

Windows Command Line

Basic System Information

Commands:

set - checks paths from command line indicated by the line Path=

```
user@WINSRV2022-CORE C:\Users\user>set
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\user\AppData\Roaming
ChocolateyInstall=C:\ProgramData\chocolatey
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=WINSRV2022-CORE
ComSpec=C:\Windows\system32\cmd.exe
DriverData=C:\Windows\System32\Drivers\DriverData
EC2LAUNCH_TELEMETRY=1
HOME=C:\Users\user
HOMEDRIVE=C:
HOMEPATH=\Users\user
LOCALAPPDATA=C:\Users\user\AppData\Local
LOGNAME=user
NUMBER_OF_PROCESSORS=2
OS=Windows_NT
Path=C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\ProgramData\chocolatey\bin;C:\Windows\system32\config\systemprofile\AppData\Local\Microsoft\WindowsApps;C:\Users\user\AppData\Local\Microsoft\WindowsApps;
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=AMD64
PROCESSOR_IDENTIFIER=AMD64 Family 23 Model 1 Stepping 2, AuthenticAMD
PROCESSOR_LEVEL=23
PROCESSOR_REVISION=0102
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
ProgramFiles(x86)=C:\Program Files (x86)
ProgramW6432=C:\Program Files
PROMPT=user@WINSRV2022-CORE $P$G
PSModulePath=C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
PUBLIC=C:\Users\Public
SHELL=c:\windows\system32\cmd.exe
SSH_CLIENT=10.0.0.106 22 57526 22
```

ver - shows what operating system and version is used

```
user@WINSRV2022-CORE C:\Users\user>ver

Microsoft Windows [Version 10.0.20348.2655]
```

systeminfo - lists various information about the system

```
user@WINSRV2022-CORE C:\Users\user>systeminfo

Host Name:                WINSRV2022-CORE
OS Name:                  Microsoft Windows Server 2022 Datacenter
OS Version:               10.0.20348 N/A Build 20348
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:         Windows User
Registered Organization:
Product ID:                00454-60000-00001-AA763
Original Install Date:     4/23/2024, 7:36:29 PM
System Boot Time:          1/5/2026, 7:02:41 PM
System Manufacturer:      Amazon EC2
System Model:              t3a.small
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2200 Mhz
BIOS Version:              Amazon EC2 1.0, 10/16/2017
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
```

| more (pipe more) - this allows commands that provide lots of info to be separated into different pages and can use space to go to the next page

Network Troubleshooting

Network Configuration

ipconfig- shows ip address, subnet mask and default gateway

```
user@WINSRV2022-CORE C:\Users\user>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : eu-west-1.compute.internal
    Link-local IPv6 Address . . . . . : fe80::a608:63d0:6250:4763%5
    IPv4 Address. . . . . : 10.80.145.33
    Subnet Mask . . . . . : 255.255.192.0
    Default Gateway . . . . . : 10.80.128.1
```

ipconfig /all- shows more information like DNS servers and to see if DHCP is enabled

```
user@WINSRV2022-CORE C:\Users\user>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : WINSRV2022-CORE
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : eu-west-1.compute.internal
                                      eu-west-1.ec2-utilities.amazonaws.com

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : eu-west-1.compute.internal
    Description . . . . . : Amazon Elastic Network Adapter
    Physical Address. . . . . : 0A-09-7C-A9-7C-C7
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::a608:63d0:6250:4763%5(Preferred)
    IPv4 Address. . . . . : 10.80.145.33(Preferred)
    Subnet Mask . . . . . : 255.255.192.0
    Lease Obtained. . . . . : Monday, January 5, 2026 7:02:48 PM
    Lease Expires . . . . . : Monday, January 5, 2026 8:02:48 PM
    Default Gateway . . . . . : 10.80.128.1
    DHCP Server . . . . . : 10.80.128.1
    DHCPv6 IAID . . . . . : 84601211
    DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-B9-B7-EF-00-0C-29-FF-E5-C8
    DNS Servers . . . . . : 10.80.0.2
    NetBIOS over Tcpip. . . . . : Enabled
```

