

Linux Samba 配置说明以及实验文档

Samba 配置文件常用详解

Samba 的主配置文件叫 `smb.conf`,

可以用 `rpm -ql samba` 查看文件都安装到了那里咯!

默认主配置在 `/etc/samba/` 目录下。这个目录下还存放着我们稍后用密码访问时的口令文件。

`smb.conf` 含有多个段, 每个段由段名开始, 直到下个段名。每个段名放在方括号中间。配置文件中一行一个段名和参数, 段名和参数名不分大小写。

除了 `[global]` 段外, 所有的段都可以看作是一个共享资源。段名是该共享资源的名字, 段里的参数是该共享资源的属性。

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。

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。

`printcap name = /etc/printcap`

//此项是用来设置开机时自动加载的打印机配置文件名称和路径

`load printers = yes`

//表示是否容许打印机中的所有打印机, 在开机时自动加载浏览列表, 以支持客户端的浏览功能

`printing = cups`

//此项用来指定打印系统的类型

; `guest account = pcguest`

//此项默认不使用, 它是用来设置 Guest 帐号名

`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，也可以用一段网段表示。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 nmbd 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 用户必须先系统是系统用户。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。

; password server = <NT-Server-Name>

//此项功能在默认的配置下不使用, 而且只有在上个选项设置为 “security=server” 时才生效, 它是用来指定密码服务的名称, 所以要使用 NETBIOS 名称, 也可以使用 “password server=*” 的方式来自动寻找可用的域控制器

; password level = 8

//这个选项是为了避免 SAMBA 服务器和客户端之间容许密码大写位数不同而产生的错误

; username level = 8

//这个选项是为了避免 SAMBA 服务器和客户端之间容许帐号大写位数不同而产生的错误

encrypt passwords = yes

//此项表示是否指定用户密码以加密的形态发送到 SAMBA 服务器

smb passwd file = /etc/samba/smbpasswd

//SAMBA 服务器使用的密码文件路径

; ssl CA certFile = /usr/share/ssl/certs/ca-bundle.crt

//它用来指定包含所有受信任 CA 名称的文件

unix password sync = Yes

// 此项是用来把 SAMBA 密码文件中的加密内容修改时, 可以使用此选项进行同步

passwd program = /usr/bin/passwd %u

//此项用来指定设置 UNIX 帐号密码的程序, 其中%U 表示用户名称

passwd chat = *New*password* %n\n *Retype*new*password* %n\n *passwd:*all*authentication*tokens*updated*successfully*

//此项用来设置用户在进行 Linux 密码转换成 SAMBA 服务器密码时, 屏幕出现的指示字符串, 以及与用户产生交互窗口

pam password change = yes

//此项表示可以使用 PAM 来修改 SMB 客户端的密码, 而不使用 “passwd program” 选项中指定的程序

```

; username map = /etc/samba/smbusers
    //此选项指定一个配置文件，在此文件中包含客户端与服务端上的用户对应数据
; include = /etc/samba/smb.conf.%m
//此选项容许 SAMBA 服务器使用其他的配置文件
; obey pam restrictions = yes
    //此项可以决定是否采用 PAM 帐号及会话管理的指令
    socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
    //这个选项在编写 TCP/IP 程序时相当重要，因为可以借此调整 SAMBA 服务器运行时的效率
; interfaces = 192.168.12.2/24 192.168.13.2/24
//此项可以使 SAMBA 服务器监视多个往来接口，如果服务器上有多张网卡应该配置此项
在配置时可以写成：
interfaces =eth0
interfaces =172.17.4.150
; remote announce = 192.168.1.255 192.168.2.44
    //此项容许 NMBD 定期公布 SAMBA 服务器的 IP 地址和群组名称到远程的网络或主机
#===== Share Definitions =====

[homes]                                //用户个日的主目录设置内容
    comment = Home Directories        //主目录注释
    browseable = no                   //是否容许其他用户浏览个人主目录
    writable = yes                    //是否容许写入个人目录
    valid users = %S                  //容许登陆的用户，%S 表示当前登陆的用户
    create mode = 0664                //新建文件的默认权限
    directory mode = 0775             //新建目录的默认权限
; map to guest = bad user
    //当用户输入不正确的帐号和密码时，可以利用“map to guest”选项来设置处理的方式，
    但是必须把前面的“security”选项设为“user”“server”“domain”
设置项
说明
user
拒绝访问
server
如果帐号正确，但密码错误，容许以 Guest 登陆
domain
如果帐号和密码都错误，还是容许以 Guest 登陆
; [netlogon]                           //登陆网域时的“netlogon”目录设置内容
; comment = Network Logon Service     //主目录注释
; path = /usr/local/samba/lib/netlogon //实际访问资源的本机路径
; guest ok = yes                       //连接时是否需要密码
; writable = no                        //是否容许写入此目录
; share modes = no                     //是否容许目录中的文件在不同的用户之间共享
;[Profiles]                           //用户配置文件目录设置内容

