# vsftp实例

在众多网络应用中，FTP（文件传输协议）有着非常重要的地位。它可以用于文件的存储和共享。与大多数Internet服务一样，FTP也是一个客户机/服务器系统。用户通过一个支持FTP协议的客户机程序，连接到主机上的FTP服务器程序。用户通过客户机程序向服务器程序发出命令，服务器程序执行用户发出的命令，并将执行结果返回给客户机。

现在我们通过一个例子来看看FTP是如何搭建起来的。在此，我们用著名的Vsftp来搭建FTP服务器。此FTP服务器主要用于公司内部文件的存储和共享。

## 一．需求

1. 某公司有5个大部门，分别为：人事行政部、财务部、技术部、市场部、生产部。

2. 各部门的文件夹只允许本部门员工有权访问；各部门之间交流性质的文件放到公用文件夹中。

3. 每个部门都有一个管理本部门文件夹的管理员账号和一个只能上传、下载和查看文件的普通用户权限的账号。

4. 公用文件夹中分为存放工具的文件夹和存放文件的文件夹。

5. 用户只能对自己的家目录文件夹及其下面的目录文件有操作权限，不允许切换到上级目录，不允许匿名用户访问。

## 二．规划

根据公司需求情况，现做出如下规划：

**1.** 在系统分区时单独分一个Company的区，在该区下有以下几个文件夹：HR、CaiWu、JiShu、ShiChang、ShengChan和Share。在Share下又有以下几个文件夹：HR、CaiWu、JiShu、ShiChang、ShengChan和Tools。

**2.** 各部门对应的文件夹由各部门自己管理，Tools文件夹由管理员维护。

**3.** HR管理员账号：hradmin；普通用户账号：hruser。

   CaiWu管理员账号：caiwuadmin；普通用户账号：caiwuuser。

   JiShu管理员账号：jishuadmin；普通用户账号：jishuuser。

   ShiChang管理员账号：shichangadmin；普通用户账号：shichanguser。

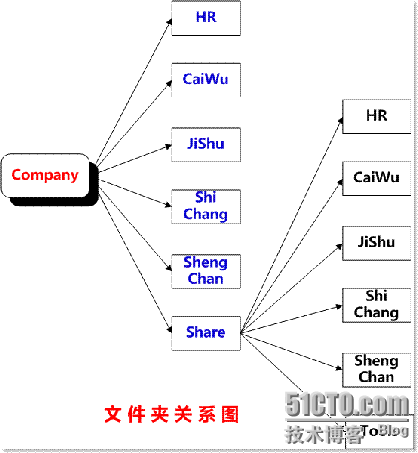
   ShengChan管理员账号：shengchanadmin；普通用户账号：shengchanuser。

   Tools管理员账号：admin。

**4.** 各部门管理员账号有完全控制本部门文件夹的权限以及下载Tools文件夹中工具的权限，普通用户账号只有上传、下载和查看本部门文件夹的权限以及下载Tools文件夹中工具的权限。

**5.** 因为此FTP服务器主要用于公司内部使用，因此，FTP使用主动工作模式，在FTP服务器上将其他不需要用到的端口屏蔽掉，增加服务器安全。

文件夹之间的关系请见下图：

[](http://img1.51cto.com/attachment/200810/27/363003_1225098834jxum.gif)

## 三．Vsftp RPM安装和启动

在系统中使用rpm –qa |grep vsftp来查看系统有没有安装该软件，如果没有安装则挂载系统盘，找到vsftp软件包，使用rpm –ivh vsftp\*即可安装。

