CAMPUS DE LONGUEUIL
CÉGEP ÉDOUARD MONTPETIT

Les journaux

Gestion de la journalisation sur Linux

Automne 2022

Séance 06C

Contenu

- ✓ Concepts généraux
- ✓ Journaux textuels sous Linux
- ✓ Voir le contenu / Rechercher dans un fichier journal
- ✓ Principaux journaux
- ✓ Commandes utilisant les logs
- ✓ Rotation des journaux (logrotate)
- ✓ Décompresser les logs archivés
- ✓ Lecture des logs par le GUI

Journalisation (logging)

Lorsqu'un problème survient dans l'un des processus en arrière-plan, il peut être utile de savoir ce qui s'est passé.

Les systèmes d'exploitation et plusieurs applications gardent une trace des étapes importantes de ce qu'ils font (leur démarrage, les erreurs rencontrées, etc.) dans un journal, ou *log*.

Pourquoi les logs sont importants?

Les logs contiennent des informations sur le fonctionnement du système d'exploitation. À quoi servent-ils concrètement?

Auditer le système

Détecter les accès non autorisés

Facturer l'utilisation des ressources

Diagnostiquer les problèmes et les erreurs

etc.

Inconvénients

Cependant, la journalisation peut avoir des impacts négatifs.

Réduire les **performances** du système

Utiliser un **espace disque** important

Augmenter le **temps** d'analyse et de traitement des données

Ce n'est donc pas absolument tout qui est journalisé, mais seulement les événements les plus importants.

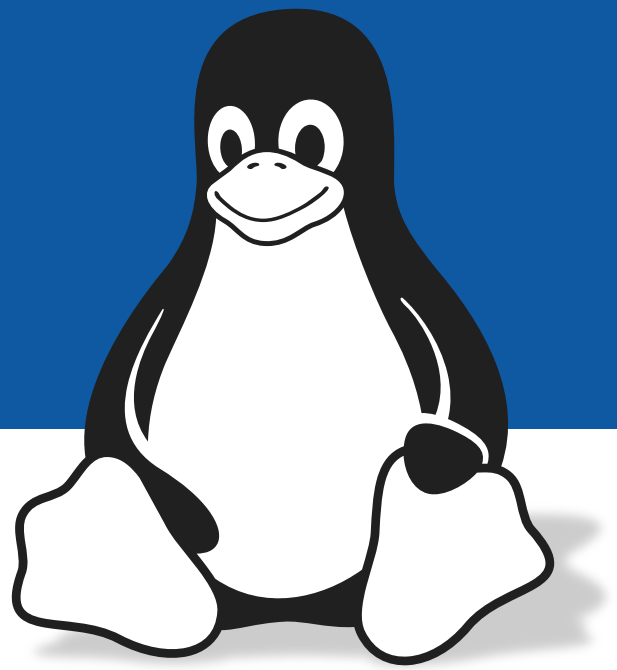
Fichiers log en format texte

La forme la plus rudimentaire des journaux prend la forme d'un **fichier texte**, lisible avec des outils de lecture de texte standard.

Chaque **événement** occupe généralement **une ligne** de texte.

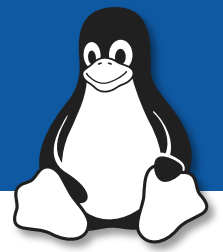
Chaque événement est **horodaté.**

Les événements sont toujours **ajoutés à la fin du fichier**. Les événements à la fin du fichier sont donc les plus **récents**.



Linux

Journaux sous Linux

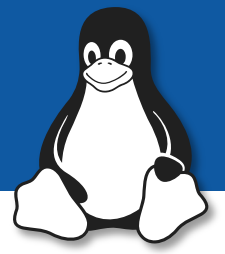


Linux ne possède pas de service de gestion d'évènements comme Windows. La journalisation se fait strictement dans des fichiers texte.

