# Linux vsftpd文件共享

简介：

vsftpd是Very Secure FTP的简写形式，是一筐非常安全的FTP软件。该软件基于GPL开发的，被设置为Linux平台下稳定、快速、安全的FTP软件，它支持IPv6以及SSL加密。

vsftpd的安全性主要体现在三个方面：进程分离，处理不同任务的进程彼此是独立运行的；进程运行均以最小权限运行；多数进程都使用chroot进行了禁锢，放置客户访问非法共享目录，这里的chroot是改变根的一种技术，如果我们通过vsftpd共享了/var/ftp目录，则该目录对客户端而言就是共享的根目录。

vsftpd虽然是一款FTP软件，但FTP不同于其他的互联网协议，它使用多端口通信。当客户端连接服务器请求资源时，服务器会使用21端口与客户端进行通信，该端口专门处理客户端发送给服务器的请求命令，也就是俗称的命令端口。而最终服务器与客户端进行数据传输时，还需要使用另一个数据端口，数据端口号取决于服务器运行的模式是主动模式还是被动模式。

## FTP的工作模式

### 1，主动模式

第一步，客户端随机开启大于1024的X端口与服务端的21端口建立连接通道，通道建立后，客户端随时可以通过该通道发送上传或下载命令。

第二步，当客户端需要与服务器进行数据传输时，客户端会在开启一个大于1024的随机端口Y，并将Y端口号通过之前的命令通道(X)传送给服务器的21端口。

第三步，服务器获取到客户端的第二个端口后会主动连接客户端的该端口(Y),通过三次握手，完成服务器与客户端数据通道的建立，所有的数据均通过该数据通道进行传输。

### 2，被动模式

第一步，客户端随意开启大于1024的X端口与服务器的21端口建立连接通道。

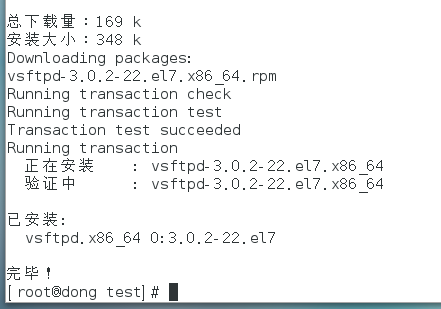
第二步，当客户端需要与服务器进行数据传输时，客户端从命令通道发送数据请求要求上传或下载数据。

第三步，服务器收到数据请求后会随机开启一个端口Y，并通过命令将该端口信息传送给客户端。

第四步，客户端在收到服务器发送过来的数据端口Y的信息后，将在客户端本地开启一个随机端口Z，此时客户端再主动通过本机的Z端口与服务器的Y端口进行连接，通过三次握手连接完成后，即可进行数据传输。

