

CAISSE A OUTILS LINUXIENNE

Kit de secours

RESUME

Présentation de Linux et plusieurs actions pour paramétrer son environnement

Donat FUZELLIER

Table des matières

- Côté Cours	6
Au départ était UNIX,	6
Alors qu'est-ce que linux	7
Les partitions Linux et autres	9
Quel type de partition choisir ?	10
Primaire et logique	10
Adressage matériel	11
Adressage par UUID	11
Affectation et format des partitions	12
Quel format choisir ?	12
Quelle distribution ?	13
SystemD est une alternative très intéressante à Init. Pourquoi ?	14
Comment utiliser ce document ? :	15
Raccourci clavier pour faire le signe dièse (#) sur PC	15
Quelle différence entre les deux ?	15
Comment faire le symbole dièse « croisillon » (réseaux sociaux et écriture web) sur PC	15
Sur clavier Azerty	15
Sur clavier Qwerty	15
Touche dièse sur Mac	15
Comment faire le symbole dièse musical (Sharp key = #) sur PC ?	15
Comment faire ce symbole en HTML :	16
Réinitialiser le mot de passe Root d'un Debian	18
Pré-requis	18
NANO	22
Ajouter sudo	23
Installation de sudo	23
Configuration de base de sudo	23
- Résolution DNS	25
avec resolvconf	25
Sources.list	26
Exemple de Fichier sources.list	26
Modification du sources.list	26

Installer la commande locate.	27
Vérifier les informations permettant la résolution DNS	27
Modification de fichier resolv.conf	27
Redémarrer le réseau	28
Obtenir des informations sur le statut du système	30
Afficher le statut du système :	30
Lister les unités échouées :	30
Lister les fichiers unités installés :	30
Pour connaître son système de démarrage, taper :	30
Vérifier et activer rc.local au démarrage	30
tty	30
getty	31
Créer une session avec SCREEN	32
PERSONNALISATION	32
IOTOP panneau d'information HardWare	32
commande htop	32
Edition de l'interface	33
Copie de sauvegarde d'un fichier	33
Test de l'accès au WAN et de la résolution DNS	33
Afficher la realese	34
# apt-cache search --names-only	34
Voir les logs :	34
Vérifier les ports	34
La commande host	34
Mise à jour	35
Changer le hostname de votre debian	35
Voir les paramètres	36
Ou placer les scripts	36
Gestion des services Debian ponctuellement	37
Désactiver le service du démarrage	37
Supprimer les fichiers	37
Compression TAR	37
Taille d'un dossier	37

Trouver les fichiers contenant une chaîne de caractère.....	38
Supprimer des .SVN (serveur subversion)	38
vider les .logs	38
Pour vider un fichier sous Unix ou linux, il faut effectuer cette manipulation :	38
Comment utiliser la commande IP sur Linux	38
10 commandes "IP" utiles pour configurer les interfaces réseau sur Linux.....	39
Autoriser la connexion en ssh	43
Connexion depuis Windows	43
Pour Installer SSH	44
Installation de SSH.....	44
Installez openSSH client.....	44
Installez openSSH server	44
Autoriser root en ssh	44
Les clés SSH	45
Authentification par clé.....	46
Générer ses clés	46
Autoriser votre clé publique.....	47
Connexion sur le port SSH (22)	47
Configuration SSH.....	47
Notions et paramétrages des droits	48
Les droits en 777 C'est le MAL !!!!.....	48
En OCTAL.....	50
À qui s'applique, le changement	50
La modification que l'on veut faire	50
Le droit que l'on veut modifier	50
Modification du groupe primaire d'un utilisateur	51
Ajout d'un groupe secondaire à un utilisateur existant.....	51
Ajout d'un nouvel utilisateur à un groupe primaire	51
Ajout d'un nouvel utilisateur à un groupe secondaire.....	51
Vérifier les groupes associés à un utilisateur.....	52
Autorisations diverses	52
adduser : gestion des utilisateurs.....	52
passwd : changer le mot de passe	53

deluser : supprimer un compte	53
addgroup : gestion des groupes	54
addgroup : créer un groupe	54
usermod : modifier un utilisateur.....	54
delgroup : supprimer un groupe	54
chown : changer le propriétaire d'un fichier	55
l'option -R de chown.	55
chgrp : changer le groupe propriétaire d'un fichier.....	56
Exemple : Donner des droits spécifiques ftp.	56
Notation symbolique.....	57
Notation numérique.....	58
Remarques importantes.....	58
Exécutable	58
Répertoire	58
Fichier.....	58
Masque de protection des fichiers (umask)	58
Manipulation	59
Remarque.....	59
Droits étendus	60
SUID.....	60
Exemple.....	60
Manipulation	60
Notation numérique	60
SGID.....	61
Exécutable	61
Répertoire	61
Manipulation	61
Sticky Bit	62
Travail sur les partitions	63
le programme di	63
Vérifier l'espace disque sous une Debian	63
La commande df.....	63
Ajout d'un disque supplémentaire	64

Créer une partition	65
Supprimer une partition	65
Vérification des partitions des lecteurs	67
À quel système de fichiers appartient un fichier.	69
Liste les différents disques et le nombre de blocs.	69
Liste les partitions du système.	69
Affiche toutes les partitions.	69
Vérifier la configuration des disques.	69
NOTA BENE :	70

- Côté Cours

Afin de comprendre un peu mieux linux, il nous faut faire un peu d'histoire de l'informatique.

On a pour habitude de parler de Linux comme étant un système d'exploitation.

En réalité, Linux, est uniquement le cœur (on dit le "noyau" ou "kernel") du système d'exploitation GNU/Linux.

(Les systèmes d'exploitation Microsoft Windows NT, 2000 et XP ont également un noyau, mais différent, c'est le noyau NT. En version 6.3 pour Windows 8.1, 6.2 pour Windows 8 et 6.1 pour Windows 7 et 10.0 pour Windows 10)

Source : <https://fr.wikipedia.org/wiki/Linux>

GNU/Linux est le nom parfois donné à un système d'exploitation associant des éléments essentiels du projet GNU et d'un noyau Linux.

C'est une terminologie créée par le projet Debian et reprise notamment par Richard Stallman, à l'origine du projet de travail collaboratif GNU, lequel manquait encore d'un noyau de système d'exploitation pour en faire un système d'exploitation complet lors de la création du noyau Linux, en 1991. Des systèmes complets prêts à l'emploi, réunissant les deux pièces, sont alors apparus, comme la distribution Debian.

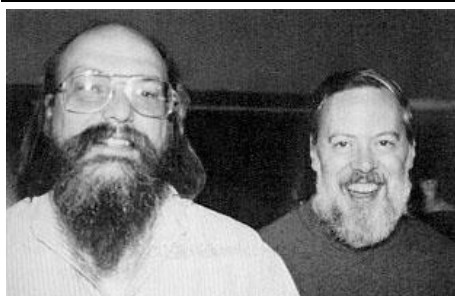
Ce qui peut porter à confusion étant donné qu'il existe quelques systèmes fondés sur Linux mais pas sur GNU

(par exemple : Android, ceci lui permettant d'éviter certaines clauses de la licence GNU).

Au départ était UNIX,

Unix, officiellement UNIX (parfois écrit « Unix », avec des petites capitales), est un système d'exploitation multitâche et multiutilisateur créé en 1969 par Kenneth Thompson et Dennis Ritchie.

Source : https://fr.wikipedia.org/wiki/Ken_Thompson



Ken Thompson (né Kenneth Lane Thompson le 4 février 1943 à La Nouvelle-Orléans) est un informaticien américain, concepteur des systèmes UNIX et Plan 9 ainsi que des langages B et Go.

https://fr.wikipedia.org/wiki/Dennis_Ritchie

Dennis MacAlister Ritchie, né le 9 septembre 1941 à Bronxville dans l'État de New York et trouvé mort le 12 octobre 2011 à Berkeley Heights dans le New Jersey, est un des pionniers de l'informatique moderne, inventeur du langage C et codéveloppeur de Unix. Il est parfois désigné par dmr, son adresse électronique aux Laboratoires Bell.

Il repose sur un interpréteur ou superviseur (le shell) et de nombreux petits utilitaires, accomplissant chacun une action spécifique, commutable entre eux (mécanisme de « redirection ») et appelée depuis la ligne de commande¹.

Particulièrement répandu dans les milieux universitaires au début des années 1980, il a été utilisé par beaucoup de start-up fondées par des jeunes entrepreneurs à cette époque et a donné naissance à une famille de systèmes, dont les plus populaires à ce jour sont les variantes de BSD (notamment FreeBSD, NetBSD et OpenBSD), GNU/Linux, iOS et OS X. On nomme « famille Unix », systèmes de type Unix ou simplement systèmes Unix l'ensemble de ces systèmes. Il existe un ensemble de standards réunis sous les normes POSIX et single UNIX spécification qui visent à unifier certains aspects de leur fonctionnement.

Le nom « UNIX » est une marque déposée de l'Open Group, qui autorise son utilisation pour tous les systèmes certifiés conformes à la single UNIX spécification ; cependant, il est courant d'appeler ainsi les systèmes de type Unix de façon générale. Il dérive de « Unics » (acronyme de « Uniplexed Information and Computing Service³ »), et est un jeu de mot avec « Multics », car contrairement à ce dernier qui visait à offrir simultanément plusieurs services à un ensemble d'utilisateurs, le système initial de Kenneth Thompson se voulait moins ambitieux et utilisable par une seule personne à la fois avec des outils réalisant une seule tâche.



Alors qu'est-ce que linux

Et bien, le noyau linux, a été crée par linux Torval, un Finlandais qui, lors de ses études, était amené à travailler sur le serveur UNIX de sa faculté. Cependant, l'accès a ce serveur étant difficile, il choisit de travailler sur minix une copie lite d'Unix, qui ressemblait à Unix, cependant, Linus Torvald souhaitait certaines modifications sur minix, par dépit, et ne voyant pas ses demandes d'ajout ou de modification, auprès du concepteur de minix, aboutir, il prit la décision de développer ses propres outils.

Ceci l'amena à créer son propre système d'exploitation, et ces travaux donnèrent le premier noyau linux, il intégra aussi certains outils développés par le projet GNU (Gnu is Not Unix). Richard Stallman, qui souhaiter rendre accessible le code source du système UNIX, pratique qui a été abandonnée par bon nombre de constructeurs.



VirtualBox : Debian –Version 9.2

Les différentes versions de kernel sont régulièrement mises à jour.

Le code source est disponible ici

<http://git.kernel.org/cgi/linux/kernel/git/stable/linux-stable.git>

Le projet GNU ont entrepris de recréer certains logiciels sur le principe de code Open source et libre, permettant ainsi à tous à chacun de modifier ce code. Linus a créé le noyau qui permettait au projet GNU d'exécuter ces outils libres sur un système libre. C'est depuis ce moment que le couple GNU/Linux a commencé à être diffusé et à créer une communauté de développeurs de modifier et d'améliorer ce système vers 1990, on pouvait déjà trouver certaines distributions sur la base de ce couple GNU/Linux, fonctionnelles.

De nos jours, ils existent bon nombre de système GNU/Linux livré avec plusieurs outils déjà préconfigurés. C'est ce que l'on appelle une distribution.

On en recense plus de 300.

Certaines distributions, bien que base sur un noyau gratuit et libre, facture une licence pour la maintenance, comme par exemple RedHat. Mais il existe d'autres cas ...

- Le logiciel est gratuit, la maintenance est payante
- Le logiciel est gratuit mais le code source est payant ou encore le support est payant.
- Le logiciel est gratuit mais son utilisation en titre « professionnel » devient payante.

Contrairement à Windows, Linux est modulable, donc on peut faire un peu ce que l'on veut

De même, l'environnement graphique n'est pas fixe, on peut choisir d'exécuter Gnu/Linux, en ligne de commande seule, ou choisir d'installer, un environnement graphique, comme par exemple Gnome ou KDE.

Certaines distributions proposent directement une installation graphique avec activation de la souris, Ubuntu est de ce type.

La souplesse de Linux diffère des autres systèmes d'exploitation, se serait-ce que lors des phases du mode d'installation, qui permet, soit de faire toute la mise en place, de manière quasi automatique ou en sélectionnant chaque option ou seulement certaines, une souplesse qui implique un minimum de connaissance technique.

Linux accepte la cohabitation avec d'autres systèmes comme par exemple avec Windows.

On peut parfaitement installer un système Linux en cohabitation avec Windows, cependant il faut que Windows soit installé en premier.

Ce système étant tellement fermé qu'il ne supporte pas d'être installé après un autre système.

Alors que Linux, permet même de tester votre matériel sans altérer d'aucune manière que ce soient les données.

Grâce à ce que l'on appelle un Live Cd ou encore une Clef USB rendu Bootable.

Lors de l'installation de Linux, celui-ci demande où installer le programme **GRUB**,

C'est **GRUB** qui va s'occuper, au démarrage de lancer le système d'exploitation.

GRUB accepte qu'on lui donne plusieurs systèmes d'exploitation, juste en renseignant un fichier de configuration. Par la suite au démarrage de la machine, il sera proposé une liste de choix afin d'exécuter tel ou tel système.

C'est ce que l'on appelle un multiboot.

En résumé, chacun a à loisir de modifier Linux et ainsi créer sa propre distribution.

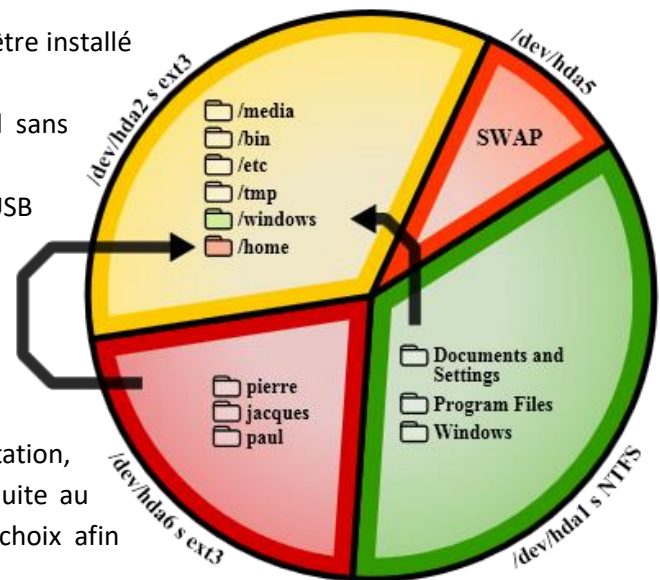
Au niveau logiciel, on trouve quasiment tout en équivalence dans le monde Linux.

L'utilisation de Linux peut se faire via un aspect graphique, mais à la base Linux est conçu pour fonctionner sur le principe d'un terminal qui reçoit des lignes de commandes.

Les actions en ligne de commandes peuvent réellement rebouter bon nombre d'utilisateurs, d'où l'existence de distribution du genre d'Ubuntu.

Les actions en ligne de commande sont dans le fonctionnement fondamental de Linux, ces lignes de commande révèlent alors une réelle puissance.

Linux a une réputation de système sécurité, il existe tout de même des failles du genre virus mais ceux-ci sont rares et la conception même de Linux permet une plus grande sécurité.



Les partitions Linux et autres

Lors de l'installation d'un système d'exploitation, que cela soit avec Linux ou Windows, il y a une étape cruciale qu'il est important de comprendre.

Le formatage du disque dur, ou la mise en format du support du système.

Il existe de nombreux formats de partitions, ceux-ci répondent à des normes bien précises.

Lors de la création d'une partition, le système d'exploitation crée un système de fichier qui lui permet de diviser l'espace de stockage en zone, en y plaçant des repères ainsi que des tables d'allocation de fichier.

Chaque système a sa manière de procéder, par exemple les systèmes Windows utilisent une notation alphabétique.

