ipconfig /?

USAGE:
    ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]

where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
```

The next command is `netstat`. Per the help manual, this command will display protocol statistics and current TCP/IP network connections.



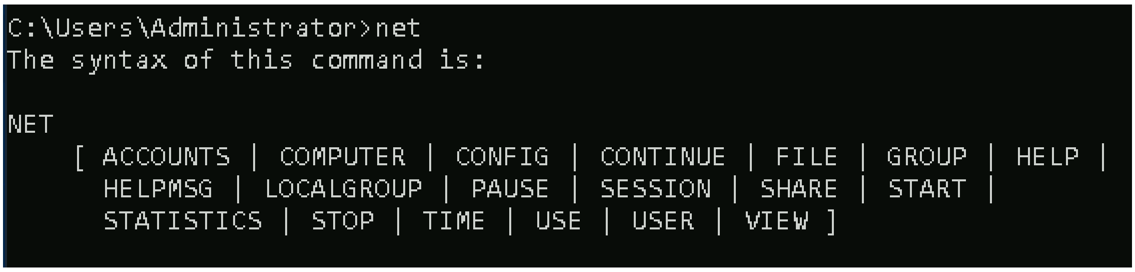
```
C:\Users\Administrator>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.10.[redacted]:3389     ip-10-13-[redacted]:38150   ESTABLISHED

C:\Users\Administrator>netstat /?

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [interval]
```

The line with the red box shows an example syntax for the command.

The structure tells us the **netstat** command can be run alone or with parameters, such as `-a`, `-b`, `-e`, etc.

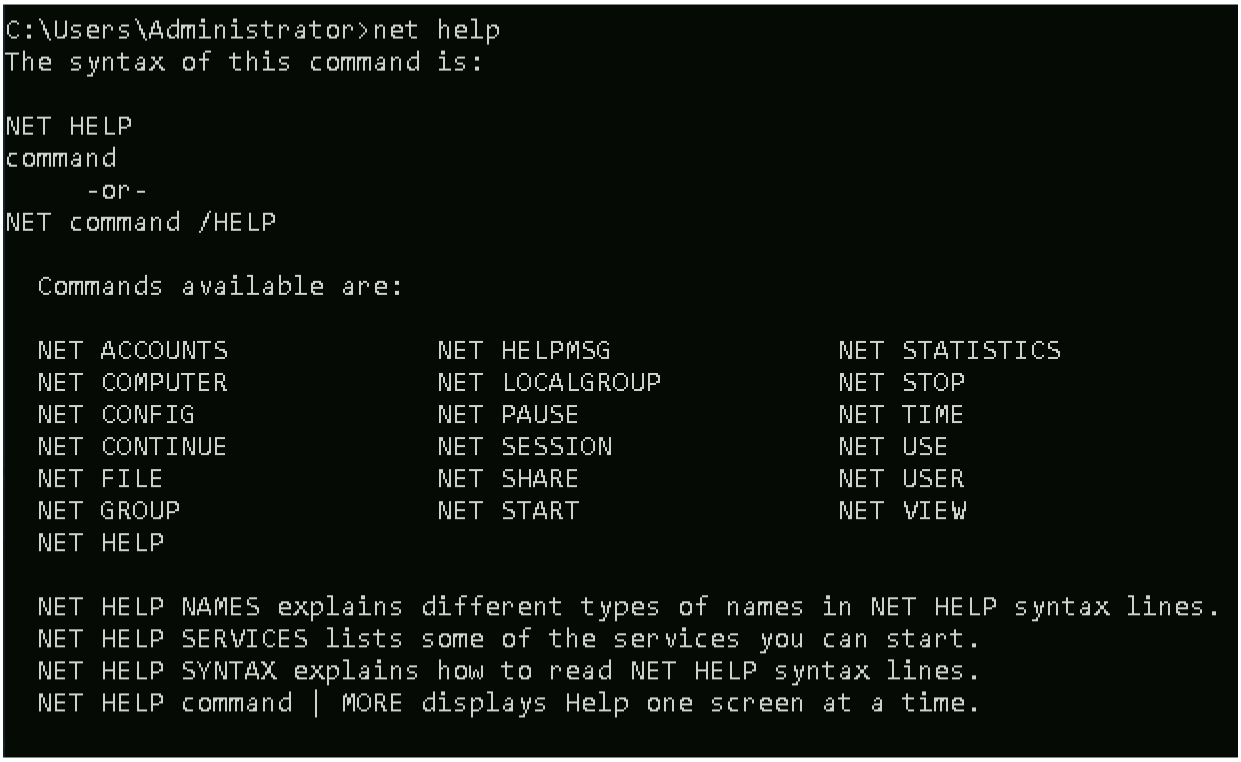
The `net` command is primarily used to manage network resources. This command supports sub-commands.

If you type **net** without a sub-command, the output will show the syntax for the root command showing a few of the sub-commands you can use.



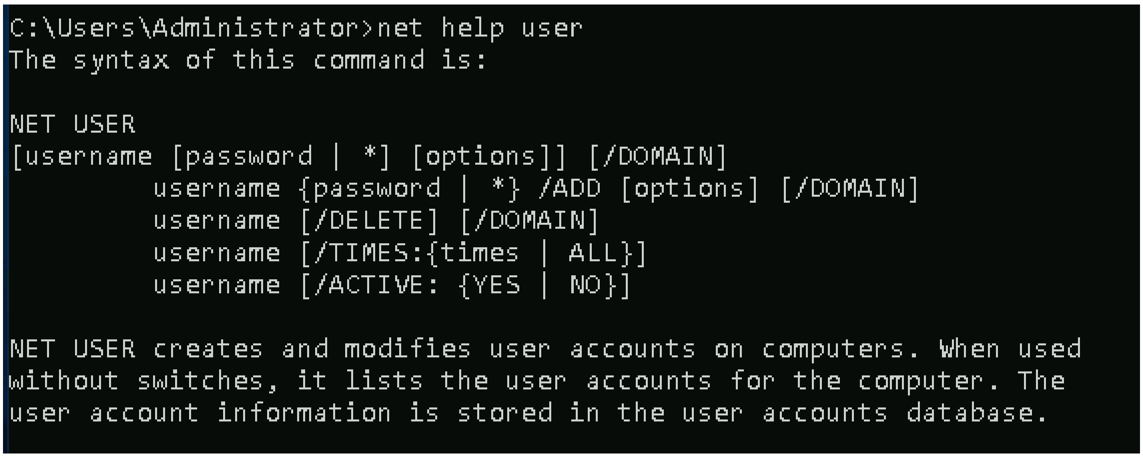
```
C:\Users\Administrator>net
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

