China-pub.com
下载

第8章　Samba服务与Windows连通性

Microsoft Windows平台的流行在很大程度下让UNIX的狂热爱好者感到悲伤。很长时间以来，因为Windows系统在企业计算中起不到任何作用，所以 UNIX比Windows系统具有更强的能力，以至于 PC平台可以完全被忽略。但是，随着时间的推移和各种或好或坏的基于Windows系统的应用程序的实现， UNIX系统有时也必须在Windows网络中占有一席之地，在TCP/IP之上的Samba系统便可以使用户达到这一目标。

NetBIOS网络环境是作为Microsoft和IBM的结合项目而提出来的；它最初使用为小型计算机网络设计的无路由协议 NetBEUI来实现，接着又在 TCP/IP之上重新加以实现。在 TCP/IP之上实现的NetBIOS仍然有着其最初设计的局限性（如： WINS）。NetBIOS和TCP/IP的接合不能说是十分协调的， Microsoft曾提出“ 通用Internet文件系统（Common Internet File System）”的概念，可以这样认为，在网络规划中， NetBIOS可以被完全忽略，但是很不幸的是事实并非如此。

Samba是UNIX的TCP/IP之上的NetBIOS的自由实现。虽然在设计中存在一些问题（如fork ( )产生了太多的进程），但Samba还是在企业中取得了较为广泛的应用，并经受住了很多挑战。 Samba的目标是在UNIX中重新生成Windows NT系统中的所有网络功能（包括象域控制这样的功能）。

在Red Hat Linux中， Samba是一个在系统安装时可选择安装的组件。若用户选择安装了Samba，即当系统初启时， Linux系统是一个完全可操作的NetBIOS文件服务器。

警告　Red Hat Linix 6.0的Samba最初版本存在安全性问题，目前通常使用的是samba-2.0.5a-1.i386.rpm或更高的版本。

注意　用户在使用Samba时，Samba的开发人员希望收到用户寄给他的礼物，Samba的Web站点http://www.samba.org有这方面的信息。这将是一件难以处理的事，因为Samba的开发人员住在澳大利亚（笔者现在还没有寄礼物给他，但如果以后在 Windows工作出了问题的话，笔者将会这么做）。

8.1　Samba和口令加密

微软并不喜欢Samba，他们有很好的理由不喜欢它。近来 Samba性能的提高使得它在大多数硬件上比Windows NT的文件和打印服务的缺省配置速度更快。

事实上，微软甚至讨厌Samba，以至于他们改变了Windows NT Service Pack3的口令，以避免它和Samba服务共享未加密的口令。 Samba的缺省设置是针对未加密口令的，但是这样的设置可以被修改以巧妙地战胜微软这种卑劣的胆怯。

最新的加密口令与在/etc/passwd或/etc/shadow文件中使用的DES格式不相容，因此当启用加密的口令时， Samba必须有自己独特的口令文件。如果与 Windows NT Service Pack3或更高的版本（Windows 98或更高）连接时，在客户开发工作之前，必须实现加密的口令。这是通

China-pub.com 下载

过删除以下两行（通常在/etc/smb.conf文件的65或66行）的注释实现的：

```
encrypt passwords = yes
smb passwd file = /etc/smbpasswd
```

然后必须作为超级用户运行下面的命令以将 Samba服务器重新启动：

```
/etc/rc.d/init.d/smb restart
```

当以上操作完成以后，将不再允许任何用户登录到 Samba服务器。每个用户必须被超级用户独立地加入到新的/etc/smbpasswd文件中；实现上述操作的方法如下：

```
# smbpasswd -a luser
New SMB password:
Retype new SMB password:
```

在这个命令执行时，用户名 luser必须在/etc/passwd数据库中已经存在，当命令执行时，/etc/smbpasswd文件中将创建与下面相似的内容：

```
# Samba SMB password file
luser:500:5EDBBAA6F82E9DD9AAD3B435B51404EE:
F908E55FD20399082E5ADEB9792D27D1:
/home/luser:/bin/bash
```

