LinuxFocus article number 177
http://linuxfocus.org

by Éric Seigne
<erics/at/rycks.com>

About the author:

I work for the free software world and among others, I develop applications for web database access using tools such as PostGreSQL ,MySQL et PHP. To keep some freedom in my way of working (to be able to do another job from time to time... like starting a new C project) I recently started to set up my own business. To make things worse, I am -still- an ABUL member www.abul.org (and I have not yet paid my subscription!).

Translated to English by:
Georges Tarbouriech
<georges.t/at/linuxfocus.org>

Samba configuration

Abstract:

I will try to explain here the work we have done for implementing a linux-samba server used as a domain controller for a Windows network. Users permissions management, profiles... will be detailed.
This document relies on Debian GNU/Linux 2.2 what may explain that your default smb.conf file can be slightly different according to your distro.
The samba version used for this article is **2.0.7**

Installing Samba

Let’s suppose you know a little bit about samba and that it is already installed on your server.
If it is not, for a quick install, check:
Debian: apt-get install samba
RedHat(Mandrake): rpm -vih /mnt/cdrom/RedHat(Mandrake)/RPMS/samba*

The configuration file: general settings

Samba uses an unique configuration file in which you can find blocks such as [global].

Only one configuration file for samba!

```
<minimalist smb.conf file>
[global]
   printing = bsd
   printcap name = /etc/printcap
   load printers = yes
   guest account = pcguest

   log file = /usr/local/samba/log.%m

[tmp]
  comment = Temporary file space
  path = /tmp
  read only = yes
  public = yes
</file>
```

If you run samba with this configuration file, the windows machines on your local network will be able to see, in their network neighborhood, that a machine called (your linux box name) shares a temp directory in which you are allowed to write.

CAUTION: when you update the samba configuration file, you must restart samba using the */etc/init.d/samba restart* script (for debian)

The configuration file, "advanced" parameters

Let’s check the following parameters:

- Section [global]
  - **netbios name:**
    You can specify the netbios name of your samba server. You can see the netbios name in the network neighborhood from your windows machines. If you don’t give any, the linux server will get its network name as its netbios name.
  - **invalid users:**
    List of users with no access to samba. For example "root" should not be allowed.
  - **interfaces:**
    If your linux server has more than one network card and you want to restrict its activity to only one network.
  - **security:**
    Selection of the security mode to be used. Using security=user requires each user to have an

account on the GNU/Linux server.
If you don't want samba to manage the users and to share the same resource for everyone, you can select security=share.

- **workgroup:**
  Name of the workgroup your linux server must be part of.
- **server string:**
  A description for your Linux box (some string).
- **socket options:**
  A list of options to "tune" samba and make it faster, for instance.
- **encrypt passwords:**
  Must you use encrypted passwords? It is important to know that every windows system (almost) use a different scheme!
- **wins support:**
  Is your Linux server working as a wins server?
- **os level:**
  OS level to know which one will be "elected" domain master , local master, etc.
- **domain master:**
  Defines samba as domain master
- **local master:**
  Defines samba as local master server
- **preferred master:**
  Must Samba to be "preferred" among other servers if there are some?
- **domain logons:**
  Must Samba manage connection control for the whole domain?
- **logon script:**
  Which script to run for this user when opening a session?
- **logon path:**
  Where are the startup script files?
- **logon home:**
  Where to store the users profiles?
- **name resolve order:**
  What is the resource order to follow to find the name of a machine in the network?
- **dns proxy:**
  Must the samba server also be used as a DNS proxy?
- **preserve case:**
  To keep the filenames case.
- **short preserve case:**
  To keep the filenames case.
- **unix password sync:**
  Must unix and windows passwords be synchronized?
- **passwd program:**
  Which program to use for password changes.
- **passwd chat:**
  What is the chat "protocol" to change the password?
- **max log size:**
  Maximum size of the log file.

- Section [netlogon]

We specify where the netlogon is.

- Section [profiles]

  Block of users profiles.

- Section [homes]

  User’s Home directory.

Samba variables

Variable	Definition
Client variables	
%a	Client architecture Example: Win95, WfWg, WinNT, Samba ...
%I	Client IP address
%m	Client NetBios name
%M	Client DNS name
User variables	
%g	User %u primary group
%H	User %u home directory
%u	Unix current username
Share variables	
%P	Root of present share
%S	Name of present share
Server variables	
%h	DNS name of the Samba server
%L	NetBios name of the Samba server
%v	Samba version
Miscellaneous variables	
%T	Current date and time

Example using these variables: if your network hosts machines running windows 3.11 and windows 98, you can create two configuration files, one for each system, using the %a variable.

