

# Cómo instalar y configurar VSFTPD

## Ubuntu 18

Tutorial para saber cómo instalar y configurar VSFTPD usando SSL/TLS en Ubuntu 18 paso por paso.

La conexión FTP (File Transfer Protocol) ha sido usada hace mucho tiempo para la transferencia de archivos entre equipos de forma segura (relativamente) y completa, pero para nadie es un secreto que estamos en un mundo en línea donde la seguridad cada día es un tema más delicado y que toda la información que viaja en la red esta vulnerable a ser atacada o afectada por algún tipo de amenaza. Esto es algo delicado ya que FTP es muchas veces inseguro porque transmite datos junto con credenciales de usuario sin ningún tipo de cifrado.

Si somos usuarios frecuentes de FTP; trae una solución integral para añadir mejores niveles de seguridad en todo el proceso de transferencia de archivos usando este protocolo y es VSFTPD.

### Qué es VSFTPD

La utilidad VSFTPD se ha desarrollado como un servidor FTP con licencia GPL para sistemas UNIX, incluyendo Linux donde se destaca su seguridad, rapidez y estabilidad.

### Prestaciones y funcionalidades

Dentro de sus prestaciones y funcionalidades encontramos:

- Permite realizar configuraciones de IP virtual
- Podemos crear usuarios virtuales
- Operación autónoma o inetd
- Amplia configurabilidad por parte del usuario
- Gestiona de forma centralizada el ancho de banda
- Configuración de dirección IP por recurso o Per-source-IP
- Establece límites por fuente de IP
- Soporta IPv6
- Soporte de encriptación a través de la integración SSL

## Utilización VSFTPD

Actualmente VSFTPD es usado por muchos sitios de FTP donde se destacan:

- [ftp.redhat.com](http://ftp.redhat.com)
- [ftp.suse.com](http://ftp.suse.com)
- [ftp.debian.org](http://ftp.debian.org)
- [ftp.freebsd.org](http://ftp.freebsd.org)
- [ftp.gnu.org](http://ftp.gnu.org)
- [ftp.gnome.org](http://ftp.gnome.org)
- [ftp.kde.org](http://ftp.kde.org)
- [ftp.kernel.org](http://ftp.kernel.org)
- [rpmfind.net](http://rpmfind.net)
- [ftp.linux.org.uk](http://ftp.linux.org.uk)

VSFTPD emplea un diseño seguro para que todas las transmisiones siempre estén protegidas y así tengamos la seguridad de que no estarán expuestas a atacantes, para ello VSFTPD implementa y ejecuta:

- Todo el análisis y la gestión en datos de red remotos que son considerados potencialmente maliciosos se llevan a cabo en un proceso que se ejecuta como un usuario sin privilegios y este proceso se ejecuta en una chroot (), con el fin de garantizar que solo se pueda acceder al área de archivos ftp.
- Todas las operaciones con privilegios son controladas en un proceso primario privilegiado, el código para este proceso principal privilegiado es lo más pequeño posible por seguridad.
- VSFTPD-2.0.0 introduce soporte para SSL/TLS usando OpenSSL, así, todo el análisis de protocolo se realiza en un chroot (), ejecutándose en un entorno no privilegiado de usuario, con ello, tanto el protocolo OpenSSL preautenticado como el posterior a la autenticación estarán seguros.

Ahora veremos cómo instalar VSFTPD en Ubuntu 18.

# 1. Cómo instalar VSFTPD en Ubuntu 18

## Paso 1

Por defecto, VSFTPD está disponible en el repositorio de Ubuntu 18.04, de modo que para su instalación ejecutaremos lo siguiente:

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

```
solvetic@192:~$ sudo apt-get install vsftpd -y
[sudo] password for solvetic:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libwrap0 ssl-cert
Suggested packages:
  openssl-blacklist
The following NEW packages will be installed:
  libwrap0 ssl-cert vsftpd
0 upgraded, 3 newly installed, 0 to remove and 59 not upgraded.
Need to get 179 kB of archives.
After this operation, 505 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu bionic/main amd64 libwrap0 amd64 7.6.q-27 [46.3 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu bionic/main amd64 ssl-cert all 1.0.39 [17.0 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu bionic/main amd64 vsftpd amd64 3.0.3-9build1 [115 kB]
Fetched 179 kB in 1s (183 kB/s)
Preconfiguring packages ...
Selecting previously unselected package libwrap0:amd64.
(Reading database ... 86773 files and directories currently installed.)
Preparing to unpack .../libwrap0_7.6.q-27_amd64.deb ...
Unpacking libwrap0:amd64 (7.6.q-27) ...
Selecting previously unselected package ssl-cert.
Preparing to unpack .../ssl-cert_1.0.39_all.deb ...
Unpacking ssl-cert (1.0.39) ...
Selecting previously unselected package vsftpd.
Preparing to unpack .../vsftpd_3.0.3-9build1_amd64.deb ...
Unpacking vsftpd (3.0.3-9build1) ...
Processing triggers for ureadahead (0.100.0-20) ...
Setting up ssl-cert (1.0.39) ...
```

