# Linux Samba文件共享

简介：

Samba是，Linux、UNIX 与 Windows之间进行交互操作的如那件组件，Samba是基于GPL协议的自由开源软件。自1992年以来，Samba开始通过SMB/CIFS协议为Winodws、OS/2、Linux以及众多其他支持该协议的操作系统提供安全，稳定，快速的文件与打印服务，在使用winbind将Linux/UNIX无缝整合到活动目录环境中时，Samba也是一个重要的组件。

所需如那件宝库奥：Samba（服务器端软件包）,Samba-client(客户端软件包)和Samba-common（Samba公共文件软件包）。其中，Samba由smbd和nmbd两个守护进程组成买两个进行的启动脚本是独立的。

## 一，快速配置Samba服务器

### 1，关闭防火墙与SELinux

[root@centos7~]# setenforce 0 # 临时关闭SELinux

[root@centos7~]# sed -i "/SELINUX=/c SELINUX=disable" \

> /etc/sysconfig/selinux # 永久关闭SELinux

[root@centos7~]# systemctl stop firewalld.service # 临时关闭防火墙

[root@centos7~]# systemctl disable firewalld.service # 永久关闭防火墙

### 2，安装Samba软件

[root@centos7~]# yum -y install samba

### 3，创建共享目录

[root@centos7~]# mkdir /common

[root@centos7~]# chmod 777 /common

[root@centos7~]# echo "hello the word" > /common/smb.txt #创建测试文件

### 4，修改配置文件

在做完以上配置后，如果希望Samba服务可以共享指定的目录给客户端，就需要在配置文件中写入目录共享的代码段，Samba默认配置文件是/etc/samba/smb.conf。

[root@centos7~]# vim /etc/samba/smb.conf

[common] #共享名称为common

common = Common share #共享说明信息

path = /common #重要，指定共享路径

browseable = yes #所有人可见

guest ok = no #拒绝匿名访问

writale = yes #支持写入数据

### 5，创建访问账号

客户端访问Samba共享时所使用的账户名就是服务器端操作系统中真是存在的系统账户名称，但不同于微软的共享设置，访问Samba共享的密码必须时独立的Samba密码，而不可以使用系统密码。

成功访问Samba服务器还需要使用smbpasswd将系统账户添加到Samba，并设置相应的密码，CentOS7系统自带的Samba软件包安装后，默认会将账户与密码文件存放在/var/lib/samba/private目录下。

[root@centos7~]# useradd -s /sbin/login smbuser

[root@centos7~]# smbpasswd -a smbuser

#提示输入密码，总共两次

smbpasswd命令的描述和用法如下：

描述：修改账户samba密码

用法：smbpasswd [选项] 账户名称

选项：

-a 添加账户并设置密码

-x 删除SMB账户

-d 禁用SMB账户

-e 启动SMB账户

### 6，启动服务

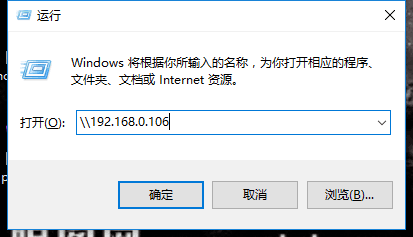
[root@centos7~]# systemctl start smb

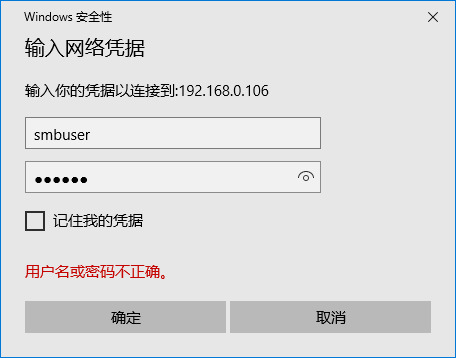
[root@centos7~]# systemctl enable smb

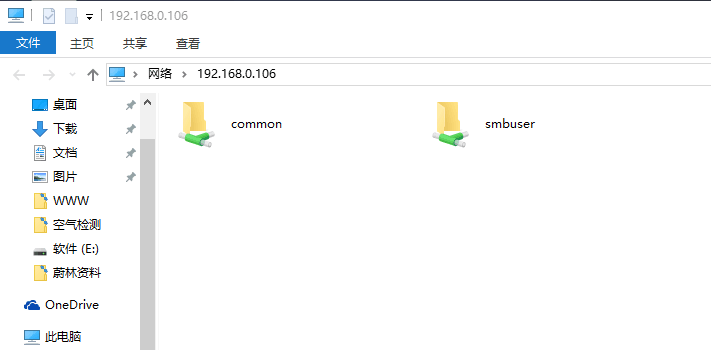
二，访问方式

1，window客户端访问

在windows环境中，通过“开始”-》“运行”菜单或直接按Win+R快捷键开启运行对话框，在该对话框中输入\\IP(其中的IP为Samba服务器的IP地址)，单击“确定”按钮访问Smaba共享，如果是基于用户名和密码的访问，系统会提示输入账号与密码。登陆成功后，可以看到Samba共享了两个目录。







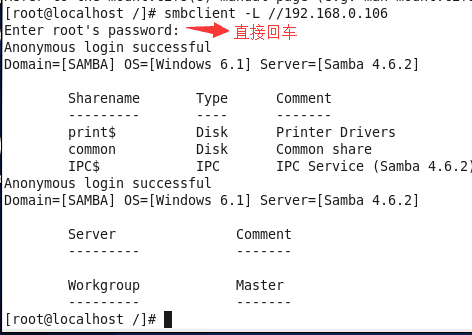
2，linux客户端访问

Linux客户端使用smbclient命令可以访问服务器上的资源。（需要安装samba-client客户端）

[root@centos7~]# smbclient -L //192.168.0.106

#查看192.168.0.106主机共享信息

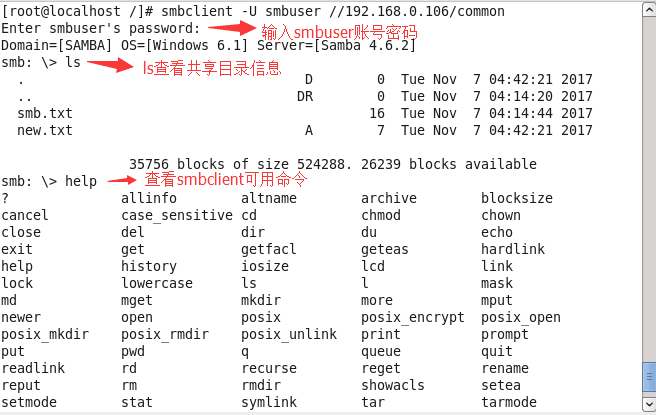
#提示输入当前账户密码。（仅查看不需要密码，直接按回车）

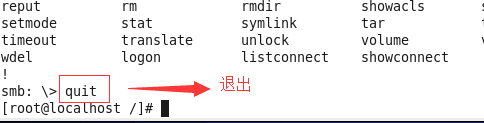


[root@centos7~]# smbclient -U smbuser //192.168.0.106/common

#访问samba共享目录

#输入账号密码





有时候，挂载Samba共享目录实现如本地文件系统一样的使用体验是很有意义的，使用root管理员身份运行mount命令可以改在这样的文件系统，将挂载信息写入fstab文件可以实现永久挂载的目的。

需要开启：nmb服务(默认使用的是137端口，满足CIFS协议共享访问环境)

