

2024

INF236 – TP DevOps Linux et plus...



VirtualBox : Debian –Version 7.0

- ©2009-2024 - Donat FUZELLIER - seo-webranking.com

Donat FUZELLIER

Seo-webranking

25/04/2024

Sommaire

Comment utiliser ce document ?	8
Raccourci clavier pour faire le signe dièse (#) sur PC	8
Quelle différence entre les deux ?	8
Comment faire le symbole dièse « croisillon » (réseaux sociaux et écriture web) sur PC	8
Sur clavier Azerty	8
Sur clavier Qwerty	8
Touche dièse sur Mac	8
Comment faire le symbole dièse musical (Sharp key = #) sur PC ?	8
Comment faire ce symbole en HTML :	8
Prérequis	10
Matériel	10
Environnement de travail	10
Informations	11
Disparition des commandes ifconfig et netstat.	11
Tableau d'adressage	12
Mot de passe et utilisateur	12
INF236 - Linux DevOps	13
Etape 1	15
Installer quelques outils	16
Avant docker	18
Créer le fichier ooconfigauto :	18
Exemple de création automatique en ligne de commande	19
Exemple avec la command echo :	19
Retour écran pour les méthodes	19
Notes sur l'utilisation de la commande printf:	20
Installer en root	21
Générer une somme de contrôle	21
Contrôler une somme de contrôle	22
Installation de Docker sous Debian 11 Bullseye	24

Vérification des étapes précédentes	24
L'installation est terminée	25
Voir la version de Docker	25
Tester Docker	26

Différence entre Docker et Kubernetes ?

Installation de Portainer	27
Comment trouver l'adresse ip du container	28
Docker inspect	30
Configuration	32
Mettre à jour Portainer	32
Cas concrets	33
Création Dockkerfile	34
Créer une image	35
Création d'un Dockerfile	36
Docker image build	36
Comment entrer dans le container pour le configurer	38
Commandes utiles	39
Démarrer ou arrêter un container :	39
Supprimer tous les container actif:	40
Supprimer une image docker	40
# Trouvez et notez votre adresse IP ↑	40

Annexes générales

Réinitialiser le mot de passe Root d'une Debian

Pré-requis

Obtenir des informations sur le statut du système

Afficher le statut du système :	44
Lister les unités échouées :	44
Lister les fichiers unités installés :	44
Pour connaître son système de démarrage, taper :	44
Vérifier et activer rc.local au démarrage	44
tty	44
getty	44

Créer une session avec SCREEN	45	Définitions.....	54
PERSONNALISATION	45	PV : Volume Physique.	54
IOTOP panneau d'information HardWare	45	VG : Groupe de Volumes.	54
commande htop.....	45	LV : Volume logique.	54
Edition de l'interface.....	46	Labels	55
Copie de sauvegarde d'un fichier.....	46	lvmdiskscan.....	58
Test de l'accès au WAN et de la résolution DNS	46	1 -Augmenter la taille du disque dur virtuel sous	
Afficher la realese	47	virtualbox.....	59
# apt-cache search --names-only	47	2 - Localiser le disque dur virtuel ainsi que son type	
Configuration de network-manager sous forme		59
graphique au sein du bureau KDE.....	47	Convertisseur en ligne	59
Voir les logs :	48	Sous Windows.....	59
Vérifier les ports.....	48	2eme avec erreur.....	60
La commande host.....	48	Utiliser Knoppix !.....	61
Mise à jour	49	Autoriser la connexion en ssh.....	61
Changer le hostname de votre debian.....	49	Connexion depuis Windows	62
Voir les paramètres.....	49	Pour Installer SSH.....	62
Ou placer les scripts	50	Installation de SSH	62
Gestion des services Debian ponctuellement....	50	Installez openSSH client.....	62
Désactiver le service du démarrage.....	50	Installez openSSH server.....	62
Supprimer les fichiers.....	50	Autoriser root en ssh	62
Sources.list	50	Les clefs SSH.....	63
Exemple de Fichier sources.list	51	Authentification par clef	64
Modification du sources.list.....	51	Générer ses clefs.....	65
Vérifier le fichier resolv.conf ou la résolution des		Autoriser votre clef publique	65
noms de domaines.....	51	Connexion sur le port SSH (22)	65
Vérifier et activer rc.local au démarrage	52	Configuration SSH	65
Compression TAR	52	Notions et paramétrages des droits	67
Taille d'un dossier	53	Les droits en 777 C'est le MAL !!!!.....	67
Trouver les fichiers contenant une chaine de		En OCTAL.....	69
caractère	53	À qui s'applique le changement.....	69
Supprimer des SVN	53	La modification que l'on veut faire	69
vider les .logs.....	53	Le droit que l'on veut modifier	69
Pour vider un fichier sous Unix ou linux, il faut		Modification du groupe primaire d'un utilisateur	
effectué cette manipulation :	#	53	70
LVM.....	54		

Ajout d'un groupe secondaire à un utilisateur existant.....	70	Répertoire.....	80
Ajout d'un nouvel utilisateur à un groupe primaire.....	70	Manipulation.....	80
Ajout d'un nouvel utilisateur à un groupe secondaire.....	70	Sticky Bit.....	80
Vérifier les groupes associés à un utilisateur.....	70	Sauvegarde des droits.....	81
Autorisations diverses.....	70	Ajouter sudo	84
adduser : gestion des utilisateurs	71	Installation de sudo	84
passwd : changer le mot de passe	72	Configuration de base de sudo	84
deluser : supprimer un compte.....	72	Activer le forwarding	86
addgroup : gestion des groupes.....	73	Travail sur les partitions.....	87
addgroup : créer un groupe	73	le programme di	87
usermod : modifier un utilisateur	73	Vérifier l'espace disque sous une Debian	87
delgroup : supprimer un groupe	74	La commande df	87
chown : changer le propriétaire d'un fichier	74	Ajout d'un disque supplémentaire	88
l'option -R de chown.	75	Créer une partition	89
chgrp : changer le groupe propriétaire d'un fichier	75	Supprimer une partition	90
Exemple : Donner des droits spécifiques ftp.	75	Vérification des partitions des lecteurs	91
Notation symbolique	76	A quel système de fichiers appartient un fichier.	93
Notation numérique	77	Liste les différents disques et le nombre de blocs.	93
Remarques importantes	77	Liste les partitions du système.....	93
Exécutable	77	Affiche toutes les partitions.....	93
Répertoire	77	Vérifier la configuration des disques.	93
Fichier.....	77	VirtualBox	94
Masque de protection des fichiers (umask)	77	Extension VirtualBox.....	94
Manipulation.....	78	1] Type de carte réseau	94
Remarque.....	78	2] Réseau Invité <-> Système Hôte	94
Droits étendus.....	79	3] Réseau Invité <-> Réseau Hôte / Internet.....	95
SUID.....	79	4] Réseau Invité <-> Réseau Invité	95
Exemple.....	79	5] Réseau Invité -> Système Hôte / Internet	95
Manipulation.....	79	Man-pages	98
Notation numérique	79	Obtenir les manpages en Français.....	98
SGID.....	80	Sources :.....	99
Exécutable	80	Liens utiles	99
		FIN.....	99

Ce document reste sous la propriété de Donat FUZELLIER.

Il vous a été remis à titre d'exemple.

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.

Vos expériences, vos tests et échecs vous amèneront vers une solution stable et viable...

Donat FUZELLIER

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 pour ce qui suis.

VirtualBox : Debian –Version 7.0



Attention !!!!

Dans un script ou un fichier de configuration, le « # » sert à commenter le texte, ce qui suit ce symbole n'est pas traité.

Au sein des 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 en, « .bak » ou « .original », ou à votre convenance, pour cela utiliser la commande **CP**.

C'est une convention de nommage, l'extension ne sert qu'à clarifier et simplifier la recherche.

`cp /CHEMIN/VERS/LE/FICHER<ESPACE>/CHEMIN/VERS/LA/COPIE<POINT><EXTENSION en BAK ou ORI>`

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 outils** ».

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...

Donat FUZELLIER

ATTENTION : les plages IP de ce document ne sont là qu'à titre informatif.

Les retours de commande et autres captures d'écran peuvent provenir d'autres VM.

Prérequis

- Comprendre les principes d'adressage réseau en ipv4.
- Pensez à adapter les masques et autres adresses IP de ce document.

Matériel

1 PC avec une connexion internet
Le logiciel VirtualBox
1 image ISO de Debian
1 image ISO des extensions VirtualBox

Environnement de travail

Mon Pc est sous Windows 10 Pro 64 Bits.

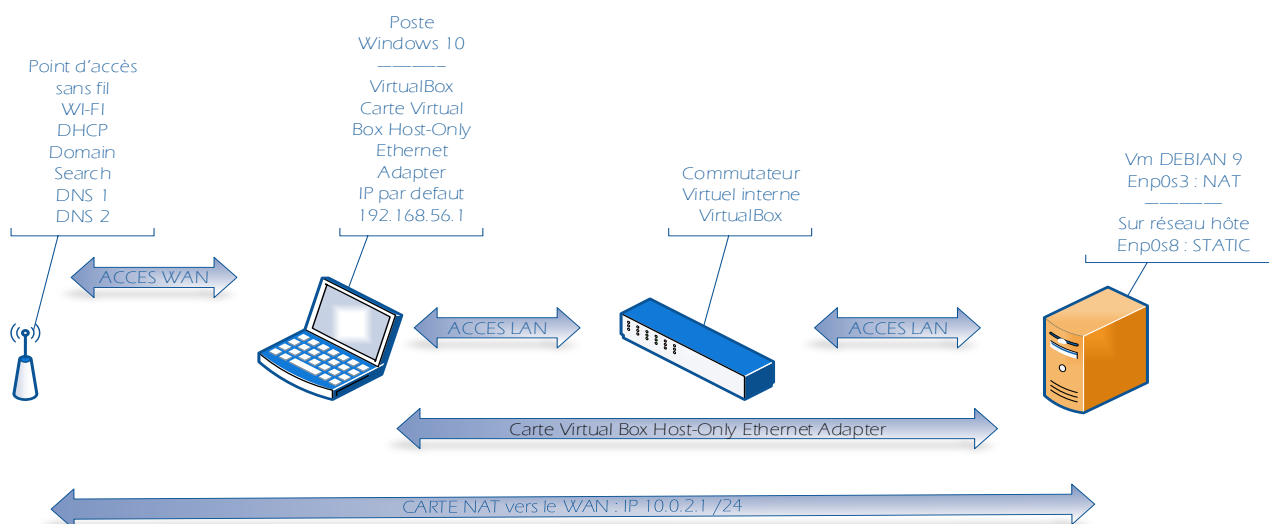
Lisez les explications en annexe et paramétrer votre réseau afin de « pinguer », de la machine hôte vers la machine virtuel afin de nous connecte en **ssh** depuis notre hôte.

Vous pouvez installer 2 cartes réseaux sur votre VM, une sur le WAN avec DHCP en NAT et l'autre en réseau privé hôte avec DHCP ou en IP Statique.

Il est possible de créer un réseau « natté », avec des règles de redirections de ports

Vous pouvez aussi mettre en place une redirection de port sur l'adresse NAT, vérifier l'adresse avec « ip addr ».

Noter dans un tableau vos paramètres IP, les adresses MAC, les appellations de carte, ceci vous sera utile par la suite. Afin d'éviter une possible confusion, choisissez deux modelés de cartes différentes.



Les exemples étant sous VirtualBox, si vous utilisez un autre hyperviseur, pensez que 2 hyperviseurs ont le plus grand mal du monde à cohabiter sur un poste Windows.

Informations.

Disparition des commandes ifconfig et netstat.

Le paquet net-tools n'est plus installé d'origine dans Stretch, net-tools est abandonné depuis 2001, de plus, la nomenclature existante eth0, wlan0 disparaît.

Depuis 2013, udev utilise la nouvelle nomenclature ifname, basée sur les caractéristiques du matériel et non plus sur l'adresse MAC. Voir ce lien pour mieux comprendre: [Understanding_the_Predictable_Network_Interface_Device_Names](#)

e = ethernet

w=wifi

les commandes suivantes ne sont plus disponibles :

- * Arp
- * Ifconfig
- * Iptunnel
- * Nameif
- * Netstat
- * Route
- * Iwconfig est déprécié? mais répond encore

tout passera par la commande ip

ifconfig => ip addr

les différents "objets" possibles après ip sont : link | address | addlabel | route | rule | neigh | ntable | tunnel | tuntap | maddress | mroute | mrule | monitor | xfrm | netns | l2tp | fou | macsec | tcp_metrics | token | netconf | ila

Si la commande netstat est présente...

