Mais où sont passés mes fichiers de log ?

Benoit Métrot (*benoit.metrot@univ-poitiers.fr)*

Institut Pprime

Rencontres Mathrice de printemps
Poitiers - Mars 2026

mathrice

Avec GNU/Linux tout est fichier

- Programmes
- Fichiers réguliers (textes, images, documents)
- Répertoires
- Disques, partitions (périphériques blocs)
- Consoles (périphériques à caractères)
- Sockets de communications
- Liens
- ...

Et le journal des évènemments ?

log file

Un fichier journal consigne tous les évènements d'un programme du système d'exploitation qu'il s'agisse d'une application ou d'un *daemon* système. Chaque élément y est associé avec la date et l'heure de survenance.

Et le journal des évènemments ?

log file

Un fichier journal consigne tous les évènements d'un programme du système d'exploitation qu'il s'agisse d'une application ou d'un *daemon* système. Chaque élément y est associé avec la date et l'heure de survenance.

Partons à leur recherche !

Plan

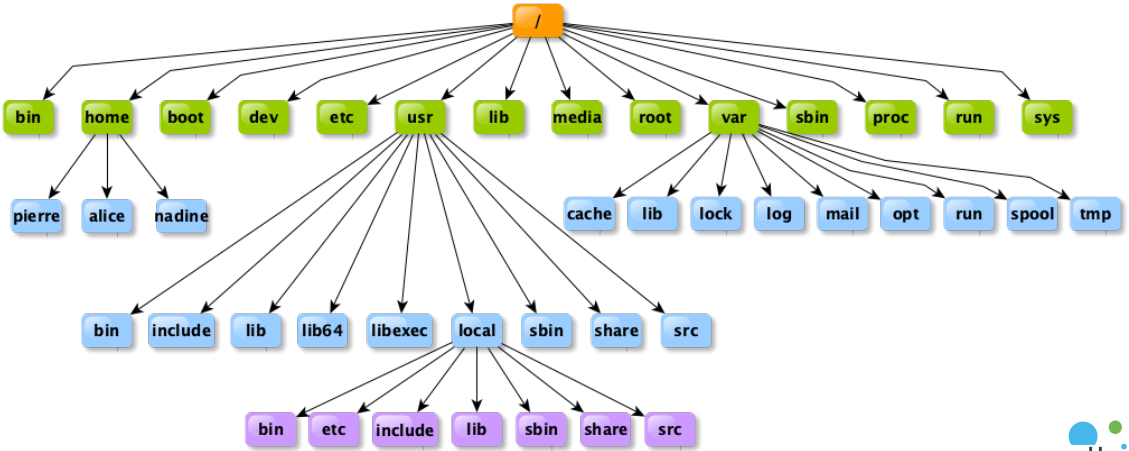
Progression

FHS

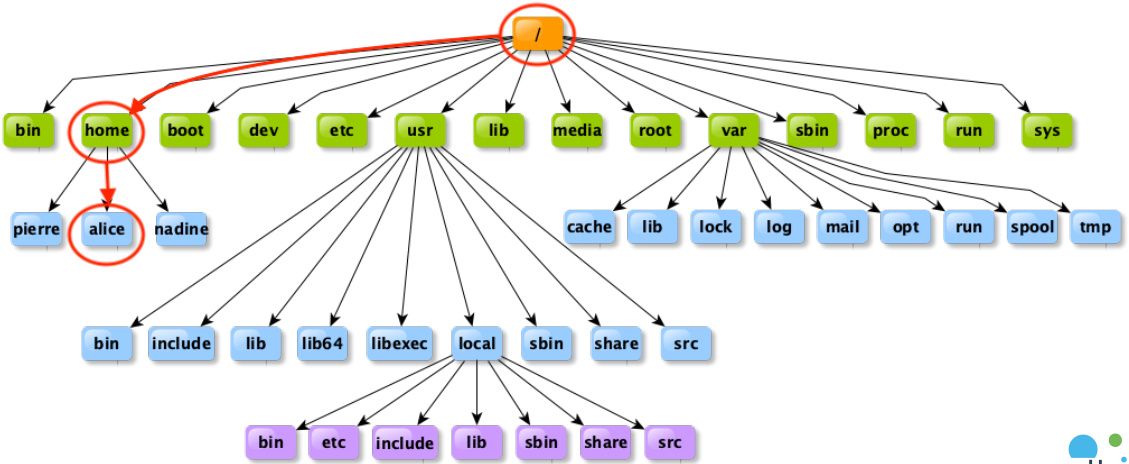
La *Filesystem Hierarchy Standard* est une convention pour le nommage et l'organisation du système de fichier d'un système GNU/Linux.

