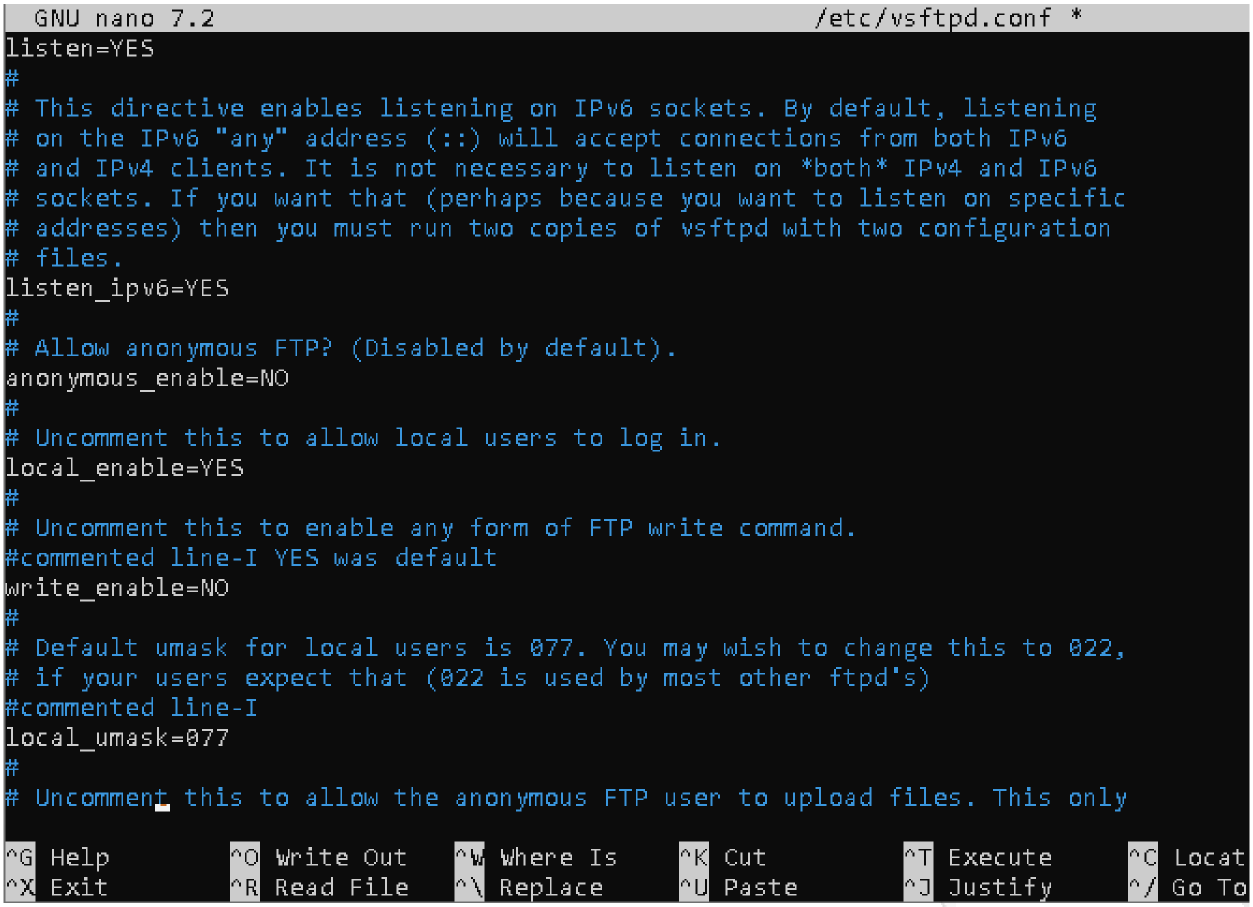
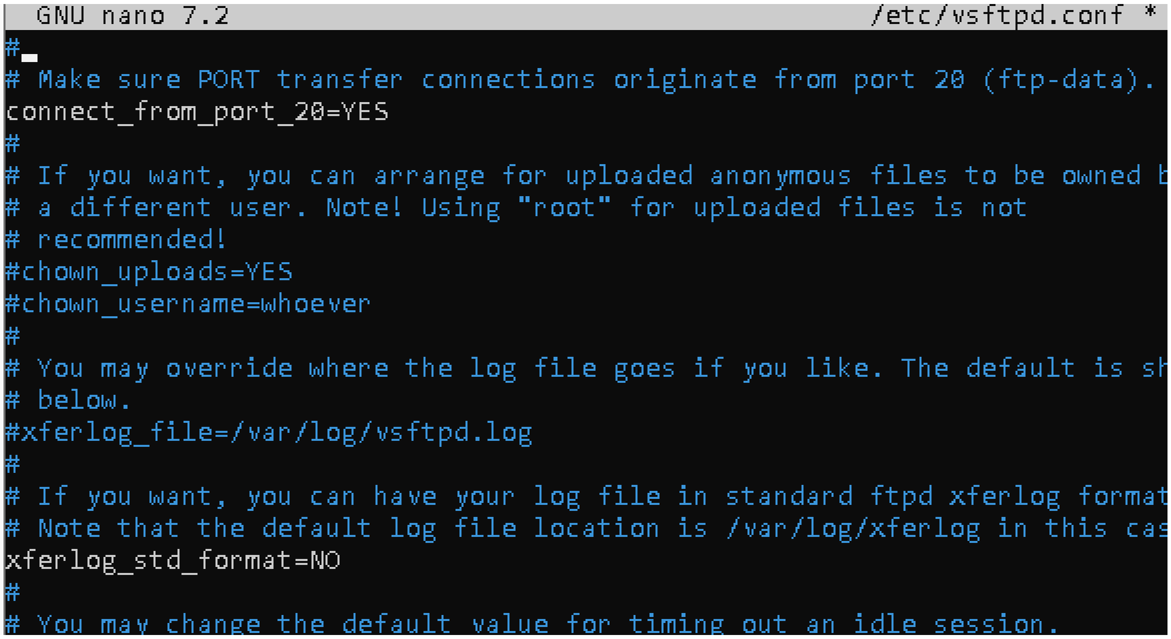
Edit /etc/vsftpd.conf file and modify the file to reflect following configuration



```
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
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
#commented line-I YES was default
write_enable=NO
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#commented line-I
local_umask=077
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
```

