

DHCP, DNS, FTP et SSH

Kevin NGO
Maxime VALLE

Outils et logiciels utilisés

Nous utiliserons le logiciel **VirtualBox** pour créer nos machines virtuelles et non VMWare car on a eu des problèmes au niveau de la création d'un réseau virtuel. Sur VMWare Étudiant, on ne peut pas créer de réseaux virtuels à part si on a VMWare Pro. Ce qui a été un problème pour pouvoir ping entre les deux machines virtuelles.

N'oublions pas de toujours mettre à jour nos paquets et logiciels :

on doit absolument faire **apt update et upgrade**

Dans ce projet, nous aurons besoin d'installer des paquets pour la création des serveurs :

apt install isc-dhcp-server : C'est le paquet pour installer le serveur DHCP qui permet de fournir automatiquement une adresse ip et d'autres informations de configuration à un autre ordinateur du même réseau.

apt install proftpd ftp : Le serveur FTP, nous allons prendre proftpd qui est proposé par l'exercice, est un serveur qui permet le partage de fichiers dans un réseau.

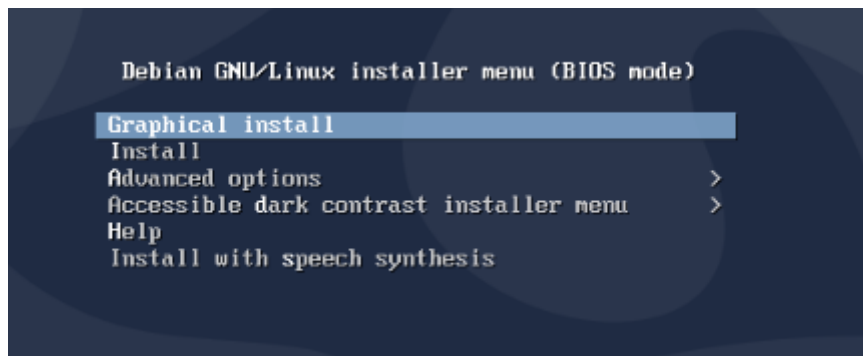
apt install ssh-openserver : Ce paquet permet d'envoyer des commandes en toute sécurité à un ordinateur sur un réseau non sécurisé

apt install bind9 : Celui la sera pour la création d'un serveur DNS, il permet d'associer un nom assez compréhensible à une adresse IP

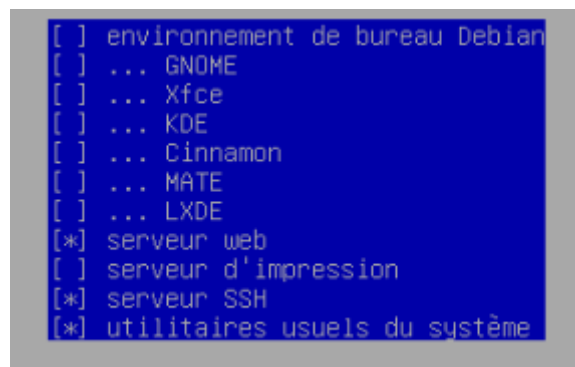


Installation de Debian sans interface graphique

Pour installer Debian sans interface graphique, on ne fera pas “Graphical Install” mais juste “Install” puis on fera comme pour les autres installations.



