

Linux Network Services: File Transfer Protocol (FTP)

*This material is based on work supported by the
National Science Foundation under Grant No. 0802551*



*Any opinions, findings, and conclusions or recommendations expressed in this material are those of
the author (s) and do not necessarily reflect the views of the National Science Foundation*

Lesson Overview

The file transfer protocol is the standard protocol to transfer a file between two computers on the internet. Like http, SMB, and email, FTP (file transfer protocol) uses TCP/IP to accomplish file transfers.

In this lesson, you will explore the FTP protocol and learn how to install an FTP server on a Fedora-based system.

Learning to use FTP is a critical function for a budding Linux administrator who wishes to access files stored on remote servers, or simply wish to transfer files from one computer to the next.



Objective

You should know what will be expected of you when you complete this lesson. These expectations are presented as objectives. Objectives are short statements of expectations that tell you what you must be able to do, perform, learn, or adjust after reviewing the lesson.

Lesson Objective:

Given a need to transfer files, a student will be able to select an appropriate FTP server and configure it for file transfer services as per industry standards.



Lesson Outline

In this lesson, you will explore:

- ❖ **FTP Protocol**

- ❖ Function of the FTP server
- ❖ Implications of hosting an FTP server

- ❖ **Installation of an FTP server**

- ❖ FTP on Fedora
- ❖ Configuration
- ❖ Testing and Access



Resources and Notes

This lesson is built using Fedora. To complete this lesson successfully, you must have access to:

- ❖ Fedora Linux on bare metal or as a virtual install
- ❖ 10 Gb of hard drive space dedicated to the operating system's use
- ❖ A command shell
- ❖ Internet for research
- ❖ Word processor

Use the resources on the right to configure your system for Fedora.

Resources:

- [Download Virtualbox](#)
- [Virtualbox for Linux Hosts](#)
- [Install Fedora to Virtualbox](#)
- [Virtualbox manual](#)
- [Using Virtualbox with Ubuntu](#)
(process similar to Fedora)

Introduction

The file transfer protocol is the standard protocol to transfer a file between two computers on the Internet. Like http, smb, and email, FTP (file transfer protocol) uses TCP/IP to transfer files.

The client, or the one using the server, can access FTP through a simple command line interface or a graphical interface. Many web browsers, such as Firefox and Internet Explorer also allow access to FTP servers.

The client logs into the server with an assigned username, or for publically accessible files, the client connects using an anonymous FTP service where the user name is “**anonymous**” and the password is the user’s email address.

FTP uses port 21 and port 20 on the TCP/IP stack.

It is important to remember that the FTP protocol is built from the Telnet protocol which is no longer used because it is insecure. The telnet protocol sends all information over the Internet in plain text, and the FTP protocol is no different. All information sent over FTP is available to anyone that chooses to snoop or eavesdrop using port-sniffing tools.

Do not transfer confidential or sensitive information in this manner.

Required Reading

- [File Transfer Protocol](#)
- [FTP Setup](#)

CLI FTP Use

The command line FTP client is accessed by typing:

ftp hostname.com

at the command prompt (replace hostname.com with a valid ftp server domain name or IP address).

Once connected, the user uses the command line to type commands to send, receive, or view files. The user can type **help** at any time to see a list of available commands.

Once the user is done using the ftp client, he or she will type **quit** to close all connections and exit the client software.

On a Fedora system, the administrator may have to install FTP by typing:

yum install ftp

from the command line prior to first use.

Suggested Reading

- [File Transfer Protocol](#)

What is VSFTPD?