Result: our configuration file

<smb.conf file>

```
[global]
printing = bsd
printcap name = /etc/printcap
load printers = yes
guest account = nobody
invalid users = root

; fix its netbios name
netbios name = pantoufle
; this is the network to listen to
; (you don't need samba on the other network card since it manages the Internet
; connection!)
interfaces = 192.168.0.1/255.255.255.0

; security user implies that every user must have an unix account on this server
security = user

; The workgroup name to which the server belongs
workgroup = rycks
; The server description, readable when displaying the details
; %h is the DNS name of the server and %v the samba version
server string = %h server (Samba %v)

; We use the samba log file, not only the syslog one
syslog only = no

; The less important information has to be written into syslog,
; the other information is found in /var/log/smb(nmb)/
syslog = 0;

; Let's tune!
socket options = IPTOS_LOWDELAY TCP_NODELAY \
SO_SNDBUF=4096 SO_RCVBUF=4096

; We use encrypted passwords. Careful,
; every W95 client must be patched with MS SMB
; security patch.
; NT4 must be patched with SP3 or higher...
; I can't remember as far as W3.11 is concerned:
; it probably doesn't support encrypted passwords:(
encrypt passwords = yes

; This server also works as a WINS server.
; WINS allows two networks using different IP ranges
; (for example 192.168.0.0/255.255.255.0 et 192.168.0.1/255.255.255.0)
; to see the shared resources in the "other" network,
```

```
; as soon as the gateway is active.
wins support = yes

; OS level. Since our server is the domain master, local logons, etc, it is
; "higher" than the NT server, if there is one!
os level = 34

; Domain management
domain master = yes
local master = yes
preferred master = yes

; Management of domain connections
domain logons = yes

; Which script to run when a client connects?
; %g corresponds to the primary group name this user is a member
logon script = %g.bat
; In which directory can we find the startup script files?
; %L is the netbios name of the samba server
logon path=\\%L\netlogon
; Where to store the users profiles?
; %U is the user’s login
logon home=\\%L\%U\winprofile

; In which order check the resources to find
; the name of a machine?
; Note the broadcast at the end ... unlike windows
; sending broadcast on a regular basis.
name resolve order = lmhosts host wins bcast

; Must Samba be used as a DNS proxy?
dns proxy = no

; Preserve filenames and their case
preserve case = yes
short preserve case = yes

; Must we synchronize windows and linux passwords?
unix password sync = yes

; What to use for passwords synchronization
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\sUNIX\spassword:* \
%n\n *Retype\snew\sUNIX\spassword:* %n\n .

; Maximum size of the log file,
; prevents from saturating the /var directory:p
```

```
max log size = 1000

; We are a time server: good thing to synchronize
; the machines time a bit.
; We'll use this feature from the logon .bat file
time server = yes

; We specify where the netlogon is.
; It is only used at connecting time,
; thus we don't need to make it public.
[netlogon]
path = /home/netlogon/%g
public = no
writeable = no
browseable = no

; The Home directory for every user
[homes]
comment = Home Directories
browseable = no

; He can write, can't he!
read only = no

; The default unix creation umask
create mask = 0700

; For security purpose, the directory
; mask is set to 700 as well!
directory mask = 0700


; We share FTP, it's easier to have it in
; the network neigborhood than to run
; a specific program.
[ftp]
path = /home/ftp/pub
public = yes
printable = no
guest ok = yes

; The temporary directory
[tmp]
path = /tmp
public = yes
printable = no
guest ok = yes
writable = yes
```

; another special temporary directory
; for a user needing much space!
[bigtemp]
path = /home/bigtemp
public = yes
printable = no
guest ok = yes
valid users = erics
writable = yes

</smb.conf file>

What we have on the server

In short, on the server we should have:

- an account for each user
- the smb.conf file
- a /home/netlogon directory (in my example)
- a .bat file for each user group in this directory (an example is coming)
- a CONFIG.POL file for system security strategy (in this directory too).
- To create the config.pol file, search for poledit.exe found in the windows CD.

```
<file /home/netlogon/admin.bat>
net use P: \\pantoufle\homes
net use T: \\pantoufle\tmp
net time \\pantoufle /SET /YES
</file admin.bat>


<file /home/netlogon/teachers/teachers.bat>
net use P: \\pantoufle\homes
net use T: \\pantoufle\tmp
net time \\pantoufle /SET /YES
regedit /s \\pantoufle\netlogon\teachers.reg
</file teachers.bat>


<file /home/netlogon/pupils/pupils.bat>
net use P: \\pantoufle\homes
net use T: \\pantoufle\tmp
net time \\pantoufle /SET /YES
regedit /s \\pantoufle\netlogon\pupils.reg
</file pupils.bat>


<file /home/netlogon/teachers/teachers.reg>
[HKEY_CURRENT_USER\Software\Microsoft\Windows
\CurrentVersion\Explorer\User Shell Folders]
```

```
"Personal"="P:\\"
</file teachers.reg>


<file /home/netlogon/pupils/pupils.reg>
[HKEY_CURRENT_USER\Software\Microsoft\Windows
\CurrentVersion\Explorer\User Shell Folders]
"Personal"="P:\\"
</file pupils.reg>
```

This file allows to automatically mount the user's personal directory on startup as P: and the temporary directory as T:. The system time is also got from the samba server.

NOTE: the .bat file line feeds must be in "DOS mode". The easiest way is to create this file with the notepad, for instance, and then send it to the server.

Defining the system security policy (C) (TM) (R)

That's a title! Well, I borrowed it from a MS doc concerning their system policy tool.

Securing Windows, is almost possible, using a domain controller.

Thus, to create a Windows system policy, for example to prevent some users (all ?) from running regedit, a DOS program, etc, you have to use POLEDIT found in the Windows 98 CD.

Run PolEdit, watch its help, write down the information... this article is not intended to teach you how proprietary software works.

Once your .POL file is ready, copy it to your samba server, into the directory found in the [netlogon] group PATH.

CAUTION: For W9x clients, the system strategy file must be CONFIG.POL ... for WindowsNT it's another name, and since I don't have NT I can't tell you:'(
No, don't send me an NT version for testing purpose. Thanks anyway, that was very kind of you:o)

NOTE: PolEdit allows to create users groups and users, but we haven't succeeded yet. Only the default user is taken into account.

For example, if I create an "admin" group in PolEdit, allowed to run regedit, when connecting as "erics" ("admin" being its primary group), I cannot run regedit:(

Nevertheless, create an user "erics" in poledit... and it works.

Since we don't feel like creating the 1056 users with poledit and that a global users management is much more interesting, we "offer" the following trick:

To do that, we went around the problem: we made 3 config.pol files only with default users, thus, on the linux server, we have:
/home/netlogon/teachers/CONFIG.POL
/home/netlogon/teachers/teachers.bat
/home/netlogon/pupils/CONFIG.POL
/home/netlogon/pupils/pupils.bat
/home/netlogon/admin/CONFIG.POL
/home/netlogon/admin/admin.bat
And we did change the smb.conf file to make it take this into account:

<smb.conf file>
[netlogon]
; we added %g to make netlogon point to a different directory according to the
; user group, in which the config.pol file corresponds to each user profile
; group.
path = /home/netlogon/%g
public = no
writeable = no
browseable = no
</smb.conf file>

