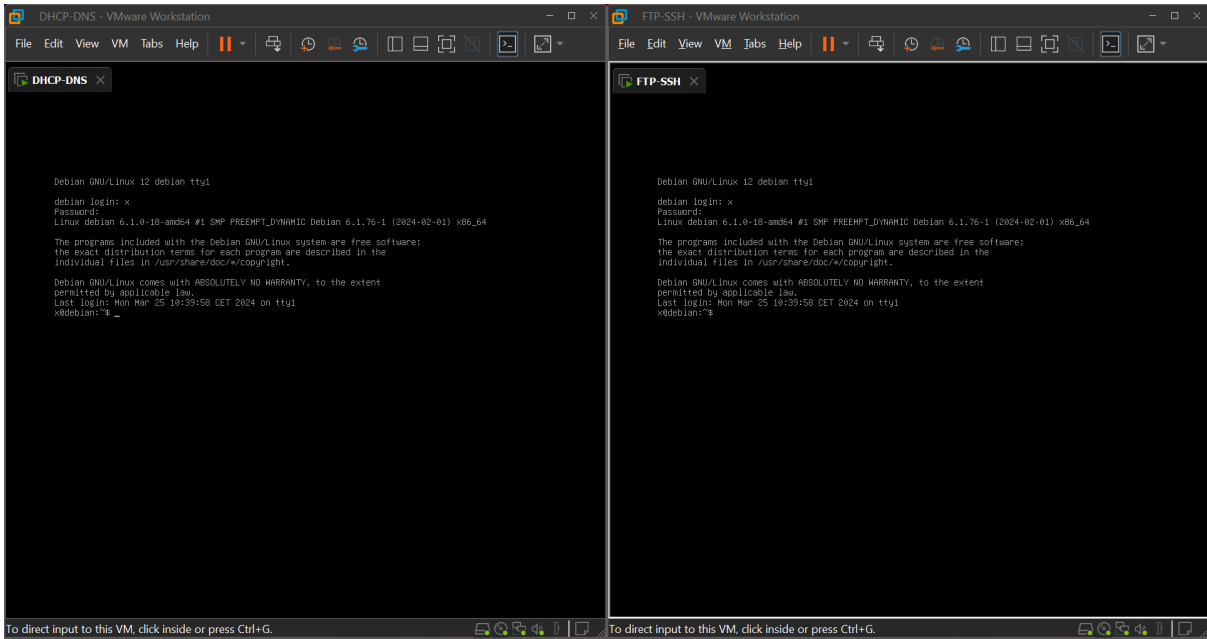


# FTP-DNS-DHCP-SSH

Compte root = mdp admin

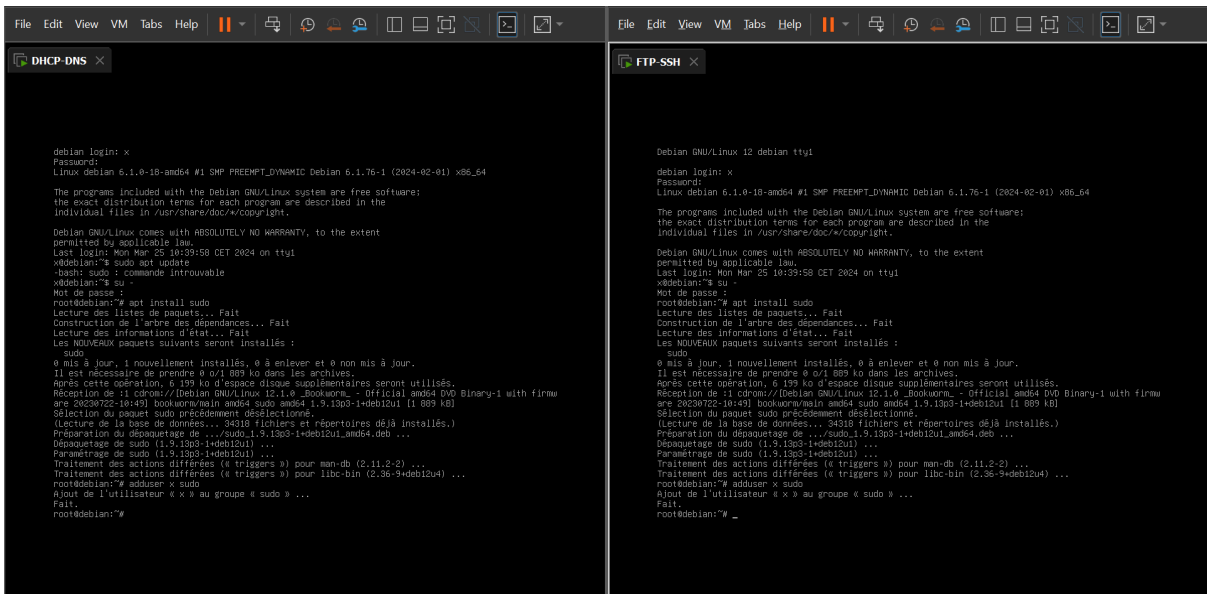
Compte x = mdp x

## 1.Création des VM's et MAJ des celles-ci !



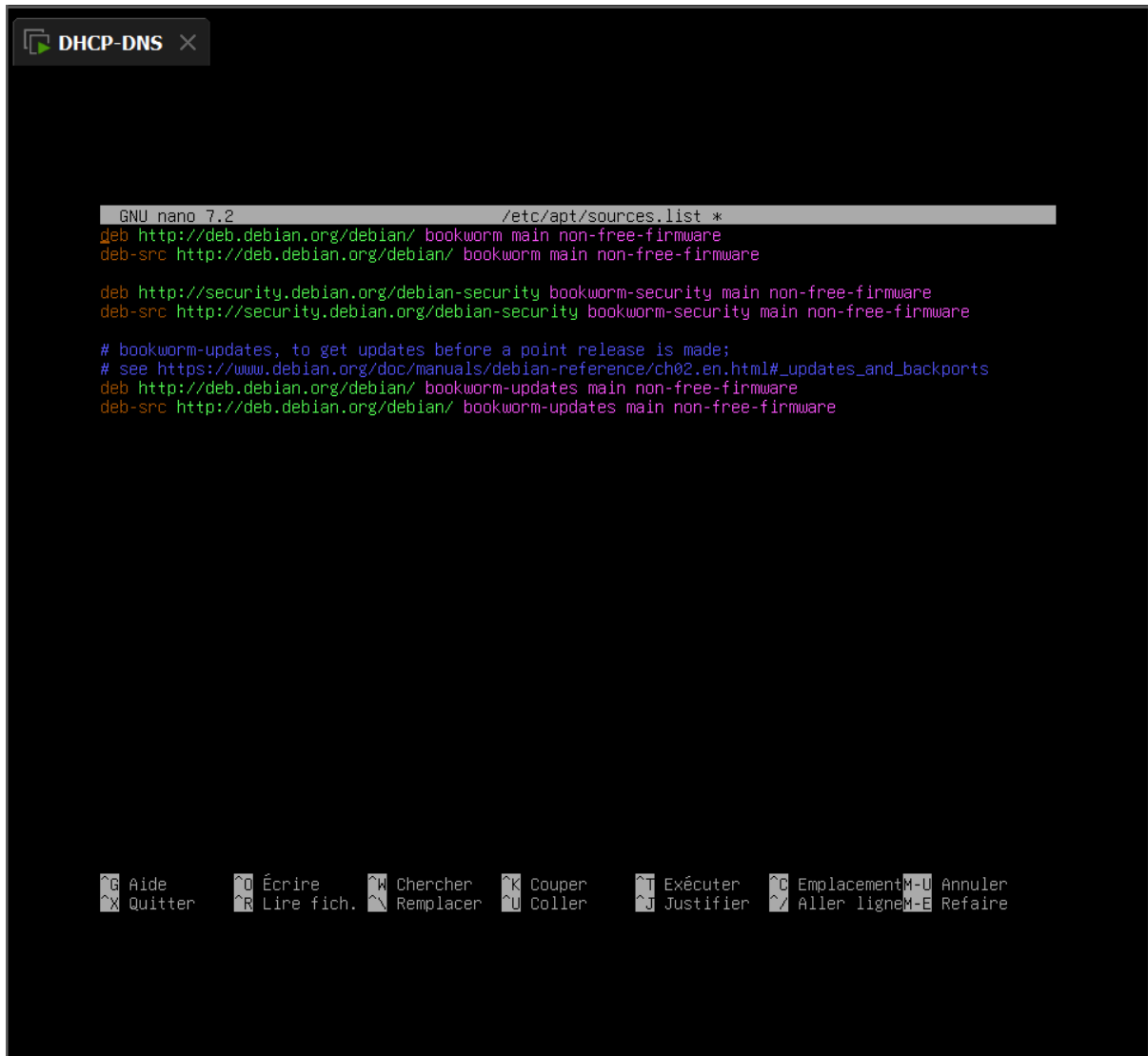
## 1ere Problématique : Mais où est le sudo ?

Ce sont des vm sans interface graphique. De ce fait, il n'y à pas de fonctionnalités de super utilisateur. On se connecte donc au root, puis apt install sudo et ajout de l'utilisateur au groupe sudo.



