# vsftpd部署

## 0 信息

服务端软件名：vsftpd

客户端软件名：ftp

服务名：vsftpd

端口号：20、21、指定范围内随机端口

配置文件：/etc/vsftpd/vsftpd.conf

## 1、vsftpd 的安装

# 确认否安装vsftpd， vsftpd为服务器端

rpm -qa | grep vsftpd

# 安装vsftpd，ftp为客户端

yum install -y vsftpd ftp

## 2、相关文件解释

/etc/vsftpd.ftpusers ---- 禁止使用vsftpd的用户列表文件；

/etc/vsftpd.user\_list ---- 禁止或允许使用vsftpd的用户列表文件 ；

/etc/vsftpd/vsftpd.conf ---- 主配置文件 ；

/etc/vsftpd/vsftpd\_conf\_migrate.sh ---- vsftpd操作的一些变量和设置；

/etc/pam.d/vsftpd ---- PAM认证文件 ；

/usr/sbin/vsftpd ---- vsftpd的主程序 ；

/etc/rc.d/init.d/vsftpd ---- 启动脚本 ；

/var/ftp ---- 匿名用户主目录 ；

/var/ftp/pub ---- 匿名用户的下载目录 ；

## 3、启动vsftpd

systemctl enable vsftpd  
systemctl start vsftpd  
systemctl status vsftpd

## 4、虚拟用户的创建和配置

#### 4.1 添加虚拟用户口令文件

vi /etc/vsftpd/vuser.list

注：该文件名可以随便定义，文件内容格式：奇数行用户，偶数行密码

#### 4.2 生成虚拟用户口令认证文件

yum install -y db4-utils  
which db\_load  
  
#将用户密码的存放文本转化为数据库类型，并使用 hash 加密  
db\_load -T -t hash -f /etc/vsftpd/vuser.list /etc/vsftpd/vuser.db  
  
  
#修改文件权限为 600，保证其安全性  
chmod 600 /etc/vsftpd/vuser.db

#### 4.3 建立支持虚拟用户的 PAM 认证文件，添加虚拟用户支持

vim /etc/pam.d/vsftpd.pam  
#添加以下内容  
auth required pam\_userdb.so db=/etc/vsftpd/vuser  
account required pam\_userdb.so db=/etc/vsftpd/vuser

#### 4.4建立本地映射用户并设置宿主目录的权限

**创建FTP 虚拟用户的映射用户，并指定其用户家目录，所有vsftpd虚拟用户需要映射到一个系统用户，该系统用户不需要密码，也不需要登录。主要用于虚拟用户映射使用。**

useradd vuser -d /data/ftpdir -s /sbin/nologin  
chown -R vuser:vuser /data/ftpdir  
chmod 755 /data/ftpdir

#### 4.5 修改vsftpd的主配置文件/etc/vsftpd/vsftpd.conf

cp /etc/vsftpd/vsftpd.conf{,.bak}  
vim /etc/vsftpd/vsftpd.conf  
cat /etc/vsftpd/vsftpd.conf | grep -v "#" | more

