

Systeme, scripts et sécurité

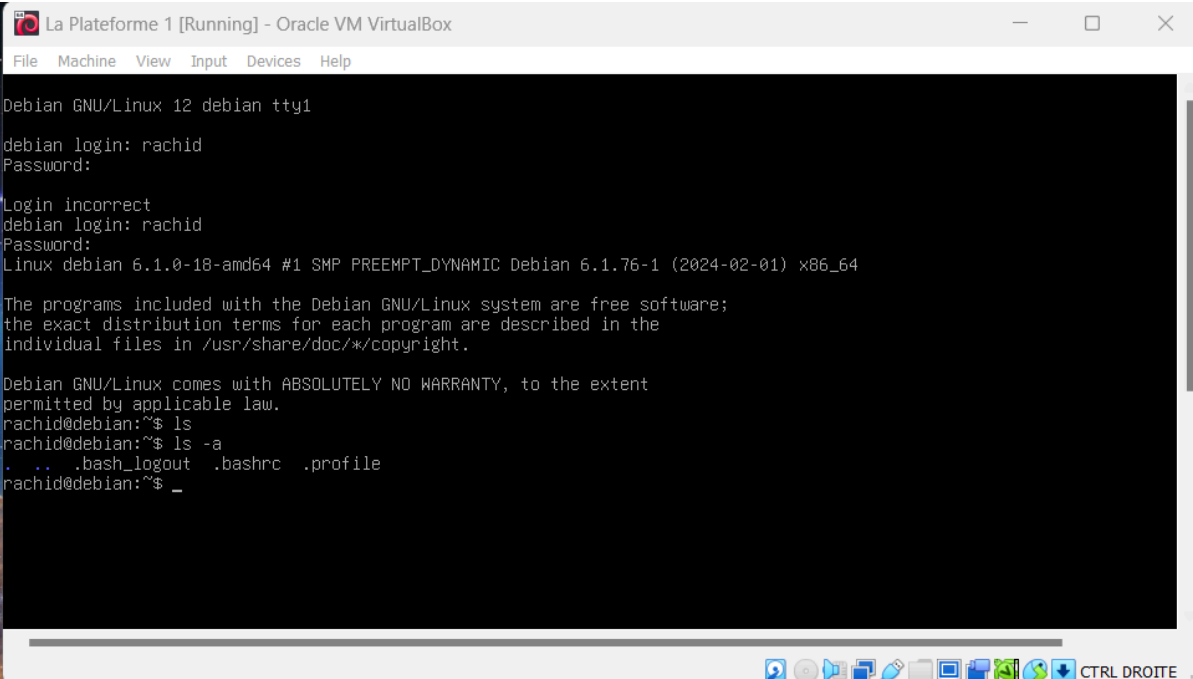
Objectif

Nous avons pour objectif de faire une documentation détaillée de la configuration d'un environnement virtuel Debian, en mettant en place un serveur DHCP et DNS sur la première machine, ainsi qu'un serveur client FTP avec SSH sur la seconde machine.

Étapes à suivre

1. Installation de Debian sans interface graphique :

- Mise en place de deux machines virtuelles sans interface graphique à l'aide de mon Hyperviseur préféré **Oracle VM Virtualbox Manager**

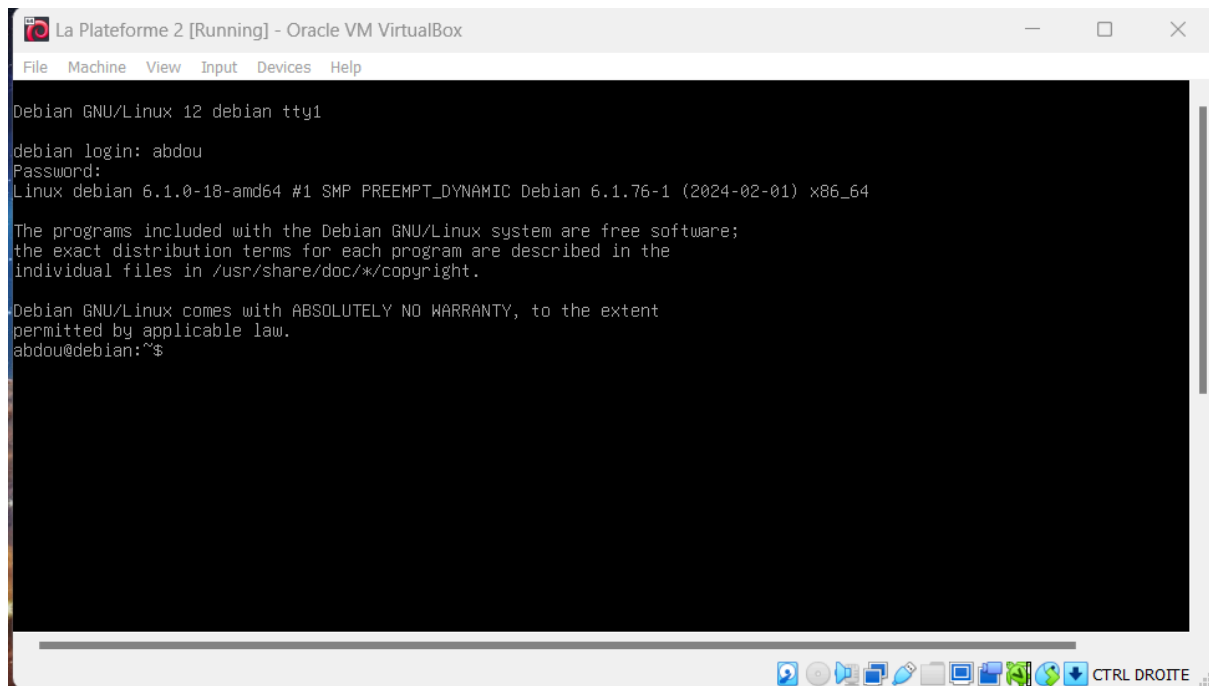


```
La Plateforme 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Debian GNU/Linux 12 debian tty1
debian login: rachid
Password:
Login incorrect
debian login: rachid
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.
rachid@debian:~$ ls
rachid@debian:~$ ls -a
.  ..  .bash_logout  .bashrc  .profile
rachid@debian:~$ _
```



2. Mise à jour des systèmes :

Pour vérifier les mise à jour disponible, il faut exécuter les commande suivantes sur chaque VM pour avoir la liste des mises à jour disponibles :

sudo apt list --upgradable : Cette commande permet de lister les mise à jour disponible.