## 安装vsftpd

[root@centos7 ~]# yum -y install vsftpd



[root@centos7 ~]# systemctl start vsftpd

[root@centos7 ~]# systemctl enable vsftpd

RPM格式的vsftpd软件安装完成后，该软件的主程序是/usr/sbin/vsftpd，下面是vsftpd相关的核心文件与目录列表的说明。

/etc/logrotate.d/vsftpd # 日志轮转备份配置文件

/etc/pam.d/vsftpd # 基于PAM的csftpd验证配置文件

/etc/vsftpd # vsftpd软件目录

/etc/vsftpd/ftpusers # 默认的vsftpd黑名单

/etc/vsftpd/user\_list # 可以通过主配置文件设置该文件为黑名单或白名单

/etc/vsftpd/vsftpd.conf # vsftpd主配置文件

/usr/sbin/vsftpd # vsftpd主程序

/usr/share/doc/vsftpd-3.0.2 # vsftpd文档资料路径

/var/ftp # 默认vsftpd共享目录

## vsftp配置文件解析

vsftpd配置文件默认位于/etc/vsftpd目录下，vsftpd会自动寻找以.conf结尾的配置文件，并使用此配置文件启动FTP服务。

配置文件的格式为：选项=值(中间不可以有任何空格符)，以#开头的行会被识别为注释行。

全局设置

listen=YES # 是否监听端口，独立运行守护进程

listen\_port=21 # 监听入站FTP请求的端口号

write\_enable=YES # 是否允许写操作，全局开关

download\_enable=YES # 如何设置为NO，则拒绝所有下载请求

dirmessage\_enable=YES # 用户进入目录是否显示消息

xferlog\_enable=YES # 是否开启xferlog日志功能

xferlog\_std\_format=YES # xferlog日志文件格式

connect\_from\_port\_20=YES # 使用主动模式连接，启用20端口

pasv\_enable=YES # 是否启用被动链接，默认为被动模式

pasv\_max\_port=24600 # 被动模式链接的最大端口号

pasv\_min\_port=24500 # 被动模式连接的最小端口号

userlist\_enable=YES # 是否启用userlist用户列表文件

userlist\_deny=YES # 是否禁止userlist文件中的账户访问FTP

max\_clients=2000 # 最大允许同时2000客户端连接，0代表无限制

max\_per\_ip=0 # 每个客户端的最大链接限制，0代表无限制

tcp\_wrappers=YES # 是否启用tcp\_wrappers

guest\_enable=YES # 如果为YES，则所有非匿名登陆都映射

# guest\_username指定的账户

guest\_username=ftp # 设定来宾账户

user\_config\_dir=/etc/vsftpd/conf # 指定目录，在该目录下可以为用户设置独立的配置文

# 件与选项

dual\_log\_enable=NO # 是否启用双日志功能，生成两个日志文件

anonymous\_enable=YES # 是否开启匿名访问功能，默认为开启

chroot\_list\_enable=YES # 是否开启限制访问配置

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

# 限制访问配置文件路径，把需要访问自己家目录的用户信息配置到文件/etc/vsftpd/chroot\_list中，并写入只允许访问家目录的用户即可。（一行一个用户）

匿名账户

anon\_root=/var/ftp # 匿名访问FTP的根路径，默认为/var/ftp

anon\_upload\_enable=YES # 是否允许匿名账户上传，默认禁止

anon\_mkdir\_write\_enable=YES # 是否允许匿名账户创建目录，默认禁止

anon\_other\_write\_enable=YES # 是否允许匿名账户进行其他所有写操作

anon\_max\_rate=0 # 匿名数据上传率(B/s)

anon\_umask=077 # 匿名上传权限掩码

本地账户

local\_enable=YES # 是否启用本机账户FTP功能

local\_max\_rate=0 # 本地账户数据上传率（B/s）

local\_umask=077 # 本地账户权限掩码

chroot\_local\_user=YES # 是否禁锢本地账户根目录，默认为NO

local\_root=/ftp/common # 本地账户访问FTP根路径

## 账户权限

vsftpd支持的常用登陆方式有：匿名登陆、本地账户登陆、虚拟账户登陆三种方式。

匿名账户登陆一般应用于下载服务器。vsftpd默认开启的是匿名共享，默认共享路径为/var/ftp

本地账户登陆则需要使用系统账户以及对应的系统密码才可以登录使用FTP。默认anonymous\_enable与local\_enable均被设置为YES，此时FTP为匿名访问模式，如果需要开启本地账户FTP功能，需要将anonymous\_enable设置为NO，默认共享路径为个人家目录。

需要注意的是，开启本地账户登陆后，用户可以离开家目录，从而进入系统中的其他目录，这样是非常危险的，如果在配置文件中使用chroot-local\_user，用户将被禁锢在自己的家目录下，放置用户进入系统中的其他目录。

当有大量用户需要使用FTP时，vsftpd支持虚拟账户模拟登陆FTP，从而避免了创建大量的系统账户，通过guest\_enable可以开启vsftpd的虚拟账户功能，guest\_username用阿里指定本地账户的虚拟映射名称。

vsftpd有两个文件（黑名单文件和白名单文件）可以对用户进行ACL控制，/etc/vsftpd/ftpusers默认是一个黑名单文件，存储在该文件的所有用户将无法访问FTP，格式为每行一个账户名称。/etc/vsftpd/user\_list文件会根据注配置文件中配置项设定的不通，而成为黑名单或白名单文件。此外，也可以禁用该文件。主配置文件中的userlist\_enable决定了是否启用user\_list文件。黑名单表示拒绝名单中的账户访问FTP，也就是其他所有的账户默认允许访问FTP。而白名单表示仅允许白名单中的账户访问FTP，没有在白名单中的其他所有账户则默认将拒绝访问FTP。

常见问题

1，提示错误代码：530 Login incorrect

如果登陆提示530错误，说明登陆过程中账户验证失败。则可能是因为你使用的是64位操作系统，而pam文件中库文件的调用却使用的是/lib/security/pam\_userdb.so。或者是用户名或密码输入有错误。此外，也可能是vsftpd主配置文件中pam\_service\_name设置的pam文件名称与/etc/pam.d中创建的pam文件名称不一致，导致无法验证成功。

2，提示错误代码：500 OOPS:cannot change directory:/home/ftp/$USER

该提示代表目录不存在或无权限导致的无法切换至目录，也有可能是SELinux导致的无法共享账户家目录，默认SELinux不允许共享家目录

3，使用windows系统访问主动模式的vsftpd服务器时无法访问成功

默认Windows会使用被动模式连接FTP服务器，如果需要以主动模式连接服务器，需要修改浏览器的属性，方法是查找Internet选项的“高级”选项卡，找到使用被动FTP，取消该功能即可。

4，账户登陆后无法上传数据

根据不用的账户类型，检查主配置文件的设置，匿名账户与虚拟账户以anon\_开头的权限设置，本地账户检查以local\_开头的权限设置，并且要确保全局write\_enable设置为YES。此外，文件系统目录的权限也需要修改，确保客户端账户有访问该目录的权限。

5，启动服务器报错：500 OOPS: bad bool value in config file

vsftpd配置文件设置错误，检查配置文件。配置文件要求每个设置项占用独立的一行，并且不可以有多余的空格