SIDEBAR Operating Systems

Windows 11 PowerShell Diagnostics Cheat Sheet

Sidebar

Operating Systems · Windows 11 PowerShell Diagnostics Cheat Sheet

Read-only PowerShell one-liners for finding out what a Windows 11 PC is, what it is running and what has been going wrong. Every command here ran as a normal user (no administrator rights) on the PC this was written on (Windows 11 Pro, build 26300, Windows PowerShell 5.1) unless a line says otherwise; the commands that need administrator rights are marked. Nothing here changes a setting.

WHO IS THIS PC?

```
Get-ComputerInfo -Property OsName,OsBuildNumber,CsProcessors,BiosVersion
```

OS, build, processor and BIOS (slow, but one call; drop `-Property` for everything)

```
systeminfo
```

Classic summary: OS, install date, boot time, RAM, hotfixes, network cards

```
Get-CimInstance Win32_ComputerSystem
```

Manufacturer, model, RAM, domain/workgroup

```
Get-CimInstance Win32_BIOS
```

BIOS vendor, version and date

```
Get-CimInstance Win32_Processor
```

CPU name, cores, logical processors, max clock

```
Get-CimInstance Win32_OperatingSystem
```

Build, install date, last boot, memory fields

UPTIME, BOOT AND ADMIN CHECK

```
(Get-CimInstance Win32_OperatingSystem).LastBootUpTime
```

When it last started

```
(Get-Date) - (Get-CimInstance Win32_OperatingSystem).LastBootUpTime
```

Time since then

```
([Security.Principal.WindowsPrincipal]
[Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole('Administrator')
```

`True` if this window has administrator rights (it was `False` here)

```
Fast Startup
```

A *shutdown* with Fast Startup on is partly a hibernate, so uptime can span shutdowns; restart rather than shut down to get a clean boot

MEMORY

```
Get-CimInstance Win32_PhysicalMemory
```

Each module: capacity, rated `Speed`, `ConfiguredClockSpeed`, part number

```
Get-Counter '\Memory\Available MBytes'
```

Available RAM (see the Memory Troubleshooting sheet)

```
Get-CimInstance Win32_PageFileUsage
```

Page file size and peak

```
Get-Process | Sort-Object WorkingSet64 -Descending | Select-Object -First 10 Name, Id, WorkingSet64
```

Top processes by RAM

DISKS AND VOLUMES

```
Get-Disk
```

Disks: number, name, size, partition style, health

```
Get-PhysicalDisk
```

Media type (SSD/HDD), `HealthStatus`, `OperationalStatus`. *Healthy* can coexist with thousands of logged errors: check the event log too

```
Get-Volume
```

Drive letters, file system, size and free space

```
Get-PhysicalDisk | Get-StorageReliabilityCounter
```

Temperature, wear, error totals: returned nothing here without administrator rights

```
chkdsk D:
```

Read-only check (no `/f`); may need administrator rights; not run here

PROCESSES, SERVICES AND STARTUP

```
Get-Process | Sort-Object CPU -Descending | Select-Object -First 10 Name, Id, CPU
```

Busiest by total CPU seconds

```
Get-Process | Sort-Object Handles -Descending | Select-Object -First 5 Name, Id, Handles
```

Most handles

```
Get-Service | Where-Object Status -eq 'Running'
```

Running services (144 here)

```
Get-CimInstance Win32_Service | Where-Object State -eq 'Running' | Select-Object Name, PathName
```

Services with the program each runs: spot unfamiliar ones

```
Get-CimInstance Win32_StartupCommand | Select-Object Name, Location
```

Programs that start at sign-in

```
Get-ScheduledTask | Where-Object State -ne 'Disabled'
```

Scheduled tasks that are enabled (181 here)

NETWORK

```
Get-NetAdapter
```

Adapters: name, description, status, link speed. Here: only Ethernet is Up; Wi-Fi and four VPN adapters are Disconnected

```
Get-NetIPConfiguration
```

IP addresses, gateway and DNS per interface

```
ipconfig /all
```

The classic equivalent

```
Test-NetConnection example.com -Port 443
```

Can this PC reach a host and port (makes a network request; not run here)

```
Get-NetTCPConnection -State Established
```

Current connections (add `-OwningProcess` to link to programs; not run here)

UPDATES, DEVICES AND SECURITY

```
Get-HotFix | Sort-Object InstalledOn -Descending
```

Installed updates with dates (reads only some update types: the full history is on the Drivers & Updates sheet)

```
Get-PnpDevice -PresentOnly | Where-Object Status -ne 'OK'
```

Devices with a problem (none here)

```
Get-MpComputerStatus | Select-Object AMServiceEnabled, RealTimeProtectionEnabled, AntivirusSignatureLastUpdated
```

Microsoft Defender state. It reports Defender only, not other antivirus products

```
Get-CimInstance -Namespace root/SecurityCenter2 -ClassName AntiVirusProduct
```

Antivirus products Windows knows about (client Windows only; not run here)

EVENTS (THE SHORT VERSIONS)

```
Get-WinEvent -FilterHashtable @{LogName='System'; Level=1,2; StartTime=(Get-Date).AddHours(-24)}
```

Critical and Error events in the last 24 hours

```
Get-WinEvent -FilterHashtable @{LogName='System'; ProviderName='Microsoft-Windows-Kernel-Power'; Id=41}
```

Unexpected restarts

```
Get-WinEvent -FilterHashtable @{LogName='System'; ProviderName='disk'} | Group-Object Id
```

How many of each disk event

```
More
```

The Event Viewer sheet has the event IDs that matter; the Crash Triage sheet the first ten minutes

HABITS THAT PREVENT TROUBLE

`-ErrorAction SilentlyContinue`	Hide errors from a command you expect to fail on some items (e.g. access denied)
`| Format-List *`	See every property of an object, to find the one you need
`| Get-Member`	List an object's properties and methods
`| Out-File -Encoding utf8 file.txt`	Save output readably (Windows PowerShell 5.1 defaults to other encodings for some redirects)
`Get-Help <cmd> -Examples`	Examples for any cmdlet
`Read-only first`	Prefer `Get-*` while investigating. Anything with `Set-`, `Remove-`, `Stop-` or `Disable-` changes the PC: note the undo first

READ-ONLY DOES NOT MEAN HARMLESS TO READ

These commands change nothing, but their output can include names, serial numbers, addresses and the programs you run. Check it before pasting into a forum or a support ticket.

SOME ANSWERS NEED ADMINISTRATOR RIGHTS

When a command returns nothing or *Access denied*, that is not the same as *no problem found*. The Crash Triage sheet shows what to copy from an administrator prompt.