## 2eme Problématique : Le fichiers source d'APT

Afin de réaliser les mises à jour sur nos deux machines nous devons modifier le fichier, sources.list afin d'aller chercher les paquets sur internet et non plus sur notre image disque.



```
GNU nano 7.2 /etc/apt/sources.list *
deb http://deb.debian.org/debian/ bookworm main non-free-firmware
deb-src http://deb.debian.org/debian/ bookworm main non-free-firmware

deb http://security.debian.org/debian-security bookworm-security main non-free-firmware
deb-src http://security.debian.org/debian-security bookworm-security main non-free-firmware

# bookworm-updates, to get updates before a point release is made:
# see https://www.debian.org/doc/manuals/debian-reference/ch02.en.html#updates_and_backports
deb http://deb.debian.org/debian/ bookworm-updates main non-free-firmware
deb-src http://deb.debian.org/debian/ bookworm-updates main non-free-firmware

^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement ^U Annuler
^X Quitter   ^R Lire fich.^M Remplacer  ^U Coller    ^J Justifier ^_ Aller ligne ^-E Refaire
```

et un `sudo apt update` pour voir si des maj sont disponibles

```
x@debian:~$ sudo apt update
Atteint :1 http://security.debian.org/debian-security bookworm-security InRelease
Atteint :2 http://deb.debian.org/debian bookworm InRelease
Atteint :3 http://deb.debian.org/debian bookworm-updates InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
x@debian:~$
```

## 2. Téléchargements des paquets pour chaque machine / Installation des différents serveurs sur les 2 VM

### Machine Virtuelle N°1

Installation des paquets pour le service DHCP

Tuto : <https://www.linuxtricks.fr/wiki/debian-installer-un-serveur-dhcp>

Je tape la commande : `sudo apt install isc-dhcp-server`

Lors de l'exécution de cette commande, le terminal me retourne une erreur qui correspond au fait que le service a bien été téléchargé, mais la tentative de démarrage du service a échoué ce qui est normal puisqu'il va falloir le configurer.

Installation des paquets bind9 pour le service DNS

Tuto : <https://debian-facile.org/atelier:chantier.dns-bind9-sur-wheezy>

Je tape la commande : `sudo apt install bind9`

### Machine Virtuelle N°2

Installation des paquets pour le serveur FTP

Tuto : <https://www.informatiweb-pro.net/admin-systeme/linux/debian-ubuntu-installer-un-serveur-ftp.html>

Je tape la commande : `sudo apt install proftpd`

Pour les service SSH

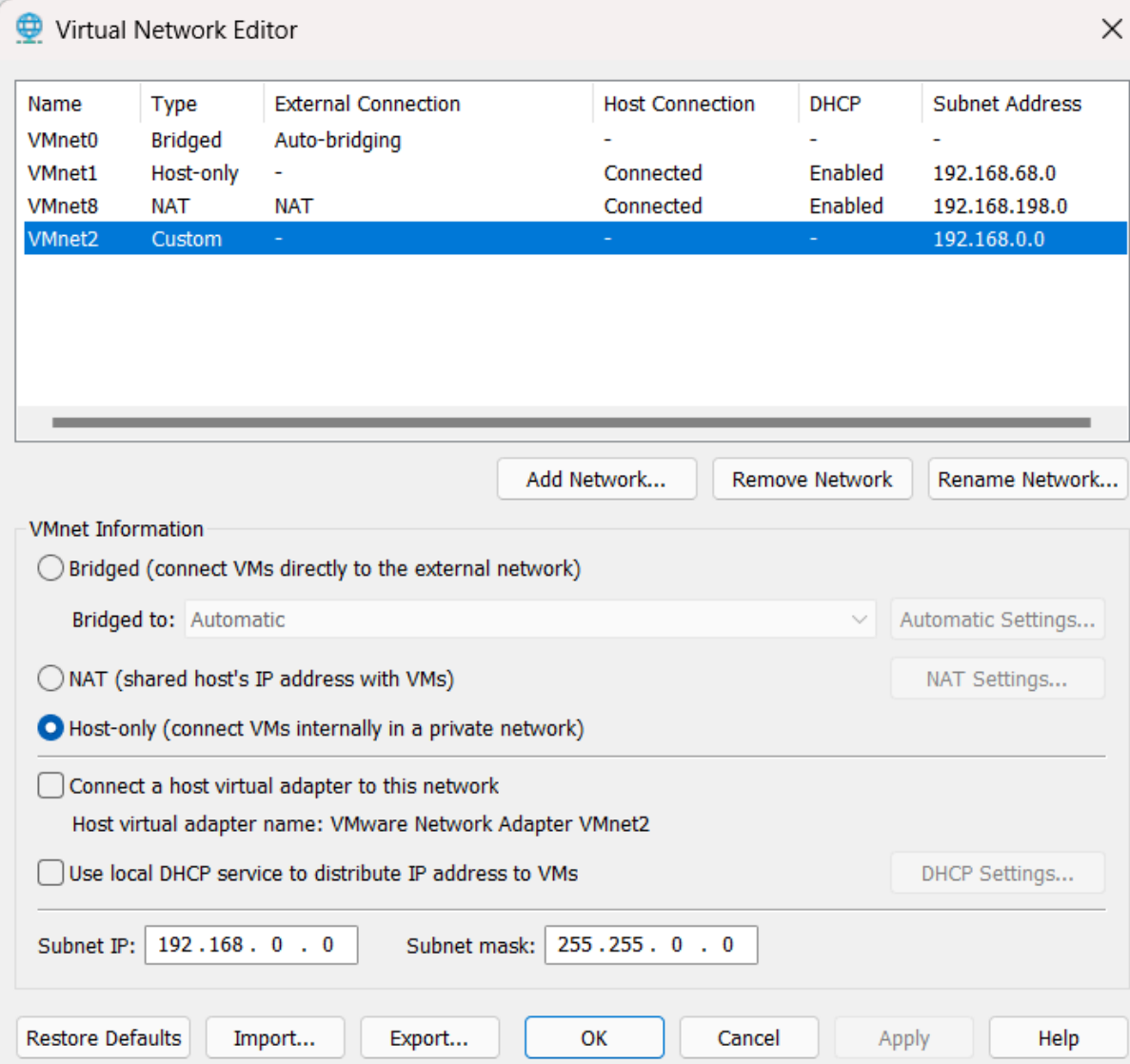
Il est installé de base sur les machines debian nous pouvons vérifier la présence du service en tapant la commande : `sudo systemctl status ssh`

