

# FTP

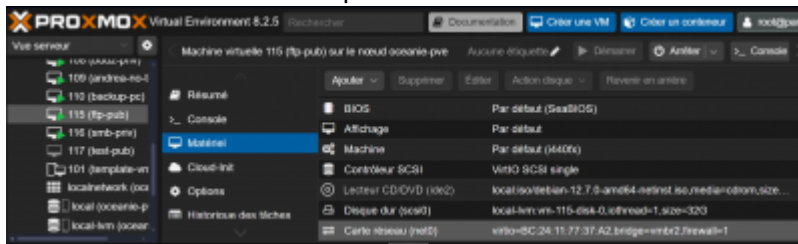
FTP (File Transfer Protocol) est un protocole réseau standard utilisé pour le transfert de fichiers d'un hôte à un autre sur un réseau TCP.

## Création du serveur

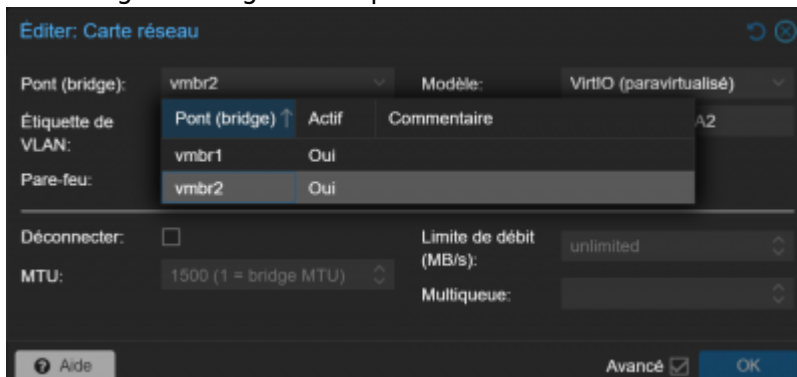
On se rend sur notre serveur Proxmox (10.31.208.1:8006) on clone notre template-vm.

On lui donne le nom 'ftp-pub'.

On se rend sur 'matériel' puis 'carte réseau' :



On change le bridge utilisé pour être sur le réseau DMZ :



Puis on copie l'adresse MAC.

On se rend sur notre serveur DHCP (10.31.208.67). On lance le programme de réservation d'IP :

```
/etc/dhcp/reserv.py
```

On rentre, le réseau concerné (LAN ou DMZ), le nom, et l'adresse MAC :

```
root@dhcp1-priv:~# /etc/dhcp/reserv.py
Quel est le reseau (LAN/DMZ) : DMZ
Nom d'hôte : ftp-pub
Adresse MAC : BC:24:11:77:37:A2
```

On peut maintenant se rendre sur notre serveur ftp.

On modifie comment la machine détermine son IP :

```
nano /etc/network/interfaces
```

```
root@ftp-pub:~# 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
auto ens18
iface ens18 inet dhcp
    #address 10.31.208.3/22
    #gateway 10.31.211.254
    # dns-* options are implemented by the resolvconf package, if installed
    #dns-nameservers 8.8.8.8
```

Puis, on change le nom d'hôte de la machine :

```
hostnamectl set-hostname ftp-pub
reboot
```

Enfin, nous devons ajouter deux interfaces réseaux virtuelles qu'on utilisera plus tard.  
Pour cela on se rend le fichier interfaces :

```
nano /etc/network/interfaces
```

On rajoute ceci :

```
auto ens18:0
iface ens18:0 inet static
    address 10.31.216.15/22

auto ens18:1
iface ens18:1 inet static
    address 10.31.216.16/22
```

```
systemctl restart networking
```

## Configuration Proftpd

Proftpd est un logiciel qui permet de configurer plusieurs serveurs FTP virtuels. Nous allons l'installer.

```
apt update
apt install proftpd
```

Une fois installé, on se rend dans le fichier de conf.