Les commandes ensuite pour mettre à jour les paquets sont les suivantes :

sudo apt update

sudo apt upgrade

sudo apt full-upgrade

Après avoir fait les mises à jour, il faut exécuter la commande suivante :

sudo reboot : Dans le but de redémarrer les VM pour qu'ils prennent en compte les nouvelles installations et modification apportées par les mise à jour.

3. Configuration du serveur DHCP :

Pour installer un serveur DHCP (Dynamic Host configuration Protocol) sur la première machine, il faut suivre les étapes suivantes :

La commande pour installer le serveur DHCP est la suivante :

sudo apt install isc-dhcp-server

Après l'installation, il va falloir configurer le fichier **conf** du serveur DHCP. Mais bien avant ça, il faut retourner dans les paramètres de l'hyperviseur afin de créer un autre réseau autre que le réseau NAT (configuré en DHCP) que nous attribue automatiquement l'hyperviseur lors de la création des VM.

Une fois le réseau créé avec une adresse IP statique, il faut donc retourner dans la VM dans les paramètres de configurations pour faire toutes les modifications/configurations en fonction de l'adresse IP du réseau que nous avons créé nous-même dans l'hyperviseur. Il faut exécuter la commande suivante pour ouvrir le fichier conf :

nano /etc/network/interfaces

Les configurations à faire sont les suivantes :

Dans le fichier il faut changer l'interface du réseau primaire **“dhcp”** en **“static”** pour ensuite définir manuellement son réseau :

address Adresse IP du réseau créé

netmask Le masque de sous réseau

network Définition de l'adresse du réseau

broadcast L'adresse de diffusion

gateway L'adresse IP de la passerelle par défaut

The screenshot shows a terminal window titled "La Plateforme 1 [Running] - Oracle VM VirtualBox". The terminal displays the following configuration for the network interface `enp0s3`:

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

At the bottom of the terminal, there is a status bar with various icons and a keyboard shortcut indicator: `CTRL DROITE`.

Pour s'assurer des modifications qu'on a faites, on peut exécuter la commande suivante pour afficher les informations sur l'interface du réseau qu'on vient de configurer.

cat /etc/network/interfaces

The screenshot shows a terminal window with the output of the command `cat /etc/network/interfaces`. The output is as follows:

```
# filename "vmunix.passacaglia";
# server-name "toccata.example.com";
#}

root@debian:~# cat /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
netmask 255.255.0.0
network 172.16.0.0
broadcast 172.16.255.255
gateway 172.16.0.1
root@debian:~#
```

At the bottom of the terminal, there is a status bar with various icons and a keyboard shortcut indicator: `CTRL DROITE`.

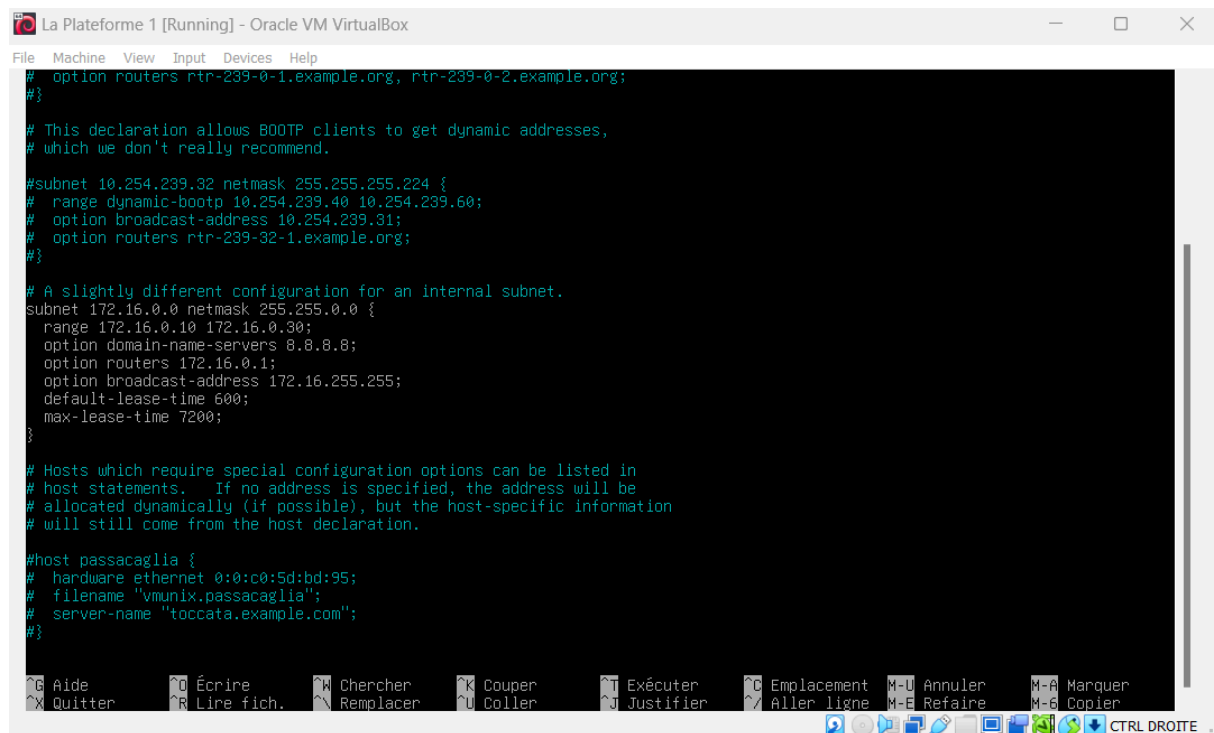
Après cette modification dans l'interface, il faut ouvrir le fichier suivant et faire la configuration ci-dessous :

nano /etc/dhcp/dhcpd.conf

Dans le fichier conf, il faut faire la configuration suivante :

```
subnet 172.16.0.0 netmask 255.255.0.0 {  
    range 172.16.0.10 172.16.0.30;  
    option domain-name-servers 8.8.8.8;  
    option routers 172.16.0.1;  
    option broadcast-address 172.16.255.555;  
    default-lease-time 600;  
    max-lease-time 7200;  
}
```

