项目 8 配置与管理 Samba 服务器-实训任务指导书（8-1）

任务 1：配置与管理 Samba 服务器

项目背景：

学校现有三个系，要创建一台 samba 服务器，包括如下五个目录：

公共目录/share/docx
公共临时空间 /temp
计算机系/computer
英语系/English
会计系/account

员工信息情况：

主管：院长 master
计算机系：系主任 wang_128，教师 zhangbin，教师 lihua。
英语系：系主任 liyouling，教师 zhanglili，教师 wangli。
会计系：系主任 dongwulun，教师 zhangshang，教师 lili。

任务要求：

1.建立公共共享目录/share/docx，允许所有老师访问，权限为只读。
2.公共临时空间：让所有用户可以读取、写入、删除，只有 master 一个用户不可以写（需要用到 setfacl 权限设置）。
3.为三个系分别建立单独目录，只有院长和相应的系的老师访问，自己系部的老师对自己系的目录有写权限。其他用户不可访问（包括列表、读、写）,无法在网络邻居查看到非本系共享目录。
4.院长可以看到并访问三个院部的共享目录，教师上传到本院部的文件，上传者本人可以删除，本院其他教师无权删除（需要用到粘滞位权限设置）

具体实训步骤：

一、安装 Samba 软件包。

```
[root@server7-1]#yum  -y  install  samba
```

```
已加载插件：fastestmirror, langpacks
cd                                                       | 3.6 kB     00:00
Loading mirror speeds from cached hostfile
正在解决依赖关系
……
 samba-libs.x86_64 0:4.4.4-9.el7    samba-winbind-modules.x86_64 0:4.4.4-
9.el7
完毕！
```

二、启用 Samba 服务

```
[root@server7-1]#systemctl  start  smb  nmb
[root@server7-1]#systemctl  enable  smb  nmb
```

Samba 运行的有两个服务：一个是 SMB，另一个是 NMB。

1. SMB 是 Samba 的核心启动服务，主要负责建立 Linux Samba 服务器与 Samba 客户机之间的对话， 验证用户身份并提供对文件和打印系统的访问，只有 SMB 服务启动，才能实现文件的共享，监听 139 TCP 端口；

2. NMB 服务是负责解析用的，类似与 DNS 实现的功能，NMB 可以把 Linux 系统共享的工作组名称与其 IP 对应起来，如果 NMB 服务没有启动，就只能通过 IP 来访问共享文件，监听 137 和 138 UDP 端口。

三、配置防火墙策略，SElinux 安全子系统放行。

```
[root@server7-1]# firewall-cmd  --permanent  --add-service=samba
[root@server7-1]# firewall-cmd  --reload
```

```
[root@server7-1 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: dhcpv6-client samba ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

设置 Selinux 为允许模式

```
[root@server7-1]# setenforce  0
```

四. 建立目录

```
[root@server7-1]# mkdir  -p  /share/docx
```

```
[root@server7-1]# mkdir  /computer  /English  /account

[root@server7-1]# mkdir  /temp
```

五.添加用户和组

```
[root@server7-1]# useradd master
[root@server7-1]# groupadd computer
[root@server7-1]# groupadd English
[root@server7-1]# groupadd account
[root@server7-1]# useradd -g computer wang_128
[root@server7-1]# useradd -g computer zhangbin
[root@server7-1]# useradd -g computer lihua
[root@server7-1]# useradd -g English liyouling
[root@server7-1]# useradd -g English zhanglili
[root@server7-1]# useradd -g English wangli
[root@server7-1]# useradd -g account dongwulun
[root@server7-1]# useradd -g account zhangshang
[root@server7-1]# useradd -g account lili
```

六.使用 smbpassswd 命令添加 samba 用户与密码

```
[root@server7-1]# smbpasswd -a master
New SMB password:
Retype new SMB password:
Added user master.
[root@server7-1]# smbpasswd -a wang_128
[root@server7-1]# smbpasswd -a zhangbin
[root@server7-1]# smbpasswd -a lihua
[root@server7-1]# smbpasswd -a liyouling
[root@server7-1]# smbpasswd -a zhanglili
[root@server7-1]# smbpasswd -a wangli
[root@server7-1]# smbpasswd -a dongwulun
[root@server7-1]# smbpasswd -a zhangshang
[root@server7-1]# smbpasswd -a lili
```

七.修改配置文件

1.复制配置文件

用户配置文件使用用户名命名，组配置文件使用组名命名。

```
[root@server7-1]# cp  /etc/samba/smb.conf  /etc/samba/master.smb.conf
[root@server7-1]# cp  /etc/samba/smb.conf  /etc/samba/computer.smb.conf
[root@server7-1]# cp  /etc/samba/smb.conf  /etc/samba/English.smb.conf
[root@server7-1]# cp  /etc/samba/smb.conf  /etc/samba/account.smb.conf
[root@server7-1]# ls  /etc/samba
```