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

Dans ce fichier nous allons décommenter le bloc Anonymous, changer le répertoire où l'utilisateur sera emprisonné (/srv/ftp/pub) :

```
<Anonymous /srv/ftp/pub>
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 10

# We want 'welcome.msg' displayed at login, and '.message' displayed
# in each newly chdir'd directory.
DisplayLogin welcome.msg
DisplayChdir .message

# 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>
```

Puis dans ce même fichier il faut changer le DefaultRoot (là où sont emprisonné tout les utilisateurs par défaut). Nous voulons qu'ils soient enfermés dans le répertoire /home/ftpdocs/ :

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

Enfin nous devons inclure les VHosts donc on décommente cette ligne :

```
#
# This is used for other add-on modules
#
#Include /etc/proftpd/dnsbl.conf
#Include /etc/proftpd/geoip.conf
#Include /etc/proftpd/snmp.conf

#
# Useful to keep VirtualHost/VirtualRoot directives separated
#
Include /etc/proftpd/virtuals.conf
```

## Configuration VHosts

On se rend dans le fichier de conf des VirtualsHosts :

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

On y ajoute cela :

```
<VirtualHost 10.31.216.15>
ServerAdmin      ftpmaster@server.com
ServerName       "FTP intranet"
User             intra
Group            intra
```

```
<Limit LOGIN>
    Order Allow,Deny
    Allowgroup intra
    Deny from all
</Limit>
TransferLog                /var/log/proftpd/xfer/ftp.server.com
MaxLoginAttempts           3
RequireValidShell          no
DefaultRoot                /srv/ftp/intranet
AllowOverwrite              yes
</VirtualHost>

<VirtualHost 10.31.216.16>
ServerAdmin                 ftpmaster@server.com
ServerName                  "FTP extranet"
User                        extra
Group                       extra
<Limit LOGIN>
    Order Allow,Deny
    Allowgroup extra
    Deny from all
</Limit>

# Empeche l'utilisateur d'ecrire
<Limit WRITE>
    DenyAll
</Limit>

TransferLog                /var/log/proftpd/xfer/ftp.server.com
MaxLoginAttempts           3
RequireValidShell          no
DefaultRoot                /srv/ftp/extranet
AllowOverwrite              yes
</VirtualHost>
```

## Configuration des utilisateurs

Nous avons deux utilisateurs à créer : 'intra' et 'extra'.  
On tape la commande :

```
adduser intra
adduser extra
```

Un mot de passe pour chaque utilisateur nous sera demandé, par défaut on mettra le même nom que l'utilisateur concerné.

Nous devons maintenant créer les répertoires où seront enfermés les utilisateurs, bah oui parce que sinon c'est complètement débile, tu peux pas enfermer quelqu'un dans une prison dans une cellule qui n'existe pas VOUS VOYEZ BIEN QUE C'EST PAS POSSIBLE.

```
mkdir /srv/ftp/intranet
mkdir /srv/ftp/extranet
mkdir /home/ftpdocs
```

```
systemctl restart proftpd
```

## FQDN des machines

Lors des tests il sera plus clair de taper non pas les IPs mais les adresses sous forme :

'<ftp.oceanie.gsb.org>'.

Pour cela on se rend sur notre serveur DNS primaire et on lance le script d'associations d'IPs :

```
/etc/bind/dns.py
```

```
root@ns1-pub:~# /etc/bind/dns.py
Nom du sous-domaine : ftp
Adresse IP : 10.31.216.20|
```

On refait 2 fois la même chose mais en mettant 'ftpin' pour l'adresse '10.31.216.15' et 'ftpex' pour '10.31.216.16'.

## Tests

Pour tester notre configuration on va tout d'abord mettre 1 fichier texte dans les répertoires de chaque utilisateurs. Le contenu de ces fichiers n'est pas important, cela à juste pour but de se repérer et savoir si on est dans le bon répertoire lors des tests.

