

Linux Monitoring & Diagnostics Cheatsheet

Tema: Monitoreo de recursos y diagnóstico técnico en Linux **Incluye:** Tabla resumen, kit de diagnóstico ideal, comandos esenciales **Extra:** Compatibilidad con WSL — qué funciona, qué no funciona y por qué

Introducción

Linux es un ecosistema ideal para monitoreo, administración de sistemas y diagnóstico profundo. Permite:

- Analizar CPU, RAM, disco, red y procesos
- Detectar cuellos de botella
- Revisar logs completos del sistema
- Depurar fallos de aplicaciones y servicios
- Automatizar diagnósticos vía terminal

WSL (Windows Subsystem for Linux) permite ejecutar muchas herramientas, pero **no todas funcionan igual** por limitaciones del kernel virtualizado.

Tabla Resumen de Herramientas de Monitoreo

Herramienta	Tipo	Nivel	Qué monitorea	Cuándo usar
top / htop	Terminal	Básico/Intermedio	Procesos, CPU, RAM	Diagnóstico rápido
atop	Terminal	Avanzado	CPU, RAM, disco, red, kernel	Bottlenecks complejos
iotop	Terminal	Intermedio	Uso de disco por proceso	Lentitud por I/O
iftop / nethogs	Terminal	Intermedio	Actividad de red	Ancho de banda
vmstat	Terminal	Intermedio	Memoria, swap, procesos	Métricas generales
dstat	Terminal	Intermedio	CPU, disco, RAM, red	Vista integral
systemd-analyze	Terminal	Intermedio	Performance del arranque	Boot lento
journalctl	Terminal	Avanzado	Logs del sistema	Debug profesional
lsof	Terminal	Intermedio	Archivos abiertos	Diagnóstico de procesos
ps / pstree	Terminal	Básico	Procesos	Inspección
netstat / ss	Terminal	Intermedio	Puertos y conexiones	Seguridad/red

Herramienta	Tipo	Nivel	Qué monitorea	Cuándo usar
glances	CLI dashboard	Intermedio	Monitoreo global	Vista "todo en uno"
strace	Terminal	Experto	Syscalls	Debug profundo
perf	Terminal	Experto	CPU profiling	Optimización avanzada

Kit de Diagnóstico Ideal para Técnicos Linux

◆ Diagnóstico rápido (procesos y recursos)

```
htop
top
glances
```

◆ Diagnóstico de disco

```
iotop
df -h
du -sh /*
lsblk
smartctl -a /dev/sdX
```

◆ Diagnóstico de red

```
iftop
nethogs
ss -tulpn
ping
traceroute
```

◆ Diagnóstico de memoria y swap

```
free -h
vmstat 1
sar -r 1 5
```

◆ Logs del sistema

```
journalctl -xe  
journalctl -u nombre_servicio  
dmesg -T
```

◆ Debug avanzado

```
strace -p PID  
perf top  
lsof -i
```

🖥 Comandos Esenciales para Monitoreo (Linux)

◆ Procesos

```
ps aux  
pstree  
kill -9 PID
```

◆ CPU

```
mpstat 1  
top -o %CPU
```

◆ Memoria

```
free -m  
vmstat 1
```

◆ Disco

```
df -h  
du -sh /ruta
```



```
iotop
```

◆ Red

```
ss -tulpn  
ip a  
ip route
```

◆ Servicios (systemd)

```
systemctl status nginx  
systemctl restart nombre_servicio  
systemd-analyze blame
```

Compatibilidad con WSL: Qué Funciona, Qué No y Por Qué

WSL es un Linux **sin acceso al kernel real** ni al hardware de Windows. Por eso algunas herramientas funcionan perfectamente, y otras **no funcionan o dan datos falsos**.

✓ Herramientas que **sí funcionan en WSL**

Funcionan porque:

- No requieren acceso a hardware real
- Usan el kernel virtualizado de WSL
- Dependen sólo de procesos y memoria del userland

Funcionan perfecto:

```
top  
htop  
ps  
free  
du  
df  
lsof  
ss  
ip  
pstree
```



```
dmesg      # limitado
journalctl # si WSL tiene systemd habilitado
strace
```

✗ Herramientas que **NO funcionan en WSL** (o dan datos falsos)

No funcionan porque WSL:

- No accede al *kernel real*
- No ve el *hardware físico*
- No controla procesos del host Windows
- No tiene dispositivos reales */dev/sda*, */dev/nvme*, */dev/ttyUSB**

✗ No funcionan o fallan:

```
iotop
iostat
smartctl
hdparm
iftop
nethogs
perf
systemd-analyze
lspci
lsusb
```

🧠 Explicación técnica rápida

Recurso	WSL puede verlo	¿Por qué?
CPU	✓ Parcial	Kernel virtualizado provee datos
Memoria	✓ Parcial	WSL reporta memoria asignada
Procesos	✓ Solo procesos Linux	No accede a procesos Windows
Disco real	✗	El disco es un VHDX virtual
S.M.A.R.T.	✗	No hay acceso a hardware
Kernel logs	✗	dmesg es limitado; sin logs reales
Network real	✗	Interfaz virtual; no tráfico del host

🔗 Conclusión

✓ Linux es potentísimo para diagnóstico profesional ✓ WSL sirve para la mayoría de herramientas lógicas
✗ Pero no sirve para monitorear hardware real o tráfico real ✓ Lo ideal:

- **WSL para desarrollo y análisis de procesos Linux**
- **PowerShell para monitoreo del sistema Windows**
- **Herramientas nativas de Windows + Sysinternals** para hardware, red y disco