LINUX

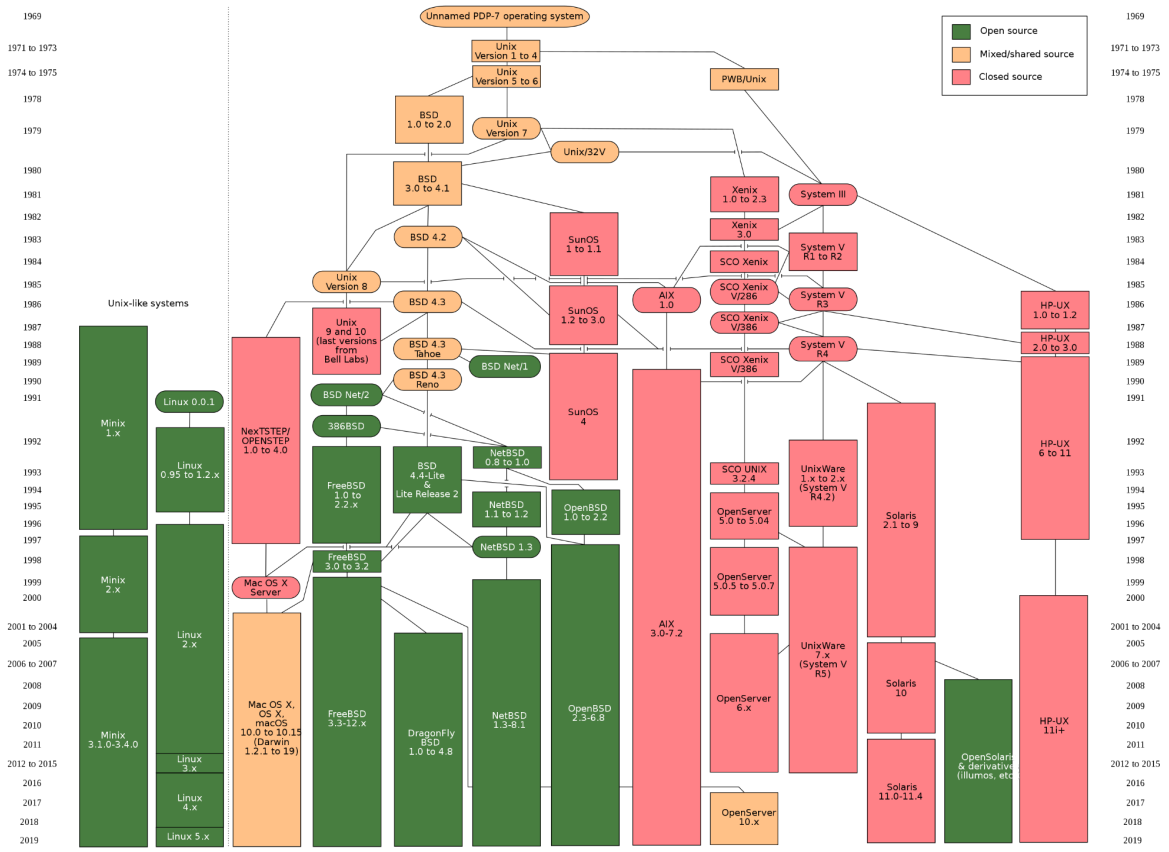
Gestion de la machine

Table des matières

Les descendants de UNIX et LINUX

UNIX

- [Unix-like - Wikipedia]



LINUX

Veuillez cliquer sur les liens ci-dessous

- [Linux — Wikipédia]
- [https://upload.wikimedia.org/wikipedia/commons/1/1b/Linux_Distribution_Timeline.svg]

Installation distribution LINUX

WSL: Windows Subsystem fot Linux

- Windows Subsystem for Linux Documentation
- FAQ's about Windows Subsystem for Linux
- What is WSL? — Whitewater Foundry.
- Whats the difference between Unix, Linux and Ubuntu?
- Ubuntu on WSL 2 Is Generally Available
- 1.1. What is Ubuntu?
- Tuto: Linux dans Windows 10
-

Machine Virtuel

User Manual
Chapter 2. Installation Details

sur Windows
sur MacOS

- Procédure
    - Installer VirtualBox
    - Télécharger Debian
    - Créer une machine virtuelle avec VirtualBox
    - Définir les différentes mémoires
    - Lier l'image Debian à la nouvelle machine virtuelle
    - Lancer la machine virtuelle
    - Créer partition cryptée (ou pas)
    - Installer le bootloader GRUB (Grub - Debian Wiki)

Boot

a booter au démarrage d'un PC

Présentation du système LINUX

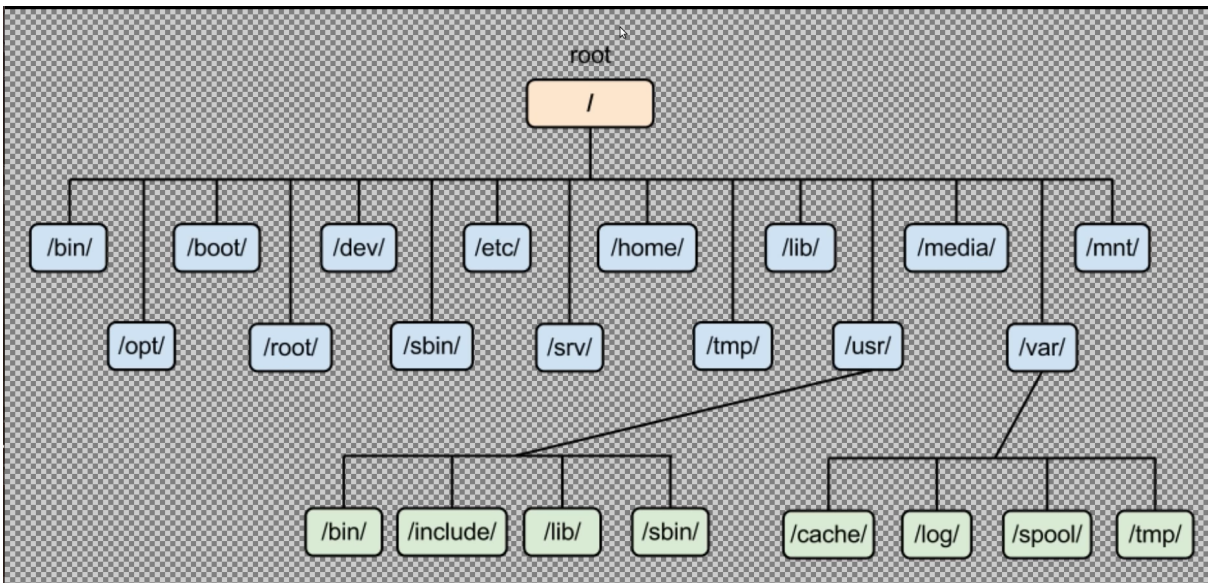
Système de fichier

Introduction:

Attention: l'arborescence de fichier sur LINUX est complètement différent de WINDOWS

- Sur WINDOWS:
  - Le niveau le plus bas pour stocker des données se trouve au niveau du disque dur (ou autre support physique).
  - Exemple:
    - C: → Disque dur
    - D: → Carte SD
    - E: → Clé USB
    - A: → Lecteur de disquette
  - Pour chaque support de stockage, il peut y avoir un nouvel arbre de fichier-dossier
  - Toute l'arborescence de fichier-dossier tourne autour des différents supports de stockage.