La commande netstat Linux peut prendre de nombreux paramètres. Mais voici une bonne base :

```
netstat -paunt
-a : Tous les ports
-t : Tous les ports TCP
-u : Tous les ports UDP
-l : Tous les ports en écoute
-n : Affiche directement les IP. Pas de résolution de nom.
-p : Affiche le nom du programme et le PID associé.
```

Comment lire les résultats de la commande netstat, par colonnes :

Proto : le protocole utilisé. Les classiques TCP et UDP mais également TCP6 et UDP6 pour les variantes IPV6.
Recv-Q : Le nombre de Bytes dans la file d'attente de réception. Devrait toujours être à zéro
Send-Q : Le nombre de Bytes dans la file d'attente d'envoi. Devrait toujours être à zéro
Adresse locale : l'adresse et le port utilisé sur la machine locale
Adresse distante : l'adresse et le port utilisé par la machine distante
Etat : LISTEN quand le programme écoute et attend une connexion. ESTABLISHED lorsque la connexion est établie.
PID/Program name : Le numéro de processus et le nom du programme

Si vous voulez continuer à utiliser netstat, il vous faudra installer les net-tools, mais ceux-ci sont en passe d'être abandonnés.

Tableau d'adressage

Machines	Adresse IPv4	MASQUE	Passerelle	Interfaces	

Mot de passe et utilisateur

Machines	Utilisateurs	Mot de passes	Root	Mot de passe root

ATTENTION



```
### Bascule temporaire du clavier en français
# setxkeymap fr
### Reconfiguration des langues du système
# sudo dpkg-reconfigure locales
### Reconfiguration permanente du clavier
# sudo dpkg-reconfigure keyboard-configuration
### Reconfiguration de l'horloge système et Timezone avec Europe/Paris et le format de l'heure.
```

```
## Passer la VM avec 256 Mo de video
## depuis la ligne de commande (cmd)
# cd I:\VirtualBox\
# VBoxManage modifyvm "kali-linux-2021.4a" --vram 256
```


Etape 1

Sous virtualbox vous pouvez ajouter un dossier partager avec votre hôte et vos VMs. Je choisis le dossier sur mon poste windows et je déclare un point de montage pour la vm , exemple : /<DOSSIER>. Ici /vpn.

Pour cela il faut installer les extensions invite de Virtualbox a partir du cd rom de virtual box

Tester les commandes suivantes « uname », « uname -a », « uname -r », vous remarquerez dans la commande ci-dessous l'utilisation de cette variable.

```
sudo apt update
sudo apt install build-essential dkms linux-headers-$(uname -r)
```

```
# apt-get install build-essential dkms linux-headers-$(uname -r)
```

Insérer le cd VBoxLinuxAdditions, soit via une image iso soit en cliquant sur le menu VBox « insérer les extensions invités ».

Repérer toutes les partitions avec la commande

```
# blkid
```

Le cd est dans /dev/sr0. Regarder s'il est déjà monté.

```
ls /media/
```

sinon, Monter le cd avec la commande suivante.

```
# mount /dev/sr0 /media/cdrom0
```

Puis saisir.

```
# sh /media/cdrom0/VBoxLinuxAdditions.run
```

```
cd /media/[Utilisateur]/VBOX_GAs_xxx/
sudo ./VBoxLinuxAdditions.run
```

```
mount -t vboxsf mount_point
mount -t vboxsf /vpn
```

```
sudo
mount -t vboxsf nom_dossier_partagé_dans_virtualbox /partage_vm
```

Installer quelques outils

Les outils ci-dessous sont donnés à titre d'exemple. IPTABLES n'est pas obligatoire mais vous pourrez expérimenter iptables persistant ou le parefeu UFW, un peu plus loin dans ce document.

Remarquez la syntaxe de la commande ! le symbole « \ » (anti slash) permet un retour à la ligne, ceci peut être plus clair pour la lecture lors de la rédaction de la commande avant de la copier coller.

```
apt-get install \
ca-certificates curl gnupg gnupg2 lsb-release \
tree sudo nano unzip tar nmap telnet wget screen locate \
sysstat iotop htop atop lsof procs \
apt-transport-https aptitude iptables iptables-persistent \
software-properties-common
```

- ne sauvegarder pas les règles iptables pour le moment
- par la suite nous pourrons sauvegarder et restaurer avec les commandes ci-dessous,
- mais cela n'est pas utile pour la suite immédiate du labo.

```
sudo iptables-save > /etc/iptables/rules.v4
sudo iptables-restore < /etc/iptables/rules.v4
sudo iptables-restore -n < /etc/iptables/rules.v4
```

ajouter sysadmin au groupe sudo et fichier sudoers

```
usermod -aG sudo sysadmin
```

ensuite vous pouvez ajouter votre utilisateur dans le fichier sudoers pour lui donner des privilèges administrateur.

```
nano /etc/sudoers
sysadmin ALL=(ALL:ALL) ALL
```

Tester les commandes ci-dessous.

```
su - sysadmin
sudo su sysadmin
```

Ici, je fait un « tree » des répertoires pour plus de lisibilité de l'arborescence des répertoires. Si besoin j'installe juste "tree".

```
#apt install tree
```

Exemple :

```
tree -v -a -u -g -L 1 /chemin/vers/un/dossier
tree -f -v -a -u -g -L 1 /chemin/vers/un/dossier
tree -r -a -u -g -L 1 /chemin/vers/un/dossier
tree -pugD -L 1 /chemin/vers/un/dossier
```

Liste des paramètres de « tree ».

```
# $ tree # Affiche les répertoires et les fichiers
# $ tree -d # Affiche uniquement les répertoires
# $ tree -L X # Affiche jusqu'à X répertoires profonds
# $ tree -f # Affiche les fichiers avec leurs chemins d'accès
```



```
# $ tree -a # Affiche tous les fichiers, y compris les fichiers cachés.  
# $ tree / # Affiche un arbre de tout le système.  
# $ tree -ugh # Affiche les fichiers avec leur propriétaire respectif (-u),  
# le groupe (-g) et la taille de chaque fichier (-h)  
# $ tree -H . -o tuddirectory.html # Exportez votre arborescence de répertoire vers un fichier FICHIER HTML  
# tree -pugfD -L 1 /boot
```

```
sysadmin@multi:~$ tree -pugfD -L 1 /boot  
/boot  
├── [-rw-r--r-- root root Jul 24 00:32] /boot/config-5.10.0-16-amd64  
├── [-rw-r--r-- root root Sep 2 15:54] /boot/config-5.10.0-18-amd64  
├── [drwxr-xr-x root root Oct 6 11:42] /boot/grub  
├── [-rw-r--r-- root root Oct 6 11:43] /boot/initrd.img-5.10.0-16-amd64  
├── [-rw-r--r-- root root Oct 6 11:43] /boot/initrd.img-5.10.0-18-amd64  
├── [drwx----- root root Oct 6 11:22] /boot/lost+found  
├── [-rw-r--r-- root root Jul 24 00:32] /boot/System.map-5.10.0-16-amd64  
├── [-rw-r--r-- root root Sep 2 15:54] /boot/System.map-5.10.0-18-amd64  
├── [-rw-r--r-- root root Jul 24 00:32] /boot/vmlinuz-5.10.0-16-amd64  
└── [-rw-r--r-- root root Sep 2 15:54] /boot/vmlinuz-5.10.0-18-amd64  
  
2 directories, 8 files  
sysadmin@multi:~$
```

Sur Debian 11/12 ;

Exemple de copie de fichier, avec la commande cp. Ici, on ajoute « .bak » a la fin du nom de fichier

```
cp /etc/openvpn/server/server.conf{,.bak}
```

Avant docker

je passe en root , puis

```
apt-get update && apt-get upgrade -y && apt-get install locate tree unzip
```

Lors de l'installation d'un logiciel , nous ne souhaitons installer que ce qui est nécessaire.

Dans le cas de la mise en place d'un environnement de dev, nous préférons que rien ne manque, l'idée étant de s'assurer d'avoir un environnement où il ne nous manquera pas régulièrement une bibliothèque ou autres composants.

pour cela , apt accepte des paramètres permettant l'installation automatique des paquets suggérés par les auteurs du logiciel, en plus des paquets nécessaires à son fonctionnement. On recherche la configuration d'APT.

```
root@debian-devops-01:/# locate apt.conf
/etc/apt/apt.conf.d
...
...
/etc/apt/apt.conf.d/00configauto

root@debian-devops-01:/#
```

Configuration pour installer les paquets suggérés automatiquement, soit en ligne de commande, de manière ponctuelle.

L'option --option (-o) de apt-get :

```
# apt-get --option APT::Install-Recommends=true --option APT::Install-Suggests=true install paquet1 paquet2 ...
```

man apt-get; man apt_preferences; man apt.conf

ou de manière permanente

Créer un fichier de configuration personnel pour apt afin qu'il installe automatiquement les dépendances.

Créer le fichier 00configauto :

```
00configauto
```

dans :

```
/etc/apt/apt.conf.d
```

et écrire les lignes suivantes :

```
APT::Install-Recommends "true";
APT::Install-Suggests "true";
```

ne pas oublier le point-virgule de fin de ligne

Exemple de création automatique en ligne de commande

Donc on copie/colle ceci et cela créera le fichier 00configauto et inscrira les commande dedans.

Ne pas oublier le EOF

Exemple avec la command echo :

```
# echo 'APT::Install-Recommends "true";  
APT::Install-Suggests "true";' > /etc/apt/apt.conf.d/00configauto
```

exemple avec la command cat

```
cat << EOF > /etc/apt/apt.conf.d/00configauto  
APT::Install-Recommends "true";  
APT::Install-Suggests "true";  
EOF
```

Retour écran pour les différentes méthodes

Actions : je crée le fichier, puis je le détruis avec la command "rm" et je test l'autre méthode.

```
root@debian-devops-01:/home/clean#  
root@debian-devops-01:/home/clean# echo 'APT::Install-Recommends "true";  
> APT::Install-Suggests "true";' > /etc/apt/apt.conf.d/00configauto  
root@debian-devops-01:/home/clean# cat /etc/apt/apt.conf.d/00configauto  
APT::Install-Recommends "true";  
APT::Install-Suggests "true";  
root@debian-devops-01:/home/clean# rm /etc/apt/apt.conf.d/00configauto  
root@debian-devops-01:/home/clean# cat << EOF > /etc/apt/apt.conf.d/00configauto  
> APT::Install-Recommends "true";  
> APT::Install-Suggests "true";  
> EOF  
root@debian-devops-01:/home/clean# cat /etc/apt/apt.conf.d/00configauto  
APT::Install-Recommends "true";  
APT::Install-Suggests "true";  
root@debian-devops-01:/home/clean#
```

ce code peut être placé dans un script rendu exécutable avec un changement de privilège : chmod +x

exemple :

mon-script-pour-apt.sh

```
#!/bin/sh  
  
cat << EOF > /etc/apt/apt.conf.d/00configauto  
APT::Install-Recommends "true";  
APT::Install-Suggests "true";  
EOF  
exit 0
```

Notes sur l'utilisation de la commande printf:

printf en bash :

```
printf "%b\n" 'Hello\nWorld'
```

donne le résultat:

```
Hello  
world
```

lisez le "man printf" pour cette commande.

Sinon

```
echo -e "Hello\nWorld"
```

qui donne le même résultat

le -e permet de traiter les séquences d'échappements "un peu à la façon du langage C".

Donc

```
echo -e "Hello\n\tWorld\ra"
```

affiche

```
Hello  
    world
```

et fait *bip*

avec le fichier 00configauto, quand on exécute apt-get update et (dist-)upgrade, cela installe les dépendances ET les paquets recommandés.

On peut aussi utiliser dans ce même fichier, l'option suivante pour les paquets suggérés :

Vérifier le contenu du fichier 00configauto avec la commande cat

```
cat /etc/apt/apt.conf.d/00configauto
```

Recherche et installation des mises à jour complète ainsi que de la distribution sans demande de confirmation.

Attention , pour une net install, vous allez avoir **une mise à jour Complete de la distribution**, la taille sur système va dépasser les 20 Gigas.

Si vous avez pris la dernière version de la release, alors dist-upgrade ne devrait rien faire.