Si le service n'est pas installé il suffit de taper : `sudo apt install openssh-server`

**Nous pouvons dès maintenant éteindre nos VM de manière à les déconnecter du réseau de la plateforme.**

## 2 Bis.Création du reseau privé

Etape 1 : Créer la nouvelle carte réseau dans VMware



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.68.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.198.0
VMnet2	Custom	-	-	-	192.168.0.0

Add Network... Remove Network Rename Network...

VMnet Information

☐ Bridged (connect VMs directly to the external network)

Bridged to: Automatic Automatic Settings...

☐ NAT (shared host's IP address with VMs) NAT Settings...

☒ Host-only (connect VMs internally in a private network)

☐ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet2

☐ Use local DHCP service to distribute IP address to VMs DHCP Settings...

Subnet IP: 192 . 168 . 0 . 0 Subnet mask: 255 . 255 . 0 . 0

Restore Defaults Import... Export... OK Cancel Apply Help

**Etape 2 :** Modification des cartes réseau des VM

DHCP-DNS

Power on this virtual machine

Edit virtual machine settings

▼ Devices

Memory4 GB

Processors2

Hard Disk (SCSI)50 GB

CD/DVD (IDE)Using file D:\For...

Network AdapterCustom (VMnet2)

USB ControllerPresent

Sound CardAuto detect

DisplayAuto detect

▼ Description

Type here to enter a description of this virtual machine.

▼ Virtual Machine Details

State: Powered off

Snapshot: Machine Vierge

Configuration file: D:\Machine

Virtual\DHCP... \DHCP-DNS.vmx

Hardware compatibility: Workstation 17.5.x virtual machine

Primary IP address: Network information is not available

FTP-SSH

Power on this virtual machine

Edit virtual machine settings

▼ Devices

Memory4 GB

Processors2

Hard Disk (SCSI)50 GB

CD/DVD (IDE)Using file D:\For...

Network AdapterCustom (VMnet2)

USB ControllerPresent

Sound CardAuto detect

DisplayAuto detect

▼ Description

Type here to enter a description of this virtual machine.