- Indépendant de la distribution
- Séparation en zones
- Détermine l'emplacement des fichiers selon leur type et usage
- Facilite la maintenance et la recherche de fichiers

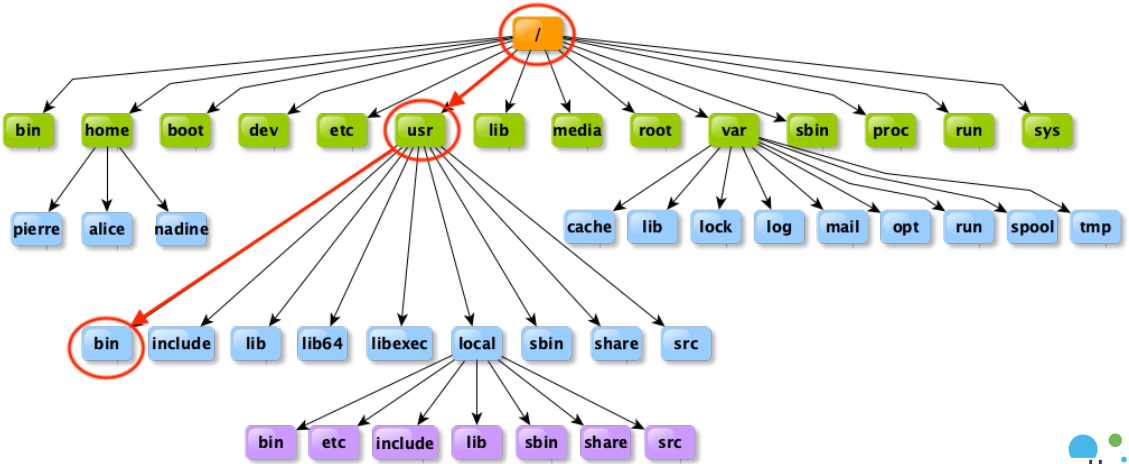
Construction arborescente



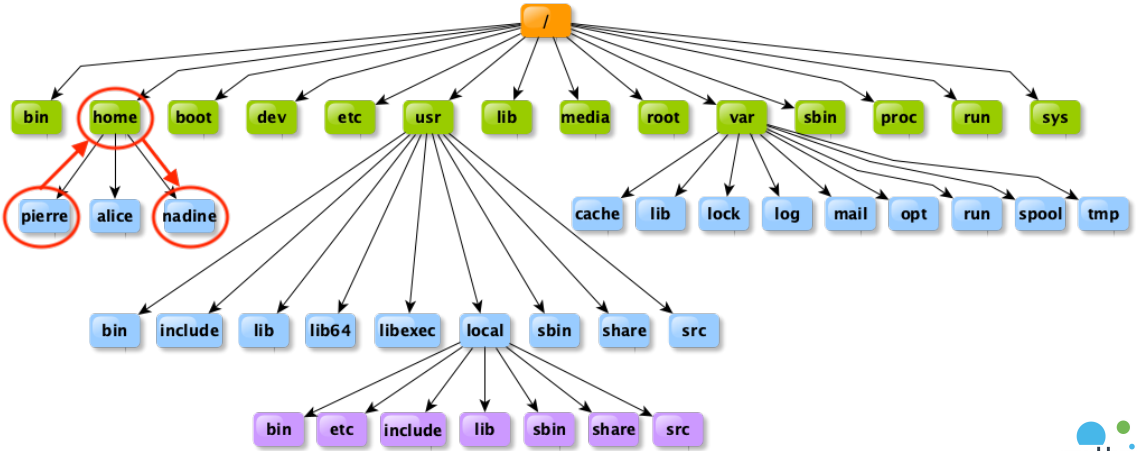
Chemin absolu - /home/alice



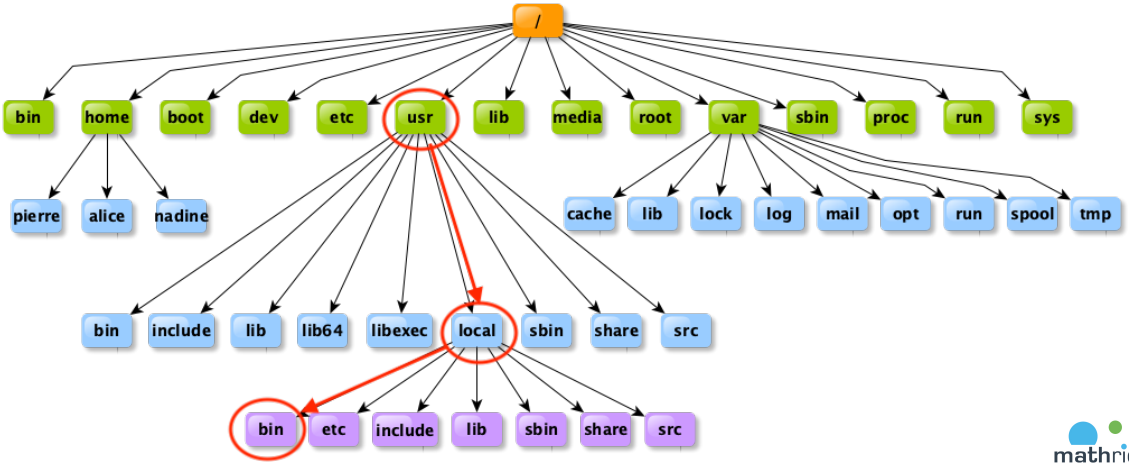
Chemin absolu - /usr/local/bin



Chemin relatif - ../nadine



Chemin relatif - local/bin



Amorçage et périphériques

- */boot* → Fichiers d'amorcage
  - Noyau, image *initrd*
  - Chargeur de démarrage GRUB avec sa configuration
- */dev* → Fichiers de périphériques
  - */dev/sda, /dev/vda, /dev/nvme0* → Disques
  - */dev/sda1, /dev/vdc4, /dev/nvmen0p2* → Partitions des disques
  - */dev/null* → Trou noir
  - */dev/random* → Générateur aléatoire

Les binaires

- */bin* → Les commandes essentielles pour les utilisateurs
- */sbin* → Les commandes essentielles pour le systèmes
- */usr/bin* → Le reste des commandes pour les utilisateurs
- */usr/sbin* → Le reste des commandes pour le système
- */usr/local/bin* → Commandes utilisateurs spécifiques (hors distribution)
- */usr/local/sbin* → Commandes systèmes spécifiques (hors distribution)

Les bibliothèques

- */usr/include* → Fichiers d'en-têtes pour les bibliothèques (compilation)
- */lib* → Bibliothèques essentielles et modules noyau
