Installer et configurer un serveur Debian 12

Préambule :

On s'attaque dans ce tuto à l'installation de base d'un serveur Debian 12.4.0 pour amd64.

Préparation de la machine (virtuelle) sous VirtualBox 7

Lancez le téléchargement de l'image iso du DVD « netinstall » de Debian depuis le site officiel :

https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/debian-12.4.0-amd64-netinst.iso

On prépare la machine en choisissant les éléments de configuration suivants :

- Nommez la machine et choisissez le fichier iso qui servira à l'installation
- Ne cochez pas l'installation automatique
- Mémoire vive 4096 Mo
- CPU 2
- Enable EFI désactivé
- Virtual Hard Disk de 40 Go sans pré-allocation
- On configure l'adaptateur réseau en mode Pont sur la carte physique connectée de l'hôte
- Dans les options avancées de l'adaptateur réseau, choisissez le mode de promiscuité qui autorise tout.

Lancement de l'installation

Lancez la machine virtuelle, elle doit démarrer sur le dvd d'installation (fichier iso) que vous avez précédemment téléchargé et déclaré dans la machine virtuelle.

ATTENTION : pensez à installer le « VirtualBox-Extension-Pack » sous VirtualBox avant de lancer l'installation de Debian, vous vous éviterez ainsi des problèmes d'affichage.

Pour plus de confort, allez dans le menu « Écran » de VirtualBox et choisissez le « mode mise à l'échelle (Host+C) » pour plus de confort.

Premiers choix : « installer menu »

« Graphical Install » ou « Install » ça n'a pas beaucoup d'importance, on choisit « Graphical Install » si l'on souhaite utiliser sa souris, « Install » si on est à l'aise avec la navigation dans les menus à l'aide de la touche Tabulation.

Choix de la langue et des paramètres régionaux

On choisit comme langue le Français. Pour la location, dans « Autre », « Océan Indien » et « Réunion, île de la ». On choisit les paramètres locaux « Français fr_FR.UTF-8 ». On choisit aussi la configuration Français pour le clavier.

Paramétrage de la machine

Donnez un nom à votre machine (SrvDeb dans notre cas) et indiquez le domaine dans lequel elle va être placée (btssio.lan pour nous).

Il faut maintenant choisir

- le mot de passe pour le super utilisateur root (2 fois)
- le nom et l'identifiant de notre utilisateur principal (« administrateur » pour nous)
- Le mot de passe pour l'utilisateur « administrateur » (2fois)

Installation du système sur le support de stockage de la machine

On choisit dans notre exemple le partitionnement « assisté- utiliser le disque entier ». On place tous dans une unique partition. En fonction des contraintes exprimées pour votre serveur, vous pouvez bien entendu choisir des paramètres différents pour que l'organisation de votre système d'exploitation soit en adéquation avec les besoins exprimés.

La machine procède alors à l'installation du système de base. Une fois l'installation achevée, indiquez que vous ne souhaitez pas analyser d'autre support.

Choix du miroir d'archive Debian pour l'installation des paquets

Choisissez un serveur local à la Réunion vous éviterez les temps d'attente lors des installations et des mises à jour, surtout quand les câbles sous-marins sont déficients. Il se trouve que Mithril propose un miroir. Comme ce sont des gens biens et que nous leur faisons pleinement confiance, nous choisissons leur miroir (debian.mithril.re)

Si vous installez votre serveur dans une infrastructure dotée d'un proxy, il faut déclarer ce dernier pour pouvoir lancer l'installation finale des paquets et des mises à jours :

http://[[nom-utilisateur][:mot-de-passe-utilisateur]@]ADRESSE-IP[:port]

