door Éric Seigne
<erics/at/rycks.com>

Over de auteur:

Ik werk onder andere aan gratis software, Ik ontwikkel applicaties die database toegang via browsers mogelijk maken met behulp van tools als PostGresSQL, MySQL en PHP. Om zelf te kunnen bepalen waaraan ik werk (om een beetje afwisseling in m'n werk aan te brengen... zoals het beginnen aan een nieuw project in C) ben ik recentelijk begonnen aan het opstarten van m'n eigen bedrijf. En om het nog erger te maken... Ik ben - nog steeds - lid van ABUL www.abul.org (en ik heb m'n lidgeld nog niet betaald!).

Vertaald naar het Nederlands door:
Hendrik-Jan Heins
<hjh/at/passys.nl>

Samba configuratie

Kort:

Ik zal hier proberen uit te leggen wat we gedaan hebben om een linux-samba server, die de rol van domain controller heeft, te implementeren in een Windows netwerk.
Toegangsbeheer voor gebruikers, profielen... daar zal tot in detail op worden ingegaan.
Voor dit document heb ik gebruik gemaakt van Debian GNU/Linux 2.2; dat verklaart dan meteen hoe het komt dat de standaard smb.conf bestand op jouw systeem er wat anders kan uitzien.
De Samba versie die is gebruikt voor dit artikel is **2.0.7**

Samba installeren

Laten we er vanuit gaan dat je al het één en ander weet over Samba en dat het al geïnstalleerd is op je server.
Als dit nog niet het geval is, kan je voor een snelle installatie het volgende doen:
Debian: apt-get install samba
RedHat(Mandrake): rpm -vih /mnt/cdrom/RedHat(Mandrake)/RPMS/samba*

Het configuratiebestand: algemene instellingen

Samba maakt gebruik van een enkel configuratiebestand. In dit bestand kan je secties vinden zoals [global].

Er is slechts één configuratiebestand voor Samba!

```
<een klein smb.conf bestand>
[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
</bestand>
```

Wanneer je Samba draait met dit configuratiebestand, kunnen de Windows computers binnen je lokale netwerk, in hun netwerkomgeving, een computer genaamd (de naam van je Linux machine) zien die een tijdelijke directory (temp) deelt, waarnaar geschreven kan worden.

PAS OP: wanneer je het Samba configuratiebestand wijzigt, moet je Samba opnieuw opstarten met behulp van het */etc/init.d/samba restart* script (dit geldt voor Debian).

Het configuratiebestand; "geadvanceerde" instellingen

Laten we eens gaan kijken naar de volgende instellingen:

- Sectie [global]
  - **netbios name:**
    Je kan de netbios naam van je Samba server hier aangeven. Je kan de netbios naam van je

machine zien in de netwerkomgeving van je Windows computers. Als je geen netbios naam opgeeft, zal de Linux server z'n netwerknaam als netbios naam opgeven.