Vsftpd is a GPL (Open Source) FTP server for Unix (therefore Linux) systems. It means **Very Secure File Transfer Protocol Daemon**. VSFTPD is secure and extremely fast. It is also stable and is used by *kernel.org* for the distribution of the Linux kernel. VSFTPD has the reputation for being an extremely mature and trusted FTP server. Additionally it is an extremely small package and does not use much disk space or memory for its operation. Though small, it has a number of important features. These features include:

- ❖ Ability to support virtual IP configurations
- ❖ Ability to support virtual users
- ❖ Standalone or inetd operation
- ❖ Per user configuration
- ❖ Bandwidth throttling
- ❖ IPv6 capability
- ❖ SSL encryption support
- ❖ Anonymous FTP access (both read and write)
- ❖ Local user access

Many of these configurations require more in-depth discussion than the contents of this lesson. However, you can always type **man vsftpd.conf** at any command line prompt to view the configuration options that enable additional functionality.

Suggested Reading

- [FTP for Unix](#)

Installing VSFTP

We are going to install Vsftpd on a Fedora system in this lesson. Why Fedora? Because it closely resembles RedHat in functionality and stability for a server. Vsftpd is used in large scale server environments and it would most likely be found on a RedHat-based build.

Follow these steps to install VSFTPD on your Fedora server. If you do not have a Fedora server available to you, return to the beginning of the course and follow the directions to install one.

1. Open or log into a terminal window as root.
2. Type: **yum upgrade**
3. Accept and allow the necessary software upgrades.
4. Type: **yum install vsftpd**
5. Accept any dependencies that need to be installed.
6. Once back at the command line, it is time to configure your server.

Select **PLAY** for a video on VSFTPD install.



View Video
VideoLesson10VSFTPInst
all(C4L10S9).mp4

Required Reading

- [Installing VSFTPD](#)

See screen captures of the install process on the next screen.

Installing VSFTPD (Images)

```
File Edit View Search Terminal Help
[root@cmvirtbox cmolnar]# yum install vsftpd
Loaded plugins: langpacks, presto, refresh-packagekit
Adding en_US to language list
Setting up Install Process
```

Image capture of yum
install of vsftpd

```
Fedora 32 [Running]
Applications Places System Sun May 1, 2:10 PM Christopher Molnar
cmolnar@cmvirtbox:/home/cmolnar
File Edit View Search Terminal Help
[cmolnar@cmvirtbox ~]$ yum upgrade
Loaded plugins: langpacks, presto, refresh-packagekit
Adding en_US to language list
You need to be root to perform this command.
[cmolnar@cmvirtbox ~]$ su
Password:
[root@cmvirtbox cmolnar]# yum upgrade
Loaded plugins: langpacks, presto, refresh-packagekit
Adding en_US to language list
Setting up Upgrade Process
No Packages marked for Update
[root@cmvirtbox cmolnar]# █
```

Image capture of yum
upgrade process


Initial Configuration of VSFTPD

VSFTPD is configured through the use of the `/etc/vsftpd.conf` file. There is an initial configuration file installed with the server but it is extremely insecure to use the default files. Follow these directions to secure and configure your system:

From the root login in terminal or on the console:

1. Type: `cd /etc/vsftpd`
2. Type: `mv vsftpd.conf vsftpd.conf.old`
3. Type: `vi vsftpd.conf`
4. Type `i` to go into insert mode in vi.
5. Enter the code on the right and press ESC when complete:
6. Type: `:w` to save file
7. Type: `:x` to exit vi

Review the next screen for a video on the configuration process.



```
Anonymous_enable=YES
Local_enable=YES
Write_enable=YES
Listen=YES
Dirmessage_enable=YES
Xferlog_enable=YES
Connect_from_port_20=YES
Xferlog_file=/var/log/vsftpd.log
Xferlog_std_format=YES
Ftpd_banner>Welcome to my test server.
Pam_service_name=vsftpd
Userlist_enable=YES
Tcp_wrappers=YES
```

VSFTPD Configuration (Image)

```
File Edit View Search Terminal Help
[root@cmvirtbox cmolnar]# cd /etc/vsftpd
[root@cmvirtbox vsftpd]# ls
ftpusers      vsftpd.conf          vsftpd.conf.old
user_list     vsftpd_conf_migrate.sh
[root@cmvirtbox vsftpd]# █
```

Select **PLAY** for a video on VSFTPD configuration.