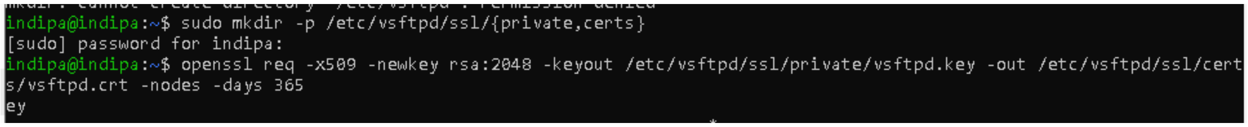


```
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned b
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# You may override where the log file goes if you like. The default is sh
# below.
#xferlog_file=/var/log/vsftpd.log
#
# If you want, you can have your log file in standard ftpd xferlog format
# Note that the default log file location is /var/log/xferlog in this cas
xferlog_std_format=NO
#
# You may change the default value for timing out an idle session.
```

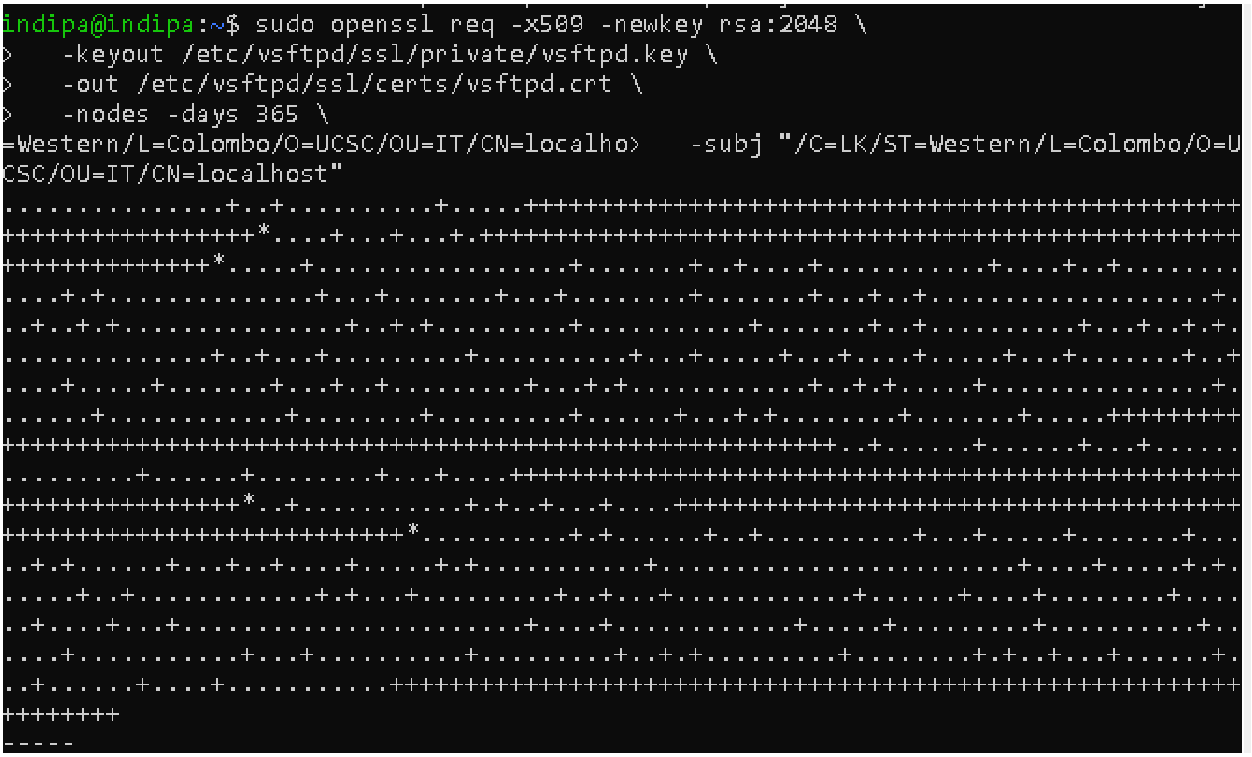
Securing VSFTPD Service

Enabling SSL/TLS

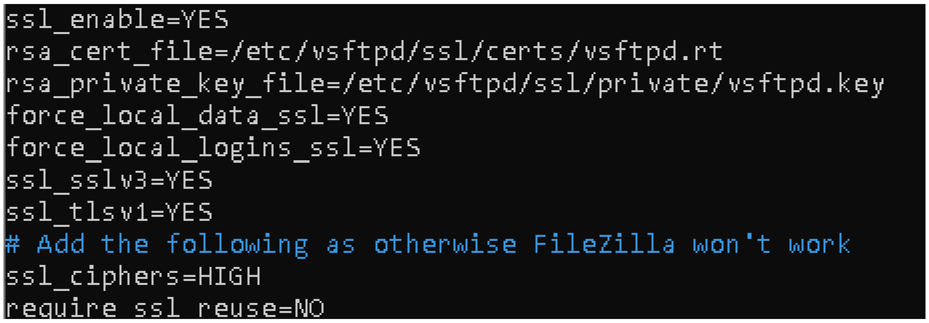
First we need to create private and public key pair for vsftpd server.



```
mkdir: cannot create directory '/etc/vsftpd': Permission denied
indipa@indipa:~$ sudo mkdir -p /etc/vsftpd/ssl/{private,certs}
[sudo] password for indipa:
indipa@indipa:~$ openssl req -x509 -newkey rsa:2048 -keyout /etc/vsftpd/ssl/private/vsftpd.key -out /etc/vsftpd/ssl/cert
s/vsftpd.crt -nodes -days 365
ey
```

