

Instala un servidor de FTP en Ubuntu con VSFTPD

Este tutorial te dará un paso a paso para instalar y configurar un servidor de FTP en tu servidor virtual y habilitar una conexión segura con FTPS. Si bien esta guía está dirigida a usuarios de Linux Ubuntu, es perfectamente aplicable a otras distros de Linux.

Abramos puertos

Partamos configurando el firewall. En el firewall que te provee VPS Guru debes abrir los puertos:

- 20 y 21 TCP
- 40000-50000 TCP
- 990 TCP

Instalemos y configuremos

Ahora actualiza Ubuntu e instala VSFTPD

```
sudo apt update && sudo apt install vsftpd
```

Revisa si ya está corriendo:

```
sudo service vsftpd status
```

Ya instalado y corriendo, hay que crear un usuario. Por ejemplo, "tuusuario":

```
sudo adduser tuusuario
```

Ahora debes definir el directorio en el cual podrá ese usuario subir y modificar archivos vía FTP. Lo normal es que la carpeta a la que tenga acceso el usuario FTP sea la de documentos del servidor HTTP (Apache o Nginx) o una subcarpeta creada dentro de ese directorio. Por lo que debes determinar dónde está esa carpeta. En Ubuntu normalmente es `/var/www`.

Por lo que si fuéramos a dejar como carpeta del usuario `/var/www` debiéramos tipear:

```
sudo usermod -d /var/www tuusuario
```

A continuación al usuario le damos propiedad sobre el directorio:

```
sudo chown tuusuario:tuusuario /var/www/html
```

No ahondaremos en los permisos, ya que extendería mucho más este artículo, pero si llegas a tener problemas de permisos, deberás interiorizarte en cómo funcionan los permisos y en cómo aplicar manejos avanzados de los mismos.

A continuación, es hora de configurar vsftpd. Antes de eso vamos a copiar el archivo y dejar un backup:

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

Ya realizado el backup, vamos a abrir el archivo con tu editor favorito, Nano o Vim. Nano suele ser el más sencillo de ocupar y puedes encontrar una [guía aquí](#). Para abrir el archivo de configuración de vsftpd vamos a tipear:

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

Dentro del archivo vamos a buscar `#write_enable=YES` y vamos a eliminar el `#`. De esta forma, el usuario podrá subir archivos, modificarlos, etc. La línea debiera quedar así:

```
write_enable=YES
```

Ahora vamos a buscar la línea `#chroot_local_user=YES` y vamos a eliminar el `#`. Esto previene que el usuario FTP pueda navegar fuera de su directorio. La línea debiera quedar así:

```
chroot_local_user=YES
```

Busca la línea `#local_umask=022` y vamos a eliminar el `#`. De esta forma establecemos permisos de escritura, lectura y ejecución al contenido. Los permisos 022 son de sólo escritura para el grupo y los demás. Pero puedes modificar estos permisos cambiando el valor 022 por el que creas más adecuado. La línea debiera quedar así:

```
local_umask=022
```

A continuación agregaremos líneas que no existen en el archivo, y que dejaremos al final del mismo:

```
force_dot_files=YES
pasv_min_port=40000
pasv_max_port=50000allow_writeable_chroot=YES
```

`force_dot_files` nos permitirá ver los archivos que se inician con un punto, como `.htaccess`. `pasv_min_port` y `pasv_max_port` nos permiten definir un rango para los puertos de FTP pasivo (¿recuerdas la configuración inicial del firewall?).

Salva los cambios y reinicia `vsftpd`:

```
sudo systemctl restart vsftpd
```

Ahora toca probar si todo está funcionando bien, para lo cual te aconsejamos utilizar [Filezilla](#). Lo más sencillo es usar el modo de conexión rápida. Allí tipeas el hostname (la IP), el nombre del usuario creado y la contraseña, y luego presionas "Conexión rápida".

Si hay falla revisa lo que indica Filezilla y también puedes revisar lo que registró `vsftpd` en su log

```
sudo tail /var/log/vsftpd.log -n 200
```

FTPS: para darle seguridad a nuestra

conexión

Lo recomendable es siempre tratar de usar FTPS ya que encripta nuestras comunicaciones con el servidor. Es decir, usar FTP con SSL/TLS.