[root@centos7~]# systemctl start nmb

[root@centos7~]# mkdir /com

[root@centos7~]# mount -e cifs //192.168.0.106/commom /com \

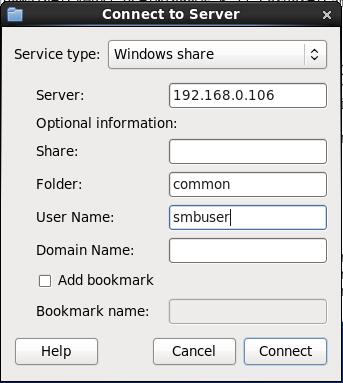
-o username=smbuser,password=<password>

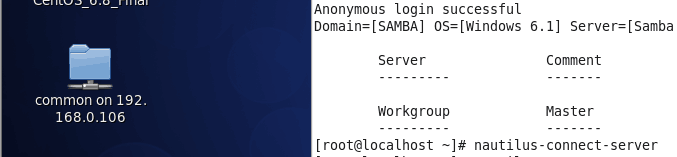
[root@centos7~]# echo "//192.168.0.106/common /com /smb \ #实现永久挂载

> cifs defaults,username=smbuser,password=<password> 0 0" >> /etc/fstab"

若希望使用图形访问Samba共享式，首先通过nautilus-connect-server命令开启图形配置界面。

[root@centos7~]# nautilus-connect-server





## 二，配置文件详解

Samba配置文件非常简洁明了，所有的设置都在/etc/samba/smb.conf配置文件中进行，通过对该配置文件的修改，可以将Samba配置为一台米明文件服务器、给予账户的文件服务器或打印服务器，默认情况下，Samba会已开启本地账号家目录共享与打印机共享，配置文件中以#或;符号开头的行为注释行，配置文件分为若干段，除了global(全局配置段)之外的其余所有段用来描述共享资源，全局段中的配置代表全局有效，是全局的默认设置。但如果全局配置段中的设置项与共享段中的设置项有冲突，则共享设置段的设置为实际有效值。

### smb.conf

config file = /usr/local/samba/lib/smb.conf.%m

说明：config file可以让你使用另一个配置文件来覆盖缺省的配置文件。如果文件 不存在，则该项无效。这个参数很有用，可以使得samba配置更灵活，可以让一台samba服务器模拟多台不同配置的服务器。比如，你想让PC1（主机名）这台电脑在访问Samba Server时使用它自己的配置文件，那么先在/etc/samba/host/下为PC1配置一个名为smb.conf.pc1的文件，然后在smb.conf中加入：config file = /etc/samba/host/smb.conf.%m。这样当PC1请求连接Samba Server时，smb.conf.%m就被替换成smb.conf.pc1。这样，对于PC1来说，它所使用的Samba服务就是由smb.conf.pc1定义的，而其他机器访问Samba Server则还是应用smb.conf。

workgroup = WORKGROUP

说明：设定 Samba Server 所要加入的工作组或者域。

server string = Samba Server Version %v

说明：设定 Samba Server 的注释，可以是任何字符串，也可以不填。宏%v表示显示Samba的版本号。

netbios name = smbserver

说明：设置Samba Server的NetBIOS名称。如果不填，则默认会使用该服务器的DNS名称的第一部分。netbios name和workgroup名字不要设置成一样了。

interfaces = lo eth0 192.168.12.2/24 192.168.13.2/24

说明：设置Samba Server监听哪些网卡，可以写网卡名，也可以写该网卡的IP地址。

hosts allow = 127. 192.168.1. 192.168.10.1

说明：表示允许连接到Samba Server的客户端，多个参数以空格隔开。可以用一个IP表示，也可以用一个网段表示。hosts deny 与hosts allow 刚好相反。

例如：hosts allow=172.17.2.EXCEPT172.17.2.50

表示容许来自172.17.2.\*.\*的主机连接，但排除172.17.2.50

hosts allow=172.17.2.0/255.255.0.0

表示容许来自172.17.2.0/255.255.0.0子网中的所有主机连接

hosts allow=M1，M2

表示容许来自M1和M2两台计算机连接

hosts allow=@xq

表示容许来自XQ网域的所有计算机连接

max connections = 0

说明：max connections用来指定连接Samba Server的最大连接数目。如果超出连接数目，则新的连接请求将被拒绝。0表示不限制。

deadtime = 0

说明：deadtime用来设置断掉一个没有打开任何文件的连接的时间。单位是分钟，0代表Samba Server不自动切断任何连接。

time server = yes/no

说明：time server用来设置让nmdb成为windows客户端的时间服务器。

log file = /var/log/samba/log.%m

说明：设置Samba Server日志文件的存储位置以及日志文件名称。在文件名后加个宏%m（主机名），表示对每台访问Samba Server的机器都单独记录一个日志文件。如果pc1、pc2访问过Samba Server，就会在/var/log/samba目录下留下log.pc1和log.pc2两个日志文件。

max log size = 50

说明：设置Samba Server日志文件的最大容量，单位为kB，0代表不限制。

security = user

说明：设置用户访问Samba Server的验证方式，一共有四种验证方式。

1. share：用户访问Samba Server不需要提供用户名和口令, 安全性能较低。【已废弃】

2. user：Samba Server共享目录只能被授权的用户访问,由Samba Server负责检查账号和密码的正确性。账号和密码要在本Samba Server中建立。

3. server：依靠其他Windows NT/2000或Samba Server来验证用户的账号和密码,是一种代理验证。此种安全模式下,系统管理员可以把所有的Windows用户和口令集中到一个NT系统上,使用Windows NT进行Samba认证, 远程服务器可以自动认证全部用户和口令,如果认证失败,Samba将使用用户级安全模式作为替代的方式。

4. domain：域安全级别,使用主域控制器(PDC)来完成认证。

例如：无用户密码访问

[global]

security = user # 先定义需要用户名和密码访问

map to guest = Bad User # 重新定义成匿名访问

passdb backend = tdbsam

说明：passdb backend就是用户后台的意思。目前有三种后台：smbpasswd、tdbsam和ldapsam。sam应该是security account manager（安全账户管理）的简写。

1.smbpasswd：该方式是使用smb自己的工具smbpasswd来给系统用户（真实

用户或者虚拟用户）设置一个Samba密码，客户端就用这个密码来访问Samba的资源。smbpasswd文件默认在/etc/samba目录下，不过有时候要手工建立该文件。

2.tdbsam：该方式则是使用一个数据库文件来建立用户数据库。数据库文件叫passdb.tdb，默认在/etc/samba目录下。passdb.tdb用户数据库可以使用smbpasswd –a来建立Samba用户，不过要建立的Samba用户必须先是系统用户。我们也可以使用pdbedit命令来建立Samba账户。pdbedit命令的参数很多，我们列出几个主要的。

pdbedit –a username：新建Samba账户。

pdbedit –x username：删除Samba账户。

pdbedit –L：列出Samba用户列表，读取passdb.tdb数据库文件。

pdbedit –Lv：列出Samba用户列表的详细信息。

pdbedit –c “[D]” –u username：暂停该Samba用户的账号。

pdbedit –c “[]” –u username：恢复该Samba用户的账号。

3.ldapsam：该方式则是基于LDAP的账户管理方式来验证用户。首先要建立LDAP服务，然后设置“passdb backend = ldapsam:ldap://LDAP Server”

encrypt passwords = yes/no

说明：是否将认证密码加密。因为现在windows操作系统都是使用加密密码，所以一般要开启此项。不过配置文件默认已开启。

smb passwd file = /etc/samba/smbpasswd

说明：用来定义samba用户的密码文件。smbpasswd文件如果没有那就要手工新建。

username map = /etc/samba/smbusers

说明：用来定义用户名映射，比如可以将root换成administrator、admin等。不过要事先在smbusers文件中定义好。比如：root = administrator admin，这样就可以用administrator或admin这两个用户来代替root登陆Samba Server，更贴近windows用户的习惯。

guest account = nobody

说明：用来设置guest用户名。

socket options = TCP\_NODELAY SO\_RCVBUF=8192 SO\_SNDBUF=8192

说明：用来设置服务器和客户端之间会话的Socket选项，可以优化传输速度。

domain master = yes/no

说明：设置Samba服务器是否要成为网域主浏览器，网域主浏览器可以管理跨子网域的浏览服务。

local master = yes/no

说明：local master用来指定Samba Server是否试图成为本地网域主浏览器。如果设为no，则永远不会成为本地网域主浏览器。但是即使设置为yes，也不等于该Samba Server就能成为主浏览器，还需要参加选举。

preferred master = yes/no

说明：设置Samba Server一开机就强迫进行主浏览器选举，可以提高Samba Server成为本地网域主浏览器的机会。如果该参数指定为yes时，最好把domain master也指定为yes。使用该参数时要注意：如果在本Samba Server所在的子网有其他的机器（不论是windows NT还是其他Samba Server）也指定为首要主浏览器时，那么这些机器将会因为争夺主浏览器而在网络上大发广播，影响网络性能。

