

# Optez pour une transformation digitale intelligente

L'INTELLIGENCE ARTIFICIELLE AU SERVICE DE VOTRE BUSINESS.



## ADMINISTRATEUR LINUX



# SOMMAIRE

1. LINUX?
2. INSTALLER LINUX ET SES APPLICATIONS.
3. ADMINISTRER LE SYSTÈME AVEC LES COMMANDES DU MODE TEXTE.
4. GÉRER L'ESPACE DISQUE.
5. GÉRER L'ARRÊT ET LE REDÉMARRAGE.
6. CONFIGURER TCP/IP EN ENVIRONNEMENT LINUX.
7. LES FONDAMENTAUX DE LA SECURITE.
8. DIVERS.

# I- C'EST QUOI LINUX?

Histoire – Caractéristiques – Outils - Documentation



# I-C'EST QUOI LINUX?

**1-1. L'Historique Unix – Linux.**

**1-2. Les caractéristiques de Linux.**

**1-3. Les fonctionnalités de Linux.**

**1-4. Les Unix-Like.**

**1-5. Les distributions Linux.**

**1-6. La documentation Linux.**

Happy 30th birthday Linux

From: torvalds@Klaava.Helsinki.FI (Linus Benedict Torvalds)

Newsgroups: comp.os.minix

Subject: What would you like to see most in minix?

Summary: small poll for my new operating system

Message-ID:

Date: 25 Aug 91 20:57:08 GMT

Organization: University of Helsinki



Hello everybody out there using minix -

I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones. This has been brewing since april, and is starting to get ready. I'd like any feedback on things people like/dislike in minix, as my OS resembles it somewhat (same physical layout of the file-system (due to practical reasons) among other things).

I've currently ported bash(1.00) and gcc(1.40), and things seem to work. This implies that I'll get something practical within a few months, and I'd like to know what features most people would want. Any suggestions are welcome, but I won't promise I'll implement them :-)

Linus (torvalds@kruuna.helsinki.fi)

PS. Yes - it's free of any minix code, and it has a multi-threaded fs. It is NOT protable (uses 386 task switching etc), and it probably never will support anything other than AT-harddisks, as that's all I have :-(.

## I-I UN PEU D'HISTOIRE

Le système **Unix** est un système d'exploitation **multi-utilisateurs**, **multi-tâches**, ce qui signifie qu'il permet à un ordinateur **mono** ou **multi-processeurs** de faire exécuter simultanément plusieurs programmes par un ou plusieurs utilisateurs.



Il possède un ou plusieurs **interpréteurs** de commandes (shell) ainsi qu'un grand nombre de commandes et de nombreux utilitaires (assembleur, compilateurs pour de nombreux langages, traitements de texte, messagerie électronique, ...).

Il possède une grande portabilité, ce qui signifie qu'il est possible de mettre en oeuvre un système Unix sur la quasi-totalité des plates-formes matérielles.

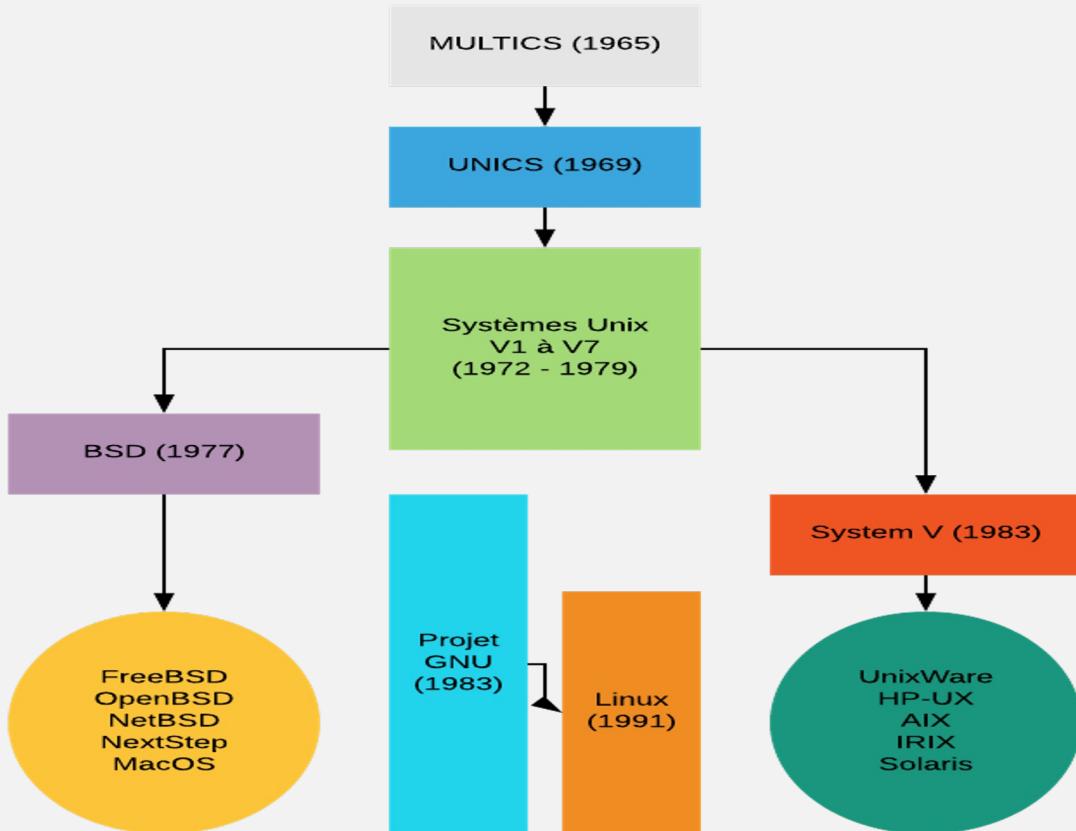
**Sécurité** élevé et le respect des grands standards, notamment en matière de réseau.

# I-I UN PEU D'HISTOIRE

- C'est en 1969 que Kenneth THOMPSON, employé chez Bell, développe un nouveau prototype de système à temps partagé ; son nom est Unics et sera Unix.
- Entre 1970 et 1975, Unix devient le système portable et officiel pour les institutions et les universités.
- En 1980, des chercheurs de l'université de Berkeley développent leur propre UNIX (BSD).
- En 1983, la société ATT tente une commercialisation d'un UNIX système V et de concurrencer l'UNIX BSD.
- En 1984, Richard Stallman lance le projet GNU qui vise à créer son système 'Unix' complètement libre.
- En 1988, c'est le début d'une normalisation avec l'organisation 'IEEE' et la norme 'POSIX' pour les développements d'applications autour d'un système UNIX.
- En 1991, un étudiant finlandais, Linus TORVALDS, créé un noyau UNIX qui a été ajouté aux travaux du projet GNU de Stallman, a donc donné naissance à GNU/Linux.



# I-I UN PEU D'HISTOIRE



## I- 2 LES CARACTÉRISTIQUES LINUX

- “**Linux ou GNU/Linux** est une famille de systèmes d'exploitation open source de type Unix fondé sur le noyau Linux, créé en 1991 par Linus Torvalds.“
- Le noyau de Linux est monolithique et modulaire.
- Ses versions sont numérotées, et ses sources sont disponibles sur le site de Linux Kernel Archives (x.y.z).
- Linux est :
  - Gratuit.
  - Open Source
  - Sécurisé
  - Multitâches.
  - Multi-utilisateurs
  - Stable
  - Scalable

Dernière version stable

5.11.16 (18/04/2021)

# I- 3 LES FONCTIONNALITÉS LINUX

## **Gestion des ressources de l'ordinateur**

Multi-tâches

Multi-utilisateurs

## **Gestion des données**

Accès aux unités de stockage (mémoire, disques durs, CD, etc.)

## **Communication entre utilisateurs**

Courrier électronique, transferts de fichiers (ftp)

## **Environnement de programmation**

Compilateurs C, éditeurs de textes (emacs, nedit), ...

## I- 4 LES UNIX-LIKE

- **UNIX-LIKE** : Un système d'exploitation de **type Unix** (en anglais :**Unix-like**) est un système d'exploitation qui se comporte d'une façon semblable à un système Unix, bien que n'étant pas nécessairement conforme ou certifié par une quelconque version de la Single UNIX spécification.

*LINUX est un système d'exploitation de type Unix ou « Unix-Like ».*

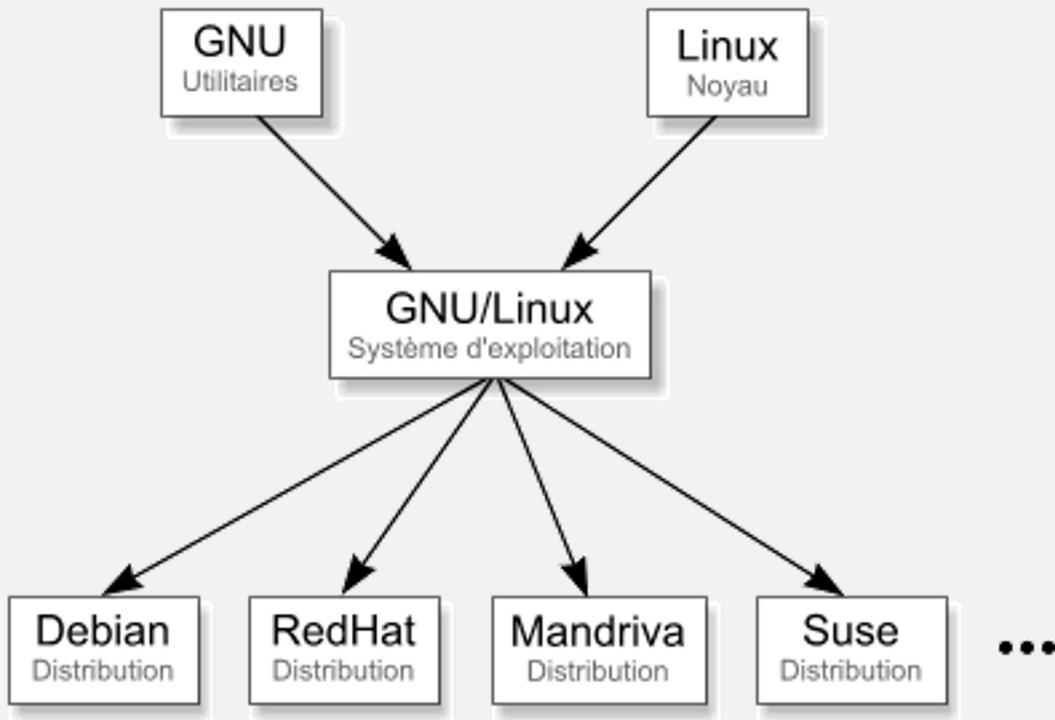
*(Il ne contient pas de code originel Unix mais il fonctionne comme système Unix).*

*Ex : macOs est un système d'exploitation UNIX (SUS / POSIX)*

## I- 5 LES DISTRIBUTIONS LINUX

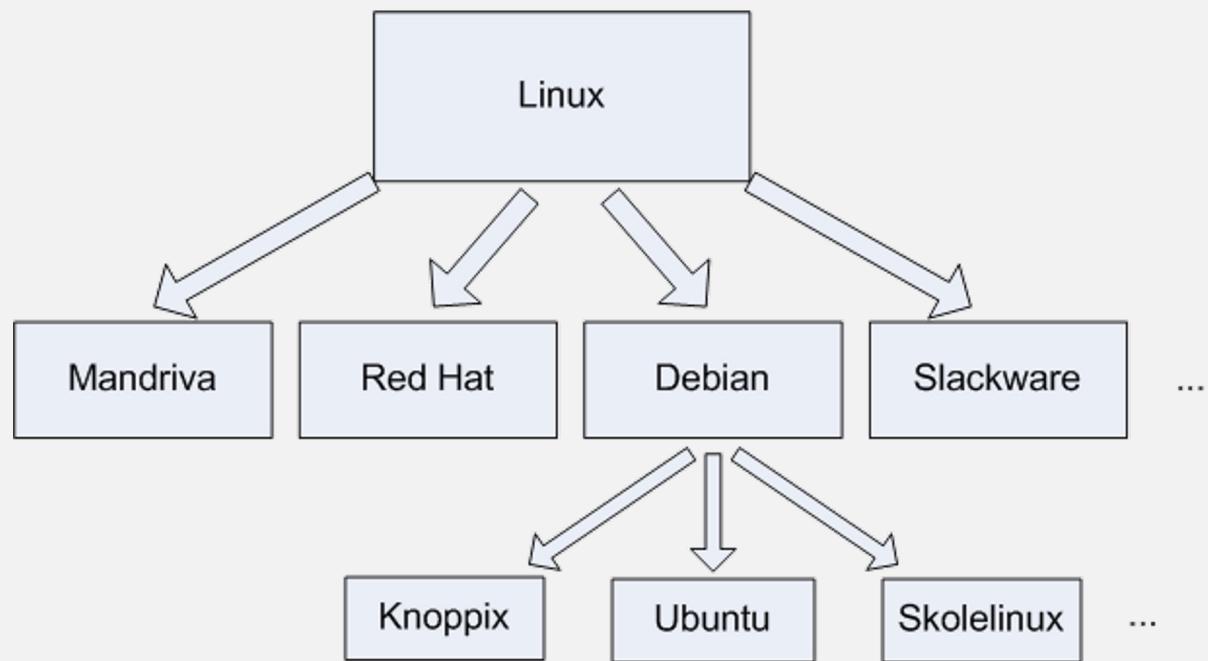
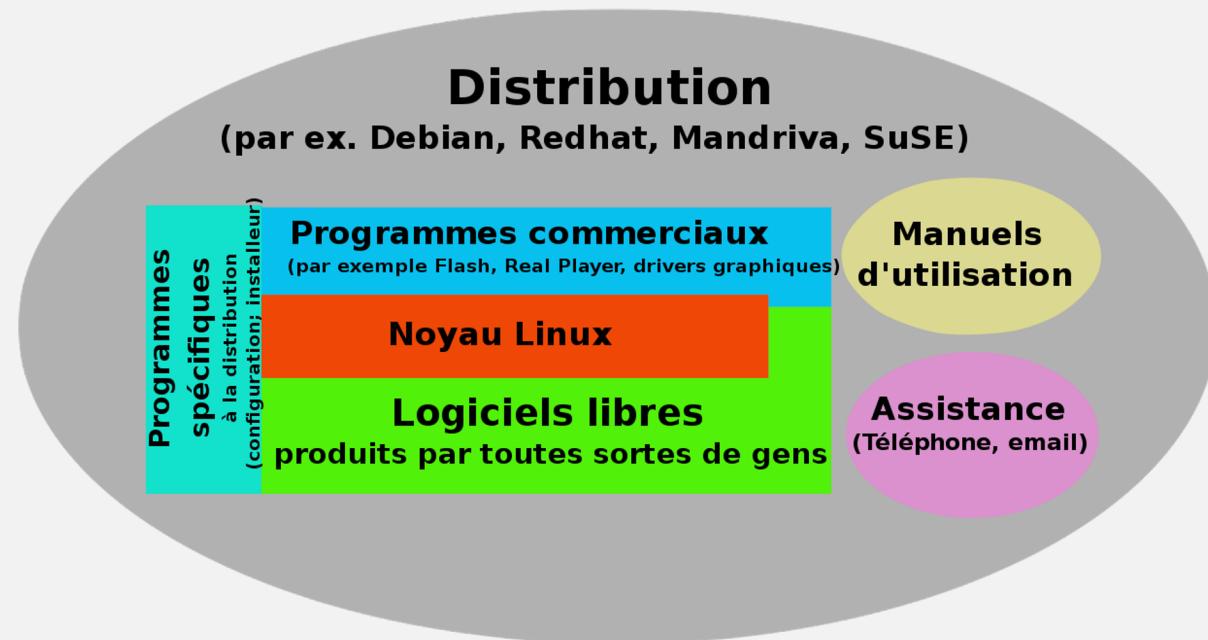
- On appelle distribution **GNU/Linux** (ou distribution Linux) une solution prête à être installée par l'utilisateur final.
- Une distribution Linux se compose d'un noyau, de packages, et d'outils pour gérer leurs dépendances.
- Les distributions sont développées pour répondre à un besoin (serveur, poste de travail ou autre).
- Debian, Red Hat et Slackware sont les 3 premières distributions Linux historiques.
- **Exemple connu :** Ubuntu est une distribution dérivée de Debian.

# I- 5 LES DISTRIBUTIONS LINUX



Les distributions Linux

# I- 5 LES DISTRIBUTIONS LINUX



## I- 4 LES DISTRIBUTIONS LINUX

Quelques distributions :

Nom	Site web	Editeur	Spécificités
 debian	<a href="http://Debian.org">Debian.org</a>	Projet open source	Distribution Linux pour serveur et ordinateur. Cette distribution est notamment connue pour avoir été retenue par la ville de Munich pour équiper 14 000 ordinateurs.
 fedora	<a href="http://Red Hat Enterprise / getfedora.org">Red Hat Enterprise / getfedora.org</a>	Red Hat	Distribution Linux pour serveur. Son éditeur Red Hat est le principal pure player des systèmes serveur open source. Il enregistre un chiffre d'affaires de 2 milliards de dollars.
 ubuntu	<a href="http://Ubuntu.com">Ubuntu.com</a>	Canonical	Distribution Linux pour ordinateur et serveur reposant sur la distribution Debian. Elle a aussi donné lieu à des déclinaisons pour TV (Ubuntu TV), smartphone (Ubuntu Touch), et IoT (Snappy Ubuntu Core)

## I- 6 LA DOCUMENTATION LINUX

- 2 sources de documentations principales officielles (LDP \* ) :
  - MAN : est une commande UNIX permettant d'accéder aux pages de manuel installées sur le système.
  - HOWTO : Les HOWTO Linux sont des documents "comment faire" détaillés sur des sujets spécifiques. L'index des HOWTO répertorie tous les HOWTO ainsi que de brèves descriptions.



# I- 6 LA DOCUMENTATION LINUX

La documentation « man » : 1356 documents

## LES DIFFÉRENTES SECTIONS :

1. Commandes utilisateur
2. Appels système
3. Fonctions de bibliothèque
4. Fichiers spéciaux
5. Formats de fichier
6. Jeux
7. Divers
8. Administration système
9. Interface du noyau [Linux](#)

## COMMANDES ET DOC DÉTAILLÉ :

- **Syntaxe :**
  - man [option] [section number] [command name]
- **Document détaillé :**
  - NAME
  - SYNOPSIS
  - DESCRIPTION
  - AUTHOR
  - REPORTING BUGS
  - COPYRIGHT
  - SEE ALSO

# I- 6 LA DOCUMENTATION LINUX

Résultat commande « man man » :

```
MAN(1)                                         Manual pager utils                                         MAN(1)

NAME
    man - an interface to the system reference manuals

SYNOPSIS
    man [man options] [[section] page ...] ...
    man -k [apropos options] regexp ...
    man -K [man options] [section] term ...
    man -f [whatis options] page ...
    man -l [man options] file ...
    man -w|-W [man options] page ...

DESCRIPTION
    man  is  the  system's  manual  pager.  Each  page  argument  given  to  man  is  normally  the  name  of  a  program,  utility  or  function.  The  manual  page  associated  with  each  of  these  arguments  is  then  found  and  displayed.  A  section,  if  provided,  will  direct  man  to  look  only  in  that  section  of  the  manual.  The  default  action  is  to  search  in  all  of  the  available  sections  following  a  pre-defined  order  (see  DEFAULTS),  and  to  show  only  the  first  page  found,  even  if  page  exists  in  several  sections.

    The  table  below  shows  the  section  numbers  of  the  manual  followed  by  the  types  of  pages  they  contain.

    1   Executable  programs  or  shell  commands
    2   System  calls  (functions  provided  by  the  kernel)
    3   Library  calls  (functions  within  program  libraries)
    4   Special  files  (usually  found  in  /dev)
    5   File  formats  and  conventions,  e.g. ./etc/passwd
    6   Games
    7   Miscellaneous  (including  macro  packages  and  conventions),  e.g. man(7), groff(7)
    8   System  administration  commands  (usually  only  for  root)
    9   Kernel  routines  [Non  standard]

    A  manual  page  consists  of  several  sections.

    Conventional  section  names  include  NAME,  SYNOPSIS,  CONFIGURATION,  DESCRIPTION,  OPTIONS,  EXIT  STATUS,  RETURN  VALUE,  ERRORS,  ENVIRONMENT,  FILES,  VERSIONS,  CONFORMING  TO,  NOTES,  BUGS,  EXAMPLE,  AUTHORS,  and  SEE  ALSO.

    The  following  conventions  apply  to  the  SYNOPSIS  section  and  can  be  used  as  a  guide  in  other  sections.

    bold  text          type  exactly  as  shown.
    italic  text        replace  with  appropriate  argument.
    [-abc]             any  or  all  arguments  within  [ ]  are  optional.
    -a|-b              options  delimited  by  |  cannot  be  used  together.
    argument ...       argument  is  repeatable.
    [expression] ...    entire  expression  within  [ ]  is  repeatable.

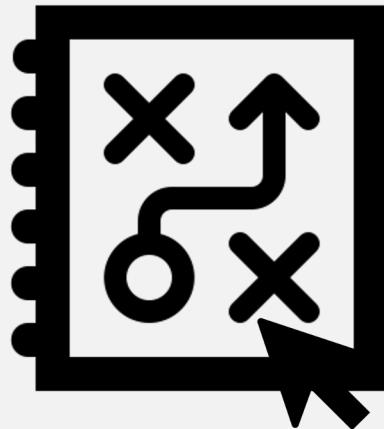
    Exact  rendering  may  vary  depending  on  the  output  device.  For  instance,  man  will  usually  not  be  able  to  render  italics  when  running  in  a  terminal,  and  will  typically  use  underlined  or  coloured  text  instead.

    The  command  or  function  illustration  is  a  pattern  that  should  match  all  possible  invocations.  In  some  cases  it  is  advisable  to  illustrate  several  exclusive  invocations  as  is  shown  in  the  SYNOPSIS  section  of  this  manual  page.

EXAMPLES
    man ls
    Man page man(1) line 1 (press h for help or q to quit)
```



## UN PETIT QUIZ



## 2- INSTALLATION LINUX ET APPLICATIONS



Rappel – Présentation – Installation distributions – Installation applications

## 2 - INSTALLATION LINUX ET APPLICATIONS

**2-1. Rappel.**

**2-2. Présentations de 2 distributions.**

**2-3. Installation de Fedora et Debian.**



**2-4. Installation d'applications sous RedHat(Fedora)**

**2-5. Installation d'applications sous Debian.**

## 2 - I RAPPEL

- **Linux** ou **GNU/Linux** est une famille de systèmes d'exploitation open source de type Unix fondé sur le noyau Linux, créé en 1991 par Linus Torvalds. De nombreuses distributions Linux ont depuis vu le jour et constituent un important vecteur de popularisation du mouvement du logiciel libre.
- Il existe plusieurs distributions Linux :
  - **Slackware** : une des plus anciennes distributions de Linux. Elle existe encore aujourd'hui !
  - **Mandriva** : éditée par une entreprise française, elle se veut simple d'utilisation ;
  - **Red Hat** : éditée par une entreprise américaine, cette distribution est célèbre et très répandue, notamment sur les serveurs ;
  - **SuSE** : éditée par l'entreprise Novell ;
  - **Debian** : la seule distribution qui soit gérée par des développeurs indépendants plutôt que par une entreprise. C'est une des distributions les plus populaires.



## 2 -2 PRÉSENTATION DE 2 DISTRIBUTIONS

**2 distributions  
GNU/Linux**



**debian**

## 2 -2 PRÉSENTATION DE 2 DISTRIBUTIONS



FEDORA



DEBIAN

- Crée en 2002 ( distribution dérivée RedHat)
- Editer par le projet Fedora (RedHat).
- 3 variantes : Workstation, Server et Cloud.
- 8 ème distribution Linux en terme de popularité.
- Gestion de paquets par RPM et DNF.
- Nouvelle version tous les 6 mois.
- Plus : Sécurité – relation Gnome – Gestion de paquets

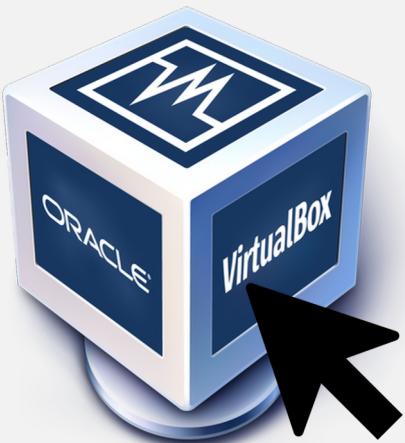
- Crée en 1993.
- Editer par Debian Project (Projet Communautaire).
- Distribution dérivée => Ubuntu, Linux Mint.
- Gestion des paquets par Apt Dpkg.
- Dernière version : version 11 Bullseye (14/08/2021)
- Plus : Sécurité – server – non commerciale – communauté.

## 2-3 INSTALLATION DES DISTRIBUTIONS LINUX

### **Les étapes générales d'installation d'une distribution Linux**

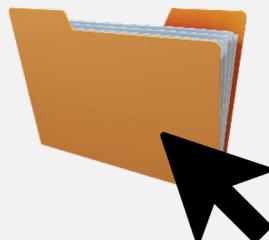
- Amorçage du système.
- Création ou redimensionnement des partitions du disque dur.
- Création des systèmes de fichiers et de la partition d'échange.
- Installation du système proprement dite.
- Installation du gestionnaire d'amorçage.
- Configuration du système.

## 2-3 INSTALLATION DES DISTRIBUTIONS LINUX



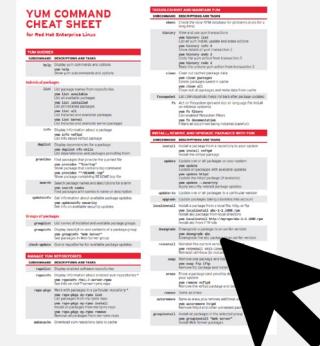
## 2-4 INSTALLATION DES APPLICATIONS SOUS FEDORA

- L'installation de programmes ou d'applications s'effectue, sous Red Hat, avec la notion de package.
- Un package est un fichier qui contient le produit à installer et des règles.
- Les règles peuvent variées :
  - Gestion des dépendances.
  - Pré-installation.
  - Post-installation.
- Le format du package par défaut est le *RPM* ( Red Hat Package Manager).
- Les informations concernant les logiciels installés sont contenues dans une bdd que contient /var/lib/rpm.
- Le package de chaque logiciel doit respecter cette nomenclature : « nom-version-edition.architecture.rpm ».
- Exemple : [php-8.0.10~RC1-3.fc36.aarch64.rpm](#)
- Requête RPM :
  - ex => rpm -i php-4.1.2-2.1.8.i586.rpm (install package php).
  - Ex => rpm -q -a => affiche la liste de tous les packages installés dans la distribution.



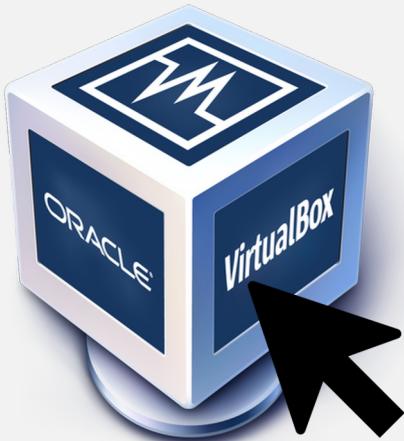
## 2-4 INSTALLATION DES APPLICATIONS SOUS FEDORA

- **YUM** est un logiciel de gestion de packages.
- Il récupère les packages au sein de dépôts et gère les dépendances à votre place.
- **YUM** signifie Yellow dog Updater Modified.
- Il est principalement utilisé sur les distributions Redhat et Fedora.
- Le fichier de configuration est /etc/yum.conf.
- Requête avec YUM :
  - Exemple installation : **yum install mc.** => installation du package Midnight Commander ( Gestionnaire de fichier).
  - Vérification mise à jour : **yum check-update.**
  - Rechercher un package : **yum search tomcat** => recherche un package dans les différents dépôts.



## 2-4 INSTALLATION DES APPLICATIONS SOUS FEDORA

Un peu de pratique



## 2-5 INSTALLATION DES APPLICATIONS SOUS DEBIAN

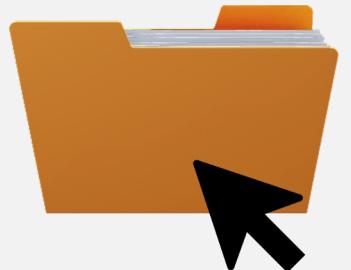
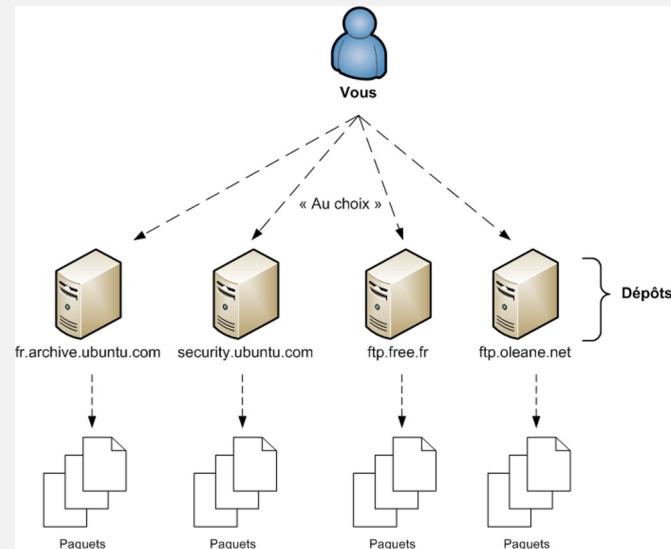
- Notion de paquets ou package comme sous Fedora (RedHat).
- Les paquets sous Debian ont une extension en .deb ( **Debian**).
- Comme avec Fedora, il y un principe de gestion des dépendances.
- Les paquets sont regroupés dans des dépôts.
- **Un dépôt** : c'est le serveur sur lequel on va télécharger nos paquets.
- La gestion de paquet se fera grâce à « apt-get » ( apt-cache) ou à « dpkg ».
- Avec dpkg (Debian package), les dépendances ne sont pas gérées.

