

# Linux和windows server 2008r2 FTP服务器的创建

## 一、Linux

### 1、安装VSFTPD服务包

通过虚拟光驱加载iso镜像：

```
[root@localhost ~]# mount -t iso9660 -o loop /home/tate/Documents/rhel-server-6.3-i386-dvd.iso /mnt/usb
mount: according to mtab /home/tate/Documents/rhel-server-6.3-i386-dvd.iso is already mounted on /mnt/usb as loop
[root@localhost ~]# ls /mnt/usb
EULA                               Packages                           RELEASE-NOTES-fr-FR.html          RELEASE-NOTES-ml-IN.html          RELEASE-NOTES-ta-IN.html          RPM-GPG-KEY-redhat-release
GPL                                 README                             RELEASE-NOTES-gu-IN.html          RELEASE-NOTES-mr-IN.html          RELEASE-NOTES-te-IN.html          Server
HighAvailability                   RELEASE-NOTES-as-IN.html          RELEASE-NOTES-hi-IN.html          RELEASE-NOTES-or-IN.html          RELEASE-NOTES-zh-CN.html          TRANS.TBL
images                             RELEASE-NOTES-bn-IN.html          RELEASE-NOTES-it-IT.html          RELEASE-NOTES-pa-IN.html          RELEASE-NOTES-zh-TW.html
isolinux                           RELEASE-NOTES-de-DE.html          RELEASE-NOTES-ja-JP.html          RELEASE-NOTES-pt-BR.html          Repodata
LoadBalancer                       RELEASE-NOTES-en-US.html          RELEASE-NOTES-ko-KR.html          RELEASE-NOTES-ru-RU.html          ResilientStorage
media.repo                         RELEASE-NOTES-es-ES.html          RELEASE-NOTES-si-LK.html          RELEASE-NOTES-si-LK.html          RPM-GPG-KEY-redhat-beta
```

寻找vsftpd的服务包并安装并进行确认，总计一个：

```
[root@localhost ~]# cd /mnt/usb
[root@localhost usb]# find . -name "vsftpd*"
./Packages/vsftpd-2.2.2-11.el6.i686.rpm
[root@localhost usb]# cd Packages
[root@localhost Packages]# rpm -ivh vsftpd-2.2.2-11.el6.i686.rpm -f --nodeps
warning: vsftpd-2.2.2-11.el6.i686.rpm: Header V3 RSA/SHA256 Signature, key ID fd431d51: NOKEY
Preparing...##### [100%]
 1:vsftpd##### [100%]
[root@localhost Packages]# cd
[root@localhost ~]# rpm -qa vsftpd*
vsftpd-2.2.2-11.el6.i686
```

### 2、配置VSFTPD.CONF文件

```
# 是否允许匿名登录FTP服务器，默认设置为YES允许
# 用户可使用用户名ftp或anonymous进行ftp登录，口令为用户的E-mail地址。
# 如不允许匿名访问则设置为NO
anonymous_enable=YES
# 是否允许本地用户(即linux系统中的用户帐号)登录FTP服务器，默认设置为YES允许
# 本地用户登录后会进入用户主目录，而匿名用户登录后进入匿名用户的下载目录/var/ftp/pub
# 若只允许匿名用户访问，前面加上#注释掉即可阻止本地用户访问FTP服务器
local_enable=YES
# 是否允许本地用户对FTP服务器文件具有写权限，默认设置为YES允许
write_enable=YES
# 掩码，本地用户默认掩码为077
# 你可以设置本地用户的文件掩码为缺省022，也可根据个人喜好将其设置为其他值
#local_umask=022
# 是否允许匿名用户上传文件，须将全局的write_enable=YES。默认为YES
#anon_upload_enable=YES
# 是否允许匿名用户创建新文件夹
#anon_mkdir_write_enable=YES
# 是否激活目录欢迎信息功能
# 当用户用CMD模式首次访问服务器上某个目录时，FTP服务器将显示欢迎信息
# 默认情况下，欢迎信息是通过该目录下的.message文件获得的
# 此文件保存自定义的欢迎信息，由用户自己建立
#dirmessage_enable=YES
# 是否让系统自动维护上传和下载的日志文件
# 默认情况该日志文件为/var/log/vsftpd.log,也可以通过下面的xferlog_file选项对其进行设定
# 默认值为NO
```

```
xferlog_enable=YES
# Make sure PORT transfer connections originate from port 20 (ftp-data).
# 是否设定FTP服务器将启用FTP数据端口的连接请求
# ftp-data数据传输，21为连接控制端口
connect_from_port_20=YES
# 设定是否允许改变上传文件的属主，与下面一个设定项配合使用
# 注意，不推荐使用root用户上传文件
#chown_uploads=YES
# 设置想要改变的上传文件的属主，如果需要，则输入一个系统用户名
# 可以把上传的文件都改成root属主。whoever: 任何人
#chown_username=whoever
# 设定系统维护记录FTP服务器上传和下载情况的日志文件
# /var/log/vsftpd.log是默认的，也可以另设其它
#xferlog_file=/var/log/vsftpd.log
# 是否以标准xferlog的格式书写传输日志文件
# 默认为/var/log/xferlog，也可以通过xferlog_file选项对其进行设定
# 默认值为NO
#xferlog_std_format=YES
# 以下是附加配置，添加相应的选项将启用相应的设置
# 是否生成两个相似的日志文件
# 默认在/var/log/xferlog和/var/log/vsftpd.log目录下
# 前者是wu_ftp类型的传输日志，可以利用标准日志工具对其进行分析；后者是vsftpd类型的日志
#dual_log_enable
# 是否将原本输出到/var/log/vsftpd.log中的日志，输出到系统日志
#syslog_enable
# 设置数据传输中断间隔时间，此语句表示空闲的用户会话中断时间为600秒
# 即当数据传输结束后，用户连接FTP服务器的时间不应超过600秒。可以根据实际情况对该值进行修改
#idle_session_timeout=600
# 设置数据连接超时时间，该语句表示数据连接超时时间为120秒，可根据实际情况对其修改
#data_connection_timeout=120
# 运行vsftpd需要的非特权系统用户，缺省是nobody
#nopriv_user=ftpsecure
# 是否识别异步ABOR请求。
# 如果FTP client会下达“async ABOR”这个指令时，这个设定才需要启用
# 而一般此设定并不安全，所以通常将其取消
#async_abor_enable=YES
# 是否以ASCII方式传输数据。默认情况下，服务器会忽略ASCII方式的请求。
# 启用此选项将允许服务器以ASCII方式传输数据
# 不过，这样可能会导致由"SIZE /big/file"方式引起的DoS攻击
#ascii_upload_enable=YES
#ascii_download_enable=YES
# 登录FTP服务器时显示的欢迎信息
# 如有需要，可在更改目录欢迎信息的目录下创建名为.message的文件，并写入欢迎信息保存后
#ftpd_banner>Welcome to blah FTP service.
# 黑名单设置。如果很讨厌某些email address，就可以使用此设定来取消他的登录权限
# 可以将某些特殊的email address抵挡住。
#deny_email_enable=YES
```

```
# 当上面的deny_email_enable=YES时，可以利用这个设定项来规定哪些邮件地址不可登录vsftpd服务器
# 此文件需用户自己创建，一行一个email address即可
#banned_email_file=/etc/vsftpd/banned_emails
# 用户登录FTP服务器后是否具有访问自己目录以外的其他文件的权限
# 设置为YES时，用户被锁定在自己的home目录中，vsftpd将在下面chroot_list_file选项值的位置寻找chroot_list文件
# 必须与下面的设置项配合
#chroot_list_enable=YES
# 被列入此文件的用户，在登录后将不能切换到自己目录以外的其他目录
# 从而有利于FTP服务器的安全管理和隐私保护。此文件需自己建立
#chroot_list_file=/etc/vsftpd/chroot_list
# 是否允许递归查询。默认为关闭，以防止远程用户造成过量的I/O
#ls_recurse_enable=YES
# 是否允许监听。
# 如果设置为YES，则vsftpd将以独立模式运行，由vsftpd自己监听和处理IPv4端口的连接请求
listen=YES
# 设定是否支持IPV6。如要同时监听IPv4和IPv6端口，
# 则必须运行两套vsftpd，采用两套配置文件
# 同时确保其中有一个监听选项是被注释掉的
#listen_ipv6=YES
# 设置PAM外挂模块提供的认证服务所使用的配置文件名，即/etc/pam.d/vsftpd文件
#此文件中file=/etc/vsftpd/ftpusers字段，说明了PAM模块能抵挡的帐号内容来自文件/etc/vsftpd/ftpusers中
#pam_service_name=vsftpd
# 是否允许ftpusers文件中的用户登录FTP服务器，默认为NO
# 若此项设为YES，则user_list文件中的用户允许登录FTP服务器
# 而如果同时设置了userlist_deny=YES，则user_list文件中的用户将不允许登录FTP服务器，甚至连输入密码提示信息都没有
#userlist_enable=YES/NO
# 设置是否阻挠user_list文件中的用户登录FTP服务器，默认为YES
#userlist_deny=YES/NO
# 是否使用tcp_wrappers作为主机访问控制方式。
# tcp_wrappers可以实现linux系统中网络服务的基于主机地址的访问控制
# 在/etc目录中的hosts.allow和hosts.deny两个文件用于设置tcp_wrappers的访问控制
# 前者设置允许访问记录，后者设置拒绝访问记录。
# 如想限制某些主机对FTP服务器192.168.57.2的匿名访问，编辑/etc/hosts.allow文件，如在下面增加两行命令：
# vsftpd:192.168.57.1:DENY 和vsftpd:192.168.57.9:DENY
# 表明限制IP为192.168.57.1/192.168.57.9主机访问IP为192.168.57.2的FTP服务器
# 此时FTP服务器虽可以PING通，但无法连接
tcp_wrappers=YES
```