Par convention, les fichiers journaux se trouvent dans le répertoire **/var/log/**

```
etudiant@vmlinux:~$ ls /var/log
alternatives.log    dmesg.2.gz          syslog.2.gz
alternatives.log.1  dmesg.3.gz          syslog.3.gz
apt                 dmesg.4.gz          syslog.4.gz
auth.log            dpkg.log            syslog.5.gz
auth.log.1          dpkg.log.1          syslog.6.gz
auth.log.2.gz       dpkg.log.2.gz       syslog.7.gz
auth.log.3.gz       faillog             ubuntu-advantage.log
auth.log.4.gz       fontconfig.log      unattended-upgrades
boot.log            gdm3                vmware-network.1.log
boot.log.1          gpu-manager.log     vmware-network.2.log
boot.log.2          hp                  vmware-network.3.log
boot.log.3          installer           vmware-network.4.log
boot.log.4          journal             vmware-network.5.log
boot.log.5          kern.log            vmware-network.6.log
boot.log.6          kern.log.1          vmware-network.7.log
boot.log.7          kern.log.2.gz       vmware-network.8.log
bootstrap.log       kern.log.3.gz       vmware-network.9.log
btmp                kern.log.4.gz       vmware-network.log
btmp.1              lastlog             vmware-vmsvc-root.1.log
cups                openvpn             vmware-vmsvc-root.2.log
dist-upgrade        private             vmware-vmsvc-root.3.log
dmesg               speech-dispatcher   vmware-vmsvc-root.log
dmesg.0             syslog              vmware-vmtoolsd-root.log
dmesg.1.gz          syslog.1            wtmp
```

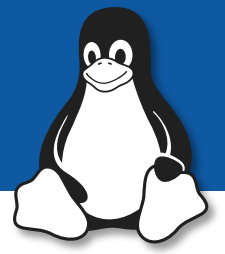
Voir le contenu d'un fichier journal



Un fichier log est un fichier texte. On peut donc les lire au moyen de commandes servant à visionner des fichiers texte: `cat`, `less`, nano, etc.

`cat /var/log/fichier`	*Affiche le journal au complet*
`less /var/log/fichier`	*Affiche le journal page par page*
`nano /var/log/fichier`	*Édite le journal*
etc.	

Afficher une portion d'un fichier journal



Les commandes `head` et `tail` affichent le nombre de lignes au début et à la fin d'un fichier.

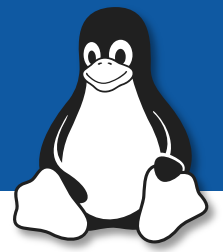
La commande `tail` est généralement très intéressante pour les logs, puisque les événements les plus récents sont à la fin.

Exemple:

```
tail -n 5 /var/log/fichier
```

affiche les 5 dernières lignes

Rechercher dans un fichier journal



On peut utiliser **grep** afin de rechercher des mots clés.

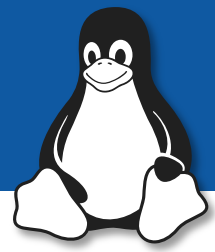
grep motclé /var/log/fichier

```
etudiant@etudiant-virtual-machine:~$ grep bob /etc/passwd
bob:x:1002:1002:,,,:/home/bob:/bin/bash
```

Attention! Linux est sensible à la casse. Utilisez **grep -i** pour faire des recherches en ignorant la casse.

```
etudiant@etudiant-virtual-machine:~$ grep BoB /etc/passwd
etudiant@etudiant-virtual-machine:~$ grep -i BoB /etc/passwd
bob:x:1002:1002:,,,:/home/bob:/bin/bash
etudiant@etudiant-virtual-machine:~$
```

Afficher le rendu « en direct » d'un fichier



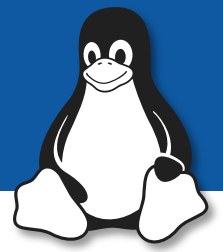
La commande tail peut montrer en direct les modifications d'un fichier.