- **invalid users:**
  Een lijst van gebruikers die geen toegang hebben tot Samba. "root" zou bijvoorbeeld niet toegestaan moeten worden.
- **interfaces:**
  Wanneer je Linux server meer dan 1 netwerkkaart heeft en je wilt Samba slechts op een bepaald deel van je netwerk laten draaien.
- **security:**
  Mogelijkheid om het beveiligingsniveau in te stellen. Het gebruik van security=user vereist een account voor iedere gebruiker op de GNU/Linux server.
  Als je niet wilt dat Samba het beheer regelt met behulp van gebruikers, maar z'n bronnen voor iedereen ter beschikking stelt, dan moet je security=share kiezen.
- **workgroup:**
  Naam van de werkgroep waartoe je Linux server behoort.
- **server string:**
  Een omschrijving van je Linux machine (wat je maar wilt).
- **socket options:**
  Een lijst met opties om Samba te optimaliseren en sneller te maken.
- **encrypt passwords:**
  Moet je gecodeerde wachtwoorden gebruiken? Het is van belang dat je weet dat (bijna) iedere Windows versie een andere codering gebruikt!
- **wins support:**
  Is je Linux server ook ingesteld als een wins server?
- **os level:**
  OS level geeft aan welke machine wordt "verkozen" tot domain master , local master, enz.
- **domain master:**
  Geeft aan of Samba een domain master is
- **local master:**
  Geeft aan of Samba een local master is
- **preferred master:**
  Is Samba de "preferred" master boven andere servers, als die er zijn?
- **domain logons:**
  Moet Samba de verbindingen beheren voor het hele domein?
- **logon script:**
  Welk script moet er gedraaid worden voor een bepaalde gebruiker wanneer hij inlogt?
- **logon path:**
  Waar staan de opstart-script bestanden?
- **logon home:**
  Waar moeten de gebruikersprofielen bewaard worden?
- **name resolve order:**
  In welke volgorde moet er gezocht worden naar de naam van een machine in het netwerk?
- **dns proxy:**
  Moet de Samba server ook dienen als DNS proxy?
- **preserve case:**
  Om bestandsnamen in hoofd- of kleine letters weer te blijven geven.
- **short preserve case:**

Om bestandsnamen te behouden zoals ze zijn.
    - **unix password sync:**
      Moeten Unix en Windows wachtwoorden tegelijkertijd worden gewijzigd?
    - **passwd program:**
      Welk programma moet er bij het wijzigen van wachtwoorden worden gebruikt?
    - **passwd chat:**
      Wat is het "chat protocol" om een wachtwoord te wijzigen?
    - **max log size:**
      De maximale grootte van het log bestand.
- Sectie [netlogon]

  We geven aan waar de netlogon staat.

- Sectie [profiles]

  De sectie die de gebruikersprofielen bevat.

- Sectie [homes]

  De Home directory van gebruikers.

Samba variabelen

Variable	Definition
Client variabelen	
%a	Client architectuur Bijvoorbeeld: Win95, WfWg, WinNT, Samba ...
%I	Client IP adres
%m	Client NetBios naam
%M	Client DNS naam
Gebruikersvariabelen	
%g	De %u primaire groep waartoe de gebruiker behoort
%H	De %u home directory van de gebruiker
%u	De nu gebruikte Unix gebruikersnaam
Share variabelen	
%P	Root van de huidige share
%S	Naam van de huidige share
Server variabelen	
%h	DNS naam van de Samba server
%L	NetBios naam van de Samba server
%v	Samba versie
Overige variabelen	
%T	Huidige datum en tijd

Een voorbeeld dat gebruik maakt van deze variabelen: wanneer je netwerk gebruik maakt van zowel Windows 3.11 als Windows 98 machines, dan kan je twee configuratie bestanden aanleggen, een voor ieder systeem, door gebruik te maken van de %a variabele.