▼ Virtual Machine Details

State: Powered off

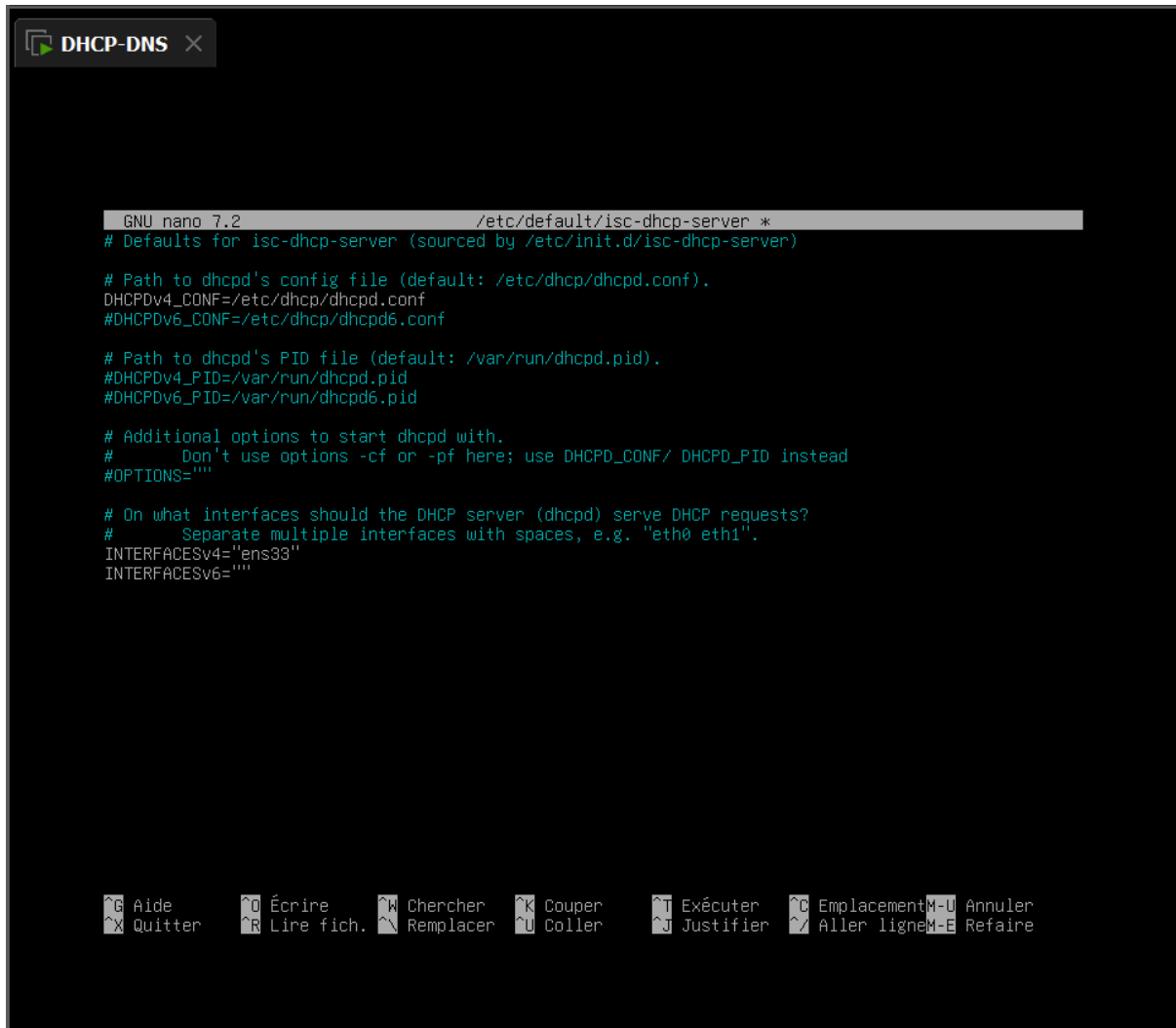
Configuration file: D:\Machine

Virtual\FTP-SSH\FTP-SSH.vmx

Hardware compatibility: Workstation 17.5.x virtual machine

Primary IP address: Network information is not available

### 3. Configuration du serveur DHCP



```
GNU nano 7.2 /etc/default/isc-dhcp-server *
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="ens33"
INTERFACESv6=""

^G Aide      ^O Écrire   ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement ^M-U Annuler
^X Quitter   ^R Lire fich. ^N Remplacer ^U Coller    ^J Justifier ^_ Aller ligne ^M-E Refaire
```

- Première ligne du fichier mis en commentaire
- Ajout du nom de la carte réseau à l'interface v4 (récupéré via "ip a")

## Contenue du fichier /etc/network/interfaces

```
GNU nano 7.2 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 ens33
iface ens33 inet static
# le static dit qu'on attribue une ip fixe_

address 192.168.0.1/16
# /16 car c'est une adress de classe B
# Sinon il faut marque netmask 255.255.0.0

^G Aide      ^O Écrire
^X Quitter   ^R Lire fich.
^W Chercher  ^K Couper
^_ Remplacer ^U Coller
^T Exécuter  ^C Emplacement
^J Justifier ^_ Aller ligne
^M-U Annuler
^M-E Refaire
```