- Sur LINUX
  - Le niveau le plus bas de stockage se trouve être le dossier `root` qui est représenté par le symbole `/`.
  - Il existe qu'un seul arbre de fichier-dossier sur LINUX
  - Ce seul arbre fichier-dossier part du dossier `root` .
  - Peu importe le nombre de disques durs, chaque dossier ou fichier a comme racine le dossier `root` .
  - LINUX est capable de considérer plusieurs disque-durs comme n'étant qu'un seul.
  - Il faudra configurer cette mécanique avec les commandes:
    - `fdisk` → Manipulation of disk partition table
    - `lvm` → Logical Volume Manager



[Learning the Linux File System]

Le dossier racine

[The Linux Directory Structure, Explained]
[Le système de fichier de LINUX].
[What Is a Linux Swap Partition? Everything You Need to Know]

La racine root est composé de dossier essentiel au fonctionnement de linux:

/	Le répertoire racine
/bin	Fichiers binaires utilisateur essentiels
/boot	Fichiers de démarrage statiques
/cdrom	Point de montage historique pour les CD-ROM
/dev	Fichiers de périphérique
/etc	Fichiers de configuration
/home	Dossiers Accueil
/lib	Bibliothèques partagées essentielles
/lost + found	Fichiers récupérés
/media	Média amovible
/mnt	Points de montage temporaires
/opt	Packages optionnels
/proc	Fichiers noyau et processus
/run	Fichiers d'état de l'application
/sbin	Fichiers binaires d'administration système
/selinux	Système de fichiers virtuel SELinux
/srv	Données de service
/tmp	Fichiers temporaires
/usr	Fichiers binaires utilisateur et données en lecture seule
/var	Fichiers de données variables

Disque dur et Partition

LVM | Logical Volume Management | Combining Drives Together

Introduction:

- Dans l'histoire, le disque-dur a eu différent type d'interface de connexion avec la carte-mère:
  - IDE en 1986
  - SCSI en 1986 aussi
  - SATA en 2003

- Sur linux, la dénomination d'un disque-dur a un nom précis, selon son type d'interfaçage:
  - SATA/SCSI:
    - `/dev/sda` → disque-dur no.1
    - `/dev/sdb` → disque-dur no.2
    - `/dev/sdc` → disque-dur no.3
    - etc…
  - IDE:
    - `/dev/hda` → disque-dur no.1
    - `/dev/hdb` → disque-dur no.2
    - `/dev/hdc` → disque-dur no.3
    - etc…
  - Virtual:
    - `/dev/vda` → disque-dur no.1
    - `/dev/vdb` → disque-dur no.2
    - `/dev/vdc` → disque-dur no.3
    - etc…

Installation:

- Vous devez installer un disque-dur dans votre machine

- Vous pouvez aussi vous entraîner sur un machine virtuelle

- **ATTENTION**: à ce moment là, LINUX détecte le matériel mais ne peut pas encore l'utiliser

Vérification

- Vous pouvez vérifier, si le nouveau disque dur est détecté par votre machine linux avec la commande:

`lsblk -a`	list block device = ???
`fdisk -l`	list disk partition

- **ATTENTION**: à ce moment là, LINUX détecte le matériel mais ne peut pas encore utiliser le disque pour stocker les informations

Partition

- Un disque-dur peut être divisé en plusieurs segments, qu'on appelle PARTITION.
- **ATTENTION**: LINUX ne travaille qu'avec les partitions d'un disque-dur. Il ne travaille pas avec le disque-dur lui-même
- Exemple:
  - Disque-dur → **`sda`**
    - partition no.1 → `sda`**`1`**
    - partition no.2 → `sda`**`2`**
    - partition no.3 → `sda`**`3`**
    - partition no.4 → `sda`**`4`**

Création de partition

[How To Create LVM in Linux | Logical Volume Manager | RHCSA Certification #17 | Tech Arkit | EX200]

- Il faut utiliser l'utilitaire **`fdisk`**
- En imaginant que le disque-dur à partitionner se nomme `/dev/`**`sdb`**:
  - `fdisk /dev/sdb`
  - **A COMPLéTER**

partition swap

[What Is a Linux Swap Partition? Everything You Need to Know]

`lvs`	Report information about Logical Volumes.
`lvdisplay`	
`vgs`	Report information about Volume Groups.
`vgdisplay`	
`pvs`	Report information about Physical Volumes.
`pvdisplay`	

LVM:

[LVM - Debian Wiki]
[Linux Partitions tutorial in details for beginners | Linux Tutorial #25]

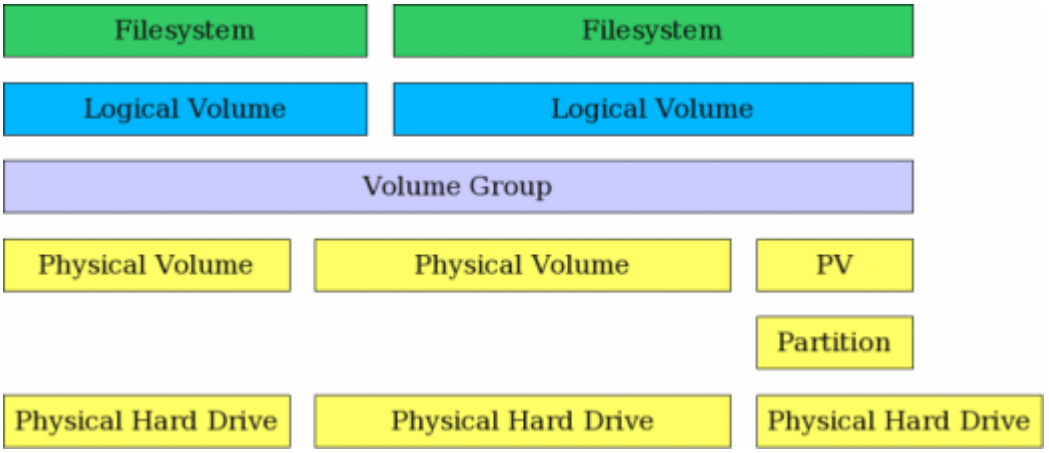
- `LVM` signifie `Logical Volume Manage`

- La gestion se fait sur 6 niveaux:
  - Niveau 6: Dossier System
  - Niveau 5: **L**V: Logical Volum
  - Niveau 4: V**G**: Volum Group
  - Niveau 3: **P**V: Physical Volum
  - Niveau 2: Partition de Disque Dur
  - Niveau 1: Disque Dur

Exemple 1:

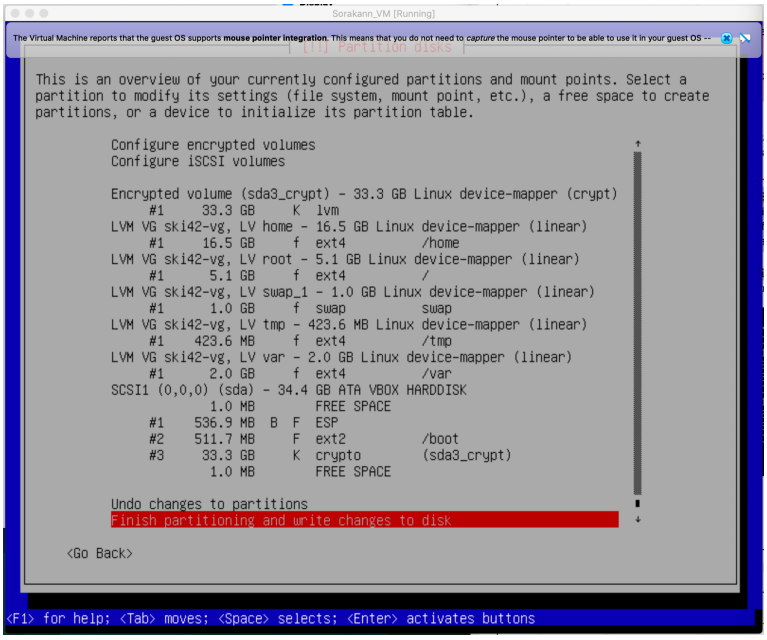
```
||------------------------OS---------------------------||
||------------------------LVM--------------------------||
||  LV-1 (/)    |LV-2 (swap)|  LV 3 (/home) | LV-4 (/tmp)|| Logical Volumes(LV)
||-----------------------------------------|------------||
||                 VG 1                    |    VG 2    || Volume Groups(VG)
||-----------------------------------------|------------||
||  /dev/sda2 |    /dev/sda3    | /dev/sdb2 | /dev/sdd4  || Physical Volumes(PV)
||-----------------------------------------------------||
```