Windows machines configuration

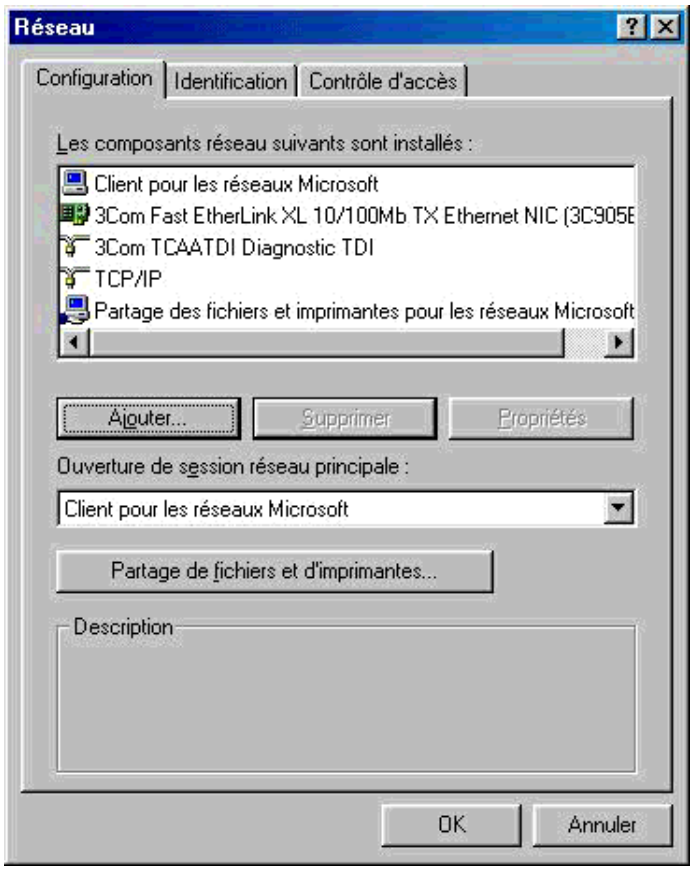
For a Win98 client type

Click on Start/Parameters/Configpanel and double-click on Network

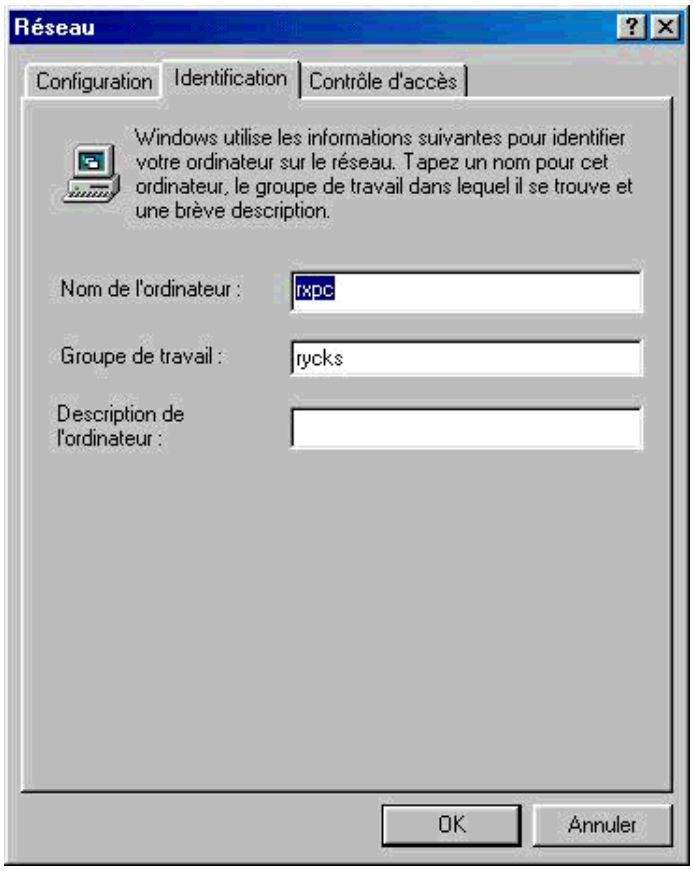
Install:

- Client for MS network
- Network card driver
- TCP/IP support and ONLY TCP/IP (no ipx or netbios)
- Files and printers sharing

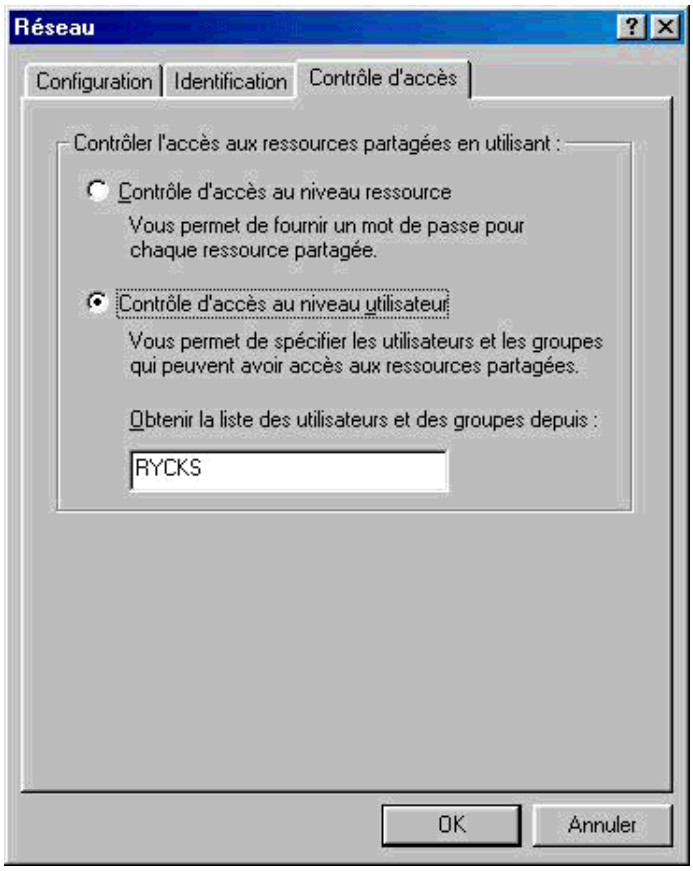
With a bit of luck, 20 mouse clicks and a reboot should be enough to configure windows!