如果同一个区域内有多台Samba Server，将上面三个参数设定在一台即可。

os level = 200

说明：设置samba服务器的os level。该参数决定Samba Server是否有机会成为本地网域的主浏览器。os level从0到255，winNT的os level是32，win95/98的os level是1。Windows 2000的os level是64。如果设置为0，则意味着Samba Server将失去浏览选择。如果想让Samba Server成为PDC，那么将它的os level值设大些。

domain logons = yes/no

说明：设置Samba Server是否要做为本地域控制器。主域控制器和备份域控制器都需要开启此项。

logon . = %u.bat

说明：当使用者用windows客户端登陆，那么Samba将提供一个登陆档。如果设置成%u.bat，那么就要为每个用户提供一个登陆档。如果人比较多，那就比较麻烦。可以设置成一个具体的文件名，比如start.bat，那么用户登陆后都会去执行start.bat，而不用为每个用户设定一个登陆档了。这个文件要放置在[netlogon]的path设置的目录路径下。

wins support = yes/no

说明：设置samba服务器是否提供wins服务。

wins server = wins服务器IP地址

说明：设置Samba Server是否使用别的wins服务器提供wins服务。

wins proxy = yes/no

说明：设置Samba Server是否开启wins代理服务。

dns proxy = yes/no

说明：设置Samba Server是否开启dns代理服务。

load printers = yes/no

说明：设置是否在启动Samba时就共享打印机。

printcap name = cups

说明：设置共享打印机的配置文件。

printing = cups

说明：设置Samba共享打印机的类型。现在支持的打印系统有：bsd, sysv, plp, lprng, aix, hpux, qnx

display charset = UTF8

说明：设置显示使用的字符集为UTF8

共享参数：

================== Share Definitions ==================

[共享名]

comment = 任意字符串

说明：comment是对该共享的描述，可以是任意字符串。

path = 共享目录路径

说明：path用来指定共享目录的路径。可以用%u、%m这样的宏来代替路径里的unix用户和客户机的Netbios名，用宏表示主要用于[homes]共享域。例如：如果我们不打算用home段做为客户的共享，而是在/home/share/下为每个Linux用户以他的用户名建个目录，作为他的共享目录，这样path就可以写成：path = /home/share/%u; 。用户在连接到这共享时具体的路径会被他的用户名代替，要注意这个用户名路径一定要存在，否则，客户机在访问时会找不到网络路径。同样，如果我们不是以用户来划分目录，而是以客户机来划分目录，为网络上每台可以访问samba的机器都各自建个以它的netbios名的路径，作为不同机器的共享资源，就可以这样写：path = /home/share/%m 。

browseable = yes/no

说明：browseable用来指定该共享是否可以浏览。

writable = yes/no

说明：writable用来指定该共享路径是否可写。

available = yes/no

说明：available用来指定该共享资源是否可用。

admin users = 该共享的管理者

说明：admin users用来指定该共享的管理员（对该共享具有完全控制权限）。在samba 3.0中，如果用户验证方式设置成“security=share”时，此项无效。

例如：admin users =bobyuan，jane（多个用户中间用逗号隔开）。

valid users = 允许访问该共享的用户

说明：valid users用来指定允许访问该共享资源的用户。

例如：valid users = bobyuan，@bob，@tech（多个用户或者组中间用逗号隔开，如果要加入一个组就用“@+组名”表示。）

invalid users = 禁止访问该共享的用户

说明：invalid users用来指定不允许访问该共享资源的用户。

例如：invalid users = root，@bob（多个用户或者组中间用逗号隔开。）

write list = 允许写入该共享的用户

说明：write list用来指定可以在该共享下写入文件的用户。

例如：write list = bobyuan，@bob

public = yes/no

说明：public用来指定该共享是否允许guest账户访问。

guest ok = yes/no

说明：意义同“public”。

only guest

说明：设置为yes表示所有用户在使用该共享目录时的用户身份都是guest，即linux系统用户nobody。

veto files = /\*.exe/\*.com/\*.dll/\*.bat/\*.vbs/\*.tmp/\*.mp3 /\*.avi/\*.mp4/\*.wmv/\*.wma/

说明：阻止Samba共享上的某些文件扩展名

注意：设置这个参数会影响Samba的性能，因为它将被强制在扫描时检查所有文件和目录是否匹配。

几个特殊共享：

[homes]

comment = Home Directories

browseable = no

writable = yes

valid users = %S

; valid users = MYDOMAIN\%S

[printers]

comment = All Printers

path = /var/spool/samba

browseable = no

guest ok = no

writable = no

printable = yes

[netlogon]

comment = Network Logon Service

path = /var/lib/samba/netlogon

guest ok = yes

writable = no

share modes = no

[Profiles]

path = /var/lib/samba/profiles

browseable = no

guest ok = yes

### 配置samba虚拟用户

在全局配置[global]中添加 username map = /etc/samba/smbusers

解释：

username map #表示用户映射

/etc/samba/smbusers #映射的虚拟用户文件

虚拟用户文件格式如下：

smb用户名 = 虚拟用户名1 虚拟用户名2 虚拟用户名3 .....

每个虚拟用户可以拥有单独的配置文件

例如：

[root@centos7~]# useradd -s /sbin/nologin smbuser2 #添加smbuser2用户

[root@centos7~]# smbpasswd -a smbuser2 #添加smb密码

[root@centos7~]# vim /etc/samba/smbusers #编辑虚拟配置文件

写入：smbuser = sm1 sm2 sm3

[root@centos7~]# sed -i "/\[global\]/a username map = /etc/samba/smbusers" \

> /etc/samba/smb.conf #加入虚拟配置文件支持

为每个虚拟用户添加单独的配置文件

[root@centos7~]# cp /etc/samba/smb.conf /etc/samba/smb.conf.sm1

[root@centos7~]# cp /etc/samba/smb.conf /etc/samba/smb.conf.sm2

[root@centos7~]# cp /etc/samba/smb.conf /etc/samba/smb.conf.sm3

编辑主配置文件，加载指定的配置文件

[root@centos7~]# sed -i "/\[global\]/a config file = /etc/samba/smb.conf.%U" \

> /etc/samba/smb.conf

其中，%U代表当前登录的用户

为每个虚拟用户配置相应的samba访问权限

例如：sm1

[root@centos7~]# vim /etc/samba/smb.conf.sm1

加入：

[sm1]

comment = data dir for sm1

path = /data/sm2

guest ok = No

valid users = sm2

writeable = Yes

directory mask = 0700

最后，重新启动samba服务即可

虚拟用户登录Samba共享资源的密码为映射用户的密码。

### 3)配置文件测试

在对smb.conf文件完成所有配置以后，可以使用testparm命令对该配置文件进行测试。testparm命令是samba服务器软件包中提供的配置文件测试工具，可以对smb.conf配置文件的语法进行检测，并显示当前配置的清单。