Dans les systèmes Linux elles sont laissées au choix de l'utilisateur, mais elles sont aussi assignables par défaut.

Quel type de partition choisir ?

Primaire et logique

Nous sommes limités à 4 partitions primaires par disque, dont seulement une peut être transformée en partition étendue.

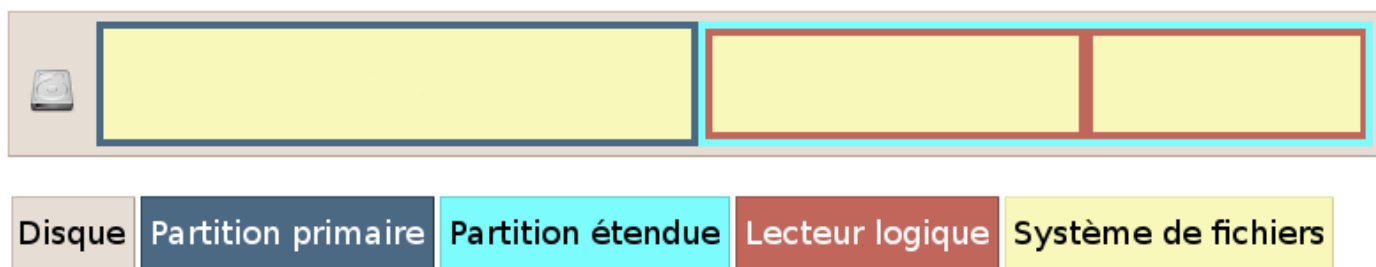
L'avantage de la partition étendue étant qu'on peut créer dedans de nombreuses partitions logiques. Linux utilise des partitions de types différents.

- Ext3
- Ext4
- Swap

et diverses Fat du monde Windows ainsi qu'un composant système pour la compatibilité avec NTFS du monde Windows.

Lors de l'installation il faut assigner un point de montage.

Linux part d'une hiérarchie ramifiée, où root (/) est le point de montage primaire qui par défaut



contient tous les autres.

Les points de montage sont des sous-répertoires

Prenons un exemple : les fichiers personnels se trouvent tous dans /home.

Si l'on veut ces fichiers sur une autre partition ou disque, il suffira d'installer un second disque ou de créer une autre partition pour ensuite paramétrer le point de montage vers /home.

La manœuvre peut être répétée pour n'importe quel sous-répertoire.

Lors de l'installation, Ubuntu propose de déterminer les points de montage suivants :

- /boot(lanceur de démarrage et en-têtes du noyau)
- /dev (périphériques et pilotes)
- /home (fichiers personnels)
- /opt (logiciels complémentaires)
- /srv (services système)
- /tmp (fichiers temporaires)
- /usr (applications)
- /usr/local (données accessibles à tout utilisateur)

- /var (spools serveur et logs)

Ce schéma de dossier est le même pour Debian, dont est sorti Ubuntu, mais aussi pour beaucoup d'autres distributions.

Si l'on souhaite utiliser plusieurs systèmes d'exploitation sur plusieurs disques, il peut être utile de créer une partition pour /boot. Mais créer une partition pour /usr implique une estimation réaliste de la taille occuper par les futures applications.

Il devrait être obligatoire d'assigner /home à une autre partition ou mieux, sur un autre disque.

Généralement, on se contenter de créer

- Une partition root,
- Une partition swap,
- Une partition ou un autre disque pour home,

On peut préserver ainsi la quasi-totalité des documents utilisateurs.

Pour ce cours nous utiliserons ce schéma.

Nous utilisons trois partitions : root, home et swap.

Source : https://fr.wikipedia.org/wiki/Partition_de_disque_dur

Adressage matériel

Historiquement, on désignait un disque par le contrôleur qu'il utilisait, et dans ce disque la partition par son numéro.

Exemple en Linux : /dev/sdb3 :

/dev est le répertoire des "devices" (=périphériques), s signifie "SCSI" ou encore "serial"

(Par opposition à h désignant les disques IDE à accès parallèle), d signifie "disk", b désigne le deuxième disque trouvé au boot

Dans cette catégorie et 3 le numéro de partition sur ce disque.

Cette méthode est bien adaptée aux disques fixes, malgré des disparités de dénomination (Grub les numérote à partir de 0, d'autres à partir de 1).

Elle devient plus hasardeuse avec des disques externes (SCSI ou USB), dont le numéro de montage va dépendre de leur ordre de branchement.

Adressage par UUID

L'UUID (« Universally unique identifier ») est un identificateur de 128 bits généré automatiquement au formatage d'une partition. Le risque de collision de deux identificateurs est infime ($2^{128} = 340\,282\,366\,920\,938\,463\,463\,374\,607\,431\,768\,211\,456$), ce qui permet d'exclure tout risque de collision excepté dans le cas d'une partition qui aurait été clonée bit à bit.

On perd évidemment la lisibilité du label. Un UUID est généralement représenté en hexadécimal avec des tirets pour aider sa lecture. En usage domestique, les quatre derniers caractères pourront suffire pour identifier rapidement le disque sur une étiquette papier.

Exemple : e8bac219-c30c-4315-9dc5-f47075bf697e

En Linux, la commande (administrateur) `blkid` permet de disposer des trois informations, si elles existent, pour chaque disque présent sur le système :

```
# blkid
/dev/sda1: SEC_TYPE="msdos" LABEL="DellUtility" UUID="3030-3030" TYPE="vfat"
/dev/sda2: LABEL="RECOVERY" UUID="FC10BC6C10BC2F8E" TYPE="ntfs"
/dev/sda3: LABEL="OS" UUID="00B8457CB8457168" TYPE="ntfs"
/dev/sdb1: UUID="c298c9ac-f202-4d1d-81a9-31dd69f62992" TYPE="ext4"
/dev/sdb2: LABEL="Mint 17.2 Mate64" UUID="c236a94f-6696-49b5-9892-3d4f4324eee4"
TYPE="ext4"
/dev/sdb3: LABEL="homecommon" UUID="e8bac219-c30c-4315-9dc5-f47075bf697e" TYPE="ext4"
/dev/sdc1: LABEL="SAMSUNG" UUID="C43CC9B13CC99EB4" TYPE="ntfs"
```

Source : <https://doc.ubuntu-fr.org/partitions>

Affectation et format des partitions

GNU/Linux est moins capricieux que d'autres systèmes d'exploitation : n'importe quelle partition et lecteur logique peuvent être affectés à tous les usages (que ce soit pour la partition système, pour une partition de données personnelles, pour l'espace d'échange [swap], etc). Le format (ou système de fichiers) utilisé par la partition est renseigné dans la table de partitions du MBR (ou dans la table de l'EBR, dans le cas des lecteurs logiques) ; il est codé sur deux des 16 octets réservés à une partition.

Du fait de l'organisation des disques durs à plateaux, une partition située en début de disque dur est plus rapide que la seconde partition, et ainsi de suite. Nous vous recommandons donc de placer vos partitions importantes (les partitions système et celles où se trouvent des données fréquemment accédées) en début de disque dur.

Quel format choisir ?

ext3 est le nom d'un système de fichiers utilisé notamment par GNU/Linux.

C'est une évolution de ext2, le précédent système de fichiers utilisé par défaut par de nombreuses distributions GNU/Linux.

Un système de fichiers ext3 est créé dans une partition, or, le format de table de partition géré par `fdisk` ne permet pas de créer des partitions de plus de 2 Tio ($2^{32} \times 512$)8.

Utilisez la commande `parted` et le format de table de partitions GPT9 pour s'affranchir de cette limite de 2 Tio.

ext4 est le successeur du système de fichiers ext3, principalement destiné aux systèmes basés sur GNU/Linux. Il garde une compatibilité avec son prédécesseur et est considéré par ses propres concepteurs comme une étape intermédiaire devant mener à un vrai système de fichiers de nouvelle génération tel que Btrfs1.

Toutefois, ext4 est une étape utile et non une simple solution temporaire.

Btrfs (B-tree file system, prononcé ButterFS4,5) est un système de fichiers des années 2010 fondé sur le Copy-On-Write (copie sur écriture en français) sous licence GNU GPL, développé conjointement par Oracle, Red Hat, Fujitsu, Intel, SUSE, STRATO AG (en) et autres. Il permet de redimensionner à chaud

la taille du système de fichiers (y compris en le rétrécissant) tout en conservant une excellente protection des métadonnées qui sont dupliquées en plusieurs endroits par sécurité.

L'opération est simple : `btrfs filesystem resize +2g /mnt` ajoute 2 Gio à son système de fichiers.

Cette fonction ne se veut pas redondante avec ce que propose le gestionnaire de volume logique de Linux mais prétend le compléter techniquement.

Ext3 étant moins efficace que Ext4, et Btrfs rendant compliquer l'utilisation de certains outils comme la commande "df" qui sert à afficher des informations sur l'espace disque, Ext4 est donc le format que nous allons utiliser.

Quelle distribution ?

Le choix d'une distribution Linux est délicat, nous ne retiendrons que des distributions où le support est assuré par la communauté. Pour exemple entre Debian et CentOS et Ubuntu

Avantages CentOS

Voici quelques avantages de l'utilisation de CentOS :

- Basé sur une solution commerciale de qualité supérieure
- Stable et cohérent
- Eh bien testé avant de le rendre disponible au public

Inconvénients CentOS

CentOS présente aussi un certain nombre d'inconvénients :

- Mises à jour rares et moins fréquentes
- Se trouve derrière la concurrence
- Correctifs pour CentOS plus lents que pour RHEL

Avantages Debian

Voici quelques avantages de l'utilisation de Debian :

- Contrôle de la qualité remarquable
- Très stable et sans bogue
- Support large de l'architecture

Inconvénients Debian

Debian présente aussi un certain nombre d'inconvénients :

- Cycle lent des mises à jour, mais plus rapidement que CentOS
- L'adhésion à la philosophie UNIX conduit au conservatisme
- Son installation n'est pas conviviale

Avantages Ubuntu

Voici quelques avantages de l'utilisation de Ubuntu :

- Facile d'utilisation par les débutants

VirtualBox : Debian –Version 9.2

- La documentation est robuste et actualisée
- Publication régulière et un excellent support

Inconvénients Ubuntu

Ubuntu présente aussi un certain nombre d'inconvénients :

- Manque de compatibilité
- Comprends les logiciels propriétaires
- Non adapté pour les utilisateurs avancés

Notre choix se portera donc sur Debian et si besoin Ubuntu, mais on pourra aussi choisir d'installer un bureau du genre Gnome ou Kde sur Debian, de plus ce que nous aborderons par la suite, se passe de manière identique sur les deux distributions,

Hormis le login et l'utilisation d'une interface graphique.

les outils s'exécute au sein de SystemD, et non plus init.D.

En 2015, la plupart des distributions GNU/Linux ont adopté ce système d'initialisation.

Source : <https://www.unix-experience.fr/2011/migrer-de-init-vers-systemd/>

SystemD est une alternative très intéressante à Init. Pourquoi ?

Init est la base de toute architecture Linux/UNIX me direz vous, il est le cœur reliant tout le système au noyau.

Le souci d'Init c'est qu'il est « ancien et mono tâche » dirons-nous. En effet, il traite de façon séquentielle les ordres.

Une fois Init chargé, il va lancer les différents services et ainsi permettre le démarrage complet du système et des services associés. Pour se faire, il se base sur un arbre de dépendances défini sous Debian dans le dossier `/etc/rc<runlevel>.d/`, et ensuite lance séquentiellement les services.

Mais pourquoi on les lance un à un, après tout on pourrait lancer le service openLDAP en même temps que la base de données MySQL ou encore le serveur Apache en même temps que le service SSH, par exemple. SystemD permet déjà d'améliorer ceci en se basant sur son propre arbre et ses dépendances afin de lancer simultanément plusieurs services, en se basant non plus sur un ordre séquentiel mais sur des niveaux d'arborescences.

Ainsi si syslog est nécessité par l'ensemble des services, il sera lancé en premier puis suivront dbus et avahi par exemple et ensuite openLDAP, MySQL et SSH.

Source : <http://linuxfr.org/news/%C3%A9volutions-techniques-de-systemd>

Comment utiliser ce document ? :

Dans la table des matières, la partie sur le labo est surligné en gris.

Lorsque vous devez saisir une commande de ce document, celle-ci est affichée avec un # devant, enlever le !

En Ligne de commande, ou CLI, le « # » indique que vous êtes « logger » en « Root » Sinon c'est le « \$ ».

```
# apt-get update deviens apt-get update
```

Dans les zones de retour écran, les résultats sont affichés partiellement

Les trois petits points indiquent qu'il y a une césure dans le copier coller.

Raccourci clavier pour faire le signe dièse (#) sur PC

Quelles touches du clavier utiliser pour faire le symbole musical dièse (#)

Ou pour faire le « croisillon » qui sert à composer des mots-clés cliquables, le fameux hashtags (#)



Croisillon



Dièse

Quelle différence entre les deux ?

- Le terme « dièse » ou hash en anglais est utilisé sur internet : celui-ci devrait être en effet appelé « croisillon »,
- Le dièse est un symbole musical spécifique de forme différente (#).

Comment faire le symbole dièse « croisillon » (réseaux sociaux et écriture web) sur PC

Sur clavier Azerty

- Raccourci clavier signe dièse (croisillon) sur PC avec un clavier Azerty : Alt gr+3 => #

Sur clavier Qwerty

- Raccourci clavier pour le signe dièse sur un clavier Qwerty anglais : Alt + 3 et américain : Shift + 3

Touche dièse sur Mac

- Shift + 3

Comment faire le symbole dièse musical (Sharp key = #) sur PC ?

- La combinaison Alt+9839 permet de faire le dièse (musical) sur les logiciels Windows ! => #

Comment faire ce symbole en HTML :

- HTML Entity (décimal) : ♯
- HTML Entity (hex) : ♯

Malgré l'explication si dessus sur le dièse et le croisillon, nous pouvons parler de « **dièse** » lors de la présence du croisillon, cela étant pour nous une convention de nommage tacite.



Attention !!!! Ce Symbole requière la plus grande attention.

- Dans un script ou un fichier de configuration, le « **#** » sert à commenter le texte, ce qui suis ce symbole n'est pas traité. De même, dans les fichiers de configuration, le « **#** » et le « **;** » en début de ligne indique un commentaire, le « **;** » étant le caractère de fin d'instruction.



En Ligne de Commande, si le Prompt est un « **#** », c'est que vous êtes en mode privilège Root, sinon c'est le symbole « **\$** ». Si vous ne comprenez pas la commande, utiliser le manuel avant => **man**<ESPACE><COMMANDE>.

[https://fr.wikipedia.org/wiki/RTFM_\(expression\)](https://fr.wikipedia.org/wiki/RTFM_(expression))

Les commandes contenant <USER> ou autre <IP_DU_SITE> doivent être adaptées sans les signes plus grand que (ou supérieur) « **>** » et plus petit que (ou inférieur) « **<** ».

Avant chaque modification de fichier, il est fortement recommandé de faire une copie. : Pensez à faire des instantanés de vos machines virtuelles

j'ai choisi : « .bak » ou « .original », à votre convenance, c'est une convention de nommage, l'extension ne sert qu'à clarifier et simplifier une recherche ultérieure.

Pour cela utiliser la commande **CP**.

```
cp /CHEMIN/VERS/LE/FICHER<ESPACE>/CHEMIN/VERS/LA/COPIE<POINT><EXTENSION en BAK ou ORI>
Exemple : cp /etc/opensvpn/server.conf /etc/opensvpn/server.conf.bak
ou
cp /CHEMIN/VERS/LE/FICHER<ACCOLADE>{<VIRGULE><POINT><EXTENSION en BAK ou ORI><ACCOLADE>}
Exemple : cp /etc/opensvpn/server.conf{,.bak}
```

Lors de vos recherches en ligne, soyez vigilant quant aux réponses données, en fonction de la date et des versions, les réponses peuvent être différentes...

