by Éric Seigne
<erics/at/rycks.com>

About the author:

Ich beteilige mich an der Freien Software Welt und entwickle neben vielen anderen Sachen z.B. Applikationen für den webbasierten Datenbankzugriff und benutze dabei vorallem PostGreSQL, MySQL und PHP.
Um mir die nötige Freiheit für meine Projekte zu erhalten (und ab und zu mal ein neues C Projekt zu initiieren) habe ich mich kürzlich selbstständig gemacht.
Na gut, eigentlich bin ich immer noch ein ABUL Mitglied und habe bis jetzt nicht mal meine Anmeldegebühr bezahlt!

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

Samba Konfiguration

Abstract:

Mit diesem Artikel möchte ich über die von uns durchgeführten Schritte berichten, um einen Linux−Samba Server als Domain Controller für ein Windows Netzwerk aufzusetzen.
Es ging dabei um Management von Benutzerrechten und Profilen... doch dazu später mehr.
Diese Beschreibung basiert auf Debian GNU/Linux 2.2 und Samba Version **2.0.7**. Deshalb könnte sich die smb.conf Datei bei anderen Distributionen natürlich leicht unterscheiden.

Installation von Samba

Gehen wir mal davon aus, dass Sie schon ein wenig über Samba wissen und die nötigen Pakete bereits auf ihrem Server installiert sind.
Falls nicht, dann hier mal kurz und knapp die entsprechenden Anweisungen:
Debian: apt−get install samba

RedHat (Mandrake): rpm −vih /mnt/cdrom/RedHat(Mandrake)/RPMS/samba*

Die Konfigurationsdatei: allgemeine Einstellungen

Samba benutzt lediglich eine einzige Konfigurationsdatei. In dieser Datei werden Blöcke wie [global] definiert.

Nur eine Konfigurationsdatei für Samba!

```
<minimalistische smb.conf Datei>
[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
</Datei>
```

Startet man Samba mit dieser Konfiguration, dann sind die Windows Maschinen in der Lage, in ihrer Netzwerkumgebung eine weitere Maschine (Name des Linux Rechners) zu sehen, die ein Verzeichnis temp teilt und auf dieses Schreibzugriff gewährt.

ACHTUNG: wenn man die Konfigurationsdatei geändert hat, muss man Samba neustarten, z.B. über das */etc/init.d/samba restart* Skript (für Debian)

Die Konfigurationsdatei, "erweiterte" Parameter

- Abschnitt [global]
  - **netbios name:**
    Man kann den netbios Namen des Samba Servers angeben. Dieser Name wird in der Netzwerkumgebung der Windows Maschinen angezeigt. Wird kein Name vergeben, so wird der Netzwerkname des Linux Servers genutzt.
  - **invalid users:**
    Liste mit Nutzer ohne Zugriff auf Samba. So sollte z.B. "root" keinen Zugriff bekommen.
  - **interfaces:**
    Falls der Linux Server über mehr als nur eine Netzwerkkarte verfügt und man die Aktivitäten auf einzelne Netzwerke beschränken möchte.
  - **security:**
    Auswahl des Sicherheitsmodus. Für security=user muss jeder Nutzer ein Nutzerkonto auf

dem GNU/Linux Server haben.
Soll Samba die Nutzer nicht verwalten und möchte man für alle Nutzer die gleichen Ressourcen zur Verfügung stellen, dann sollte man security=share nutzen.

- **workgroup:**
  Name der Arbeitsgruppe, zu der der Linux Server gehören soll.
- **server string:**
  Eine Beschreibung des Linux Servers (einige Zeichen).
- **socket options:**
  Einige Optionen um Samba zu tunen, damit es noch schneller arbeitet. (z.B. für Instanzen)
- **encrypt passwords:**
  Sollen Passwörter verschlüsselt werden? Wichtig, fast jedes Windows System benutzt dazu ein anderes Verfahren!
- **wins support:**
  Arbeitet der Linux Server als ein WINS Server?
- **os level:**
  OS Ebene, um zu wissen, wer als Domain Master, Lokal Master, usw. gewählt wird.
- **domain master:**
  Samba als Domain Master definieren.
- **local master:**
  Samba als Lokal Master definieren.
- **preferred master:**
  Soll Samba gegenüber anderen Servern (falls vorhanden) bevorzugt werden?
- **domain logons:**
  Soll Samba die komplette Verbindungskontrolle für die ganze Domain verwalten?
- **logon script:**
  Welches Logon Skript für Nutzer ausführen?
- **logon path:**
  Wo sind die Startdateien?
- **logon home:**
  Wo werden die Nutzerprofile abgelegt?
- **name resolve order:**
  Wie ist die Reihenfolge um einen Namen einer Maschine im Netzwerk zu ermitteln?
- **dns proxy:**
  Soll Samba auch als DNS Proxy benutzt werden?
- **preserve case:**
  Dateinamen sollen beibehalten werden.
- **short preserve case:**
  Dateinamen sollen beibehalten werden.
- **unix password sync:**
  Sollen UNIX und Windows Passwörter synchronisiert werden?
- **passwd program:**
  Welches Programm soll für Passwortänderungen genutzt werden?
- **passwd chat:**
  Welches "CHAT Protokoll" soll für Passwortänderungen benutzt werden?
- **max log size:**
  Maximale Größe der Log Datei