Het resultaat: ons configuratiebestand

<smb.conf bestand>

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

; verander de netbios naam
netbios name = pantoffel
; dit is het netwerk waar aan gekoppeld moet worden
```

; (je hebt Samba niet nodig op de andere netwerkkaart, aangezien die gebruikt wordt ; voor de internetverbinding
!)
interfaces = 192.168.0.1/255.255.255.0

; security user houdt in dat iedere gebruiker een unix account op deze server moet hebben ; (noot van de vertaler: kan ook d.m.v. PAM-module)
security = user

; De naam van de werkgroep waartoe de server behoort
workgroup = rycks
; De omschrijving van de server, die zichtbaar wordt wanneer de details worden opgevraagd
; %h is de DNS naam van de server en %v is de Samba versie
server string = %h server (Samba %v)

; We gebruiken het Samba log bestand, niet alleen het syslog log bestand
syslog only = no

; De minder belangrijke informatie wordt weggeschreven naar syslog,
; meer informatie kan worden gevonden in /var/log/smb(nmb)/
syslog = 0;

; Laten we eens wat gaan optimaliseren!
socket options = IPTOS_LOWDELAY TCP_NODELAY \
SO_SNDBUF=4096 SO_RCVBUF=4096

; We gebruiken gecodeeerde wachtwoorden. Pas Op,
; iedere W95 client moet worden opgelapt met de MS SMB
; veiligheidspatch.
; NT4 moet worden opgelapt met SP3 of hoger...
; Ik weet niet precies hoe het zit met W3.11:
; dit maakt waarschijnlijk geen gebruik van gecodeerde wachtwoorden:(
encrypt passwords = yes

; Deze server is ook WINS server.
; WINS laat twee netwerken die verschillende IP bereiken gebruiken
; (bijvoorbeeld 192.168.0.0/255.255.255.0 en 192.168.0.1/255.255.255.0)
; gedeelde bronnen (shares) in het "andere netwerk" zien,
; zodra de gateway actief is.
wins support = yes

; OS level. Aangezien onze server domain master is, lokale logons, enz, is z’n niveau
; "hoger" dan dat van de NT server, als die er mocht zijn!
os level = 34

; Domain management
domain master = yes
local master = yes

```
preferred master = yes

; Beheer van domain verbindingen
domain logons = yes

; Welk script moet er gedraaid worden wanneer een client verbinding maakt?
; %g correspondeert met de naam van de primaire groep waar deze gebruiker lid van is
logon script = %g.bat
; In welke directory kunnen we de opstart script bestanden vinden?
; %L is de netbios naam van de Samba server
logon path=\\%L\netlogon
; Waar worden de gebruikersprofielen opgeslagen?
; %U is de login van de gebruiker
logon home=\\%L\%U\winprofile

; In welke volgorde worden de bronnen aangesproken om de naam
; van een machine te vinden?
; Let op de "broadcast" aan het einde ... anders dan bij Windows
; stuurt Samba regelmatig een "broadcast".
name resolve order = lmhosts host wins bcast

; Moet Samba worden gebruikt als DNS proxy?
dns proxy = no

; Behoud de bestandsnamen en hun hoofd- of kleien letters
preserve case = yes
short preserve case = yes

; Moeten we Windows en Linux wachtwoorden tegelijk wijzigen?
unix password sync = yes

; Wat moet er gebruikt worden om de wachtwoorden gelijk te houden?
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\sUNIX\spassword:* \
%n\n *Retype\snew\sUNIX\spassword:* %n\n .

; De maximale grootte van het log bestand,
; zorgt ervoor dat de /var directory niet te groot wordt :p
max log size = 1000

; We hebben een tijdserver: slim om tijd/datum gelijk te laten lopen
; op alle machines.
; We zullen deze mogelijkheid gebruiken via het logon .bat bestand
time server = yes

; We geven aan waar de netlogon staat.
; Die wordt alleen gebruikt tijdens het aanmaken van de verbinding,
; dus de directory hoeft niet voor iedereen gedeeld te worden.
```

```
[netlogon]
path = /home/netlogon/%g
public = no
writeable = no
browseable = no

; De Home directory voor iedere gebruiker
[homes]
comment = Home Directories
browseable = no

; Hij kan schrijven, of niet?
read only = no

; Het standaard Unix umask
create mask = 0700

;Om veiligheidsredenen, wordt het masker voor de directory
; ook op 700 gezet!
directory mask = 0700


; We delen FTP, het is eenvoudiger om dit beschikbaar te hebben
; in de netwerkomgeving dan om een
; apart programma te draaien.
[ftp]
path = /home/ftp/pub
public = yes
printable = no
guest ok = yes

; De tijdelijke directory
[tmp]
path = /tmp
public = yes
printable = no
guest ok = yes
writable = yes

