

# DHCP, DNS, FTP et SSH



Un projet de :

Jordan

Youcef

Lucas

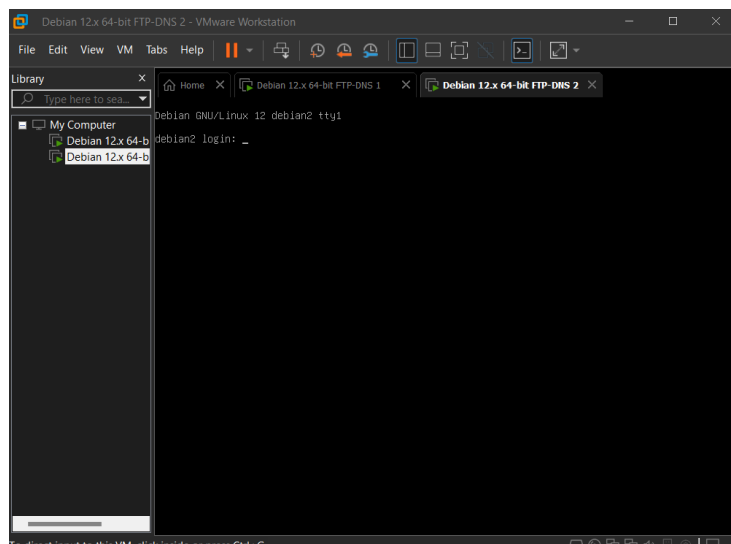
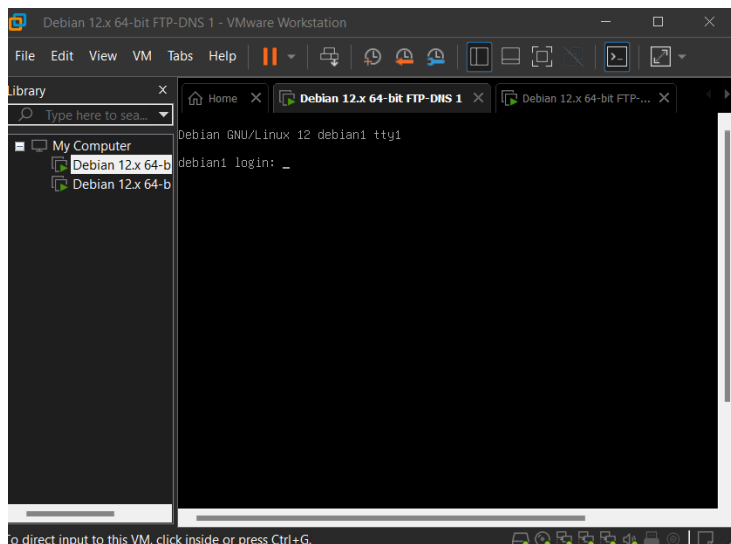


## ETAPES A SUIVRE :

### 1. Installation de Debian sans interface graphique :

On commence par l'installation de nos deux machines virtuelles Debian sans interface graphique :

Une fois l'installation terminée on a nos deux machines qui ressemblent à ceci :



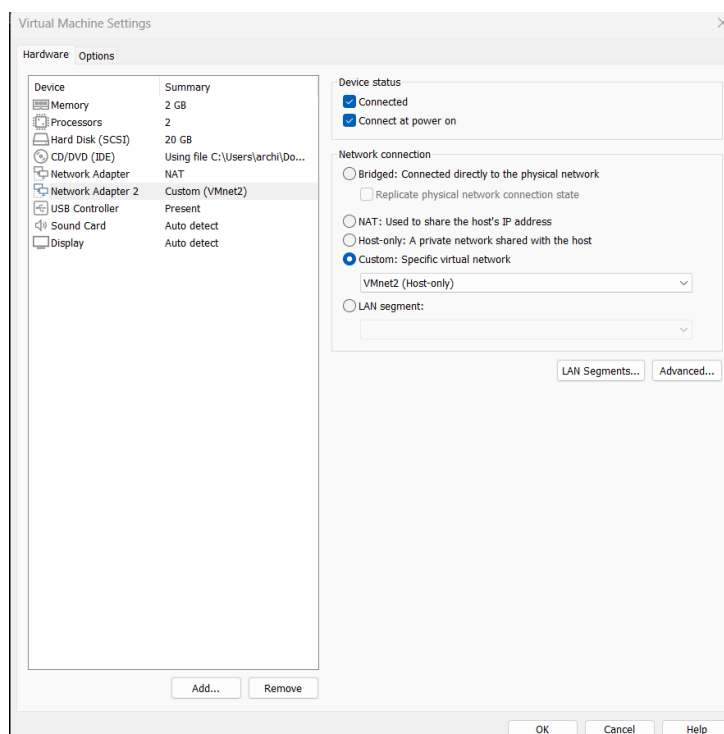
### 2. Mise à jour des systèmes :

Pour appliquer les mises à jour nécessaires sur les deux machines.

