Replacing a Windows NT/2000 server using Linux and SAMBA

by Sebastian Sasías
<sasias(at)linuxmail(dot)org>

About the author:

He has used Linux for several years as a support tool to develop technological solutions. Works in device control by using Linux, signal processing, communications and networks security. Professional in Electronics - Automation and Computer Science. He has contributed to Free Software development under GNU/GPL.

Translated to English by:
Sebastian Sasías
<sasias(at)linuxmail(dot)org>

Abstract:

This article supplements some aspects previously presented in other LinuxFocus articles about the SAMBA product and its use to share resources in heterogeneous Unix-Windows networks. Particularly it is focused on a Linux system with SAMBA in order to run some services, typically provided by Windows operating systems.
This is not only a demonstartion of the power and flexibility of Linux but it has as well an important economic consequence:

- Big savings in payments of licenses for Windows servers.
- A similar or better performance can be achieved, even using less hardware resources than required by a Windows server (in terms of processor and RAM).

A Linux server with SAMBA properly configured can substitute a Windows NT/2000 server, it commonly shares directories, gives an active directory service (ADS) but it can also work as PDC (Primary Domain Controller), doing the users authentication with Windows 2000/NT/98/95 clients, sharing resources (directories and printers) and customizing the user sessions.
This article concentrates particularly on these aspects.

As a result, for many environments where this is the main function of a Windows server, the Linux server with SAMBA substitutes all functions of a server based on Microsoft operating system, with no changes in the clients computers.
For the steps that will be presented, it is assumed that: SAMBA is already installed and working correctly on the machine that will be used as server. The reader knows basic concepts about Linux and Windows servers.

_____ _____ _____

Case Study

Consider a Linux/Samba server working as a PDC, where every authenticated user also has access to two shared directories on the server, one for a public area and other for a private area. In this article it will be considered a quite frequent case to access a private data area, the access to a personal directory for each user.

Details to be considered:

Linux/Samba NetBIOS Name:**SMBServer**
Windows domain name (workgroup): **THEDOMAIN**
Private partition for each user: H: (Windows) => **/home/** (Linux server)
Public partition: P: (Windows) => **/home/public**

Figure 1 shows a simple network diagram with clients machines, running Windows systems that are using resources and services from the Windows NT/2000 server. This server can be replaced by using the Linux/SAMBA server.
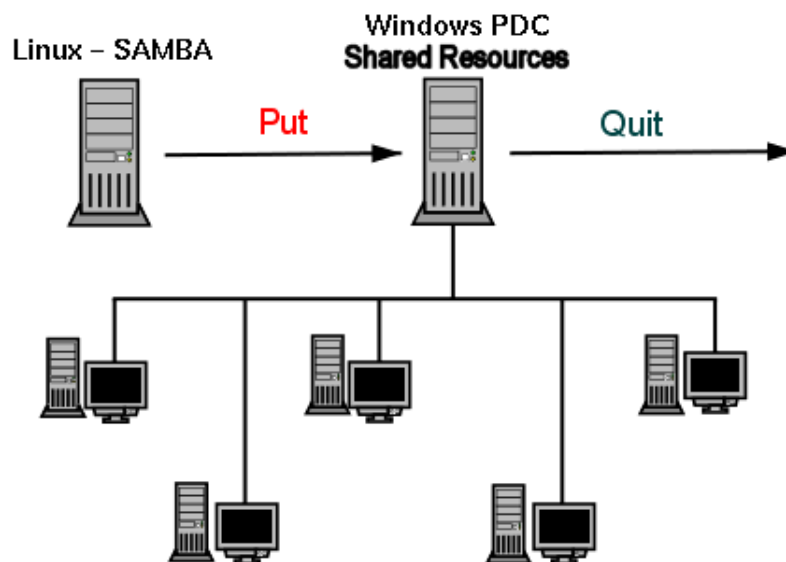

Fig. 1 – PDC and File Server on Windows

Configuration

Follow the steps:

1) Create the users that should be authenticated in the PDC server (Linux with Samba).
Use the **adduser** command, **useradd** or **userconf**, you can also use some tool for users administration, but with graphic user interfase (Webmin, Linuxconf, Yast, etc.).

Be sure that users have access only to Linux/Samba services (if you want it), it implies they don't have access to the Linux shell, to do it they will have **/dev/null** as home directory and **/bin/false** as shell.