- Abschnitt [netlogon]

  Angabe, wo das netlogon ist.
- Abschnitt [profiles]

  Block mit Benutzerprofilen.

- Abschnitt [homes]

  Home Verzeichnisse der Nutzer.

Samba Variablen

Variable	Definition
Client Variablen	
%a	Client Architektur Beispiel: Win95, WfWg, WinNT, Samba ...
%I	Client IP Adresse
%m	Client NetBios Name
%M	Client DNS Name
Benutzer Variablen	
%g	Benutzer %u Hauptgruppe
%H	Benutzer %u Homeverzeichnis
%u	aktueller Unix Benutzername
Freigabe Variablen	
%P	Wurzel der aktuellen Freigabe
%S	Name der aktuellen Freigabe
Server Variablen	
%h	DNS Name des Samba Servers
%L	NetBios Name des Samba Servers
%v	Samba Version
verschiedene Variablen	
%T	aktuelles Datum und Zeit

Beispiel zur Nutzung dieser Variablen: wenn auf dem Netzwerk sowohl Windows 3.11 als auch Windows 98 Maschinen laufen, legt man für jedes System eine eigene Konfigurationsdatei über die %a Variable an.

Ergebnis: unsere Konfigurationsdatei

<smb.conf Datei>

```
[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 Datei>

Was auf dem Server sein sollte

Man könnte sagen, auf dem Server müssen folgende Dinge sein:

- ein Konto für jeden Nutzer
- die smb.conf Datei
- ein /home/netlogon Verzeichnis (laut meinem Beispiel)
- eine .bat Datei für jede Benutzergruppe in diesem Verzeichnis (Beispiel folgt)
- eine CONFIG.POL Datei für die Systemsicherheitsstrategie (ebenfalls in diesem Verzeichnis)

- um die config.pol Datei anzulegen, sollte man nach dem Tool poledit.exe auf einer Windows CD suchen

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

<Datei /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
</Datei teachers.bat>

<Datei /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
</Datei pupils.bat>

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

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