```



```

;    path = /usr/local/samba/profiles           //实际访问资源的本机路径
;    browseable = no                           //是否容许浏览此主目录
;    guest ok = yes                             //连接时是否需要密码
[printers]                                     //设置打印机环境内容
    comment = All Printers                     //打印机注解
    path = /var/spool/samba                     //打印队列路径
    public=yes                                 //是否容许 Guest 打印
    browseable = no                           //是否容许浏览打印机内的暂时存盘内容
    guest ok = no                             //连接时是否不需要密码
    writable = no                             //是否容许写入此目录
wins support = yes //设置将 samba 服务器作为 wins 服务器，默认不使用
    //wins 服务器由微软开发，功能是将 NetBIOS 名称转换为对应的 ip 地址
    username map = /etc/samba/smbusers //去掉前面的;号，用于用户映射
    然后编辑文件/etc/samba/smbusers，将需要映射的用户添加进去，格式为
    单独的 linux 用户 = 要映射的 windows 用户列表
    例： test = alarm back //test 用户对应 windows 下的 alarm 和 back 两个用户
    encrypt password = yes 或 no //yes 表示采用加密方式发送密码，no 为不采用
    若此项为 no,则 windows 系统必须响应的修改注册表项，注册表文件存放在
    /usr/share/doc/samba-2.2.7a/docs/Registry 下
[homes] //设置共享目录
    comment = Home Directories //简要说明
    browseable = no //是否允许用户浏览所有人的主目录
    writable = yes //是否允许用户写入自己的主目录
[share] //设置一个共享目录
    comment = Samba's share Directory //简要说明
    read list = test //只读用户或组
    write list = @share //可写用户或组
    path = /home/share //共享文件夹目录路径
    //设置共享目录后需要做以下操作
    1.root 登录，使用命令 groupadd share 建立 share 组，并用 usermod -g share abc 命令将
    abc 用户添加到 share 组
    2.mkdir /home/share 在/home 下建立目录 share
    3.chown :share /home/share 设置 share 目录所属组为 share 组，chmod 777 /home/share 设
    置 share 组对该目录有最大权限
    :wq //保存退出
    #testparm //测试 smb.conf 文件是否有语法错误
    #su - //切换 root 用户
    #service smb start restart stop //启动 重启 停止 samba 服务器
    #ntsysv //设置 samba 服务器开机启动
对于此选项要很小心-它可能带来一些想不到的事情。
; case sensitive = no
[homes]
comment = Home Directories
browseable = no

```

writable = yes

valid users = %S

create mode = 0664

directory mode = 0775

如果不要 samba 不承认已经映射为 guest 的用户，可用如下设置

; map to guest = bad user

如果想创建 netlogon 目录给域登录，不要注释下面的内容。

:[netlogon]

; comment = Network Logon Service

; path = /usr/local/samba/lib/netlogon

; guest ok = yes

; writable = no

; share modes = no

想提供一个指定的不固定的共享 profile 那么就不要再注释下面的内容，默认使用用户主目录。

:[Profiles]

; path = /usr/local/samba/profiles

; browseable = no

; guest ok = yes

注意：如果你有一个 BSD 风格的打印系统，则没有必须单独的特别指定每一个打印机。

[printers]

comment = All Printers

path = /var/spool/samba

browseable = no

设置 public=yes 表示允许 ' guest account ' 打印

guest ok = no

writable = no

printable = yes

下面的内容对人们共享文件是有用的。

:[tmp]

; comment = Temporary file space

; path = /tmp

; read only = no

; public = yes

公用的可访问的目录，除了在 staff 组中的成员外，对其它人为只读

:[public]