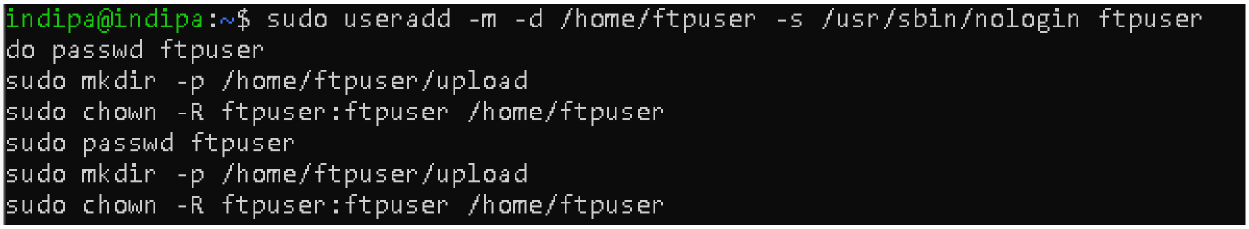


```
indipa@indipa:~$ sudo openssl req -x509 -newkey rsa:2048 \
>   -keyout /etc/vsftpd/ssl/private/vsftpd.key \
>   -out /etc/vsftpd/ssl/certs/vsftpd.crt \
>   -nodes -days 365 \
=Western/L=Colombo/O=UCSC/OU=IT/CN=localho>   -subj "/C=LK/ST=Western/L=Colombo/O=U
CSC/OU=IT/CN=localhost"
...............+..+..........+.....++++++++++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++*....+...+...+.+++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++*.....+.................+.......+..+....+...........+....+..+........
....+.+..............+...+.......+...+........+.......+...+..+...................+.
..+..+.+...............+..+.+.........+...........+.......+..+..........+...+..+.+.
..............+..+...+.........+..........+...+.....+...+....+.....+...+.......+..+
....+.....+.......+...+..+.........+...+.+............+..+.+.....+...............+.
......+............+........+.........+......+...+.+........+.......+.....+++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++..+......+......+...+......
.........+......+........+...+....+++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++*..+...........+.+..+...+....++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++*..........+.+......+..+..........+...+.....+.......+...
..+.+......+...+..+....+.....+.+...........+........................+....+.....+.+.
.....+..+............+.+...+.........+..+...+............+......+....+........+....
..+....+...+.......................+....+............+.....+.........+..........+..
....+...........+...+..........+.........+..+.+.........+........+.+..+...+......+.
..+......+....+...........+++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++
-----
```

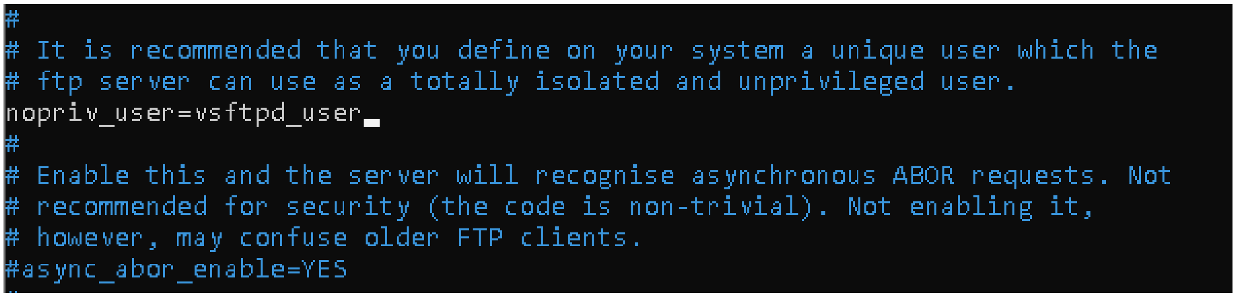


```
ssl_enable=YES
rsa_cert_file=/etc/vsftpd/ssl/certs/vsftpd.rt
rsa_private_key_file=/etc/vsftpd/ssl/private/vsftpd.key
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_sslv3=YES
ssl_tlsv1=YES
# Add the following as otherwise FileZilla won't work
ssl_ciphers=HIGH
require_ssl_reuse=NO
```