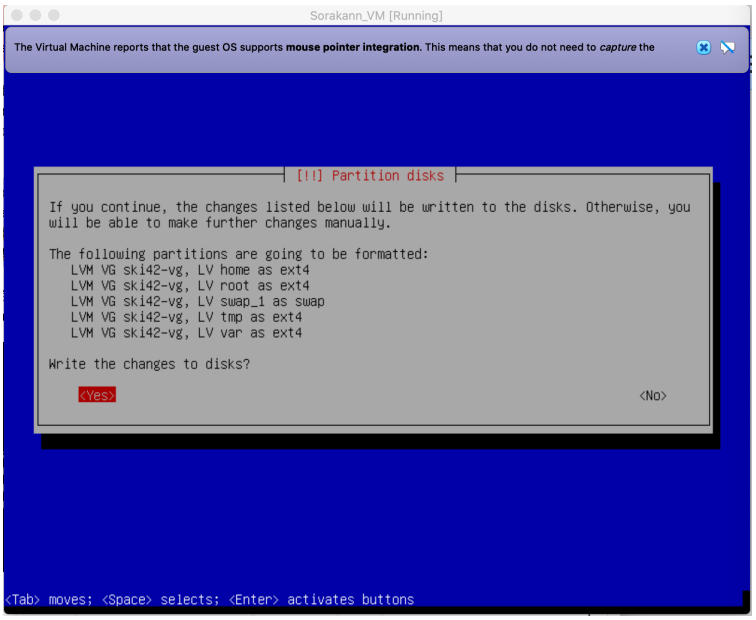
Exemple 2:



Pendant la 1ère installation de debian

Exemple de résultat de partition part LVM durant l’installation de Debian





La gestion (après la 1ère installation de debian)

[A Linux user's guide to Logical Volume Management | Opensource.com]

- `lvm` est une commande qui contient d'autre commande utile pour gérer les:
  - Niveau 3: **L**V: Logical Volum
  - Niveau 2: V**G**: Volum Group
  - Niveau 1: **P**V: Physical Volum

Commande - Niveau 3 - Logical Volume

`lvchange`	Change attributes of a Logical Volume.
`lvconvert`	Convert a Logical Volume from linear to mirror or snapshot.
`lvcreate`	Create a Logical Volume in an existing Volume Group.
`lvdisplay`	Display attributes of a Logical Volume.
`lvextend`	Extend the size of a Logical Volume.
`lvmconfig`	Display the configuration information after loading lvm.conf(5) and any other configuration files.
`lvmdiskscan`	Scan for all devices visible to LVM2.
`lvmdump`	Create lvm2 information dumps for diagnostic purposes.
`lvreduce`	Reduce the size of a Logical Volume.
`lvremove`	Remove a Logical Volume.
`lvrename`	Rename a Logical Volume.
`lvresize`	Resize a Logical Volume.
`lvs`	Report information about Logical Volumes.
`lvscan`	Scan (all disks) for Logical Volumes.

Commande - Niveau 2 - Volume Group

`vgcfgbackup`	Backup Volume Group descriptor area.
`vgcfgrestore`	Restore Volume Group descriptor area.
`vgchange`	Change attributes of a Volume Group.
`vgck`	Check Volume Group metadata.
`vgconvert`	Convert Volume Group metadata format.
`vgcreate`	Create a Volume Group.
`vgdisplay`	Display attributes of Volume Groups.
`vgexport`	Make volume Groups unknown to the system.
`vgextend`	Add Physical Volumes to a Volume Group.
`vgimport`	Make exported Volume Groups known to the system.
`vgimportclone`	Import and rename duplicated Volume Group (e.g. a hardware snapshot).
`vgmerge`	Merge two Volume Groups.
`vgmknodes`	Recreate Volume Group directory and Logical Volume special files
`vgreduce`	Reduce a Volume Group by removing one or more Physical Volumes.
`vgremove`	Remove a Volume Group.
`vgrename`	Rename a Volume Group.
`vgs`	Report information about Volume Groups.
`vgscan`	Scan all disks for Volume Groups.
`vgsplit`	Split a Volume Group into two, moving any logical volumes from one Volume Group to another by moving entire Physical Volumes.

Commande - Niveau 1 - Physical Volume

`pvchange`	Change attributes of a Physical Volume.
`pvck`	Check Physical Volume metadata.
`pvcreate`	Initialize a disk or partition for use by LVM.
`pvdisplay`	Display attributes of a Physical Volume.
`pvmove`	Move Physical Extents.
`pvremove`	Remove a Physical Volume.
`pvresize`	Resize a disk or partition in use by LVM2.
`pvs`	Report information about Physical Volumes.
`pvscan`	Scan all disks for Physical Volumes.

Creation de PV: Physical Volume

How To Create LVM in Linux | Logical Volume Manager | RHCSA Certification #17 | Tech Arkit | EX200

pvcreate <partition_name>
pvcreate /dev/sdb3

Création de VG: Volume Group

How To Create LVM in Linux | Logical Volume Manager | RHCSA Certification #17 | Tech Arkit | EX200

pvcreate <partition_name> <partition_name> <partition_name>
pvcreate /dev/sdb1 /dev/sdb2

Création de LV: logical Volume

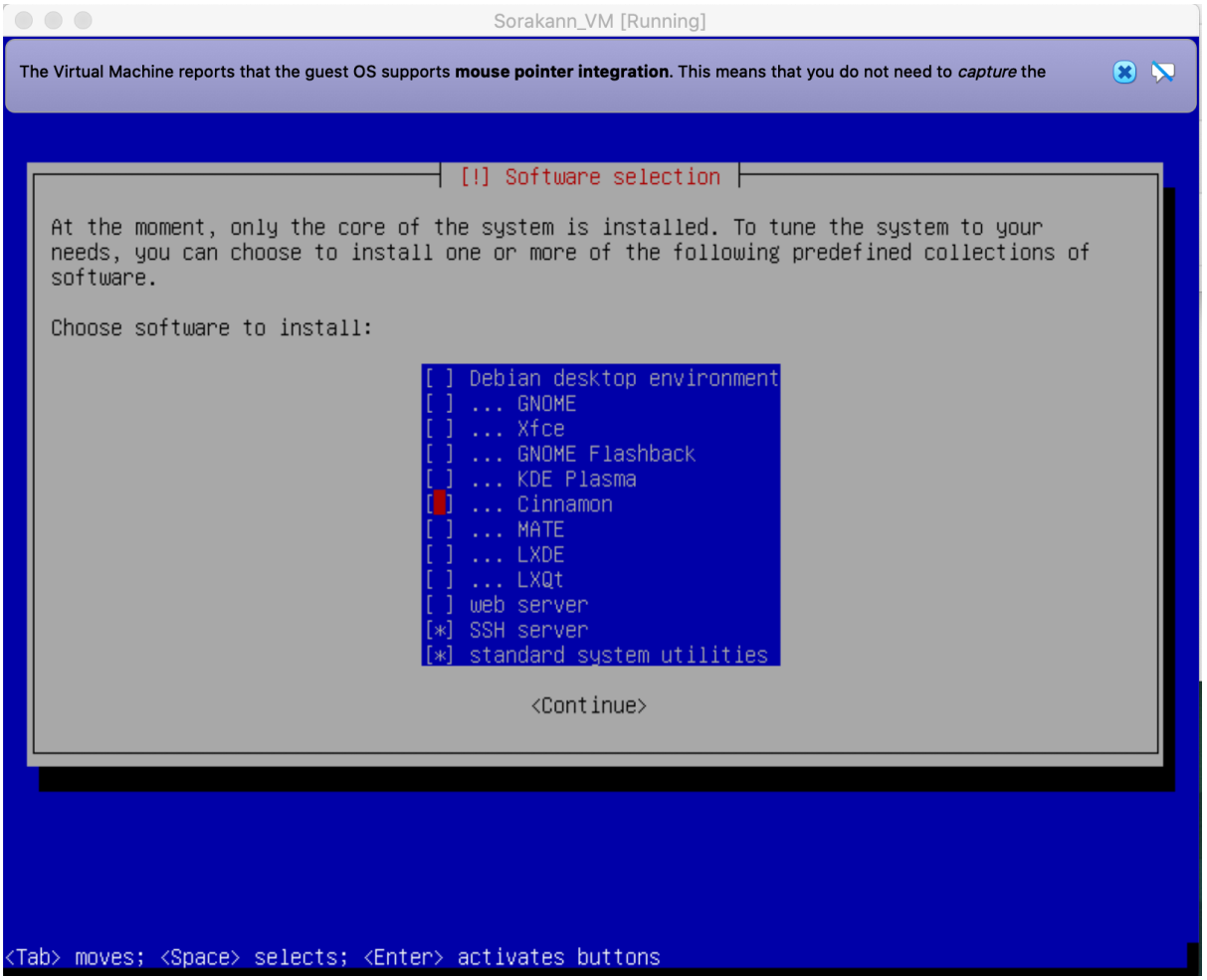
How To Create LVM in Linux | Logical Volume Manager | RHCSA Certification #17 | Tech Arkit | EX200
Linux mount an LVM volume / partition command - nixCraft

