


une approche de la ligne de commande: La CLI(deuxième partie)

- Objet : du tuto la ligne de commande
- Niveau requis : tous les pingouins
[débutant](#), [avisé](#)
- Commentaires : *Contexte d'utilisation du sujet du tuto.* ARTICLE EN CONSTRUCTION
- Création par  [lagrenouille](#) 03/02/2020
- Débutant, à savoir : [Utiliser GNU/Linux en ligne de commande, tout commence là !](#) 😊

Introduction



Il existe déjà sur ce wiki plusieurs tutos consacrés aux commandes linux, voir:

<https://debian-facile.org/doc:systeme:commandes:alphabetique>

Voir aussi “les cahiers du débutant”:

[https://debian-facile.org/projets:ebook-facile:lescahiersdudebutant?s\[\]=ligne&s\[\]=de&s\[\]=commandes](https://debian-facile.org/projets:ebook-facile:lescahiersdudebutant?s[]=ligne&s[]=de&s[]=commandes)

Nous allons, ici, tenté de montré, et d'expliqué si nécessaire, quelques unes des commandes de base, puis des commandes nécessaires à des applications.

Nous aborderons quelques approches, sur les groupes, les utilisateurs et les droits sous linux.

Rappel: le prompt c'est \$ pour l'utilisateur et # pour root (administrateur)

Les commandes de base

la commande ls :

commande	option	explication
ls	-l	liste vos répertoires et fichiers par ordre alphabétique
ls	-lha	ordre alphabétique avec les droits de chaque fichiers

ls	-lhaF	F montre les fichiers exécutables avec le signe *
l	a	Le a montre les fichiers cachés
ls	-r	Inverse l'ordre d'affichage
ls	-S	affiche par taille de fichier
ls	-lshaF	commande assez complète
ls	-i	affiche le numéro d'inode du fichier ou du répertoire,
ls	-m	Affichage des éléments en lignes et séparés par des virgules

. . Tout fichier possède son unique inode. (aves ses infos, Type de fichier, Droits d'accès, Nombre de liens, taille, adresse, dernière connexion,lecture,modif

la commande cd:

cd	Permet de se déplacer d'un répertoire à un autre
cd Documents/charles/écritures	Va dans le fichier écriture

La commande mv :renomme ou déplace un fichier

commande	explication
mv toto.txt titi.txt	renomme le fichier toto en titi
mv toto.txt Documents/charles/écritures	Déplace le fichier toto dans le dossier écriture
la commande "pwd	vous indique où vous êtes
pwd	/home/momo/PROGRAMMATION-LINUX/formation-bash-shell

commandes cat, tail, head, more, less: pour Lire vos fichiers :

cat fichier	Lis votre fichier
cat -n fichier	Affiche les numéros de ligne
cat text1.txt test2.txt test3.txt	Concatène et lis les 3 fichiers
cat /etc/apt/source.list	Affiche votre source.list
tail -56 fichier	Affiche les 56 dernières lignes
head -56 fichier	Affiche les 56 premières lignes
more fichier	Lira le fichier page par page
less fichier	Rendra possible la navigation dans la lecture du fichier avec les flèches
less +56 fichier	Ouvrira en plaçant la ligne 56 en haut de page

- créer un fichier texte :

```
touche install-nginx.txt
```

- effacé le fichier texte :

```
rm install-nginx.txt
```

- créer un répertoire WEB:

```
mkdir WEB
```

- créer un répertoire et ses sous-répertoires en une seule commande :

```
mkdir -p
bibliothèque/{littérature_générale,philosophie,sociologie,histoire_sociale}/
{auteur,notes}
```

```
ls -lha bibliothèque/
```

```
total 24K
drwxr-xr-x  6 momo momo 4,0K févr.  2 17:50 .
drwxr-xr-x 16 momo momo 4,0K févr.  2 17:50 ..
drwxr-xr-x  4 momo momo 4,0K févr.  2 17:50 histoire_sociale
drwxr-xr-x  4 momo momo 4,0K févr.  2 17:50 littérature_générale
drwxr-xr-x  4 momo momo 4,0K févr.  2 17:50 philosophie
drwxr-xr-x  4 momo momo 4,0K févr.  2 17:50 sociologie
ls -lha bibliothèque/histoire_sociale/
total 16K
drwxr-xr-x  4 momo momo 4,0K févr.  2 17:50 .
drwxr-xr-x  6 momo momo 4,0K févr.  2 17:50 ..
drwxr-xr-x  2 momo momo 4,0K févr.  2 17:50 auteur
drwxr-xr-x  2 momo momo 4,0K févr.  2 17:50 notes
ls -lha bibliothèque/philosophie/
total 16K
drwxr-xr-x  4 momo momo 4,0K févr.  2 17:50 .
drwxr-xr-x  6 momo momo 4,0K févr.  2 17:50 ..
drwxr-xr-x  2 momo momo 4,0K févr.  2 17:50 auteur
drwxr-xr-x  2 momo momo 4,0K févr.  2 17:50 notes
```

la commande rf :

rm mon fichier	Efface le fichier
rm -rf répertoire	Efface le répertoire et tous fichiers à l'intérieur
rm -rf ./*	Efface tout ce qui est dans le répertoire où vous faite la commande (prudence)
rmdir	supprime un répertoire vide

Les liens symbolique :La commande ln:il faut commencer par le nom du dossier qu'on veut lier, et ensuite mettre le nom du lien.

je fais un site web sur mon serveur et je ne veux pas prendre toute la place dans /var/www/html.

Je vais donc créer et développer mon site dans un DD de 2 Terras fait pour ça. Les données seront donc stockées dans le DD et non dans html, et je fais le lien .

```
ln -s /home/chemin/mon_DD/mon_site /var/www/html/
```

maintenant si je fais un ls -lha /home/chemin/mon_DD/mon_site, et que mon site se nomme sitesting, je verrais le liens comme ceci

```
mon_DD/spidtesting -> /var/www/html/spidtesting/
```

alors que dans /var/www/html

```
ls -lha /var/www/html/
-rw-r--r-- 1 root root 11K août 24 17:27 index.html
-rw-r--r-- 1 root root 21 août 31 16:41 phpinfo.php
drwxrwxrwx 13 momo momo 4,0K sept. 18 15:05 spidtesting
```

quelques commandes réseau

on trouve tous les protocoles supportés de niveau réseau dans le fichier `/etc/protocols`

on trouve tous les services réseau dans `/etc/services`, fournissant une correspondance entre: service Internet: numéro de port : protocole utilisé.

le fichier `/etc/hosts`: Correspondances statiques de noms d'hôtes. Il s'agit d'un fichier de texte simple qui associe les adresses IP avec les noms d'hôtes, une ligne par adresse IP. Pour chaque hôte, une unique ligne doit être présente, avec les informations suivantes : Adresse_IP Nom_officiel [Alias...]

`/etc/fstab` Le fichier `fstab` contient des informations sur les différents systèmes de fichiers. `fstab` est uniquement lus par les programmes, jamais écrit. Chaque système de fichier est décrit sur une ligne indépendante.

Le fichier `/etc/resolv.conf` se compose de deux informations importantes que sont: ``nameserver" qui définit la machine sur laquelle devront être transmises les requêtes DNS c'est à dire les machines permettant de transformer les adresses telles que www.rachat.fr en adresse IP.

