FTP：File Transfer Protocol

21/tcp:

文件共享服务：应用层，ftp

NFS: Network File System (RPC: Remote Procedure Call, 远程过程调用)

Samba: CIFS/SMB

FTP: tcp, 两个连接

命令连接，控制连接：21/tcp

数据连接:

主动模式：20/tcp

被动模式：端口随机

数据传输模式(自动模式)：

二进制：

文本：

ftp server --> ftp client

vsftpd:

/etc/vsftpd: 配置文件目录

/etc/init.d/vsftpd: 服务脚本

/usr/sbin/vsftpd: 主程序

基于PAM实现用户认证：

/etc/pam.d/\*

/lib/security/\*

/lib64/security/\*

支持虚拟用户

vsftpd: (ftp, ftp)

/var/ftp：ftp服务根目录

ftp: 系统用户，下面的三种用户都会映射为系统用户

匿名用户 --> 系统用户: anonymous\_enable

系统用户: local\_enable

虚拟用户 --> 系统用户

/var/ftp: ftp用户的家目录

匿名用户访问目录

/etc/vsftpd/vsftpd.conf：主配置文件

/usr/sbin/vsftpd：Vsftpd的主程序

/etc/rc.d/init.d/vsftpd：启动脚本

/etc/pam.d/vsftpd：PAM认证文件（此文件中file=/etc/vsftpd/ftpusers字段，指明阻止访问的用户来自/etc/vsftpd/ftpusers文件中的用户）

/etc/vsftpd/ftpusers：禁止使用vsftpd的用户列表文件。记录不允许访问FTP服务器的用户名单，管理员可以把一些对系统安全有威胁的用户账号记录在此文件中，以免用户从FTP登录后获得大于上传下载操作的权利，而对系统造成损坏。（注意：linux-4中此文件在/etc/目录下）

/etc/vsftpd/user\_list：禁止或允许使用vsftpd的用户列表文件。这个文件中指定的用户缺省情况（即在/etc/vsftpd/vsftpd.conf中设置userlist\_deny=YES）下也不能访问FTP服务器，在设置了userlist\_deny=NO时,仅允许user\_list中指定的用户访问FTP服务器。（注意：linux-4中此文件在/etc/目录下）

/var/ftp：匿名用户主目录；本地用户主目录为：/home/用户主目录，即登录后进入自己家目录

/var/ftp/pub：匿名用户的下载目录，此目录需赋权根chmod 1777 pub（1为特殊权限，使上载后无法删除）

/etc/logrotate.d/vsftpd.log：Vsftpd的日志文件

chroot: 禁锢用户于其家目录中

系统用户：

write\_enable=YES: 上传文件

文件服务权限：文件系统权限\*文件共享权限

守护进程：

独立守护：适用于访问量大，用户在线时间长的用户

瞬时守护

由xinetd代为管理

vsftpd:

max\_clients=#

max\_per\_ip=#

安全通信方式：

ftps: ftp+ssl/tls

sftp: OpenSSH, SubSystem, sftp(SSH)

vsftpd: PAM(手动定义配置文件)

匿名

本地

虚拟用户

MySQL: VSFTPD, users ： Name,Password

/etc/vsftpd/vusers: --> db\_load

USERNAME

PASSWORD

db4-utils 这个软件包提供的db\_load命令将配置文件改成二进制格式

目前为止学了三个将配置文件改成二进制格式的工具：newalias postmap db\_load

postconf -m

[root@mail ~]# yum install vsftpd -y

[root@mail ~]# rpm -ql vsftpd

/etc/logrotate.d/vsftpd.log

/etc/pam.d/vsftpd

/etc/rc.d/init.d/vsftpd

/etc/vsftpd

/etc/vsftpd/ftpusers

/etc/vsftpd/user\_list

/etc/vsftpd/vsftpd.conf

/etc/vsftpd/vsftpd\_conf\_migrate.sh

/var/ftp

/var/ftp/pub

[root@mail ~]# service vsftpd start

Starting vsftpd for vsftpd: [ OK ]

[root@mail ~]# chkconfig vsftpd on

\*匿名用户上传下载的公共目录

[root@mail ~]# cd /var/ftp/

[root@mail ftp]# ls

pub

\*用windows终端测试

C:\Users\yu>ftp 192.168.3.55

连接到 192.168.3.55。

220 (vsFTPd 2.0.5)

用户(192.168.3.55:(none)): anonymous

331 Please specify the password.

密码:

230 Login successful.

ftp> ls

200 PORT command successful. Consider using PASV.

150 Here comes the directory listing.

pub

226 Directory send OK.

ftp: 收到 5 字节，用时 0.00秒 5000.00千字节/秒。

ftp> ?

命令可能是缩写的。 命令为:

! delete literal prompt send

? debug ls put status

append dir mdelete pwd trace

ascii disconnect mdir quit type

bell get mget quote user

binary glob mkdir recv verbose

bye hash mls remotehelp

cd help mput rename

close lcd open rmdir

ftp>

\*配置文件详解

[root@mail ~]# vim /etc/vsftpd/vsftpd.conf

# 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\_ftpd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个修改

#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

# 设置是否阻扯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，编缉/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

[root@mail ~]# ftp 192.168.3.55

\*lcd客户端目录切换，方便上传下载文件指定目录

Connected to 192.168.3.55.

220 (vsFTPd 2.0.5)

530 Please login with USER and PASS.

530 Please login with USER and PASS.

KERBEROS\_V4 rejected as an authentication type

Name (192.168.3.55:root): hadoop

331 Please specify the password.

Password:

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files.

ftp> lcd /etc

Local directory now /etc

ftp> put inittab

local: inittab remote: inittab

227 Entering Passive Mode (192,168,3,55,189,245)

150 Ok to send data.

226 File receive OK.

1666 bytes sent in 9.9e-05 seconds (1.6e+04 Kbytes/s)

ftp> ls

227 Entering Passive Mode (192,168,3,55,130,228)

150 Here comes the directory listing.

-rw-r--r-- 1 500 500 532 May 07 20:11 fstab

-rw-r--r-- 1 500 500 1666 May 07 20:18 inittab

226 Directory send OK.

ftp> pwd

257 "/home/hadoop"

[root@mail ~]# cd /home/hadoop/

[root@mail hadoop]# ls

fstab inittab

\*将用户禁固在其家目录下，避免到处逛不安全

[root@mail hadoop]# vim /etc/vsftpd/vsftpd.conf

chroot\_list\_enable=YES

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

[root@mail hadoop]# vim /etc/vsftpd/chroot\_list

hadoop

[root@mail hadoop]# service vsftpd restart

Shutting down vsftpd: [ OK ]

Starting vsftpd for vsftpd: [ OK ]

[root@mail hadoop]# ftp 192.168.3.55

Connected to 192.168.3.55.

220 (vsFTPd 2.0.5)

530 Please login with USER and PASS.

530 Please login with USER and PASS.

KERBEROS\_V4 rejected as an authentication type

Name (192.168.3.55:root): hadoop

331 Please specify the password.

Password:

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files.

ftp> pwd

257 "/"

ftp> cd /etc

550 Failed to change directory.

\*禁固本地所有用户在其家目录

[root@mail ~]# vim /etc/vsftpd/vsftpd.conf

chroot\_local\_user=YES

\*用下面两项来控制谁能登陆谁不能

[root@mail vsftpd]# vim /etc/vsftpd/vsftpd.conf

\*如果没有userlist\_deny这一项，默认在userlist里面的用户都不允许

userlist\_enable=YES

userlist\_deny=YES

[root@mail vsftpd]# vim user\_list

hadoop

[root@mail vsftpd]# ftp 192.168.3.55

Connected to 192.168.3.55.

