

修改ftp的默认根目录只要修改/etc/vsftpd/vsftpd.conf文件即可：

加入如下几行：

local\_root=/var/www/html

chroot\_local\_user=YES

anon\_root=/var/www/html

|  |  |
| --- | --- |
| **文件** | **说明** |
| /etc/vsftpd/vsftpd.conf | VSFTPD主配置文件 |
| /etc/rc.d/init.d/vsftpd | VSFTPD启动脚本，独立（stand alone）服务模式 |
| /etc/pam.d/vsftpd | PAM认证文件（此文件中file=/etc/vsftpd/ftpusers字段，指明阻止来自/etc/vsftpd/ftpusers文件中的用户访问） |
| /etc/vsftpd/ftpusers | 禁止使用vsftpd的ftp用户列表文件 |
| /etc/vsftpd/user\_list | 禁止或允许使用vsftpd的ftp用户列表文件（根据主配置文件来定） |
| /var/ftp | 匿名用户主目录 |
| /var/log/xferlog | VSFTPD日志文件 |

一、FTP服务器         <http://ming228.blog.51cto.com/421298/112083/>

1.安装vsftpd

yum install vsftpd

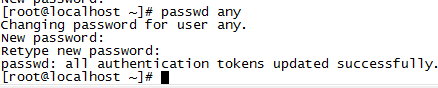
2.新增ftp用户

useradd -s /sbin/nologin -d /data1/jenkins/workspace/ -g dev vstp

useradd -d /home/ftp   test //增加用户test，并制定test用户的主目录为/home/ftp

C:\Users\Administrator\AppData\Local\YNote\data\qqCED47168DC2F90564C19440FF1BBF0DB\8132275df4d64491b979c39c5dd6d45d\clipboard.png

3.设置密码



4.禁止匿名登录

 修改/etc/vsftpd/vsftpd.conf文件如下：  
anonymous\_enable=NO

5.账号权限控制

vsftpd的配置，配置文件中限定了vsftpd用户连接控制配置。  
vsftpd.ftpusers：位于/etc目录下。它指定了哪些用户账户不能访问[FTP服务器](http://www.myhack58.com/Article/sort099/sort0101/Article_101_1.htm" \t "_blank)，例如root等。  
vsftpd.user\_list：位于/etc目录下。该文件里的用户账户在默认情况下也不能访问[FTP服务器](http://www.myhack58.com/Article/sort099/sort0101/Article_101_1.htm" \t "_blank)，仅当vsftpd .conf配置文件里启用userlist\_enable=NO选项时才允许访问。  
vsftpd.conf：位于/etc/vsftpd目录下。来自定义用户登录控制、用户权限控制、超时设置、服务器功能选项、服务器性能选项、服务器响应消息等[FTP服务器](http://www.myhack58.com/Article/sort099/sort0101/Article_101_1.htm" \t "_blank)的配置。

6.修改好之后，重启FTP服务

 #service vsftpd restart

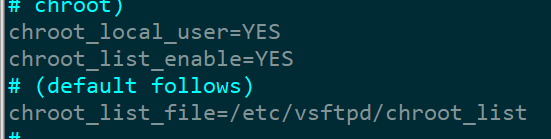
或者

C:\Users\Administrator\AppData\Local\YNote\data\qqCED47168DC2F90564C19440FF1BBF0DB\c91f7dd50bd6422e8c06d3d7bd41f3fd\clipboard.png

7、创建账号

1、vsftp上创建账号

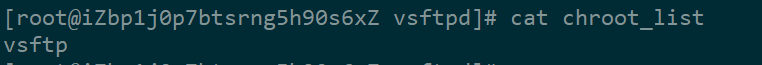
2、更改vsftp配置：



chroot\_list\_enable=YES //限制访问自身目录

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

8、vi /etc/vsftpd/chroot\_list



9、修改默认端口

vi /etc/vsftpd/vsftpd.conf

修改/etc/services

vi /etc/services  
修改成：  
ftp             3009/tcp  
ftp             3009/udp

主动模式配置：

pasv\_enable=NO #关闭被动模式

listen\_port=3009 #指定命令通道为8021,默认为21

listen\_data\_port=3010 #指定数据通道为8020,默认为20

被动模式配置：

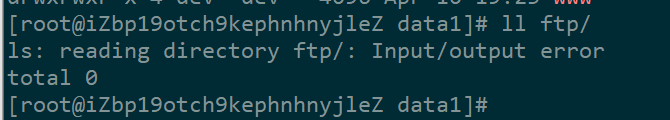
在原来的基础上加上：

connect\_from\_port\_20=NO 默认是yes,主动模式，默认是注释掉的。所以改成NO  
listen\_port=3009 #监听端口

pasv\_enable=YES #启用被动模式  
pasv\_min\_port=3010 #设定在PASV模式下，建立数据传输所时可以使用port范围的下界和上界

pasv\_max\_port=3010  
pasv\_promiscuous=YES #此选项激活时，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。默认值为NO。  
ftpd\_banner=Welcome to  FTP service