## 2-5 INSTALLATION DES APPLICATIONS SOUS DEBIAN

### GESTION PAQUET AVEC APT-GET (GESTION DÉPENDANCE)

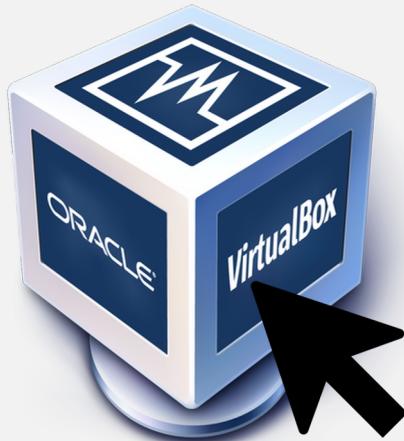
- **apt-get update** : Cela va permettre de mettre à jour la liste des paquets présents dans le dépôt. A faire régulièrement.
- **apt-get install <package\_name>** : installer un nouveau package sur votre ordinateur.
- **apt-cache search <package\_name>** : pour rechercher le paquet que nous voulons télécharger si nous ne connaissons pas son nom exact.
- **apt-get remove <package\_name>** : Supprimer le paquet mais les dependances inutiles.
- **apt-get autoremove <package\_name>** : Supprimer le package ainsi que les dependances inutiles.
- **apt-get upgrade** : Cela met à jour les paquets installés et corrige aussi les failles de sécurité.

### GESTION PAQUET SOUS UBUNTU



## 2-4 INSTALLATION DES APPLICATIONS SOUS DEBIAN

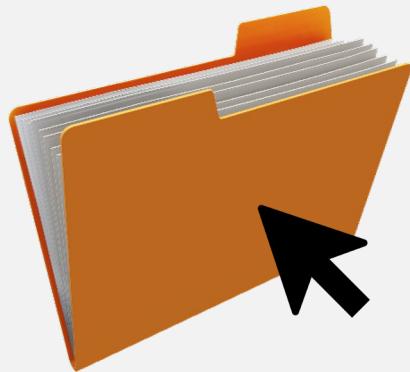
Un peu de pratique





TP TIME

TP\_0 INSTALLATION\_APPLICATION :



## 3 - ADMINISTRER LE SYSTÈME AVEC LES COMMANDES CONSOLE

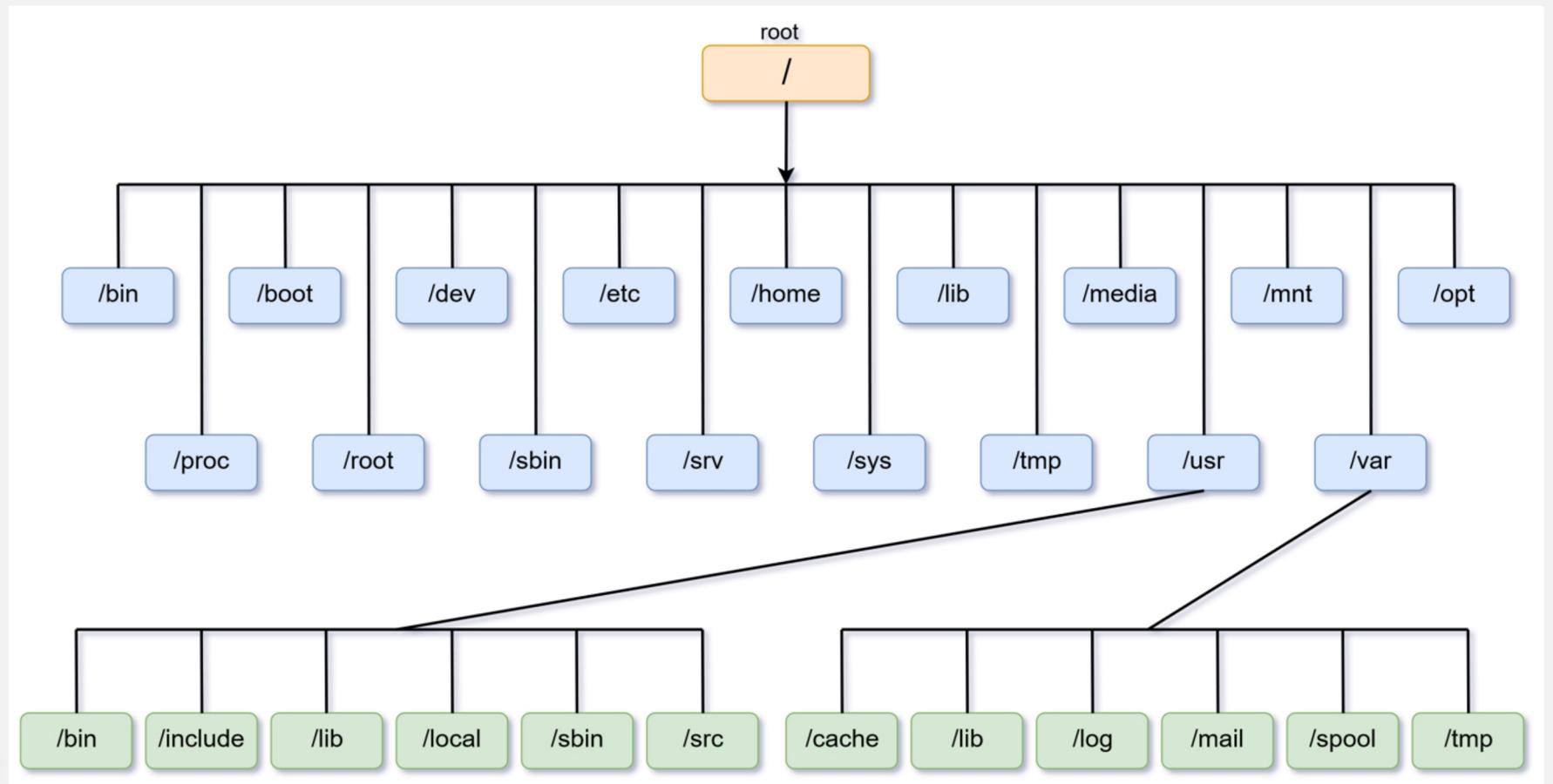


Système fichiers – Commandes de base – Gestion utilisateurs –  
Processus - Journalisation

## **3 - ADMINISTRER LE SYSTÈME AVEC LES COMMANDES CONSOLE**

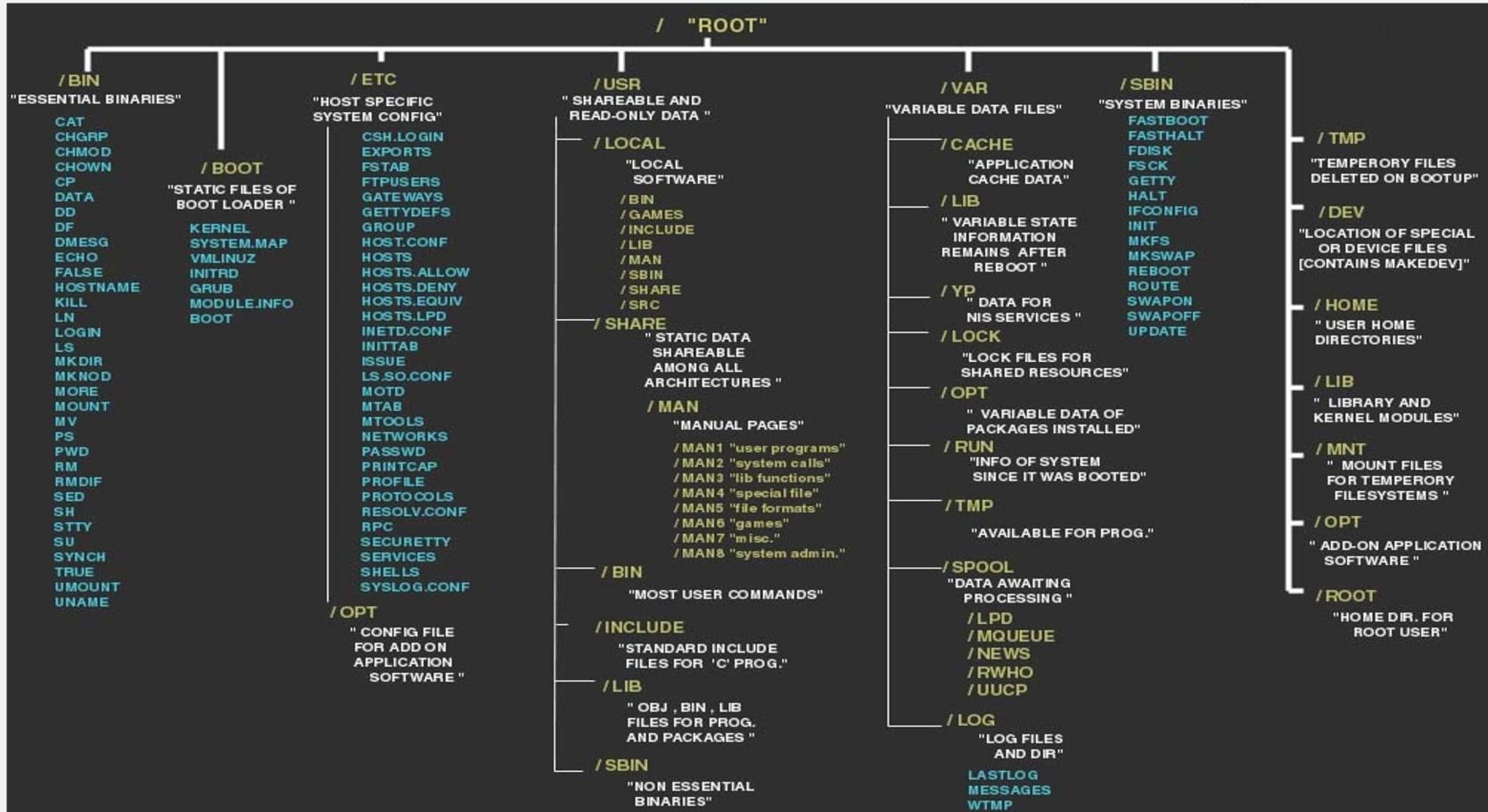
- 3-1. Le système de fichier avec Linux.***
- 3-2. Les commandes de base du système (rappels).***
- 3-3. Lire des scripts Shell (rappels).***
- 3-4. Gérer les utilisateurs (rappels).***
- 3-5. Gérer les processus (rappels).***
- 3-6. Gérer les bibliothèques partagées.***
- 3-7. Programmer des travaux périodiques.***
- 3-8. Organiser les journaux de bords et leur rotation.***

## 3-I LE SYSTÈME DE FICHIER AVEC LINUX



## 3-I LE SYSTÈME DE FICHIER AVEC LINUX

Un peu plus  
détailé



## 3- I LE SYSTÈME DE FICHIER AVEC LINUX

Répertoire	Signification
/	Répertoire racine. Point de départ de toute la hiérarchie du système de fichiers. Le système de fichiers contenant ce répertoire est monté automatiquement par le noyau pendant l'amorçage du système. Ce système de fichiers est appelé système de fichiers racine (« root » en anglais).
/boot/	Répertoire contenant le noyau de Linux et ses informations de symboles. Ce répertoire est parfois le point de montage d'un système de fichiers de très petite taille, dédié au noyau. Dans ce cas, il est recommandé que le système de fichiers correspondant soit monté en lecture seule.
/dev/	Répertoire contenant tous les fichiers spéciaux permettant d'accéder aux périphériques.
/sbin/	Répertoire contenant les commandes systèmes nécessaires à l'amorçage et réservées à l'administrateur. Ce répertoire doit être impérativement placé dans le système de fichiers racine. En général, seul l'administrateur utilise ces commandes.
/bin/	Répertoire contenant les commandes systèmes générales nécessaires à l'amorçage. Ce répertoire doit être impérativement placé dans le système de fichiers racine. Tous les utilisateurs peuvent utiliser les commandes de ce répertoire.
/lib/	Répertoire contenant les bibliothèques partagées (« DLL » en anglais, pour « Dynamic Link Library ») utilisées par les commandes du système des répertoires /bin/ et /sbin/. Ce répertoire doit être impérativement placé dans le système de fichiers racine.
/etc/	Répertoire contenant tous les fichiers de configuration du système. Ce répertoire doit être impérativement placé dans le système de fichiers racine.

## 3-I LE SYSTÈME DE FICHIER AVEC LINUX

Répertoire	Signification
/tmp/	Répertoire permettant de stocker des données temporaires. En général, /tmp/ ne contient que des données très éphémères. Il est préférable d'utiliser le répertoire /var/tmp/. En effet, le répertoire /tmp/ ne dispose pas nécessairement de beaucoup de place disponible.
/usr/	Répertoire contenant les fichiers du système partageables en réseau et en lecture seule.
/var/	Répertoire contenant toutes les données variables du système. Ce répertoire contient les données variables qui ne pouvaient pas être placées dans le répertoire /usr/, puisque celui-ci est normalement accessible en lecture seule.
/opt/	Répertoire historique contenant les applications qui ne font pas réellement partie du système d'exploitation. En particulier, sur les anciennes distributions, le gestionnaire de bureau KDE était installé dans le sous-répertoire /opt/kde/, mais à présent il est considéré comme partie intégrante du système et est donc installé directement dans le répertoire /usr/ sur les distributions récentes.
/home/	Répertoire contenant les répertoires personnels des utilisateurs.
/root/	Répertoire contenant le répertoire personnel de l'administrateur. Il est donc recommandé que le répertoire personnel de l'administrateur soit placé en dehors de / home/ pour éviter qu'un problème sur le système de fichiers des utilisateurs ne l'empêche de travailler.
/media/	Répertoire réservé au montage des systèmes de fichiers sur périphériques amovibles (CD-ROM, disquettes, etc.). Ce répertoire peut contenir plusieurs sous-répertoires pour chaque périphérique amovible, afin de permettre d'en monter plusieurs simultanément.
/proc/	Répertoire contenant le pseudo système de fichiers du noyau. Ce pseudo système de fichiers contient des fichiers permettant d'accéder aux informations sur le matériel, la configuration du noyau et sur les processus en cours d'exécution.
/sys/	Répertoire contenant le pseudo système de fichiers des gestionnaires de périphériques. Ce pseudo système de fichiers contient des fichiers permettant d'obtenir des informations sur l'ensemble des objets du noyau, en particulier sur l'ensemble des périphériques de l'ordinateur.

## 3-2 LES COMMANDES DE BASE LINUX



```
MBP-de-Mohamed:~ mohamed$ ls
Applications          Movies
Applications (Parallels)  Music
Desktop               Parallels
Documents              Pictures
Downloads              Public
Library                VirtualBox VMs

MBP-de-Mohamed:~ mohamed$ pwd
/Users/mohamed

MBP-de-Mohamed:~ mohamed$ cd Desktop

MBP-de-Mohamed:Desktop mohamed$ ls
Capture d'écran 2021-07-25 à 18.17.03.png
Éléments déplacés.nosync
Simulator Screen Shot - iPhone 12 Pro Max - 2021-08-11 at 11.17.22.png
Ubuntu 20.04.2 ARM64
scanNdf
```

### 1. Commande **pwd** :

Utilisez la commande **pwd** pour trouver le chemin du répertoire de travail (dossier) dans lequel vous êtes actuellement. La commande retournera un chemin absolu (complet), qui est en fait un chemin de tous les répertoires qui commence par une barre oblique (/). Un exemple de chemin absolu est **/home/utilisateur**.

### 2. Commande **cd**

Pour naviguer dans les fichiers et répertoires de Linux, utilisez la commande **cd (Change Directory)**. Elle nécessite soit le chemin d'accès complet, soit le nom du répertoire, selon le répertoire de travail dans lequel vous vous trouvez.

### 3. Commande **ls**

La commande 'ls' est utilisée pour visualiser le contenu d'un répertoire. Par défaut, cette commande affichera le contenu de votre répertoire de travail actuel.

## 3-2 LES COMMANDES DE BASE LINUX

```
MBP-de-Mohamed:Desktop mohamed$ ls
Capture d'écran 2021-07-25 à 18.17.03.png
Éléments déplacés.nosync
Simulator Screen Shot - iPhone 12 Pro Max - 2021-08-11 at 11.17.22.png
Ubuntu 20.04.2 ARM64
scanNdf

MBP-de-Mohamed:Desktop mohamed$ mkdir dossier

MBP-de-Mohamed:Desktop mohamed$ ls
Capture d'écran 2021-07-25 à 18.17.03.png
Éléments déplacés.nosync
Simulator Screen Shot - iPhone 12 Pro Max - 2021-08-11 at 11.17.22.png
Ubuntu 20.04.2 ARM64
dossier
scanNdf

MBP-de-Mohamed:Desktop mohamed$ rmdir dossier

MBP-de-Mohamed:Desktop mohamed$ ls
Capture d'écran 2021-07-25 à 18.17.03.png
Éléments déplacés.nosync
Simulator Screen Shot - iPhone 12 Pro Max - 2021-08-11 at 11.17.22.png
Ubuntu 20.04.2 ARM64
scanNdf
```

### 4. Commande mkir :

Utilisez la commande **mkdir (*make directory*)** pour créer un nouveau répertoire – si vous tapez **mkdir « dossier »**, cela créera un répertoire appelé « dossier ».

### 5. Commande rmdir

Pour naviguer dans les fichiers et répertoires de Linux, utilisez la commande **cd**. Elle nécessite soit le chemin d'accès complet, soit le nom du répertoire, selon le répertoire de travail dans lequel vous vous trouvez.

### 6. Commande rm

La commande **rm** est utilisée pour supprimer les répertoires et leur contenu. Si vous voulez seulement supprimer le répertoire – comme alternative à **rmdir** – utilisez **rm -r**.

## 3-2 LES COMMANDES DE BASE LINUX

```
MBP-de-Mohamed:Desktop mohamed$ mkdir Dossier
MBP-de-Mohamed:Desktop mohamed$ cd Dossier/
MBP-de-Mohamed:Dossier mohamed$ touch message.txt
MBP-de-Mohamed:Dossier mohamed$ ls
message.txt
MBP-de-Mohamed:Dossier mohamed$ echo je suis un texte >> message.txt
MBP-de-Mohamed:Dossier mohamed$ cat message.txt
je suis un texte
```

### 7. Commande touch

La commande **touch** vous permet de créer un nouveau fichier vierge via la ligne de commande Linux.

*Par exemple, entrez `touch /home/username/Documents/Web.html` pour créer un fichier HTML intitulé Web dans le répertoire Documents.*

### 8. Commande echo

Cette commande est utilisée pour déplacer certaines données dans un fichier.

*Par exemple, si vous voulez ajouter le texte « Bonjour, je suis Ihab » dans un fichier appelé nom.txt, vous devez taper **echo Bonjour, je suis Ihab >> nom.txt***

### 9. Commande cat

**cat** (abréviation de concatenate) est l'une des commandes Linux les plus fréquemment utilisées. Elle est utilisée pour lister le contenu d'un fichier sur le résultat standard (sdout). Pour exécuter cette commande, tapez **cat** suivi du nom du fichier et de son extension.

*Par exemple : **cat fichier.txt**.*

## 3-2 LES COMMANDES DE BASE LINUX

```
MacBook-Pro-de-Mohamed:Dossier mohamed$ touch message2.txt  
  
MacBook-Pro-de-Mohamed:Dossier mohamed$ ls  
message.txt message2.txt  
  
MacBook-Pro-de-Mohamed:Dossier mohamed$ find message.txt  
message.txt  
  
MacBook-Pro-de-Mohamed:Dossier mohamed$ echo un autre message dans un fichier txt >> message.txt  
  
MacBook-Pro-de-Mohamed:Dossier mohamed$ cat message.txt  
je suis un texte  
un autre message dans un fichier txt  
  
MacBook-Pro-de-Mohamed:Dossier mohamed$ grep je message.txt  
je suis un texte  
  
MacBook-Pro-de-Mohamed:Dossier mohamed$ grep un message.txt  
je suis un texte  
un autre message dans un fichier txt  
  
MacBook-Pro-de-Mohamed:Dossier mohamed$ grep autre message.txt  
un autre message dans un fichier txt
```

### 10. Commande locate

Vous pouvez utiliser cette commande pour **localiser** un fichier, tout comme la commande de recherche dans Windows.

De plus, l'utilisation de l'argument **-i** avec cette commande la rendra insensible à la casse, ce qui vous permettra de rechercher un fichier même si vous ne vous souvenez pas de son nom exact.

Pour rechercher un fichier qui contient deux mots ou plus, utilisez un astérisque (\*). Par exemple, la commande « **locate -i school\*note** » permettra de rechercher tout fichier contenant les mots « **school** » et « **note** », qu'ils soient en majuscules ou en minuscules.

### 11. Commande find

Comme la commande **locate**, l'utilisation de **find** permet également de rechercher des fichiers et des réertoires. La différence est que vous utilisez la commande **find** pour localiser des fichiers dans un répertoire donné.

### 12. Commande grep

Une autre commande de base de Linux qui est sans aucun doute utile pour une utilisation quotidienne est **grep**. Elle vous permet de rechercher tout le texte d'un fichier donné.

Par exemple, **grep blue notepad.txt** recherchera le mot **blue** dans le fichier **notepad**. Les lignes qui contiennent le mot recherché s'afficheront entièrement.

## 3-2 LES COMMANDES DE BASE LINUX

```
MacBook-Pro-de-Mohamed:Dossier mohamed$ cp message.txt /Users/mohamed/Desktop
MacBook-Pro-de-Mohamed:Dossier mohamed$ cd ..
MacBook-Pro-de-Mohamed:Desktop mohamed$ ls
Capture d'écran 2021-07-25 à 18.17.03.png
Dossier
Éléments déplacés.nosync
Simulator Screen Shot - iPhone 12 Pro Max - 2021-08-11 at 11.17.22.png
Ubuntu 20.04.2 ARM64
message.txt
scanNdf
MacBook-Pro-de-Mohamed:Desktop mohamed$ history
 1 node --version
 2 node -v
 3 brew install node
 4 export PATH=/home/david/pear/bin:$PATH
 5 brew install node
 6 brew install node

MacBook-Pro-de-Mohamed:Desktop mohamed$ top
Processes: 377 total, 2 running, 375 sleeping, 2048 threads          16:50:38
Load Avg: 1.69, 1.51, 1.54   CPU usage: 2.73% user, 3.68% sys, 93.57% idle
SharedLibs: 210M resident, 45M data, 9024K linked.
MemRegions: 128025 total, 1543M resident, 114M private, 866M shared.
PhysMem: 7337M used (1101M wired), 205M unused.
VM: 141T vszie, 3272M framework vszie, 812486(0) swapins, 897002(0) swapouts.
Networks: packets: 3115296/3355M in, 1818848/328M out.
Disks: 4936658/228G read, 1916444/43G written.

PID  COMMAND %CPU TIME #TH #WQ #PORT MEM PURG CMPRS PGRP
351 WindowServer 13.4 03:14:18 23 5 4978 490M- 17M+ 165M 351
0 kernel_task 8.9 73:44.09 480/8 0 0 34M 0B 0B 0
467 TouchBarSrv 8.9 41:23.90 4 2 2844 40M+ 64K- 24M 467
24595 top 4.5 00:00.54 1/1 0 26 4897K 0B 0B 24595
24155 Terminal 4.4 00:27.79 13 7 322- 50M+ 6224K 11M 24155
10996 Microsoft Po 3.8 55:15.33 21 10 3184 628M 1104K 340M 10996
24454 Spotify 2.5 00:50.17 45 1 583 137M 0B 369M 24454
24452 bluetoothaud 1.9 00:26.97 4 1 157 4994K 0B 1920K 24452
11301 Zettlr Help 1.5 09:59.79 16 1 215 129M 0B 111M 11296
11298 Zettlr Help 1.0 06:20.52 10 2 178 133M 704K 25M 11296
427 coreaudiod 0.9 06:32.74 6 1 450 23M 0B 16M 427
344 corebrightne 0.5 04:59.41 7 6 147 4386K- 0B 1904K 344
24462 Spotify Help 0.3 00:06.96 10 2 168 130M 0B 128M 24454
746 Google Chrom 0.3 50:55.47 34 1 2065 557M 0B 379M 746
```

### 13. Commande cp

Utilisez la commande **cp** pour copier les fichiers du répertoire actuel dans un autre répertoire.

Par exemple, la commande **cp scenery.jpg /home/utilisateur/Photos** créera une copie de *scenery.jpg* (de votre répertoire actuel) dans le répertoire *Photos*.

### 14. Commande history

Lorsque vous utilisez Linux depuis un certain temps, vous remarquerez rapidement que vous pouvez exécuter des centaines de commandes chaque jour.

Ainsi, l'exécution de la commande **history** est particulièrement utile si vous voulez revoir les commandes que vous avez entrées auparavant.

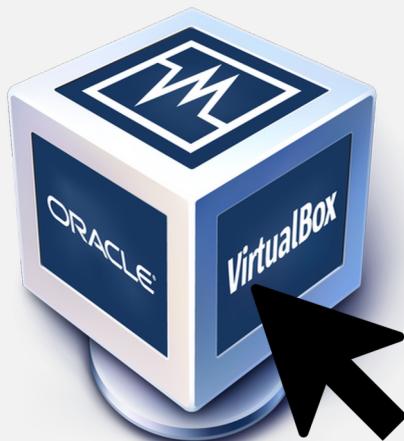
### 15. Commande top

Comme un terminal équivalent au gestionnaire de tâches dans Windows, la commande **top** affichera une liste des processus qui sont en cours d'exécution et la quantité de CPU utilisée par chaque processus. Il est très utile de surveiller l'utilisation des ressources du système, en particulier de savoir quel processus doit être arrêté en cas de surconsommation de ressources.



## 3-2 LES COMMANDES DE BASE LINUX

Un peu de pratique





TP TIME

TP\_I LINUX : Basic command line





TP TIME 2

TP\_MANIPULATION\_FICHIER : fichier.csv



## 3-3 GÉRER LES UTILISATEURS



- **Rappel** : Linux est un système multi-utilisateurs. Cela signifie que plusieurs personnes peuvent travailler simultanément sur le même OS, en s'y connectant à distance notamment.
- **L'identification**, c'est savoir qui est connecté, afin de déterminer les droits de la personne qui se connecte. Un utilisateur est identifié par un login.
- **L'authentification**, c'est apporter la preuve de qui on est, par exemple via un secret partagé entre l'utilisateur et le système, et connus d'eux seuls. L'utilisateur est authentifié par un mot de passe.



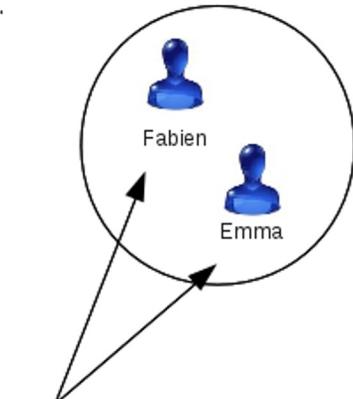
## 3-3 GÉRER LES UTILISATEURS

**Le root** a l'ensemble des droits sur la machine, c'est lui seul qui peut créer des utilisateurs et des groupes et mettre en place des droits sur les répertoires et fichiers du système



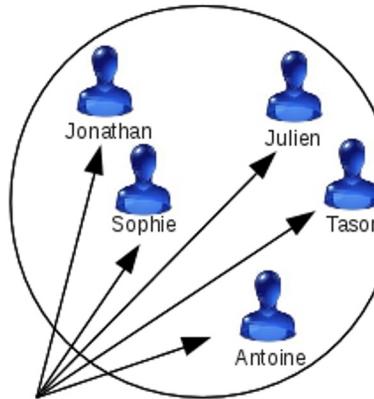
**Un groupe** sous Linux est un ensemble d'utilisateurs qui partagent les mêmes fichiers et répertoires.. .

Groupe maison



Utilisateurs du groupe maison

Groupe amis



Utilisateurs du groupe amis

## 3-3 GÉRER LES UTILISATEURS



### UN UTILISATEUR

- Login : nom de connexion.
- UID : User ID.
- GID : Group ID.
- Un descriptif.
- Un répertoire de connexion.
- Une commande de connexion.

### LES CARACTÉRISTIQUES

- UID si  $> 100 \Rightarrow$  compte spéciaux.
- Si UID = 0  $\Rightarrow$  administrateur (root).
- A partir de 100, 500 ou 1000 jusqu'à 60 000  $\Rightarrow$  UID sans particularités.
- Login  $< 8$  caractères + Ne doit pas commencer par un chiffre.

