## [Linux 创建sftp用户并限制目录权限](https://www.cnblogs.com/grimm/p/12156576.html)

最近搞一个sftp项目，用于给第三方公司上传文件，期间查询了很多种方式，依然无法限制目录，很苦恼，本次经过无数次试验，终于成功了。

提供sftp服务的有vsftpd和internal-sftp，这里用的是系统自带的internal-sftp，操作步骤如下：

下面是千篇一律的步骤，网上大抵相同。

1、创建用户 sftpuser，并禁止ssh登录，不创建家目录

       useradd -s /sbin/nologin -M sftpuser

2、设置用户密码

       passwd sftpuser

3、创建sftp根目录，所有sftp用户都将在该目录下活动。（如果以后不会在新增新用户的话，可跳过此目录）

       mkdir /home/sftp

4、设置目录权限，目录的权限设定有两个要点：

      目录开始一直往上到系统根目录为止的目录拥有者都只能是root

      目录开始一直往上到系统根目录为止都不可以具有群组写入权限

      chown root:root /home/sftp

      chmod 755 /home/sftp      注：该目录权限最大为755，设置成777会报错，这个也是我困扰我的一个地方。

5、创建用户sftpuser根目录，目录名为用户名

       cd /home/sftp

       mkdir sftpuser

6、设置sftpuser目录权限

       chown root:sftpuser /home/sftp/sftpuser

       （注：设置用户sftpuser，如果设置拥有者为root，表示该目录sftpuser没有权限读写，在该目录下建立其它目录，赋权给sftpuser用户读写权限；

           若需要对该目录拥有读写权限，设置权限：chown sftpuser:sftpuser /home/sftp/sftpuser）

        chmod 755 /home/sftp/sftpuser   注：这里的目录sftpuser  权限也只能是755，否则无法限制目录。

7、配置sshd\_config

        vi /etc/ssh/sshd\_config

8、修改如下内容，并保存退出

|  |
| --- |
| #注释掉这行          #Subsystem sftp /usr/libexec/openssh/sftp-server          添加这行：          Subsystem sftp internal-sftp  #指定使用sftp服务使用系统自带的internal-sftp，如果不添加，用户无法通过sftp登录。          #添加在配置文件末尾          Match User sftpuser#匹配用户，如果要匹配多个组，多个组之间用逗号分割          ChrootDirectory /home/sftp/%u #用chroot将指定用户的根目录，chroot的含义：http://www.ibm.com/developerworks/cn/linux/l-cn-chroot/；                #这里的%u指的是账号名，/home/sftp/%u 含义是：/home/sftp/sftpuser          ForceCommand internal-sftp #指定sftp命令          X11Forwarding no #这两行，如果不希望该用户能使用端口转发的话就加上，否则删掉          AllowTcpForwarding no |

 9、重启sshd服务器

|  |
| --- |
| systemctl restart sshd.service          #查询sshd启动状态命令：          systemctl status sshd.service |

10、sftpuser用户登录测试：

|  |
| --- |
| sftp -oPort=22 sftpuser@127.0.0.1 |

      至此已经完成了sftp创建用户，并修改权限，限制根目录。

在用户登录测试过程中，可能会遇到如下错误：

         Couldn't read packet: Connection reset by peer

这是什么原因导致的呢，当时我一直很困惑，后来发现，是目录权限导致了该问题，具体解决方案，回看以上4、5、6步骤！