Network Troubleshooting

ping [target_name (typically ip or website)] - will send ICMP packets and listen for a response.
IF a response is received we know we can reach the target.

```
C:\>ping example.com

Pinging example.com [93.184.215.14] with 32 bytes of data:
Reply from 93.184.215.14: bytes=32 time=78ms TTL=52
Reply from 93.184.215.14: bytes=32 time=78ms TTL=52
Reply from 93.184.215.14: bytes=32 time=78ms TTL=52
Reply from 93.184.215.14: bytes=32 time=78ms TTL=52

Ping statistics for 93.184.215.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 78ms, Maximum = 78ms, Average = 78ms
```

tracert target_name (trace route) - traces network route traversed to reach target. routers will notify if a packet is dropped if its time to live reaches 0.

```
C:\>tracert example.com

Tracing route to example.com [93.184.215.14]
over a maximum of 30 hops:

  1  59 ms  32 ms  42 ms  ec2-3-248-240-3.eu-west-1.compute.amaz
  2  *      *      *      Request timed out.
  3  *      *      *      Request timed out.
  4  *      *      *      Request timed out.
  5  *      *      *      Request timed out.
  6  *      *      *      Request timed out.
  7  *      *      *      Request timed out.
  8  *      *      *      Request timed out.
  9  <1 ms  13 ms  <1 ms  100.100.2.56
 10  15 ms  11 ms  11 ms  ae-42.a03.londen12.uk.bb.gin.ntt.net [
 11  17 ms  11 ms  12 ms  ae-14.r20.londen12.uk.bb.gin.ntt.net [
 12  81 ms  80 ms  80 ms  ae-7.r20.nwrknj03.us.bb.gin.ntt.net [1
 13  83 ms  83 ms  86 ms  ae-0.a02.nycmny17.us.bb.gin.ntt.net [1
 14  79 ms  79 ms  96 ms  ce-0-3-0.a02.nycmny17.us.ce.gin.ntt.ne
 15  81 ms  86 ms  79 ms  ae-67.core1.nyd.edgecastcdn.net [152.1
 16  78 ms  78 ms  78 ms  93.184.215.14
```

More Networking Commands

nslookup [host or domain (example.com)] - looks up a host or domain and returns it IP address

if adding an address on the end like example.com 1.1.1.1 it uses that as the server name

```

C:\>nslookup example.com
Server:  ip-10-0-0-2.eu-west-1.compute.internal
Address:  10.0.0.2

Non-authoritative answer:
Name:     example.com
Addresses: 2606:2800:21f:cb07:6820:80da:af6b:8b2c
          93.184.215.14

C:>nslookup example.com 1.1.1.1
Server:  one.one.one.one
Address: 1.1.1.1

Non-authoritative answer:
Name:     example.com
Addresses: 2606:2800:21f:cb07:6820:80da:af6b:8b2c
          93.184.215.14

```

netstat - displays current network connections and listening ports.

```
user@WINSRV2022-CORE C:\Users\user>netstat
```

Active Connections

| Proto | Local Address | Foreign Address | State |
|-------|--------------------|------------------------|-------------|
| TCP | 10.80.145.33:22 | ip-10-80-106-82:57526 | ESTABLISHED |
| TCP | 10.80.145.33:49879 | ip-10-80-142-166:https | ESTABLISHED |

can be combined with various flags:

netstat - h: displays the help page

- -a displays all established connections and listening ports
- -b shows the program associated with each listening port and established connection
- -o reveals the process ID (PID) associated with the connection
- -n uses a numerical form for addresses and port numbers