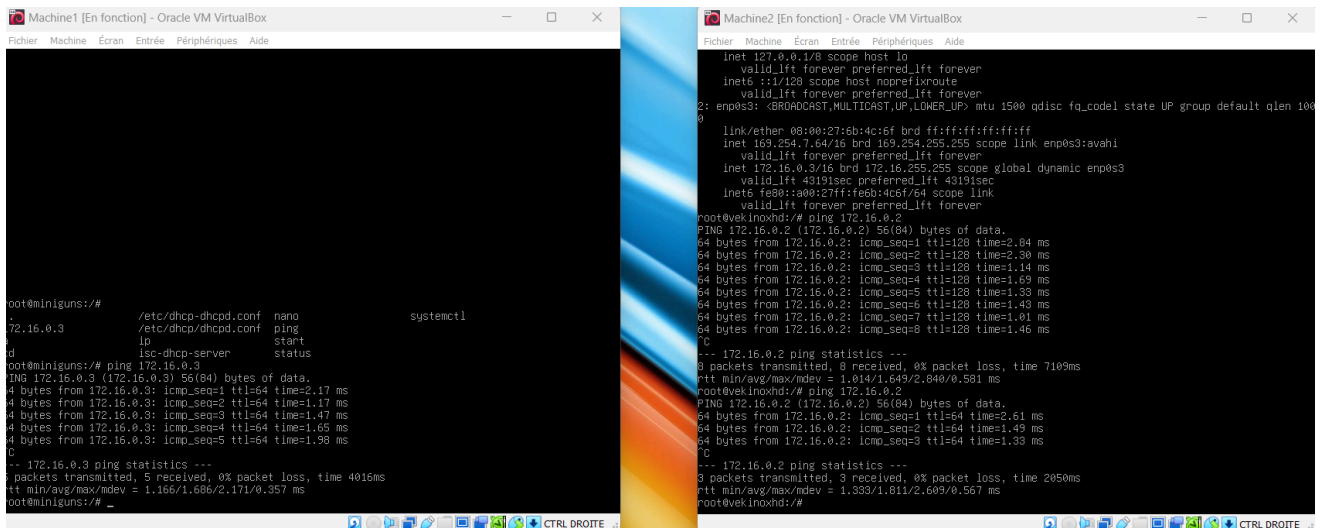
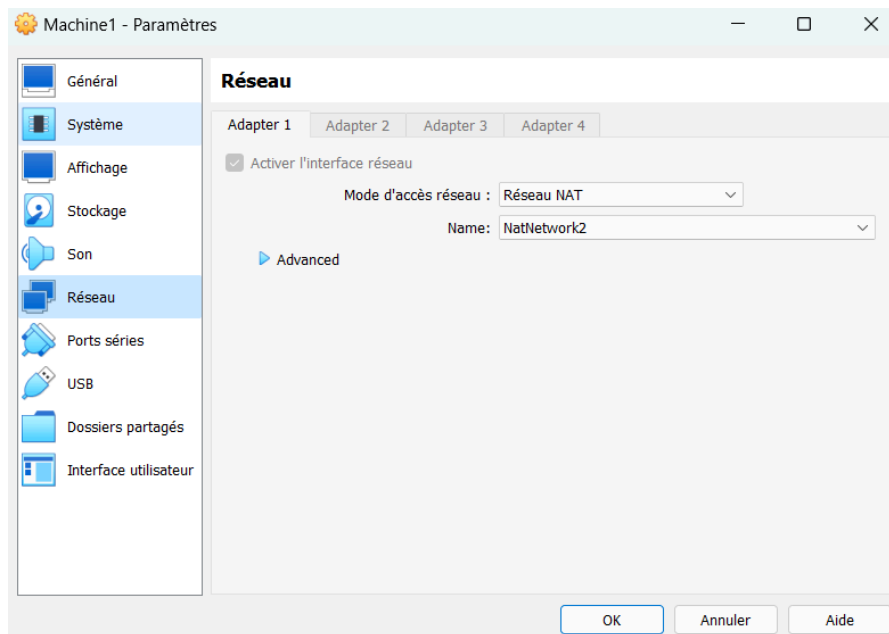
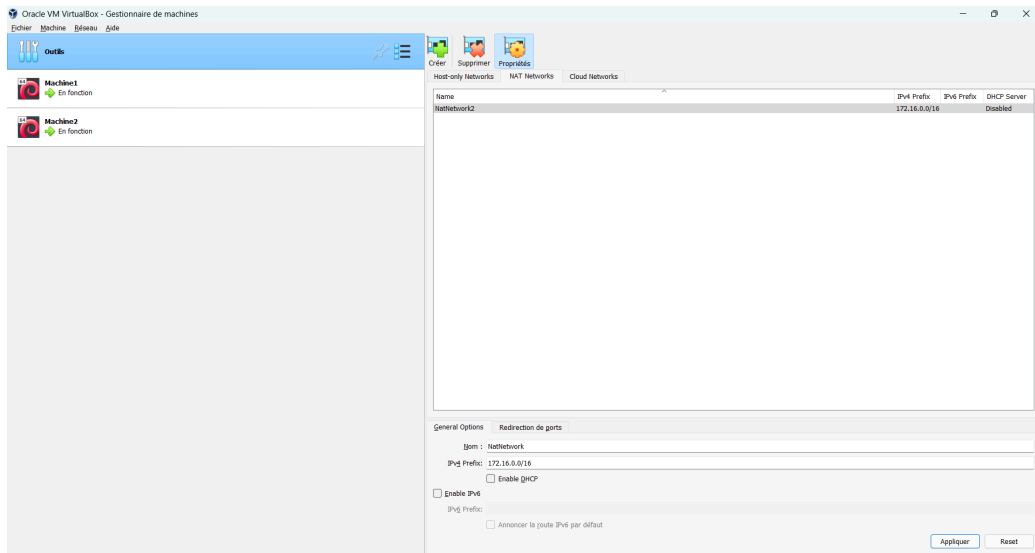
Ici, on décrochera les deux premiers et on coche les deux derniers