; een andere speciale tijdelijke directory
; voor een gebruiker die veel ruimte nodig heeft!
[bigtemp]
path = /home/bigtemp
public = yes
printable = no
guest ok = yes
valid users = erics
writable = yes
```

</smb.conf bestand>

Wat we op de server hebben

In het kort, zouden we het volgende op de server moeten hebben:

- Een account voor iedere gebruiker.
- Het smb.conf bestand.
- Een /home/netlogon directory (in mijn voorbeeld).
- Een .bat bestand voor iedere gebruikersgroep in deze directory (een voorbeeld volgt straks).
- Een CONFIG.POL bestand voor de beveiligings-strategie van het systeem (in dezelfde directory).
- Om een config.pol bestand te kunnen maken. moet je zoeken naar poledit.exe op de Windows CD.

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


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


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


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


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

Dit bestand maakt het mogelijk om automatisch de eigen directory van een gebruiker als P: te "mounten" bij het opstarten, en de ’tmp’ directory als T:. De systeemtijd komt ook van de Samba server.

Opmerking: De regels in het .bat bestand moeten in "DOS modus" worden gegeven. De eenvoudigeste manier hiervoor is het maken van dit bestand met, bijvoorbeeld, het kladblok, en het daarna naar de server te sturen.

Het definiëren van het veiligheidsbeleid van het systeem (C) (TM) (R)

Dat is nog eens een titel! Eigenlijk heb ik die "geleend" van een MS document over hun systeembeveiligings-beleids gereedschap.

Met een domain controller wordt het bijna mogelijk om Windows te beveiligen.