NB : Faites cette configuration en fonction de l'adresse IP de votre réseau.



```
La Plateforme 1 [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
# option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;  
#}  
# This declaration allows BOOTP clients to get dynamic addresses,  
# which we don't really recommend.  
#subnet 10.254.239.32 netmask 255.255.255.224 {  
# range dynamic-bootp 10.254.239.40 10.254.239.60;  
# option broadcast-address 10.254.239.31;  
# option routers rtr-239-32-1.example.org;  
#}  
# A slightly different configuration for an internal subnet.  
subnet 172.16.0.0 netmask 255.255.0.0 {  
    range 172.16.0.10 172.16.0.30;  
    option domain-name-servers 8.8.8.8;  
    option routers 172.16.0.1;  
    option broadcast-address 172.16.255.255;  
    default-lease-time 600;  
    max-lease-time 7200;  
}  
# Hosts which require special configuration options can be listed in  
# host statements.  If no address is specified, the address will be  
# allocated dynamically (if possible), but the host-specific information  
# will still come from the host declaration.  
#host passacaglia {  
# hardware ethernet 0:0:c0:5d:bd:95;  
# filename "vmunix.passacaglia";  
# server-name "toccata.example.com";  
#}
```

Pour s'assurer que la machine hébergeant le serveur DHCP possède une adresse IP fixe, il faut procéder de la manière suivante :

Il faut toujours ouvrir le fichier conf en faisant :

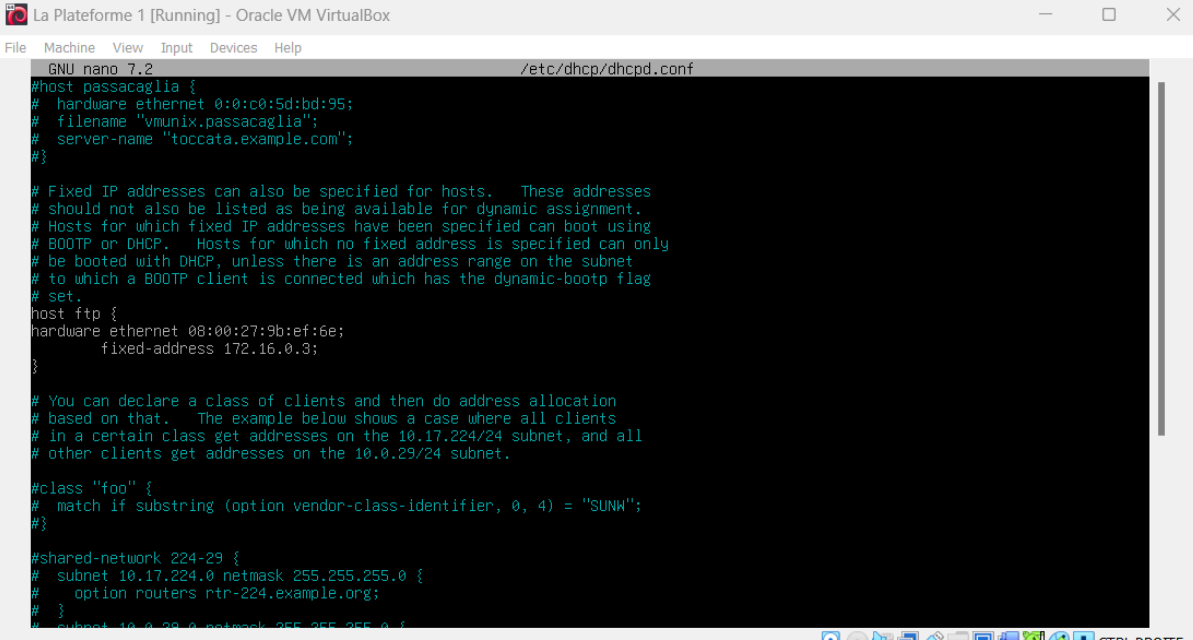
nano /etc/dhcp/dhcpd.conf

host ftp {

hardware ethernet 08:00:27:9b:ef:6e; (Adresse Mac)

fixed-address 172.16.0.3; (Adresse fixe qu'il faut définir)

}



```
La Plateforme 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 7.2 /etc/dhcp/dhcpd.conf
#host passacaglia {
#   hardware ethernet 0:0:c0:5d:bd:95;
#   filename "vmunix.passacaglia";
#   server-name "toccata.example.com";
#}

# Fixed IP addresses can also be specified for hosts.  These addresses
# should not also be listed as being available for dynamic assignment.
# Hosts for which fixed IP addresses have been specified can boot using
# BOOTP or DHCP.  Hosts for which no fixed address is specified can only
# be booted with DHCP, unless there is an address range on the subnet
# to which a BOOTP client is connected which has the dynamic-bootp flag
# set.
host ftp {
    hardware ethernet 08:00:27:9b:ef:6e;
    fixed-address 172.16.0.3;
}

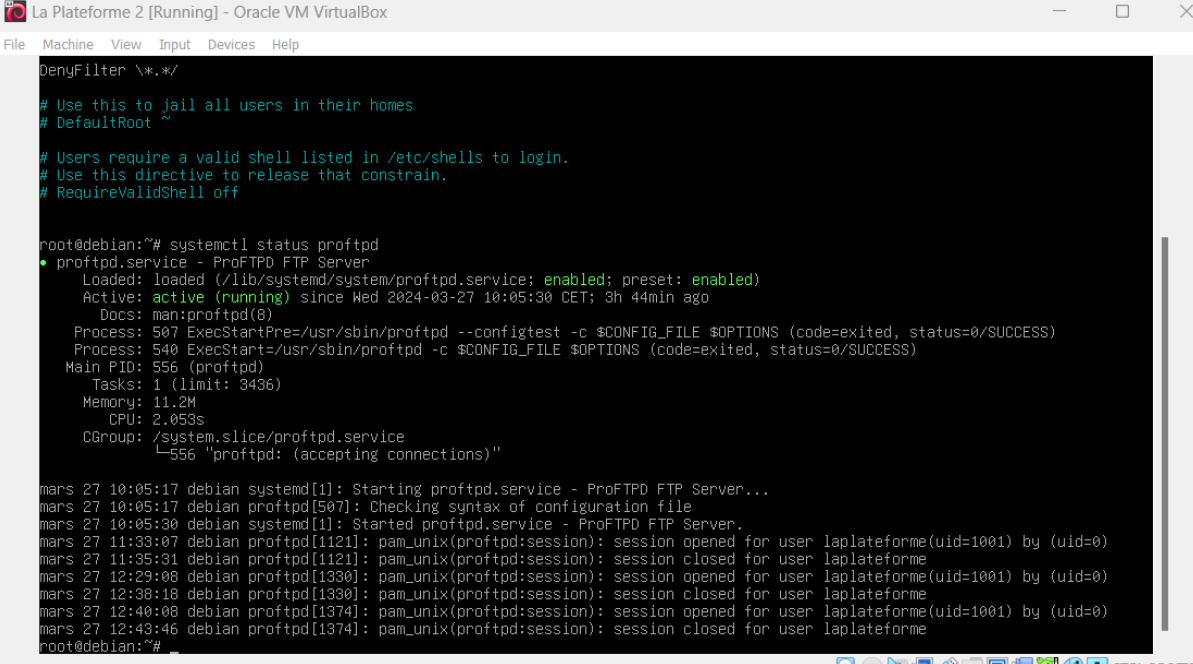
# You can declare a class of clients and then do address allocation
# based on that.  The example below shows a case where all clients
# in a certain class get addresses on the 10.17.224/24 subnet, and all
# other clients get addresses on the 10.0.29/24 subnet.

#class "foo" {
#   match if substr (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;
#   }
#}
```