Une fois que la machine virtuelle est créée, nous ferons de même pour la deuxième machine virtuelle.

Fini, on a nos deux machines virtuelles, maintenant nous allons les mettre sur un même réseau pour qu'ils puissent communiquer.

Pour cela, on a utilisé VirtualBox qui nous propose de créer un réseau virtuel comparé à VMWare sur la version étudiante.

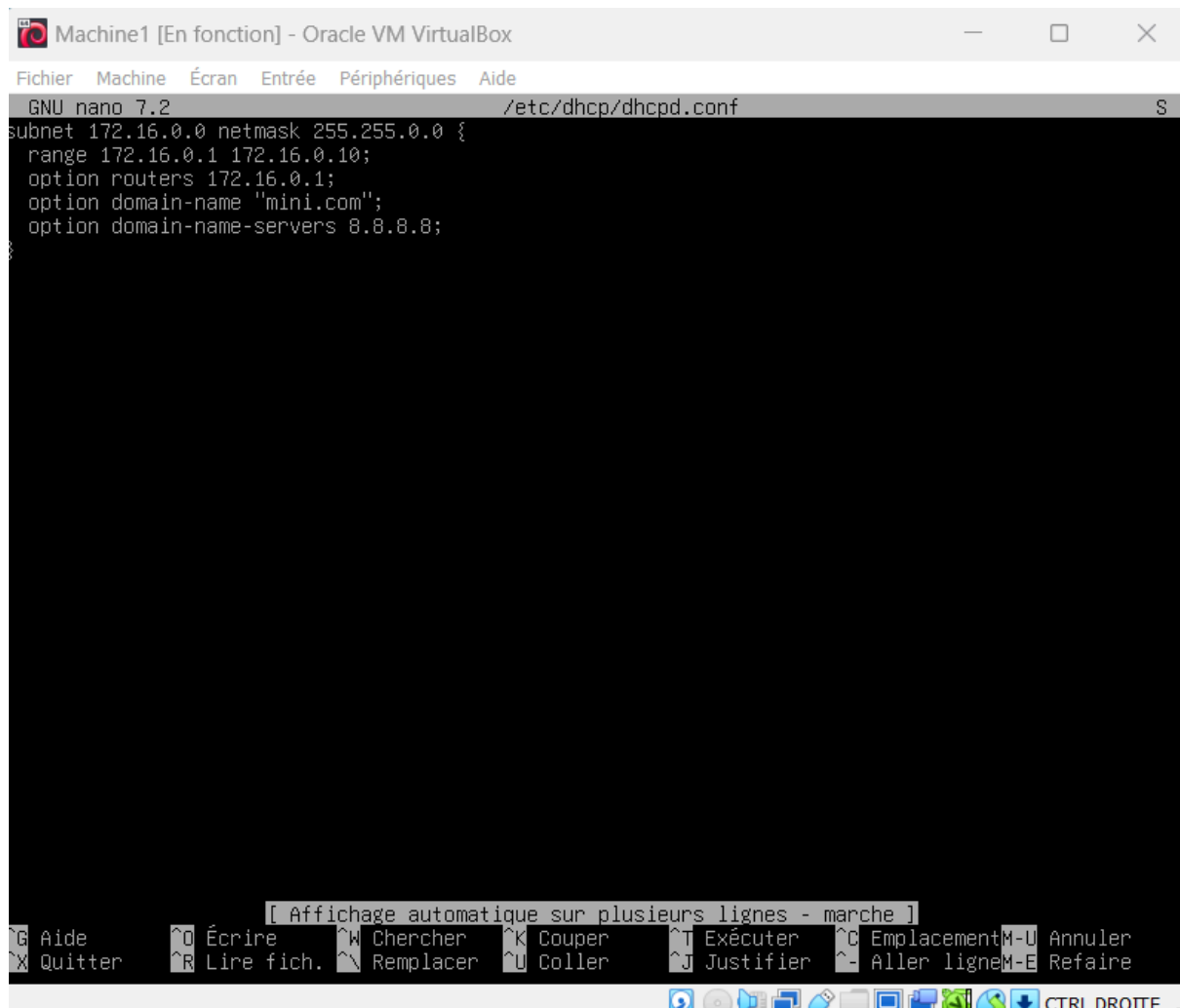


Installation et configuration d'un serveur DHCP

Installons le paquet avec `apt install isc-dhcp-server`

Pour pouvoir configurer le serveur dhcp, on ira dans les fichiers conf :
`nano /etc/dhcp/dhcpd.conf`

Configuration dhcp :