Dus, om een Windows systeembeleid op te zetten, om bijvoorbeeld sommige gebruikers (allemaal?) het niet toe te staan om regedit, een DOS programma, te draaien, moet je POLEDIT dat op de Windows CD staat, gebruiken.

Start POLEDIT, bekijk z’n help bestanden, schrijf de gegevens op... dit artikel is niet bedoeld om je te leren hoe dit soort software werkt.

Zodra je .POL bestand klaar is, moet je het naar de Samba server kopiëren, in de directory die staat in het [netlogon] groep PATH.

LET OP: Voor W9x clients moet het systeem strategie bestand CONFIG.POL heten ... voor WindowsNT moet het een andere naam krijgen, en aangezien ik geen gebruik maak van NT kan ik je niet vertellen welke :’(
Nee, stuur me geen NT versie om te testen. Toch bedankt voor het aanbod :o)

Opmerking: POLEDIT maakt het mogelijk om gebruikers en groepen aan te maken, maar we zijn er nog niet. Er wordt alleen rekening gehouden met de standaard gebruiker.

Wanneer ik, bijvoorbeeld een "admin" groep aanmaak in POLEDIT, die regedit mag draaien, en ik log in als "erics" (die "admin" als primaire groep heeft), kan ik nog geen regedit draaien:(

Echter, wanneer je een gebruiker "erics" aanmaakt in POLEDIT... werkt het wel.

Aangezien we er niet van houden om 1056 gebruikers aan te maken met POLEDIT en aangezien een globaal ingesteld gebruikersbeheer veel interresanter is, "bieden we een truc aan":

We moeten het probleem anders benaderen: we hebben 3 config.pol bestanden gemaakt met slechts standaard gebruikers, dus, op de Linux server hebben we nu:
/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
En we moesten het smb.conf bestand veranderen om dit voor elkaar te kunnen krijgen:

<smb.conf bestand>
[netlogon]
