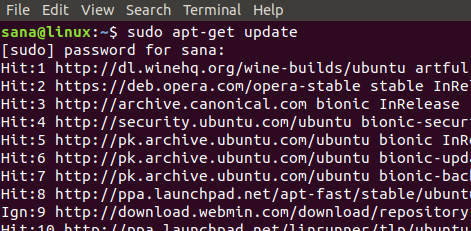
FTP Server Installation

In this process, we will be installing VsFTPD-Very secure FTP Daemon on our Ubuntu System. VsFTPD utility is more powerful and secure than the native FTP.

Step1: Install VsFTPD

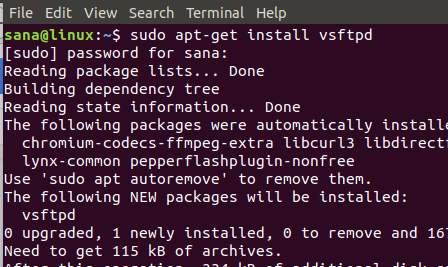
In order to install the VsFTPD package through our Terminal, let us first update our repositories through the following command:

$ sudo apt-get update



Now is the time to install the latest available binary package for VsFTPD through the following command as root:

$ sudo apt-get install vsftpd



The system will ask you for user credentials and might also give you a Y/n option for proceeding with the installation process. Please enter Y to proceed.

Once the installation is complete, you can verify it by checking the version number of the installed VsFTPD package as follows:

$ vsftpd -verions

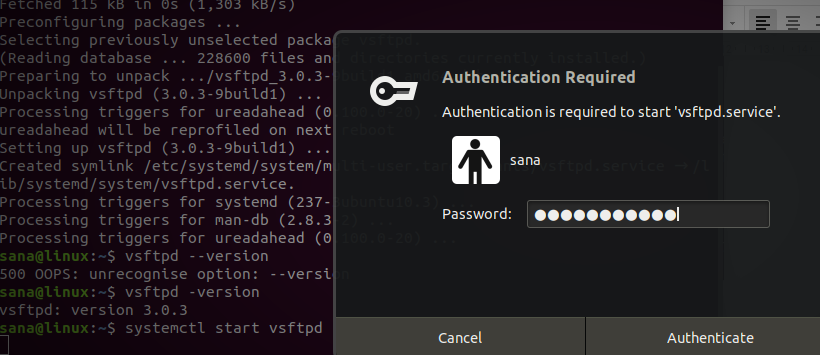
Check vsftpd version

The above output shows the version number and verifies that VsFTPD is now installed on your system.

Step 2: Start the VsFTPD service

When you install VsFTPD, the service is disabled by default. Let us start the service through the following command:

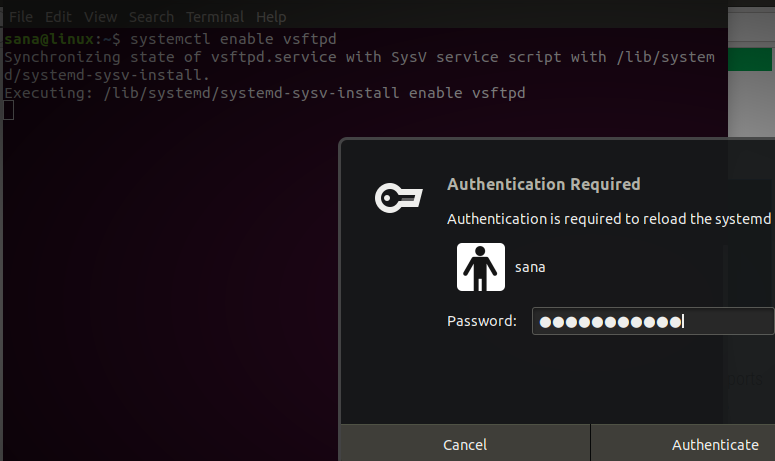
$ systemctl start vsftpd

Advertisement

You will be asked to provide user authentication, as above. Enter your password and then click the Authenticate button. The service will then be started.

You can also enable the service to be automatically started at boot through the following command:

$ systemctl enable vsftpd



You will be asked to provide user authentication multiple times for various purposes. Enter your password and then click the Authenticate button.

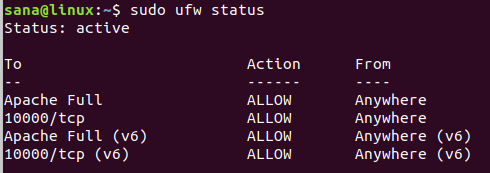
VsFTPD Configuration

After the installation is complete, let us now set up and configure FTP on our Ubuntu system.