Votre fichier `network/interfaces`, c'est votre configuration réseau: Voir les documentations:

<http://debian-facile.org/doc:reseau:interfaces>

<https://wiki.debian.org/fr/NetworkConfiguration>

```
cat /etc/network/interfaces
```

Surveiller mon réseau Lan:

```
netdiscover -i enp3s0 -r 192.168.1.0/24
```

ou encore

```
iftop -i enp3s0
```

ping : la commande ping teste la connexion de votre réseau. teste si une connexion existe entre deux machines. L'affichage donne du délai de la réponse sur votre console et si la connexion n'est pas établie, vous aurez un message.

traceroute ou mtr : outil de diagnostic des réseaux qui permet de déterminer le chemin suivi par un paquet. La commande traceroute permet de donner la liste des routeurs entre la machine sur laquelle on lance la commande et la machine cible.

```
traceroute debian-facile.org
```

```
tracert to debian-facile.org (151.80.145.212), 30 hops max, 60 byte packets
 1 livebox.home (192.168.1.1)  2.081 ms  3.694 ms  5.531 ms
 2 80.10.125.82 (80.10.125.82)  43.212 ms  45.642 ms  47.101 ms
 3 10.123.173.138 (10.123.173.138)  48.839 ms  10.123.173.202
(10.123.173.202)  50.480 ms  51.882 ms
 4 ae44-0.nrp0101.Poitiers.francetelecom.net (193.252.100.50)  54.063 ms
ae44-0.nrp0102.Poitiers.francetelecom.net (193.252.100.54)  58.254 ms
ae44-0.nrp0101.Poitiers.francetelecom.net (193.252.100.50)  63.658 ms
 5 ae45-0.nridf102.Aubervilliers.francetelecom.net (193.251.126.14)  67.585
ms ae45-0.nridf101.Paris3eArrondissement.francetelecom.net (193.251.126.10)
106.527 ms  108.008 ms
 6 ae41-0.noidf001.Paris3eArrondissement.francetelecom.net (193.252.98.102)
103.730 ms ae41-0.noidf002.Aubervilliers.francetelecom.net (193.252.98.106)
52.878 ms ae41-0.noidf001.Paris3eArrondissement.francetelecom.net
(193.252.98.102)  34.430 ms
 7 be100-169.th2-1-a9.fr.eu (91.121.131.193)  37.019 ms be100-101.gsw-1-
a9.fr.eu (91.121.131.49)  47.701 ms  49.732 ms
 8 be102.rbx-g2-nc5.fr.eu (94.23.122.214)  123.545 ms be102.rbx-g1-
nc5.fr.eu (94.23.122.146)  53.235 ms be102.rbx-g2-nc5.fr.eu (94.23.122.214)
63.250 ms
 9 * * *
10 * * *
11 * * *
12 11.ip-151-80-138.eu (151.80.138.11)  51.866 ms  53.638 ms  61.204 ms
13 * * *
14 * * *
15 * * *
16 * * *
```

```
mtr debian-facile.org

My traceroute  [v0.92]

arthur (192.168.1.12)
2020-02-06T09:14:43+0100
Keys:  Help    Display mode    Restart statistics    Order of fields    quit
Packets

Pings
Host                                     Loss%
Snt  Last  Avg  Best  Wrst StDev
 1. livebox.home                                     0.0%
19   1.3   1.3   1.2   2.1   0.2
 2. 80.10.125.82                                     0.0%
19  22.0  20.4  19.4  22.7   0.8
 3. 10.123.173.202                                    0.0%
19  20.4  20.3  19.7  21.4   0.5
 4. ae44-0.nrp0101.Poitiers.francetelecom.net        0.0%
19  25.9  26.4  25.2  27.3   0.5
 5. ae45-0.nridf101.Paris3eArrondissement.francetelecom.net  0.0%
19  30.1  30.5  29.7  31.2   0.5
 6. ae41-0.noidf001.Paris3eArrondissement.francetelecom.net  0.0%
```

```
19  35.9  32.8  30.9  38.7  2.3
7.  be100-169.th2-1-a9.fr.eu          0.0%
19  32.4  32.2  31.3  33.5  0.5
8.  be102.rbx-gl-nc5.fr.eu          0.0%
19  36.5  36.5  35.6  37.6  0.5
9.  ???
10. ???
11. ???
12. 11.ip-151-80-138.eu              0.0%
18  35.0  35.4  34.2  36.6  0.7
13. debian-facile.org               0.0%
18  41.0  35.7  34.3  41.0  1.4
```

voir aussi: pour obtenir que l'ip
dig debian-facile.org +trace

nslookup (de plus en plus délaissé en faveur de la commande dig) la commande nslookup (Name System Look Up) fait partie du paquet dnsutils

dig:La commande dig permet de diagnostiquer les dysfonctionnements dans la résolution de nom et de vérifier vos dns.

```
dig debian.fr

; <<>> DiG 9.11.5-P4-5.1-Debian <<>> debian.fr
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 50686
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1460
; COOKIE: df8a695547654e75337b91255e3bd7353bf6247e2ce014e6 (good)
;; QUESTION SECTION:
;debian.fr.          IN      A

;; ANSWER SECTION:
debian.fr.           86400    IN      A      149.20.4.15

;; Query time: 74 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: jeu. févr. 06 10:07:01 CET 2020
;; MSG SIZE rcvd: 82
```

Si je demande l'adresse ip public de mon serveur auto-hébergé avec la commande:

```
dig funambule.org
;funambule.org.      IN      A

;; ANSWER SECTION:
```

```
funambule.org.      0      IN      A      192.168.1.15
```

j'obtiens l'adresse ip locale car c'est ma box qui réponds

si je demande aux services opendns j'obtiens l'ip public, j'obtiens la bonne ip. (merci du tuyau à captnfab)

```
dig funambule.org @208.67.222.222
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;funambule.org.      IN      A

;; ANSWER SECTION:
funambule.org.      10800    IN      A      92.123.345.102
```

Pour Info OpenDNS est un service gratuit de redirection DNS. Il se consulte via deux serveurs DNS récursifs accessibles sous les IP anycast suivantes : IPv4 : 208.67.222.222 et 208.67.220.220 ; 208.67.222.220 et 208.67.220.222 ; 208.67.222.123 et 208.67.220.123 ; IPv6 (Sandbox) : 2620:0:ccc::2 et 2620:0:ccd::2.

la commande

```
whois -Bd ip
vous donnera des informations supplémentaires.
```

La commande ss:

```
Liste de tous les ports tcp en utilisant

ss -at
Liste de tous les ports UDP en utilisant la commande

ss -ua
Liste Sockets qui sont dans un état d'attente

ss -l
Liste seuls ports tcp en écoute en utilisant

ss -lt
Liste écoute uniquement les ports UDP en utilisant

ss -lou
Liste seulement les ports d'écoute UNIX en utilisant la commande

ss -lx

Voir si un port est à l'écoute (exemple le port 80
ss -ln | grep 80
```

Voir les statistiques pour chaque protocole Voir les statistiques pour tous les ports en utilisant la

commande

```
ss -s
```

ss -laput infos assez complète sur l'état du réseau

ss -ntap (voir en console ce qui entre et sort du pc)

ss -alpe (voir si des ports bloqués)

Voir les statistiques pour les ports TCP et UDP (ou) en utilisant la commande

```
ss -er (ou) -su
```

Savoir rapidement quels services tournent sur votre machine : affichage des noms PID et le programme de sortie de netstat utilisant

```
<code root> ss -p
ss -pt
ss -an fournit un aperçu des sockets qui sont ouvertes sur un système
nsst -c
ss- verbose
ss -r
ss -ap | grep ssh
ss -an | grep ' : 80'
ss -dire
ss -nr permet de connaître la table de routage construite par ifconfig
ss -laputen infos assez complètes sur l'état du réseau
ss -ntap (voir en console ce qui entre et sort du pc)
ss -alpe ( voir si des ports sont bloqués)
ss -tanp |grep LISTEN
voir aussi la commande
ss -ln
```

</code>

ip: les différents ordinateurs sur le réseau sont identifiés par un code chiffré appelé «adresse IP» («IP» signifie «Internet Protocol»)

Pour connaître votre adresse ip locale

```
ip addr
```

Pour connaître votre ip public

```
wget -q http://checkip.dyndns.org -O- | cut -d: -f2 | cut -d\< -f1
ou plus simplement
curl ifconfig.me
```

Voir aussi wput qui est un programme en ligne de commande de chargement (envoi) de fichiers sur le réseau. Il supporte le protocole FTP. :


```
wput monFichier ftp://login:password@serveur/
```

```
ip link list
-
ip address show
-
ip route show
-
ip route list table local
-
ip route list table main
```

curl: un outil qui permet de faire des requêtes à un serveur. Il télécharge vos fichiers à travers divers protocoles (DICT, FILE, FTP, FTPS, Gopher, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMTP, SMTPS, Telnet et TFTP).

