

journalctl

gestión centralizada de logs

- archivo principal de configuración: `/etc/systemd/journald.conf`
- importancia de tener bien establecida la zona horaria con [timedatectl](#)
- [journalctl-remote](#)

comandos

- listar todos los registros: `journalctl`
- mostrar mensajes del kernel: `journalctl -k`
- mostrar mensajes en tiempo real (tail -f): `journalctl -f`
 - de un servicio: `journalctl -f sshd.service`
- mostrar logs más recientes: `journalctl -r`
- mostrar log del último arranque (boot): `journalctl -b`
- mostrar log de antepenúltimo arranque (2 atrás): `journalctl -b -2`
- mostrar log de arranque de hace cinco arranques: `journalctl -k -b -5`
- listar arranques (0 es el actual) e ID asignado: `journalctl --list-boots`
- mostrar cuánto ocupan los registros de journald: `journalctl --disk-usage`
- limpiar registros reteniendo 2GB: `journalctl --vacuum-size=2G`
- limpiar registros reteniendo 2 años: `journalctl --vacuum-time=2years`
- ver registros por PID/UID usuario/ID arranque (nº boot):
 - `journalctl _PID=pid`
 - `journalctl _UID=uid`
 - `journalctl _BOOT_ID=identificador_de_boot`
 - `journalctl _COMM=<programa>`
- ver registro de un servicio: `journalctl -u nombre.service`
- ver registros filtrando por prioridades (0 mayor, 7 menor)
 - debug - 7, info - 6, notice - 5, warning - 4, err - 3, crit - 2, alert - 1, emerg - 0
 - `journalctl -p 1`
 - `journalctl -p alert`
- ver las últimas X entradas (por defecto 10): `journalctl -n X`
- ver registros filtrando por fecha
 - `journalctl --since «YYYY-MM-DD HH:MM:SS»`
 - `journalctl --since «YYYY-MM-DD» --until «YYYY-MM-DD HH:MM»`
 - `journalctl --since=09:00 --until=16:30`
 - `journalctl --since=yesterday`
- mostrar registros a partir de binarios (no siempre posible): `journalctl /sbin/sshd`
- mostrar registros de una unidad: `journalctl -u sshd`

se pueden combinar diferentes filtros. /via:

<https://www.elarraydejota.com/guia-tecnica-de-gestion-de-servicios-en-systemd-para-administradores-de-sistemas/>

/via: <https://blog.elhacker.net/2021/04/journalctl-analizar-logs-del-sistema-en-linux.html>

persistencia

- crear directorio **`/var/log/journal`**
- editar:

</etc/systemd/journald.conf>

```
. . .  
[ Journal ]  
Storage=persistent
```

From:

<https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link:

<https://miguelangel.torresegea.es/wiki/linux:systemd:journalctl?rev=1637992702>

Last update: **26/11/2021 21:58**

