第 12 章 FTP 服务器配置

实验任务：配合教材、课件，完成 Window、linux 环境下 ftp 服务器的配置，实现匿名用户的上传下载。

Linux FTP 实验

1. FTP 服务器的安装与配置文件解析

1. FTP 服务器的安装与启动

在进行 FTP 服务器配置之前，首先要检查系统中是否安装了 FTP 服务器。检查的方法可以使用如下命令：

#rpm –qa |grep vsftpd

如果在安装 RHEL6 时没有安装 vsftpd，可在光盘中的 Packages 目录中找到相关的 RPM 包，然后在终端中输入下面的命令来安装所需的 RPM 包：

#rpm –ivh vsftpd-2.2.2-1.el6.i686.rpm //vsftp 服务器软件

#rpm -ivh ftp-0.17-51.1.el6.i686.rpm //ftp 客户端命令

也可以使用 yum 命令在线安装，安装命令如下：

yum install vsftpd –y //安装服务器端软件

yum install ftp –y //安装 ftp 命令

设置 vsftp 服务开机启动：# chkconfig vsftpd on

安装完毕后，使用下面的命令来进行 FTP 服务器的启动、停止和重启：

#service vsftpd start //启动；#service vsftpd stop //停止；#service vsftpd restart //重启

使用下面的命令检查 vsftpd 服务的状态以及 vsftpd 是否被启动：

#service vsftpd status 或#pstree|grep vsftpd

2. vsftpd 服务器的配置文件

vsFTP 服务器的主要配置文件是/etc/vsftpd/vsftpd.conf。配置文件提供大量的参数设置以对服务器的运行模式、性能、安全属性、登录用户等具体配置。vsFTP 有两种运行模式：一种是独立（standalone）运行模式；一种是 xinetd（eXtended Internet Services Daemon，扩展的 Internet 服务守护进程）模式。两种模式运行机制不同，独立运行模式适合专业的 FTP 服务器，通常 FTP 总是一直有人访问，占用资源比较大。如果 FTP 服务器访问人数比较少，建议用 xinetd 模式。xinetd 模式通过 super daemon 监听端口，当客户端有 FTP 连接请求时，首先会将连接传至 super daemon，然后启动相应的 vsftp 服务进程。vsFTPD 将用户分为三类：匿名用户（anonymous user）、本地用户（local user）以及虚拟用户（guest）。 下面分别从以下几方面对配置文件中的参数进行介绍：

（1）服务器设置

listen=YES //使用 standalone 而不是 xinetd 模式启动 vsftpd

pam_service_name=vsftpd //服务器的验证方式

设置服务器的 port 工作模式

port_enable=YES //若启用此选项（默认启用），表示允许使用 PORT 模式数据传输。

connect_from_port_20=YES //设置 FTP 数据端口的数据连接，控制以 PORT 模式进行数据传输时是否使用 20 端口。

listen_port=2121 //从 2121 端口进行数据连接

服务器的 pasv 工作模式

pasv_enable=yes|no //是否将服务器设定为被动模式。

pasv_min_port=50000 //将服务器被动模式最小端口设在 50000

pasv_max_port=50010 //将服务器被动模式最大端口改在 50010

数据的传输模式

ascii_upload_enable= YES|NO //允许使用 ASCII 模式上传文件，默认不允许。

ascii_download_enable=YES|NO //控制是否允许使用 ASCII 模式下载文件。

性能与负载控制：

max_clients=200 //FTP 的最大连接数

max_per_ip=4 //每 IP 的最大连接数

Idle_session_timeout=600 //用户会话空闲后的端口时间，单位秒，即 10 分钟断开

data_connection_timeout=120 //将数据连接空闲 120 秒，即 2 分钟后断开

accept_timeout=60 //被动模式时，客户端空闲 1 分钟后将断开

connect_timeout=60 //中断 1 分钟后又重新连接

local_max_rate=50000 //本地用户传输率 50Kpbs

anon_max_rate=30000 //匿名用户传输率 30Kbps

服务器的欢迎信息设置

dirmessage_enable=YES //是否定制欢迎信息，也就是我们登入有些 FTP 之后，会出现的一些信息，如：欢迎您来到 LinuxSir FTP 等提示。