Voir les nombreuses doc sur le net

exemple très simpliste, si je veux téléchargé cet article en cours, le -# affiche la barre de progression du téléchargement

```
curl -# -O
https://debian-facile.org/utilisateurs:lagrenouille:tutos:votre-ordinateur-e
n-ligne-de-commande-deuxieme-partie#les-commandes-de-base
```

surveillance réseau

glances:est un outil de surveillance de votre réseau, installez le avec “apt install glances”

affichage en console avec la commande “glances”

affichage dans votre navigateur web “glances -w” vous renvoie l'url à ouvrir.

tcpdump

tcpdump est un analyseur de paquets en ligne de commande. Il permet d'obtenir le détail du trafic visible depuis une interface réseau.

affichage verbeux

```
tcpdump -v
```

Interfaces réseaux disponibles pour la capture

```
tcpdump -D
```

Affichage des adresses numériques plutôt que des adresses symboliques (DNS):

```
tcpdump -n
```

Capture du trafic d'une interface particulière:

```
tcpdump -i enp2s0
```

Capture du trafic du port ssl

```
tcpdump -v port https
```

il peut arriver qu'il y ait un problème avec le port 80, vous pourrez, par l'intermédiaire de cette commande voir l'état du port.

```
nc -zv localhost 80
localhost [127.0.0.1] 80 (http) open
```

plusieurs autres logiciels vous donneront satisfaction, selon ce que vous voulez consulté, essayez ceux là:

Moniteur de ressources système et d'activité de processus Atop est un moniteur en mode texte plein écran, similaire à la commande top, mais qui ne montre que les processus et ressources système actifs, et n'affiche que les différences depuis le dernier intervalle. À intervalle régulier, il affiche l'activité du système concernant l'utilisation du processeur en mode utilisateur et système, de l'évolution de la mémoire virtuelle et résidente, des priorités, des utilisateurs, des états et des codes de sortie. Le niveau d'activité des processus est aussi affiché pour les processus qui se sont terminés lors du dernier intervalle de temps, afin d'avoir un aperçu complet de la consommation d'éléments comme le temps CPU.

```
atop
```

la commande htop liste les processus, vous pouvez retrouver l'utilisateur qu'il l'a exécutée, le pourcentage de mémoire et de CPU qu'il utilise ainsi que la commande qui sert à l'exécuter. * F4 inversera l'ordre de trie. croissant et décroissant. * F9 permet de tuer un processus * F1 affiche de l'aide * F6 permet de choisir le trie par critère, un petit menu déroulant s'affiche pour vous permettre de choisir .

```
htop
```

bmon pour une surveillance réseau et bande passante

```
bmon
```

nmon est un outils de surveillance, permettant de monitorer les ressources physiques des machines qui sont sous Linux nmon peut générer un fichier nmon (ressemblant un peu à du CSV

```
nmon
```

Essayez par exemple de lancez nmon pour capturer les données pendant une heure en faisant une snapshot.(instantané en français) toutes les 30 secondes, en utilisant :

```
nmon -f -s 30 -c 120
```

iptraf. pour voir votre réseau, en temps réel, pour diagnostiquer et vérifier vos le trafic de votre réseau, amusez vous, le menu et ses sous-menu sont plein de petites choses sympa.

```
iptraf-ng
```

tload- représentation graphique de la charge moyenne du système

imprime un graphique de la moyenne de charge du système en cours au tty

- en haut a gauche trois valeurs du temps actif demandé au processeur

- charge moyenne depuis xtemps

- charge moyenne depuis xtemps

- harge moyenne depuis xtemps

depuis ce temps, il y a en moyenne 0,xx processus qui réclament le processeur. Votre processeur est donc actif xx % du temps.

ce nombre dépend du nombre de processeurs de votre ordinateur. Un ordinateur dual core ne sera complètement chargé que lorsque la valeur aura atteint 2. Pour un quad core (4 coeurs de processeur), la valeur maximale avant surcharge sera de 4.

```
tload
```

Pour consulté vos logs à la demande..plus lisible :

```
lnav
```

ssh et rsync

```
apt install openssh-client openssh-server  rsync
```

Ce qui va créer un dossier .ssh et à l'interieur un fichier known_hosts . Si vous avez des clés rsa, elles seront aussi dans ce dossier, vos clés publiques se terminent par .pub.

connexion à un serveur:

```
ssh nom@ip  
ou  
ssh nom@serveur
```

ou si le port est spécifique ssh -P6678 nom@serveur</code>

envoyé un fichier :

```
scp -P2289 monfichier.odt nom@serveur
```

rsync est une commande à rallonge, pleine d'options

```
rsync -pavz nom@hometoto87654.1and1-data.host: /chemin/dossier/machin/
```

<https://linux.die.net/man/1/rsync>

<https://man.developpez.com/man1/rsync/>

commandes utiles et quelques utilitaires pratiques

commandes utiles

```
uname -a
Linux arthur 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11)
x86_64 GNU/Linux
```

```
uname -r
4.19.0-6-amd64
```

Le bash-complétation est installé d'office sur debian.

Avec la touche tab vous tapez le début de la commande et le reste vous sera soit proposé soit affichera la commande complète

afficher l'historique des commandes dans votre console

```
history
```

la commande ncd u affiche le repertoire courant avec le poids de chaque fichier.

```
ncdu
ncdu 1.13 ~ Use the arrow keys to navigate, press ? for help
--- /home/momo/WEB -----
-----
 6,5 GiB [#####] /documentation-linux
 1,5 GiB [##      ] /ADMIN-chezlagrenouille.fr
648,4 MiB [       ] /ADMIN_DEBIAN_FACILE
315,9 MiB [       ] /Serveur-momo
311,2 MiB [       ] /ADMIN-PMB
268,1 MiB [       ] /archivesautonomies
245,0 MiB [       ] /MES_SITES_WEB
228,3 MiB [       ] /ADMIN-P.I.C
189,4 MiB [       ] /BDD
 52,9 MiB [       ] /libreboot
 34,7 MiB [       ] /chatons
 30,3 MiB [       ] /CLICLI
 25,6 MiB [       ] /dolibar
  5,8 MiB [       ] /notes-pour-articles
  5,5 MiB [       ] ordi_en_cli.pdf
```

```

    2,2 MiB [          ] /Heberge_GANDI
    2,0 MiB [          ] /Heberge_OVH-Doc
    1,1 MiB [          ] /garradin_doc
  436,0 KiB [          ] /ADMIN-ESCAL-clippasse
  184,0 KiB [          ] /ascasso-sources
  168,0 KiB [          ] /infos_machine_configurations
   24,0 KiB [          ] facture-auto-collants-bépo-FR20190177.pdf
   16,0 KiB [          ] siteon0-38e4a.jpg
   16,0 KiB [          ] /index-anti-vol
   12,0 KiB [          ] /html
    8,0 KiB [          ] /la_chapelle
@    0,0   B [          ] spidtesting

```

La commande `lspci` affiche la liste de votre matériel, `-v` ou `-vv` pour mode bavard

```
lspci
```

Pour voir votre carte réseau

```

lspci -v | grep Ethernet
02:00.0 Ethernet controller: Intel Corporation 82574L Gigabit Network
Connection
03:00.0 Ethernet controller: Intel Corporation 82574L Gigabit Network
Connection

```

Pour plus d'infos sur votre carte réseau

```
lshw -C network
```

`cal` vous affiche un simple calendrier, `ncal` aligne les jours à gauche du calendrier

```

cal
      Février 2020
di lu ma me je ve sa
                1
 2  3  4  5  6  7  8
 9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29

```

```

date
samedi 8 février 2020, 00:08:42 (UTC+0100)

```

les commandes `ps -e`, `-aux`, `-xl` et `pstree`:

Le processus `INIT`, son `PID` est 1, il est le père de tous les processus, on relance un processus après modif de la configuration avec `/etc/init.d restart "nom du processus"`

la commande `ps -e` liste les processus et retourne 4 colonnes soit : `PID TTY TIME CMD`.

la commande `ps -aux` ou `ps auxww` affiche des infos détaillées, tous les processus et leur identifiant

utilisateur associé sur onze colonne, soit :