### 3-3 GÉRER LES UTILISATEURS

```
# Exemple avec utilisateur classique sous Ubuntu
parallels@ubuntu-linux-20-04-desktop:~$ id parallels
uid=1000(parallels) gid=1000(parallels)
groups=1000(parallels),4(adm),24(cdrom),
27(sudo),30(dip),46(plugdev),116(lxd)

# Exemple avec utilisateur admin(root) sous Fedora
[root@fedora ~]# id
uid=0(root) gid=0(root) groupes=0(root)
contexte=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023

# liste des groupes auxquels appartient parallels
parallels@ubuntu-linux-20-04-desktop:~$ groups parallels
parallels : parallels adm cdrom sudo dip plugdev lxd

# On cree un fichier et on voit le proprietaire et son groupe primaire
parallels@ubuntu-linux-20-04-desktop:~/Documents$ touch message
parallels@ubuntu-linux-20-04-desktop:~/Documents$ ls -l
-rw-rw-r-- 1 parallels parallels 0 Aug 19 10:23 message
```

## LES GROUPES

- **Un groupe** est un ensemble d'utilisateurs qui partagent les mêmes fichiers et répertoires.
- Chaque **utilisateur** appartient à au moins un groupe.
- Chaque **groupe** dispose d'un GID (Groupe ID).
- **Un utilisateur** peut appartenir un ou plusieurs groupes.
- Il a donc **un groupe** primaire et peut avoir un ou plusieurs groupes secondaires.
- **Un utilisateur** dispose des droits et priviléges des groupes auxquels il appartient.
- La commande « **id** » permet d'afficher les informations essentielles sur l'utilisateur.

## 3-3 GÉRER LES UTILISATEURS

```
# Affiche la liste des utilisateurs du système local
parallels@ubuntu-linux-20-04-desktop:~/Documents$ cat /etc/passwd
# Login:password:UID:GID:comment:homedir:shell
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
parallels:x:1000:1000:Parallels:/home/parallels:/bin/bash
```

## LES FICHIERS

- La gestion des utilisateurs va avoir une incidence sur un certain nombre de dossiers et fichiers de notre système d'exploitation.
- Les principaux fichiers concernés :
  1. **/etc/passwd**
  2. **/etc/group**
  3. **/etc/shadow**
  4. **/etc/gshadow**
- Le fichier **/etc/passwd** :
  - Contient la liste des utilisateurs du système local.
  - Il est lisible par tous.
  - Les informations sont publiques.
  - Chaque ligne représente un utilisateur avec 7 champs.
  - Syntaxe :  
**Login:password:UID:GID:comment:homedir:shell**

## 3-3 GÉRER LES UTILISATEURS

```
# Affiche la liste des groupes et leurs utilisateurs
root@41242c7d9028:/# cat /etc/group
# Group : password : GID : user1, user2, ...
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:
floppy:x:25:
tape:x:26:
sudo:x:27:
audio:x:29:pulse
dip:x:30:
www-data:x:33:
```

## LES FICHIERS

- Le fichier **/etc/group** :

- Contient la définition des groupes d'utilisateurs et pour chacun la liste des utilisateurs dont il est le groupe secondaire.
- Chaque ligne représente un groupe avec 7 champs.
- Syntaxe : **Group:password:GID:user1,user2, user3, ...**



### Password dans un groupe?

**Explication :** Un utilisateur a le droit de changer de groupe afin de prendre, temporairement tout du moins, un groupe secondaire comme groupe principal avec la commande **newgrp**. Dans ce cas, l'administrateur peut mettre en place un mot de passe sur le groupe pour protéger l'accès à ce groupe en tant que groupe principal.

## 3-3 GÉRER LES UTILISATEURS

```
# Liste des utilisateurs avec leurs informations sur le mot de passe
root@41242c7d9028:/# cat /etc/shadow
# * signifie mot de passe jamais établi...
root:*:18830:0:99999:7:::
daemon:*:18830:0:99999:7:::
bin:*:18830:0:99999:7:::
sys:*:18830:0:99999:7:::
sync:*:18830:0:99999:7:::
games:*:18830:0:99999:7:::
man:*:18830:0:99999:7:::
lp:*:18830:0:99999:7:::
mail:*:18830:0:99999:7:::
news:*:18830:0:99999:7:::
uucp:*:18830:0:99999:7:::
proxy:*:18830:0:99999:7:::
www-data:*:18830:0:99999:7:::
backup:*:18830:0:99999:7:::
list:*:18830:0:99999:7:::
irc:*:18830:0:99999:7:::
gnats:*:18830:0:99999:7:::
nobody:*:18830:0:99999:7:::
systemd-timesync:*:18830:0:99999:7:::
systemd-network:*:18830:0:99999:7:::
systemd-resolve:*:18830:0:99999:7:::
systemd-bus-proxy:*:18830:0:99999:7:::
_apt:*:18830:0:99999:7:::
messagebus:*:18858:0:99999:7:::
whoopsie:*:18858:0:99999:7:::
syslog:*:18858:0:99999:7:::
avahi:*:18858:0:99999:7:::
avahi-autoipd:*:18858:0:99999:7:::
```

## LES FICHIERS

- Le fichier **/etc/shadow** :

- Accompagne le fichier **/etc/passwd**.
- Contient le mot de passe crypté de chaque utilisateur.
- Contient des informations sur le mot de passe comme sa durée de validité.
- Chaque ligne représente un groupe avec 7 champs.
- **Syntaxe vu ci-après**

## /etc/gshadow

Le fichier **/etc/gshadow** est le pendant du fichier précédent mais pour les groupes. Il n'est cependant pas supporté par défaut sur la plupart des distributions Linux

## 3-4 GÉRER LES UTILISATEURS

### LES FICHIERS

Détails : /etc/shadow

**Root : \$2a\$10\$AjADxPEfE5iUJcltzYA4wOZO.f2UZ0qP/8EnOFY.P.m10HifS7J8i:I39I3 : 0 : 99999: 7 : :**

Login ou  
username

Mot de passe crypté  
(hashé) avec algo hashage  
\$2a\$

Nombre de jours avant  
lesquels le mode de passe  
ne peut être changé (0, il est  
n'importe quand)

Le nombre de jours depuis le 1<sup>er</sup>  
Janvier 1970 du dernier  
changement de mot de passe.

Nombre de jours après  
lequel le mot de passe doit  
être changé

Nombre de jours après  
l'expiration du mot de passe  
après lesquels le compte est  
désactivé.

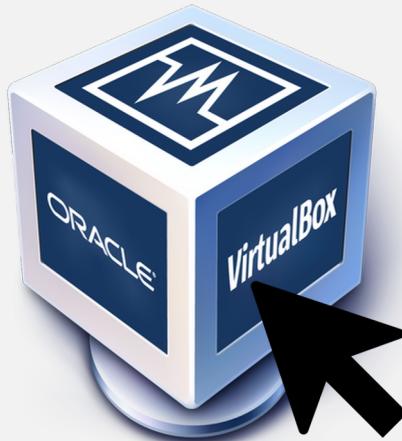
Réserve

Nombre de jours avant l'expiration du  
mot de passe durant lesquels  
l'utilisateur doit être prévenu

Nombre de jours depuis le 1er janvier  
1970 à partir du moment où le compte  
a été désactivé.

## 3-3 GÉRER LES UTILISATEURS

Un peu de pratique



## AJOUTER UN UTILISATEUR

### 3-3 GÉRER LES UTILISATEURS



```
root@41242c7d9028:/# adduser thomas
Adding user `thomas' ...
Adding new group `thomas' (1012) ...
Adding new user `thomas' (1007) with group `thomas' ...
Creating home directory `/home/thomas' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for thomas
Enter the new value, or press ENTER for the default
  Full Name []: Thomas pesquet
  Room Number []: 46 rue des fleurs
  Work Phone []: 0633125467
  Home Phone []: 0987654334
  Other []: thomas.pesquet@gmail.com
Is the information correct? [Y/n] y
```

- 2 possibilités pour le faire :
  - Avec la commande « **adduser** ». -> **Debian**
  - Avec la commande « **useradd** ». -> **Autres**
- Impact les fichiers suivants : /etc/passwd, /etc/group et /etc/shadow
- Plusieurs options peuvent être intégrées lors de la création d'un utilisateur, ci-dessous pour **adduser**:

Option	Rôle
--conf FICHIER	Utilise <i>FICHIER</i> plutôt que /etc/adduser.conf.
--disabled-login	N'utilise pas passwd pour fixer le mot de passe. L'utilisateur ne pourra pas utiliser son compte avant que son mot de passe soit donné.
--disabled-password	Comme --disabled-login, mais les connexions sont toujours possibles (par exemple par SSH avec des clés RSA), mais pas par une authentification par mot de passe.
--force-badname	Par défaut, les utilisateurs et les groupes sont comparés à une expression rationnelle configurable. Cette option oblige adduser et addgroup à ne réaliser qu'une faible vérification du nom.
--gid ID	Lorsqu'un groupe est créé, cette option permet de forcer l'identifiant numérique du groupe. Lorsqu'un utilisateur est créé, cette option place cet utilisateur dans ce groupe.
--group	Avec l'option --system, un groupe ayant le même nom et le même identifiant numérique que l'utilisateur système est créé. Sans l'option --system, un groupe avec le nom fourni en argument est créé. C'est le comportement par défaut lorsque addgroup est appelé.
--home REP	Utilise <i>REP</i> comme répertoire personnel de l'utilisateur, plutôt que la valeur par défaut définie dans le fichier de configuration. Si le répertoire n'existe pas, il est créé, et les fichiers du squelette y sont copiés.

## AJOUTER UN UTILISATEUR

### 3-3 GÉRER LES UTILISATEURS

```
root@41242c7d9028:/# useradd -u 1045 -g utilisateurs -G video,lp -s /bin/bash -d /home/arthur -c "arthur.halluin@gmail.com" arthur

root@41242c7d9028:/# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:0:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
thomas:x:1007:1012:Thomas pesquet,46 rue des
fleurs,0633125467,0987654334,thomas.pesquet@gmail.com:/home/thomas:/bin/bash
arthur:x:1045:1014:arthur.halluin@gmail.com:/home/arthur:/bin/bash

root@41242c7d9028:/# cat /etc/shadow
root:**:18830:0:99999:7:::
daemon:**:18830:0:99999:7:::
bin:**:18830:0:99999:7:::
sys:**:18830:0:99999:7:::
sync:**:18830:0:99999:7:::
games:**:18830:0:99999:7:::
man:**:18830:0:99999:7:::
lp:**:18830:0:99999:7:::
mail:**:18830:0:99999:7:::
thomas:$6$ljFrtegs$GHDJhjuZEKUJ/akqMMkIUDnVP.CgAZ2QtZ.4g6CR8u7pYkWLh0zdJ0vWNe/eqjRxhVUYi21lU7akdwovjxJ
q0:18862:0:99999:7:::
arthur:**:18862:0:99999:7:::
```

- Seul un « super utilisateur » peut rajouter un utilisateur.
- Quelques options peuvent être intégrées lors de la création d'un utilisateur en utilisant la commande **useradd**:

Option	Rôle
<b>-m</b>	Crée aussi le répertoire personnel. Elle est parfois comprise par défaut, mais il vaut mieux vérifier si le répertoire personnel est présent après l'utilisation de la commande si vous n'utilisez pas cette option.
<b>-u</b>	Précise l'UID numérique de l'utilisateur, pour le forcer. Autrement l'UID est calculé selon les règles du fichier login.defs et les UID existants.
<b>-g</b>	Précise le groupe principal de l'utilisateur, par GID ou par son nom (variable GROUP).
<b>-G</b>	Précise les groupes additionnels (secondaires, de l'utilisateur) séparés par des virgules (variable GROUPS).
<b>-d</b>	Chemin du répertoire personnel. Généralement /home/<login>, mais n'importe quel chemin peut être précisé (variable HOME/<login>).
<b>-c</b>	Un commentaire associé au compte. Il peut être quelconque mais est parfois utilisé par certaines commandes comme <b>finger</b> . Son contenu peut être modifié par l'utilisateur avec la commande <b>chfn</b> .
<b>-k</b>	Chemin du répertoire contenant le squelette de l'arborescence du répertoire utilisateur. C'est généralement /etc/skel (variable SKEL).
<b>-s</b>	Shell (commande de connexion) par défaut de l'utilisateur (variable SHELL). L'utilisateur peut le changer via la commande <b>chsh</b> .
<b>-p</b>	Le mot de passe de l'utilisateur. Attention ! le mot de passe doit déjà être crypté ! À moins de recopier le mot de passe d'un compte générique, vous préférerez utiliser ensuite la commande <b>passwd</b> .

### 3-3 GÉRER LES UTILISATEURS

```
root@41242c7d9028:/home# ls  
loic martin pierre remy robert thomas  
  
# Modification du login de martin en martineau  
root@41242c7d9028:/home# usermod -l martineau martin  
  
root@41242c7d9028:/home# grep martineau /etc/shadow  
martineau:$S$0St9UkUv$3YIMMNQil156LwFJmpSFEcTRnpfxTnj2o5Ze/Ns89jaSjfLTDBYGbArgSZFXQPH/8.e.nXuLhH4/g52fw  
FJ6X1:18859:0:99999:7:::
```

## MODIFIER UN UTILISATEUR

- La commande pour modifier un utilisateur est :

- Usermod <option> <login>**

- Ci-dessous quelques options :

Option	Rôle
-L	Lock du compte, comme passwd l.
-U	Unlock du compte, comme passwd u.
-e <n>	Expire : le mot de passe expire n jours après le 01/01/1970.
-u<UID>	Modifie l'UID associé au login. Le propriétaire des fichiers appartenant à l'ancien UID au sein du répertoire personnel est modifié en conséquence.
-l <login>	Modifie le nom de login.
-m	Move : implique la présence de d pour préciser un nouveau répertoire personnel. Le contenu de l'ancien répertoire est déplacé dans le nouveau.

## 3-3 GÉRER LES UTILISATEURS

### SUPPRIMER UN UTILISATEUR

```
● ● ●  
# Avec userdel :  
root@41242c7d9028:/# grep remy /etc/shadow  
remy:$6$Pry/wY$09aj09Yt9fFSNsEj/9jjBCrPt85AeMyIGoVmZBKkuixBh.s8D0H8sS6s/RBxd82Tgf641FkN2AvxnaJ1Io.//  
:18859:::99999:7:::  
  
root@41242c7d9028:/# userdel remy  
  
root@41242c7d9028:/# grep remy /etc/shadow  
  
root@41242c7d9028:/home# ls  
alain loic martin michel pierre remy robert thomas  
  
root@41242c7d9028:/home# rm -r michel  
  
root@41242c7d9028:/home# ls  
alain loic martin pierre remy robert thomas  
  
# Avec deluser :  
root@41242c7d9028:/home# deluser loic  
Removing user 'loic' ...  
Warning: group 'loic' has no more members.  
Done.  
root@41242c7d9028:/home# ls  
alain loic martin pierre remy robert thomas  
  
root@41242c7d9028:/home# deluser --remove-home --remove-all-files alain  
Looking for files to backup/remove ...  
/usr/sbin/deluser: Cannot handle special file /dev/console  
/usr/sbin/deluser: Cannot handle special file /dev/core  
/usr/sbin/deluser: Cannot handle special file /dev/stderr  
/usr/sbin/deluser: Cannot handle special file /dev/stdout  
/usr/sbin/deluser: Cannot handle special file /dev/stdin  
/usr/sbin/deluser: Cannot handle special file /dev/ptmx  
/usr/sbin/deluser: Cannot handle special file /dev/urandom  
/usr/sbin/deluser: Cannot handle special file /dev/zero  
/usr/sbin/deluser: Cannot handle special file /dev/tty  
/usr/sbin/deluser: Cannot handle special file /dev/full  
/usr/sbin/deluser: Cannot handle special file /dev/random  
/usr/sbin/deluser: Cannot handle special file /dev/null  
/usr/sbin/deluser: Cannot handle special file /dev/pts/1  
...  
Removing files ...  
Removing user 'alain' ...  
Warning: group 'alain' has no more members.  
Done.  
root@41242c7d9028:/home# ls  
loic martin pierre remy robert thomas
```

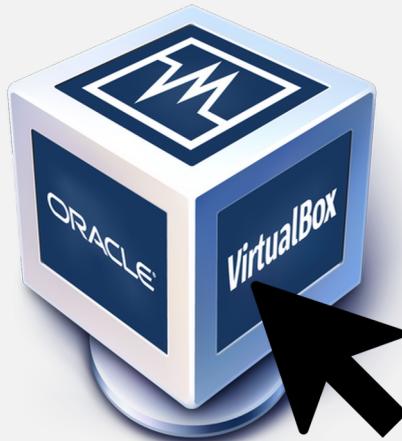
- **Userdel** supprime l'utilisateur mais pas son répertoire personnel.
- **Userdel –r <login user>**, supprime l'utilisateur et son répertoire.

OU

- **Deluser** supprime l'utilisateur mais pas son répertoire personnel.
- **deluser – –remove-home <login user>**, supprime l'utilisateur et son répertoire.

## 3-3 GÉRER LES UTILISATEURS

Un peu de pratique



### 3-3 GÉRER LES UTILISATEURS



```
#Tentative de changement de mot de passe
ahmed@41242c7d9028:/$ passwd
Changing password for ahmed.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
You must choose a longer password
Enter new UNIX password:
Retype new UNIX password:
Bad: new password is too simple
Enter new UNIX password:
Retype new UNIX password:
You must choose a longer password
passwd: Authentication token manipulation error
passwd: password unchanged
```

#### MOT DE PASSE

- La commande « **passwd** » permet la gestion des mots de passe mais aussi les autorisations de connexion.
- A chaque changement de mot de passe, l'ancien est demandé avant.
- La saisie est masquée.
- Les modules **PAM** sont des modules paramétrables qui mettent en place des contraintes plus ou moins sévères d'authentification et de connexion ( ex : longueur mot de passe).
- L'utilisateur root peut modifier tous les mots de passe et forcer les contraintes des PAM. A red devil face emoji with horns and a mischievous expression.
- Tous les champs dans le fichier /etc/shadow peuvent être modifiés avec un profil user « root ».

## 3-3 GÉRER LES UTILISATEURS



```
#chage autre commande pour gérer les mots de passe. Affiche les infos sur la gestion du mot de passe
ahmed@41242c7d9028:/$ chage -l ahmed
Last password change          : Aug 24, 2021
Password expires              : never
Password inactive              : never
Account expires                : never
Minimum number of days between password change   : 0
Maximum number of days between password change   : 99999
Number of days of warning before password expires : 7
```

```
#Changement des paramètres de gestion du mot de passe pour l'utilisation ahmed
root@41242c7d9028:/# passwd -n 1 -x 30 -w 7 -i 5 ahmed
passwd: password expiry information changed.
```

```
#Recherche et affiche les infos d'authentification pour l'utilisateur ahmed
root@41242c7d9028:/# grep ahmed /etc/shadow
ahmed:$6$ffDGp3gu$Svu43spvZzXmLVIBzmcUb92fM07PA90HVLLia8FCheiomf2E5yt0gRF5kNxil2ZDcA3JH0jGHx1.qo1yjFt5
.:18863:1:30:7:5::
```

```
# Affiche les infos sur la gestion du mot de passe, après le changement
root@41242c7d9028:/# chage -l ahmed
```

```
Last password change          : Aug 24, 2021
Password expires              : Sep 23, 2021
Password inactive              : Sep 28, 2021
Account expires                : never
Minimum number of days between password change   : 1
Maximum number of days between password change   : 30
Number of days of warning before password expires : 7
```

## MOT DE PASSE « passwd »

Option	Rôle
-l	Lock : verrouille le compte en rajoutant un ! devant le mot de passe crypté.
-u	Unlock : déverrouille le compte. Il n'est pas possible de déverrouiller un compte qui n'a pas de mot de passe, il faut utiliser en plus f pour cela.
-d	(root) Supprime le mot de passe du compte.
-n <j>	(root) Durée de vie minimale en jours du mot de passe.
-x <j>	(root) Durée de vie maximale en jours du mot de passe.
-w <j>	(root) Nombre de jours avant avertissement.
-i <j>	(root) Délai de grâce avant désactivation si le mot de passe est expiré.
-s	(root) Statut du compte.

### Exemple à gauche :

- Ahmed va devoir attendre 1 jour avant de pouvoir changer son mot de passe.
- Son mot de passe sera valide 30 jours.
- Après ce délai, il aura 5 jours pour modifier son mot de passe avant d'être désactivé.
- Il sera prévenu 7 jour avant que son mot de passe va devoir être modifié.

## 3-3 GÉRER LES UTILISATEURS



```
# Modification du nom du groupe "famille" en "familles"
root@41242c7d9028:/# groupmod -n familles famille

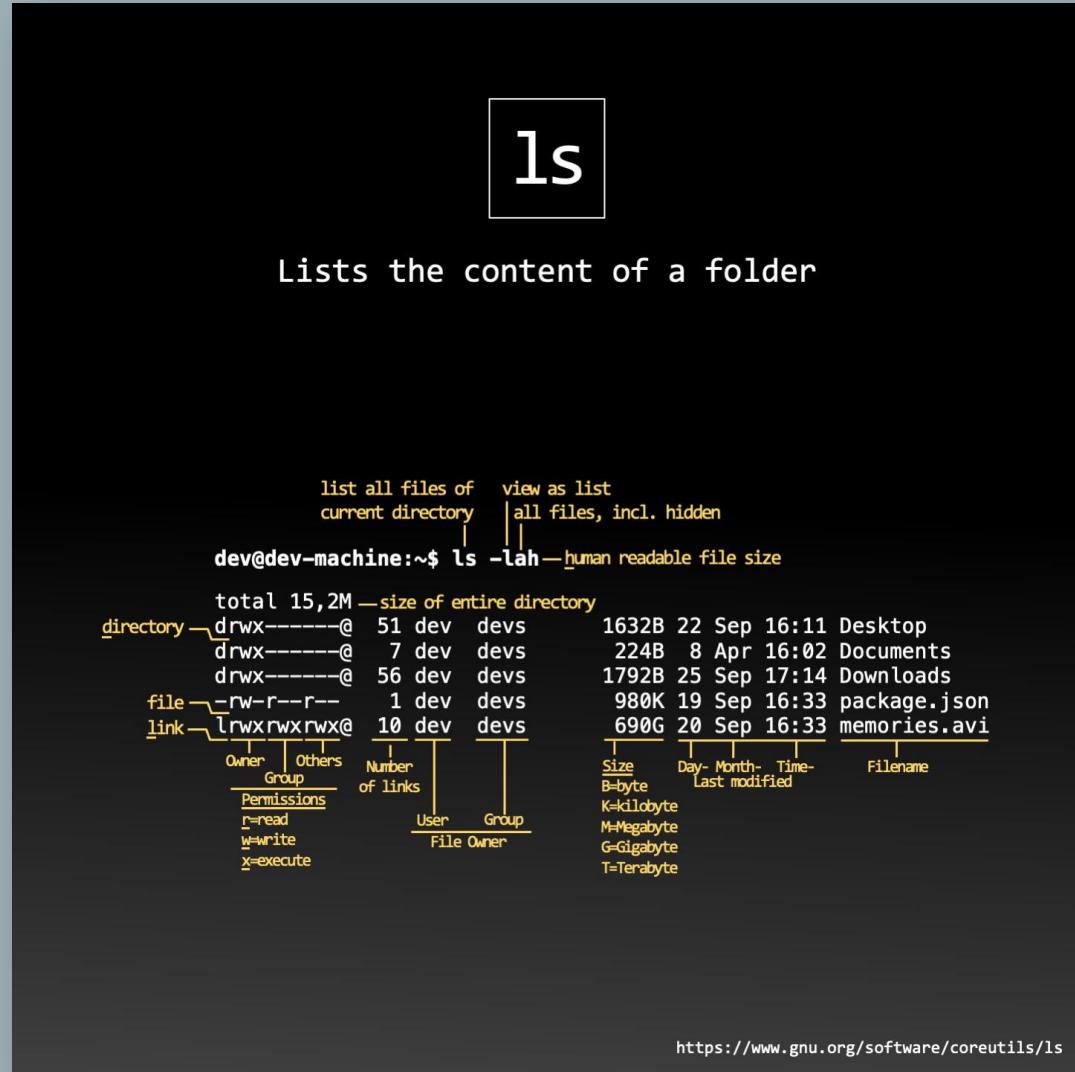
root@41242c7d9028:/# cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog
tty:x:5:
disk:x:6:
lp:x:7:arthur
mail:x:8:
kmem:x:15
...
dialout:x:20:
fax:x:21:
ahmed:x:1002:
employee:x:1015:
familles:x:1005:martineau
```

## AJOUTER / MODIFIE / SUPPRIME UN GROUPE

- La commande pour créer un groupe est « **groupadd** » ( et **addgroup sous Debian**).
- La commande pour modifier un groupe est « **groupmod** ».
- **gpasswd -d « nom\_groupe » « login\_utilisateur »** : Supprime un utilisateur d'un groupe.
- Ci-dessous les options « **groupmod** » :

Option	Rôle
<b>-g &lt;GID&gt;</b>	Modifie le GID. Attention, le groupe d'appartenance des fichiers concernés n'est pas modifié.
<b>-h</b>	Affiche un message d'aide et quitter
<b>-n &lt;nouveau_nom&gt;</b>	Le nom du groupe sera modifié de <u>GROUPE</u> vers <u>NOUVEAU NOM GROUPE</u> .
<b>-o</b>	En combinaison avec l'option <b>-g</b> , cette option permet de changer l'identifiant du groupe ( <u>GID</u> ) vers une valeur déjà utilisée.
<b>-p</b>	Mot de passe chiffré, comme renvoyé par <u>crypt(3)</u> .
<b>-R</b>	Appliquer les changements dans le répertoire <u>RÉP_CHROOT</u> et utiliser les fichiers de configuration du répertoire <u>RÉP_CHROOT</u> .

## 3-4 gérer les utilisateurs



The terminal window shows the output of the `ls -lah` command, which lists the contents of the current directory in a long format. The output includes file names, sizes, modification dates, and permissions. A legend at the bottom explains the permission symbols (r, w, x) and file types (d for directory, - for file, l for link). The terminal also displays help text for the `list` command.

```
list all files of      view as list
current directory      | all files, incl. hidden

dev@dev-machine:~$ ls -lah--human readable file size

total 15,2M --size of entire directory
directory  drwx-----@ 51 dev  devs   1632B 22 Sep 16:11 Desktop
           drwx-----@  7 dev  devs   224B  8 Apr 16:02 Documents
           drwx-----@ 56 dev  devs  1792B 25 Sep 17:14 Downloads
file     -rw-r--r--  1 dev  devs   980K 19 Sep 16:33 package.json
link     lrwxrwxrwx@ 10 dev  devs  6906 20 Sep 16:33 memories.avi

Owner   Others   Number   Size   Day- Month- Time-   Filename
Group   Group   of links  B-byte K=kilobyte M=Megabyte G=Gigabyte T=Terabyte
Permissions          User       Group
r=read
w=write
x=execute

https://www.gnu.org/software/coreutils/ls
```

## MODIFIER LES DROITS SUR UN DOSSIER OU UN FICHIER

- La commande pour modifier les droits sur un fichier ou un dossier est « **chmod** ».
- Pour utiliser cette commande sur un dossier ou un fichier, il faut être :
  - ROOT (super utilisateur).
  - Propriétaire du dossier ou fichier.
- Il existe différents niveaux concernant les droits :
  - r (4) : autorisation de lecture
  - w (2) : autorisation d'écriture
  - x (1) : autorisation d'exécution.
- Ces droits peuvent être différents pour 3 entités :
  - ❑ (u) propriétaire ou owner.
  - ❑ (g) Groupe utilisateur du fichier.
  - ❑ (o) Les autres.