## Paso 2

Una vez que VSFTPD haya sido instalado, vamos a iniciar el servicio Vsftpd y habilitarlo en el arranque de Ubuntu 18:

```
sudo systemctl start vsftpd
sudo systemctl enable vsftpd
```



```
solvetic@192:~$ sudo systemctl start vsftpd
solvetic@192:~$ sudo systemctl enable vsftpd
Synchronizing state of vsftpd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable vsftpd
solvetic@192:~$ _
```



## 2. Creación de la estructura de directorio de VSFTPD en Ubuntu 18

### Paso 1

En primer lugar, vamos a crear el usuario para acceder a través de FTP, para ello ejecutamos lo siguiente:

```
sudo adduser vsftpd
```

Será necesario completar la información, si aplica, desplegada:

```
solvetic@192:~$ sudo adduser vsftpd
Adding user `vsftpd' ...
Adding new group `vsftpd' (1001) ...
Adding new user `vsftpd' (1001) with group `vsftpd' ...
Creating home directory `/home/vsftpd' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for vsftpd
Enter the new value, or press ENTER for the default
    Full Name []: Solvetic
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] Y
solvetic@192:~$ _
```



## Paso 2

Ahora, vamos a crear el directorio ftp y establecer la propiedad con el siguiente comando:

```
sudo mkdir /home/vsftpd/ftp
sudo chown nobody:nogroup /home/vsftpd/ftp
sudo chmod a-w /home/vsftpd/ftp
```

```
solvetic@192:/home$ sudo mkdir /home/vsftpd/ftp
solvetic@192:/home$ sudo chown nobody:nogroup /home/vsftpd/ftp
solvetic@192:/home$ sudo chmod a-u /home/vsftpd/ftp
solvetic@192:/home$
```



### Paso 3

El siguiente paso consiste en crear un directorio para cargar los archivos y se debe brindar propiedad al usuario de vsftpd así:

```
sudo mkdir /home/vsftpd/ftp/test
sudo chown vsftpd:vsftpd /home/vsftpd/ftp/test
```

```
solvetic@192:/home$ sudo mkdir /home/vsftpd/ftp/test
solvetic@192:/home$ sudo chown vsftpd:vsftpd /home/vsftpd/ftp/test
solvetic@192:/home$
```



### 3. Cómo configurar VSFTPD en Ubuntu 18

#### Paso 1

Ahora, vamos a llevar a cabo algunas configuraciones para el servidor FTP, en primer lugar, crearemos una copia de seguridad del archivo de configuración original en caso de que algo salga mal y así contar con la integridad del archivo original, para ello ejecutamos lo siguiente:

```
sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.bak
```

```
solvetic@192:/home$ sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.bak  
solvetic@192:/home$ _
```



## Paso 2

Accederemos al archivo de configuración usando el editor deseado:

```
sudo nano /etc/vsftpd.conf
```

Este será el archivo de configuración:

```
GNU nano 2.9.3 /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=NO
#
# 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
#
# 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
#
# [ Read 155 lines ]
^G Get Help      ^O Write Out    ^W Where Is    ^K Cut Text     ^J Justify     ^C Cur Pos     ^U Undo
^X Exit          ^R Read File    ^M Replace     ^U Uncut Text  ^I To Spell    ^G Go To Line  ^E Redo
```

### Paso 3

Allí añadiremos las siguientes líneas al final de este archivo:

```
listen=NO
listen_ipv6=YES
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
use_localtime=YES
xferlog_enable=YES
connect_from_port_20=YES
chroot_local_user=YES
secure_chroot_dir=/var/run/vsftpd/empty
pam_service_name=vsftpd
pasv_enable=Yes
pasv_min_port=10000
pasv_max_port=11000
user_sub_token=$USER
local_root=/home/$USER/ftp
```

```
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
```

```
GNU nano 2.9.3 /etc/vsftpd.conf Modified
pan_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO
#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES
listen=NO
listen_ipv6=YES
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
use_localtime=YES
xferlog_enable=YES
connect_from_port_20=YES
chroot_local_user=YES
secure_chroot_dir=/var/run/vsftpd/empty
pan_service_name=vsftpd
pasv_enable=YES
pasv_min_port=10000
pasv_max_port=11000
user_sub_token=$USER
local_root=/home/$USER/ftp
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO_
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos ^T-U Undo
^X Exit ^R Read File ^M Replace ^U Uncut Text ^I To Spell ^G Go To Line ^I-E Redo
```