注意：testparm命令显示的配置清单可能与smb.conf中的配置内容稍有不同，这是由于testparm命令对配置文件的内容进行了处理，文件中的默认值设置项的内容会被忽略。可以看出testparm命令显示的配置清单与smb.conf文件中配置含义是完全相符的。

### 配置变量

配置文件变量含义：

%S 当前服务名（如果有的话）

%P 当前服务的根目录（如果有的话）

%u 当前服务的用户名（如果有的话）

%U 当前对话的用户名

%H 当前服务的用户的Home目录

%v Samba服务的版本号

%h 运行Samba服务机器的主机名

%m 客户机的NETBIOS名称

%L 服务器的NETBIOS名称

%M 客户机的主机名

%I 客户机的IP

%T 当前日期和时间

%D 登陆主机名

## 三，samba各命令解析

smbpasswd 命令：

描述：将系统账户添加到Samba,并设置相应密码。

（默认将账户与密码文件存放在/var/lib/samba/private目录下）

格式：

使用root管理员运行：smbpasswd [选项] [用户名]

除此之外：smbpasswd [选项]

选项:

-L本地模式（必须是第一个选项）

-h打印这个使用信息

-s使用标准提示输入密码

-c smb.conf文件使用给定的路径到smb.conf文件

-D LEVEL调试级别

-MACH MACHINE远程机器

-U USER远程用户名（例如SAM /用户）

以root或本地模式运行时的额外选项：

   -a 添加用户

   -d禁用用户

   -e启用用户

   -i域间信任帐户

   -m机器信任帐户

   -n设置密码

   -W使用stdin ldap管理员密码

   -w密码ldap管理员密码

   -x删除用户

   -R ORDER名称解析顺序

我们也可以使用pdbedit命令来建立Samba账户。pdbedit命令的参数很多，我们列出几个主要的。

pdbedit –a username：新建Samba账户。

pdbedit –x username：删除Samba账户。

pdbedit –L：列出Samba用户列表，读取passdb.tdb数据库文件。

pdbedit –Lv：列出Samba用户列表的详细信息。

pdbedit –c “[D]” –u username：暂停该Samba用户的账号。

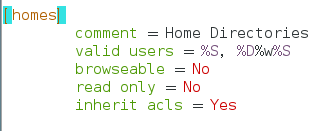
pdbedit –c “[]” –u username：恢复该Samba用户的账号。

## 四，常见Samba配置

### 需求：不允许共享家目录

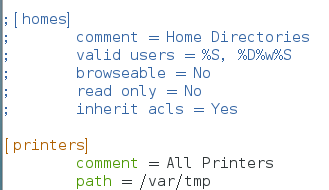
解：

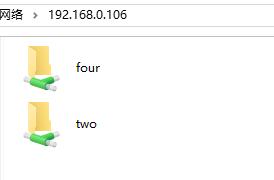
smb.conf默认配置时共享家目录的，但只共享当前登陆用户的家目录。如：





若不想共享家目录的话，则把Homes共享配置全部注释。如：



注：; 或者 # 符号开头的行都是注释。  
 

若要取消打印机共享，也可以注销打印机共享块配置。

打印机共享块有两个：[printers] 和 [print$]

### 需求：公司有5个部门。1个老板，1个领导部门，4个小部门。创建6个文件夹，老板有权限浏览并管理所有共享文件（小部门只可读不可写），领导可以浏览并管理4个小部门的共享文件，4个小部分各自用于自己的部分分享文件夹，最后有一个公共共享文件夹，该公司所有人都可以在公共文件夹读写，但老板只有权限浏览，无法写。

解：

1，首先为每个部分创建文件夹

[root@centos /]# mkdir -p ABC/{manage,sales,design,develop,ops,public}

manage 经理部门

sales 商务部

design 设计部

develop 开发部

ops 运维部

public 公共目录

2，添加账户

这里使用shell脚本创建用户。

[root@centos /]# cat create\_samba\_user.sh

#!/bin/bash

#Add samba\_user

USERS=(boss manage sales design develop ops) #定义管理员列表

for g in ${USERS[@]}

do

groupadd ${g} # 创建组

useradd -M -s /sbin/nologin -g ${g} ${g} # 创建部门管理员账号

useradd -M -s /sbin/nologin -g ${g} ${g}1 # 创建普通员工账号

expect /root/ABC/add\_smbuser.sh ${g} ${g} > /dev/null 2>&1

expect /root/ABC/add\_smbuser.sh ${g}1 ${g}1 > /dev/null 2>&1

# 使用expect完成smb服务器密码的创建，默认密码=账号名称

done

[root@centos /]# cat add.smbuser.sh

#!/usr/bin/expect

set timeout 20 # 设置响应超时事件

set username [lindex $argv 0] # 获取脚本的第一个参数为用户名

set password [lindex $argv 1] # 获取脚本的第二个参数为密码

spawn smbpasswd -a $username # 发送命令

expect "\*SMB password\*" # 程序交互，判断交互返回的数据

send "$password\r" # 自动输入密码

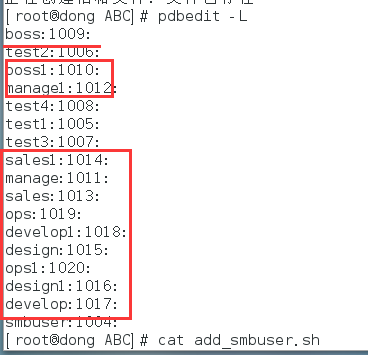
expect "\*new SMB password\*" # 再次程序交互，判断交互返回的数据

send "$password\r" # 再次输入密码

expect "\*#" # 回车

exit # 完成账户创建，退出

注：该脚本的第一行是 #!/usr/bin/expect，表明这是一个使用expect来解析的脚本代码，需要安装expect脚本解析程序。运行脚本使用: expect path(脚本路径)



3，配置smb.conf文件

[root@centos /]# cat /etc/samba/smb.conf

.........

[global]

workgroup = SAMBA

security = user

passdb backend = tdbsam

log file = /var/log/samba/log.%D # 记录日志

max log size = 50 # 日志大小

printing = cups

printcap name = cups

load printers = yes

cups options = raw

[design]

comment = design share

path = /ABC/develop # 共享路径

browseable = yes # 共享可见

writable = no # 共享不可写

write list = @develop # 允许可写的组

guest ok = no # 不允许匿名登陆

valid users = @boss,@manage,@ops # 可访问该共享的组

admin users = develop # 该共享的管理员

[ops]

comment = ops shar

path = /root/ABC/ops

browseable = yes

writable = no

write list = @ops

guest ok = no

valid users = @boss,@manage,@ops

admin users = ops

[sales]

comment = sales shar

path = /root/ABC/sales

browseable = yes

writable = no

write list = @sales

guest ok = no

valid users = @boss,@manage,@sales

admin users = sales

[manage]

comment = manage shar

path = /root/ABC/manage

browseable = yes

writeable = no

write list = @manage

guest ok = no

valid users = @boss,@manage

admin users = manage

[public]