can also combine the flags like netstat -abon

```

user@WINSRV2022-CORE C:\Users\user>netstat -abon

Active Connections

    Proto Local Address           Foreign Address         State           PID
    TCP    0.0.0.0:22              0.0.0.0:0              LISTENING      1628
    [sshd.exe]
    TCP    0.0.0.0:135             0.0.0.0:0              LISTENING      896
    RpcSs
    [svchost.exe]
    TCP    0.0.0.0:445             0.0.0.0:0              LISTENING      4
    Can not obtain ownership information
    TCP    0.0.0.0:3389            0.0.0.0:0              LISTENING      988
    TermService
    [svchost.exe]
    TCP    0.0.0.0:5985            0.0.0.0:0              LISTENING      4
    Can not obtain ownership information
    TCP    0.0.0.0:47001           0.0.0.0:0              LISTENING      4
    Can not obtain ownership information
    TCP    0.0.0.0:49664           0.0.0.0:0              LISTENING      676
    [lsass.exe]
    TCP    0.0.0.0:49665           0.0.0.0:0              LISTENING      536
    Can not obtain ownership information
    TCP    0.0.0.0:49666           0.0.0.0:0              LISTENING      392
    EventLog
    [svchost.exe]
    TCP    0.0.0.0:49667           0.0.0.0:0              LISTENING      500
    Schedule

```

File and Disk Management

Working with directories

cd - in windows displays current directory

- `cd target_directory` like linux goes to that directory

dir - shows child directories

- `dir /a` - Displays hidden and system files as well.

- `dir /s` - Displays files in the current directory and all subdirectories.

```

user@WINSRV2022-CORE C:\Users\user>cd
C:\Users\user

user@WINSRV2022-CORE C:\Users\user>dir
Volume in drive C has no label.
Volume Serial Number is 5448-D41F

Directory of C:\Users\user

06/14/2024  08:02 AM    <DIR>          .
06/11/2024  09:53 AM    <DIR>          ..
05/08/2021  08:15 AM    <DIR>          Desktop
06/11/2024  09:53 AM    <DIR>          Documents
05/08/2021  08:15 AM    <DIR>          Downloads
05/08/2021  08:15 AM    <DIR>          Favorites
05/08/2021  08:15 AM    <DIR>          Links
05/08/2021  08:15 AM    <DIR>          Music
05/08/2021  08:15 AM    <DIR>          Pictures
05/08/2021  08:15 AM    <DIR>          Saved Games
05/08/2021  08:15 AM    <DIR>          Videos
               0 File(s)                0 bytes
               11 Dir(s)      8,333,262,848 bytes free

```

`tree` - visually represents the child directories and subdirectories.

`mkdir directory_name` - makes directory

`rmdir directory_name` - removes directory

Working with files

`type` - views textfiles

`more` - can be considered for longer textfiles and is like the `| more`

`copy` - allows to copy files from one location to another.

`move` - can move files

`del` or `erase` - deletes a file

wildcard `*` refers to multiple files

I found a flag hidden in a directory

```
User@WINSRV2022-CORE C:\Treasure>cd /Treasure/Hunt

User@WINSRV2022-CORE C:\Treasure\Hunt>dir
Volume in drive C has no label.
Volume Serial Number is 5448-D41F

Directory of C:\Treasure\Hunt

08/20/2024  12:54 PM    <DIR>          .
08/20/2024  12:54 PM    <DIR>          ..
08/20/2024  12:54 PM                18 flag.txt
               1 File(s)                18 bytes
               2 Dir(s)  8,332,148,736 bytes free

User@WINSRV2022-CORE C:\Treasure\Hunt>type flag.txt

THM{CLI_POWER}

User@WINSRV2022-CORE C:\Treasure\Hunt>
```