#### Paso 4

Guardamos los cambios usando la combinación de teclas Ctrl + O y salimos del editor usando Ctrl + X. Ahora, vamos a agregar el usuario de vsftp al archivo /etc/vsftpd.userlist para permitir el acceso FTP:

```
sudo nano /etc/vsftpd.userlist
```

Allí añadimos el usuario creado para FTP:

```
GNU nano 2.9.3 /etc/vsftpd.userlist Modified
vsftpd_

[ New File ]
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    ^-U Undo
^X Exit      ^R Read File  ^_ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line ^-E Redo
```

#### Paso 5

Guardamos los cambios usando las teclas Ctrl + O y salimos usando Ctrl + X. Reiniciamos el servicio de VSFTPD para aplicar los cambios:

```
sudo systemctl restart vsftpd
```

## 4. Cómo acceder a VSFTPD en Ubuntu 18

#### Paso 1

Para acceder a VSFTPD iremos a algún navegador y usaremos la siguiente sintaxis:

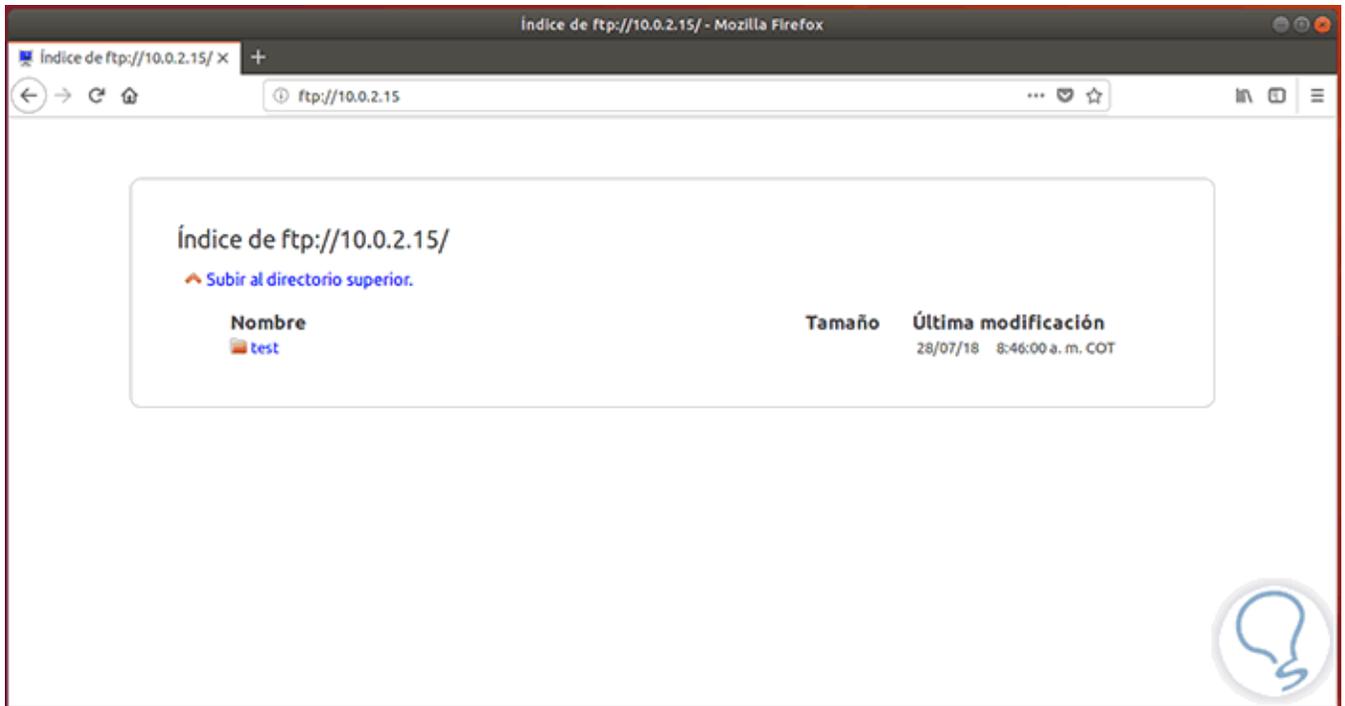
```
ftp://Direccion_IP
```

Al acceder al navegador ingresaremos el usuario y contraseña asignados:



Paso 2

Pulsamos en Aceptar y tendremos acceso a el servidor a través de FTP:



De este modo accedemos con los valores básicos de seguridad de FTP.

