**VSFTPD (Very Secured FTP server)**

**(**[**http://www.computernetworkingnotes.com/network-administration/how-to-configure-ftp-server-in-rhel6.html**](http://www.computernetworkingnotes.com/network-administration/how-to-configure-ftp-server-in-rhel6.html) **)**

**File Transfer Protocol** (**FTP**) is a network protocol used to copy a file from one computer to another over the Internet or LAN. **FTP** follows a client-server architecture which utilizes separate control and data connections between the **ftp** client and server. The default port for **ftp** is 21.

vsftpd is lightweight, highly stable, secure, and fast FTP server for Linux environment. vsftpd powers lot of heavily used FTP service in the internet

**VsFTPd** stands for **Very Secure FTP Daemon**. VSFTPD is the most popular ftp server. Also probably the most secure and fastest FTP server for UNIX-like systems. If you are searching an FTP server which can provide you Security, Performance and Stability then your searching is finished here, vsFTPd can be best suitable option for you.

**PEM** or Privacy Enhanced Mail

**Defaults**

* The default port – **21 and 20**
* The default directory to upload your files – **/var/ftp/pub** for anonymous access. By default all users are chrooted to /var/ftp and they are not allowed to change the directory.
* Anonymous login details – Use **anonymous / anonymous** or **ftp / ftp** as username / password combo.

1.Check for the vsftpd rpm is installed on the system or not

# rpm -qa vsftpd

2.If it is not installed already then install it.

# yum install vsftpd

3.Then check for the files that are installed on the system by the vsftpd rpm. Then it have some of important files are discuss below.

# rpm -ql vsftpd

/etc/vsftpd/vsftpd.conf :- Main configuration file

/etc/vsftpd/ftpusers :- list of user that are denied permanently.

/etc/vsftpd/user\_list :- contains users taht are allowed/denied.

/etc/vsftp/chroot\_list :- jail User (Home Dir allow permision)

4.Add new sample users that we want to test on the system and give their respective password for them.

**Important Note**: The normal users can easily able to do the “ssh” on the ftp server and can easily get the information that they want. So it is preferred to have the login shell of ftp users as “nologin”. So remove and modify login shell entry in /etc/passwd file as /sbin/nologin

# useradd -s /sbin/nologin <username>

(forchanging the existing user shell .users are not able to login to the server using SSH)

# usermod –s /sbin/nologin <username>

5.Now start the vsftpd service. You can also make the service permanent on using chkconfig command.

# service vsftpd start

# chkconfigvsftpd --level 345 on

# chkconfigvsftpd --list

vsftpd 0:off 1:off 2:off 3:on 4:on 5:on 6:off

6.You can also check using the netstat command which shows the tcp service is start on the port number 21

7.Now try to login as usr1 using the command #ftp ip\_address\_of\_system

# ftp 192.168.1.9

Name (192.168.1.9:root):usr1

Password:

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files.

8.It shows that the any user on 192.168.1.9 are able to login on ftp server except the root user.Because the root user don’t have permission to login to ftp server.

9.Now append the following entries to vsftpd.conf file, restart the service then try to login as different users.

a) userlist\_enable=YES

b) userlist\_deny=NO

10.Add the user usr1 to the /etc/vsftpd/user\_list, restart the service ant try to login as different users but only the usr1 is able to login but other users are not able to login to ftp server.

The contents of the user\_list file are as follows:

# If userlist\_enable=YES and

i) userlist\_deny=NO, then only users in the user\_list file are allowed.

ii) userlist\_deny=YES (default), never allow users in user\_list file, and do not even

prompt for a password.

11.Now change the userlist\_enable=NO in step9 and restart the service. Try to login as different users then it shows that all the users are able to login successfully. Since the userlist is disable.