listen\_port=64421

# 是否开启匿名登录

anonymous\_enable=NO

# 是否允许使用本地帐户进行FTP用户登录验证

local\_enable=YES

# 是否允许写

write\_enable=YES

# 设置本地用户默认文件掩码022

local\_umask=022

# 是否允许匿名上传

#anon\_upload\_enable=YES

# 是否允许匿名创建新目录

#anon\_mkdir\_write\_enable=YES

# 同时开放其它权限

#anon\_other\_write\_enable=YES

# 可以发送消息当访问某个目录时

dirmessage\_enable=YES

# 开启上传下载记录

xferlog\_enable=YES

# 数据链通过20端口建立，默认21端口,主动连接模式的端口设置

#connect\_from\_port\_20=YES

# 是否允许其它用户上传匿名文件

#chown\_uploads=YES

# 所有用户

#chown\_username=whoever

# 日志保存位置

xferlog\_file=/var/log/vsftpd.log

# 是否使用日志标准输出格式

xferlog\_std\_format=YES

# 空闲会话时间

idle\_session\_timeout=600

# 数据连接超时时间

data\_connection\_timeout=120

# 隔离的安全用户

#nopriv\_user=ftpsecure

# 是否开启异步数据线程

#async\_abor\_enable=YES

# 是否开启ASCII协议上传

ascii\_upload\_enable=YES

# 是否开启ASCII协议下载

ascii\_download\_enable=YES

# 是否开启邮箱验证

#deny\_email\_enable=YES

# 拒绝的邮箱列表

#banned\_email\_file=/etc/vsftpd/banned\_emails

# 是否允许直接获取子目录信息

#ls\_recurse\_enable=YES

# 监听IPv4

listen=NO

# 监听IPv6和监听IPv4

listen\_ipv6=YES

# 是否用户组管理

userlist\_enable=YES

# 是否访问控制

tcp\_wrappers=YES

# 是否使用被动模式

pasv\_enable=YES

# 指定使用被动模式时打开端口的最小值

pasv\_min\_port=30060

# 指定使用被动模式时打开端口的最大值。

pasv\_max\_port=30090

pasv\_promiscuous=yes

# 用户宽带限制200kps

#local\_max\_rate=200000

# 登录后欢迎内容

ftpd\_banner=Welcome to My FTP service.

# ---------开启虚拟用户组参数--------

# 虚拟用户启用pam认证

pam\_service\_name=vsftpd.pam

# 是否开启虚拟用户

guest\_enable=YES

# 主虚拟用户名vuser

guest\_username=vuser

# 虚拟用户配置（可以对每一个虚拟用户进行单独的权限配置,需要自行创建此目录）

user\_config\_dir=/etc/vsftpd/vusers\_conf.d

# 虚拟用户是否具有写权限（上传、下载、删除、重命名）

#virtual\_use\_local\_privs=YES

#write\_enable=YES

# 是否启用限定用户在其主目录下

chroot\_local\_user=YES

# 是否开启用户列表chroot管理

chroot\_list\_enable=YES

# chroot管理的用户列表（一行一用户,虚拟用户都要添加进去）

# 当设置用户只能在登录目录时，chroot管理的用户为不受限制，否则相反

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

# 是否允许chroot管理用户进行写操作

allow\_writeable\_chroot=YES

#########开启https#####

ssl\_enable=YES

#启用 ssl 认证

ssl\_tlsv1=YES

ssl\_sslv2=YES

ssl\_sslv3=YES

#开启 tlsv1、sslv2、sslv3 都支持

allow\_anon\_ssl=YES

#允许匿名用户{虚拟用户}

force\_anon\_logins\_ssl=YES

force\_anon\_data\_ssl=YES

#匿名登录和传输时强制使用 ssl

force\_local\_logins\_ssl=YES

force\_local\_data\_ssl=YES

#本地登录和传输时强制使用 ssl

rsa\_cert\_file=/etc/ssl/certs/itdance.cn.cert

#rsa格式的证书

rsa\_private\_key\_file=/etc/ssl/certs/itdance.cn.key

#rsa格式的密钥

配置详解

################################## 基本设定 #########################################

#接受匿名用户

anonymous\_enable=YES

#匿名用户login时不询问口令

no\_anon\_password=YES

#匿名用户主目录

anon\_root=(none)

#接受本地用户

local\_enable=YES

#本地用户主目录

local\_root=(none)

#如果匿名用户需要密码,那么使用banned\_email\_file里面的电子邮件地址的用户不能登录

deny\_email\_enable=YES

#仅在没有pam验证版本时有用,是否检查用户有一个有效的shell来登录

check\_shell=YES

#若启用此选项,userlist\_deny选项才被启动

userlist\_enable=YES

#若为YES,则userlist\_file中的用户将不能登录,为NO则只有userlist\_file的用户可以登录

userlist\_deny=NO

#如果和chroot\_local\_user一起开启,那么用户锁定的目录来自/etc/passwd每个用户指定的目录(这个不是很清楚,很哪位熟悉的指点一下)

passwd\_chroot\_enable=NO

#定义匿名登入的使用者名称。默认值为ftp。

ftp\_username=FTP

################################### 用户权限控制 ####################################

#可以上传(全局控制).

write\_enable=YES

#本地用户上传文件的umask

local\_umask=022

#上传文件的权限配合umask使用

#file\_open\_mode=0666

#匿名用户可以上传

anon\_upload\_enable=NO

#匿名用户可以建目录

anon\_mkdir\_write\_enable=NO

匿名用户其它的写权利(更改权限?)