; comment = Public Stuff

; path = /home/nw

; public = yes

; writable = yes

; printable = no

; write list = @staff

私有打印机，仅仅 fred 本人可用。打印池中的数据将被放到 fred 的主目录中。注意：fred 用户无论在什么地方都必须对打印池有写访问的权限。

:[fredsprn]

```
; comment = Fred's Printer
```

```
; valid users = fred
```

```
; path = /home/fred
```

```
; printer = fred's_printer
```

```
; public = no
```

```
; writable = no
```

```
; printable = yes
```

私有目录，仅能对 fred 开放。注意 fred 对这个目录需要写访问的权限。

```
:[fredsdir]
```

```
; comment = Fred's Service
```

```
; path = /usr/somewhere/private
```

```
; valid users = fred
```

```
; public = no
```

```
; writable = yes
```

```
; printable = no
```

允许你制作配置文件去引入的连接到这里的每一台机器都有不同的目录的服务。

使用%U 选去配置用户名，%m 代替连接到的机器名。

```
:[pchome]
```

```
; comment = PC Directories
```

```
; path = /usr/local/pc/%m
```

```
; public = no
```

```
; writable = yes
```

公共可访问的目录，对所有的用户都可读/写。注意：在这个目录中的所有由用户创建的文件都会被标识成默认用户所有。所以有访问权限的用户可以删除别的用户的文件。很明显这个目录必须是可以被默认用户写的。另一个用户当然可以指定，这样所有的文件都将被那个用户所替代。

```
[public]
```

```
path = /tmp/aaaa
```

```
public = yes
```

```
guest ok = yes
```

```
writable = yes
```

```
printable = no
```

下面的两个例子是怎样共享一个目录给两个用户，在这个共享目录中他们可以放置文件且分别属于各自所有。在这个设置中，目录将可以被两个用户同时使用且在其上有粘滞位保护。很明显，可以扩展为多个用户的情况。

```
:[myshare]
```

```
; comment = Mary's and Fred's stuff
```

```
; path = /usr/somewhere/shared
```

```
; valid users = mary fred
```

```
; public = no
```

```
; writable = yes
```

```
; printable = no
```

```
; create mask = 0765
```


(一)实验手册

1, 以下实验针对 Red Hat Linux Enterprise Linux 5 系统实验, 或者是 Red Hat 公司的其他版本。所有安装包, 均为系统光盘或镜像文件内。如有不同出处, 则另行说明! 实验操作如有异样, 请联系: 980617577。谢谢

安装系统包: samba-3.0.23c-2.i386.rpm

然后安装 samba-client-3.0.23c-2.i386.rpm 默认是安装过的, samba-common-3.0.23c-2.i386.rpm

如果系统提示没有安装或不能安装 samba 这个主配置文件包, 那么按照提示依次安装即可

首先测试共享目录

设置主配置文件

```
# vi /etc/samba/smb.conf
```

然后输入 security = share (红色代表我们要更改的地方)

在最后添加说明

```
[share]
comment = share Directory
path = /linshi/public
public = yes
writable = no
guest ok = yes
```

当然, 这里我们并没有给权限, 如果大家想给可以加入: cr

记得我们这里的 path = /linshi/public (注意这里的目录哦, 可以随便写路径的, 但是首先你要有这个路径哦, O(∩_∩)O~。可以参照 mkdir 命令创建)

最后的效果:



为了下次我们操作不会有什么妨碍, 那么我们可以注销。或者.....(*^__^*) 嘻嘻.....

```
C:\Documents and Settings\Administrator>net use * /del
列表是空的。
```

如果这样操作, 则可以避免太多繁杂的操作咯。嘿嘿...列表是空的, 因为我们还没有设置私有目录呢。下边我们开始咯

设置安全的私有目录以及共有目录

将上边的[share]这个删除。然后我们更改：security = **user** (这里我们设置为安全级别，而对于上边描述的有 4 个级别我们这里不讨论了。)

首先我们创建目录：a1 a2 b1 b2

然后我们创建系统账户开始映射，但是不用设置密码：useradd a1 然后依次进行

对于安全目录，不想让用户看到你服务器上的一丁点资料。

那么我们开始删：进入系统账户存放地：/home/，

然后进入每个账户中（记得是你想要映射的账户目录哦，别进错啦！进入 a1 a2 b1 b2），然

后删除：rm -rf .bash* (删除这几个系统创建账户后就带有的默认文件，当然你也可以修改让系统创建就不会有这些文件，具体参看/etc/default 看这个目录中文件以及/etc/skel 这个文件)