USER ...PID ...%CPU...%MEM...VSZ...RSS...TTY...STAT...START...TIME...COMMAND

la commande pstree affiche l'arborescence des processus :

```
pstree
systemd--ModemManager--2*[{ModemManager}]
      |--NetworkManager--dhclient
      |                   |
      |                   +--2*[{NetworkManager}]
      |
      |--agetty
      |--apache2--10*[apache2]
      |--atd
      |--atop
      |--atopacctd
      |--avahi-daemon--avahi-daemon
      |--cron
      |--dbus-daemon
      |--exim4
      |--fail2ban-server--2*[{fail2ban-server}]
      |--glances
      |--lightdm--Xorg--17*[{Xorg}]
      |          |
      |          +--lightdm--lightdm-gtk-gre--18*[{lightdm-gtk-gre}]
      |          |                   |
      |          |                   +--2*[{lightdm}]
      |          |
      |          +--lightdm
      |          |
      |          +--2*[{lightdm}]
      |
      |--loolwsd--forkit--kit_spare_006
      |          |
      |          +--4*[{loolwsd}]
      |
      |--mysqld--37*[{mysqld}]
      |--php-fpm7.3--2*[php-fpm7.3]
      |--polkitd--2*[{polkitd}]
      |--postgres--6*[postgres]
      |--redis-server--3*[{redis-server}]
      |--rsyslogd--3*[{rsyslogd}]
      |--sshd--sshd--sshd--bash--tmux: client
      |      |
      |      +--sshd--sshd--bash--pstree
      |
      |--systemd--(sd-pam)
      |          |
      |          +--at-spi-bus-laun--dbus-daemon
      |          |                   |
      |          |                   +--3*[{at-spi-bus-laun}]
      |          |
      |          +--at-spi2-registr--2*[{at-spi2-registr}]
      |          |
      |          +--dbus-daemon
      |          |
      |          +--gvfsd--2*[{gvfsd}]
      |
      |--systemd--(sd-pam)
      |--systemd-journal
      |--systemd-logind
      |--systemd-timesyn--{systemd-timesyn}
      |--systemd-udev
      |--tmux: server--bash--weechat--{weechat}
      |--udisksd--4*[{udisksd}]
```

Le PID d'un processus peut se récupérer avec la commande "ps -edf | grep "processus". Par exemple pour le processus "apache"

```
ps -edf | grep apache
www-data 6904 10269 0 07:41 ? 00:00:02 /usr/sbin/apache2 -k start
www-data 6905 10269 0 07:41 ? 00:00:02 /usr/sbin/apache2 -k start
www-data 6906 10269 0 07:41 ? 00:00:03 /usr/sbin/apache2 -k start
www-data 6908 10269 0 07:41 ? 00:00:04 /usr/sbin/apache2 -k start
www-data 6909 10269 0 07:41 ? 00:00:03 /usr/sbin/apache2 -k start
www-data 6915 10269 0 07:42 ? 00:00:03 /usr/sbin/apache2 -k start
www-data 6924 10269 0 07:45 ? 00:00:03 /usr/sbin/apache2 -k start
lagreno+ 7112 7092 0 08:31 pts/2 00:00:00 grep apache
root 10269 1 0 févr.03 ? 00:00:10 /usr/sbin/apache2 -k start
```

Le PID du processus Apache est le premier numéro (2ème colonne). Nous pourrions donc spécifier ce numéro comme suivant à la commande lsof pour avoir les fichiers ouverts par apache:

```
lsof -p 6904
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
apache2 6904 www-data cwd DIR 8,2 4096 2 /
apache2 6904 www-data rtd DIR 8,2 4096 2 /
apache2 6904 www-data txt REG 8,2 687944 1184619
/usr/sbin/apache2
apache2 6904 www-data mem REG 8,2 337024 1183204
/usr/lib/locale/aa_DJ.utf8/LC_CTYPE
apache2 6904 www-data mem REG 8,2 200752 1179422
/usr/lib/locale/C.UTF-8/LC_CTYPE
apache2 6904 www-data mem REG 8,2 1517626 1179421
/usr/lib/locale/C.UTF-8/LC_COLLATE
apache2 6904 www-data mem REG 8,2 282752 1178637
/usr/lib/x86_64-linux-gnu/libnss_systemd.so.2
apache2 6904 www-data DEL REG 0,5 972876 /dev/zero
apache2 6904 www-data DEL REG 0,5 972875 /dev/zero
apache2 6904 www-data mem REG 8,2 105672 1210245
/usr/lib/x86_64-linux-gnu/libzip.so.4.0
apache2 6904 www-data mem REG 8,2 67688 1183384
/usr/lib/php/20180731/zip.so
apache2 6904 www-data mem REG 8,2 264320 1195499
/usr/lib/x86_64-linux-gnu/libxslt.so.1.1.32
```

du et df: la commande df permet d'afficher à l'écran la taille de l'espace disque occupée et la taille de l'espace disque libre.

```
df
Sys. de fichiers blocs de 1K Utilisé Disponible Uti% Monté sur
udev 16407620 0 16407620 0% /dev
tmpfs 3292080 42884 3249196 2% /run
/dev/sda2 28705700 8172960 19051524 31% /
tmpfs 16460396 8 16460388 1% /dev/shm
tmpfs 5120 0 5120 0% /run/lock
tmpfs 16460396 0 16460396 0% /sys/fs/cgroup
```

/dev/sda4	2821372528	33837188	2644147436	2%	/home
/dev/sdc	3844641608	133567900	3515706396	4%	/home/malignum
/dev/sdb	3844641608	128769556	3520504740	4%	/home/cumulus
tmpfs	3292076	4	3292072	1%	/run/user/113
tmpfs	3292076	0	3292076	0%	/run/user/1000

la commande du affichera le repertoire courant, le h dans la commande du permet d'affiché le résultat en Megas, Gigas ou en Kilo octet Pour afficher la taille d'un repertoire en kilo octets du -sB K

```
du -sh
33G
```

```
du -sh WEB/
11G WEB/
```

who:La commande who permet d'avoir des informations sur les différents utilisateurs connectés.

```
who
lagrenouille pts/0      2020-02-04 17:33 (192.168.1.12)
lagrenouille pts/1      2020-02-03 12:54 (tmux(1651).%0)
lagrenouille pts/2      2020-02-04 09:39 (192.168.1.12)
```

la commande who -b affiche la date du dernier démarrage du système.

Certaines commandes tel que : **la commande find la commande sed les commandes grep/egrep et la commande awk** possèdent tellement de possibilités que je me contente de les cités.. la commande awk est un véritable langage de programmation à lui seul, vous trouverez un grand nombre de doc sur le web.Ce langage est asé ou inspiré par le langage C.

Syntaxe awk [-Fs] [-v variable] [-f fichier de commandes] 'program' fichier

- F Spécifie les séparateurs de champs
- v Définit une variable utilisée à l'intérieur du programme.
- f Les commandes sont lu à partir d'un fichier.

Je ne mettrai pas d'exemple de cette puissante commande, pour la simple raison que je la connais pas : :o) Je vous abandonne à RTFM.

Quelques exemples avec find et grep:

Supprimer une ligne selon son numéro. Attention les lignes vides sont comptées, ici les lgnés 1,4 et 7 sont supprimées Il faut utiliser l'option d. sed '1d;4d;7d' fichier.txt

Supprimer une ligne selon une REGEX (en faites une "Expressions Regulieres")

Toujours avec l'option d : va supprimer toutes les lignes qui commencent par #

```
sed '/^#/d' fichier.txt
```


Afficher seulement les lignes commentées qui commencent par #

```
sed -n '/^#/p' fichier.txt
```

pour avoir tous les répertoires et sous répertoires

```
find /home -type d
```

nombre de fichiers et répertoires en chiffre : (en root pour tout avoir)

```
find ./ -type f | wc -l
```

nombre de dossiers :

```
find ./ -type d | wc -l
```

pour avoir le nombre de fichier en chiffres dans le répertoire courant

```
find . -name \* | wc -l
```

de fichier en chiffres dans le répertoire WEB

```
find /home/momo/WEB -type d | wc -l
```

autres exemples avec find et grep :

rechercher tous vos fichiers .odt

```
find -name "*.odt" -print
```

cherche tous les répertoires dont le nom se termine par B

```
find . -type d -name "*B" -print
```

tous les .jpg dont le nom comporte oiseaux

```
find -name "*.jpg" -print | grep oiseaux
```

Pour afficher tous les fichiers ayant une permission 444

```
find . -perm 444 -print
```

voir les droits de tous les fichiers dont le nom contient conf `find . -type f -exec ls -lha {} \; | less | grep conf`

ce grep affichera que les fichiers dont le nom se termine par conf dans `/etc/apache2 ls /etc/apache2/ | grep "conf$"`

utilitaires

nano: un éditeur installé d'office sur debian:Le menu s'affiche en bas de page de l'éditeur commande | explication|

