

# Chapitre 5

## ftp et ssh

# Introduction

FTP (File Transfer Protocol - Protocole pour le Transfert de Fichiers) est un protocole TCP qui permet le téléchargement de fichiers à partir d'un serveur. Ce protocole n'est pas sécurisé du fait que l'envoi des données entre le client et le serveur n'est pas crypté. Pour l'opération inverse (chargement) et pour plus de sécurité, on peut utiliser **ssh** (Secure shell).

Il existe plusieurs serveurs ftp, **ftpd**, **proftpd**, **twoftpd**, ...

**ftp** permet l'accès de deux façons :

- **anonyme** : l'accès se fera au serveur via le nom d'utilisateur par défaut « anonymous » ou « ftp » ;
- **authentifié** : l'utilisateur doit disposé sur le système distant d'un compte. Cette façon est déconseillé du fait que la connexion au serveur n'est pas sécurisée.

# Serveur vsftpd

Dans cette section, nous allons utiliser **vsftpd** qui est facile à installer et à maintenir. Pour l'installer, tapez la commande :

```
sudo apt-get install vsftpd
```

# Configuration de la connexion anonyme

Par défaut, **vsftpd** n'est pas configuré pour autoriser la connexion anonyme. Pour l'autoriser, modifiez le fichier **/etc/vsftpd.conf** en changeant la ligne :

**anonymous\_enable=YES**

Par défaut, la valeur était **NO**. Après cette modification, il faut redémarrer le serveur ftp en tapant la commande :

```
sudo restart vsftpd
```

# Utilisateur ftp

Durant l'installation, l'utilisateur **ftp** avec le répertoire personnel **/srv/ftp** seront créés. Les fichiers qui seront visibles par connexion ftp anonyme doivent être mises dans ce répertoire.

La commande :

```
tail -n1 /etc/passwd
```

Fournira le résultat :

```
ftp:x:111:119:ftp daemon,, :/srv/ftp:/bin/false
```

## Configuration de la connexion authentifiée

Par défaut, **vsftpd** est configuré pour autoriser les utilisateurs authentifiés à télécharger des fichiers. Il n'autorise ni le chargement de fichiers ni la création de répertoires. Pour autoriser le chargement de fichiers et la création de répertoires, il faut éditer le fichier **/etc/vsftpd.conf** et enlever le commentaire à la ligne :

```
#write_enable=YES
```

pour devenir :

```
write_enable=YES
```

Après, il faut redémarrer le serveur **vsftpd** en tapant la commande :

```
sudo restart vsftpd
```

# Connexion à partir d'un client

On peut se connecter à un serveur ftp, soit à partir d'un :

- terminal ;
- navigateur.



## Connexion à partir d'un terminal

Pour se connecter à partir d'un terminal, il faut taper la commande :

```
ftp 192.168.56.101
```

Changez **192.168.56.101** par l'adresse ou le nom de votre serveur.