; we hebben %g toegevoegd om netlogon naar een andere directory te laten wijzen volgens
; gebruikersgroep, waarin het config.pol bestand staat dat correspondeert met iedere
; gebruikersgroep.
path = /home/netlogon/%g
public = no
writeable = no
browseable = no
</smb.conf bestand>

Windows machine configuratie

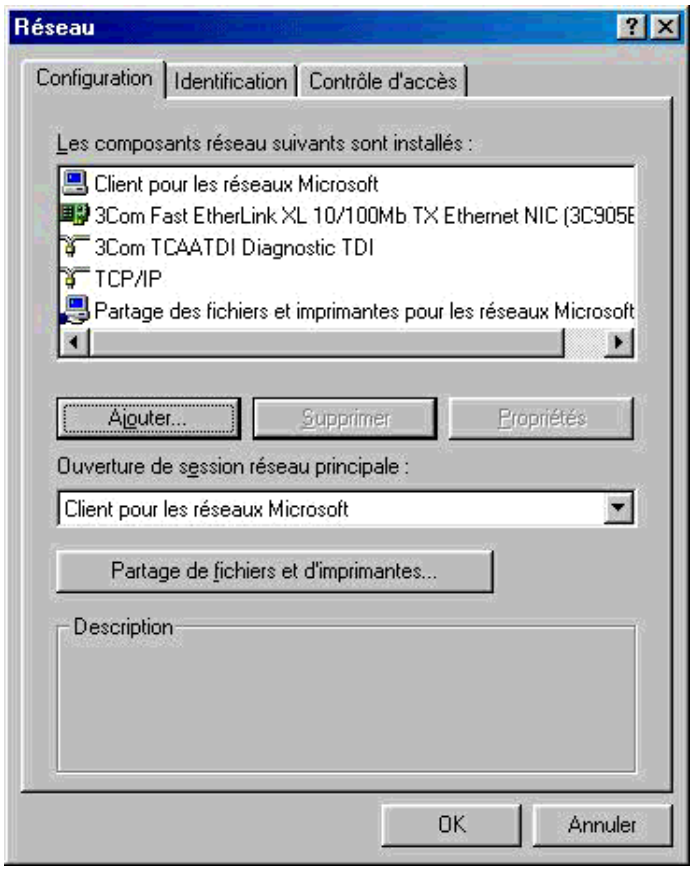
Voor een Win98 type client

Klik op Start/Parameters/Configpanel en dubbelklik op Network

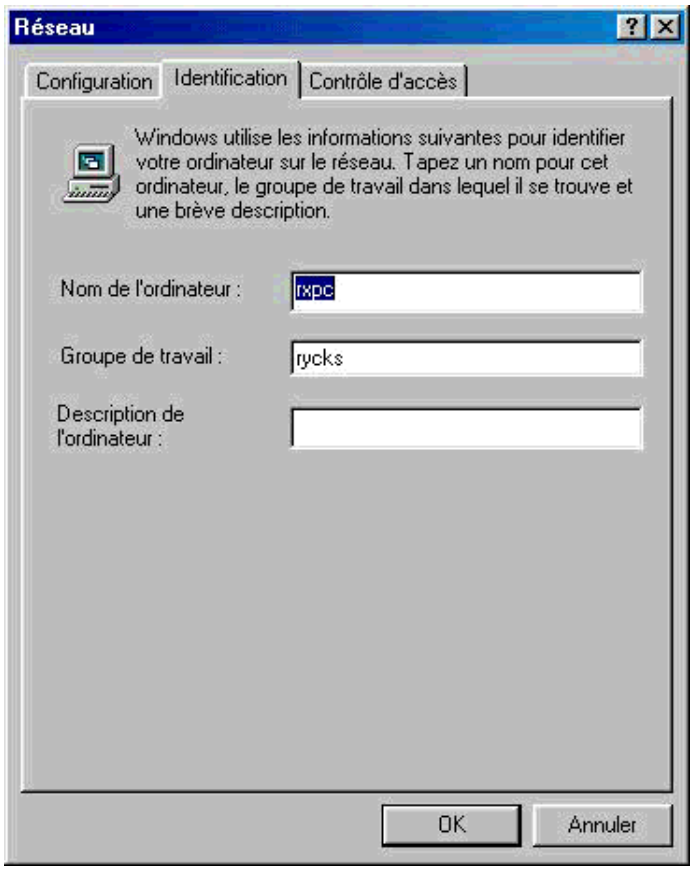
Installeer:

- Client for MS networks
- Netwerk kaart driver
- TCP/IP support en ALLEEN TCP/IP (geen ipx of netbios)
- Bestands-en printerdeling

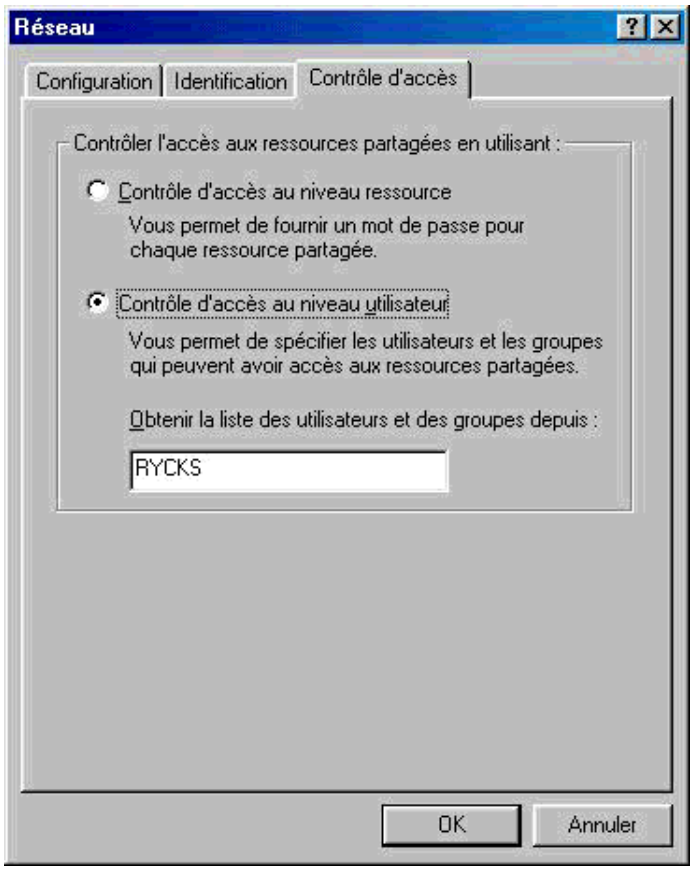
Met een beetje geluk, 20 maal klikken met de muis en een herstart, zou Windows geconfigureerd moeten zijn!



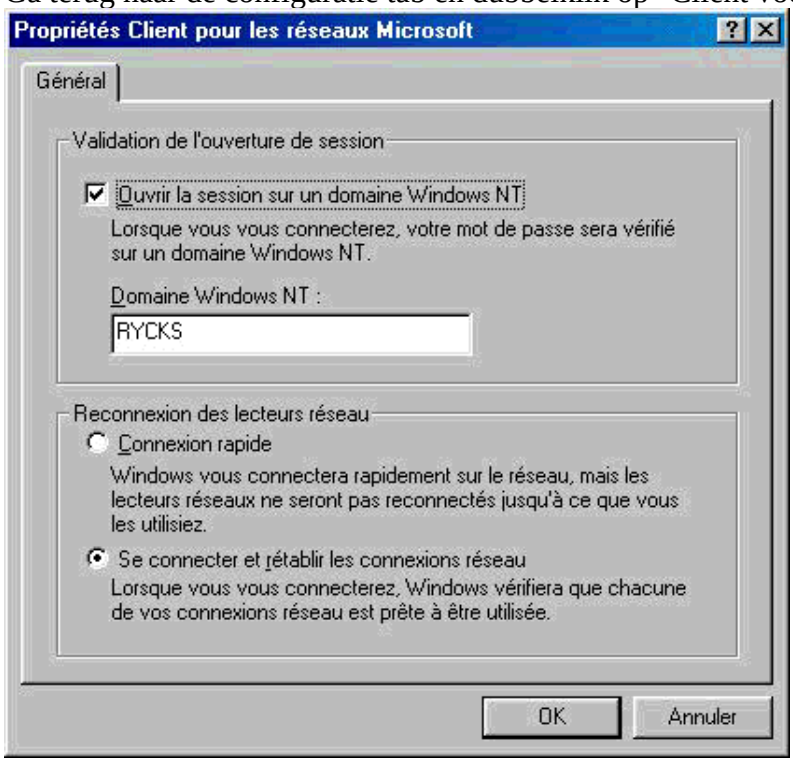
Klik vervolgens op de "Identification" tab en geef de computernaam en werkgroep op.



Klik op "Access control" en kies gebruikerscontrole op netwerktoegang.



Ga terug naar de configuratie tab en dubbelklik op "Client voor MS netwerk".



Vergeet niet om TCP/IP ondersteuning in te stellen:
Dubbelklik op TCP/IP.
IP adres:

- Het IP adres dat je wilt voor deze machine (bijvoorbeeld: 192.168.0.2)
- Subnetmask (bijvoorbeeld: 255.255.255.0)

WINS configuratie:

- Activeer de WINS dienst
- Voeg een WINS server toe, IP 192.168.0.1 (als dit het IP adres van de Samba server is)
- Gateway: als je een gateway hebt, is dit waar je hem aangeeft
- DNS configuratie: configureer je DNS toegang

Opmerkingen "optimalisatie/prestaties/gezond verstand?"

Tijdens het gebruik ontstaat er al snel een bottleneck door het gebruik van Windows profielen.