Correspondances de représentation des droits			
Droit	Valeur alphanumérique	Valeur octale	Valeur binaire
aucun droit	---	0	000
exécution seulement	--x	1	001
écriture seulement	-w-	2	010
écriture et exécution	-wx	3	011
lecture seulement	r--	4	100
lecture et exécution	r-x	5	101
lecture et écriture	rw-	6	110
tous les droits (lecture, écriture et exécution)	rwx	7	111

## 3-4 gérer les utilisateurs

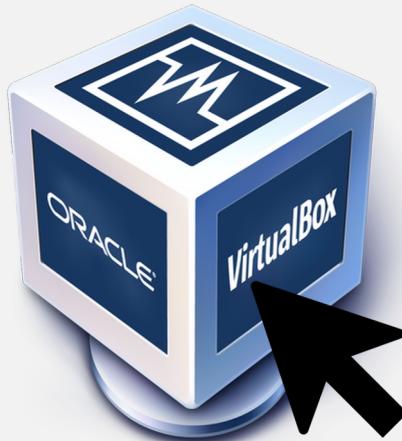
### EXEMPLE MODIFICATION DROIT DOSSIER ET FICHIER

```
mohamed@mohamed-test3:~$ chmod 744 file.txt
mohamed@mohamed-test3:~$ ls -l
total 36
drwxr-xr-x 2 mohamed mohamed 4096 nov. 14 10:17 Bureau
drwxr-xr-x 2 mohamed mohamed 4096 nov. 14 10:17 Documents
-rwxr--x--x 1 root root 0 nov. 14 15:17 file
-rwxr--r-- 1 mohamed comptabilite 28 nov. 14 17:13 file.txt
drwxr-xr-x 2 mohamed mohamed 4096 nov. 14 10:17 Images
drwxr-xr-x 2 mohamed mohamed 4096 nov. 14 10:17 Modèles
drwxr-xr-x 2 mohamed mohamed 4096 nov. 14 10:17 Musique
drwxr-xr-x 2 mohamed mohamed 4096 nov. 14 10:17 Public
drwxr-xr-x 2 mohamed mohamed 4096 nov. 14 10:17 Téléchargements
drwxr-xr-x 2 mohamed mohamed 4096 nov. 14 10:17 Vidéos
mohamed@mohamed-test3:~$ chmod 664 file.txt
mohamed@mohamed-test3:~$ ls -l
total 36
drwxr-xr-x 2 mohamed mohamed 4096 nov. 14 10:17 Bureau
drwxr-xr-x 2 mohamed mohamed 4096 nov. 14 10:17 Documents
-rwxr--x--x 1 root root 0 nov. 14 15:17 file
-rw-rw-r-- 1 mohamed comptabilite 28 nov. 14 17:13 file.txt
drwxr-xr-x 2 mohamed mohamed 4096 nov. 14 10:17 Images
drwxr-xr-x 2 mohamed mohamed 4096 nov. 14 10:17 Modèles
drwxr-xr-x 2 mohamed mohamed 4096 nov. 14 10:17 Musique
drwxr-xr-x 2 mohamed mohamed 4096 nov. 14 10:17 Public
drwxr-xr-x 2 mohamed mohamed 4096 nov. 14 10:17 Téléchargements
drwxr-xr-x 2 mohamed mohamed 4096 nov. 14 10:17 Vidéos
```

- « **chmod 744 dossier\_1** » : On octroie tous les droits (rwx) au propriétaire, les droits de lecture au groupe et aux autres sur le dossier : dossier\_1.
- « **chmod -R 766 dossier\_2** » : On octroie tous les droits (rwx) au propriétaire, les droits de lecture et écriture au groupe et aux autres sur le dossier : dossier\_2 et à l'ensemble de ses sous-dossiers et fichiers.
- « **chmod o+x startup.sh** » : On octroie les droits d'exécution pour les autres sur le fichier : startup.sh .

## 3-3 GÉRER LES UTILISATEURS

Un peu de pratique





TP TIME

TP\_2 LINUX : Gestion utilisateur



TP avec un Google Forms

## 3-4 GÉRER LES PROCESSUS

- Rappel : Linux est un système multi-tâches et multi-utilisateurs.
- Il y a donc beaucoup de processus exécuter sur les distributions et sur les machines.
- Un **processus** représente à la fois un programme en cours d'exécution et tout son environnement d'exécution (mémoire, état, identification, propriétaire, père...).
- Un processus peut passer par plusieurs états ou stades (process state) :
  - exécution en mode utilisateur (**user mode**) ;
  - exécution en mode noyau (**kernel mode**) ;
  - en attente E/S (**waiting**) ;
  - endormi (**sleeping**) ;
  - prêt à l'exécution (**runnable**) ;
  - endormi dans le swap (**mémoire virtuelle**) ;
  - nouveau processus ;



***Il existe plusieurs commandes afin de connaître les processus en cours et ainsi interagir avec eux au sein de sa machine...***

## 3-4 GÉRER LES PROCESSUS

```
alain@mohamed-VirtualBox:~$ w
16:18:27 up 4:08, 1 user, load average: 0,21, 0,39, 0,21
UTIL.   TTY      DE          LOGIN@    IDLE    JCPU    PCPU QUOI
alain    tty7    :0          16:15     4:56m  2.37s  0.29s cinnamon-sessio
```

### LES PRINCIPALES COMMANDES (W)

- La commande « **w** » permet de savoir qui est connecté et depuis quand ainsi que d'autres informations. Il donne un état rapide du système.
- **La première ligne nous donne :**
  1. L'heure au moment où notre commande a été tapé.
  2. **up** (ou **uptime**) : Depuis combien de temps l'ordinateur est en état de fonctionnement.
  3. Le nombre d'utilisateur connecté à la machine.
  4. Le **load average** : représente le nombre moyen de processus en train de fonctionner et qui réclame le processeur de votre machine. *Valeur 1 : charge moyenne depuis 1 minutes, Valeur 2 : charge moyenne depuis 5 minutes et enfin valeur 3 : charge moyenne depuis 15 minutes.*
- **La seconde ligne nous informe (liste des connectés) :**
  1. **User** : le login de la personne connectée.
  2. **TTY** : le nom de la console utilisé par l'utilisateur.
  3. **DE ou FROM** : adresse IP depuis laquelle l'utilisateur se connecte.
  4. **LOGIN@** : l'heure à laquelle l'utilisateur s'est connecté.
  5. **IDLE** : durée de connexion
  6. **JCPU** : Le temps JCPU est le temps utilisé par tous les processus attachés au tty
  7. **PCPU** : Le temps PCPU est le temps utilisé par le processus actuel
  8. **WHAT** : Quel commande l'utilisateur est-il en train d'effectuer.

## 3-4 GÉRER LES PROCESSUS

```
# commande "ps" sans option :  
ahmed@41242c7d9028:/$ ps  
 PID TTY          TIME CMD  
301 pts/4        00:00:00 bash  
309 pts/4        00:00:00 ps
```

### LES PRINCIPALES COMMANDES (PS)

- La commande « **ps** » (**process state**) permet de lister, de manière statique, les processus qui tournent sur votre pc.
- Il s'agit d'une photo à un instant T et non pas en temps réel. La liste ne s'actualise pas malgré l'évolution des différents processus.
- Il existe beaucoup d'option avec la commande « **ps** ». Tester avec man ps.
- La commande « **ps** » donne un affichage en plusieurs parties (avec options):
  1. **PID** : Process ID : chaque processus (UNIX) est identifié par un numéro unique.
  2. **PPID** : Parent Process ID : chaque process peut lui-même lancer d'autres processus et être lancé par d'autres processus.
  3. **C** : facteur de priorité (plus grande = plus importante).
  4. **STIME** : heure de lancement du processus.
  5. **UID et GID** : User ID : Il s'agit de l'ID de l'utilisateur à l'origine du processus et de l'ID du groupe de l'utilisateur qui a lancé le processus.
  6. **TTY** : Il s'agit du nom de la console depuis laquelle le processus a été lancé.
  7. **TIME** : C'est la durée d'exécution du processus => durée pendant laquelle le processus a occupé le processeur depuis son lancement.
  8. **CMD** : C'est le programme à l'origine du processus. Il peut y avoir plusieurs fois le même programme mais avec un processus différent (PID).

## 3-4 GÉRER LES PROCESSUS

```
# exemple avec l'option pour la relation de filiation dans les processus :  
ahmed@41242c7d9028:/$ ps -efH  
UID      PID  PPID  C STIME TTY          TIME CMD  
root     285    0   0 05:24 pts/4    00:00:00 /bin/bash  
root     300    285  0 07:09 pts/4    00:00:00   su ahmed  
ahmed   301    300  0 07:09 pts/4    00:00:00   bash  
ahmed   311    301  0 08:28 pts/4    00:00:00   ps -efH  
root     252    0   0 00:55 pts/3    00:00:00 /bin/bash  
root     235    0   0 00:45 pts/2    00:00:00 /bin/bash  
root     12     0   0 Aug25 pts/1   00:00:00 /bin/bash  
root     225    12    0 00:28 pts/1   00:00:00   su ahmed  
ahmed   226    225  0 00:28 pts/1   00:00:00   bash  
ahmed   234    226  0 00:32 pts/1   00:00:22   top  
root     1     0   0 Aug25 pts/0   00:00:00 bash
```

## LES PRINCIPALES COMMANDES (PS)

Quelques options avec la commande « ps » :

- I. **ps -ef** : On obtient la liste complète de tous les processus lancés par tous les utilisateurs sur l'ensemble des consoles.
- I. **ps -efH** : Avec cette commande, on visualise l'ensemble des processus avec une notion de parentalité ou de filiation dans les relations de processus. L'indentation permet de voir les processus enfant.
- I. **ps -u <user>** : La liste des processus d'un utilisateur s'affiche dans la console.

## 3-4 GÉRER LES PROCESSUS

```
# exemple commande top (FR):
alain@mohamed-VirtualBox:~$ top
Tâches: 169 total, 1 en cours, 168 en veille, 0 arrêté, 0 zombie
%Cpu(s): 5,0 ut, 1,7 sy, 0,0 ni, 92,0 id, 1,3 wa, 0,0 hi, 0,0 si, 0,0 st
MiB Mem : 10862,4 total, 9110,1 libr, 714,7 util, 1037,6 tamp/cache
MiB Éch: 739,1 total, 739,1 libr, 0,0 util. 9851,5 dispo Mem

 PID UTIL. PR NI VIRT RES SHR S %CPU %MEM TEMPS+ COM.
 1532 alain 20 0 3346000 217100 134284 S 3,7 2,0 0:20.35 cinnamon
 1847 alain 20 0 541492 41056 31884 S 1,3 0,4 0:00.62 gnome-t+
 960 root 20 0 682916 125108 71752 S 1,0 1,1 0:02.77 Xorg
 8 root 20 0 0 0 I 0,3 0,0 0:00.02 kworker+
 1 root 20 0 101832 11188 8216 S 0,0 0,1 0:01.14 systemd
 2 root 20 0 0 0 S 0,0 0,0 0:00.00 kthreadd
 3 root 0 -20 0 0 0 I 0,0 0,0 0:00.00 rcu_gp
 4 root 0 -20 0 0 0 I 0,0 0,0 0:00.00 rcu_par+
 5 root 20 0 0 0 I 0,0 0,0 0:00.00 kworker+
 6 root 0 -20 0 0 0 I 0,0 0,0 0:00.00 kworker+
 7 root 20 0 0 0 I 0,0 0,0 0:00.03 kworker+
 9 root 0 -20 0 0 0 I 0,0 0,0 0:00.00 mm_perc+
10 root 20 0 0 0 S 0,0 0,0 0:00.08 ksoftirq+
11 root 20 0 0 0 I 0,0 0,0 0:00.18 rcu_sch+
12 root rt 0 0 0 S 0,0 0,0 0:00.00 migrati+
13 root -51 0 0 0 S 0,0 0,0 0:00.00 idle_in+
14 root 20 0 0 0 S 0,0 0,0 0:00.00 cpuhp/0
```

## LES PRINCIPALES COMMANDES (TOP)

- La commande « **top** » va afficher une liste dynamique des processus contrairement à la commande « **ps** ».
- L'affichage des informations de la commande « **top** » se décompose en 6 parties :
  - I. La première partie a déjà été abordé avec la commande « **w** ».
  - I. La deuxième partie : Nous donne des informations sur l'ensemble des processus en cours avec une répartition par état => total – en cours – en veille – arrêté – zombie.
  - I. Activité CPU :
    - **us** : Charge processeur demandée par des processus utilisateurs.
    - **sy** : Tout temps CPU passé par des instructions bas niveau, niveau kernel.
    - **ni** : Charge demandée par des processus utilisateurs « nicés ».
    - **id** : Pourcentage de ressources processeur libres ( tâches inactives).
    - **wa** : charge de processus dédiés à une tâche système ou utilisateur.

## 3-4 GÉRER LES PROCESSUS

Exemple avec « htop » : interface colorée et lisible

```
CPU[|||] 3.4% Tasks: 100, 216 thr; 1 running
Mem[|||||] 782M/10.6G Load average: 0.00 0.03 0.07
Swp[ ] 0K/739M Uptime: 02:34:47

PID USER PRI NI VIRT RES SHR S CPU% MEM% TIME+ Command
883 root 20 0 698M 168M 74552 S 2.0 1.6 0:37.03 /usr/lib/xorg/Xorg -core :0 -s
1463 mohamed 20 0 3319M 257M 135M S 0.7 2.4 10:38.55 cinnamon --replace
2564 mohamed 20 0 529M 41760 31792 S 0.7 0.4 0:15.27 /usr/libexec/gnome-terminal-se
4775 mohamed 20 0 13976 4812 3316 R 0.7 0.0 0:00.48 htop
1189 mohamed 20 0 154M 2820 2448 S 0.7 0.0 0:22.70 /usr/bin/VBoxClient --dragandd
898 root 20 0 698M 168M 74552 S 0.7 1.6 0:00.92 /usr/lib/xorg/Xorg -core :0 -s
491 messagebu 20 0 8720 5508 3896 S 0.7 0.0 0:01.94 /usr/bin/dbus-daemon --system
1183 mohamed 20 0 154M 2820 2448 S 0.0 0.0 0:22.70 /usr/bin/VBoxClient --dragandd
1533 mohamed 20 0 698M 70876 48380 S 0.0 0.6 0:01.79 nemo-desktop
496 root 20 0 239M 9660 8656 S 0.0 0.1 0:00.18 /usr/lib/accountsservice/accou
866 root 20 0 355M 2960 2548 S 0.0 0.0 0:01.67 /usr/sbin/VBoxService --pidfil
1 root 20 0 99M 11348 8372 S 0.0 0.1 0:01.57 /sbin/init splash
288 root 19 -1 51624 17296 15988 S 0.0 0.2 0:00.41 /lib/systemd/systemd-journald
323 root 20 0 23700 7440 4120 S 0.0 0.1 0:00.79 /lib/systemd/systemd-udevd
471 systemd-r 20 0 24024 13276 9192 S 0.0 0.1 0:00.27 /lib/systemd/systemd-resolved
615 root 20 0 239M 9660 8656 S 0.0 0.1 0:00.01 /usr/lib/accountsservice/accou
486 root 20 0 239M 9660 8656 S 0.0 0.1 0:00.26 /usr/lib/accountsservice/accou
487 root 20 0 2540 784 716 S 0.0 0.0 0:00.05 /usr/sbin/acpid
488 avahi 20 0 8524 3540 3212 S 0.0 0.0 0:00.06 avahi-daemon: running [mohamed
489 root 20 0 11960 2952 2696 S 0.0 0.0 0:00.02 /usr/sbin/cron -f
490 root 20 0 30588 8596 7384 S 0.0 0.1 0:00.03 /usr/sbin/cupsd -l

F1Help F2Setup F3Search F4Filter F5Tree F6SortBy F7Nice -F8Nice +F9Kill F10Quit
```

## LES PRINCIPALES COMMANDES (TOP)

4. La 4ème partie : affiche des informations sur la mémoire vive physique : totale, utilisé (cache + buffer) et libre.
4. La 5ème partie (swap) : affiche des informations sur la mémoire vive virtuelle : totale, utilisé (cache + buffer) et libre.
4. La dernière partie est présentée sous forme de tableau ou liste :
  - **PID** : *Id unique du processus ( déjà abordé).*
  - **USER** : *login utilisateur.*
  - **PR** : *Le champ "PR" montre la priorité d'ordonnancement du processus du point de vue du noyau. La valeur nice affecte la priorité d'un processus.*
  - **NI** : *Valeur de nice. Il s'agit de la priorité d'un processus sur le temps processeur (CPU Time).*
  - **VIRT** : *nous donne la quantité totale de mémoire consommée par un processus. Cela inclut le code du programme, les données stockées par le processus en mémoire, ainsi que toutes les régions de mémoire qui ont été échangées sur le disque.*
  - **RES** : *est la mémoire consommée par le processus en RAM.*
  - **MEM%** : *exprime la valeur de RES en pourcentage de la RAM totale disponible.*
  - **SHR** : *la quantité de mémoire partagée avec d'autres processus.*
  - **CPU%** : *Représente la part de la tâche dans le temps CPU écoulé depuis la dernière mise à jour de l'écran, exprimée en pourcentage du temps CPU total.*

## 3-4 GÉRER LES PROCESSUS

```
# exemple commande top avec l'option -u:  
alain@mohamed-VirtualBox:~$ top -u alain  
top - 17:03:28 up 30 min,  1 user,  load average: 0,00, 0,06, 0,18  
Tâches: 162 total,  1 en cours, 161 en veille,  0 arrêté,  0 zombie  
%Cpu(s): 4,7 ut, 0,7 sy, 0,0 ni, 93,2 id, 1,4 wa, 0,0 hi, 0,0 si, 0,0 st  
MiB Mem : 10862,4 total, 8923,8 libr, 749,4 util, 1189,1 tamp/cache  
MiB Éch: 739,1 total, 739,1 libr, 0,0 util. 9792,7 dispo Mem  
  
 PID UTIL. PR NI VIRT RES SHR S %CPU %MEM TEMPS+ COM.  
1532 alain 20 0 3365912 238164 134448 S 3,0 2,1 2:24.60 cinnam+  
1847 alain 20 0 542540 42224 32216 S 1,0 0,4 0:01.65 gnome--+  
1190 alain 20 0 380192 27784 20812 S 0,3 0,2 0:00.37 cinnam+  
1248 alain 20 0 157904 2716 2344 S 0,3 0,0 0:03.77 VBoxCl+  
1392 alain 20 0 302860 26268 20104 S 0,3 0,2 0:00.26 csd-ke+  
1578 alain 20 0 400016 45292 37056 S 0,3 0,4 0:00.18 nm-app+  
2875 alain 20 0 736608 85696 47724 S 0,3 0,8 0:01.67 xed  
1174 alain 20 0 18500 9856 8176 S 0,0 0,1 0:00.13 systemd  
1175 alain 20 0 105288 3504 4 S 0,0 0,0 0:00.00 (sd-pa+  
1184 alain 9 -11 1148900 19808 15872 S 0,0 0,2 0:00.15 pulsea+  
1187 alain 20 0 243080 8056 7048 S 0,0 0,1 0:00.03 gnome-+  
1191 alain 20 0 8096 5176 3896 S 0,0 0,0 0:00.33 dbus-d+  
1203 alain 20 0 242444 8008 7000 S 0,0 0,1 0:00.06 gvfsd  
1208 alain 20 0 382052 8556 7656 S 0,0 0,1 0:00.00 gvfsd--+  
1229 alain 20 0 25152 360 0 S 0,0 0,0 0:00.00 VBoxCl+  
1231 alain 20 0 157288 2204 1656 S 0,0 0,0 0:00.00 VBoxCl+  
1241 alain 20 0 25152 360 0 S 0,0 0,0 0:00.00 VBoxCl+
```

## LES PRINCIPALES COMMANDES (TOP)

6. La dernière partie est présenté sous forme de tableau ou liste (suite):

- **TIME+** : Il s'agit du temps CPU total utilisé par le processus depuis son démarrage, précis au centième de seconde.
- **COMMAND** : Nom du programme ou ligne de commande utilisée (si on appuie sur « c ») pour lancer le programme.

Quelques options avec « top » :

Option	Rôle
-u <utilisateur>	Filtre en fonction de l'utilisateur que vous voulez.
-F	Change la colonne selon laquelle les processus sont triés.
-k	Tue un processus, c'est-à-dire arrête ce processus
v	Pendant l'utilisation de top => fait apparaitre une arborescence
-o <nom colonne>	Trie la liste en fonction de la colonne sélectionnée

# 3-4 GÉRER LES PROCESSUS

## LES PRINCIPALES COMMANDES (KILL)

```
root@41242c7d9028:/# top
top - 16:11:31 up 1 day, 16:51, 0 users, load average: 0.00, 0.00, 0.00
Tasks: 10 total, 1 running, 9 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.1 us, 0.3 sy, 0.0 ni, 99.6 id, 0.0 wa, 0.0 hi, 0.1 si, 0.0 st
KiB Mem : 2036732 total, 479584 free, 334856 used, 1222292 buff/cache
KiB Swap: 1048572 total, 868996 free, 179576 used. 1293264 avail Mem

PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 1 root      20   0  3560  2812  2348 S  0.0  0.1  0:00.02 bash
 12 root     20   0  3572  2872  2380 S  0.0  0.1  0:00.53 bash
225 root     20   0  4960  2536  2140 S  0.0  0.1  0:00.01  `-- su
226 ahmed   20   0  3548  2888  2416 S  0.0  0.1  0:00.03  `-- ba+
235 root     20   0  3568  2876  2380 S  0.0  0.1  0:00.05 bash
252 root     20   0  3564  2880  2392 S  0.0  0.1  0:00.04 bash
285 root     20   0  3568  2912  2428 S  0.0  0.1  0:00.07 bash
841 root     20   0  3840  2424  1972 S  0.3  0.1  0:07.00  `-- htop
842 root     20   0  3564  2840  2380 S  0.0  0.1  0:00.03 bash
855 root     20   0  5700  2592  2164 R  0.0  0.1  0:00.08  `-- top

root@41242c7d9028:/# kill 226

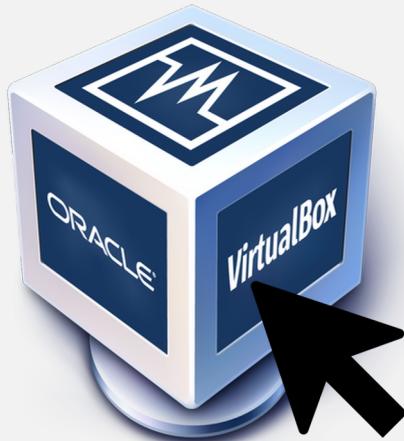
root@41242c7d9028:/# top
top - 16:12:36 up 1 day, 16:52, 0 users, load average: 0.00, 0.00, 0.00
Tasks: 8 total, 1 running, 7 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.2 us, 0.2 sy, 0.0 ni, 99.7 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 2036732 total, 480008 free, 334392 used, 1222332 buff/cache
KiB Swap: 1048572 total, 868996 free, 179576 used. 1293700 avail Mem

PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 1 root      20   0  3560  2812  2348 S  0.0  0.1  0:00.02 bash
 12 root     20   0  3572  2872  2380 S  0.0  0.1  0:00.53 bash
235 root     20   0  3568  2876  2380 S  0.0  0.1  0:00.05 bash
252 root     20   0  3564  2880  2392 S  0.0  0.1  0:00.04 bash
285 root     20   0  3568  2912  2428 S  0.0  0.1  0:00.07 bash
841 root     20   0  3840  2424  1972 S  0.0  0.1  0:07.11 htop
842 root     20   0  3564  2864  2376 S  0.0  0.1  0:00.03 bash
856 root     20   0  5700  2596  2172 R  0.0  0.1  0:00.01 top
```

- La commande « **kill** » va stopper un processus.
- Pour préciser quel processus, on utilisera son PID ( unique).
- Vigilance de ne pas supprimer n'importe quel processus.
- On peut tuer plusieurs processus en même temps.
- On peut tuer de manière brutale un processus qui tarderait à s'arrêter avec la commande « **kill -9 <numero PID** » .
- Avec cette commande risque de perte de donnée ou autres.
- La commande « **killall** » tue tous les processus avec le nom du programme => notamment les programmes qui génèrent plusieurs processus comme les navigateurs web.

## 3-4 GÉRER LES PROCESSUS

Un peu de pratique



## 3-4 GÉRER LES PROCESSUS

```
root@41242c7d9028:/# apt update && sudo apt install kubuntu-desktop &
[1] 2443
Hit:1 http://ppa.launchpad.net/gnome3-team/gnome3/ubuntu xenial InRelease
Get:2 https://download.docker.com/linux/ubuntu xenial InRelease [66.2 kB]
Err:2 https://download.docker.com/linux/ubuntu xenial InRelease
  The following signatures couldn't be verified because the public key is not available: NO_PUBKEY
7EA0A9C3F273FC08
Hit:3 http://ports.ubuntu.com/ubuntu-ports xenial InRelease
Get:4 http://ports.ubuntu.com/ubuntu-ports xenial-updates InRelease [109 kB]
Get:5 http://ports.ubuntu.com/ubuntu-ports xenial-backports InRelease [107 kB]
Get:6 http://ports.ubuntu.com/ubuntu-ports xenial-security InRelease [109 kB]
Get:7 http://ports.ubuntu.com/ubuntu-ports xenial-updates/main arm64 Packages [1556 kB]

root@41242c7d9028:/# nohup apt update && sudo apt install kubuntu-desktop
nohup: ignoring input and appending output to 'nohup.out'
```

## LES PROCESSUS EN ARRIERE PLAN (& et nohup)

- La commande « **&** » va permettre de lancer un processus en arrière plan et ainsi éviter que la console soit mobilisée pendant l'opération.
  - La commande s'utilise à la fin la ligne (peut être collé au dernier mot).
  - En réponse à la commande, le numéro du processus en arrière plan est communiqué ainsi que le PID (pour pouvoir le tuer si nécessaire).
- 
- Risque : Si la console se ferme, le processus est arrêté. 
  - La commande « **nohup** » permet de corriger cet écueil.
  - Elle s'utilise comme cela « nohup <reste de la commande>

## 3-4 GÉRER LES PROCESSUS

```
# commande de recherche du mot "lib" dans le dossier racine du système de fichier
root@41242c7d9028:/# find / "lib"
/
/dev
/dev/console
/dev/core
/dev/stderr
/dev/stdout
/dev/stdin
/dev/fd
/dev/ptmx
/dev/urandom
/dev/zero
/dev/tty
/dev/full
/dev/random
/dev/null
/dev/shm
/dev/mqueue
/dev/pts
/dev/pts/6
/dev/pts/5
...
[1]+  Stopped                  find / "lib"
# stopper par ctrl + z

#apparaît avec le statut de stopped (arrêté) avec la commande jobs
root@41242c7d9028:/# jobs
[1]+  Stopped                  find / "lib"

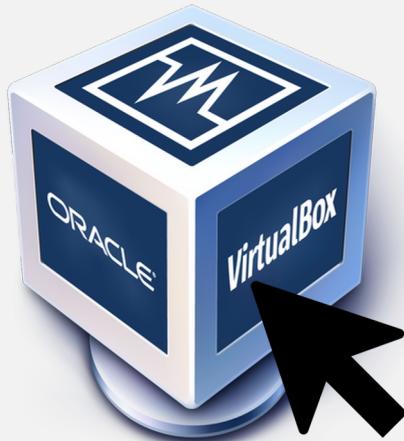
# On remet au premier plan le processus numéro 1 en arrière plan
root@41242c7d9028:/# fg %1
find / "lib"
/usr/lib/python3.5/distutils/_pycache__
/usr/lib/python3.5/distutils/_pycache__/util.cpython-35.pyc
/usr/lib/python3.5/distutils/_pycache__/msvc9compiler.cpython-35.pyc
/usr/lib/python3.5/distutils/_pycache__/ccompiler.cpython-35.pyc
/usr/lib/python3.5/distutils/_pycache__/core.cpython-35.pyc
/usr/lib/python3.5/distutils/_pycache__/cmd.cpython-35.pyc
/usr/lib/python3.5/distutils/_pycache__/msvccompiler.cpython-35.pyc
/usr/lib/python3.5/distutils/_pycache__/bccppcompiler.cpython-35.pyc
/usr/lib/python3.5/distutils/_pycache__/cygwinccompiler.cpython-35.pyc
/usr/lib/python3.5/distutils/_pycache__/_init__.cpython-35.pyc
/usr/lib/python3.5/distutils/_pycache__/unixccompiler.cpython-35.pyc
```

### LES PROCESSUS EN ARRIERE PLAN (Crtl + Z, jobs, bg et fg)

- La commande « **Ctrl + Z** » va permettre de suspendre le processus pour vous permettre d'effectuer une action par exemple.
- La commande « **bg** » peut être utilisé à la suite de la commande « **Ctrl + Z** » pour que le processus bascule en arrière plan.
- La commande « **jobs** » va indiquer les processus en arrière plan.
- La commande « **jobs** » indiquera le numéro du processus en arrière plan, son statut et son nom.
- La commande « **fg** » va remettre un processus au premier plan.
- Si rien n'est précisé, il remettra à chaque exécution de la commande le premier processus de la liste que nous fournit la commande « **jobs** ».
- Si on souhaite précisé un processus spécifique au premier plan, il faudra rajouter %<numéro processus en arrière plan > à la suite de la commande « **fg** ».

## 3-4 GÉRER LES PROCESSUS

Un peu de pratique





TP TIME

TP\_3 LINUX : Processus



TP avec un Google Forms

## 3-5 PROGRAMMER DES TRAVAUX PÉRIODIQUES

- Le service **cron** permet la programmation d'événements à répétition.
- Plusieurs outils avec Linux existent comme **crontab**.
- Cela va permettre de programmer des actions dans le temps et de manière répétitive.
- La commande « **at** » permet une programmation non répétitive.

## 3-5 PROGRAMMER DES TRAVAUX PÉRIODIQUES

### PROGRAMMATION NON REPETITIVE (at)

```
root@30f9b8a2ed06:/# at 16:00
warning: commands will be executed using /bin/sh
at> touch fichier3.txt
at> <EOT>
job 9 at Sat Aug 28 16:00:00 2021

root@30f9b8a2ed06:/# at 16:45 30.08.2021
warning: commands will be executed using /bin/sh
at> echo salut à tous
at> <EOT>
job 12 at Mon Aug 30 16:45:00 2021

root@30f9b8a2ed06:/# at now +4 minutes
warning: commands will be executed using /bin/sh
at> touch fichier4.txt
at> <EOT>
job 13 at Sat Aug 28 16:38:00 2021

root@30f9b8a2ed06:/# at 14:17 tomorrow
warning: commands will be executed using /bin/sh
at> echo good morning
at> <EOT>
job 14 at Sun Aug 29 14:17:00 2021
```

- La commande « **at** » va permettre d'effectuer une action qui sera programmé dans le temps.
- Pour que **at** fonctionne le service **atd** (*at daemon*) doit fonctionner.
- Elle prend en paramètre une date soit juste une horaire ou une horaire + une journée.
- Une fois, ces premiers paramètres pris en compte, il faudra indiquer la ou les actions à réaliser.
- Chaque action devra être enregistré sur une ligne et se terminer par « entrée ».
- La dernière action ou tache devra se terminer par « entrée » et par « **ctrl + D** ».