Vérifier la version de votre distribution avant cela

Installer en root

```
apt-get update && apt-get install lsb-release
```

lsb_release -cs retourne le nom de la distribution soit : busllseye

```
lsb_release -d && cat /etc/debian_version
```

```
apt-get update && apt-get upgrade && apt-get dist-upgrade -y
```

Générer une somme de contrôle

exemple,

je veux vérifier que mon fichier 'Mon-Fichier.zip' n'a pas été corrompu durant son transfert.

J'utilise donc openssl avec les options dgst -md5 pour calculer et afficher la somme de contrôle du fichier réceptionné :

```
openssl dgst -md5 Mon-Fichier.zip
```

retour de la commande

```
MD5(Mon-Fichier.zip)= bce3ca34ab01377b93763795210a7895
```

Le programme openssl accepte aussi les options -md5 -md4 -md2 -sha1 -sha -mdc2 -ripemd160 et -dss1.

Pour les algorithmes sha1, sha et md5 on peut utiliser un raccourci :

sha1sum, shasum et md5sum.

```
md5sum Mon-Fichier.zip
```

retour de la commande

```
bce3ca34ab01377b93763795210a7895 Mon-Fichier.zip
```

On peut aussi utiliser une redirection pour créer un fichier texte

avec le retour de la commande :

```
md5sum Mon-Fichier.zip > md5_Mon-Fichier.zip.txt
```

Contrôler une somme de contrôle

Dans le but de comparer la somme de contrôle md5 d'un fichier reçu par rapport à celle du fichier original, il est possible de vérifier la conformité d'un ou plusieurs fichiers par rapport aux sommes de contrôle inscrites dans un fichier.

Par exemple, j'ai reçu le fichier Mon-Fichier.zip associé à un fichier texte md5_Mon-Fichier.zip.txt contenant la somme de contrôle:

```
bce3ca34ab01377b93763795210a7895 Mon-Fichier.zip
```

En plaçant les deux fichiers dans le même dossier je peux contrôler l'empreinte du fichier :

```
md5sum -c md5_Mon-Fichier.zip.txt
```

retour de la commande

```
Mon-Fichier.zip: Réussi
```

Le fichier texte peut contenir plusieurs noms de fichier avec chacun sa somme de contrôle.

Les fichiers images ISO debian...

...sont généralement regroupés dans un répertoire, par exemple le répertoire accessible depuis le lien :

```
http://cdimage.debian.org/debian-cd/11.6.0/amd64
```

```
http://cdimage.debian.org/debian-cd/11.6.0/amd64/iso-dvd/
```

Dans ce même répertoire, vous trouverez aussi un fichier nommé SHA256SUMS

contenant la liste de chaque fichier image ISO du répertoire

avec sa somme SHA256

Si par exemple, vous avez téléchargé depuis ce répertoire les fichiers :

```
[ICO]  Name  Last modified  Size
[PARENTDIR]  Parent Directory          -
[SUM]  SHA256SUMS  2022-12-17 19:52      2.1K
[CRT]  SHA256SUMS.sign  2022-12-17 20:07      833
[SUM]  SHA512SUMS  2022-12-17 19:52      3.5K
[CRT]  SHA512SUMS.sign  2022-12-17 20:07      833
[ISO]  debian-11.6.0-amd64-DVD-1.iso  2022-12-17 13:28      3.6G
Apache/2.4.54 (Unix) Server at cdimage.debian.org Port 80
```

et que les fichiers .iso du répertoire courant proviennent tous du même répertoire

vous pourrez vérifier la somme md5 des fichiers images iso avec la ligne de commandes suivante :

```
for fichISO in *.iso; do sed -n "/${fichISO}/p" MD5SUMS | md5sum -c - 2>/dev/null; done
```

Des manuels sont disponibles pour openssl, md5 et md5sum, accessibles grâce aux commandes:

```
man openssl
man md5
man md5sum
man sha256sum
```

Sources : https://debian-facile.org/doc:systeme:openssl:openssl_checksum

Pour tester ceci, je choisis arbitrairement un dépôt

Je télécharge une image iso, ici une netinstall de 639 M.

```
wget http://cdimage.debian.org/debian-cd/12.5.0/amd64/iso-cd/debian-12.5.0-amd64-netinst.iso
ainsi que
```

```
wget http://cdimage.debian.org/debian-cd/12.5.0/amd64/iso-cd/SHA256SUMS
```

Sauvegarde en : « debian-12.5.0-amd64-netinst.iso »

```
debian-12.5.0-amd64-netinst.iso          100%[=====>]
629,00M  71,0MB/s  ds 9,2s
```

Terminé — 2023-04-17 15:01:56 —

Temps total effectif : 9,2s

Téléchargés : 1 fichiers, 629,00M en 9,2s (71,0 MB/s)

sysadmin@deb-dev-0:~/Téléchargements\$

```
$ sha256sum debian-12.5.0-amd64-netinst.iso
```

```
013f5b44670d81280b5b1bc02455842b250df2f0c6763398feb69af1a805a14f  debian-12.5.0-amd64-netinst.iso
```

vérifier le SHA256SUMS

```
# sha256sum --ignore-missing -c SHA256SUMS
```

```
debian-12.5.0-amd64-netinst.iso: Réussi
```

Installation de Docker sous Debian 12

Vérification des étapes précédentes

Je recherche la présence du fichier 00configauto.

```
updatedb && locate 00configauto
```

```
sysadmin@deb-dev-0:~/Téléchargements$ sudo updatedb && sudo locate 00configauto
[sudo] Mot de passe de sysadmin :
/etc/apt/apt.conf.d/00configauto
sysadmin@deb-dev-0:~/Téléchargements$
```

Pour être sûr, on commence par mettre à jour nos dépôts :

```
apt-get update
```

Installez ces paquets pour permettre à « apt » d'utiliser un dépôt par HTTPS:

<https://manpages.debian.org/unstable/apt/apt-transport-https.1.fr.html>

```
apt-get install \
apt-transport-https \
ca-certificates \
curl \
gnupg2 \
software-properties-common
```

On va ensuite chercher la clé du dépôt officiel de Docker :

```
curl -fsSL https://download.docker.com/linux/debian/gpg | apt-key add -
```

Utilisez la commande suivante pour installer le dépôt stable.

Vous avez toujours besoin du dépôt stable :

```
lsb_release -cs retourne le nom de la distribution soit : bookworm
```

```
add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/debian $(lsb_release -cs) stable"
```

Autre exemple :

```
add-apt-repository \
"deb [arch=amd64] https://download.docker.com/linux/debian \
$(lsb_release -cs) \
stable"
```

Puis on remet à jour nos dépôts et on installe Docker :

```
apt-get update
```


Les paquets suivants seront mis à jour :

```
libbasicusageenvironment1 libgroupsock8 liblivemedia57 libopenjp2-7 libusageenvironment3 openssh-client  
openssh-server  
openssh-sftp-server
```

8 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.

Il est nécessaire de prendre 1 647 ko dans les archives.

Après cette opération, 8 192 o d'espace disque supplémentaires seront utilisés.

Souhaitez-vous continuer ? [O/n] O

Nous n'avons plus besoin de saisir cette longue commande ...

```
apt-get --option APT::Install-Recommends=true --option APT::Install-Suggests=true install docker-ce
```

mais simplement la commande

```
# apt-get install docker-ce
```

ceci fonctionne et installe vraiment la totalité des Paquets suggérés et des Paquets recommandés

0 mis à jour, 10 nouvellement installés, 0 à enlever et 0 non mis à jour.

Il est nécessaire de prendre 120 Mo dans les archives.

Après cette opération, 430 Mo d'espace disque supplémentaires seront utilisés.

Souhaitez-vous continuer ? [O/n] O

L'installation est terminée

Si vous êtes en « root », passez sous votre utilisateur.

On démarre Docker et on vérifie sa version pour vérifier qu'il est bien lancé:

```
sudo \  
systemctl start docker
```

Pour activer automatiquement le démarrage du service Docker à chaque démarrage du système, utilisez :

```
sudo \  
systemctl enable docker
```

Voir la version de Docker

```
docker version
```

```
sysadmin@Deb12KDE:~$ sudo docker version
```

Client: Docker Engine - Community

Version: 26.0.2

API version: 1.45

Go version: go1.21.9

Git commit: 3c863ff

Built: Thu Apr 18 16:27:49 2024

OS/Arch: linux/amd64

Context: default

Server: Docker Engine - Community

```
Engine:
Version:      26.0.2
API version:   1.45 (minimum version 1.24)
Go version:    go1.21.9
Git commit:    7cef0d9
Built:         Thu Apr 18 16:27:49 2024
OS/Arch:       linux/amd64
Experimental:  false
containerd:
Version:       1.6.31
GitCommit:     e377cd56a71523140ca6ae87e30244719194a521
runc:
Version:       1.1.12
GitCommit:     v1.1.12-0-g51d5e94
docker-init:
Version:       0.19.0
GitCommit:     de40ad0
sysadmin@Deb12KDE:~$
```

Tester Docker

Pour tester le bon fonctionnement de l'installation de Docker nous allons lancer le container

```
« hello-world »:
```

```
sudo \
docker run hello-world
```

```
root@debian-devops-01:/home/clean# docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
1b930d010525: Pull complete
Digest: sha256:2557e3c07ed1e38f26e389462d03ed943586f744621577a99efb77324b0fe535
Status: Downloaded newer image for hello-world:latest
```

Hello from Docker!

This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:

1. The Docker client contacted the Docker daemon.
2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
(amd64)
3. The Docker daemon created a new container from that image which runs the executable that produces the output you are currently reading.

4. The Docker daemon streamed that output to the Docker client, which sent it to your terminal.

To try something more ambitious, you can run an Ubuntu container with:

```
$ docker run -it ubuntu bash
```

Share images, automate workflows, and more with a free Docker ID:

<https://hub.docker.com/>

For more examples and ideas, visit:

<https://docs.docker.com/get-started/>

```
root@debian-devops-01:/home/clean#
```

Notre environnement de conteneurisation est prêt

Différence entre Docker et Kubernetes ?

Docker est une plateforme de conteneurisation et d'exécution, tandis que Kubernetes est une plateforme permettant d'exécuter et de gérer des conteneurs à partir de nombreux systèmes d'exécution de conteneurs.

Installation de Portainer

Portainer est livré nativement dans un container docker.

Afin de conserver les données de Portainer (rappel : Stateless) On crée un volume et on vérifie

```
sudo docker volume create portainer_data
```

```
sysadmin@Deb12KDE:~$ sudo docker volume ls
DRIVER    VOLUME NAME
local     portainer_data
sysadmin@Deb12KDE:~$
```

Ensuite, Pour le déployer : On installe le container en indiquant le volume avec l'argument « -v ». :Tester ceci ..

```
docker run -d -p 9000:9000 --name portainer \
--restart=always \
-v /var/run/docker.sock:/var/run/docker.sock \
-v portainer_data:/data \
portainer/portainer-ce:latest
```

Avant d'aller plus loin , vérifier.

```
sysadmin@Deb12KDE:~$ sudo docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS        PORTS
a829d11fcd6    portainer/portainer-ce:latest       "/portainer"            12 seconds ago Up 10 seconds  8000/tcp, 9443/tcp,
0.0.0.0:9000->9000/tcp, :::9000->9000/tcp portainer
```

Une fois le container déployé connectez-vous à l'interface web via l'adresse suivante: <http://ipdevotremachine:9000>

```
sysadmin@deb-dev-0:~/Téléchargements$ sudo docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS
fc198291c5df	portainer/portainer	"/portainer"	2 minutes ago	Up 2 minutes	8000/tcp, 9443/tcp, 0.0.0.0:9000->9000/tcp, :::9000->9000/tcp

```
romantic_wilson
sysadmin@deb-dev-0:~/Téléchargements$
```

TEST EN LOCAL SI VOUS AVEZ UN ENVIRONNEMENT DE BUREAU SUR VOTRE VM.

Sinon

Il vous faudra pouvoir "tapper" l'ip de la VM depuis un poste avec un navigateur internet.

127.0.0.1:9000

Comment trouver l'adresse ip du container

On vérifie que notre docker est bien installé et on récupère son identifiant : ici c'est le a15204973b0a