一旦根用户在 /etc/smbpasswd文件中创建了表项，那么各个用户可以使用不带参数的smbpasswd命令来改变他们自己的Samba口令。这个过程应该为系统中的每个用户执行，在一个新的系统中，上面的操作应该是建立一个新的用户帐号的一部分操作。

在已经存在了许多帐号的旧系统中，用上面的方法来移植各个独立的用户有些不切实际。在这种情况下，存在着一种（相当笨拙的）方法来移植这样的用户。要把已存在的未加密的口令文件移植为/etc/smbpasswd文件，那么不需要设置文件 /etc/smb.conf的加密选项。首先作为超级用户执行以下的命令：

```
cat /etc/passwd | /usr/bin/mksmbpasswd.sh /etc/smbpsswd
chmod 600 /etc/smbpasswd
```

上述操作将为每个用户在/etc/smbpasswd文件中创建一个表项，该表项的形式可能如下：

```
luser:500:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:
:/home/luser:/bin/bash
```

该表项不包含口令，而且用户无法对它进行修改。

下面的两个选项必须被加入到/etc/smb.conf文件中：

```
update encrypted = yes
smb passwd file = /etc/smbpasswd
```

必须作为超级用户来运行下面的命令，以重启 Samba服务：

```
/etc/rc.d/init.d/smb restart
```

这样，用户就可以使用旧的未加密客户来登录了（如同 Windows 95一样），而且对每一个用户帐号，/etc/smbpasswd文件都有一个加密的口令。

当移植完成后，文件 /etc/smb.conf中的选项update encrypted = yes应被替换为encrypt passwords = yes。

Samba将切换到加密的版本，并且只有新的客户可以登录。

以上讨论的移植需要很好的计划、时间和深入的思考，尤其是对大型企业而言。在新客户进入Samba网络之前应该试用几个月。

China-pub.com
下载

8.2 用户映像

Windows 95和Windows 98与Windows NT之间相当大的区别在于它们使用网络资源的能力。Windows NT允许用户针对不同的服务器改变自己的登录标识；而 Windows 95/98对所有的网络资源只使用一个登录标识，该标识是在启动 /登录时输入的。这样，当用户登录进入了Windows网络，并想用他们的帐号与 Samba系统相连，但是两个环境下的用户名又不相同时，就引起了很大的不便。

为此，将到来的用户名转换为另一个 UNIX用户是一件方便的事。为了实现此目标，应去掉/etc/smb.conf文件中的第79行（如下）上的注释：

```
username map = /etc/smbusers
```

这样，带有用户转换的/etc/smbusers如下：

```
# Unix_name = SMB_name1 SMB_name2 ...
#root = administrator admin
#nobody = guest pcguest smbguest
luser = FunnyWindowsUser
user2 = WindowsUser2 Otheruser diewindowsdie
```

在标准的Samba RPM发布中，/etc/smbusers文件的root和nobody用户被注释掉了；最好是去掉这些注释，除非有足够的理由说明这些用户可以被转换。

8.3 Samba和主浏览器

在Windows NT网络中，一个集中的主机负责维护 BIOS服务及可浏览共享表。该主机便被称为主浏览器（master browser）。如果Windows NT网络有一个主域控制器，则该主域控制器便是网络的主浏览器。如果网络中不存在主域控制器，那么就在 Windows NT服务器计算机中进行选择，选择的结果决定哪一个 NT系统作为主浏览器。如果没有可用的 Windows NT服务器系统，那么Windows NT工作站计算机将相互会话并决定其中一台计算机作为主浏览器。

如果没有正确配置，那么Samba将不停地在网络中进行选择，试图挑选出主浏览器，这样将引起与真正的主浏览器之间的冲突。

为了终止这种冲突，将下面几行加入到 /etc/smb.conf文件中：

```
domain master = no
local master = no
preferred master = no
os level = 0
```