message_file=.message //定制.message 文件作为登录后的显示信息。

服务器的日志设置

xferlog_enable=YES //激活上传和下传的日志

xferlog_std_format=YES //使用标准的日志格式

文件操作设置

hide_ids=YES|NO //是否隐藏文件的所有者和组信息。若为 YES，当用户使用 ls –al 之类的指令时，在目录列表中所有文件的拥有者和群组信息都显示为 ftp。默认值为 NO。

ls_recurse_enable= **YES|NO** //是否可以使用 ls –R 命令。默认为 no。

用户登录设置

pam_service_name=vsftpd //**指出 vsFTPD 进行 PAM（Pluggable Authentication Modules）认证时所使用的 PAM 配置文件名，默认值是是/etc/pam.d/vsftpd。**

userlist_enable=**YES|NO** //是否开启 userlist 来限制用户访问的功能，如果想限制某些账户不能登录，可以创建个名为 user_list 的文件，将用户添加进去。

userlist_file=/etc/vsftpd/user_list //指出 userlist_enable 选项生效后，被读取的包含用户列表的文件。默认值是/etc/vsftpd.user_list。

userlist_deny=YES|NO 此选项在 userlist_enable 选项启动后才生效。决定禁止还是只允许由/etc/userlist_file 指定文件中的用户登录 FTP 服务器。YES，默认值，禁止文件中的用户登录，同时也不向这些用户发出输入口令的提示。若设为停用（即为 NO），则只允许在文件中的用户登录 FTP 服务器。

下面分别介绍匿名用户、本地用户以及虚拟用户相关的配置。

（2）针对匿名用户的设置

anonymous_enable=yes //允许匿名用户登录

no_anon_password=no //匿名登录时是否需要输入密码，默认为 NO

anon_world_readable_only=YES|NO //控制是否只允许匿名用户下载可阅读文档。YES，只允许匿名用户下载可阅读的文件。NO，允许匿名用户浏览整个服务器的文件系统。默认

值为 YES。

anon_upload_enable=yes //允许匿名用户上传

anon_upload_enable=YES|NO //控制是否允许匿名用户上传文件，YES 允许，NO 不允许，默认是 NO。注意：除了这个参数外，匿名用户要能上传文件，还需要两个条件：一是 write_enable 参数为 YES；二是 FTP 匿名用户对某个目录有写权限。

write_enable=yes //赋写权限

anon_mkdir_write_enable=yes //允许匿名用户新建文件夹

anon_umask=022 //设定匿名用户的权限掩码

anon_other_write_enable=YES|NO //控制匿名用户是否拥有除了上传和新建目录之外的其他权限，如删除、更名等。默认值为 NO。

chown_uploads=YES|NO //是否修改匿名用户所上传文件的所有权

chown_username=whoever //指定拥有匿名用户上传文件所有权的用户。此参数与 chown_uploads 联用。不推荐使用 root 用户。

anon_root= //设定匿名用户的根目录，即匿名用户登入后，被定位到此目录下。主配置文件中默认无此项，默认值为/var/ftp/。

ftp_username= //匿名用户所使用的系统用户名。主配置文件中默认无此项，默认 ftp。

no_anon_password=YES|NO //若值为 YES，表示匿名用户登录时，vsFTP 服务器不会要求用户输入密码。默认值为 NO。

deny_email_enable=YES|NO //此参数默认值为 NO。当值为 YES 时，拒绝使用 banned_email_file 参数指定文件中所列出的 e-mail 地址进行登录的匿名用户。也就是说，当匿名用户使用 banned_email_file 文件中所列出的 e-mail 进行登录时，被拒绝。当此参数生效时，需追加 banned_email_file 参数

banned_email_file=/etc/vsftpd.banned_emails //指定包含被拒绝的 e-mail 地址清单的文件，默认文件为/etc/vsftpd.banned_emails。

（3）本地用户设置

在使用 FTP 服务的用户中，除了匿名用户外，还有一类在 FTP 服务器所属主机上拥有账号的用户。vsFTP 中称此类用户为本地用户（local users），等同于其他 FTP 服务器中的 real 用户。

local_enable=yes //本地帐户能够登陆

local_root= //设定本地用户的 FTP 根目录，默认是其家目录

write_enable=no //是否具有写权限，如果为 yes 则允许删除和修改文件

local_umask=022 //设置本地用户的文件的掩码是 022，默认值是 077

chroot_local_user=yes //设置本地所有帐户都只能在自家目录里。如果只想让部分账户只能待在自家目录里，其他用户不受此限制的话，要结合接下来的 2 个参数。

chroot_list_enable=yes //启用通过列表来禁锢用户在其家目录中的功能

chroot_list_file=/etc/vsftpd/chroot_list //指定禁锢在家目录中的用户列表文件路径，将受限的用户写在此文件里，一行一个账户名。此文件名可以改。