220 (vsFTPd 2.0.5)

530 Please login with USER and PASS.

530 Please login with USER and PASS.

KERBEROS\_V4 rejected as an authentication type

Name (192.168.3.55:root): hadoop

530 Permission denied.

Login failed.

\*\*\*vsftpd基于ssl的认证

[root@mail ~]# cd /etc/pki/CA

[root@mail CA]# mkdir certs newcerts crl

[root@mail CA]# touch index.txt

[root@mail CA]# echo 01 > serial

[root@mail CA]# (umask 077;openssl genrsa -out private/cakey.pem 2048)

Generating RSA private key, 2048 bit long modulus

........+++

..................+++

e is 65537 (0x10001)

[root@mail CA]# openssl req -new -x509 -key private/cakey.pem -out cacert.pem -days 3650

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [GB]:CN

State or Province Name (full name) [Berkshire]:HB

Locality Name (eg, city) [Newbury]:ZZ

Organization Name (eg, company) [My Company Ltd]:YuLiang

Organizational Unit Name (eg, section) []:Tech

Common Name (eg, your name or your server's hostname) []:ca.yuliang.com

Email Address []:

[root@mail CA]#

[root@mail CA]# mkdir /etc/vsftpd/ssl

[root@mail CA]# cd /etc/vsftpd/ssl/

[root@mail ssl]# (umask 077;openssl genrsa -out vsftpd.key 2048)

Generating RSA private key, 2048 bit long modulus

.....................................................................................................+++

.........................+++

e is 65537 (0x10001)

[root@mail ssl]# openssl req -new -key vsftpd.key -out vsftpd.csr

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [GB]:CN

State or Province Name (full name) [Berkshire]:HB

Locality Name (eg, city) [Newbury]:ZZ

Organization Name (eg, company) [My Company Ltd]:YuLiang

Organizational Unit Name (eg, section) []:ftp.yuliang.com

Common Name (eg, your name or your server's hostname) []:

[root@mail ssl]# openssl req -new -key vsftpd.key -out vsftpd.csr

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [GB]:CN

State or Province Name (full name) [Berkshire]:HB

Locality Name (eg, city) [Newbury]:ZZ

Organization Name (eg, company) [My Company Ltd]:YuLiang

Organizational Unit Name (eg, section) []:Tech

Common Name (eg, your name or your server's hostname) []:ftp.yuliang.com

Email Address []:

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:

[root@mail ssl]#

[root@mail ssl]# openssl ca -in vsftpd.csr -out vsftpd.crt

Using configuration from /etc/pki/tls/openssl.cnf

Error opening CA private key ../../CA/private/cakey.pem

8101:error:02001002:system library:fopen:No such file or directory:bss\_file.c:352:fopen('../../CA/private/cakey.pem','r

')8101:error:20074002:BIO routines:FILE\_CTRL:system lib:bss\_file.c:354:

unable to load CA private key

[root@mail ssl]#

[root@mail ssl]# vim /etc/pki/tls/openssl.cnf

[ CA\_default ]

dir = /etc/pki/CA # Where everything is kept

[root@mail ssl]# openssl ca -in vsftpd.csr -out vsftpd.crt

[root@mail ssl]# vim /etc/vsftpd/vsftpd.conf

#ssl or tls

ssl\_enable=YES

ssl\_sslv3=YES

ssl\_tlsv1=YES

allow\_anon\_ssl=NO

force\_local\_data\_ssl=YES

force\_local\_logins\_ssl=YES

rsa\_cert\_file=/etc/vsftpd/ssl/vsftpd.crt

rsa\_private\_key\_file=/etc/vsftpd/ssl/vsftpd.key

[root@mail ssl]# service vsftpd restart

Shutting down vsftpd: [ OK ]

Starting vsftpd for vsftpd: [ OK ]

\*\*\*注释掉上面的加密机制，接下来实现基于pam\_mysql认证

一、安装所需要程序

1、事先安装好开发环境和mysql数据库;

# yum -y install mysql-server mysql-devel

# yum -y groupinstall "Development Tools" "Development Libraries"

2.安装pam\_mysql-0.7RC1

# tar zxvf pam\_mysql-0.7RC1.tar.gz

# cd pam\_mysql-0.7RC1

# ./configure --with-mysql=/usr --with-openssl

# make

# make install

3.安装vsftpd

# yum -y install vsftpd

二、创建虚拟用户账号

1.准备数据库及相关表

首先请确保mysql服务已经正常启动。而后，按需要建立存储虚拟用户的数据库即可，这里将其创建为vsftpd数据库。

mysql> create database vsftpd;

mysql> grant select on vsftpd.\* to vsftpd@localhost identified by 'www.magedu.com';

mysql> grant select on vsftpd.\* to vsftpd@127.0.0.1 identified by 'www.magedu.com';

mysql> flush privileges;

mysql> use vsftpd;

mysql> create table users (

-> id int AUTO\_INCREMENT NOT NULL,

-> name char(20) binary NOT NULL,

-> password char(48) binary NOT NULL,

-> primary key(id)

-> );

2、添加测试的虚拟用户

根据需要添加所需要的用户，需要说明的是，这里将其密码采用明文格式存储，原因是pam\_mysql的password()函数与MySQL的password()函数可能会有所不同。

mysql> insert into users(name,password) values('tom','magedu');

mysql> insert into users(name,password) values('jerry','magedu');

三、配置vsftpd

1.建立pam认证所需文件

#vi /etc/pam.d/vsftpd.mysql

添加如下两行

auth required /lib/security/pam\_mysql.so user=vsftpd passwd=www.magedu.com host=localhost db=vsftpd table=users usercolumn=name passwdcolumn=password crypt=0

account required /lib/security/pam\_mysql.so user=vsftpd passwd=www.magedu.com host=localhost db=vsftpd table=users usercolumn=name passwdcolumn=password crypt=0

2.修改vsftpd的配置文件，使其适应mysql认证

建立虚拟用户映射的系统用户及对应的目录

#useradd -s /sbin/nologin -d /var/ftproot vuser

#chmod go+rx /var/ftproot

请确保/etc/vsftpd.conf中已经启用了以下选项

anonymous\_enable=YES

local\_enable=YES

write\_enable=YES

anon\_upload\_enable=NO

anon\_mkdir\_write\_enable=NO

chroot\_local\_user=YES

而后添加以下选项

guest\_enable=YES

guest\_username=vuser

并确保pam\_service\_name选项的值如下所示

pam\_service\_name=vsftpd.mysql

四、启动vsftpd服务

# service vsftpd start

# chkconfig vsftpd on

查看端口开启情况

# netstat -tnlp |grep :21

tcp 0 0 0.0.0.0:21 0.0.0.0:\* LISTEN 23286/vsftpd

使用虚拟用户登录,验正配置结果，以下为本机的命令方式测试，你也可以在其它Win Box上用IE或者FTP客户端工具登录验正

# ftp localhost

五、配置虚拟用户具有不同的访问权限

vsftpd可以在配置文件目录中为每个用户提供单独的配置文件以定义其ftp服务访问权限，每个虚拟用户的配置文件名同虚拟用户的用户名。配置文件目录可以是任意未使用目录，只需要在vsftpd.conf指定其路径及名称即可。