8.4 Samba服务器组件

文件/etc/smb.conf中包含了许多重要的参数和配置实例。一个值得考虑的选项是工作组名：

```
workgroup = MYGROUP
```

这个名称应改为网络中相应的域名或工作组名。

客户可能无法看到Samba服务器，因为它位于离路由器很远的地方。如果用户碰到这样的问题，那么可以创建一个LMGOSTS文件，以便客户可以直接查询特定的 IP地址。此文件的正确位置依赖于所使用的 Windows版本；在Windows 95/98中，该文件位于\windows目录下。而

China-pub.com 下载

在NT系统中，用户应查找 LMHOST.SAM文件（该文件是一个可用于各种常见配置下的LMGOSTS示例文件），LMGOSTS文件应被放置在和示例文件同一个目录下。

为了让客户机可以见到Samba服务器，LMHOSTS文件中的表项应该具有如下的形式：

```
1.2.3.4 remotehost # PRE
```

#PRE指示Windows预装载此表项，从而使得表项在动态查找开始前就可用。如果LMHOSTS文件被修改了，那么可以在DOS提示符下键入nbtstat -R命令，以使Windows重新装载该文件。如果因为客户数量太多而使得 LMHOSTS文件变得不便，那么应该考虑对 WINS服务器（Samba或NT）的使用，特别是与DHCP的连接（参见第2章）。Samba有许多针对WINS服务的选项。

有时，因为装载了错误的协议，可能引起客户机无法与 Samba服务器相连。Samba需要在客户端提供TCP/IP支持；而有的版本的Windows（尤其是Windows 95）在缺省情况下并不装载TCP/IP协议。为了让Windows 95/98可以使用Samba资源，必须在Windows控制面板的网络设置中装载Microsoft网络客户和TCP/IP。更多的细节可以参见有关Windows网络的书籍。

8.4.1 文件服务

在缺省情况下，一旦Samba服务器启动后，用户就可以用如下的形式将他们的 HOME目录安装为Windows系统下的一个子驱动器。

```
\\remotehost\luser
```

这里的remotehost就是远程的Red Hat Samba服务器，而luser是在该服务器主机上的任意一个用户。

如果不希望实现上述安装，那么将下面的一段代码从 /etc/smb.conf文件中删除。

```
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
```

为了创建一个公用的可浏览区，向/etc/smb.conf文件中加入如下一段代码：

```
# 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
```

为了创建一组可以向这样的目录进行写操作的用户，应该在 /etc/group文件中创建一个staff表项，并且将选择的用户加入该组，所选择的用户应该在/etc/passwd文件中有相应的表项。注意，同UNIX访问权限的实施一样，目录的权限应设置为 staff组可写。

下面的代码示例说明了使用组的“有效用户”目录。

```
# The following two entries demonstrate how to share a
directory so that two
```

China-pub.com
下载


```
# users can place files there that will be owned by the
specific users. In this
# setup, the directory should be writable by both users and
should have the
# sticky bit set on it to prevent abuse. Obviously this
could be extended to
# as many users as required.
[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
```

下面，我们描述在Windows客户机上映像服务器资源的过程。首先，在 Windows 95/98中，用鼠标右键点击“ My Computer ”图标，并在菜单中选择“ Map Network Drive ”（如图8-1所示）。