Run vsftpd under a non privileged user

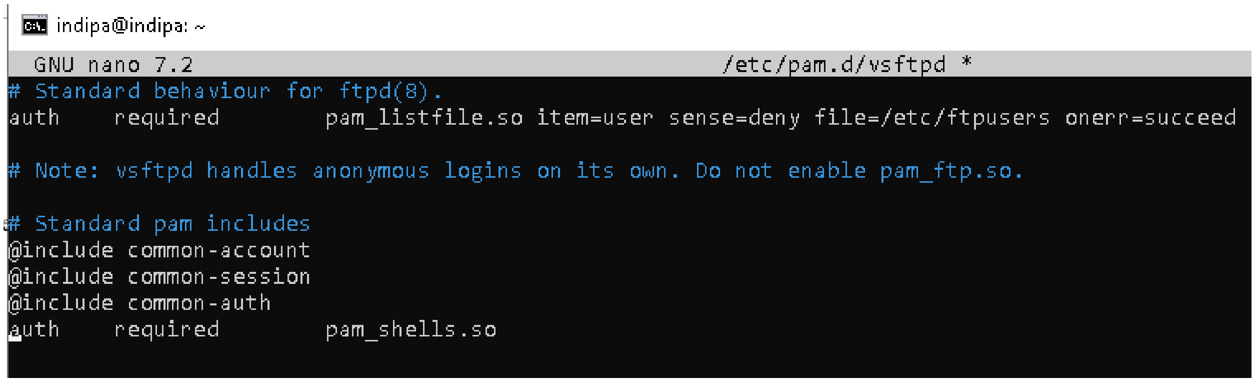


```
indipa@indipa:~$ sudo useradd -m -d /home/ftpuser -s /usr/sbin/nologin ftpuser
do passwd ftpuser
sudo mkdir -p /home/ftpuser/upload
sudo chown -R ftpuser:ftpuser /home/ftpuser
sudo passwd ftpuser
sudo mkdir -p /home/ftpuser/upload
sudo chown -R ftpuser:ftpuser /home/ftpuser
```



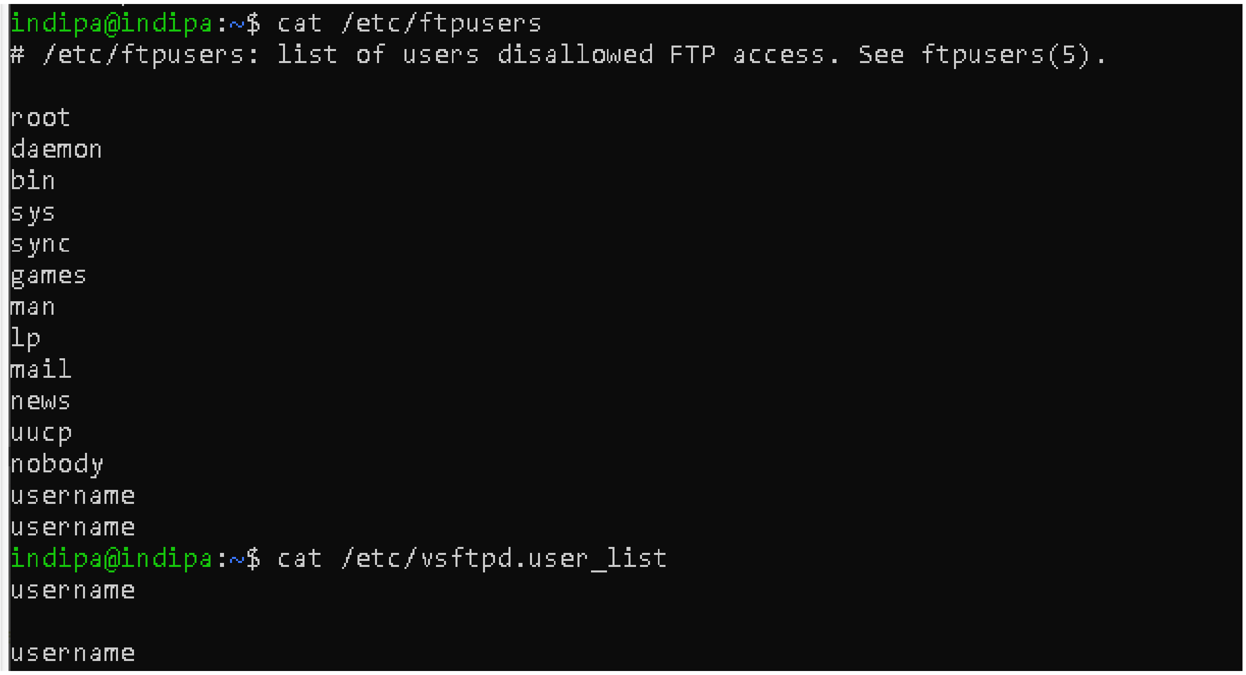
```
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
nopriv_user=vsftpd_user
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
#async_abor_enable=YES
```