## 5. Cómo asegurar la conexión VSFTPD usando SSL/TLS

Para una mejor seguridad a la hora de transferir información, vamos a habilitar SSL / TLS con el fin de cifrar los datos transferidos a través de FTP.

### Paso 1

Para eso, se debe crear un certificado usando OpenSSL con el siguiente comando:

```
sudo mkdir /etc/cert
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/cert/vsftpd.pem -out /etc/cert/vsftpd.pem
```

```
solvetic@solvetic-Ubuntu: ~
Archivo Editar Ver Buscar Terminal Ayuda
solvetic@solvetic-Ubuntu:~$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:
2048 -keyout /etc/cert/vsftpd.pem -out /etc/cert/vsftpd.pem
Generating a 2048 bit RSA private key
.....
..+++
.+++
writing new private key to '/etc/cert/vsftpd.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Madrid
Locality Name (eg, city) []:Madrid
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Solvetic
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:Solvetic
Email Address []:solvetic@outlook.com
solvetic@solvetic-Ubuntu:~$
```

## Paso 2

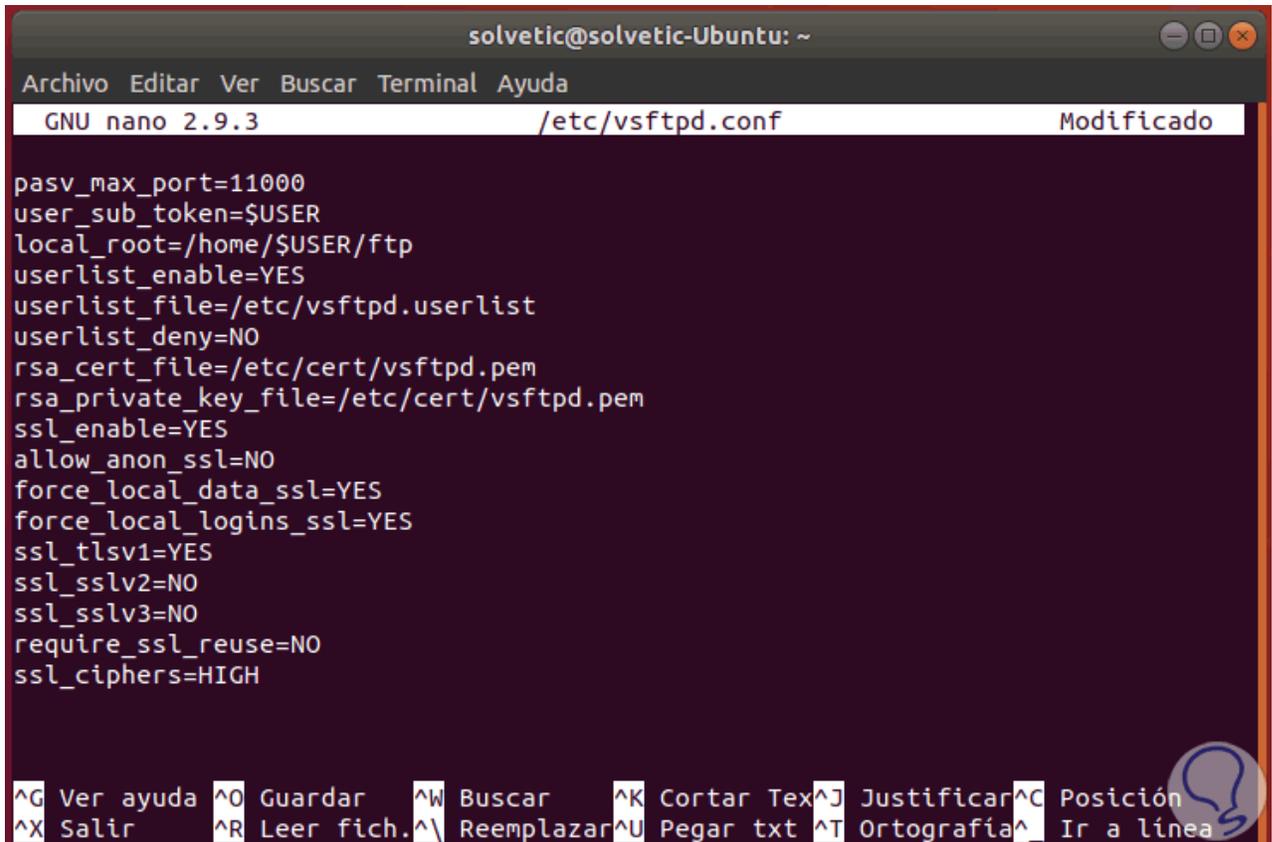
En este caso, cuando se crea el certificado se solicitan detalles como:

- Nombre
- Ciudad
- Pais
- Correo, etc.