### 3、访问FTP服务器

登录FTP的几种方法：

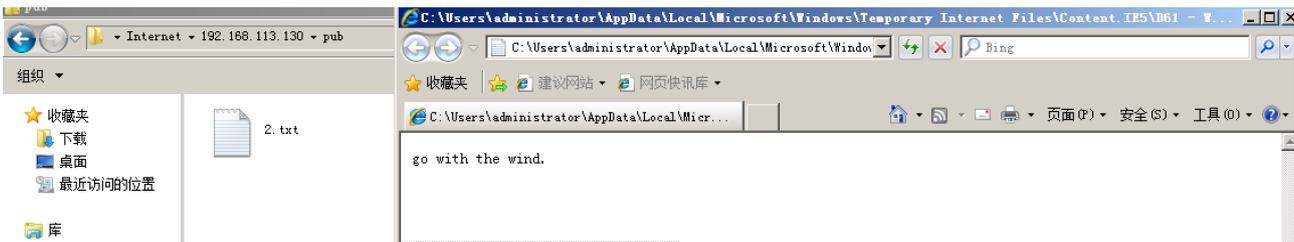
linux系统IP地址为192.168.113.130.

- 1、通过资源管理器键入ftp://192.168.113.130;
- 2、通过浏览器键入ftp://192.168.113.130;
- 3、通过DOS命令键入ftp://192.168.113.130。

在用匿名用户登录FTP之前，打开文件默认路径位于Linux中/var/ftp/pub中，在pub中创建一个文档2.txt，在内容输入go with the wind。

```
[root@localhost ~]# cd /var
[root@localhost var]# ls
account  crash  empty  games  lib  lock  mail  opt  run  tmp  yp
cache   db     ftp    gdm    local  log   nis   preserve  spool  www
[root@localhost var]# cd /ftp
bash: cd: /ftp: No such file or directory
[root@localhost var]# cd ftp
[root@localhost ftp]# ls
pub
[root@localhost ftp]# cd pub
[root@localhost pub]# ls
[root@localhost pub]# ls -al
total 8
drwxr-xr-x. 2 ftp  root    4096 Mar  2  2012 .
drwxr-xr-x. 3 ftp  user  ftp_user 4096 Dec 15 12:32 ..
[root@localhost pub]# touch 2.txt
[root@localhost pub]# vi 2.txt
```

匿名用户登录FTP服务器后，看到的内容如下所示：



疑问：禁止匿名用户登录后，采用本地新建用户ftp\_user账户登录，则会弹出窗口显示输入账户和密码，目前遇到一个问题，即输入后总显示500 OOPS报错。

解决：修改vstftpd.conf文件禁止匿名用户登录，新建用户try1、try2、try3并添加至组try，在try文件夹下创建一个新的520.txt文件并输入“Happy New Year!!!”字样，随后制定各自的家目录和属组，为新用户设置密码，依次设置目录属主为用户try1，设置目录属组为try，最后设置各个用户的访问权限，分别为7（可读写执行）、5（可读执行）、5，如下图所示。

```

[root@localhost Desktop]# ls /home
love snow test
[root@localhost Desktop]# mkdir -p /home/try
[root@localhost Desktop]# ls /home
love snow test try
[root@localhost Desktop]# groupadd try
[root@localhost Desktop]# useradd -g try -d /home/try try1
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
[root@localhost Desktop]# useradd -g try -d /home/try try2
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
[root@localhost Desktop]# useradd -g try -d /home/try try3
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
[root@localhost Desktop]# passwd try1
Changing password for user try1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost Desktop]# passwd try2
Changing password for user try2.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost Desktop]# passwd try3
Changing password for user try3.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost Desktop]# chown try1 /home/try
[root@localhost Desktop]# chown .try /home/try
[root@localhost Desktop]# chmod 750 /home/try

