TP5 Chapitre 5 – Serveur Debian DS2 : installation du service FTP

2. Installation et configuration du service FTP

2.1 Configuration dans le cadre d'une connexion anonyme

- Installez le paquetage sur le serveur DS2 à l'aide de la commande apt install vsftpd :

```
root@DS2: ~#apt install vsftpd
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  vsftpd
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 153 ko dans les archives.
Après cette opération, 357 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://deb.debian.org/debian buster/main amd64 vsftpd amd64 3.0.3-12 [153 kB]
153 ko réceptionnés en 0s (794 ko/s)
Préconfiguration des paquets...
Sélection du paquet vsftpd précédemment désélectionné.
(Lecture de la base de données... 36150 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../vsftpd_3.0.3-12_amd64.deb ...
Dépaquetage de vsftpd (3.0.3-12) ...
Paramétrage de vsftpd (3.0.3-12) ...
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /lib/systemd/system/vsf
tpd.service.
[vsftpd.conf:1] Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empt
y → /run/vsftpd/empty; please update the tmpfiles.d/ drop-in file accordingly.
Traitement des actions différées (« triggers ») pour man-db (2.8.5-2) ...
Traitement des actions différées (« triggers ») pour systemd (241-7~deb10u6) ...
root@DS2: ~#_
```

- L'installation crée l'utilisateur ftp.

```
root@DS2: ~#id ftp
uid=107(ftp) gid=114(ftp) groupes=114(ftp)
root@DS2: ~#
```

- Modifiez le fichier de configuration /etc/vsftpd.conf afin que le serveur ftp fonctionne en mode standalone et que la connexion anonyme soit autorisée :

```
  GNU nano 3.2                                /etc/vsftpd.conf

# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
#
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=YES
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
#listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
anon_root=/var/ftp
```

- Relancez le service ftp avec la commande systemctl restart vsftpd :

```
root@DS2: ~#systemctl restart vsftpd
root@DS2: ~#
```

- Vérifiez l'état du service vsftpd :

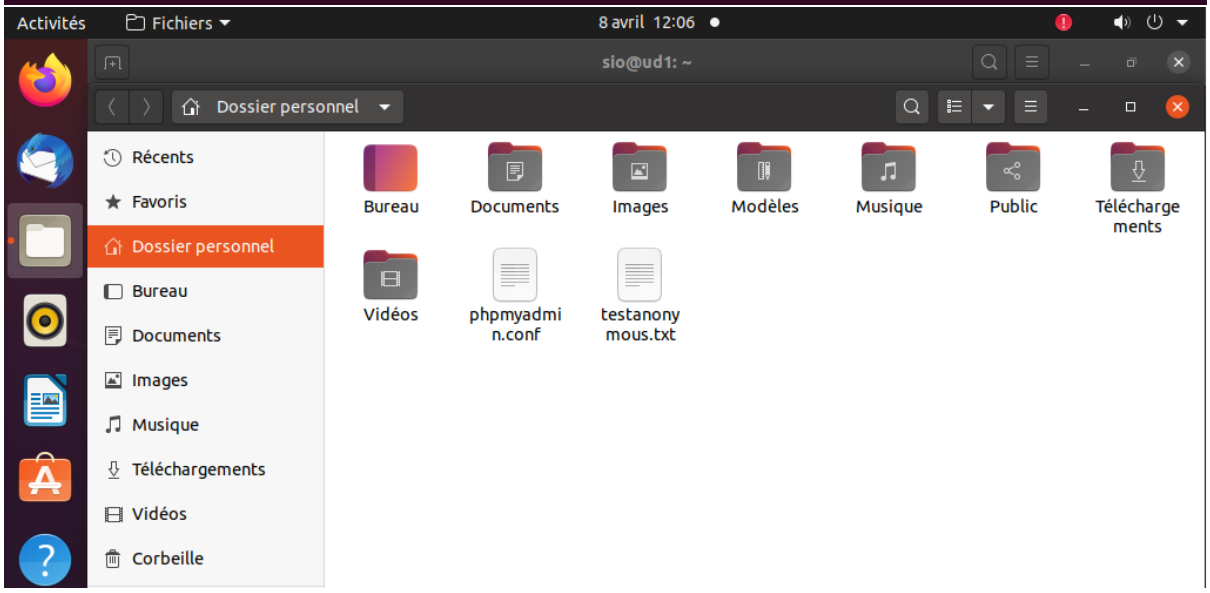
```
root@DS2: ~#systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2021-04-08 12:01:02 CEST; 9s ago
  Process: 5355 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
 Main PID: 5356 (vsftpd)
    Tasks: 1 (limit: 1149)
   Memory: 596.0K
   CGroup: /system.slice/vsftpd.service
           └─5356 /usr/sbin/vsftpd /etc/vsftpd.conf

avril 08 12:01:02 DS2 systemd[1]: Starting vsftpd FTP server...
avril 08 12:01:02 DS2 systemd[1]: Started vsftpd FTP server.
root@DS2: ~#_
```