Task and Process Management

tasklist- lists running processes

```
User@WINSRV2022-CORE C:\Users>tasklist
```

| Image Name | PID | Session Name | Session# | Mem Usage |
|---------------------|-----|--------------|----------|-----------|
| System Idle Process | 0 | Services | 0 | 8 K |
| System | 4 | Services | 0 | 140 K |
| Registry | 96 | Services | 0 | 13,300 K |
| smss.exe | 328 | Services | 0 | 1,260 K |
| csrss.exe | 436 | Services | 0 | 6,300 K |
| csrss.exe | 512 | Console | 1 | 7,980 K |
| wininit.exe | 536 | Services | 0 | 7,212 K |
| winlogon.exe | 592 | Console | 1 | 12,284 K |
| services.exe | 656 | Services | 0 | 7,316 K |
| lsass.exe | 676 | Services | 0 | 17,152 K |
| svchost.exe | 780 | Services | 0 | 11,952 K |
| fontdrvhost.exe | 804 | Services | 0 | 4,140 K |
| fontdrvhost.exe | 812 | Console | 1 | 4,844 K |
| svchost.exe | 896 | Services | 0 | 9,152 K |
| svchost.exe | 988 | Services | 0 | 15,132 K |

can list filters with tasklist /?

tasklist /FI "imagename eq file_name"

```
user@WINSRV2022-CORE C:\Users>tasklist /?
```

```
TASKLIST [/S system [/U username [/P [password]]]]  
          [/M [module] | /SVC | /V] [/FI filter] [/FO format] [/NH]
```

Description:

This tool displays a list of currently running processes on either a local or remote machine.

Parameter List:

| | | |
|-------|---------------|---|
| /S | system | Specifies the remote system to connect to. |
| /U | [domain\]user | Specifies the user context under which the command should execute. |
| /P | [password] | Specifies the password for the given user context. Prompts for input if omitted. |
| /M | [module] | Lists all tasks currently using the given exe/dll name. If the module name is not specified all loaded modules are displayed. |
| /SVC | | Displays services hosted in each process. |
| /APPS | | Displays Store Apps and their associated processes. |
| /V | | Displays verbose task information. |
| /FI | filter | Displays a set of tasks that match a given criteria specified by the filter. |
| /FO | format | Specifies the output format. Valid values: "TABLE" "LIST" "CSV" |

Filters:

| Filter Name | Valid Operators | Valid Value(s) |
|-------------|------------------------|---|
| ----- | ----- | ----- |
| STATUS | eq, ne | RUNNING SUSPENDED NOT RESPONDING UNKNOWN |
| IMAGENAME | eq, ne | Image name |
| PID | eq, ne, gt, lt, ge, le | PID value |
| SESSION | eq, ne, gt, lt, ge, le | Session number |
| SESSIONNAME | eq, ne | Session name |
| CPUTIME | eq, ne, gt, lt, ge, le | CPU time in the format of hh:mm:ss. hh - hours, mm - minutes, ss - seconds |
| MEMUSAGE | eq, ne, gt, lt, ge, le | Memory usage in KB |
| USERNAME | eq, ne | User name in [domain\]user format |
| SERVICES | eq, ne | Service name |
| WINDOWTITLE | eq, ne | Window title |
| MODULES | eq, ne | DLL name |

NOTE: "WINDOWTITLE" and "STATUS" filters are not supported when querying a remote machine.

Examples:

```
TASKLIST
TASKLIST /M
TASKLIST /V /FO CSV
TASKLIST /SVC /FO LIST
TASKLIST /APPS /FI "STATUS eq RUNNING"
TASKLIST /M wbem*
TASKLIST /S system /FO LIST
TASKLIST /S system /U domain\username /FO CSV /NH
TASKLIST /S system /U username /P password /FO TABLE /NH
TASKLIST /FI "USERNAME ne NT AUTHORITY\SYSTEM" /FI "STATUS eq running"
```

`taskkill /PID target_pid`

other commands

- `chkdsk` : checks the file system and disk volumes for errors and bad sectors.
- `driverquery` : displays a list of installed device drivers.
- `sfc /scannow` : scans system files for corruption and repairs them if possible.

`/?` can be used with most commands to display a help page.