lvcreate **-n** <LV_name> **-L** <lv_size> <vg_name>
lvcreate **-n** lv_sorakann **-L** 50M sorakann_vg

lvmdiskscan

Task Selection

During the installation on Debian



After the 1st installation, you can still install the above software with the command tasksel ([tasksel - Debian Wiki]())

Les comptes-utilisateur dans Linux

Types of Users in Linux Explained with Accounts

Linux prévoit 3 type de comptes d'utilisateurs:

- ROOT (ou SUPER USER)
- REGULAR (ou NORMAL)
- SERVICE

ROOT user

- Compte utilisateur principal du système Linux.
- Créé lors de l'installation Linux
- Privilèges les plus élevés du système.
- Il peut effectuer toutes les tâches administratives et accéder à tous les services.
- A utiliser uniquement pour l'administration du système
- Il ne peut pas être supprimé.
- Mais si nécessaire, il peut être désactivé.

REGULAR user

- Utilisateur normal.
- Pendant l'installation, un compte d'utilisateur normal est créé automatiquement.
- Après installation de Linux, on peut créer autant de compte que l'on souhaite.
- Privilèges modérés.
- Pour travaux de routine.
- Il ne peut effectuer que les tâches pour lesquelles il est autorisé et ne peut accéder qu'aux fichiers et services pour lesquels il est autorisé.
- Selon les besoins, il peut être désactivé ou supprimé.

SERVICE user

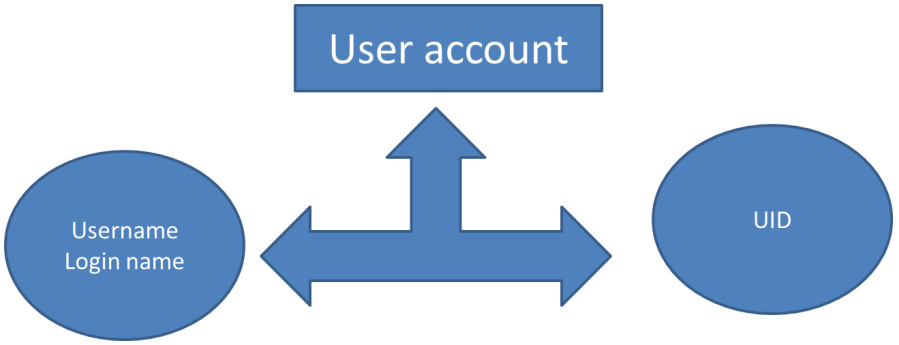
- Les comptes de service sont créés par les paquets d'installation lors de leur installation.
- Ces comptes sont utilisés par les services pour exécuter des processus et des fonctions.
- Ces comptes ne sont pas prévus et ne doivent pas être utilisés pour des travaux de routine.

Identifiant User

Un compteur user a toujours:

- **UID**:
    - User ID
    - (ne change jamais)
    - est utilisé par Linux

- **Username**
    - ou Login
    - il peut être modifié après coup
    - est utilisé par l'utilisateur



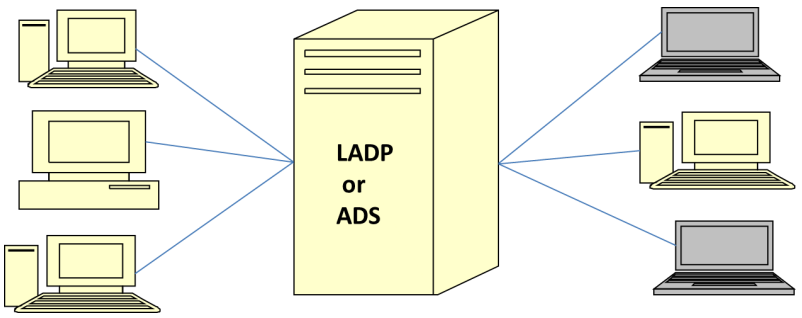
Gestion des comptes utilisateurs

Il éxiste 2 types de gestions de compte utilisateur:

- centralized
- standalone

Gestion centralisée des utilisateurs

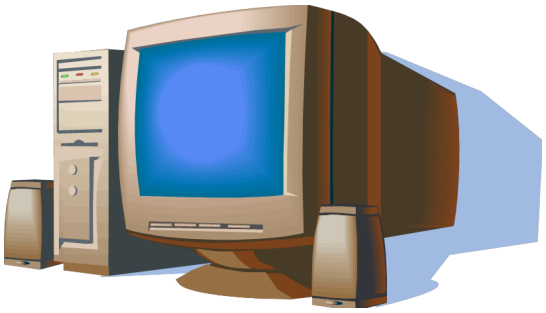
- Dans la gestion centralisée, les comptes utilisateurs de tous les systèmes sont gérés dans un système serveur centralisé.
- Dans le système serveur, un service d'annuaire tel que **LDAP** et **ADS** est utilisé pour la gestion et l'authentification des utilisateurs.



- Dans ce modèle, le système local envoie les informations de connexion de l'utilisateur au système serveur.
- Sur la base des informations stockées dans le service d'annuaire, le système serveur authentifie si l'utilisateur est autorisé à se connecter ou non.

Gestion autonome

- Dans la gestion autonome, les comptes des utilisateurs sont gérés dans le système local.
- Pour stocker les détails des comptes des utilisateurs, des fichiers texte sont utilisés.



Dans ce modèle, en fonction des informations de connexion stockées localement, le système local authentifie lui-même si l'utilisateur est autorisé à se connecter ou non.

