

DHCP, DNS, FTP et SSH

1. Installer les machines virtuelles

- Sur l'ordinateur hôte, nous avons déjà téléchargé VMware Workstation.
- Les deux machines virtuelles Debian :
Debian_serveur et Debian_client

2. Mise à jour des systèmes

- Sur les deux machines virtuelles :
 - Pour mettre à jour la liste des paquets :
`apt-get update`
 - Pour installer les mises à jour disponibles :
`apt-get upgrade`
- Redémarrer les machines virtuelles.

3. Configuration du serveur DHCP

- Sur la première machine (serveur DHCP):
- Installer le paquet `isc-dhcp-server` :
`apt-get install isc-dhcp-server`
- Configurer le fichier `/etc/network/interfaces` :
Pour avoir une adresse IP du serveur DHCP statique

```
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
iface ens33 inet static
    address 172.16.0.1
    netmask 255.255.0.0
```

```
root@debianserver:~# _
```

- Configurer le fichier `/etc/dhcp/dhcpd.conf` :

```
GNU nano 7.2 /etc/dhcp/dhcpd.conf *
#}

# This is a very basic subnet declaration.
subnet 172.16.0.0 netmask 255.255.0.0 {
    range 172.16.0.100 172.16.0.150;
    option routers 172.16.0.1;
}
# range 10.254.239.10 10.254.239.20;
# 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 10.5.5.0 netmask 255.255.255.224 {
# range 10.5.5.26 10.5.5.30;
# option domain-name-servers ns1.internal.example.org;
# option domain-name "internal.example.org";
# option routers 10.5.5.1;
# option broadcast-address 10.5.5.31;
# default-lease-time 600;
# max-lease-time 7200;
#}

# Hosts which require special configuration options can be listed in

^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
```

- Configurer le fichier `/etc/default/isc-dhcp-server` pour indiquer l'interface réseau sur laquelle le serveur DHCP doit écouter : `ens33`

```
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=""
```

- Redémarrer le service dhcp :
systemctl restart isc-dhcp-server
On peut vérifier qu'il est actif en faisant la commande :
systemctl status isc-dhcp-server.

4. Installation du serveur FTP et SSH

Sur la deuxième machine (serveur FTP/SSH) Debian_server :

- Installer les paquets :
apt install proftpd-core proftpd-mod-crypto wget clamav clamav-daemon -y

```
Préparation du dépaquetage de .../3-libmemcachedutil2_1.1.4-1_amd64.deb ...
Dépaquetage de libmemcachedutil2:amd64 (1.1.4-1) ...
Sélection du paquet libpcre2-posix3:amd64 précédemment désélectionné.
Préparation du dépaquetage de .../4-libpcre2-posix3_10.42-1_amd64.deb ...
Dépaquetage de libpcre2-posix3:amd64 (10.42-1) ...
Sélection du paquet proftpd-core précédemment désélectionné.
Préparation du dépaquetage de .../5-proftpd-core_1.3.8+dfsg-4+deb12u3_amd64.deb ...
Dépaquetage de proftpd-core (1.3.8+dfsg-4+deb12u3) ...
Sélection du paquet proftpd-doc précédemment désélectionné.
Préparation du dépaquetage de .../6-proftpd-doc_1.3.8+dfsg-4+deb12u3_all.deb ...
Dépaquetage de proftpd-doc (1.3.8+dfsg-4+deb12u3) ...
Sélection du paquet ssh précédemment désélectionné.
Préparation du dépaquetage de .../7-ssh_1:9.2p1-2+deb12u2_all.deb ...
Dépaquetage de ssh (1:9.2p1-2+deb12u2) ...
Paramétrage de proftpd-doc (1.3.8+dfsg-4+deb12u3) ...
Paramétrage de ssh (1:9.2p1-2+deb12u2) ...
Paramétrage de libhashkit2:amd64 (1.1.4-1) ...
Paramétrage de libpcre2-posix3:amd64 (10.42-1) ...
Paramétrage de libmemcached11:amd64 (1.1.4-1) ...
Paramétrage de libhiredis0.14:amd64 (0.14.1-3) ...
Paramétrage de libmemcachedutil2:amd64 (1.1.4-1) ...
Paramétrage de proftpd-core (1.3.8+dfsg-4+deb12u3) ...
Ajout de l'utilisateur système « proftpd » (UID 102) ...
Ajout du nouvel utilisateur « proftpd » (UID 102) avec pour groupe d'appartenance « nogroup » ...
Pas de création du répertoire personnel « /run/proftpd ».
Ajout de l'utilisateur système « ftp » (UID 103) ...
Ajout du nouvel utilisateur « ftp » (UID 103) avec pour groupe d'appartenance « nogroup » ...
Création du répertoire personnel « /srv/ftp » ...
'/usr/share/proftpd/templates/welcome.msg' -> '/srv/ftp/welcome.msg.proftpd-new'
Server configured as standalone.
Created symlink /etc/systemd/system/multi-user.target.wants/proftpd.service → /lib/systemd/system/proftpd.service.
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.36-9+deb12u7) ...
root@debian:~# _
```