Estos campos no son obligatorios de completar. Una vez realizado esto, vamos a realizar algunos cambios en el archivo vsftpd.conf usando el siguiente comando:

```
sudo nano /etc/vsftpd.conf
Allí agregaremos las siguientes líneas al final del archivo:
rsa_cert_file=/etc/cert/vsftpd.pem
rsa_private_key_file=/etc/cert/vsftpd.pem
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
```

```
ssl_sslv2=NO
ssl_sslv3=NO
require_ssl_reuse=NO
ssl_ciphers=HIGH
```



```
solvetic@solvetic-Ubuntu: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.9.3 /etc/vsftpd.conf Modificado
pasv_max_port=11000
user_sub_token=$USER
local_root=/home/$USER/ftp
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
rsa_cert_file=/etc/cert/vsftpd.pem
rsa_private_key_file=/etc/cert/vsftpd.pem
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
require_ssl_reuse=NO
ssl_ciphers=HIGH
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Text ^J Justificar ^C Posición
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea
```

Guardamos los cambios usando las teclas Ctrl + O y salimos del editor usando las teclas Ctrl + X.

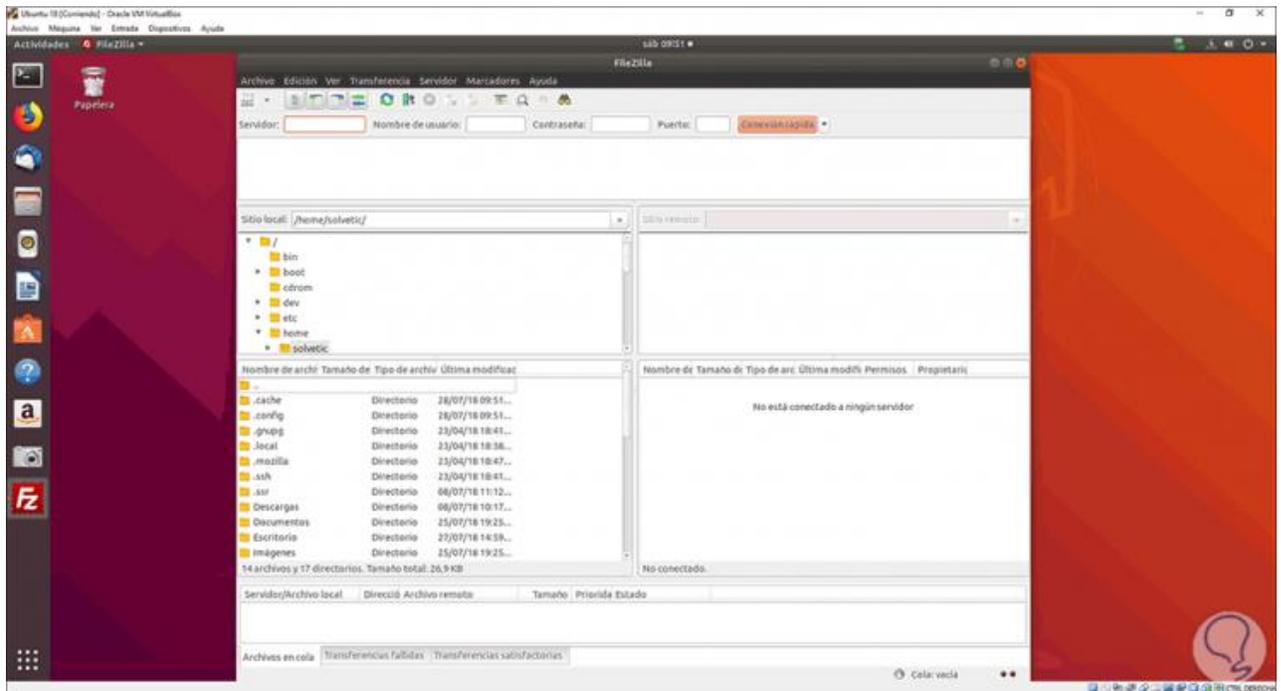
## 6. Cómo acceder a FTP usando SSL/TLS en Ubuntu 18

### Paso 1

No será posible acceder al servidor FTP a través de SSL/TLS desde un navegador, para ello será necesario instalar el cliente FTP de FileZilla con el fin de acceder al servidor FTP ya que este admite FTP sobre SSL/TLS, para instalar este cliente vamos a ejecutar lo siguiente:

```
sudo apt-get install filezilla -y
```