Removing Shell capabilities from users

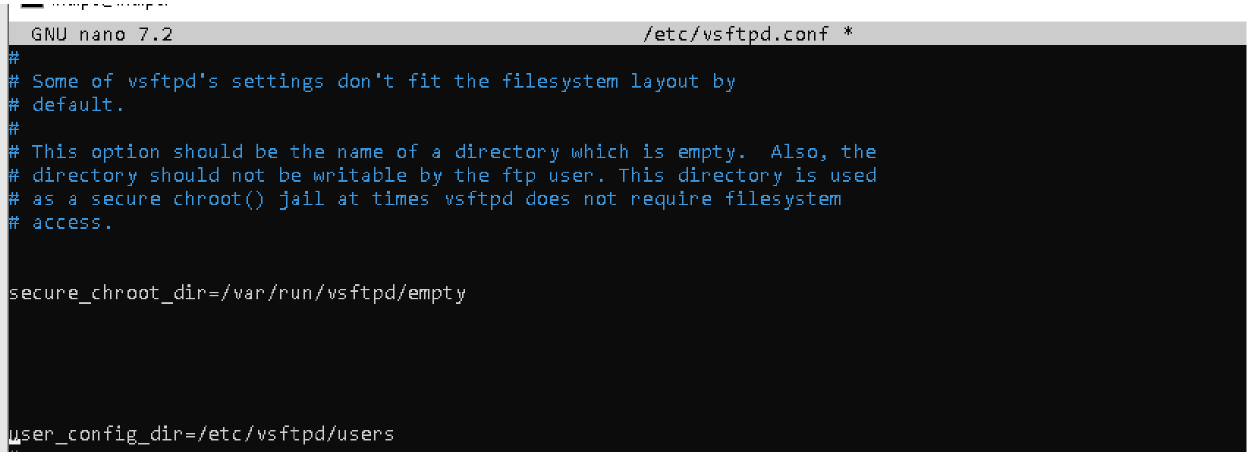


```
  GNU nano 7.2                                       /etc/pam.d/vsftpd *
# Standard behaviour for ftpd(8).
auth    required        pam_listfile.so item=user sense=deny file=/etc/ftpusers onerr=succeed

# Note: vsftpd handles anonymous logins on its own. Do not enable pam_ftp.so.

# Standard pam includes
@include common-account
@include common-session
@include common-auth
auth    required        pam_shells.so
```