```
account.smb.conf    English.smb.conf   master.smb.conf   smb.conf.example
computer.smb.conf   lmhosts            smb.conf
```

2.设置主配置文件 smb.conf

[root@server7-1]#vim /etc/samba/smb.conf

添加以下语句(只有 smb.conf 才有下列语句)：

include=/etc/samba/%U.smb.conf

include=/etc/samba/%G.smb.conf

说明：如果在主配置文件 smb.conf 声明了这两个语句的话，smb 服务器会去找对应的路径文件。

%U 是声明用户名（User 名）的配置文件

%G 是声明组（Group）的配置文件

```
[pub]
path=/share/docx
browseable=yes          #指定该共享是否可以浏览
writable=no             #指定该共享路径是否可写
guest ok=yes            #指定该共享是否允许 guest 账户访问
[temp]
path=/temp
browseable=yes
writable=yes
guest ok=yes
```

root@localhost:~

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

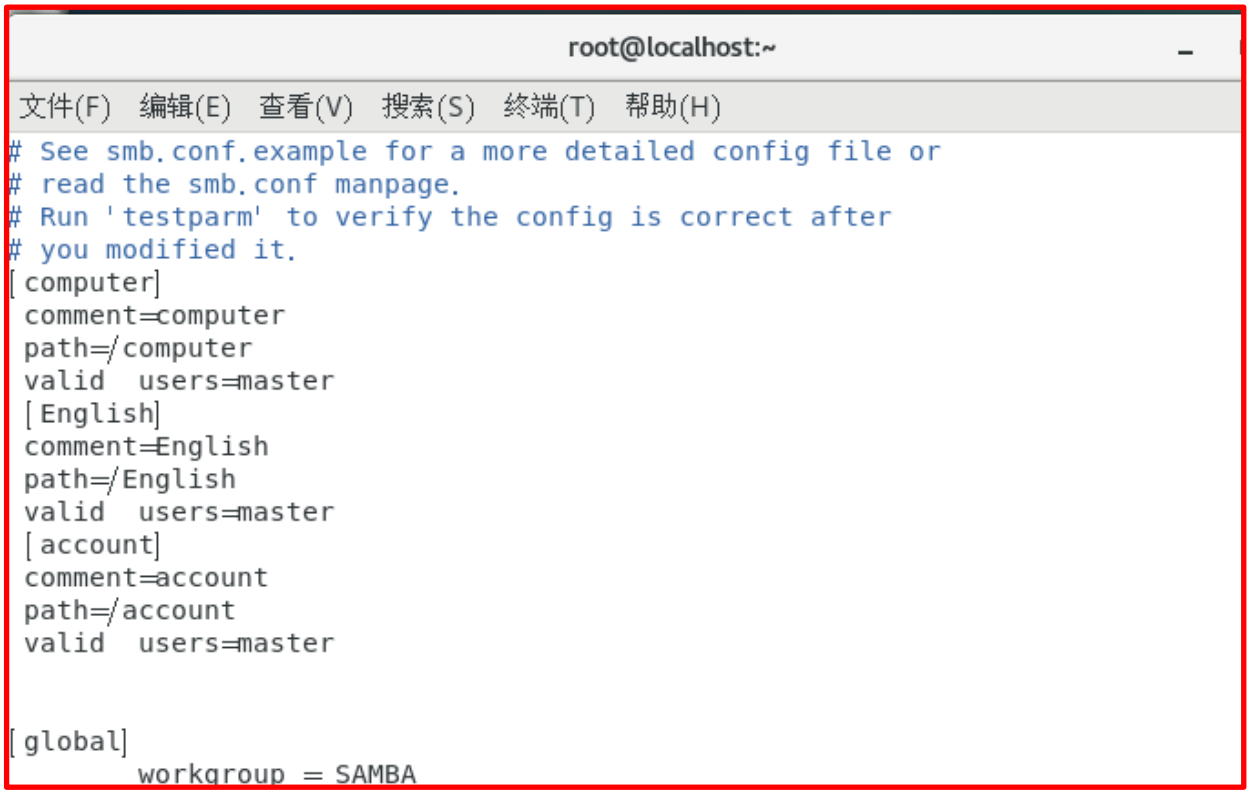
```
# See smb.conf.example for a more detailed config file or
# read the smb.conf manpage.
# Run 'testparm' to verify the config is correct after
# you modified it.
include=/etc/samba/%U.smb.conf
include=/etc/samba/%G.smb.conf
[pub]
 path=/share/docx
 browseable=yes
 writable=no
 guest ok=yes
[temp]
 path=/temp
browseable=yes
 writable=yes
 guest ok=yes
```

3.设置 master 配置文件

[root@server7-1]#vim /etc/samba/master.smb.conf

添加如下内容：