Encore plus d’info sur:

[Types of Users in Linux Explained with Accounts]

La gestion des utilisateur

[How To Change User on Linux – devconnected]

Afficher la liste des utilisateurs

- La liste de tous les utilisateurs se trouvent dans le fichier `/etc/passwd`

```
cat /etc/passwd
```

- Chaque ligne dans le fichier `passwd` a le format suivant:

```
user_name:user_pswd:uuid:guid:commentaire:home:shell
```

user_name	login de l'utilisateur
user_pswd	mot de passe de l'utilisateur
uuid	identifiant système de l'utilisateur.
guid	groupe principal de l'utilisateur.
commentaire	commentaire textuel sur l'utilisateur qui est souvent son nom réél (Prénom et Nom).
home	répertoire home de l'utilisateur sur ce système
shell	interpréteur shell par défaut de l'utilisateur

Ajouter un nouvel utilisateur

- **Attention**: il faut être logué en tant que `root` (ou utilisateur avec droit `sudo`)
- Commande à utiliser:
  - `adduser` → user-friendly et recommandé
  - `useradd` → low-level utility
- Exemple:

```
adduser sorakann
```

- Le nouvel utilisateur sera créé selon les indications contenues dans le fichier:

```
/etc/default/useradd
```

- Le home du nouvel utilisateur aura le même squelette que le dossier suivant:

```
/etc/skel/
```

Supprimer un utilisateur

- **Attention**: il faut être logué en tant que `root` (ou utilisateur avec droit `sudo`)
- Commande à utiliser:
  - `deluser` → user-friendly et recommandé
  - `userdel` → low-level utility
- exemple:

```
deluser sorakann
```

- effacer l'utilisateur avec son dossier `home`:

```
deluser --remove-home username
```

Login ou Logout

- Chapitre à créer

- Il existe 3 commandes pour faire ça.
  - exit: à clarifier
  - logout: à clarifier
  - su

[Nohup and the difference between logout and exit on a remote shell - Super User]
[Linux Nohup Command]
[nohup - Wikipedia]
[SIGHUP - Wikipedia]

su : Switch User

[Utiliser la commande 'su' - Linux]

- Pour changer d'utilisateur, utilisez la commande `su`
- La commande `su` veut dire `Switch User`
- Exemple du format du commande:

```
su <option> <user>
```

- **ATTENTION**: En omettant le tiret-court dans la commande `su`, vous héritez des variables d'environnement du compte duquel vous provenez.
- La commande RECOMMANDE est:

```
su - <user>
```

La gestion des groupes

Un utilisateur ? Dans quel groupe est-il ?

groups	group memberships for the current user
groups *<username>*	group memberships for *<username>*

Un groupe ? Qui sont membres de ce groupe?

```
grep -i <group_name> /etc/group
```

Liste de tous les groupes et utilisateurs

- Se trouve dans le fichier de configuration `/etc/`**`group`**

`less /etc/`**`group`**	ou	`cat /etc/`**`group`**

- Chaque ligne dans ce fichier `/etc/`**`group`** a le format suivant:

```
group_name:group_pswd:gid:user_name1,user_name2,...
```

group_name	It is the name of group. If you run ls -l command, you will see this name printed in the group field.
group_pswd	Generally password is not used, hence it is empty/blank. It can store encrypted password. This is useful to implement privileged groups.
gid	Each user must be assigned a group ID. You can see this number in your `/etc/passwd` file.
user_name	User name of users who are members of the group. The user name must be separated by commas.

Autre commande:

- **Attention**: il faut être logué en tant que `root` (ou utilisateur avec droit `sudo`) pour exécuter les commandes ci-dessous:

usermod -aG <group> <user>	Ajouter un utilisateur à 1 groupe -a = --append -G = --group
adduser *<user> <group>*	Ajouter un utilisateur à 1 groupe
usermod -a -G <group1>,<group2> <user>	Ajouter un utilisateur à plusieurs groupe
Always use the -a (append) option when adding a user to a new group. If you omit the -a option, the user will be removed from any groups not listed after the -G option.	

- **Attention**: il faut être logué en tant que `root` (ou utilisateur avec droit `sudo`) pour exécuter les commandes ci-dessous:

gpasswd -d <user> <group>	Retirer un utilisateur d'un groupe
groupadd <group>	Créer un nouveau groupe
delgroup <group>	Supprimer un groupe

sudo

Introduction

- `sudo` veut dire `Super User DO`
- `sudo` est un programme (qui n'est pas toujours installé par défaut)
- `sudo` permet à un utilisateur d'exécuter des commandes avec des droits de SuperUser (= `root`)
- Si besoin, la commande **`visudo`** permet d'éditer le fichier **`/etc/sudoers`** pour gérer des règles spécifiques d'utilisation de la commande `sudo` par utilisateurs avec les droits de super user.

Installation

- **Attention**, il faut être logué en tant que `root`
- Installation de `sudo` (si besoin)

```
apt install sudo
ou
apt-get install sudo
```

Conférer les droits root à un utilisateur

- Il existe le groupe `sudo` sur linux
- Tous les utilisateurs faisant partie du group `sudo` ont les droits d'utiliser la commande `sudo` pour exécuter des commandes avec des droits de Su

```
usermod -aG sudo <user_name>
```

Passer au compte root directement

`sudo -s`	ou	`su -`

Configuration supplémentaire:

[10 Useful Sudoers Configurations for Setting 'sudo' in Linux]

- Il est possible de rajouter des règles supplémentaire à l'utilisateur qui a des droits `root`
- Pour modifier les droit sudo d'un utilisateur, il faut modifier le fichier → `/etc/sudoers` avec la commande → **`visudo`**
- Les règles supplémentaires doivent être rédigé dans le fichier `/etc/sudoers` et être précédé par le mot clé **`Defaults`**
- La commande **`visudo`** permet d'éviter des erreurs de rédaction

Les règles supplémentaire

`Defaults` **`passwd_tries`**`=`*`<number_of_try>`
nombre maximum d'essai avant qu'un message d'erreur s'affiche

`Defaults` **`badpass_message`**`="`*`<message>`*`"`
message d'erreur affiché après tous les essais d'introduction du mot de passe

`Defaults` **`logfile`**`="<custom_log_file>"`
 	
exemple:
`Defaults` **`logfile`**`="/var/log/sudo/sudo.log"`

Configure le fichier qui recevra le "journal" d'utilisation de la commande **`sudo`** Attention: il faut créer le dossier `/var/log/`**`sudo/`**qui contiendra le journal `sudo.log` si ce dossier n'existe pas

`Defaults` **`log_input,log_output`**
à clarifier: permet de journaliser les entrées et sorties de la commande `sudo`

`Defaults` **`requiretty`**
Permet d'activer le mode `tty`

`Defaults` **`secure_path`**`="`*`<path_to_guard>`*`"`
 	
exemple:
`Defaults` **`secure_path`**`="`*`/usr/local/sbin:/usr/local/bin:...`*`"`

à clarifier:

`Defaults` **`passwd_timeout`**`=`*`<min>`
Détermine le nombre de minutes sans activité, avant que l'utilisateur doit remettre son mot de passe pour ré-utiliser la commande `sudo`

Gestion de paquets d'outils

- `APT` veut dire *`Advanced Package Tool`*
    - Ces paquets sont des outils ou programmes à installer sur votre système.
    - Ces paquets sont à disposition sur un serveur.

- Pour installer et désinstaller des paquets sur votre système, il faut utiliser les programmes suivants:

    - `apt`
        - réponds à la majorité des cas d'usage
        - intègre des fonctions automatique
        - convient pour un débutant dans le monde linux

    - `apt-get`
        - nécessite une configuration plus lourde que apt

- **ATTENTION**: `apt` et `apt-get` sont 2 programmes différents

apt command	the command it replaces	function of the command
`apt` **`install`**	`apt-get` **`install`**	Installs a package
`apt` **`remove`**	`apt-get` **`remove`**	Removes a package
`apt` **`purge`**	`apt-get` **`purge`**	Removes package with configuration
`apt` **`update`**	`apt-get` **`update`**	Refreshes repository index
`apt` **`upgrade`**	`apt-get` **`upgrade`**	Upgrades all upgradable packages
`apt` **`autoremove`**	`apt-get` **`autoremove`**	Removes unwanted packages
`apt` **`full-upgrade`**	`apt-get` **`dist-upgrade`**	Upgrades packages with auto-handling of dependencies
`apt` **`search`**	`apt-cache` **`search`**	Searches for the program
`apt` **`show`**	`apt-cache` **`show`**	Shows package details

`apt` has a few commands of its own as well:

new apt command	function of the command
`apt` **`list`** `apt list` **`--upgradable`** `apt list` **`--installed`**	Lists packages with criteria (installed, upgradable etc)
`apt` **`edit-sources`**	Edits sources list

Combinaison de commande:

```
sudo apt update && sudo apt upgrade
```

UFW: le firewall

- `ufw` est un firewall
- `ufw` est un programme
- `ufw` veut dire `Uncomplicated FireWall`
- `ufw` permet de gérer les ports entrants pour des raisons de sécurité
- Pour gérer ces ports de communication, `ufw` a besoin de créer des règles.

