Lnav, le navigateur de logs

LNAV le navigateur de log

1) Les logs

Les **logs** sont les fichiers dans lesquels sont enregistrés les informations des différents services qui tournent sur une machine.
C'est informations ont un **timestamp** : la date et l'heure, ainsi que différents niveau d'informations **loglevel**: * info * error * warning * alert
Ils ont également différents **format** en fonction de l'application, ou du service .

1.1) Arborescence

Ils sont généralement situés dans `/var/log`:

```
tree -L 2 /var/log
/var/log
├── alternatives.log
├── apt
│   ├── eipp.log.xz
│   ├── history.log
│   └── term.log
├── auth.log
├── auth.log.1
├── bandwidth
├── btmp
├── btmp.1
├── clamav
│   ├── clamav.log
│   ├── clamav.log.1
│   ├── freshclam.log
│   └── freshclam.log.1
├── ConsoleKit
│   └── history
├── cups
│   ├── access_log
│   ├── access_log.1
│   ├── cups-pdf_log
│   ├── error_log
│   ├── page_log
│   └── page_log.1
├── daemon.log
├── daemon.log.1
├── debug
├── debug.1
├── dmesg
├── dpkg.log
├── exim4
├── faillog
├── fontconfig.log
├── fsck
│   ├── checkfs
│   └── checkroot
├── installer
│   ├── cdebconf
│   ├── hardware-summary
│   ├── lsb-release
│   ├── partman
│   ├── status
│   ├── syslog
│   └── Xorg.0.log
├── kern.log
├── kern.log.1
├── lastlog
├── lynis.log
├── lynis-report.dat
├── messages
├── messages.1
├── mysql
├── ntpstats
├── prelink.log
├── rkhunter.log
├── rkhunter.log.old
├── samba
├── slim.log
├── syslog
├── syslog.1
├── teamviewer13
│   ├── install_teamviewerd.log
│   ├── ordinatous -> /home/ordinatous/.local/share/teamviewer13/logfiles/
│   ├── signaturekey.log
│   ├── TeamViewer13_Logfile.log
│   └── TeamViewer13_Logfile_OLD.log
├── tor
├── unattended-upgrades
├── user.log
├── user.log.1
├── wtmp
├── wtmp.1
├── Xorg.0.log
└── Xorg.0.log.old

15 directories, 59 files
```

Ca fait beaucoup de fichiers, néanmoins sous **linux** on sait à peu près toujours ce que l'on cherche..
Je trouve ça plutot clair et pratique, c'est du texte on peut très facilement rechercher une information dedans à coup de `grep`, c'est justement ce qu'il y a d'intéressant dans les fichiers texte.

```
sudo grep "error" /var/log/lynis.log
2018-06-07 16:50:54 Result: grpck binary didn't find any errors in the group files
2018-06-07 16:50:55 Result: mount system / is configured with options: errors=remount-ro
```