```
sudo \
    docker ps -a
```

```
clean@debian-devops-01:~$ sudo docker ps -a
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS
a15204973b0a	portainer/portainer	"/portainer"	31 seconds ago	Up 28 seconds	0.0.0.0:9000->9000/tcp
agitated_vaughan	4cd50b6686db	hello-world	"/hello"	About an hour ago	Exited (0) About an hour ago

```
condescending_dhawan
clean@debian-devops-01:~$
```

On démarre notre container :

```
sysadmin@deb-dev-0:~/Téléchargements$ sudo docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS
fc198291c5df	portainer/portainer	"/portainer"	12 minutes ago	Up 11 minutes	8000/tcp, 9443/tcp, 0.0.0.0:9000->9000/tcp, :::9000->9000/tcp

```
romantic_wilson
```

```
sysadmin@deb-dev-0:~/Téléchargements$ sudo docker stop fc198291c5df
fc198291c5df
```

```
sysadmin@deb-dev-0:~/Téléchargements$ sudo docker start fc198291c5df
fc198291c5df
```

```
sysadmin@deb-dev-0:~/Téléchargements$ sudo docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS
fc198291c5df	portainer/portainer	"/portainer"	13 minutes ago	Up 14 seconds	8000/tcp, 9443/tcp, 0.0.0.0:9000->9000/tcp, :::9000->9000/tcp

```
romantic_wilson  
sysadmin@deb-dev-0:~/Téléchargements$
```

```
docker start <container id>
```

```
sudo docker start fc198291c5df
```

Docker inspect

Nous allons maintenant inspecter la configuration de notre conteneur afin de déterminer l'adresse IP local du container :

Si vous utiliser pour la première fois cette commande, vous devez savoir que le retour écran s'étire sur plusieurs écrans, Vous pouvez peut être utiliser "|" suivi de "less" pour une lecture complète plus simple.

```
docker inspect <id du container>
```

```
sudo docker inspect fc198291c5df
```

Vous verrez toutes les informations de votre container et notamment un élément qui nous intéresse :

```
...
...

  "Config": {
    "Hostname": "a15204973b0a",
    "Domainname": "",
    "User": "",
    "AttachStdin": false,
    "AttachStdout": false,
    "AttachStderr": false,
    "ExposedPorts": {
      "9000/tcp": {}
    }
  }
...
...

  "NetworkSettings": {
    "Bridge": "",
    ...
    ...

    "Ports": {
      "9000/tcp": [
        {
          "HostIp": "0.0.0.0",
          "HostPort": "9000"
        }
      ]
    }
    ...
    ...

    "Gateway": "172.17.0.1",
    "IPAddress": "172.17.0.2",
    ...
    ...
```

Adaptez maintenant la commande afin d'afficher uniquement ce que nous cherchons

soit :

ExposedPorts
HostIp
HostPort
Gateway
IPAddress

ce qui peut être fait avec la commande grep.

```
sudo docker inspect fc198291c5df | grep <ARGUMENT>
```

```
sudo docker inspect fc198291c5df | grep
```

```
sudo docker inspect fc198291c5df | grep ExposedPorts &&  
sudo docker inspect fc198291c5df | grep HostIp &&  
sudo docker inspect fc198291c5df | grep HostPort &&  
sudo docker inspect fc198291c5df | grep Gateway &&  
sudo docker inspect fc198291c5df | grep IPAddress
```

Retour écran de la commande

```
...  
...  
  
  "ExposedPorts": {  
    "HostIp": "",  
    "HostIp": "0.0.0.0",  
    "HostIp": ":::",  
    "HostPort": "9000"  
    "HostPort": "9000"  
    "HostPort": "9000"  
  "Gateway": "172.17.0.1",  
  "IPv6Gateway": "",  
    "Gateway": "172.17.0.1",  
    "IPv6Gateway": "",  
  "SecondaryIPAddresses": null,  
  "IPAddress": "172.17.0.2",  
    "IPAddress": "172.17.0.2",  
...  
...
```

Les informations étant standardisé dans leur présentations, on peut conserver cette longue ligne de commande.

L'adresse IP du conteneur est 172.17.0.1

On vérifie que celui-ci répond sur un ping local

```
sudo ping -c4 172.17.0.1
```

Configuration

Lors de la première connexion, il vous sera demandé de créer le mot de passe du user admin:

Une fois le container déployé connectez-vous à l'interface web via l'adresse suivante: <http://ipdevotremachine:9000>

Mettre à jour Portainer

Arrêter le conteneur puis le supprimer.

Comme nous utilisons un volume, les données importantes du conteneur ne seront pas supprimées.

On télécharge ensuite la dernière image de Portainer, puis nous relançons le conteneur avec les mêmes réglages qu'à l'origine.

```
sudo docker stop fc198291c5df
sudo docker rm fc198291c5df
sudo docker pull portainer/portainer-ce:latest
```

```
sudo docker run -d -p 9000:9000 --name portainer \
--restart=always \
-v /var/run/docker.sock:/var/run/docker.sock \
-v portainer_data:/data \
portainer/portainer-ce:latest
```


Cas concrets

Nous allons maintenant voir des utilisations concrètes de conteneurs docker.

Voici la liste des arguments que nous utiliserons dans cette partie :

```
-t : fournit un terminal au docker ;  
-i : permet d'écrire dans le conteneur (couplé à -t) ;  
-d : exécute le conteneur en arrière-plan ;  
-v : permet de monter un répertoire local sur le conteneur ;  
-p : permet de binder un port sur le conteneur vers un port sur le host ;  
-e : permet l'ajout d'une variable d'environnement ;  
--name : donne un nom au conteneur ;  
--rm : détruit le conteneur une fois terminé ;  
-w : choisit le répertoire courant (dans le conteneur) ;  
--link : permet de faire un lien entre deux conteneurs.
```

Bien évidemment, beaucoup d'autres options existent, je vous renvoie à la documentation de docker run.

Je passe en root avec « **su -** »

Créer les dossiers pour y placer une page html pour SRV01 et SRV02

```
mkdir /var/www/projets /var/www/projets/srv01 /var/www/projets/srv01/html /var/www/projets/srv02  
/var/www/projets/srv02/html
```

ou plus rapide...

```
mkdir -p /var/www/projets/{srv01/html,srv02/html}
```

```
cat > /var/www/projets/srv01/html/index.html <<EOF  
<html><head>  
  <title>Apache2 Debian SRV01</title>  
</head>  
<body>  
<h1>Apache2 Debian SRV01 Page: It works</h1>  
</body>  
EOF
```

```
cat > /var/www/projets/srv02/html/index.html <<EOF  
<html><head>  
  <title>Apache2 Debian SRV02</title>  
</head>  
<body>  
<h1>Apache2 Debian SRV02 Page: It works</h1>  
</body>  
EOF
```

Je me connecte sur la WebUI de Portainer,

Notes : sur le HUB docker je trouve des informations sur le Dockerfile

```
https://hub.docker.com/_/httpd?tab=description
```

Création Dockerfile

Pour mon projet, je crée un Dockerfile.

Je passe en root :

```
nano /var/www/projets/srv01/Dockerfile
```

```
FROM httpd:2.4
COPY ./html/ /usr/local/apache2/htdocs/
```

```
cd /var/www/projets/srv01/
```

```
docker build -t srv01 .
```

```
root@debian-devops-01:/var/www/projets# docker build -t srv01 .
Build an image from a Dockerfile
root@debian-devops-01:/var/www/projets/srv01# docker build -t srv01 .
Sending build context to Docker daemon 3.584kB
Step 1/2 : FROM httpd:2.4
--> 2d1e5208483c
Step 2/2 : COPY ./html/ /usr/local/apache2/htdocs/
--> ee9f1519593b
Successfully built ee9f1519593b
Successfully tagged srv01:latest
root@debian-devops-01:/var/www/projets/srv01#
```

```
root@debian-devops-01:/var/www/projets/srv01# cd ../srv02
```

```
cat > /var/www/projets/srv02/Dockerfile <<EOF
FROM httpd:2.4
COPY ./html/ /usr/local/apache2/htdocs/
EOF
```

```
root@debian-devops-01:/var/www/projets/srv02# docker build -t srv02 .
Sending build context to Docker daemon 3.584kB
```

```
Step 1/2 : FROM httpd:2.4
--> 2d1e5208483c
Step 2/2 : COPY ./html/ /usr/local/apache2/htdocs/
--> 88e822c8f7d6
Successfully built 88e822c8f7d6
Successfully tagged srv02:latest
root@debian-devops-01:/var/www/projets/srv02#
```

Rappel !

```
-t : fournit un terminal au docker ;
-i : permet d'écrire dans le conteneur (couplé à -t) ;
-d : exécute le conteneur en arrière-plan ;
```

```
docker run -it --name srv01web -p 8080:80 srv01
```

je lance un second container basé sur celui-ci, en lui ajoutant le dossier contenant la page et je donne à ce conteneur le nom de srv02

```
docker run -it --name srv02web -p 8181:80 srv02
```

Créer une image

Utiliser des images docker c'est bien, mais les fabriquer soi-même c'est mieux.

Nous avons plusieurs façons de faire une image.

- Nous pouvons le faire à partir d'un conteneur existant (via docker save), facile à mettre en place, mais compliqué à maintenir.
- From scratch, complexe, et difficile à maintenir.
- Puis via un dockerfile, un fichier qui comporte les instructions de la création de l'image (la recette), en se basant sur une image existante, c'est facile à maintenir.

Création d'un Dockerfile

Créons une image apache php mysql

Le Dockerfile (toujours avec une majuscule)

est un fichier qui contient toutes les instructions pour créer une image, comme des métadonnées (Mainteneur, label, etc.), ou même les commandes à exécuter pour installer un logiciel.

Voici la liste des instructions d'un Dockerfile :

```
FROM # Pour choisir l'image sur laquelle on se base, toujours en premier
RUN # Permet d'exécuter une commande
CMD # Commande exécutée au démarrage du conteneur par défaut
EXPOSE # Ouvre un port
ENV # Permet d'éditer des variables d'environnement
ARG # Un peu comme ENV, mais seulement le temps de la construction de l'image
COPY # Permet de copier un fichier ou répertoire de l'hôte vers l'image
ADD # Permet de copier un fichier de l'hôte ou depuis une URL vers l'image, permet également de décompresser une archive tar
LABEL # Des métadonnées utiles pour certains logiciels de gestion de conteneurs, comme rancher ou swarm, ou tout simplement pour mettre des informations sur l'image.
ENTRYPOINT # Commande exécutée au démarrage du conteneur, non modifiable, utilisée pour package une commande
VOLUME # Crée une partition spécifique
WORKDIR # Permet de choisir le répertoire de travail
USER # Choisit l'utilisateur qui lance la commande du ENTRYPOINT ou du CMD
ONBUILD # Crée un step qui sera exécuté seulement si notre image est choisie comme base
HEALTHCHECK # Permet d'ajouter une commande pour vérifier le fonctionnement de votre conteneur
STOPSIGNAL # permet de choisir le [signal](http://man7.org/linux/man-pages/man7/signal.7.html) qui sera envoyé au conteneur lorsque vous ferez un docker container stop
```

Pour plus d'informations, je vous conseille de consulter la documentation officielle

Docker image build

La commande pour construire l'image :

```
docker image build -t [imagename]:[tag] [dockerfile folder]
```

Pour pouvoir construire une image, il faut connaître un minimum le logiciel que l'on souhaite conteneuriser, par exemple ici je vais conteneuriser apache, et je sais qu'il lui faut certaines variables d'environnement pour fonctionner.