From the above steps 9-11 we can conclude that

\*userlist\_enable=YES(default):examine userlist\_deny entry

a)userlist\_deny=YES(default):users not present in user\_list and ftpusers files areallowed.

b)userlist\_deny=NO :only users in user\_list file are allowed if they are not in ftpusers file.

\* userlist\_enable=NO :userlist\_deny not examine allow all users which are not present in ftpusers file.

Some important Points to be remembered about the VSFTPD .conf file

i)Default port: TCP / UDP - 21 and 20

ii)Lock down users to their home directories:chroot\_local\_user=YES

iii)Create warning banners for all FTP users: banner\_file=/etc/vsftpd/issue

iv)Restrict Access to Anonymous User Only: local\_enable=NO

v) Disable FTP Uploads: write\_enable=NO

12.If we want to display the message whenever user is login to ftp server then we need to create the .message file in the home directory of the user. We need to run the following command to run and restart the service. Now try to login as any user on ftp server it will shows the message given in the .message file.

#setsebool -P ftp\_home\_dir=1

#service vsftpd restart

**Restricting users to their home directory:**

1) Normal ftp user can able to access file and if we do not wish FTP users to be able to access any files outside of their own home directory, set up chroot jail.

# vi /etc/vsftpd/vsftpd.conf

Make sure following line exists (and uncommented):

chroot\_local\_user=YES or

chroot\_local\_user=NO

chroot\_list\_enable=YES

chroot\_list\_file=/etc/vsftp/chroot\_list

Save and close the file. Restart vsftpd.

# servicevsftpd restart

2)When you try to login to ftp server it gives an error :-

500 OOPS: could not open chroot() list file:/etc/vsftpd/chroot\_list

Login failed

3)Then we need to create chroot\_list file in /etc/vsftpd/ directory and give the names of the users that you want to restrict.

4)Now all users of VSFTPD/FTP will be limited to accessing only files in their own home directory. They will not able to see /, /etc, /root and /tmp and all other directories. This is an essential security feature.

**On Client Machine :**

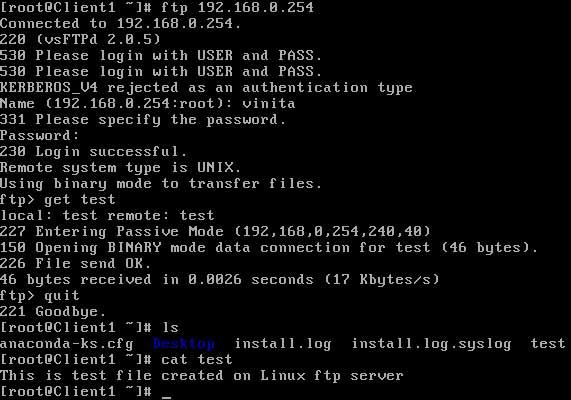
ftp rpm must install

# rpm –qa ftp

# ftp <IPAddress of server machine>

Name :

Passward :



### Most commonly commands used on ftp prompt are

**put** To upload files on server

**get** To download files from server

**mput** To upload all files

**mget** To download all files

**?** To see all available command on ftp prompts

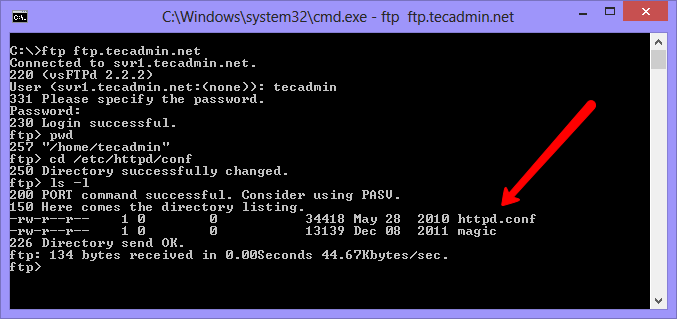
**cd** To change remote directory

**lcd** To change local directory.

**What is Chroot jail**

A chroot on Unix operating systems is an operation that changes the apparent disk root directory for the current running process