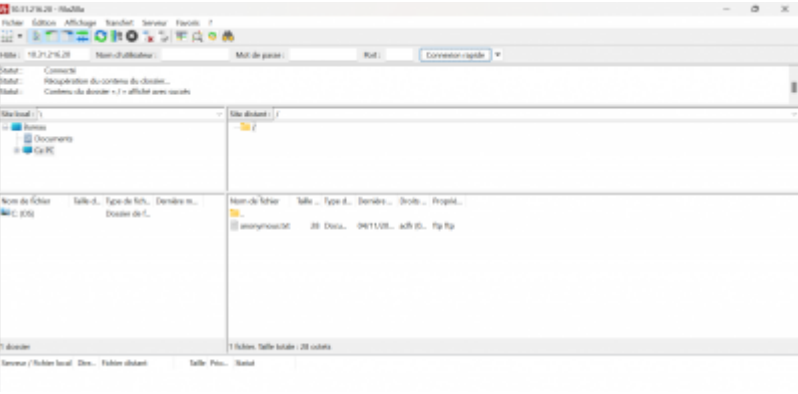
```
nano /srv/ftp/intranet/intranet.txt
nano /srv/ftp/extranet/extranet.txt
nano /home/ftdocs/std.txt
nano /srv/ftp/pub/anonymous.txt
```

Pour effectuer nos tests nous devons être sur une machine cliente, installer FileZilla Client et bien être sur le même réseau que notre serveur FTP. Pour utiliser les adresses FQDN il faut aussi mettre nos DNS dans la configuration de notre machine cliente.

On peut lancer FileZilla.

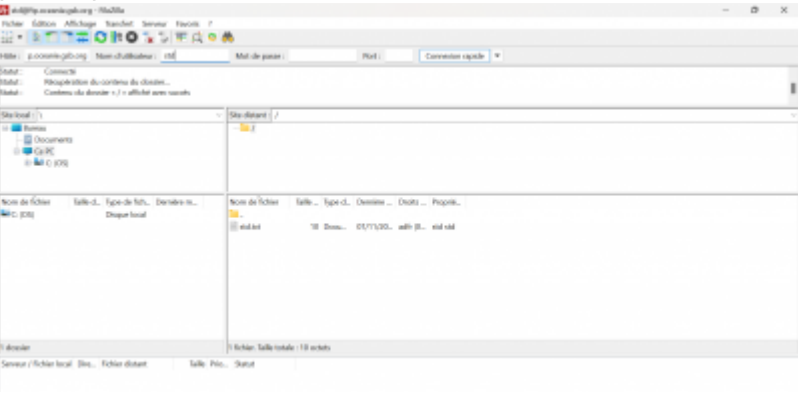
## Anonymous

Pour se connecter en anonymous sur le serveur il suffit d'entrer seulement l'adresse IP du serveur :



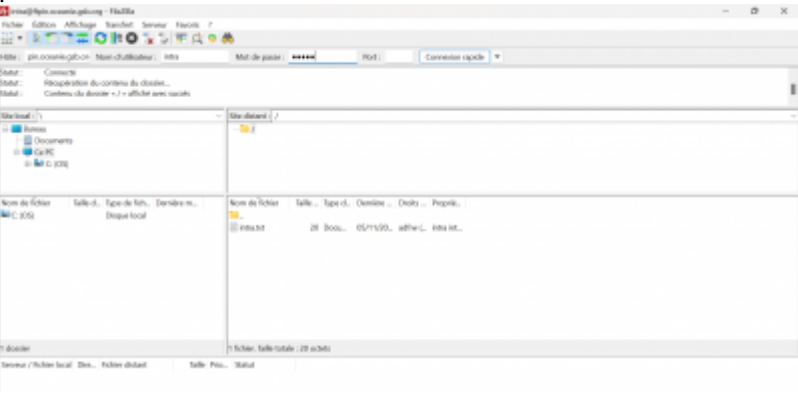
std

Pour se connecter au compte std il faut entrer '[ftp.oceanie.gsb.org](ftp://oceanie.gsb.org)', l'utilisateur 'std' et le mot de passe 'password' :