Ctrl + O	enregistrer le fichier (écrire)
Ctrl + X	quitter Nano.
Ctrl + W	rechercher dans le fichier
Ctrl + U	coller la ligne de texte que vous venez de couper

Écoutez vos ziques 🎵 🎵 🎵 🎵 🎵 🎵 🎵 🎵 🎵 🎵

```
apt install moc
```

commande moc	explications
mocp	pour lancer l'appli
h	pour l'aide
q	pour quitter

dans ce répertoire

|touches dans moc | explications | |flèche BAS |Déplacer vers le bas dans le menu | |flèche UP | Déplacez-vous dans le menu | |s ou p | pour arrêter la musique | |n |lire le fichier suivant | |b | ESPACE p Pause la touche , réduit le son

la touche maj + ; augmente le son

AVEC D'AUTRES CLAVIERS

la touche > augmente le son (touche , ; pour clavier bépo)

la touche < réduit le son (touche . pour clavier bépo)

compression extraction la commande zip :

zip -r nom_du_fichier.zip nom de l'archive à zipper

exemple pour ziper le fichier blablabla.sql en blablabla.sql.zip

```
zip -r blablabla.sql.zip blablabla.sql
```

Pour décompresser

```
unzip nom_du_fichier.zip
```

Les fichiers tar:

c : crée l'archive

x : extrait l'archive

f : utilise le fichier donné en paramètre

v : active le mode « verbeux

Créer une archive tar:

```
tar -cvf archive.tar nom_dossier_à_compresser
```

Pour extraire un fichier tar

```
tar -xvf archive.tar
```

Compression avec gzip (.tar.gz)

```
tar -zcvf votre_archive.tar.gz nom_dossier_à_compresser
```

Extraction

```
tar -zcvf votre_archive.tar.gz
```

archiver et compresser un dossier avec Gunzip:

```
tar cvzf mon_archive.tar.gz
```

Pour extraire une archive tar.gz

```
tar xf (ou xvf)mon_archive.tar.gz
```

pour archiver en Bzip2:

```
tar cvjf mon_archive.tar.bz2
```

decompresser

```
tar xvjf mon_archive.tar.bz2
```

compresser un fichier en 7zip:

```
7z a nom-de-mon-archive.7z
```

décompresser avec

```
7z x archive
```

Compresser en Lzma:

```
tar cvJf mon_archive.tar.lzma
```

Decompresser

```
tar xvJf mon_archive.tar.lzma
```

task

```
apt install taskwarrior
```

choisissez votre thème en enlevant le commentaire # dans le fichier .taskrc

```
task calendar
```

February 2020								March 2020								April 2020							
May 2020								June 2020															
	Su	Mo	Tu	We	Th	Fr	Sa		Su	Mo	Tu	We	Th	Fr	Sa		Su	Mo	Tu	We	Th	Fr	
Sa		Su	Mo	Tu	We	Th	Fr	Sa		Su	Mo	Tu	We	Th	Fr	Sa		Su	Mo	Tu	We	Th	Fr
5								1	10	1	2	3	4	5	6	7	14				1	2	3
4	18							1	2	23		1	2	3	4	5	6						
	6	2	3	4	5	6	7	8	11	8	9	10	11	12	13	14	15	5	6	7	8	9	10
11	19	3	4	5	6	7	8	9	24	7	8	9	10	11	12	13							
	7	9	10	11	12	13	14	15	12	15	16	17	18	19	20	21	16	12	13	14	15	16	17
18	20	10	11	12	13	14	15	16	25	14	15	16	17	18	19	20							
	8	16	17	18	19	20	21	22	13	22	23	24	25	26	27	28	17	19	20	21	22	23	24
25	21	17	18	19	20	21	22	23	26	21	22	23	24	25	26	27							
	9	23	24	25	26	27	28	29	14	29	30	31					18	26	27	28	29	30	
22	24	25	26	27	28	29	30		27	28	29	30											
23	31																						

Legend: today, due, due-today, overdue, weekend, holiday, weeknumber.

ajouté des travaux à faire:

```
task add installer docker
```

affiché avec

```
task long
```

on peut corrigé, effacé ...supprimé la tâche 9

```
task delete 9
```

voir le man task pour les autres options

buku

```
apt install buku
```

Pour ajouter des marques-pages a votre fichier bookmarks favoris.

```
buku --add https://www.leradeau.org/
```

Pour effacer des marques-pages

```
buku -d 2
```

Pour exporter vos favoris

```
buku -p --nc > bookmark.txt  
et  
buku -p --nc > bookmark.html
```

quelques commandes système

infos mémoire (ram)

```
free -m
```

Pour afficher les informations concernant le micro-processeur cat /proc/cpuinfo

Pour obtenir des informations sur le BIOS d'un ordinateur

```
biosdecode
```

Statistiques périodiques sur l'utilisation du CPU (commande root), cpustat doit être installé

```
cpustat
```

dstat pour savoir à chaque fois quel processus a utilisé le plus de ressources mémoire et disque,

```
dstat --io --top --mem
```

Surveiller son disque dur avec sysstat

```
iostat -tmdx 1
```

vmstat : commande permettant d'afficher des statistiques concernant la charge du système, en particulier l'utilisation de la mémoire virtuelle. donc des statistiques de mémoire virtuelle.

Il est possible de collecter périodiquement en tâche de fond ces mesures via un script

vous en trouverez des exemples sur le web

Ces rapports ont pour but d'aider à identifier les goulots d'étranglement du système. Linux vmstat ne se compte pas comme un processus en cours d'exécution, process qui bouffent trop de mémoire ou qui en perdent...

exemple : avec -w 1 : une nouvelle ligne de rapport est affichée par vmstat toutes les secondes (le 1). le paramètre -w permet d'élargir les colonnes pour éviter un décalage des informations avec de grandes valeurs..

<http://www.delafond.org/traducmanfr/man/man8/vmstat.8.html>

```
vmstat -w 1
ou
vmstat -at
```

Pour récupérer des informations sur le matériel de votre -ordinateur en les collectant depuis le BIOS.

```
dmidecode
```

Pour afficher le tampon des messages du noyau

```
dmesg
```

afficher des informations détaillées sur les périphériques d'un ordinateur

```
lshw
```

Liste des périphériques usb

```
lsusb
```

apt

```
apt-cache show apt
```

Package: apt Version: 1.8.2 Installed-Size: 4064 Maintainer: APT Development Team deity@lists.debian.org Architecture: amd64 Replaces: apt-transport-https (« 1.5~alpha4~), apt-utils (« 1.3~exp2~) Provides: apt-transport-https (= 1.8.2) Depends: adduser, gpgv | gpgv2 | gpgv1, debian-archive-keyring, libapt-pkg5.0 (>= 1.7.0~alpha3~), libc6 (>= 2.15), libgcc1 (>= 1:3.0), libgnutls30 (>= 3.6.6), libseccomp2 (>= 1.0.1), libstdc++6 (>= 5.2) Recommends: ca-certificates Suggests: apt-doc, aptitude | synaptic | wajig, dpkg-dev (>= 1.17.2), gnupg | gnupg2 | gnupg1, powermgmt-base Breaks: apt-transport-https (« 1.5~alpha4~), apt-utils (« 1.3~exp2~), aptitude (« 0.8.10) Description-fr: gestionnaire de paquets en ligne de commande Ce paquet fournit des outils en ligne de commande pour la recherche, la gestion ainsi que la demande d'informations à propos de paquets, le tout grâce à un accès bas niveau aux fonctionnalités de la bibliothèque libapt-pkg. . Ces outils sont : - apt-get pour la récupération de paquets et d'informations à leur sujet depuis des sources authentifiées et pour l'installation, la mise à niveau et la suppression de paquets ainsi que leurs dépendances ; - apt-cache pour consulter les informations disponibles sur les paquets installés et installables ; - apt-cdrom pour utiliser des médias amovibles en tant que source de paquets ; - apt-config qui sert d'interface pour les réglages de configuration ; - apt-key qui sert d'interface pour gérer les clés d'authentification. Description-md5: 9fb97a88cb7383934ef963352b53b4a7 Tag: admin::package-management, devel::lang:ruby, hardware::storage, hardware::storage:cd, implemented-in::c++, implemented-in::perl, implemented-in::ruby, interface::commandline,

```
network::client, protocol::ftp, protocol::http, protocol::ipv6, role::program, scope::application,
scope::utility, suite::debian, use::downloading, use::organizing, use::playing, use::searching, works-
with-format::html, works-with::audio, works-with::software:package, works-with::text Section: admin
Priority: required Filename: pool/main/a/apt/apt_1.8.2_amd64.deb Size: 1418108 MD5sum:
0e80dedab6ec1e66a8f6c15f1925d2d3 SHA256:
80e9600822c4943106593ca5b0ec75d5aafa74c6130ba1071b013c42c507475e
```

affiché votre source.list

```
cat /etc/apt/sources.list
```

mettre les dépôts à jour

```
apt update
```

mettre les paquets deb à jour

```
apt upgrade
```

mettre à jour en prenant en compte toutes les dépendances

```
apt full-upgrade
```

rechercher un paquet

```
apt search paquet
```

ou si l'on veut le paquet seul

```
apt search ^paquet$
```

connaître les dépendances et lire les suggestions

```
apt depends vim
```

Affiche les bugs à l'installatiojn du paquet

```
apt install apt-listbugs
```

installé un paquet deb

```
apt install vim-nox
```

vimcommandes de l'éditeur:

commande	explication
i	Passer dans le mode insertion
A	Ajouter en fin de ligne
:q	Quitter

