sftp 限制用户登陆指定目录(家目录)

限制 sftp 用户登陆后，只能在家目录下活动，不能到其他或上级目录，可以按照下面方法进行操作：

一、升级ssh软件，版本必须在 4.8 以上；

二、备份配置文件：(以下所有命令，都需要使用root用户来执行)

1 cd /etc/ssh/

2 mv sshd\_config sshd\_config.bak

3 mv sshd\_config.rpmnew sshd\_config

三、修改 /etc/ssh/sshd\_config

1 #Subsystem sftp /usr/libexec/openssh/sftp-server （这行必须注释掉）

2 Subsystem sftp internal-sftp

3 Match Group chroot

4 ChrootDirectory /chroot/%u

5 ForceCommand internal-sftp

说明：本配置中，ChrootDirectory 是 /chroot/%u，匹配这个规则的组名为 chroot，所以以后添加需要限制活动目录的用户时，必须属于chroot这个组；

四、建立相关目录，添加用户和组，这里以work用户为例：

1 cd /

2 mkdir chroot

3 groupadd chroot

4 useradd -g chroot -d /chroot/work -m -s /bin/bash work

5 passwd work

6 chown root /chroot/work

7 chmod 750 /chroot/work

说明：在/chroot目录下，用户家目录 work 的属主必须是root，而不能是用户本身，属组的话，必须是chroot，权限 750 (需要注意的是，新建用户的家目录，权限是700，但这样sftp登陆的话，是看不到目录下的列表的，所以，必须是750的权限) 例如：

1 drwxr-x--- 7 root chroot 4096 Aug 5 13:23 work

五、如果需要上传文件，则按照下面执行：

1 cd /chroot/work

2 mkdir {upload,pub}

3 chmod a+w upload -R upload

其中，upload目录为可读写权限，可以用来上传，pub目录为只读权限，可以用来下载。

六、测试

1 service sshd restart

2 sftp work@ip