```
[computer]
 comment=computer
 path=/computer
 valid  users=master
 [English]
 comment=English
 path=/English
 valid  users=master
 [account]
 comment=account
 path=/account
 valid  users=master
```



4. 设置 computer 配置文件

[root@server7-1]#vim /etc/samba/computer.smb.conf

添加如下内容：

```
[computer]
        comment=computer
        path=/computer
        valid users=@computer,master
        writable=yes
```

```
文件(F)  编辑(E)  查看(V)  搜索(S)  终端(T)  帮助(H)
# See smb.conf.example for a more detailed config file or
# read the smb.conf manpage.
# Run 'testparm' to verify the config is correct after
# you modified it.
[computer]
     comment=computer
     path=/computer
     valid users=@computer,master
     writable=yes

[global]
        workgroup = SAMBA
```

5. 设置 English 配置文件

[root@server7-1]# vim /etc/samba/English.smb.conf

添加如下内容：

```
[English]
 comment=English
 path=/English
valid users=@English,master
writable=yes
```

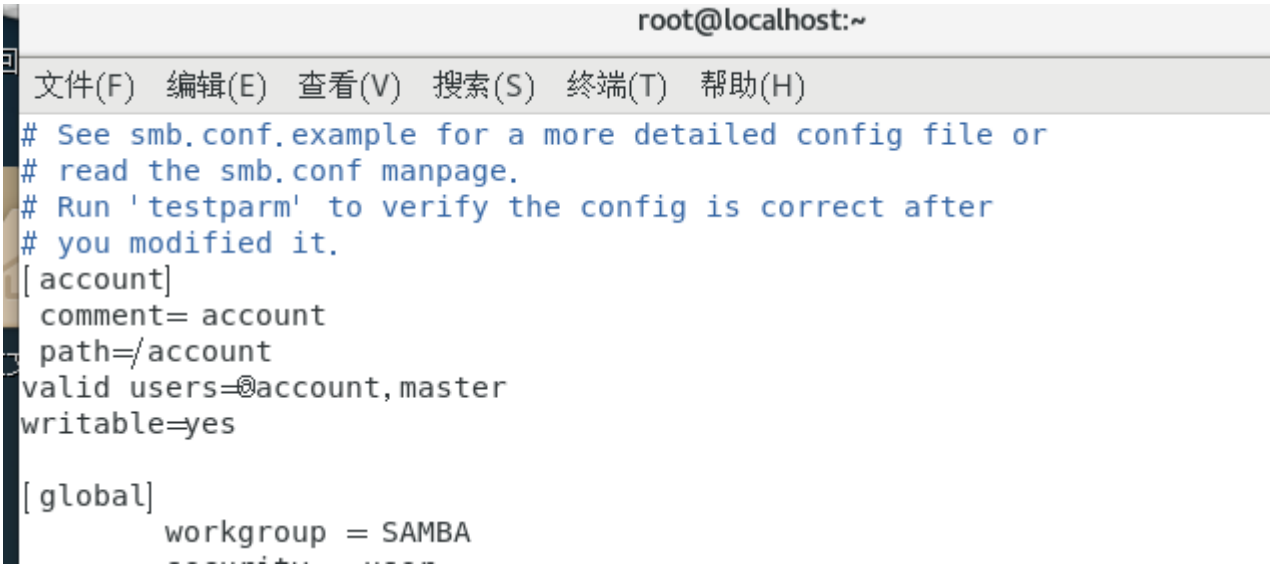
```
文件(F)  编辑(E)  查看(V)  搜索(S)  终端(T)  帮助(H)
# See smb.conf.example for a more detailed config file or
# read the smb.conf manpage.
# Run 'testparm' to verify the config is correct after
# you modified it.
[English]
 comment=English
 path=/English
valid users=@English,master
writable=yes

[global]
        workgroup = SAMBA
        security = user
```

6. 设置 account 配置文件

[root@server7-1]#vim /etc/samba/account.smb.conf

添加如下内容：

```
[account]
 comment= account
 path=/account
valid users=@account,master
writable=yes
```



7.重新启动 smb 服务

```
[root@server7-1]# systemctl  restart  smb
```

八、修改目录的权限

1. 查看公共目录/share/docx 权限，默认没有写权限，不需修改

```
[root@server7-1]# ll  -d  /share/docx
```

2. 查看并修改公共空间 temp 权限

```
[root@server7-1]# ll  -d  /temp
drwxr-xr-x. 2 root root 6 12月 22 21:41 /temp
[root@server7-1]# chmod  777  /temp
```

3. 设置 master 没有写权限

```
[root@server7-1]# setfacl -m u:master:r-x /temp
```

4.每个系部的老师对自己的系部的目录有写权限,但是不能删除别人建立的文件或目录.

