

下一篇文章学习FTP协议过程中需要实际抓包验证，本文以在云服务器centos系统上为例介绍如何安装FTP服务。

一、简单概述

1.1、什么是FTP?

FTP 是一种数据传输协议，负责将我们电脑上的数据与服务器数据进行交换。专业的说，**FTP**（全称：**File Transfer Protocol**）是 **TCP/IP** 网络上两台计算机传送文件的协议，**FTP** 是在 **TCP/IP** 网络和 **INTERNET** 上最早使用的协议之一，它属于网络协议组的应用层。

所以，**FTP** 是一个古老的文件传输协议，是互联网协议的化石级别协议，下节我们会再来细说。

1.2 什么是客户端和服务端?

客户端实际上就是我们的电脑、手机等设备上安装的一些软件，比如典型的就是浏览器。我们可以登录浏览器输入 www.baidu.com 连接百度服务器。

那么什么是服务端呢？服务端有个最大的特点是：24小时不间断工作。就是一个任劳任怨的铁人。比如我们用微信客户端发消息，实际上背后是24小时工作的微信服务端，消息都是通过服务端进行传输和转发的。

这里说到24小时工作，实际上我们每个人电脑也可以作为服务器对外服务，不过不幸的是，我们的电脑会经常关机甚至死机。

另外，服务器一般都是选用 **linux**，因为它的诸多优点：稳定、安全性更高、开源、免费、轻量级，天生适合作为服务器系统，只要地球不爆炸，他就永远不倒下！

1.3 什么是 **FTP** 服务器呢?

简单的说 **FTP** 服务器就是一台存储文件的服务器，供用户上传或下载文件。

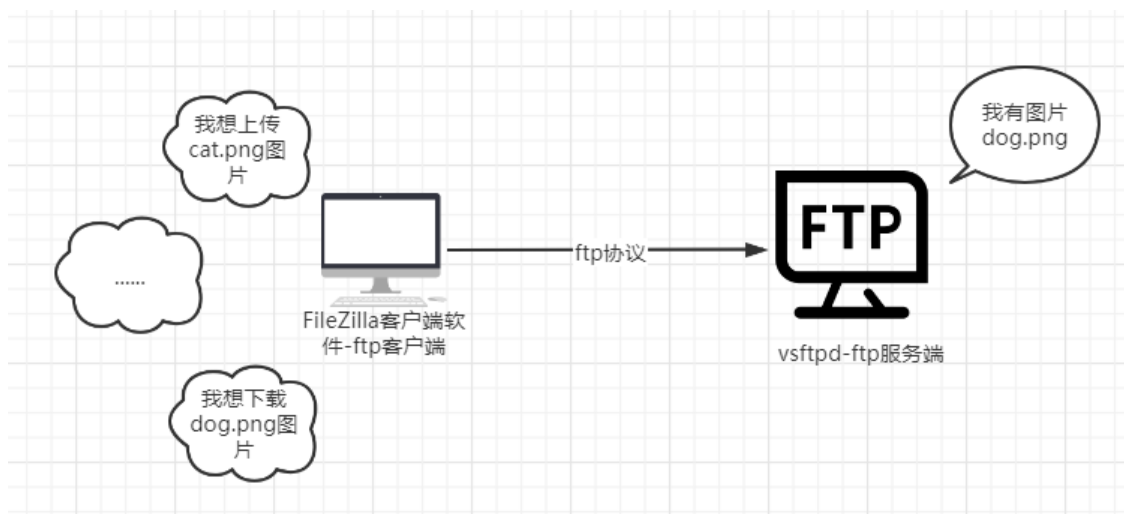
本文要搭建的 **vsftpd** 是一个完全免费的、开放源代码的ftp服务器软件，最大的特点是安全。当然了，还有很多其他的 **ftp** 服务器软件。安装了 **vsftpd** 的主机就是 **FTP** 服务器，可以对外提供 **FTP** 服务。

1.4 下文中有个工具叫 **FileZilla**，这是啥?

