

PowerShell diagnostics

Read-only checks for Windows systems, networking and event logs.

Network configuration

```
Get-NetIPConfiguration
```

Show addresses, gateways and DNS settings.

```
Get-NetIPAddress -AddressFamily IPv4
```

List IPv4 addresses on interfaces.

DNS and connectivity

```
Resolve-DnsName example.com -Type A
```

Resolve an IPv4 record.

```
Resolve-DnsName example.com -Type MX
```

Inspect inbound mail routing.

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

Test TCP connectivity; does not validate HTTPS content or the certificate.

Listening TCP ports

```
Get-NetTCPConnection -State Listen
```

Show local listeners and their owning process IDs.

```
Get-Process -Id 1234
```

Look up a process ID from the previous result. Replace 1234.

Learn a command

```
Get-Help Test-NetConnection -Examples
```

Read installed usage examples. Some help content or modules may need installation.

Services and processes

```
Get-Service | Where-Object Status -eq Stopped
```

List stopped services; stopped does not necessarily mean faulty.

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

One pipeline; CPU is cumulative processor time, not current percentage.

Recent system events

```
Get-WinEvent -LogName System -MaxEvents 30
```

Read the most recent system events. Permissions vary by log.

```
Get-WinEvent -FilterHashtable @{  
  LogName="System"; Level=2  
} -MaxEvents 20
```

Read recent error-level events. The brace block is one command.

Check file integrity

```
Get-FileHash .\download.iso -Algorithm SHA256
```

Compare against a trusted, independently obtained checksum. A matching untrusted checksum proves little.

Use the right environment

Network cmdlets here use Windows modules and may not exist in PowerShell on Linux/macOS. Commands inspect local state or contact the named target. Review output for internal names and other private information before sharing.