```
[root@server7-1]#chgrp  computer  /computer
[root@server7-1]#chgrp  English  /English
[root@server7-1]#chgrp  account  /account
[root@server7-1]# chmod 1770   /computer
[root@server7-1]# chmod 1770  /English
[root@server7-1]# chmod 1770  /account
```

我们可以看到，权限位表示为 drwxrwxrwt，即这是一个目录（第一位为字母 d），属主可读可写可执行，属组可读可写可执行，其他人可读可写可执行，最后那个小写字母 t，表示这个目录具有粘滞位。

所谓粘滞位，意思为：

普通用户在此目录中创建的文件，读写受其权限位的限制，但是删除却只能由文件所有者或 root 删除，其他用户即使拥有写权限，也不能删除之。（当一个目录被设置为"粘着位"(用 chmod a+t),则该目录下的文件只能由

一、超级管理员删除

二、该目录的所有者删除

三、该文件的所有者删除

也就是说,即便该目录是任何人都可以写,但也只有文件的属主才可以删除文件。

chmod 777 abc

chmod +t abc

等价于

chmod 1777 abc

5. 设置院长对各院部目录有读权限

```
[root@server7-1]# setfacl -m u:master:r-x /computer
[root@server7-1]# setfacl -m u:master:r-x /account
[root@server7-1]# setfacl -m u:master:r-x /English
```