- Puis on arrête le service :
systemctl stop proftpd
- On crée une clé et un certificat SSL/TLS pour proftpd :
openssl req pour la gestion des requêtes d'un nouveau certificat qui sera auto-signé ; openssl req-new-x509.
On spécifie le chemin et le nom du fichier où la clé privée sera enregistrée ; /etc/proftpd/ssl/proftpd.key.pem
On définit la durée de validité du certificat pour 365 jours ; -days 365.
On indique à OpenSSL de ne pas crypter la clé privée avec un mot de passe ; -nodes

Enfin, on spécifie le chemin et le nom du fichier où le certificat sera enregistré ; -out /etc/proftpd/ssl/proftpd.cert.pem

- On modifie les permissions de lecture, écriture et exécution des fichiers /etc/proftpd/ssl avec la commande : `chmod 740 /etc/proftpd/ssl/*`
- On supprime les fichiers de configuration pour les remplacer :
`rm /etc/proftpd/proftpd.conf`
`rm /etc/proftpd/tls.conf`
`rm /etc/proftpd/modules.conf`

Fichier /etc/proftpd/proftpd.conf

```
# This file is used to manage DSO modules and features.
#
# This is the directory where DSO modules reside
ModulePath /usr/lib/proftpd

# Allow only user root to load and unload modules, but allow everyone
# to see which modules have been loaded
ModuleControlsACLs insmod,rmmod allow user root
ModuleControlsACLs lsmod allow user *

#This is required only if you need to set IdentLookups on
#LoadModule mod_ident.c

LoadModule mod_ctrls_admin.c

# Install proftpd-mod-crypto to use this module for TLS/SSL support.
#LoadModule mod_tls.c
# Even these modules depend on the previous one
#LoadModule mod_tls_fscache.c
#LoadModule mod_tls_shmcache.c

# Install one of proftpd-mod-mysql, proftpd-mod-pgsql or any other
# SQL backend engine to use this module and the required backend.
# This module must be mandatory loaded before anyone of
# the existent SQL backends.
#LoadModule mod_sql.c

# Install proftpd-mod-ldap to use this for LDAP support.
#LoadModule mod_ldap.c
```