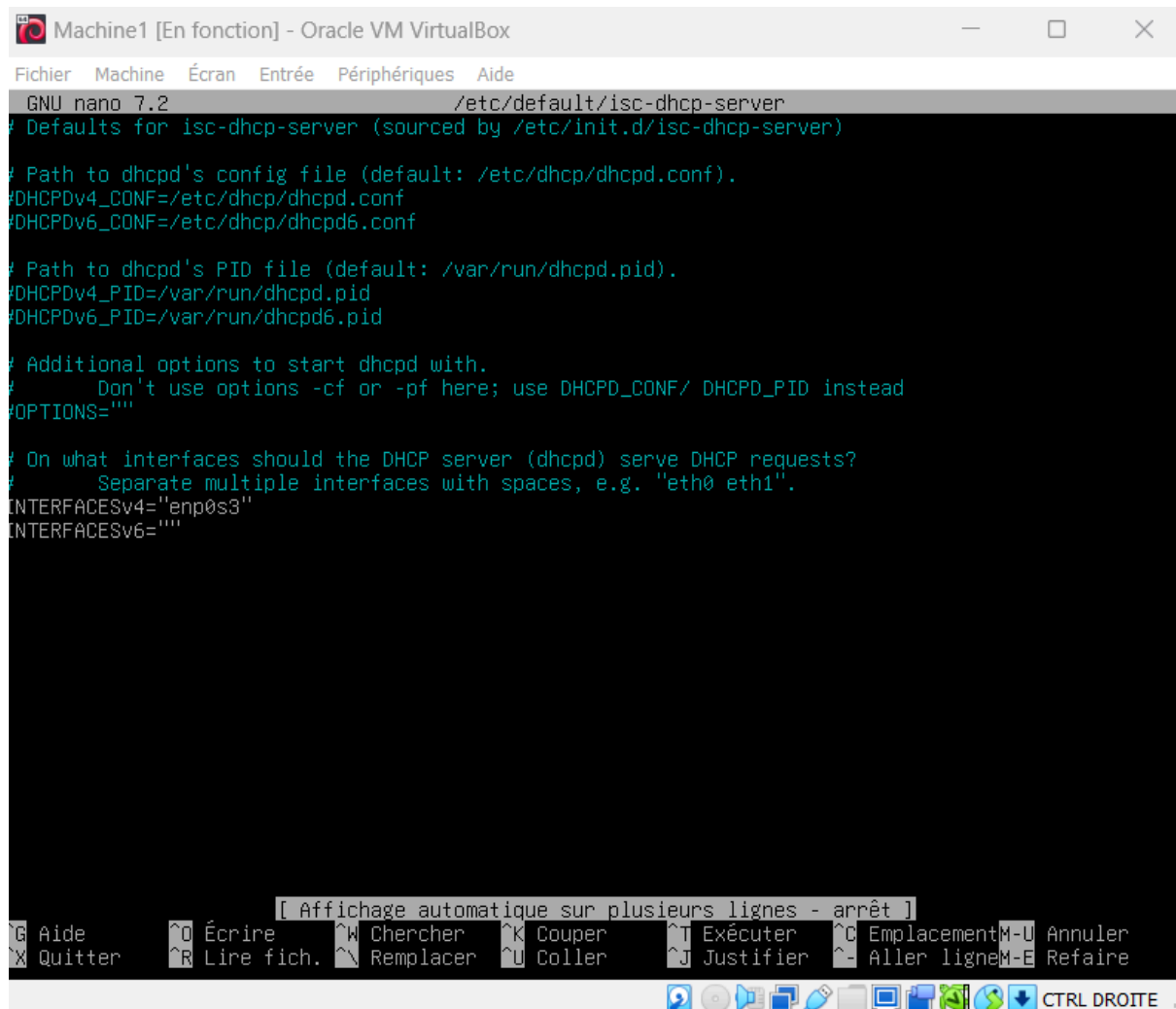


The screenshot shows a terminal window titled "Machine1 [En fonction] - Oracle VM VirtualBox". The terminal is running the nano text editor, editing the file `/etc/dhcp/dhcpd.conf`. The content of the file is as follows:

```
GNU nano 7.2 /etc/dhcp/dhcpd.conf
subnet 172.16.0.0 netmask 255.255.0.0 {
  range 172.16.0.1 172.16.0.10;
  option routers 172.16.0.1;
  option domain-name "mini.com";
  option domain-name-servers 8.8.8.8;
}
```

At the bottom of the terminal, there is a status bar with the text "[Affichage automatique sur plusieurs lignes - marche]" and a list of keyboard shortcuts for nano, such as "Aide", "Écrire", "Chercher", "Couper", "Exécuter", "Emplacement", "Annuler", "Refaire", etc.

ip a et on regardera le nom de notre adresse ip qu'on mettra dans le serveur dhcp : `nano/etc/default/isc-dhcp-server`



```
Machine1 [En fonction] - Oracle VM VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
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="enp0s3"
INTERFACESv6=""

[ Affichage automatique sur plusieurs lignes - arrêt ]
Aide  Écrire  Chercher  Couper  Exécuter  Emplacement  Annuler
Quitter  Lire fich.  Remplacer  Coller  Justifier  Aller ligne  Refaire
CTRL DROITE
```

```
host ftp {
    hardware ethernet 08:00:27:6b:4c:6f;
    fixed-address 172.16.0.3;
}
```

Adresse IP fixe :

Le serveur dhcp fonctionne mais maintenant pour la connexion internet, il faudra encore configurer pour que la machine puisse envoyer des commandes dans d'autres serveurs :