On commence par créer le répertoire de notre projet :

```
$ mkdir ./srv-apache-00
$ cd ./srv-apache-00
$ nano Dockerfile
```

Puis on crée notre Dockerfile (le D toujours en majuscule) :

On commence par mettre le FROM :

VirtualBox : Debian –Version 7.0

```
FROM debian
```

Puis on ajoute les variables d'environnement (qui sont normalement gérées par le système d'init) :

```
ENV APACHE_RUN_USER www-data
ENV APACHE_RUN_GROUP www-data
ENV APACHE_LOG_DIR /var/www/log/apache2
ENV APACHE_PID_FILE /var/run/apache2.pid
ENV APACHE_RUN_DIR /var/run/apache2
ENV APACHE_LOCK_DIR /var/lock/apache2
```

On installe apache :

```
RUN export DEBIAN_FRONTEND=noninteractive && apt-get update && apt-get -y -q upgrade && apt-get -y -q install
apache2
```

Dans un Dockerfile, il ne faut aucune interactivité,

donc on utilise : **DEBIAN_FRONTEND=noninteractive**

et surtout l'option **-y** de apt-get

On expose les ports (facultatif) :

```
EXPOSE 80 443
```

Et pour finir, on ajoute la commande par défaut :

```
CMD ["apache2ctl","-D","FOREGROUND"]
```

Le Dockerfile au complet :

```
FROM debian
```

```
ENV APACHE_RUN_USER www-data
ENV APACHE_RUN_GROUP www-data
ENV APACHE_LOG_DIR /var/www/log/apache2
ENV APACHE_PID_FILE /var/run/apache2.pid
ENV APACHE_RUN_DIR /var/run/apache2
ENV APACHE_LOCK_DIR /var/lock/apache2
```

```
RUN export DEBIAN_FRONTEND=noninteractive && apt-get update && apt-get -y -q upgrade && apt-get -y -q install
apache2 nano tree locate \
apt-transport-https lsb-release ca-certificates wget
```

```
RUN wget -O /etc/apt/trusted.gpg.d/php.gpg https://packages.sury.org/php/apt.gpg
RUN echo "deb https://packages.sury.org/php/ $(lsb_release -sc) main" | tee /etc/apt/sources.list.d/php.list
```

```
RUN export DEBIAN_FRONTEND=noninteractive && apt-get update && apt-get -y -q upgrade && apt-get -y -q install
php-fpm php-gd php-xdebug \
libgd-tools libmcrypt-dev mcrypt php-pear apache2 apache2-doc libapache2-mod-php
```

Puis on construit notre image :

```
docker image build -t srv-apache-00 .
```

On peut tester :

```
$ docker container run -ti -p 80:80 srv-apache-00
```

Si on se connecte maintenant au site, vous devriez avoir la page Apache2 Default Page.

[Comment entrer dans le container pour le configurer](#)

Vous connecter directement sur votre container:

```
docker run -it <votre container> /bin/bash
```

```
sudo docker run -it httpd:latest /bin/bash
```

```
root@f5fede6ce135:/usr/local/apache2# apachectl -v
Server version: Apache/2.4.38 (Unix)
Server built:   Mar  5 2019 06:01:32
root@f5fede6ce135:/usr/local/apache2#
```

```
service apache2 status && apachectl -t
```

Consultez la liste des modules chargés:

```
apachectl -t -D DUMP_MODULES
```

Voir tous les Vhosts

```
apachectl -t -D DUMP_VHOSTS
```

```
apache2ctl -t -D DUMP_VHOSTS
```

```
root@9eaa1ffc0957:/usr/local/apache2# apachectl -t -D DUMP_VHOSTS
AH00558: httpd: Could not reliably determine the server's fully qualified domain name, using 172.17.0.4. Set the
'ServerName' directive globally to suppress this message
VirtualHost configuration:

root@9eaa1ffc0957:/usr/local/apache2#
```

```
sysadmin@Deb12KDE:~/srv-apache-00$ sudo docker exec -it adoring_shamir /bin/bash
[sudo] Mot de passe de sysadmin :
root@c374d221bd1a:/# cd /var/www/html/
root@c374d221bd1a:/var/www/html# ls
index.html
root@c374d221bd1a:/var/www/html# cp index.html{,.ori}
root@c374d221bd1a:/var/www/html# ls
```

```
index.html index.html.ori
root@c374d221bd1a:/var/www/html#
```

```
echo '<?php echo "<h1>Espace web utilisateur</h1><p>avec phpinfo </p></ br>"; phpinfo(); ?>' >
/var/www/html/info.php
```

On installe le container

```
sudo docker run -d --name=SRV-LAMP-01 <DOCKER>:latest
```

```
sudo docker run -p 80:80 -t -i <DOCKER> /bin/bash
```

On vérifie que notre docker est bien installé.

```
clean@debian-devops-01:~$ sudo docker ps -a
```

On démarre notre conteneur :

```
docker start <container id>
```

```
sudo docker start 940316d1afd0
```

Nous allons maintenant inspecter la configuration de notre container afin de déterminer

L'adresse IP local du conteneur :

```
docker inspect <id du container>
```

```
sudo docker inspect 940316d1afd0
```

Vous verrez toutes les informations de votre container et notamment un élément qui nous intéresse :

Commandes utiles

Supprimer tous les containers actifs :

```
docker rm `docker ps -a -q`
```

```
clean@debian-devops-01:~$ su
Mot de passe :
root@debian-devops-01:/home/clean# docker rm `docker ps -a -q`
940316d1afd0
4cd50b6686db
root@debian-devops-01:/home/clean#
```

Démarrer ou arrêter un container :

```
docker start <container>
```

```
docker stop <container>
```

Supprimer tous les container actif:

```
docker rm $(docker ps -a -q)
```

Supprimer une image docker

(vérifier qu'aucun container n'est actif):

```
docker rmi <image>
```

Vous connecter directement sur votre conteneur :

```
docker run -it <votre container> /bin/bash
```

Trouvez et notez votre adresse IP ↑

Utilisez la commande ip comme suit (voir comment trouver le nom de votre Ethernet sous Linux pour plus d'infos) :

```
ip a
```

Obtenir l'adresse IP de l'interface eth0

```
ip a show eth0
```

Une autre option consiste à exécuter la commande dig suivante pour trouver votre adresse IP publique à partir de la ligne de commande Linux :

```
# dig TXT +short o-o.myaddr.l.google.com @ns1.google.com | awk -F'"' '{print $2}'
```

Par défaut, il retournera l'IPv6 de vos serveurs :

```
root@deb11-vpn:/etc/easy-rsa# dig TXT +short o-o.myaddr.l.google.com @ns1.google.com | awk -F'"' '{print $2}'  
<IPPUBLICUEIPV6>  
root@deb11-vpn:/etc/easy-rsa#
```

Mais, nous pouvons forcer et obtenir l'IPv4 aussi : avec l'ajout du paramètre « -4 »

```
dig -4 TXT +short o-o.myaddr.l.google.com @ns1.google.com | awk -F'"' '{print $2}'  
<IPPUBLICUEIPV4>
```

Annexes générales

Réinitialiser le mot de passe Root d'une 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.

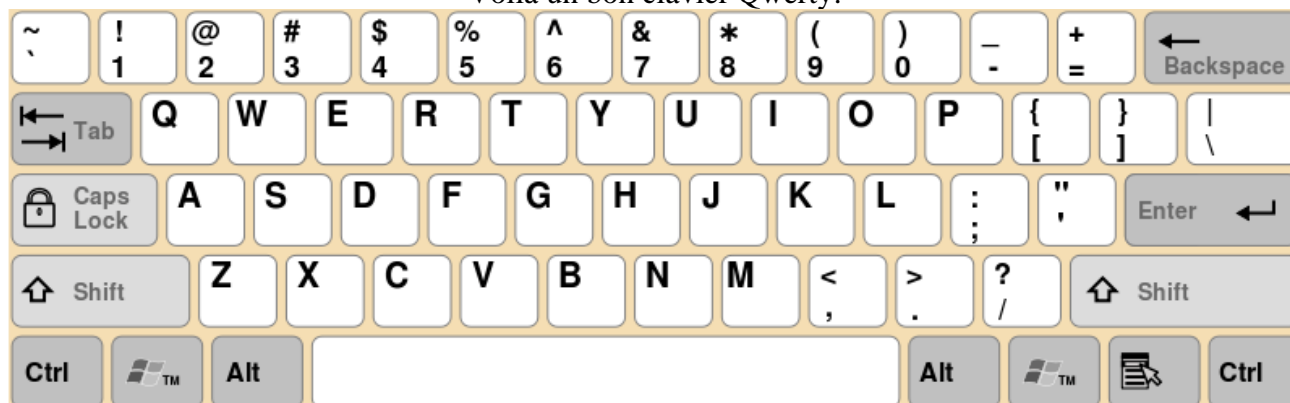
Comment réinitialiser le mot de passe Root d'un Debian (ou Ubuntu) si vous ne pouvez plus vous connecter en Root (ou avec un utilisateur disposant des droits sudo).

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

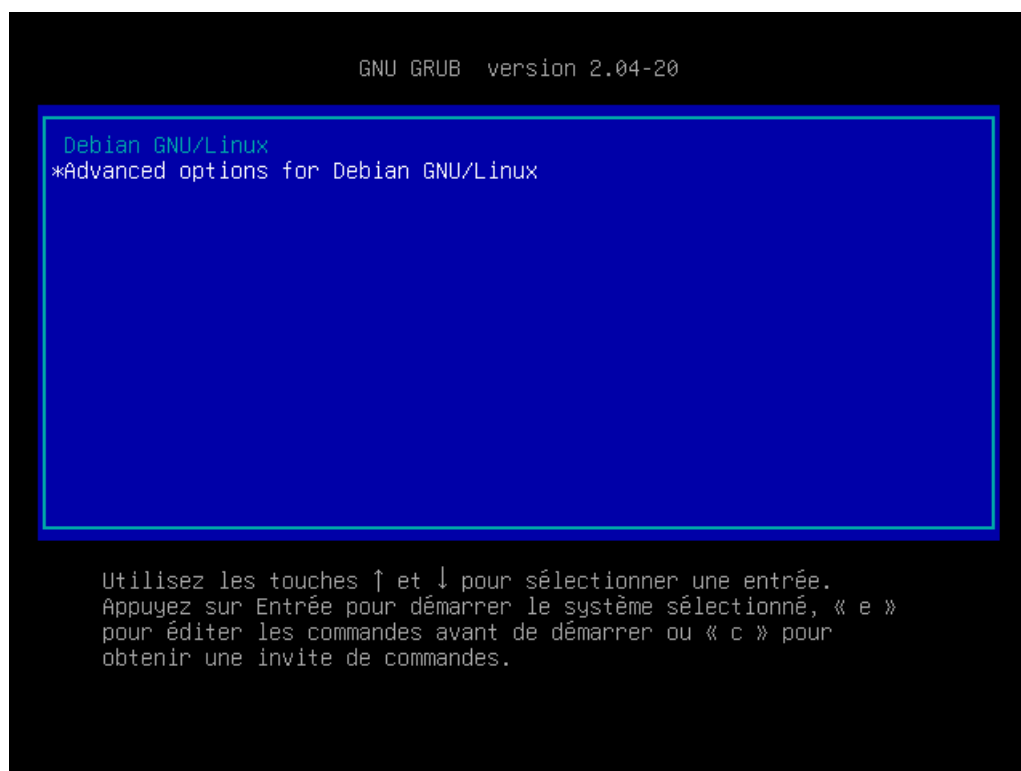
Votre ordinateur doit être éteint.

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:



Dmarrez 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 »

```
GNU GRUB version 2.04-20

insmod part_msdos
insmod ext2
set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint-bios=hd\
0,msdos1 --hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 4355a8d5-d\
9b3-4dcb-a764-85317b87c414
else
  search --no-floppy --fs-uuid --set=root 4355a8d5-d9b3-\
4dcb-a764-85317b87c414
fi
echo      'Loading Linux 5.10.0-10-amd64 ...'
linux     /boot/vmlinuz-5.10.0-10-amd64 root=UUID=435\
5a8d5-d9b3-4dcb-a764-85317b87c414 ro quiet init=/bin/bash_
echo      'Loading initial ramdisk ...'
```

Édition basique à l'écran de type Emacs possible. Tab affiche les compléments. Appuyez sur Ctrl-x ou F10 pour démarrer, Ctrl-c ou F2 pour une invite de commandes ou Échap pour revenir au menu GRUB.

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

Une fois démarré vous vous retrouvez avec un Prompt en root

```
/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 HARDDISK
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

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 7.0

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_du_fichier <espace> /chemin/vers/le/nouveau/fichier/nom_du_fichier.auchois

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

ou

```
cp /etc/network/interfaces /etc/network/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)  
#
```

Configuration de network-manager sous forme graphique au sein du bureau KDE.

```
apt-get install synaptic
```

```
/etc/NetworkManager/NetworkManager.conf  
[ifupdown]  
managed=false  
plasma-widget-networkmanagements
```

```
sysadmin@debian-bind-kde:~$ systemctl enable NetworkManager  
sysadmin@debian-bind-kde:~$ systemctl start NetworkManager  
sysadmin@debian-bind-kde:~$ systemctl start network-online.target  
  
sysadmin@debian-bind-kde:~$ su  
Mot de passe :  
root@debian-bind-kde:/home/sysadmin# /etc/init.d/networking restart  
[ ok ] Restarting networking (via systemctl): networking.service.  
root@debian-bind-kde:/home/sysadmin# ip addr  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
```

```
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:0e:01:b1 brd ff:ff:ff:ff:ff:ff
root@debian-bind-kde:/home/sysadmin#
```

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: <BROADC...
    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
```

Windows.