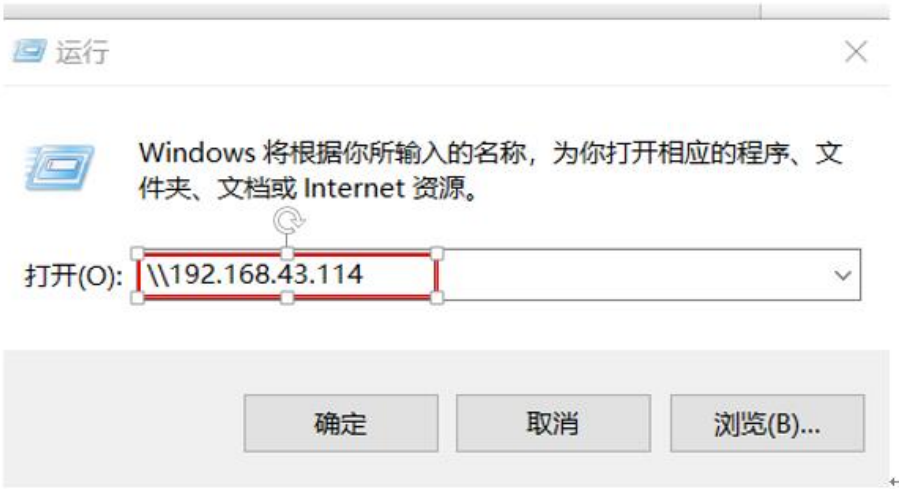
chmod 命令可以把文件权限分为 u,g,o 三个组，而 setfacl 可以对每一个文件或目录设置更精确的文件权限。换句话说，setfacl 可以更精确的控制权限的分配。比如：让某一个用户对某一个文件具有某种权限。

九．验证测试

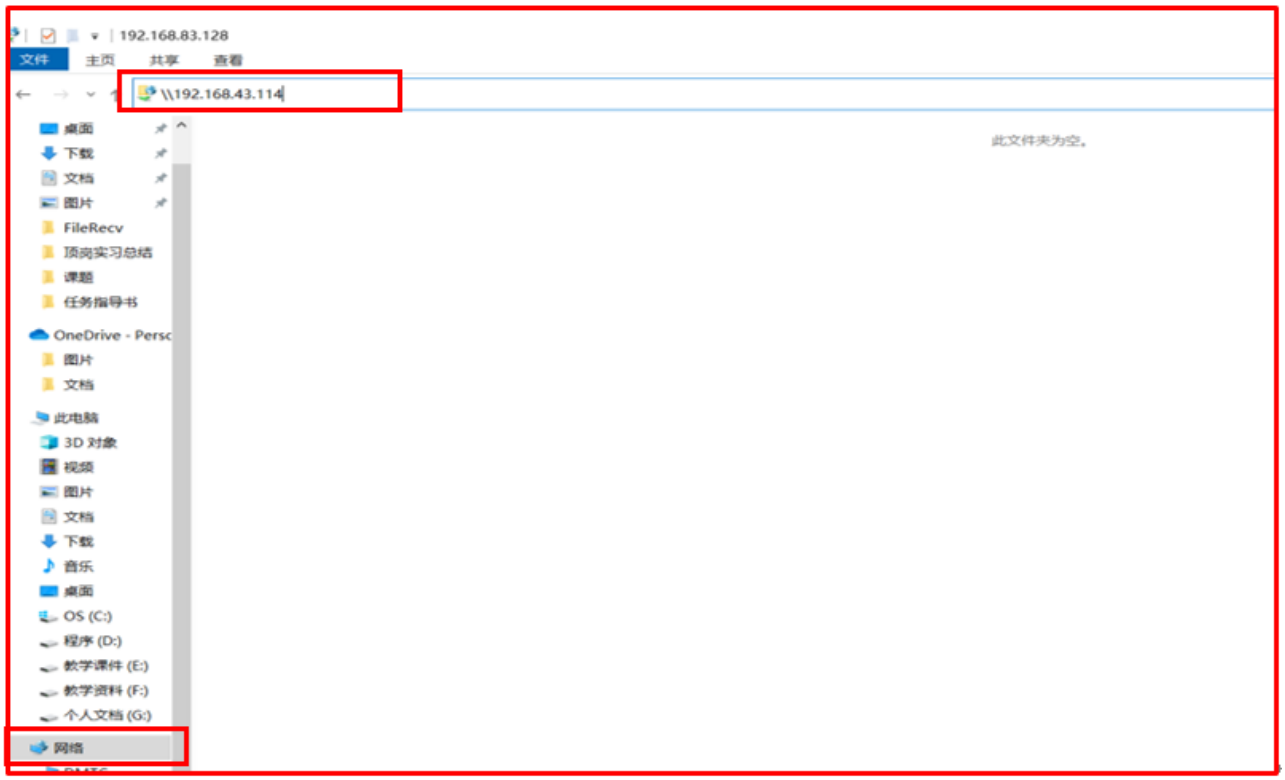
1. 院长 master 登录

院长 master 登录，可以看到公共目录、三个系部的目录和公共空间目录，windows 系统中，打开网络，在地址栏输入（或者在运行对话框中）输入本机的 ip 地址：如 \\192.168.43.114

见下图

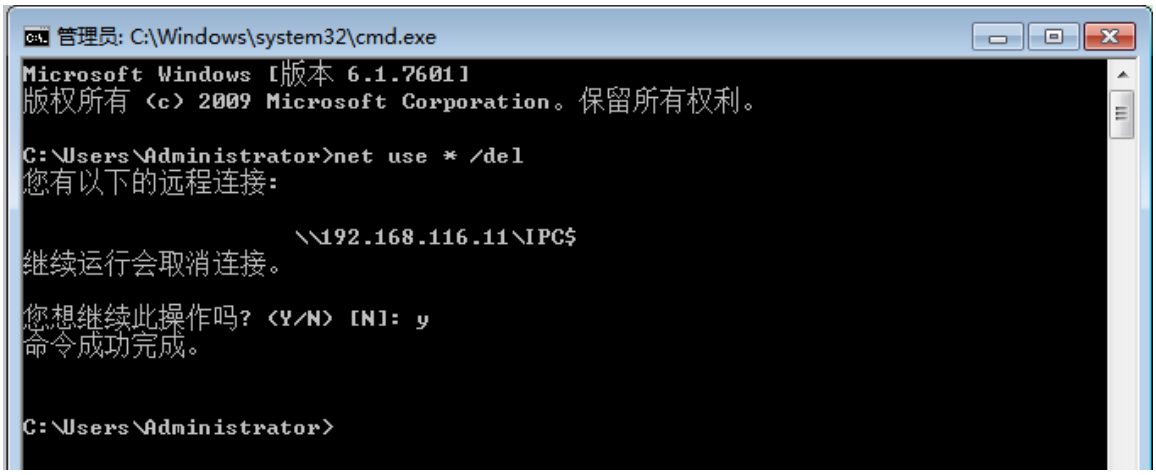


或者

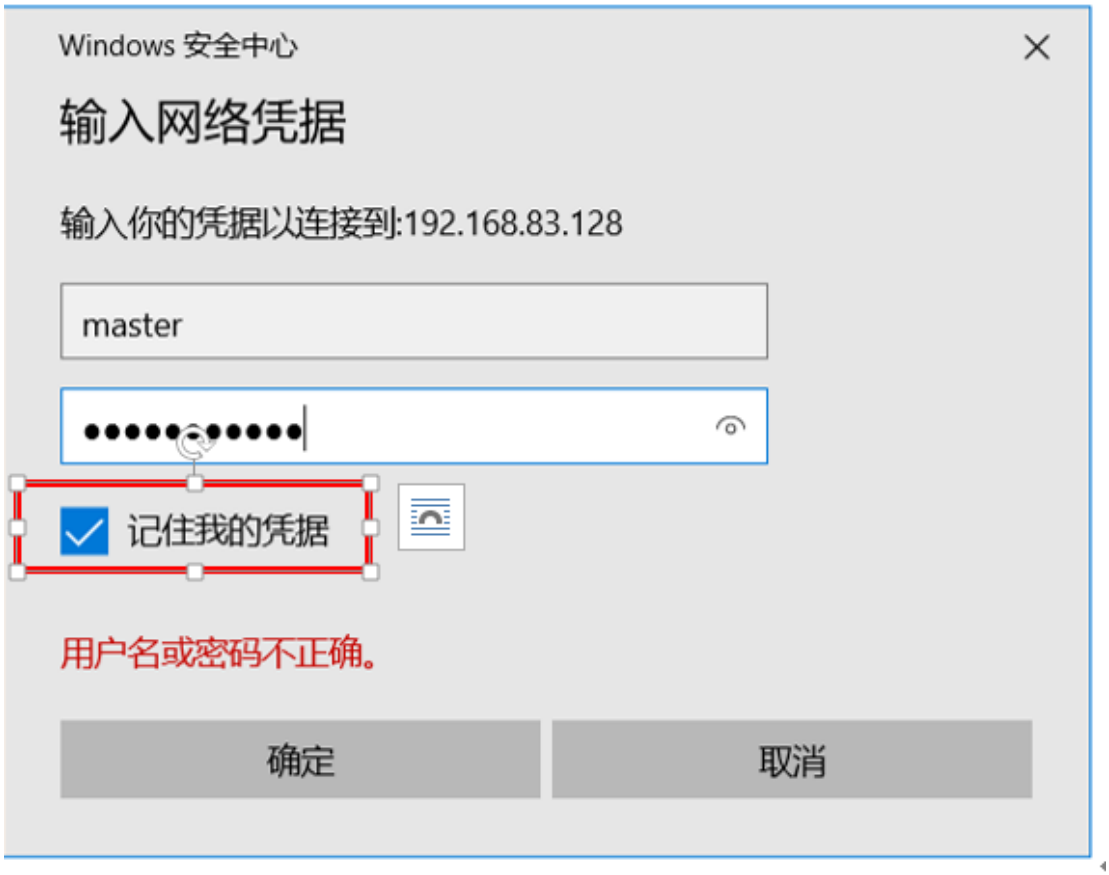