以及 rm -rf .zsh*

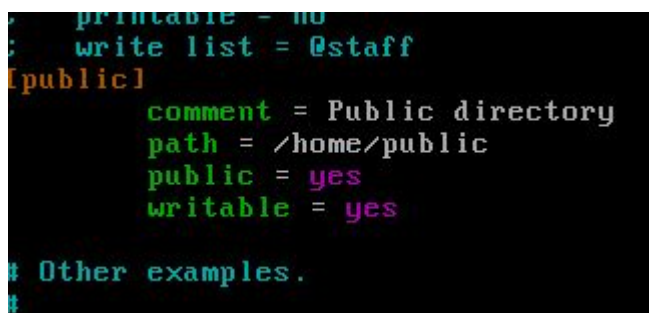
然后修改主配置文件

可以在这里

```
# This one is useful for people to share files
:[tmp]
; comment = Temporary file space
; path = /tmp
; read only = no
; public = yes

# A publicly accessible directory, but read only, except for people in
# the "staff" group
:[public]
; comment = Public Stuff
; path = /home/samba
; public = yes
; writable = yes
; printable = no
; write list = @staff
```

中间写入：

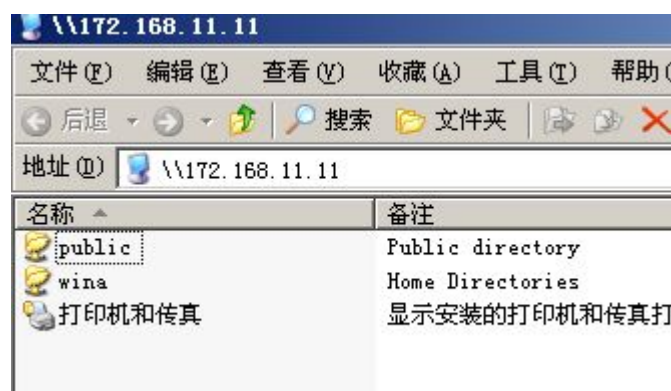


```
printable = no
; write list = @staff
[public]
    comment = Public directory
    path = /home/public
    public = yes
    writable = yes
# Other examples.
```

最后测试结果，这个是用 win 账户登录



这是我们就可以用这个命令咯，net use * /del，然后我们用 wina 这个账户登录，看看是不是还是这两个目录如果没有 win 这个目录。那么我们此次目的达到！



好，我们成功，但是没有权限。

现在我们来说明一下权限问题：首先我们需要知道我们想给用户什么权限，是读，还是写。那么我们在主配置文件中加入：

```

create mode = 0664                                //新建文件的默认权限
directory mode = 0775                              //新建目录的默认权限
    
```

然后就是目录的权限。我们需要弄明白这些问题

如果我们想让用户到 public 这个目录中，你可以建立自己的文件，但是别人不能给你随便删除，除了管理员。那么我们这里就要设置一下粘着位咯（参看我们上期文档中的权限介绍）！

管理个人目录（user）

根据上边我们的文件描述。我们可以让组访问，其实这个很好玩滴！

在/linshi/中创建 a1 a2 b1 b2 (/linshi/目录中，我们上边已经创建过)

我们上边在主配置文件中，继续写入

[a1]

Comment=a1 Directory

Path=/linshi/a1

Public=yes

Writable=yes

[a2].....其他和这个一样，当然可以根据需要配置符合自己的

图像画面管理（英文操作界面）

安装包：

rpm -ivh xinetd-2.3.14-10.el5.i386.rpm

rpm -ivh samba-swath-3.0.23c-2.i386.rpm

默认情况下在 3 级别中是禁止使用的，因为这个程序依赖于 xinetd 管理服务程序，在安装默认状态下是关闭

我们可以：

```
[root@linux1 Server]# chkconfig --level 35 swat on
```

```
[root@linux1 Server]# chkconfig --list |grep swat
swat:                on
```

然后我们修改/etc/xinetd.d/swat 这个文件

```
# 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
{
    disable = no
    port    = 901
    socket_type = stream
    wait    = no
    only_from = 172.168.11.123
    user    = root
    server  = /usr/sbin/swat
    log_on_failure += USERID
}
~
~
~
~
```

把 only_from 这个选项修改成你想要用户访问的 ip（这个 ip 地址就是 client 远程准备管理 samba 服务器的 PC 地址）

然后重启服务哦，http://samba 服务器的地址:901/

嘿嘿...估计出不来吧，(*^__^*) 嘻嘻……，重启 xinetd 服务，O(∩_∩)O~再次访问，可以.....