## 3-5 PROGRAMMER DES TRAVAUX PÉRIODIQUES

### Contrôle des tâches programmées (atq & atrm)

```
root@30f9b8a2ed06:/# atq
4  Sat Aug 28 17:00:00 2021 a root
3  Sat Aug 28 16:59:00 2021 a root
5  Sat Aug 28 17:02:00 2021 a root
2  Sat Aug 28 16:56:00 2021 a root
13 Sat Aug 28 16:38:00 2021 a root
12 Mon Aug 30 16:45:00 2021 a root
7   Sat Aug 28 17:11:00 2021 a root
11 Sat Aug 28 16:56:00 2021 a root
6   Sat Aug 28 17:04:00 2021 a root

root@30f9b8a2ed06:/# atrm 11

root@30f9b8a2ed06:/# atq
4  Sat Aug 28 17:00:00 2021 a root
14 Sun Aug 29 14:17:00 2021 a root
3  Sat Aug 28 16:59:00 2021 a root
5  Sat Aug 28 17:02:00 2021 a root
2  Sat Aug 28 16:56:00 2021 a root
12 Mon Aug 30 16:45:00 2021 a root
7   Sat Aug 28 17:11:00 2021 a root
6   Sat Aug 28 17:04:00 2021 a root
```

- La commande « **atq** » (at queue) va lister les tâches programmées en attente d'être exécutées.
- Elle s'affiche avec un numéro unique permettra de les cibler si nécessaire.
- La commande « **atrm** » (at remove) va supprimer la tâche programmée grâce à son numéro.

## 3-5 PROGRAMMER DES TRAVAUX PÉRIODIQUES

Editeur nano suite commande : « crontab -e »

```
GNU nano 4.8          /tmp/crontab.R7nG5W/crontab
# Edit this file to introduce tasks to be run by cron.

#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Paste Text^T To Spell  ^_ Go To Line
```

## PROGRAMMATION REPETITIVE (crontab)

- **crontab** est un fichier qui contient la liste des programmes qui sont exécutés régulièrement.
- **cron** est le programme ou le service qui se charge d'exécuter les tâches aux périodes demandées.
- « **crontab -l** » affiche la liste des tâches périodiques programmées. Si elle est vide : ‘no crontab for root’
- « **crontab -e** » permet de modifier le fichier et d'y enregistrer de nouvelles instructions. Un éditeur de texte va apparaître (nano ou vim).
- « **crontab -r** » supprime les éléments de la crontab.
- La syntaxe doit suivre cette structure : **m h dom mon dow command**

## 3-5 PROGRAMMER DES TRAVAUX PÉRIODIQUES

### PROGRAMMATION REPETITIVE (crontab)

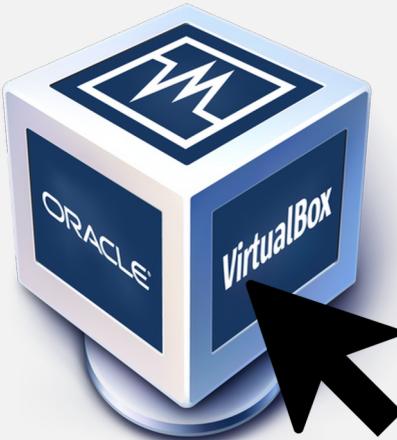


```
# Un fichier nommé fichier.txt est crée tous les jours à 15h47 dans le dossier Document du Bureau de l'utilisateur mohamed.  
47 15 * * * touch /home/mohamed/Document/fichier.txt  
  
# Une copie du fichier fichier.txt sera faite vers le fichier Musique du Bureau de l'utilisateur mohamed à 06h00 du matin tous les 2 du mois.  
0 6 2 * * cp /home/mohamed/Document/fichier.txt /home/mohamed/Musique  
  
# Entre Mai et Decembre, tous les jours et à toutes les heures et 15 minutes, on ecrire test dans le fichier fichier.txt  
15 * * 5-12 * echo "test" >> /home/mohamed/fichier.txt  
  
# Tous les vendredis à 6h, 12h et 18h, on écrit dans le fichier texte nommé message "c'est bientôt le week-end"  
0 6,12,18 * * 5 echo "c'est bientot le week-end" >> /home/mohamed/message.txt
```

- Pour écrire les instructions, il faut suivre une syntaxe précise d'écriture (m h dom mon dow command) :
  1. **m** : nombre de minutes en 0 et 59.
  2. **h** : heures entre 0 et 23.
  3. **dom (day of month)** : le jour du mois entre 1 et 31.
  4. **mon (month)** : entre 1 et 12.
  5. **mow (month of the week)** : jour dans la semaine entre 1 à 5 => Lundi au vendredi. 0 et 6 => dimanche et samedi.
  6. **command** : tâches à effectuer.
- On peut écrire pour la partie mon : 1, 2, 6, 12 : pour les mois de Janvier, Février, Juin et Décembre.
- Lorsque la tâche doit s'appliquer à l'ensemble des éléments d'une période, il faut utiliser \*.

## 3-5 PROGRAMMER DES TRAVAUX PÉRIODIQUES

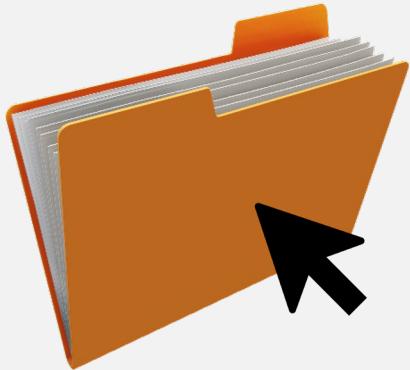
Un peu de pratique





TP TIME

TP\_4 LINUX : Programmation travaux périodiques



TP avec un Google Forms

## 3-5 ORGANISER LES JOURNAUX DE BORDS ET LEURS ROTATIONS

- **Syslog** est à la fois un protocole de journalisation des évènements systèmes et aussi un programme qui est responsable de la prise en charge des fichiers de journalisation du système.
- L'intérêt de **Syslog** est donc de centraliser les journaux d'événements, permettant de repérer plus rapidement et efficacement les défaillances d'ordinateurs présents sur un réseau
- Les journaux **log** sont stockés dans le répertoire **/var/log/**.
- Les **logs** sont catégorisés : auth ( évènements authentification ou sécurité), cron ( evenements relatifs aux tâches planifiées), user ( événements quand aucun service n'est planifié), etc.
- Chaque ligne au sein de ces **logs suit une syntaxe précise** :
  1. La date à laquelle l'évènement a été déclenché.
  2. Le processus déclencheur de l'évènement.
  3. Le processus ayant demandé l'ajout du message correspondant au log.
  4. Le niveau de gravité du message (priority).

**Sep 14 14:09:09 machine\_de\_test dhcp service[warning] 110 corps du message**

## 3-5 ORGANISER LES JOURNAUX DE BORDS ET LEURS ROTATIONS

- Chaque **log** dispose d'un niveau de gravité qui associé à sa catégorie permet de déduire sa priorité.

Code numérique	Sévérité	Description
0	emerg	Système inutilisable (urgence)
1	alert	Intervention immédiate nécessaire (Alerte)
2	crit	Erreur système critique (Critique)
3	err	Erreur de fonctionnement (Erreur)
4	warning	Avertissement
5	notice	Événement normal mais devant être signalé
6	info	Messages d'information
7	debug	Message de débogage

Priorité = (catégorie x 8 ) + gravité

Codes de catégorie		
Code	Mot-clé	Description
0	kern	messages du noyau
1	user	messages de l'espace utilisateur
2	mail	messages du système de messagerie
3	daemon	messages des processus d'arrière plan
4	auth	messages d'authentification
5	syslog	messages générés par syslogd lui-même
6	lpr	messages d'impressions
7	news	messages d'actualités
8	uucp	messages UUCP
9	cron	Tâches planifiées (at/cron)
10	authpriv	sécurité / élévation de priviléges
11	ftp	logiciel FTP

## 3-5 ORGANISER LES JOURNAUX DE BORDS ET LEURS ROTATIONS

### CONTENU D'UN LOG

- ***Details d'un log :***
  1. La date à laquelle a été émis le log.
  2. Le nom de l'équipement ayant généré le log (hostname).
  3. Une information sur le processus qui a déclenché cette émission.
  4. Le niveau de priorité du log.
  5. Un identifiant du processus ayant généré le log.
  6. Enfin un corps de message.

```
# Exemple du log pour le programme syslog
root@mohamed-VirtualBox:/home/alain# cat /var/log/syslog
Sep 3 09:34:18 mohamed-VirtualBox rsyslogd: [origin software="rsyslogd" swVersion="8.2001.0" x-
pid="633" x-info="https://www.rsyslog.com"] rsyslogd was HUPed
Sep 3 09:34:19 mohamed-VirtualBox systemd[1]: logrotate.service: Succeeded.
Sep 3 09:34:19 mohamed-VirtualBox systemd[1]: Finished Rotate log files.
Sep 3 09:34:24 mohamed-VirtualBox systemd[1]: NetworkManager-dispatcher.service: Succeeded.
Sep 3 09:34:24 mohamed-VirtualBox dbus-daemon[602]: [system] Successfully activated service
'org.freedesktop/fwupd'
Sep 3 09:34:24 mohamed-VirtualBox systemd[1]: Started Firmware update daemon.
Sep 3 09:34:24 mohamed-VirtualBox systemd[1]: fwupd-refresh.service: Succeeded.
Sep 3 09:34:24 mohamed-VirtualBox systemd[1]: Finished Refresh fwupd metadata and update motd.
Sep 3 09:34:25 mohamed-VirtualBox systemd[1]: man-db.service: Succeeded.
Sep 3 09:34:25 mohamed-VirtualBox systemd[1]: Finished Daily man-db regeneration.
Sep 3 09:34:33 mohamed-VirtualBox kernel: [ 3076.758001] show_signal_msg: 14 callbacks suppressed
```

## 3-5 ORGANISER LES JOURNAUX DE BORDS ET LEURS ROTATIONS

### CONFIGURATION SYLOG

```
# Details fichier de configuration des logs
root@mohamed-VirtualBox:/home/alain# cat /etc/rsyslog.d/50-default.conf
# Default rules for rsyslog.
#
# For more information see rsyslog.conf(5) and /etc/rsyslog.conf
#
# First some standard log files. Log by facility.
#
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

#
# Logging for the mail system. Split it up so that
# it is easy to write scripts to parse these files.
#
#mail.info            -/var/log/mail.info
#mail.warn             -/var/log/mail.warn
mail.err              /var/log/mail.err

#
# Some "catch-all" log files.
#
#*=debug;
# auth,authpriv.none;
# news.none;mail.none -/var/log/debug
#*=info;*=notice;*=warn;
# auth,authpriv.none;
# cron,daemon.none;
# mail,news.none      -/var/log/messages

#
# Emergencies are sent to everybody logged in.
#
*.emerg    :omusrmsg:*

#
# I like to have messages displayed on the console, but only on a virtual
# console I usually leave idle.
#
#daemon,mail.*;
# news.=crit;news.=err;news.=notice; \
# *=debug;*=info; \
# *=notice;*=warn  /dev/tty8
```

- On peut configurer la gestion des logs avec le fichier de configuration **/etc/syslog.conf** (ou **/etc/rsyslog.d** ou **/etc/vsyslog**).
- Il est en 2 parties :
  - **1ère partie** : (le ou) les processus demandeurs (séparés par un point virgule) suivi d'un point et de leur niveau de priorité. (\* tous niveaux de priorité).
  - **2ème partie** : le fichier log correspondant (qui reçoit le message et l'ajoute à la liste de ses messages) : <fichier de log>

**Syntaxe => service.gravité      destination**

## 3-5 ORGANISER LES JOURNAUX DE BORDS ET LEURS ROTATIONS

● ● ●

```
# Details fichier de rotation pour le service dpkg
# Une rotation tous les mois.
# Un archivage sur les 12 derniers mois.
# Une compression à la 2ème archive.
# Processus continue même si erreur.
# N'effectue pas de rotation si le fichier est vide.
# Cree un nouveau fichier avec comme propriétaire root

root@mohamed-VirtualBox:/home/alain# cat /etc/logrotate.d/dpkg
/var/log/dpkg.log {
    monthly
    rotate 12
    compress
    delaycompress
    missingok
    notifempty
    create 644 root root
}
```

## ROTATION DES JOURNAUX (logs)

### avec `/etc/logrotate`

- Il faut épurer et vider régulièrement les fichiers logs de leurs contenus anciens pour éviter de saturer le stockage de nos disques durs.
- **Important : Si un log est créé, il est important d'assurer qu'un système de rotation est bien mis en place.**
- Structuration d'un fichier dans `/etc/logrotate.d` :
  - **intervalle** : daily, weekly, monthly : période de la rotation du journal.
  - **rotate** : durée conservation des données.
  - **compress** : les logs peuvent être compréssé.
  - **missingok** : permet au processus de ne pas s'arrêter à chaque erreur. Il passe au log suivant.
  - **notempty** : bloque la rotation si le fichier est vide.
  - **create** : crée un fichier vide pour la nouvelle rotation des logs.
  - **size** : donne une taille limite au fichier en m octet.

## 3-5 ORGANISER LES JOURNAUX DE BORDS ET LEURS ROTATIONS



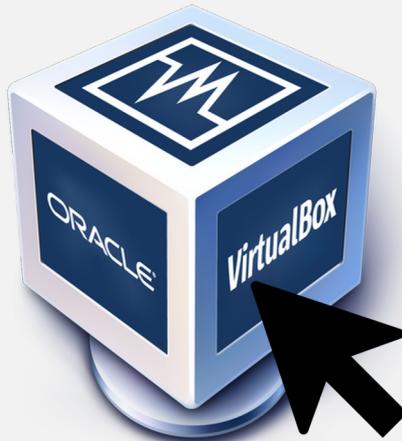
```
# Affiche le status des rotations des différents logs
root@mohamed-VirtualBox:/home/alain# cat /var/lib/logrotate/status
logrotate state -- version 2
"/var/log/syslog" 2021-9-3-9:34:9
"/var/log/dpkg.log" 2021-9-1-9:52:29
"/var/log/unattended-upgrades/unattended-upgrades.log" 2021-9-1-9:0:0
"/var/log/speech-dispatcher/debug-flite" 2021-8-26-16:0:0
"/var/log/unattended-upgrades/unattended-upgrades-shutdown.log" 2021-9-1-9:0:0
"/var/log/auth.log" 2021-9-2-9:23:18
"/var/log/apt/term.log" 2021-9-1-9:52:29
"/var/log/ppp-connect-errors" 2021-8-26-16:0:0
"/var/log/apport.log" 2021-9-1-9:0:0
"/var/log/speech-dispatcher/speech-dispatcher-protocol.log" 2021-8-26-16:0:0
"/var/log/cups/error_log" 2021-9-3-9:34:9
"/var/log/apt/history.log" 2021-9-1-9:52:29
"/var/log/pm-powersave.log" 2021-8-26-16:0:0
"/var/log/boot.log" 2021-9-3-9:34:9
```

## AUTRES INFOS (logs)

- *On peut vérifier le bon fonctionnement des rotations avec*
  - **« cat /var/lib/logrotate/status »**
- *Dans /var/log :*
  - *Le fichier en cours d'utilisation est sans extension.*
  - *Les archives sont numérotés de la plus récente à la plus ancienne.*
  - *Le fichier le plus ancien est supprimé à chaque rotation.*
  - *Exemple :*
    - **/var/log/syslog**
    - **/var/log/syslog.1**
    - **/var/log/syslog.2.gz**
    - **/var/log/syslog.3.gz**

## 3-5 ORGANISER LES JOURNAUX DE BORDS ET LEURS ROTATIONS

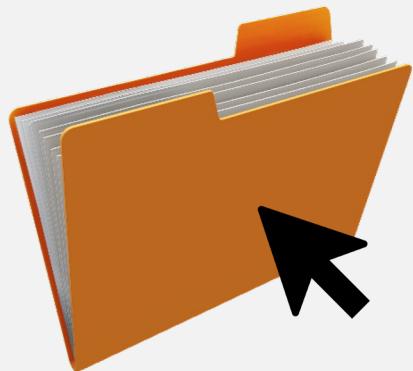
Un peu de pratique





TP TIME

TP\_5 LINUX :Journaux de bord et rotation



TP avec un Google Forms

## 4 - GÉRER L'ESPACE DISQUE.



La vision Linux des disques – partitionner des disques – gestion du LVM

## **4 - GÉRER L'ESPACE DISQUE.**

***4-1. La vision Linux des disques.***

***4-2. Partitionner des disques (MBR, GPT).***

***4-3. Gérer le LVM.***

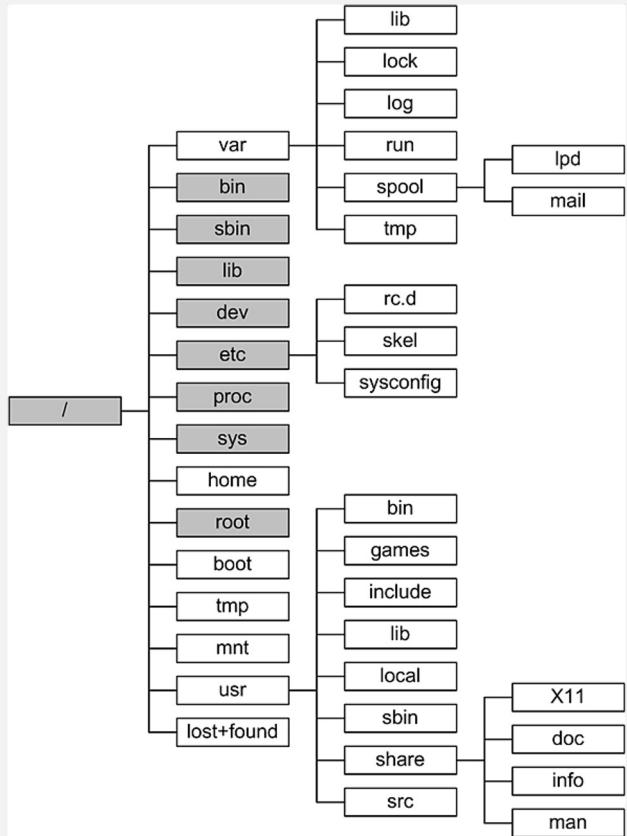
## 4-I LA VISION LINUX DES DISQUES

- La vision Linux de la gestion des disques ( unités de stockage) se base sur le principe **du système de fichier**.
- **Le système de fichier** est un type de formatage qui va s'appliquer sur une partition (une partie hermétique d'un disque).
- Le système de fichier de Linux est tout entier organisé à l'intérieur d'une seule **arborescence** (avec répertoire et sous-répertoire).
- On peut donc voir le système fichier comme **un index géant** qui viendrait organiser et faciliter la recherche de données.



## 4-I LA VISION LINUX DES DISQUES

Représentation système de fichiers



- **/ (La racine, root)**
- **/bin (Les commandes)**
- **/boot (l'amorçage LILO)**
- **/dev (Les périphériques, "devices")**
- **/etc (La configuration)**
- **/home (Les répertoires de base des utilisateurs)**
- **/lib (Les bibliothèques de routines, le module du kernel, "library")**
- **/var (Les journaux systèmes)**
- **/mnt (Les volumes montés)**
- **/root (le répertoire du super utilisateur)**
- **/sbin (Les fichiers systèmes binaires)**
- **/tmp (Le répertoire temporaire)**
- **/usr (les applications)**
- **/usr/doc (La documentation)**
- **/usr/man (le manuel de l'utilisateur)**

## 4-I LA VISION LINUX DES DISQUES

**Il existe plusieurs types de système de fichier :**

### SOUS MICROSOFT

- **MSDOS** ou **FAT** pour la FAT 16 de DOS et de Windows 95.
- **VFAT** pour la FAT 32 de Windows 95/98
- **NTFS** pour Windows NT
- **JOLIET** pour le CDROM à nom long de Microsoft.



### SOUS UNIX

- **MINIX** pour Unix
- **SYS V** pour Unix Système V
- **UFS** pour Unix BSD
- **UMSDOS** pour Unix sur une partition MSDOS
- **EXT** pour l'ancien Linux native.
- **EXT2FS** ou **EFS** pour Linux native.
- **EXT3FS** pour Linux native 3° génération avec la journalisation des fichiers.
- **REISERFS**

## 4- I LA VISION LINUX DES DISQUES

Il existe plusieurs types de système de fichier :

Ext2	Ext3	Ext4	Reiserfs	Fat32	BtrFs
<ul style="list-style-type: none"><li>• Système de fichiers natif de Linux.</li><li>• Désuet, car non journalisé.</li><li>• Taille max fichier : 2TiB.</li><li>• Taille max partition : 4 TiB.</li><li>• Journalisation : non</li><li>• Gestion des droits d'accès : oui</li></ul>	<ul style="list-style-type: none"><li>• Comme Ext2 mais journalisation.</li><li>• Possibilité de passer d'une partition Ext2 vers Ext3.</li><li>• Taille max fichier : 2TiB.</li><li>• Taille max partition : 4 TiB.</li><li>• Journalisation : oui</li><li>• Gestion des droits d'accès : oui</li></ul>	<ul style="list-style-type: none"><li>• Successeur Ext3.</li><li>• Taille max fichier : 16TiB.</li><li>• Taille max partition : 1EiB.</li><li>• Journalisation : oui</li><li>• Gestion des droits d'accès : oui</li></ul>	<ul style="list-style-type: none"><li>• Adapté aux fichiers temporaires.</li><li>• Gère bien les fichiers temporaires.</li><li>• Non recommandé pour les pc portables.</li><li>• Très consommateurs en énergies.</li><li>• Taille max fichier : 8TiB.</li><li>• Taille max partition : 16TiB.</li><li>• Journalisation : oui</li><li>• Gestion des droits d'accès : oui</li></ul>	<ul style="list-style-type: none"><li>• Evolution du Fat.</li><li>• Très utilisé pour les clés usb.</li></ul>	<ul style="list-style-type: none"><li>• Développé par Oracle et RedHat.</li><li>• Successeur d'Ext4.</li><li>• Taille max fichier : 16EiB.</li><li>• Taille max partition : 16EiB.</li><li>• Pas mal utilisé.</li></ul>

## 4-I LA VISION LINUX DES DISQUES

### **Les caractéristiques d'un système de fichier :**

#### I. LE NOM DES FICHIERS

- Longueur maximale 255 caractères.
- L'extension comprise dans la longueur du fichier.
- Le type du fichier est déterminé par son contenu. (type MIME).
- L'extension va surtout servir à la clarification pour l'utilisateur.

#### 2. LA JOURNALISATION

- Un système de journal est mis en place pour éviter les problèmes de corruption de fichier.
- Le système viendra récupérer la version enregistrer dans le journal pour restaurer une version corrompue du fichier.
- La journalisation est un système qui nécessite une certaine capacité de stockage.
- Il n'est pas adapté à pour des périphériques de faibles capacités comme carte mémoire par exemple.



## 4- I LA VISION LINUX DES DISQUES



### Les caractéristiques d'un système de fichier :

#### 3. LA TABLE INODE (TABLE DE NŒUD)

- « Une table Inode (**Index node**) est une structure de données contenant des informations à propos d'un fichier ou répertoire stocké dans certains systèmes de fichiers (notamment de type Linux/Unix) ».
- Chaque fichier ou dossier est répertorié avec un numéro « inode » **unique** même si le fichier peut avoir plusieurs noms.
- Les tables d'inode vont contenir les métadonnées des fichiers (ci-après).

#### 4. LES ACCÈS AUX DONNÉES

- Différents droits d'accès : ***L'écriture, la lecture et l'exécution.***
- Les droits sur les fichiers ou les dossiers peuvent évoluer en fonction de l'utilisateur ou des droits du groupe auquel l'utilisateur appartient.
- Chaque fichier ou répertoire disposent des informations concernant ces droits d'accès ( r w x).

## 4-I LA VISION LINUX DES DISQUES

### Les caractéristiques d'un système de fichier :

#### 5. LES MÉTADONNÉES (INODE)

- Les droits ;
- Les dernières dates d'accès et de modification ;
- Le propriétaire et le groupe ;
- La taille ;
- Le nombre de blocs utilisés ;
- Le type de fichiers ;
- Le compteur de liens ;
- Un arbre d'adresses de blocs de données.



```
# Affiche le détail des fichiers et dossiers présentent dans le dossier home de l'utilisateur alain
# Première colonne indique le numéro d'inode.
alain@mohamed-VirtualBox:~$ ls -ail
total 148
681746 drwxr-xr-x 18 alain alain 4096 août 30 17:59 .
654081 drwxr-xr-x 4 root root 4096 août 29 15:23 ..
660514 -rw----- 1 alain alain 1891 août 27 11:17 .bash_history
684820 -rw-r--r-- 1 alain alain 220 août 24 15:54 .bash_logout
684822 -rw-r--r-- 1 alain alain 3771 août 24 15:54 .bashrc
684835 drwxr-xr-x 4 alain alain 4096 août 27 16:19 Bureau
684853 drwxr-xr-x 9 alain alain 4096 août 26 16:18 .cache
684899 drwxrwxr-x 4 alain alain 4096 août 24 16:04 .cinnamon
681793 drwxr-xr-x 18 alain alain 4096 août 27 16:15 .config
660522 -rw-r--r-- 1 alain alain 27 août 24 16:03 .dmrc
684839 drwxr-xr-x 2 alain alain 4096 août 24 16:03 Documents
681637 drwx----- 3 alain alain 4096 août 24 16:03 .gnupg
684821 -rw-r--r-- 1 alain alain 22 août 24 15:54 .gtkrc-2.0
684818 -rw-r--r-- 1 alain alain 516 août 24 15:54 .gtkrc-xfce
684841 drwxr-xr-x 2 alain alain 4096 août 24 16:03 Images
803855 drwxrwxrwx 3 alain alain 4096 août 24 17:12 .linuxmint
681640 drwxrwxr-x 3 alain alain 4096 août 24 16:03 .local
684837 drwxr-xr-x 2 alain alain 4096 août 24 16:03 Modèles
685558 drwx----- 5 alain alain 4096 août 25 10:09 .mozilla
684840 drwxr-xr-x 2 alain alain 4096 août 24 16:03 Musique
685608 -rw----- 1 alain alain 224 août 27 09:55 nohup.out
684819 -rw-r--r-- 1 alain alain 807 août 24 15:54 .profile
```

## 4-2 PARTITIONNER DES DISQUES

- **Le partitionnement** est une étape clef de l'installation de GNU/Linux et de la prise en compte des supports de stockage de données.
- Le disque physique, réel, est fractionné en plusieurs disques virtuels, logiques, les partitions.
- Chaque partition est vue comme un disque indépendant et contient son propre système de fichiers.
- Le but d'une partition est de rassembler les données informatiques qui ont un lien commun.
- Il existe plusieurs sortes de partitions : primaire, secondaire et logique.



## 4-2 PARTITIONNER DES DISQUES

- Chaque disque contient une table de répartition.
- Cette table qui contient toutes les informations concernant le **découpage du disque en partitions**.
- Il existe **deux tables de partitionnement** : celle du **MBR** (Master Boot Record) et le **GPT** (GUID Partition Table).

### Type MBR

- Mode de partitionnement historique.
- Jusqu'à 2010.
- Une zone réservée de 512 octets appelée MBR.
- Le MBR contient les informations relative à 4 partitions maximum.
- Le disque dur qui va être géré ne peut excéder 2,2 To.



### Type GPT

- Mode de partitionnement depuis 2010
- Depuis 2006 pour les Mac.
- Une zone Protective MBR.
- Un table partition en 2 exemplaires.
- Cette zone contient les informations relative à 128 partitions.
- Le disque dur qui va être géré peut excéder 2,2 To.