Ce document a pour but de vous éclairer quant aux différentes étapes, il n'a pas vocation à être « LA » solution.

La partie annexe générale regroupe des explications sur le réseau virtuel, les commandes de base ainsi qu'une explication sur les ACL.



Attention !!!! : Les annexes ne sont pas des étapes chronologiques, mais plutôt une « **caisse à**

Pour chaque étape :

- Vous devrez adapter à votre propre configuration.
- Effectuez des recherches sur certains termes et techniques.
- Tenir un cahier de route précis et détaillé, permettant de rendre un document technique.

Seule votre expérience, vos tests et échecs vous amèneront vers une solution stable et viable...

Réinitialiser le mot de passe Root d'un Debian

Pré-requis

Être sûr que les mots de passe n'ont pas été cachés à l'aide de la commande `shadowconfig`. Si c'est le cas, cette procédure est sans effet, il vous faudra réinstaller la machine.

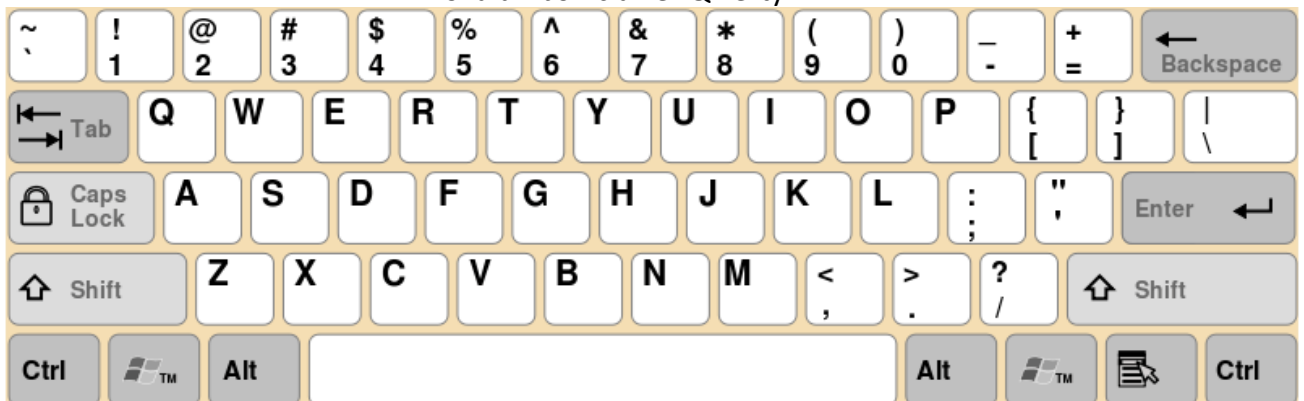
Comment réinitialiser le mot de passe Root d'un Debian (ou Ubuntu) si vous ne pouvez plus vous connecter en Root (ou avec un utilisateur disposant des droits `sudo`).

Pour commencer, il faut que vous ayez un accès physique à la machine, car nous allons devoir modifier des lignes dans le grub.

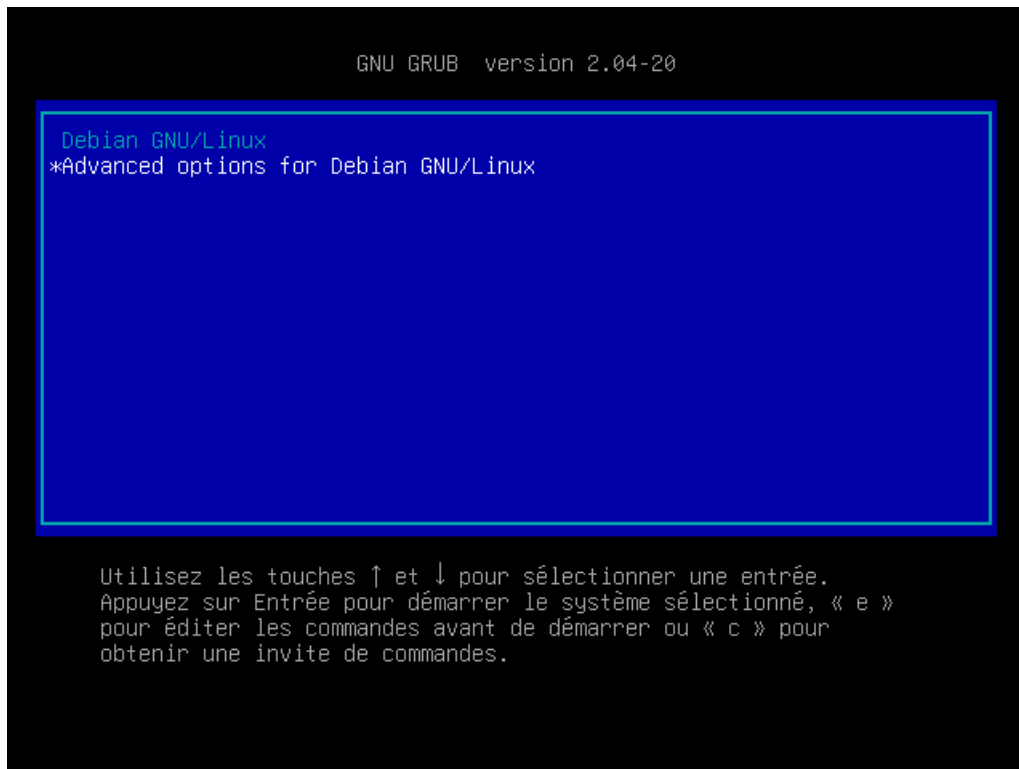
Votre ordinateur doit être éteint.

Je vous conseille de repérer les touches du clavier Qwerty, car le clavier ne sera pas en Azerty pour faire les modifications.

Voilà un bon clavier Qwerty:



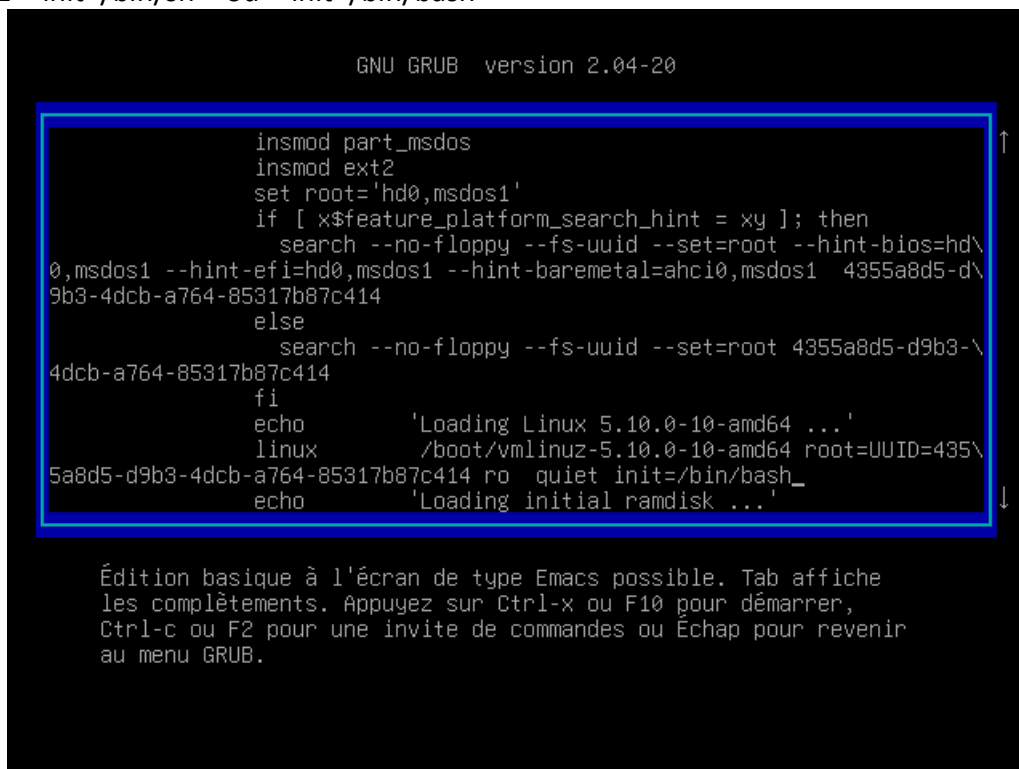
Démarrez votre ordinateur, puis, à l'écran du GRUB, déplacez le curseur sur la ligne ayant le mode de dépannage comme ci-dessous.



Appuyez sur la touche « e » pour éditer les paramètres de boot.

Puis, ajoutez la ligne suivante comme indiquée dans la capture :

Placez le curseur à la fin de la ligne commençant par « linux /vmlinuz... » après « ro quiet » et ajoutez « init=/bin/sh » ou « init=/bin/bash »



Voilà, maintenant, appuyez sur « Crlt+x » pour démarrer.

Une fois démarré vous vous retrouvez avec un Prompt en root

VirtualBox : Debian –Version 9.2

```

/dev/sda1: clean, 42082/3219456 files, 677032/12856832 blocks
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/#

```

Petite précision, la modification sera supprimée au prochain reboot.

Nous allons chercher la partition à monter pour modifier le mot de passe.

Pour cela, faites la commande « fdisk -l »,

identifiez la ligne contenant « * » qui indique la partition de boot

Retenez l'adresse de la partition, dans cet exemple c'est /dev/sda1

```

/dev/sda1: clean, 42082/3219456 files, 677032/12856832 blocks
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/# fdisk -l
Disk /dev/sda: 50 GiB, 53687091200 bytes, 104857600 sectors
Disk model: UBOX HARDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x594e2474

Device      Boot    Start        End    Sectors    Size Id Type
/dev/sda1   *        2048    102856703    102854656    49G 83 Linux
/dev/sda2             102858750    104855551     1996802    975M  5 Extended
/dev/sda5             102858752    104855551     1996800    975M 82 Linux swap / Solaris
root@(none):/#

```

Monter celle-ci.

Attention, le shell est en QWERTY !!

Donc sur un clavier AZERTY il faut taper :

,ount)o re,ount;rz ! /dev/sdw& /

Pour afficher ceci

mount -o remount,rw /dev/sda1 /

```
root@(none):/# mount -o remount,rw /dev/sda1 /
root@(none):/# passwd
New password:
Retype new password:
passwd: password updated successfully
root@(none):/# _
```

Maintenant que la partition est montée, vous pouvez faire la commande « passwd ».
Vous pouvez redémarrer

```
### Bascule temporaire du clavier en français en environnement graphique.  
# setxkeymap fr
```

```
### Reconfiguration des langues du système  
# sudo dpkg-reconfigure locales
```

```
### Reconfiguration permanente du clavier  
# sudo dpkg-reconfigure keyboard-configuration
```

NANO

```
#####  
#####  
#          RACCOURCI NANO  
#  
#####  
#####  
CTRL + A : Permet d'aller au début de la ligne  
CTRL + E : Permet d'aller à la fin de la ligne  
CTRL + Y : Permet de remonter de page en page  
CTRL + V : Permet de descendre de page en page  
CTRL + _ : Permet de se rendre au n° de ligne indiqué  
CTRL + C : Permet de savoir à quel n° de ligne / colonne / caractère se trouve votre curseur  
CTRL + W : Permet de faire une recherche  
CTRL + D : Permet de supprimer un caractère  
CTRL + K : Permet de supprimer une ligne complète (comme la commande dd sous Vi)  
CTRL + O : Permet de sauvegarder votre fichier  
CTRL + X : Permet de quitter nano  
CTRL + G : Affiche l'aide
```

Ajouter sudo

Installation de sudo

Si Sudo n'est pas déjà installé

On peut devenir root **temporairement** à l'aide de la commande sudo.

Cette commande signifie « Faire en se substituant à l'utilisateur » : **Substitute User DO**.

Suivez les instructions si dessous.

Une fois que vous êtes connecté avec votre utilisateur "standard" sur votre Debian, commencer par taper la commande su pour ouvrir une session en tant que root (le mot de passe associé est requis).

Puis lancer l'installation du paquet sudo en tapant la commande apt-get install sudo

```
sysadmin@myserver:~$ su
Password:
root@myserver:/home/sysadmin# apt-get install sudo
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  sudo
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
```

Configuration de base de sudo

Toujours en tant que root, ouvrir le fichier /etc/sudoers avec votre éditeur de texte préféré (pour moi c'est nano)

```
nano /etc/sudoers
```

Puis ajouter la ligne <user> ALL=(ALL:ALL) ALL juste après la ligne root ALL=(ALL:ALL) ALL
En prenant soin de remplacer <user> pour votre nom d'utilisateur standard (non root).
Exemple ci-dessous avec mon utilisateur sysadmin.

```
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification
```



```
# Cmnd alias specification
```

```
# User privilege specification
```

```
root    ALL=(ALL:ALL) ALL
```

```
sysadmin ALL=(ALL:ALL) ALL
```

```
# Allow members of group sudo to execute any command
```


```
%sudo   ALL=(ALL:ALL) ALL
```

```
# See sudoers(5) for more information on "#include" directives:
```

```
#includedir /etc/sudoers.d
```

Pour ceux qui ne souhaitent pas modifier le fichier de configuration ci-dessus, un utilisateur peut également utiliser la commande sudo s'il est membre du groupe sudo.

Vous pouvez donc simplement exécuter la commande `adduser sysadmin sudo` pour que l'utilisateur sysadmin soit autorisé à utiliser sudo.

 **Attention !!!!**
: dans ce cas, une nouvelle session SSH doit être ouverte pour l'utilisateur sysadmin pour que ça fonctionne.

```
adduser sysadmin sudo
```

Ou aussi de cette façon ...

```
Usermod -aG sudo sysadmin
```

- Résolution DNS

Vérifier le contenu de /etc/resolv.conf

```
# cat /etc/resolv.conf
nameserver 192.168.3.100
nameserver 80.10.242.128
root@debian:/home/sysadmin#
```

en cas de problème

Ajouter votre serveur dns directement dans interfaces , comme ci-dessous.

```
# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet dhcp

dns-nameservers 8.8.4.4
```

avec resolvconf



Attention !!!!

Si vous avez installé un environnement graphique, il est fort probable que le programme NetworkManager soit présent, dans ce cas, paramétrez le réseau via les outils graphiques. De même pour la déclaration des DNS.

Si le programme **resolvconf** est installé, vous n'aurez pas à modifier à la main le fichier de configuration **resolv.conf** car il sera changé de façon dynamique par les programmes. Si vous avez besoin de définir vous-même les serveurs de noms de domaine (comme avec une interface statique), ajoutez au fichier de configuration **interfaces** du répertoire /etc/network/interfaces une ligne comme celle-ci :

```
dns-nameservers 12.34.56.78 12.34.56.79
```

Mettez la ligne indentée dans un paragraphe **iface**, par exemple juste après la ligne **Gateway**. Entrez les adresses IP des serveurs de noms de domaine dont vous avez besoin après **dns-nameservers**, toutes sur la même ligne, séparées par des espaces. N'oubliez pas le "s" à la fin de **dns-nameservers**.

Le programme **resolvconf** est un ajout plutôt récent à Debian et plusieurs anciens programmes ont besoin d'être mis à jour ou reconfigurés pour fonctionner correctement avec lui . Si vous rencontrez des problèmes, regardez /usr/share/doc/resolvconf/README qui contient beaucoup d'informations sur la manière de faire fonctionner **resolvconf** avec d'autres programmes.