提示：

我们每次的修改主配置文件后，大家记得重启服务哦！

samba 服务器启动后，能看到共享目录，但是不能访问共享目录

tail -f var/log/message

可以看到 SELinux is preventing the samba daemon from reading users home directories. For complete SELinux messages. run

sealert -l a0c1c154-bc37-44f5-a6eb-cfc88fed18b9

然后我们运行：**sealert -l a0c1c154-bc37-44f5-a6eb-cfc88fed18b9**

根据提示：Allowing Access

If you want samba to share home directories you need to turn on the

samba_enable_home_dirs boolean: "setsebool -P samba_enable_home_dirs=1"

The following command will allow this access:

setsebool -P samba_enable_home_dirs=1

我们再次运行：**setsebool -P samba_enable_home_dirs=1**

-P 参数是永久有效的意思。

当然如果我们不想如此麻烦，可以 **setup** 将 **selinux** 关闭掉（这里我们不说明 **iptables**，稍后我们详细说明。）

这里我把从网上收集来的 **samba** 做一些实验给大家贴出来，大家可以自行参考研究。

说明以下文章系统或者并非 **Red Hat Enterprises Linux 5**，大家可以

参考

PAM（需要认证模块）:

对于主机和用户访问控制而言,PAM(可插入认证模块)是一个非常有效的工具.Samba3.0 已经与 PAM 结合得相当完善了.借助 PAM 强大灵活的认证机制,可以同时实现对用户和主机的访问控制功能.

某 Samba 服务器上有一个共享目录/var/myAREA,现希望用户 st02 可以在网段 192.168.1.0/24 中的任何一台主机上访问该共享段,而用户 update 则不能在网段 192.168.1.0/24 中的任何一台主机上访问该共享段.

(1)编辑 smb.conf 配置文件,以支持 PAM 认证以及配置共享段 myAREA

```
[global]
```

```
...
```

```
obey restrictions=yes
```

```
[myAREA]
```

```
path=/var/myAREA
```

(2)编辑配置文件/etc/pad.d/samba,以增加访问控制文件

在第一 accout 指令前添加如下语句:

```
account required pam_access.so accessfile=/etc/mysmblogin
```

(3)创建自定义的 Samba 访问控制文件/etc/mysmblogin

```
vi /etc/mysmblogin
```

内容如下:

```
+:st02:192.168.1.
```

```
-.update:192.168.1.
```

重启 samba 服务,测试.

以上实验在 RedHatAS4,AS5 下顺利通过,希望对大家有所帮助.

文章来源: baike.duba.net

对于主机和用户访问控制而言,PAM(可插入认证模块)是一个非常有效的工具.Samba3.0 已经与 PAM 结合得相当完善了.借助 PAM 强大灵活的认证机制,可以同时实现对用户和主机的访问控制功能. 某 Samba 服务器上有一个共享目录/var/myAREA,现希望用户 st02 可以在网段 192.168.1.0/24 中的任何一台主机上访问该共享段,而用户 update 则不能在网段 192.168.1.0/24 中的任何一台主机上访问该共享段. (1)编辑 smb.conf 配置文件,以支持 PAM 认证 以及 配置共享段 myAREA [global] ... obey restrictions=yes [myAREA] path=/var/myAREA (2)编辑配置文件/etc/pad.d/samba,以增加访问控制文件 在第一 accout 指令前添加如下语句: account required pam_access.so accessfile=/etc/mysmblogin (3)创建自定义的 Samba 访问控制文件/etc/mysmblogin vi /etc/mysmblogin 内容如下: +:st02:192.168.1. -.update:192.168.1. 重启 samba 服务,测试. 以上实验在 RedHatAS4,AS5 下顺利通过,希望对大家有所帮助. 文章来源: baike.duba.net

对于主机和用户访问控制而言,PAM(可插入认证模块)是一个非常有效的工具,Samba3.0 已经与 PAM 结合得相当完善了.借助 PAM 强大灵活的认证机制,可以同时实现对用户和主机的访问控制功能.

某 Samba 服务器上有一个共享目录/var/myarea,现希望用户 st02 可以在网段 192.168.1.0/24 中的任何一台主机上访问该共享段,而用户 update 则不能在网段 192.168.1.0/24 中的任何一台主机上访问该共享段.