（1）虚拟用户设置

pam_service_name= //服务器的验证方式，在虚拟用户中应添加相关的 pam 认证配置

guest_enable=YES|NO //若是启动这项功能，所有的不以匿名登录的用户，都视为“guest”类型，而此类用户的实际权限就是“guest_username”选项中所指定的帐号。默认不启用此选项。

guest_username=ftp //定义 vsFTPD 的 guest 用户登录时在系统中的帐号名称，默认为 ftp。

user_config_dir=/etc/vsftpd/userconf //定义用户配置文件的目录

virtual_use_local_privs= YES|NO　//#当该参数激活（YES）时，虚拟用户使用与本地用户相同的权限。所有虚拟用户的权限使用 local 参数。 当此参数关闭（NO）时，虚拟用户使用与匿名用户相同的权限，所有虚拟用户的权限使用 anon 参数。 这两者种做法相比，后者更加严格一些，特别是在有写访问的情形下。默认情况下此参数是关闭的（NO）。

（2）SSL 安全设置

ssl_enable=yes　　//打开 SSL 支持

allow_anon_ssl=yes　　//允许匿名用户使用 SSL 连接

force_local_data_ssl=yes　　//非匿名用户强制使用 SSL 连接，用于数据收发

force_local_logins_ssl=yes　//对非匿名用户强制使用 SSL 连接，用于密码传送

ssl_tlsv1=yes　//对 SSL 版本 1 支持，

ssl_sslv2=no　//不支持 SSL 版本 2

ssl_sslv3=no　//不支持 SSL 版本 3

rsa_cert_file=/etc/vsftpd/vsftpd.pem　　//rsa_cert_file 指定安全证书的位置和文件名

2.具体配置步骤

1、配置 Linux FTP 服务器，实现匿名上传下载的实现

任务说明：在开启防火墙和 SElinux 情况下，实现匿名用户的登录，可以上传下载，可以创建目录，创建权限掩码为 022，可以删除文件，最大上传速度 100KB/S

（1）首先是服务器端设置

第一步：修改配置文件开放匿名用户上传、下载及其他权限，请添加以下几项

vim /etc/vsftpd/vsftpd.conf

anonymous_enable=YES

anon_upload_enable=yes

write_enable=YES

anon_mkdir_write_enable=yes

anon_other_write_enable=yes

anon_umask=022

anon_max_rate=102400

修改完毕后使用#service vsftpd restart 重启服务。

第二步：修改上传目录的权限

为了让匿名用户实现上传，必须开放目录的写权限。以 anonymous 用户名登录后，相当于 ftp 用户的身份，所以要知道 anonymous 用户登陆后位于服务器端的哪个目录。这时可以查看 ftp 这个用户的登陆目录，#cat /etc/passwd|grep ftp //通过查看/etc/passwd 这个文件中 ftp 用户相关的行。结果显示 ftp 的登录目录是/var/ftp。下面开放此目录的写权限：

#chmod 777 /var/ftp

重启服务，并在服务器上用 ftp 登录时,出现了以下的错误提示

```
500 OOPS: vsftpd: refusing to run with writable anonymous root
Login failed.
```

这是因为/var/ftp 的权限不对所致，这个目录的权限是不能打开所有权限的。那如何实现匿名用户的修改、上传文件呢？解决方法是在/var/ftp 下再建一个目录，权限是 777 的就行了，注意不要直接修改/var/ftp 的写权限。