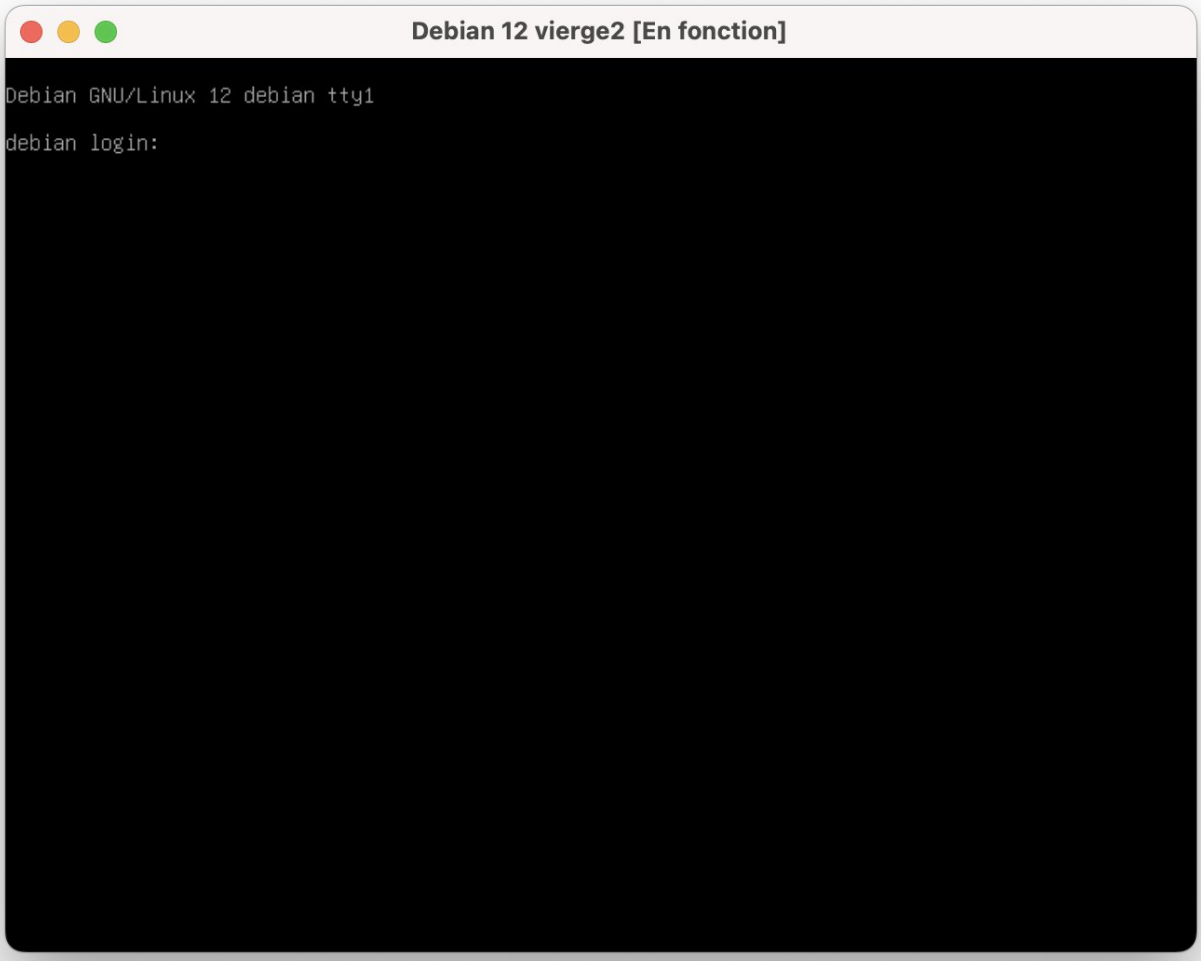
Par exemple :
http://user:motdepasse@192.168.0.1:3128
si l'utilisateur « user » ayant pour mot de passe « motdepasse » qui l'autorise à accéder à internet via le proxy d'adresse 192.168.0.1 configuré sur le port 3128.

Sélection des logiciels

On retire tout sauf la dernière ligne « utilitaires usuels du système ». Nous faisons ici le choix de ne pas installer d'interface graphique pour notre serveur. Nous installerons nous même les paquets au fur et à mesure de nos besoins.