(1)编辑 `smb.conf` 配置文件,以支持 PAM 认证以及配置共享段 `myarea`
[global]

...

`obey pam restrictions=yes`

`path=/var/myarea`

(2)编辑配置文件/etc/pad.d/samba,以增加访问控制文件

在第一 `accout` 指令前添加如下语句:

`account required pam_access.so accessfile=/etc/mysmblogin`

(3)创建自定义的 Samba 访问控制文件/etc/mysmblogin

`vi /etc/mysmblogin`

内容如下:

`+:st02:192.168.1.`

`-.update:192.168.1.`

重启 samba 服务,测试.

Samba 做 pdc

前面我们已经讲了关于 samba 服务器如何充当一个局域网的文件服务器,以满足平时的工作需要,在看本文档之前,大家最好先看看那篇文档《Samba3.0 服务器实战调试》(<http://www.5ilinux.com/samba.html>),大家只有领会了那篇文档以后,再来看用 samba 实现 PDC 就不死很困难了。

其实早在 samba2.2 版本已经能非常好的支持 samba 做 PDC (主域控制器),只不过到了 3.0 对域的支持更加好,到现在为止最新的版本 3.0,已经支持 AD,并且支持 Microsoft Kerberos 认证、完全重写和可配置的认证子系统等新功能。

好了,我们来开始今天的任务,我们今天只是实现简单的域控制器 PDC 的建立,至于他支持的 AD 和 Kerberos 等功能大家慢慢的自己去研究,我也不是很懂哦:)

1. 安装 samba,这个很简单了,如果你是 fedora,就可以从光盘直接安装 samba 的 rpm 包。
`rpm -ivh samba-3.0.0-15.i386.rpm`

大家也可以直接到 samba 的官方网站 (<http://www.samba.org/>) 去下载最新的软件包

或者下载最新的 tar 包, <http://us1.samba.org/samba/ftp/samba-3.0.0.tar.gz>

那就最好按下面的方法编译

`tar zxvf samba-3.0.0.tar.gz`

`cd samba-3.0.0`

`./configure \`

`--prefix=/usr \`

`--bindir=/usr/bin \`

`--sbindir=/usr/sbin \`

`--libexecdir=/usr/libexec \`

`--datadir=/usr/share/samba \`

`--sysconfdir=/etc/samba \`

`--localstatedir=/usr/local/samba/var \`

`--libdir=/usr/lib \`

`--with-lockdir=/var/locks/samba \`



```
--with-swatdir=/usr/share/samba/swat \
--with-codepagedir=/etc/samba/codepages \
--with-configdir=/etc/samba \
--with-smbwrapper \
--with-automount \
--with-smbmount \
--with-pam \
--with-pam_smbpass \
--with-winbind
```

```
make
```

```
make intall
```

ok!安装完以后，下面才是我们的重点，修改/etc/samba/smb.conf，大家最好在原来的基础上修改。

```
[global]
```

```
workgroup = bmit
```

```
netbios name = proxy
```

```
server string = Samba PDC running %v
```

```
socket    options    =    TCP_NODELAY    IPTOS_LOWDELAY    SO_SNDBUF=8192
SO_RCVBUF=8192
```

这里的 workgroup = bmit 就代表 bmit 域，当然如果用 bmit.com 那就更加规范，但为了客户端输入的方便，还是直接 bmit 的好，netbios name = proxy 表示这台服务器的 netbios 名,socket options 选项设置控制 TCP/IP 性能。所显示的设置就可以与基于 Linux 的系统一起很好地工作了。

```
os level = 64
```

```
preferred master = yes
```

```
local master = yes
```

```
domain master = yes
```

#domain master 选项是一个“开关”，通告 Samba 将成为主域控制器。(local master browser) 是维护局域网机器列表的服务器被称为本地主浏览器。

```
security = user
```

```
encrypt passwords = yes
```

```
domain logons = yes
```

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

```
log level = 2
```

```
max log size = 50
```

```
hosts allow = 127.0.0.1 192.168.1.0/255.255.255.0
```

#这里我们还是使用 user 验证方式，不要悬在所谓的 domain，至于 hosts allow 大家可以根据自己的需求写那些网段可以访问你的服务器，或者索性不写也行。

```
logon home = \\%L\%U\profile
```

```
logon drive = H:
```

```
logon path = \\%L\profiles\%U
```

```
logon script = netlogon.bat
```

