

在Linux中搭建一个FTP服务器 - SherrySXL - 博客园

在Linux中搭建一个ftp服务器，以供两个工作小组保管文件使用。禁用匿名。第一个小组使用ftp账号：ftp1，工作目录在：/var/ftp/ftp1；第二个小组使用ftp2，工作目录在：/var/ftp/ftp2。

两个小组互相不能访问各自的文件，需要限制用户不能离开自己的工作目录。

【实现步骤】

1.检查安装vsftpd服务器

以root进入终端后（其他账户进入终端的可以用su root 输入密码后进入root 模式）之后，在终端命令窗口输入以下命令进行验证：# rpm -qa | grep vsftpd。如果结果显示为“vsftpd-1.1.3-8”，则说明系统已经安装vsftpd服务器。若没有回复，即系统中没有安装。

```
[root@localhost ~]# rpm -q vsftpd
package vsftpd is not installed
[root@localhost ~]# rpm -qa | grep vsftpd
[root@localhost ~]#
```

2.rhel版本的系统光盘中带有vsftpd安装包，所以接下来，是挂载系统光盘到/media下以便调取。

```
[root@localhost ~]# mount /dev/cdrom /mnt
mount: can't find /dev/cdrom/media in /etc/fstab or /etc/mtab
[root@localhost ~]# mkdir /mnt/cdrom/media
[root@localhost ~]# ls
anaconda-ks.cfg  Desktop  game  install.log  install.log.syslog
```

3.上述截图显示本系统中没有安装vsftpd服务器，则用rpm命令安装。

即在终端命令窗口中安装vsftpd的命令：#rpm -ivh vsftpd-1.1.3-8.i386.rpm。

(1) 先mount光驱，在/mnt/cdrom/Server目录里有rpm，rpm -ivh vsftpd*

```
[root@localhost ~]# mount /dev/cdrom /mnt
mount: 找不到介质
[root@localhost ~]# mount /dev/cdrom /mnt
mount: 找不到介质
[root@localhost ~]# mount /dev/cdrom /mnt
mount: block device /dev/cdrom is write-protected, mounting read-only
[root@localhost ~]#
```

点亮一下右下角的光盘

```
[root@localhost ~]# cd /mnt/Server
[root@localhost Server]# rpm -ivh vsftpd-*
warning: vsftpd-2.0.5-10.el5.i386.rpm: Header V3 DSA signature: NOKEY, key ID 37
017186
Preparing...
1:vsftpd
[root@localhost Server]#
```

首先要进入Server目录里面

4.创建用户

(1) 首先要启动服务

```
l:vsftpd
[root@localhost Server]# service vsftpd start
为 vsftpd 启动 vsftpd
[root@localhost Server]# adduser -s/ bin/false -d/var/ftp/ftpl ftp1
Usage: useradd [options] LOGIN
```

[确定]

(2) 创建两个用户

```

[root@localhost Server]# adduser -s /bin/false -d /var/ftp/ftpl ftp1
[root@localhost Server]# passwd ftp1
Changing password for user ftp1.
New UNIX password: 密码是123456
BAD PASSWORD: it is too simplistic/systematic
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@localhost Server]# adduser -s /bin/false -d /var/ftp/ftpl ftp2
adduser: 警告: 此主目录已经存在。
不从 skey 目录里向其中复制任何文件。
[root@localhost Server]# adduser -s /bin/false -d /var/ftp/ftp2 ftp2
adduser: 用户 ftp2 已存在
[root@localhost Server]# passwd ftp2
Changing password for user ftp2.
New UNIX password: 密码是123456
BAD PASSWORD: it is too simplistic/systematic
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@localhost Server]#

```

5.vsftpd的配置

安装完之后在/etc/vsftpd/路径下会存在三个配置文件。

vsftpd.conf: 主配置文件

ftputers: 指定哪些用户不能访问FTP服务器,这里的用户包括root在内的一些重要用户。

user_list: 指定的用户是否可以访问ftp服务器, 通过vsftpd.conf文件中的userlist_deny的配置来决定配置中的用户是否可以访问, userlist_enable=YES, userlist_deny=YES, userlist_file=/etc/vsftpd/user_list 这三个配置允许文件中的用户访问FTP。

(1) 查看主配置文件的默认配置:

(使用: cat /etc/vsftpd/vsftpd.conf | grep -v '^#';)

```

cat: /var/ftp/f/vsftpd.conf: 没有那个文件或目录
[root@localhost Server]# cat /etc/vsftpd/vsftpd.conf | grep -v '^#'
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_std_format=YES
listen=YES

pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
[root@localhost Server]#

```

(2) 修改配置文件:

登录ftp后会发现, 用户可以访问其他目录, 并且具有mpsp组的权限, 这样做是不允许的, 我们需要将用户的访问范围控制在其主目录下。方法如下:

a. vi /etc/vsftpd/vsftpd.conf进入ftp配置文件目录并编辑此文件,

```

userlist_enable=YES
tcp_wrappers=YES
[root@localhost Server]# vi /etc/vsftpd/vsftpd.conf
[root@localhost Server]#

```

b.找到#chroot_list_enable=YES,删除前面的那个#号,表示开启此限制功能;

找到chroot_list_file: chroot_list_file=/etc/vsftpd/chroot_list, 删除前面的那个#号,表示开启此限制功能; 加入chroot_local_use=NO (进入编辑框后按进行开始编辑)

```

# You may specify an explicit list of local users to chroot() to th
# directory. If chroot_local_user is YES, then this list becomes a
# users to NOT chroot().

chroot_local_user=NO 添加这一行
chroot_list_enable=YES

# (default follows)

chroot_list_file=/etc/vsftpd/chroot_list

```

c.进入配置文件后, 在末尾加入如下三行:

① userlist_enable=YES

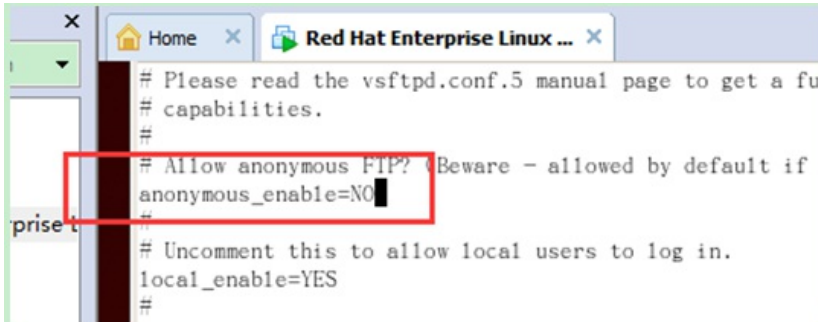
userlist_deny=NO

userlist_file=/etc/vsftpd/vsftpd.user_list

```
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES

userlist_enable=YES
userlist_deny=NO
userlist_file=/etc/vsftpd/vsftpd.user_list
```

d. 禁止匿名用户登录

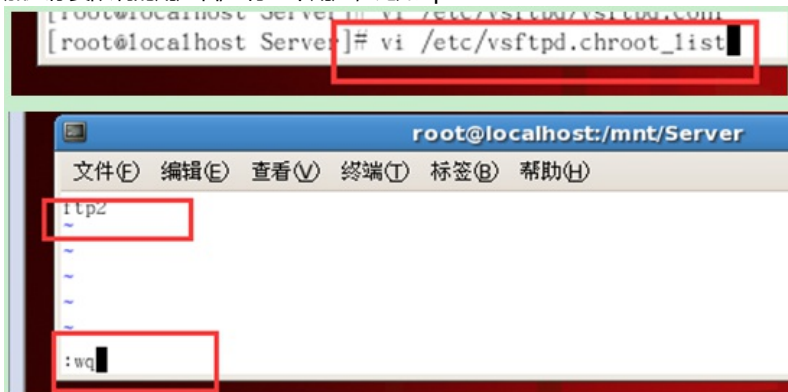


(编辑完, 按esc后使用 “: wq” 保存并退出)

e. 对一些文件进行编辑

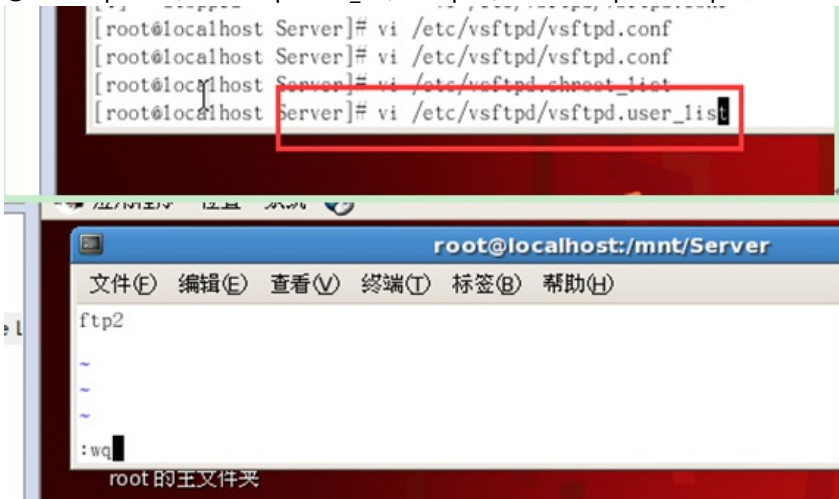
① 在etc目录找到vsftpd.chroot_list文件, 进入编辑状态

加入你要限制的用户名, 一行一个用户, 比如ftp2



(编辑完, 按esc后使用 “: wq” 保存并退出)