1、配置vsftpd为虚拟用户使用配置文件目录

# vim vsftpd.conf

添加如下选项

user\_config\_dir=/etc/vsftpd/vusers\_dir

2、创建所需要目录，并为虚拟用户提供配置文件

# mkdir /etc/vsftpd/vusers\_dir/

# cd /etc/vsftpd/vusers\_dir/

# touch tom jerry

3、配置虚拟用户的访问权限

虚拟用户对vsftpd服务的访问权限是通过匿名用户的相关指令进行的。比如，如果需要让tom用户具有上传文件的权限，可以修改/etc/vsftpd/vusers\_dir/tom文件，在里面添加如下选项即可。

anon\_upload\_enable=YES

\*\*\*NFS文件系统：

服务器端：nfs-utils

nfs: nfsd(nfs主服务), mountd(接受客户端挂载请求), quotad(限定客户端配额)

nfsd: 主服务2049/tcp, 2049/udp端口不变

mountd: 端口由rpc随机分配

quotad: 端口由rpc随机分配

半随机的

配置文件：

/etc/exports

格式：/path/to/somedir CLIENT\_LIST（多个客户之间使用空白字符分隔）

每个客户端后面必须跟一个小括号，里面定义了此客户访问特性，如访问权限等

172.16.0.0/16(ro,async) 192.16.0.0/24(rw,sync)

showmount命令：

showmount -e NFS\_SERVER: 查看NFS服务器“导出”的各文件系统

showmount -a NFS\_SERVER: 查看NFS服务器所有被挂载的文件系统及其挂载的客户端对应关系列表

showmount -d NFS\_SERVER: 显示NFS服务器所有导出的文件系统中被客户端挂载了文件系统列表

客户端使用mount命令挂载：

mount -t nfs NFS\_SERVER:/PATH/TO/SOME\_EXPORT /PATH/TO/SOMEWHRERE

文件系统导出属性：

ro:

rw:

sync:

async:

root\_squash: 将root用户映射为来宾账号；

no\_root\_squash: 保留root的权限

all\_squash:

anonuid, anongid: 指定映射的来宾账号的UID和GID；

让mountd和quotad等进程监听在固定端口，编辑配置文件/etc/sysconfig/nfs

exportfs命令：可以立即生效以免正在存的人因为重启服务而崩溃

-a：跟-r或-u选项同时使用，表示重新挂载所有文件系统或取消导出所有文件系统；

-r: 重新导出

-u: 取消导出

-v: 显示详细信息

[root@mail ~]# service nfs start

Starting NFS services: [ OK ]

Starting NFS quotas: [ OK ]

Starting NFS daemon: [ OK ]

Starting NFS mountd: [ OK ]

[root@mail ~]#

[root@mail ~]# netstat -tnlp | grep "rpc"

tcp 0 0 0.0.0.0:874 0.0.0.0:\* LISTEN 2812/rpc.statd

tcp 0 0 0.0.0.0:752 0.0.0.0:\* LISTEN 30253/rpc.mountd

tcp 0 0 0.0.0.0:720 0.0.0.0:\* LISTEN 30220/rpc.rquotad

[root@mail ~]#

\*nfs会向rpc注册申请随机端口

[root@mail ~]# rpcinfo -p localhost

program vers proto port

100000 2 tcp 111 portmapper

100000 2 udp 111 portmapper

100024 1 udp 871 status

100024 1 tcp 874 status

100011 1 udp 717 rquotad

100011 2 udp 717 rquotad

100011 1 tcp 720 rquotad

100011 2 tcp 720 rquotad

100003 2 udp 2049 nfs

100003 3 udp 2049 nfs

100003 4 udp 2049 nfs

100021 1 udp 60754 nlockmgr

100021 3 udp 60754 nlockmgr

100021 4 udp 60754 nlockmgr

100003 2 tcp 2049 nfs

100003 3 tcp 2049 nfs

100003 4 tcp 2049 nfs

100021 1 tcp 56923 nlockmgr

100021 3 tcp 56923 nlockmgr

100021 4 tcp 56923 nlockmgr

100005 1 udp 749 mountd

100005 1 tcp 752 mountd

100005 2 udp 749 mountd

100005 2 tcp 752 mountd

100005 3 udp 749 mountd

100005 3 tcp 752 mountd

\*而rpc自身的服务器端应用端口就只有下面几个

[root@mail ~]# service nfs stop

Shutting down NFS mountd: [ OK ]

Shutting down NFS daemon: [ OK ]

Shutting down NFS quotas: [ OK ]

[root@mail ~]# rpcinfo -p localhost

program vers proto port

100000 2 tcp 111 portmapper

100000 2 udp 111 portmapper

100024 1 udp 871 status

100024 1 tcp 874 status

[root@mail ~]#

\*nfs软件提供好几个服务

[root@mail ~]# rpm -ql nfs-utils | grep "init.d"

主服务：

/etc/rc.d/init.d/nfs

锁服务：为了避免多个用户同时操作一个文件导致崩溃，第一个人会向rpc申请锁，其他人不能应用

/etc/rc.d/init.d/nfslock

/etc/rc.d/init.d/rpcgssd

/etc/rc.d/init.d/rpcidmapd

/etc/rc.d/init.d/rpcsvcgssd

[root@mail ~]# mkdir /var/share

[root@mail ~]# vim /etc/exports

/var/share 192.168.3.0/24(ro,async)

[root@mail ~]# service nfs restart

\*在客户端也可以查看

[root@RHEL6 ~]# showmount -e 192.168.3.55

Export list for 192.168.3.55:

/var/share 192.168.3.0/24

[root@RHEL6 ~]#

[root@RHEL6 ~]# mount -t nfs 192.168.3.55:/var/share /media

[root@RHEL6 ~]# ls /media/

[root@RHEL6 ~]#

[root@RHEL5 ~]# cp /etc/fstab /var/share/

[root@RHEL6 ~]# ls /media/

fstab

[root@RHEL5 ~]# vim /etc/exports

/var/share 192.168.3.0/24(ro,async)

/var/log 192.168.3.0/24(ro)

[root@RHEL5 ~]# exportfs -arv

exporting 192.168.3.0/24:/var/share

exporting 192.168.3.0/24:/var/log

\*显示被客户端挂载了的

[root@RHEL5 ~]# showmount -d 192.168.3.55

Directories on 192.168.3.55:

/var/share

[root@RHEL5 ~]#

\*服务器端通过UID来标示用户，毕竟是两个主机，UID一样名字不一样被视为同一权限用户

[root@RHEL5 ~]# id hadoop

uid=500(hadoop) gid=500(hadoop) groups=500(hadoop)