On utilise simplement les commandes « **sudo apt update** » et « **sudo apt upgrade** ». Après avoir mis à jour les paquets installés, il est recommandé de mettre à jour le système d'exploitation Debian lui-même on utilise alors la commande « **sudo apt dist-upgrade** ».

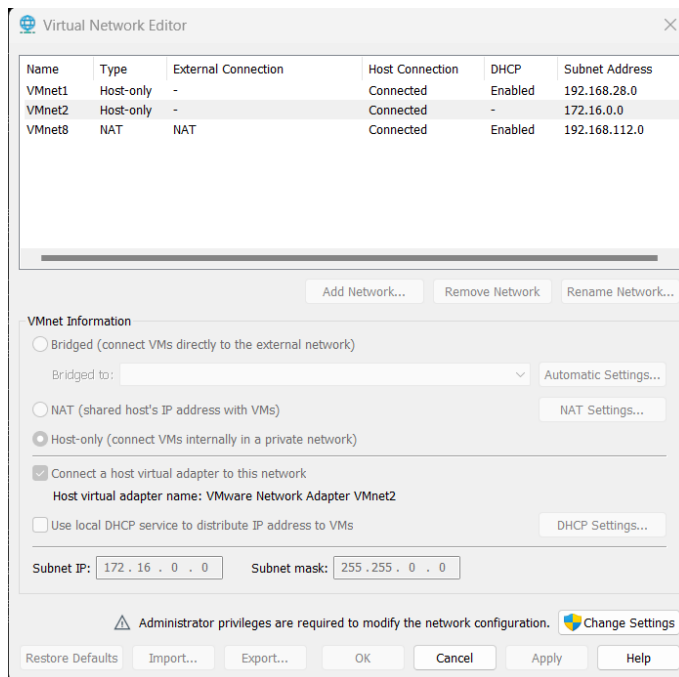
### 3-Configuration du Serveur DHCP :

Pour l'installation du serveur DHCP on a décidé d'ajouter une nouvelle carte réseau.





Ensuite on se rend dans « **Edit** » puis on va dans « **Virtual Network Editor** »



On retire le fait d'utiliser le DHCP local et on modifie le sub net IP pour le passer en classe B .

Par la suite avant toutes choses on regarde notre environnement réseau en tapant « **ip addr** » ou bien il y'a « **ip route | grep default** »

```
youcef1@debian1:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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 noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:28:de:ae brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 172.16.0.13/16 brd 172.16.255.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet 192.168.112.138/24 brd 192.168.112.255 scope global dynamic ens33
        valid_lft 1110sec preferred_lft 1110sec
    inet6 fe80::20c:29ff:fe28:deae/64 scope link
        valid_lft forever preferred_lft forever
```

-On se rend sur le fichier interfaces à l'aide de la ligne de commande suivante :

```
GNU nano 7.2 /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 static
#    address 172.18.0.2
#    netmask 255.255.0.0
#    gateway 192.168.229.2

allow-hotplug ens33
iface ens33 inet dhcp
```



« **sudo nano /etc/network/interfaces** » et on y ajoute ceci :

Maintenant on passe à l'installation et la configuration du DHCP en utilisant la commande :

« **sudo apt install isc-dhcp-server** »

Une fois que c'est fait on se rend dans « **isc-dhcp-server** » à l'aide de la ligne de commande suivante :

« **sudo nano /etc/default/isc-dhcp-server** » et on ajoute dans l'interface v4 notre « **ens** »

```
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="ens36"
INTERFACESv6=""
```

Ensuite on se rend dans le fichier « **dhcpd.conf** » avec les commandes suivantes :