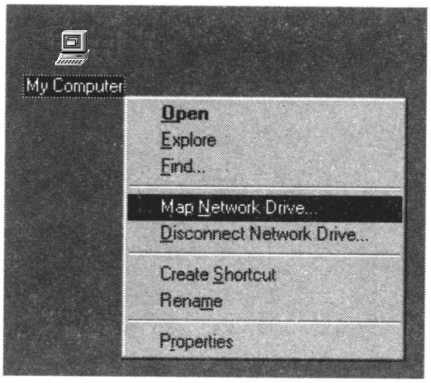


图8-1 Windows 95/98—— 映射网络驱动器

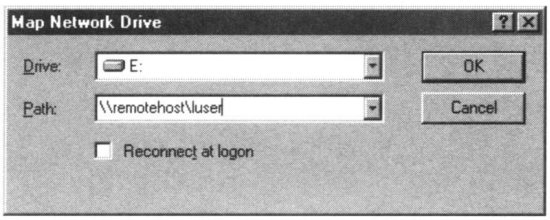


图8-2 Windows 95/98—— 映射网络驱动器细节

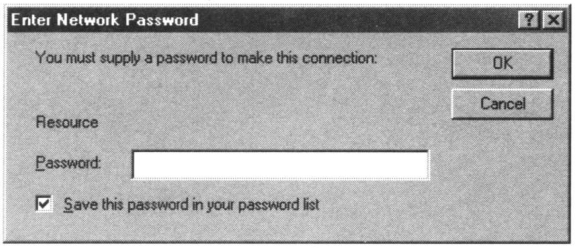


图8-3 Windows 95/98—— 口令对话框

China-pub.com 下载

选择一个空的虚拟驱动器，并键入用于映射的共享名（如图 8-2所示）。
提供服务器上的用户口令以完成连接（如图 8-3所示）。
在Windows NT下的操作略有不同（如图8-4所示）。

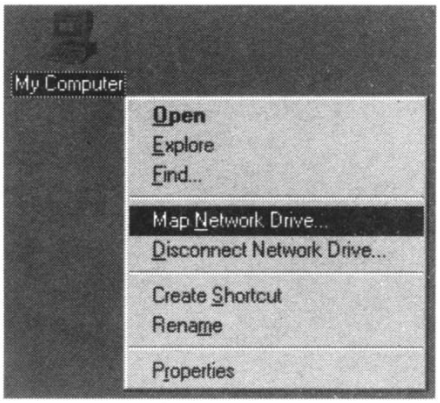


图8-4 Windows NT—— 映射网络驱动器

Windows NT允许用户填充到“ Connect As ”中（如图8-5所示），该特征是Windows 95/98的版本中所缺乏的。

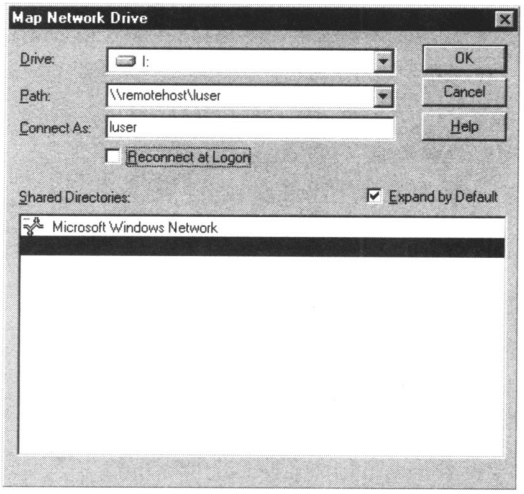


图8-5 Windows NT—— 映射网络驱动器细节

提供服务器上的用户口令以完成连接（如图 8-6所示）。

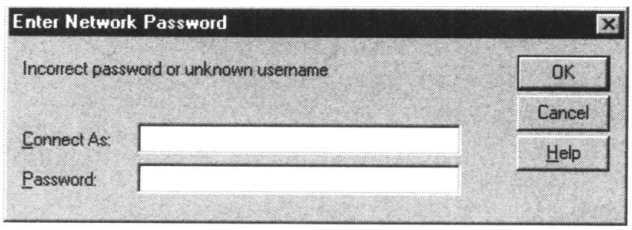


图8-6 Windows NT—— 口令对话框

China-pub.com
下载

8.4.2 打印服务

在缺省的情况下，系统中所有的打印机都可以通过 Samba来共享。这种共享是由文件/etc/smb.conf中的下面几行来控制的：

```
# if you want to automatically load your printer list
rather
# than setting them up individually then you'll need this
   printcap name = /etc/printcap
   load printers = yes
```

如果不希望这种共享，那么只需将这段代码从文件 /etc/smb.conf中删除。

如果删除了这段代码，那么下面这个取自 /etc/smb.conf中的代码段示例可用于共享一台独立的打印机：

```
# A private printer, usable only by fred. Spool data will
be placed in fred's
# home directory. Note that fred must have write access to
the spool directory,
# wherever it is.
[fredsprn]
   comment = Fred's Printer
   valid users = fred
   path = /homes/fred
   printer = freds_printer
   public = no
   writable = no
   printable = yes
```