Commande de base

`sudo apt install ufw`
installation de `ufw`

`sudo ufw` **`status`**	ou	`sudo ufw status` **`verbose`**
affiche le status `ufw` et les règle du		

`sudo ufw status` **`numbered`**
affiche le status `ufw` et les règle du `ufw` avec une numérotation

`sudo ufw` **`enable`**	`sudo ufw` **`disable`**
activation du firewall	désactivation du firewall

`sudo ufw` **`default deny incoming`**
refuse toutes communications entrantes

`sudo ufw` **`default allow outgoing`**
autorise toutes communications sortantes

Fichier de configuration

`/etc/default/ufw`

à enquêter

allow

`allow` permet de **créer** une règle pour autoriser une communication entrantes IP/TCP/UDP.

```
sudo ufw allow <port_number>
sudo ufw allow ssh    → ssh      peut être remplacé par    22
sudo ufw allow http   → http     peut être remplacé par    80
sudo ufw allow https  → https    peut être remplacé par    443
sudo ufw allow ftp    → ftp      peut être remplacé par    21
```

autorisation d'un seul port TCP/UDP entrant

```
sudo ufw allow 6000:6007/tcp
sudo ufw allow 6000:6007/udp
```

autorisation de plusieurs port TCP/UDP entrants

```
sudo ufw allow from <ip_address>
```

autorise la communication provenant de *<ip_address>*

```
sudo ufw allow from <ip_address> to any port <port_number>
```

autorise la communication provenant de *<ip_address>* avec le port spécifié *<port_number>* et rien d'autre

deny

`deny` permet de **créer** une règle pour bloquer une communication entrante IP/TCP/UDP.

La syntaxe est la même qu'avec `allow`, mais il faut remplacer `allow` avec `deny`.

delete

- `delete` permet de **supprimer** une règle créer avec `allow` ou `deny`.

- Format de la commande:

```
ufw delete allow <port_number>
ufw delete allow <port_number>/tcp
ufw delete allow <port_number>/udp
```

```
ufw delete deny <port_number>
ufw delete deny <port_number>/tcp
ufw delete deny <port_number>/udp
```

```
ufw delete <rule_number>
```

Communication SSH client-server

How to Enable SSH on Debian 9/10 | PhoenixNAP KB

Introduction

- `SSH` veut dire `Secure SHell` ou `Secure socket SHell`
- `SSH` est un protocole de communication sécurisé sur un réseau (internet) non sécurisé
- Il est possible de commander une machine linux depuis une autre machine linux dont leurs adresses IP seront différentes.
- Il faudra installer:
    - un serveur SSH sur la machine commandé
    - un client SSH sur la machine qui commande

A connaître lors de la connexion server-client

- Si le client et le serveur se trouve sur le **MÊME réseau**, il faut connaître:
    - l'adresse IP du serveur-SSH à commander
    - et le port TCP utilisé par le serveur-SSH (usuellement le TCP22)
- Si le client et le serveur se trouve sur des **réseaux DIFFÉRENTS**, il faut connaître:
    - l'adresse IP publique du routeur auquel le serveur-SSH est connecter
    - configurer plein de paramètres (port forwarding, etc…)
- Si le client et le serveur se trouve la **même machine**, il faut:
    - se renseigner sur l'adressse 127.0.0.1
    - et plein d'autre chose encore

Le serveur SSH

[How to Enable SSH on Debian 9/10 | PhoenixNAP KB]

`sudo apt install` **`openssh-server`**	Installer un server SSH
`sudo` **`systemctl status`** `ssh`	Vérifier l'activation
`sudo` **`service`** `ssh` **`start`**	Démarrer le ssh-server
`sudo` **`service`** `ssh` **`stop`**	Arrêter le ssh-server
`cat` **`/etc/ssh/sshd_config`**	Vérifier le port utilisé dans `sshd_config`
`grep -i port` **`/etc/ssh/sshd_config`**	Vérifier le port utilisé dans `sshd_config`

Reconfigurer le port du serveur-ssh

- Par défaut: **`22/tcp`**

- Marche à suivre:
  - Ouvrir le fichier de configuration du serveur: `/etc/ssh/`**`sshd_config`**
  - Enlever le symbole `#` → enlever le commentaire
  - Changer le numéro du port
  - Sauvegarder les modifications
  - Redémarrer le daemon `sshd`

    ```
    sudo systemctl restart sshd
    ```
  - Vérifier si le server-ssh écoute le nouveau port concerné

    ```
    sudo ss -tulpn | grep ssh
    ou
    sudo netstat -tulpn | grep ssh
    ```
  - Vérifier erreur de configuration du fichier

    ```
    sudo sshd -t
    ```

Dans une machine virtuelle:

- **ATTENTION:** configurer le port forwarding de la machine virtuelle
  [Easy way to SSH into VirtualBox machine | Any OS - DEV Community]

- Marche à suivre:
  - Ouvrir VirtualBox
  - Sélectionner la machine virtuelle
  - Puis: Settings → Network → Advanced → Port Forwarding

Empêcher une connection avec le login “root”

[Linux OpenSSH server deny root user access / log in - nixCraft]

- Ouvrir le fichier: `/etc/ssh/sshd_config`
- Configurer le paramètre: `PermitRootLogin no`
- Redémarrer le server: `systemctl restart sshd`

Le client-ssh

How to Enable SSH on Debian 9/10 | PhoenixNAP KB
Which is the most gentle way to end a ssh session [closed]

`sudo apt instal` **`openssh-client`**	Installation du client-SSH
`ssh` *`<user_name>@<ip_addr>`*	- LOGIN ou **Connection** à un serveur-SSH *- par défaut le port 22/tcp sera utilisé*

`logout`
ou
`exit`
	LOGOUT ou **Déconnection** du serveur-SSH

Si le port de connection est différent, vous pouvez le spécifier avec:

`ssh` **`-p`** **`<port>`** *`<user_name>@<ip_addr>`*	

Connection au serveur-ssh d'une machine virtuelle:

- Une machine hôte peut **contenir** une machine virtuel
- Une machine hôte peut **communiquer** avec une machine virtuel
- Cette communication se fait à l'aide d'une adresse IP spéciale
- Une machine virtuelle a l'adresse spéciale `127.0.0.1` aux yeux de la machine hôte
- Cette adresse `127.0.0.1` est accessible et connue QUE par la machine hôte.
  127.0.0.1 IP Address Explained
- Cette adresse `127.0.0.1` est appelé `loopback address` ou `localhost`

- Pour se connecter au server-ssh qui se trouve dans un machine virtuelle, il faut exécuter la commande suivante:

`ssh` *`<user_name>@`***`127.0.0.1`** ou `ssh` **`-p <port>`** *`<user_name>@`***`127.0.0.1`**
Attention: **`<port>`** doit être configuré dans le port forwarding de la machine virtuelle qui héberge le server-ssh

systemctl

Service (vs process vs daemon)

Difference between systemctl and service commands - Ask Ubuntu
daemon: **à clarifier**
service: **à clarifier**
process: **à clarifier**

systemctl

systemd - System and service manager in Linux - SoftPrayog
The systemctl command is used for controlling the systemd system and service manager.
Some of the commonly used variations of the systemctl command are,

Information sur les services

`systemctl` **`status`**	Show systemd status
`systemctl status` *`<unit-name>`*	Status for a unit If we skip extension , `.service` is assumed.