comment = common share

path = /root/ABC/public

browseable = yes

guest ok = no

writable = no

write list = @manage,@sales,@ops,@develop,@design

valid users = @boss,@manage,@sales,@ops,@develop,@design

4，设置文件夹权限

[root@centos /]# chmod 570 {public,manage,sales,ops,develop,design}

[root@centos /]# chown boss:boss {public,mamage,sales,ops,develop,design}

[root@centos /]# chown :manage manage

[root@centos /]# chown :sales sales

[root@centos /]# chown :ops ops

[root@centos /]# chown :develop develop

[root@centos /]# chown :design design

[root@centos /]# setfacl -mR g:manage:rx {sales,ops,develop,design} #设置acl权限

[root@centos /]# setfacl -mR g:boss:rx {sales,ops,develop,design,manage}

5，重启samba服务

[root@centos /]# systemctl restart smb

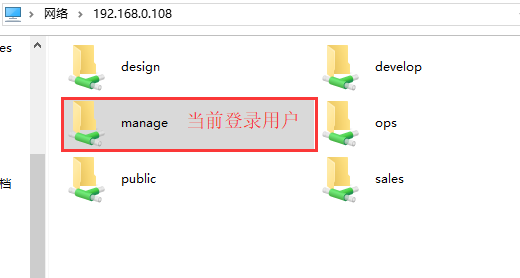
6，结果

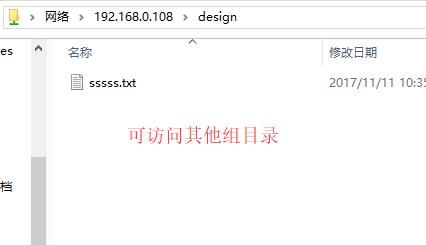
boss组用户可以访问所有共享资源，但除了public共享资源可写外，其余均不可写。

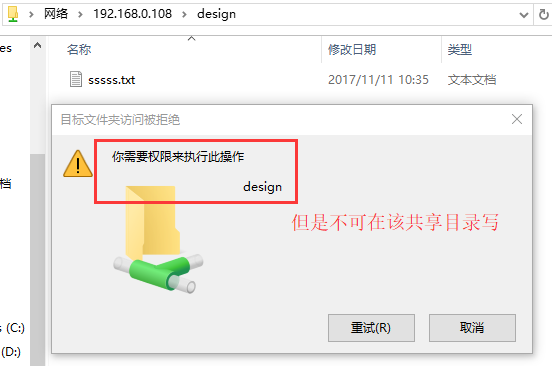
manage组可以访问所有的共享资源，但除了manage 和 public 共享资源可写外，其余均不可写。

余下各部门同manage一样，只有自己部门和public的共享资源可写，其余不可写。

（但是，其余部门只能访问自己部门的共享资源和public的共享资源）







### 允许匿名登陆，共享文件

解：

1) 创建共享文件夹，并设置权限

[root@centos7 /]# mkdir -m 777 /ABC/common

2) 配置smb.conf文件

[root@centos7 /]# cat /etc/samba/smb.conf

[global]

workgroup = SAMBA

security = user

map to guest = Bad User # 允许匿名访问

guest account = nobody # 匿名访问账号

passdb backend = tdbsam

log file = /var/log/samba/log.%m

max log size = 50

printing = cups

printcap name = cups

load printers = yes

[common]

comment = common directory

path = /ABC/common # 共享文件路径

browseable = yes # 共享资源可见

writable = no # 共享资源不可写

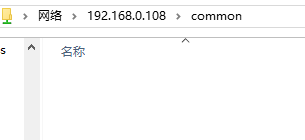
guest ok = yes # 允许匿名访问

1. 重新启动samba服务器

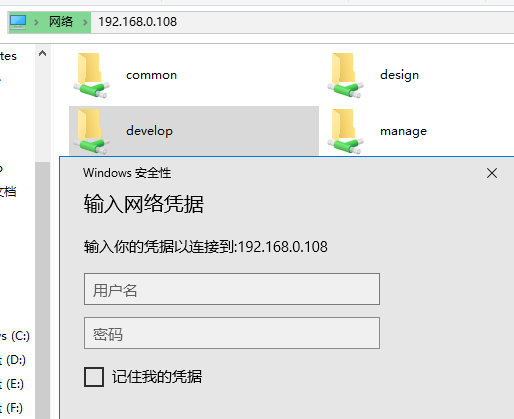
[root@centos7 /]# systemctl restart smb



无需登录，直接进入。



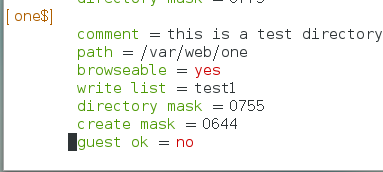
其他共享文件，提示输入登录信息。



### 隐藏某个共享文件

在共享名称后加上 $ 符号 或者 设置 browseable = no 即可。

例如



## 五，常见错误解决

### 1，客户端无法访问Smaba共享资源

解决：

1. 查看Samba服务端是否关闭防火墙或者开放139、137、445这三个端口。

CentOS7以上版本：

[root@centos7~]# systemctl stop firewalld.service #临时关闭防火墙

[root@centos7~]# systemctl enable firewalld.service #永久关闭防火墙

CentOS7以下版本：

关闭防火墙：

[root@centos7~]# service iptables stop #临时关闭防火墙

[root@centos7~]# chkconfig iptables off #永久关闭防火墙

开放端口：

[root@centos7~]# -A INPUT -m state --state NEW -m tcp -p tcp --dport 137 -j ACCEPT

[root@centos7~]# -A INPUT -m state --state NEW -m tcp -p tcp --dport 139 -j ACCEPT

[root@centos7~]# -A INPUT -m state --state NEW -m tcp -p tcp --dport 445 -j ACCEPT

1. 关闭selinux

[root@centos7~]# setenforce 0 #临时关闭selinux

[root@centos7~]# sed -i "/SELINUX=/c SELINUX=disable" \

> /etc/sysconfig/selinux #永久关闭selinux

c) 查看getsebool -a

[root@centos7~]# getsebool -a | grep samba

#查看 samba\_enable\_home\_dirs 和 samba\_export\_all\_rw 是否开启 == on

#未开启则执行下面的命令

[root@centos7~]# setsebool -P samba\_enable\_home\_dirs on 开启配置

[root@centos7~]# setsebool -P samba\_export\_all\_rw on 开启配置

### 2，NT\_STATUS\_BAD\_NETWORK\_NAME

若提示该错误信息，则说明输入了错误的共享名称，一般为输入性错误，需要检查客户端请求的共享资源在服务器中是否存在。

### 3，NT\_STATUS\_LOGIN\_FAILURE

若提示该错误信息，则索命登陆失败，一般是由于账户名或密码不对，则需要检查账户与密码后重试。

### 4，NT\_STATUS\_ACCESS\_DENIED

若提示该错误信息，则说明访问被拒绝，权限不足。可以可能是Samba服务设置的访问权限，也有可能是服务器文件系统的访问权限不允许客户端访问。

### 5，Error NT\_STATUS\_HOST\_UNREACHABLE

若提示该错误信息，则说明客户端无法连接Samba服务器，一般是由于网络故障或防火墙问题引起的，需要检查客户端与服务器的网络连接是否正常。此外，还要检查防火墙规则是否允许客户端请求，Samba端口有137、138、139、445。

