# Vsftpd

**Vsftpd**, short for **Very Secure FTP daemon**, is a secure FTP daemon that is an upgrade of FTP protocol. It enforces secure connections to FTP servers by encrypting traffic send to and from the server, and by so doing, the file transfer is kept safe and secure from hackers.

# Step 1) Install vsftpd using dnf command

Right off the bat, we are going to install vsftpd. To achieve this, we will run the command below:

$ sudo dnf install vsftpd

The output indicates that we have installed vsftpd version 3.0.3-31.el8.x86\_64. To confirm this, execute the following command:

[linuxtechi@centos8-vsftpd ~]$ rpm -q vsftpd

To start the vsftpd service, run the command:

$ sudo systemctl start vsftpd

You may also want to enable it to start automatically upon a reboot. To achieve this, run the command

$ sudo systemctl enable vsftpd --now

To verify the status of vsftpd on your system, run:

$ sudo systemctl status vsftpd

# Step 2) Create a ftp user and its directory

Next, we will create a user that we will use to access the FTP server. In this case, the user will be ftpuser but feel free to give your user a name of your choice.

$ sudo adduser ftpuser

$ sudo passwd ftpuser

With the FTP user in place, we will proceed and create the FTP directory and assign the following permissions and directory ownership.

$ sudo mkdir -p /home/ftpuser/ftp\_dir

$ sudo chmod -R 750 /home/ftpuser/ftp\_dir

$ sudo chown -R ftpuser: /home/ftpuser/ftp\_dir

We also need to add the FTP user to the **/etc/vsftpd/user\_list** file to allow the user access to the vsftp server.

$ sudo bash -c 'echo ftpuser >> /etc/vsftpd/user\_list'

# Step 3) Configure vsftpd via its configuration file

The default configuration file for vsftpd is the /etc/vsftpd/vsftpd.conf file.

To allow local users to access the FTP server remotely, and block anonymous users, ensure you have the directives as shown:

anonymous\_enable=NO

local\_enable=YES

To grant users rights to run any FTP command & make changes such as uploading, downloading and deleting files, have the following line in place.

write\_enable=YES

For security purposes, you may opt to restrict users from accessing any files & directories outside their home directories. Therefore, have the following directive in place.

chroot\_local\_user=YES

To grant users write access to their respective home directories, ensure you have this directive.

allow\_writeable\_chroot=YES

Next, we are going to define custom ports to enable Passive FTP connections. In this case, we will specify ports 30000 and 31000. We shall later open these on the firewall.

pasv\_min\_port=30000

pasv\_max\_port=31000

Next, we are going to only allow the users defined in the **/etc/vsftpd/user\_list** access to the server and block the rest. To achieve this, have the lines below.

userlist\_file=/etc/vsftpd/user\_list

userlist\_deny=NO

to set directory of user in which user's file will locate

local\_root=/home/$USER/ftp

Finally, save and close the file. For the changes to persist, restart the Vsftpd service.

If add an user in file "ftpuser" this user will prevent to access to ftp server

$ sudo systemctl restart vsftpd

At this point, you can test for FTP connectivity by running

# Step 4) Configure SSL / TLS for vsftpd

To encrypt communications between the server and a client system, we need to generate a TLS certificate and later configure the server to use it.

To generate the certificate, run the command below:

$ sudo openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -keyout /etc/vsftpd.pem -out /etc/vsftpd/vsftpd.pem

This will be followed by a series of prompts where you will be required to provide a few details such as country name, state or province, and organizational name to mention a few. Fill out all the details accordingly as shown.

We also need to tell the server where the certificate files are stored. So, head back to the configuration file /etc/vsftpd/vsftpd.conf and specify the path to the certificate files.

rsa\_cert\_file=/etc/vsftpd/vsftpd.pem

rsa\_private\_key\_file=/etc/vsftpd.pem

And then, instruct the server to turn on SSL.

ssl\_enable=YES

Save and exit the configuration file. To make above changes into the effect, restart vsftpd service,

$ sudo systemctl restart vsftpd

# Step 5) Allow ftp server (vsftpd) ports in the firewall

If you are running a firewall, you need to allow these salient ports”

* 20 – to allow FTP traffic
* 21 – FTP data port
* 30000-31000 – To allow passive communication with the FTP server.

Therefore, run the commands below:

$ sudo firewall-cmd --permanent --add-port=20-21/tcp

$ sudo firewall-cmd --permanent --add-port=30000-31000/tcp

Then reload the firewall for the changes to come into effect.

$ sudo firewall-cmd --relo­ad