```

查看FTP状态，用语句 `sestatus -b | grep ftp`，可见各列状态显示为off，开启`ftp_home_dir`之后，对应状态变更为on，重启FTP服务器，

```

[root@localhost vsftpd]# sestatus -b | grep ftp
allow_ftpd_anon_write          off
allow_ftpd_full_access        off
allow_ftpd_use_cifs            off
allow_ftpd_use_nfs             off
ftp_home_dir                   off
ftpd_connect_db                off
ftpd_use_passive_mode          off
httpd_enable_ftp_server        off
tftp_anon_write                 off
[root@localhost vsftpd]# setsebool -P ftpd_disable_trans on
libsemanage.dbase_llist_set: record not found in the database (No such file or d
irectory).
libsemanage.dbase_llist_set: could not set record value (No such file or directo
ry).
Could not change boolean ftpd_disable_trans
Could not change policy booleans
[root@localhost vsftpd]# setsebool -P ftp_home_dir on
[root@localhost vsftpd]# sestatus -b | grep ftp
allow_ftpd_anon_write          off
allow_ftpd_full_access        off
allow_ftpd_use_cifs            off
allow_ftpd_use_nfs             off
ftp_home_dir                   on
ftpd_connect_db                off
ftpd_use_passive_mode          off
httpd_enable_ftp_server        off
tftp_anon_write                 off
[root@localhost vsftpd]# service vsftpd restart
Shutting down vsftpd:          [ OK ]
Starting vsftpd for vsftpd:    [ OK ]

```

访问`ftp://192.168.113.130`，输入try1账号和密码后登录，即会访问到520.txt。



## 二、windows server 2008r2

### 1、添加角色WEB服务器（IIS）

添加对应角色，勾选管理工具、IIS6管理兼容性以及FTP服务器几个选项。

安装完毕后打开信息服务（IIS）管理器，在网站右键选择添加FTP站点，输入如下信息：



### 2、匿名访问FTP服务器

事先在C盘创建ftp\_user文件夹，即为FTP站点指向的路径地址，里面创建两个子文件夹ftp\_user1和ftp\_user2，分别放置1.txt和2.txt并输入随意文字，选择匿名并设置所有用户都可以访问，则在浏览器端访问FTP服务器后，会看到：