anon\_other\_write\_enable=NO

如果设为YES，匿名登入者会被允许下载可阅读的档案。默认值为YES。

anon\_world\_readable\_only=YES

#如果开启,那么所有非匿名登陆的用户名都会被切换成guest\_username指定的用户名

#guest\_enable=NO

所有匿名上传的文件的所属用户将会被更改成chown\_username

chown\_uploads=YES

匿名上传文件所属用户名

chown\_username=lightwiter

#如果启动这项功能，则所有列在chroot\_list\_file之中的使用者不能更改根目录

chroot\_list\_enable=YES

#允许使用"async ABOR"命令,一般不用,容易出问题

async\_abor\_enable=YES

管控是否可用ASCII 模式上传。默认值为NO。

ascii\_upload\_enable=YES

#管控是否可用ASCII 模式下载。默认值为NO。

ascii\_download\_enable=YES

#这个选项必须指定一个空的数据夹且任何登入者都不能有写入的权限，当vsftpd 不需要file system 的权限时，就会将使用者限制在此数据夹中。默认值为/usr/share/empty

secure\_chroot\_dir=/usr/share/empty

############################### 超时设置 ###############################

#空闲连接超时

idle\_session\_timeout=600

#数据传输超时

data\_connection\_timeout=120

#P\*\*\*S请求超时

ACCEPT\_TIMEOUT=60

#PROT模式连接超时

connect\_timeout=60

############################### 服务器功能选项 #############################

#开启日记功能

xferlog\_enable=YES

#使用标准格式

xferlog\_std\_format=YES

#当xferlog\_std\_format关闭且本选项开启时,记录所有ftp请求和回复,当调试比较有用.

#log\_ftp\_protocol=NO

#允许使用pasv模式

pasv\_enable=YES

#关闭安全检查,小心呀.

#pasv\_promiscuous=NO

#允许使用port模式

#port\_enable=YES

#关闭安全检查

#prot\_promiscuous

#开启tcp\_wrappers支持

tcp\_wrappers=YES

#定义PAM 所使用的名称，预设为vsftpd。

pam\_service\_name=vsftpd

#当服务器运行于最底层时使用的用户名

nopriv\_user=nobody

#使vsftpd在pasv命令回复时跳转到指定的IP地址.(服务器联接跳转?)

pasv\_address=(none)

########################### 服务器性能选项 ###########################

#是否能使用ls -R命令以防止浪费大量的服务器资源。是否允许递归查询。默认为关闭，以防止远程用户造成过量的I/O

ls\_recurse\_enable=YES

#是否使用单进程模式。这个设定项目比较危险一点～当设定为YES时，表示每个建立的连线都会拥有一支process在负责，可以增加vsftpd的效能。

#不过，除非您的系统比较安全，而且硬体配备比较高，否则容易耗尽系统资源喔！一般建议设定为NO的啦！

one\_process\_model=NO

#绑定到listen\_port指定的端口,既然都绑定了也就是每时都开着的,就是那个什么standalone模式

listen=YES

#当使用者登入后使用ls -al 之类的指令查询该档案的管理权时,预设会出现拥有者的UID,而不是该档案拥有者的名称。

#若是希望出现拥有者的名称,则将此功能开启。

text\_userdb\_names=NO

#显示目录清单时是用本地时间还是GMT时间,可以通过mdtm命令来达到一样的效果

use\_localtime=NO

#测试平台优化

#use\_sendfile=YES

########################### 信息类设置 ############################

login时显示欢迎信息.如果设置了banner\_file则此设置无效

ftpd\_banner="欢迎登录kevin的ftp服务"