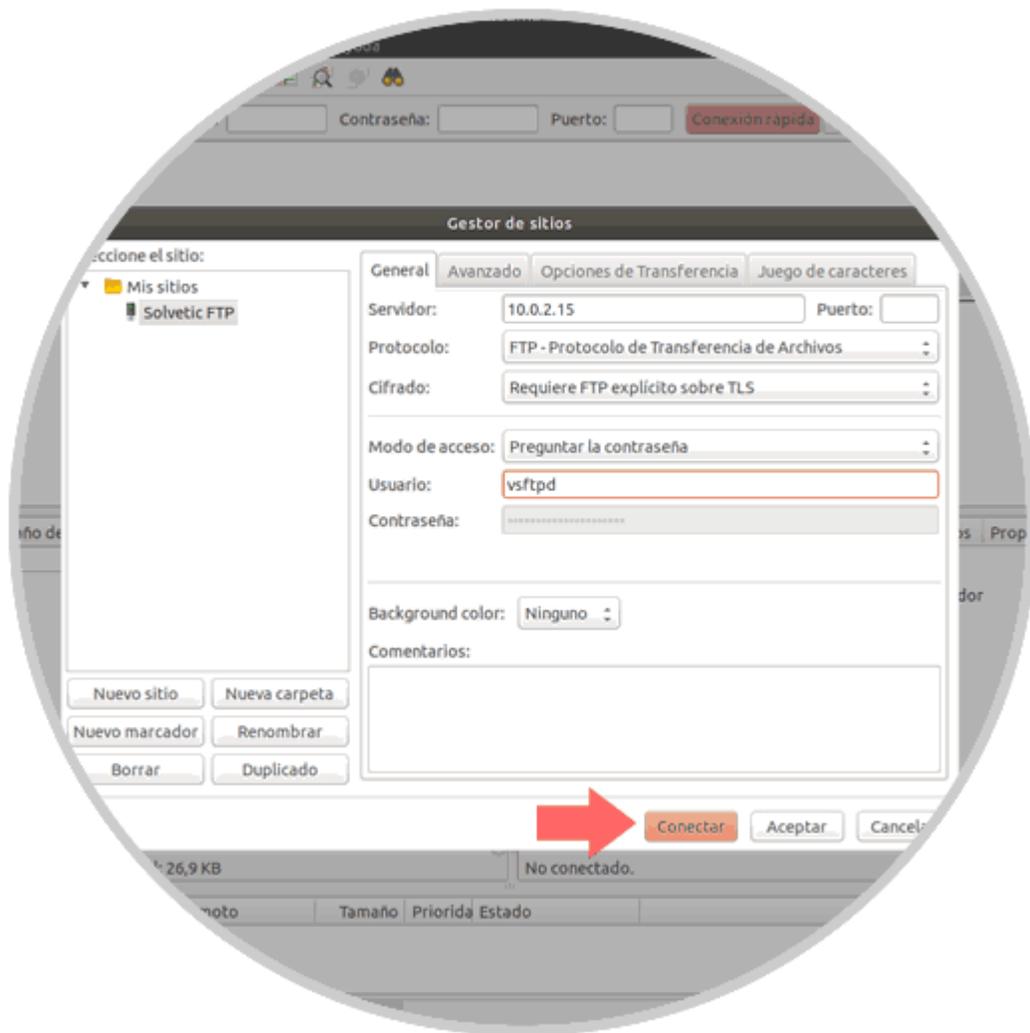
Una vez instalado, en este caso vamos a acceder desde Ubuntu 18.04 Desktop, accedemos a la aplicación donde veremos lo siguiente:



## Paso 2

Allí vamos al menú Archivo / Gestor de sitios y en la nueva ventana pulsamos en el botón Nuevo sitio y lo configuramos de la siguiente manera:

- Asignamos un nombre al sitio FTP
- En el campo Servidor ingresamos la IP del servidor a conectar
- En el campo Protocolo seleccionamos FTP – Protocolo de Transferencia de Archivos
- En la sección Cifrado definimos Requiere FTP explícito sobre TLS
- En el campo Modo de acceso establecemos Preguntar la contraseña e ingresamos el nombre del usuario creado en VSFTPD