打开目录ftp\_user2，显示出内容：

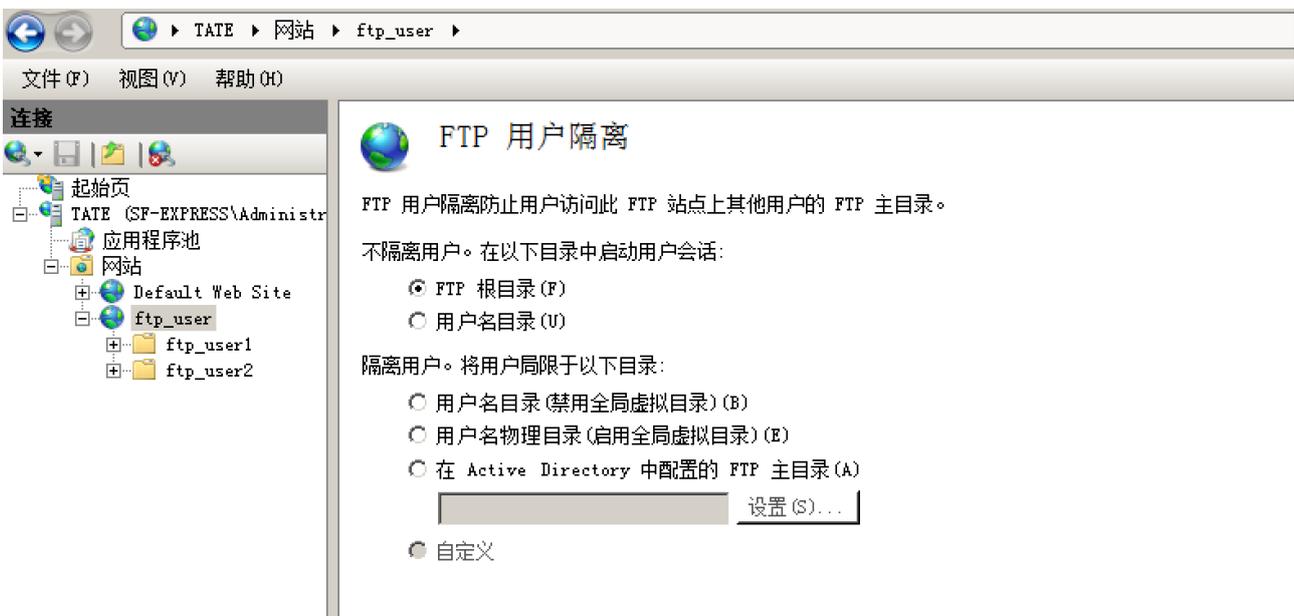


### 3、实现本地用户访问

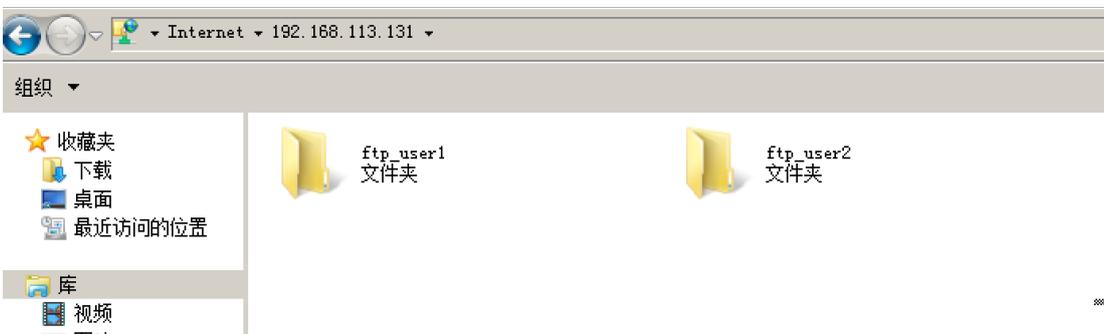
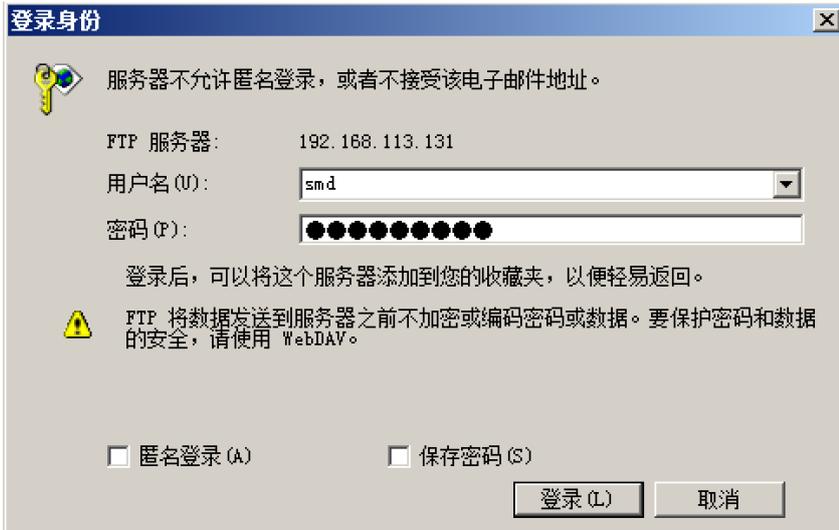
首先创建FTP站点ftp\_user，将身份验证和授权信息中匿名勾去掉，禁止匿名登陆。



之前在IT组织单位里建立过用户余孟都和王亮，在用户隔离选择访问根目录，使用该用户登录FTP服务器，可以访问到ftp\_user1和ftp\_user2两个文件夹，