[root@RHEL5 ~]# setfacl -m u:hadoop:rwx /var/share

[root@RHEL5 ~]# su - hadoop

[hadoop@RHEL5 ~]$ cd /var/share/

[hadoop@RHEL5 share]$ touch a.hadoop

[hadoop@RHEL5 share]$ ll

total 4

-rw-rw-r-- 1 hadoop hadoop 0 May 10 01:53 a.hadoop

-rw-r--r-- 1 root root 532 May 10 01:15 fstab

[root@RHEL6 ~]# groupadd -g 500 openstack

[root@RHEL6 ~]# useradd -g 500 -u 500 openstack

[root@RHEL6 ~]# ll /media/

total 4

-rw-rw-r--. 1 openstack openstack 0 May 10 01:53 a.hadoop

-rw-r--r--. 1 root root 532 May 10 01:15 fstab

[root@RHEL6 ~]#

\*默认情况下root用户是不能删除UID挂载nfs里面的文件，但是可以通过no\_root\_squash设置保留root权限

[root@RHEL6 media]# rm -rf a.hadoop

rm: cannot remove `a.hadoop': Permission denied

[root@RHEL6 media]# rm -rf fstab

rm: cannot remove `fstab': Permission denied

\*开机自动挂载nfs时，千万注意如果nfs服务器没开机，那么这边也开不了机，要用到\_rnetdev忽略才能正常启动

[root@RHEL6 media]# vim /etc/fstab

192.168.3.55:/var/share /media nfs defaults,\_rnetdev 0 0

\*让mountd和quotad等进程监听在固定端口，编辑配置文件/etc/sysconfig/nfs

[root@RHEL6 media]# vim /etc/sysconfig/nfs

RQUOTAD\_PORT=875

LOCKD\_TCPPORT=32803

LOCKD\_UDPPORT=32769

MOUNTD\_PORT=892

Samba应用：

**一、简介**

　　Samba是一个能让Linux系统应用Microsoft网络通讯协议的软件，而SMB是Server Message Block的缩写，即为服务器消息块 ，SMB主要是作为Microsoft的网络通讯协议，后来Samba将SMB通信协议应用到了Linux系统上，就形成了现在的Samba软件。后来微 软又把 SMB 改名为 CIFS（Common Internet File System），即公共 Internet 文件系统，并且加入了许多新的功能，这样一来，使得Samba具有了更强大的功能。

　　Samba最大的功能就是可以用于Linux与windows系统直接的文件共享和打印共享，Samba既可以用于windows与Linux 之间的文件共享，也可以用于Linux与Linux之间的资源共享，由于NFS(网络文件系统）可以很好的完成Linux与Linux之间的数据共享，因 而 Samba较多的用在了Linux与windows之间的数据共享上面。

　　SMB是基于客户机/服务器型的协议，因而一台Samba服务器既可以充当文件共享服务器，也可以充当一个Samba的客户端，例如，一台在 Linux 下已经架设好的Samba服务器，windows客户端就可以通过SMB协议共享Samba服务器上的资源文件，同时，Samba服务器也可以访问网络中 其它windows系统或者Linux系统共享出来的文件。  
Samba在windows下使用的是NetBIOS协议，如果你要使用Linux下共享出来的文件，请确认你的windows系统下是否安装了NetBIOS协议。

　　组成Samba运行的有两个服务，一个是SMB，另一个是NMB；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；而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。

　　例如，某台Samba服务器的IP地址为10.0.0.163，对应的工作组名称为davidsamba，那么在Windows的IE浏览器输入下面两条指令都可以访问共享文件。其实这就是Windows下查看Linux Samba服务器共享文件的方法。  
　　\\10.0.0.163\共享目录名称  
　　\\davidsamba\共享目录名称

　　Samba服务器可实现如下功能：WINS和DNS服务； 网络浏览服务； Linux和Windows域之间的认证和授权； UNICODE字符集和域名映射；满足CIFS协议的UNIX共享等。

**二、系统环境**

系统平台：CentOS release 6.3 (Final)

Samba版本：samba-3.5.10-125.el6.x86\_64

Samba Server IP：10.0.0.163

防火墙已关闭/iptables: Firewall is not running.

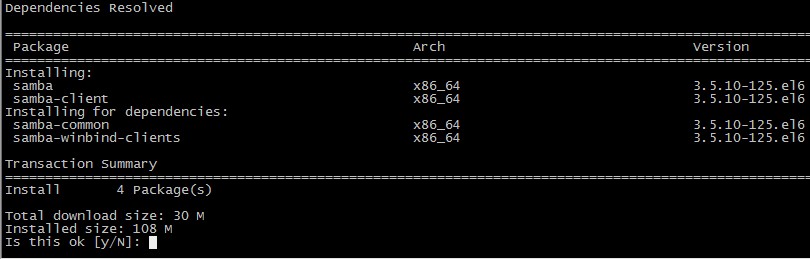
SELINUX=disabled

**三、安装Samba服务**

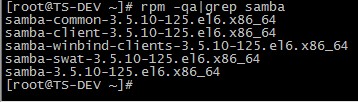
1、在可以联网的机器上使用yum工具安装，如果未联网，则挂载系统光盘进行安装。

# yum install samba samba-client samba-swat

有依赖关系的包samba-common、samba-winbind-clients、libsmbclient将自动安装上去。



2、查看安装状况



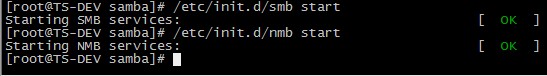
3、安装包说明

samba-common-3.5.10-125.el6.x86\_64               //主要提供samba服务器的设置文件与设置文件语法检验程序testparm  
samba-client-3.5.10-125.el6.x86\_64                    //客户端软件，主要提供linux主机作为客户端时，所需要的工具指令集  
samba-swat-3.5.10-125.el6.x86\_64                    //基于https协议的samba服务器web配置界面  
samba-3.5.10-125.el6.x86\_64                            //服务器端软件，主要提供samba服务器的守护程序，共享文档，日志的轮替，开机默认选项

Samba服务器安装完毕，会生成配置文件目录/etc/samba和其它一些samba可执行命令工具，/etc/samba/smb.conf是samba的核心配置文件，/etc/init.d/smb是samba的启动/关闭文件。

4、启动Samba服务器

可以通过/etc/init.d/smb start/stop/restart来启动、关闭、重启Samba服务，启动SMB服务如下所示：



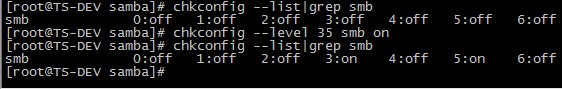
5、查看samba的服务启动情况

# service smb status

http://pic002.cnblogs.com/images/2012/370046/2012121414260339.jpg

6、设置开机自启动

# chkconfig --level 35 smb on             //在3、5级别上自动运行samba服务



**四、配置Samba服务**

Samba的主配置文件为/etc/samba/smb.conf

主配置文件由两部分构成

* Global Settings (55-245行)

　　该设置都是与Samba服务整体运行环境有关的选项，它的设置项目是针对所有共享资源的。

* Share Definitions （246-尾行）

　　该设置针对的是共享目录个别的设置，只对当前的共享资源起作用。

**全局参数：**

#==================Global Settings ===================  
[global]

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=@pega  
表示容许来自pega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。  
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。

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 script = %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  
   
**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 =david，sandy（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 = david，@dave，@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 = david，@dave

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”。  
   
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

Samba安装好后，使用testparm命令可以测试smb.conf配置是否正确。使用testparm –v命令可以详细的列出smb.conf支持的配置参数。

默认的smb.conf有很多个选项和内容，比较繁琐，这里我们按照案例来讲解配置选项，先备份一下自己的smb.conf文件，然后重新建立一个smb.conf。

# cp -p /etc/samba/smb.conf    /etc/samba/smb.conf.orig

**案例一**、公司现有一个工作组workgroup，需要添加samba服务器作为文件服务器，并发布共享目录/share，共享名为public，此共享目录允许所有员工访问。

a. 修改samba的主配置文件如下：

[复制代码](javascript:void(0);)