4. Installation du serveur FTP et SSH :

Installation du serveur **FTP; proFTPD (File Transfer Protocol)** et **SSH (Secure Shell)** sur la deuxième machine.



```
La Plateforme 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

DenyFilter *.*/

# 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 off

root@debian:~# systemctl status proftpd
● proftpd.service - ProFTPD FTP Server
   Loaded: loaded (/lib/systemd/system/proftpd.service; enabled; preset: enabled)
   Active: active (running) since Wed 2024-03-27 10:05:30 CET; 3h 44min ago
     Docs: man:proftpd(8)
   Process: 507 ExecStartPre=/usr/sbin/proftpd --configtest -c $CONFIG_FILE $OPTIONS (code=exited, status=0/SUCCESS)
   Process: 540 ExecStart=/usr/sbin/proftpd -c $CONFIG_FILE $OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 556 (proftpd)
      Tasks: 1 (limit: 3436)
     Memory: 11.2M
        CPU: 2.053s
    CGroup: /system.slice/proftpd.service
           └─556 "proftpd: (accepting connections)"

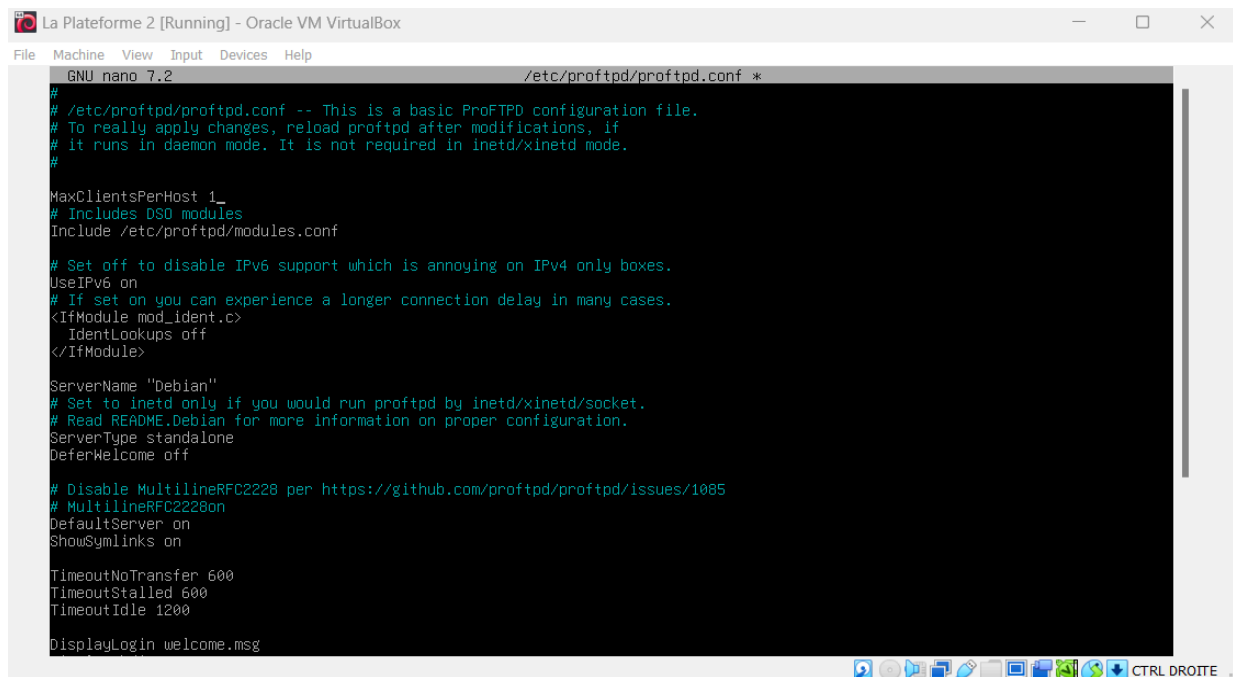
mars 27 10:05:17 debian systemd[1]: Starting proftpd.service - ProFTPD FTP Server...
mars 27 10:05:17 debian proftpd[507]: Checking syntax of configuration file
mars 27 10:05:30 debian systemd[1]: Started proftpd.service - ProFTPD FTP Server.
mars 27 11:33:07 debian proftpd[1121]: pam_unix(proftpd:session): session opened for user laplateforme(uid=1001) by (uid=0)
mars 27 11:35:31 debian proftpd[1121]: pam_unix(proftpd:session): session closed for user laplateforme
mars 27 12:29:08 debian proftpd[1330]: pam_unix(proftpd:session): session opened for user laplateforme(uid=1001) by (uid=0)
mars 27 12:38:18 debian proftpd[1330]: pam_unix(proftpd:session): session closed for user laplateforme
mars 27 12:40:08 debian proftpd[1374]: pam_unix(proftpd:session): session opened for user laplateforme(uid=1001) by (uid=0)
mars 27 12:43:46 debian proftpd[1374]: pam_unix(proftpd:session): session closed for user laplateforme
root@debian:~#
```

Configurez le serveur FTP avec une seule session de connexion possible :
il faut exécuter la commande suivante :

nano /etc/proftpd/proftpd.conf

Puis ajouter la ligne suivante :

MaxClientsPerHost 1



```
GNU nano 7.2 /etc/proftpd/proftpd.conf *
#
# /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.
#
MaxClientsPerHost 1_
# 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
TimeoutIdle 1200

DisplayLogin welcome.msg
```

Utilisez les identifiants suivants pour le FTP :

- Identifiant : **laplateforme**
- Mot de passe : **Marseille13!**

Pour faire ça, il faut exécuter la commande suivante pour créer un utilisateur en lui attribuant les identifiants et mot de passe indiqué dans la consigne.