`systemctl` ou `systemctl` **`list-units`**	List running units
`systemctl` **`list-unit-files`**	List all installed unit files
`systemctl --failed`	List all failed units
`systemctl is-enabled <unit-name>`	Check whether a unit is enabled

`sudo systemctl` **`start`** *`<unit-name>`*	Start a unit
`sudo systemctl` **`stop`** *`<unit-name>`*	stop a unit
`sudo systemctl` **`restart`** *`<unit-name>`*	Restart a unit
`sudo systemctl` **`reload`** *`<unit-name>`*	Reload the configuration for a unit

Service qui démarre à chaque booting or rebooting

`sudo systemctl` **`enable`** *`<unit-name>`*	Enable a unit **to be started at boot**
`sudo systemctl` **`disable`** *`<unit-name>`*	Disable a unit

Masquage de service

`sudo systemctl` **`mask`** *`<unit-name>`*	Mask a unit so that it becomes impossible to start it
`sudo systemctl` **`unmask`** *`<unit-name>`*	Unmask a unit

apparmor

- `apparmor` permet à l'administrateur système d'associer **à chaque programme** un **profil de sécurité** qui restreint ses **accès au système d'exploitation**.

- Vérification de l'activité de `apparmor`:

`sudo` **`apparmor_status`**	
`sudo` **`systemctl status`** `apparmor`	

Hostname (= nom du pc)

[hostname command in Linux with examples - GeeksforGeeks]

Afficher le hostname

`cat /etc/`**`hostname`**	fichier avec le hostname
`hostname`	commande pour afficher le hostname

Changer le hostname

[Ubuntu Linux Change Hostname (computer name) - nixCraft]

Méthode 1: avec le fichier /etc/hostname

`sudo vim /etc/`**`hostname`**	remplacer l'ancien nom par un nouveau

`sudo vim /etc/`**`hosts`**	ATTENTION: remplacer les occurence de l'ancien nom avec le nouveau nom

`sudo` **`reboot`**	redémarrer le pc

Méthode 2: avec la commande hostnamectl

`hostnamectl` **`set-hostname`** `<new_name>`
Changer le nom du host

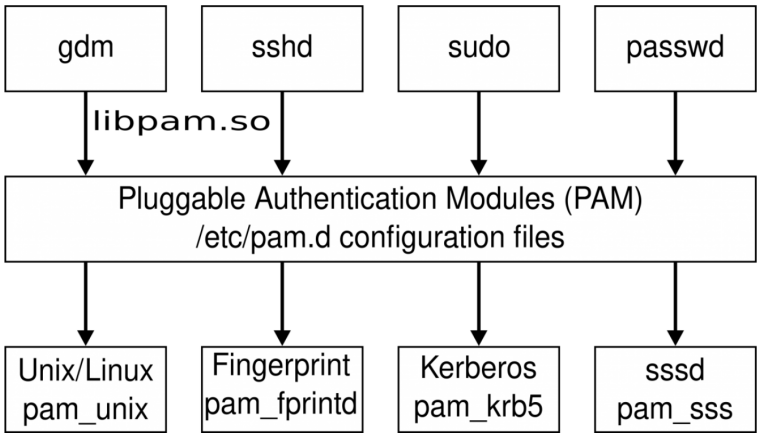
`sudo vim /etc/hosts`
ATTENTION: remplacer les occurence de l'ancien nom avec le nouveau nom

`sudo` **`reboot`**	redémarrer le pc

Gestion des mots de passe

Introduction au PAM: Pluggable Authentication Modules

[An introduction to Pluggable Authentication Modules (PAM) in Linux | Enable Sysadmin]



Changer le mode de passe

`sudo` **`passwd`** `root`	pour changer le mot de passe du `root`

Renforcer la sécurité des mots de passe.

Sécurité passwd - libpam-pwquality / Wiki / Debian-facile
PasswordManagement - Debian Wiki
Force Users To Use Strong Passwords In Debian And Ubuntu
Sécurité passwd - libpam-pwquality / Wiki / Debian-facile
Détails du paquet libpam-pwquality dans sid
Détails du paquet libpam-cracklib dans sid

Installation

Pour renforcer le code de sécurité, il faut utiliser le paquet: `libpam-pwquality`

```
apt update
```

```
apt install libpam-pwquality libpwquality-tools
```

Connaître ou changer l'utilitaire de gestion de mots de passe

```
pam-auth-update
```

Fichier à configurer

```
/etc/pam.d/common-password
```

Les règles de sécurité

MOTS-CLÉS	ACTION/DESCRIPTION
difok=N	Nombre de caractères du nouveau mot de passe qui ne sont pas présents dans l'ancien, par défaut difok=1
minlen=N	Taille minimum du nouveau mot de passe. Cependant un bonus d'un caractère en plus est rajouté si un type de caractères différent de plus est présent dans le mot de passe.
dcredit=N	Si dcredit < 0, dcredit est l'opposé du nombre minimum de chiffres dans le nouveau mot de passe, exemple si dcredit = -5, il faut au moins 5 chiffres dans le mot de passe.
ucredit=N	Si ucredit < 0, ucredit est l'opposé du nombre minimum de lettres majuscules dans le nouveau mot de passe, exemple si ucredit = -4, il faut au moins 4 lettres majuscules dans le mot de passe
lcredit=N	Si lcredit < 0, lcredit est l'opposé du nombre minimum de lettres minuscules dans le nouveau mot de passe, exemple si lcredit = -10, il faut au moins 10 lettres minuscules dans le mot de passe. Si lcredit > 0, alors le nombre de caractères minimum utilisé par le mot de passe diminue de minlen à (minlen - lcredit). (par défaut 0)
ocredit=N	Si ocredit < 0, ocredit est l'opposé du nombre minimum de caractères spéciaux dans le nouveau mot de passe, exemple si ocredit = -4, il faut au moins 4 caractères spéciaux dans le mot de passe. Si ocredit > 0, alors le nombre de caractères minimum utilisé par le mot de passe diminue de minlen à (minlen - ocredit). (par défaut 0)
minclass=N	Le nombre minimum de types de caractères requis pour le nouveau mot de passe (chiffres, majuscules, minuscules, autres). (par défaut 0)
maxrepeat=N	Si maxrepeat=N, alors un caractère ne pourra pas être présent plus de N fois
maxclassrepeat=N	Rejete les mots de passe contenant plus de N caractères consécutifs du même type. La valeur par défaut est 0, ce qui signifie que la vérification est désactivée
gecoscheck=N	Si différent de zéro, vérifie si les mots de plus de 3 caractères des champs GECOS du mot de passe de l'utilisateur sont contenues dans le nouveau mot de passe. Cette vérification n'est pas effectuée si gecoscheck=0, qui est aussi la valeur par défaut. On peut avoir une idée rapide de ce que sont les champs GECOS en tapant : chfn --help
dictcheck=N	Si dictchech est différent de 0, vérifie si le mot de passe est présent dans le dictionnaire cracklib des mots de passe trop courants. Si l'on veut créer son propre dictionnaire des mots à bannir comme mot de passe, regarder et interpréter les résultats de la commande : find / -iname '*cracklib*' -print | grep dict
usercheck=N	Si usercheck est différent de 0, vérifie si le mot de passe contient le nom de l'utilisateur $USER. Cette vérification n'est pas effectuée pour les noms d'utilisateur de moins de 3 caractères.
usersubstr	à faire
enforcing=N	Si N=0, il ne sera pas tenu compte du reste des vérifications effectuées par les autres options, le mot de passe sera accepté quelque soit sa qualité, seulement un message d'avertissement sera émis. Si N différent de 0, un mot de passe qui échoue à remplir les conditions posées par les autres options est rejeté. C'est le comportement par défaut.
dictpath	Définit le choix du chemin dans l'arborescence (*PATH*) du dictionnaire des mots de passe bannis, par défaut, il s'agit du dictionnaire des mots de passe bannis fourni par l'outil gestionnaire de mot de passe cracklib. Pour savoir où est ce dictionnaire, interprétez les résultats de : find / -iname '*cracklib*' -print | grep dict

retry=N	Nombre maximum de tentatives ratées de connexion au compte
enforce_for_root	Cette option renverra une erreur en cas d'échec de la vérification même si l'utilisateur qui modifie le mot de passe est root. Cette option est désactivée par défaut, ce qui signifie que dans ce cas seul le message concernant l'échec de la vérification est affiché mais que root peut quand même changer le mot de passe. Pour la sécurité, il vaut mieux donc activer cette option. Notez qu'à root on ne demande pas un ancien mot de passe, donc les vérifications qui comparent l'ancien et le nouveau mot de passe ne seront pas effectuées.
local_users_only	à faire