:q!	Quitter sans enregistrer
:w	Enregistrer le fichier
:wq	Enregistrer et quitter
:x	Enregistrer (seulement en cas de modification) et quitter
:set paste	Passer en mode "collage"
Exemples	Action
u	Annuler la dernière opération
<control>-r	Rétablir la dernière opération annulée
.	Répéter la dernière opération d'édition
yy	Copier la ligne (4yy = 4 lignes)
dd	Couper la ligne (4dd = 4 lignes)
p	Coller après (P = insérer avant)
x	Effacer le caractère
dw	Effacer le texte jusqu'à la fin du mot
diw	Effacer le mot sous le curseur
/	Rechercher du texte
n	Rechercher l'occurrence suivante
N	Rechercher l'occurrence précédente
cw	Remplacer le texte jusqu'à la fin du mot
ciw	Remplacer le mot
C	Remplacer jusqu'en fin de ligne
:%s/A/B/g	Remplacer tous (g) les A par des B
<control-w>-s	Diviser horizontalement
<control-w>-v	Diviser verticalement
<control-w>-w	Passer à la fenêtre suivante
<control-w>-n	Ouvrir un fichier vierge dans une nouvelle fenêtre
: tabnew nom_fichier	Ouvrir le fichier nom_fichier dans un onglet
<control-w>-q	Fermer la fenêtre

si un paquet est mal installé ou si l'on a un doute, on peut tenté«:

```
apt install --reinstall le paquet deb
```

supprimé un paquet et ses dépendances, sachant que vos fichiers de conf perso dans votre home ne seront pas éffacés.

```
apt remove --purge paquet deb
```

effacer les fichiers de paquets en cache déjà installés

```
apt clean
```

conserver un cache local contenant uniquement les versions les plus récentes :

```
apt autoclean
```

apt autoremove souvent conseillé par l'installateur, permet de désinstaller les paquets indiqués

avec leurs dépendances logicielles. Ceci laisse toutefois en place les fichiers de configuration de ces paquets. bien lire et faire attention à cette commande, elle peut parfois désinstallé des paquets qu'il ne faudrait pas.. à vos risques et persil :o)

Autres paquets spécifiques de apt

```
apt install apt-show-source
    Afficher les informations des paquets source

apt install apt-show-versions
    afficher les versions de paquet disponibles dans la distribution

apt install apt-src
    questionnaire des paquets source Debian

apt install apt-transport-https
    transport de téléchargement https pour APT

apt install apt-transport-s3
    transport APT pour les dépôts privés sur AWS S3

apt install apt-transport-spacewalk
    transport APT pour communiquer avec des serveurs Spacewalk

apt -install apt-transport-tor
    transport APT pour les téléchargements de paquets anonymes via Tor

apt install apt-utils
    utilitaires liés à la gestion de paquets

apt install apt-venv
    environnement virtuel apt

apt install apt-xapian-index
    outils de recherche et de maintenance dans un index Xapian des paquets
Debian
```

dpkg

dpkg est le programme principal de gestion des paquets,il peut être exécuté avec beaucoup d'options, je ne mettrai ici que quelques commandes de base, pour le reste voir les man et rtff :o)

Afficher toutes les options :

```
dpkg --help
```

Affiche les paquets installés

```
dpkg -l
ou
```

```
dpkg -l | grep '^i
```

Affiche les paquets mal installés ou mal purgés `dpkg -l | grep -v ^ii`

installer un paquet deb

```
dpkg -i nom du paquet
```

Supprimer un paquet deb et ses fichiers configuration

```
dpkg remove --purge nom du paquet
```

affiche le statut d'un paquet

```
dpkg -s vim-nox
```

`dpkg-reconfigure` des reconfigurations sont faites à partir de `dpkg`

reconfigure de nouvelles locales de votre choix une boîte de dialogue s'ouvre et vous donne le choix de cocher vos locales.

```
dpkg-reconfigure locales
```

Reconfigurer votre clavier

```
dpkg-reconfigure keyboard-configuration
```

Il y en a d'autres, bonne pêche..

Et n'oubliez pas de relancer les services

pdftk c'est ici

<https://debian-facile.org/utilisateurs:lagrenouille:tutos:pdftk>

users et group

La commande `ls -lha` nous permet d'afficher les droits d'un fichier. caché ou pas.

`rwX` : read pour lecture, write pour écriture, x pour exécution

Faites un `ls -lha` sur votre console et vous verrez les droits affectés pour chaque fichier.

Extrait d'une partie de cette commande :

```
ls -lha
drwxr-xr-x  3 lagrenouille lagrenouille 4,0K déc. 27 20:58 .cpanm
```

```
-rw-r--r--  1 lagrenouille lagrenouille    0 oct.  21 23:37 .databases
-rw-r--r--  1 lagrenouille lagrenouille  96M janv.  24 00:23 'Dinner for One
- Original.mp4'
-rw-r--r--  1 lagrenouille lagrenouille    35 oct.   1 14:40 .dmrc
drwxr-xr-x  2 lagrenouille lagrenouille  4,0K sept.  30 17:52 Documents
-rw-r--r--  1 lagrenouille lagrenouille   60K déc.  18 17:37 doli2.png
```

Nous voyons que l'image doli2.png est modifiable par son propriétaire "rw- et "r-juste lisible pour tous les autres

Lorsque il y a un d en première lettre, cela signifie que c'est un répertoires

Les groupes sont disponibles dans le fichier /etc/group

La commande `id` :retourne l'identification de l'utilisateur, permet de lire les group où un user est attaché.

```
id
uid=1000(momo) gid=1000(momo)
groupes=1000(momo),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),33(www-
data),44(video),46(plugdev),109(netdev),114(lpadmin),115(scanner)
```

La commande `group` affiche les groupes auxquels vous appartenez.

```
groups
lagrenouille disk cdrom floppy sudo audio dip www-data video plugdev netdev
scanner lpadmin
```

Nous verrons plus loin et plus en détail les explications sur les droits, les groupes et utilisateurs.

Une équipe de développeur travaillent actuellement sur un module qui permettrait de se passé de sudo, en considérant que donné tous les privilège de root avec l'identifiant 0, peut amené à l'utilisateur sudo à réalisé des installations malveillantes ou à faire des commandes malencontreuses, volontaires ou pas.

Ce nouveau programme découpera les privilèges et donnera les droits aux besoins de ces programmes et pas plus.Lors de l'utilisation d'un processus, pour réalisé une opération, le noyau du système va allé vérifié si le privilège est bien présent et peut être requis et s'il peut être requis.

Actuellement, le fichier /etc/sudoers vous dit ceci :

```
cat /etc/sudoers
[sudo] Mot de passe de toto :
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults    env_reset
```

```
Defaults      mail_badpass
Defaults
secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo    ALL=(ALL:ALL) ALL
```

Vous pouvez aussi faire la commande:

```
sudo -l
```

quelques notions sur les identités

En gros, on a les fichiers ordinaires, les fichiers de configuration, les fichiers de données et des fichiers spéciaux

Tous les fichier se voit attribuer des droits pour 3 identités :

Les droits sont affectés en fonction de vos appartenances .