- */lib64* → Bibliothèques essentielles et modules noyau (64bits)
- */usr/lib* → Bibliothèques pour le développement et les applications
- */usr/lib64* → Bibliothèques pour le développement et les applications (64bits)

La configuration

- Fichiers et sous-dossiers de */etc*
- Organisation spécifique à chaque application

Les répertoires d'accueil

- Les dossiers sous */home*
- Un sous-répertoire par utilisateur

Les données

/var

Ce dossier contient les fichiers de données qui vont bouger au fil du temps. Il est conçu de façon à ce que tout ce qui est présent dans */usr* soit immuable.

- */var/cache* → Cache de données des applications
- */var/lib* → Consigne les informations d'état d'une application de façon persistante
- */var/lock* → Fichiers verrous
- */var/log* → Fichiers journaux
- */var/mail* → Boites à lettres locales de courrier électronique des utilisateurs
- */var/opt* → Données des paquets logiciels installés dans */opt*
- */var/run* → Etat du système. Déplacé vers */run*
- */var/spool* → Données en attente de traitement
- */var/tmp* → Fichier temporaires préservés au redémarrage

Les fichiers journaux du système

- Rangés dans */var/log*
- Archivés et compressés en *.1, .2.gz, .3.gz, .4.gz, ...*
- Un ou plusieurs journaux par application (*.err, .info*)
- Eventuellement un sous-dossier par application (*/var/log/apache2, /var/log/exim4*)
- Mais tout n'est pas ici...