#mkdir /var/ftp/pub

#chmod　777 /var/ftp/pub

第三步：开启防火墙和 SElinux

iptables -I INPUT -p tcp --dport 21 -j ACCEPT

setsebool allow_ftpd_anon_write on

setsebool allow_ftpd_full_access on

（2）在客户机上验证：

```
# ftp 192.168.0.60
Connected to 192.168.0.60 (192.168.193.120).
220 (vsFTPd 2.2.2)
Name (192.168.193.120:lwj): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd pub
250 Directory successfully changed.
ftp> put openssl-0.9.8l.tar.gz
local: openssl-0.9.8l.tar.gz    remote: openssl-0.9.8l.tar.gz
227 Entering Passive Mode (192,168,193,120,240,28).
150 Ok to send data.
226 Transfer complete.
4179422 bytes sent in 0.221 secs (18938.58 Kbytes/sec)
ftp> get hello.txt
local:hello.txt    remote:hello.txt
227 Entering Passive Mode (192,168,193,120,123,229).
150 Opening BINARY mode data connection for hello.txt(6 bytes).
226 Transfer complete.
6 bytes received in 0.00021 secs (28.57 Kbytes/sec)
ftp> rename hello.txt xyz
350 Ready for RNTO
250 Rename successful.
ftp>delete xyz
250 Delete operation successful
ftp>mkdir dir1
257 “/pub/dir1” created
ftp>rm dir1
250 Remove directory operation successful.
ftp>quit
221 goodbye.
```

2、关于添加本地用户及打开读写权限示例

实现本地用户登录 ftp 时，位于自己的主目录

local_enable=YES //开启本地用户（真实用户）的登录功能

write_enable=YES //开启本地用户的上传功能

chroot_local_user=YES //将所有登录用户限制在自己的主目录

（1）限制用户在家目录

如果想限制部分用户，则使用

chroot_list_enable=YES

chroot_list_file=/etc/vsftpd.chroot_list //位于/etc/vsftpd.chroot_list 该文件的用户不能浏览主目录之外的目录

情况一：如果要将用户锁定在主目录，不允许切换到其他目录，但是除了指定的用户 ftp1、ftp2 以外。修改 vsftpd.conf 中的参数设置：

chroot_local_user=YES 并且 chroot_list_enable=YES

修改/etc/vsftpd.chroot_list 列表名单如下：

ftp1

ftp2

也就说 vsftpd.chroot_list 名单里面添加的是要排除被锁定主目录的用户名单.

情况二：如果只禁止指定用户 ftp1 跟 ftp2 切换到其他目录，允许其他用户切换到其他目录。修改 vsftpd.conf 中的参数设置：

chroot_local_user=NO 并且 chroot_list_enable=YES

修改/etc/vsftpd.chroot_list 列表名单如下：

ftp1

ftp2

情况三：如果 chroot_local_user=YES 并且 chroot_list_enable=NO 的时候，那列表名单也就不生效了。因此满足上面的条件时, 所有的 FTP 用户将全部锁定在主目录。

（2）限制部分本地用户登录 ftp

情况一：禁止指定用户，如 ftp1、ftp2 登陆 ftp，这时可以使用/etc/ftpusers 文件或是管理员添加一个文件，此文件记录了所有不能登录 ftp 服务器的用户列表，俗称黑名单。

修改 vsftpd.conf 如下：

pam_service_name=vsftpd //指出 vsFTPD 进行 PAM（Pluggable Authentication Modules）认证时所使用的 PAM 配置文件名，默认值是是/etc/pam.d/vsftpd。

userlist_enable=YES //开启 userlist 来限制用户访问的功能

userlist_file=/etc/vsftpd/user_list //禁止登陆的用户列表文件

修改/etc/vsftpd/user_list 为

ftp1

ftp2

情况二：只允许指定用户，如 ftp1、ftp2 登陆 ftp

只需要在情况 1 的基础上，添加下面的选项：

userlist_deny= NO

3、配置虚拟用户

VSFTPD 的本地用户本身是系统的用户，除了可以登录 FTP 服务器外，还可以登录系统使用其他系统资源，而 VSFTPD 的虚拟用户则是 FTP 服务的专用用户，虚拟用户只能访问 FTP 服务器资源。对于只需要通过 FTP 对系统有读写权限，而不需要其他系统资源的用户或情况来说，采用虚拟用户方式是很适合的。

对于虚拟用户的管理，可以借助数据库来完成，最简单的数据库就是柏克利数据库，当然也可以用 mysql 等其它数据库。VSFTPD 可以采用数据库文件来保存用户/口令，如 hash; 也可以将用户/口令保存在数据库服务器 中，如 MySQL 等。因为 VSFTPD 的虚拟用户采用单独的用户名/口令或通过专门的数据库服务器来保存，与系统账号（passwd/shadow）分离，大大增强了系统的安全性。