« **sudo nano /etc/dhcp/dhcpd.conf** »

```
GNU nano 7.2 /etc/dhcp/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;

default-lease-time 600;
max-lease-time 7200;

# 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).
log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.
#
# This is a very basic subnet declaration.
#
#subnet 10.152.187.0 netmask 255.255.255.0 {
#}

# This is a very basic subnet declaration.
#
#subnet 10.254.239.0 netmask 255.255.255.224 {
#}

GNU nano 7.2 /etc/dhcp/dhcpd.conf
#class 'foo' {
# match if substring (option vendor-class-identifier, 0, 4) = "SUNW";
#}

#shared-network 224-29 {
# subnet 10.17.224.0 netmask 255.255.255.0 {
# option routers rtr-224.example.org;
# }
# subnet 10.0.29.0 netmask 255.255.255.0 {
# option routers rtr-29.example.org;
# }
# pool {
# allow members of "foo";
# range 10.17.224.10 10.17.224.250;
# }
# pool {
# deny members of "foo";
# range 10.0.29.10 10.0.29.230;
# }
#}

subnet 172.16.0.0 netmask 255.255.0.0 {
range 172.16.0.100 172.16.0.150;
option subnet-mask 255.255.0.0;
option broadcast-address 172.16.255.255;
default-lease-time 600;
max-lease-time 7200;
}

host ftp {
hardware ethernet 00:0c:29:e8:a7:41;
fixed-address 172.16.0.3;
}
```



Une fois dessus on décommente « authoritative » .

**Authoritative** : dans le fichier de configuration dhcpd.conf indique au serveur DHCP qu'il est l'autorité pour le réseau spécifié. Cela signifie que si un client DHCP envoie une demande de configuration d'adresse IP à ce serveur, ce serveur est autorisé à répondre avec une adresse IP et d'autres informations de configuration.

Lorsque cette ligne est commentée (précédée d'un symbole dièse "#"), le serveur DHCP n'est pas considéré comme l'autorité pour le réseau. Cela signifie que s'il reçoit une demande DHCP pour un réseau spécifique pour lequel il est configuré, il transmettra cette demande à un autre serveur DHCP (s'il en existe un) qui est autorisé à répondre pour ce réseau.

Ensuite on ajoute à la fin notre subnet avec l'adresse ip qu'on a configuré juste avant ..

Juste après on retourne sur notre seconde VM et on ajoute dans le fichier « **interface** »

```
GNU nano 7.2 /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

#The secondary network interface
allow-hotplug ens36
iface ens36 inet dhcp
```

[ Lecture de 16 lignes ]

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



### 1. **allow-hotplug** :

- Cette directive permet de gérer dynamiquement l'état de l'interface. Elle indique au système d'activer l'interface lorsqu'elle est branchée et de la désactiver lorsqu'elle est débranchée, sans nécessiter de redémarrage du système. Cela permet une gestion plus flexible des interfaces réseau.

### 2. **iface** :

- Cette directive indique l'interface réseau à configurer, suivie du protocole à utiliser (dans ce cas, **inet** pour les réseaux IPv4).
- La section suivante après **iface** définit la configuration réseau pour l'interface spécifiée.

### 3. **inet dhcp** :

- Cette ligne indique que l'interface doit obtenir sa configuration réseau via DHCP. Cela signifie que l'interface essaiera d'obtenir une adresse IP automatiquement à partir d'un serveur DHCP sur le réseau auquel elle est connectée.

Pour s'assurer que notre DHCP fonctionne on utilise la commande « **sudo systemctl status isc-dhcp-server** »

Entre chaque manipulation il faut s'assurer de restart le dhcp et le network à l'aide des commandes suivantes :

« **sudo systemctl restart isc-dhcp-server** »

« **sudo systemctl restart networking** »

Pour s'assurer que les deux VM puissent communiquer entre elles , il suffisait d'effectuer un ping :

```
youcef2@debian2:~$ sudo systemctl -p
youcef2@debian2:~$ ping 192.168.112.138
PING 192.168.112.138 (192.168.112.138) 56(84) bytes of data.
64 bytes from 192.168.112.138: icmp_seq=1 ttl=64 time=1.48 ms
64 bytes from 192.168.112.138: icmp_seq=2 ttl=64 time=0.912 ms
64 bytes from 192.168.112.138: icmp_seq=3 ttl=64 time=1.13 ms
^C
--- 192.168.112.138 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.912/1.175/1.481/0.234 ms
youcef2@debian2:~$
```