2) Convert the UNIX users to Linux/Samba/Windows users, creating the **smbpasswd** file.

cat /etc/passwd | mksmbpasswd.sh > /etc/samba/smbpasswd

Another way to do it, execute the following Samba commands for users creation and for passwords definition:

smbadduser
smbpasswd

These commands work in a similar way to adduser and passwd commands.

3) Edit the Samba configuration file (smb.conf), making sure to include or to remove the comment signs for the options that are shown below:

netbios name = SMBServer
workgroup = THEDOMAIN
server string = Linux Samba NT Server
log file = /var/log/samba/%m.log
max log file = 0
security = user
encrypt password = yes
smb password file = /etc/samba/smbpasswd
ssl CA certificate = /usr/share/ssl/.... (cancel comment)
socket options = (cancel comment)
local master = yes
preferred master = yes
domain master = yes
domain logons = yes
logon script = logon.bat
wins support = yes

Note:
*For a specific login for each user, replace the logon script with %U.bat", therefore each user has a "logon script" with his user name, %u could also be used. If you want some way to consider the group to which the user belongs, you can use %g or %G, the meaning of these parameters and others can be found in the manual (**man smb.conf**)*

4) Create the shared resources

Edit the **smb.conf** file and comment all the "shares" samples, making the necessary changes to add the following information:

[netlogon]
comment = Initialization Scripts
path = /home/netlogon
read only = yes
guest ok = yes
browseable = no

[home]
comment = User Directory
path = /home/%U
browseable = yes
writable = yes

[public]
comment = Public Directory
path = /home/public
browseable = yes
writable = yes
guest ok = yes
create mask = 0777
force create mask = 0777

Save the **smb.conf** file

5) You can test the smb.conf correctness by using this command:

testparm

This command analyzes the smb.conf file and reports errors if it finds them.

6) Create the directories **/home/netlogon** and **/home/public** with permissions 0754(netlogon) and 0777 (public).

7) Edit the script Logon file: **logon.bat**.
Important: Use a text editor for DOS/Windows (like Notepad or Edit) to create the file logon.bat (so that it is saved as text file in a MS compatible format), also you can do it using a text editor running on Linux and after that you must convert to the correct text format. You can e.g use vim's ":set textmode" command to get a file with MS line endings.

net time \\SMBServer /y *(you can also use: /yes instead of /y)*
net use H: \\SMBServer\home -y *(you can also use: /yes or /y instead of -y)*
net use P: \\SMBServer\public -y

8) Include SMBServer information in the lmhosts file.

Edit the **/etc/samba/lmhosts** file (or /etc/lmhosts) and add a line with your SMBSever information.

SMBServer, i.e: **192.168.0.10 SMBServer**

9) Start/Restart the Samba daemon (smbd)

service smb restart

If it does not work correctly in your Linux distribution, you can use:
ps -auxgx | grep smb
kill -9 <process ID of smb>
smbd

10) Use smbclient to verify if the previously specified configuration is working correctly.

smbclient -L //SMBServer

if "Password:" is displayed, press "Enter" and shared resources by the server will be shown.

11) Do a client login, using some Windows 95/98/NT computer, in the domain THEDOMAIN, use some Linux/Samba user previously created (see steps 1 and 2).

On Windows 95/98/ME, it should be configured according to the following actions sequence:

Start => Setup => Control Panel=> Network =>Network Client for Microsoft Networks => Properties.

A very similar idea can be used for Windows NT/2000 clients (Workstation/Professional), although the sequence could not be the same.

Click in the option "Start session in Windows NT/2000 domain" and write this domain: THEDOMAIN (WORKGROUP).

A sample of configuration file

A complete SAMBA configuration file is presented here, this file has been tested with several Linux distributions. The reader can modify it to obtain the needed results presented in this article. Each instruction that appears is properly commented.