En validant la commande, vous obtiendrez :

```
Connected to 192.168.56.101.  
220 (vsFTPd 3.0.2)  
Name (192.168.56.101:lakhouaja): ftp  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

# Connexion

Pour fermer la connexion, tapez **quit** ou **exit** dans l'invite de commandes de ftp. Pour plus de commandes, tapez dans l'invite « help » ou « ? ». Pour l'aide sur une commande, tapez :

? commande

(par exemple : ftp> ? get). Vous pouvez aussi utiliser le manuel en ligne de ftp :

man ftp.

# Connexion

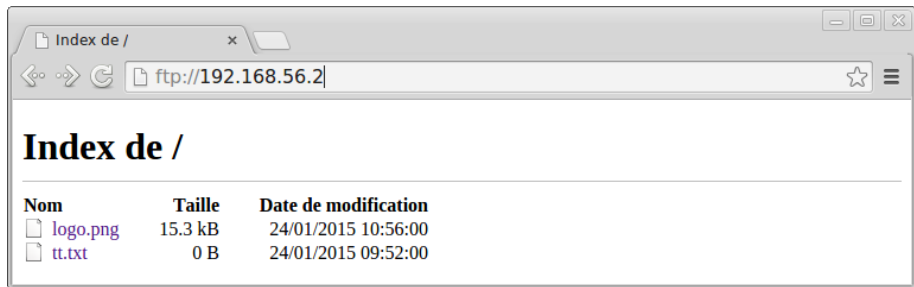
Pour une connexion :

- anonyme, tapez **ftp** ou **anonymous** après : de Name ; pour le mot de passe, il faut juste valider par la touche « Entrée » ;
- authentifié, tapez votre nom de connexion après : de Name et saisissez votre mot de passe.

# Connexion à partir d'un navigateur

Vous pouvez vous connecter au serveur **ftp** en utilisant un navigateur.  
Pour une connexion :

**anonyme** : tapez **ftp** **:://adresse** (par exemple :  
`ftp://192.168.56.101`);



# Connexion authentifié à partir d'un navigateur

Pour une connexion :

**authentifié**, tapez `ftp://login@adresse` (par exemple : `ftp://smi@192.168.56.101`) après validation, saisissez votre mot de passe.

# ssh

Comme nous l'avons signalé au début de ce chapitre, pour le transfert de fichiers en utilisant une connexion sécurisée, il faut utiliser **ssh** (Secure Shell). Sous Linux, le serveur **ssh** disponible de façon libre et gratuite s'appelle **OpenSSH**.

# Installation

Pour installer le client, tapez la commande

```
sudo apt-get install openssh-client
```

Pour installer le serveur, tapez la commande :

```
sudo apt-get install openssh-server
```

# Connexion à partir d'un client Linux

Pour se connecter à partir d'un client, tapez : `ssh login@adresse`.  
Par exemple :

```
ssh smi@192.168.56.101
```



## Utilisation de ssh comme ftp sécurisé

Pour utiliser le serveur **ssh** comme serveur **ftp** sécurisé, tapez la commande : `sftp login@adresse`. Par exemple :

```
sftp smi@192.168.56.101
```

Après saisi du mot de passe, vous obtiendrez l'invite de commandes :

```
sftp>
```

Pour fermer la connexion, tapez **quit**, **bye** ou **exit** dans l'invite de commandes. Pour plus de commandes, tapez dans l'invite « help » ou « ? ». Vous pouvez aussi utiliser le manuel en ligne de sftp :

```
man sftp.
```

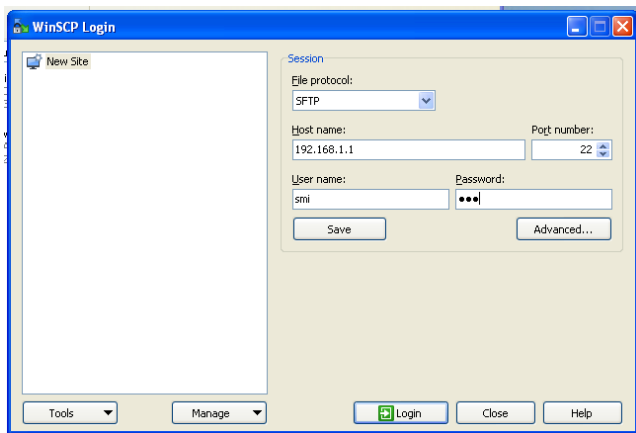
# Remarque

Si votre navigateur supporte le protocole **sftp**, vous pouvez taper par exemple :