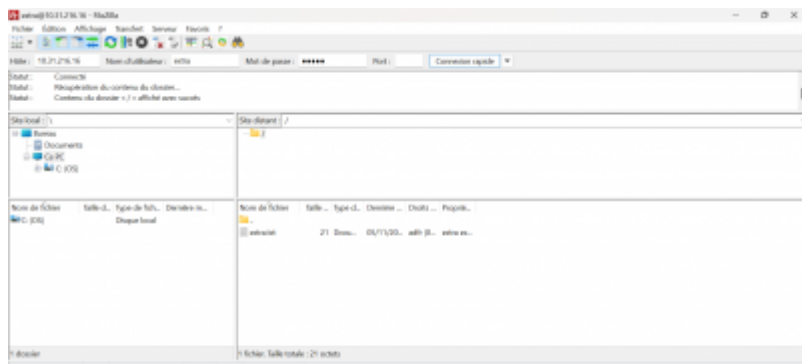
intra

Pour se connecter au compte intra il faut entrer '[ftp.pin.oceanie.gsb.org](ftp://pin.oceanie.gsb.org)', l'utilisateur 'intra' et le mot de passe 'intra' :



extra

Pour se connecter au compte extra il faut entrer '[ftp.pex.oceanie.gsb.org](ftp://pex.oceanie.gsb.org)', l'utilisateur 'extra' et le mot de passe 'extra' :



Pour le compte extra on doit s'assurer que l'écriture est impossible, pour cela plus tôt dans le virtualhost de xtra nous avons indiqué que l'écriture est impossible avec le bloc :

```
<Limit WRITE>
    Deny from all
</Limit>
```

## SAMBA

# Configuration du serveur Samba pour le réseau privé

### 1. Clonage de la VM sur proxmox

1. Assignez une adresse IP statique : **10.31.208.13** dans le DNS.

### 2. Installation du système d'exploitation

1. Installez un système Linux (ex. Ubuntu Server ou Debian) sur la VM.
2. Mettez à jour le système :

```
apt update
apt upgrade
```

### 3. Installation de Samba

1. Installez Samba avec la commande :

```
apt install samba
```

## 4. Configuration du nom d'hôte

1. Changez le nom d'hôte en **smb-priv** :

```
hostnamectl set-hostname smb-priv
```

## 5. Création des groupes et utilisateurs

1. Créez deux groupes : **admin** et **users** :

```
groupadd admin  
groupadd users
```

1. Créez deux utilisateurs, chacun associé à un groupe :

```
useradd -m -s /bin/bash admin1 -G admin  
useradd -m -s /bin/bash user1 -G users
```

1. Attribuez un mot de passe aux utilisateurs :

```
passwd admin1  
passwd user1
```

## 6. Création des répertoires de partage

1. Créez les répertoires partagés pour les groupes :

```
sudo mkdir -p /srv/admins  
sudo mkdir -p /srv/users
```

1. Assignez les permissions d'accès :

```
chown :admin /srv/admins  
chown :users /srv/users  
chmod 770 /srv/admins
```



```
chmod 770 /srv/users
```

## 7. Configuration de Samba

1. Ouvrez le fichier de configuration Samba :

```
nano /etc/samba/smb.conf
```

1. Ajoutez les sections de partage suivantes :

```
[admins]
path = /srv/admins
valid users = @admin
read only = no
browseable = yes
create mask = 0660
directory mask = 0770
force group = admin

[users]
path = /srv/users
valid users = @users
read only = no
browseable = yes
create mask = 0660
directory mask = 0770
force group = users
```