sudo adduser laplateforme

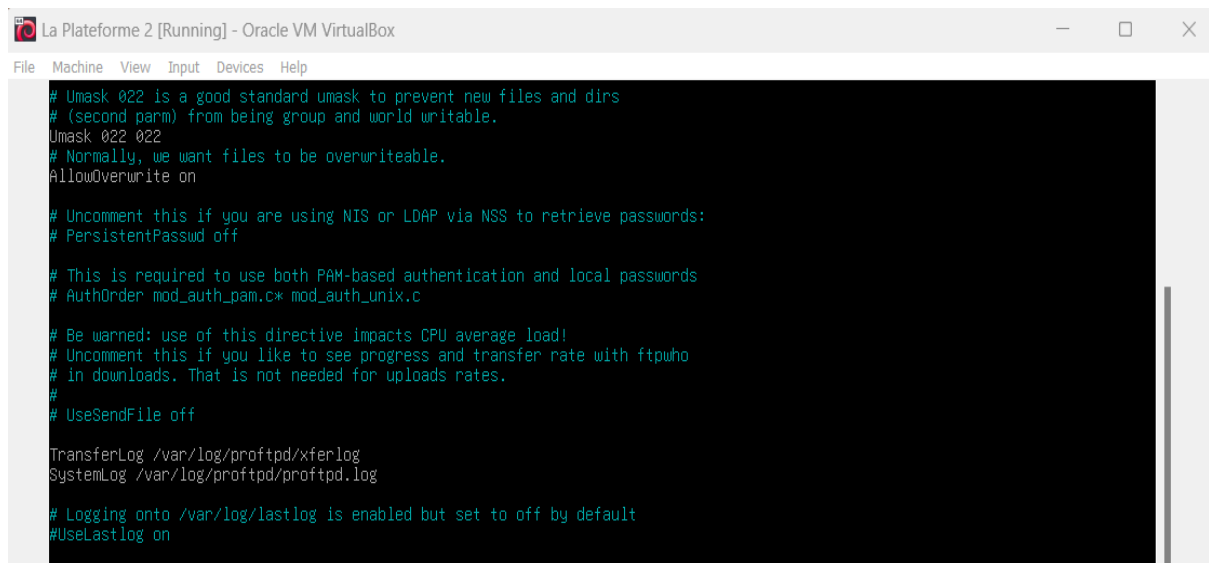
Et après il faut définir le mot de passe et les informations nécessaires qui vont avec.

Utilisez le serveur SSH pour les connexions au FTP en SFTP, renforçant ainsi la sécurité.

Pour répondre à cette question, il faut ouvrir toujours le fichier conf du serveur proFTP via la commande suivante :

nano /etc/proftpd/proftpd.conf

Afin de décommenter la ligne qui se trouve dans la capture d'écran suivante :



```
# 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

# Uncomment this if you are using NIS or LDAP via NSS to retrieve passwords:
# PersistentPasswd off

# This is required to use both PAM-based authentication and local passwords
# AuthOrder mod_auth_pam.c* mod_auth_unix.c

# Be warned: use of this directive impacts CPU average load!
# Uncomment this if you like to see progress and transfer rate with ftpwho
# in downloads. That is not needed for uploads rates.
#
# UseSendFile off

TransferLog /var/log/proftpd/xferlog
SystemLog /var/log/proftpd/proftpd.log

# Logging onto /var/log/lastlog is enabled but set to off by default
#UseLastlog on
```

5. Installation du serveur DNS :

Pour l'installation du serveur DNS, il faut exécuter la commande suivante :

Nous avons choisi d'utiliser **Bin9** pour exécuter cette tâche.

sudo apt install bind9

Après l'installation, il faut donc configurer les fichiers conf et zone de Bind9.

Les configurations à faire sont les suivantes :

Naviguer vers le fichier conf en tapant la commande suivante :

cd /etc/bind/ : Dans ce dossier se trouvent les fichiers à configurer. il faut faire par la suite :

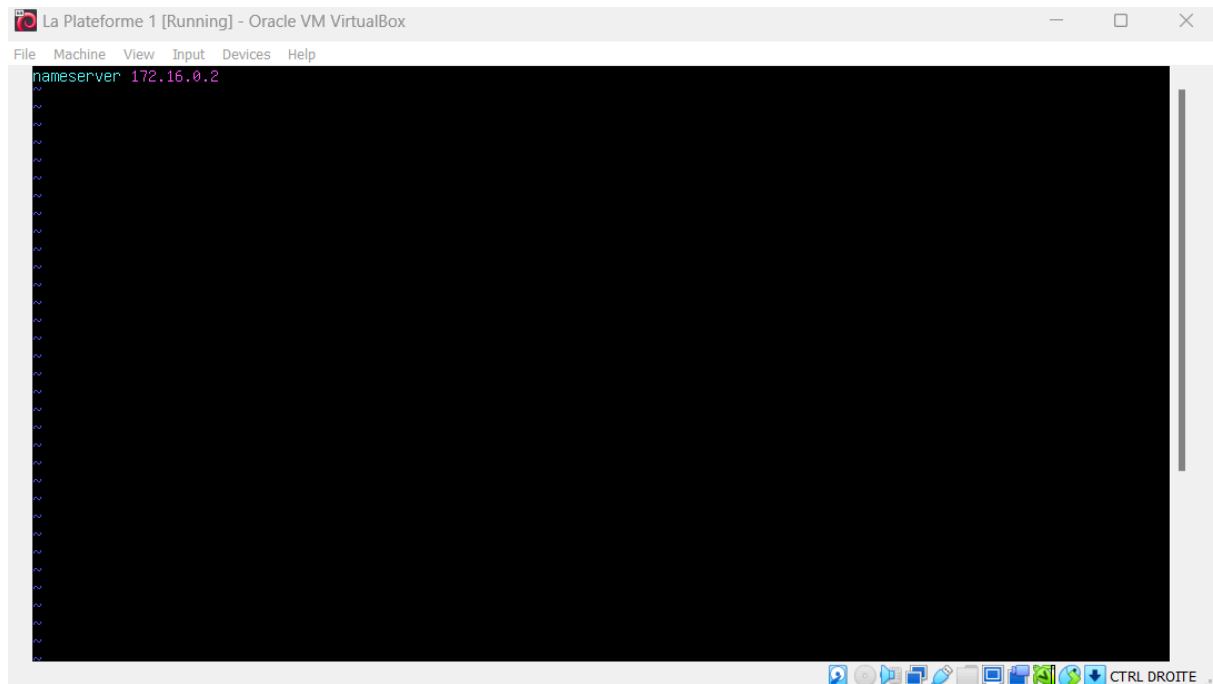
nano named.conf.local

Une fois que le fichier est ouvert, il faut le configurer comme suit :