**Why use Chroot jail in VSFTPD ?**  
Chroot jail is used for that any user login to ftp cannot access filesystem outside of its home directory. For example if chroot is not enabled and login to ftp server and try to access any location like /etc/httpd/conf for /etc directories



As per above screenshot, you can see a normal user ‘tecadmin’ can view the apache configuration files. Although you can go anywhere ( all directories ) in system

**Enable Chroot Jail in VSFTPD :-**

To enable chroot jail in vsftp, Edit vsftp configuration file in your favorite editor

# vim /etc/vsftpd/vsftpd.conf

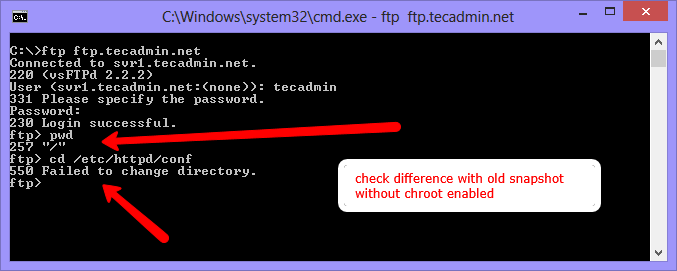
and un comment or add following entry in configuration file

chroot\_local\_user=YES

After adding above line, save file and restart vsftpd service.

# service vsftpd restart

Now your vsftp server has enabled chroot jail and all users has limited access to there home directory.  
Check the below screenshot created after enabling chroot jail and compare difference with old screenshot.



**You can see that now user ‘tecadmin’ has limited access to there home directory only**

**Create “chroot\_list” in /**etc/vsftp  **and Enter user name that you want to** ftp cannot access filesystem outside of its home directory.

Unument chroot\_local\_user=NO

chroot\_list\_enable=YES

chroot\_list\_file=/etc/vsftp/chroot\_list

**/etc/vsftpd/ftpusers:-**

The text file ftpusers contains a list of users that may not log in using the File Transfer Protocol (FTP) server daemon. This file is used not merely for system administration purposes but for improving security within a TCP/IP networked environment. It will typically contain a list of the users that either have no business using ftp or have too many privileges to be allowed to log in through the FTP server daemon. Such users usually include root, daemon, bin, uucp, and news.

# Users that are not allowed to login via ftp

root

bin

daemon

adm

lp

sync

shutdown

halt

mail

news

uucp

operator

games

nobody

**/etc/vsftpd/user\_list:-**

The user\_list file is one of those files that is acted upon differently depending on the invocation of a boolean directive in the vsftpd.conf file. If userlist\_deny=NO in the vsftpd.conf file then it will only allow users in this file. If it is equal to YES which is the default, then the users in this file are not allowed to login via FTP and no password will be prompted for.

# vsftpd userlist

# If userlist\_deny=NO, only allow users in this file

# If userlist\_deny=YES (default), never allow users in this file, and

# do not even prompt for a password.

# Note that the default vsftpd pam config also checks /etc/vsftpd/ftpusers

# for users that are denied.

root

bin

daemon

adm

lp

sync

shutdown

halt

mail

news

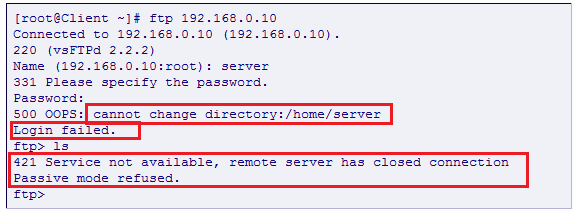
uucp

operator

games

nobody

* **supoose we faceing following type of Error :**



Then that time run following command : -

# getsebool –a | more

Check “ ftp\_home\_dir 🡪 on ” suppose this is off then run following comaand to on ftp\_home\_dir

# setsebool –P ftp\_home\_dir 1