## 4-2 PARTITIONNER DES DISQUES

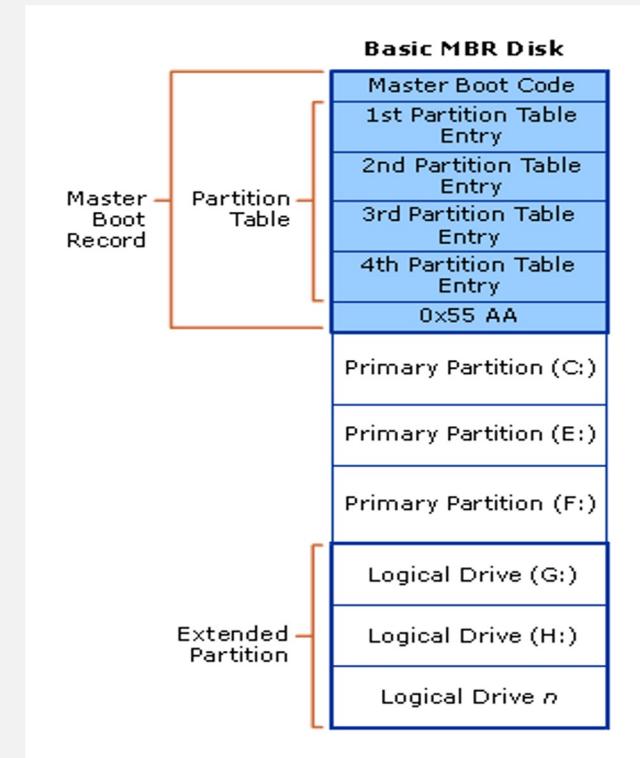


### Partitionnement de type MBR:

#### Structure du disque :

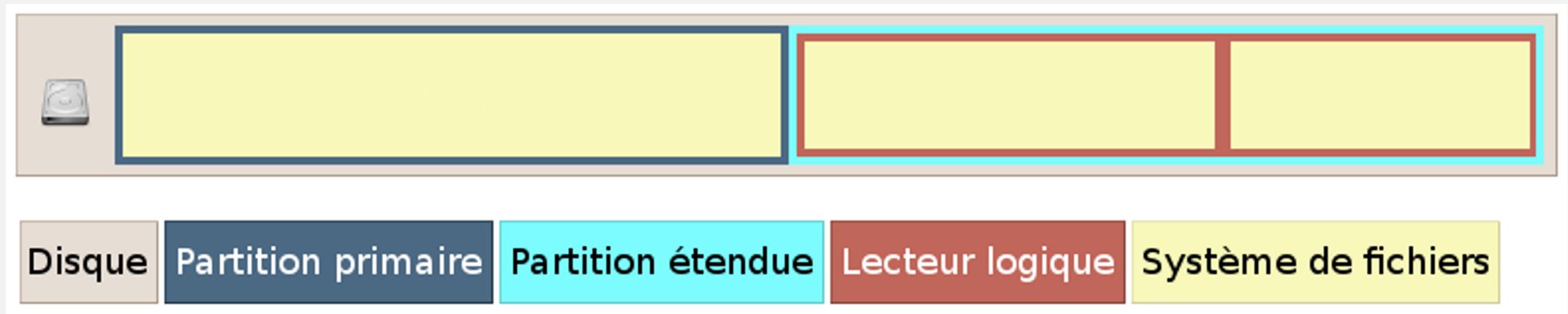
- **1 MBR.**
- **4 partitions primaires** maximum.
- **1 partition étendue :** dernière partition primaire découpée en N partitions secondaires.
- **N partitions secondaires :** sous-partitions contenus dans une partition étendue. On les appelle aussi **partitions logiques (Limitées à la taille maximale de 2.2 To).**
- **EBR :** il s'agit d'un découpage qui décrit la partition secondaire qu'il précède.

- **Les étapes de démarrage:**
- **Après le POST (Power-On Self Test ).**
- **Le BIOS** lit le contenu du **MBR**.
- **Le BIOS** exécute le code d'amorçage du **MBR**.
- 
- Le code d'amorçage va lancer le chargeur d'amorçage du système d'exploitation dans la partition dédiée.
- Le chargeur d'amorçage sous Linux s'appelle de **GRUB (Grand Unified Bootloader)**



## 4-2 PARTITIONNER DES DISQUES

**Partitionnement de type MBR (schéma):**

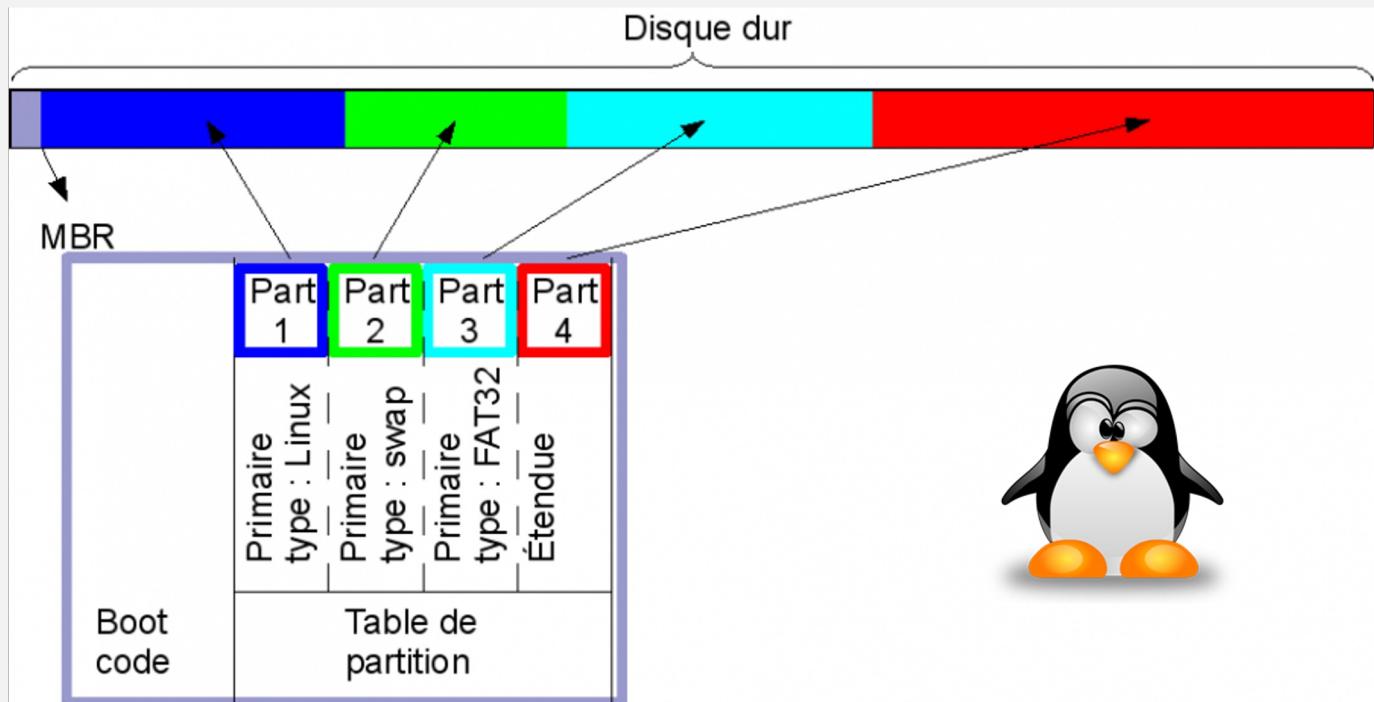


## 4-2 PARTITIONNER DES DISQUES

### Le MBR

- Un **code d'amorçage (Master Boot Code)**.
- La **table des partitions** : les 4 partitions primaires.
- Une **signature** (0x55 AA).

### Détails du MBR:



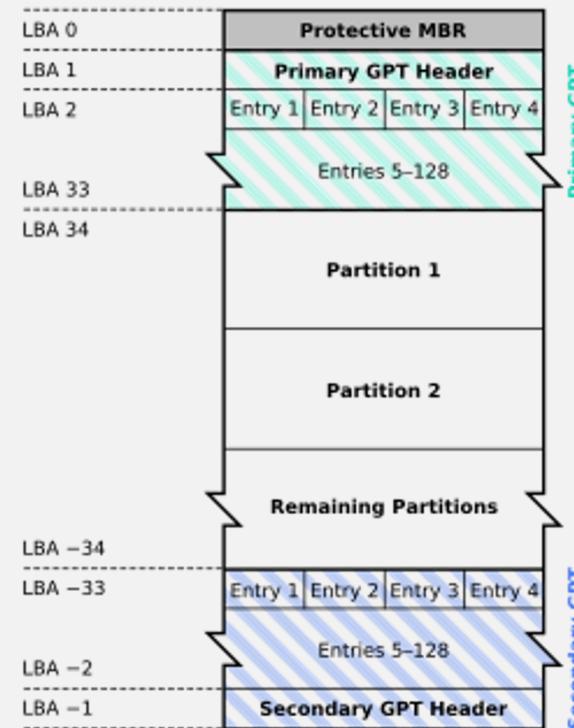
## 4-2 PARTITIONNER DES DISQUES

### Partitionnement de type GPT:

#### Structure du disque :

- **MBR protecteur** (début du disque dur), garantit la comptabilité avec des logiciels gérant le MBR.
- **GPT primaire** : entête, contient les infos blocs utilisables, GUID, nombre et taille des partitions...
- **GPT primaire** : tableau de partitions
- **Partitions** : début de la partition 1
- ...
- **Partitions** : fin de la partition n
- **GPT secondaire** : tableau de partitions
- **GPT secondaire** : entête, copie identique du GPT primaire (fin du disque dur)

#### GUID Partition Table Scheme



## 4-2 PARTITIONNER DES DISQUES

### Désignation des répartitions sous Linux (Ubuntu) avec partition MBR :

- **Règle de dénomination :**

- Un disque est désigné avec l'appellation « **sdx** » (mass-storage-driver) :
  1. "a" pour le maître de la nappe IDE primaire ou l'ID0 du connecteur primaire SATA
  2. "b" pour l'esclave de la nappe IDE primaire ou l'ID1 du connecteur primaire SATA
  3. "c" pour le maître de la nappe IDE secondaire ou l'ID0 du connecteur secondaire SATA
  4. "d" pour l'esclave de la nappe IDE secondaire ou l'ID1 du connecteur secondaire STA
- **/dev/**, il désigne un répertoire sous GNU/Linux qui est utilisé afin de communiquer avec ces partitions.
- Ainsi, **/dev/sda1** est un fichier qui permet d'interagir avec le contenu de la partition **sda1**.
- **Exemple 1** : *sda1* est la première partition du disque *sda*; *sda2* est la seconde partition du disque *sda*; *sdb1* est la première partition du disque *sdb*;
- **Exemple 2** : *sda5* représente le premier lecteur logique de la partition étendue du disque dur *sda*, et ce, même si ce disque est divisé en une partition primaire et une partition étendue qui contient un lecteur logique.



## 4-2 PARTITIONNER DES DISQUES

**Désignation des répartitions sous Linux (Ubuntu) avec partition MBR :**

- **Ordre de répartitions :**

- L'ordre des partitions est attribué en fonction de l'ordre de création.
- L'emplacement d'une partie partition dans un disque ne garantit pas son bon ordre.
- La première partition ( primaire) placée en fin de disque restera toujours une partition primaire.
- Dans un souci de clarté, il est recommandé de respecter l'ordre de création dans le positionnement des partitions.



## 4-2 PARTITIONNER DES DISQUES

### **Désignation des répartitions sous Linux (Ubuntu) :**

- **Affectation et format des partitions :**

- Sous Linux, chaque partition peut être affecté à n'importe quel usage.
- Comme la partition Système, la partition des données personnelles, etc.
- Le format ou le système de fichier de chaque partition est renseigné dans la table de répartition ( ou table EBR pour les partitions logiques).
- Dans un souci de performance, il est recommandé de placer les partitions par ordre d'importance (Système, etc.).



## 4-2 PARTITIONNER DES DISQUES

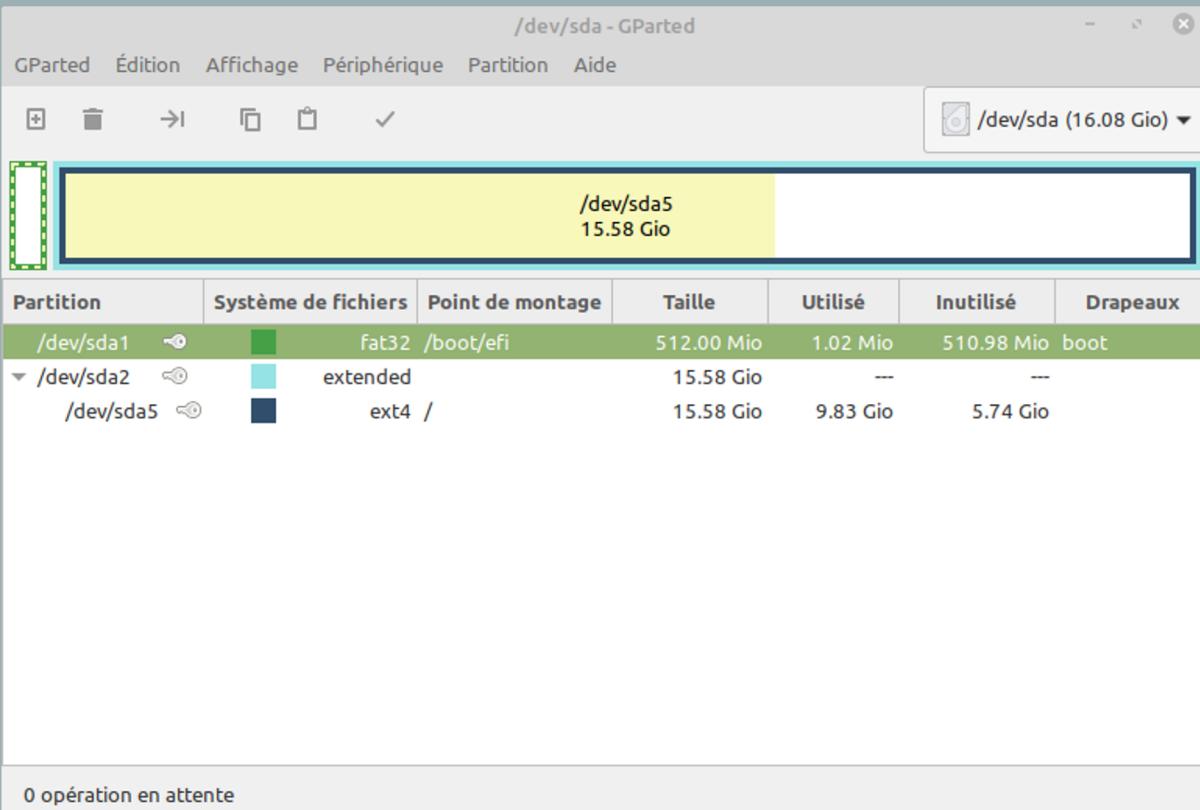
### Manipulation des partitions:

- **Il existe plusieurs outils pour manipuler les partitions :**
  - **fdisk** est le plus ancien et le plus utilisé des outils de partitionnement. Il est à base de menus et raccourcis textuels.
  - **cfdisk** est un peu plus « visuel » et s'utilise avec les flèches directionnelles. Il permet les mêmes opérations que fdisk mais de manière plus conviviale.
  - **sfdisk** fonctionne en interactif ou non, est assez compliqué mais plus précis.
  - **parted** permet des opérations très avancées sur les partitions comme par exemple leur redimensionnement. Il est soit interactif (c'est un interpréteur de commandes) soit scriptable. Il existe des interfaces graphiques comme **qtparted** ou **gparted**.



## 4-2 PARTITIONNER DES DISQUES

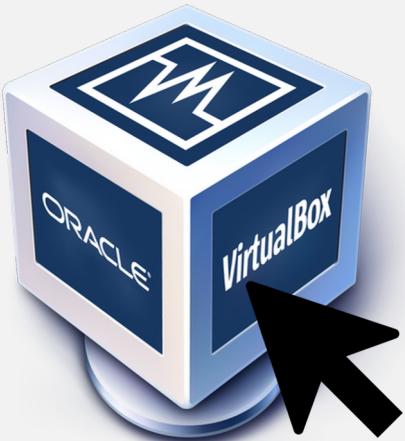
### OUTILS GESTION PARTITION (**gparted**)



- Interface graphique de gestion des partitions très visuelle.
- Il n'est pas présent par défaut dans la plupart des distributions.
- Il faut donc l'installer : « **sudo apt-get install gparted** »
- Une fois installer lancer : « **gparted** ».

## 4-2 PARTITIONNER DES DISQUES

Un peu de pratique



## 4-2 PARTITIONNER DES DISQUES



```
alain@mohamed-VirtualBox:~$ sudo fdisk /dev/sda
Bienvenue dans fdisk (util-linux 2.34).
Les modifications resteront en mémoire jusqu'à écriture.
Soyez prudent avant d'utiliser la commande d'écriture.

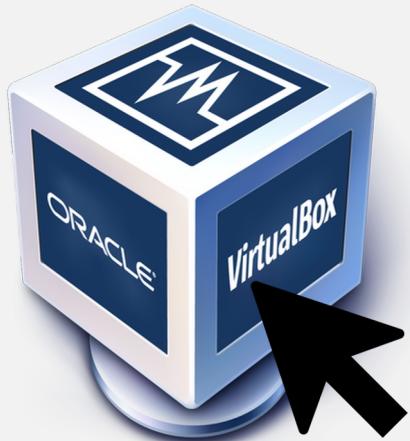
Commande (m pour l'aide) : m
Aide :
  DOS (secteur d'amorçage)
    a  modifier un indicateur d'amorçage
    b  éditer l'étiquette BSD imbriquée du disque
    c  modifier l'indicateur de compatibilité DOS
  Générique
    d  supprimer la partition
    F  afficher l'espace libre non partitionné
    l  afficher les types de partitions connues
    n  ajouter une nouvelle partition
    p  afficher la table de partitions
    t  modifier le type d'une partition
    v  vérifier la table de partitions
    i  Afficher des renseignements sur la partition
  Autre
    m  afficher ce menu
    u  modifier les unités d'affichage et de saisie
    x  fonctions avancées (réservées aux spécialistes)
  Script
    I  chargement de l'agencement à partir du fichier de script sfdisk
    O  sauvegarde de l'agencement vers le fichier de script sfdisk
  Sauvegarder et quitter
    w  écrire la table sur le disque et quitter
    q  quitter sans enregistrer les modifications
  Créez une nouvelle étiquette
    g  créer une nouvelle table vide de partitions GPT
    G  créer une nouvelle table vide de partitions SGI (IRIX)
    o  créer une nouvelle table vide de partitions DOS
    s  créer une nouvelle table vide de partitions Sun
```

### OUTILS GESTION PARTITION (**fdisk**)

- Généralement utilisé par les administrateurs et les ingénieurs système.
- Présent par défaut dans les distributions Linux.
- Quelques commandes :
  - . « **sudo fdisk /dev/sda** » : lance l'accès aux partitions du disque et au menu principal avec la commande « **m** ».
  - « **p** » : Affiche la table de partition.
  - « **n** » : Crée une nouvelle partition.
  - « **d** » : Supprime une partition.
  - « **i** » : Affiche les informations sur une partition.
  - « **L** » : Affiche la liste de tous les types de partition que la machine connaît.

## 4-2 PARTITIONNER DES DISQUES

Un peu de pratique



## 4-3 GESTION DU LVM

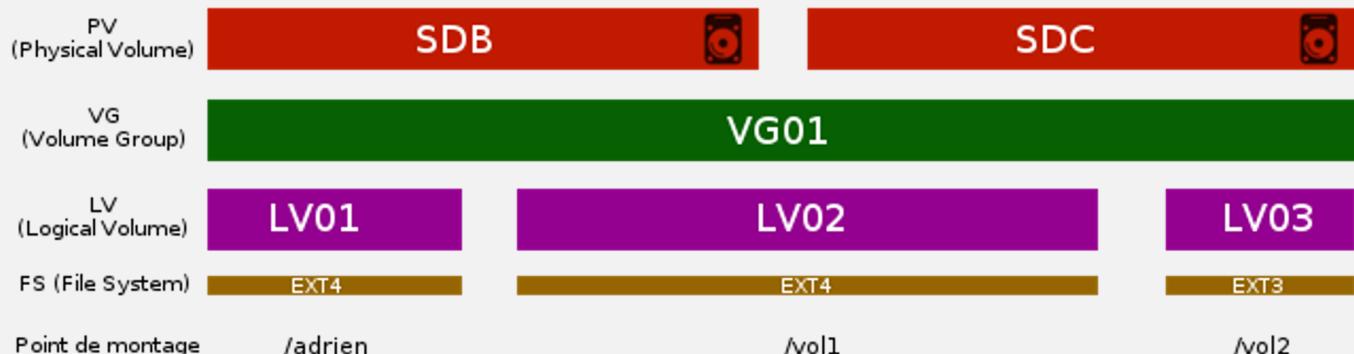
- **LVM** (Logical Volume Manager) permet la création et la gestion de volumes logiques sous Linux.
- L'utilisation de volumes logiques remplace en quelque sorte le partitionnement des disques.
- **L'objectif dépasser la vision physique de découpage de données par disque et partitions pour aller vers une gestion globale et logique des supports de données.**
- Le concept est basé sur 3 niveaux d'abstractions :
  1. **Le volume physique** : Il s'agit de découpage basés sur les supports physiques (partitions, disques durs, etc.).
  2. **Les groupes de volume** : il sont équivalents à des pseudo-disques-durs. On concatène ces volumes physiques (1 ou plusieurs) dans des « groupes de volumes » (volume groups ou VG).
  3. **Le volume logique** : On découpe ces VG en volumes logiques, puis formatés et montés dans des systèmes de fichiers. Les LV sont équivalents à des pseudo-partitions.



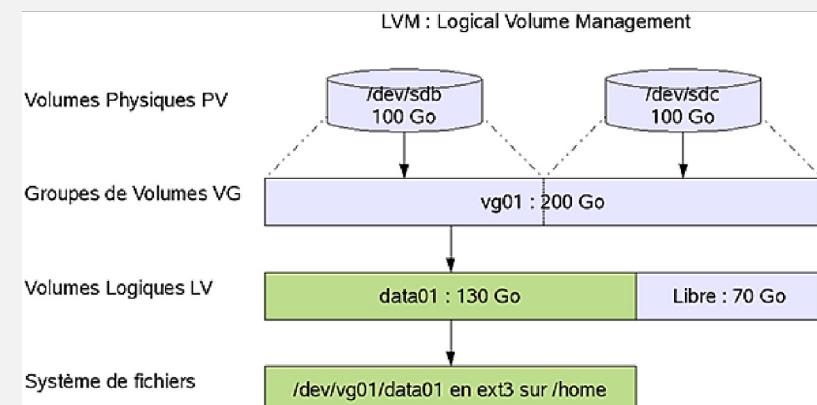
## 4-3 GESTION DU LVM

### Représentation du LVM

**Schéma 1**



**Schéma 2**



**Pour information, toutes les commandes qui concernent :**

- Les volumes physiques commencent par `pv*`
- Les groupes de volumes commencent par `vg*`
- Les volumes logiques commencent par `lv*`



## 4-2 GESTION DU LVM

### COMMANDE D'UN PV ( PHYSICAL VOLUME)

```
root@mohamed-VirtualBox:/home/alain# pvcreate /dev/sdc
Physical volume "/dev/sdc" successfully created.

root@mohamed-VirtualBox:/home/alain# pvdisplay

"/dev/sdc" is a new physical volume of "<2,00 GiB"
--- NEW Physical volume ---
PV Name           /dev/sdc
VG Name
PV Size          <2,00 GiB
Allocatable       NO
PE Size           0
Total PE          0
Free PE           0
Allocated PE      0
PV UUID          Cf73ar-cS8V-V3DD-yhSt-rwHf-QUi2-3HYQEe

"/dev/sdd" is a new physical volume of "2,07 GiB"
--- NEW Physical volume ---
PV Name           /dev/sdd
VG Name
PV Size          2,07 GiB
Allocatable       NO
PE Size           0
Total PE          0
Free PE           0
Allocated PE      0
PV UUID          PDinXr-aLW2-xarS-RbDV-nhS0-Quc5-nWI1tu
```

- Nous allons utiliser 2 disques que l'on va appeler **sdc** et **sdd**.
- « ***pvcreate /dev/sdc*** » : permet de créer un volume physique.
- « ***pvremove /dev/sdc*** » : permet de supprimer un volume physique.
- « ***pvdisplay /dev/sdc*** » : affiche le détail d'un volume physique.

## 4-2 GESTION DU LVM

### COMMANDÉ D'UN VG ( VOLUME GROUP )

```
root@mohamed-VirtualBox:/home/alain# vgcreate datavg /dev/sdc /dev/sdd
Volume group "datavg" successfully created

root@mohamed-VirtualBox:/home/alain# vgdisplay
--- Volume group ---
VG Name           datavg
System ID
Format           lvm2
Metadata Areas   2
Metadata Sequence No 1
VG Access        read/write
VG Status         resizable
MAX LV
Cur LV
Open LV
Max PV
Cur PV
Act PV
VG Size          <4,07 GiB
PE Size           4,00 MiB
Total PE          1041
Alloc PE / Size  0 / 0
Free PE / Size   1041 / <4,07 GiB
VG UUID          iR3tVM-xLT1-cfeN-KNW0-l3M0-QlyT-CLB168
```

- « ***vgcreate <nom du vg groupe> <chemin vp1> <chemin vp2> ...*** » : permet de créer un groupe de volume avec un ou plusieurs de volumes physiques.
- « ***vgremove <nom du vg groupe>*** » : permet de supprimer un groupe volume par son nom.
- « ***vgdisplay <nom du vg groupe>*** » : affiche le détail d'un groupe volume.
- « ***vgextend <nom du groupe> <chemin vp>*** » : permet de rajouter un physical volume au groupe volume.

## 4-2 GESTION DU LVM

### COMMANDE D'UN LV ( LOGICAL VOLUME )

```
root@mohamed-VirtualBox:/home/alain# lvcreate -n datav1 -l 500M0 datavg
Logical volume "datav1" created.

root@mohamed-VirtualBox:/home/alain# lvcreate -n datav2 -l 800M0 datavg
Logical volume "datav2" created.

root@mohamed-VirtualBox:/home/alain# lvdisplay
  --- Logical volume ---
  LV Path          /dev/datavg/datalv1
  LV Name          datalv1
  VG Name          datavg
  LV UUID          TXvZDV-IrDM-udr4-Xmte-AFJl-scKJ-3ebp8v
  LV Write Access  read/write
  LV Creation host, time mohamed-VirtualBox, 2021-09-01 18:01:24 +0200
  LV Status        available
  # open           1
  LV Size          500,00 MiB
  Current LE       125
  Segments         1
  Allocation       inherit
  Read ahead sectors auto
  - currently set to 256
  Block device    253:0

  --- Logical volume ---
  LV Path          /dev/datavg/datalv2
  LV Name          datalv2
  VG Name          datavg
  LV UUID          w7ufRG-XLV4-AuN5-7X0z-iirl-mnya-rygYAv
  LV Write Access  read/write
  LV Creation host, time mohamed-VirtualBox, 2021-09-01 18:01:41 +0200
  LV Status        available
  # open           1
  LV Size          800,00 MiB
  Current LE       200
  Segments         1
  Allocation       inherit
  Read ahead sectors auto
  - currently set to 256
  Block device    253:1

root@mohamed-VirtualBox:/home/alain#
```

- « ***lvcreate -n <nom du lv> -L <taille du lv> <nom du vg>*** » : permet de créer un LV avec une taille défini et le groupe volume .
- « ***lvremove <nom du vg /nom du lv>*** » : permet de supprimer un groupe volume par son nom.
- « ***lvdisplay <nom du vg /nom du lv>*** » : affiche le détail d'un volume logique.

## 4-2 GESTION DU LVM

### AGRANDIR UN LV

```
# Affiche l'ensemble les informations concernant les groupes de volume :  
root@mohamed-VirtualBox:/home/alain# vgdisplay  
--- Volume group ---  
VG Name          datavg  
System ID        lvm2  
Format           2  
Metadata Areas   5  
Metadata Sequence No  5  
VG Access        read/write  
VG Status        resizable  
MAX LV           0  
Cur LV           2  
Open LV          2  
Max PV           0  
Cur PV           2  
Act PV           2  
VG Size          <4,07 GiB  
PE Size          4,00 MiB  
Total PE         1041  
Alloc PE / Size  325 / <1,27 GiB  
Free  PE / Size  716 / <2,80 GiB  
VG UUID          iR3tVM-xLT1-cfeN-KNW0-l3M0-QlyT-CLB168  
  
# Accroit la dimension du volume logique "datalv1" de 250 PE.  
root@mohamed-VirtualBox:/home/alain# lvresize -l +250 /dev/datavg/datalv1  
  Size of logical volume datavg/datalv1 changed from 500,00 MiB (125 extents) to 1,46 GiB (375  
extents).  
 Logical volume datavg/datalv1 successfully resized.  
  
# Adapte la taille du File System du volume logique (lv) "datalv1" après l'augmentation du lv.  
root@mohamed-VirtualBox:/home/alain# resize2fs /dev/datavg/datalv1  
resize2fs 1.45.5 (07-Jan-2020)  
Le système de fichiers de /dev/datavg/datalv1 est monté sur /media/alain/697b35b4-ab8a-4b59-870f-  
f66a9d388207 ; le changement de taille doit être effectué en ligne  
old_desc_blocks = 1, new_desc_blocks = 1  
Le système de fichiers sur /dev/datavg/datalv1 a maintenant une taille de 384000 blocs (4k).
```

- I. Vérifier la place disponible dans le VG avec la commande « **vgdisplay** ».
- I. Augmenter la taille du LV sélectionné avec la commande suivante : « **lvextend -l <taille en PE> <chemin vers le LV>** » . (« **lvresize** » fonctionne aussi).
- I. Il faut ensuite agrandir le système de fichier (File System = FS), pour l'adapter à la nouvelle taille du LV, avec la commande : « **resize2fs <chemin vers le LV>** ».