Si besoin, Installer resolvconf avec

```
apt-get install resolvconf
```

Puis éditer

```
nano /etc/resolvconf/resolv.conf.d/head
domain google.fr
search google.fr
nameserver 8.8.8.8
```

ou

VirtualBox : Debian –Version 9.2

```
cat > /etc/resolvconf/resolv.conf.d/head <<EOF
domain google.fr
search google.fr
nameserver 8.8.8.8
EOF
```

Ne pas oublier le End Of File

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

Sources.list

Le fichier /etc/apt/sources.list contient les « URL » indiquant les depots officiels de DEBIAN.

Ce fichier a été garni à partir de votre choix, lors de l'installation.

J'édite le fichier sources.list

```
# nano /etc/apt/sources.list
```

LE « # » place la ligne en commentaire, elle ne sera pas traitée.

Exemple de Fichier sources.list

```
# 2018-10-25-debian 9 - stretch
# deb cdrom:[Debian GNU/Linux 9.2.1 _Stretch_ - Official amd64 DVD Binary-1 20171013-13:09]/ stretch contrib
main

deb http://ftp.fr.debian.org/debian/ stretch main non-free
deb-src http://ftp.fr.debian.org/debian/ stretch main non-free

deb http://security.debian.org/debian-security stretch/updates main contrib non-free
deb-src http://security.debian.org/debian-security stretch/updates main contrib non-free

# stretch-updates, previously known as 'volatile'
deb http://ftp.fr.debian.org/debian/ stretch-updates main contrib non-free
deb-src http://ftp.fr.debian.org/debian/ stretch-updates main contrib non-free
```

Modification du sources.list

On ajoute « contrib non-free » après main.

Debian est open source, elle ne propose par défaut que des logiciels libres, mais dans le cas où l'on souhaite, par exemple lire des fichiers de type « propriétaire », par exemple le format PDF ou mp3, il faut indiquer le paramètre « non-free ». « contrib » regroupe les contributions de la communauté.

```
# 2018-10-25-debian 9 - stretch
# deb cdrom:[Debian GNU/Linux 9.2.1 _Stretch_ - Official amd64 DVD Binary-1 20171013-13:09]/
stretch contrib main

deb http://ftp.fr.debian.org/debian/ stretch main contrib non-free
deb-src http://ftp.fr.debian.org/debian/ stretch main contrib non-free

deb http://security.debian.org/debian-security stretch/updates main contrib non-free
```

```
deb-src http://security.debian.org/debian-security stretch/updates main contrib non-free

# stretch-updates, previously known as 'volatile'
deb http://ftp.fr.debian.org/debian/ stretch-updates main contrib non-free
deb-src http://ftp.fr.debian.org/debian/ stretch-updates main contrib non-free
```

Redémarrez votre système :

```
#init 6
```

Installer la commande locate.

```
# apt-get update && apt-get upgrade && apt-get install locate -y

# updatedb
# locate resolvconf

/etc/resolvconf
/etc/resolvconf/update-libc.d
/etc/resolvconf/update-libc.d/avahi-daemon
/lib/systemd/system/systemd-resolved.service.d/resolvconf.conf
/usr/share/bash-completion/completions/resolvconf
```

```
# ls -l /etc/resolvconf
total 0
```

Le contenu de /etc/resolvconf est vide, donc celui-ci n'est pas installé.

Vérifier les informations permettant la résolution DNS

```
# cat /etc/resolv.conf
nameserver 192.168.3.100
nameserver 80.10.242.128
```

Modification de fichier resolv.conf

Si resolvconf n'est pas présent, et que vous souhaitez indiquer vos serveur DNS.

Exemple avec IPv4 et IPv6 :

```
nameserver ::1
nameserver 127.0.0.1
#nameserver 2001:41d0:1:d6e::110
nameserver 192.168.1.1
```

Attention ; en mode DHCP, le fichier resolv.conf est écrasé à chaque boot, il faut éditer et renseigner, ~~comme expliquer durant le labo~~, en installant le programme resolvconf et en éditant /etc/resolvconf/resolv.conf.d/head .

Cependant, certains programmes ne fonctionnent pas correctement avec le programme resolvconf, il est possible de bloquer en écriture le fichier /etc/resolv.conf avec la commande chattr -V +i, liser man chattr.

```
# cat /etc/resolv.conf
domain <NOM_DU_DOMAINE>
search <NOM_DU_DOMAINE>
nameserver <IP-DNS1>
nameserver <IP-DNS2>
```

Redémarrer le réseau

```
service networking restart
```

Puis vérifier le fichier resolv.conf qui est générer automatiquement, celui-ci reçoit les DNS du fichier head ainsi que ceux fourni par le DHCP

```
# cat /etc/resolv.conf
```

À ce stade, ping vers un nom de domaine dois retourner une réponse correcte, sans resolution DNS, vous ne pourrez pas faire les mises à jour ou installer les programmes disponibles sur les dépôts, ceux ci étant accessible par l'adresse ftp.dedbian.org.

Vérifier les groupes

```
# cat /etc/group

root:x:0:
...
...
www-data:x:33:
...
users:x:100:
nogroup:x:65534:
sysadmin:x:1000:
ntp:x:117:
sambashare:x:118:
winbindd_priv:x:119:
bind:x:120:
#
```

Vérifier les utilisateurs

```
# cat /etc/passwd

root:x:0:0:root:/root:/bin/bash
....
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
....
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
sysadmin:x:1000:1000:sysadmin,,,:/home/sysadmin:/bin/bash
ntp:x:111:117::/home/ntp:/bin/false
bind:x:112:120::/var/cache/bind:/bin/false
#
```

Obtenir des informations sur le statut du système

Afficher le statut du système :

```
$ systemctl status
```

Lister les unités échouées :

```
$ systemctl --failed
```

Lister les fichiers unités installés :

```
$ systemctl list-unit-files
```

Pour connaître son système de démarrage, taper :

```
ps -p 1
```

Si vous voulez Tuer tous les processus, avec « killall », il faut installer psmisc

```
# apt-get install psmisc
```

```
root@debian-base:~# ps -p 1
PID TTY      TIME CMD
  1 ?        00:00:00 systemd
root@debian-base:~#
```

Si le résultat de la colonne CMD est "systemd" on est sous systemd si on a "init" on est sous sysVinit.

Vérifier et activer rc.local au démarrage

```
sudo systemctl status rc-local
sudo systemctl enable rc-local

# updatedb
# locate rc.local
# /lib/systemd/system/rc.local.service
```

/etc/init.d/rc.local est systématiquement appelé à chaque démarrage

Ce script lance /etc/rc.local où tu peux mettre un appel à tes programmes.

Pour un script local c'est la solution.

tty

tty est une commande Unix qui affiche sur la sortie standard le nom du fichier

Connecté sur l'entrée standard. L'origine du nom tty vient de l'anglais teletypewriter, qui se traduit téléscripteur, et a été abrégé en « TTY ».

getty

getty est la contraction de "get teletype" en anglais ce qui signifie obtenir un téléscripteur, c'est un programme Unix qui tourne sur un ordinateur hôte qui permet de gérer un terminal tty physique ou virtuel.

Créer une session avec SCREEN

```
apt-get install screen
screen -S nom de la session
screen -x
```

Les commandes screen à partir de la console:

```
> screen // démarre screen
> screen -r // Reprends un screen détaché
> screen -d // Force le détachement d'un screen en cas de plantage pour en reprendre le contrôle
> screen -ls // Affiche la liste des screen mère
ctrl a backspace // fenêtre précédente
killall screen : ordre de tuer le processus : kill -9
commandes à partir d'une console screen:
CTRL+A puis C = créer une nouvelle console screen
CTRL+A puis N = passer à la console screen suivante
CTRL+A puis P = passer à la console screen précédente
CTRL+A puis D = Détacher le screen et revenir sur la console classique
CTRL+D = fermer une console screen. Lorsqu'il n'y a plus qu'une seule console, ça quitte screen.
```

PERSONNALISATION

Dans le répertoire « /root » afin de personnaliser un minimum bash.

D'abord, par précaution, on fait une sauvegarde du fichier à modifier :

```
# cp -av /root/.bashrc /root/.bashrc.original
```

Ensuite on ajoute les lignes suivantes au fichier « /root/.bashrc » :

```
# nano /root/.bashrc
```

```
# personnalisation
export PS1='\u@\`hostname -f\`:\w\$\$ '
export LESS='-S'
alias l='ls -aF --color=yes --full-time --time-style=long-iso | more'
alias ll='ls -aF --color=yes --full-time --time-style=long-iso'
~/bashrc
```

IOTOP panneau d'information HardWare

```
apt-get install iotop iftop
```

commande htop

Ctrl + c

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

shift + pageUp ou pageDown pour défiler vers le haut ou bas

VirtualBox : Debian –Version 9.2

Edition de l'interface

```
nano /etc/network/interfaces
```

me permet d'éditer le fichier

Ctrl + o pour enregistrer

et

Ctrl + x pour sauver et quitter

Copie de sauvegarde d'un fichier

```
cp /chemin/vers/le/fichier/nom_fichier <espace>  
/chemin/vers/le/nouveau/fichier/nom_du_fichier.auchoix
```

```
cp /etc/network/interfaces /etc/netwotk/interface.save
```

ou

```
cp /etc/network/interfaces /etc/netwotk/interface.bak
```

ou. old, c'est une convention de nommage, donc c'est à vous de voir !

Utilisation de la commande ping

Linux

```
ping -c<nombre de test> <ip_de_la_machine>
```

Windows

```
ping <ip_de_la_machine>
```

Le mode par pont permet d'obtenir une ip de pour l'interface WAN dans le même réseau que mon poste de travail

Test de l'accès au WAN et de la résolution DNS

Je tente un ping vers, par exemple, l'IP de google

```
# ping -c4 8.8.8.8
```

-c4 indique de faire 4 tentatives

Si on omet la valeur, celui ne s'arrête pas. On stoppe le ping avec Ctrl + c

```
# ping -c4 google.fr
```

Il me faut maintenant éditer de plus en plus de fichier, et une connexion en ssh via PuTTY sera plus souple

Mais pour cela, il me faut être sur le même réseau que la VM.

Le réseau privé hôte. Le poste Windows a une carte dans ce réseau

```
Exécuter > cmd> entrer
```

Saisir

```
# ipconfig /all
```

pour voir toutes les interfaces Windows , repérer l'IP 192.168.101.253.

Afficher la release

```
uname -r  
4.9.0-6-amd
```

apt-cache search --names-only

```
# apt-cache search --names-only linux-headers-4.9.0-6  
    linux-headers-4.9.0-6-all - All header files for Linux 4.9 (meta-package)  
    linux-headers-4.9.0-6-all-amd64 - All header files for Linux 4.9 (meta-package)  
    linux-headers-4.9.0-6-amd64 - Header files for Linux 4.9.0-6-amd64  
    linux-headers-4.9.0-6-common - Common header files for Linux 4.9.0-6  
    linux-headers-4.9.0-6-common-rt - Common header files for Linux 4.9.0-6-rt  
    linux-headers-4.9.0-6-rt-amd64 - Header files for Linux 4.9.0-6-rt-amd64  
  
#  
  
# apt-cache search --names-only linux-headers-4.9.0-6-amd  
    linux-headers-4.9.0-6-amd64 - Header files for Linux 4.9.0-6-amd64
```

```
# apt-show-versions
```

Le paquet show-versions peut être absent.

```
# apt-get install apt-show-versions  
apt-show-versions <PACKAGE>  
apt-show-versions linux-headers  
linux-headers not installed (not available)  
  
#
```

Voir les logs :

```
tail -30 /var/log/syslog
```

Vérifier les ports

```
netstat -uta -u UDP -t TCP
```

La commande host

```
# host -a debian
```

Affinage des résultats grâce à l'outil « grep »

Le « pipe » prononcer « paillepe » s'obtient grâce à « Alt Gr+6 » => |.

```
root@debian-cli:~# ip addr | grep 2
```

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default  
qlen 1000  
    link/ether 08:00:27:ae:55:22 brd ff:ff:ff:ff:ff:ff
```

```
inet 192.168.101.100/24 brd 192.168.101.255 scope global dynamic enp0s3
    valid_lft 85700sec preferred_lft 85700sec
inet6 fe80::883b:2c93:2b23:b723/64 scope link
    valid_lft forever preferred_lft forever
```

```
root@debian-cli:~# ip addr | grep 2
```

```
2: enp0s3: <BROADCAST...
    inet 192.168.101.100/24 brd 192.168.101.255 scope global dynamic enp0s3
```

```
root@debian-cli:~# dhclient
root@debian-cli:~# ip addr | grep 2
2: enp0s3: <BROA.. ...
    inet 192.168.101.101/24 brd 192.168.101.255 scope global secondary enp0s3
```

Mise à jour

apt-get update et apt-get upgrade

```
apt-get update && apt-get upgrade
```

J'en profite pour installer quelques outils

Pour en savoir plus sur une commande utiliser la commande man pour manuel. Presser « **q** » pour quitter « **man** ».

Tester man man

```
# man man
MAN(1)      Utilitaires de l'afficheur des pages de manuel      MAN(1)
....
Manual page man(1) line 1 (press h for help or q to quit)
```

Rechercher un fichier avec la commande locate

Installer la commande « locate » et Mettre à jour la base locale avec

```
apt install locate
```

puis

```
updatedb # puis recherche avec locate
```

Installer unzip et tree

Unzip pour décompresser une archive zip simplement, et tree qui liste les dossiers sous forme d'arborescence en CLI.

```
apt install unzip tree
```

Changer le hostname de votre debian

Depuis **Debian 8.x**, il n'est plus nécessaire de modifier le fichier `etc/hostname`.

La commande `hostnamectl` avec l'option **set-hostname** permet de **changer** le nom de la machine sans redémarrage. : Pour voir ce nom apparaître il faut se connecter avec un autre utilisateur ou se délogger/reloguer.

```
hostnamectl set-hostname <POSTE>.<DOMAINE>.<TLD>
```

Si vous êtes en « ssh » vous ne verrez le changement que lors de votre prochaine connexion.

Voir les paramètres

```
# hostnamectl
Static hostname: debian
    Icon name: computer-vm
    Chassis: vm
Machine ID: c37aff73c7b64b2cabe483ef987292d1
    Boot ID: 976d79e630204243a3225e5292ed4f69
Virtualization: oracle
Operating System: Debian GNU/Linux 9 (stretch)
    Kernel: Linux 4.9.0-4-amd64
Architecture: x86-64
```

Où placer les scripts

La réponse nous est donnée par la norme de la hiérarchie des systèmes de fichiers (FHS).

- Cela dépend du script.

Pour les logiciels tiers, non inclus dans la distribution et destinés à tous les utilisateurs, la pratique est de les mettre dans /opt.

Pour les logiciels destinés à un seul utilisateur,

ils devraient être dans le répertoire utilisateur, typiquement dans ~/bin.

La convention veut que l'on place les scripts spécifiques à une machine dans /usr/local/bin.

Ce répertoire est a priori vide lors d'une installation de distribution.

Le local de /usr/local signifie que les logiciels ici sont propres à cet ordinateur et qu'ils ne sont pas contrôlés par le système de paquet de la distribution.

Dans le doute, vos binaires devront donc être dans /usr/local/bin.

Par analogie, les bibliothèques associées seront dans /usr/local/lib,

La documentation dans /usr/local/share etc.

Source : <http://refspecs.linuxfoundation.org/fhs.shtml>

Gestion des services Debian ponctuellement

Pour gérer un service ponctuellement on utilise la commande `service nom_du_service commande`.

Cette commande prend plusieurs paramètres en fonction de ce que l'on veut faire du service.

En général on peut utiliser les commandes suivantes :

- `start` : pour le démarrer
- `stop` : pour l'arrêter
- `restart` : pour le redémarrer ou le démarrer s'il est arrêté
- `reload` : pour recharger la configuration sans le redémarrer (donc sans couper les connexions actives)
- `status` : Pour connaître l'état du service. Démarré ou arrêté.

Désactiver le service du démarrage

```
systemctl disable <LENOMDUSERVICE>
```

Supprimer les fichiers

La commande « `rm` » pour remove, Consulter le manuel avant de supprimer.

En mode root, il n'y a pas de retour en arrière possible. Pas de corbeille comme sous Windows.

