

前言

本文，主要以vsftp软件为主进行讲解，版本为3.0.2。以介绍设置虚拟用户、权限验证为主，linux权限知识默认大家都有所了解。vsftpd设置有两种模式：主动模式、被动模式。

Linux网络文件共享。例如NFS、Sambfs、FTP，其中以FTP应用最为广泛，成为了当下linux文件系统中主流的网络文件共享工具。介绍FTP主要有几种常见的工具vsftp、proftp、wu-ftp、pureftp，各种FTP软件无优劣之分，实际工作中选择自己熟悉的一款即可。



正文

一、vsftp安装

注意：以Redhat7系列（或者支持systemd环境的linux系统）

1、准备安装包

我的gitee仓库：<https://gitee.com/dywangk/SQL-study/tree/master/vsftpd>

当然可以到此网站下载各个版本：<http://www.rpmfind.net/linux/rpm2html/search.php?query=vsftpd>

```
vsftpd-3.0.2-29.e17_9.x86_64.rpm
```

2、安装

```
rpm -ivh vsftpd-3.0.2-29.e17_9.x86_64.rpm
```

查询是否安装

```
rpm -qa | grep vsftpd
```

二、启动与停止

1、设置开启自启

```
systemctl enable vsftpd.service
```

2、启动vsftpd服务

```
systemctl start vsftpd.service
```

3、查看vsftpd服务状态

```
systemctl status vsftpd.service
```

4、查看vsftpd进程

```
ps -ef | grep vsftpd  
#或者  
ps -aux | grep vsftpd
```

三、错误排查

1、通过Git Bash验证ftp登录

在本机会提示没有ftp命令，直接就在远端测试连接。

```
ftp remote_ip
```

2、排查错误

其实翻译一下就知道了，chroot配置没有写入的权限。

```
OOPS: vsftpd: refusing to run with writable root inside chroot()  
Login failed.
```

3、在vsftpd.conf加入如下配置

后续的版本更新了，需要手动加上allow_writeable_chroot=YES参数配置

```
allow_writeable_chroot=YES
```

4、重启vsftpd服务 (Redhat7系列)

```
systemctl restart vsftpd.service
```

四、优化设置

1、设置防火墙规则

关于防火墙的设置，可以参考我的历史文章

【Redhat系列linux防火墙工具】firewalld与iptables防火墙工具的激烈碰撞

https://blog.csdn.net/Tolove_dream/article/details/122293458

重启测试vsftpd上传文件，默认存储路径为该用户的home目录下

```
#例如  
/home/vsftpd/test
```

如需更改配置，如下设置

```
local_root=/var/ftp/pub
```

防火墙加入ftp服务

```
firewall-cmd --zone=public --add-service=ftp --permanent
```

主动模式，防火墙开启20、21端口

```
firewall-cmd --zone=public --add-port=21/tcp --permanent  
firewall-cmd --zone=public --add-port=20/tcp --permanent
```

设置当前ftp存储目录用户权限、chroot_list文件配置用户登录、设置虚拟用户。

注意：在Windows资源管理访问，网络共享中心->Internet属性->高级，开启被动访问ftp（开启兼容模式）

2、设置selinux

1、设置SELinux为宽容模式或者临时关闭

```
#临时改成宽容模式  
setenforce 0  
#查看selinux  
[root@dywangk test]# getenforce  
Permissive
```

2、永久设置selinux，修改配置文件 /etc/sysconfig/selinux

```
#查看，默认配置文件是开启的
cat /etc/sysconfig/selinux
SELINUX=enforcing
#禁用selinux
SELINUX=disable
#宽容模式
SELINUX=Permissive
```