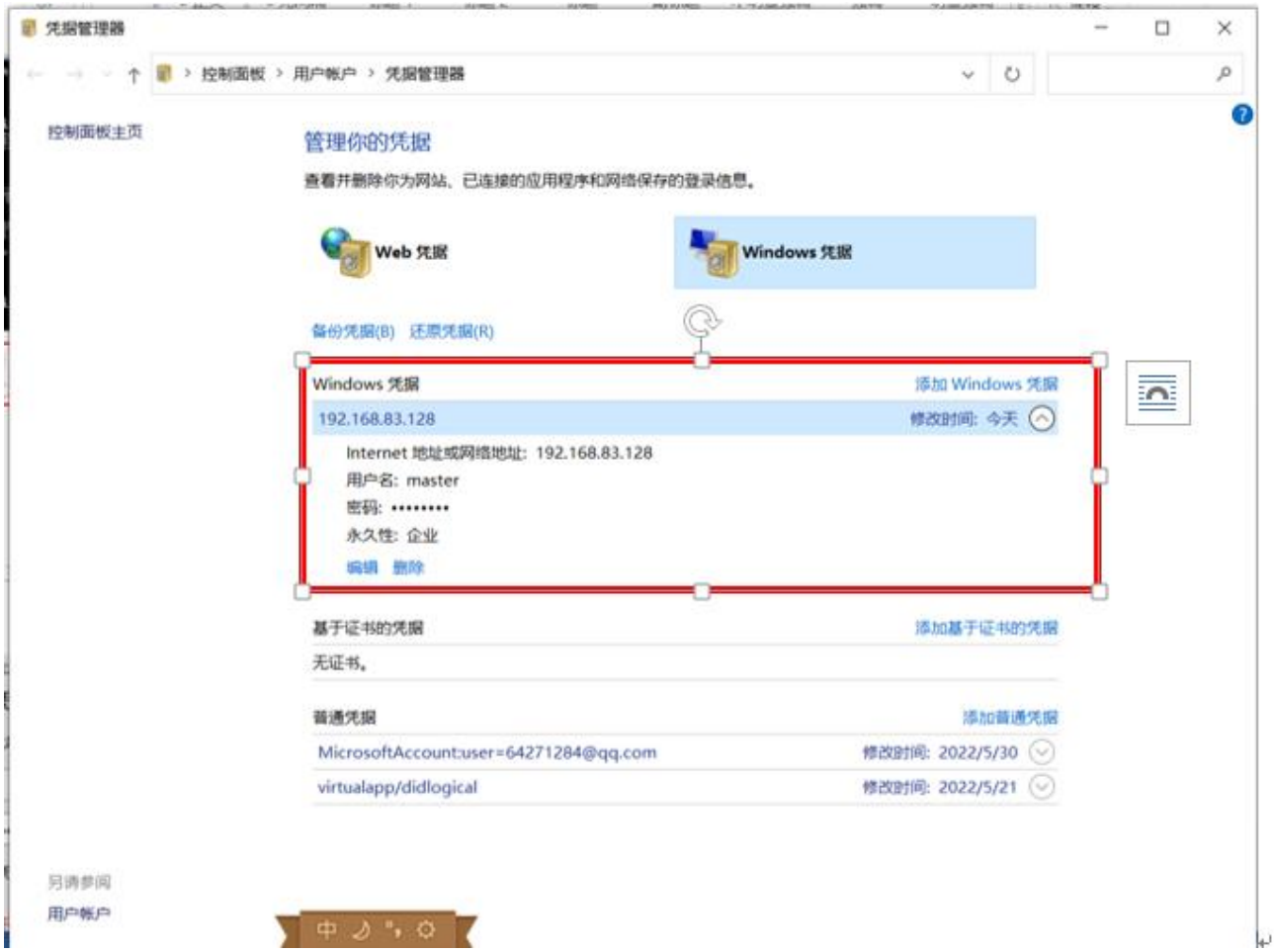
记住我的凭据，就无法在 cmd 窗口中使用 net use * /del 断开本次连接，需要在凭据管理器中删除本次连接。

注意：
因为登录后，windows 后自动记住密码，
必须用 CMD 命令断开本次连接（前提是登录时没有记住我的凭据）
输入命令：net use * /del

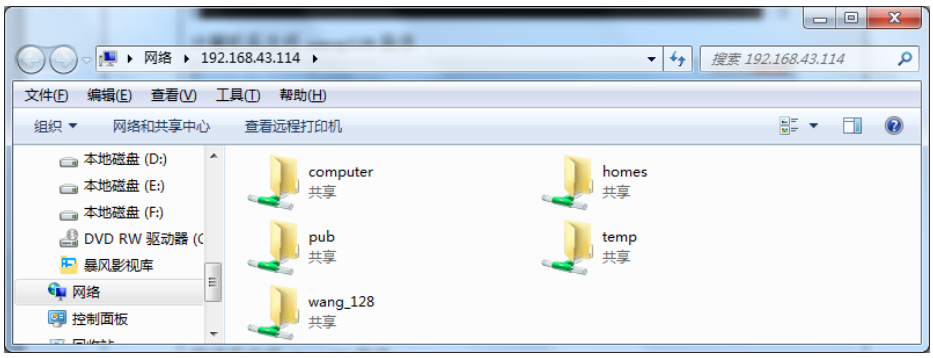


注意：如果登录时记住我的凭据，就无法在 cmd 窗口中使用 net use * /del 断开本次连接，需要在凭据管理器中删除本次连接。

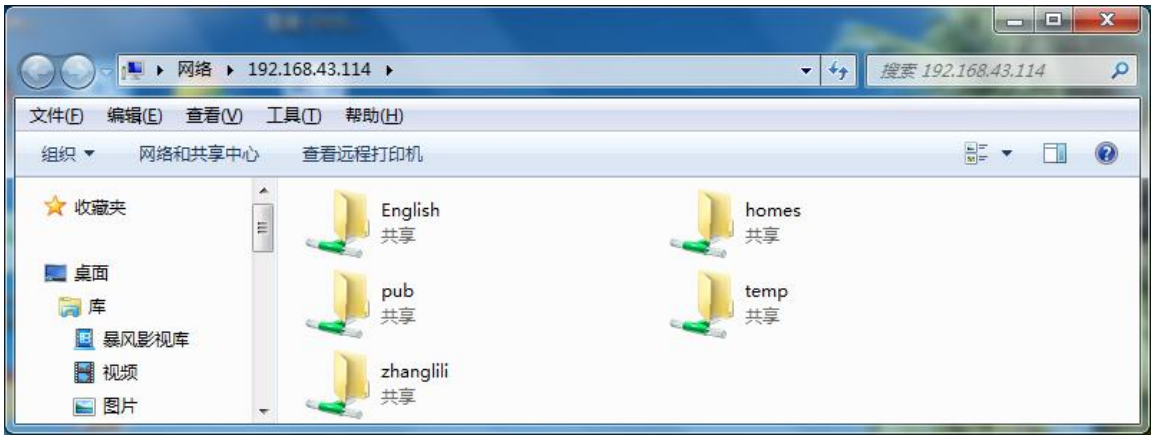




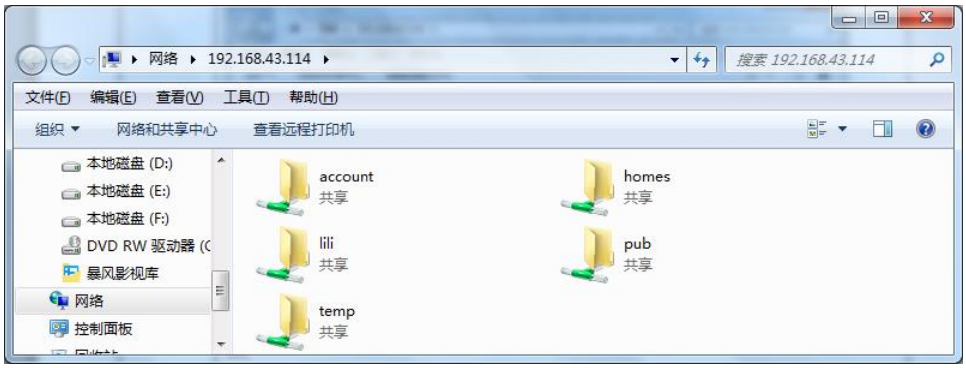