- 1) le propriétaire - c'est l'utilisateur qui a créé le fichier ou l'utilisateur que root a désigné comme propriétaire
- 2) le groupe (qui n'est pas forcément le groupe du propriétaire)
- 3) les autres (ceux qui ne font pas partie du groupe)

les users et les groupes

je laisserai volontairement de coté les programmes useradd et groupadd, bien que les résultats fournis soient les mêmes.

Ces commandes "adduser" et "addgroup" ajoutent des utilisateurs ou des groupes au système .

adduser est un outil en mode console permettant de créer un compte d'utilisateur de manière interactive, tout comme addgroup.

Lorsqu'il est exécuté avec un seul paramètre qui n'est pas une option et sans les options -system ou -group, adduser ajoute un utilisateur normal.Vous n'êtes pas tenu de répondre aux questions qui

suivent la création et le password.

```
adduser toto
Ajout de l'utilisateur « toto »
Ajout du nouveau groupe « toto »
Création du répertoire personnel « /home/toto »
Copie des fichiers depuis « /etc/skel »
Nouveau mot de passe: rustine
Retapez le mot de passe: rustine
passwd: password updated successfully
Changing The user information for toto
Enter the new value, or press Enter for the default
  Full Name [] : germain letout
  room Number[]: 45678
  work Phone []: 0654348790
  Home Phone []: 7998654324
  Other []:
  Cette information est elle correcte ?[0/n]
```

Pour lui attribuer le mot de passe :

```
passwd toto
saisir le password et le confirmé
```

changé les infos de l'utilisateur toto avec la commande “chfn”

```
chfn toto
```

Les options pour chfn

-f ⇒ Nom complet de l'utilisateur

-r ⇒ N° de bureau

-w ⇒ Téléphone de bureau

-h ⇒ Téléphone personnel

-o ⇒ Autre information

une fois l'utilisateur créer, vous pouvez le placé dans un groupe

```
adduser toto www-data
Ajout de l'utilisateur «toto» au groupe «www-data»
Adding user toto to group www-data
Fait.
```

Si vous faites un “cat /etc/group”, vous verrez que le groupe toto est présent.

La commande “deluser toto ” supprimera l'utilisateur avec tout ce qu'il contient.

Structure de /etc/group

Ce fichier comprend 4 champs, séparés par le symbole :

- 1) nom du groupe
- 2) x pour remplacer un mot de passe non attribué maintenant
- 3) numéro de groupe, c-à-d l'identifiant gid
- 4) la liste des membres du groupe

le systemd

Systemd est une alternative au démon init de System depuis la version Jessie (Debian 8), c'est un gestionnaire de système et de services pour Linux.

```
ls -lha /lib/systemd/system
```

systemd est il actif ?

```
systemctl status systemd-journald
```

lister toutes les unités présentes sur le système.

```
systemctl list-units
```

vérifié si un service est actif, ici apache.

```
systemctl status apache2
```

voir si rien n'est cassé

```
systemctl status
```

si un problème existe, failed et l'erreur seront écrits en rouge

vérification de l'erreur

```
systemctl --failed
```

les logs de démarrage (ça peut être assez long à lire)

```
journalctl -b
```

arrêter un service

```
systemctl stop apache2
```

redémarrer le service avec start ou reload

```
systemctl reload apache2
```

consulter les logs en temps réel

```
journalctl -f
```

Visualiser les erreurs dans le journal

```
journalctl -r -p err
```

les droits et les acl sous linux

chmod

Correspondances des droits en binaire/octale et leurs significations représentés par une chaîne de 9 caractères, regroupés 3 par 3 (rwx rwx rwx), définissent les droits des 3 identités (propriétaire, groupe et les autres). La commande chmod (CHangeMODE) permet de définir et de changer les droits d'accès d'un fichier ou un ensemble de fichiers.

Parmi les options de la commande chmod (qui ne sont pas nombreuses - voir man chmod) je vais en citer seulement deux :

v pour verbose (affichage sur la sortie standard STDOUT du résultat de la commande)

R traiter les répertoires de façon récursive (application de la commande à l'arborescence entière du répertoire en question)

Il y a deux modes d'utilisation de la commande chmod : de façon littérale, de façon numérique.

binaire	octale	droits	explication
000	0	—	aucun droit
001	1	x	exécutable
010	2	-w-	écriture
011	3	-wx	écrire et exécuter
100	4	r—	lire
101	5	r-x	lire et exécuter
110	6	rw-	lire et écrire
111	7	rwx	lire écrire et exécuter

```
Chmod -R 770 documents_administratifs/
```

donne tous les droits au propriétaire et au groupe, sur ce répertoire ainsi que tous les fichiers de ce répertoire

Un chmod 755 donne tous les droits au propriétaire, l'exécution et la lecture au groupe, et aux autres

Les permissions sont soit la lecture read=r, l'écriture write=w et l'exécution .

read = r	write = w	execute = x
----------	-----------	-------------

symbol octale	symbole octale	symbole octale
5 binaire de 100	2 binaire de 10	1 binaire de 001
7	5	5
u=utilisateur	g=groupe	o=autres
4 + 2 + 1 = 7	4 + 1 = 5	4 + 1 = 5

444 = r-r-r- lecture pour tous

644 = rw-r—r— Lecture, écriture pour le propriétaire / Lecture pour les autres

666 = rw-rw-rw- Lecture, écriture pour tout le monde

700 =rwx— — Lecture, écriture, exécution juste pour le propriétaire

705 =rwx—r-x Le propriétaire à tous les droits / Le groupe aucun / Les autres lire et exécuter

755 =rwxr-xr-x Le propriétaire à tous les droits / Les autres lire et exécuter

764 =rwxrw-r— Tous droits pour le propriétaire / Lecture, écriture pour le groupe / Lecture seule pour les autres

774 =rwxrwxr— Tous les droits pour le propriétaire et le groupe / Lecture seule pour les autres

775 =rwxrwxr-x Tous les droits pour le propriétaire et le groupe / Lecture et exécution pour les autres

chmod utilise la notation suivante :

```
u - pour le propriétaire (user)
g - pour le groupe (group)
o - pour les autres (other)
a - pour tous (all)
```

Une autre notation sera utilisée pour attribuer et/ou retirer des droits.

```
+ (plus) pour attribuer
- (moins) pour retirer
-
= (égale) pour fixer l'accès exact
```

```
chmod o+r-w fichier
```

on attribue le droit de lecture (r) mais on retire le droit d'écriture (w) pour les autres (o)

```
chmod u+x,og-w fichier
```

on attribue (+) le droit d'exécution (x) pour le propriétaire (u) et on retire (-) les droits d'écriture (w) pour les membres du groupe (g) et les autres (o).

chown

Pour changer le propriétaire d'un fichier il faut utiliser la commande chown

chown usager fichier

Votre fichier appartient à root, et vous voulez que le propriétaire appartienne www-data et au groupe de lagrenouille

```
chown www-data:lagrenouille /var/www/html/compta/dolibarr/
```

chgrp

Pour changer le groupe d'un fichier : chgrp groupe fichier . La commande « chgrp » est utilisée pour changer le groupe de fichier ou de répertoire Seul l'utilisateur de la racine peut changer les attributs/processus du fichier - R Changer l'autorisation sur tous les sous-répertoires du répertoire(et leurs fichiers) - c Changer l'autorisation pour chaque fichier

changer le groupe de ce fichier qui ne sera plus lagrenouille mais compta

```
chgrp -R compta var/www/html/compta/dolibarr/
```

```
ls -lha
drwxrwxr-x 33 www-data lagrenouille 4,0K janv. 15 10:00 documents
drwxrwxr-x 70 www-data lagrenouille 4,0K nov. 27 11:54 htdocs
```

mais

```
ls -lha
drwxrwxr-x 33 www-data compta 4,0K janv. 15 10:00 documents
drwxrwxr-x 70 www-data compta 4,0K nov. 27 11:54 htdocs
```

Les acl

Permet de mettre des droits d'accès supplémentaires, accorder des privilèges à un ou plusieurs utilisateurs (ou groupes) qui se substitueront aux droits d'accès de base, même si ils ne font pas partie du groupe du fichier.