Diese Datei mounted automatisch das Homeverzeichnis des Nutzers auf Laufwerk P: und das temporäre Verzeichnis auf Laufwerk T:. Weiterhin wird die Systemzeit mit dem Samba Server synchronisiert.

HINWEIS: in der .bat Datei müssen Zeilenumbrüche im "DOS Modus" gesetzt werden. Das geht am einfachsten, indem man die Datei mit dem Notepad anlegt und dann auf den Server hochlädt.

Die System Sicherheitsstrategie (C) (TM) (R) festlegen

Es ist möglich, Windows über einen Domain Controller abzusichern.

Dieser Abschnitt besteht eigentlich nur aus einer Überschrift. Schlimmer noch, die Überschrift stammt nicht mal von mir, sondern ich habe sie aus einem MS Dokument über das System Sicherheitswerkzeug geborgt.

Um eine Windows System Sicherheitstrategie anzulegen, z.B. dass nur einige Nutzer (oder eben alle) keinen Zugriff auf regedit, DOS Programme, usw. erhalten, muss man das Programm POLEDIT, welches man auf der Windows 98 CD findet, verwenden.

PolEdit starten, die Hilfe lesen, Informationen notieren... dieser Artikel soll nicht zeigen, wie proprietäre Software zu bedienen ist.

Sobald man eine funktionierende .pol Datei hat, muss man sie auf den Samba Server in das entsprechnede Verzeichnis (Abschnitt [netlogon] group PATH) kopieren.

ACHTUNG: Für W9x Clients muss die Datei config.pol heißen. Für Windows NT ist es ein anderer Name, den ich aber nicht kenne, da ich kein NT habe. :'(
Äähh, nein, bitte mir keine NT Version für Testzwecke senden. Trotzdem danke, das war sehr freundlich gemeint :o)

HINWEIS: PolEdit ermöglicht die Einrichtung von Benutzern und Benutzergruppen. Das haben wir aber noch nicht umsetzen können und wir haben so immer den Standardbenutzer verwendet.