```
sftp://smi@192.168.56.101/
```

# Connexion à partir d'un client Windows

Sous Windows il existe l'application **winscp** disponible en téléchargement à partir du site officiel <http://winscp.net>. Son interface graphique se présente comme suit :



# Connexion à partir d'un client Windows

The screenshot displays the WinSCP interface with two panes. The left pane shows the local Windows file system, and the right pane shows the remote Linux file system.

**Local File Explorer (Left Pane):**

Nom	Ext	Taille	Type	Date de modif...
..			Répertoire parent	29/01/201...
Application Data			Dossier de fichiers	15/01/201...
Bureau			Dossier de fichiers	29/01/201...
Cookies			Dossier de fichiers	23/04/201...
Downloads			Dossier de fichiers	20/03/201...
Favoris			Dossier de fichiers	19/03/201...
IECompatCache			Dossier de fichiers	20/03/201...
IETldCache			Dossier de fichiers	19/03/201...
Local Settings			Dossier de fichiers	15/10/200...
Menu Démarrer			Dossier de fichiers	15/10/200...
Mes documents			Dossier de fichiers	14/10/201...
Modèles			Dossier de fichiers	15/10/200...
PrivacIE			Dossier de fichiers	20/03/201...
Recent			Dossier de fichiers	23/11/201...
SendTo			Dossier de fichiers	29/01/201...
UserData			Dossier de fichiers	15/10/200...
Voisinage d'impression			Dossier de fichiers	15/10/200...
Voisinage réseau			Dossier de fichiers	13/12/201...
WINDOWS			Dossier de fichiers	08/03/201...

**Remote File Explorer (Right Pane):**

Nom	Ext	Taille	Date de modif...	Droits	Prop
..			17/01/2015 23:...	rwxt-xr-x	root
.cache			26/04/2014 05:...	rw-----	smi
.gfclient			26/04/2014 17:...	rwxt-rw-r-x	smi
glassfish-4.0			26/04/2014 17:...	rwxt-rw-r-x	smi
public_html			17/01/2015 15:...	rwxt-rw-r-x	smi
test			23/01/2015 15:...	rwxt-rw-r-x	smi
.bash_history		110	24/01/2015 12:...	rw-----	smi
.bash_logout		220	26/04/2014 05:...	rw-r--r--	smi
.bashrc		3 637	26/04/2014 05:...	rw-r--r--	smi
.profile		675	26/04/2014 05:...	rw-r--r--	smi
.viminfo		1 230	17/01/2015 15:...	rw-----	smi
ArabicDictionary.sql		50 715 420	26/04/2014 17:...	rw-r--r--	smi
hello-jaxws.war		3 915	26/04/2014 06:...	rwxt-rw-r-x	smi
logo.png		15 667	24/01/2015 10:...	rw-r--r--	smi
phpmyadmin_4%3a4.0...		6 969 346	26/04/2014 17:...	rw-r--r--	smi
webclient.war		8 136	26/04/2014 06:...	rwxt-rw-r-x	smi

**Status Bar:**

- Local: 0 B de 1 537 KB dans 0 de 22
- Remote: 0 B de 56 365 KB dans 0 de 15
- Keyboard shortcuts: F2 Renommer, F4 Editer, F5 Copier, F6 Déplacer, F7 Créer un répertoire, F8 Effacer, F9 Propriétés, F10 Quitter
- Transfer mode: SFTP-3
- Time: 0:01:49

## Copie vers le serveur

Pour copier un fichier ou un répertoire dans le serveur ssh, vous pouvez utiliser la commande **scp** (analogue à la commande **cp** de Linux). Son utilisation est comme suit :

```
scp fichier1 fichier2 ... smi@192.168.56.101:
```

Pour copier un répertoire, il faut simplement ajouter l'option `-r` :

```
scp -r Rep smi@192.168.56.101:
```

**Remarque** : il ne faut pas oublier `:`, sinon la copie se fera en local (utilisation de **cp**).

# Chapitre 6

## Partage de dossiers et d'imprimantes

# Introduction

Le partage de dossiers et d'imprimantes permet de :

- réduire le coût d'investissement ;
- mutualiser les ressources.

Pour partager des dossiers entre des machines Unix/Linux on utilise le protocole NFS (Network File System).

Pour partager des dossiers et des imprimantes entre des machines Unix/Linux et des machines Windows on utilise le service samba.

# Le protocole NFS



# Le protocole NFS

C'est un protocole qui fonctionne suivant le modèle client/serveur :

- un serveur met des dossiers à la disposition des machines sur le réseau suivant des droits d'accès.
- d'autres machines peuvent monter ces dossiers. Qui seront vus comme des dossiers locaux.

# Côté serveur

Il faut installer le serveur NFS, en tapant la commande :