Progression

Vous avez dit *systemd ?*

Définition

Ensemble de composants logiciels pour les systèmes d'exploitation GNU/Linux qui prend en charge le démarrage du système avec une gestion des dépendances entre les services. Il propose également des outils de remplacement pour des utilitaires et des daemons.

- Nom d'hote → *hostnamectl*
- Configuration réseau → *networkd*
- Résolution DNS → *resolved*
- Synchronosation horaire → *timesyncd*
- Gestionnaire de connxions → *logind*

Lire le journal du système sans filtre

```
bash:$ sudo journalctl
Dec 19 18:01:38 pmoptilisto kernel: Linux version 6.12.57+deb13-amd64 (debian-kernel@lists
    .deb>
Dec 19 18:01:38 pmoptilisto kernel: Command line: BOOT_IMAGE=/vmlinuz-6.12.57+deb13-amd64
    root>
Dec 19 18:01:38 pmoptilisto kernel: BIOS-provided physical RAM map:
Dec 19 18:01:38 pmoptilisto kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000057fff]
     usa>
Dec 19 18:01:38 pmoptilisto kernel: BIOS-e820: [mem 0x0000000000058000-0x0000000000058fff]
     res>
Dec 19 18:01:38 pmoptilisto kernel: BIOS-e820: [mem 0x0000000000059000-0x000000000009cfff]
     usa>
Dec 19 18:01:38 pmoptilisto kernel: BIOS-e820: [mem 0x000000000009d000-0x000000000009efff]
     res>
```

- Commence par les plus anciens messages consignés
- Indépendant de la rotation des journaux observés dans */var/log*
- Défileur intégré (page suivante avec espace, flèche droite pour décaler)

Lire le journal de la session utilisateur sans filtre

```
bash:$ journalctl --user
Dec 19 18:02:24 pmoptilisto systemd[1469]: Queued start job for default target default.
    target.
Dec 19 18:02:24 pmoptilisto systemd[1469]: Created slice app.slice - User Application
    Slice.
Dec 19 18:02:24 pmoptilisto systemd[1469]: Created slice session.slice - User Core Session
     Sli>
Dec 19 18:02:24 pmoptilisto systemd[1469]: Reached target paths.target - Paths.
Dec 19 18:02:24 pmoptilisto systemd[1469]: Reached target timers.target - Timers.
```

- Option *–user* pour se connecter au journal de l'utilisateur courant
- Commence par les plus anciens messages consignés
- Défileur intégré (page suivante avec espace, flèche droite pour décaler)

Quelques options pour agir sur l'affichage

```
bash:$ sudo journalctl -r
bash:$ sudo journalctl -n
bash:$ sudo journalctl -n 118
bash:$ sudo journalctl --no-pager
bash:$ sudo journalctl -n --no-pager
bash:$ sudo journalctl --no-pager -n --output=json
bash:$ journalctl --output=help
```

- *-r* → Commencer par la fin
- *-n* → Limiter au 10 derniers évènements
- *-n 118* → Limiter aux 118 derniers évènements
- *–no-pager* → Désactiver le défileur
- *–output=json* → Affichage au format JSON
- *–output=help* → Liste les formats d'affichage prédéfinis
- *–output=short* → Format d'affichage par défaut

Lire le journal depuis le démarrage de l'ordinateur

```
## Messages depuis le dernier demarrage
bash:$ sudo journalctl --boot
Mar 09 08:45:17 pmoptilisto kernel: Linux version 6.12.73+deb13-amd64 (debian-kernel@l>
Mar 09 08:45:17 pmoptilisto kernel: Command line: BOOT_IMAGE=/vmlinuz-6.12.73+deb13-amd>

## Liste des amorcages
bash:$ sudo journalctl --list-boot
IDX BOOT ID                          FIRST ENTRY                 LAST ENTRY
-72 eac913018a9b4fa9a43122ec8d438c15 Fri 2025-12-19 18:01:38 CET Fri 2025-12-19 18:30:17
[...]
 -2 1b46d8bc59264127888a2d6918786da2 Thu 2026-03-05 12:19:36 CET Thu 2026-03-05 17:05:00
 -1 8d1b983c33b54df1b8188c2df718d6ec Fri 2026-03-06 08:45:17 CET Fri 2026-03-06 15:34:33

## Amorcge precedent
bash:$ sudo journalctl --boot=-1 --no-pager
Mar 06 08:45:17 pmoptilisto kernel: Linux version 6.12.73+deb13-amd64 (debian-kernel@li>
Mar 06 08:45:17 pmoptilisto kernel: Command line: BOOT_IMAGE=/vmlinuz-6.12.73+deb13-amd>
[...]
Mar 06 15:34:33 pmoptilisto systemd[1]: Shutting down.
Mar 06 15:34:33 pmoptilisto systemd-shutdown[1]: Syncing filesystems and block devices.
Mar 06 15:34:33 pmoptilisto systemd-journald[322]: Journal stopped
```