ET C'EST PARTI POUR LA DERNIERE ETAPE : le système installe les paquets manquants et les dernières mises à jours à partir du miroir que nous lui avons déclaré.

On laisse le système installer le GRUB sur le disque principal, et voilà la résultat :



Notre serveur est installé et il a redémarré. Il faut maintenant se connecter en tant qu'utilisateur principal (« administrateur » dans notre cas). Pour obtenir l'invite de commande standard :

```
administrateur@debian:~$
```

Nous sommes actuellement connecté en tant qu'utilisateur « administrateur » sur le serveur nommé « debian ». Dans l'arborescence, nous sommes situé dans le répertoire personnel de l'utilisateur courant (symbolisé par le caractère tilde ~).

Configuration de base de notre serveur

La commande sudo

Pour Linux, certaines commandes ne sont pas accessibles aux utilisateurs, même s'ils sont administrateurs du système. Pour pouvoir lancer ces commandes, il existe deux possibilités :

- Disposer des droits de Super utilisateur (nommé root)
- Pouvoir s'octroyer les droits de Super Utilisateur le temps d'une commande en la faisant précéder de l'instruction « sudo »

Nous allons donc installer la commande sudo et la configurer pour permettre à notre utilisateur de l'utiliser.

Il faut donc commencer par se connecter en tant que Super Utilisateur (su) et installer le paquet sudo (apt install sudo).

```
administrateur@debian:~$ su
Mot de passe :
root@debian:/home/administrateur# apt install sudo
```

Notez que lorsque l'on est connecté en tant que root, le prompt $ est remplacé par le caractère # qui nous indique que nous sommes en possession des pleins pouvoir sur le système.

Ensuite il faut configurer sudo pour permettre à notre utilisateur « administrateur » d'utiliser sudo. Pour celà il existe deux méthodes :

- Autoriser uniquement « administrateur »
- Autoriser tous les membres du groupe « sudo »

Première méthode (la plus rapide) :

Il faut éditer le fichier sudoers de paramètrage du paquet sudo pour autoriser explicitement « administrateur ».

```
root@debian:/home/administrateur# nano /etc/sudoers
```

Dans le fichier, ajouter la ligne :

```
Admininstrateur                ALL=(ALL:ALL)          ALL
```

Vous pouvez la placer juste après la ligne « root ALL=(ALL:ALL) ALL »

Pour enregistrer vos modifications et quitter le fichier sudoers, <CTL+X> puis Y (ou O)

Pour vérifier : déconnectez vous du compte root (exit) et lancez une commande avec sudo :

```
root@debian:/home/administrateur# exit
administrateur@debian:~$ sudo apt update
[sudo]mot de passe de administrateur :
```

La commande « apt update » se lance. Si vous essayez sans la précéder de « sudo » vous verrez que vos droits sont insuffisants en temps qu' « administrateur ».

Deuxième méthode (la plus complète) :

On va ajouter l'utilisateur « administrateur » au groupe « sudo ». Ainsi, il pourra utiliser la commande pour s'octroyer temporairement les droits de super utilisateur.

On commence par se connecter en tant que root avec la commande su - (ne pas oublier le tiret qui permet de charger les variables d'environnement du super utilisateur root). On ajoute ensuite « administrateur » au groupe « sudo » à l'aide de la commande usermod.

On reboot ensuite la machine et on peut tester.

```
administrateur@debian:~$ su -
root@debian:/home/administrateur# usermod –aG sudo administrateur
root@debian:/home/administrateur# systemctl reboot
```

Une fois reconnecté comme « administrateur », lancez la commande sudo whoami. La réponse devrait être « root ».

```
administrateur@debian:~$ sudo apt update
[sudo]mot de passe de administrateur :
```

Modifier le positionnement géographique de son serveur.