Commande: `tail -f /var/log/fichier`

Pour quitter: ctrl+C

```
etudiant@etudiant-virtual-machine:/var/log$ tail -f syslog
Oct 17 10:50:41 etudiant-virtual-machine NetworkManager[636]: <info>  [1571323841.6894] dhcp4 (ens33)
Oct 17 10:50:41 etudiant-virtual-machine NetworkManager[636]: <info>  [1571323841.6894] dhcp4 (ens33)
Oct 17 10:50:41 etudiant-virtual-machine NetworkManager[636]: <info>  [1571323841.6894] dhcp4 (ens33)
Oct 17 10:50:41 etudiant-virtual-machine dbus-daemon[606]: [system] Activating via systemd: service n
'dbus-org.freedesktop.nm-dispatcher.service' requested by ':1.10' (uid=0 pid=636 comm="/usr/sbin/Netw
d")
Oct 17 10:50:41 etudiant-virtual-machine systemd[1]: Starting Network Manager Script Dispatcher Servi
Oct 17 10:50:41 etudiant-virtual-machine dhclient[810]: bound to 192.168.64.129 -- renewal in 787 sec
Oct 17 10:50:41 etudiant-virtual-machine dbus-daemon[606]: [system] Successfully activated service 'o
Oct 17 10:50:41 etudiant-virtual-machine systemd[1]: Started Network Manager Script Dispatcher Servic
Oct 17 10:50:41 etudiant-virtual-machine nm-dispatcher: req:1 'dhcp4-change' [ens33]: new request (1
```

Principaux journaux: /var/log/**syslog**

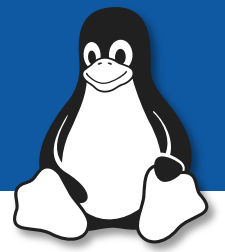


Le *system log* décrit les activités générales du système d'exploitation.

- Changements de configuration
- Erreurs déclenchées dans un service
- etc.

```
Oct 17 11:16:34 etudiant-virtual-machine gnome-software[3899]: no app for changed ubuntu-dock@ubuntu.com
Oct 17 11:17:01 etudiant-virtual-machine CRON[6606]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Oct 17 11:30:34 etudiant-virtual-machine dhclient[810]: DHCPREQUEST of 192.168.64.129 on ens33 to 192.168.64.254 port 67 (xid=0x394328ed)
Oct 17 11:30:34 etudiant-virtual-machine dhclient[810]: DHCPACK of 192.168.64.129 from 192.168.64.254
Oct 17 11:30:34 etudiant-virtual-machine NetworkManager[636]: <info>  [1571326234.8301] dhcp4 (ens33):   address 192.168.64.129
Oct 17 11:30:34 etudiant-virtual-machine NetworkManager[636]: <info>  [1571326234.8303] dhcp4 (ens33):   plen 24 (255.255.255.0)
Oct 17 11:30:34 etudiant-virtual-machine NetworkManager[636]: <info>  [1571326234.8303] dhcp4 (ens33):   gateway 192.168.64.2
Oct 17 11:30:34 etudiant-virtual-machine NetworkManager[636]: <info>  [1571326234.8304] dhcp4 (ens33):   lease time 1800
Oct 17 11:30:34 etudiant-virtual-machine NetworkManager[636]: <info>  [1571326234.8304] dhcp4 (ens33):   nameserver '192.168.64.2'
Oct 17 11:30:34 etudiant-virtual-machine NetworkManager[636]: <info>  [1571326234.8304] dhcp4 (ens33):   domain name 'localdomain'
Oct 17 11:30:34 etudiant-virtual-machine NetworkManager[636]: <info>  [1571326234.8304] dhcp4 (ens33):   wins '192.168.64.2'
Oct 17 11:30:34 etudiant-virtual-machine NetworkManager[636]: <info>  [1571326234.8304] dhcp4 (ens33): state changed bound -> bound
Oct 17 11:30:34 etudiant-virtual-machine dbus-daemon[606]: [system] Activating via systemd: service name='org.freedesktop.nm_dispatcher' unit=
'dbus-org.freedesktop.nm-dispatcher.service' requested by ':1.10' (uid=0 pid=636 comm="/usr/sbin/NetworkManager --no-daemon " label="unconfine
d")
Oct 17 11:30:34 etudiant-virtual-machine dhclient[810]: bound to 192.168.64.129 -- renewal in 710 seconds.
```