```
rm <CHEMIN/VERS/LE/FICHER>
```

Compression TAR

Il nous faut donc lire le fichier `README.debian.gz`, attention ce sont des dossiers `.gz`

Les fichiers en `.tar` sont archivés (simplement réunis tous ensemble, ils ne sont pas compressés)

Les fichiers en `.tar.gz` sont appelés archives compressées car elles sont mises en archives d'où l'extension `.tar` PUIS compressées d'où l'extension `.gz`.

La commande `tar -zxvf`

- l'option `-z` va appeler le logiciel `gzip` (pour la compression car `tar` est un outil d'archivage ne l'oublier pas),
- l'option `-x` permet l'extraction (si on indique « `-c` » à la place de « `x` » c'est pour créer une archive et non l'extraire)
- l'option « `-v` » signifie « verbose », donc indique que la commande va indiquer clairement ce qu'elle fait, en mode bavard le « `v` » est facultatif.
- L'option « `-f` » signifie file pour indiquer qu'on parle de fichiers.

On pourrait mettre `tar --extract --verbose --gzip --file fichier.tar.gz` en noms complets ou encore `tar -x -v -z -f` (l'ordre des options n'est pas important)

En écriture simplifier on les colle tous ensemble avec un seul tiret : `tar -zxvf`

Taille d'un dossier

`h` pour humain

```
du -<CHEMIN/LE/DOSSIER> | tail -n 1
```

Trouver les fichiers contenant une chaîne de caractère

```
find . | xargs grep 'string' -sl
```

Plus simple :

```
grep -lR "string" *
```

Supprimer des .SVN (serveur subversion)

```
find . -name ".svn" -type d -exec rm -rf {} \;
```

vider les .logs

Vérifier la taille

```
du -hs /var/log  
du -hs /tmp  
find / -type f -name "*.log" -exec cat /dev/null > {} \;
```

en mode root :

```
find / -name '*.log' | awk '{print "echo -n > \"$1\"' | sh
```

Les fichiers d'archivages des logs peuvent être supprimés sans danger pour votre système

```
*.1.log, 2.log, 3.log ..  
find / -name '*.?.log' -exec rm {} \;  
find / -name '*.?.log.?' -exec rm {} \;
```

Pour vider un fichier sous Unix ou linux, il faut effectuer cette manipulation :

```
echo /dev/null > fichier_a_vider
```

On a aussi:

```
echo « » > fichier_a_vider (Générera un fichier de 1ko avec un saut de ligne)  
printf « » > fichier_a_vider (Générera un fichier de 0ko sans saut de ligne)
```

Encore plus rapide dans le rep ou avec le chemin :

```
> fichier_a_vider
```

Comment utiliser la commande IP sur Linux

Voici la syntaxe de la commande ip :

```
ip [OPTION] OBJECT {COMMANDE | help}
```

Les objets (ou les sous-commandes) principaux incluent :

Link (l) : interfaces réseau, telles que les connexions filaires et les adaptateurs Wi-Fi (eth0, eno1, wlan0, ens1, enp2s0, p7p1, ..)

VirtualBox : Debian –Version 9.2

Address (a) : adresses IP IPv4 ou IPv6

Route (r) : table de routage – les règles qui gèrent le routage du trafic envoyé aux adresses via des interfaces (liens)

Neigh (n) – utilisé pour afficher et manipuler des objets voisins (tableau ARP)

Ainsi, on peut utiliser le mot complet ou son abréviation.

Par exemple :

```
ip link
```

peut aussi s'écrire :

```
ip l
```

Lors de la configuration des interfaces réseau, vous devez exécuter les commandes en tant que root ou utilisateur avec des privilèges sudo.

Les modifications de la configuration réseau opérées ne sont pas persistantes et sont perdues au redémarrage.

Pour rendre les modifications permanentes :

Deux méthodes :

1. Ajoutez les commandes à un script de démarrage
2. Modifiez les fichiers de configuration spécifiques à la distribution.

10 commandes "IP" utiles pour configurer les interfaces réseau sur Linux

Comment attribuer une adresse IP à une interface spécifique

```
ip addr add 192.168.1.10 dev eth0
```

Comment attribuer une adresse IP à une interface spécifique

Autre exemple avec une interface eno1 :

```
sudo ip addr add 192.168.1.193/24 dev eno1
```

Ici l'interface eno1 aura pour adresse IP 192.168.1.193 avec le masque de sous-réseau 255.255.255.0.

Autre exemple, pour changer l'interface enp0s3 aura pour adresse IP 192.168.2.44 :

```
sudo ip addr add 192.168.2.44/24 dev enp0s3
```

Enfin notez que l'on peut aussi attribuer plusieurs adresses IP à une même interface réseau :

```
sudo ip addr add 10.7.8.40/24 dev eno1
```

```
sudo ip addr add 10.7.8.46/24 dev eno1
```

Anciennement avec ifconfig, cela va remplacer l'adresse IP et non la rajouter :

```
ifconfig eth1 192.168.1.10
```

Comment vérifier une adresse IP

Pour obtenir et afficher l'adresse IP des interfaces réseaux

```
ip addr show
```

Une variante de la commande ip que l'on peut utiliser :

```
ip a
```

Enfin on peut aussi utiliser ces syntaxes :


```
ip address show  
ip addr  
ip a
```

Avec ifconfig, il suffisait de saisir la commande :

```
ifconfig  
ifconfig -a
```

La présentation diffère mais le contenu reste le même avec notamment l'adresse IP et l'adresse MAC de la carte réseau.

On trouve toutes sortes d'informations :

MTU 65536 : L'unité de transfert maximale. C'est la taille du plus gros paquets de données que cette interface peut transmettre

QDisc Noqueue : Un QDISC est un mécanisme de mise en file d'attente. Il planifie la transmission de paquets. Il existe différentes techniques de file d'attente appelées disciplines. La discipline de NoQueue signifie "Envoyer instantanément, ne pas faire la queue". Il s'agit de la discipline QDISC par défaut pour les périphériques virtuels, tels que l'adresse de bouclage.

State UNKNOWN : Cela peut être en panne (l'interface réseau n'est pas opérationnelle), Inconnu (l'interface réseau est opérationnelle mais rien n'est connecté), ou up (le réseau est opérationnel et il existe une connexion). Par défaut de groupe: les interfaces peuvent être regroupées de manière logique. La valeur par défaut est de les placer dans un groupe appelé "Par défaut"

QLEN 1000 : La longueur maximale de la file d'attente de transmission

Link / Loopback / Ether : l'adresse du contrôle d'accès aux médias (Mac) de l'interface

INET : L'adresse IP version 4. La partie de l'adresse après la barre oblique (/) est la notation de routage inter-domaines sans classes (CIDR) représentant le masque de sous-réseau. Il indique combien de bits contigus de premier plan sont définis sur un dans le masque de sous-réseau. La valeur de huit signifie huit bits. Huit bits définis sur un représentent 255 en binaire, le masque de sous-réseau est de 255.0.0.0

Scope Host : la portée de l'adresse IP. Cette adresse IP n'est valide que dans l'ordinateur (l'hôte »).
LO: l'interface avec laquelle cette adresse IP est associée

Valid_lft : Durée de vie valide. Pour une adresse IP version IP allouée par le protocole de configuration d'hôte dynamique (DHCP), il s'agit de la durée de l'adresse IP considérée comme valide et capable de faire et d'accepter les demandes de connexion

Preferred_lft : Vie préférée. Pour une adresse IP version 4 IP allouée par DHCP, il s'agit de la quantité de temps que l'adresse IP peut être utilisée sans restrictions. Cela ne devrait jamais être plus grand que la valeur valid_lft

INET6 : L'adresse IP version 6 et le scope

Comment supprimer une adresse IP

Pour supprimer l'adresse IP d'une carte réseau :

```
ip addr del 192.168.1.10/24 dev eth0
```

Avec la commande ifconfig, cela donnait :

```
ifconfig eth0 0.0.0.0
```

Comment activer l'interface réseau

```
ip link set eth0 up
```

Et la version ifconfig :

```
ifconfig eth0 up
```

Ainsi lorsque vous allez lister les interfaces réseaux, celle-ci ne sera plus présente.

Comment désactiver l'interface réseau

Le paramètre down vous permet de désactiver une interface réseau.

On l'utilise ainsi :

```
ip link set eth1 down
```

Avec ifconfig :

```
ifconfig eth0 down
```

Comment vérifier la table de routage?

Tapez la commande suivante pour vérifier les informations de la table de routage du système.

```
ip route show
```

Cela donne ceci :

```
default via 37.187.125.254 dev eth0 onlink  
37.187.125.0/24 dev eth0 proto kernel scope link src 37.187.125.200
```

Je rappelle aussi qu'il existe la commande route qui permet aussi d'afficher la table de routage :

```
route -N
```

Comment ajouter une route statique

```
ip route add 10.10.20.0/24 via 192.168.50.100 dev eth0
```

Changer la route par défaut

```
ip route add default via IP adresse_ip
```

Par exemple :

```
ip route add default via IP 192.168.1.254
```

Comment supprimer une route statique

```
ip route del 10.10.20.0/24
```

Comment ajouter des routes statiques de persistance

Cela se fait dans chaque fichier de configuration réseaux qui est différent d'une distribution à l'autre.
/etc/network/interfaces

On utilise alors l'option up pour passer une commande au moment où l'interface se monte :

```
auto eth0
iface eth0 inet static
address 192.168.50.2
netmask 255.255.255.0
gateway 192.168.50.100
#####{Static Route}#####
up ip route add 10.10.20.0/24 via 192.168.50.100 dev eth0
```

Puis on relance le service networking :

```
sudo /etc/init.d/network restart
```

Comment ajouter une passerelle par défaut

La passerelle par défaut est en général l'adresse IP du routeur afin de sortir du réseau.

La commande ip route permet de créer une passerelle par défaut de cette manière :

```
ip route add default via 192.168.1.1
```

<https://www.malekal.com/commandes-ip-utiles-pour-configurer-les-interfaces-reseau-sur-linux/>

Autoriser la connexion en ssh

Ainsi, lors des phases de configuration, je vais m'affranchir des sécurités de base.

Lors d'une mise en production, il faudra impérativement désactiver cette fonction.

Une fois la connexion établie en ssh via Putty, je vais bénéficier des fonctions de **copier-coller**, ce qui me permettra de capturer plus facilement, les informations du terminal, mais aussi me permettre de préparer mes syntaxes avant de les saisir évitant ainsi les fautes de frappe.

Lors de l'installation, je coche le choix serveur ssh, ou sinon je serai obligé d'en faire l'installation à la main avec tous ce que cela implique de configuration... autant bénéficier de cette fonction dès l'installation terminé.

Sinon, une simple ligne de commande suffit à installer sshd

```
# apt install openssh-server openssh-client
```

et je me connecte depuis W10 avec PuTTY vers la VM 192.168.101.10.

Connexion depuis Windows

Ouvrir putty.exe, saisir **l'adresse ip de la carte** dans le champ « **hostname** » ainsi que 22 pour le choix du port, puis cliquer sur « open ».

Le système demande le nom d'utilisateur puis le mot de passe.

À la 1ere connexion ; Lisez et accepter le certificat.

Pour Installer SSH

Pour exemple :

S'il n'a pas été sélectionné lors de l'installation ou s'il a été désinstallé par erreur.

Installation de SSH

Installez openSSH client

```
apt-get install openssh-client
```

Installez openSSH server

```
apt-get install ssh openssh-server
```

Cette étape est longue du fait de la génération des clés de cryptage servant à authentifier le serveur.

(A priori unique car aléatoire, cette clé est échangée à la connexion du client.

Celui-ci doit accepter la clé lors de la première connexion, et refuse de se reconnecter sur le serveur ayant le même nom si cette clé change, ceci afin d'éviter les usurpations de serveur.)

Conseil : Interdire aux utilisateurs de se connecter en root directement quand ils passent par ssh.

Indépendamment de la "force" des mots de passe,

Cela oblige un intrus éventuel à connaître le login d'un autre compte avant de pouvoir passer root sur la machine.

Autoriser root en ssh

Je vous recommande de ne pas autoriser root en ssh mais plutôt d'utiliser la commande su pour passer en root ou encore la commande sudo pour votre utilisateur.

Cependant, si vous le voulez, vous pouvez autoriser la connexion ssh de root avec son mot de passe

Editer /etc/sshd_config et ajouter et/ou remplacer

```
#PermitRootLogin without-password
```

```
PermitRootLogin yes
```

Ou comme cela !

```
PermitRootLogin yes
```

```
#without-password
```

Ou avec VI

```
vi /etc/ssh/sshd_config -> édite le fichier de conf du serveur
```

```
appuyez sur "echap" puis saisissez "/PermitRootLogin without-password" -> recherche la ligne à changer
```

```
se placer sur le "w" de "without-password"
```

```
tapez "cw" (change word => changer un mot)
```

```
tapez "no"
```

```
appuyez sur "echap" puis saisissez ":wq" (sauvegarder et quitter)
```

Ainsi, vous pourrez vous connecter en root depuis putty.



Attention !!!!

Cela implique de savoir ce que l'on fait, on peut parfaitement être en root tant que le système n'est pas en production, il faudra juste penser à l'interdire de nouveau en annulant la modification, de même que l'on devra changer le port par défauts de SSH par la suite.



Attention !!!!

Enfin, relancez le serveur ssh avec la nouvelle configuration :

Relancer ssh pour la prise en compte

```
# /etc/init.d/ssh restart
```

Ou

```
# service ssh restart
```

Ou

Avec **systemd** :

```
# systemctl restart ssh
```

Les clefs SSH

OpenSSH permet une authentification par clef. Cela est très intéressant notamment pour utiliser des copies par dessus SSH, et ce sans mot de passe.

Sur le serveur qui va initier la connexion, il faut générer la clef SSH.

Nous allons donc générer une clef de 1024 bits, ce qui est suffisant pour la plupart des utilisations.

Authentification par mot de passe

C'est la méthode la plus simple. Depuis la machine cliente, tapez :

```
% ssh login@nom_DNS_du_serveur_SSH
```

Si vous utilisez le même identifiant sur le client et sur le serveur, vous pouvez vous contenter de taper :

```
% ssh nom_DNS_du_serveur_SSH
```

Si c'est la première connexion SSH depuis ce client vers ce serveur, il vous demande si le fingerprint de la clef publique présentée par le serveur est bien le bon. Pour être sûr que vous vous connectez au bon serveur, vous devez connaître de façon certaine le fingerprint de sa clef publique et la comparer à celle qu'il vous affiche. Si les deux fingerprints sont identiques, répondez yes, et la clef publique du serveur est alors rajoutée au fichier

```
~/.ssh/known_hosts.
```

Si vous vous êtes déjà connecté depuis ce client vers le serveur, sa clef publique est déjà dans le fichier `~/.ssh/known_hosts` et il ne vous demande donc rien.

Ensuite, entrez votre mot de passe...

et vous verrez apparaître le prompt, comme si vous vous étiez connecté en local sur la machine.

Authentification par clef

Au lieu de s'authentifier par mot de passe, les utilisateurs peuvent s'authentifier grâce à la cryptographie asymétrique et son couple de clefs privée/publique, comme le fait le serveur SSH auprès du client SSH.

Si vous vous êtes connecté à votre compte root à l'aide de clés SSH, l'authentification par mot de passe est désactivée pour SSH.

Vous devrez ajouter une copie de votre clé publique locale
au fichier `~/.ssh/registered_keys`
du nouvel utilisateur pour vous connecter avec succès.

Puisque votre clé publique se trouve déjà dans
le fichier `~/.ssh/registered_keys` du compte root sur le serveur, nous pouvons copier ce fichier et cette structure de répertoires dans notre nouveau compte d'utilisateur dans notre session existante à l'aide de la commande `cp`.

Ensuite, nous pouvons ajuster la propriété des fichiers à l'aide de la commande `chown` au nom de votre utilisateur habituel.

Exemple :