五、配置参考

1、示例配置虚拟用户

编辑配置文件 `vim /etc/vsftpd/vsftpd.conf`

```
# Example config file /etc/vsftpd/vsftpd.conf
#绑定本机IP
listen_address=192.168.245.134
#禁止匿名用户登录
anonymous_enable=NO
#允许本地用户访问
local_enable=YES
#开启写入权限
write_enable=YES
#在后续比较高的版本中需要加入允许chroot写的权限
allow_writeable_chroot=YES
#上传文件后默认权限掩码
local_umask=022
#默认不开放匿名用户上传权限
#anon_upload_enable=YES
#默认不开放匿名用户创建于写的权限
#anon_mkdir_write_enable=YES
#
dirmessage_enable=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
#默认为FTP主动模式，需要开启防火墙20、21端口
connect_from_port_20=YES
#
#chown_uploads=YES
#chown_username=whoever
#
#xferlog_file=/var/log/xferlog
#
xferlog_std_format=YES
#
#idle_session_timeout=600
#
#data_connection_timeout=120
#
#nopriv_user=ftpsecure
#
```

```

#async_abor_enable=YES
#
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
#ftpd_banner=welcome to blah FTP service.
#
#deny_email_enable=YES

#banned_email_file=/etc/vsftpd/banned_emails
#禁止FTP用户离开自己的主目录
chroot_local_user=YES
chroot_list_enable=NO
# (default follows)
#虚拟用户列表，设置默认允许登录FTP的用户，每行一个用户
chroot_list_file=/etc/vsftpd/chroot_list
#开启虚拟用户功能
guest_enable=YES
#虚拟用户宿主目录
guest_username=ftp
#用户登录后操作主目录和本地用户具有同样的权限
virtual_use_local_privs=YES
#虚拟用户主目录配置文件
user_config_dir=/etc/vsftpd/vconf

#ls_recurse_enable=YES
#开启监听,开启ipv4就禁用listen_ipv6
listen=YES
#
listen_ipv6=NO
#权限验证需要的加密文件
pam_service_name=vsftpd.vu
#pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES

```

在/etc/vsftpd/chroot_list加入虚拟用户user1和user2。这里直接用vim编辑是一样的加入配置，每行对应一个用户。

```

echo 'user1' >> /etc/vsftpd/chroot_list
echo 'user2' >> /etc/vsftpd/chroot_list

```

2、新增用户并指定目录

建议：linux下赋予权限底线，在最小权限范围内满足需求即可。

```

#创建虚拟用户目录
mkdir -p /data/{user1,user2}
#赋予权限，测试直接赋予最高权限了，实际工作中建议在最小权限范围内满足即可。
chmod -R 777 /data/user1
chmod -R 777 /data/user2

```

3、设置用户名密码数据库

下面使用的\n并非错误输入，是的，就是正常的换行。熟悉编程的小伙伴应该不陌生，在Java语言的打印输出大家应该有印象吧！

```
class test{
    public static void main(String args){
        system.out.println("hello world!!!");
    }
}
```

在虚拟用户存储用户名以及密码

```
#用vusers.list来区分本机用户与虚拟用户配置
echo -e "user1\n123456\nuser2\n123456" > /etc/vsftpd/vusers.list
#切换到vsftpd配置目录
cd /etc/vsftpd/
#解析vusers.list到vusers.db
db_load -T -t hash -f vusers.list vusers.db
#赋予权限
chmod 600 vusers.*
```

4、指定认证方式

```
echo -e "#%PAM-1.0\n\nauth required pam_userdb.so db=/etc/vsftpd/vusers\naccount
required pam_userdb.so db=/etc/vsftpd/vusers" > /etc/pam.d/vsftpd.vu
#创建虚拟配置文件目录
mkdir /etc/vsftpd/vconf
#进入虚拟用户配置文件目录
cd vconf/
#新增配置
echo 'local_root=/data/user1' > user1
echo 'local_root=/data/user2' > user2
#查看配置
ls
user1 user2
#查看user1与user2的主目录
cat user1
local_root=/data/user1
cat user2
local_root=/data/user2

#新建测试文件
touch /data/user1/test1
touch /data/user2/test2
```

如果没有指定虚拟用户的ftp目录，默认访问目录如下

```
/var/ftp/pub/
```

经过测试设置的虚拟用户user2禁锢在了 `/data/user2` 目录下

```
#在Windows下访问到新增的test1、test2文件，如果没变过来多刷新几遍  
/data/user1/test1  
/data/user2/test2
```

5、ftp命令登录验证

Git Bash验证

```
ftp remote_ip
```

或者在资源管理验证测试新增、删除、修改。

```
ftp://remote_ip
```

[by 龙腾万里sky 原创不易，白嫖有瘾](#)