On relance le service networking : `sudo service networking restart`

Contenue du fichier /etc/dhcp/dhcpd.conf

Tuto: <https://www.linuxtricks.fr/wiki/dhcp-sous-linux-le-fichier-de-configuration-dhcpd-conf>

```
GNU nano 7.2 /etc/dhcp/dhcpd.conf *
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# option definitions common to all supported networks...
option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;

# Bail par défaut (10h)
default-lease-time 36000;
# Bail max (20h)
max-lease-time 72000;
# Déclaration d'un réseau
subnet 192.168.0.0 netmask 255.255.0.0 {
    range                192.168.0.2 192.168.0.5;
    option domain-name-servers 192.168.0.254;
    option routers         192.168.0.1;
}

# The ddns-updates-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
#authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).

^G Aide      ^O Écrire   ^W Chercher  ^K Couper    ^T Exécuter  ^C EmplacementM-U Annuler
^X Quitter   ^R Lire fich.^N Remplacer ^U Coller    ^J Justifier ^_ Aller ligneM-E Refaire
```

Attention à ne pas oublier les “;” lors de l’édition de ce fichier. De plus les bail sont toujours donnés en seconde par exemple 3600s = 1heure.

Ensuite on redémarre le service DHCP : `sudo systemctl start isc-dhcp-server`



## 4. Configuration du serveur FTP

Modification du fichier /etc/proftpd/proftpd.conf

- désactive les adresses ipv6

```
# Set off to disable IPv6 support which is annoying on IPv4 only boxes.
UseIPv6 off
# If set on, you can experience a longer connection delay in many cases
```

- désactive les liens symboliques ( équivalent raccourcis windows )

```
# Disable MultilineRFC2228 per https://github.com/proftpd/proftpd/issues/1085
# MultilineRFC2228on
DefaultServer on
ShowSymlinks off
```

- Empêche les utilisateurs de remonter dans les fichiers systèmes
- Par défaut un utilisateur linux sur la machine hébergeant le serveur est un utilisateur FTP

```
# Use this to jail all users in their homes
DefaultRoot ~

# Users require a valid shell listed in /etc/shells to login.
# Use this directive to release that constrain.
RequireValidShell on
```

```
# Port 21 is the standard FTP port.
Port 21

# In some cases you have to specify passive ports range to by-pass
# firewall limitations. Ephemeral ports can be used for that, but
# feel free to use a more narrow range.
PassivePorts 49152 65534
```

- L'exercice demandait qu'une seule connexion soit possible

```
# To prevent DoS attacks, set the maximum number of child processes
# to 30. If you need to allow more than 30 concurrent connections
# at once, simply increase this value. Note that this ONLY works
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd)
MaxInstances 1
```

- Ajout d'option pour le confort du transfert des données

```
# Umask 022 is a good standard umask to prevent new files and dirs
# (second parm) from being group and world writable.
Umask 022 022
# Normally, we want files to be overwriteable.
AllowOverwrite on
# Autorise la reprise d'un envoi
AllowStoreRestart On
# Autorise la reprise d'un téléchargement
AllowRetrieveRestart On
```

Puis on redémarre le service : `sudo /etc/init.d/proftpd restart`

**Attention au sudo sinon erreur**

```
x@debian:~$ /etc/init.d/proftpd restart
Restarting proftpd (via systemctl): proftpd.serviceFailed to restart proftpd.service: Access denied
See system logs and 'systemctl status proftpd.service' for details.
failed!
x@debian:~$ sudo /etc/init.d/proftpd restart
Restarting proftpd (via systemctl): proftpd.service.
x@debian:~$ _
```

## 4 Bis. Test de Connexion au serveur FTP/SSH

Afin de tester la connexion a mon serveur FTP, il faut que j'installe le paquet FTP sur la première machine.