Trouver les *daemons* systèmes en cours d'execution

```
bash:$ systemctl list-units --type=service --state=active
  UNIT                              LOAD   ACTIVE SUB     DESCRIPTION
  apparmor.service                  loaded active exited  Load AppArmor profiles
  console-setup.service             loaded active exited  Set console font and keymap
  cron.service                      loaded active running Regular background program proce
  dbus.service                      loaded active running D-Bus System Message Bus
  exim4.service                     loaded active running LSB: exim Mail Transport Agent
  getty@tty1.service                loaded active running Getty on tty1
  keyboard-setup.service            loaded active exited  Set the console keyboard layout
  kmod-static-nodes.service         loaded active exited  Create List of Static Device Nod
  networking.service                loaded active exited  Raise network interfaces
  ssh.service                       loaded active running OpenBSD Secure Shell server
```

Lire le journal d'un service

```
bash:$ sudo journalctl --unit=ssh
Jun 25 14:17:02 debian12 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Jun 25 14:17:02 debian12 sshd[438]: Server listening on 0.0.0.0 port 22.
Jun 25 14:17:02 debian12 sshd[438]: Server listening on :: port 22.
Jun 25 14:17:02 debian12 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Jun 25 14:38:56 debian12 systemd[1]: Stopping ssh.service - OpenBSD Secure Shell server...
Jun 25 14:38:56 debian12 sshd[438]: Received signal 15; terminating.
Jun 25 14:38:56 debian12 systemd[1]: ssh.service: Deactivated successfully.
```

- Option *–unit* pour sélectionner le service voulu
- Affiche le journal depuis le début qu'il existe
- A combiner avec l'option *-n* pour voir les derniers évènements

Lire le journal d'une instance de service

```
bash:$ sudo journalctl --unit=postfix
-- No entries --
bash:$ systemctl list-units --type=service | grep postfix
  postfix.service            loaded active exited  Postfix Mail Transport Agent
  postfix@-.service          loaded active running Postfix Mail Transport Agent (instance
    -)
bash:$ sudo journalctl --unit=postfix@-
janv. 20 15:03:32 sympa-test-pprime.ensma.fr postfix/anvil[1068013]: statistics: max conn>
janv. 20 15:03:32 sympa-test-pprime.ensma.fr postfix/anvil[1068013]: statistics: max conn>
janv. 20 15:03:32 sympa-test-pprime.ensma.fr postfix/anvil[1068013]: statistics: max cach>
```

- Plusieurs instances d'un même service peuvent cohabiter avec différents ports d'écoute
- L'arobase sépare le nom du programme du nom d'instance dans le nom du service

Lire le journal en direct

```
bash:$ sudo journalctl --unit ssh --follow
Mar 09 08:45:19 pmoptilisto systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
Mar 09 09:21:25 pmoptilisto sshd-session[2916]: Accepted password for benoit from
    10.15.47.40 port 57038 ssh2
Mar 09 09:21:25 pmoptilisto sshd-session[2916]: pam_unix(sshd:session): session opened for
     user benoit(uid=1000) by benoit(uid=0)
Mar 09 09:22:39 pmoptilisto sshd-session[3004]: Accepted password for benoit from
    10.15.47.40 port 57054 ssh2
Mar 09 09:22:39 pmoptilisto sshd-session[3004]: pam_unix(sshd:session): session opened for
     user benoit(uid=1000) by benoit(uid=0)
```

- Option *–follow* ou *-f* pour afficher les évènements au fur et à mesure de leur appartition
- Ne rend pas la main
- Interrompre avec Ctrl + c