对于虚拟用户的认证，VSFTPD 采用 PAM 方式验证虚拟用户。由于虚拟用户的用户名/口令被单独保存，因此在验证 时，VSFTPD 需要用一个系统用户的身份来读取数据库文件或数据库服务器以完成验证，这就是 guest 用户，这正如同匿名用户也需要有一个系统用户 ftp 一样。当然，guest 用户也可以被认为是用于映射虚拟用户。

总之，对于虚拟用户的配置，要包括以下几部分：guest 用户的创建、虚拟用户/口令的保存、PAM 认证配置、vsftpd.conf 文件设置等。

下面通过一个具体的配置来说明虚拟用户的配置步骤。

配置要求：实现虚拟用户 user1 和 user2 登录，映射到 vusers 用户，并且 user1 能够上传下载文件，创建目录，删除文件目录，而 user2 只能下载没有其它权限。

（1）创建本地账户 vusers 作为虚拟用户映射的帐号，它是虚拟用户在系统中的代表

```
# useradd -d /etc/vsftpd/vusers -s /sbin/nologin vusers
# chmod 755 –R /etc/vsftpd/vusers     //如果其他用户没有赋予 rx 的权限，登录后会出现无法查看目录的情况
```

（2）生成虚拟用户列表，将 user1、user2 加入到列表中

```
# cd /etc/vsftpd/
# vim vusers.list
user1
123456
user2
321456
```

说明：vusers.list 文件中的奇数行为用户名，偶数行为上一行用户的密码。

（3）将虚拟用户列表导出为 BDB 数据库

```
# db_load -T -t hash -f vusers.list vusers.db    //创建虚拟用户需要 db4-utils 工具的支持，在 rhel6 中已经默认安装，rhel5 默认没有安装。其中-T 表示允许 BerkeyDB 的应用程序使用文本格式转换成 DB 数据文件；-t hash 用来指定读取数据文件的基本方法；-f：指定要导出的用户密码文件
# file vusers.db
vusers.db: Berkeley DB (Hash, version 8, native byte-order)
# chmod 600 vusers.db    //为了安全性，只赋予管理员读取和修改这个数据库的权限
```

（4）创建虚拟用户的身份验证模块-vsftpd.vu

```
# cd /etc/pam.d
# vim vsftpd.vu
#%PAM-1.0
auth       required     pam_userdb.so     db=/etc/vsftpd/vusers
account    required     pam_userdb.so     db=/etc/vsftpd/vusers
```

说明：其中第一行是身份必须经过 pam_userdb.so 模块用/etc/vsftpd/vusers 的验证，第二行是帐户必须经过 pam_userdb.so 模块用/etc/vsftpd/vusers 的验证。

（5）修改 vsftpd.conf 配置文件

```
# vim /etc/vsftpd/vsftpd.conf
anonymous_enable=no
local_enable=YES
write_enable=YES
local_umask=022
guest_enable=yes
```

guest_username=vusers

pam_service_name=vsftpd.vu

user_config_dir=/etc/vsftpd/vusers_conf

注意：要将原本的 pam_service_name=vsftpd 删除掉，另外虚拟用户本质上是映射到本地用户身上的，所以本地用户一定要能登录 local_enable=yes，同时其他控制虚拟用户权限的配置项借用了匿名用户的配置项。

（6）为 user1 和 user2 分别创建控制文件

mkdir /etc/vsftpd/vusers_conf

cd etc/vsftpd/vusers_conf

vim user1

anon_upload_enable=no

anon_mkdir_write_enable=no

anon_other_write_enable=no

vim user2

anon_upload_enable=yes

anon_mkdir_write_enable=yes

anon_other_write_enable=yes

anon_umask=022

注意：因为虚拟用户权限的配置项是借用了匿名用户的配置项，所以控制上传、创建、删除等权限的配置项都要写 anon_*。

（7）调整 SElinux 和防火墙

setsebool ftp_home_dir on　//允许改变 ftp 目录，否则会在登录时报 500 OOPS: cannot change directory:/vusers

setsebool allow_ftpd_full_access on //开发所有权限，否则会在上传文件时报 553 Could not create file.