On ira configurer `resolv.conf` et le `/network/interfaces` pour permettre à la machine de se connecter au serveur

Machine1 [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

GNU nano 7.2 /etc/resolv.conf

```
domain mini.com
search mini.com
nameserver 8.8.8.8
```

[Lecture de 3 lignes]

Aide Écrire Chercher Couper Exécuter Emplacement Annuler
Quitter Lire fich. Remplacer Collier Justifier Aller ligne Refaire

CTRL DROITE

Machine1 [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

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 enp0s3
iface enp0s3 inet static
    address 172.16.0.2
    network 172.16.0.0
    broadcast 172.16.255.255
    netmask 255.255.0.0
    gateway 172.16.0.1
    dns-nameservers 8.8.8.8
```

[Lecture de 18 lignes]

Aide Écrire Chercher Couper Exécuter Emplacement Annuler
Quitter Lire fich. Remplacer Collier Justifier Aller ligne Refaire

CTRL DROITE

Pour finir, on redémarre le serveur DHCP et tout sera bon, on vérifiera si la deuxième machine a une adresse ip de classe B et du même réseau

```
systemctl restart isc-dhcp-server  
systemctl start isc-dhcp-server  
systemctl status isc-dhcp-server
```

Installation et configuration d'un serveur FTP et SSH

Installons les paquets :

```
apt install proftpd ssh ftp
```

Pour configurer notre serveur ftp tout d'abord, nous allons sur le fichier :

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