### 6，Not enough '\' characters in service

若提示该错误信息，则说明客户端访问时共享路径输入错误，特别是//IP与//IP/是不同的，使用//IP格式访问服务器时会报错。

### 7，如何删除Windows连接Samba服务器记录

Win+R 或 开始菜单 + 运行，输入 "net use \* /del" 命令，按“Y”删除远程连接记录。

### 8，Windows计算机的远程控制

Samba提供了一套与Windows通信的工具。如果通过远程桌面访问Windows计算机不是一个选项，这些可以很方便，如一些示例所示。

发送关机命令与评论：

$ net rpc shutdown -C "comment" -I IPADDRESS -U USERNAME%PASSWORD

强制关机可以通过将-C注释改为单个-f来调用。对于重新启动，只能添加-r，后跟一个-C或-f。

停止并启动服务：

$ net rpc service stop SERVICENAME -I IPADDRESS -U USERNAME%PASSWORD

要查看所有可能的net rpc命令：

$ net rpc

### 9，无法启动smb服务器

检查smbd日志中出现的错误信息 或者 使用 testparm检查配置文件是否出现错误，再从新启动samba服务器。

### 10，即使使用访客权限创建Samba共享，Windows客户端仍然要求输入密码

在/etc/samba/smb.conf 文件的global部分加入以下：

**map to guest = Bad User**

### 11，无法覆盖文件，权限错误

1) 将挂载选项追加到nodfs到/etc/fstab文件中。

2) 添加 msdfs root = no 到 [global] 服务器部分 /etc/samba/smb.conf。

### 12，挂载windows的共享文件。

1，首先在windown上共享一个文件夹

2，使用mount命令挂载。【注：mount命令只能由root用户执行】

[root@centos ~]# mount -t cifs -o username=用户名,password=密码 \

> //window IP地址/共享路径 /本地挂载目录

例如：

[root@centos ~]# mount -t cifs -o username=admin,password=admin \

> //192.168.0.105/ABC /mnt

如提示以下错误：

mount error(13): Permission denied

Refer to the mount.cifs(8) manual page (e.g. man mount.cifs)

则检查挂载语法是否错误，若无错误，则在加上一个参数：

[root@centos ~]# mount -t cifs -o username=admin,password=admin,sec=ntlm \

> //192.168.0.105/ABC /mnt

13，linux系统挂载Samba共享目录报错。

出现如下错误：

mount error(13): Permission denied

Refer to the mount.cifs(8) manual page (e.g. man mount.cifs)

则有可能挂载格式错误 或者 samba版本相差太远，导致验证失败。

mount挂载格式：

mount -t cifs //<Server>/<Share> /local\_path \

> -o user=<Username>,password=<Password>

或者

mount -t cifs //<Server>/Share /local\_path \

> -o user=<domain>/<Username>,password=<Password>

注：

Server = 共享资源服务器主机名或IP地址

domain = 域名（工作组）

Share = 共享目录

Username = 可登陆Samba的用户名

Password = 密码

## 六，mount.cifs详解

mount.cifs

描述

这个工具是 cifs-utils软件包的一部分。

mount.cifs 用于挂载 CIFS 文件系统。它通常由使用"-t cifs"选项的 mount(8) 命令间接调用。

这个命令只能在支持 CIFS 文件系统的Linux内核上使用。CIFS 协议是 SMB 协议的替代版本，

它被包括 Windows 在内的几乎所有操作系统所以及 NAS(Network Attached Storage)应用和Samba服务器所支持。

mount.cifs 可以将 service 表示的 UNC 名称挂载到本地的 mount-point 挂载点上。

service 使用 //server/share 语法，其中的"server"是主机名或者 IP 地址，而 "share" 是共享名。

mount.cifs 的选项是用逗号分隔的 key=value 列表。

除了下面列出的选项外，还可以使用其他选项，只要 cifs 文件系统内核模块(cifs.ko)支持即可。

不能被 cifs 文件系统内核模块(cifs.ko)识别的选项将会被记录到内核日志中。

mount.cifs 将会引起cifs vfs启动一个名为 cifsd 的进程，并保持运行直到该资源被卸载(通常是通过 umount 工具)。

mount.cifs -V 会显示该程序的版本信息。

modinfo cifs 会显示 cifs 模块的版本信息。

选项

username=arg 用户名

指定连接时使用的用户名。如果没有在这里指定，那么将使用环境变量 USER 的值。

password=arg 密码

指定连接时使用的口令。如果没有在这里指定，那么将使用环境变量 PASSWD 的值。

如果没有在命令行参数中给出口令，mount.cifs 将会在挂载时提示用户输入口令。

需要注意的是，如果口令中含有逗号(,)，那么将不能在命令行参数中指定，因为会发生解析错误。

不过在环境变量 PASSWD 和 cred 文件(见下文)中可以安全的使用逗号，或者在提示输入口令时也可以安全的输入。

domain=arg

指定user所属的域(工作组)。

credentials=filename 凭据文件

指定一个包含用户名，或密码，或域(工作组)的文件。该文件的格式如下:

username=value

password=value

domain=value

这样做比直接在诸如 /etc/fstab 这样的共享文件中以明文方式写出密码要安全的多。请确保该cred文件的安全。

guest

不提示输入密码，而以来宾身份登录。

uid=arg

设置uid会拥有所有文件与目录，在mount文件系统时对没有提供拥有信息的服务器。uid的佱可以是用户名或数值。

没有指定时，默认为0。mount.cifs helper 必需在1.10以上版本才提供对非数值uid格式的支持。

具体参考：FILE AND DIRECTORY OWNERSHIP AND PERMISSIONS

forceuid

忽略服务器提供的文件和目录的UID信息，强制使用 uid= 选项设置的值。

更多信息参见下面的“文件和目录的属主及权限”小节。

cruid=arg

设置credentials 凭据缓存的拥有者uid. 主要用于sec=krb5.

默认为执行mount的真实进程uid。设置此参数指示回调寻找此用户拥有的凭据缓存。

gid=arg

如果被挂载的文件系统服务器没有提供文件和目录的GID信息，那么就使用这里的设置。

arg 可以是字符串形式的组名或着是数字形式的gid值。默认值是数字'0'。

更多信息参见下面的“文件和目录的属主及权限”小节。

forcegid

忽略服务器提供的文件和目录的GID信息，强制使用 gid= 选项设置的值。

更多信息参见下面的“文件和目录的属主及权限”小节。

port=num

设置将要连接的 CIFS 服务器端口。

如果 CIFS 服务器并未在该端口监听或者未指定此选项，那么将首先尝试默认的 445 端口，如果没有应答就再尝试 139 端口。

servernetbiosname=arg

指定要连接服务器的netbios name（RFC1001名称）。虽然对于挂载新的服务器很少需要，但是对于挂载一些老的(OS/2, Windows 98 Windows ME)

服务器，当通过139端口连接，不像新的服务器，不需要服务器名。一个服务器名最多15个字符并且 大小字敏感。

servern=name

与servernetbiosname 一样。

netbiosname=name

当挂载服务通过139端口时，指定RFC1001 源名称来代替客户端netbios机器名 在RFC1001 netbios会话初始化阶段。只在连接 Windows 98/ME 服务器(139端口)时才需要这个参数。

file\_mode=arg

如果服务器端不支持 CIFS Unix扩展，那么就使用这里设置的值替代默认的文件权限模式。

这里的 nnn 是八进制的权限模式，且前导零不能省略。

dir\_mode=arg //0nnn

如果服务器端不支持 CIFS Unix扩展，那么就使用这里设置的值替代默认的目录权限模式。

这里的 nnn 是八进制的权限模式，且前导零不能省略。

ip=arg

指定目标服务器的IP地址。

如果 UNC 名称中已经包含了这个信息(包括从DNS中解析得到)，就没必要在这里设置了，所以这个选项很少使用。

domain=arg

设置使用的domain域(工作组)