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


Il faut également s'assurer que dans le fichier resolv, l'adresse IP du serveur soit spécifiée :

nano /etc/resolv.conf



6. Test de connexion au serveur SFTP :

Maintenant, tentons de nous connecter à notre serveur SFTP de la deuxième en utilisant l'adresse **“dns.ftp.com”** pour la connexion :

sftp laplateforme@dns.ftp.com

```
File Machine View Input Devices Help
*rachid@debian:~$ sftp laplateforme@dns.ftp.com
The authenticity of host 'dns.ftp.com (172.16.0.3)' can't be established.
ED25519 key fingerprint is SHA256:1qU3aSgpQImQ7M0gPwKl4yndQEnXdPMM3/mgCcF0Lsc.
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 'dns.ftp.com' (ED25519) to the list of known hosts.
laplateforme@dns.ftp.com's password:
Connected to dns.ftp.com.
sftp> _
```

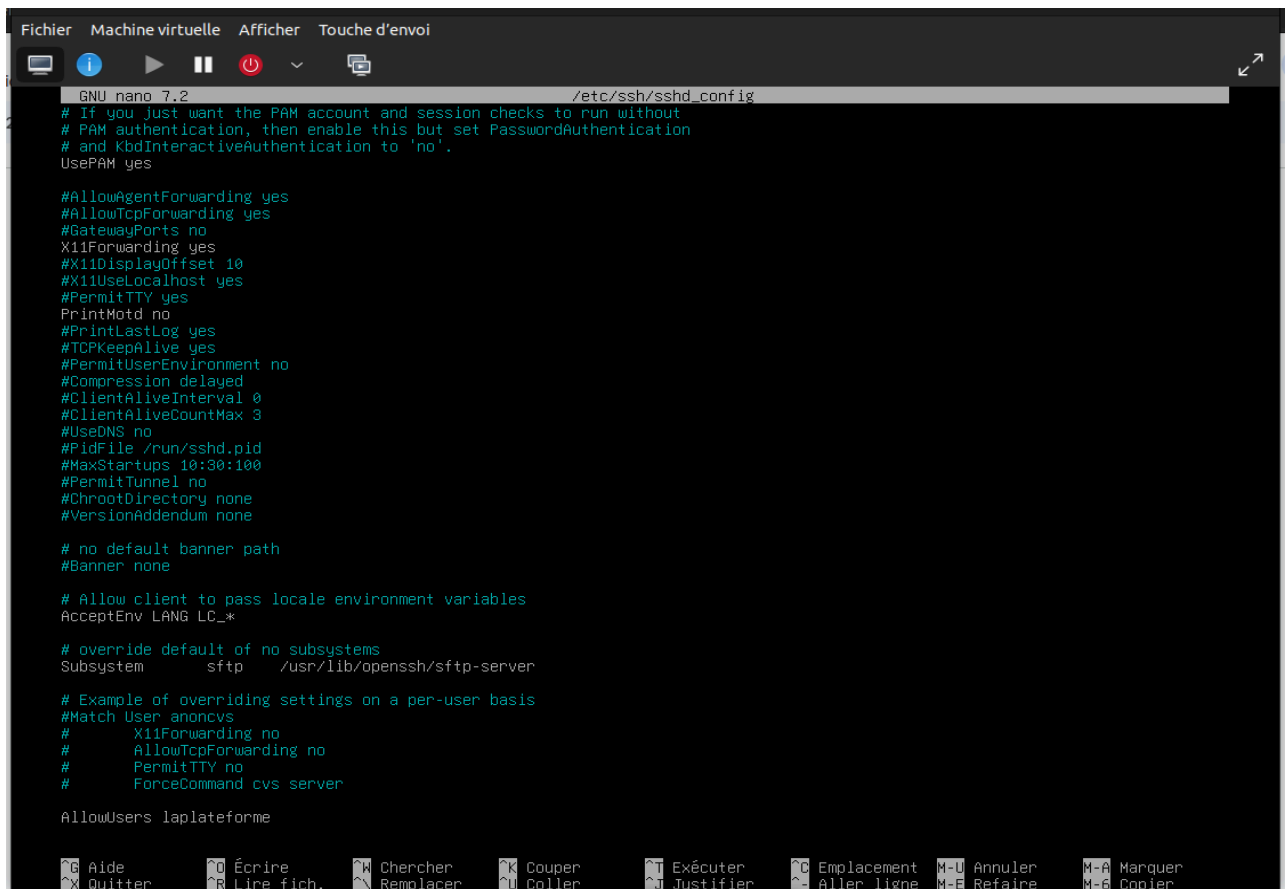
7. Paramètre de sécurité Additionnelle :

Pour restreindre L'accès au serveur uniquement avec les identifiants fournis, il faut ouvrir le fichier :

nano /etc/ssh/sshd_config

Ensuite ajouter la ligne suivante à ce fichier :