Quand un utilisateur se connecte sur un système GNU/Linux, il détient 2 UID (UserIdentity) et 2 GID (GroupIdentity) : le réel et l'effectif.

```
id
uid=1000(momo) gid=1000(momo) groupes=1000(momo).....
```

Pour ajouter une ACL, vous devez utiliser la commande setfacl avec l'option -m : Les préfixes disponibles sont toujours les mêmes: ainsi quel les droits rwx.

u : Pour modifier les droits d'un utilisateur

g : Pour modifier les droits d'un groupe

o : Pour modifier les droits du reste du monde (other)

la syntaxe est : préfixe:[utilisateurOuGroupe:]droits

donner le droits de lecture et écriture à l'utilisateur momo sur un fichier. setfacl -m u:momo:rw-

mon_fichier.txt

donner les droits lecture et ecriture à momo sur tout le repertoire web (le R est avant le m) setfacl -Rm u:momo:rw web/

pour que les sous-dossiers de web profitent de ce droit il faudra rajouter d: setfacl -m d:u:momo:rw web/

Si vous voulez que les autres bénéficient de ces droits dans web setfacl -m d:u:momo:rw,o:— web/

avec -d au début rw sera un droit par défaut pour momo et tous les autres dans le repertoire web. setfacl -dm u:momo:rw,o:— web/

pour supprimé tous les droits dans le repertoire web setfacl -b web/

On voit donc que les droits sont affichés par une série de 9 caractères, associé 3 par 3 (rwx rwx rwx) définissent les droits des 3 identités (u,g et o).

Au lieu de donner l'accès à un fichier, on donne le droit d'accès à une commande. Le kernel (ou noyau), au moment de l'exécution de la commande endosse l'identité du propriétaire ou du groupe de la commande au lieu de celle de l'utilisateur qui a lancé la commande.

setfacl: Cette commande permet l'attribution des acl. Voici quelques explications sur son utilisation.

Spécifier des permissions pour plusieurs utilisateurs/groupes à la fois, pour cela, séparez-les par une virgule : Ici l'utilisateur momo à tous les droits, toto a le droit de lecture_écriture, mais pas d'exécution, (ce qui peut être contradictoire) le groupe testeur le droit de lire et de listé le répertoire

```
setfacl -m u:momo:rwx,u:toto:rw,g:testeur:r,o:--- mutualisation
```

ou

momo peut modifier le fichier, toto et testeur peuvent juste lire et exécuter

```
setfacl -m u:momo:rwx,u:toto:rx,g:testeur:rx,o:--- mutualisation
```

getfacl: Cette commande permet l'affichage des acl .

avez vous accès aux acl sur votre machine ?

```
grep ACL /boot/config-*
```

```
/boot/config-4.19.0-4-amd64:CONFIG_EXT4_FS_POSIX_ACL=y
/boot/config-4.19.0-4-amd64:CONFIG_REISERFS_FS_POSIX_ACL=y
/boot/config-4.19.0-4-amd64:CONFIG_JFS_POSIX_ACL=y
/boot/config-4.19.0-4-amd64:CONFIG_XFS_POSIX_ACL=y
/boot/config-4.19.0-4-amd64:CONFIG_BTRFS_FS_POSIX_ACL=y
/boot/config-4.19.0-4-amd64:CONFIG_F2FS_FS_POSIX_ACL=y
/boot/config-4.19.0-4-amd64:CONFIG_FS_POSIX_ACL=y
/boot/config-4.19.0-4-amd64:CONFIG_TMPFS_POSIX_ACL=y
/boot/config-4.19.0-4-amd64:CONFIG_JFFS2_FS_POSIX_ACL=y
```

```
/boot/config-4.19.0-4-amd64:CONFIG_NFS_V3_ACL=y
/boot/config-4.19.0-4-amd64:CONFIG_NFSD_V2_ACL=y
/boot/config-4.19.0-4-amd64:CONFIG_NFSD_V3_ACL=y
/boot/config-4.19.0-4-amd64:CONFIG_NFS_ACL_SUPPORT=m
/boot/config-4.19.0-4-amd64:CONFIG_CEPH_FS_POSIX_ACL=y
.....

/boot/config-4.19.0-8-amd64:CONFIG_F2FS_FS_POSIX_ACL=y
/boot/config-4.19.0-8-amd64:CONFIG_FS_POSIX_ACL=y
/boot/config-4.19.0-8-amd64:CONFIG_TMPFS_POSIX_ACL=y
/boot/config-4.19.0-8-amd64:CONFIG_JFFS2_FS_POSIX_ACL=y
/boot/config-4.19.0-8-amd64:CONFIG_NFS_V3_ACL=y
/boot/config-4.19.0-8-amd64:CONFIG_NFSD_V2_ACL=y
/boot/config-4.19.0-8-amd64:CONFIG_NFSD_V3_ACL=y
/boot/config-4.19.0-8-amd64:CONFIG_NFS_ACL_SUPPORT=m
/boot/config-4.19.0-8-amd64:CONFIG_CEPH_FS_POSIX_ACL=y
/boot/config-4.19.0-8-amd64:CONFIG_CIFS_ACL=y
/boot/config-4.19.0-8-amd64:CONFIG_9P_FS_POSIX_ACL=y
```

apparemment, oui

le sticky bit

Donc l'accès au fichier se fait par le biais de la commande et non pas directement.

Pour placer le sticky bit, le SUID ou le SGID il faut causer en octal, c'est plus pratique.

1777 (le 777 est ici un exemple, cela peut-être 755 ou autre...)

2777

4777

Pour faire simple :

1000 correspond au sticky bit,

2000 correspond au SUID

4000 correspond au SGID.

Quand on écrit les permissions en octal, setuid, setgid et sticky bit sont représentés par une nouvelle série de 3 bits, qui se place avant les 3 autres séries: setuid=4, setgid=2, sticky=1. Ainsi, sur ma machine, le serveur de mail /usr/sbin/sendmail a les droits rwsr-sr-x (rwxr-xr-x, setuid, setgid); en octal, ça donne 6775.

le droit SUID

Son flag est la lettre s ou S qui vient remplacer le x du propriétaire.

droit d'exécution du propriétaire) qui est donc masqué par le droit SUID 's' ou 'S'

C'est un s si le droit d'exécution du propriétaire est présent, ou un S sinon —s— ou —S—

Un fichier avec les droits

```
- rwxr-xr-x
```

auquel on ajoute le droit SUID aura donc la notation

```
rwsr-xr-x
```

Le droit SUID possède la valeur octale 4000. Exemple : - r w s r - x r - x correspond à 4755 (chmod 4755)

le droit SGID

ce droit est appliqué aux groupes

quand vous créez un fichier, normalement, vous en êtes l'utilisateur et le propriétaire. vous êtes aussi dans un ou plusieurs groupes.

Si vous créez votre fichier dans un répertoire ayant les droits SGID, il se verra automatiquement attribué le groupe de ce répertoire

le droit SGID aura donc la notation

a la place de

```
- rwxr-r-
```

vous aurez

```
- rwxr-Sr-
```

Le droit SGID possède la valeur octale 2000. (chmod 2744 répertoire)(chmod -R 2744 répertoire)

Exemple : - r w x r - S r - - correspond à 2744

le sticky bit

Dixit wikipedia: "Ce droit est utilisé pour manier de façon plus subtile les droits d'écriture d'un répertoire. En effet, le droit d'écriture signifie que l'on peut créer et supprimer les fichiers de ce répertoire. Le sticky bit permet de faire la différence entre les deux droits."

Lorsque ce droit est positionné sur un répertoire, il interdit la suppression d'un fichier qu'il contient à tout utilisateur autre que le propriétaire du fichier

Le droit sticky bit possède la valeur octale 1000.

Exemple : - r w x r - x r - t correspond à 1755. (chmod 1755)

Son flag est le t ou T, qui vient remplacer le droit d'exécution x des autres utilisateurs que le propriétaire et ceux appartenant au groupe du fichier

chmod -R 1700 stick/

```
ls -lha stick/
total 16K
drwx-----T  2 momo momo 4,0K févr. 13 12:44 .
drwxr-xr-x 80 momo momo 12K févr. 13 12:44 ..
-rwx-----T  1 momo momo   0 févr. 13 12:38 lapinous.txt
```

From:

<http://debian-facile.org/> - Documentation - Wiki

Permanent link:

<http://debian-facile.org/utilisateurs:lagrenouille:tutos:votre-ordinateur-en-ligne-de-commande-deuxieme-partie>

Last update: 12/08/2020 10:22