Beispiel: Legt man mit PolEdit eine "admin" Gruppe an, der Zugriff auf regedit gewährt wird, und stellt man dann eine Verbindung z.B. als Nutzer "erics" (dessen primäre Gruppe natürlich "admin" ist) her, kann man trotzdem regedit nicht starten. :(

Wie auch immer, einen Nutzer "erics" in poledit anlegen... und es funktioniert.

Da uns irgendwie nicht danach war, mit PolEdit 1056 Benutzer anzulegen und da wir eigentlich ein globales Management bevorzugen würden, haben wir uns folgenden Trick ausgedacht:

Um das zu machen, haben wir das Problem einfach umgangen: Wir haben 3 config.pol Dateien angelegt, jeweils mit einem Standardnutzer. Auf dem Linux Server sieht das dann so aus:
/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
Weiterhin haben wir die smb.conf Datei abgeändert, um dies zu berücksichtigen:

<smb.conf Datei>
[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 Datei>

Konfiguration der Windows Rechner

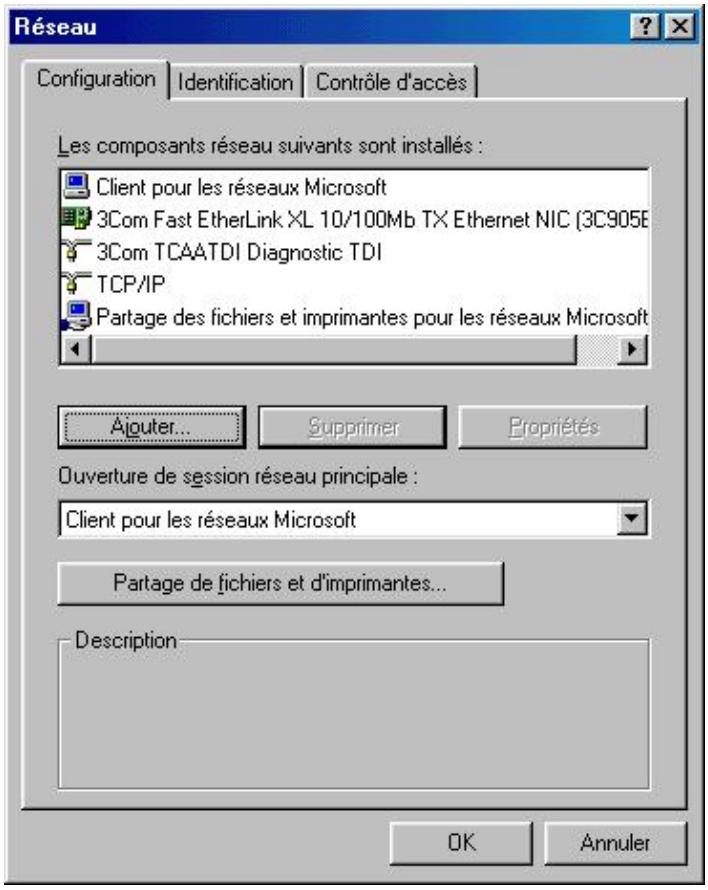
Mit etwas Glück, 20 Mausklicks und einem Neustart, sollte Windows erfolgreich konfiguriert sein!

für einen Win98 Client

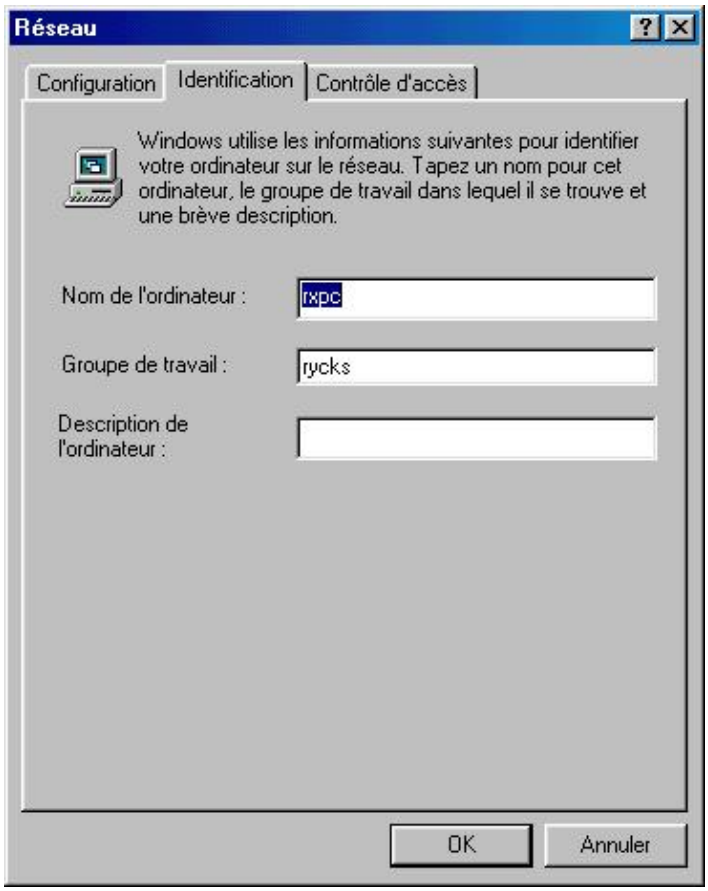
Klick auf Start/Einstellungen/Systemsteuerung und Doppelklick auf Netzwerk

Install:

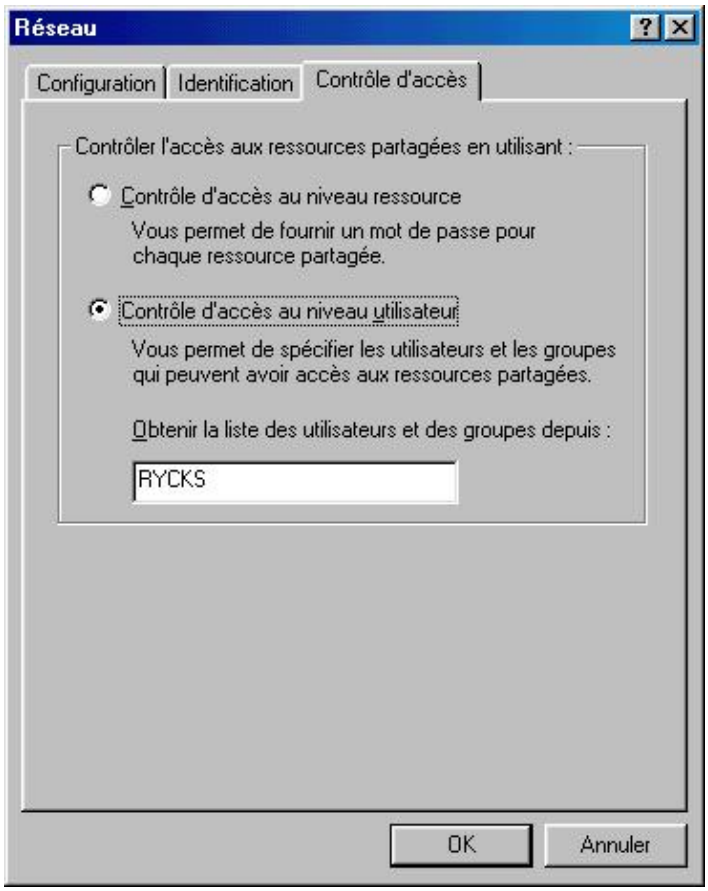
- Client für MS Netzwerk
- Netzwerkkartentreiber
- Unterstützung für TCP/IP und wirklich NUR TCP/IP (kein IPX oder Netbios)
- Datei– und Druckerfreigabe



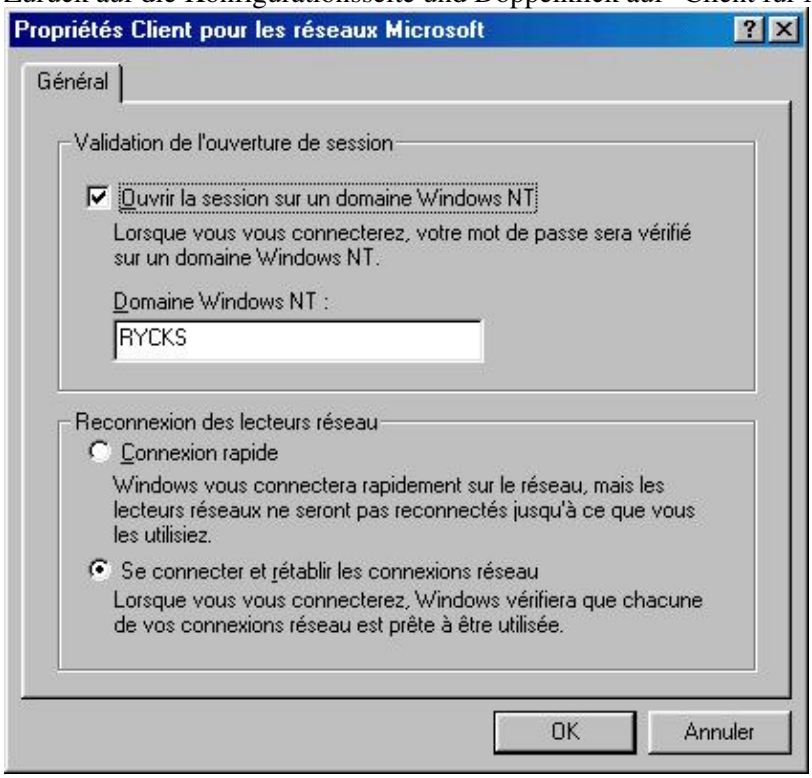
Jetzt auf "Identifikation" klicken und den Computernamen sowie die Arbeitsgruppe angeben.



Klick auf "Zugriffkontrolle" und Checkbox "Zugriff auf Benutzerebene" ("user level control access") aktivieren



Zurück auf die Konfigurationsseite und Doppelklick auf "Client für MS Netzwerk"



TCP/IP Unterstützung nicht vergessen:
Doppelklick auf TCP/IP
IP Adresse:

- die IP Adresse für diese Maschine (z.B.: 192.168.0.2)