挂载成功后，目录无法写入文件：



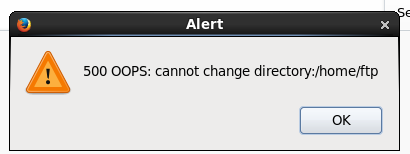
安全配置：

1. 3、限制登录
2. userlist\_enable=yes      //用userlist来限制用户访问
3. userlist\_deny=no          //名单中的人不允许访问
4. userlist\_file=/etc/vsftpd/userlist\_deny.chroot     //限制名单文件放置的路径
5. 4、限制目录
6. chroot\_local\_user=yes   //限制所有用户都在家目录
7. chroot\_list\_enable=YES   //调用限制在家目录的用户名单
8. chroot\_list\_file=/etc/vsftpd/chroot\_list   //限制在家目录的用户名单所在路径

1、可以上传(全局控制) 删除，重命名。write\_enable=YES

2、只能下载。不能上传、删除、重命名。write\_enable=NO   
3、只能上传、删除、重命名。不能下载。download\_enable＝NO

搭建后，使用Windows登录，有可能只出现登录框  会让你一直输入用户名和密码认证，用centOS登录，提示如下错误：



[VsFTP出现500 OOPS: cannot change directory的解决办法](http://blog.chinaunix.net/uid-24917554-id-1644947.html)

    在linux中搭建ftp服务后使用ftp查看，只能看见ftp目录中的pub文件夹，看不到其他文件夹，使用ls -ld查看两个文件夹的权限设置是一模一样的，怎么会出现这种状况呢，网上找资料原来是selinux阻止了对其他目录的访问了，setsebool -P ftpd\_disable\_trans 1 ，让selinux 开放对ftp的访问，并vi /etc/vsftpd/vsftpd.conf 在最后加上一行anon\_root=/var/ftp 将ftp匿名访问的默认路径设置到/var/ftp下，将所有要访问的资源mount到这个目录下，service vsftpd restart ，再进ftp查看，这次不止显示pub文件夹了。

[root@localhost ~]# setsebool ftpd\_disable\_trans 1

Could not change active booleans: Invalid boolean

又出现一个错误，我们将ftp\_home\_dir设置为on，重启vsftpd。

[root@localhost ~]# setsebool ftp\_home\_dir=1

[root@localhost ~]# service vsftpd restart

关闭 vsftpd：[确定]

为 vsftpd 启动 vsftpd：[确定]

[root@localhost ~]# sestatus -b| grep ftp

allow\_ftpd\_anon\_write                       off

allow\_ftpd\_full\_access                      off

allow\_ftpd\_use\_cifs                         off

allow\_ftpd\_use\_nfs                          off

ftp\_home\_dir                                on

ftpd\_connect\_db                             off

ftpd\_use\_passive\_mode                       off

httpd\_enable\_ftp\_server                     off

tftp\_anon\_write                             off

重新在windows 7下面连接，正常啦！用户可以登陆啦！

**问题一：ftpusers和user\_list两个文件各自的用途是什么？有何关系？**

**ftpusers不受任何配制项的影响，它总是有效**，它是一个黑名单！  
该文件存放的是一个禁止访问FTP的用户列表，通常为了安全考虑，管理员不希望一些拥有过大权限的帐号（比如root)登入FTP，以免通过该帐号从FTP上传或下载一些危险位置上的文件从而对系统造成损坏。  
  
而user\_list则是和vsftpd.conf中的userlist\_enable和userlist\_deny两个配置项紧密相关的，它可以有效，也可以无效，有效时它可以是一个黑名单，也可以是一个白名单！那么是什么的设置决定了它的作用呢？这就是问题二要解释的。  
  
所以简单总结就是：ftpusers和user\_list没有任何关系，ftpusers文件总是生效，user\_list则取决于userlist\_enable和userlist\_deny两项配置。

**问题二：vsftpd.conf中的userlist\_enable和userlist\_deny两个配置项各自起什么作用，两者如何搭配使用?**  
  
为了说明这个问题，我们来建立两个测试用户：

tom: 在user\_list中  
jim:不在user\_list中

然后我们分别给两个配置项取不同的值，分4种Case进行测试：  
  
Case 1: userlist\_enable=YES, userlist\_deny=YES

tom: 拒绝登入  
jim: 允许登录

Case 2: userlist\_enable=YES, userlist\_deny=NO

tom: 允许登录  
jim:拒绝登录（如user\_list文件开头的注释所述，甚至不会提示输入密码，即无登入提示框，直接拒绝连接）

Case 3: userlist\_enable=NO,userlist\_deny=NO

tom: 允许登录  
jim: 允许登录

Case 4: userlist\_enable=NO,userlist\_deny=YES

tom: 允许登录  
jim: 允许登录

综上实验得出以下结论：

1. userlist\_enable和userlist\_deny两个选项联合起来针对的是：本地全体用户（除去ftpusers中的用户）和出现在user\_list文件中的用户以及不在在user\_list文件中的用户这三类用户集合进行的设置。
2. 当且仅当userlist\_enable=YES时：userlist\_deny项的配置才有效，user\_list文件才会被使用；当其为NO时，无论userlist\_deny项为何值都是无效的，本地全体用户（除去ftpusers中的用户）都可以登入FTP
3. 当userlist\_enable=YES时，userlist\_deny=YES时：user\_list是一个**黑名单**，即：所有出现在名单中的用户都会被拒绝登入；
4. 当userlist\_enable=YES时，userlist\_deny=NO时：user\_list是一个**白名单**，即：只有出现在名单中的用户才会被准许登入(user\_list之外的用户都被拒绝登入)；另外需要特别提醒的是：**使用白名单后，匿名用户将无法登入！除非显式在user\_list中加入一行：anonymous**