- Créez-le répertoire /var/ftp/. La connexion anonyme y aura accès en lecture seule. Créez ensuite un fichier testanonymous.txt dans ce répertoire.

```
root@DS2: ~#mkdir /var/ftp/
root@DS2: ~#chmod 755 /var/ftp/
root@DS2: ~#chgrp ftp /var/ftp
root@DS2: ~#ls -ld /var/ftp
drwxr-xr-x 2 root ftp 4096 avril  8 12:01 /var/ftp
root@DS2: ~#touch /var/ftp/testanonymous.txt
root@DS2: ~#ls -l /var/ftp/
total 0
-rw-r--r-- 1 root root 0 avril  8 12:02 testanonymous.txt
root@DS2: ~#_
```

- Connectez-vous en ligne de commandes depuis UD1 en anonymous avec un mot de passe vide :

```
sio@ud1:~$ ftp 192.168.4.10
Connected to 192.168.4.10.
220 (vsFTPd 3.0.3)
Name (192.168.4.10:sio): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0               0 Apr 08 12:02 testanonymous.txt
226 Directory send OK.
ftp> get testanonymous.txt
local: testanonymous.txt remote: testanonymous.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for testanonymous.txt (0 bytes).
226 Transfer complete.
ftp>
```



- Modifiez le fichier /etc/vsftpd.conf afin de désactiver la connexion anonyme (directive anonymous_enable=NO).

```
 GNU nano 3.2                                /etc/vsftpd.conf

# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
#
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=YES
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
#listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#anon_root=/var/ftp
```

- Relancez le service avec la commande systemctl restart vsftpd et vérifiez que la connexion anonyme ne soit plus possible :

```
sio@ud1:~$ ftp 192.168.4.10
Connected to 192.168.4.10.
220 (vsFTPd 3.0.3)
Name (192.168.4.10:sio): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp>
```

2.2. Configuration dans le cadre d'une connexion authentifiée

- Créez depuis UD1 un fichier nommé fichier.txt. Ce fichier figurera, dans la machine UD1, dans le répertoire personnel de l'utilisateur sio (compte local de la machine UD1) :

```
sio@ud1:~$ touch fichier.txt
sio@ud1:~$
```

- Connectez-vous depuis UD1 au serveur ftp en ligne de commandes avec le login sio et le mot de passe Azerty0 (compte local de la machine DS2). Vous accédez à son répertoire personnel figurant sur DS2. Les droits d'écriture ne sont pas encore accordés. L'utilisateur sio ne peut pas B2-AP Chapitre 5 - Page 6 uploader un fichier depuis la machine cliente FTP vers son répertoire personnel sur le serveur FTP :

```
sio@ud1:~$ ftp 192.168.4.10
Connected to 192.168.4.10.
220 (vsFTPd 3.0.3)
Name (192.168.4.10:sio): sio
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put fichier.txt
local: fichier.txt remote: fichier.txt
200 PORT command successful. Consider using PASV.
550 Permission denied.
ftp>
```

- Depuis DS2, modifiez le fichier /etc/vsftpd.conf afin de décommenter la directive write_enable=YES :

```
  GNU nano 3.2                                /etc/vsftpd.conf

# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
#listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#anon_root=/var/ftp
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
```