FileZilla 是一个免费开源的适合 **Windows**、**Mac** 和 **Linux** 的 **FTP** 客户端软件。可以通过这个软件，输入 **FTP** 服务器的地址、用户名、密码，就可以连接上去，通过这个可视化软件，可以连接到 **vsftpd** 上，可以将任何格式的文件上传到服务器上，或者从服务器上下载下来文件。

当然了，也可以通过代码来模拟一个客户端，来实现文件的上传和下载。

下面图示下关系：



二、环境介绍

Linux 使用的是 **Centos** 系统，版本为：

```
[root@VM-0-13-centos ftp]# cat /etc/redhat-release
CentOS Linux release 7.8.2003 (Core)
```

所安装的 **vsftpd** 版本是 **yum** 上最新的：

```
[root@VM-0-13-centos ftp]# rpm -q vsftpd
vsftpd-3.0.2-28.el7.x86_64
```

开始前，需要保证是以 **sudo** 权限的用户操作的。

三、安装vsftpd

查询是否已安装 **vsftpd**：

```
[root@VM-0-13-centos ~]# rpm -q vsftpd
package vsftpd is not installed
```

没有则进行安装，有可以先卸载，卸载文末有介绍。

```
sudo yum install vsftpd
```

```
[root@VM-0-13-centos ~]# yum -y install vsftpd
Loaded plugins: fastestmirror, langpacks, product-id, search-disabled-repos, subscription-manager
This system is not registered with an entitlement server. You can use subscription-manager to register.

Determining fastest mirrors
epel
extras
os
updates
(1/5): extras/7/x86_64/primary_db
(2/5): epel/7/x86_64/updateinfo
(3/5): updates/7/x86_64/primary_db
(4/5): epel/7/x86_64/primary_db
(5/5): os/7/x86_64/primary_db
Resolving Dependencies
--> Running transaction check
--> Package vsftpd.x86_64 0:3.0.2-28.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                                           Arch
=====
Installing:
vsftpd                                           x86_64

Transaction Summary

=====
Install 1 Package

Total download size: 172 k
Installed size: 353 k
Downloading packages:
vsftpd-3.0.2-28.el7.x86_64.rpm
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : vsftpd-3.0.2-28.el7.x86_64
  Verifying  : vsftpd-3.0.2-28.el7.x86_64

Installed:
vsftpd.x86_64 0:3.0.2-28.el7

Complete!
[root@VM-0-13-centos ~]# rpm -q vsftpd
vsftpd-3.0.2-28.el7.x86_64
[root@VM-0-13-centos ~]#
```

```
#设置开机启动
systemctl enable vsftpd.service

#启动
systemctl start vsftpd.service

#停止
systemctl stop vsftpd.service

#查看状态
systemctl status vsftpd.service

#重启
```

```
systemctl restart vsftpd.service
```

启动vsftpd服务器

```
# 设置开机启动
systemctl enable vsftpd.service

# 启动vsftpd服务器
systemctl start vsftpd.service

# 查看启动状态
systemctl status vsftpd.service
```

```
[root@VM-0-13-centos ~]# systemctl enable vsftpd
Created symlink from /etc/systemd/system/multi-user.target.wants/vsftpd.service to /usr/lib/systemd/system/vsftpd.service.
[root@VM-0-13-centos ~]# systemctl start vsftpd.service
[root@VM-0-13-centos ~]# ps -ef | grep vsftpd
root      17428      1  0 11:51 ?        00:00:00 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf
root      17511 15805  0 11:51 pts/0    00:00:00 grep --color=auto vsftpd
[root@VM-0-13-centos ~]# systemctl status vsftpd.service
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Sat 2020-11-21 11:51:11 CST; 44s ago
     Process: 17427 ExecStart=/usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf (code=exited, status=0/SUCCESS)
    Main PID: 17428 (vsftpd)
   CGroup: /system.slice/vsftpd.service
           └─17428 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

Nov 21 11:51:11 VM-0-13-centos systemd[1]: Starting Vsftpd ftp daemon...
Nov 21 11:51:11 VM-0-13-centos systemd[1]: Started Vsftpd ftp daemon.
[root@VM-0-13-centos ~]#
```