## 8. Ajout des utilisateurs dans Samba

1. Ajoutez les utilisateurs dans la base de données Samba :

```
smbpasswd -a admin1
smbpasswd -a user1
```

## 9. Redémarrage du service Samba

1. Redémarrez le service pour appliquer les changements :

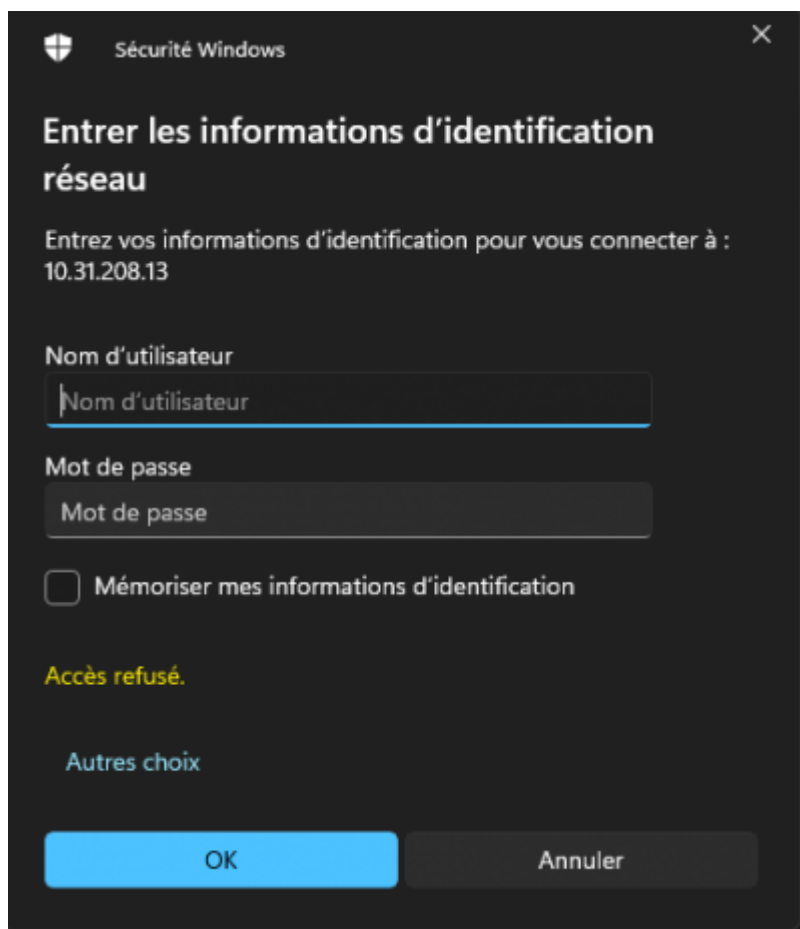
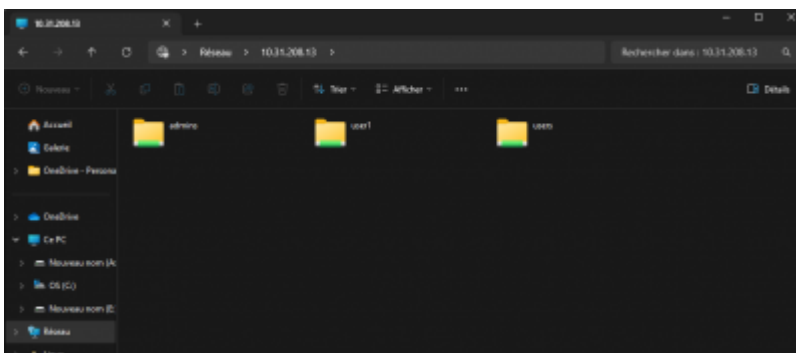
```
systemctl restart smbd
```

1. Vérifiez que le service est actif :

```
systemctl status smbd
```

## 10. Test d'accès depuis Windows

1. Sur une machine Windows, ouvrez l'Explorateur de fichiers.
2. Dans la barre d'adresse, tapez `\\10.31.208.13` et appuyez sur **Entrée**.
3. Entrez les identifiants Samba (ex. admin1 ou user1).
4. Vérifiez l'accès aux répertoires **admins** et **users** selon les permissions du groupe.



file:///C:/Users/USER/Downloads/sch%20r%C3%A9seau.drawio.html

From:

<https://sisr2.beaupeyrat.com/> - **Documentations SIO2 option SISR**

Permanent link:

<https://sisr2.beaupeyrat.com/doku.php?id=sisr2-oceanie:mission10>

Last update: **2024/11/15 09:41**