Effectuer une requête DHCP sur le client

Ouvrir le cmd, taper


```
la commande "ipconfig /release"  
puis ipconfig /renew".
```

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

Sous **Debian 9.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 déloger/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
```

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/FICHIER>
```

Sources.list

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

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

J'édite le fichier sources.list

VirtualBox : Debian –Version 7.0

```
# 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
```

Vérifier le fichier resolv.conf ou la résolution des noms de domaines.

Historiquement, on indiquait les adresses ip des serveur DNS dans le fichier /etc/resolv.conf.

Depuis debian 8, ce fichier n'en est plus un ! c'est un lien symbolique et le contenu est crée par le programme resolvconf (le nom du programme est très proche !).

Resolvconf concatène le contenu du fichier « head » avec les informations reçu du DHCP réseau.

Lors d'une connexion en NAT, ce sont les adresses IP des DNS fourni par l'accès au réseau qui s'affiche dans le fichier resolv.conf.

Si l'on souhaite forcer un serveur DNS , il y a deux solutions , ajouter la commande

```
« nameserver <IPDUSERVEURDNS> dans le fichier head du programme resolvconf
```

ou

```
« dns-nameserver <IPDUSERVEURDNS> dans le fichier /etc/network/interfaces
```

Une fois sur de la résolution DNS on peut sans crainte faire les mises à jours.

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

Vérifier et activer rc.local au démarrage

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

dans le cas d'une erreur, rechercher avec locate, si non présent installer le !

```
root@debian-base:~# updatedb  
root@debian-base:~# 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 on peut mettre un appel à des programmes.

Pour un script local c'est la solution.

Redémarrez votre système :

```
#init 6
```

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 t'indiquer clairement ce qu'elle fait, en mode bavardise 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

Le plus simple est probablement de ne pas le décompresser, mais plutôt d'utiliser zless (paquet gzip) qui permet de lire le fichier compressé directement. En fait, zless est l'équivalent de : gzip -d fichier.gz | less

Taille d'un dossier

h pour humain

```
du -<CHEMINDUDOSSIER>/ | tail -n 1
```

Trouver les fichiers contenant une chaîne de caractère

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

Plus simple :

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

Supprimer des SVN

```
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
```

Si vous voulez faire des tests, **je vous conseille Eyes of network, qui est gratuit et Français !**

Sinon, vous avez Centreon, qui reste le plus utilisé en entreprise !

Le logiciel de supervision, qu'on appelle aussi le gestionnaire ou le manager, enverra des messages « **GET SNMP** » pour demander un état des différentes variables MIB, à **peu près toutes les minutes**.

LVM

LVM signifie "Logical Volume Manager".

Il s'intercale entre les partitions et le disque dur,

et apporte souplesse et puissance à la gestion des partitions.

Il donne la possibilité de créer des partitions s'étendant sur plusieurs disques dur (RAID logiciel),

de redimensionner à la volée des partitions, etc.

LVM utilise un vocabulaire précis. Voici quelques définitions :

Définitions

PV : Volume Physique.

Les disques durs, partitions de disques durs, volumes RAID ou unités logiques provenant d'un SAN forment des "volumes physiques" (physical volumes ou PV).

C'est l'espace de stockage où seront inscrites les données des volumes logiques.

VG : Groupe de Volumes.

C'est un assemblage d'un ou plusieurs Volumes Physiques (PV).

Un groupe de volumes peut être constitué de un ou plusieurs volumes physiques.

Pour utiliser LVM, il faut obligatoirement créer un groupe de volumes.

Le concept des groupes de volumes permet de gérer du RAID logiciel via LVM.

LV : Volume logique.

Les LV redécoupent les Groupes de Volumes sous forme de partition virtuelle.

Un volume logique ou « LV » pour « logical volume » est l'équivalent d'une partition pour LVM.

Un volume logique est un espace « quelque part dans un groupe de volume » où l'on peut mettre un système de fichiers.

PE : pour être manipuler, les données sont divisées en blocs de données appelé extensions physiques (Physical Extents).

Un extent, ou « physical extent » aussi appelé « PE », est l'équivalent du secteur pour les groupes de volumes.

La taille d'un volume logique sera toujours un multiple de la taille de PE d'un groupe de volumes.

Par défaut, les PE ont une taille de 4 Mio.

LE : même chose que pour les PE mais au niveau logique (Logical Extent). La taille des blocs est la même dans pour chaque volume logique (LV) d'un même groupe de volume (VG).

Un exemple :

Vérifier avec les commandes lvm si le volume est toujours opérationnel

pvscan

```
root@debian8-RAID2:/# pvscan
PV /dev/md1 VG systeme lvm2 [9,06 GiB / 0 free]
Total: 1 [9,06 GiB] / in use: 1 [9,06 GiB] / in no VG: 0 [0 ]
```

lvscan

```
root@debian8-RAID2:/# lvscan
ACTIVE      '/dev/systeme/swap' [952,00 MiB] inherit
ACTIVE      '/dev/systeme/root' [1,86 GiB] inherit
ACTIVE      '/dev/systeme/usr' [952,00 MiB] inherit
ACTIVE      '/dev/systeme/var' [1,86 GiB] inherit
```

```
||-----OS-----||
||-Non-LVM-||-----LVM-----||
|| /boot || LV-1 (/) | LV-2 (swap)| LV 3 (/home) | LV-4 (/tmp)|| Logical Volumes(LV)
||      ||-----||-----||
||      || VG 1      | VG 2  || Volume Groups(VG)
||      ||-----||-----||
||/dev/sda1|| /dev/sda2 | /dev/sda3 | /dev/sdb2 | /dev/sdd4 || Physical Volumes(PV)
||-----||-----||
```

Labels

Vous devriez utiliser les noms ou labels des volumes logiques (LV) dans /etc/fstab pour les identifier, plutôt que les UUID ou les règles de nommage du noyau (/dev/sda) afin d'éviter les conflits avec la restauration d'images des volumes (snapshots).

/boot

Grub et LiLo ne sont pas compatibles avec LVM,

donc /boot devra être installé en dehors de l'espace disque géré par LVM.

Les commandes LVM sont simples à utiliser et elles intègrent toutes une aide en ligne très bien conçue.

De plus, leur nom se « devine » assez facilement :

Les commandes agissant sur les volumes physiques commencent par pv.

Les commandes agissant sur les groupes de volumes commencent par vg.

Les commandes agissant sur les volumes logiques commencent par lv.

Vous pouvez les lister avec la commande :

```

root@debian8-RAID2:/home/sysadmin# command man -k '^pv'
pvchange (8)      - change attributes of a physical volume
pvck (8)         - check physical volume metadata
pvcreate (8)      - initialize a disk or partition for use by LVM
pvdisplay (8)     - display attributes of a physical volume
pvmove (8)       - move physical extents
pvremove (8)     - remove a physical volume
pvresize (8)     - resize a disk or partition in use by LVM2
pvs (8)          - report information about physical volumes
pvscan (8)       - scan all disks for physical volumes
root@debian8-RAID2:/home/sysadmin#

```

```

root@debian8-RAID2:/home/sysadmin# pvscan
PV /dev/md1  VG systeme  lvm2 [9,06 GiB / 0  free]
Total: 1 [9,06 GiB] / in use: 1 [9,06 GiB] / in no VG: 0 [0  ]
root@debian8-RAID2:/home/sysadmin# pvs
PV      VG      Fmt  Attr PSize PFree
/dev/md1  systeme lvm2 a-- 9,06g  0
root@debian8-RAID2:/home/sysadmin# pvdisplay
--- Physical volume ---
PV Name      /dev/md1
VG Name      systeme
PV Size      9,06 GiB / not usable 0
Allocatable  yes (but full)
PE Size      4,00 MiB
Total PE     2319
Free PE      0
Allocated PE 2319
PV UUID      XktM8d-KVUr-7imC-keWc-BCwt-YfFu-JlmDJY

```

```

root@debian8-RAID2:/home/sysadmin# lvdisplay | less
--- Logical volume ---
LV Path      /dev/systeme/swap
LV Name      swap
VG Name      systeme
LV UU
...
....

(END)

```

```

root@debian8-RAID2:/home/sysadmin# fdisk /dev/sda

```


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.

Commande (m pour l'aide) : p
Disque /dev/sda : 10 GiB, 10737418240 octets, 20971520 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 : 0xf36b24c1

Device	Boot	Start	End	Sectors	Size	Id	Type
/dev/sda1	*	2048	1953791	1951744	953M	fd	Linux raid autodetect
/dev/sda2		1953792	20969471	19015680	9,1G	fd	Linux raid autodetect

Commande (m pour l'aide) : q

```
root@debian8-RAID2:/home/sysadmin# ls -l /dev/sda*
brw-rw---- 1 root disk 8, 0 févr. 17 16:45 /dev/sda
brw-rw---- 1 root disk 8, 1 févr. 17 16:45 /dev/sda1
brw-rw---- 1 root disk 8, 2 févr. 17 16:45 /dev/sda2
root@debian8-RAID2:/home/sysadmin#
```

```
root@debian8-RAID2:/home/sysadmin# vgdisplay | tail
Max PV          0
Cur PV         1
Act PV          1
VG Size         9,06 GiB
PE Size         4,00 MiB
Total PE        2319
Alloc PE / Size 2319 / 9,06 GiB
Free PE / Size  0 / 0
VG UUID         1lffTg-evkW-B7o5-dVOP-x106-KBgR-Xtg4yB
```

```
root@debian8-RAID2:/home/sysadmin# tree /dev/mapper/
/dev/mapper/
├── control
├── systeme-home -> ../dm-5
├── systeme-root -> ../dm-0
├── systeme-swap -> ../dm-1
└── systeme-tmp -> ../dm-4
```

```
|— systeme-usr -> ../dm-2
|— systeme-var -> ../dm-3
```

0 directories, 7 files

lvmdiskscan

— Analyser tout les supports visibles par LVM2.

```
root@debian8-RAID2:/home/sysadmin# lvmdiskscan
/dev/md0      [ 952,44 MiB]
/dev/systeme/root [ 1,86 GiB]
/dev/md1      [ 9,06 GiB] LVM physical volume
/dev/systeme/swap [ 952,00 MiB]
/dev/systeme/usr [ 952,00 MiB]
/dev/systeme/var [ 1,86 GiB]
/dev/systeme/tmp [ 952,00 MiB]
/dev/systeme/home [ 2,55 GiB]
6 disks
1 partition
0 LVM physical volume whole disks
1 LVM physical volume
```

```
root@debian8-RAID2:/home/sysadmin# df -h
Sys. de fichiers    Taille Utilisé Dispo Uti% Monté sur
/dev/dm-0           1,8G  229M 1,5G 14% /
udev                10M   0 10M  0% /dev
tmpfs               201M  4,5M 196M  3% /run
/dev/dm-2           922M  507M 352M 60% /usr
tmpfs               501M   0 501M  0% /dev/shm
tmpfs               5,0M   0 5,0M  0% /run/lock
tmpfs               501M   0 501M  0% /sys/fs/cgroup
/dev/md0            922M   33M 842M  4% /boot
/dev/mapper/systeme-tmp 922M  1,2M 857M  1% /tmp
/dev/mapper/systeme-home 2,5G  3,9M 2,4G  1% /home
/dev/mapper/systeme-var 1,8G  207M 1,5G 12% /var
```

1 -Augmenter la taille du disque dur virtuel sous virtualbox



Attention !!!!

Nous allons augmenter la taille du disque dur mais pas l'espace de stockage du système de la VM

Ce processus change uniquement la taille du disque virtuel, mais pas des partitions qu'il contient !

Vous devez donc augmenter la taille des partitions sous Linux ...

Avec Le Live CD Knoopix, l'outil GParted

2 - Localiser le disque dur virtuel ainsi que son type

```
J:\.VirtualBox\mondomaine.moi\CESI -INFAL12\debian-bind-kde\debian-bind-kde.vdi
```

[Convertisseur en ligne](#)

<http://mon-ip.awardspace.com/convertisseur.php>

Taille en Octets - kilo - mega - giga

8388608 Ko

8192 Mo

8 Go

10485760 Ko

10240 Mo

10 Go

20971520 Ko

20480 Mo

20 Go

[Sous Windows](#)

Ouvrir une invite de commande et se rendre dans le dossier de VirtualBox