#允许为目录配置显示信息,显示每个目录下面的message\_file文件的内容

dirmessage\_enable=YES

#显示会话状态信息

#setproctitle\_enable=YES

############################ 文件定义 #############################

#定义不能更改用户主目录的文件

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

#定义限制/允许用户登录的文件

userlist\_file=/etc/vsftpd/vsftpd.user\_list

#定义登录信息文件的位置

banner\_file=/etc/vsftpd/banner

#禁止使用的匿名用户登陆时作为密码的电子邮件地址

#如果deny\_email\_enable=YES时，可以利用这个设定项目来规定哪个email address不可登入我们的vsftpd喔！在上面设定的档案内，一行输入一个email address即可！

banned\_email\_file=/etc/vsftpd.banned\_emails

#日志文件位置

xferlog\_file=/var/log/vsftpd.log

#目录信息文件

#当进入一个新目录的时候，会查找这个文件并显示文件里的内容给远程用户。dirmessage\_enable需启用。默认值：.message

message\_file=.message

########################### 目录定义 #############################

#定义用户配置文件的目录

user\_config\_dir=/etc/vsftpd/userconf

#定义本地用户登陆的根目录,注意定义根目录可以是相对路径也可以是绝对路径

相对路径是针对用户家目录来说的

local\_root=webdisk

#此项设置每个用户登陆后其根目录为/home/username/webdisk#匿名用户登陆后的根目录

anon\_root=/var/ftp

########################## 用户连接选项 ##########################

#可接受的最大client数目

max\_clients=100

#每个ip的最大client数目

max\_per\_ip=5

#使用标准的20端口来连接ftp

connect\_from\_port\_20=YES

#绑定到某个IP,其它IP不能访问

listen\_address=192.168.0.2

#绑定到某个端口

listen\_port=2121

#数据传输端口

ftp\_data\_port=2020

#pasv连接模式时可以使用port 范围的上界,0 表示任意。默认值为0。

pasv\_max\_port=100010

#pasv连接模式时可以使用port 范围的下界,0 表示任意。默认值为0。

pasv\_min\_port=100050

######################### 数据传输选项 ##########################

#匿名用户的传输比率(b/s)

# 这个设定值后面接的数值单位为bytes/秒，限制anonymous的传输速度，如果是0则不限制(由最大频宽所限制)，

# 如果您想让anonymous仅有30 KB/s的速度，可以设定『anon\_max\_rate=30000』

anon\_max\_rate=51200

#本地用户的传输比率(b/s)

local\_max\_rate=5120000

#限制anonymous的权限！如果是077则anonymous传送过来的档案权限会是-rw

anon\_umask=077

重点注意的细节

=============================================================================================================

1》限制vsftpd最大连接数和传输速率

在FTP服务器的管理中，无论对本地用户还是匿名用户，对于FTP服务器资源的使用都需要进行控控制，避免由于负担过大造成FTP服务器运行异常，

可以添加以下配置项对FTP客户机使用FTP服务器资源进行控制：

max\_client设置项

用于设置FTP服务器所允许的最大客户端连接数，值为0时表示不限制。

例如max\_client=100表示FTP服务器的所有客户端最大连接数不超过100个。

max\_per\_ip设置项

用于设置对于同一IP地址允许的最大客户端连接数，值为0时表示不限制。

例如max\_per\_ip=5表示同一IP地址的FTP客户机与FTP服务器建立的最大连接数不超过5个。

local\_max\_rate设置项

用于设置本地用户的最大传输速率，单位为B/s，值为0时表示不限制。

例如local\_max\_rate=500000表示FTP服务器的本地用户最大传输速率设置为500KB/s.

anon\_max\_rate设置项

用于设置匿名用户的最大传输速率，单位为B/s,值为0表示不限制。

例如ano\_max\_rate=200000，表示FTP服务器的匿名用户最大传输速率设置为200KB/s.

=============================================================================================================

2》指定用户的权限设置

vsftpd.user\_list文件需要与vsftpd.conf文件中的配置项结合来实现对于vsftpd.user\_list文件中指定用户账号的访问控制：

a）设置禁止登录的用户账号

当vsftpd.conf配置文件中包括以下设置时，vsftpd.user\_list文件中的用户账号被禁止进行FTP登录：

userlist\_enable=YES

userlist\_deny=YES

userlist\_enable设置项设置使用vsftpd.user\_list文件，userlist\_deny设置为YES表示vsftpd.user\_list文件用于设置禁止的用户账号。

b）设置只允许登录的用户账号

当vsftpd.conf配置文件中包括以下设置时，只有vsftpd.user\_list文件中的用户账号能够进行FTP登录：

userlist\_enable=YES

userlist\_deny=NO

userlist\_enable设置项设置使用vsftpd.user\_list文件，

userlist \_deny设置为NO表示vsftpd.usre\_list文件用于设置只允许登录的用户账号，文件中未包括的用户账号被禁止FTP登录。

userlist\_deny和userlist\_enable选项限制用户登录FTP服务器

注意：使用userlist\_deny选项和user\_list文件一起能有效阻止root,apache,www等系统用户登录FTP服务器，从而保证FTP服务器的分级安全性。