Step 1: Open port 20 and 21 if the firewall is enabled

You can check the status of your firewall through the following command:

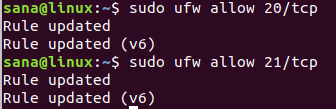
$ sudo ufw status



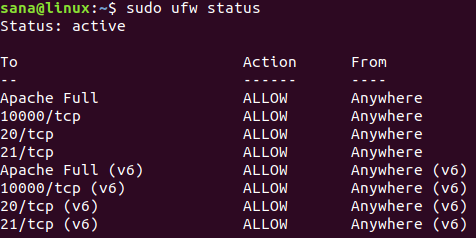
If the firewall is enabled and the status is active, you can open ports 20 and 21 through the following command:

$ sudo ufw allow 20/tcp

$ sudo ufw allow 21/tcp



Now again if you view the status of the firewall, you will see these two ports open and allowed:



Step 2: Configure the vsftpd.conf file and enable SSL/TLS

The most important step in configuring FTP is to make some changes in the vsftpd configuration file. But before making any changes to this important file, let us make a backup for it through the following command:

$ sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.orig

**Backup the old vsftpd configuration file**

Now open the configuration file in your favorite text editor. We are using the nano editor for editing this file:

$ sudo nano /etc/vsftpd.conf

In order to make the most basic FTP configuration, copy the following settings at the end of the file:

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

rsa\_cert\_file=/etc/ssl/certs/ssl-cert-snakeoil.pem

rsa\_private\_key\_file=/etc/ssl/private/ssl-cert-snakeoil.key

ssl\_enable=Yes

pasv\_enable=Yes

pasv\_min\_port=10000

pasv\_max\_port=10100

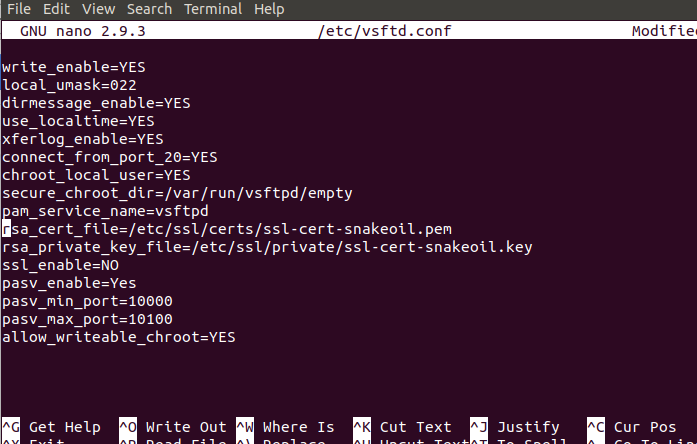
allow\_writeable\_chroot=YES

ssl\_tlsv1=YES

ssl\_sslv2=NO

ssl\_sslv3=NO

Exit and Save the file by pressing Ctrl+X and then hit enter.

****

Step 3: Restart the VsFTPD service

After making changes to the vsftpd.conf file, you need to restart the VsFTPD service for these changes to take effect. Enter the following command as root in order to restart the service:

$ sudo systemctl restart vsftpd

Step 4: Create an FTP user

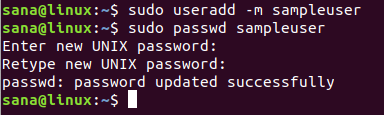
Let us now create a user for FTP who will be able to use the FTP server, through this command:

$ sudo useradd -m “username”

Assign a password to that user through this command:

$ sudo passwd “username”

In this example, we have created a user by the name of sampleuser and assigned it a password:



Lets us also create a **sample file** in the new user’s home directory. This file will later be used when we are testing our FTP connection:

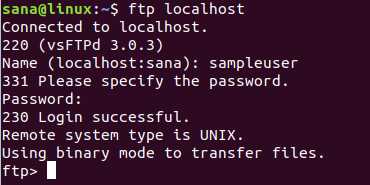
$ sudo bash -c “echo This is a sample file for FTP > /home/sampleuser/sampleFile”

Test the FTP Connection

Finally, let us test our FTP connection. I am testing this connection on localhost. You can use an available FTP server to test your connection:

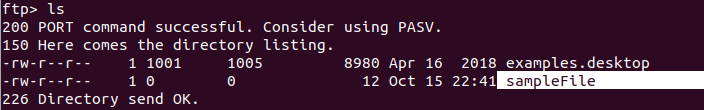
$ ftp “hostname”

Example:



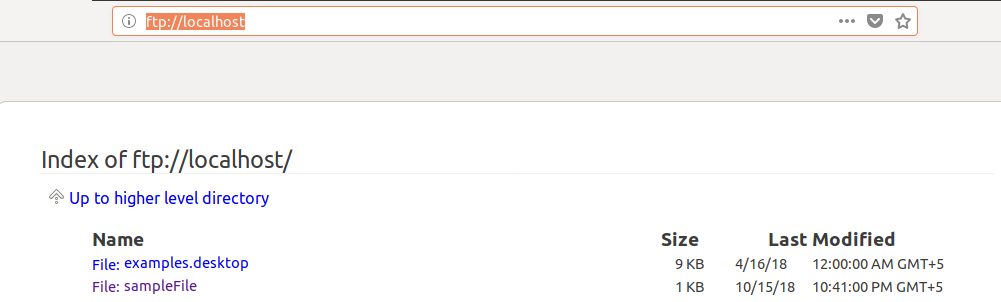
Here you need to provide username and password of the user you created in order to access the FTP server.

Once you are successfully logged in, you can list the available files through the ls command. In the following image, you can see the sample file we created on the sample user’s home directory.

****

You can also access the FTP server through your web browser by entering the FTP site. For example, in order to access the local host, I will use the following link:

ftp://localhost/



You can easily access the available files from here as well.

So, we have presented the simplest and most basic procedure for installing and configuring the FTP server on your Ubuntu system. By following the above-mentioned steps, you can access the FTP server and upload/download files from there.