```
# sudo apt-get install nfs-kernel-server
```

# Configuration

Le fichier de configuration est **/etc/exports**. On indique dans ce fichier la liste des répertoires à exporter (partagés) et les noms des machines autorisées à les utiliser.

## Exemple :

```
/home machinel(rw, sync, no_subtree_check)
/home *(ro, sync, no_subtree_check)
/TP machinel(rw, sync, no_root_squash, no_subtree_check)
/test *(ro, sync, no_subtree_check)
```

## Explication :

- **machine1** peut monter **/home** en lecture/écriture (**rw**) ;
- toutes les autres machines du réseau peuvent monter **/home** en lecture seulement (**ro**) ;
- **machine1** peut monter **/TP** en lecture/écriture (**rw**) ;
- toutes les machines du réseau peuvent monter **/test** en lecture seule (**ro**).

On peut utiliser des noms ou adresses IP pour les machines.

### Par exemple :

```
/home 192.10.1.1 (rw, sync, no_subtree_check)  
/TP smi.ump.ma (ro, sync, no_subtree_check)
```

# Configuration

Une fois le fichier **/etc/exports** bien configuré il faut redémarrer (ou relancer) **nfs** :

```
# sudo service nfs-kernel-server restart
```

ou bien

```
# sudo service nfs-kernel-server reload
```

# Affichage des répertoires partagés

La commande **exportfs** permet d'afficher les répertoires partagés.

## Exemple :

```
# exportfs
```

```
affichera
```

```
/etc          192.168.56.1  
/var          192.168.56.1  
/test        <world>
```

# Options

Principales options du fichier exports :

<b>Option</b>	<b>Signification</b>
<b>ro</b>	read-only (accès en lecture seule au répertoire exporté)
<b>rw</b>	read-write : le client accède au répertoire en lecture/écriture
<b>root_squash</b>	convertit les UID/GID root, en utilisateur anonyme. L'administrateur de la machine cliente ne peut pas modifier le contenu des répertoires et des fichiers.

## Options (suite)

Option	Signification
<b>no_root_squash</b>	désactive la conversion des UID/GID root.
<b>all_squash</b>	convertit tous les UID/GID en utilisateurs anonymes. Utile pour exporter avec NFS des répertoires publics.
<b>sync</b>	ne répondre aux requêtes qu'après l'exécution de tous les changements sur le support réel.
<b>no_subtree_check</b>	annule la vérification des sous-répertoires



# Remarque

Les options doivent être séparées par des virgules, SANS ESPACE.  
Pour plus d'options, veuillez consulter le manuel du fichier **exports**  
(**man exports**).

# Côté client

Pour pouvoir monter des répertoires, il faut installer la package **nfs-common** :

```
#sudo apt-get install nfs-common
```

En tant qu'administrateur du système, pour monter un répertoire distant, il faut utiliser la commande **mount** avec l'option **-t nfs**.

**Exemple :**

```
#mount -t nfs nom_machine:/home /test
```

ou

```
#mount -t nfs 192.168.56.2:/home /test
```

# Montage au démarrage

Pour monter un répertoire au démarrage du système, il suffit d'ajouter les renseignements nécessaire au fichier **/etc/fstab**

Par exemple :