## 4-3 GESTION DU LVM

Un peu de pratique



## **5 - GÉRER L'ARRÊT ET LE REDÉMARRAGE.**



Les grandes étapes du démarrage – la gestion des services

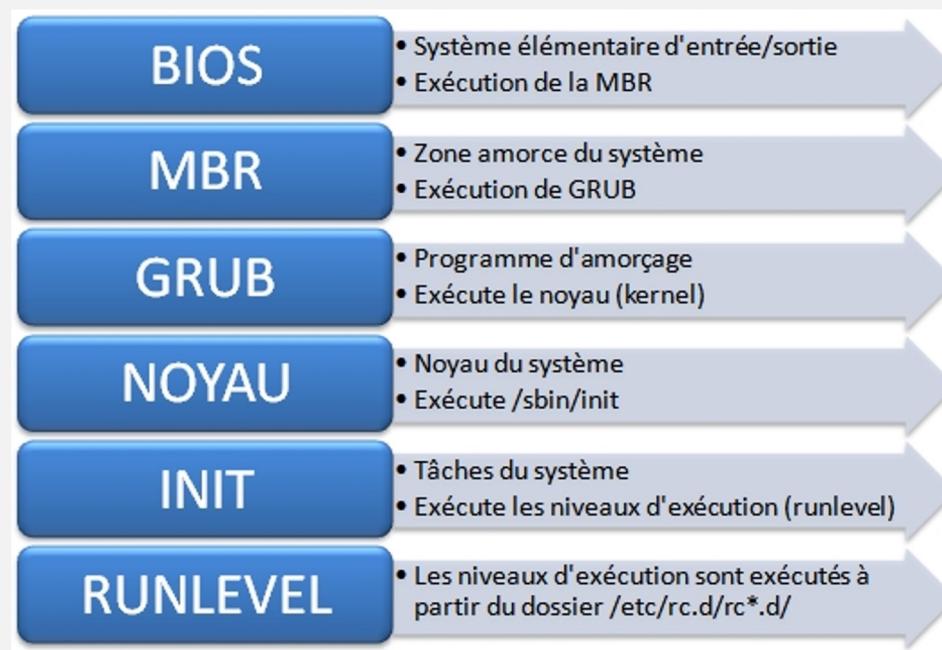
## 5 - GÉRER L'ARRÊT ET LE REDÉMARRAGE.

*5-1. Les grandes étapes du démarrage.*

*5-2. Le démarrage des services.*

## 5-I LES GRANDES ÉTAPES DU DÉMARRAGE

- Lors de l'allumage de votre ordinateur sous Linux , il y a un certain nombres d'opération qui vont s'effectuer pour rendre votre système d'exploitation opérationnel.
  - Il y a 5 grandes étapes dans le processus de démarrage :



## 5-I LES GRANDES ÉTAPES DU DÉMARRAGE

### I - Le BIOS

- Le **BIOS (Basic Input Output System)** est l'interface logicielle entre le matériel et le logiciel à un niveau très basique.
- **Le BIOS** fournit l'ensemble des instructions de base utilisées par le système d'exploitation.
- Le **BIOS** est présent sur une mémoire morte **ROM** (*ReadOnly Memory*) de l'ordinateur.
- Le **BIOS** effectue un autotest de l'allumage (POST : power on self-test ) puis recherche les périphériques, notamment ceux utilisés pour démarrer.
- Le **BIOS** lit et exécute le premier secteur (512 octets) physique du média de démarrage qui sont contenus dans le **MBR** (*Master Boot Record*, vu précédemment).



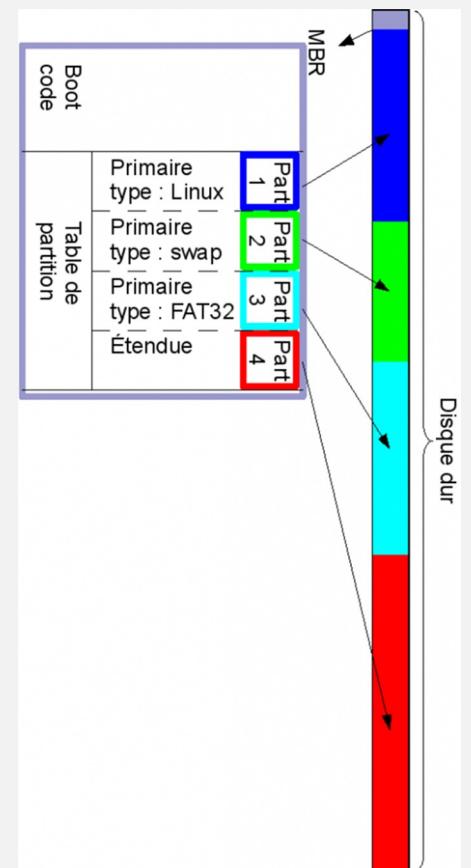
## 5-I LES GRANDES ÉTAPES DU DÉMARRAGE

### 2 - Le MBR

- Le **MBR (Master Boot Record)** est le premier secteur adressable d'un disque dur.
- Le **MBR** est présent dans la première partie du disque dur qui s'appelle **hda** ou **sda**.
- **Le MBR** est de 512 octets et il contient les éléments suivants :
  - Le programme d'amorçage se trouve dans les 446 premiers bits.
  - La table des partitions (les 4 partitions primaires) du disque dur sur les 64 bits suivants.
  - Vérification de la validité du MBR dans les 2 derniers bits.



- **Le MBR** va lancer une routine d'amorçage (**GRUB**) qui lui va se charger de lancer le système d'exploitation en passant par le noyau.

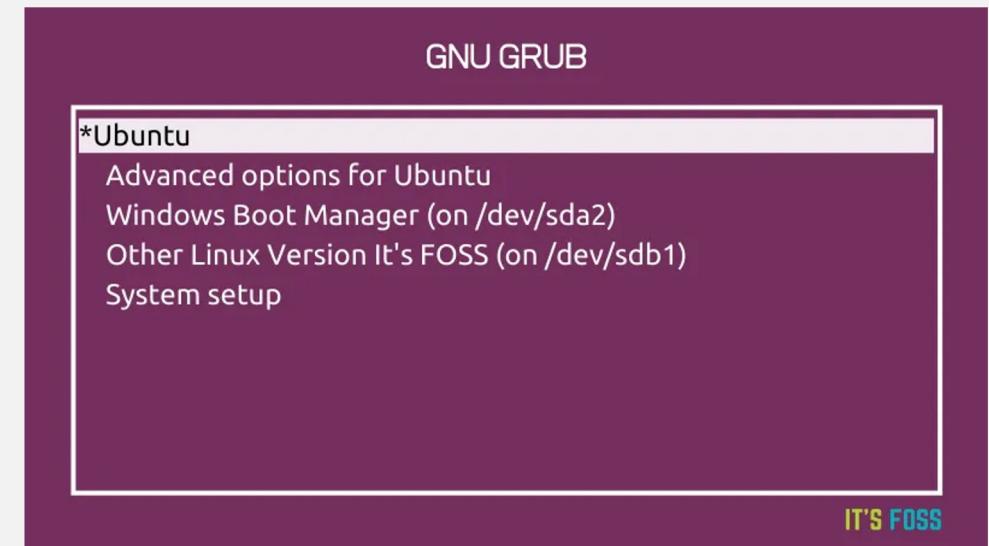


## 5-I LES GRANDES ÉTAPES DU DÉMARRAGE



### 3 – Le GRUB

- **Le GRUB (Grand Unified Bootloader) est un programme d'amorçage.**
- Si votre machine dispose de plusieurs système d'exploitation, **Le GRUB** vous demandera d'en sélectionner un.
- **Le GRUB** apparaît sous forme d'une interface pour l'utilisateur pour effectuer votre choix.
- **Le GRUB** va s'occuper de charger et d'exécuter le noyau (Kernel) du SE sélectionné.

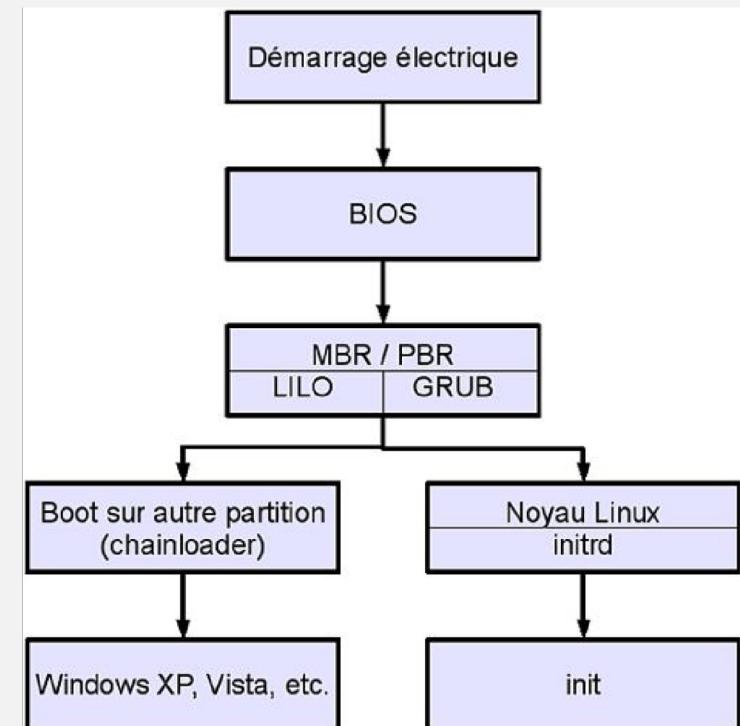


## 5- I LES GRANDES ÉTAPES DU DÉMARRAGE



### 4- Le kernel (noyau)

- Le **kernel (noyau en français)** va monter le système de fichier en partant de la racine (/) avec les différentes partitions de nos périphériques ou partitions.
- **Le kernel** charge et exécute le programme **/sbin/init**.
- Initrd est utilisé afin d'avoir une version minimal temporaire du système de fichier au démarrage.
- A cette étape, la première console est créée.
- Comme le programme **init** est le premier programme à être exécuté par le noyau Linux, il porte le PID (ID du processus) numéro 1.



## 5-I LES GRANDES ÉTAPES DU DÉMARRAGE

### 5 - Init

- Le programme **init** est le premier lancer et le dernier arrêté de notre système.
- **Init** est un peu le père de tous les processus (l).
- Le rôle d'**init** est de démarrer et d'arrêter tous les services.
- **Init** va exécuter les diverses tâches initiales nécessaires au bon fonctionnement de Linux.
- La configuration d'**init** est présente sous forme de fichier **/etc/inittab**.
- **Init** se charge aussi de contrôler le niveau d'exécution d'un système Linux (**Runlevel**).





## 5-I LES GRANDES ÉTAPES DU DÉMARRAGE

### 6 - Runlevel

- Un **niveau d'exécution (RunLevel)** est un état dans lequel se trouve Unix/Linux.
- Chaque **niveau d'exécution** dispose d'un répertoire avec l'ensemble des programmes et configurations qui correspondent à son niveau.
- Dans ces répertoires, on retrouve des noms de programme qui commencent par la lettre S et K.
- Ceux qui commencent par la lettre S sont exécutés au démarrage du système (la lettre S pour « startup » = démarrage).
- Ceux qui commencent par la lettre K sont exécutés à l'arrêt du système (la lettre K pour « kill » = arrêt).
- De plus, dans le nom de ces programmes, il y a un chiffre après la lettre S ou K. Ce chiffre indique l'ordre d'exécution de chaque programme lors du démarrage.
- On peut changer de **niveau d'exécution** après le démarrage.
  - **«runlevel »** : donne le niveau d'exécution actuel.
  - **«telinit <numero niveau execution> »** : change le niveau d'exécution

```
# /etc/init.d/rc takes care of runlevel handling
#
# runlevel 0 is System halt  (Do not use this for initdefault!)
# runlevel 1 is Single user mode
# runlevel 2 is Local multiuser without remote network (e.g. NFS)
# runlevel 3 is Full multiuser with network
# runlevel 4 is Not used
# runlevel 5 is Full multiuser with network and xdm
# runlevel 6 is System reboot (Do not use this for initdefault!)
#
l0:0:wait:/etc/init.d/rc 0
l1:1:wait:/etc/init.d/rc 1
l2:2:wait:/etc/init.d/rc 2
l3:3:wait:/etc/init.d/rc 3
#l4:4:wait:/etc/init.d/rc 4
l5:5:wait:/etc/init.d/rc 5
l6:6:wait:/etc/init.d/rc 6
```



## 5-3 LE DÉMARRAGE DES SERVICES

- Chaque niveau d'exécution dispose d'un certain nombre de services qui vont être chargé aux démarrage du système.
- Le script **/etc/init.d/rc** initialise le niveau d'exécution et est responsable de l'arrêt ou du démarrage des services en fonction du niveau d'exécution notamment si celui-ci change.
- Chaque niveau d'exécution **n** dispose aussi d'un répertoire **rcn.d (localisation : /etc/rcn.d)** qui contient des liens symboliques (raccourcis) vers les services présents dans **/etc/init.d** à lancer ou arrêter.
- Le préfixe du nom de chaque lien définit son ordre de lancement ou son ordre d'arrêt. Le nom est sous la forme suivante : [SK]nnservice
  - **S** : start.
  - **K** : kill (stop).
  - **nn** : ordre numérique de démarrage ou d'arrêt. (00=premier, 99=dernier).
  - **service** : nom du service.

Exemple : **Le lien S10network indique que le service network, responsable de la mise en place du réseau, sera démarré en ordre 10, après les S01, S05, etc. mais avant les S11, S15, S20.**

## 5-3 LE DÉMARRAGE DES SERVICES

```
alain@mohamed-VirtualBox:~$ systemctl stop bluetooth  
alain@mohamed-VirtualBox:~$ service bluetooth start  
alain@mohamed-VirtualBox:~$ /etc/init.d/bluetooth start  
Starting bluetooth (via systemctl): bluetooth.service.
```

### Contrôle manuel des services

#### **START (3 manières)**

- I. « **/etc/init.d/<nom du service> start** » : Démarre un service.
- I. « **service <nom du service> status** » : Démarre un service.
- I. « **systemctl start <nom du service>** » : Démarre aussi un service.

## 5-3 LE DÉMARRAGE DES SERVICES

```
root@mohamed-VirtualBox:/home/alain# systemctl status openvpn
● openvpn.service - OpenVPN service
  Loaded: loaded (/lib/systemd/system/openvpn.service; enabled; vendor preset: enabled)
  Active: active (exited) since Thu 2021-09-02 18:57:34 CEST; 2min 15s ago
    Process: 7167 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 7167 (code=exited, status=0/SUCCESS)

sept. 02 18:57:34 mohamed-VirtualBox systemd[1]: Starting OpenVPN service...
sept. 02 18:57:34 mohamed-VirtualBox systemd[1]: Finished OpenVPN service.

root@mohamed-VirtualBox:/home/alain# service openvpn status
● openvpn.service - OpenVPN service
  Loaded: loaded (/lib/systemd/system/openvpn.service; enabled; vendor preset: enabled)
  Active: active (exited) since Thu 2021-09-02 18:57:34 CEST; 1min 12s ago
    Process: 7167 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 7167 (code=exited, status=0/SUCCESS)

sept. 02 18:57:34 mohamed-VirtualBox systemd[1]: Starting OpenVPN service...
sept. 02 18:57:34 mohamed-VirtualBox systemd[1]: Finished OpenVPN service.

root@mohamed-VirtualBox:/home/alain# /etc/init.d/openvpn status
● openvpn.service - OpenVPN service
  Loaded: loaded (/lib/systemd/system/openvpn.service; enabled; vendor preset: enabled)
  Active: active (exited) since Thu 2021-09-02 18:57:34 CEST; 7s ago
    Process: 7167 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 7167 (code=exited, status=0/SUCCESS)

sept. 02 18:57:34 mohamed-VirtualBox systemd[1]: Starting OpenVPN service...
sept. 02 18:57:34 mohamed-VirtualBox systemd[1]: Finished OpenVPN service.
```

## CONTRÔLE MANUEL DES SERVICES

### **STATUS (3 manières)**

- I. « **/etc/init.d/<nom du service> status** » : Affiche le statut d'un service.
- I. « **service <nom du service> status** » : Affiche le statut d'un service.
- I. « **systemctl status <nom du service>** » : Affiche le statut d'un service.

## 5-3 LE DÉMARRAGE DES SERVICES

### Contrôle manuel des services

```
root@mohamed-VirtualBox:/home/alain# /etc/init.d/openvpn stop
Stopping openvpn (via systemctl): openvpn.service.

root@mohamed-VirtualBox:/home/alain# systemctl stop openvpn

root@mohamed-VirtualBox:/home/alain# service openvpn stop

root@mohamed-VirtualBox:/home/alain# systemctl status openvpn
● openvpn.service - OpenVPN service
    Loaded: loaded (/lib/systemd/system/openvpn.service; enabled; vendor prese>
    Active: inactive (dead) since Thu 2021-09-02 19:00:32 CEST; 6s ago
      Process: 7167 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
     Main PID: 7167 (code=exited, status=0/SUCCESS)

sept. 02 18:57:34 mohamed-VirtualBox systemd[1]: Starting OpenVPN service...
sept. 02 18:57:34 mohamed-VirtualBox systemd[1]: Finished OpenVPN service.
sept. 02 19:00:32 mohamed-VirtualBox systemd[1]: openvpn.service: Succeeded.
sept. 02 19:00:32 mohamed-VirtualBox systemd[1]: Stopped OpenVPN service.
```

#### **STOP (3 manières)**

- I. « **/etc/init.d/<nom du service> stop** » : Arrête un service.
- II. « **service <nom du service> stop** » : Arrête un service.
- III. « **systemctl stop <nom du service>** » : Arrête aussi un service.

Il existe aussi d'autres commandes comme « **restart** », « **reload** »..

## 5-3 LE DÉMARRAGE DES SERVICES

INIT => SYSTEMD

...

```
root@mohamed-VirtualBox:/home/alain# systemctl disable cron
Synchronizing state of cron.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable cron

root@mohamed-VirtualBox:/home/alain# systemctl list-unit-files --type service -all
UNIT FILE                                STATE        VENDOR PRESET
accounts-daemon.service                   enabled     enabled
acpid.service                            disabled    enabled
alsa-restore.service                     static      enabled
alsa-state.service                      static      enabled
alsa-utils.service                      masked     enabled
anacron.service                          enabled     enabled
apparmor.service                         enabled     enabled
bluetooth.service                       enabled     enabled
console-getty.service                   disabled    disabled
console-setup.service                   enabled     enabled
container-getty@.service                static      enabled
cron.service                            disabled    enabled
cryptdisks-early.service               masked     enabled

root@mohamed-VirtualBox:/home/alain# systemctl enable cron
Synchronizing state of cron.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable cron
Created symlink /etc/systemd/system/multi-user.target.wants/cron.service → /lib/systemd/system/cron.service.

root@mohamed-VirtualBox:/home/alain# systemctl list-units
UNIT                                         LOAD   ACTIV>
proc-sys-fs-binfmt_misc.automount           loaded activ>
sys-devices-pci0000:00-0000:00:01.1-ata2-host1-target1:0:0-1:0:0:0-block-sr0.device    loaded activ>
sys-devices-pci0000:00-0000:00:03.0-net-ens3.device          loaded activ>
sys-devices-pci0000:00-0000:00:05.0-sound-card0.device    loaded activ>
sys-devices-pci0000:00-0000:00:0d.0-ata3-host2-target2:0:0-2:0:0:0-block-sda-sdal.device loaded activ>
sys-devices-pci0000:00-0000:00:0d.0-ata3-host3-target2:0:0-2:0:0:0-block-sda-sda2.device loaded activ>
sys-devices-pci0000:00-0000:00:0d.0-ata3-host4-target2:0:0-2:0:0:0-block-sda-sda5.device loaded activ>
sys-devices-pci0000:00-0000:00:0d.0-ata5-host4-target4:0:0-4:0:0:0-block-sdc.device       loaded activ>
sys-devices-pci0000:00-0000:00:0d.0-ata6-host5-target5:0:0-5:0:0:0-block-sdd.device       loaded activ>

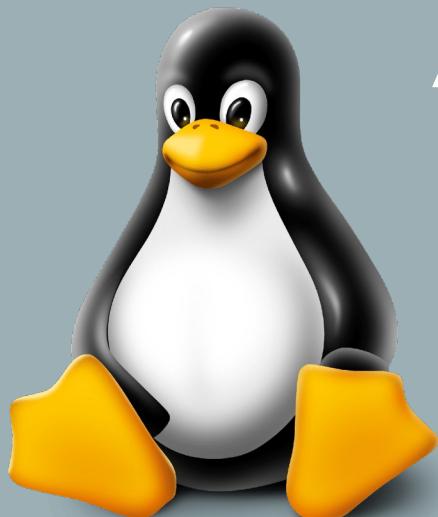
root@mohamed-VirtualBox:/home/alain# systemctl list-unit-files --type service -all
UNIT FILE                                STATE        VENDOR PRESET
accounts-daemon.service                   enabled     enabled
acpid.service                            disabled    enabled
alsa-restore.service                     static      enabled
alsa-state.service                      static      enabled
alsa-utils.service                      masked     enabled
anacron.service                          enabled     enabled
casper.service                           enabled     enabled
clean-mount-point@.service              static      enabled
colord.service                           static      enabled
configure-printer@.service              static      enabled
console-getty.service                   disabled    disabled
console-setup.service                  enabled     enabled
container-getty@.service                static      enabled
cron.service                            enabled     enabled
```

### Avec la commande *systemctl*

- « **systemctl enable <nom du service>** » : permettre au service d'être lancé au démarrage.
- « **systemctl disable <nom du service>** » : ne pas lancer le service au démarrage.
- « **systemctl list-units** » : Affiche tous les units (services et autres).
- « **systemctl list-units --type service** » : Affiche les units de type service

## 6 - CONFIGURER TCP/IP EN ENVIRONNEMENT LINUX.

Ajouter un système dans un réseau Ipv4 / Ipv6 - Les commandes de diagnostics - Le fonctionnement des systèmes INETD – Les wrappers.



## **6 - CONFIGURER TCP/IP EN ENVIRONNEMENT LINUX.**

- 6-1. Ajouter un système (Debian, RedHat) dans un réseau ipv4 / ipv6.***
- 6-2. Les commandes de diagnostics.***
- 6-3. Le fonctionnement des systèmes INETD.***
- 6-4. Les wrappers.***

## 6-I AJOUTER UN SYSTÈME LINUX À UN RÉSEAUX IPV4 OU IPV6

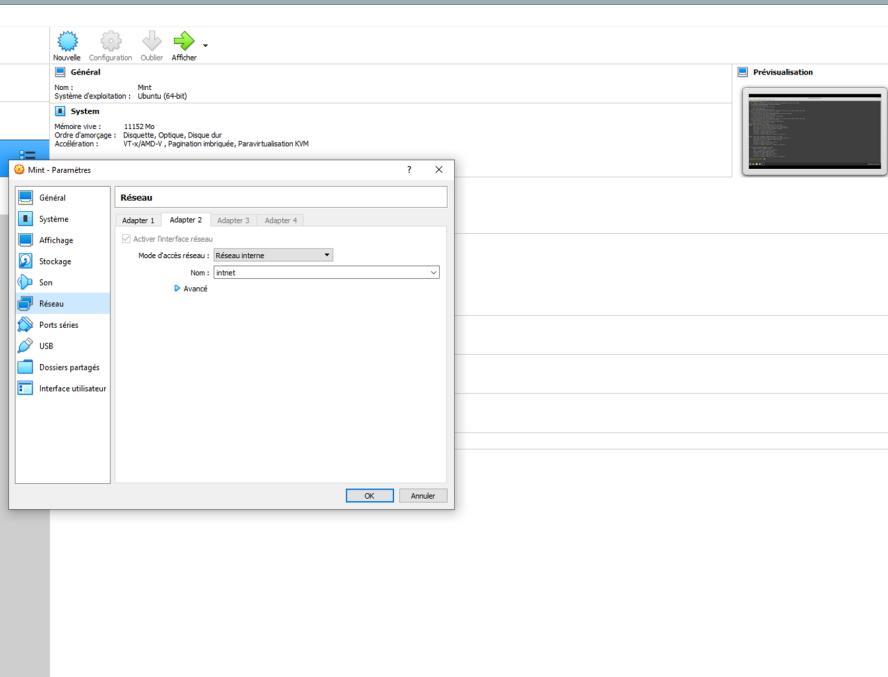
- Quelques définitions de base :
  - **Le réseau informatique** est un ensemble d'équipements reliés entre eux pour échanger des informations.
  - **Un hôte** est une machine sur un réseau.
  - **Une Adresse IP** permet d'identifier une machine (hôte) sur un réseau.
  - Il existe 2 types d'adresse IP : **Ipv4** sur 32 bits et **Ipv6** sur 64 bits.
  - Les machines communiquent entre elles via un protocole bien défini, le **protocole TCP/IP**.
  - L'adresse **127.0.0.1** représente la machine elle-même sur un réseau. On l'appelle **localhost**.
  - Un **masque réseau** est le délimiteur entre la partie réseau et la partie machine (ex : 255.255.255.0).
  - Un **réseau local** ( LAN : Local Area Network ) ou sous-réseau est le réseau local sur lequel une ou plusieurs machines peuvent être connectées et qui est rattaché à un réseau plus grand (**WAN : Wide Area Network**) sur lequel se trouve d'autres LAN.



## 6-1 AJOUTER UN SYSTÈME LINUX A UN RÉSEAU IPV4

EN MODE MANUEL

### ***Simulation avec Virtual Box***



- Dans virtualBox, nous allons créer un nouveau point de connexion pour notre distribution.
1. Eteindre la distribution si allumée.
  2. Sélectionner votre distribution .
  3. Cliquer sur Configuration > Réseau > Adapter 2 :
    - **Active l'interface réseau : coché.**
    - **Mode d'accès réseau : Réseau interne**
    - **Validation avec ok.**

# 6-1 AJOUTER UN SYSTÈME LINUX A UN RÉSEAU IPV4

EN MODE MANUEL

## ***Simulation avec Virtual Box***

```
# Affiche toutes les interfaces de connexion avec les informations relatives à leurs adresse IP.  
# On apperçoit notamment la nouvelle interface réseau : enp0s8  
alain@mohamed-VirtualBox:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inetc6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:3b:a5:90 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3  
        valid_lft 86287sec preferred_lft 86287sec  
    inetc6 fe80::1f53:ee4:977e:5e09/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:ec:a5:2e brd ff:ff:ff:ff:ff:ff  
    inetc6 fe80::8f4a:b4df:e4b2:97ca/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
  
# Affiche toutes les interfaces de connexion avec les informations relatives à leurs adresse IP.  
# On apperçoit notamment la nouvelle interface réseau : enp0s8  
alain@mohamed-VirtualBox:~$ ifconfig  
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255  
    inetc6 fe80::1f53:ee4:977e:5e09 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:3b:a5:90 txqueuelen 1000 (Ethernet)  
    RX packets 77 bytes 10380 (10.3 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 123 bytes 14096 (14.0 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inetc6 fe80::8f4a:b4df:e4b2:97ca prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:ec:a5:2e txqueuelen 1000 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 84 bytes 13481 (13.4 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inetc6 127.0.0.1 netmask 255.0.0.0  
    inetc6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Boucle locale)  
    RX packets 231 bytes 20289 (20.2 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 231 bytes 20289 (20.2 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
# crée un fichier yaml pour la configuration réseau de la nouvelle interface réseau créée : enp0s8  
root@mohamed-VirtualBox:/home/alain# touch /etc/netplan/2-lan_statique.yaml
```

- Allumons la distribution modifiée.
- Vérifions que la modification a bien été prise en compte :
  - Saisir « **ip a** » ou « **ifconfig** ».
  - Un nouveau point de connexion (interface) doit apparaître :
    - **enpS08**
- On va utiliser **netplan** qui est un programme qui va nous permettre d'écrire nos configurations réseaux dans un fichier yaml.
- Création d'un fichier de configuration au format yaml :
  - « **touch /etc/netplan/2-lan\_statique.yaml** »

## 6-1 AJOUTER UN SYSTÈME LINUX A UN RÉSEAU IPV4

The screenshot shows a terminal window titled "root@mohamed-VirtualBox: /home/alain". The window contains the following text:

```
GNU nano 4.8          /etc/netplan/2-lan_statique.yaml
network :
  version: 2
  ethernets:
    enp0s8:
      dhcp4: no
      dhcp6: no
      addresses: [192.168.0.10/24]
      gateway4: 0.0.0.0
      nameservers:
        addresses: [127.0.0.1]
```

The status bar at the bottom of the terminal window shows "[ Lecture de 10 lignes ]". Below the status bar, there is a menu bar with "Fichier", "Édition", "Affichage", "Rechercher", "Terminal", and "Aide". At the bottom, there is a toolbar with various keyboard shortcut keys: ^G Aide, ^O Écrire, ^W Chercher, ^K Couper, ^J Justifier, ^C Pos. cur., ^X Quitter, ^R Lire fich., ^R Remplacer, ^U Coller, ^T Orthograp., ^ Aller ligne.

EN MODE MANUEL

### Simulation avec Virtual Box

- Ouvrir le fichier créé, **2-lan\_statique.yaml** avec nano :  
« nano /etc/netplan/2-lan\_statique.yaml »
- Saisir les informations suivantes en respectant le système d'indentation du fichier yaml :  
**network :**  
**version: 2**  
**ethernets:**  
**enp0s8:**  
**dhcp4: no**  
**dhcp6: no**  
**addresses: [192.168.0.10/24]**  
**gateway4: 0.0.0.0**  
**nameservers:**  
**addresses: [127.0.0.1]**
- Pour définir **l'adresse IP** de cette interface, il faut se baser sur le masque réseau et **l'adresse IP** de la machine sur le réseau local.
- Enregistrer le fichier nano et lancer : « **sudo netplan apply** ».