#======================= Global Settings =====================================

[global] //该设置与Samba服务整体运行环境有关，它的设置项目针对所有共享资源

# ----------------------- Network Related Options -------------------------

#

# workgroup = NT-Domain-Name or Workgroup-Name, eg: MIDEARTH

#

# server string is the equivalent of the NT Description field

#

# netbios name can be used to specify a server name not tied to the hostname

workgroup = WORKGROUP //定义工作组，也就是windows中的工作组概念

server string = David Samba Server Version %v //定义Samba服务器的简要说明

netbios name = DavidSamba //定义windows中显示出来的计算机名称

# --------------------------- Logging Options -----------------------------

#

# Log File let you specify where to put logs and how to split them up.

log file = /var/log/samba/log.%m //定义Samba用户的日志文件，%m代表客户端主机名

//Samba服务器会在指定的目录中为每个登陆主机建立不同的日志文件

# ----------------------- Standalone Server Options ------------------------

#

# Scurity can be set to user, share(deprecated) or server(deprecated)

security = share //共享级别，用户不需要账号和密码即可访问

#============================ Share Definitions ==============================

[public] //设置针对的是共享目录个别的设置，只对当前的共享资源起作用

comment = Public Stuff //对共享目录的说明文件，自己可以定义说明信息

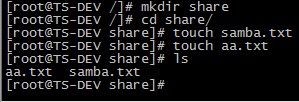
path = /share //用来指定共享的目录，必选项

public = yes //所有人可查看,等效于guest ok = yes

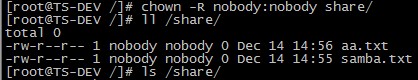
[复制代码](javascript:void(0);)

b. 建立共享目录

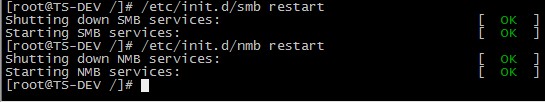
上面设置了共享目录为/share，下面就需要建立/share目录：



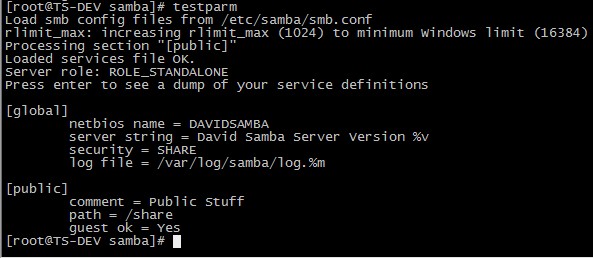
由于要设置匿名用户可以下载或上传共享文件，所以要给/share目录授权为nobody权限。



c. 重启smb服务

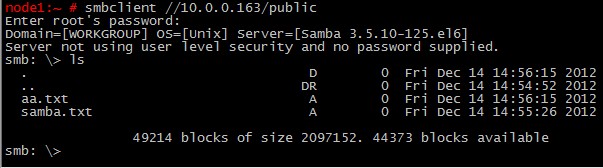


d. 测试smb.conf配置是否正确

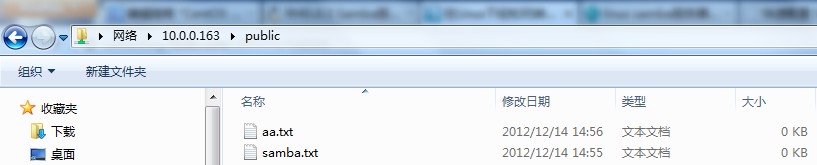


e. 访问Samba服务器的共享文件

* 在Linux下访问Samba服务器的共享文件

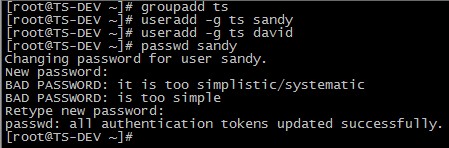


* 在windows下访问Samba服务器的共享文件



**案例二**、公司现有多个部门，因工作需要，将TS部的资料存放在samba服务器的/ts 目录中集中管理，以便TS人员浏览，并且该目录只允许TS部员工访问。

a. 添加TS部组和用户

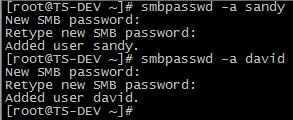


建立用户的同时加入到相应的组中的方式：useradd -g 组名 用户名

b. 在根目录下建立/ts 文件夹



c. 将刚才建立的两个帐户添加到samba的账户中



d. 修改主配置文件如下：

[复制代码](javascript:void(0);)

#======================= Global Settings =====================================

[global]

# ----------------------- Network Related Options -------------------------

#

# workgroup = NT-Domain-Name or Workgroup-Name, eg: MIDEARTH

#

# server string is the equivalent of the NT Description field

#

# netbios name can be used to specify a server name not tied to the hostname

workgroup = WORKGROUP

server string = David Samba Server Version %v

netbios name = DavidSamba

# --------------------------- Logging Options -----------------------------

#

# Log File let you specify where to put logs and how to split them up.

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

# ----------------------- Standalone Server Options ------------------------

#

# Scurity can be set to user, share(deprecated) or server(deprecated)

security = user //用户级别，由提供服务的Samba服务器负责检查账户和密码

#============================ Share Definitions ==============================

[homes] //设置用户宿主目录

comment = Home Directories

browseable = no

writable = yes

; valid users = %S

; valid users = MYDOMAIN\%S

[public]

comment = Public Stuff

path = /share

public = yes

[ts] //ts 组目录，只允许ts组成员访问

comment = TS

path = /ts

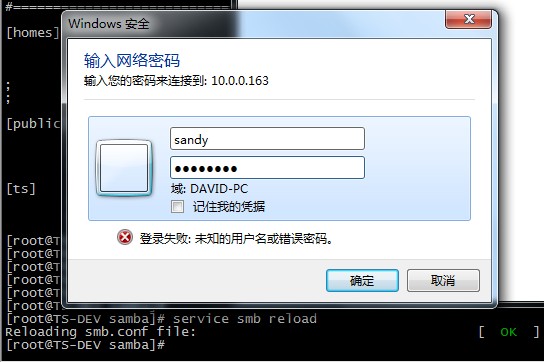
valid users = @ts

[复制代码](javascript:void(0);)

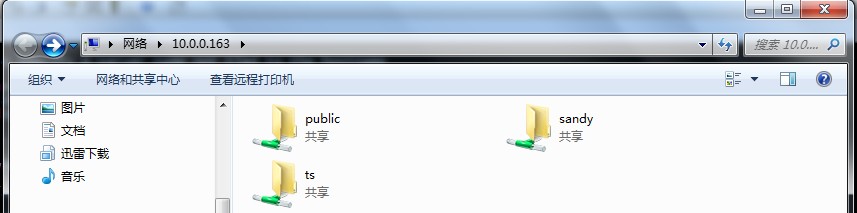
e. 重新加载配置

http://pic002.cnblogs.com/images/2012/370046/2012121712045822.jpg

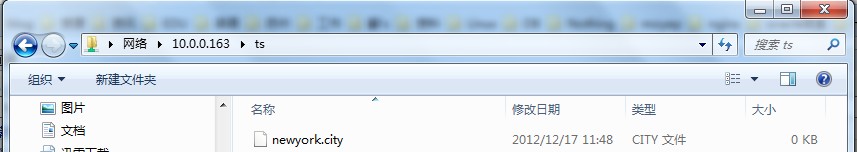
f. 到windows客户端验证，访问\\10.0.0.163，提示输入用户名和密码，在此输入sandy验证，如下图：



