

vSFTPd

`vsftpd` (Very Secure FTP Daemon) is a popular FTP server for Linux systems. To use vSFTPd, you'll need to install the `vsftpd` package.

vSFTPd Config Options

<code>pasv_enable=YES</code> <code>pasv_min_port=40000</code> <code>pasv_max_port=40100</code>	Enable passive mode and set port range
<code>pasv_address=your.external.ip.address</code>	Specify FTP listening IP.
<code>anonymous_enable=NO</code>	Disable anonymous access
<code>write_enable=YES</code>	Enable file uploads
<code>local_enable=YES</code>	Enable local users
<code>chroot_local_user=YES</code>	Enable user chroot
<code>chroot_list_enable=YES</code> <code>chroot_list_file=/etc/vsftpd.chroot_list</code>	Configure chroot bypass for users.
<code>ssl_enable=YES</code>	Enable SSL
<code>rsa_cert_file=/etc/ssl/certs/vsftpd.pem</code> <code>rsa_private_key_file=/etc/ssl/private/vsftpd.pem</code>	Specify SSL certificate files for FTPS/ES
<code>force_local_data_ssl=YES</code> <code>force_local_logins_ssl=YES</code>	Force SSL usage
<code>ssl_tlsv1=YES</code> <code>ssl_sslv2=NO</code> <code>ssl_sslv3=NO</code>	SSL Protocol options
<code>ssl_ciphers=HIGH</code>	SSL cipher
<code>force_local_data_ssl=NO</code> <code>force_local_logins_ssl=NO</code>	Enable FTPES

Adding users for FTP usage

1. In order to create an account that can use VSFTPD, you will first need to set up a user on the server that you want to transfer files to and from.

```
useradd guest
```

2. Once created, you'll want to set a password for that user

```
passwd guest
```

3. Also disable shell access for the user

```
usermod -s /sbin/nologin guest
```

Chrooting users

Chrooting a user in `vsftpd` ensures that the user is restricted to their home directory and cannot navigate to other parts of the file system.

1. Add the user

Either alter the existing user's home directory, or add a new user to be used for FTP

```
sudo adduser --home /var/ftp/ftpuser ftpuser
```

2. Set a password

```
passwd ftpuser
```

3. Set home directory permissions

```
sudo chown ftpuser:ftpuser /var/ftp/ftpuser  
sudo chmod 755 /var/ftp/ftpuser
```

4. Configure vsftpd

Ensure that the following is present within `/etc/vsftpd.conf`

```
chroot_local_user=YES
```

FTPS & FTPES

```
# Enable SSL
ssl_enable=YES

# Paths to the SSL certificate and key
rsa_cert_file=/etc/ssl/certs/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem

# Require SSL for both data and login
force_local_data_ssl=YES
force_local_logins_ssl=YES

# Allow anonymous users to use SSL
allow_anon_ssl=YES

# SSL protocol options
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO

# Strong ciphers
ssl_ciphers=HIGH

# Optional: Require SSL reuse for data connections
require_ssl_reuse=NO

# Enable Explicit SSL (FTPES)
# By default, vsftpd will use implicit FTPS (default port 990)
# If you prefer explicit FTPS (FTPES), enable the following:
force_local_data_ssl=NO
force_local_logins_ssl=NO

# Explicitly request SSL for login
ssl_request_cert=YES
```

=====
=====

Revision #3

Created 2024-06-30 22:39:18 UTC by Daniel

Updated 2024-06-30 23:02:01 UTC by Daniel