guest

不用提示输入密码

iocharset

指定默认以什么字符集显示路径名。如果服务器端支持Unicode字符，网络路径名将默认使用Unicode字符。。

例如在"en\_US.UTF-8"的情况下应该使用"utf8"。

如果没有指定该选项，将使用客户端内核中的 CONFIG\_NLS\_DEFAULT 值。

如果服务器端不支持Unicode字符，那么该选项就没有任何意义。

ro

只读挂载

rw

读写挂载

setuids

如果服务器端支持 CIFS Unix扩展，那么客户端将会在新建的文件/目录/设备上为本地进程设置有效UID/GID(effective uid/gid)。

如果服务器端不支持 CIFS Unix扩展，那么客户端对于新建的文件/目录/设备并不使用命令行上指定的默认UID/GID，

而是将新建文件的UID/GID缓存在本地，这就意味着文件的UID/GID在重新加载inode或者重新挂载该文件系统之后可能会发生变化。

nosetuids

不管服务器端是否支持 CIFS Unix扩展，客户端都不会在新建的文件/目录/设备(create, mkdir, mknod)上设置UID/GID。

这将导致服务器端按照默认规则设置文件/目录/设备的UID/GID(通常是连接用户的UID/GID)。

让服务器端(而不是客户端)设置UID/GID是默认行为。

如果服务器端不支持 CIFS Unix扩展，那么新建文件/目录/设备的UID/GID将显示为连接用户的UID/GID或命令行上指定的UID/GID值。

perm

客户端执行权限检查(用 vfs\_permission 函数根据 mode 和相应的操作检查 uid/gid )。这个选项是默认开启的。

注意，这是在服务器端根据连接的用户对客户端操作执行一般的 ACL 检查之外，客户端对自身操作进行的权限检查。

noperm

客户端不对自身操作进行任何权限检查。这可能会导致被挂载的服务器端文件系统被本地系统上的其他用户访问。

这个选项仅在服务器端支持 CIFS Unix扩展，但是客户端和服务器端的UID/GID并不匹配，

并且无法通过执行挂载操作的用户身份进行访问控制时才需要。

注意，这个选项并不影响在服务器端根据连接的用户对客户端操作执行一般的 ACL 检查。

dynperm

要求服务器端仅在内存中维护 UID/GID 和权限，而不将它们记录到实际的文件系统上。

这些信息可能会随时丢失(比如从缓存中重新加载inode)，

所以虽然这个选项可以让某些程序正常工作，但是其实际行为是不可预测的。

更多信息参见下面的“文件和目录的属主及权限”小节。

cache=

缓存模式。可能的值有： 详细见：CACHE COHERENCY.

none: 从不缓存文件数据

strict: 严格按照 CIFS/SMB2 协议

loose: 允许缓存丢失

directio

不对文件的 inode 数据做缓存。这样就不会对文件作内存映射(mmap)。

在某些具有快速网络连接的情况下，客户端可以从此选项中受益，

例如，需要进行超长序列读取的应用程序就不需要再次读取相同的数据，

从而可以比对读写都进行缓冲的默认行为(预读取/后台延迟写入)提供更好的性能。

该选项允许向服务器发送大于页面尺寸的写操作，

而且要求内核的 cifs.ko 模块在编译时开启了 CIFS\_EXPERIMENTAL 选项。

该选项在3.7版本后不再推荐使用，可用 cache=none代替。

strictcache

用于在strict 缓存模式转换。 在本模式下，客户端拥有Oplock Level II 锁就从缓存中读，否则从服务器中读。

作为写：客户存数据到缓存在扩展Oplock 锁情况下。否则，直接写服务器。

该选项在3.7版本后不再推荐使用，可用 cache=strict 代替。

rwpidforward

提示打开文件的进程，在对文件进行读或写时。

这会防止应用程序(如 WINE) 读或写失败，如果使用强制brlock 风格

mapchars

将7个保留字符(\:?|\*><)中的6个(不包括反斜杠)重新映射到新的字符(高于0xF000)。

这样就允许客户端可以识别 Windows POSIX 模拟层创建的包含这些保留字符的文件名。

该选项还可以用于将文件名中包含保留字符的文件系统挂载到同样禁止使用保留字符的 Samba 服务器。

注意，在使用了此选项挂载的文件系统上创建的文件可能在不使用此选项挂载的情况下无法访问。

该选项对于不支持 Unicode 的服务器没有意义。

nomapchars

不对7个保留字符做任何重新映射。这是默认值。

intr

当前尚未实现

nointr

当前尚未实现(默认值)

hard

当服务器端失去响应后访问其上文件的应用程序将被挂起。

soft

(默认值)当服务器端失去响应后访问其上文件的应用程序将收到一个错误信号而不是被挂起。

noacl

即使服务器端支持，也禁用 POSIX ACL 特性。

CIFS 客户端可以获取和设置 Samba 服务器上的 POSIX ACL(getfacl,setfacl) (samba 3.0.10 及以上)，但是可以通过该选项强制关闭。

设置 POSIX ACL 要求客户端内核的 CIFS 模块同时支持 CIFS\_XATTR 和 CIFS\_POSIX 特性.

POSIX ACL 支持可以被禁止在mount 时通过 指定noacl.

cifsacl

这个选项用于映射 CIFS/NTFS ACLs to/from linux 权限位。映射 SIDs to/from UIDs 和GIDs, 并获取与设置安全描述符。

详细参考：CIFS/NTFS ACL, SID/UID/GID MAPPING, SECURITY DESCRIPTORS

backupuid=arg

限制用户的备份，需要提供一个用户名或uid，没有默认值。

详细参考：ACCESSING FILES WITH BACKUP INTENT

backupgid=arg

限制用户组的备份，需要提供一个用户名或id,没有默认值。

See section ACCESSING FILES WITH BACKUP INTENT for more details

nocase

对路径名进行大小写无关的匹配(在服务器端支持的情况下，大小写敏感的匹配是默认值)。

ignorecase

同上

sec={none|krb5|krb5i|ntlm|ntlmi|ntlmv2|ntlmv2i}

选择安全模型:

none 尝试以空用户连接(不提供用户名)