Het profiel zit eigenlijk vol met rommel waarvan MS heeft besloten dat het belangrijk is, zoals het IE cache, Outlook cache enz.

Dit betekent in het kort dat ongeveer 10 MB wordt binnengehaald wanneer er verbinding wordt gelegd met de server (mijn profiel is echter een "klassiek" profiel, een achtergrond plaatje, en zonder outlook...). Er wordt dus ook 10 MB ge-upload naar de server bij het beindigen van de verbinding.

10 MB voor iedere gebruiker, bij 15 machines (de "normale" grootte van een computerklas, bijvoorbeeld), betekent dat 150 MB, en als een gebouw 10 kamers heeft... reken maar eens uit hoeveel gebruikers uitloggen wanneer de bel gaat.

Dus als gebruiker moet je daar dan op anticiperen en uitloggen om 5 vóór... (ik moet toegeven dat dit is wat ik deed toen ik student was...) en dat is beter dan uitloggen om 5 ná. Het is net zoiets als een file in grote steden: het is beter om ofwel 10 minuten eerder te vertrekken ofwel 2 uur later!

Dus, volgens het beleid dat je geïmplementeerd hebt, is het een goed idee om de home directory op P: te "mounten" (bijvoorbeeld, P voor Persoonlijk) voor iedereen en de gebruikers te leren dat ze hun documenten moeten bewaren op P en niet in "My documents", anders vind je ze nooit meer terug.

Hierna moet je software vinden die zo kan worden ingesteld dat alle bookmarks in P:\bookmarks.html worden opgeslagen. Dit geldt ook voor andere instellingen.

Ik weet niet of er wel zoiets bestaat in de wereld van Windows!

Als je een oplossing kent, schrijf er dan een artikel over, dit is kennis die gedeeld moet worden!

Vragen en suggesties voor een volgend artikel

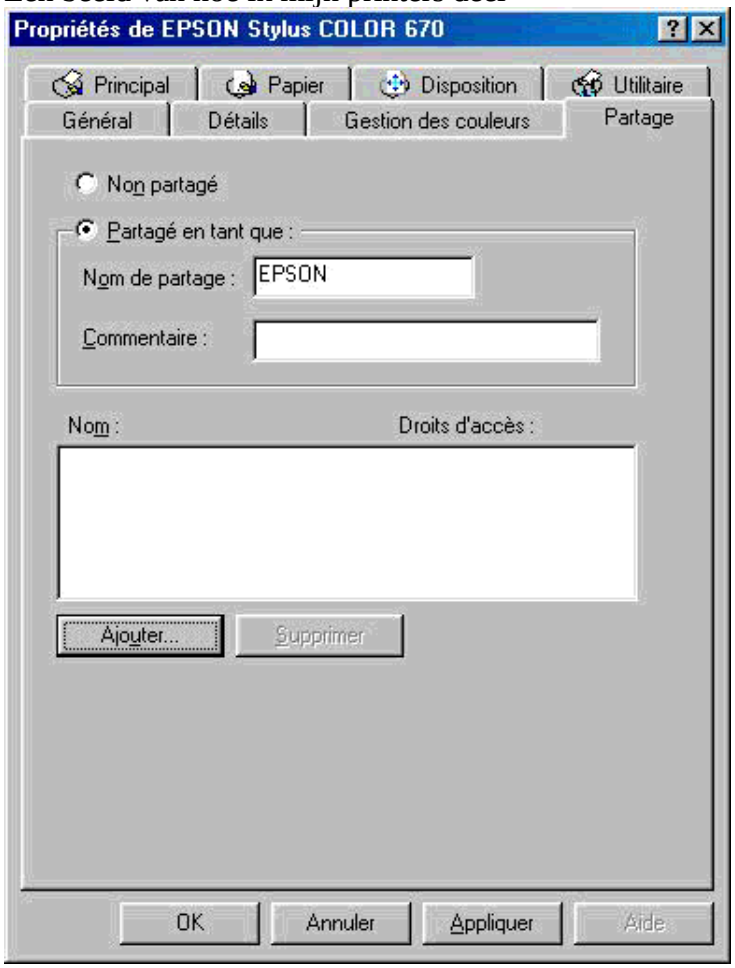