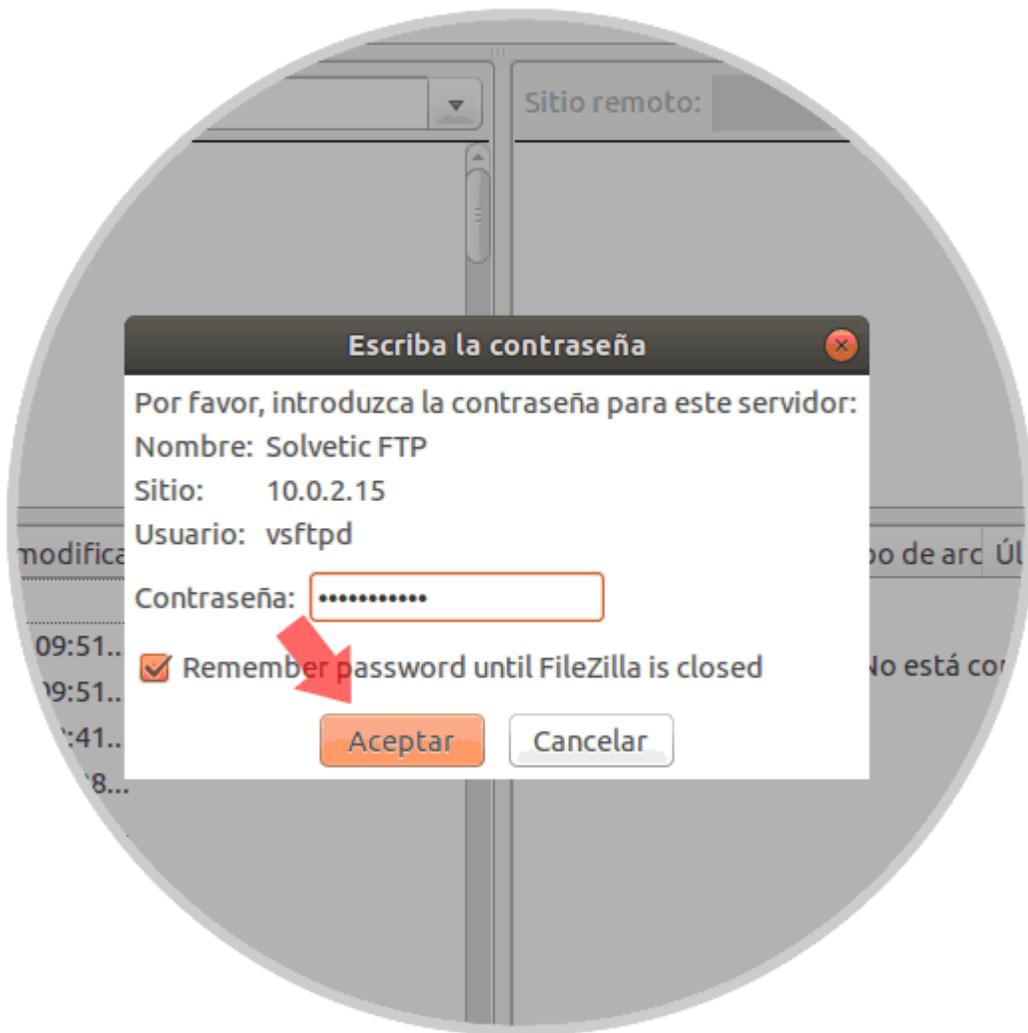
### Paso 3

Pulsamos en el botón Conectar y se desplegará el siguiente mensaje. Allí definimos si deseamos guardar o no las contraseñas.