```
cp -r ~/.ssh /home/sammy  
chown -R sammy:sammy /home/sammy/.ssh
```

Now, open up a new terminal session and using SSH with your new username:

Ouvrez maintenant une nouvelle session de terminal et utilisez SSH avec votre nouveau nom d'utilisateur:

```
ssh utilisateur@adresse_ip_du_serveur
```

Vous devez être connecté au nouveau compte d'utilisateur sans utiliser de mot de passe.

Générer ses clefs

Pour générer un couple de clefs DSA, tapez :

```
% ssh-keygen -t dsa
```

Les clefs générées ont par défaut une longueur de 1024 bits, ce qui est aujourd'hui considéré comme suffisant pour une bonne protection.

La clef privée est stockée dans le fichier `~/.ssh/id_dsa` avec les permissions 600

et

la clef publique est stockée dans le fichier `~/.ssh/id_dsa.pub` avec les permissions 644.

Lors de la création, OpenSSH vous demande une pass phrase qui est un mot de passe pour protéger la clef privée.

Cette pass phrase sert à chiffrer la clef privée.

La pass phrase vous sera alors demandée à chaque utilisation de la clef privée,

C'est-à-dire à chaque fois que vous vous connecterez en utilisant cette méthode d'authentification.

Vous pouvez à tout moment changer la pass phrase qui protège votre clef privée avec la commande

```
ssh-keygen -p.
```

Autoriser votre clef publique

Pour cela, il suffit de copier votre clef publique dans le

```
fichier ~/.ssh/authorized_keys
```

de la machine sur laquelle vous voulez vous connecter à distance.

La commande suivante permet de réaliser cette opération via SSH :

```
% ssh-copy-id -i ~/.ssh/id_dsa.pub login@nom_DNS_du_serveur
```

La commande est la même que pour une authentification par mot de passe.

Connexion sur le port SSH (22)

À partir d'ici nous sommes donc connecter en SSH sur notre VM, faire un snapshot de la machine à ce stade par sécurité

Configuration SSH

Afin de sécuriser l'accès SSH au serveur, éditons-le fichier `/etc/ssh/sshd_config`. Nous allons changer le port de connexion par défaut pour éviter quelques attaques par bruteforce sur le port 22, qui est bien connu pour héberger ce service.

N'oubliez pas de préciser ce nouveau port (dans Putty ou en ligne de commande ssh sous Linux) à la prochaine connexion.

```
nano /etc/ssh/sshd_config
```

```
Port 2222          # Changer le port par défaut
PermitRootLogin no  # Ne pas permettre de login en root
Protocol 2         # Protocole v2
AllowUsers dew      # N'autoriser qu'un utilisateur précis
```

Redémarrez le service SSH après ces modifications :

```
/etc/init.d/ssh restart
```


Notions et paramétrages des droits



Attention !!!!



Les droits en 777 C'est le MAL !!!!

Plus sérieusement

Donner des droits en 777 revient à donner les droits à tout le monde

Le tableau ci-après permet de faire la conversion entre les différents « triplets » possibles et leur notation octale (nombre en base 8).

Triplet	Nombre binaire	Nombre octal
---	000	0
--x	001	1
-w-	010	2
-wx	011	3
r--	100	4
r-x	101	5
rw-	110	6
rwX	111	7

L'emploi de cette numérotation suppose de connaître ou de savoir retrouver aisément le nombre octal associé à chaque triplet.

Ce qui est assez simple, puisque cette numérotation est la conversion en octal de la représentation binaire du triplet.

Considérez la présence d'un droit comme un booléen valant 1 et son absence comme 0, vous obtenez alors un nombre binaire qu'il est aisé de convertir en octal (ce qui revient à du décimal car on ne passe pas aux dizaines dans la base 8).

Exemple	Droits globaux associés
chmod 640 temps.txt	rw-r-----
chmod 700 temps.txt	rwX-----
chmod 664 temps.txt	rw-rw-r--
chmod 761 temps.txt	rwXrw-r--
chmod 610 temps.txt	rw-r-----

Les droits globaux d'un fichier sont identifiés par l'association de 3 triplets de droits.
Ce qui nous fait donc $8^3=512$ combinaisons différentes

Droits globaux	Description
rwxr-xr-x	Le propriétaire a tous les droits, et le groupe ainsi que les autres n'ont pas accès en écriture.
rwxr--r--	Le propriétaire a tous les droits, et le groupe ainsi que les autres n'ont accès qu'en lecture.
rwxr-x---	Le propriétaire a tous les droits, le groupe possède les droits de lecture et d'exécution alors que les autres n'ont aucun droit.
rwx-----	Le propriétaire a tous les droits mais le groupe et les autres aucuns.
rw-r--r--	Le propriétaire possède les droits de lecture, écriture mais pas exécution. Et le groupe et les autres ont le droit en lecture.
rw-rw----	Le propriétaire et le groupe ont le droit en lecture et écriture mais les autres n'ont aucun droit.

En OCTAL

r = 4

w = 2

x = 1

- = 0

Pour rwx, on aura : $4+2+1 = 7$

Pour rw-, on aura : $4+2+0 = 6$

Pour r--, on aura : $4+0+0 = 4$

6	4	0
RW-	R--	---
4	4	4
R--	R--	R--

7	5	0
RWX	R-X	---
$7(4+2+1)$	$5(4+0+1)$	$0(0+0+0)$

```
chmod -R g+rwX /mon/rep
```

À qui s'applique, le changement

- u (user, utilisateur) représente la catégorie "propriétaire" ;
- g (group, groupe) représente la catégorie "groupe propriétaire" ;
- o (others, autres) représente la catégorie "reste du monde" ;
- a (all, tous) représente l'ensemble des trois catégories.

La modification que l'on veut faire

- + : ajouter
- - : supprimer
- = : ne rien changer

Le droit que l'on veut modifier

- r : read \Rightarrow lecture
- w : write \Rightarrow écriture
- x : execute \Rightarrow exécution

X : eXecute ⇒ exécution, concerne uniquement les répertoires et les fichiers qui ont déjà une autorisation d'exécution pour l'une des catégories d'utilisateurs.

Nous allons voir plus bas dans la partie des traitements récursifs l'intérêt du X.

Pour demo1

proprietaire groupe uti

RWX RW- R-X

7 6 5

drwxr-xrw- 4 demo1 www-data 4096 2016-03-07 20:45 demo1/

drwxrw-r-x

donc

u+rwX,g+rw-X,o+rx-w

chmod -R g+rwX

chmod u+rwX,g+r-wX,o+rx-w

Il ne restera ensuite qu'à ajouter/supprimer les utilisateurs qui font partie de ce groupe pour autoriser/refuser l'accès en écriture au(x) répertoire(s) concerné(s)

Modification du groupe primaire d'un utilisateur

Pour changer le groupe primaire de l'utilisateur <UTILISATEUR> à <GROUPE1>,

```
usermod -g <GROUPE1> <UTILISATEUR>
```

Ajout d'un groupe secondaire à un utilisateur existant

Pour ajouter un groupe secondaire <GROUPE2> un utilisateur existant <UTILISATEUR>,

```
usermod -a -G <GROUPE2> <UTILISATEUR>
```

Ajout d'un nouvel utilisateur à un groupe primaire

Pour ajouter le nouvel utilisateur <NEWUSER> et lui configurer comme groupe primaire admin,

```
useradd -g admin <NEWUSER>
```

Ajout d'un nouvel utilisateur à un groupe secondaire

Pour ajouter le nouvel utilisateur <NEWUSER> et lui configurer un comme groupe secondaire <GROUPE2>,

```
useradd -G <GROUPE2> <NEWUSER>
```

À noter qu'il est possible d'utiliser l'option -G avec plusieurs groupes.

Exemples pour ajouter <USER1> au groupe secondaire <GROUPE2> et <GROUPE3>:

```
useradd -G <GROUPE2>,<GROUPE3> <USER1>
```

Vérifier les groupes associés à un utilisateur

```
# groups <USER1>  
<USER1>: <GROUPE2> <GROUPE3>
```

Autorisations diverses

N'autorisons les compilateurs et installeurs que pour root (le numéro de version est à adapter selon la fraîcheur de votre installation) :

```
chmod o-x /usr/bin/gcc-4.1  
chmod o-x /usr/bin/make  
chmod o-x /usr/bin/apt-get  
chmod o-x /usr/bin/dpkg
```

adduser : gestion des utilisateurs

adduser et deluser

Si vous essayez de les appeler avec votre utilisateur normal, on vous dira que vous n'avez pas le droit de les utiliser. Seul root peut gérer les utilisateurs.

adduser : ajouter un utilisateur

La commande adduser permet d'ajouter un utilisateur. Vous devez au minimum fournir un paramètre : le nom de l'utilisateur à créer.

Par exemple, pour créer un compte pour AlphonseBrown :

```
root@debian11:/home# adduser AlphonseBrown  
Ajout de l'utilisateur « AlphonseBrown »...  
Ajout du nouveau groupe « AlphonseBrown » (1001)...  
Ajout du nouvel utilisateur « AlphonseBrown » (1001) avec le groupe « AlphonseBrown »...  
Création du répertoire personnel « /home/AlphonseBrown »...  
Copie des fichiers depuis « /etc/skel »...
```

Pensez à rajouter un sudo devant la commande si vous n'êtes pas déjà root ;

Tapez sudo adduser AlphonseBrown.

Si vous tentez d'exécuter la commande avec votre compte limité, vous aurez une erreur de ce genre :
« adduser : Seul le superutilisateur peut ajouter un utilisateur ou un groupe sur le système ».

Le répertoire personnel de AlphonseBrown est automatiquement créé (/home/AlphonseBrown) et son compte est préconfiguré.

On vous demande ensuite de taper son mot de passe :

```
Entrez le nouveau mot de passe UNIX :  
Retapez le nouveau mot de passe UNIX :  
passwd : le mot de passe a été mis à jour avec succès
```

Tapez le mot de passe de AlphonseBrown puis faites Entrée. Retapez-le pour valider.

Encore une fois, si vous ne voyez pas d'étoiles * quand vous tapez le mot de passe, c'est normal ; c'est une sécurité pour qu'on ne puisse pas compter le nombre de caractères derrière votre épaule.

On vous propose ensuite de rentrer quelques informations personnelles sur AlphonseBrown, comme son nom, son numéro de téléphone... Si vous voulez le faire, faites-le, mais sinon sachez que vous pouvez taper Entrée sans rien écrire

```
Modification des informations relatives à l'utilisateur AlphonseBrown
Entrez la nouvelle valeur ou « Entrée » pour conserver la valeur proposée
  Nom complet []: Alphonse Bronw
  N° de bureau []: cabine du port
  Téléphone professionnel []: idem
  Téléphone personnel []: tu m'appel pas
  Autre []: le fils de J.B
Ces informations sont-elles correctes ? [o/N] o
```

À la fin, on vous demande de confirmer par un « o » (oui) que tout est bon. Tapez Entrée et ça y est, le compte de AlphonseBrown est créé !

passwd : changer le mot de passe

S'il était nécessaire de changer le mot de passe de AlphonseBrown par la suite, utilisez la commande passwd en indiquant en paramètre le nom du compte à modifier.

```
root@debian11:/home# passwd AlphonseBrown
Entrez le nouveau mot de passe UNIX :
Retapez le nouveau mot de passe UNIX :
passwd : le mot de passe a été mis à jour avec succès
```

Attention ! Si vous appelez passwd sans préciser de compte en paramètre, c'est le mot de passe de root que vous changerez !

deluser : supprimer un compte

AlphonseBrown vous ennuie ? AlphonseBrown est parti ? Si son compte n'est plus nécessaire (ou que vous voulez vous venger) vous pouvez le supprimer avec deluser.

```
deluser AlphonseBrown
```

Aucune confirmation ne vous sera demandée !

Toutefois, cette commande seule ne supprime pas le répertoire personnel de AlphonseBrown. Si vous voulez supprimer aussi son home et tous ses fichiers personnels, utilisez le paramètre --remove-home :

```
deluser --remove-home AlphonseBrown
```

adduser et deluser sont des commandes qui n'existent que sous Debian et tous ses descendants. Partout ailleurs on doit utiliser useradd et userdel, qui sont les commandes Unix traditionnelles fonctionnant partout. Elles font globalement la même chose mais de manière beaucoup plus basique : si vous n'appellez pas passwd vous-mêmes, le compte ne sera pas activé et n'aura pas de mot de passe.

addgroup : gestion des groupes

Chaque utilisateur appartient à un groupe, par défaut le groupe porte le nom de l'utilisateur.

On peut le vérifier en regardant à qui appartiennent les dossiers dans /home via un ls -l :

```
root@debian11:~# cd /home
root@debian11:/home# ls -l
...
drwxr-xr-x 65 alphonsebrown alphonsebrown 4096 2022-02-16 19:40 alphonsebrown...
```

Souvenez-vous : la 3ème colonne indique le propriétaire du fichier ou dossier ; la 4ème indique le groupe qui possède ce fichier ou dossier.

Ainsi, le dossier alphonsebrown appartient à l'utilisateur alphonsebrown et au groupe alphonsebrown.

addgroup : créer un groupe

La commande addgroup crée un nouveau groupe.

```
root@debian11:/home# addgroup <NOM_DU_GROUPE>
Ajout du groupe « <NOM_DU_GROUPE> » (identifiant 1002)...
Terminé.
```

usermod : modifier un utilisateur

La commande usermod permet d'éditer un utilisateur. Elle possède plusieurs paramètres ; nous allons en retenir deux :

- -l : renomme l'utilisateur (le nom de son répertoire personnel ne sera pas changé par contre) ;
- -g : change de groupe.

Si je veux mettre AlphonseBrown dans le groupe <NOM_DU_GROUPE>, je ferai donc comme ceci :

```
usermod -g <NOM_DU_GROUPE> alphonsebrown
```

Et pour remettre alphonsebrown dans le groupe alphonsebrown comme il l'était avant :

```
usermod -g alphonsebrown alphonsebrown
```

Il est aussi possible de faire en sorte qu'un utilisateur appartienne à plusieurs groupes. Pour ce faire, utilisez le paramètre -G (majuscule).