```
nom_machine:/home /home nfs auto,rw,user 0 0
```

# NFS et la Sécurité

NFS n'est pas un protocole très sécurisé :

- l'authentification des clients repose uniquement sur le nom de domaine ou l'adresse IP ;
- l'identification des utilisateurs repose sur le « user id » sur le poste client => usurpation possible ;
- le transfert des données est non crypté ;
- utilisation recommandée en intranet isolé, protégé de l'internet par un Firewall.

# Le protocole SAMBA

# Installation

Samba peut être utilisé pour partager des dossiers et des imprimantes entre des machines Unix/Linux et des machines Windows.

En ligne de commandes, il suffit de taper la commande :

```
#sudo apt-get install samba
```

# Configuration

Le fichier principal de configuration de samba est :  
**/etc/samba/smb.conf.**

Avant de modifier le fichier de configuration, il faut le sauvegarder par prudence (`cp smb.conf smb.conf.old`).

Ce fichier est organisé en sections. L'administrateur **root** peut éditer, modifier et ajouter des sections, pour définir de nouvelles ressources à partager.

# Section

Une section commence par un mot entre crochets et se termine lorsqu'une autre section commence.

## **Exemple de sections :**

```
[global]
```

```
#ensemble de directives
```

```
[homes]
```

```
#ensemble de directives
```



## Remarque :

D'une façon générale, les permissions de partage définies dans les sections ne peuvent pas dépasser les permissions des fichiers du serveur hôte.

Pour plus d'informations concernant le fichier `smb.conf`, veuillez consulter le manuel en ligne :

```
man smb.conf
```

# Vérification des changements

L'outil **testparm**, permet de tester la syntaxe du fichier de configuration et de détecter les erreurs. Il est recommandé de le lancer systématiquement lors de la modification de **smb.conf**.

# Activation des changements

A chaque changement effectué dans **smb.conf**, il faut relancer les démons **smbd nmbd**. Commande :

```
#service smbd restart
```

suivie de :

```
#service nmbd restart
```

# Les principaux paramètres de smb.conf

paramètre	valeur par défaut	Description
path =		chemin du répertoire à partager
comment =		texte visible dans le voisinage réseau client
guest ok = yes no	no	permettre l'accès sans authentification
valid users =	tous	liste des utilisateurs autorisés à se connecter à la ressource
printable = true false	false	partage d'un service d'impression et non d'un répertoire.
writable = yes no	no	permet ou non l'écriture sur le répertoire, contraire de read only

# Les principaux paramètres de smb.conf

paramètre	valeur par défaut	Description
browseable =	yes	visibilité du partage par tous, même les utilisateurs non autorisés
create mask =	0744	droits maxi accordés à un fichier créé dans la ressource ces droits seront en intersection (and) avec les droits Linux (umask)
directory mask =	0755	droits maxi accordés à un répertoire créé dans la ressource ces droits seront en intersection (and) avec les droits Linux (umask)

# Commande umask

L'umask permet d'attribuer des permissions aux fichiers et répertoires créés par l'utilisateur. Il se présente sous la forme de 4 chiffres. La valeur par défaut de l'umask est 0022. Pour obtenir les permissions qui seront utilisées, il faut appliquer la règle suivante :

- pour les fichiers, il faut soustraire le umask de 666.  
Par exemple  $666 - 0022 = 644$  ce qui donne les droits  
**rw-r--r--**
- pour les répertoires, il faut soustraire le umask de 777.  
Par exemple  $777 - 0022 = 755$  ce qui donne les droits  
**rwxr-xr-x**

## Commande umask (suite)

Si l'utilisateur veut que les nouveaux fichiers soient créés avec les droits **rw-----** et que les nouveaux répertoires soient créés avec les droits **rw-x-----**, il doit utiliser le masque **0077**. Pour cela, il doit taper la commande :

```
umask 0077
```

ou tout simplement :

```
umask 77
```

### Remarque

**umask** accepte les symboles (r, w et x) comme **chmod**

**umask 77** peut être utilisée comme suit :

```
umask u=rwx, g=, o=
```

## La section globale

```
[global]
# donner le meme nom de groupe de travail que celui
  des stations Windows (Voisinage reseau/
  identification)
workgroup = SMI

# restreindre par sécurité les sous-réseaux autorisés à se connecter
  au serveur
# ici on se limite aux adresses réseau privé 192.168.1.0 et à
  l'interface "loopback"
hosts allow = 192.168.1.    127.

