FTP服务器的搭建，我要实现的需求是：

　　不允许匿名访问，因为我的机器不想让谁都能登录上来，随便获取文件，

　　需要锁定一个目录，因为在家里，我需要给媳妇下载一些电影 韩剧之类的东西，媳妇会来我机器下载，但是我不想让他随意操作我的东西。

　　万一删除我的配置文件，我就惨了（吐槽一下韩剧：媳妇问我，你都没看过韩剧怎么知道它不好看呢，我说：我没吃过屎 但是知道它一定不好吃！）

　　另外，需要本机也能访问，因为我要做一些关于FTP的测试。

　 不单独建立FTP用户，FTP也使用ubuntu桌面的用户进行登录和操作，

　　我还不希望FTP开始启动。

好了 我们开始安装，很简单。

sudo apt-get install vsftpd

30秒内估计就能安装完。

下面开始配置：

首先备份配置文件。

linuxidc@ubuntu:/etc/init$ cd /etc/

linuxidc@ubuntu:/etc$ sudo cp vsftpd.conf vsftpd.conf.old

接下来就是开始配置了，

咱们就针对需求来：

1. 不允许匿名访问，因为我的机器不想让谁都能登录上来，随便获取文件，

　　配置如下：

　　23 anonymous\_enable=NO

　　2.需要锁定一个目录，因为在家里，我需要给媳妇下载一些电影 韩剧之类的东西，

　　　媳妇会来我机器下载，但是我不想让他随意操作我的东西。

　　　万一删除我的配置文件，我就惨了

　　配置如下：

　　152 local\_root=/home/linuxidc/公共的/FTP共享文件

备注：[FTP共享文件] 这个文件夹是我新建出来的

　　另外，需要本机也能访问，因为我要做一些关于FTP的测试。

　　配置如下：

　　26 local\_enable=YES

　 不单独建立FTP用户，FTP也使用ubuntu桌面的用户进行登录和操作，

　　配置如下：

　　120 #chroot\_local\_user=YES

　　121 chroot\_list\_enable=YES

　　122 # (default follows)

　　123 chroot\_list\_file=/etc/vsftpd.chroot\_list

　　这里需要/etc/vsftpd.chroot\_list 这个文件，如果没有请新建：

　　sudo gedit /etc/vsftpd.chroot\_list

　　内容如下（例如我桌面的用户名为linuxidc）：

duoduo

　　其实就是把你的用户名写进去

　　我还不希望FTP开始启动。 一会单独说！

贴出我的配置文件。

# Example config file /etc/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.  
#  
#  
# Run standalone?  vsftpd can run either from an inetd or as a standalone  
# daemon started from an initscript.  
listen=YES  
#  
# Run standalone with IPv6?  
# Like the listen parameter, except vsftpd will listen on an IPv6 socket  
# instead of an IPv4 one. This parameter and the listen parameter are mutually  
# exclusive.  
#listen\_ipv6=YES  
#  
# Allow anonymous FTP? (Disabled by default)  
anonymous\_enable=NO  
#  
# Uncomment this to allow local users to log in.  
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.  
#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  
#  
# If enabled, vsftpd will display directory listings with the time  
# in  your  local  time  zone.  The default is to display GMT. The  
# times returned by the MDTM FTP command are also affected by this  
# option.  
use\_localtime=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/vsftpd.log  
#  
# 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.  
# 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 linuxidc's 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 restrict local users to their home directories.  See the FAQ for  
# the possible risks in this before using chroot\_local\_user or  
# chroot\_list\_enable below.  
#chroot\_local\_user=YES  
#  
# 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)  
#chroot\_local\_user=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  
#  
# Customization  
#  
# Some of vsftpd's settings don't fit the filesystem layout by  
# default.  
#  
# This option should be the name of a directory which is empty.  Also, the  
# directory should not be writable by the ftp user. This directory is used  
# as a secure chroot() jail at times vsftpd does not require filesystem  
# access.  
secure\_chroot\_dir=/var/run/vsftpd/empty  
#  
# This string is the name of the PAM service vsftpd will use.  
pam\_service\_name=vsftpd  
#  
# This option specifies the location of the RSA certificate to use for SSL  
# encrypted connections.  
rsa\_cert\_file=/etc/ssl/certs/ssl-cert-snakeoil.pem  
# This option specifies the location of the RSA key to use for SSL  
# encrypted connections.  
rsa\_private\_key\_file=/etc/ssl/private/ssl-cert-snakeoil.key  
#  
local\_root=/home/linuxidc/公共的/FTP共享文件