此外用户还可以定义所使用的打印命令：

```
[laser]
comment = Laser Printer
path = /var/spool/samba
printer driver = "Generic Laser"
print command = lpr-P lp1 %s
public = no
writable = no
printable = yes
```

注意 有时，在Red Hat RPM的Samba版本中，将会出现以下的情况：除了上面最后一个例子中直接定义了打印命令的方法外，其他所有共享打印机的方法都将失败。所以如果用户遇到这种问题，那么就可以像此处所使用的方法一样直接定义打印命令。

8.5 Linux的NetBIOS客户服务

在Windows NT网络中，Linux可以作为客户去访问共享的文件和打印机。

8.5.1 文件服务

如果远程的NT或95/98服务器运行TCP/IP，并且有可用的共享资源，那么这种共享可以通过smbmount命令来访问（请注意，达到这个目的并不使用标准的 mount命令）。

以根用户方式运行下面的命令，将把远程主机 nthost上的共享目录data安装为本地的/mnt

China-pub.com 下载

目录。

```
smbmount //nhost/data -c 'mount /mnt'
```

命令将首先提示输入口令，然后再将共享安装到 /mnt上。

命令执行时假定在远程的 NT系统上定义了用户“ root ”，并且nthost主机在本地网络中可见。

如果使用另一个用户去访问远程主机，那么可以使用 -U选项来定义：

```
smbmount //nthost/data -U luser -c 'mount/mnt'
```

如果远程主机在本地网络不可见，那么可以使用 -l选项来定义远程主机的 IP地址或主机名：

```
smbmount //nthost/data -l nthost.com -c 'mount /mnt'
```

NT服务器中的文件权限通常与 UNIX中不大相同。若NT服务器使用FAT文件系统，那么文件没有权限。若服务器使用 NTFS，它的安全模式比UNIX更灵活，但两者不兼容。可以采用如下方式来使用一些选项，以控制 Linux指定安装的文件系统中的用户、组和文件模式以及目录模式：

```
smbmount //nthost/data -U luser -l nthost.com -c 'mount /mnt -u 500 -g 500 -f 644 -d 755'
```

采用如下变换的命令形式有时更有效：

```
smbmount //nthost/data /mnt -U luser -l nthost.com \ -u 500 -g 500 -f 644 -d 755
```

读者可以通过在Red Hat Linux 6.0中的示例学习所使用的语法。

8.5.2 打印服务

把Windows系统中的打印机加入为 Linux系统的打印机，这相对而言要直接一些。在Xwindow环境下，以根用户方式运行如下的命令：

```
printtool
```