# on peut exclure des machines de l'accès au réseau
hosts allow = 192.168.1.    EXCEPT 192.168.1.125

# d'autres possibilités existent : voir le manuel man smb
```



# Le répertoire personnel

[homes]

#accès au répertoire personnel de chaque utilisateur.

#la valeur du champ "comment" apparaîtra dans le voisinage réseau

#inutile pour cette section de préciser le path, c'est celui de  
l'utilisateur, en fait /home/%u

browsable = no

writable = yes

create mode = 0700

## Rendre un répertoire public en lecture seule

Pour rendre un répertoire accessible par tous le monde, il faut tout d'abord le créer ou vérifier qu'il existe.

```
# mkdir /home/partage
```

```
ls -ld /home/partage
```

doit renvoyer les droits par défaut `drwxr-xr-x`, sinon il faut les changer en tapant la commande :

```
chmod 755 /home/partage
```

ou son équivalent

```
chmod u=rwx,go=rx /home/partage
```

pour y ajouter les permissions d'accès et de lecture pour tous.

# Rendre un répertoire public en lecture seule

Ensuite, il faut ajouter une nouvelle section « **[partage]** » comme suit :

```
[partage]  
path = /home/partage  
browsable = yes  
writable = no  
guest ok = yes
```

## Rendre un répertoire public en lecture et écriture

Si on veut rendre ce répertoire partagé en écriture aussi, il faut modifier les droits d'accès du répertoire et modifier la section [partage] :

```
chmod 777 /home/partage
```

```
[partage]  
path = /home/partage  
browsable = yes  
writable = yes  
guest ok = yes  
create mode = 0755
```

# Utilitaires SAMBA

- testparm** : permet la validation du fichier de configuration de Samba.
- smbclient** : client Linux/Unix similaire à FTP permettant de se connecter à des partages Samba.
- smbpasswd** : permet à un administrateur de modifier les mots de passe chiffrés utilisés par Samba.
- smbstatus** : dresse l'état des connexions aux partages d'un serveur Samba.

# Ajout d'un utilisateur samba

Pour permettre à un utilisateur de se connecter à son répertoire personnel à partir d'autres machines, il faut l'ajouter en tant qu'utilisateur samba en tapant la commande suivante :

**smbpasswd -a utilisateur**

Par exemple :

**smbpasswd -a smi**

## Problème de connexion avec Windwos

Sous Windows, si on se connecte avec un utilisateur 1 (par exemple **smi**) et on veut se connecter avec un autre utilisateur (par exemple **sma**), la connexion ne réussisse pas. Pour cela, il faut supprimer la connexion à l'utilisateur 1, en tapant la commande (sous un invite de commande) :

```
net use \\nom-partage\utilisateur /delete
```

Par exemple :

```
net use \\Ubuntu\smi /delete
```

Ou **Ubuntu** est le nom de partage et **smi** est le nom de l'utilisateur déjà connecté.

## Connexion à partir d'un client Linux

Pour se connecter à partir d'un client Linux en utilisant la commande **smbclient**, il faut taper la commande

```
smbclient //nom-machine/repertoire
```

Par exemple :

```
smbclient //192.168.56.2/partage
```

Pour se connecter en utilisant le compte d'un utilisateur qui s'appelle **smi**, il faut taper la commande :

```
smbclient //192.168.56.2/smi -U smi
```

ensuite, on saisit le mot de passe.



## Connexion à partir d'un client Linux

On peut utiliser la commande **mount** pour monter un répertoire partagé (fonctionne sous root) :

```
mount -o username=smi //192.168.56.2/smi Rep
```

Ou **Rep** est le répertoire de montage.