以下是两个选项的具体表现形式和两种搭配使用方式的效果：

Userlist\_enable=YES 表示：Ftpusers中用户允许访问；User\_list中用户允许访问

Userlist\_enable=NO 表示：Ftpusers中用户禁止访问；User\_list中用户允许访问

Userlist\_deny=YES 表示：Ftpusers中用户禁止访问（登录时可以看到密码输入提示，但仍无法访问）；User\_list 中用户禁止访问

Userlist\_deny=NO 表示：Ftpusers中用户禁止访问；User\_list中用户允许访问

Userlist\_enable=YES 并且 Userlist\_deny=YES 表示：Ftpusers中用户禁止访问；User\_list中用户禁止访问（登录时不会出现密码提示，直接被服务器拒绝）

Userlist\_enable=YES 并且 Userlist\_deny=NO 表示：Ftpusers中用户禁止访问；User\_list中用户允许访问

-----------------------------------

Linux下FTP虚拟账号环境部署记录 (vsftpd)

<https://blog.51cto.com/u_6215974/4938487>

touch /etc/vsftpd/chroot\_list

#### 4.6 创建目录/etc/vsftpd/vusers\_conf.d

mkdir -pv /etc/vsftpd/vusers\_conf.d

#### 4.7 在目录/etc/vsftpd/vusers\_conf.d中创建虚拟用户配置文件

为每个虚拟用户创建对应目录

mkdir /data/{vuser1,vuser2,vuser3}  
chown -R vuser.vuser /data/{vuser1,vuser2,vuser3}  
  
# 创建虚拟用户家目录如  
# mkdir /home/vsftp/ftptest1  
# chown vuser:vuser /home/vsftp/ftptest1/

**对应目录可以是其他路径，但是vuser必须对其有权限。**

**注意：配置文件名必须和虚拟用户名保持一致,见4.1**

cd /etc/vsftpd/vusers\_conf.d/  
vim vuser1 #虚拟用户各自配置文件和自己的用户名对应起来

# 虚拟用户不能浏览目录，只能上传/创建文件，无其他权限

local\_root=/data/vuser1

virtual\_use\_local\_privs=NO

write\_enable=YES

anon\_world\_readable\_only=YES

anon\_upload\_enable=YES

vim vuser2

# 虚拟用户只能下载文件，无其他权限

local\_root=/data/vuser2

virtual\_use\_local\_privs=NO

write\_enable=YES

anon\_world\_readable\_only=NO

anon\_upload\_enable=NO

vim vuser3

# 虚拟用户具有写权限（上传、下载、删除、重命名）

local\_root=/data/vuser3

virtual\_use\_local\_privs=YES

write\_enable=YES

可以任选一组虚拟用户高级参数作为 vsftpd 的配置

# 虚拟用户和本地用户有相同的权限

virtual\_use\_local\_privs=YES

# 虚拟用户和匿名用户有相同的权限，默认是NO

virtual\_use\_local\_privs=NO

# 虚拟用户具有写权限（上传、下载、删除、重命名）

virtual\_use\_local\_privs=YES

write\_enable=YES

# 虚拟用户不能浏览目录，只能上传文件，无其他权限

virtual\_use\_local\_privs=NO

write\_enable=YES

anon\_world\_readable\_only=YES

anon\_upload\_enable=YES

# 虚拟用户只能下载文件，无其他权限

virtual\_use\_local\_privs=NO

write\_enable=YES

anon\_world\_readable\_only=NO

anon\_upload\_enable=NO

# 虚拟用户只能上传和下载文件，无其他权限

virtual\_use\_local\_privs=NO

write\_enable=YES

anon\_world\_readable\_only=NO

anon\_upload\_enable=YES

# 虚拟用户只能下载文件和创建文件夹，无其他权限

virtual\_use\_local\_privs=NO

write\_enable=YES

anon\_world\_readable\_only=NO

anon\_mkdir\_write\_enable=YES

# 虚拟用户只能下载、删除和重命名文件，无其他权限

virtual\_use\_local\_privs=NO

write\_enable=YES

anon\_world\_readable\_only=NO

anon\_other\_write\_enable=YES

## 5、修改vsftpd服务ftp默认端口

常规情况下ftp默认21端口容易遭到别人的扫描、带来了一定程度的不安全。所以，最好的就是把21端口修改掉。把ftp端口改成 64421 ,修改后能保证用户上传下载不受影响