这时，如图8-7所示的打印机系统管理器将显示出来。

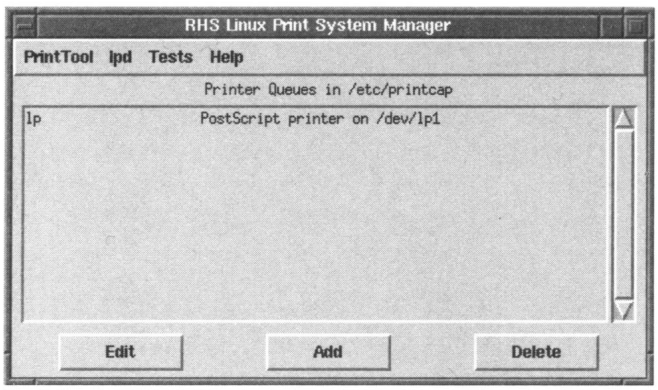


图8-7 Red Hat Linux打印机系统管理器

选择“ Add ”选项，则显示出如图8-8所示的对话框。

选择“ Lan Manager Printer ”，并点击“ OK ”，再继续点击图8-9所示的警告对话框中的“ OK ”按钮。

China-pub.com
下载

在图8-10所示的对话框中加入相关信息，并点击“OK”。这样，打印机系统管理配置就完成了（如图 8-11所示）。

任何用户都可以使用下面的命令以将输出发到Windows系统的打印机中打印：

```
lpr-Plp0 /etc/passwd
```

如果NT打印机被安装为缺省的打印机lp，那么上面命令中的-P选项可以不要。

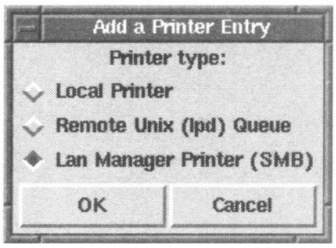


图8-8 打印机类型

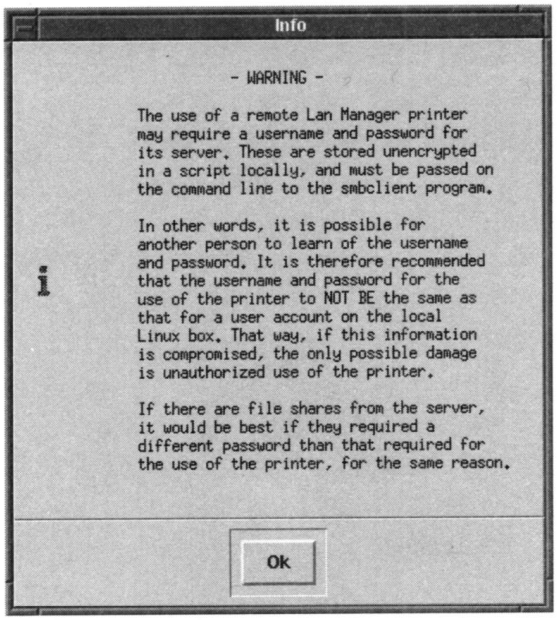


图8-9 安全警告

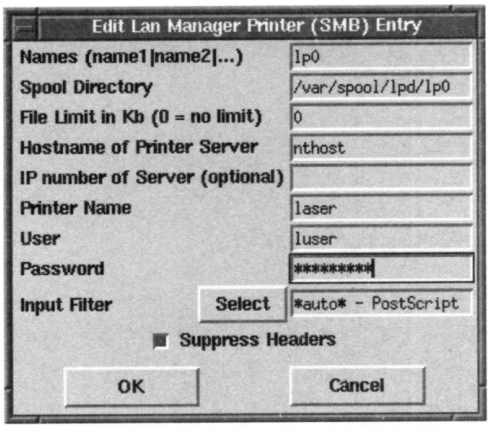


图8-10 SMB打印机的配置

可以使用一个简单的Shell脚本来实现在远程Windows系统的打印机上的打印。这段代码可以在文件winprint中找到，如下所示：

China-pub.com 下载

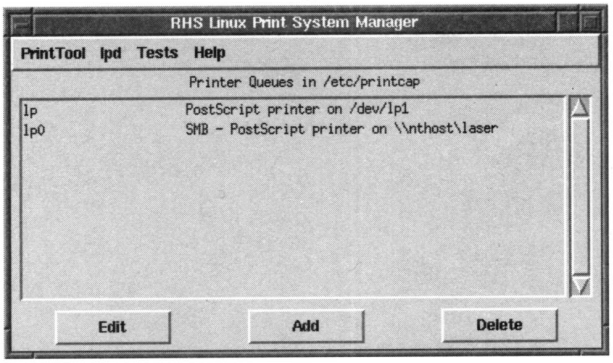


图8-11 Red Hat Linux打印机系统管理器

```
winprint:

#!/bin/sh
SERVER="NTHOST"
SERVICE="PRINTER"
USER="luser"
PASSWORD="secret"
(
echo "print -"
cat $*
) | /usr/bin/smbclient "\\\\$SERVER\\$SERVICE" $PASSWORD -U
$SERVER -N
```

使用winprint的一个示例如下：

```
winprint /etc/passwd /etc/group /etc/hosts
```

关于这类SMB打印机还有很重要的一点要指出。在打印机系统管理器对话框中输入的用户名和口令被保护下来，并且直接对 Shell脚本开放。

基于上述的原因，""; rm-rf/这样的口令有着潜在的危险。为了安全，应该将共享名、用户名以及口令限制为字母和数字字符。