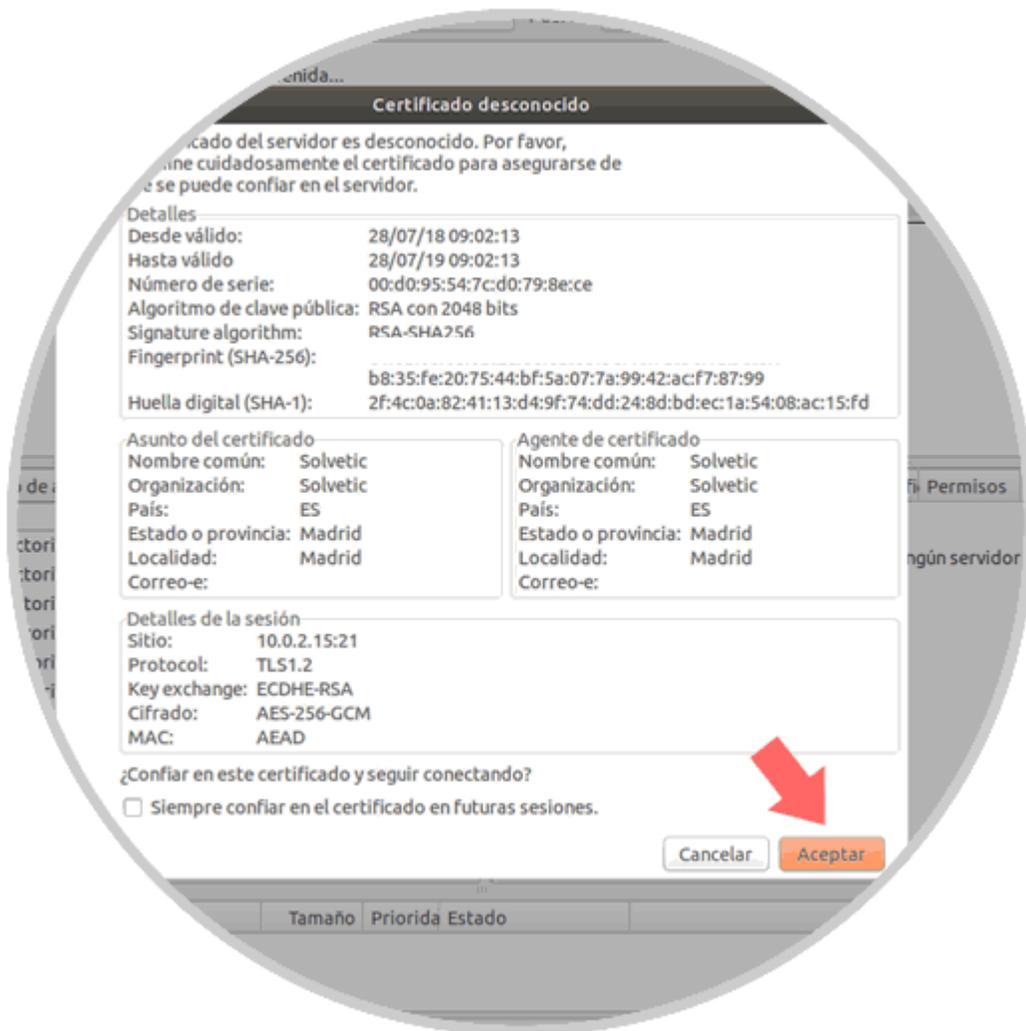
Paso 4

Pulsamos en Aceptar e ingresaremos la contraseña del usuario seleccionado:



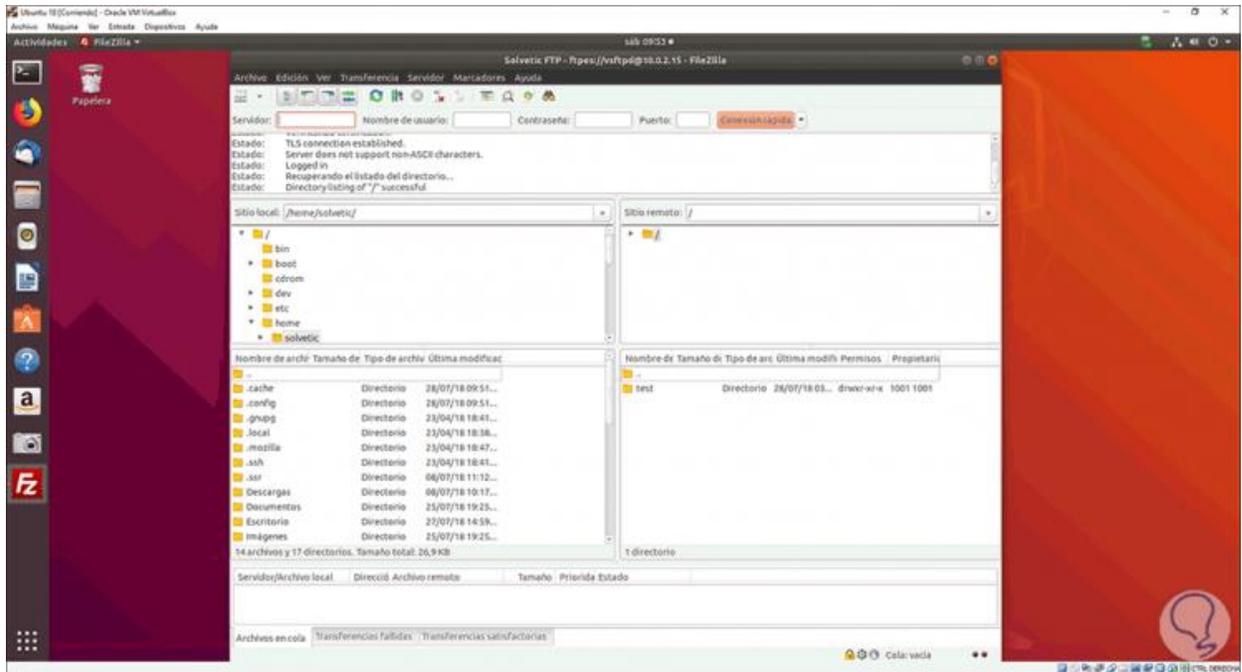
## Paso 5

Pulsamos en Aceptar y ahora veremos el certificado que se ha añadido con los detalles que hemos configurado:



Paso 6

Pulsamos en Aceptar y ahora se tendrá acceso al servidor FTP protegido con SSL/TLS:



Hemos visto cómo usar VSFTP para crear conexiones seguras, completas y dinámicas en Linux.