四、vsftpd配置文件

```
[root@VM-0-13-centos ~]# cd /etc/vsftpd/
[root@VM-0-13-centos vsftpd]# ll
total 20
-rw-r--r-- 1 root root 125 Oct 14 00:10 ftpusers
-rw-r--r-- 1 root root 361 Oct 14 00:10 user_list
-rw-r--r-- 1 root root 5116 Oct 14 00:10 vsftpd.conf
-rwxr--r-- 1 root root 338 Oct 14 00:10 vsftpd_conf_migrate.sh
[root@VM-0-13-centos vsftpd]# cp vsftpd.conf vsftpd.conf.bak
[root@VM-0-13-centos vsftpd]# ll
total 28
-rw-r--r-- 1 root root 125 Oct 14 00:10 ftpusers
-rw-r--r-- 1 root root 361 Oct 14 00:10 user_list
-rw-r--r-- 1 root root 5116 Oct 14 00:10 vsftpd.conf
-rw-r--r-- 1 root root 5116 Nov 21 15:51 vsftpd.conf.bak
-rwxr--r-- 1 root root 338 Oct 14 00:10 vsftpd_conf_migrate.sh
[root@VM-0-13-centos vsftpd]#
```

配置文件路径

备份

修改配置文件如下，修改了三个地方，已标注出来，具体参数的含义参考此链接：

<https://www.cnblogs.com/sopcce/p/10743359.html>

```
[root@centos-7-06-64-206 ~]# vi /etc/vsftpd/vsftpd.conf

# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample
file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
```

```
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd
options.
# Please read the vsftpd.conf.5 manual page to get a full idea of
vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment
this out).
#anonymous_enable=YES
# 修改点1: 取消匿名登录
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
# When SELinux is enforcing check for SE bool ftp_home_dir
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# 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)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files.
This only
# has an effect if the above global write enable is activated.
Also, you will
# obviously need to create a directory writable by the FTP user.
# When SELinux is enforcing check for SE bool
allow_ftp_d_anon_write, allow_ftp_d_full_access
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to
create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when
they
# go into a certain directory.
dirmessage_enable=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
```

```
#
# 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 by
# 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 shown
# below.
#xferlog_file=/var/log/xferlog
xferlog_file=/var/log/xferlog
#
# 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 case.
xferlog_std_format=YES
#
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
#
# You may change the default value for timing out a data
connection.
#data_connection_timeout=120
#
# 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=ftpsecure
#
# 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
#
# By default the server will pretend to allow ASCII mode but in
fact ignore
```

```
# the request. Turn on the below options to have the server
actually do ASCII
# mangling on files when in ASCII mode. The vsftpd.conf(5) man page
explains
# the behaviour when these options are disabled.
# Beware that on some FTP servers, ASCII support allows a denial of
service
# attack (DoS) via the command "SIZE /big/file" in ASCII mode.
vsftpd
# predicted this attack and has always been safe, reporting the
size of the
# raw file.
# ASCII mangling is a horrible feature of the protocol.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
ftpd_banner=sopcce.com welcome to ftp service,
#
# You may specify a file of disallowed anonymous e-mail addresses.
Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd/banned_emails
#
# You may specify an explicit list of local users to chroot() to
their home
# directory. If chroot_local_user is YES, then this list becomes a
list of
# 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)
# 修改点2: 希望限制ftp用户只能在其主目录下活动, 不允许他们跳出主目录之外浏览服
务器上的其他目录
chroot_list_enable=YES
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd/chroot_list
#
# You may activate the "-R" option to the builtin ls. This is
disabled by
```

```
# default to avoid remote users being able to cause excessive I/O
on large
# sites. However, some broken FTP clients such as "ncftp" and
"mirror" assume
# the presence of the "-R" option, so there is a strong case for
enabling it.
#ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone
mode and
# listens on IPv4 sockets. This directive cannot be used in
conjunction
# with the listen_ipv6 directive.
listen=NO
#
# 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.
# Make sure, that one of the listen options is commented !!
listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES

# 修改点3: ADD 201900509
userlist_file=/etc/vsftpd/user_list
userlist_deny=NO
user_sub_token=$USER
local_root=/home/sopftpuser/ftp

allow_writeable_chroot=YES

pasv_min_port=30000
pasv_max_port=30010
```