Principaux journaux: /var/log/**auth.log**

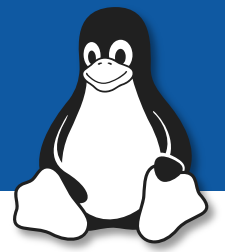


Authentication log

- Contient l'historique des connexions au système (réussies ou non)
- Historique de l'utilisation de la commande sudo (réussie ou non)

```
etudiant@etudiant-virtual-machine:/var/log$ tail -n 10 auth.log
Oct 17 11:17:01 etudiant-virtual-machine CRON[6605]: pam_unix(cron:session): session closed for user root
Oct 17 11:30:59 etudiant-virtual-machine gdm-password]: pam_unix(gdm-password:auth): authentication failure; logname=
d=0 euid=0 tty=/dev/tty2 ruser= rhost=  user=etudiant
Oct 17 11:31:05 etudiant-virtual-machine gdm-password]: gkr-pam: unlocked login keyring
Oct 17 11:32:12 etudiant-virtual-machine sudo: etudiant : TTY=pts/0 ; PWD=/var/log ; USER=root ; COMMAND=/bin/ls -la
Oct 17 11:32:12 etudiant-virtual-machine sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Oct 17 11:32:12 etudiant-virtual-machine sudo: pam_unix(sudo:session): session closed for user root
Oct 17 11:58:58 etudiant-virtual-machine gdm-password]: gkr-pam: unlocked login keyring
Oct 17 12:13:05 etudiant-virtual-machine gdm-password]: gkr-pam: unlocked login keyring
Oct 17 12:17:01 etudiant-virtual-machine CRON[6892]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 17 12:17:01 etudiant-virtual-machine CRON[6892]: pam_unix(cron:session): session closed for user root
etudiant@etudiant-virtual-machine:/var/log$
```

Principaux journaux: /var/log/**apt/history.log**



Historique de l'utilisation de l'outil **apt** (installation, désinstallation, mises à jour, etc.)

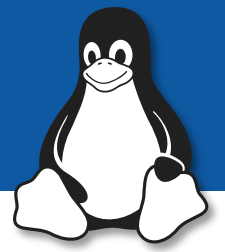
Le format est différent des autres journaux

```
etudiant@etudiant-virtual-machine:/var/log$ tail -n 10 apt/history.log

Start-Date: 2019-10-17  09:26:06
Commandline: /usr/bin/unattended-upgrade
Upgrade: thunderbird-gnome-support:amd64 (1:60.8.0+build1-0ubuntu0.18.04.1, 1:60.9.0+build1-0ubuntu0.18.04.1), thunderb
rd:amd64 (1:60.8.0+build1-0ubuntu0.18.04.1, 1:60.9.0+build1-0ubuntu0.18.04.1), thunderbird-locale-en:amd64 (1:60.8.0+bu
ld1-0ubuntu0.18.04.1, 1:60.9.0+build1-0ubuntu0.18.04.1), thunderbird-locale-fr:amd64 (1:60.8.0+build1-0ubuntu0.18.04.1,
1:60.9.0+build1-0ubuntu0.18.04.1)
End-Date: 2019-10-17  09:26:15

Start-Date: 2019-10-17  09:26:19
Commandline: /usr/bin/unattended-upgrade
Upgrade: libpython3.6-minimal:amd64 (3.6.8-1~18.04.2, 3.6.8-1~18.04.3), libpython3.6-stdlib:amd64 (3.6.8-1~18.04.2, 3.6
8-1~18.04.3), libpython3.6:amd64 (3.6.8-1~18.04.2, 3.6.8-1~18.04.3), python3.6:amd64 (3.6.8-1~18.04.2, 3.6.8-1~18.04.3)
 python3.6-minimal:amd64 (3.6.8-1~18.04.2, 3.6.8-1~18.04.3)
End-Date: 2019-10-17  09:26:25
etudiant@etudiant-virtual-machine:/var/log$
```