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

```

GNU nano 7.2 /etc/proftpd/modules.conf
LoadModule mod_quotatab_radius.c
# Install proftpd-mod-wrap module to use this
#LoadModule mod_wrap.c
LoadModule mod_rewrite.c
LoadModule mod_load.c
LoadModule mod_ban.c
LoadModule mod_wrap2.c
LoadModule mod_wrap2_file.c
# Install one of the previous SQL backends and decomment
# the previous mod_sql.c module to use this
#LoadModule mod_wrap2_sql.c
LoadModule mod_dynmasq.c
LoadModule mod_exec.c
LoadModule mod_shaper.c
LoadModule mod_ratio.c
LoadModule mod_site_misc.c

# Install proftpd-mod-crypto to use this module for SFTP support.
#LoadModule mod_sftp.c
#LoadModule mod_sftp_pam.c

# Install one of the previous SQL backends and decomment
# the previous mod_sql.c module to use this
#LoadModule mod_sftp_sql.c

LoadModule mod_facl.c
LoadModule mod_unique_id.c
LoadModule mod_copy.c
LoadModule mod_deflate.c
LoadModule mod_ifversion.c
LoadModule mod_memcache.c
# Install proftpd-mod-crypto to use this module for TLS/SSL support.
#LoadModule mod_tls_memcache.c

^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

```

Fichier /etc/proftpd/proftpd.conf

```
# Install proftpd-mod-ldap to use this for LDAP support.
#LoadModule mod_ldap.c

#
# 'SQLBackend mysql' or 'SQLBackend postgres' (or any other valid backend) directives
# are required to have SQL authorization working. You can also comment out the
# unused module here, in alternative.
#

# Install proftpd-mod-mysql and uncomment the previous
# mod_sql.c module to use this.
#LoadModule mod_sql_mysql.c

# Install proftpd-mod-pgsql and uncomment the previous
# mod_sql.c module to use this.
#LoadModule mod_sql_postgres.c

# Install proftpd-mod-sqlite and uncomment the previous
# mod_sql.c module to use this
#LoadModule mod_sql_sqlite.c

# Install proftpd-mod-odbc and uncomment the previous
# mod_sql.c module to use this
#LoadModule mod_sql_odbc.c

# Install one of the previous SQL backends and uncomment
# the previous mod_sql.c module to use this
#LoadModule mod_sql_passwd.c

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

fichier /etc/proftpd/proftpd.conf

- On configure le service ProFTPD pour qu'il démarre automatiquement au démarrage du système avec la commande :
systemctl enable proftpd

Fichier /etc/proftpd/proftpd.conf

```
<IfModule mod__tls.c>
TLSEngine                on
TLSLog                   /var/log/proftpd/tls.log
TLSProtocol               SSLv23

TLRSACertificateFile     /etc/proftpd/ssl/proftpd.cert.pem
TLRSACertificateKeyFile  /etc/proftpd/ssl/proftpd.key.pem
#
TLSVerifyClient          off
TLSRequired              on
#
</IfModule>
```

Fichier /etc/proftpd/tls.conf

```
Include /etc/proftpd/modules.conf
UseIPv6 off
```

```
<IfModule mod_ident.c>
  IdentLookups off
</IfModule>
```

```
ServerName "Debian-FTP"
ServerType standalone
DeferWelcome off
DefaultServer on
ShowSymlinks on
```

```
TimeoutNoTransfer 600
TimeoutStalled 600
TimeoutIdle 1200
```

```
DisplayLogin welcome.msg
DisplayChdir .message true
ListOptions "-l"
```

```
DenyFilter \*.*/
```

```
  DefaultRoot ~
  RequireValidShell off
Port 21
```

```
MaxInstances 30
```

```
User proftpd
Group nogroup
```

```
Umask 022 022
```

```
root@debian:/etc/proftpd#
```

Fichier /etc/proftpd/modules.com

•Configuration du serveur SSH :

- apt update
- apt install openssh-server

```
# <Anonymous ~ftp>
#   User ftp
#   Group nogroup
#   # We want clients to be able to login with "anonymous" as well as "ftp"
#   UserAlias anonymous ftp
#   # Cosmetic changes, all files belongs to ftp user
#   DirFakeUser on ftp
#   DirFakeGroup on ftp
#
#   RequireValidShell off
#
#   # Limit the maximum number of anonymous logins
MaxClients 1
#
#   # We want 'welcome.msg' displayed at login, and '.message' displayed
#   # in each newly chdir'd directory.