Lors de l'installation, nous avons choisi l'emplacement « Océan Indien / Ile de la Réunion ». Comment peut-on modifier ces paramètres après l'installation ? Déclarons notre serveur comme étant maintenant à Paris :

```
administrateur@debian:~$ sudo dpkg-reconfigure tzdata
```

On choisit alors l'Europe puis Paris. Vous remarquerez que le système vous indique désormais la nouvelle heure locale :

```
Current default time zone : 'Europe/Paris'
Local time is now : 15 :38 :00 CEST 2023.
Universal Time is now : 13 :38 :00 UTC 2023.
```

Se connecter à travers un proxy

Nous n'avons pas déclaré de proxy lors de l'installation, mais il se peut que vous deviez déplacer votre serveur et qu'il doive alors utiliser un proxy authentifiant pour accéder à internet, télécharger des paquets ou des mises-à-jour.

Nous allons voir comment procéder :

De façon pérenne, on peut déclarer un proxy pour apt en modifiant le fichier apt.conf :

```
administrateur@debian:~$ sudo nano /etc/apt/apt.conf.d/apt.conf
```

Ajouter :

```
Acquire::http::proxy "<protocole>://<user>:<motdepasse>@<adresse-proxy>:port>/";
Acquire::https::proxy "<protocole>://<user>:<motdepasse>@<adresse-proxy>:port>/";
Acquire::ftp::proxy "<protocole>://<user>:<motdepasse>@<adresse-proxy>:port>/";
```

Enregistrer le fichier (<CTL+X> puis Y (ou O))

Déclarer un proxy pour wget (accès à Internet)

Pour cela il suffit de modifier le fichier /etc/wgetrc

Trouvez les lignes :

```
#https_proxy = ...
#http_proxy = ...
#ftp_proxy = ...
```

Retirez le # (pour les décommenter) et adaptez les à votre situation (sans oublier le / final) :

<protocoleduproxy>://<user>:<motdepasse>@<adresse du proxy> :<port>/

Autoriser la connexion distante via openssh

Il suffit d'installer le paquet server d'openssh :

```
administrateur@debian:~$ sudo apt install openssh-server
```

Pour tester la connexion distante :

Trouvez l'adresse ip de votre serveur debian avec ip a, puis utilisez une autre machine et lancez :

```
ssh administrateur@ipduserveurdebian
```

À l'invite, entrez le mot de passe du compte administrateur. Vous devrez maintenant être connecté à distance à votre serveur.

Modifier la configuration IP

La configuration IP de la machine Debian est détaillée dans le fichier /etc/network/interfaces

Après modification de ce fichier, il faut relancer le service réseau pour appliquer les modifications apportées :

```
administrateur@debian:~$ sudo systemctl restart networking
```

Regardons le contenu du fichier interfaces :

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet dhcp
# This is an autoconfigured IPv6 interface
iface enp0s3 inet6 auto
```

On peut voir que notre machine ne possède qu'un seul adaptateur réseau nommé enp0s3 et que ce dernier est automatiquement configuré par DHCP (instructions inet dhcp). Il reçoit une configuration IPv4 et une configuration IPv6. On peut noter aussi que l'adaptateur lo (le loopback) est déclaré et configrué (instruction inet loopback).

Modifions la configuration de notre interface enp0s3 pour lui attribuer :

L'adresse 10.10.0.200/24, 10.10.0.254 comme passerelle par défaut, 10.30.0.1 et 9.9.9.9 comme sevrerus DNS et btssio.lan comme domaine par défaut :

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
#iface enp0s3 inet dhcp
iface enp0s3 inet static
        address 10.10.0.200/24
        gateway 10.0.0.254
        dns-nameservers 10.30.0.1 9.9.9.9
        dns-domain btssio.lan

# This is an autoconfigured IPv6 interface
iface enp0s3 inet6 auto
```

Il faut ensuite relancer (restart) le service networking pour appliquer les changements... Attention, si vous êtes connecté à distance à travers ssh, vous allez perdre votre connexion.