Lire le journal de la semaine

```
bash:$ sudo journalctl --since='2026-03-02 12:00:00'
Mar 02 12:17:01 pmoptilisto CRON[3995]: pam_unix(cron:session): session opened for user
    root(u>
Mar 02 12:17:01 pmoptilisto CRON[3997]: (root) CMD (cd / && run-parts --report /etc/cron.
    hourl>
Mar 02 12:17:01 pmoptilisto CRON[3995]: pam_unix(cron:session): session closed for user
    root
Mar 02 12:30:01 pmoptilisto CRON[4088]: pam_unix(cron:session): session opened for user
    root(u>
Mar 02 12:30:01 pmoptilisto CRON[4090]: (root) CMD (if [ -x /etc/init.d/anacron ] && ! [ -
    d /r>
Mar 02 12:30:01 pmoptilisto CRON[4088]: pam_unix(cron:session): session closed for user
    root
```

- option *–since* pour filtrer les évènements depuis une date
- date au format `année-mois-jour heure:minute:seconde`

Lire le journal de jeudi entre 9h et 17h39

```
bash:$ sudo journalctl --since='2026-03-05 09:00:00' --until='2026-03-05 17:39:00'
Mar 05 09:00:07 pmoptilisto PackageKit[2855]: daemon quit
Mar 05 09:00:07 pmoptilisto systemd[1]: packagekit.service: Deactivated successfully.
Mar 05 09:00:07 pmoptilisto systemd[1]: packagekit.service: Consumed 16.804s CPU time,
    92.1M m>

[...]

Mar 05 17:05:00 pmoptilisto systemd[1]: Reached target poweroff.target - System Power Off.
Mar 05 17:05:00 pmoptilisto systemd[1]: Shutting down.
Mar 05 17:05:00 pmoptilisto systemd-shutdown[1]: Syncing filesystems and block devices.
Mar 05 17:05:00 pmoptilisto systemd-shutdown[1]: Sending SIGTERM to remaining processes...
Mar 05 17:05:00 pmoptilisto systemd-journald[323]: Received SIGTERM from PID 1 (systemd-
    shutdow).
Mar 05 17:05:00 pmoptilisto systemd-journald[323]: Journal stopped
```

- option *–until* pour filtrer les évènements jusqu'à une date
- date au format `année-mois-jour heure:minute:seconde`

Chercher dans le journal

```
bash:$  sudo journalctl -b --grep='benoit'
Mar 09 08:45:19 pmoptilisto gdm-autologin][894]: pam_unix(gdm-autologin:session): session>
Mar 09 08:45:19 pmoptilisto systemd-logind[747]: New session 1 of user benoit.
Mar 09 08:45:19 pmoptilisto (systemd)[903]: pam_unix(systemd-user:session): session opene>
Mar 09 08:45:19 pmoptilisto systemd-logind[747]: New session 2 of user benoit.

bash:$ sudo journalctl -b --grep='sudo.*ben'
Mar 09 09:28:53 pmoptilisto sudo[3170]: pam_unix(sudo:session): session opened for user r>
Mar 09 09:59:16 pmoptilisto sudo[3598]: pam_unix(sudo:auth): authentication failure; logn>
Mar 09 09:59:29 pmoptilisto sudo[3598]: pam_unix(sudo:session): session opened for user r>
```

- Option *–grep* affiche uniquement les lignes répondant au motif spécifié
- Le motif est une chaine simple ou une expression régulière compatible PERL
- Cherche uniquement dans le contenu des évènements

Filtrer selon l'identification du programme émetteur

```
bash:$ sudo journalctl -b --identifier=systemd
Mar 09 14:56:17 pmoptilisto systemd[1]: Inserted module 'autofs4'
Mar 09 14:56:17 pmoptilisto systemd[1]: systemd 257.9-1~deb13u1 running in system mode>
Mar 09 14:56:17 pmoptilisto systemd[1]: Detected architecture x86-64.
Mar 09 14:56:17 pmoptilisto systemd[1]: Hostname set to <pmoptilisto>.


bash:$ journalctl --user -b --identifier=dynamic-display.desktop
Mar 09 14:56:22 pmoptilisto dynamic-display.desktop[1253]: Driver Info:
Mar 09 14:56:22 pmoptilisto dynamic-display.desktop[1253]:     Driver Name    : i915
Mar 09 14:56:22 pmoptilisto dynamic-display.desktop[1253]:     Adapter Name   : DP-1
Mar 09 14:56:22 pmoptilisto dynamic-display.desktop[1253]:     Capabilities   : 0x0000037e
```