#以上是漫游设置和登录脚本，logon path = \\%L\profiles\%U，会于下面我们要说的 [profiles] 共享成对应关系。



[homes]

comment = Home Directories

browseable = no

writable = yes

[profiles]

path = /home/samba/profiles

writable = yes

browseable = no

create mask = 0600

directory mask = 0700

[netlogon]

comment = Network Logon Service

path = /home/netlogon

read only = yes

browseable = no

write list= root

以上是关于共享的手腕子，其中 **profile** 是用来存放每个登录用户的设置文件，以便用户以后登录可以从服务器读取以前的桌面设置，**netlogon** 是用来存放登录脚本的，所以要限制写的权限，假设这里只有 **root** 用户可以有权限。

至于其他共享，完全可以参照《Samba3.0 服务器实战调试》(<http://www.5ilinux.com/samba.html>)

这篇文章共享设置，我就不再重复讲了

接着是将用户和机器帐户添加到域控制器。

先建立创建了下列各组以及创建两个必要目录，并设置正确的所有权。

groupadd admin

groupadd machines

mkdir -m 0775 /home/netlogon

chown root.admins /home/netlogon

mkdir /home/samba /home/samba/profiles

chown 1757 /home/samba/profiles

对上述目录设置正确的权限和所有权是保护服务器的关键一步哦 :)

手工添加机器帐号

比如我的客户端的机器名是 **ibm240**，那么我们可以这么做

useradd -g machines -d /dev/null -c "machine id" -s /bin/false ibm240\$

passwd -l ibm240\$

输入两遍密码；

不要忘记标上美元符号；这是必需的，它将该项标识为信任帐户

创建 **linux** 帐户后，我们现在可以将该机器添加到 **/etc/samba/smbpasswd**

smbpasswd -a -m ibm240

当然你也可以让系统自动添加机器帐号，用下面的方法，不过大家最好先试手动添加，成功后再试验系统自动添加

自动添加只要在[global]添加

add user script = /usr/sbin/useradd -d /dev/null -g machines -s /bin/false -M %u

添加用户帐号



首先添加的是 root 帐户，把 root 加入到 smb 帐户中

`smbpasswd -c root`

这一步很重要，因为后面的加入域要用到有管理员的帐号加入域的权限，否则用普通用户好像不能顺利加入域

然后添加普通用户

`useradd frank`

`passwd frank`

`smbpasswd -a frank`

为了方便以后的管理，最好 smb 的用户密码和 unix 系统密码一样，这样我们还可以用到 samba 的密码同步功能

#下面的选项语句将允许用户从 Windows 客户机上更改他们的 Samba 密码，这样会随即更新他们的 UNIX 密码以与新的 Samba 项相匹配。但是如果更改了 UNIX 密码，那么同一技术不能逆向工作；必需手工同步更改 Samba 密码。也是在[global]，初学者可以先不做这个工作。

`unix password sync = yes`

`passwd program = /usr/bin/passwd %u`

```
passwd chat = *New*UNIX*password* %n\n *Retype*new*UNIX*password* %n\n *Enter*new*UNIX*password* %n\n *Retype*new*UNIX*password* %n\n *passwd:
*all*authentication*tokens*updated*successfully*
```

#上述语句中唯一值得一提的是 `passwd chat` 选项，不管这里如何显示它，都要将它输入成一行。还要注意有些选项使用 “password”，而有些使用 “passwd”。

Samba PDC 的配置就这样完成了。剩下唯一要做的是将客户机加入到域中。记得重启 samba 服务哦！

客户端的设置，这里由于条件的限制，我只试验了 windows2000 客户端加入域，至于 winxp 和 win98 的加入大家自己去试验。

（win200 机器最好先重启一下，可以避免一些不必要的问题）然后转至 控制面板 -> 网络 -> 网络标示，如果机器目前被配置在 工作组 选项下，那么选中 域 单选按钮并输入域名 bmit。

现在，通过使用用户名 root 和相应的密码登录到域。必需初始化服务器和客户机机器之间的“秘密”。从此时起，任何已认证的用户都可以从这台机器登录。

应该出现一个欢迎您来到 XX 域的消息

恭喜你已经成功将 samba 配置成 PDC

据说 xp 加入 samba 建立的域有点复杂，我没试验过，大家有兴趣的话，最好去 samba 的老家看看文档，好像是要设置安全选项，并修改注册表，好麻烦哦，幸亏我没有 xp :)

谢谢！

制作人：小孩

2009 年 9 月 16 号