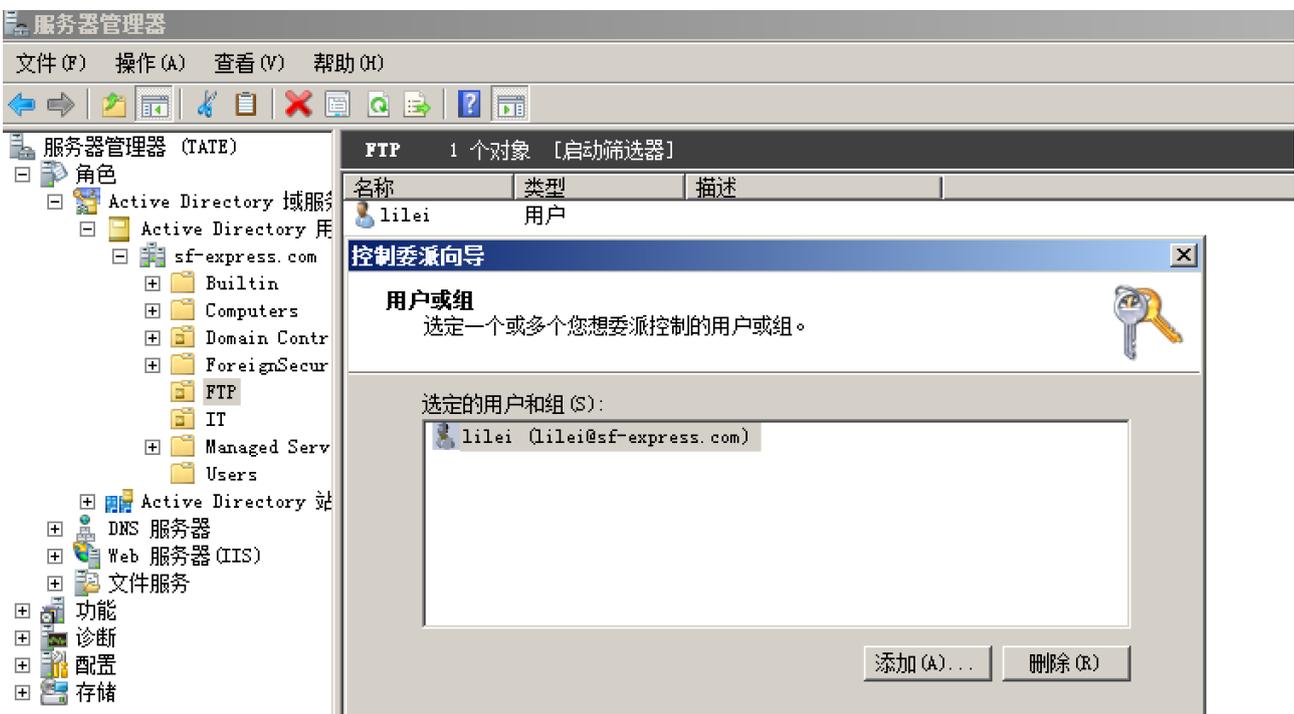


使用用户余孟都登陆，用户名为smd，密码重置为smd920716，

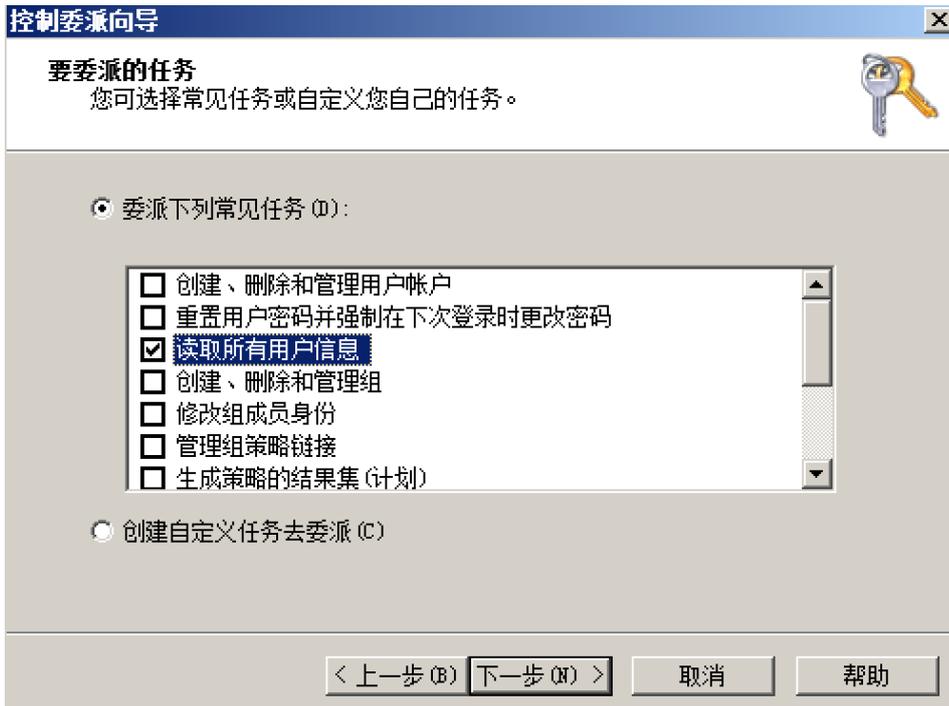


#### 4、访问目录的限制

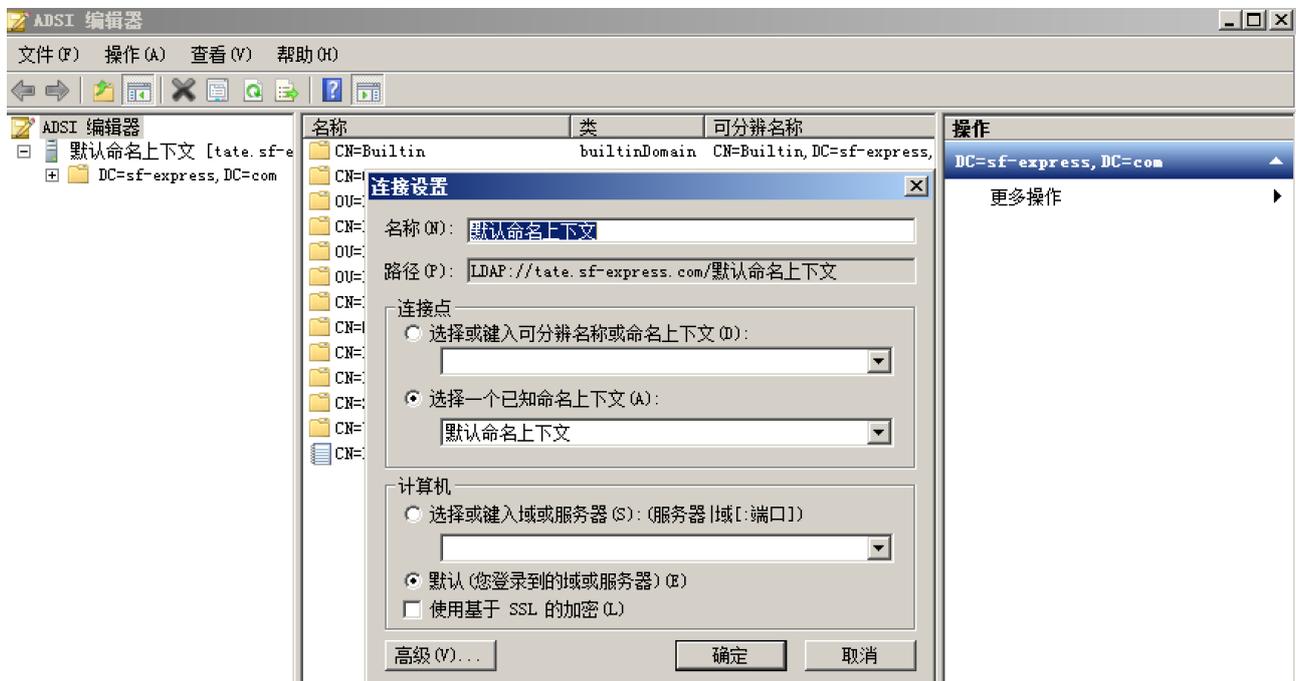
在服务管理器新建组织单位FTP并创建用户lilei，右键FTP实现控制委派，



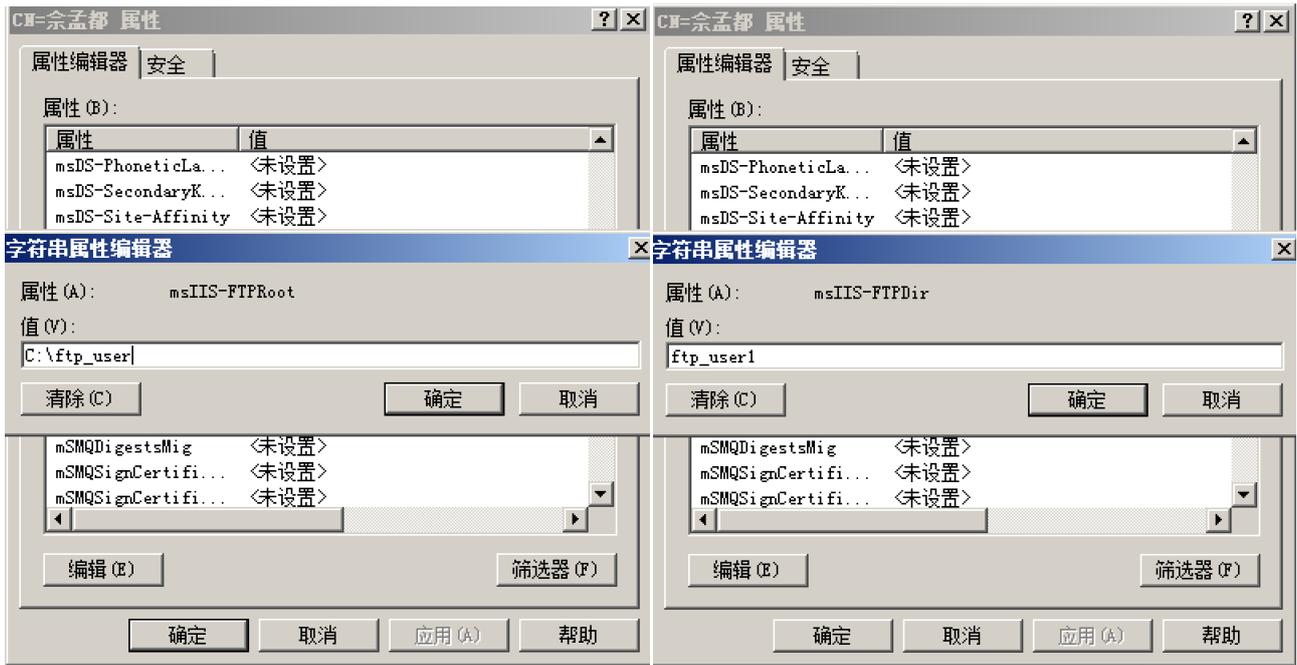
选择委派的任务为“读取所有用户信息”，委派即可完成。



从管理工具中打开ADSI编辑器，连接到默认设置，



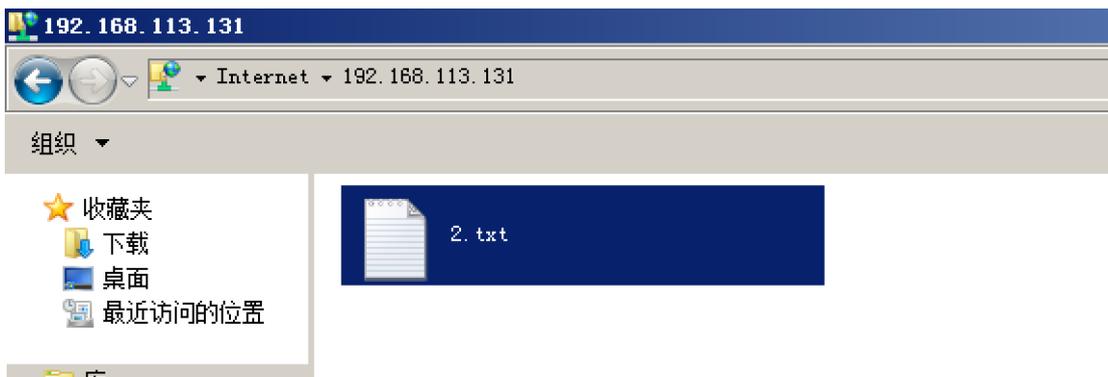
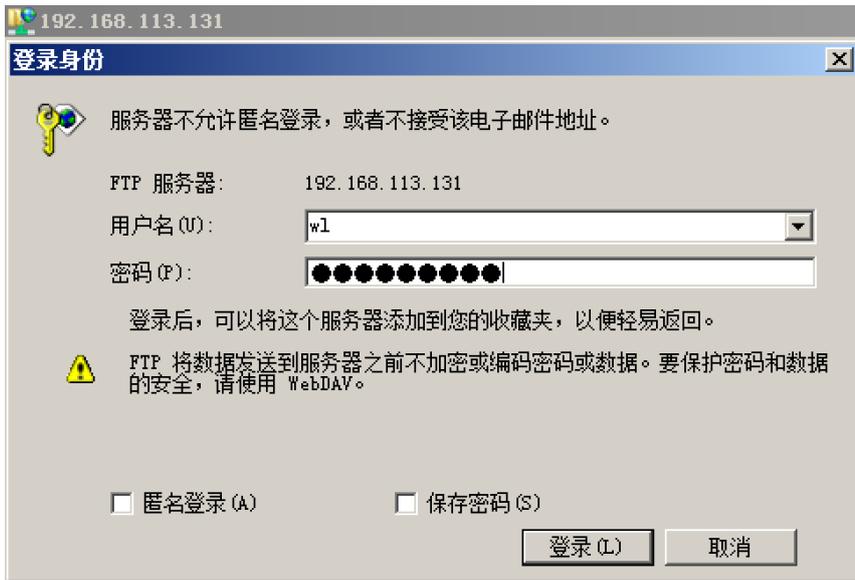
在用户余孟都右键属性，修改属性编辑器，找到msIIS-FTPRoot修改值为FTP站点指向的路径，msIIS-FTPDir为访问FTP的路径文件夹，使得用户余孟都只能访问ftp\_user1，用户王亮只能访问ftp\_user2，