On effectue un ping 8.8.8.8 pour vérifier la connectivité réseau d'une machine à Internet.

```
alrname erp2ss
youcef1@debian1:/etc$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=5.22 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=7.83 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=20.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=8.43 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=128 time=6.59 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=128 time=6.46 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=128 time=6.39 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=128 time=6.76 ms
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7015ms
rtt min/avg/max/mdev = 5.216/8.506/20.370/4.574 ms
youcef1@debian1:/etc$ _
```

Avant de passer à l'installation de FTP , même si c'est sur l'autre machine virtuelle on procède par effectuer un snapshot, ce qui nous permet de sauvegarder notre travail opérationnel et fonctionnel et d'y pouvoir y revenir si besoin .

#### 4. Installation du Serveur FTP :

On commence par installer ftp avec la commande :

« **sudo apt install proftpd** »

Maintenant on créer notre user et on lui définit un mot de passe à l'aide de la commande :

« **sudo add user laplateforme** »

Une fois que l'user créer et l'installation terminé on se rend sur le dossier « **proftpd**» avec la commande suivante :

« **sudo nano /etc/proftpd/proftpd.conf** »



```
GNU nano 7.2 /etc/proftpd/proftpd.conf
MaxClientsPerHost 1 "only one session per host allowed"
<Limit LOGIN>
AllowUser laplateforme
DenyALL
</Limit>
# /etc/proftpd/proftpd.conf -- This is a basic ProFTPD configuration file.
# To really apply changes, reload proftpd after modifications, if
# it runs in daemon mode. It is not required in inetd/xinetd mode.
#
# Includes DSO modules
Include /etc/proftpd/modules.conf
# Set off to disable IPv6 support which is annoying on IPv4 only boxes.
UseIPv6 on
# If set on you can experience a longer connection delay in many cases.
<IfModule mod_ident.c>
    IdentLookups off
</IfModule>
ServerName "Debian"
# Set to inetd only if you would run proftpd by inetd/xinetd/socket.
# Read README.Debian for more information on proper configuration.
ServerType standalone
DeferWelcome off
# Disable MultilineRFC2228 per https://github.com/proftpd/proftpd/issues/1085
# MultilineRFC2228 on
DefaultServer on
ShowSymlinks on
TimeoutNoTransfer 600
TimeoutStalled 600
[ Lecture de 214 lignes ]
^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
```

Une fois dedans on y ajoute le nombre de Client que l'on souhaite et on autorise user »laplateforme » de s'y connecter .

Avant de pouvoir se connecter on récupère notre IP avec la commande : « **hostname -I** »

```
youcef2@debian2:/$ hostname -I
192.168.112.139 172.16.0.3
youcef2@debian2:/$ _
```

Pour se connecter il suffit de taper : « **sftp laplateforme@notre ip** » et d'entrer le mot de passe .

