Journalisation des évènements (logs)

*NIX contient un système de **fichiers de journalisation (logs), lesquels enregistrent la trace**

- des **sessions de connexion en cours, précédentes et les plus récentes**
- des **évènements systèmes** (e.g. connexion d'un périphérique)
- des **évènements du fonctionnement des applications**

En générale stockées dans le répertoire `/var/log` ou dans le répertoire personnel des utilisateurs (`/home/`)
Utiles pour détecter les intrusions (connexion ou manipulation malveillante), pour traquer un bug

Logs des sessions de connexion...

en cours stocké dans `/var/run/utmp`
lu avec `who -a`

précédentes depuis le début du mois/de l'installation (dépend configuration de `logrotate`)
stocké dans `/var/log/wtmp`
lu avec *last -aix -n 5*

les plus récentes stocké dans `/var/log/lastlog`
lu avec `lastlog`

En général la structure des fichiers de logs des connexions contient les informations suivantes : login, tty devices utilisés, date et durée de connexion, adresse hôte source, parfois le runlevel...

Astuce : *watch* exécute périodiquement un programmme (ici chaque seconde)

```
$ watch -n 1 who
```

Logs des évènements systèmes et des messages du noyau

Anciennement géré par le démon *syslog-ng* et son fichier de configuration `/etc/syslog.conf`
Nouvellement géré par *rsyslog* (version améliorée et étendue de syslog-ng) avec `/etc/rsyslog.conf` et notamment *the Default logging rules* qui peuvent être trouvées `/etc/rsyslog.d/50-default.conf`
Ce dernier définit notamment

```
auth,authpriv.* /var/log/auth.log
*.*;auth,authpriv.none -/var/log/syslog
#cron.* /var/log/cron.log
daemon.* -/var/log/daemon.log
kern.* -/var/log/kern.log
lpr.* -/var/log/lpr.log
mail.* -/var/log/mail.log
user.* -/var/log/user.log
```

Lisible par un simple éditeur de texte... depuis un compte root

Utiliser journalctl, les logs de systemd

- Voir les logs systèmes : `journalctl`
- En continu sur la console jusqu'à ctrl+C : `journalctl -f`
- Par service : `journalctl -u apache2`
- Par PID : `journalctl _PID=1`
- Par programme : `journalctl /etc/init.d/apache2`
- Par niveau de log (info, warning, err) : `journalctl -p err`
- Par date :
  `journalctl --since "2016-02-10 21:00:00" --until "yesterday"`
- Possibilité de combiner...
- Configurer la taille du journal... `/etc/systemd/journald.conf`

Un peu doublon avec le démon syslog mais log plus structurés et en binaire pour ne pas être lisible

`https://www.linuxtricks.fr/wiki/utiliser-journalctl-les-logs-de-systemd`,

`https://unix.stackexchange.com/questions/332274/is-systemd-journald-a-syslog-implementation`,

`https://www.loggly.com/blog/why-journald/`

Logs spécifiques à chaque utilisateur (shell et applications)

- Contenu dépend des spécificités des démons qui écrivent dedans
- En général lisible en clair avec un simple éditeur de texte
- Soit stocké dans `/var/log/`
  e.g. logs d'apache2 `/var/log/apache2/access.log.1` et `/var/log/apache2/error.log.1`...
- Soit stockées dans le répertoire personnel des utilisateurs (`/home/hernandez`)
  e.g. `.bashrc_history` pour le shell bash qui contient toutes les commandes tapées par l'utilisateur accessible avec la commande *history*
  Pour le désactiver pour le root, placer dans le `~/.bashrc`, la ligne `export HISTFILE=/dev/null`

Astuce : le niveau (debug, info, warn...) des logs d'Apache2 se configure dans `/etc/apache2/apache2.conf`

On peut ensuite les consulter avec journalctl ou bien `tail -f`

`/var/log/apache2/access.log` (error.log, error_ssl.log...)