Notez que vous pouvez aussi déclarer l'adresse et le masque de la façon suivante :

```
        address 10.10.0.200
        netmask 255.255.255.0
```

Vous pouvez aussi spécifier l'adresse de diffusion du réseau :

```
        broadcast 10.10.0.255
```

NB : Vous pouvez désactiver et activer une interface réseau de la sorte :

```
administrateur@debian:~$ sudo ifdown enp0s3
administrateur@debian:~$ sudo ifup enp0s3
```

Contrôler les entrées/sortie à l'aide d'un firewall simplifié (ufw)

Afin de mieux contrôler la sécurité de notre serveur, nous allons installer ufw (Uncomplicated FireWall), un coupe-feu simple qui va nous permettre de définir ce que nous laissons entrer.

Il faut commencer par installer ufw :

```
administrateur@debian:~$ sudo apt install ufw
```

Une fois installé, regardons son statut :

```
administrateur@debian:~$ sudo systemctl status ufw
○ ufw.service - Uncomplicated firewall
     Loaded: loaded (/lib/systemd/system/ufw.service; enabled; preset: enabled)
     Active: inactive (dead)
       Docs: man:ufw(8)
```

On voit que le service est « enabled » mais « inactive » : par défaut le service sera chargé à chaque démarrage de la machine (enabled) mais il n'a pas encore été activé.

On peut aussi regarder son statut en lançant la commande « sudo ufw status » mais le résultat est moins complet :

```
administrateur@debian:~$ sudo ufw status verbose
Status: inactive
administrateur@debian:~$
```

Ufw connaît déjà un certain nombre de ports par défaut qui sont réservés pour des protocoles connus. On peut par exemple dire que le port 22 est le port d'écoute du serveur ssh. Si on souhaite interdire ou autoriser les connexions ssh à notre serveur, il faudra donc définir une règle pour le port 22 ou pour SSH.

Pour obtenir la liste des « protocoles connus », il suffit de lancer :

```
administrateur@debian:~$ sudo ufw app list
```

<u>Comment définir une règle simple pour ufw ?</u>

La définition d'une règle entrante se fait avec la commande :

ufw [allow/deny/reject] [port/app nam] [incoming/outgoing]

> Allow autorise le traffic, deny l'interdit et reject l'interdit également mais il retourne un message « Destination host unreachable ».
>
> On peut définir le port concerné ou le protocole s'il utilise le port par défaut : exemple 22 ou SSH
>
> On peut aussi définir si la règle s'applique au trafic entrant ou sortant.

On va définir une politique par défaut : on souhaite interdire le trafic entrant et autoriser le trafic sortant :

```
administrateur@debian:~$ sudo ufw default deny incoming
administrateur@debian:~$ sudo ufw default allow outgoing
```

Ces règles par défaut sont une base de départ mais ne conviennent pas à un serveur qui doit pouvoir laisser entrer des requêtes pour les services qu'il propose. Attention, pensez à autoriser les connexion entrantes ssh si vous travaillez sur votre serveur à distance :

```
administrateur@debian:~$ sudo ufw allow SSH
```

Puis activez votre service :

```
administrateur@debian:~$ sudo ufw enable
```

Regardez maintenant le statut d'ufw :

```
administrateur@debian:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)
```

Ajoutons une règle pour autoriser le trafic entrant sur le protocole HTTP (si le serveur debian est serveur web notamment) :

```
administrateur@debian:~$ sudo ufw allow WWW
administrateur@debian:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
WWW                        ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)
WWW (v6)                   ALLOW       Anywhere (v6)
```

Comment retirer cette règle ?

On peut retirer une règle en faisant ainsi :

```
administrateur@debian:~$ sudo ufw delete allow WWW
Rule deleted
Rule deleted (v6)
```

La règle a bien été retirée :

```
administrateur@debian:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)
```

Pour finir avec ufw, on peut l'arrêter avec la commande ufw disable (il sera inactif au prochain lancement de la machine). On peut aussi remettre à 0 toutes les règles avec ufw reset.

Pour plus de détails et des règles plus complètes : lire