**Problématique : Mes machines sont dans un réseau privé donc plus connecté à internet !**

**Solution :**

- Modifier le fichier /etc/network/interfaces

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

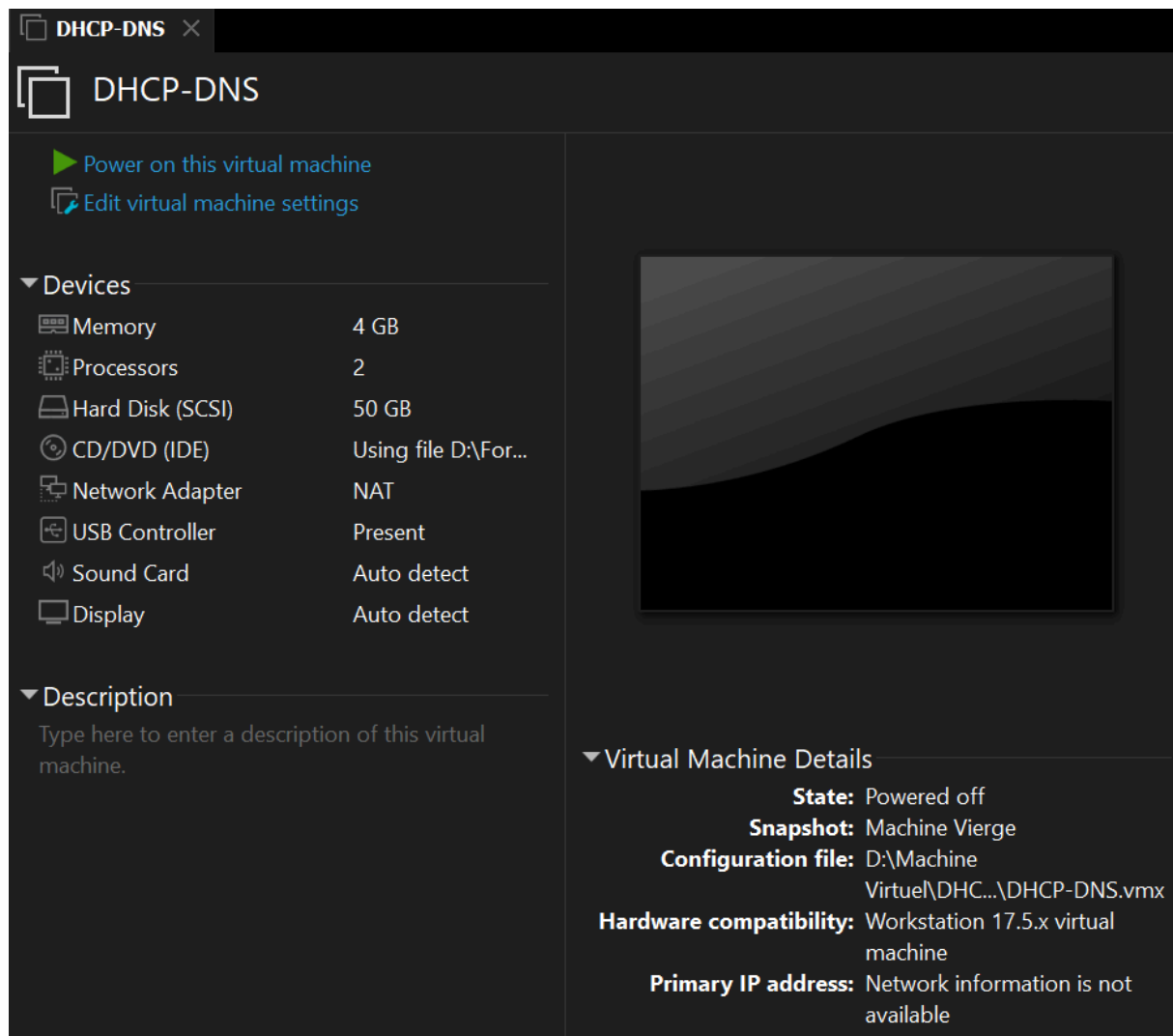
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet dhcp
# le static dit qu'on attribue une ip fixe

# address 192.168.0.1/16
# /16 car c'est une adress de classe B
# Sinon il faut marque netmask 255.255.0.0
```

- Remettre la carte réseau en NAT



- Pour finir on télécharge le paquet ftp sudo apt install ftp.
- Et on configure la machine comme dans le chapitre 4.
- **Surtout pensez à redémarrer le service DHCP !!!!**

Via la commande `ssh laplateforme@192.168.02` j'ai pu m'assurer de la bonne installation du serveur ssh sur ma vm FTP, ainsi que le bon fonctionnement du canal SSH.

## 5. Configuration du serveur DNS

On commence par attribuer une adresse fixe à mon serveur FTP.

J'en ai profité pour modifier la plage d'adresse que mon DHCP peut donner selon les conseils de Thierry et ce qui le fait le plus en entreprise.