As last advice for those who want to achieve a quick configuration of SAMBA, can install the Webmin and/or SWAT, tools that allow to configure it in a friendly way.

```
#================================================================#
# /etc/smb.conf
#---------------------------------------------------------------------------------------------------#
# Main SAMBA configuration file
```

File Skeleton for configuration, select the
parameters according to your requirements.
#---#
Tested with the systems: Solaris and Linux/Distributions:
RedHat 6.0, 7.0 and 7.1
Solaris 7
Slackware 7.x
Mandrake 6.1, 7.0 and 8.1
SuSe 7.2
#---#
Last changes: 08/12/2001
Sebastian Sasias - sasias(at)linuxmail(dot)org
#===#
#
This file has been developed following documentation specifications of
SAMBA, from smb.conf(5) manual
#
OBS: After modify this file, test it with the "testparm" command
#
#===================== Global Options =====================#
#
General configuration
#
[global]
#...#
workgroup = NT-Domain-Name o Workgroup-Name, ie: THEDOMAIN
PDC Domain
workgroup = THEDOMAIN
#...#
Name which this machine will be anounced in the others machines
netbios name = SMBServer
#...#
This comment will appear in the "Network Neighborhood" Windows
server string = Samba Server de este lugar
#...#
This line is important for security reasons, to allow connections
with some specified computers in a local network.
In this example, access is granted to computers connected to 192.168.8.0 network
(commonly C class) and from "loopback" interfase. For more details, read the smb.conf
man pages
I.E: Shared resources can only be used from computers where IP address begins
with 192.168.8 and with 127 (commented sentence in the following line)
; hosts allow = 192.168.8. 127.
#...#
If you want to load automaticaly a printer list instead of write
one by one, use this:
; load printers = yes
#...#
Overwrite the printcap location (path) is possible

; printcap name = /etc/printcap

#...#
In SystemV printcap name properties for lpstat must allow
automaticaly obtain a printers list from spool system
of SystemV (good word redundance :-)
; printcap name = lpstat

#...#
It should not be necessary to specify the print system type unless it is non-standard.
Currently supported print systems are:
bsd, sysv, plp, lprng, aix, hpux, qnx
; printing = bsd

#...#
Uncomment this if you want a guest account
you must add this to /etc/passwd otherwise the user "nobody" is used
; guest account = pcguest

#...#
This is to force the use of a different log file for each computer
that will connect with the SAMBA server
log file = /var/log/samba/log.%m

#...#
Put a limitation on the size of the log files (in Kb).
max log size = 50

#...#
Read security_level.txt for more details
# Indicates the mode to do a passwords validation
User level security = each user with his password (smbpasswd)
security = user

#...#
If security = server then validation will be made using another server
Use the value "password server" only with security = server
password server = [server authentication IP address].
; password server = <NT-Server-Name>

#...#
If you want to use password encryption. Please read ENCRYPTION.TXT,
Win95.txt and WinNT.txt in the Samba documentation.
Do not enable this option unless you have enough information about this property.
Information: Win95, Win98 and WinNT sends encrypted passwords.
encrypt passwords = yes

#...#
Using the following line enables you to customize your configuration
for each machine in the network. The %m gets replaced with the netbios name
of the machine that is connecting .
; include = /usr/local/samba/lib/smb.conf.%m

#...#
Documentation and some popular "tips" says: possibly you will find
that this option gives better performance. Try it !
See speed.txt and the manual pages for details
socket options = TCP_NODELAY

#...#
Samba configuration to use multiple network interfaces

If you have multiple network interfaces then you must list them here. Like the example
Read the man page for details.
; interfaces = 192.168.8.2/24 192.168.12.2/24
#..#
Browser Control Options:
set local "master = no" if you don't want Samba to become a master browser on your network.
local master = yes
#..#
OS Level determines the precedence of this server in master browser election
Commonly, the default value should be reasonable
; os level = 33
#..#
Domain Master specifies Samba to be the Domain Master Browser.
This allows Samba to run services as domain controller and can "view" machines
in different TCP/IP subnets
Don't use this if you already have a Windows NT/2000 domain controller doing this job.
domain master = yes
#..#
Preferred Master causes Samba to force a local browser election on startup
and gives it a slightly higher chance of winning the election.
If we have more than one server, the preferred master will be the "favorite"
when clients search for a server in a list
preferred master = yes
#..#
Use this, only if you have a NT/2000 server in your network, and it is working
as a PDC (primary domain controller).
; domain controller = <NT-Domain-Controller-SMBName>
#..#
Enable this if you want to use SAMBA as "domain logon server" for
Windows 9x/Me workstations.
domain logons = yes
#..#
If you enables "domain logons" then you must to use a logon script,
for each machine or for each user in the Windows network

For specific logon batch for each workstation computer
; logon script = %m.bat

For specific logon batch for each user
; logon script = %U.bat
#..#
Where to store roving profiles (only for Win95 and WinNT)
%L substitutes this server's NetBIOS name, %U substitutes the username

You must uncomment the [Profiles] share below
; logon path = \\%L\Profiles\%U
#..#
Support for Windows Internet Name Service:
WINS Support - tells to NMBD to enables his WINS Server.
WINS protocol, converts machine names to IP addresses,
it works like DNS works with TCP/IP.