AllowUsers laplateforme



```
GNU nano 7.2 /etc/ssh/sshd_config
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /run/ssh.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

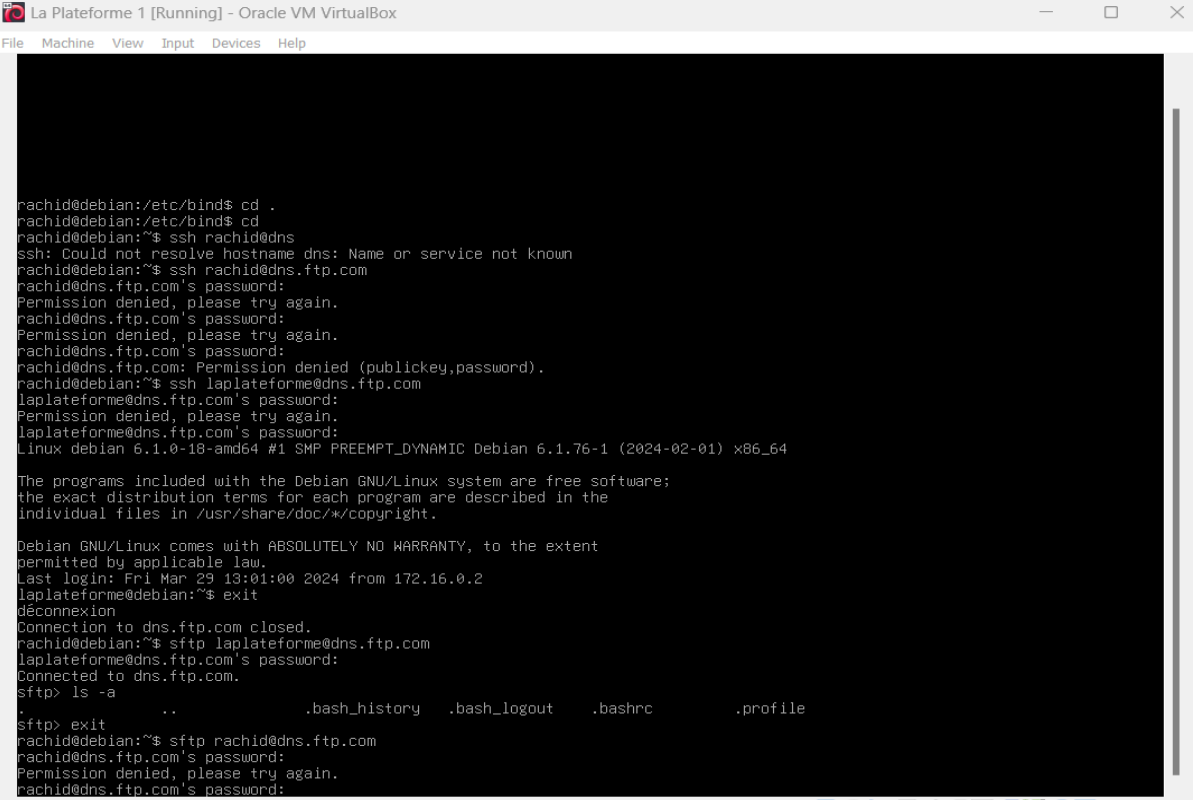
# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem sftp /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#    X11Forwarding no
#    AllowTcpForwarding no
#    PermitTTY no
#    ForceCommand cvs server

AllowUsers laplateforme
```

Nous avons essayé de nous connecter au serveur avec un utilisateur autre que **laplateforme** et nous voyons bien que **l'accès y a été refusé**



```
La Plateforme 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

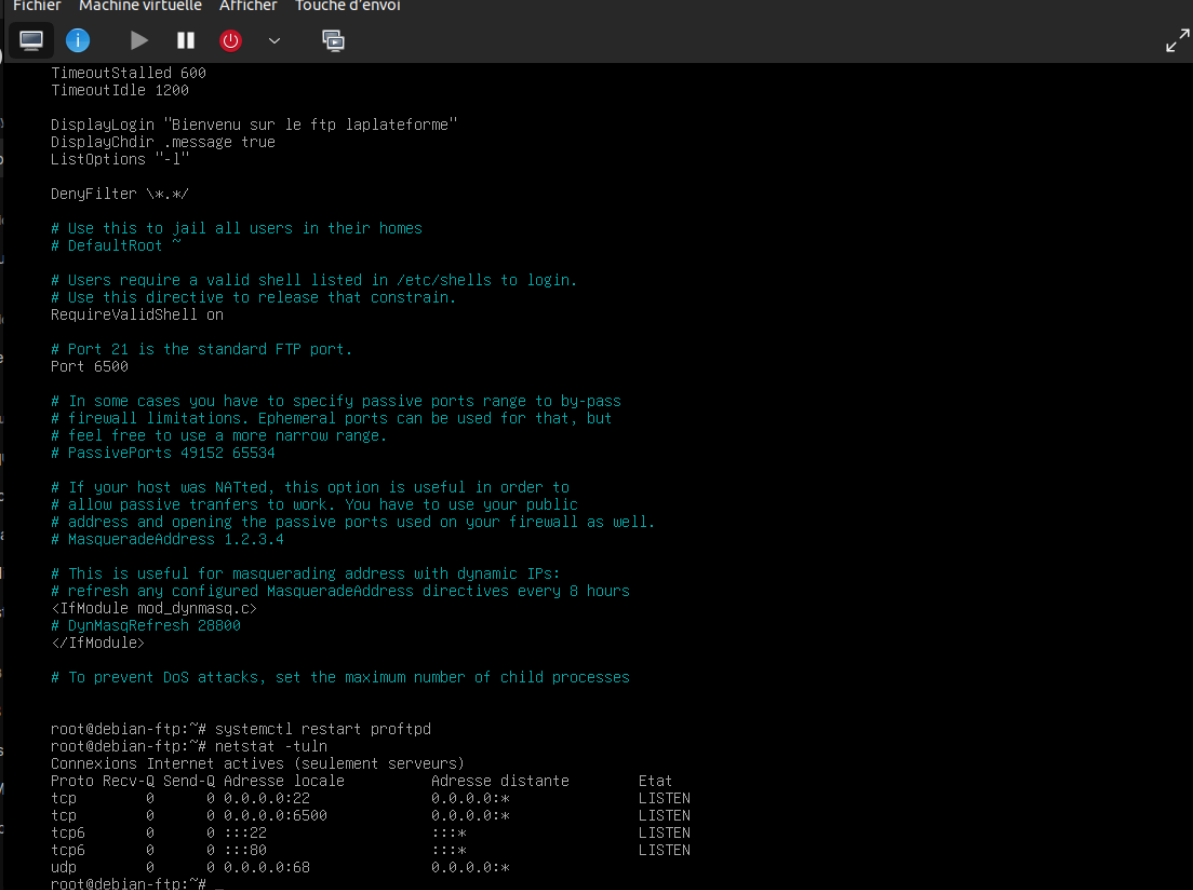
rachid@debian:/etc/bind$ cd .
rachid@debian:/etc/bind$ cd
rachid@debian:~$ ssh rachid@dns
ssh: Could not resolve hostname dns: Name or service not known
rachid@debian:~$ ssh rachid@dns.ftp.com
rachid@dns.ftp.com's password:
Permission denied, please try again.
rachid@dns.ftp.com's password:
Permission denied, please try again.
rachid@dns.ftp.com's password:
Permission denied (publickey,password).
rachid@debian:~$ ssh laplateforme@dns.ftp.com
laplateforme@dns.ftp.com's password:
Permission denied, please try again.
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: Fri Mar 29 13:01:00 2024 from 172.16.0.2
laplateforme@debian:~$ exit
déconnexion
Connection to dns.ftp.com closed.
rachid@debian:~$ sftp laplateforme@dns.ftp.com
laplateforme@dns.ftp.com's password:
Connected to dns.ftp.com.
sftp> ls -la
.                ..                .bash_history  .bash_logout  .bashrc        .profile
sftp> exit
rachid@debian:~$ sftp rachid@dns.ftp.com
rachid@dns.ftp.com's password:
Permission denied, please try again.
rachid@dns.ftp.com's password:
```