```
GNU nano 7.2 /etc/dhcp/dhcpd.conf
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# option definitions common to all supported networks...
option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;

# Bail par défaut (10H)
default-lease-time 36000;
# Bail max (20h)
max-lease-time 72000;
# Déclaration d'un réseau
subnet 192.168.0.0 netmask 255.255.0.0 {
    range 192.168.0.100 192.168.0.150;
    option domain-name-servers 192.168.0.1;
    option routers 192.168.0.1;
    # Reservation d'une adresse ip pour le serveur FTP
    host serveur-ftp {
        hardware ethernet 00:0c:29:22:26:b4;
        fixed-address 192.168.0.2;
    }
}
```

On tape `sudo systemctl restart isc-dhcp-server` pour redémarrer le serveur DHCP

Puis on restart le networking sur le serveur FTP pour avoir l'adresse ip attribuée :

- `sudo service networking stop`
- `sudo service networking start`

On créer la zone FTP

```
GNU nano 7.2 /etc/bind/named.conf.local *
//
// Do any local configuration here
//
zone "ftp.com" {
    type master;
    file "/etc/bind/db.ftp.com";
};

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
```

On copie le fichier de base pour configurer la zone :

- `sudo cp /etc/bind/db.local /etc/bind/db.ftp.com`

Puis on edite le fichier creer :

- `sudo nano /etc/bind/db.ftp.com`

```
GNU nano 7.2 /etc/bind/db.ftp.com
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      debian. root.localhost. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200; Expire
                        604800 )      ; Negative Cache TTL
;
@         IN      NS       debian.
debian    IN      A        192.168.0.1
dns       IN      A        192.168.0.2
```

Redémarrage de bind : `sudo systemctl restart bind9`

## **ATTENTION**

```
GNU nano 7.2 /etc/bind/named.conf.local *
//
// Do any local configuration here
//

zone "ftp.com" {
    type master;
    file "/etc/bind/db.ftp.com";
};

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
```

J'avais oublié le point virgule ce qui m'empêchait de restart le service bind9.

En tapant : `sudo journalctl -xeu named.service |more`

Puis en utilisant la flèches il était marqué qu'une erreur se produisait dans la lecture du fichier `/etc/bind/named.conf.local` à la ligne 12.

**Lorsque je tente de ping mon nom de domaine cela ne marche pas  
!!!**

### SOLUTION

- Corriger le fichier config dhcp

```
option domain-name-servers    192.168.0.1;  
option routers                192.168.0.1;
```

- Changer l'adresse du domaine du serveur dhcp de 192.168.0.254 à 192.168.0.1.
- Change cette même adresse dans le fichier /etc/resolv.conf

## 6. Test de connexion au serveur FTP

### 1. Test de la connexion en ftp :

```
x@debian:~$ ftp dns.ftp.com  
Connected to dns.ftp.com.  
220 ProFTPD Server (Debian) [192.168.0.2]  
Name (dns.ftp.com:x): laplateforme  
331 Mot de passe requis pour laplateforme  
Password:  
230 Utilisateur laplateforme authentifié  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

La connexion FTP est établie avec succès !!!!!

### 2. Test de la connexion en SFTP

```
x@debian:~$ ssh laplateforme@dns.ftp.com  
laplateforme@dns.ftp.com's password:  
Linux debian 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x86_64  
  
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: Wed Mar 27 12:14:10 2024  
laplateforme@debian:~$
```

La connexion SFTP est établie avec succès !!!!!

## 7. Paramètres de Sécurité Additionnels :

Afin de renforcer la sécurité du serveur SFTP :

```
sudo nano /etc/proftpd/proftpd.conf
```

- Restreignez l'accès au serveur uniquement avec les identifiants fournis.

**1ere étape :** Récupération de l'UID et du GID de l'utilisateur

```
laplateforme@debian:/etc/proftpd$ id laplateforme
uid=1000(laplateforme) gid=1000(laplateforme) groupes=1000(laplateforme),27(sudo)
laplateforme@debian:/etc/proftpd$
```

**2eme étape :** Création du fichier password

```
sudo ftpasswd --passwd --name=laplateforme --uid=1000 --gid=1000
--home=/home/laplateforme --shell=/bin/bash
```

```
laplateforme@debian:/etc/proftpd$ sudo ftpasswd --passwd --name=laplateforme --uid=1000 --gid=1000 -
-home=/home/laplateforme --shell=/bin/bash
ftpasswd: creating passwd entry for user laplateforme

Password:
Re-type password:

Passwords do not match. Please try again.

Password:
Re-type password:

ftpasswd: entry created
```

**3eme étape :** Configuration du serveur pour utiliser le fichier mot de passe

```
# Activez l'authentification basée sur les utilisateurs
AuthUserFile /etc/proftpd/ftpd.passwd
```

- Configurez le serveur pour fonctionner sur le port 6500.

```
# Port 21 is the standard FTP port.
# Port 6500 à la demande de l'exercice
Port 6500
```

Désormais il faut se connecter en ftp via la commande `ftp dns.ftp.com -P 6500`  
l'option -P permet de spécifier le port

- Évitez toute connexion anonyme ou invitée sur le serveur.

```
# Users require a valid shell listed in /etc/shells to login.
# Use this directive to release that constrain.
# Desactive l'accès Anonyme_
RequireValidShell on
```