```
ServerName "172.16.0.3"
```

```
# Set off to disable IPv6 support which is annoying on IPv4 only boxes.  
UseIPv6 off
```

```
# Use this to jail all users in their homes  
DefaultRoot /home/laplateforme
```

```
# 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
```

```
# This is used for SFTP connections  
#  
#Include /etc/proftpd/sftp.conf  
<IfModule mod_sftp.c>  
    SFTPEngine on  
    Port 2222  
  
    SFTPLog /var/log/proftpd/sftp.log  
    SFTPHostKey /etc/ssh/ssh_host_rsa_key  
    SFTPHostKey /etc/ssh/ssh_host_dsa_key  
  
    SFTPAuthMethods password  
  
    SFTPCompression delayed  
</IfModule>
```

On va créer un utilisateur, pour ceci `/usr/sbin/adduser laplateforme`
et on va utiliser le mot de passe Marseille13!

Faisons un restart du serveur à chaque fois qu'on modifie les fichiers :

`systemctl restart proftpd`

Essayons de nous connecter au serveur ftp et sftp

pour ceci ftp 172.16.0.3 et sftp 172.16.0.3 si cela fonctionne tout est bon !

```
root@vekinoxhd:/# ftp laplateforme@172.16.0.3
Connected to 172.16.0.3.
220 ProFTPD Server (172.16.0.3) [172.16.0.3]
331 Mot de passe requis pour laplateforme
Password:
230 Utilisateur laplateforme authentifié
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> _
```

```
root@vekinoxhd:/# sftp laplateforme@172.16.0.3
laplateforme@172.16.0.3's password:
Connected to 172.16.0.3.
sftp> _
```

Installation et configuration d'un serveur DNS

Installons le paquet dns : `apt install bind9`

Nous allons configurer les fichiers et aussi le dhcp pour que tout fonctionne bien car nous avons aussi des soucis sur le dhcp qui renvoie sur le resolv.conf en nameserver 8.8.8.8 à chaque fois sur la deuxième machine

Configurons le DNS :


```

GNU nano 7.2                                     db.dns.ftp.com
$TTL      86400
@          IN      SOA      dns.ftp.com. admin.ftp.com. (
                        2022030102      ; Serial
                        3600             ; Refresh
                        1800             ; Retry
                        604800           ; Expire
                        86400 )          ; Negative Cache TTL

@          IN      NS       ns
@          IN      A        172.16.0.2
ns         IN      A        172.16.0.2
dns        IN      A        172.16.0.3

```

```

GNU nano 7.2                                     named.conf.local
zone "ftp.com" {
    type master;
    file "/etc/bind/db.dns.ftp.com";
};

```

```

GNU nano 7.2                                     named.conf.options
options {
    directory "/var/cache/bind";

    // 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;

    listen-on-v6 { any; };
};

```

Pour tester, il faut ping le serveur dns.ftp.com sur la première machine.

```
root@miniguns:/etc/bind# ping dns.ftp.com
PING dns.ftp.com (172.16.0.3) 56(84) bytes of data.
64 bytes from 172.16.0.3 (172.16.0.3): icmp_seq=1 ttl=64 time=2.18 ms
64 bytes from 172.16.0.3 (172.16.0.3): icmp_seq=2 ttl=64 time=1.94 ms
64 bytes from 172.16.0.3 (172.16.0.3): icmp_seq=3 ttl=64 time=1.78 ms
64 bytes from 172.16.0.3 (172.16.0.3): icmp_seq=4 ttl=64 time=1.71 ms
^C
--- dns.ftp.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 1.713/1.903/2.183/0.181 ms
```

Une fois que le DNS est configuré, allons modifier quelques fichiers du DHCP pour permettre la connexion de la deuxième machine sur le serveur DNS :
Le problème de pourquoi la deuxième machine prenait tout le temps nameserver 8.8.8.8 est car dans la configuration du dhcp, j'ai mis en domain-name-servers 8.8.8.8 et dans l'interface aussi.