#### 5.1修改主配置文件/etc/vsftpd/vsftpd.conf

##修改默认端口号##

listen\_port=64421

##开启被动访问模式##

pasv\_enable=YES

pasv\_min\_port=30060

pasv\_max\_port=30090

pasv\_promiscuous=yes

pasv\_min\_port=（你希望的被动传输端口号最小值）

pasv\_max\_port=（你希望的被动传输端口号最大值）

pasv\_promiscuous=yes #此选项激活将关闭PASV模式的安全检查。该检查确保数据连接和控制连接是来自同一个ip地址。#此选项唯一合理的用法是存在于由安全隧道方案构成的组织中。默认值为NO

#开启被动模式，使得公网能够登录

#### 5.2 修改/etc/services

vi /etc/services

**找到21 is registered to ftp**



修改成64421



<https://www.cnblogs.com/cash/p/14029877.html>

<http://t.zoukankan.com/fan-yuan-p-11347942.html>

<https://blog.csdn.net/qq_25378657/article/details/109496131>

#### 5.3 重启vsftpd

systemctl restart vsftpd  
netstat -apn|grep vsftpd

## 6. openssl+vsftpd 加密验证方式：

**1. 查看是否安装了 openssl**

rpm -q openssl

**2. 查看 vsftpd 是否支持 openssl**

ldd /usr/sbin/vsftpd | grep libssl

**3. 生成加密信息的秘钥和证书文件**

位置：/etc/ssl/certs/

a. openssl genrsa -out vsftpd.key 1024

#建立服务器私钥，生成 RSA 密钥

b. openssl req -new -key vsftpd.key -out vsftpd.csr

#需要依次输入国家，地区，城市，组织，组织单位，

Email 等信息。最重要的是有一个 common name，

可以写你的名字或者域名。如果为了https 申请，这个必须和域名吻合，否则会引发浏览器警报。

生成的csr 文件交给 CA 签名后形成服务端自己的证书

c. openssl x509 -req -days 365 -sha256 -in vsftpd.csr -signkey vsftpd.key -out   
vsftpd.crt

#使用 CA 服务器签发证书，设置证书的有效期等信息

**注意1：生成完秘钥和证书文件后，将本目录{/etc/ssl/certs/}的权限修改为 500.**

**注意2：在实验环境中可以用命令生成测试，在生产环境中必须要在 https 证书厂商注册（否则浏览器不识别）**

**4. 修改主配置文件/etc/vsftpd/vsftpd.conf**

ssl\_enable=YES

#启用 ssl 认证

ssl\_tlsv1=YES

ssl\_sslv2=YES

ssl\_sslv3=YES

#开启 tlsv1、sslv2、sslv3 都支持

allow\_anon\_ssl=YES

#允许匿名用户{虚拟用户}

force\_anon\_logins\_ssl=YES

force\_anon\_data\_ssl=YES

#匿名登录和传输时强制使用 ssl

force\_local\_logins\_ssl=YES

force\_local\_data\_ssl=YES

#本地登录和传输时强制使用 ssl

rsa\_cert\_file=/etc/ssl/certs/itdance.cn.cert

#rsa格式的证书

rsa\_private\_key\_file=/etc/ssl/certs/itdance.cn.key

#rsa格式的密钥

**注：密钥文件要在配置文件中单独声明（写入配置文件时，注释要单独一行，否则会报错）**

**5. 重启服务**

service vsftpd restart

**6. 测试(使用第三方客户端连接)**

tcpdump -i ens33 -nn -X -vv tcp port 64421 and ip host 192.168.0.1

## 7 vsftpd 使用虚拟用户及单用户多目录的配置

[参考文档](https://blog.51cto.com/xmomo/2074258)

<http://t.zoukankan.com/ilanni-p-4779416.html>

<https://www.cnblogs.com/-bobo/p/11615647.html>