root@debian:~# systemctl restart proftpd
root@debian:~# apt update
Atteint :1 http://deb.debian.org/debian bookworm InRelease
Réception de :2 http://security.debian.org/debian-security bookworm-security InRelease [48,0 kB]
Réception de :3 http://deb.debian.org/debian bookworm-updates InRelease [55,4 kB]
103 ko réceptionnés en 1s (119 ko/s)
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.
root@debian:~# apt install openssh-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
openssh-server est déjà la version la plus récente (1:9.2p1-2+deb12u2).
openssh-server passé en « installé manuellement ».
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@debian:~# _
```

- Configurer le fichier `/etc/ssh/sshd_config` pour modifier les paramètres SSH (par exemple, le port).

```
GNU nano 7.2 /etc/ssh/sshd_config *
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
ForceCommand internal-sftp
# Example of overriding settings on a per-user basis

Ⓜ Aide      Ⓞ Écrire   Ⓜ Chercher  Ⓚ Couper    Ⓜ Exécuter  Ⓞ Emplacement Ⓜ Annuler
Ⓚ Quitter   Ⓞ Lire fich. Ⓚ Remplacer Ⓚ Coller    Ⓜ Justifier Ⓚ Aller ligne Ⓜ Refaire
```



```
GNU nano 7.2 /etc/proftpd/proftpd.conf
#
# # Limit WRITE everywhere in the anonymous chroot
# <Directory */
#   <Limit WRITE>
#     DenyAll
#   </Limit>
# </Directory>
#
# # Uncomment this if you're brave.
# # <Directory incoming>
# #   # Umask 022 is a good standard umask to prevent new files and dirs
# #   # (second parm) from being group and world writable.
# #   Umask 022 022
# #   <Limit READ WRITE>
# #     DenyAll
# #   </Limit>
# #   <Limit STOR>
# #     AllowAll
# #   </Limit>
# # </Directory>
#
# </Anonymous>

# Include other custom configuration files
# !! Please note, that this statement will read /all/ file from this subdir,
# i.e. backup files created by your editor, too !!!
# Eventually create file patterns like this: /etc/proftpd/conf.d/*.conf
#
Include /etc/proftpd/conf.d/
AuthUserFile /etc/proftpd/ftpd.passwd
AuthGroupFile /etc/proftpd/ftpd.group
AuthOrder mod_auth_file.c

root@debian:~#
```

- Configuration pour une seule session de connexion possible

On édite le fichier de configuration de ProFTPD /etc/proftpd/proftpd.conf

- A la ligne MaxInstances, on le définit à 1. Ainsi, il est programmé pour une seule session.
- On ajoute à ce fichier les lignes suivantes pour configurer l'authentification FTP avec les identifiants fournis :
AuthUserFile /etc/proftpd/ftpd.passwd
AuthGroupFile /etc/proftpd/ftpd.group
AuthOrder mod_auth_file.c
- On crée le fichier 'ftpd.passwd' avec les informations d'identification
htpasswd -cd /etc/proftpd/ftpd.passwd laplateforme
Le terminal nous invite à entrer le mot de passe « Marseille13 » et de le confirmer.
- On ajoute la commande suivante pour que le fichier 'ftpd.passwd' soit accessible en lecture pour proFTPD :
chmod 640 /etc/proftpd/ftpd.passwd
- On redémarre proFTPD pour appliquer les modifications :
service proftpd restart

```

# 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

# 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
# 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

root@debian:~# mkdir /home/laplateforme
root@debian:~# useradd -d /home/laplateforme -s /bin/false laplateforme
root@debian:~# passwd laplateforme
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
root@debian:~#

```