Modifier les règles de sécurité

Les règles sont à rajouter dans le fichier `/etc/pam.d/`**`common-password`** dans la ligne suivante:

```
# here are the per-package modules (the "Primary" block)
password        requisite                       pam_pwquality.so retry=3
```

Gérer les informations d'expiration

Linux Check User Password Expiration Date and Time - nixCraft

Visualiser toutes les information d'expiration

Méthode 1: (pas compréhensible)

```
sudo cat /etc/shadow
```

Méthode 2: (lisible)

`chage -l <username>`
chage → commande pour manipuler les informations d'expiration du mot de passe **-l** → pour afficher les informations

Modifier les informations d'expiration

- **Attention**: la validité du mot de passe et du compte utilisateur sont 2 choses différentes

voir /etc/login.defs

Durée MAXIMUM pour garder le même mot de passe

`sudo chage -M <day> <user>`	-
`sudo chage -M -1 <user>`	Aucune durée maximum

Durée MINIMUM avant de pouvoir changer le mot de passe

`sudo chage -m <day> <user>`	-
`sudo chage -m 0 <user>`	changement du mot de passe sans contrainte

Date d'expiration FINALE d'utilisation du mots de passe

`sudo chage -E <date> <user>`	format YYYY-MM-DD
`sudo chage -E <day> <user>`	nombre de jours après le 1er janvier 1970

`sudo chage -E -1 <user>`	AUCUNE expiration pour l'utilisation du mdp
`sudo chage -E 0 <user>`	BLOQUE de facto l'utilisation du mdp

Avertissement déclenché un jour avant le jour ou date d'expiration:

`sudo chage -W <day> <user>`	

Bloquer ou Autoriser l'utilisation du mot de passe

`sudo passwd -l <user>`	lock
`sudo passwd -u <user>`	unlock

Lock and Unlock un compte utilisateur

[Three Ways to Lock and Unlock User Account in Linux | 2DayGeek]

- **Attention**: à ne pas confondre avec le bloquage et l'autorisation d'utilisation du mot de passe utilisateur

Le journal ou SysLog

Veuillez lire le lien suivant: [syslog : Les journaux système sous Linux - Wiki]

Script exécuter à intervalle régulier

[How To Add Jobs To cron Under Linux or UNIX - nixCraft]
[https://github.com/HEADLIGHTER/Born2BeRoot-42/blob/main/monitoring.sh]

Introduction

- Pour exécuter une commande ou un script automatique à intervalle régulier sur une machine linux, on peut utiliser le service (ou daemon) `cron`
- La commande `crontab` signifie "chronology table"
- La commande `crontab -e` permet de configurer et spécifier le fonctionnement du service `cron` pour chaque utilisateur.
- Le service `cron` lit régulièrement les fichiers et dossiers :

`/etc/`**`crontab`**	→ fichier
`/etc/`**`cron.d`**	→ dossier
`/etc/`**`cron.daily`**	→ dossier
`/etc/`**`cron.hourly`**	→ dossier
`/etc/`**`cron.monthly`**	→ dossier
`/etc/`**`cron.weekly`**	→ dossier
`/var/spool/cron/`	**`crontabs`** → fichier analysé, mais pas accessible

La commande `crontab`

`crontab` **`-e`**	pour définir la fréquence ou périodicité et inscrire les commandes (à exécuter périodiquement)
`crontab` **`-l`**	pour afficher les commandes (exécutées périodiquement)
`crontab` **`-r`**	pour supprimer les commandes (à exécuter périodiquement)
`crontab` **`-ir`**	comme `crontab` **`-r`** avec demande de confirmation

Configuration:

`<mm> <hh> <day_of_month> <month> <day_of_week> <command>`
Chaque variable de temps doit être écrit avec 2 digits

Exemple 1:

`01 * * * * echo bonjour`
La commande `echo bonjour` sera exécuté à chaque fois que l'horloge indiquera la minute `01` de n'importe quel heure

Exemple 2:

`*/7 * * * * echo bonjour`
La commande `echo bonjour` sera exécuté chaque **`7`** minute

Exemple 3:

`*/7 * * * sun echo bonjour`
La commande `echo bonjour` sera exécuté chaque **`7`** minute chaque dimanche

Autre exemple:

De multiple combinaison sont encore possible

Fichier de log

`/var/log/syslog`
ou
`/var/log/cron`

Information système

Info générale

`uname -a`	affiche les informations système
`hwinfo -- short`	affiche le hardware

CPU

`/proc/`**`cpuinfo`**	fichier qui contient les infos sur le cpu
`lscpu`	affiche les infos sur le cpu
`arch`	affiche l'architecture
`nproc`	affiche le nombre de processeur

How to check how many CPUs are there in Linux system - nixCraft
How to Display the Number of Processors (vCPU) on Linux VPS

Process

`top`	affiche les processus LINUX

Mémoire

`/proc/`**`meminfo`**	Fichier qui contient les infos sur la mémoire
`free` `-m`	affiche la quantité de RAM libre/utilisé
`df`	affiche l'espace uitilsé dans le dique-dur
`df -Bg`	
`df -Bm`	
`lsblk`	affiche les partitions et les logical-volums de LINUX

Réseau

`/proc/net/`**`sockstat`**
fichier avec les infos des sockets, des ports TCP et des ports UDP, etc…

/etc/network/**interfaces**

`ss`
affiche les infos des sockets, des ports TCP et UDP

Utilisateur

`who`	commande qui indique qui est logué sur la machine
`users`	similaire à la commande `who`

Server Web

What is a Web Server and How Does it Work?

Wordpress: How To Install WordPress On Debian 9 With LAMP (Tutorial) | Serverwise

Ligthttpd: WebServers - Debian Wiki
Installing & Configuring Lighttpd Web Server on Ubuntu 15.04

Snapshot sur une VM

How to use snapshots in VirtualBox - TechRepublic
VirtualBox 4 - Using Snapshots.

Autre fonction

Signature d'un disque dur

ZSH and ohmyzsh

- How to Install Oh My Zsh in Ubuntu 20.04
- How to Install and Setup Zsh in Ubuntu 20.04
-

Lien internet utile

- Lister les utilisateurs - Linux
- How to Add and Delete Users on Debian 9 | Linuxize
- Understanding the /etc/skel directory in Linux – The Geek Diary

- How to Add User to Group in Linux
- How To Change User on Linux – devconnected
- Understanding /etc/group File - nixCraft
- Unix/Linux Privilege Management: Should You Sudo? Here's What It Does and Why It's Not Enough | BeyondTrust
- How do I update Ubuntu using terminal command line

- Difference Between apt and apt-get Explained - It's FOSS
- Uncomplicated Firewall (ufw) - Debian Wiki