- Subnetmask (z.B.: 255.255.255.0)

WINS Konfiguration:

- WINS Auflösung aktivieren
- WINS Server hinzufügen, IP 192.168.0.1 (falls das die IP des Samba Servers ist)
- Gateway: falls ein Gateway vorhanden ist, kann es hier konfiguriert werden
- DNS Konfiguration: DNS Zugriff hier konfigurieren

Hinweise zum tunen – überhaupt sinnvoll?

Bei der Arbeit bemerkt man schnell einen Flaschenhals, nämlich die Nutzung von Windows Profilen.

Weil MS es für richtig hält, ist das Profil voll mit verschiedenem Müll wie Cachedateien vom IE und von Outlook etc.

Das bedeutet, beim Login werden erst mal 10 MB vom Server geladen und beim Logout 10 MB wieder hoch (mein Profil ist ein ganz klassisches mit einem Hintergrundbild, IE und Outlook).

10 MB für jeden Nutzer bei 15 Maschinen pro Raum (normale Größe eines Labors z.B.), macht 150 MB, und ein Gebäude mit 10 Räumen... einfach mal zusammenrechnen und sich vorstellen, was passiert, wenn die Klingel läutet.

Man sollte dann schnell nachgeben und sich kurz vor 5 ausloggen (ich muss gestehen, so habe ich es immer als Student gemacht), denn kurz nach 5. Es ist wie mit dem Berufsverkehr: lieber 10 Minuten eher unterwegs sein als alle anderen oder eben 2 Stunden später!

Abhängig von der umgesetzten Strategie ist es eine gute Idee, das Homeverzeichnis auf ein Laufwerk zu mounten (z.B. P: für Personal) und jedem zu sagen: "speichert eure Dokumente auf P und nicht in "Meine Dateien", sonst seht ihr sie nie wieder!".

Weiterhin sollte man dann sich auf die Suche nach einer Software machen, der man das Verzeichnis zu den Lesezeichen per Parameter angeben kann und diese dann auch auf P: ablegen.

Keine Ahnung, ob sowas in der Windows Welt überhaupt existiert!

Sollte jemanden eine Lösung kennen, dann schnell einen Artikel schreiben. Das ist Wissen, was man teilen sollte!