Is het mogelijk om meerdere werkgroepen op hetzelfde domein te hebben? Hoe moet dit beheerd worden, is het mogelijk om de problemen te delen tussen verschillende versies van GNU/Linux Samba?

Hoe gebruik je zowel NT als Samba servers?

NT clients configuratie: Het CONFIG.POL bestand heeft een andere naam bij NT.

Een echt probleem dat je hebt bij enkel een Samba server (en geen NT): Ik werk met Windows 98 en ik wil een lokale bron delen, mijn printer bijvoorbeeld:

Een beeld van hoe ik mijn printers deel



Klik op ’toevoegen’...

Vers van de pers: iemand gaf me de oplossing. Het is voldoende om "resource level access control" te kiezen tijdens stap 3 van de Windows configuratie.

Bedankingen

Bruno <bcarrere(at)asp-france.fr> voor het doorlezen van de ruwe versie en voor z'n geweldige hulp:o)

JohnPerr die me vroeg/dwong om m'n eerste artikel voor Linuxfocus te schrijven, en die het vertaald heeft in het Engels.
Michel Billaud alias MiB voor alle oplossingen die hij gevonden heeft voor onze problemen; hij heeft ons dingen geleerd als strace, enz.:o)
Etienne, Éric, en de onzichtbare man, wiens naam ik ben vergeten, sorry! Toch bedankt voor het delen van de kennis die je hebt opgedaan bij MS cursussen over NT servers.
Jean Peyratout, moeten we nog vertellen waarom? Dat zou veel te lang duren.
De Abul over het algemeen
Rycks die me de tijd en mogelijkheden heeft gegeven om gratis software te ontwikkelen en te documenteren.

Bronnen

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

Dit document zal up-to-date gehouden worden op de documentatie sectie op Rycks.com

---

Vertaling info:
fr --> -- : Éric Seigne <erics/at/rycks.com>
fr --> en: Georges Tarbouriech <georges.t/at/linuxfocus.org>
en --> nl: Hendrik-Jan Heins <hjh/at/passys.nl>