```
# cd "C:\Program Files\Oracle\VirtualBox"
```

Saisir la commande VBoxManage.exe modifyhd "{chemin-vers-le-disque}" --resize 20480

```
# VBoxManage.exe modifyhd "J:\.VirtualBox\mondomaine.moi\CESI -INFAL12\debian-bind-kde\debian-bind-kde.vdi" --resize 20480
```

```
# VBoxManage.exe modifyhd "J:\.VirtualBox\debian-dns-kde\debian-dns-kde.vdi" --resize 20480
```

```
# VBoxManage.exe modifyhd "J:\.VirtualBox\debian-dns\debian-dns.vdi" --resize 20480
```

Cette ligne de commande, une fois adaptée au contexte, devrait permettre de résoudre le problème :

```
VBoxManage modifymedium <chemin et nom du fichier vdi> --resize <nouvelle taille en MB>
```

```
# VBoxManage modifymedium "J:\.VirtualBox\mondomaine.moi\CESI -INFAL12\debian-bind-kde\debian-bind-kde.vdi" --resize 20480
```

```
# VBoxManage modifymedium "J:\.VirtualBox\debian-dns-kde\debian-dns-kde.vdi" --resize 20480
```

```
# VBoxManage modifymedium "J:\.VirtualBox\debian-dns\debian-dns.vdi" --resize 20480
```

Ça ne changera pas la taille du fichier vdi, mais ça modifiera la taille du système de fichiers virtualisé.

Il peut y avoir des erreurs, ce qui s'est produit, j'effectue un 2eme test identique.

2eme avec erreur

```
C:\Program Files\Oracle\VirtualBox>VBoxManage.exe modifyhd "J:\.VirtualBox\debian-dns-kde\debian-dns-kde.vdi"
--resize 20480
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
```

```
C:\Program Files\Oracle\VirtualBox>VBoxManage modifymedium "J:\.VirtualBox\debian-dns-kde\debian-dns-kde.vdi" --resize 20000
0%...
Progress state: VBOX_E_NOT_SUPPORTED
VBoxManage.exe: error: Resize medium operation for this format is not implemented yet!
```

```
C:\Program Files\Oracle\VirtualBox>VBoxManage modifymedium "J:\.VirtualBox\debian-dns-kde\debian-dns-kde.vdi" --resize 20000
0%...
Progress state: VBOX_E_NOT_SUPPORTED
VBoxManage.exe: error: Resize medium operation for this format is not implemented yet!
```

```
C:\Program Files\Oracle\VirtualBox>VBoxManage modifymedium "J:\.VirtualBox\debian-dns-kde\debian-dns-kde.vdi" --resize 20480
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
```

```
# VBoxManage showhinfo "J:\.VirtualBox\debian-dns\debian-dns.vdi"
```

```
C:\Program Files\Oracle\VirtualBox>VBoxManage showhinfo "J:\.VirtualBox\debian-dns-kde\debian-dns-kde.vdi"
UUID:      f567b987-5d63-40d7-8c4a-c3bc7de665eb
Parent UUID: base
State:      created
Type:       normal (base)
Location:   J:\.VirtualBox\debian-dns-kde\debian-dns-kde.vdi
Storage format: VDI
Format variant: dynamic default
Capacity:   20480 MBytes
Size on disk: 6629 MBytes
Encryption: disabled
In use by VMs: debian-dns-kde (UUID: 7ad9d482-1da8-4ccc-bd44-97fd37d2e6f3)
```

```
C:\Program Files\Oracle\VirtualBox>
```

Vérifier que la taille du disque est bien passée à 20 GO ou relancer VirtualBox.

L'agrandissement du disque n'occupera pas plus de place avec le disque virtuel VDI

sur votre machine hôte si vous avez opté au départ pour un stockage dynamique, contrairement au mode statique.

C'est pour cette raison qu'il vaut mieux être généreux au moment de la création d'une VM car seul l'espace nécessaire est consommé.

[Utiliser Knoppix !](#)

English version of KNOPPIX 8.1 DVD+USB edition.

Release notes at <http://knopper.net/knoppix/knoppix810-en.html>

```
sysadmin@debian-bind-kde:~$ su -
Mot de passe :
root@debian-bind-kde:~# fdisk -l
Disque /dev/sda : 10 GiB, 10737418240 octets, 20971520 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 : 0x2c3b14f3
```

```
Périphérique Amorçage Début Fin Secteurs Taille Id Type
/dev/sda1 * 2048 16777215 16775168 8G 83 Linux
/dev/sda2 16779262 20969471 4190210 2G 5 Étendue
/dev/sda5 16779264 20969471 4190208 2G 82 partition d'échange Linux / Solaris

root@debian-bind-kde:~#
```

Voilà, nous avons augmenté la taille de notre disque Virtuel.

10 240,00 MiB

[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.

A la 1ere connexion ; Liser et accepter le certificat.

```
login as: sysadmin
sysadmin@192.168.101.254's password:
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Dec 15 17:36:41 2017
sysadmin@debian:~$
```

Pour Installer SSH

Pour exemple :

S'il n'a pas été sélectionné lors de l'installation ou s'il a été désinstaller 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 clefs de cryptage servant à authentifier le serveur.

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

Celui-ci doit accepter la clef lors de la première connexion, et refuse de se reconnecter sur le serveur ayant le même nom si cette clef 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 passez en root ou encore la commande sudo pour votre utilisateur (voir annexe).

VirtualBox : Debian –Version 7.0

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 pourra 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)

A 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
rx-	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
<code>chmod 640 temps.txt</code>	<code>rw-r-----</code>
<code>chmod 700 temps.txt</code>	<code>rwX-----</code>
<code>chmod 664 temps.txt</code>	<code>rw-rw-r--</code>
<code>chmod 761 temps.txt</code>	<code>rwXrw-r--</code>
<code>chmod 610 temps.txt</code>	<code>rw-r-----</code>

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 ⇒ lecture
- w : write ⇒ écriture
- x : execute ⇒ 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 récurifs 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-w+x,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>
```

A 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.

Vous pourriez très bien vous contenter de ce fonctionnement (un utilisateur = un groupe), mais au cas où vous auriez beaucoup d'utilisateurs, je vais quand même vous montrer comment créer des groupes.

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 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 <répertoire>
chgrp ftpgroup <répertoire>
chmod 570 <répertoire>
```

Ce qui signifie respectivement :

Le répertoire appartient à www.data ;

Le répertoire est placé 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 être 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	Écriture (write)
o	Others (autres)	=r	définir	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 `x` 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, quelque 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 représenté 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.

Sauvegarde des droits

Dans le cadre d'une migration de serveur je voudrai sauvegarder l'ensemble des ACL's.

`getfacl` sauvegarde récursivement les droits d'une arborescence dans le fichier *get_rep.acl*;

Il est utile d'enregistrer l'ensemble des acl quand on a un serveur de fichiers dans une communauté de travail hétérogène (des centaines d'utilisateurs et de groupes). Cette manipulation peut se faire grâce à la commande:

```
getfacl -R /donnees > nom_de_fichier      # L'option -R permet la récursivité sur tous
les répertoires,                           # sous-répertoires et fichiers de la
partition /donnees                         # L'enregistrement de l'ensemble de ces
acl est effectué dans                      # le fichier nom_de_fichier
```

Attribution des acl à l'aide d'un fichier

Il est possible de restituer l'ensemble des acl d'une partition grâce au fichier obtenu par la commande :

```
getfacl -R /donnees > nom_de_fichier
```

Pour ce faire, il suffit de se placer à la racine et d'exécuter la commande :

```
setfacl --restore=nom_de_fichier
```

```
getfacl -R /chemin/vers/partage /chemin/vers/get_rep.acl
```

```

root@debian11:/home# tree -puga
.
├── [drwxr-xr-x root  root  ] shares
│   └── [drwxr-xr-x w10a  w10a  ] w10a
└── [drwxr-xr-x sysadmin sysadmin] sysadmin
    ├── [-rw----- sysadmin sysadmin] .bash_history
    ├── [-rw-r--r-- sysadmin sysadmin] .bash_logout
    ├── [-rw-r--r-- sysadmin sysadmin] .bashrc
    ├── [drwxr-xr-x sysadmin sysadmin] .local
    │   └── [drwx----- sysadmin sysadmin] share
    │       └── [drwx----- sysadmin sysadmin] nano
    └── [-rw-r--r-- sysadmin sysadmin] .profile

```

pour la restauration :

setfacl lit le contenu du fichier *get_rep.acl* pour en restaurer les droits sur l'arborescence existante.

```
setfacl --restore=/chemin/vers/get_rep.acl
```

```

root@debian11:/home# chmod -R ug+rw,ox-w /home/shares/
root@debian11:/home# tree -puga

```

```

.
├── [drwxrwxr-x root  root  ] shares
│   └── [drwxrwxr-x w10a  w10a  ] w10a
└── [drwxr-xr-x sysadmin sysadmin] sysadmin
    ├── [-rw----- sysadmin sysadmin] .bash_history
    ├── [-rw-r--r-- sysadmin sysadmin] .bash_logout
    ├── [-rw-r--r-- sysadmin sysadmin] .bashrc
    ├── [drwxr-xr-x sysadmin sysadmin] .local
    │   └── [drwx----- sysadmin sysadmin] share
    │       └── [drwx----- sysadmin sysadmin] nano
    └── [-rw-r--r-- sysadmin sysadmin] .profile

```

6 directories, 4 files

```

root@debian11:/home# chmod -R ug+rw,ox-w /home/sysadmin/.bash_history
root@debian11:/home# tree -puga

```

```

.
├── [drwxrwxr-x root  root  ] shares
│   └── [drwxrwxr-x w10a  w10a  ] w10a
└── [drwxr-xr-x sysadmin sysadmin] sysadmin
    ├── [-rwxrwxr-x sysadmin sysadmin] .bash_history
    ├── [-rw-r--r-- sysadmin sysadmin] .bash_logout
    ├── [-rw-r--r-- sysadmin sysadmin] .bashrc
    └── [drwxr-xr-x sysadmin sysadmin] .local

```

```
| └─ [drwx----- sysadmin sysadmin] share
|   └─ [drwx----- sysadmin sysadmin] nano
└─ [-rw-r--r-- sysadmin sysadmin] .profile
```

6 directories, 4 files

```
root@debian11:/home# cd ..
```

```
root@debian11:/# setfacl --restore=/get_rep.acl
```

```
root@debian11:/# ls -la /home/
```

total 16

```
drwxr-xr-x 4 root  root  4096 15 févr. 19:22 .
```

```
drwxr-xr-x 18 root  root  4096 15 févr. 19:39 ..
```

```
drwxr-xr-x 3 root  root  4096 15 févr. 19:22 shares
```

```
drwxr-xr-x 3 sysadmin sysadmin 4096 10 janv. 14:10 sysadmin
```

```
root@debian11:/# tree -puga /home/
```

/home/

```
└─ [drwxr-xr-x root  root  ] shares
```

```
|   └─ [drwxr-xr-x w10a  w10a  ] w10a
```

```
└─ [drwxr-xr-x sysadmin sysadmin] sysadmin
```

```
    └─ [-rw----- sysadmin sysadmin] .bash_history
```

```
    └─ [-rw-r--r-- sysadmin sysadmin] .bash_logout
```

```
    └─ [-rw-r--r-- sysadmin sysadmin] .bashrc
```

```
    └─ [drwxr-xr-x sysadmin sysadmin] .local
```

```
    |   └─ [drwx----- sysadmin sysadmin] share
```

```
    |     └─ [drwx----- sysadmin sysadmin] nano
```

```
    └─ [-rw-r--r-- sysadmin sysadmin] .profile
```

6 directories, 4 files

```
root@debian11:/# chmod -R ug+rw,ox-w /home/sysadmin/.bash_history
```

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 smiley)

```
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:

#include_dir /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
```

Activer le forwarding

Modifiez le fichier : /etc/sysctl.conf

```
# nano /etc/sysctl.conf
```

Dé-commenter la ligne suivante :

```
net.ipv4.ip_forward=1
```

Et sauvegardez

Vérifiez la présence de ce fichier

```
# /proc/sys/net/ipv4/ip_forward
```

Si le paramètre est à zéro

Écrivez directement la valeur 1 à la place

```
root@debian:/home/sysadmin# cat /proc/sys/net/ipv4/ip_forward  
0
```

Écrivez directement la valeur 1 à la place en utilisant la commande « echo »

```
root@debian:/home/sysadmin# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Vérifiez

```
root@debian:/home/sysadmin# cat /proc/sys/net/ipv4/ip_forward  
1
```

Appliquez les changements

```
root@debian:/home/sysadmin# sysctl -p /etc/sysctl.conf  
net.ipv4.ip_forward = 1
```

```
#sysctl -p /etc/sysctl.conf
```

Relancez le réseau

```
#service network-manager restart
```

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 UtilisÃ© Dispo Uti% MontÃ© 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 jocker *

```
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

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	QN4.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

[A 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)

```

VirtualBox

Extension VirtualBox

Avec debian, je vous conseille de vérifier si votre version de **VirtualBox** est supporté, pour ma part, et bien que **VirtualBox** en soit a la version 5.2.8, j'ai du descendre de version pour la : **5.1.30r18389(Qt5.6.2)** et ses extensions.