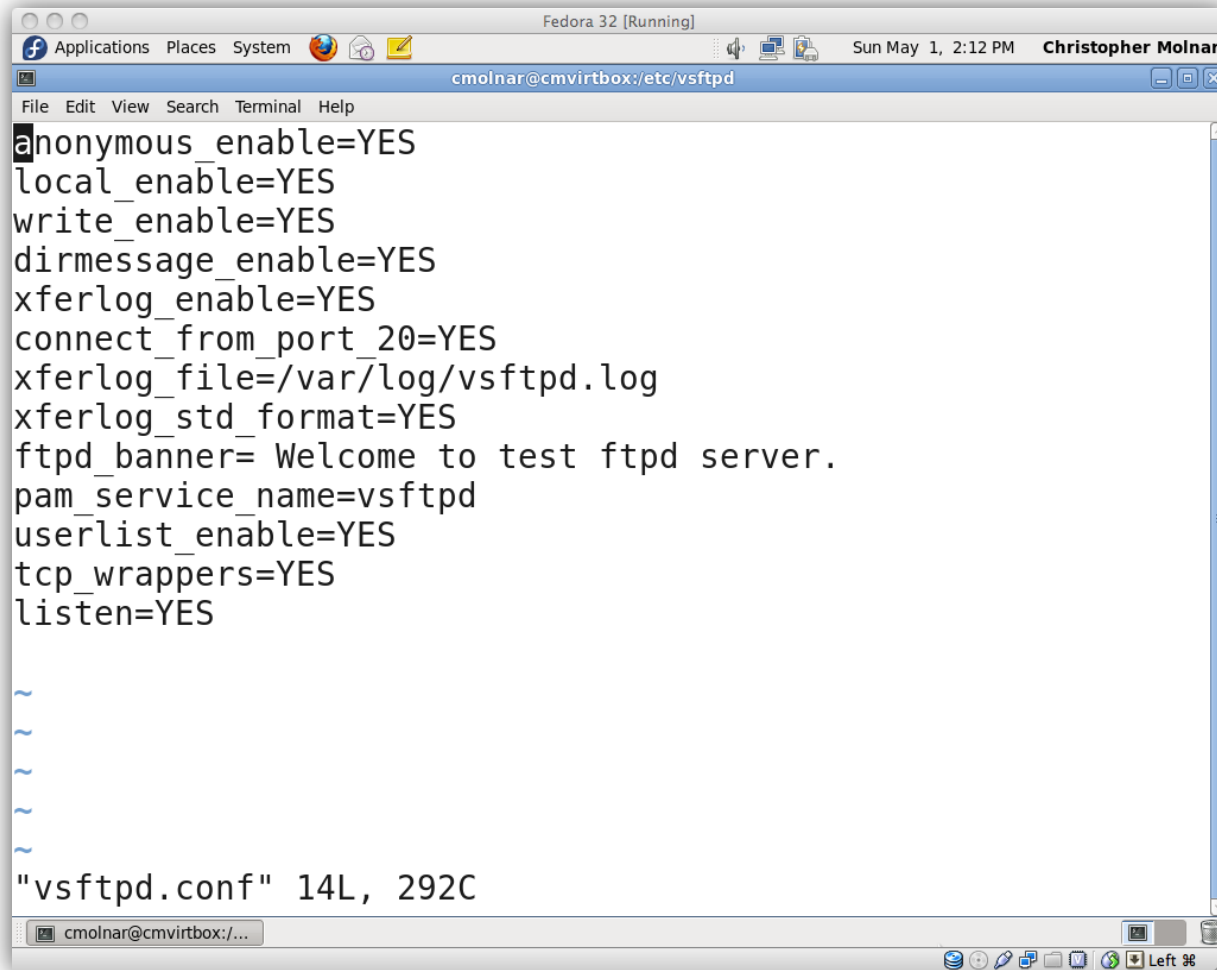


View Video
VideoLesson10VSFTPDC
onfig(C4L10S12).mp4

Recommended Reading

- [VSFTPD Configuration](#)