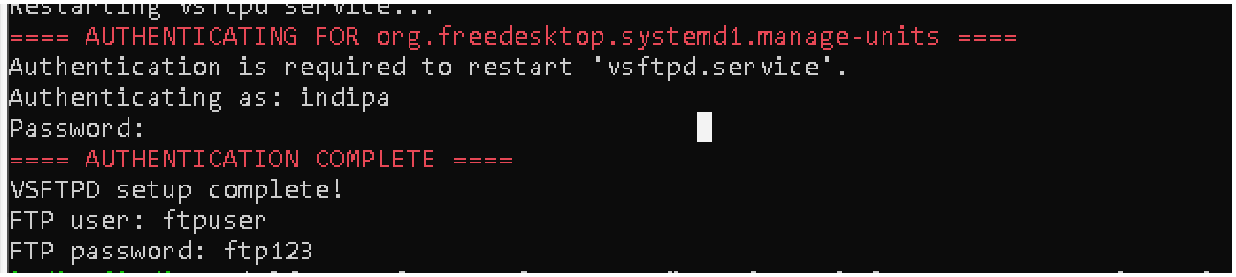
Restricting FTP access to SSH users



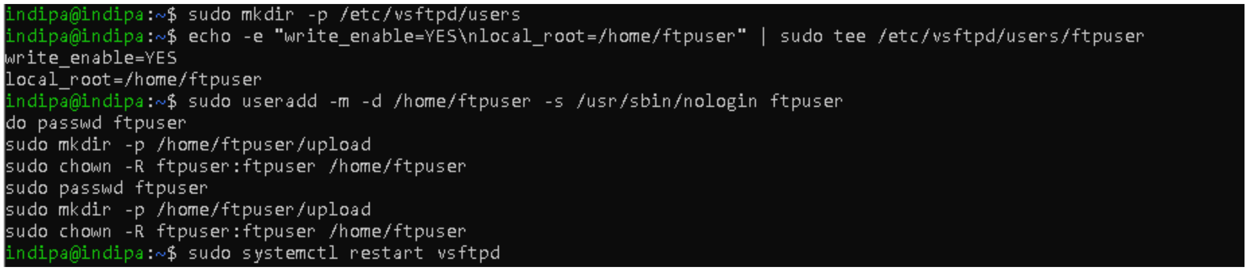
```
indipa@indipa:~$ cat /etc/ftpusers
# /etc/ftpusers: list of users disallowed FTP access. See ftpusers(5).

root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
nobody
username
username
indipa@indipa:~$ cat /etc/vsftpd.user_list
username

username
```



```
  GNU nano 7.2                                          /etc/vsftpd.conf *
#
# Some of vsftpd's settings don't fit the filesystem layout by
# default.
#
# This option should be the name of a directory which is empty.  Also, the
# directory should not be writable by the ftp user. This directory is used
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.


secure_chroot_dir=/var/run/vsftpd/empty





user_config_dir=/etc/vsftpd/users
```

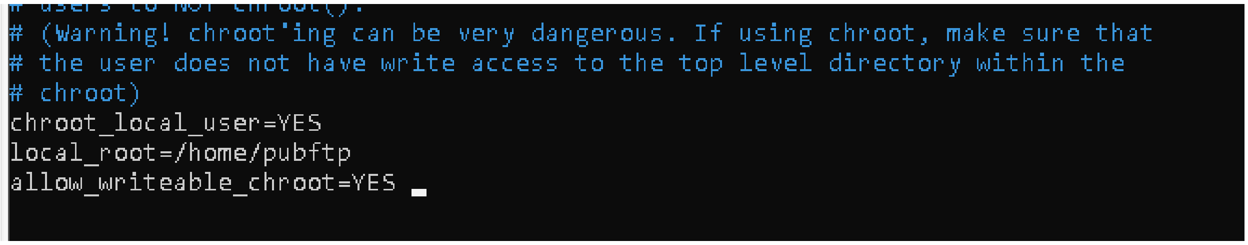


```
Restarting vsftpd service...
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'vsftpd.service'.
Authenticating as: indipa
Password:
==== AUTHENTICATION COMPLETE ====
VSFTPD setup complete!
FTP user: ftpuser
FTP password: ftp123
```