g. 访问成功，可以看到公共的public目录，用户sandy的宿主目录，和其有权限访问的ts目录



h. 进入ts目录，有刚才创建的newyork.city文件



**案例三**、实现不同的用户访问同一个共享目录具有不同的权限，便于管理和维护。基本上能满足一些企业用户的需求。（整理自网络）

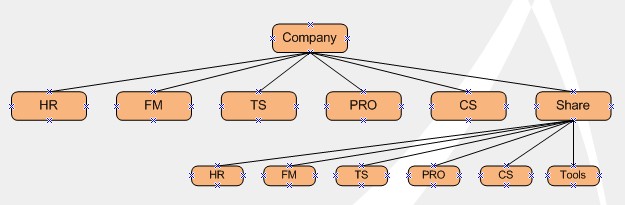
a. 需求

1. 某公司有5个大部门，分别为：人事行政部（HR & Admin Dept）、财务部（Financial Management Dept）、技术支持部（Technical Support Dept）、项目部（Project Dept）、客服部（Customer Service Dept）。  
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新建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各部门共享文件的文件夹。  
5. 对于各部门自己的文件夹，各部门管理员具有完全控制权限，而各部门普通用户可以在该部门文件夹下新建文件及文件夹，并且对于自己新建的文件及文件夹有完全控制权限，对于管理员新建及上传的文件和文件夹只能访问，不能更改和删除。不是本部门用户不能访问本部门文件夹。  
6. 对于公用文件夹中的各部门共享文件夹，各部门管理员具有完全控制权限，而各部门普通用户可以在该部门文件夹下新建文件及文件夹，并且对于自己新建的文件及 文件夹有完全控制权限，对于管理员新建及上传的文件和文件夹只能访问，不能更改和删除。本部门用户（包括管理员和普通用户）在访问其他部门共享文件夹时， 只能查看不能修改删除新建。对于存放工具的文件夹，只有管理员有权限，其他用户只能访问。

b. 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、 FM、TS、PRO、CS和Share。在Share下又有以下几个文件夹：HR、FM、TS、PRO、CS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。  
   FM管理员账号：fmadmin；普通用户账号：fmuser。  
   TS管理员账号：tsadmin；普通用户账号：tsuser。  
   PRO管理员账号：proadmin；普通用户账号：prouser。  
   CS管理员账号：csadmin；普通用户账号：csuser。  
   Tools管理员账号：admin。

文件夹之间的关系见下图：



c. 新建用户

使用useradd命令新建系统账户，然后再使用smbpasswd –a建立SMB账户。

[复制代码](javascript:void(0);)

[root@TS-DEV ~]# useradd -s /sbin/nologin hradmin

[root@TS-DEV ~]# useradd -g hradmin -s /sbin/nologin hruser

[root@TS-DEV ~]# useradd -s /sbin/nologin fmadmin

[root@TS-DEV ~]# useradd -g fmadmin -s /sbin/nologin fmuser

[root@TS-DEV ~]# useradd -s /sbin/nologin tsadmin

[root@TS-DEV ~]# useradd -g tsadmin -s /sbin/nologin tsuser

[root@TS-DEV ~]# useradd -s /sbin/nologin proadmin

[root@TS-DEV ~]# useradd -g proadmin -s /sbin/nologin prouser

[root@TS-DEV ~]# useradd -s /sbin/nologin csadmin

[root@TS-DEV ~]# useradd -g csadmin -s /sbin/nologin csuser

[root@TS-DEV ~]# useradd -s /sbin/nologin admin

[root@TS-DEV ~]#

[root@TS-DEV ~]# smbpasswd -a hradmin

New SMB password:

Retype new SMB password:

Added user fmuser.

[root@TS-DEV ~]# smbpasswd -a hruser

[root@TS-DEV ~]# smbpasswd -a fmadmin

[root@TS-DEV ~]# smbpasswd -a fmuser

[root@TS-DEV ~]# smbpasswd -a tsadmin

[root@TS-DEV ~]# smbpasswd -a tsuser

[root@TS-DEV ~]# smbpasswd -a proadmin

[root@TS-DEV ~]# smbpasswd -a prouser

[root@TS-DEV ~]# smbpasswd -a csadmin

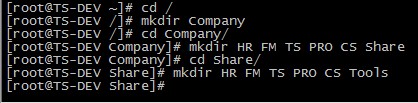
[root@TS-DEV ~]# smbpasswd -a csuser

[root@TS-DEV ~]# smbpasswd -a admin

[root@TS-DEV ~]#

[复制代码](javascript:void(0);)

d. 新建目录



e. 更改目录属性

[root@TS-DEV Company]# chown hradmin.hradmin HR

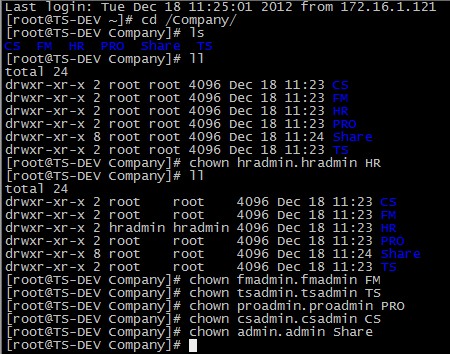
[root@TS-DEV Company]# chown fmadmin.fmadmin FM

[root@TS-DEV Company]# chown tsadmin.tsadmin TS

[root@TS-DEV Company]# chown proadmin.proadmin PRO

[root@TS-DEV Company]# chown csadmin.csadmin CS

[root@TS-DEV Company]# chown admin.admin Share



[root@TS-DEV Company]# cd Share/

[root@TS-DEV Share]# chown hradmin.hradmin HR && chown fmadmin.fmadmin FM && chown tsadmin.tsadmin TS && chown proadmin.proadmin PRO && chown csadmin.csadmin CS && chown admin.admin Tools

[root@TS-DEV Share]# chmod 1775 HR FM TS PRO CS



f. 配置samba如下：

[复制代码](javascript:void(0);)

#======================= Global Settings =====================================

[global]

# ----------------------- Network Related Options -------------------------

#

# workgroup = NT-Domain-Name or Workgroup-Name, eg: MIDEARTH

#

# server string is the equivalent of the NT Description field

#

# netbios name can be used to specify a server name not tied to the hostname

workgroup = WORKGROUP

server string = David Samba Server Version %v

netbios name = DavidSamba

# --------------------------- Logging Options -----------------------------

#

# Log File let you specify where to put logs and how to split them up.

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

max log size = 50

# ----------------------- Standalone Server Options ------------------------

#

# Scurity can be set to user, share(deprecated) or server(deprecated)

security = user

passdb backend = tdbsam

#============================ Share Definitions ==============================

[HR]

comment = This is a directory of HR.

path = /Company/HR/

public = no

admin users = hradmin

valid users = @hradmin

writable = yes

create mask = 0750

directory mask = 0750

[FM]

comment = This is a directory of FM.

path = /Company/FM/

public = no

admin users = fmadmin

valid users = @fmadmin

writable = yes

create mask = 0750

directory mask = 0750

[TS]

comment = This is a directory of TS.

path = /Company/TS/

public = no

admin users = tsadmin

valid users = @tsadmin

writable = yes

create mask = 0750

directory mask = 0750

[PRO]

comment = This is a PRO directory.

path = /Company/PRO/

public = no

admin users = proadmin

valid users = @proadmin

writable = yes

create mask = 0750

directory mask = 0750

[CS]

comment = This is a directory of CS.

path = /Company/CS/

public = no

admin users = csadmin

valid users = @csadmin

writable = yes

create mask = 0750

directory mask = 0750

[Share]

comment = This is a share directory.