- Uploadez le fichier créé depuis UD1 vers le répertoire personnel de l'utilisateur sio du serveur DS2 à l'aide de la commande put :

```
sio@ud1:~$ ftp 192.168.4.10
Connected to 192.168.4.10.
220 (vsFTPd 3.0.3)
Name (192.168.4.10:sio): sio
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put fichier.txt
local: fichier.txt remote: fichier.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp>
```

- Déplacez-vous dans l'arborescence de fichiers comme indiqué ci-dessous :

```
ftp> pwd
257 "/home/sio" is the current directory
ftp> ls -l
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-------    1 1000     1000            0 Apr 08 12:14 fichier.txt
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> pwd
257 "/home" is the current directory
ftp> cd ..
250 Directory successfully changed.
ftp> pwd
257 "/" is the current directory
ftp>
```

- Les directives du fichier /etc/vsftpd.conf à prendre en compte sont les suivantes :

```
  GNU nano 3.2                                /etc/vsftpd.conf

# predicted this attack and has always been safe, reporting the size of the
# raw file.
# ASCII mangling is a horrible feature of the protocol.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd.banned_emails
#
# You may restrict local users to their home directories.  See the FAQ for
# the possible risks in this before using chroot_local_user or
# chroot_list_enable below.
#chroot_local_user=YES
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd.chroot_list
#
```

- Créez à vide le fichier /etc/vsftpd.chroot_list :

```
root@DS2: ~#touch /etc/vsftpd.chroot_list
root@DS2: ~#_
```

- Créez un utilisateur nommé sio2 sur le serveur DS2 avec la commande adduser sio2 (mot de passe Azerty0) :

```
root@DS2: ~#adduser sio2
Ajout de l'utilisateur « sio2 » ...
Ajout du nouveau groupe « sio2 » (1001) ...
Ajout du nouvel utilisateur « sio2 » (1001) avec le groupe « sio2 » ...
Création du répertoire personnel « /home/sio2 »...
Copie des fichiers depuis « /etc/skel »...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully
Changing the user information for sio2
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Cette information est-elle correcte ? [O/n]o
root@DS2: ~#_
```

- Créez, en tant que sio2 (commande su sio2), le répertoire repweb dans le répertoire personnel de sio2 :

```
root@DS2: ~#su sio2
sio2@DS2:/root$ pwd
/root
sio2@DS2:/root$ cd /home/sio2
sio2@DS2:~$ mkdir repweb
sio2@DS2:~$ ls -l
total 4
drwxr-xr-x 2 sio2 sio2 4096 avril  8 12:20 repweb
sio2@DS2:~$ _
```