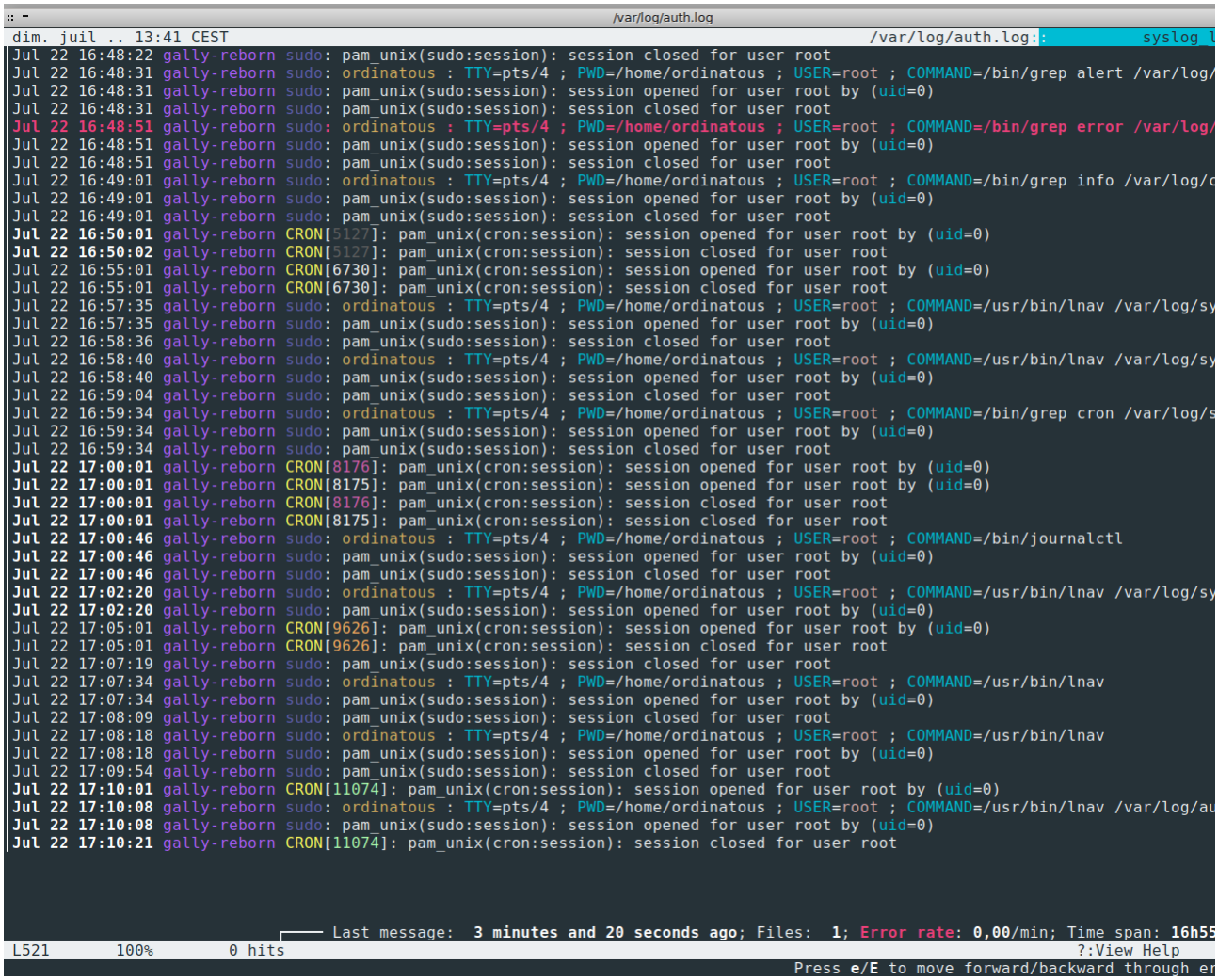
Car non seulement on peut rechercher une occurence , mais on peut transmettre à une application pour traiter ce que l'on a trouvé.

C’est ce qu’on verra avec `sed`, et les `scripts`.Mais revennons à **lnav** et les logs.

2) Lnav

Site de lnav
The log file navigation , est un outil permettant d’avoir une vue plus dynamique , les logs sont rafraichis automatiquement, et il y a une coloration , et ça: c’est vraiment pas mal.

➥ Exemple: `sudo lnav /var/log/auth.log`



lnav_auth

➥ Il garde en mémoire les sessions.
➥ Nous indique le raffraichissement
➥ Egalement le taux d’erreurs par minute.
➥ Le dernier messages
➥ l’heure que l’on peut comparait

2.1) Installation

lnav est dans les dépot en version 0.8.3 * `sudo apt install lnav` Si vous souhaitez compiler vous même, je vous laisse le soin de cloner les dépots Git du projet. Depot Github

2.1.1) Utilisation

Fichier d’aide de **lnav**, car ce dernier dispose de nombreuses fonctionnalités.
Il suffit simplement de lui indiquer quel fichier de **logs** nous souhaitons lire.

➥ `sudo lnav /vat/log/syslog`

Mais il peut lire également les logs archivés. * `sudo /var/log/syslog*`
Il peut même prendre l’intégrale de `/var/log`, par contre c’est un peu plus long.
Pour les fonctionnalités:
Difficile d’en faire le tour ici tellement elles sont nombreuses , je vous recommande de lire le fichier d’aide, ou d’aller sur le site du du projet **lnav**.