在FTP用户隔离选择局限目录“在Active Directory中配置的FTP主目录”，并使用用户lilei设置凭据，



重启FTP服务器，继续登陆，使用用户王亮登陆后，会发现访问目录直接转至ftp\_user2，且无法访问其他同级目录。



疑问：怎么实现以上隔离后有用户可以访问全部，或者访问其中两个及两个以上？

解决：在根目录ftp\_user下再创建一个子文件夹ftp\_user0，然后将需要访问的文件夹ftp\_user1-3放到该文件夹下，修改ADSI编辑器中对应的属性值即可，起到一个桥梁作用。

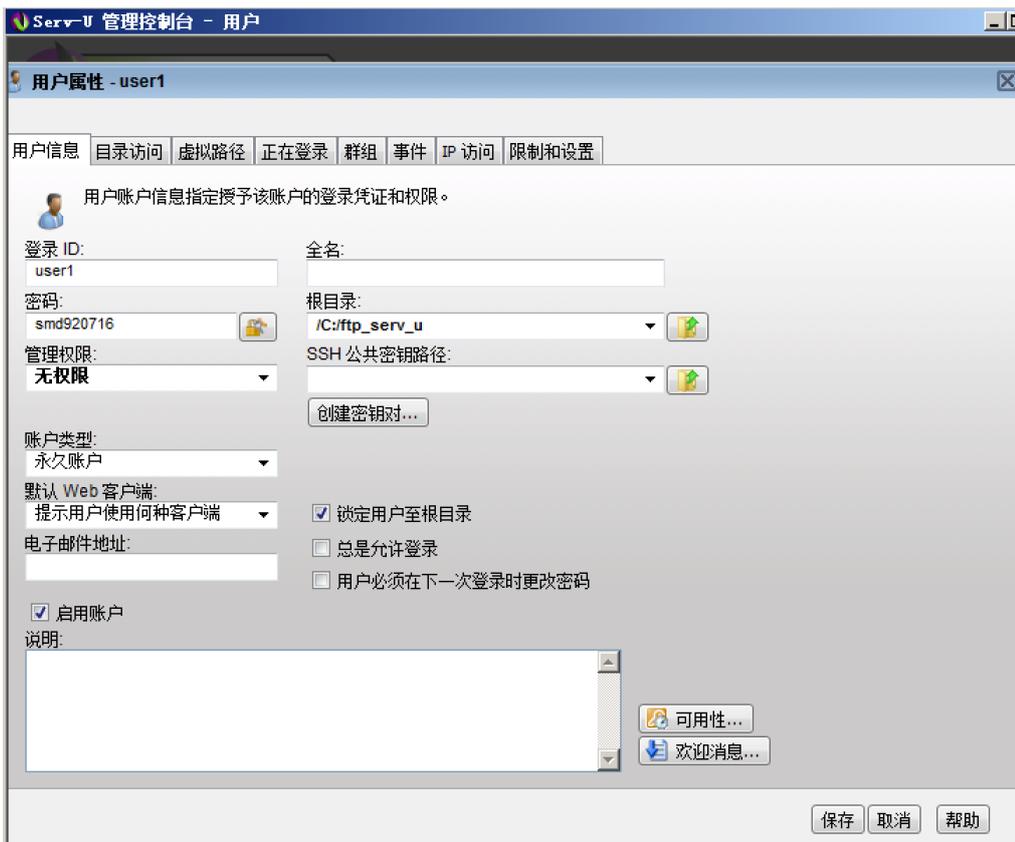


## 5、SERV-U

Serv-U是一款服务器架设软件,用于架设FTP服务器。首先安装Serv-U, 选择域sf-express,创建访问路径文件夹为ftp\_serv\_u, 且其下另建3个子文件夹ftp\_serv\_u (1-3), 管理控制台界面如下:

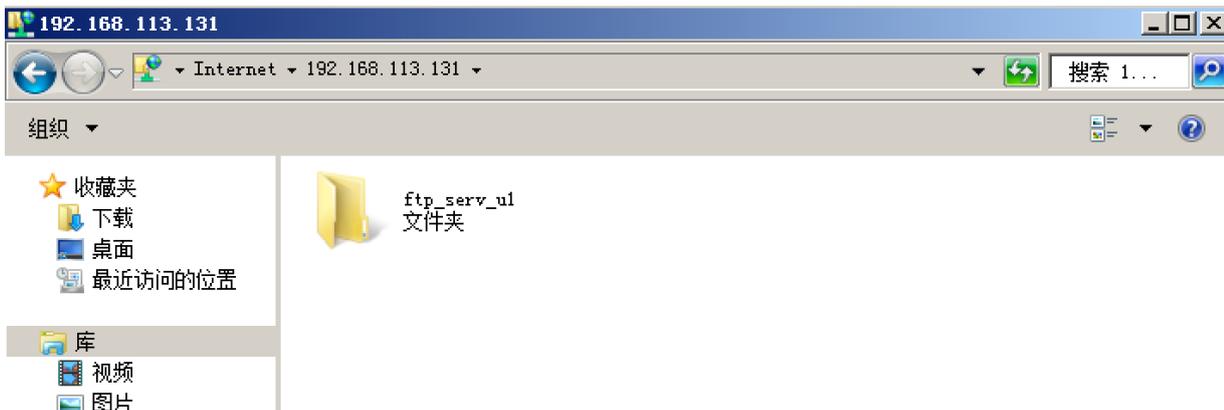
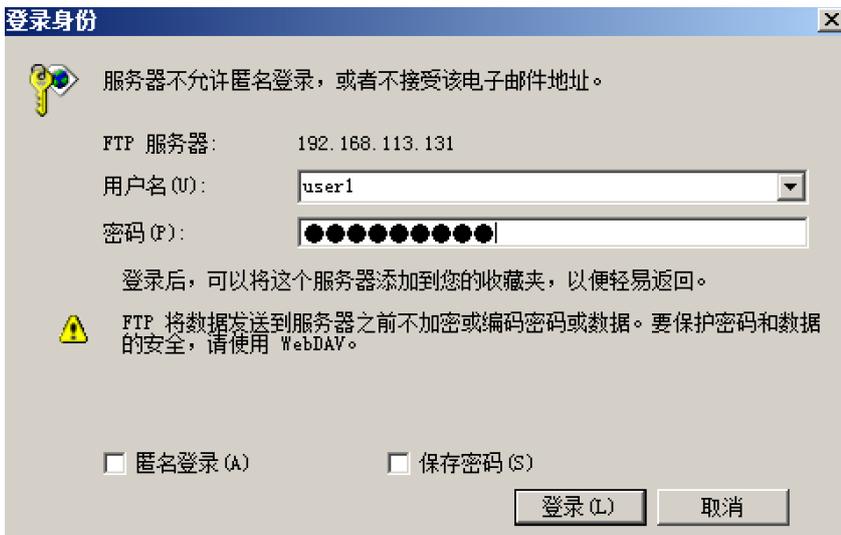


创建用户user1, 填写信息如下, 访问路径限定到子文件夹ftp\_serv\_u1, 访问规则可自定义,





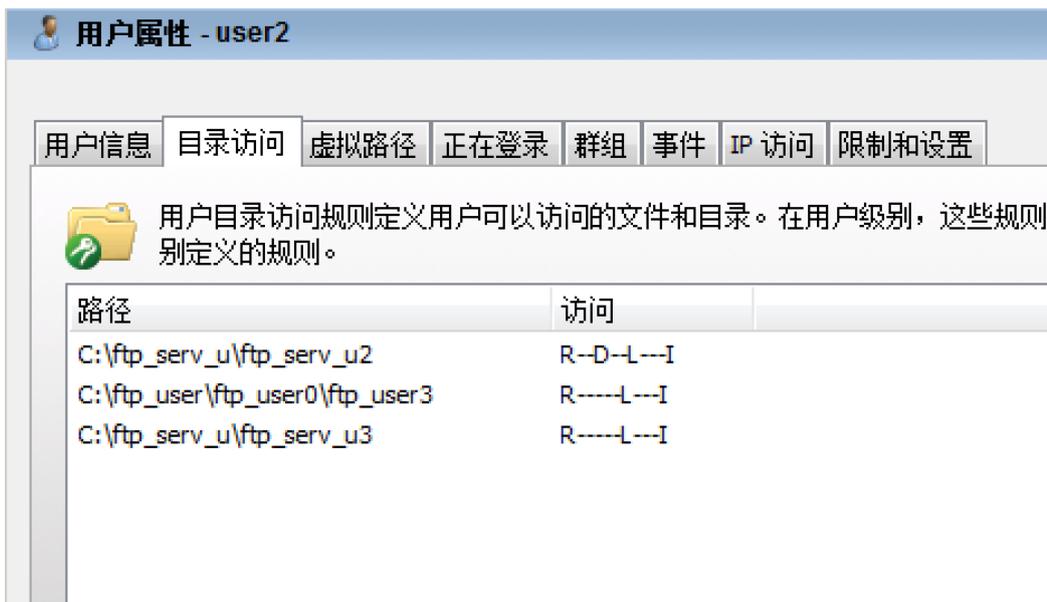
使用该账户访问FTP服务器，可以直接转到路径文件夹下，且限定在该文件夹之内，如果添加多个路径，则会访问到相对应的文件夹下，不同用户可以设置不同的访问路径，