Fragen und Vorschläge für anschließende Artikel

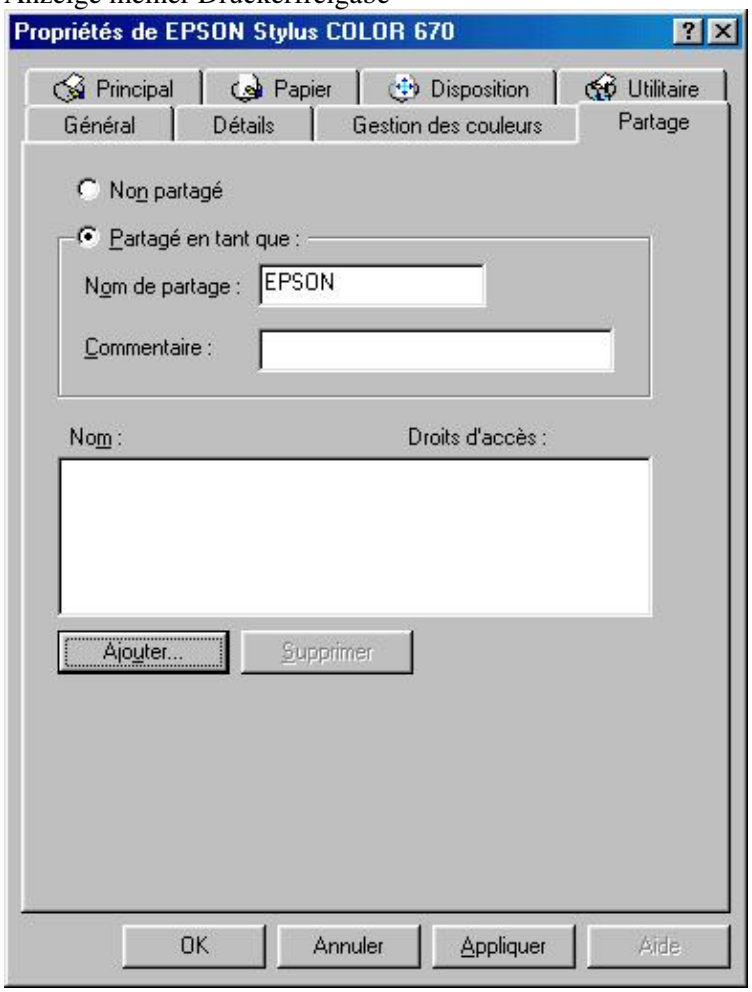
Ist es möglich, mehrere Arbeitsgruppen in der gleichen Domain zu haben? Wie kann man das verwalten und kann man die Probleme auf mehrere GNU/Linux Samba Server verteilen?

Wie kann man NT und Samba Server zusammen nutzen?

NT Clients Konfiguration: das Äquivalent zu CONFIG.POL hat unter NT einen anderen Namen.

Ein echtes Problem ist, wenn man nur Samba Server (und kein NT) hat: Ich arbeite unter W98 und möchte eine lokale Ressource freigeben, z.B. meinen Drucker:

Anzeige meiner Druckerfreigabe



Klickt man nun auf den "Hinzufügen" Button...

Brandaktuelle Neuigkeit: mir hat jemand die Lösung gegeben. Es reicht während der Windows Konfiguration Schritt 3 "resource level access control" zu aktivieren.

Danksagungen

Bruno <bcarrere(at)asp−france.fr> für Korrekturlesen und seine aufopferungsvolle Hilfe :o)

JohnPerr, dass er mich lange überredet hat, meinen ersten Artikel für den LinuxFocus zu schreiben und diesen ins Englische zu übersetzen.
Michel Billaud aka MiB für alle seine Hinweise und Lösungen; er hat uns gezeigt, wie nützlich z.B. strace, etc. sein kann :o)
Etienne, Éric, und der unsichtbare Mann, ich habe leider den Namen vergessen, Entschuldigung! Danke, dass ihr euer Wissen von MS NT Kursen mit uns geteilt habt.
Jean Peyratout, soll ich wirklich sagen warum? Es wäre eine viel zu lange Liste.
The Abul, allgemeine Hilfe
Rycks für die Unterstützung mit Zeit und Ressourcen, damit ich Freie Software entwickeln und dokumentieren kann.

Resourcen

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

Neue Versionen dieses Dokuments werden zu finden sein unter: rycks.com Dokumentationsberiech

---

2005−01−11, generated by lfparser_pdf version 2.51