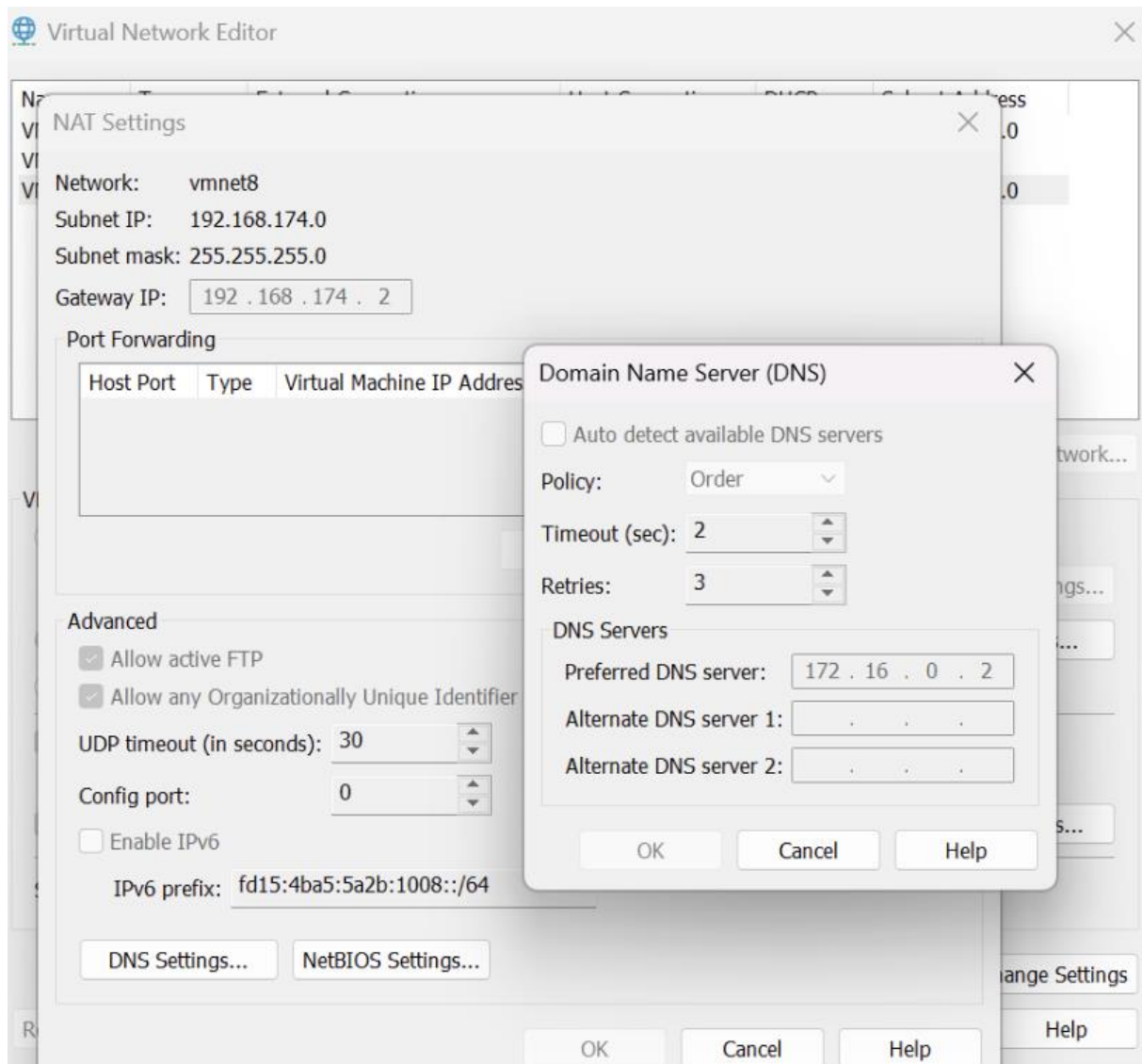
```
192.168.112.139 172.16.0.3
youcef2@debian2:/$ sftp laplateforme@172.16.0.3
laplateforme@172.16.0.3's password:
Connected to 172.16.0.3.
sftp> _
```

## 5. Installation du Serveur DNS :





Sur notre seconde carte réseau , on commence par désactiver la détection automatique des serveurs DNS disponible et on lui définit le serveur DNS préféré en lui donnant l'adresse IP de notre première machine.



« On précise que notre première carte réseau nous sert d'accès à Internet »

Installation du serveur **BIND** sur la première machine :



« **sudo apt install bind9** »

Une fois l'installation terminée, on se rend sur le fichier interfaces :

« **sudo nano /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
    address 192.168.174.10/24
    gateway 192.168.174.2

#secondary network
allow-hotplug ens37
iface ens37 inet static
    address 172.16.0.2
    netmask 255.255.0.0
```

Nous avons décidé de modifier la configuration pour que l'interface réseau soit configurés avec une adresses IP statiques . Cette étape est essentielle pour notre serveur DNS car il a besoin d'une interface réseau avec une adresse IP statique pour être toujours accessible.

Configuration DNS :



On se rend dans le fichier « **named.conf.options** »

**allow-query { any; };** : Cette ligne spécifie que le serveur BIND acceptera les requêtes de résolution DNS de n'importe quelle adresse IP. C'est un paramètre de contrôle d'accès qui détermine qui peut faire des requêtes à votre serveur DNS.

**Forwarders** : utilisé pour définir les serveurs DNS auxquels BIND doit transmettre les requêtes qu'il ne peut pas résoudre avec les données dont il dispose localement. Ici, 8.8.8.8 est l'adresse du serveur DNS de Google, ce qui signifie que toutes les requêtes que le serveur DNS ne peut pas résoudre seront envoyées à ce serveur pour résolution.