使用RPM包安装后，vsftp的配置文件默认在/etc/vsftpd/下。

使用service vsftpd start启动vsftp。Vsftp默认允许匿名用户访问。

使用chkconfig --level 35 vsftpd .，可以使vsftp随系统一起启动。

在/etc/sysconfig/iptables中将20和21端口开放，然后用service iptables restart重启iptables服务。

在/etc/selinux/config中将“SELINUX”项关闭，SELINUX=disabled。

## 四．新建用户

使用useradd命令新建用户，使用passwd命令添加密码。

useradd hradmin -r -m -d /Company/ -s /sbin/nologin

useradd hruser -r -m -g hradmin -d /Company/ -s /sbin/nologin

useradd caiwuadmin -r -m -d /Company/ -s /sbin/nologin

useradd caiwuuser -r -m -g caiwuadmin -d /Company/ -s /sbin/nologin

useradd jishuadmin -r -m -d /Company/ -s /sbin/nologin

useradd jishuuser -r -m -g jishuadmin -d /Company/ -s /sbin/nologin

useradd shichangadmin -r -m -d /Company/ -s /sbin/nologin

useradd shichanguser -r -m -g shichangadmin -d /Company/ -s /sbin/nologin

useradd shengchanadmin -r -m -d /Company/ -s /sbin/nologin

useradd shengchanuser -r -m -g shangchanadmin -d /Company/ -s /sbin/nologin

useradd admin -r -m -g root -d /Company/Share/Tools

## 五．新建目录

在/Company中添加各部门的私密文件夹以及一个用于放置共享东西的共享文件夹。

#cd /Company/

#mkdir HR CaiWu JiShu ShiChang ShengChan Share

在/Company下的共享文件夹中，添加各部门的文件夹以及一个放置共享工具的文件夹，这些部门文件夹用于放置需要共享的文件。

#cd /Company/Share/

#mkdir HR CaiWu JiShu ShiChang ShengChan Tools

## 六．修改目录属性

修改/Company中的各部门文件夹的文件权限为1770（实现效果：本部门管理员和普通用户可以进入，非本部门用户禁止进入；本部门管理员上传的文件，本部门的普通用户只能下载和查看，不能修改；本部门普通用户上传的文件，本部门的管理员可以查看，下载，删除，重命名，但是不能修改里面的内容；如果管理员想要修改普通用户上传的文件，可以先下载该文件，然后在FTP上删除该文件，在本机编辑好后再将该文件上传），属主和组为各部门的管理员及管理员组。

cd /Company/

chmod -R 1770 HR CaiWu JiShu ShiChang ShengChan

chown -R hradmin.hradmin HR/

chown -R caiwuadmin.caiwuadmin CaiWu/

chown -R jishuadmin.jishuadmin JiShu/

chown -R shichangadmin.shichangadmin ShiChang/

chown -R shengchanadmin.shengchanadmin ShengChan/

chmod -R 1775 Share/

chown admin.root Share/

cd /Company/Share

chown -R hradmin.hradmin HR/

chown -R caiwuadmin.caiwuadmin CaiWu/

chown -R jishuadmin.jishuadmin JiShu/

chown -R shichangadmin.shichangadmin ShiChang/

chown -R shengchanadmin.shengchanadmin ShengChan/

chown -R admin.root Tools/

## 七．配置vsftp

Vsftp的配置文件在/etc/vsftpd/下。文件名为vsftpd.conf。

#cd /etc/vsftpd/

#cp vsftpd.conf vsftpd.conf.bak

#vi vsftpd.conf

write\_enable=YES

#允许登入者有写权限

anonymous\_enable=NO

#禁止匿名用户访问

local\_enable=YES

#允许本地用户访问

local\_umask=022

#本地用户新增档案时的umask值

file\_open\_mode=0755

#本地用户上传档案后的档案权限

ftpd\_banner=Welcome to BOB's FTP server.

#定义欢迎话语的字符串

xferlog\_enable=YES

#启用上传/下载日志记录

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

#日志文件所在的路径及名称

xferlog\_std\_format=YES

#将日志文件写成xferlog的标准格式

ascii\_upload\_enable=YES

#启用ASCII 模式上传数据

ascii\_download\_enable=YES

#启用ASCII 模式下载数据

chroot\_list\_enable=YES

#在chroot\_list中列出的用户不允许切换到家目录的上级目录

chroot\_local\_user=NO

#

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

#

userlist\_enable=YES

#在user\_list中列出的用户不能访问FTP服务器，未列出的可以访问

userlist\_deny=YES

#

userlist\_file=/etc/vsftpd/user\_list

#

tcp\_wrappers=NO

#不使用tcp wrapper来控制主机访问

setproctitle\_enable=YES

#每个与FTP服务器的连接，都以不同的进程表现出来

listen=YES

#FTP服务器以standalone模式运行

port\_enable=YES

#FTP服务器启用PORT模式

pasv\_enable=NO

#禁用FTP服务器的PASV模式

listen\_port=21

#FTP服务器监听21端口

connect\_from\_port\_20=YES

#指定FTP服务器使用20端口进行数据传输

ftp\_data\_port=20

#FTP服务器数据传输端口为20

pam\_service\_name=vsftpd

#使用PAM模块控制，vsftpd文件在/etc/pam.d目录下

idle\_session\_timeout=600

#600秒钟不对FTP服务器进行任何操作，则断开该FTP连接

data\_connection\_timeout=120

#建立FTP数据连接的超时时间为120秒

max\_clients=0

#不限制用户的连接数量

max\_per\_ip=3

#每个IP只能与FTP服务器同时建立3个连接

local\_max\_rate=512000

#本地用户使用的最大传输速度

编辑chroot\_list，一个用户一行。此文件中列出的用户不允许访问其家目录的上级目录。

#vi /etc/vsftpd/chroot\_list

hradmin

hruser

caiwuadmin

caiwuuser

jishuadmin

jishuuesr

shichangadmin

shichanguser

shengchanadmin

shengchanuser

编辑user\_list，一个用户一行。在此文件中列出的用户不能访问FTP服务器，未列出的可以访问。

#vi /etc/vsftpd/user\_list

## 八．测试

使用flashFXP软件作为FTP客户端。