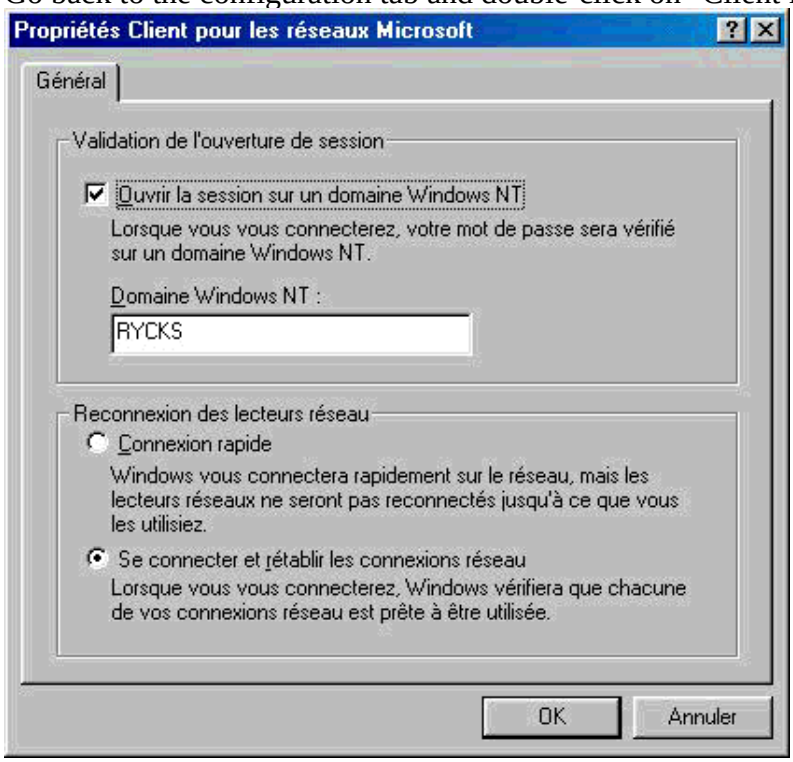
Next click on the "Identification" tab and provide the computer name and the corresponding workgroup.



Click on "Access control" and select the user level control access checkbox



Go back to the configuration tab and double-click on "Client for MS network"



Don’t forget to configure TCP/IP support:
Double-click on TCP/IP
IP address:

- the IP address you want for this machine (ex: 192.168.0.2)
- Subnetmask (ex: 255.255.255.0)

WINS configuration:

- Activate WINS resolution
- Add a WINS server, IP 192.168.0.1 (if this is the samba server IP address)
- Gateway: if you have a gateway, this is where to configure it
- DNS configuration: configure your DNS access

Notes "tuning/performances/good sense?"

At work, a bottleneck quickly appears because of the use of windows profiles.

As a matter of fact, the profile is full of stuff MS decided to be important, such as IE cache, OutLook cache, etc.

In short, this means that about 10 MB will be downloaded when connecting to a machine (however, my profile is a "classical" one, a background image, ie ans outlook...) and 10 MB will be uploaded to the server when disconnecting.

10 MB for each user, in a 15 machines room ("normal" size of a lab, for instance), makes 150 MB, and if the building holds 10 rooms... just calculate the users disconnecting time when the bell rings.

You then should anticipate and log out at to 5... (well, I must admit that is what I was doing when I was a student)... rather than at past 5. It’s a bit like the big cities traffic jam: better to go either 10 minutes before or 2 hours after!