```
root@debian1:/# cat /etc/bind/named.conf.options

options {
    directory "/var/cache/bind";
    allow-query { any; };

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        8.8.8.8;
    };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;
    auth-nxdomain no;
    listen-on-v6 { any; };
};
```

Ensuite on se rend sur le « **named.conf.local** »



zone "ftp.com" IN {: indique le chemin vers le fichier sur le serveur DNS qui gère les enregistrements pour le domaine ftp.com. Cette déclaration commence la configuration de la zone pour le domaine ftp.com. IN représente l'Internet class et est souvent utilisé dans les configurations de zone DNS.

type master;; Cela indique que le serveur BIND agit en tant que serveur maître pour la zone ftp.com. Cela signifie qu'il détient le fichier de zone autoritaire, qui contient les enregistrements DNS réels.

file "/etc/bind/db.ftp.com"; Ceci spécifie le chemin vers le fichier de données de la zone pour le domaine ftp.com. Ce fichier doit contenir tous les enregistrements DNS pour le domaine,

Ensemble, cette configuration informe le serveur DNS que pour toute requête liée à ftp.com, il doit consulter le fichier spécifié (/etc/bind/db.ftp.com) pour déterminer comment répondre à la requête

```
root@debian1:/# cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

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

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

//zone "16.172.in-addr.arpa" {
//    type master;
//    file "etc/bind/db.172";
//};
root@debian1:/# cat /etc/bind/named.conf.local
```

Le fichier de zone pour ftp.com définit les paramètres essentiels et les serveurs responsables du domaine. L'enregistrement SOA inclut des informations de contact et des numéros de série pour



suivre les mises à jour. Les intervalles de rafraîchissement et d'expiration dictent quand les serveurs secondaires vérifient et considèrent les données comme obsolètes. Les enregistrements NS et A lient les noms de sous-domaines à des adresses IP spécifiques, dirigeant le trafic vers l'hôte désigné pour le service FTP.

```
root@debian1:/# cat /etc/bind/db.ftp.com
;
; BIND data file for ftp.com
;
$TTL      604800
@         IN      SOA      ftp.com  admin.ftp.com (
                        3      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       ns
ns        IN      A        172.16.0.2
dns       IN      A        172.16.0.3
root@debian1:/#
```

## 6. Test de Connexion au Serveur SFTP :

```
jordan@debian2:/etc/proftpd$ sftp laplateforme@172.16.0.3
The authenticity of host '172.16.0.3 (172.16.0.3)' can't be established.
ED25519 key fingerprint is SHA256:j2xkIV0qAgdA24QJNQURbNO4TeKnyVo0ZYLFDDDe5f8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.16.0.3' (ED25519) to the list of known hosts.
laplateforme@172.16.0.3's password:
Connected to 172.16.0.3.
sftp>
```

## 7. Paramètres de Sécurité Additionnels :

Afin de renforcer la sécurité du serveur SFTP :



Nous avons limité l'accès seulement à l'utilisateur « laplateforme »

```
GNU nano 7.2                                proftpd.conf
MaxClientsPerHost 1 "only one session per host allowed"
<Limit LOGIN>
AllowUser laplateforme
DenyALL
</Limit>
```

« `sudo nano /etc/ssh/sshd_config` » et on enlève le #port 22, on décommente et on écrit Port 6500

Cela nous permet de sécuriser notre connexion, le port 22 étant le port par défaut et pouvant être utilisé comme porte d'entrée par des individus mal intentionnés.

```
GNU nano 7.2                                sshd_config
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 6500
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
[ Lecture de 122 lignes ]
 Aide  Écrire Chercher Couper Exécuter Emplacement Annuler
 Quitter Lire fich. Remplacer Coller Justifier Aller ligne Refaire
```

Ensuite nous utilisons la commande « `sudo lsof -i :6500` » pour être sûr que le port écouté est bien le 6500

```
jordan@debian:/etc/ssh$ sudo lsof -i :6500
COMMAND PID USER  FD  TYPE DEVICE SIZE/OFF NODE NAME
sshd    1129 root   3u   IPv4 25873      0t0  TCP *:6500 (LISTEN)
sshd    1129 root   4u   IPv6 25884      0t0  TCP *:6500 (LISTEN)
```

Nous utilisons maintenant la première machine et nous nous connectons de manière sécurisée à l'adresse dns.ftp.com sur le port 6500.

```
jordan@debian:~$ sftp -oPort=6500 laplateforme@dns.ftp.com
laplateforme@dns.ftp.com's password:
Connected to dns.ftp.com.
sftp> _
```