krb5 使用 Kerberos version 5 认证

krb5i 使用 Kerberos version 5 和包签名(packet signing)认证

ntlm 使用 NTLM 口令散列认证

ntlmi 使用 NTLM 签名口令散列和包签名(packet signing)认证

ntlmv2 使用 NTLMv2 口令散列认证

ntlmv2i 使用 NTLMv2 口令散列认证和包签名(packet signing)认证

ntlmssp 使用 NTLMv2 口令散列用原始NTLMSSP消息压缩

ntlmsspi 使用 NTLMv2 口令散列用原始NTLMSSP消息压缩，和包签名(packet signing)认证

在主线内核中，3.8以前默认为sec=ntlm,从3.8开始，默认为sec=ntlmssp

如果服务器需要在协议协商时签名，就可以自动使能。/proc/fs/cifs/SecurityFlags

nobrl

不向服务器发送对 byte range lock 的请求。

对于某些不遵守 cifs 风格的 byte range lock 规范的应用程序来说，这个选项是必须的。

另一方面，目前大多数 cifs 服务器也尚未实现 advisory byte range lock 。

sfu

如果服务器端不支持 CIFS Unix扩展，那么就以兼容SFU(Services for Unix)的格式创建设备文件和管道(FIFO)文件。

也就是通过 SETFILEBITS 属性额外检查文件权限的高 10-12 位(和 SFU 的做法一样)。

而剩余的低 9 位依然可以用于描述权限(ACL)。

serverino

使用服务器提供的inode编号(连续的、文件唯一标识符)，而不使用客户端自动生成的临时inode编号。

虽然服务器的inode编号可以很轻易的分辨硬链接文件(它们的inode编号相同)并且保持稳定不变(这对某些程序很有必要)，

但是当同时挂载多个服务器端文件系统时，依然可能由于inode编号重叠而导致混乱。

而且，也有少数服务器不支持提供inode编号。如果服务器不能提供inode编号，这个选项就没有任何实际效果。

noserverino

使用客户端自动生成的临时inode编号，即使服务器提供了inode编号。这是默认值。

更多信息参见"INODE编号"小节。

nounix

强制关闭 CIFS Unix扩展。这相当于一次性关闭多个选项，

包括:POSIX ACL, POSIX lock, POSIX path, 服务器端软连接(symlink), 服务器端的 uids/gids/mode 值。

这个选项也可以用于对 CIFS Unix扩展支持有缺陷的服务器。

更多信息请参见"INODE编号"小节。

nouser\_xattr

即使服务器端支持，也不允许 getfattr/setfattr 获取和设置 xattr 。这是默认值。

rsize=num

默认网络读取尺寸(通常是 16K)。目前还不能使用比 CIFSMaxBufSize 大的值。

CIFSMaxBufSize 的默认值是 16K 并且可以在加载 cifs.ko 时，

将其设置为从 8K 到最大允许的 kmalloc 尺寸之间的任意值。

将 CIFSMaxBufSize 设为一个很大的值将会导致使用更多的内存，并且有可能在某些情况下降低性能。

使用大于127K(原始cifs协议允许的最大值)的值还需要服务器端的额外支持(比如 Samba 3.0.26 或更高版本)。

num 的最小值是 2048 ，最大值是 130048(127K)与 CIFSMaxBufSize 中的较小者。

wsize=num

默认网络写入尺寸。内核3.0.0以前允许的最大值是57344(14个4K页面)。

3.0.0以后，如果客户端与服务器端协商通过POSIX扩展提供大写，则默认为1M，最大允许为16M。

如果不是，则默认为65536，并且最大为131007.

fsc

使能本地磁盘缓存用于FS-Cache 为CIFS。这可以提高性能在低连接，高负载服务器 ，或读磁盘比读服务器快的网络。

这也减少了可扩展性，服务器的连接数减小。

但是，本地缓存并不适合所有工作负载，如：只读一次。

所以，你要仔细考虚 情况/工作负载。当前，本地磁盘缓存使能对于CIFS 文件以只读方式打开时。

注：本选项需要内核对CONFIG\_CIFS\_FSCACHE支持。还需要安装cachefilesd守护进程。

multiuser

映射用户访问服务器时去访问独立的凭据文件。默认，CIFS挂载只使用单一的用户凭据文件。

actimeo=

CIFS客户端对文件与目录的属性缓存时间。默认为1s.

noposixpaths

不使用posix风格的路径名

posixpaths

同上

prefixpath

挂载一个共享的子目录是可能的。它可以添加路径到挂载时的UNC。

vers= SMB 协议版本。可能值有：

1.0-- 典型的CIFS/SMBv1 协议。这是默认的。

2.0-- 这个SMBv2.002协议，它被初始引入是在windows vista service pack 1,windows server2008.

注：windows vista 初始版本说了一点方言(2.000)，不支持。

2.1-- 这个SMBv2.1协议由windows 7 和windows server 2008r2引入。

3.0-- 这个SMBv3.0协议由windows 8 和windows server 2012 引入。

注：当使用给定的协议时，不是所有的特性在每个版本上都是可用的。

--verbose

在挂载时输出额外的调试信息。注意，该选项必须在 -o 选项之前使用，也就是这样:

mount -t cifs //server/share /mnt --verbose -o user=username

SERVICE 的格式和分割符

通常在 service 中用正斜杠(/)作为分隔符。

由于正斜杠(/)不能用于Windows平台的文件名中，所以可以被看做"全局分割符"，并被Linux客户端无条件的转换成反斜杠(\)。

另一方面，由于POSIX标准允许在文件名中使用反斜杠(\)，所以不能自动将其转换为正斜杠(/)。

mount.cifs 将会在可以转换而不产生混淆的情况下，自动将反斜杠(\)转换成正斜杠(/)。

但是它不会将共享名(sharename)之后的路径中所包含的反斜杠(\)自动转换成正斜杠(/)。

INODE编号

如果服务器端支持Unix扩展，并且客户端也允许使用Unix扩展，那么将使用服务器实际提供的inode编号响应 POSIX 调用。

如果Unix扩展被nounix禁用(或者服务器端本身就不支持)，但同时又开启了"serverino"选项的话，那么将无法获取真正的服务器端inode编号。

此时客户端将把 server-assigned "UniqueID" 映射到一个inode编号。

UniqueID 的值和服务器端inode编号是两个不同的值。

UniqueID 的值在整个服务器范围内是唯一的，其值通常大于232(2的32次方)。

这个值通常会让不支持LFS(Large File Support)的程序触发一个 glibc EOVERFLOW 错误。

因此强烈建议你重新编译此程序，并开启LFS支持(也就是 -D\_FILE\_OFFSET\_BITS=64)，以避免这个错误。

当然，你也可以使用"noserverino"选项来客户端确保生成的inode编号小于232(2的32次方)。

但是这样做的缺点是无法正确检测到硬链接。

文件和目录的属主及权限：FILE AND DIRECTORY OWNERSHIP AND PERMISSIONS

核心 CIFS 协议并不提供文件和目录的 unix 属主或权限信息。

正因为如此，文件和目录才会看上去像被 uid= 和 gid= 选项指定的用户和组所拥有，

并且其权限才会看上去和 file\_mode 以及 dir\_mode 指定的权限一致。

可以通过 chmod/chown 来修改这些值，但是并不会在服务器端产生真正的实际效果。

如果服务器端支持Unix扩展，并且客户端也允许使用Unix扩展，文件和目录的 uid, gid, mode 将由服务器端提供。

因为 CIFS 通常由同一个用户挂载，所以不管是哪个用户访问此文件系统，所使用的 credentials 文件都是同一个。

这样，新创建的文件和目录其属主/属组就都根据同一个 credentials 文件中的连接用户来设置。

如果客户端和服务器端使用的 uid 和 gid 并不匹配，那么 forceuid 和 forcegid 选项就很有用处了。

注意，并没有强制改写 mode 的选项。

当指定了 forceuid 和/或 forcegid 后，文件和目录的权限就可能不能反映真正的权限了。

如果Unix扩展被nounix禁用(或者服务器端本身就不支持)，仍然有可能使用"dynperm"选项在服务器上模拟出来。

使用该选项后，新创建的文件和目录将看上去拥有了正确的权限。

不过这些权限并不真正存储在服务器端的文件系统上(仅在内存中)，因此可能会随时丢失(比如内核刷新了inode缓存)。

因此，我们不鼓励使用此选项。

还可以使用 noperm 选项在客户端完全越过权限检查。

但是服务器端的权限检查是无法越过的，服务器端将始终根据 credentials 文件中提供的用户信息进行权限检查，

而与客户端实际访问文件系统的用户无关。

环境变量

环境变量 USER 用于指定连接服务器的用户名。该变量也可以使用 username%password 的格式同时给出口令。

环境变量 PASSWD 用于指定连接服务器的用户密码。

环境变量 PASSWD\_FILE 用于给出读取密码的文件的路径。其中的第一行将被作为密码读取。

注意

该命令可能只允许 root 使用，除非以 setuid 安装。

在setuid的情况下，默认将开启 noexec 和 nosuid 挂载标记。

当安装为 setuid 程序后，该程序就将遵守 mount 程序对于用户挂载限制的约定。

某些 samba 客户端工具，例如 smbclient(8) ，会根据客户端的配置文件 smb.conf 中的参数决定其行为。

但是 mount.cifs 与他们不同，它完全无视 smb.conf 的内容。

配置

修改和读取 CIFS 配置、读取 CIFS 调试信息的首要途径就是 Linux 的 /proc 文件系统。

/proc/fs/cifs 目录中包含了许多配置和调试信息。

启动选项(例如最大buffer尺寸和buffer个数)只能在内核加载 cifs.ko 模块的时候指定，

它们可以通过"modinfo /path/to/cifs.ko"命令看到。

更多信息参见 Documentation/filesystems/cifs/README 文件。

缺陷

使用 CIFS URL 进行挂载目前尚未实现。

credentials 文件目前尚不能处理带有前导空格的 usernames 和 passwords