```
Exemple : usermod -G <NOM_DU_GROUPE>,<AUTRE_GROUPE> alphonsebrown.
```

Séparez les noms des groupes par une virgule, sans espace entre chaque nom de groupe.

Faites très attention en utilisant usermod ! Lorsque vous avez recours à -G, l'utilisateur change de groupe et ce peu importe les groupes auxquels il appartenait auparavant.

Si vous voulez ajouter des groupes à un utilisateur (sans perdre les groupes auxquels il appartenait avant cela), utilisez -a :

```
usermod -aG <NOM_DU_GROUPE> alphonsebrown
```

delgroup : supprimer un groupe

Si vous voulez supprimer un groupe, c'est tout simple :

```
delgroup <NOM_DU_GROUPE>
```

addgroup et delgroup n'existent que sous Debian et ses dérivés (même remarque que pour adduser et deluser).

Les commandes « traditionnelles » qui fonctionnent partout sont groupadd et groupdel, mais elles offrent moins d'options.

chown : : gestion des propriétaires d'un fichier

Seul l'utilisateur root peut changer le propriétaire d'un fichier.

Supposons par exemple que alphonsebrown possède dans son répertoire personnel un fichier appelé rapport.txt.

Voici le résultat d'un ls -l pour ce fichier :

```
sysadmin@debian11:~$ ls -l rapport.txt
-rw-r--r-- 1 alphonsebrown alphonsebrown 0 2022-02-16 20:33 rapport.txt
```

Le joker * est là aussi utilisable : ls -l *.jpg afficherait uniquement les images JPEG contenues dans ce dossier.

je souhaite le « donner » à sysadmin

chown : changer le propriétaire d'un fichier

La commande chown, qui doit être utilisée en tant que root, attend deux paramètres au moins :

- le nom du nouveau propriétaire ;
- le nom du fichier à modifier.

Cela donne donc :

```
chown sysadmin rapport.txt
```

On peut voir ensuite que sysadmin est bien le nouveau propriétaire du fichier :

```
sysadmin@debian11:~$ ls -l rapport.txt
-rw-r--r-- 1 sysadmin alphonsebrown 0 2022-02-16 20:35 rapport.txt
```

chown peut aussi changer le groupe propriétaire d'un fichier !

```
chown sysadmin:<NOM_DU_GROUPE> rapport.txt
```

Cela affectera le fichier à l'utilisateur sysadmin et au groupe <NOM_DU_GROUPE>.

Il suffit de séparer par un symbole deux points (« : ») le nom du nouvel utilisateur (à gauche) et le nom du nouveau groupe (à droite).

-R : affecter récursivement les sous-dossiers

l'option -R de chown.

Elle modifie tous les sous-dossiers et fichiers contenus dans un dossier pour y affecter un nouvel utilisateur (et un nouveau groupe si on utilise la technique du deux points que l'on vient de voir).

On peut voir cinq lettres différentes. Voici leur signification :

- d (Directory) : indique si l'élément est un dossier ;
- l (Link) : indique si l'élément est un lien (raccourci) ;
- r (Read) : indique si on peut lire l'élément ;
- w (Write) : indique si on peut modifier l'élément ;
- x (eXecute) : si c'est un fichier, « x » indique qu'on peut l'exécuter. Ce n'est utile que pour les fichiers exécutables (programmes et scripts).

Si c'est un dossier, « x » indique qu'on peut le « traverser », c'est-à-dire qu'on peut voir les sous-dossiers qu'il contient si on a le droit de lecture dessus.

Si la lettre apparaît, c'est que le droit existe. S'il y a un tiret à la place, c'est qu'il n'y a aucun droit.

Les droits sont découpés en fonction des utilisateurs (figure suivante).

Le premier élément d mis à part, on constate que r, w et x sont répétés trois fois en fonction des utilisateurs :

- le premier triplet rwx indique les droits que possède le propriétaire du fichier sur ce dernier ;
- le second triplet rwx indique les droits que possèdent les autres membres du groupe sur ce fichier ;
- enfin, le dernier triplet rwx indique les droits que possèdent tous les autres utilisateurs de la machine sur le fichier.

chgrp : changer le groupe propriétaire d'un fichier

chgrp s'utilise exactement de la même manière que chown à la différence près qu'il affecte cette fois le groupe propriétaire d'un fichier.

chgrp <NOM_DU_GROUPE> rapport.txt

Cette commande affectera le fichier rapport.txt au groupe <NOM_DU_GROUPE>.

Un petit ls -l nous confirmera que rapport.txt appartient désormais à sysadmin et au groupe <NOM_DU_GROUPE> :

```
-rw-r--r-- 1 sysadmin <NOM_DU_GROUPE> 0 2022-02-16 20:36 rapport.txt
```

Exemple : Donner des droits spécifiques ftp.

On ne donne que le droit de lecture au processus apache, afin que si un pirate réussit à s'introduire dans le système via apache, il n'ait le droit que de lire les fichiers.

Configurons Linux de telle sorte que le processus apache soit lancé en tant qu'utilisateur apache.

Il faut donc que :

le propriétaire = demo1 ait les droits en lecture et écriture dans un répertoire et sur des fichiers donnés ;

le FTP = ftpuser ait les droits en lecture et écriture dans le même répertoire et sur les mêmes fichiers ;

www-data = droits en lecture uniquement dans le même répertoire et sur les mêmes fichiers.

Il faut créer un groupe pour les utilisateurs à qui on souhaite donner les droits de lecture et d'écriture.

Appelons ce groupe ftpgroup. Il faut éditer le fichier /etc/group et y ajouter :

ftpgroup:x:2001:demo1,ftpuser

avec tous les utilisateurs à qui l'on veut donner la possibilité de lire et d'écrire.

Puis sur le(s) répertoire(s) de travail, il faut appliquer les droits suivants :

```
chown www-data <repertoire>
chgrp ftpgroup <repertoire>
chmod 570 <repertoire>
```

Ce qui signifie respectivement :

Le répertoire appartient à www.data ;

Le répertoire est place dans le groupe « ftpgroup » ;

5=user:read+execute, 7=group:read+write+execute, 0=other:no access

Droits propriétaire			Droits groupe			Droits autres		
Read	Write	eXecute	Read	Write	eXecute	Read	Write	eXecute
R	-	X	R	W	X	-	-	-
4	0	1	4	2	1		0	
	5			7			0	

Triplet			Droit correspondants
-	-	-	Aucun
-	-	X	Exécution
-	W	-	Écriture
-	W	X	Écriture et exécution
R	-	-	Lecture
R	-	X	Lecture et exécution
R	W	-	Lecture et écriture
r	W	X	Lecture, écriture et exécution

Notation symbolique

Pour affecter à chaque catégorie les droits voulus, on peut utiliser une notation symbolique selon la syntaxe :

`chmod catégorie+opération+liste-des-droits fichier`

Où les termes catégorie, opération et liste des droits doivent êtres respectivement remplacés par leur notation décrite dans les tableaux suivants.

Catégorie	Description	Opération	Description	Droit	Description
u	Propriétaire (user)	+	Ajouter	r	Lecture (read)
g	Groupe	-	Retirer	w	Ecriture(write)
o	Others (autres)	=r	definir	x	Exécution(eXecute)

Comme le montre le tableau ci-dessous, la commande chmod lorsqu'elle est utilisée en notation symbolique ne permet de modifier les droits que pour une catégorie d'utilisateurs à la fois.

On peut retirer, ajouter ou définir un ou plusieurs droits en même temps.

Exemple	Description
<code>chmod g=rwx temps.txt</code>	Alloue au groupe tous les droits.
<code>chmod g-w temps.txt</code>	Retire au groupe le droit d'écriture.
<code>chmod a-rwx temps.txt</code>	Retire aux autres tous les droits.
<code>chmod u=rw temps.txt</code>	Alloue au propriétaire les droits en lecture et en écriture.
<code>chmod a+r temps.txt</code>	Rajoute aux autres le droit en lecture.

Notation numérique

L'avantage de la notation numérique sur la précédente est de permettre sur un fichier la définition absolue des droits de toutes les catégories en même temps selon la syntaxe :

```
chmod serie-de-3-chiffres fichier
```

Ainsi on remplace chacun des triplets par un nombre compris entre 0 et 7. Ce qui nous fait un nombre à trois chiffres en guise de notation numérique.

Remarques importantes

Exécutable

Un programme ne peut être exécuté que si le fichier exécutable correspondant possède le droit d'exécution dans la catégorie à laquelle appartient l'utilisateur.

Répertoire

On ne peut accéder à un fichier que si les répertoires successifs constitutifs du chemin absolu de ce fichier possèdent le droit en exécution.

Pour pouvoir lister les fichiers d'un répertoire, ce dernier doit être accessible en lecture.

Fichier

Le droit en exécution n'a aucune incidence sur un fichier non exécutable.

Par contre, un script (c'est-à-dire un fichier texte contenant des commandes du Shell) doit avoir les droits en lecture et en exécution pour pouvoir être interprété et exécuté par le Shell.

Masque de protection des fichiers (umask)

Le masque de protection de fichier permet de définir les droits par défaut de tout fichier créé.

Manipulation

Ce masque se comporte comme un filtre et utilise la notation numérique. On parle de filtre car il ne contient pas la série des 3 chiffres octaux correspondants aux droits à allouer aux fichiers, mais celle correspondant aux droits à ne pas allouer.

Le système Unix affecte à un fichier les droits globaux résultant de la soustraction des droits maxima 777 par le masque de protection.

Exemple : si le masque de protection vaut 037 alors 740 (=777-037) seront les droits alloués à tout nouveau fichier.

La commande permettant de définir un nouveau masque de protection est umask.

Syntaxe : umask *droits*

Exemple : umask 037

777	=	rwx	rwx	rwx	=	111	111	111
- 037	=	---	-wx	rwx	=	000	011	111
= 740 = rwx r-- --- = 111 100 000								

D'après cet exemple, tout nouveau fichier aura les droits 740 (rwxr----) car le masque de protection vaudra 037 (---wxrwx).

Pour connaître la valeur du masque de protection, tapez umask sans attribut.

Remarque

Lors de la création d'un fichier, même si le masque de protection spécifie le droit en exécution, ce dernier ne sera pas affecté au fichier nouvellement créé mais seulement à un répertoire. Donc, si vous créez un fichier exécutable ou un script il faudra lui rajouter manuellement le droit en exécution.

Droits étendus

SUID

Définition

Nous avons vu plus haut que chaque catégorie d'utilisateurs dispose de droits différenciés sur les fichiers. Et seul le propriétaire d'un fichier a le pouvoir de céder des droits à d'autres utilisateurs.

Lorsqu'un utilisateur lance un programme, ce programme s'approprie les droits de l'utilisateur pour la manipulation des fichiers et non pas ceux du propriétaire du fichier (sinon quel souk!).

Mais il est quelque fois nécessaire de permettre à d'autres utilisateurs l'accès à des données normalement protégées. Ce droit SUID permet de prêter à un utilisateur de façon temporaire, des droits supplémentaires par l'intermédiaire d'un programme (fichier exécutable).

En exécutant un programme possédant un droit SUID, un utilisateur s'approprie les droits du propriétaire du fichier exécutable durant le temps d'exécution du programme. Ces droits supplémentaires ne sont valables que sur les fichiers appelés par le programme et les opérations effectuées par le programme et que durant le temps d'exécution du programme.

Son utilité vient du fait qu'il n'est pas besoin d'accorder durablement des droits étendus à n'importe qui sur des fichiers sensibles. Puisque l'accès à ces fichiers est filtré par un programme qui est seul à prendre des initiatives sur ces fichiers.

Exemple

L'exemple le plus flagrant est celui du programme `/usr/bin/passwd (rws--x--x)` qui appartient à l'utilisateur `root`. Ce programme possède le droit `s` en lieu et place du droit `e` en exécution du triplet du propriétaire. Ce programme sert à modifier votre mot de passe personnel qui est stocké dans le fichier `/etc/passwd (rw-r--r--)` appartenant à `root` dont vous n'avez pas les droits en écriture.

Comment donc modifier votre mot de passe si vous n'êtes pas autorisé à écrire sur le fichier stockant les mots passés ?!! Pour des raisons de sécurité évidentes, le `root` interdit à quiconque de pouvoir modifier ou supprimer ce fichier. Par contre le programme `/usr/bin/passwd` vous y autorise grâce au droit SUID : vous utilisez le droit en écriture du `root` durant l'exécution du programme qui change votre mot de passe.

Manipulation

Pour ajouter un droit SUID à un programme, utiliser la commande `chmod` de la même manière que vous procéderiez pour un droit normal.

Notation symbolique

Syntaxe : `chmod u+s fichier-exécutable`.

Exemple : `chmod u+s data/hotprog`.

Notation numérique

La valeur numérique d'un SUID est 4000 et s'ajoute à la valeur de la série numérique globale.

Syntaxe : `chmod 4+droits fichier-exécutable`.

Exemple : `chmod 4755 monprog`.

Dans cet exemple on donne les droits `rwsr-xr-x` au fichier `monprog`. Ne pas oublier que le droit SUID s'affiche à la place du droit en exécution du propriétaire sans que ce dernier soit supprimé!
Nota : la présence du droit SUID suppose la présence du droit en exécution qui permet de lancer le fichier exécutable.

SGID

Le droit SGID fonctionne différemment selon qu'il est affecté à un fichier exécutable ou à un répertoire.

Exécutable

Sur un fichier exécutable, le SGID est similaire au droit SUID vu précédemment sauf qu'il donne à un utilisateur les droits du groupe auquel appartient le propriétaire de l'exécutable et non plus les droits du propriétaire.

Répertoire

Tout fichier créé porte les droits du masque de protection de son propriétaire. De plus, tout fichier porte un UID (identificateur de propriétaire) et un GID (identificateur de groupe). C'est-à-dire qu'un fichier est toujours identifié par le nom de son propriétaire ainsi que par le nom du groupe auquel appartient le propriétaire.

Le droit SGID, lorsqu'il est affecté à un répertoire, casse cette logique. Puisque tout nouveau fichier créé dans un répertoire marqué par le SGID sera de groupe non pas celui du propriétaire du fichier mais celui du propriétaire du répertoire.

Ainsi, tout fichier créé dans un répertoire portant le SGID, héritera du groupe du propriétaire du répertoire.

Manipulation

La valeur numérique du droit SGID est 2000, il est symbolisé par la lettre `s` et est affiché à la place du droit d'exécution du groupe.

Notation symbolique

Syntaxe : `chmod g+s fichier-exécutable/répertoire`.

Exemple : `chmod g+s data/`.

Notation numérique

Syntaxe : `chmod 2+droits fichier-exécutable/répertoire`.

Exemple : `chmod 2755 monprog`.

Dans cet exemple on donne les droits `rwxr-sr-x` au fichier `monprog`. Ne pas oublier que le droit GUID s'affiche à la place du droit en exécution du groupe sans que ce dernier soit supprimé!

Sticky Bit

Le droit Sticky Bit (appelé aussi *bit collant*) est alloué à la catégorie autres d'un répertoire.

Il permet d'interdire à tout utilisateur (sauf le `root`) de supprimer un fichier dont il n'est pas le propriétaire, quels que soient ses droits.

Si le répertoire en question est accessible en écriture par n'importe quel utilisateur (`rwxrwxrwx`), n'importe qui peut poser ce bit collant qui protège tous les fichiers d'une suppression ou modification de la part d'un utilisateur autre que son propriétaire.

Ce bit collant permet donc d'aller à l'encontre du droit en écriture d'un répertoire dont héritent les fichiers du répertoire.

Sa valeur numérique est 1000 et est représentée symboliquement par `t`.

Exemple : `chmod 1755 tmp/`.

Exemple : `chmod a+t tmp/`.

Ce droit s'affiche en lieu et place du droit en exécution de la catégorie autres.

Travail sur les partitions

Nous allons commencer par découvrir notre système de fichier

le programme du

```
# apt-get install du
```

"du" permet de customiser l'affichage des informations et d'effectuer au besoin des tris pour tracker les fichiers les plus lourds et faire de la place si nécessaire.

Un "du -g" permet d'afficher l'espace disponible mais en Mo.

la commande du (disk usage) pour afficher les fichiers du plus lourd au moins lourd.

exemple :

```
du -ah | sort -rn > espace.txt
```

Vérifier l'espace disque sous une Debian

la commande "df -h" pour vérifier l'espace disque sur une distribution GNU/Linux de type Debian.

```
# df -h
```

La commande df

Saisissez ...