So, according to the policy you implement, it could be a good idea to mount the home directory to P: (for example, P as Personal) for everyone and teach the users: "save your documents into P and not in "My documents", otherwise you won’t get them back".

Next, you have to find the software able to be configured to have its bookmarks in P:\bookmarks.html and so on for the parameters.

I don’t even know if this exists in the windows world!

If you are aware of a solution, write an article from it, this is a knowledge to share!

Questions and suggestions for a follow-up

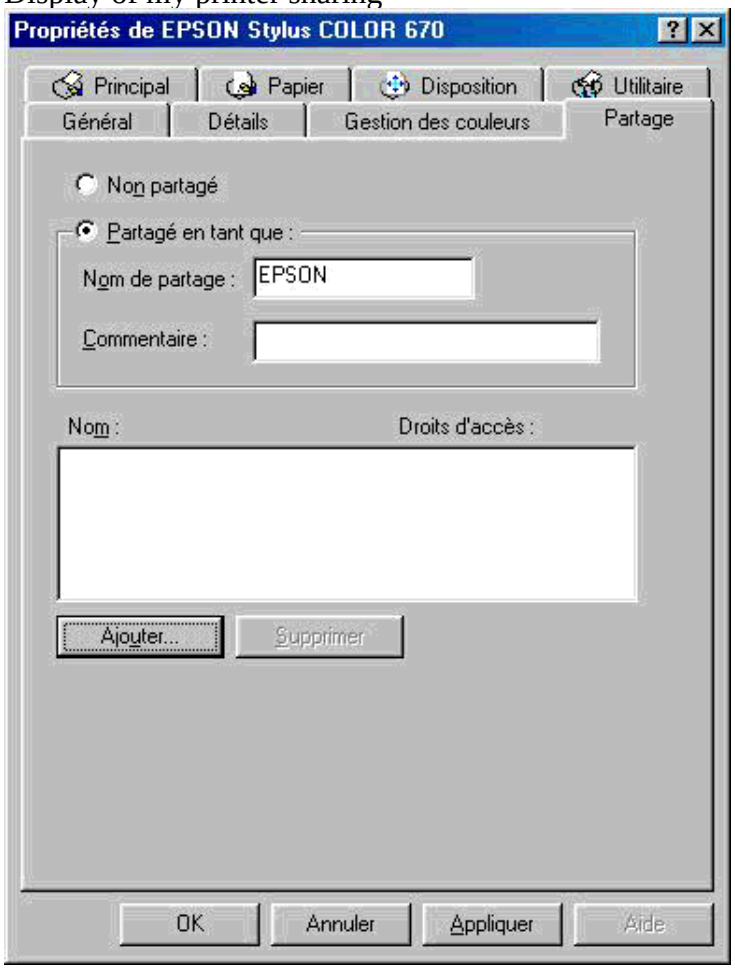
Is it possible to have various workgroups on the same domain, how can this be managed, is it possible to share the problems between various GNU/Linux Samba?

How to use both NT and Samba servers?

NT clients configuration: the equivalent of CONFIG.POL has another name under NT.

A real problem when only having a Samba server (and no NT): I'm working under W98 and I want to share a local resource, my printer for instance:

Display of my printer sharing



Following the click on the Add button...

HOT NEWS: someone gave me the solution. Enough to select "resource level access control" during step 3 of the windows configuration.

Acknowledgements

Bruno <bcarrere(at)asp-france.fr> for his proofreading work and his precious help:o)

JohnPerr for urging me to write my first article for LinuxFocus, and to have translated it to English.
Michel Billaud aka MiB for all the solutions he found to our problems; he teaches us with tips like strace, etc.:o)
Etienne, Éric, and the invisible man I forgot the name, sorry for that! Then, thank you to have shared your knowledge from MS courses about NT servers.
Jean Peyratout, do we need to say why? It would be much too long.
The Abul generally speaking
Rycks to provide me with time and resources to develop and document free software.

Resources

Onlin O'Reilly book: http://www.oreilly.com/catalog/samba/chapter/book/index.html

This document will be updated at the rycks.com documentation section

---

Translation information:
fr --> -- : Éric Seigne <erics/at/rycks.com>
fr --> en: Georges Tarbouriech <georges.t/at/linuxfocus.org>

2005-01-14, generated by lfparser_pdf version 2.51