Il faut installer ce paquet qui est nécessaire pour l'utilisation les extensions Vbox, remarquez l'utilisation de la commande « `uname` » !

```
# apt-get install build-essential linux-headers-$(uname -r)
```

Insérer le cd VBoxLinuxAdditions, soit via une image iso soit en cliquant sur le menu Vbox « insérer les extensions invités ».

Repérer toutes les partitions avec la commande

```
# blkid
```

Le cd est dans `/dev/sr0`

Voir s'il est déjà monté,

```
ls /media/
```

sinon, Monter le cd avec la commande suivante

```
# mount /dev/sr0 /media/cdrom0
```

Puis saisir.

```
# sh /media/cdrom0/VBoxLinuxAdditions.run
```

Et validez l'installation

Après installation,

Redémarrez votre système :

```
# shutdown -r
```

L'ajout des extensions ne fonctionne pas sur une debian en ligne de commande donc connexion en ssh , avec putty, qui permet le copier/coller.

1] Type de carte réseau

PCnet-PCI II : 10 Mb/s

PCnet-FAST III : 100 Mb/s

Intel PRO/1000 MT Desktop : 1000 Mb/s

Intel PRO/1000 T Server : 1000 Mb/s

Intel PRO/1000 MT Server : 1000 Mb/s

2] Réseau Invité <-> Système Hôte

Mode d'accès réseau : Accès privé hôte

Cela permet de créer un nouveau réseau entre les machines virtuelles et le système hôte. Le système hôte et les machines virtuelles ont accès à leurs ressources communes, mais pas au reste du réseau auquel le système hôte est connecté ni à internet.

Dans ce mode, votre machine virtuelle ne peut communiquer qu'avec votre machine hôte. Pour cela, une carte Ethernet virtuelle est spécifiquement créée sur la machine hôte (vboxnet0). Cette carte se configure de la même manière qu'une carte physique standard (ifconfig vboxnet0...). Cela permet de pouvoir travailler en réseau avec une machine virtuelle alors qu'aucune carte physique n'est présente (dans l'avion ou au milieu du désert par exemple).

Pour information :

? Adresse réseau : 192.168.56.0

? DHCP : actif

Pour accéder au premier système invité depuis le système hôte :

? http://192.168.56.101/

Pour accéder au système hôte depuis un des systèmes invités :

? http://192.168.56.1/

3] Réseau Invité <-> Réseau Hôte / Internet

Mode d'accès réseau : Accès par pont

Ce mode crée un pont vers la carte réseau du système hôte.

Dans le réseau local, la machine virtuelle est visible, elle est vue exactement

Comme n'importe quel autre ordinateur de ce réseau.

Elle a donc accès à toutes les ressources réseau (y compris internet) que les autres ordinateurs du réseau local.

Pour information :

? DHCP : actif si celui-ci est actif sur le réseau local

4] Réseau Invité <-> Réseau Invité

Mode d'accès réseau : Réseau interne

Cela permet de créer un nouveau réseau entre les machines virtuelles.

Elles n'accèdent pas au réseau local des machines physiques.

Il n'y a donc pas d'accès à internet et pas d'accès aux ressources du réseau local.

Ce mode permet de connecter des machines virtuelles entre-elles sur un réseau virtuel isolé de la machine hôte.

Par défaut le premier réseau virtuel est nommé « intnet ».

Pour information :

? Adresse réseau : non configuré

? DHCP : inactif

5] Réseau Invité -> Système Hôte / Internet

Mode d'accès réseau : NAT

Fait de la transposition d'adresse avec le système hôte.

La machine virtuelle utilise la connexion réseau du système hôte pour communiquer avec internet.

La machine virtuelle est invisible dans le réseau local et n'a accès à aucun ordinateur sauf celui du système hôte.

Dans ce mode, les trames sortantes, de votre machine virtuelle posséderont la même adresse que votre machine hôte

(Quelle que soit l'adresse IP de votre machine virtuelle). Une translation d'adresse réseau est systématiquement effectuée (Network Adresse Translation).

Particularité : Dans ce mode, la machine virtuelle ne peut être utilisée qu'en client (navigation, mail, etc.) et non en serveur. Elle ne peut pas recevoir de requêtes directes de l'extérieur.

Pour information :

? Adresse réseau : 10.0.2.0

? Passerelle : 10.0.2.2

? DHCP : actif

Pour accéder au système hôte depuis un des systèmes invités :

? <http://10.0.2.2/>

Une petite précision concernant le point 2 (Réseau Hôte <-> Réseau Invité).

Il serait plus juste de dire que le mode Accès privé hôte crée un accès Système hôte <-> Réseau Invité.

La raison est que toutes les machines virtuelles configurées avec ce mode d'accès réseau peuvent communiquer entre elles

(= le réseau invité) et avec le système hôte uniquement, pas avec tout le réseau auquel l'hôte appartient.

D'où Accès privé hôte.

Si l'on souhaite faire rejoindre la machine virtuelle au même réseau que celui auquel appartient l'hôte

(donc créer réellement Réseau Hôte <-> Réseau Invité), il faut plutôt choisir le mode Accès par pont, qui "duplique" une carte réseau de la machine hôte pour permettre à la machine virtuelle un accès direct au réseau hôte, comme si la machine virtuelle était un ordinateur distinct.

Le mode d'accès réseau indique comment la machine virtuelle pourra communiquer avec le reste du LAN :

- Non attaché indique qu'une carte réseau est branchée dans la machine virtuelle,
 - mais qu'elle n'est raccordée à aucun réseau. Bref, aucun accès au réseau local ni à Internet ;
- NAT fait de la transposition d'adresse avec le système d'exploitation hôte.
 - La machine virtuelle utilise la connexion réseau du système hôte pour communiquer avec Internet.
 - La machine virtuelle est invisible dans le LAN et n'a accès à aucun ordinateur dans le LAN, seulement à Internet ;
- Accès par pont crée un pont vers la carte réseau de l'ordinateur réel, sélectionnée dans la liste Nom.

- Dans le LAN, la machine virtuelle est visible, elle est vue exactement comme n'importe quel autre ordinateur.
 - Elle a accès à toutes les mêmes ressources réseau (y compris Internet) que les autres ordinateurs du réseau local ;
- Réseau interne permet de créer un nouveau LAN entre plusieurs machines virtuelles.
 - Elles n'accèdent pas au LAN des machines physiques. Pas d'accès à Internet ni aux ressources du LAN ;
 - Accès privé hôte crée un nouveau LAN entre les machines virtuelles et le système d'exploitation hôte.
 - L'OS hôte et les machines virtuelles ont accès à leurs ressources communes, mais pas au reste du LAN ni à Internet.

Le mode le plus simple, c'est NAT.

Pas de configuration nécessaire. Mais ça ne fait que donner accès à Internet.

Si on a besoin de davantage de possibilités (ex : accéder à des imprimantes réseau, accéder à des dossiers partagés d'un autre ordinateur)

à partir de la machine virtuelle, alors Accès par pont est une meilleure option.

L'intérêt d'utiliser 2 cartes physiques dans votre machine est de les relier à deux réseaux différents.

Le poste Windows est présent sur le réseau hôte privé, tester un ping depuis Windows vers l'IP de la carte de votre VM.

Par exemple,

L'une des cartes est reliée à un premier commutateur.

- Celui-ci est relié à un routeur (et à Internet).
- Toutes les machines (physiques ou virtuelles) reliées à ce réseau ont accès à Internet ;

L'autre carte est reliée à un second commutateur.

- Ceci-ci est relié à aucun routeur.
- C'est un réseau interne uniquement.
- Toutes les machines reliées à ce réseau n'ont pas accès à Internet.

On indique que la machine hôte dispose de deux cartes réseau physiques.

Dans ce cas d'exemple, on pourra donc relier par câble l'une des cartes au premier commutateur

(La machine hôte aura accès à Internet) et l'autre carte, au second commutateur

(La machine hôte aura accès au réseau interne).

Si on lie en accès par pont tous les serveurs virtuels à cette seconde carte réseau, alors effectivement, ils ne seront accessibles et visibles que sur le réseau interne.

Mais les clients physiques, s'ils n'ont qu'une seule carte réseau, ne pourront rejoindre qu'un seul des deux réseaux.

Ils seront soit raccordées au premier commutateur (à Internet seulement) soit au second commutateur (au réseau interne seulement).

Pour communiquer dans les deux réseaux, les clients physiques devront eux-aussi avoir deux cartes réseau physiques, reliées chacune aux deux réseaux. Sinon, ils ne peuvent communiquer qu'avec un seul des deux réseaux.

Man-pages

Obtenir les manpages en Français

Le système dispose d'une commande man, permettant d'obtenir des informations sur une commande.

Toutefois il se peut que se soit en Anglais suivant la version de Debian

Les man-pages ont été traduites grâce au projet de traduction perkamon sur traduc.org , voici comment les obtenir:

```
sudo apt-get install manpages-fr
```

Sous Debian 8 Jessie, les man-pages sont bien traduites, pas de soucis.

Sous Debian Wheezy ce n'est pas tout à fait le cas, on voit que c'est encore en Anglais.

Afin de résoudre ce manque de traduction il faut ajouter le paquet manpages-fr-extra:

```
apt-get install manpages-fr-extra manpages-fr-dev
```

Man utilise le lecteur de fichier : **more**, il existe d'autres lecteurs qui ont quelques différences comme **less**, cependant, nous pouvons utiliser **most**, ce lecteur est plus attrayant et coloré.

```
apt-get install most
```

Et pour l'utiliser il faut indiquer au système que nous souhaitons l'utiliser avec :

```
export PAGER=most
```

Comme on peut le voir il y a une coloration syntaxique, ce que le rend un peu plus lisible.

Si l'on ouvre un second terminal, ou si on le ferme puis ouvre, on constate que la configuration, n'est pas valable dans le second terminal.

Pourquoi?

La modification ne s'applique qu'à la session active, lorsque vous lancez un second terminal, le shell va lire le fichier de configuration **.bashrc** qui se trouve dans votre répertoire utilisateur, et ce fichier est inchangé.

Si vous souhaitez garder le PAGER **most** il faut éditer le fichier comme ceci:

```
nano ~/.bashrc
```

Puis ajoutez à la fin

```
export PAGER=most
```

Puis il faut dire au shell de recharger le fichier de configuration avec

```
source ~/.bashrc
```

most sera alors votre lecteur de fichier texte par défaut.

Sources :

<http://www.informatique-astuces.com/installer-un-firewall-sur-debian/>

<https://fr.wikipedia.org/wiki/Iptables>

<https://www.paranoiaque.fr/tutorial/installation-lamp-facile-debian>

<http://manpages.debian.org/cgi-bin/man.cgi>

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

<https://www.virtualbox.org/>

<https://www.debian.org/index.fr.html>

<http://virtualboxes.org/doc/installing-guest-additions-on-debian/>

<http://www.linux-france.org/prj/edu/archinet/systeme/ch62s03.html>

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

<https://debian-facile.org/doc:systeme:apt:clients>

<http://les-raccourcis-clavier.fr/signer-d'une-pc/>

Liens utiles

Liens en rapport au sujet :

- à propos de gestionnaire de volume logique : [lvm](#)
- à propos de RAID : http://fr.wikipedia.org/wiki/RAID_%28informatique%29
- à voir : [supprimer-un-raid-logiciel](#)

FIN