Configuring VSFTPD (Image)



```
cmolnar@cmvirtbox:/etc/vsftpd
File Edit View Search Terminal Help
anonymous_enable=YES
local_enable=YES
write_enable=YES
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_file=/var/log/vsftpd.log
xferlog_std_format=YES
ftpd_banner= Welcome to test ftpd server.
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
listen=YES

~
~
~
~
~
"vsftpd.conf" 14L, 292C
cmolnar@cmvirtbox:/...
```

Screen capture of VSFTPD configuration code

Explanation of Code

Starting from the top of our configuration (See code on right:)

Line 1: We will allow anonymous users.

Line 2: We are also allowing local users to log in using *userid* and *password*.

Line 3: We will allow users to upload files providing they have proper authentication and permissions.

Line 4: We are allowing the server to run in standalone listen mode without the use of any additional software.

Line 5: We are telling the server to send a message regarding the directories into which the user changes.

Line 6: We are going to log activities in the xferlog.

Line 7: We are allowing the use of port 20 and connections from that port. Port 20 is the default data port for FTP.

1. Anonymous_enable=YES
2. Local_enable=YES
3. Write_enable=YES
4. Listen=YES
5. Dirmessage_enable=YES
6. Xferlog_enable=YES
7. Connect_from_port_20=YES
8. Xferlog_file=/var/log/vsftpd.log
9. Xferlog_std_format=YES
10. Ftpd_banner>Welcome to my test server.
11. Pam_service_name=vsftpd
12. Userlist_enable=YES
13. Tcp_wrappers=YES

Suggested Review:

- [VSFTPD Configuration](#)

Explanation of Code (Contd)

Line 8: We set the location and name of our xferlog in the `/var/log` directory.

Line 9: We tell the server to use the standard xferlog format so automated statistical tools will work.

Line 10: We set an FTP banner that is displayed on login by the user that identifies our system and gives required information.

Line 11: We tell what name the PAM authentication server is expecting for user login.

Line 12: We tell the server that we are going to use the `userlist` file that prevents certain names from accessing the system.

Line 13: We tell the server we are using TCP wrappers (always use this).

There are many additional configuration options that can change the way your system operates, but these are the basic options that will allow you to operate a basic FTP server.

1. Anonymous_enable=YES
2. Local_enable=YES
3. Write_enable=YES
4. Listen=YES
5. Dirmessage_enable=YES
6. Xferlog_enable=YES
7. Connect_from_port_20=YES
8. Xferlog_file=/var/log/vsftpd.log
9. Xferlog_std_format=YES
10. Ftpd_banner>Welcome to my test server.
11. Pam_service_name=vsftpd
12. Userlist_enable=YES
13. Tcp_wrappers=YES

Starting VSFTPD

We have now installed VSFTPD on your test Fedora server. Now, it is time to start and test it. Follow these directions from your command line:

1. Type: **ftp localhost**
2. Make sure you do not already have a working ftp server running. If you do not, you should see a message that the “connection was denied.” This is a good thing.
3. Type **quit** to exit FTP.
4. Type: **service vsftpd start**

You should see a message that says: *starting vsftpd [OK]*

It is now time to test your installation.

Select **PLAY** for a video on starting VSFTP.



View Video
VideoLesson10VSFTPStarting(C4L10S16).mp4

```
File Edit View Search Terminal Help
[root@cmvirtbox vsftpd]# service vsftpd restart
Shutting down vsftpd:           [ OK ]
Starting vsftpd for vsftpd:    [ OK ]
[root@cmvirtbox vsftpd]# █
```

Image capture starting VSFTP

Testing Anonymous Access

The first access level we are going to test is the anonymous access. In order to do this please follow these directions:

From the command line or terminal:

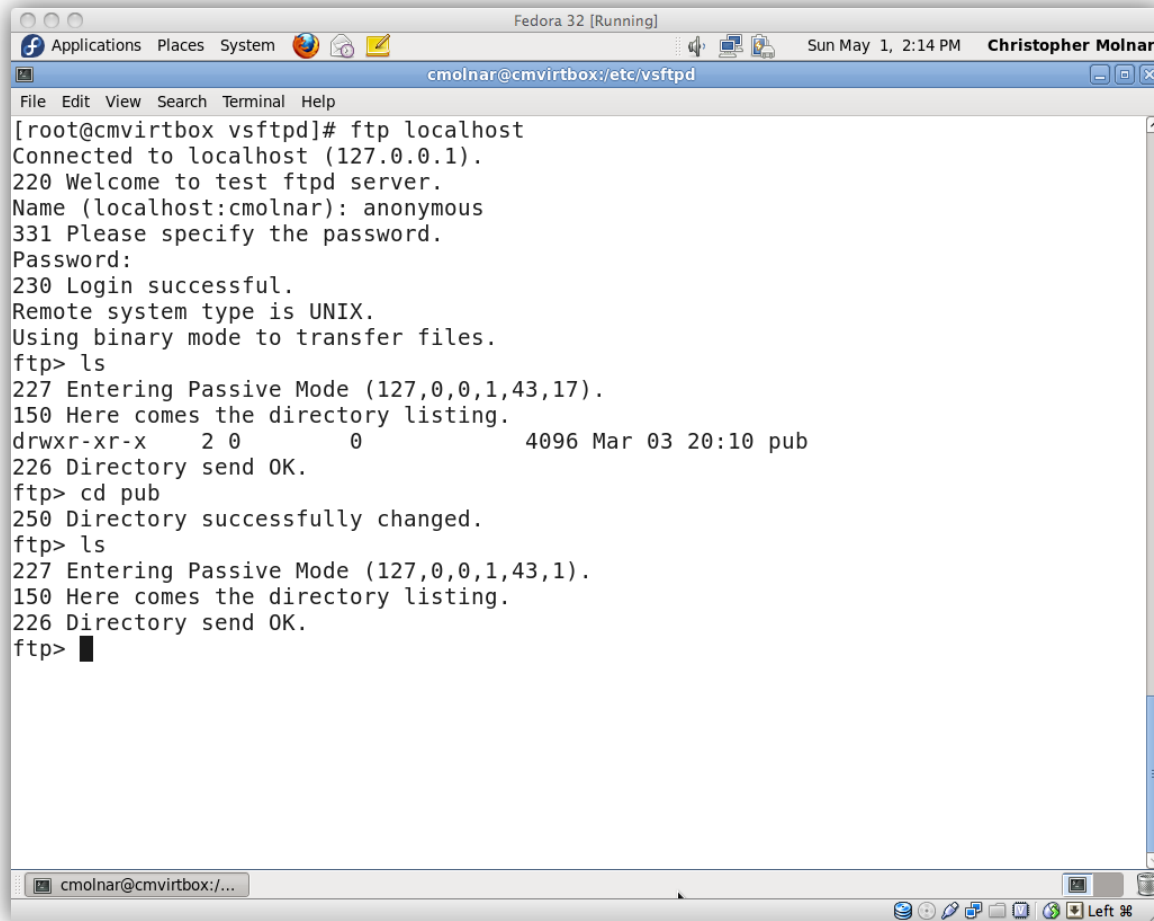
1. Type: **ftp localhost** (If you need to install ftp you will be told at this time.)
2. Type **anonymous** at the login prompt.
3. Type your *email address* at the password prompt. (You should see a message that states “login accepted.”)
4. Type: **cd pub** (You should see a message that you have changed to the *pub* directory.)
5. Type: **ls** (You should receive a directory listing.)
6. Type: **quit** (You should exit ftp and be back at a command line.)

If all the steps worked in the above sequence, your ftp server is setup properly to handle anonymous logins. If one or more of the steps did not work, you can look at the system and *xferlogs* to find the problem.