```
# man df
```

Afin d'afficher le manuel de la commande df

et la touche "q" pour quitter le manuel

```
# df -h(human)
```

```
# df -Th (affiche le Type en plus)
```

puis

```
root@debian:~# df -h
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
/dev/sda1      5,1G  964M  3,9G  20% /
udev           10M    0  10M   0% /dev
tmpfs          403M   5,4M  397M   2% /run
tmpfs          1006M    0 1006M   0% /dev/shm
tmpfs          5,0M    0  5,0M   0% /run/lock
tmpfs          1006M    0 1006M   0% /sys/fs/cgroup
/dev/sda6       14G   36M  13G   1% /home
root@debian:~#
```

repérer les différentes partitions

```
/dev/sda1      5,1G  964M  3,9G  20% /
/dev/sda6       14G   36M  13G   1% /home
```


maintenant nous allons afficher le contenu du dossier /dev/

```
ls -l /dev/
```

la liste est longue

affinons la recherche avec uniquement sd et le joker *

```
root@debian:~# ls -l /dev/sd*  
brw-rw---- 1 root disk 8, 0 mars  8 18:33 /dev/sda  
brw-rw---- 1 root disk 8, 1 mars  8 18:33 /dev/sda1  
brw-rw---- 1 root disk 8, 2 mars  8 18:33 /dev/sda2  
brw-rw---- 1 root disk 8, 5 mars  8 18:33 /dev/sda5  
brw-rw---- 1 root disk 8, 6 mars  8 18:33 /dev/sda6
```

nous voyons ici nos partitions.

Ajout d'un disque supplémentaire

nous allons maintenant ajouter un 2eme disque dur.

pour cela nous arrêtons la vm et de la même manière que si nous intervenions sur du matériel réel, nous ajoutons un disque SATA

stopper le système proprement

sur la machine

Vous pouvez aussi appuyer sur la combinaison de touches Ctrl+Alt+Del.

Vous pouvez aussi vous connecter en tant que super utilisateur et exécuter l'une de ces commandes :

```
poweroff  
halt  
shutdown -h now
```

Quand les combinaisons de touches ne fonctionnent pas ou si vous préférez exécuter des commandes. Pour redémarrer le système, utilisez la commande reboot.

Puis ajouter un disque supplémentaire via le panel VirtualBox

nommer sata1,(le sata0 étant le disque present) d'une taille de 20 GO au format Qcow.

redémarrer la machine , logger vous en SSH et vérifier a nouveau

```
root@debian:~# ls -l /dev/sd*  
brw-rw---- 1 root disk 8, 0 mars  8 19:16 /dev/sda  
brw-rw---- 1 root disk 8, 1 mars  8 19:16 /dev/sda1  
brw-rw---- 1 root disk 8, 2 mars  8 19:16 /dev/sda2  
brw-rw---- 1 root disk 8, 5 mars  8 19:16 /dev/sda5  
brw-rw---- 1 root disk 8, 6 mars  8 19:16 /dev/sda6  
  
brw-rw---- 1 root disk 8, 16 mars  8 19:16 /dev/sdb
```

notre disque est présent

mais il n'est pas utilisable, nous devons le formater, le monter vers un fichier, et rendre ce montage permanent

il nous servira par exemple d'emplacement de sauvegarde de /home

VirtualBox : Debian –Version 9.2

Créer une partition

```
root@debian:~# fdisk /dev/sdb
```

Bienvenue dans fdisk (util-linux 2.25.2).

Les modifications resteront en mémoire jusqu'à écriture.

Soyez prudent avant d'utiliser la commande d'écriture.

Le périphérique ne contient pas de table de partitions reconnue.

Created a new DOS disklabel with disk identifier 0x8caf9689.

Commande (m pour l'aide) : p

Disque /dev/sdb : 20 GiB, 21474836480 octets, 41943040 secteurs

Unités : secteur de 1 à 512 = 512 octets

Taille de secteur (logique / physique) : 512 octets / 512 octets

taille d'E/S (minimale / optimale) : 512 octets / 512 octets

Type d'étiquette de disque : dos

Identifiant de disque : 0x8caf9689

On commence par créer une nouvelle partition, on indique "n" et on valide avec "Entrée".

Commande (m pour l'aide): n

Type de partition :

p primaire (0 primaire(s), 0 étendue(s), 4 libre(s))

e étendue

En formatage de base,

Il est possible de créer 4 partitions primaires sur un disque dur, actuellement il n'y en a aucune, comme l'indique la mention "4 libre(s)". Ici nous n'utilisons pas LVM.

Notes : LVM (Logical Volume Manager) permet de gérer des partitions logiques, et non pas physiques, ce qui a notamment comme avantage de pouvoir plus facilement modifier leur taille.

Pour en créer une, on indique "p" et on valide.

Ensuite, on la positionne en numéro 1 comme la place est disponible, et on valide automatiquement pour le "Premier secteur" et le "Dernier secteur" afin de disposer d'une partition unique qui remplit tout le disque.

Supprimer une partition

Soyez sûr d'être bien sur le bon disque, Indiquez "d" et si vous effectuez "p" à nouveau ensuite, vous verrez qu'il n'y a plus de partitions.

Sélection (p par défaut) : p

Numéro de partition (1-4, par défaut 1): 1

Premier secteur (2048-41943039, par défaut 2048):

Utilisation de la valeur par défaut 2048

Dernier secteur, +secteurs or +taille{K,M,G} (2048-41943039, 41943039 par défaut):

Utilisation de la valeur par défaut 41943039

Maintenant que la partition est définie, on va indiquer le système de fichier que l'on souhaite utiliser grâce à "t".

Commande (m pour l'aide) : t

Partition 1 sélectionnée

Code Hexa (taper L pour afficher tous les codes) :L

0	Vide	24	NEC DOS	81	Minix / Linux a bf	Solaris
1	FAT12	27	TFS WinRE masqu	82	partition d'éch c1	DRDOS/sec (FAT-
2	root XENIX	39	Plan 9	83	Linux	c4 DRDOS/sec (FAT-
3	usr XENIX	3c	récupération Pa	84	OS/2 masquée di	c6 DRDOS/sec (FAT-
4	FAT16 <32M	40	Venix 80286	85	Linux étendue	c7 Syrinx
5	etendue	41	PPC PReP Boot	86	NTFS volume set da	Non-FS data
6	FAT16	42	SFS	87	NTFS volume set db	CP/M / CTOS / .
7	HPFS/NTFS/exFAT	4d	QNX4.x	88	Linux plaintext de	Dell Utility
8	AIX	4e	2e partie QNX4.	8e	LVM Linux	df BootIt
9	Amorçable AIX	4f	3e partie QNX4.	93	Amoeba	e1 DOS access
a	Gestionnaire d'	50	OnTrack DM	94	Amoeba BBT	e3 DOS R/O
b	W95 FAT32	51	OnTrack DM6 Aux	9f	BSD/OS	e4 SpeedStor
c	W95 FAT32 (LBA)	52	CP/M	a0	IBM Thinkpad hi	eb BeOS fs
e	W95 FAT16 (LBA)	53	OnTrack DM6 Aux	a5	FreeBSD	ee GPT
f	etendue W95 (LB	54	OnTrackDM6	a6	OpenBSD	ef EFI (FAT-12/16/
10	OPUS	55	EZ-Drive	a7	NeXTSTEP	f0 Linux/PA-RISC b
11	FAT12 masquée	56	Golden Bow	a8	UFS Darwin	f1 SpeedStor
12	Compaq diagnost	5c	Priam Edisk	a9	NetBSD	f4 SpeedStor
14	FAT16 masquée <	61	SpeedStor	ab	Amorçage Darwin	f2 DOS secondaire
16	FAT16 masquée	63	GNU HURD ou Sys	af	HFS / HFS+	fb VMware VMFS
17	HPFS/NTFS masqu	64	Novell Netware	b7	BSDI fs	fc VMware VMKCORE
18	AST SmartSleep	65	Novell Netware	b8	partition d'éch	fd RAID Linux auto
1b	W95 FAT32 masqu	70	DiskSecure Mult	bb	Boot Wizard mas	fe LANstep
1c	W95 FAT32 masqu	75	PC/IX	be	Amorçage Solari	ff BBT
1e	W95 FAT16 masqu	80	Minix ancienne			

Code Hexa (taper L pour afficher tous les codes) :83

Type de partition « Linux » modifié en « Linux ».

Commande (m pour l'aide) : w

La table de partitions a été altérée.

Appel d'ioctl() pour relire la table de partitions.

Synchronisation des disques.

root@debian:~#

reste a formater cette partition en EXT4 avec des blocs de 4096 octets.

mkfs.ext4 -b 4096 /dev/sdb1

```

root@debian:~# mkfs.ext4 -b 4096 /dev/sdb1
mke2fs 1.42.12 (29-Aug-2014)
En train de créer un système de fichiers avec 5242624 4k blocs et 1310720 i-noeuds.
UUID de système de fichiers=4e3f4ac0-c4d6-43ca-858b-fc73aef54246
Superblocs de secours stockés sur les blocs :
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000

Allocation des tables de groupe : complété
écriture des tables d'i-noeuds : complété
Création du journal (32768 blocs) : complété
écriture des superblocs et de l'information de comptabilité du système de
fichiers : complété

```

Vérification des partitions des lecteurs

```

# e2fsck -f /dev/sda1
# e2fsck -f /dev/sdb1

```

```

mkdir /mnt/save
chmod 777 /mnt/save
mount -t ext4 /dev/sdb1 /mnt/save

```

```

root@debian:~# df -Th
Sys. de fichiers Type  Taille Utilisé Dispo Util Monté sur
/dev/sda1    ext4   5,1G  965M  3,9G  20% /
udev        devtmpfs 10M    0  10M   0% /dev
tmpfs       tmpfs   403M   5,5M  397M   2% /run
tmpfs       tmpfs  1006M    0 1006M   0% /dev/shm
tmpfs       tmpfs   5,0M    0  5,0M   0% /run/lock
tmpfs       tmpfs  1006M    0 1006M   0% /sys/fs/cgroup
/dev/sda6    ext4   14G   36M  13G   1% /home
/dev/sdb1    ext4   20G   44M  19G   1% /mnt/save

```

```
fdisk -l
```

```

Disque /dev/sda : 20 GiB, 21474836480 octets, 41943040 secteurs
Unités : secteur de 1 × 512 = 512 octets
Taille de secteur (logique / physique) : 512 octets / 512 octets
taille d'E/S (minimale / optimale) : 512 octets / 512 octets
Type d'étiquette de disque : dos
Identifiant de disque : 0xa0059dbb

```

Device	Boot	Start	End	Sectors	Size	Id	Type
/dev/sda1	*	2048	11003903	11001856	5,3G	83	Linux
/dev/sda2		11005950	41940991	30935042	14,8G	5	Extended
/dev/sda5		11005952	12396543	1390592	679M	82	Linux swap / Solaris
/dev/sda6		12398592	41940991	29542400	14,1G	83	Linux

Disque /dev/sdb : 20 GiB, 21474836480 octets, 41943040 secteurs

Unités : secteur de 1 × 512 = 512 octets

Taille de secteur (logique / physique) : 512 octets / 512 octets

taille d'E/S (minimale / optimale) : 512 octets / 512 octets

Type d'étiquette de disque : dos

Identifiant de disque : 0x8caf9689

Device	Boot	Start	End	Sectors	Size	Id	Type
/dev/sdb1		2048	41943039	41940992	20G	83	Linux

root@debian:/mnt/save# blkid

/dev/sda1: UUID="704f3250-9043-4cc1-a80c-c5ca134e2279" TYPE="ext4" PARTUUID="a0059dbb-01"

/dev/sda5: UUID="b10b7878-886f-4890-9f34-939ff0534dd3" TYPE="swap" PARTUUID="a0059dbb-05"

/dev/sda6: UUID="a13179a1-dd9b-446c-b1a1-da935f5e427c" TYPE="ext4" PARTUUID="a0059dbb-06"

/dev/sdb1: UUID="4e3f4ac0-c4d6-43ca-858b-fc73aef54246" TYPE="ext4" PARTUUID="8caf9689-01"

Après un redémarrage, la partition ne sera pas montée automatiquement.

Pour cela, il faut éditer le fichier /etc/fstab,

```
# /dev/sdb1 /data ext4 defaults, 0 0
UUID=4e3f4ac0-c4d6-43ca-858b-fc73aef54246 /mnt/save ext4 defaults 0 0
```

nano /etc/fstab

/etc/fstab: static file system information.

#

Use 'blkid' to print the universally unique identifier for a

device; this may be used with UUID= as a more robust way to name devices

that works even if disks are added and removed. See fstab(5).

#

<file system> <mount point> <type> <options> <dump> <pass>

/ was on /dev/sda1 during installation

UUID=704f3250-9043-4cc1-a80c-c5ca134e2279 / ext4 errors=remount-ro 0 1

/home was on /dev/sda6 during installation

UUID=a13179a1-dd9b-446c-b1a1-da935f5e427c /home ext4 defaults 0 2

swap was on /dev/sda5 during installation

UUID=b10b7878-886f-4890-9f34-939ff0534dd3 none swap sw 0 0

```
/dev/sr0    /media/cdrom0  udf,iso9660 user,noauto  0    0
# /dev/sdb1 /data ext4 defaults, 0    0
UUID=4e3f4ac0-c4d6-43ca-858b-fc73aef54246 /mnt/save ext4 defaults 0 0
```

La commande mount -a permet de relire/réaffecter le contenu du fichier /etc/fstab

```
# mount -a
```

On pourra alors vérifier la présence de notre nouveau disque en listant les montages de notre système

```
# mount
```

voilà , au reboot notre disque sata1 de 20 Go, sera accessible par le chemin /mnt/save

À quel système de fichiers appartient un fichier.

```
# df /home/fichier.txt
```

Liste les différents disques et le nombre de blocs.

```
# sfdisk -s
```

Liste les partitions du système.

```
# fdisk -l
```

Affiche toutes les partitions.

```
# sfdisk -l
root@pve:/dev# fdisk -l
```

Vérifier la configuration des disques.

Commande introuvable !

```
# lvs -a -o +devices
```

```
# lvs -a -o +devices
LV VG Attr   LSize Pool Origin Data% Meta% Move Log Cpy%Sync Convert Devices
root pve -wi-ao---- 35,00g                               /dev/md0(0)
swap pve -wi-ao---- 1,00g                               /dev/md0(8960)
```

NOTA BENE :

Si vous constatez que les droits de root sur le système ont été altérés ou que certaines commandes nécessitent l'utilisation de sudo alors qu'elles ne devraient pas, vous pouvez essayer de rétablir les droits de root en suivant les étapes suivantes :

Vérifiez si le compte root est actif :

Assurez-vous que le compte root est actif en utilisant la commande "sudo passwd -S root".

Si le compte root est désactivé, vous pouvez l'activer en utilisant la commande "sudo passwd root".

Vérifiez les fichiers de configuration :

Vérifiez les fichiers de configuration du shell pour vous assurer que les commandes nécessitant des privilèges administratifs sont correctement identifiées comme telles.

Vérifiez également les fichiers de configuration des applications pour vous assurer qu'elles sont configurées pour fonctionner avec l'utilisateur root.

Vérifiez les autorisations des fichiers système :

Assurez-vous que les autorisations des fichiers système sont correctes.

Vous pouvez utiliser la commande "ls -l" pour afficher les autorisations de chaque fichier.

Si les autorisations ne sont pas correctes, vous pouvez les corriger en utilisant la commande "chmod" ou "chown".

Vérifiez les fichiers journaux :

Consultez les fichiers journaux du système pour détecter des erreurs ou des dysfonctionnements qui pourraient affecter les droits de root.

Les fichiers journaux se trouvent généralement dans le répertoire /var/log.

Si ces étapes ne résolvent pas le problème, vous pouvez envisager de réinstaller le système d'exploitation pour rétablir les droits de root par défaut.

Cependant, cela peut être une solution de dernier recours et vous devriez sauvegarder toutes vos données importantes avant de réinstaller le système.