Para lograrlo partamos por crear un nuevo certificado con la herramienta openssl:

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/certs/vsftpd.crt
```

Te pedirá que ingreses tu país, provincia y otros datos. No es necesario que los ingreses, por lo que puedes presionar "Enter" en cada uno de ellos.

Volvamos a abrir el archivo de configuración de vsftpd:

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

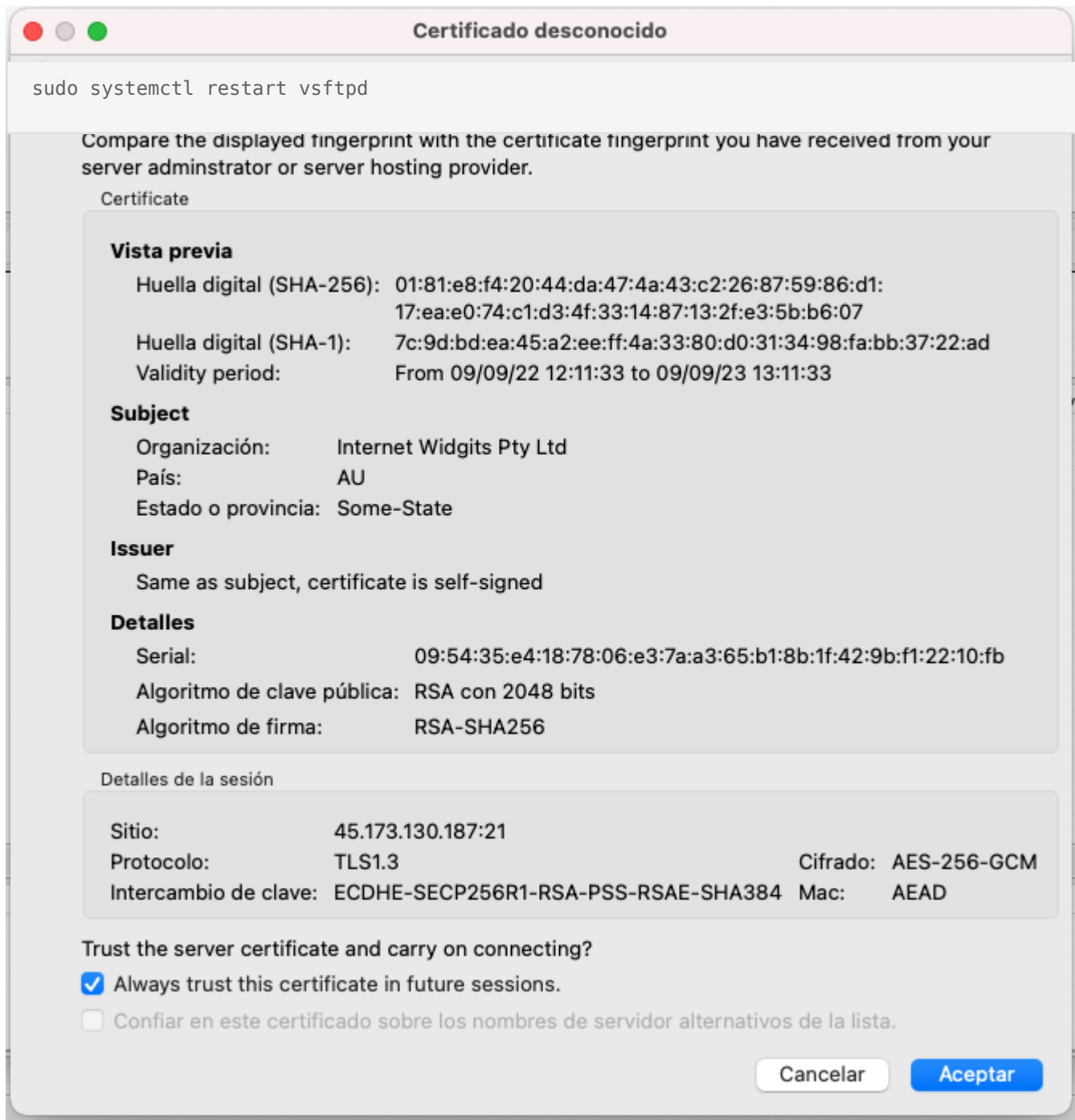
Encuentra la línea `ssl_enable=NO`, que debe quedar así:

```
ssl_enable=YES
```

Pega lo siguiente debajo de esa línea:

```
rsa_cert_file=/etc/ssl/private/vsftpd.pemrsa_private_key_file=/etc/ssl/private/vsftpd.pem
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
pasv_min_port=40000pasv_max_port=50000
```

Salva los cambios y reinicia vsftpd:



Luego de eso debiera ver los siguientes mensajes en el "registro de mensajes" de Filezilla:

Estado: Conexión establecida, esperando el mensaje de bienvenida...
Estado: Inicializando TLS...
Estado: Verificando certificado...
Estado: Conexión TLS establecida.

Revision #5

Created 2 years ago by [José Reyes](#)

Updated 2 years ago by [José Reyes](#)