iptables -I INPUT -p tcp --dport 21 -j ACCEPT

4、带 SSL 加密的 vsftpd 的配置

对于 ssl 环境的安装与配置，在 RHEL6 中，可以使用#yum install mod_ssl 安装 ssl 模块，也可以下载相关的软件包，如 openssl-0.9.8l.tar.gz 手动安装（SSL 安装与配置的详细步骤参考第 11 章 WEB 服务器的安装与配置中的配置安全的 web 服务器）。下面以 openssl-0.9.8l.tar.gz 的安装环境为例，给出 SSL 加密的 vsftpd 的配置。具体步骤如下：

（1）在服务器上用 openssl 生成安全证书，生成的需要填写信息，内容可以任意填写

#cd /usr/local/ssl-0.9.8l/bin //要使用 SSL 命令，需要将安装目录加入 PATH 变量，或者进入到安装目录，以使用下面的命令

使用 openssl 命令将秘钥和证书信息输出至 vsftpd.pem 文件

./openssl req -x509 -nodes -days 365 -newkey rsa:1024 -keyout vsftpd.pem -out vsftpd.pem

ll vsftpd.pem

-rw-r--r--. 1 root root　1921 12 月　15 17:07 vsftpd.pem

#cp –p /usr/local/ssl-0.9.8l/bin/ vsftpd.pem /etc/vsftpd　//复制文件到/etc/vsftpd 目录

（2）修改 vsftpd.conf

vim vsftpd.conf

#以下是关于 SSL 配置部分

ssl_enable=yes　　//打开 SSL 支持

allow_anon_ssl=yes　　//允许匿名用户使用 SSL 连接

force_local_data_ssl=yes　　//非匿名用户强制使用 SSL 连接，用于数据收发

force_local_logins_ssl=yes　//非匿名用户强制使用 SSL 连接，用于密码传送

ssl_tlsv1=yes　　//ssl_tlsv1=yes 对 SSL 版本 1 支持，

ssl_sslv2=no　　// ssl_sslv2/ssl_sslv3=no 不支持 SSL 版本 2、3

ssl_sslv3=no

rsa_cert_file=/etc/vsftpd/vsftpd.pem　　//rsa_cert_file 指定安全证书的位置和文件名

重启服务# service vsftpd restart

（3）为了能够更好观察 FTP 客户机登录的情况，这里用 lftp –d 命令来调试登录过程，可以看到数据传输方向，包括证书的信息。

在 rhel4、rhel5 中默认提供了 lftp 命令，但在 rhel6 里面没有安装。因此首先在 rhel6 光盘 Packages 目录中找到 lftp 的安装包，使用下面的命令安装：

```
[root@localhost Packages]# rpm -ivh lftp-4.0.4-1.el6.i686.rpm
warning: lftp-4.0.4-1.el6.i686.rpm: Header V3 RSA/SHA256 Signature, key ID f2154
1eb: NOKEY
Preparing...                ########################################### [100%]
   1:lftp                   ########################################### [100%]
```

接下来，使用 lftp –d 命令调试登录过程：

lftp -d

lftp :~> connect -u user1 192.168.0.60　//指定使用虚拟用户 user1 登录

口令:

---- 正在解析主机地址...

---- 1 address found: 192.168.0.60

lftp ftp@192.168.0.60:~> ls　　//登录后使用 ls 命令，因为使用 SSL，接下来可看到证书相关信息

---- 正在连接到 192.168.0.60 (192.168.0.60) 端口 21

<--- 220 (vsFTPd 2.2.2)

---> FEAT

<--- 211-Features:

<---　AUTH SSL

<---　AUTH TLS

<---　EPRT

… …

上面的例子是同时产生公私钥，也可以分别产生。在服务器上执行以下命令

./openssl genrsa 1024 > vsftpd_key.pem　　//产生私钥

#./openssl req -new -x509 -key vsftpd_key.pem -out vsftpd_cert.pem -days 365 //根据上面的私钥以 x.509 的格式产生名为 vsftpd_cert.pem 的数字证书

修改 vsftpd.conf，指定私钥及证书

rsa_cert_file=/etc/vsftpd/ssl/vsftpd_cert.pem　　//指定证书文件

rsa_private_key_file=/etc/vsftpd/ssl/vsftpd_key.pem　　//指定私钥文件

.....

vsftpd 的常用功能还有很多，这些功能的实现都可以通过修改 vsftpd.conf 配置文件万成。由于篇幅所限，本文就不再一一列出。