For the net command, to display the help manual `/?` will not work. In this case, you need to use different syntax, which is `net help`.



```
C:\Users\Administrator>net help
The syntax of this command is:

NET HELP
command
     -or-
NET command /HELP

  Commands available are:

  NET ACCOUNTS             NET HELPMSG              NET STATISTICS
  NET COMPUTER             NET LOCALGROUP           NET STOP
  NET CONFIG               NET PAUSE                NET TIME
  NET CONTINUE             NET SESSION              NET USE
  NET FILE                 NET SHARE                NET USER
  NET GROUP                NET START                NET VIEW
  NET HELP

  NET HELP NAMES explains different types of names in NET HELP syntax lines.
  NET HELP SERVICES lists some of the services you can start.
  NET HELP SYNTAX explains how to read NET HELP syntax lines.
  NET HELP command | MORE displays Help one screen at a time.
```

So, if you wish to see the help information for `net user` , the command is `net help user`.



```
C:\Users\Administrator>net help user
The syntax of this command is:

NET USER
[username [password | *] [options]] [/DOMAIN]
         username {password | *} /ADD [options] [/DOMAIN]
         username [/DELETE] [/DOMAIN]
         username [/TIMES:{times | ALL}]
         username [/ACTIVE: {YES | NO}]

NET USER creates and modifies user accounts on computers. When used
without switches, it lists the user accounts for the computer. The
user account information is stored in the user accounts database.
```

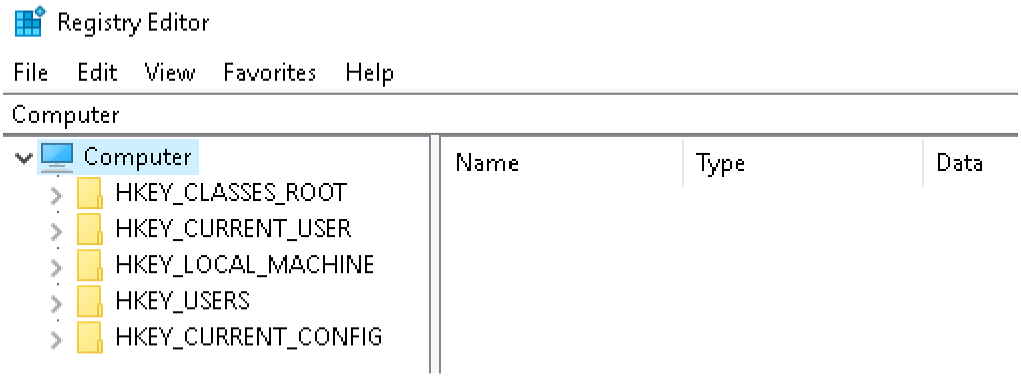
You can use the same command to view the help information for other useful **net** sub-commands, such as **localgroup**, **use**, **share**, and **session**.

## Registry Editor

The registry contains information that Windows continually references during operation, such as:

- Profiles for each user
- Applications installed on the computer and the types of documents that each can create
- Property sheet settings for folders and application icons
- What hardware exists on the system
- The ports that are being used.

There are various ways to view/edit the registry. One way is to use the **Registry Editor** (`regedit`).


Registry Editor
File
Edit
View
Favorites
Help
Computer
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG
Name
Type
Data