Commandes utilisant les logs



`last`

- Montre la dernière connexion réussie pour chaque utilisateur
- Les informations sont obtenues du fichier `/var/log/wtmp`

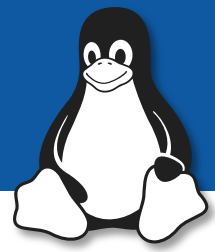
`who`

- Montre les utilisateurs présentement connectés à la machine
- Les informations sont obtenues dans le fichier `/var/log/utmp`

`w`

- Semblable à la commande who, mais donne plus d'informations

Rotation des journaux (logrotate)



Les fichiers journaux grossissent continuellement et peuvent éventuellement prendre tout l'espace disque.

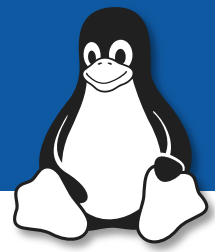
La rotation des logs les empêche de devenir trop gros en archivant les vieux évènements, qui sont moins utiles.

Les vieux fichiers journaux sont automatiquement renommés et compressés avec *gzip*.

Par défaut, les journaux sont conservés pendant 4 semaines.

```
etudiant@etudiant-virtual-machine:/var/log$ ls
alternatives.log    btmp.1          gpu-manager.log
alternatives.log.1  cups            hp
apt                 dist-upgrade    installer
auth.log            dpkg.log        journal
auth.log.1          dpkg.log.1      kern.log
auth.log.2.gz       faillog         kern.log.1
bootstrap.log       fontconfig.log  kern.log.2.gz
btmp                gdm3            lastlog
```

Décompresser les logs archivés

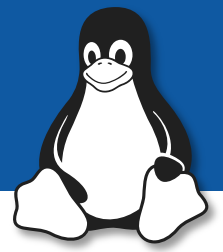


`sudo gzip -d fichier.gz`

```
ual-machine:~$ ls /var/log/
 gdm3                    tallylog
 gpu-manager.log         unattended-upgrades
 hp                      vmware-network.1.log
 installer               vmware-network.2.log
 journal                 vmware-network.3.log
 kern.log                vmware-network.4.log
 kern.log.1              vmware-network.5.log
 kern.log.2.gz           vmware-network.6.log
 kern.log.3.gz           vmware-network.7.log
 kern.log.4.gz           vmware-network.8.log
 lastlog                 vmware-network.9.log
 speech-dispatcher       vmware-network.log
 syslog                  vmware-vmsvc.1.log
 syslog.1                vmware-vmsvc.2.log
 syslog.2                vmware-vmsvc.3.log
 syslog.3                vmware-vmsvc.log
 syslog.4.gz             wtmp
 syslog.5.gz             wtmp.1
 syslog.6.gz
 syslog.7.gz
```

```
virtual-machine:~$ sudo gzip -d /var/log/syslog.4.gz
virtual-machine:~$ ls /var/log/
     gdm3                    tallylog
     gpu-manager.log         unattended-upgrades
.gz  hp                      vmware-network.1.log
     installer               vmware-network.2.log
     journal                 vmware-network.3.log
     kern.log                vmware-network.4.log
     kern.log.1              vmware-network.5.log
     kern.log.2.gz           vmware-network.6.log
     kern.log.3.gz           vmware-network.7.log
     kern.log.4.gz           vmware-network.8.log
     lastlog                 vmware-network.9.log
     speech-dispatcher       vmware-network.log
     syslog                  vmware-vmsvc.1.log
     syslog.1                vmware-vmsvc.2.log
     syslog.2                vmware-vmsvc.3.log
     syslog.3                vmware-vmsvc.log
     syslog.4                wtmp
     syslog.5.gz             wtmp.1
     syslog.6.gz
```

Lecture des logs par le GUI



Recherchez l'application Journaux