Double-check your configuration file and make sure you are not trying to log in with a user name found in the */etc/vsftpd/userlist* file.

Review the image capture of this testing process on the next screen. Since anonymous is working properly, let us ensure the local user login is working as well.

Anonymous Access (Contd)



The screenshot shows a terminal window titled "Fedora 32 [Running]" with the user "Christopher Molnar". The terminal session is as follows:

```
[root@cmvirtbox vsftpd]# ftp localhost
Connected to localhost (127.0.0.1).
220 Welcome to test ftpd server.
Name (localhost:cmolnar): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (127,0,0,1,43,17).
150 Here comes the directory listing.
drwxr-xr-x  2 0      0          4096 Mar 03 20:10 pub
226 Directory send OK.
ftp> cd pub
250 Directory successfully changed.
ftp> ls
227 Entering Passive Mode (127,0,0,1,43,1).
150 Here comes the directory listing.
226 Directory send OK.
ftp> █
```

*Image capture testing
anonymous FTP login.*

Local User Login

The first access level we are going to test is the anonymous access. In order to do this please follow these directions:

From the command line or terminal

1. Type: **ftp localhost** (If you need to install ftp you will be told at this time.)
2. Type your *user name* on the local system at the login prompt.
3. Enter your *password* at the logging prompt. (You should see a message that states login accepted.)
4. Type: **ls** (You should see a directory listing of your home directory on your test server.)
5. Type: **cd Desktop**
6. Type: **ls** (You should receive a directory listing of your desktop.)
7. Type: **quit** (You should exit ftp and return to the command line.)

If all the steps worked in the above sequence, your ftp server is setup properly to handle local user logins. If one or more of the steps above did not work, you can look at the system and *xferlogs* to find the problem.

Double-check your configuration file and make sure you are not trying to log in with a user name found in the */etc/vsftpd/userlist* file.

Recommended Reading

- [Manpage of VSFTP](#)
- [Securing VSFTPD](#)

Access of FTP Users

It is very important to understand the level of access FTP users have to your file system.

The first type of user, the **anonymous user** is “jailed” or chroot’d to the `/var/ftp` directory. By being jailed to this directory, anonymous users are unable to get to any other directory on the system, and they are unable to download configuration files (from the `/etc` or other directories). Limiting users to the `/var/ftp` directory is the safest form of FTP access on your system.

The second type of user is the **local user**. In our example, we setup the local user to have default access. If local users wish to change to the `/etc` directory and download files, they can make the change as long as their local `userIDs` have rights to that directory and the files within it. If local users have rights to the `/etc` directory, they can copy configuration files from the system. To prevent this access, add the following line to your configuration file:

```
chroot_local_user=YES
```

The line above will “jail” or chroot local users to their own home directory (`/home/username`) and will not allow them to browse the rest of the system. Another configuration option will allow you to list specific users that are not “jailed” to their home directory. This option is also followed by a second line that lists the name of the configuration file. For example:

```
chroot_file_enabled=YES  
chroot_list_file=/etc/chroot_allow
```

It is recommended that on any commercial or publically accessible server, these three options are used.

Lesson Summary

In this lesson, we discussed FTP and explored the purpose of FTP servers. Then we installed, configured, and started an FTP server using the `vsftpd` package. Following that, we tested both anonymous and local user logins.

Many additional options are available for the VSFTPD server. They are found in the `vsftpd.conf` manual pages. If you are tempted to use any of the options, be sure to read the instructions carefully.

Finally, we discussed how users are able to access various files and directories and recommended using the `chroot` command to “jail” or limit users to specific directories. Use `chroot` to protect your configuration files from unauthorized copying that may be used to gain unauthorized access to your server.

To finish this lesson, you should explore and complete the labs, participate in the discussion boards, and then take the quiz for the lesson.

Recommended Reading

- ❖ [Configuring VSFTPD](#)
- ❖ [FTP Server](#)
- ❖ [Linux FTP setup](#)