journalctl

gestión centralizada de logs

archivo principal de configuración: `/etc/systemd/journald.conf`

zona horaria

- `timedatectl list-timezones`
- `sudo timedatectl set-timezone zone`
- `timedatectl status`

comandos

- listar todos los registros: `journalctl`
- mostrar mensajes del kernel: `journalctl -k`
- mostrar mensajes en tiempo real (tail -f): `journalctl -f`
- mostrar log del último arranque (boot): `journalctl -b`
- mostrar log de antepenúltimo arranque (2 atrás): `journalctl -b -2`
- 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`
- 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 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/

persistencia

- `/var/log/journal` (si no lo está, se crea)