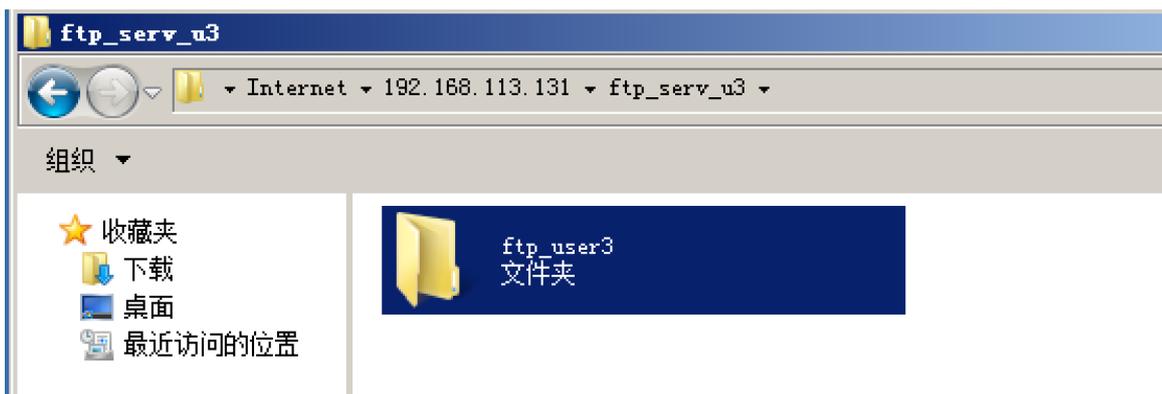
根据公司业务的需求，可能用户会需求访问根目录之外的目录，这样就需要使用serv\_u虚拟目录功能，虚拟目录功能可以设置不同域、群组、用户访问非文件服务器根目录下的文件及文件夹。创建用户user2，访问路径限制为ftp\_serv\_u（2、3），现需要访问根目录之外的某个文件夹内容，比如ftp\_user下的ftp\_user3，编辑用户user2，打开虚拟路径设置，操作如下：



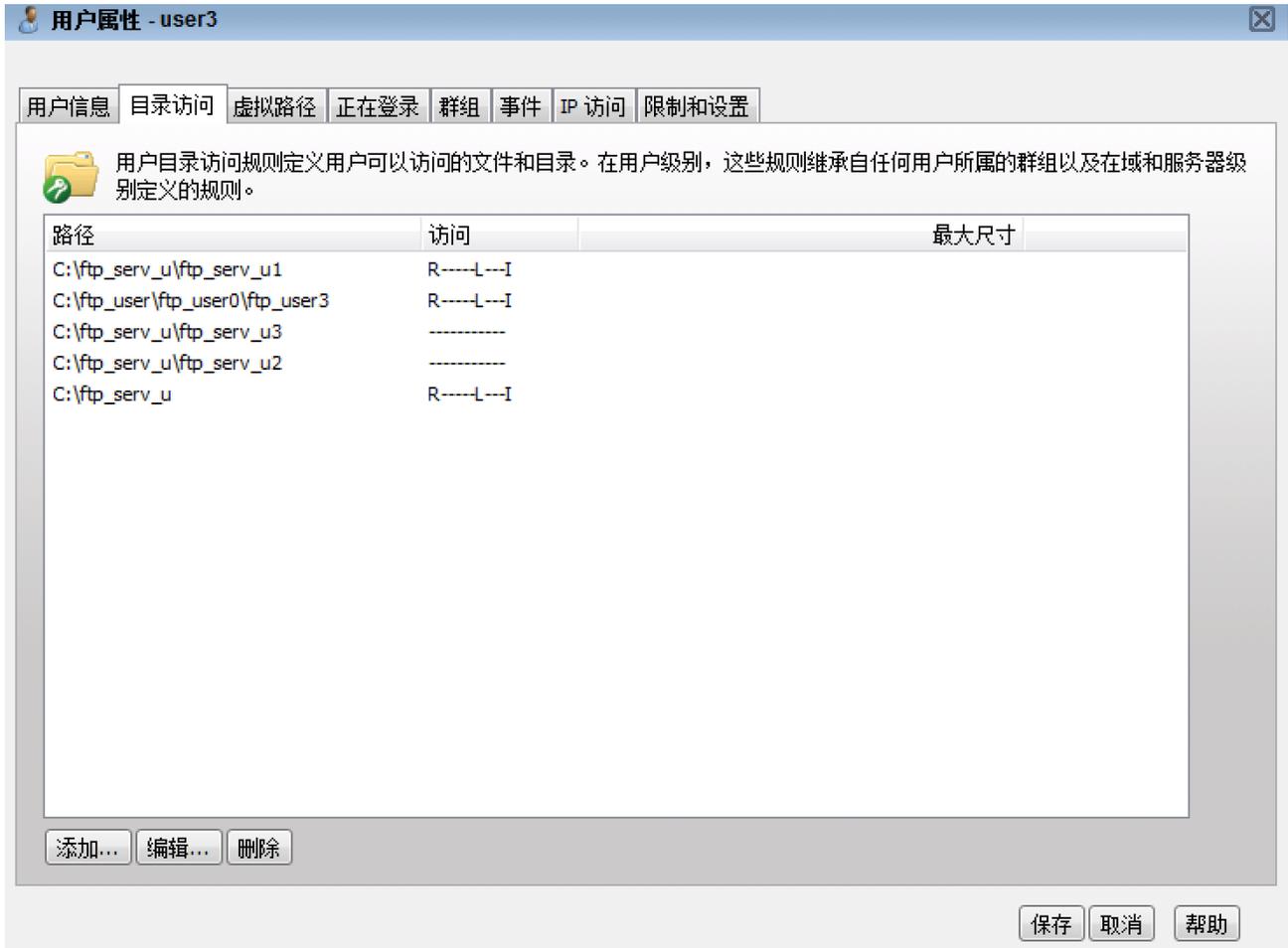
%HOME%代表的是根目录，即C:\ftp\_serv\_u，然后在访问目录中添加物理路径，



访问FTP服务器，用user2账号登录后，即可访问到ftp\_user3。



访问权限的控制：创建用户user3，实现访问根目录所有文件夹和上述根目录外文件夹 ftp\_user3，但是ftp\_serv\_u（2-3）无访问权限，可将访问目录直接限制在根目录下，对ftp\_serv\_u（2-3）文件夹访问权限进行控制，



通过用户user3访问FTP服务器，可访问的文件夹如下：