path = /Company/Share/

public = no

valid users = admin,@hradmin,@fmadmin,@tsadmin,@proadmin,@csadmin

writable = yes

create mask = 0755

directory mask = 0755

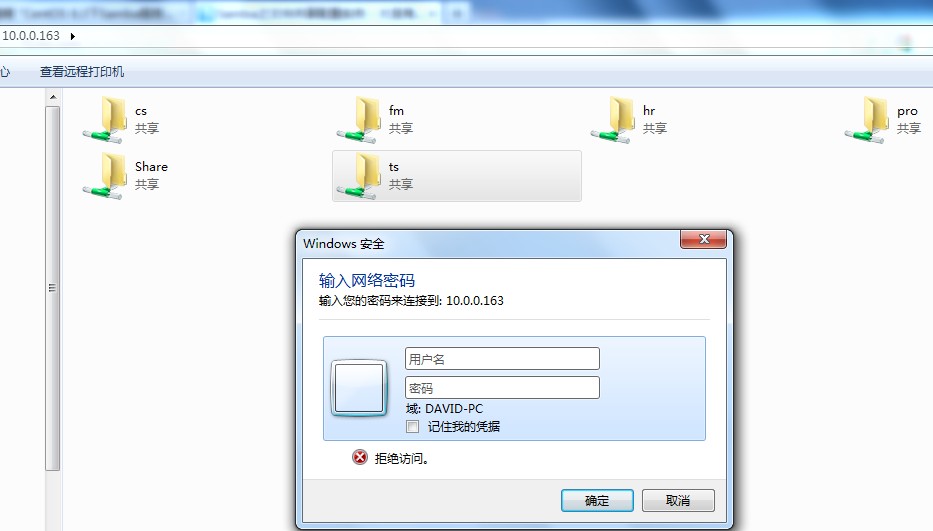
[复制代码](javascript:void(0);)

g. 测试

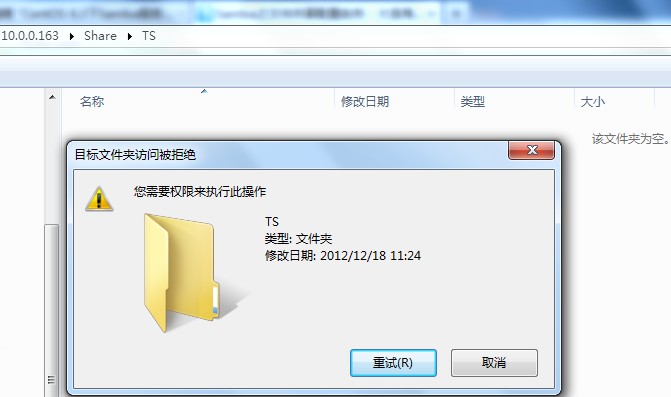
以 hradmin登录系统



试图访问ts部门文件夹，要求输入用户名及密码



试图在\\10.0.0.163\Share\TS下新建文件



在自己部门所属文件夹下新建成功



其他测试自行完成。

配置完毕。

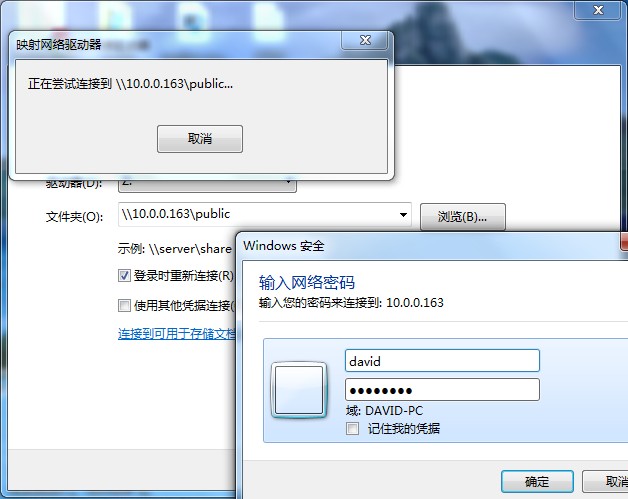
**五、将共享目录映射成Windows的驱动器**

将Samba共享的public目录，映射成 Windows 的一个驱动器盘符：

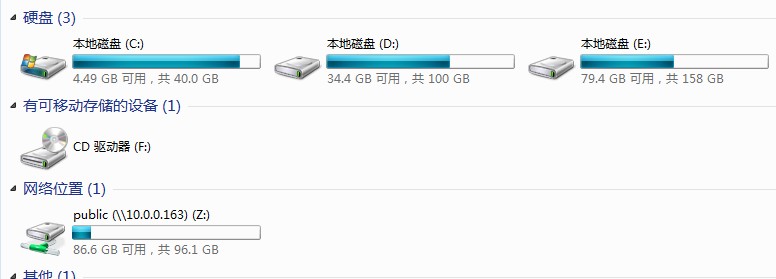
a. 右击“计算机”-->“映射网络驱动器”



b. 在文件夹栏输入共享地址及路径，点击“完成”输入用户名和密码



c. 映射完毕后，打开资源管理器可以看到映射的共享目录



***Tips：***

在windows下通过“\\ip地址”的方式访问其它文件资源时，一般第一次需要输入密码，以后就无需输入密码直接登陆了，那么如果我们要切换到其它Samba用户怎么办呢？可以在windows下执行如下指令实现：  
首 先通过开始-->运行-->cmd 输入：“net use”命令查看现有的连接，然后执行“net use \\Samba服务器IP地址或者netbios名称\ipc$  /del”，删除Samba服务器已经建立的连接。或者执行“net use \* /del”将现在所有的连接全部删除。最后，再次执行“\\ip地址”时，就可以切换用户了。  
  
**六、Linux客户端访问操作**

上面介绍了windows客户端访问Samba服务器的操作，那么在Linux作为客户端时，查看其它Linux Samba服务器共享的文件时，应该如何操作呢？

这就要用到smbclient这个工具，系统默认自带了这个命令，Smbclient常见用法介绍如下：

1、查看Samba服务器的共享资料

# smbclient  –L  //Samba服务器的ip地址  -U  Samba用户名

 “-L”即为list的含义，“-U”是user的意思，如果Samba服务器是无密码访问的话，可以省略“-U  Samba用户名”。

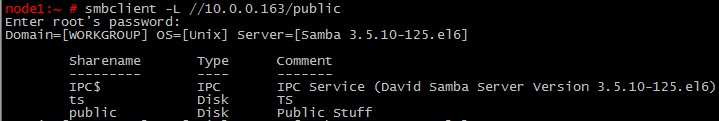
例如：samba需要密码登陆时，查看共享方法如下：

# smbclient  -L //10.0.0.163/public –U david



Samba无密码访问时，执行如下命令：

# smbclient  -L //10.0.0.163/public



password: 直接回车即可。

2、登陆Samba服务器

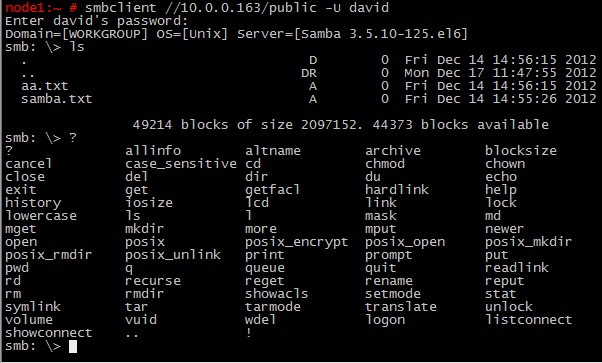
如果需要在Linux客户端登陆Samba服务器，用法如下：

# smbclient  //Samba服务器的ip地址  -U  Samba用户名

请看下面执行的操作：

# smbclient //10.0.0.163/public -U david

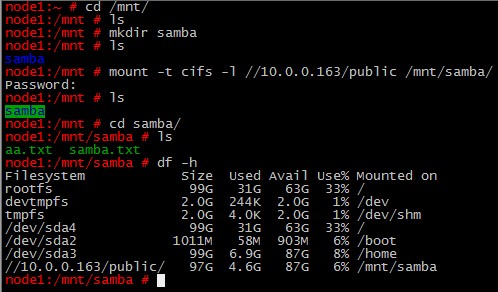
smb: \> ?                     //在这里输入?即可查看在smb命令行可用的所有命令。