2. 计算机系主任 wang_128 登录，可以看到公共目录、公共空间目录、本系的目录.



3. 英语系主任 zhanglili 登录，可以看到公共目录、公共空间目录、本系的目录



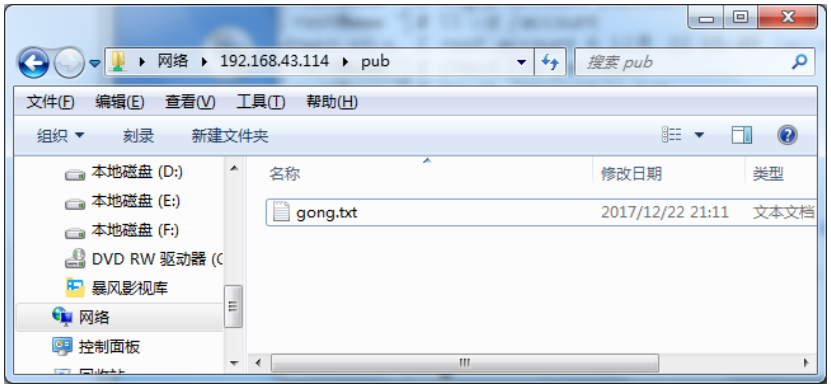
4. 会计系老师 lili 登录，可以看到公共目录、公共空间目录、本系的目录

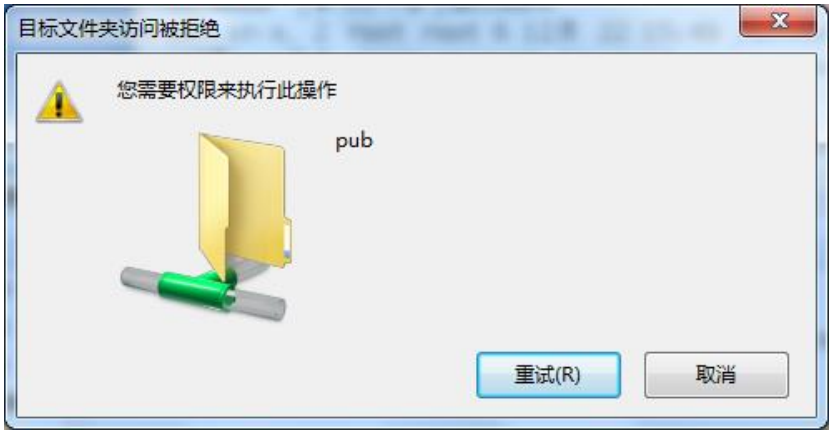


5.验证公共目录 pub 权限为只读

[root@server7-1]# vim /share/docx/gong.txt

在文件中输入内容，此时用任何一个帐户登录，可以看到这个文件，但是不能在该目录中建文件、建目录.





6.验证公共空间 temp 权限

以 zhangbin 的身份登录建立一个文件 123.txt，然后退出登录以 lihua 的身份登录试图删除 123.txt，系统会如下提示。