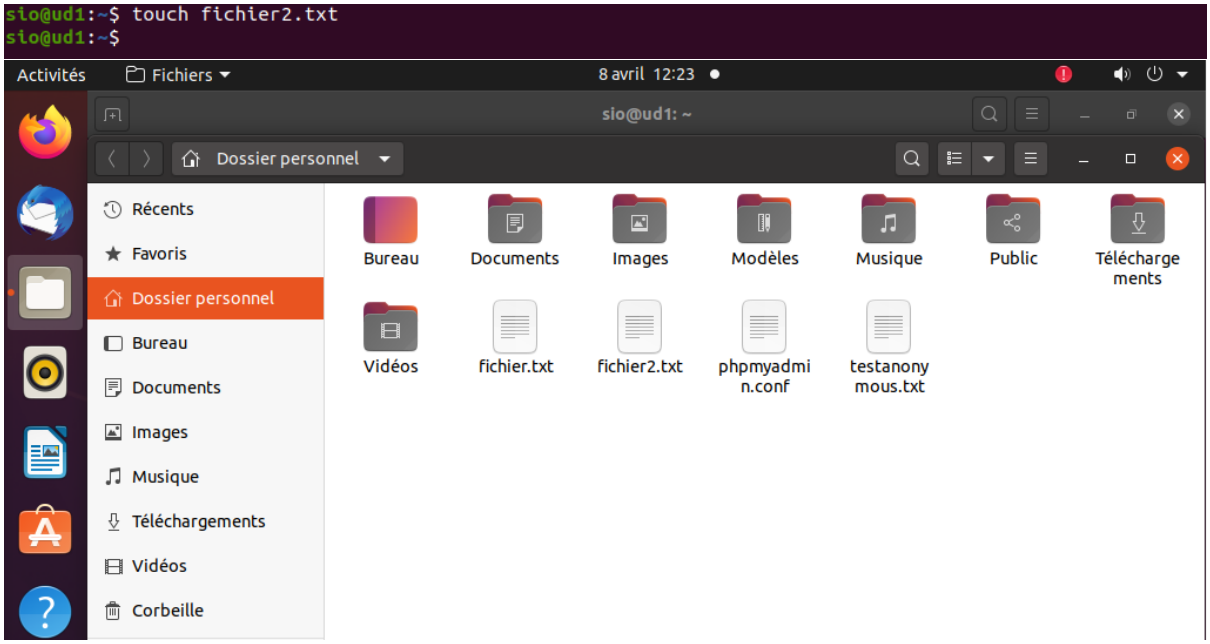
- Testez une connexion FTP en mode texte avec cet utilisateur depuis la machine UD1. Vous devez obtenir le message suivant de la part du serveur FTP :

```
sio@ud1:~$ ftp 192.168.4.10
Connected to 192.168.4.10.
220 (vsFTPd 3.0.3)
Name (192.168.4.10:sio): sio2
331 Please specify the password.
Password:
500 OOPS: vsftpd: refusing to run with writable root inside chroot()
Login failed.
ftp>
```

- En tant que root sur DS2, retirez à l'utilisateur sio2 le droit d'écriture sur la racine de son répertoire avec la commande chmod u-w /home/sio2 :

```
root@DS2: ~#chmod u-w /home/sio2
root@DS2: ~#ls -ld /home/sio2
dr-xr-xr-x 3 sio2 sio2 4096 avril  8 12:21 /home/sio2
root@DS2: ~#_
```

- Créez un fichier vide nommé fichier2.txt depuis la machine UD1 :



- Retentez une connexion FTP en mode texte avec l'utilisateur sio2 depuis la machine UD1. Celui-ci est confiné dans son répertoire personnel (environnement chrooté) :

```
sio@ud1:~$ ftp 192.168.4.10
Connected to 192.168.4.10.
220 (vsFTPd 3.0.3)
Name (192.168.4.10:sio): sio2
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/" is the current directory
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 1001     1001         4096 Apr 08 12:20 repweb
226 Directory send OK.
ftp> cd repweb
250 Directory successfully changed.
ftp> pwd
257 "/repweb" is the current directory
ftp> put fichier2.txt
local: fichier2.txt remote: fichier2.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-------    1 1001     1001            0 Apr 08 12:24 fichier2.txt
226 Directory send OK.
ftp> cd
(remote-directory) cd ..
550 Failed to change directory.
ftp>
```