现在可以重启FTP了。

linuxidc@ubuntu:/etc$ sudo service vsftpd restart  
vsftpd stop/waiting  
vsftpd start/running, process 303

OK 看到这些 证明配置文件没有问题，FTP启动了

下面直接访问FTP 看看：

linuxidc@ubuntu:/etc$ ftp 127.0.0.1  
Connected to 127.0.0.1.  
Welcome to linuxidc's FTP service.  
Name (127.0.0.1:linuxidc): duoduo  
Please specify the password.  
Password:  
OOPS: vsftpd: refusing to run with writable root inside chroot()  
Login failed.  
Service not available, remote server has closed connection  
ftp>

居然报了一个500的错误  
vsftpd: refusing to run with writable root inside chroot()

。其实这里是需要特殊说明的，原因出在这里

120 #chroot\_local\_user=YES

121 chroot\_list\_enable=YES

122 # (default follows)

123 chroot\_list\_file=/etc/vsftpd.chroot\_list

我们用

chroot\_list\_enable=YES 和 chroot\_list\_file=/etc/vsftpd.chroot\_list配合使用，使得只有在vsftpd.chroot\_list中配置的用户才能登录FTP。

对于这要的配置有一个特殊的要求，就是vsftpd.chroot\_list里面配置的用户，对于前面local\_root配置的目录不能有写的权限！

也就是/home/linuxidc/公共的/FTP共享文件 这个文件夹 对于linuxidc这个用户不能有写的权限，

我们为了额操作方便可以这么做：

 sudo chown -R root:root /home/linuxidc/公共的/FTP共享文件/

这样，linuxidc这个用户对于/home/linuxidc/公共的/FTP共享文件没有写权限了，

现在重启FTP 重新登录看看：

linuxidc@ubuntu:/etc$ ftp 127.0.0.1  
Connected to 127.0.0.1.  
Welcome to linuxidc's FTP service.  
Name (127.0.0.1:linuxidc): duoduo  
Please specify the password.  
Password:  
Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>

OK  FTP 好了 可以登录了

但是我刚才 sudo chown -R root:root /home/linuxidc/公共的/FTP共享文件/ 这个操作 还带来了一个麻烦。就是FTP共享文件在我桌面登录时，不能任意复制粘贴操作文件了，但是我还要必须保持linuxidc用户对[FTP共享文件] 这个文件夹不可写。这该怎么办呢？

其实很简单，

cd /home/linuxidc/公共的/FTP共享文件  
sudo mkdir FTPFILES  
sudo chown -R linuxidc:duoduo FTPFILES

这样 就保持了 FTP共享文件 文件夹linuxidc用户不可写，但duoduo用户用可以在桌面登录时任意操作文件了，只不过此时的随意范围在FTPFILES文件夹范围呢了。

这样基本FTP服务基本搭建完成了。

对了 忘记了一点。就是不让FTP服务开机启动。操作如下：

linuxidc@ubuntu:/etc/init$ cd /etc/init/  
linuxidc@ubuntu:/etc/init$ sudo cp vsftpd.conf vsftpd.conf.old

编辑配置文件

sudo gedit /etc/init/vsftpd.conf

将#start on runlevel [2345] or net-device-up IFACE!=lo 修改为start on runlevel [345] 如下：

#start on runlevel [2345] or net-device-up IFACE!=lo  
start on runlevel [345]  
stop on runlevel [!2345]

这次重启FTP 重启系统 彻底完成。

这里建议大家查一下：chroot\_local\_user  chroot\_list\_enable=YES chroot\_list\_file=/etc/vsftpd.chroot\_list 相关的资料，这里面灵活性配置很高的。

玩转vsftpd服务器的四大高级配置：<http://www.linuxidc.com/Linux/2013-09/90565.htm>

vsFTPd配置教程：<http://www.linuxidc.com/Linux/2013-09/90562.htm>