ftp服务搭建

1. 匿名服务搭建

1.1、ftp服务器配置：vi /etc/vsftpd/vsftpd.conf，具体内容如下：

anonymous\_enable=YES

anon\_upload\_enable=YES

anon\_mkdir\_write\_enable=YES

1.2、ftp目录的权限设置

默认情况下，ftp的根目录为/var/ftp，为了安全，这个目录默认不允许设置为777权限，否则ftp将无法访问。但是我们要匿名上传文件，需要“other”用户的写权限，正确的做法：

在/var/ftp中建立一个upload（名子自己起吧）文件夹，将个文件夹权限设置为777（视具体需要自己设），在upload这个文件夹中，匿名用户可以上传文件、创建文件夹、删除文件等。

vsftpd增强了安全检查，如果用户被限定在了其主目录下，则该用户的主目录不能再具有写权限了。可以用命令chmod a-w /var/ftp 去除用户主目录的写权限。

一般至此，便实现vsftpd匿名用户的上传下载了。如果还不行，就是下面的问题。

1.3、SELinux(Security-Enhanced Linux) 是美国国家安全局（NAS）对于强制访问控制的实现，是 Linux上最杰出的新安全子系统。NSA是在Linux社区的帮助下开发了一种访问控制体系，在这种访问控制体系的限制下，进程只能访问那些在他的任务中所需要文件。SELinux 默认安装在 Fedora 和 Red Hat Enterprise Linux 上，也可以作为其他发行版上容易安装的包得到。

最简单的办法，关闭selinux

方法1：用命令setenforce 0，无需重启。（setenforce的格式：setenforce [ Enforcing | Permissive | 1 | 0 ]）

方法2：在lilo或者grub的启动参数中增加：selinux=0,也可以关闭selinux。

使用getenforce查看当前selinux是否正在运行。

**不关闭selinux，就要设置selinux的ftp权限。**

1、使用getsebool -a | grep ftp查看ftp相关设置状态，我们要将allow\_ftpd\_anon\_write设为on。

2、使用setsebool -P 进行设置。例：setsebool -P allow\_ftpd\_anon\_write=on。

或使用togglesebool进行bool值取反，例如togglesebool　allow\_ftpd\_anon\_write。

3、修改selinux安全上下文，先介绍两个命令：

命令1、ls -Zps -Zid -Z# 分别可以看到文件,进程和用户的SELinux属性

命令2、#chcon 改变SELinux安全上下文

chcon -u [user] 对象 -r [role] -t [type] -R 递归 --reference 源文件 目标文件 # 复制安全上下文。

使用方法：

步骤1、ls -Zd /var/ftp/upload/ 通常会看到：

drwxr-xr-x ftp root system\_u:object\_r:public\_content\_t /var/ftp/upload/

步骤2、chcon -R -t public\_content\_rw\_t /var/ftp/upload/

步骤3、ls -Zd /var/ftp/upload/ 如果看到如下信息就OK了：

drwxr-xr-x ftp root system\_u:object\_r:public\_content\_rw\_t /var/ftp/upload/

最后还是重启下selinux和vsftpd吧，不重启其实也没关系。重新登录到ftp上，应该就能解决问题了。

还有啊，selinux的图形界面 可由system-config-selinux命令进入。

1. Vsftpd.conf参数说明

# 禁止匿名用户anonymous登录

anonymous\_enable=NO

# 允许本地用户登录

local\_enable=YES

local\_root=/data/wwwroot/

# 让登录的用户有写权限(上传，删除)

write\_enable=YES

# 默认umask

local\_umask=022

# 把传输记录的日志保存到/var/log/vsftpd.log

dual\_log\_enable=YES

dirmessage\_enable=YES

xferlog\_enable=YES

xferlog\_file=/var/log/vsftpd.log

xferlog\_std\_format=NO

# 允许ASCII模式上传

ascii\_upload\_enable=YES

# 允许ASCII模式下载

ascii\_download\_enable=YES

# 使用20号端口传输数据

connect\_from\_port\_20=YES

connect\_timeout=60

accept\_timeout=60

idle\_session\_timeout=300

max\_clients=2000

max\_per\_ip=0

# 欢迎标语

ftpd\_banner=Welcome to use my test ftp server.

#限制用户到指定目录

allow\_writeable\_chroot=YES

chroot\_local\_user=yes

#chroot\_list\_enable=YES

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

use\_localtime=YES

listen=YES

pam\_service\_name=vsftpd

anon\_max\_rate=50000

local\_max\_rate=200000

#主动模式开：需要防火墙放开20和21号端口

#port\_enable=yes

#被动模式开：需要防火墙放开21号端口和高位端口（）

#pasv\_enable=YES

#pasv\_min\_port=30000

#pasv\_max\_port=35000

#指定被动模式监听ip

#pasv\_address=172.16.1.131

1. 配置本地用户
2. 创建用户

登录Linux主机后，运行命令：”useradd ftpname -s /sbin/nologin “。该账户路径默认指向/home/ftpadmin目录；如果需要将用户指向其他目录，请运行命令：useradd ftpname-s /sbin/nologin –d /www(其他目录) 或者执行 adduser -d /data/ -g ftp -s /sbin/nologin ftpname

【修改用户指向目录运行命令：useradd -d /home/www ftpname】

设置ftpadmin用户密码，运行命令：”passwd ftpadmin” ; 输入两次密码，匹配成功后，就设置好了ftpadmin用户的密码了。

1. 创建chroot\_list文件，添加新创建的用户。
2. 修改用户家目录权限，/home/用户名 755，/home/用户名/pub 777
3. 修改vsftpd.conf文件

修改local\_umask=002

将匿名模式关掉，然后追加如下内容。

# 允许ASCII模式上传

ascii\_upload\_enable=YES

# # 允许ASCII模式下载

ascii\_download\_enable=YES

check\_shell=NO

seccomp\_sandbox=NO

connect\_timeout=60

accept\_timeout=60

idle\_session\_timeout=300

max\_clients=2000

max\_per\_ip=0

allow\_writeable\_chroot=YES

#是否将所有用户限制在主目录

chroot\_local\_user=YES

#是否启动限制用户的名单

chroot\_list\_enable=YES

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

#允许user\_list用户登录

userlist\_deny=NO

userlist\_enable=YES

local\_root=/home/用户名/pub

1. 修改selinux

setenforce 0 #暂时让SELinux进入Permissive模式

getsebool -a | grep ftpd 判断查看权限

setsebool -P tftp\_home\_dir 1

setsebool -P allow\_ftpd\_full\_access 1

setenforce 1 #进入Enforcing模式

1. 修改/etc/pam.d/vsftpd文件

注释掉auth required pam\_shells.so