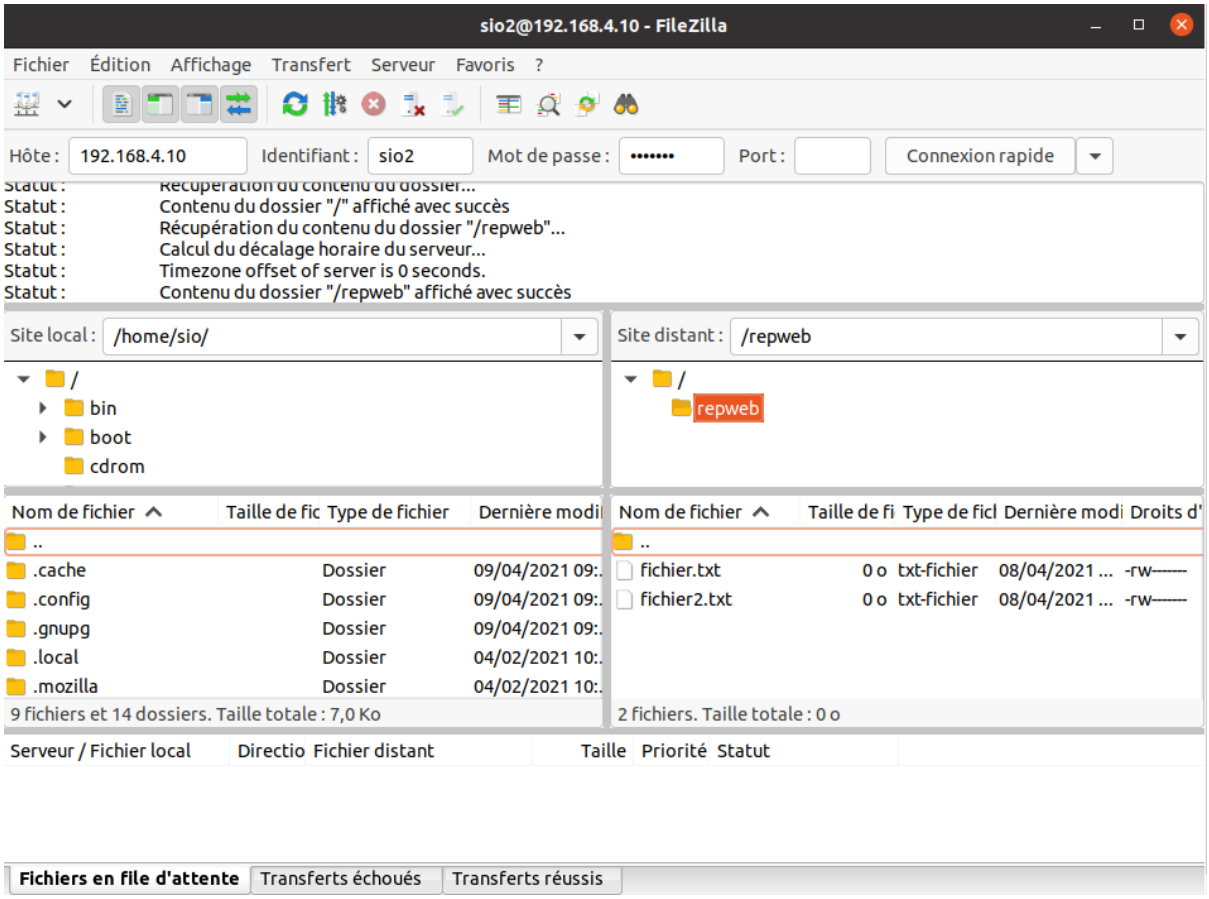
- Constatez que vous ne pouvez pas envoyer un fichier directement à la racine du répertoire personnel (commande cd pour retourner à la racine du répertoire personnel) :

```
ftp> put fichier.txt
local: fichier.txt remote: fichier.txt
200 PORT command successful. Consider using PASV.
553 Could not create file.
ftp>
```