- Option *–identifier* pour afficher uniquement les messages émis par un programme portant ce nom
- Equivalent aux identifiants SYSLOG

Afficher le journal du noyau

```
bash:$ sudo journalctl -k
Mar 09 08:45:18 pmoptilisto kernel: audit: type=1400 audit(1773042318.374:8): apparmor="
    STATUS" ope>
Mar 09 08:45:18 pmoptilisto kernel: audit: type=1400 audit(1773042318.374:9): apparmor="
    STATUS" ope>
Mar 09 08:45:18 pmoptilisto kernel: audit: type=1400 audit(1773042318.374:10): apparmor="
    STATUS" op>
Mar 09 08:45:18 pmoptilisto kernel: input: ydotoold virtual device as /devices/virtual/
    input/input15
Mar 09 08:45:18 pmoptilisto kernel: NET: Registered PF_QIPCRTR protocol family
Mar 09 08:45:22 pmoptilisto kernel: rfkill: input handler disabled
Mar 09 08:45:22 pmoptilisto kernel: e1000e 0000:00:19.0 eno1: NIC Link is Up 1000 Mbps
    Full Duplex,>
Mar 09 09:17:18 pmoptilisto kernel: kauditd_printk_skb: 114 callbacks suppressed
Mar 09 09:17:18 pmoptilisto kernel: audit: type=1400 audit(1773044238.751:125): apparmor="
    DENIED" o>
Mar 09 09:17:18 pmoptilisto kernel: audit: type=1400 audit(1773044238.751:126): apparmor="
    DENIED" o>
```

- Equivalent à la commande *dmesg* sans la limite du buffer

Afficher l'état d'un service

```
bash:$ sudo systemctl status ssh
  ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Mon 2026-03-09 08:45:19 CET; 1h 27min ago
 Invocation: 9cb01b2cdad1484f955518e03f76249e
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 870 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 885 (sshd)
      Tasks: 1 (limit: 4419)
     Memory: 10.6M (peak: 29.1M, swap: 4K, swap peak: 4K)
        CPU: 191ms
     CGroup: /system.slice/ssh.service
             885 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Mar 09 08:45:19 pmoptilisto systemd[1]: Starting ssh.service - OpenBSD Secure Shell server
    ...
Mar 09 08:45:19 pmoptilisto sshd[885]: Server listening on 0.0.0.0 port 22.
Mar 09 08:45:19 pmoptilisto sshd[885]: Server listening on :: port 22.
```

Démarrer / Arreter un service

```
## Stopper le service OpenSSH
bash:$ systemctl stop ssh

## Lancer le service OpenSSH
bash:$ systemctl start ssh

## Relancer le service OpenSSH
bash:$ systemctl restart ssh
```

Bonus : résolution DNS

```
bash:$ resolvectl
Global
         Protocols: +LLMNR +mDNS -DNSOverTLS DNSSEC=no/unsupported
  resolv.conf mode: stub
Current DNS Server: 194.167.50.187
        DNS Servers 194.167.50.187 195.220.223.1 10.15.44.50
         DNS Domain pprime.fr

Link 2 (eth0)
Current Scopes: LLMNR/IPv4 LLMNR/IPv6
     Protocols: -DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
```

Bonus : synchronisation horaire

```
bash:$ timedatectl
               Local time: Sun 2026-03-08 08:04:33 CET
           Universal time: Sun 2026-03-08 07:04:33 UTC
                 RTC time: Sun 2026-03-08 07:04:34
                Time zone: Europe/Paris (CET, +0100)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
```

Progression

Webographie

- Filesystem Hierarchy Standard
  `https://refspecs.linuxfoundation.org/FHS_3.0/fhs/index.html`
- Site web officiel du projet *systemd*
  `https://systemd.io/`
- Maitriser la gestion des Logs avec Journald
  `https://blog.stephane-robert.info/docs/admin-serveurs/linux/journalisation/`
- Matriser la gestion des services Linux avec systemd
  `https://blog.stephane-robert.info/docs/admin-serveurs/linux/services/`