② 进入vsftpd目录, 找到vsftpd.user_list, 键入ftp11, 意味允许ftp11登陆ftp服务器



(编辑完, 按esc后使用 “: wq” 保存并退出)

再在本机上, 通过控制台, 用ftp1通过ftp访问系统, 用户成功登陆, 并且成功的被限制在自己的主目录下, 无法访问其他目录。

依次方法创建了2个用户, ftp1、ftp2。

查看ftp状态 `sestatus -b | grep ftp`:

```
bash: status: command not found
[root@localhost Server]# sestatus -b | grep ftp
allow_ftpd_anon_write off
allow_ftpd_full_access off
allow_ftpd_use_cifs off
allow_ftpd_use_nfs off
allow_tftp_anon_write off
ftp_home_dir off
ftpd_connect_db off
ftpd_disable_trans off
ftpd_is_daemon on
httpd_enable_ftp_server off
tftpd_disable_trans off
[root@localhost Server]#
```

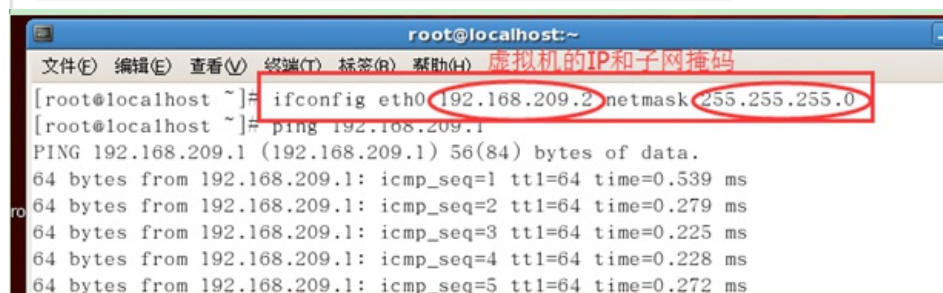
然后输入:

```
bash: setsebool: command not found
[root@localhost Server]# setsebool -P ftpd_disable_trans on
ftp3 homedir /var/ftp/ftp1 or its parent directory conflicts with a
defined context in /etc/selinux/targeted/contexts/files/file_contexts.
/usr/sbin/genhomedircon will not create a new context. This usually indicates an incorrectly def
ined system account. If it is a system account please make sure its login shell is /sbin/nologi
n.
ftp4 homedir /var/ftp/ftp4 or its parent directory conflicts with a
defined context in /etc/selinux/targeted/contexts/files/file_contexts.
/usr/sbin/genhomedircon will not create a new context. This usually indicates an incorrectly def
ined system account. If it is a system account please make sure its login shell is /sbin/nologi
n.
[root@localhost Server]#
```

关闭防火墙:

```
[root@localhost Server]# vi /etc/xsftpd/xsftpd_user_list
[root@localhost Server]# /etc/init.d/iptables stop
清除防火墙规则:
把 chains 设置为 ACCEPT 策略: filter
正在卸载 iptables 模块:
[root@localhost Server]#
```

以下步骤是实现主机和虚拟机的互相ping通:



C:\WINDOWS\system32\cmd.exe 主机ping虚拟机，ping通了

C:\Users\acer>ping 192.168.209.2

正在 Ping 192.168.209.2 具有 32 字节的数据:
来自 192.168.209.2 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.209.2 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.209.2 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.209.2 的回复: 字节=32 时间<1ms TTL=64

192.168.209.2 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 0ms, 最长 = 0ms, 平均 = 0ms

最终结果:

C:\WINDOWS\system32\cmd.exe

C:\Users\acer>ping 192.168.209.2

正在 Ping 192.168.209.2 具有 32 字节的数据:
来自 192.168.209.2 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.209.2 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.209.2 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.209.2 的回复: 字节=32 时间<1ms TTL=64

192.168.209.2 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\acer>ftp 192.168.209.2

连接到 192.168.209.2。
220 (vsFTPd 2.0.5)
530 Please login with USER and PASS.
用户(192.168.209.2:(none)): ftp3
331 Please specify the password.
密码:
500 OOPS: could not open chroot(<) list file:/etc/vsftpd/chroot_list
远程主机关闭连接。

C:\Users\acer>