```

GNU nano 7.2                                ftpd.passwd *
laplateforme:Marseille13!

```

5. Installation du serveur DNS

Sur la première machine `Debian_server` (serveur DNS):

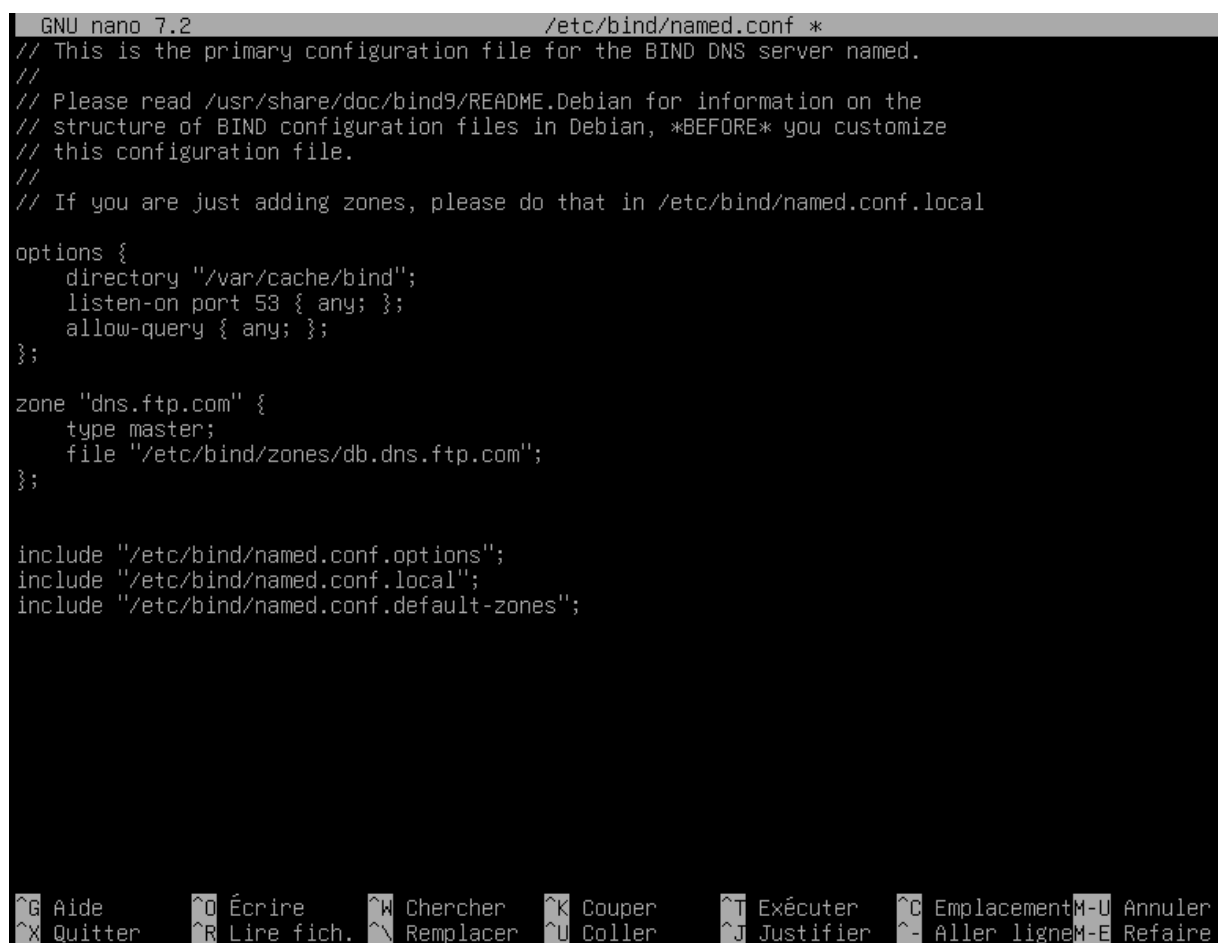
- Installer le paquet `bind9` :

`apt-get install bind9`

- Configurer le fichier `/etc/bind/named.conf` :

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

include "/etc/bind/zones.conf";
```



```
GNU nano 7.2 /etc/bind/named.conf *
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

options {
    directory "/var/cache/bind";
    listen-on port 53 { any; };
    allow-query { any; };
};

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

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";

^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
```

