

5.4 - Consulter les journaux avec journalctl et dmesg

Les journaux permettent de comprendre ce qui s'est produit avant de modifier la configuration. Avec systemd, `journalctl` interroge le journal central.

Journaux d'un service

```
journalctl -u ssh
journalctl -u nginx --since today
journalctl -u nginx -n 100
journalctl -u nginx -f
```

`-f` suit les nouvelles entrées ; quitter avec `Ctrl` + `C`.

Journaux du démarrage

```
journalctl -b          # démarrage actuel
journalctl -b -1       # démarrage précédent
journalctl --list-boots
```

Priorités importantes :

```
journalctl -p warning..alert -b
journalctl -p err -b
```

Filtrer dans le temps :

```
journalctl --since "2026-08-07 08:00:00" --until "2026-08-07 09:00:00"
journalctl --since "30 minutes ago"
```

Afficher sans pagination :

```
journalctl -u nginx --no-pager -n 50
```

Messages du noyau

```
dmesg -T  
sudo dmesg -T | tail -n 100  
sudo dmesg -T | grep -Ei 'error|fail|warn'  
journalctl -k -b
```

Les dates produites par `dmesg -T` peuvent être approximatives après une veille ou une modification de l'horloge ; `journalctl -k` fournit souvent un contexte temporel plus cohérent.

Journaux classiques

Selon la distribution et le service :

```
ls -lah /var/log  
sudo less /var/log/auth.log  
sudo less /var/log/syslog  
sudo less /var/log/messages
```

Espace occupé

```
journalctl --disk-usage  
sudo journalctl --vacuum-time=14d
```

La dernière commande supprime les journaux archivés plus anciens que 14 jours. Elle doit respecter la politique de conservation et les besoins d'audit.

Collecte de diagnostic

```
journalctl -u mon-service --since "1 hour ago" --no-pager > journal-service.txt  
systemctl status mon-service --no-pager >> journal-service.txt
```

Avant de partager un journal, rechercher et masquer mots de passe, jetons, adresses privées sensibles, noms d'utilisateurs et autres secrets.

Revision #2

Created 2026-08-08 01:24:53 CEST by Admin

Updated 2026-08-08 01:46:53 CEST by Admin