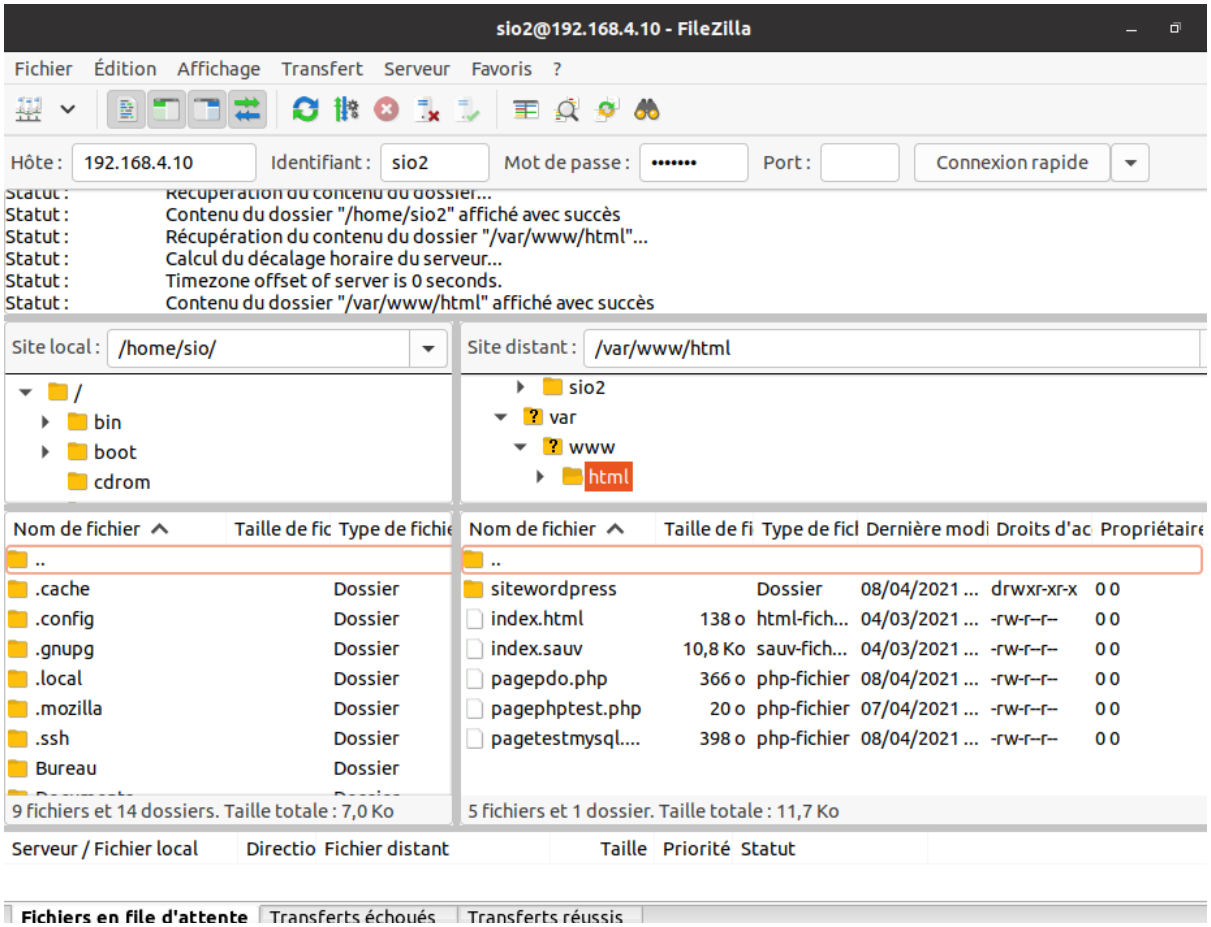
- Installez le client FTP graphique FileZilla (client FTP, SFTP, FTPS) sur la machine UD1 avec la commande sudo apt install filezilla :

```
sio@ud1:~$ sudo apt-get install filezilla
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  filezilla-common libfilezilla0 libpugixml1v5 libwxbase3.0-0v5 libwxgtk3.0-gtk3-0v5
Les NOUVEAUX paquets suivants seront installés :
  filezilla filezilla-common libfilezilla0 libpugixml1v5 libwxbase3.0-0v5 libwxgtk3.0-gtk3-0v5
0 mis à jour, 6 nouvellement installés, 0 à enlever et 390 non mis à jour.
Il est nécessaire de prendre 9 821 ko dans les archives.
Après cette opération, 40,6 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
```

- Testez une connexion FTP de l'utilisateur sio2 à son répertoire personnel :



- Inscrivez l'utilisateur sio2 dans le fichier /etc/vsftpd.chroot_list sur le serveur FTP :

```
 GNU nano 3.2                    /etc/vsftpd.chroot_list

sio2
```

- Vérifiez maintenant par une autre connexion FTP que l'utilisateur sio2 a dorénavant accès à tout le système de fichiers. Cela ne veut pas dire pour autant que sio2 puisse faire ce qu'il veut ; il est confronté aux droits rwx affectés respectivement à u, g et o sur les répertoires et fichiers.