保存好记得重启下。

添加用户：

```
# 新增一个叫sopftpuser的用户
[root@VM-0-13-centos vsftpd]# adduser sopftpuser
# 赋予密码
[root@VM-0-13-centos vsftpd]# passwd sopftpuser
Changing password for user sopftpuser.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
# 加到user_list中, 因为我们上面配置了userlist_deny=NO, 所以只有在user_list
文件中的用户才可以访问, 如果userlist_deny=YES, 则配置在user_list中的用户是不
允许访问的。
[root@VM-0-13-centos vsftpd]# echo "sopftpuser" | sudo tee -a
/etc/vsftpd/user_list
sopftpuser
```

创建FTP目录树并设置正确的权限：

```
mkdir -p /home/sopftpuser/ftp/
chmod 750 /home/sopftpuser/ftp/
chown -R sopftpuser: /home/sopftpuser/ftp
```

下面就要连接测试下了, 不过有个注意点, 我这里用的是云服务器, 我把防火墙全部关闭了, 否则就需要配置防火墙放开诸如 21 还有 30000-30010 的端口。我这里需要配置安全组, 放开端口才行。

安全组规则 关联实例

入站规则		出站规则	
添加规则	导入规则	排序	删除
一键放通	规则设置		
<input type="checkbox"/> 来源	协议端口	策略	备注
<input type="checkbox"/> 0.0.0.0/0	TCP:30000,30001,30002,30003,30004,30005,30006,30007,30008,30009,30010	允许	ftp被动模式端口
<input type="checkbox"/> 0.0.0.0/0	UDP:8301,8302,8600	允许	
<input type="checkbox"/> 0.0.0.0/0	TCP:8500,8300,8301,8302,8600	允许	consul-server访问端口
<input type="checkbox"/> 0.0.0.0/0	TCP:22	允许	放通Linux SSH登录
<input type="checkbox"/> 0.0.0.0/0	TCP:21	允许	21端口临时开放

我们可以先用 fileZilla 来连接, 设置如下, 否则会有 AUTH TLS 的错误:

主机(H): 端口(P):

协议(T):

加密(E):

登录类型(L):

用户(U):

密码(W):

背景颜色(B)

注释(M):

我新建了一个目录，并且上传了一张图片：

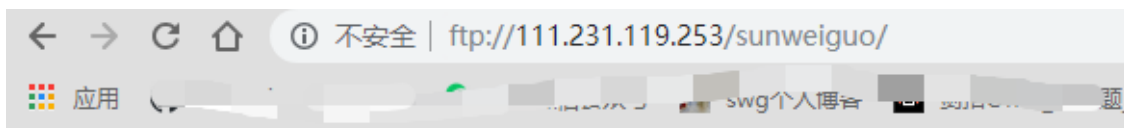
远程站点: /sunweiguog

/

sunweiguog

文件名	文件大小	文件类型	最近修改	权限	所有者/组
..					
network22-1.png	52,945	PNG 文件	2020/11/21 1...	-rw-r--r--	0 0

用谷歌浏览器访问也没啥问题：



/sunweiguo/ 的索引

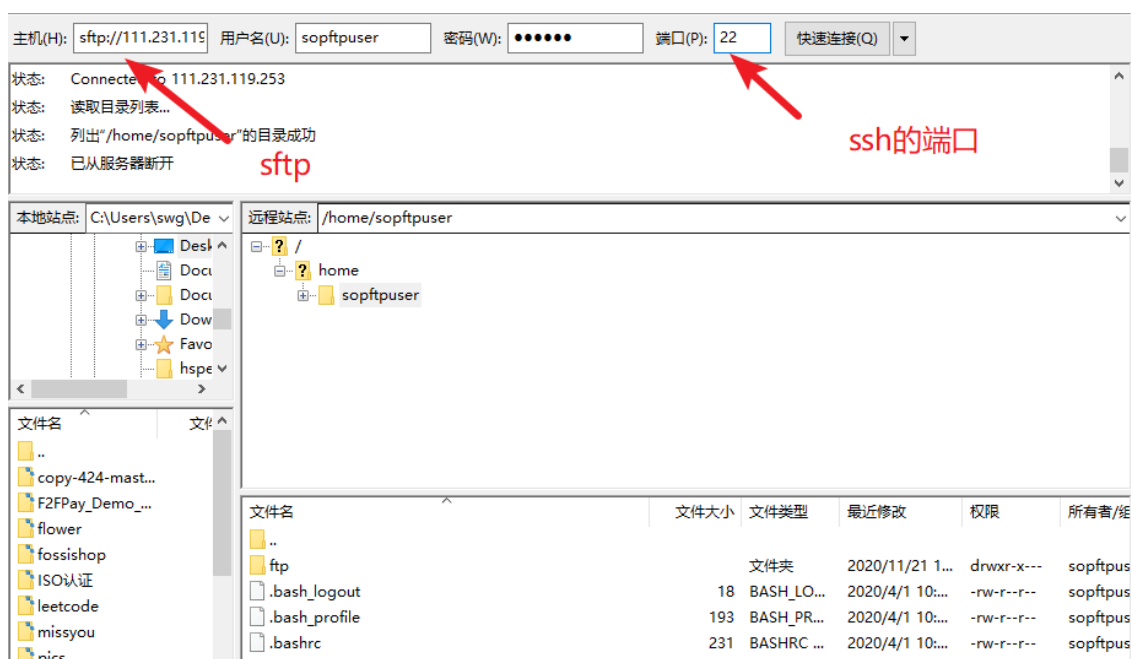
[上级目录]