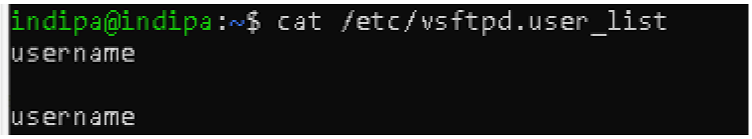
```
indipa@indipa:~$ sudo mkdir -p /etc/vsftpd/users
indipa@indipa:~$ echo -e "write_enable=YES\nlocal_root=/home/ftpuser" | sudo tee /etc/vsftpd/users/ftpuser
write_enable=YES
local_root=/home/ftpuser
indipa@indipa:~$ sudo useradd -m -d /home/ftpuser -s /usr/sbin/nologin ftpuser
do passwd ftpuser
sudo mkdir -p /home/ftpuser/upload
sudo chown -R ftpuser:ftpuser /home/ftpuser
sudo passwd ftpuser
sudo mkdir -p /home/ftpuser/upload
sudo chown -R ftpuser:ftpuser /home/ftpuser
indipa@indipa:~$ sudo systemctl restart vsftpd
```

Put Users in chroot Jail



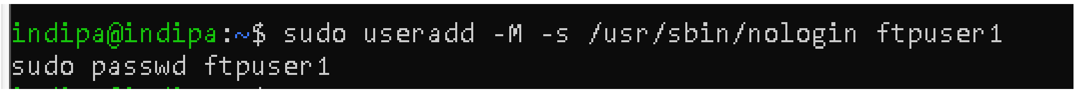
```
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
chroot_local_user=YES
local_root=/home/pubftp
allow_writeable_chroot=YES
```

Allowing only required users to vsftpd service



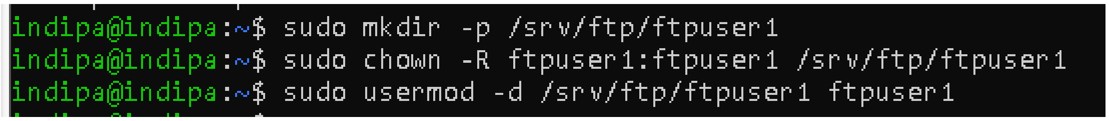
```
indipa@indipa:~$ cat /etc/vsftpd.user_list
username

username
```

Create a system user to use FTP



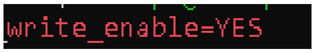
```
indipa@indipa:~$ sudo useradd -M -s /usr/sbin/nologin ftpuser1
sudo passwd ftpuser1
```

Create the FTP directory for user

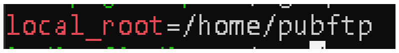


```
indipa@indipa:~$ sudo mkdir -p /srv/ftp/ftpuser1
indipa@indipa:~$ sudo chown -R ftpuser1:ftpuser1 /srv/ftp/ftpuser1
indipa@indipa:~$ sudo usermod -d /srv/ftp/ftpuser1 ftpuser1
```

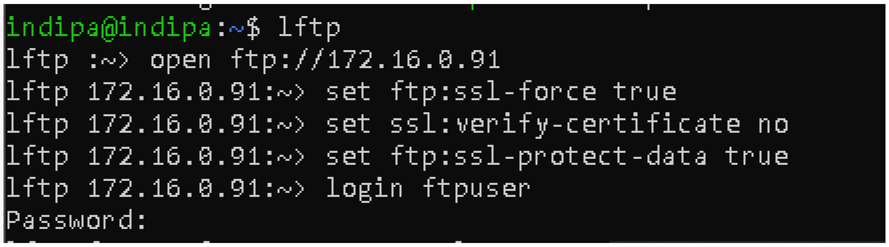
Configuring FTP access to the user



```
write_enable=YES
```



```
local_root=/home/pubftp
```



```
indipa@indipa:~$ lftp
lftp :~> open ftp://172.16.0.91
lftp 172.16.0.91:~> set ftp:ssl-force true
lftp 172.16.0.91:~> set ssl:verify-certificate no
lftp 172.16.0.91:~> set ftp:ssl-protect-data true
lftp 172.16.0.91:~> login ftpuser
Password:
```