; wins support = yes

#..#

WINS Server - Tells the NMBD components of Samba to be a WINS Client

SAMBA Server can be one of these: WINS Server or WINS Client,

but NO both at the same time.

Here WINS IP Server must be specified

; wins server = 192.168.8.1

#..#

WINS Proxy - Tells Samba to answer name resolution queries on behalf of a non WINS

capable client, for this to work there must be at least one WINS Server on the network.

The default value is NO.

; wins proxy = yes

#..#

DNS Proxy - tells Samba whether or not to try to resolve NetBIOS names via DNS nslookups.

The built-in default for versions 1.9.17 is yes, this has been changed since version 1.9.18 to no.

Here we can tell to SAMBA that name resolution will be made by using DNS or not.

 # dns proxy = yes

 # dns proxy = no (name resolution will be made by using the file lmhosts)

#..#

If logon drive is not specified, the Z: unit is automounted

logon drive = P:

#..#

#When a login occurs this script is executed: /etc/samba/netlogon/SAMBA.BAT

and mount disk units by using "net use"

logon script = SAMBA.BAT

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

Personal directory for each user

Unit P:

[homes]

comment = Home Directories

browseable = no

writable = yes

readonly = no

force create mode = 0700

create mode = 0700

force directory mode = 0700

directory mode = 700

#---#

Directory for temporal files

Unit T:

[tmp]

comment = Tempora Files

path = /tmp

readonly = no
public = yes
writable = yes
force create mode = 0777
create mode = 0777
force directory mode = 0777
directory mode = 0777

#--#
CD-ROM in server
Unit L:

[cdrom]
comment = CD-ROM
path = /mnt/cdrom
public = yes
writable = no

#--#
Group, corresponding to /home/grp.name_group
/home/user/group is a link to /home/grp.name_group
grp.name_group have permissions 770
Unit G:

[group]
comment = Directory of Group
path = /home/%u/group
writable = yes
readonly = no
force create mode = 0770
create mode = 0770
force directory mode = 0770
directory mode = 0770

#--#
This unit is to store applications, installation software,
corporative software, etc.
permissions of /net and /net/install 755, i.e: here root is the owner
Unit N:

[net]
comment = Directory Net
path = /net
writable = yes
readonly = no
force create mode = 0750
create mode = 0750

```
force directory mode = 0750
directory mode = 0750


#-----------------------------------------------------------------------------------------------#
[netlogon]
comment = Logon Services in the Network
path = /etc/samba/netlogon
guest ok = yes
writable = no
locking = no
public = no
browseable = yes
share modes = no


#-----------------------------------------------------------------------------------------------#
#=========================================================#
```

Final considerations

The SAMBA package and other tools for Linux evolve continiously, therefore it is possible that some details presented here, will lose validity. In fact during the history of SAMBA evolution, some parameters names in configuration files have changed lightly, with the objective of achieving a better structure.

If you get during the SAMBA configuration some error messages about some unknown parameter, you have two simple possibilities to solve the problem:

- See the smb.conf file which is installed by default, the same one generally contains commented lines that can have some information about the "problematic parameter".
- Read the SAMBA documentation, begin with the file that describes the changes related to previous versions.

References: Bibliography and software tools

- SAMBA, official website: http://www.samba.org
- Webmin, official website: http://www.webmin.com a remote administration tool for computers running UNIX systems.
- GNU Project and Free Software Foundation: http://www.gnu.org
- An interesting website to obtain RPM packages: http://www.rpmfind.net
- LinNeighborhood home page: http://www.bnro.de/~schmidjₒan interesting Linux tool to use shared resources over "SMB networks".

Copyright Notes

SAMBA is a product distributed under GPL Licence
Linux is a registered mark of Linus Torvalds.
Solaris is operating system and registered mark of Sun Microsystems.
MS Windows is operating system and registered mark of Microsoft.
The use of SAMBA implies big savings on licence fees to Microsoft.

2005-01-14, generated by lfparser_pdf version 2.51