操作过程与登陆FTP服务器很类似，登陆Samba服务器后，就可以进行文件的上传与下载，如果有足够的权限，还可以进行修改文件操作。

此外，Samba服务器共享出来的文件还可以在Linux客户端进行挂载，这就要用到mount命令，如下所示：

# mount -t cifs -l //10.0.0.163/public /mnt/samba/



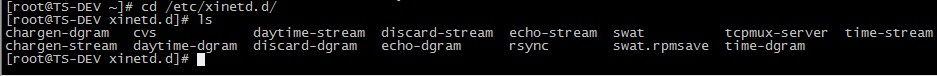
**七、Samba Web管理工具 SWAT**

SWAT(Samba WEB Administration Tool) 是通过浏览器对 Samba 进行管理的工具之一。通过 SWAT，可以在 Samba 允许访问范围内的客户端，用浏览器对服务端的 Samba 进行控制。在线文档的阅览、smb.conf 的确认和编辑，以及密码的变更、服务的重启等等都可以通过 SWAT 来完成，它的直观让 Samba 变得温和化，对那些不喜欢文本界面管理服务器的朋友来说，是一个强大的工具。

swat工具嵌套在xinetd超级守护进程中，要通过启用xinetd进程来启用swat。因此要先安装xinetd工具包，然后安装swat工具包。上面已经安装过samba-swat-3.5.10-125.el6.x86\_64，这里不再赘述。

1、配置swat

因为swat是xinetd超级守护进程的一个子进程，所以swat工具配置文件在xinetd目录中。我们要设置swat配置文件，开启此子进程，以便在启用xinetd进程是来启用swat。swat配置文件在/etc/xinetd.d目录中。



打开并编辑 /etc/xinetd.d/swat

[复制代码](javascript:void(0);)

# default: off

# description: SWAT is the Samba Web Admin Tool. Use swat \

# to configure your Samba server. To use SWAT, \

# connect to port 901 with your favorite web browser.

service swat

{

port = 901 //swat默认使用tcp的901端口, 可以修改

socket\_type = stream //通过web来配置samba, 默认使用root账号进入, 可以修改成其他的系统用户

wait = no

only\_from = 127.0.0.1   
 only\_from = 10.0.0.0 //添加此行, 将“only\_from=127.0.0.1”改成“only\_from=10.0.0.0”, 只允许内网范围对SWAT进行访问

user = root

server = /usr/sbin/swat //swat的执行程序默认在/usr/sbin目录下

log\_on\_failure += USERID

disable = yes //将“disable=yes”改成“disable=no”, 这样swat子进程就可以随xinetd超级守护进程一起启动了

}

[复制代码](javascript:void(0);)

2、启动 swat

因为swat是xinetd的子进程，所以只要启用了xinetd，那么swat也就会伴随xinetd启动。

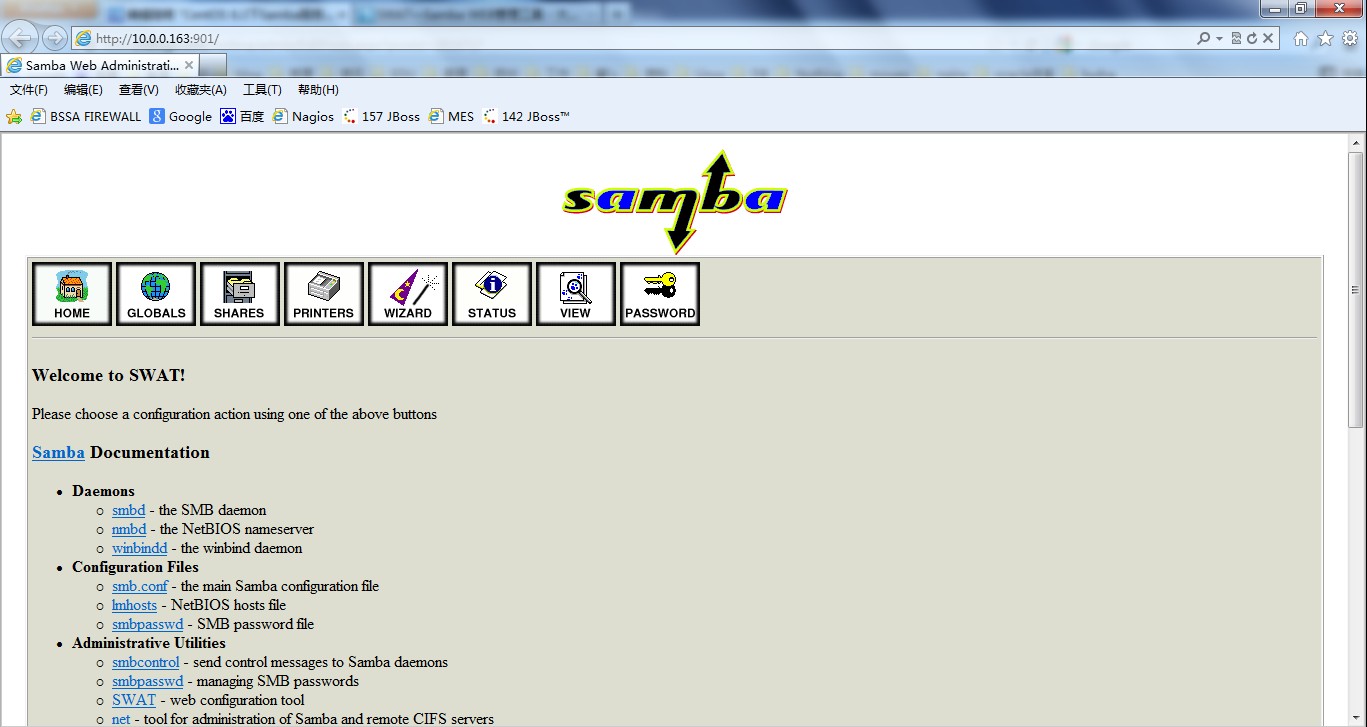
http://pic002.cnblogs.com/images/2012/370046/2012121813431439.jpg

3、打开 swat

在服务端启动 swat后，我们就可以通过 swat允许范围内的客户机的浏览器中，通过 http://服务器的内网IP:901 来访问服务端的 swat了，输入 root用户的用户名及密码进入 swat的管理首页，如下所示：



swat管理中心的首页



通过 swat管理 Samba 与直接修改 smb.conf 的方式，在本质上并无差异，但通过浏览器访问的方式，可以使 Samba 的管理更加温和化，更加适用于不擅长使用文本界面、直接修改配置文件的朋友。

4、通过swat配置samba

在swat页面我们可以看到有8个选项，每个选项可以配置samba的不同功能。

HOME：Samba相关程序及文件说明。

GLOBALS：设置Samba的全局参数。即smb.conf文件的[global]。

SHARES：设置Samba的共享参数。

PRINTERS：设置Samba的打印参数。

WIZARD：Samba配置向导。

STATUS：查看和设置Samba的服务状况。

VIEW：查看Samba的文本配置文件，即smb.conf。

PASSWORD：设置Samba用户，可以修改密码，新建删除用户。