```
GNU nano 7.2 /etc/dhcp/dhcpd.conf
ddns-update-style none;

subnet 172.16.0.0 netmask 255.255.0.0 {
    range 172.16.0.10 172.16.0.30;
    option routers 172.16.0.1;
    option broadcast-address 172.16.255.255;
    option domain-name-servers 172.16.0.2;
    default-lease-time 600;
    max-lease-time 7200;
}

host ftp {
    hardware ethernet 08:00:27:6b:4c:6f;
    fixed-address 172.16.0.3;
}
```

```

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 enp0s3
iface enp0s3 inet static
    address 172.16.0.2
    network 172.16.0.0
    broadcast 172.16.255.255
    netmask 255.255.0.0
    gateway 172.16.0.1

```

Une fois fini, il faut que dans les deux resolv.conf des machines virtuelles il y a sans modifier soit même, juste que ca soit le serveur dhcp qui distribue bien l'adresse ip et la configuration :

```

GNU nano 7.2 /etc/resolv.conf
gameserver 172.16.0.2

```

Il faut toujours restart tous les paquets soit

`systemctl restart networking`

`systemctl restart bind9`

`systemctl restart isc-dhcp-server`

Il faut aussi faire cela pour la deuxième machine donc restart juste le réseau soit `systemctl restart networking`

Si il y a ceci dans le resolv.conf et qu'on peut ping google.fr et dns.ftp.com c'est que l'exercice est rempli, le serveur DNS fonctionne bien :

```

GNU nano 7.2 /etc/resolv.conf
gameserver 172.16.0.2

```

```

root@vekinoxhd:/# ping google.fr
PING google.fr (142.251.37.227) 56(84) bytes of data.
64 bytes from 142.251.37.227: icmp_seq=1 ttl=118 time=5.39 ms
64 bytes from 142.251.37.227: icmp_seq=2 ttl=118 time=5.21 ms
64 bytes from 142.251.37.227: icmp_seq=3 ttl=118 time=22.1 ms
64 bytes from 142.251.37.227: icmp_seq=4 ttl=118 time=7.32 ms
^C
--- google.fr ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3648ms
rtt min/avg/max/mdev = 5.210/10.007/22.108/7.035 ms
root@vekinoxhd:/# ping dns.ftp.com
PING dns.ftp.com (172.16.0.3) 56(84) bytes of data.
64 bytes from 172.16.0.3 (172.16.0.3): icmp_seq=1 ttl=64 time=0.036 ms
64 bytes from 172.16.0.3 (172.16.0.3): icmp_seq=2 ttl=64 time=0.118 ms
64 bytes from 172.16.0.3 (172.16.0.3): icmp_seq=3 ttl=64 time=0.041 ms
64 bytes from 172.16.0.3 (172.16.0.3): icmp_seq=4 ttl=64 time=0.104 ms
^C
--- dns.ftp.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 0.036/0.074/0.118/0.036 ms
root@vekinoxhd:/#

```

Test de connexion au serveur SFTP

Machine 1 :

```

root@miniguns:/# sftp laplateforme@dns.ftp.com
laplateforme@dns.ftp.com's password:
Connected to dns.ftp.com.
sftp>

```

Machine 2 :

```

root@vekinoxhd:/# sftp laplateforme@dns.ftp.com
laplateforme@dns.ftp.com's password:
Connected to dns.ftp.com.
sftp> _

```

Paramètres de sécurité et additionnels

Pour renforcer le serveur SFTP nous allons sur deux fichiers et ajouter des instructions :

`nano /etc/proftpd/proftpd.conf`

Autoriser seulement l'utilisateur laplateforme:

```
# Display the .message file
<Limit LOGIN>
    AllowUser laplateforme
    DenyAll
</Limit>
```

```
# Port 21 is the standard FTP port.
Port 6500
```

```
MaxSessions 1
```

```
<IfModule mod_sftp.c>
    SFTPEngine on
    Port 6500

    SFTPLog /var/log/proftpd/sftp.log
    SFTPHostKey /etc/ssh/ssh_host_rsa_key
    SFTPHostKey /etc/ssh/ssh_host_dsa_key

    SFTPAuthMethods password

    SFTPCompression delayed
</IfModule>
```

`nano /etc/ssh/sshd_config`

Autoriser seulement l'utilisateur laplateforme et éviter toute connexion anonyme

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
PermitEmptyPasswords no
AllowUsers laplateforme
```

```
MaxSessions 1
```

```
Port 6500
```