Nous avons modifié le port pour qu'il puisse se connecter sur le **port 6500**

A partir du fichier : **nano /etc/proftpd/proftpd.conf**



```
Fichier  Machine virtuelle  Afficher  Touche d'envoi

TimeoutStalled 600
TimeoutIdle 1200

DisplayLogin "Bienvenu sur le ftp laplateforme"
DisplayChdir .message true
ListOptions "-l"

DenyFilter \*.*/

# 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 6500

# 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

# If your host was NATted, this option is useful in order to
# allow passive tranfers to work. You have to use your public
# address and opening the passive ports used on your firewall as well.
# MasqueradeAddress 1.2.3.4

# This is useful for masquerading address with dynamic IPs:
# refresh any configured MasqueradeAddress directives every 8 hours
<IfModule mod_dynmasq.c>
# DynMasqRefresh 28800
</IfModule>

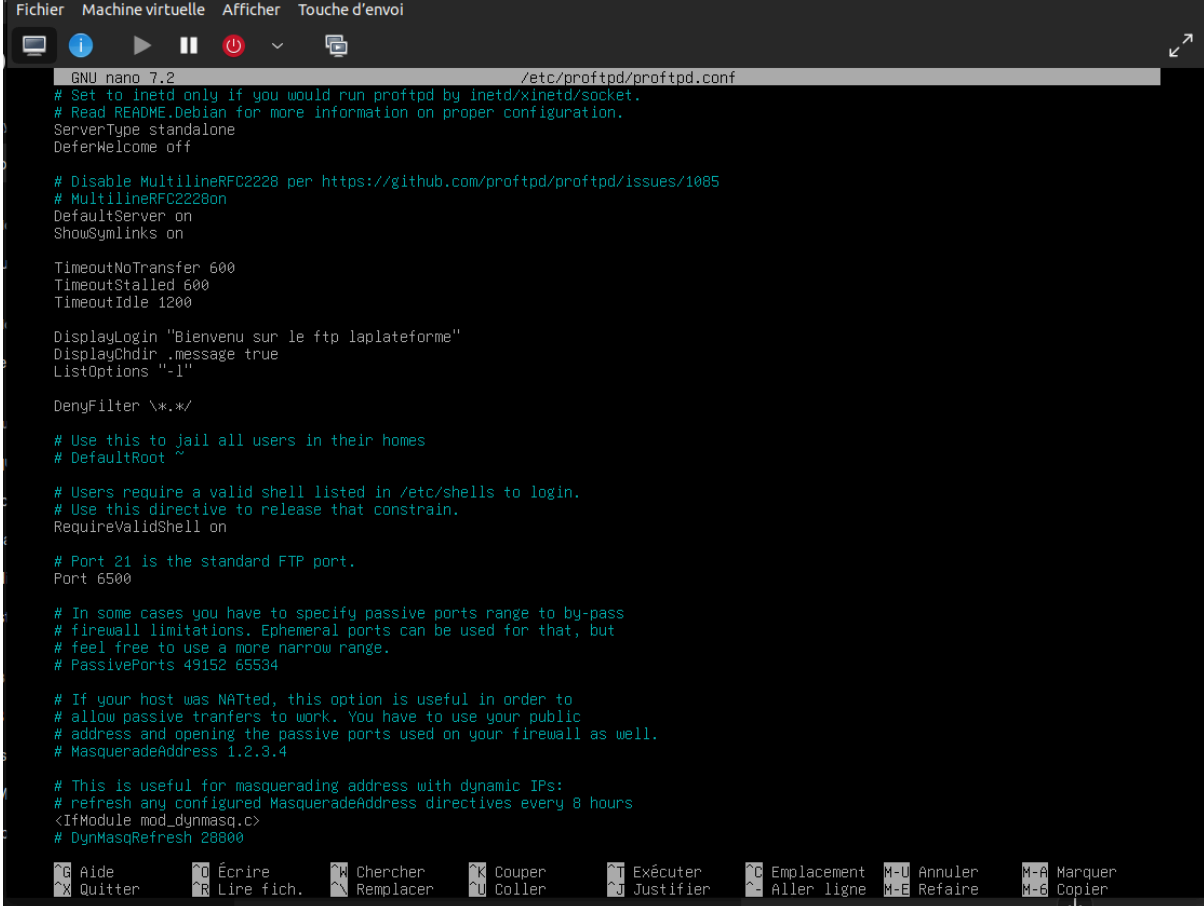
# To prevent DoS attacks, set the maximum number of child processes

root@debian-ftp:~# systemctl restart proftpd
root@debian-ftp:~# netstat -tuln
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale Adresse distante Etat
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:6500 0.0.0.0:* LISTEN
tcp6 0 0 :::22 :::* LISTEN
tcp6 0 0 :::80 :::* LISTEN
udp 0 0 0.0.0.0:68 0.0.0.0:*
```

Pour vérifier cette dernière modification nous avons utilisé la commande :

netstat -tuln et nous voyons bien que notre **port 6500** est bien actif.

Pour éviter toute connexion anonyme ou invité sur le serveur, nous avons ajouté la ligne : **RequireValidShell on** dans le fichier proftpd.conf en faisant: **nano /etc/proftpd/proftpd.conf** .



```
GNU nano 7.2 /etc/proftpd/proftpd.conf
# 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
# MultilineRFC2228on
DefaultServer on
ShowSymlinks on

TimeoutNoTransfer 600
TimeoutStalled 600
TimeoutIdle 1200

DisplayLogin "Bienvenu sur le ftp laplateforme"
DisplayChdir .message true
ListOptions "-l"

DenyFilter \*.*/

# 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 6500

# 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

# If your host was NATted, this option is useful in order to
# allow passive tranfers to work. You have to use your public
# address and opening the passive ports used on your firewall as well.
# MasqueradeAddress 1.2.3.4

# This is useful for masquerading address with dynamic IPs:
# refresh any configured MasqueradeAddress directives every 8 hours
<IfModule mod_dynmasq.c>
# DynMasqRefresh 28800

^G Aide      ^O Écrire
^X Quitter   ^R Lire fich.
^_ Chercher  ^K Couper
^~ Remplacer ^U Coller
^T Exécuter  ^G Emplacement
^J Justifier ^_ Aller ligne
^M-U Annuler ^M-A Marquer
^M-E Refaire ^M-6 Copier
```