名称	大小	修改日期
network22-1.png	51.7 kB	2020/11/21 上午11:50:00

进去的根目录就是我们设置的 `/home/sopftpuser/ftp`，并且也不能随便切换到其他的目录，达到了我们的目的。

上面提到了 `AUTH TLS` 错误，实际上是因为他是基于SSH的FTP：`sftp`，即安全的安全文件传送协议，通过对数据的加密实现安全的传输。我们下节分析下直接 `ftp` 协议的报文情况，就会知道极其不安全，连密码都暴露在报文中。

我们可以通过 `sftp` 协议进行直接的连接：



五、vsftpd卸载

检查是否安装及包名

```
[root@VM-0-13-centos ~]# rpm -qa | grep vsftpd
vsftpd-3.0.2-28.el7.x86_64
```

如果有服务则先关闭：

```
[root@VM-0-13-centos ~]# systemctl stop vsftpd.service
[root@VM-0-13-centos ~]# systemctl status vsftpd.service
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled;
  vendor preset: disabled)
   Active: inactive (dead) since Sat 2020-11-21 15:35:29 CST; 5s
 ago
   Process: 19647 ExecStart=/usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf
 (code=exited, status=0/SUCCESS)
   Main PID: 19649 (code=killed, signal=TERM)

Nov 21 12:01:46 VM-0-13-centos systemd[1]: Stopping Vsftpd ftp
daemon...
Nov 21 12:01:46 VM-0-13-centos systemd[1]: Stopped Vsftpd ftp
daemon.
Nov 21 12:01:46 VM-0-13-centos systemd[1]: Starting Vsftpd ftp
daemon...
Nov 21 12:01:46 VM-0-13-centos systemd[1]: Started Vsftpd ftp
daemon.
Nov 21 12:01:54 VM-0-13-centos vsftpd[19669]:
pam_unix(vsftpd:auth): check pass; user unknown
Nov 21 12:01:54 VM-0-13-centos vsftpd[19669]:
pam_unix(vsftpd:auth): authentication failure; logname= uid=0
euid=0 tt...1.140
Nov 21 15:35:29 VM-0-13-centos systemd[1]: Stopping Vsftpd ftp
daemon...
Nov 21 15:35:29 VM-0-13-centos systemd[1]: Stopped Vsftpd ftp
daemon.
Hint: Some lines were ellipsized, use -l to show in full.
```

备份配置文件卸载:

```
[root@VM-0-13-centos ~]# rpm -e vsftpd-3.0.2-28.el7.x86_64
warning: /etc/vsftpd/vsftpd.conf saved as
/etc/vsftpd/vsftpd.conf.rpmsave
[root@VM-0-13-centos ~]# rpm -qa | grep vsftpd
[root@VM-0-13-centos ~]#
```

如不需要备份配置文件则直接删除即可:

```
[root@VM-0-13-centos ~]# rm -rf /etc/vsftpd/vsftpd.conf.rpmsave
[root@VM-0-13-centos ~]#
```