- Créer le fichier de zone /etc/bind/ftp.com :

\$TTL 1d

```
@      IN  A      172.16.0.1
www    IN  A      172.16.0.100
ftp    IN  CNAME  dns.ftp.com
```

```
GNU nano 7.2 /etc/bind/ftp.com *
$TTL 1d
@      IN      SOA      dns.ftp.com. admin.dns.ftp.com. (
                        2024031301 ; Serial
                        3600       ; Refresh
                        1800       ; Retry
                        604800     ; Expire
                        86400      ; Minimum TTL

                        IN      NS      dns.ftp.com.

dns    IN      A      172.16.0.1
www    IN      A      172.16.0.100
ftp    IN      CNAME  dns.ftp.com

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

- Redémarrer le service DNS :
systemctl restart bind9

6. Test de connexion au serveur SFTP

Sur la deuxième machine virtuelle (client FTP/SSH):

.Utiliser la commande `sftp` pour se connecter au serveur SFTP en utilisant l'adresse "`dns.ftp.com`" et les identifiants fournis (laplateforme et Marseille13!):

```
sftp laplateforme@dns.ftp.com
```

.Entrer le mot de passe Marseille13 !.

On fait la commande `ls` pour voir dans quel répertoire on se trouve.

```
ls
```

Pour télécharger un fichier du serveur vers notre machine locale, on utilise la commande `get` :

```
get remote_file local_file
```

Pour téléverser un fichier de notre machine locale vers le serveur, utiliser la commande `put` :

```
put local_file remote_file
```

Pour quitter la session SFTP, utiliser la commande `quit` :

```
quit
```

7. Paramètres de sécurité additionnels pour le serveur SFT

1. Restreindre l'accès au serveur uniquement avec les identifiants fournis :

- **Modifier le fichier `/etc/proftpd/proftpd.conf` et ajouter dans la section `LimitPerUser` :**

```
LimitPerUser
  AuthType per-user
  RequireAuth yes
  AuthUserFile /etc/proftpd/ftpd.passwd
  AllowUser laplateforme
```

- **Créer le fichier `/etc/proftpd/ftpd.passwd` et ajouter l'utilisateur FTP avec son mot de passe haché :**

```
laplateforme:On peut générer un mot de passe haché en utilisant l'outil
htpasswd :
htpasswd -c /etc/proftpd/ftpd.passwd laplateforme
```

- **Redémarrer le service FTP :**

```
systemctl restart proftpd
```

2. Configurer le serveur pour fonctionner sur le port 6500 :

- **Modifier le fichier /etc/ssh/sshd_config et remplacer la ligne Port 22 par :**
Port 6500
- **Redémarrer le service SSH :**

```
sudo systemctl restart ssh
```

3. Éviter toute connexion anonyme ou invité sur le serveur :

- **Modifier le fichier /etc/proftpd/proftpd.conf et commenter les lignes suivantes :**
AllowAnonymous
AllowGuest
- **Redémarrer le service FTP :**
systemctl restart proftpd

Avec ces modifications, seul l'utilisateur "laplateforme" pourra se connecter au serveur SFTP en utilisant le mot de passe "Marseille13!" et le port 6500.

- **Mettre à jour régulièrement le logiciel du serveur.**
- **Utiliser un pare-feu pour restreindre l'accès au serveur uniquement aux adresses IP autorisées.**
- **Activer la journalisation des connexions SSH et FTP pour suivre les activités.**
- **Effectuer des audits de sécurité régulièrement pour identifier et corriger les vulnérabilités.**