## 6-1 AJOUTER UN SYSTÈME LINUX A UN RÉSEAU IPV4

```
root@mohamed-VirtualBox:/home/alain# nano /etc/hosts
root@mohamed-VirtualBox:/home/alain# ip link set enp0s3 down
root@mohamed-VirtualBox:/home/alain# ip link set enp0s8 up

# L'interface réseau enp0s8 est bien active avec une adresse IP4 : 192.168.0.10 (inet)
# L'interface réseau enp0s3 est désactivée.
root@mohamed-VirtualBox:/home/alain# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 08:00:27:3b:a5:90 brd ff:ff:ff:ff:ff:ff
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ec:a5:2e brd ff:ff:ff:ff:ff:ff
        inet 192.168.0.10/24 brd 192.168.0.255 scope global noprefixroute enp0s8
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:feec:a52e/64 scope link
            valid_lft forever preferred_lft forever

# Les paquets sont bien transmis aucune perte. L'adresse ip est bien fonctionnel.
root@mohamed-VirtualBox:/home/alain# ping -c 4 192.168.0.10
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 octets de 192.168.0.10 : icmp_seq=1 ttl=64 temps=0.031 ms
64 octets de 192.168.0.10 : icmp_seq=2 ttl=64 temps=0.045 ms
64 octets de 192.168.0.10 : icmp_seq=3 ttl=64 temps=0.074 ms
64 octets de 192.168.0.10 : icmp_seq=4 ttl=64 temps=0.046 ms

--- statistiques ping 192.168.0.10 ---
4 paquets transmis, 4 reçus, 0 % paquets perdus, temps 3052 ms
rtt min/avg/max/mdev = 0.031/0.049/0.074/0.015 ms
```

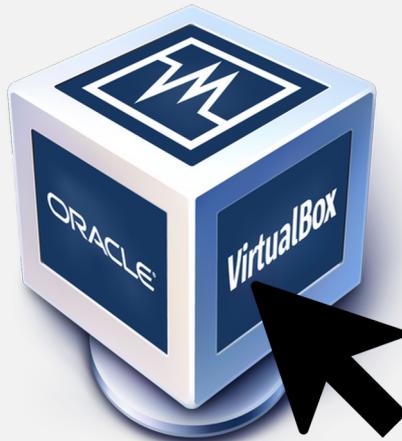
### EN MODE MANUEL

#### ***Simulation avec Virtual Box***

- Rajouter la nouvelle adresse IP ( 192.168.0.10/24) au fichier **/etc/hosts** avec la commande : « nano /etc/hosts »
  - **192.168.0.10 'nom du serveur'**
- Désactiver l'interface enp0s3 : **« ip link set enp0s3 down ».**
- Activer l'interface réseau que l'on a créée : **« ip link set enp0s8 up ».**
- Vérifier l'état des interfaces et s'assurer que les modifications ont bien été prise en compte : « ip a ».
- Vérifier que l'interface réseau est fonctionnel et que notre serveur est intégré au réseau local et non plus à celui de VB avec la commande : **« ping 192.168.0.10 »**

## 6-I AJOUTER UN SYSTÈME LINUX A UN RESEAU IPV4 / IPV6

Un peu de pratique avec le mode interface



## 6-2 LES COMMANDES DE DIAGNOSTICS

- Il existe beaucoup de commandes qui vont permettre d'effectuer un diagnostic du réseaux sur lequel est branché votre machine.
- Nous allons voir les principales commandes qui vont permettre d'avoir une vue sous différents angles de votre réseau :
  - IFCONFIG – IP.
  - PING – HOST – DIG.
  - NMAP – TRACEROUTE.
  - NETSTAT – IFTOP.
  - DCPFUMP - NGREP



## 6-2 LES COMMANDES DE DIAGNOSTICS

```
root@mohamed-VirtualBox:/home/alain# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::1f53:ee4:977e:5e09 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:3b:a5:90 txqueuelen 1000 (Ethernet)
            RX packets 12222 bytes 12475822 (12.4 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 14203 bytes 1397349 (1.3 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Boucle locale)
            RX packets 9218 bytes 621628 (621.6 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 9218 bytes 621628 (621.6 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@mohamed-VirtualBox:/home/alain# ip -4 -o addr show
1: lo    inet 127.0.0.1/8 scope host lo\      valid_lft forever preferred_lft forever
2: enp0s3  inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3\
valid_lft 85505sec preferred_lft 85505sec
3: enp0s8  inet 192.168.0.10/24 brd 192.168.0.255 scope global enp0s8\
valid_lft forever preferred_lft forever
```

### LES COMMANDES : IFCONFIG – IP

#### IFCONFIG :

- **ifconfig** est une commande Unix qui permet de configurer et d'afficher les informations des interfaces réseau IP à partir de l'interpréteur de commandes.
- « **man ifconfig** » : liste des commandes.

#### IP :

- Commande qui tend à remplacer **ifconfig**.
- « **ip a** » : Affiche toutes les adresses IP d'un réseau.
- « **Ip addr add 192.168.1.5/24 dev eth0** » : attribue une adresse ip à l'interface eth0.
- « **ip -4 -o addr show** » : affiche les informations sur les interfaces réseaux avec une Ipv4 sur une ligne.
- « **ip addr del 192.168.1.5/24 dev eth0** » : supprime l'adresse ip de l'interface eth0.
- « **ip link set eth0 up** » : active l'interface réseau.
- « **ip link set eth0 down** » : désactive l'interface réseau.
- « **man ip** » : liste des commandes.

## 6-2 LES COMMANDES DE DIAGNOSTICS

```
root@mohamed-VirtualBox:/home/alain# ping -c 4 google.fr
PING google.fr (142.250.201.163) 56(84) bytes of data.
64 octets de par2ls23-in-f3.1e100.net (142.250.201.163) : icmp_seq=1 ttl=113 temps=33.9 ms
64 octets de par2ls23-in-f3.1e100.net (142.250.201.163) : icmp_seq=2 ttl=113 temps=65.5 ms
64 octets de par2ls23-in-f3.1e100.net (142.250.201.163) : icmp_seq=3 ttl=113 temps=48.2 ms
64 octets de par2ls23-in-f3.1e100.net (142.250.201.163) : icmp_seq=4 ttl=113 temps=69.2 ms

--- statistiques ping google.fr ---
4 paquets transmis, 4 reçus, 0 % paquets perdus, temps 3005 ms
rtt min/avg/max/mdev = 33.919/54.209/69.219/14.148 ms

root@mohamed-VirtualBox:/home/alain# host www.google.fr
www.google.fr has address 216.58.214.163
www.google.fr has IPv6 address 2a00:1450:4007:81a::2003

root@mohamed-VirtualBox:/home/alain# dig www.google.fr
<>> DiG 9.16.1-Ubuntu <>> www.google.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 32515
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.fr.      IN  A

;; ANSWER SECTION:
www.google.fr.    137 IN  A   216.58.206.227

;; Query time: 52 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: sam. sept. 04 11:52:54 CEST 2021
;; MSG SIZE  rcvd: 58
```

### LES COMMANDES : PING – HOST - DIG

#### PING :

- **ping** est un outil d'administration qui permet de diagnostiquer l'accessibilité d'une machine à travers un réseau.
- Sa mission principale consiste à vérifier les connexions établies entre un ou plusieurs hôtes distants
- La commande « **ping -c 4 www.google.fr** » : va envoyer 4 paquets sur le réseau à l'adresse IP du serveur sur lequel se trouve Google.

#### Host :

- **Host** permet de convertir des DNS en adresse ip.
- Exemple : « **host www.google.fr** ».

#### DIG :

- **Dig ( Domain Information Groper)** est un outil très complet pour effectuer des requêtes DNS.
- Exemple : « **dig www.google.fr** ».

## 6-2 LES COMMANDES DE DIAGNOSTICS

### LES COMMANDES : TRACEROUTE - NMAP

```
root@mohamed-VirtualBox:/home/alain# nmap -v www.leboncoin.fr
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-04 11:17 CEST
Initiating Ping Scan at 11:17
Scanning www.leboncoin.fr (52.222.174.122) [4 ports]
Completed Ping Scan at 11:17, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:17
Completed Parallel DNS resolution of 1 host. at 11:17, 0.06s elapsed
Initiating SYN Stealth Scan at 11:17
Scanning www.leboncoin.fr (52.222.174.122) [1000 ports]
Discovered open port 443/tcp on 52.222.174.122
Discovered open port 21/tcp on 52.222.174.122
Discovered open port 80/tcp on 52.222.174.122
Completed SYN Stealth Scan at 11:17, 4.79s elapsed (1000 total ports)
Nmap scan report for www.leboncoin.fr (52.222.174.122)
Host is up (0.016s latency).
Other addresses for www.leboncoin.fr (not scanned): 52.222.174.18 52.222.174.76 52.222.174.10
rDNS record for 52.222.174.122: server-52-222-174-122.cdg50.r.cloudfront.net
Not shown: 997 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.04 seconds
Raw packets sent: 2003 (88.100KB) | Rcvd: 6 (252B)

C:\Users\afpa>tracert -4 -h 10 www.google.fr
Détermination de l'itinéraire vers www.google.fr [142.250.179.67]
avec un maximum de 10 sauts :

 1  <1 ms   <1 ms   <1 ms  192.168.0.254
 2  6 ms    6 ms    6 ms  194.149.169.174
 3  7 ms    7 ms    6 ms  194.149.166.54
 4  7 ms    6 ms    6 ms  72.14.220.92
 5  6 ms    6 ms    6 ms  108.170.231.95
 6  6 ms    7 ms    6 ms  142.251.49.131
 7  7 ms    6 ms   12 ms  par21s19-in-f3.1e100.net [142.250.179.67]

Itinéraire déterminé.
```

#### NMAP :

- **NMAP** est un scanner de port libre. Il est conçu pour détecter les ports ouverts, identifier les services hébergés et obtenir des informations sur le système d'exploitation d'un ordinateur distant.
- **« nmap -vv www.leboncoin.fr ».**
- **« man nmap »** : pour le détails d'autres commandes.

#### TRACEROUTE :

- **TRACEROUTE** est un programme utilitaire qui permet de suivre les chemins qu'un paquet de données (paquet IP) va prendre pour aller de la machine locale à une autre machine connectée au réseau IP.
- **« traceroute -4 10 google.com »** : affiche les 10 premiers sauts vers le DNS google.com pour les ipv4.
- **« man traceroute »** : pour le détails d'autres commandes.

## 6-2 LES COMMANDES DE DIAGNOSTICS

```
root@mohamed-VirtualBox:/home/alain# netstat -e
Connexions Internet actives (sans serveurs)
Proto Recv-Q Send-Q Adresse locale      Adresse distante     Etat      Utilisatr Inode
tcp      0      0 mohamed-VirtualBo:41010  ec2-44-239-97-185:https ESTABLISHED alain    119584
udp      0      0 mohamed-VirtualB:bootpc _gateway:bootps   ESTABLISHED root     102447
Sockets du domaine UNIX actives (sans serveurs)
Proto RefCnt Flags     Type      State          I-Node  Chemin
unix  2      [ ]  DGRAM      CONNECTE       29968  /run/user/1001/systemd/notify
unix  3      [ ]  DGRAM      CONNECTE       15857  /run/systemd/notify
unix  2      [ ]  DGRAM      CONNECTE       15875  /run/systemd/journal/syslog
unix  19     [ ]  DGRAM      CONNECTE       15885  /run/systemd/journal/dev-log
unix  8      [ ]  DGRAM      CONNECTE       15889  /run/systemd/journal/socket
unix  3      [ ]  STREAM     CONNECTE      92880
unix  3      [ ]  STREAM     CONNECTE      31407  @/tmp/dbus-RD1V5rSxFx
unix  2      [ ]  DGRAM      CONNECTE      42652
unix  3      [ ]  STREAM     CONNECTE      31690  /run/user/1001/pulse/native
unix  3      [ ]  STREAM     CONNECTE      20283  /run/systemd/journal/stdout
unix  2      [ ]  STREAM     CONNECTE      94041
unix  3      [ ]  STREAM     CONNECTE      32249
unix  3      [ ]  STREAM     CONNECTE      33105
unix  3      [ ]  STREAM     CONNECTE      31085  /run/systemd/journal/stdout
unix  3      [ ]  STREAM     CONNECTE      118526  /run/dbus/system_bus_socket
unix  3      [ ]  STREAM     CONNECTE      92895
unix  3      [ ]  STREAM     CONNECTE      92870
```

```
Fichier Édition Affichage Rechercher Terminal Aide
1,91Mb      3,81Mb      5,72Mb      7,63Mb      9,54Mb
mohamed-VirtualBox  => par21s17-in-f14.1e100.net  476b  1,58Kb  1,26Kb
mohamed-VirtualBox  <=                           476b  417b  279b
mohamed-VirtualBox  => par21s17-in-f3.1e100.net  320b  96b   48b
mohamed-VirtualBox  <=                           320b  96b   48b
mohamed-VirtualBox  => par21s20-in-f22.1e100.net  476b  95b   24b
mohamed-VirtualBox  <=                           476b  95b   24b
mohamed-VirtualBox  => 93.184.220.29           0b    0b   40b
mohamed-VirtualBox  <=                           0b    0b   40b
mohamed-VirtualBox  => ec2-52-50-19-116.eu-west- 0b    0b   25b
mohamed-VirtualBox  <=                           0b    0b   25b
mohamed-VirtualBox  => par10s39-in-f1.1e100.net  0b    0b   24b
mohamed-VirtualBox  <=                           0b    0b   24b
mohamed-VirtualBox  => fra15s10-in-f6.1e100.net  0b    0b   24b
mohamed-VirtualBox  <=                           0b    0b   24b
mohamed-VirtualBox  => 104.19.183.2            0b    0b   24b
mohamed-VirtualBox  <=                           0b    0b   24b
mohamed-VirtualBox  => 221.209.102.34.bc.googleu 0b    0b   24b
mohamed-VirtualBox  <=                           0b    0b   24b

TX:          cum:  500KB  peak:  11,6Kb  rates:  1,24Kb  1,77Kb  1,76Kb
RX:              1,88MB  5,48Kb  1,24Kb  608b   797b
TOTAL:        2,37MB  17,1Kb  2,48Kb  2,36Kb  2,54Kb
```

## LES COMMANDES : NETSTAT - IFTOP

### NETSTAT :

- **netstat**, pour « network statistics », est une ligne de commande affichant des informations sur les connexions réseau, les tables de routage et un certain nombre de statistiques.
- « **netstat -e** » : affiche les statistiques ethernet.

### IFTOP :

- **iftop** fait partie des commandes "top" mais pour le réseau qui permet de visualiser en temps réel le débit par adresses contactées.
- « **iftop** » : Affiche les informations concernant les débits consommés lors des appels d'adresses IP.

## 6-2 LES COMMANDES DE DIAGNOSTICS



```
root@mohamed-VirtualBox:/home/alain# tcpdump -i enp0s3 host 142.250.178.131
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
10:29:01.535635 IP mohamed-VirtualBox.42070 > par21s22-in-f3.1e100.net.443: UDP, length 1357
10:29:01.611182 IP par21s22-in-f3.1e100.net.443 > mohamed-VirtualBox.42070: UDP, length 1357
10:29:01.611394 IP par21s22-in-f3.1e100.net.443 > mohamed-VirtualBox.42070: UDP, length 1357
10:29:01.611652 IP par21s22-in-f3.1e100.net.443 > mohamed-VirtualBox.42070: UDP, length 1357
10:29:01.612195 IP mohamed-VirtualBox.42070 > par21s22-in-f3.1e100.net.443: UDP, length 86
10:29:01.614215 IP par21s22-in-f3.1e100.net.443 > mohamed-VirtualBox.42070: UDP, length 1357
10:29:01.614309 IP mohamed-VirtualBox.42070 > par21s22-in-f3.1e100.net.443: UDP, length 42
10:29:01.614679 IP par21s22-in-f3.1e100.net.443 > mohamed-VirtualBox.42070: UDP, length 446
10:29:01.617932 IP mohamed-VirtualBox.42070 > par21s22-in-f3.1e100.net.443: UDP, length 43
```

### LES COMMANDES : TCPDUMP - NGREP

#### TCPDUMP :

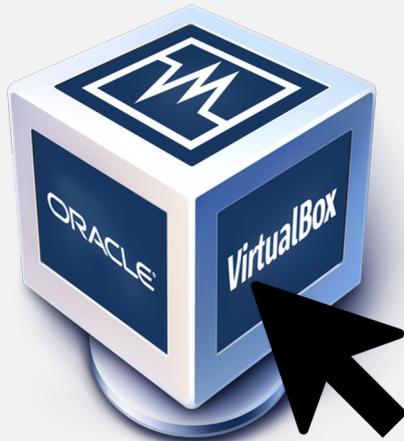
- **TCPDUMP** capture et affiche les paquets réseaux échangés par une ou plusieurs interfaces réseaux.
- On peut rediriger ce flux vers un fichier texte.
- « **tcpdump -i enps03** » : écoute l'échange de paquets entre l'interface enps03 et les autres interfaces.
- « **tcpdump -i enps03 host 142.250.178.131** » : écoute l'échange de paquets entre l'interface enps03 et l'hôte à l'adresse ip (142.250.178.131).
- « **tcpdump src 13.225.25.50** » : Ecoute les échanges de paquets en prévision de l'adresse ip 13.225.25.50.
- « **tcpdump dst 13.225.25.125** » : Ecoute les échanges de paquets à destination de 13.255.25.125

#### NGREP :

- **NGREP** fonctionne comme tcpdump à la seule différence qu'il ne va afficher que les strings des paquets.
- « **ngrep -d enps03 host 142.250.178.131** » : écoute l'échange de paquets entre l'interface enps03 et l'hôte à l'adresse ip (142.250.178.131).

## 6-2 LES COMMANDES DE DIAGNOSTICS

Un peu de pratique



## 6-3 LE FONCTIONNEMENT DES SYSTÈMES INETD (XINETD)

- XINETD (e**X**tend Inter**N**ET **D**aemon) version plus sécurisée d'INETD est un démon qui a comme rôle de piloter l'accès à un ou plusieurs réseaux.
- En fonction de sa configuration, il pourra sécuriser et contrôler l'accès à votre server en contrôlant et vérifiant les requêtes qui transitent sur le réseau vers votre server.
- Ses principales fonctionnalités sont :
  - Paramétrage d'accès par service et non pas de manière globale.
  - Paramétrage d'accès par créneaux ou plages horaires pour des services.
  - Possibilité de limiter les attaques de type deny of service par exemple ou autres.
  - Possibilité d'affiner les logs des services gérés.
- S'il est pas installé ou présent: « **apt install xinetd** ».



## 6-3 LE FONCTIONNEMENT DES SYSTÈMES INETD (XINETD)

- Il existe 2 types de configuration d'accès au fichier :
  - I. Un accès via **/etc/xinetd.conf** avec un seul fichier qui prendra la configuration globale et par service.
  - I. Un accès via /etc/ mais avec 1 fichier et 1 dossier :
    - Un fichier **/etc/xinetd.conf** : configuration générale.
    - Un dossier **/etc/xinetd.d** : avec plusieurs fichiers de configuration dédiés chacun d'eux à un service.
- **La seconde configuration avec les 2 fichiers est la plus courante dans les distributions Linux.**



## 6-3 LE FONCTIONNEMENT DES SYSTÈMES INETD (XINETD)

```
# Affiche le dossier de configuration (xinetd.d) des services et le fichier de configuration générale (xinetd.conf) Xinetd
root@mohamed-VirtualBox:/home/alain# ls /etc/xinetd/
/etc/xinetd.conf

/etc/xinetd.d:
chargen    daytime    discard    echo    servers    time
chargen-udp  daytime-udp  discard-udp  echo-udp  services  time-udp

# Fichier de configuration générale avec exemple : 60 requêtes maximal - journalisation
/var/log/secure - nom hôte et numéro processus en cas de succès de connexion - nom de l'hôte en cas d'échec - 25 connexions par seconde sinon blocage 30 secondes.
root@mohamed-VirtualBox:/home/alain# cat /etc/xinetd.conf
# Simple configuration file for xinetd
#
# Some defaults, and include /etc/xinetd.d/

defaults
{
    instances          = 60
    log_type           = SYSLOG authpriv
    log_on_success     = HOST PID
    log_on_failure     = HOST
    cps                = 25 30
}

includedir /etc/xinetd.d
```

### CONFIGURATION GLOBALE

#### **/etc/xinetd.conf**

- Ces paramètres de configurations vont influencer l'ensemble des services gérées par **xinetd**.
- **Les attributs du fichier de configuration générale /etc/xinetd.conf :**
  - I. **instances** : nombre maximal de requête qu'un service peut gérer à un moment donné.
  - I. **log\_type** : localisation journalisation.
  - I. **log\_on\_success** : donnée de journalisation si la connexion est établie avec le service.
  - I. **log\_on\_failure** : donnée de journalisation si la connexion a échoué.
  - I. **cps** : Limite le nombre de connexion par seconde pour chacun des services gérés par xinetd et le retire pendant une période définie.
  - I. **includedir /etc/xinetd.d/** : Inclut des options stipulées dans les fichiers de configuration spécifiques aux services qui se trouvent dans le répertoire /etc/xinetd.d/

## 6-3 LE FONCTIONNEMENT DES SYSTÈMES INETD (XINETD)

```
# Fichier de configuration pour le service "servers"
#(service interne : fonctionnement du Deamon xinetd)
root@mohamed-VirtualBox:/home/alain# cat /etc/xinetd.d/servers
# default: off
# description: An internal xinetd service, listing active servers.

service servers
{
    type      = INTERNAL UNLISTED
    port      = 9099
    socket_type = stream
    protocol   = tcp
    wait       = no
    disable    = yes
    only_from  = 127.0.0.1
}
```

### CONFIGURATION D'UN SERVICE

#### **/etc/xinetd.d/nom du service**

- Ces paramètres de configurations vont impacter uniquement le service concerné.
- **Les attributs du fichier (non exhaustifs) de configuration du service /etc/xinetd.d/ :**

Attribut	Définition
socket-type	Type de socket utilisé pour le service : dgram s'il utilise le protocole UDP, stream s'il utilise le protocole TCP - consulter le fichier /etc/services pour avoir l'information.
user	Identité sous laquelle le service sera lancé
server	chemin et nom du serveur
wait	Définit le comportement du service dans le traitement des threads : yes pour un service mono-thread (une connexion simultanée par service et une seule), no pour un service multithread (possibilité d'avoir plusieurs connexions simultanées au service)
protocol	Protocole utilisé par le service. Si rien n'est précisé, c'est le protocole spécifié dans le fichier /etc/services qui sera utilisé.
rpc_version rpc_number	Ne concerne que les services basés sur les RPC (exemple : NFS)
port	Port associé au service. Là encore, s'il n'est pas précisé, c'est le port spécifié pour le service dans le fichier /etc/services.

## 6-3 LE FONCTIONNEMENT DES SYSTÈMES INETD (XINETD)

```
root@mohamed-VirtualBox:/home/alain# cat /etc/xinetd.d/servers
# default: off
# description: An internal xinetd service, listing active servers.

service servers
{
    type      = INTERNAL UNLISTED
    port      = 9099
    socket_type = stream
    access_times = 09:45-16:15
    nice      = -19
    protocol   = tcp
    no_access  = 10.0.1.0/24
    wait      = no
    disable    = yes
    only_from  = 127.0.0.1
}
```

## PARAMETRE SUPPLEMENTAIRE DE SECURITE POUR UN SERVICE

### **Limiter les attaques Deny of Service**

Action	nom paramètre	Définition
Contrôle de la charge CPU	rlimit_cpu = seconds.	Cet attribut vous permet de limiter le temps CPU utilisé par un ou plusieurs services
Priorité du processus	nice = level	l'attribut permet de fixer une priorité d'ordonnancement pour le serveur. Le level peut prendre les valeurs de -20 (le plus prioritaire) à 19 (le moins prioritaire).
Limite nbre connexion par service	instances = value	L'attribut détermine le nombre d'instances simultanées du serveur qui seront autorisées. Préciser un nombre
Limite nombre de connexion avec la même origine	per_source = value.	Non seulement vous pouvez filtrer les adresses IP clientes, le nombre d'instances du serveur mais vous pouvez aussi limiter le nombre de connexions à un serveur donné provenant d'une même adresse IP
Ip blacklist	Ex : 192.168.0.12 flags = SENSOR deny_time = minutes	Il est possible blacklister des adresses IP qui tenteraient des connexions sur des services
Période d'accès	access_time	On pourra choisir le moment auquel vous autoriserez les accès à tout ou partie de vos services réseaux.
Limiter l'accès à certaines adresses	only_from	On va aussi pouvoir filtrer les clients qui vont pouvoir ou non se connecter à vos serveurs.

## 6-4 LES WRAPPERS

- **TCP-Wrapper** est un outil de sécurité réseau qui permet de contrôler les accès, les tentatives de connexion sur une machine donnée.
- Il permet à tout instant :
  - De filtrer les accès.
  - De tracer ( journalisation syslog) les connexions et tentatives de connexions à la machine.
- **Le Wrapper** va s'intercaler entre le super daemon xinetd et le serveur.
- Le daemon xinetd va passer pour le wrapper au lieu d'activer directement le service.
- Xinetd va lancer le daemon de Wrapper (**TCPD**) qui va se charger des contrôles et de vérifier les mécanismes de contrôle mis en place.



## 6-4 LES WRAPPERS

- On va pouvoir utiliser 2 fichiers: **/etc/hosts.allow et /etc/hosts.deny** pour filtrer les accès à sa machine.
  - **/etc/hosts.deny**: on indique dans ce fichier les services et les hôtes pour lesquels l'accès est interdit.
  - **/etc/hosts.allow**: on indique dans ce fichier les services et les hôtes pour lesquels l'accès est autorisé.
- Principe de fonctionnement : « *si c'est autorisé, c'est autorisé. Si c'est interdit, c'est interdit. Si ce n'est pas interdit, c'est autorisé* ».
- La stratégie la plus sûre : « *Interdire tout et autorisé explicitement ( relation service / clients)* ».



## 6-4 LES WRAPPERS

```
# /etc/hosts.allow
vsftpd: 192.168.1.
in.telnetd, portmap: poste1, poste2

# /etc/hosts.deny
ALL : .hacker.org except white-hacker.org
vsftpd,in.telnetd,portmap : ALL
dovecot : 192.168.0. EXCEPT 192.168.1.5
```

## AUTORISATION / INTERDICTION TCP-WRAPPER

Syntaxe au sein des fichiers **/etc/hosts.allow** et **/etc/hosts.deny**

**daemon\_list : client\_list [:options]**

- **daemon\_list** : liste des exécutables (PAS DES SERVICES) séparés par des virgules. Vous pouvez mettre ALL pour spécifier tous les services.
- **client\_list** : clients autorisés ou interdits pour ce service. On peut spécifier l'adresse IP, le nom, le masque de réseau, le nom du réseau, etc.
- **La client\_list admet une syntaxe particulière :**
  1. ALL : correspondance systématique.
  2. LOCAL : tous les hôtes dont le nom ne contient pas de point (poste1, poste2, etc.).
  3. UNKNOWN : hôtes dont le nom ne peut pas être résolu.
  4. KNOWN : hôtes dont le nom peut être résolu.
  5. PARANOID : hôtes dont le nom ne peut être résolu ou dont l'IP n'a pas de résolution inverse.
  6. EXCEPT : permet d'exclure certains hôtes.

## 8 – LES FONDAMENTAUX DE LA SECURITE.



## **8 – LES FONDAMENTAUX DE LA SÉCURITÉ.**

***8-1. Les bases de la sécurité.***

***8-2. Sécurité des services et du réseau .***

## 8-I – LES BASES DE LA SÉCURITÉ

**Les objectifs principaux de la sécurité informatique concernent :**

- **La sécurité de la connexion** : il s'agit de contrôler que les utilisateurs qui se connectent sont bien autorisés à le faire et de leur interdire l'accès au système dans le cas contraire.
- **L'intégrité des données** : il s'agit de faire en sorte que les fichiers et les bases de données ne soient pas corrompus et de maintenir la cohérence entre les données.
- **La confidentialité des données** : l'accès aux données en consultation et en modification doit être limité aux seuls utilisateurs autorisés.

## 8-I – LES BASES DE LA SÉCURITÉ

**Il existe plusieurs moyens pour réduire les risques liés à la sécurité (1/2):**

- L'authentification des utilisateurs par un mot de passe.
- Le cryptage des données.
- La sécurité physique en contrôlant l'accès des personnes aux salles informatiques, en utilisant des circuits inviolables matériellement.
- L'information sur les risques pénaux encourus en cas d'infraction. Un « braquage » informatique est un délit, pas un jeu.
- Le contrôle fréquent des droits d'accès aux fichiers et aux bases de données.
- Le contrôle des « checksum » des fichiers pour s'assurer de leur intégrité.
- La sauvegarde régulière des données.
- L'audit des principaux évènements du système.

## 8-I – LES BASES DE LA SÉCURITÉ

**Il existe plusieurs moyens pour réduire les risques liés à la sécurité (2/2) :**

- L'installation de murs de feu « firewall » qui contrôlent les accès au système informatique depuis l'extérieur et limitent l'accès à des services externes par des utilisateurs non avertis ou qui n'en ont pas besoin pour, par exemple, limiter le risque de rapatriement de virus.
- L'installation d'un antivirus, même sous Linux, si le serveur traite des données depuis et vers des systèmes d'exploitation concernés par les virus.
- L'installation d'outils antispams et antispywares, selon le même principe, afin d'éviter une intrusion et la saturation des serveurs de courrier électronique.
- Le démarrage uniquement des services réellement utiles sur le serveur et sur le client.