LinuxFocus article number 177
http://linuxfocus.org

par Éric Seigne
<erics/at/rycks.com>

L´auteur:

Je travaille dans le monde des logiciels libres où je développe, entre autres, des applications d'accès aux bases de données sur le web avec des outils comme PostGreSQL ,MySQL et PHP.
Pour pouvoir garder une certaine liberté dans ma manière de travailler (pouvoir "changer de métier" de temps en temps, ne pas rester a faire toujours du PHP/MySQL par exemple ... se lancer dans un bon projet C, Java ou autre) je me suis récemment installé à mon compte.
Et pour tout arranger, je suis -encore- membre de l'ABUL www.abul.org (et je n'ai pas encore payé ma cotisation !).

Configuration de samba

Résumé:

Je vais essayer de vous exposer ici le travail que nous avons réalisé dans la mise en place d'un serveur linux-samba comme contrôleur de domaine d'un réseau Windows.
La gestion des restrictions utilisateurs, les profils itinérants ... seront exposés en détails.
Ce document est basé sur une Debian GNU/Linux 2.2 ce qui fait que le fichier smb.conf par défaut sur votre distribution risque d'être légèrement différent.
Pour ce qui est de la version de samba utilisée **Samba 2.0.7**

Installation de Samba

On part du principe que vous connaissez un minimum samba et qu'il est déjà installé sur votre serveur de test.

Si jamais ce n’etait pas le cas, pour installer samba rapidement, regardez du côté de :
Debian: apt-get install samba
RedHat(Mandrake): rpm -vih /mnt/cdrom/RedHat(Mandrake)/RPMS/samba*

Le fichier de configuration: informations générales

Samba utilise un fichier de configuration unique dans lequel se trouvent des blocs comme par exemple le bloc [global].

```
<fichier smb.conf minimal>
[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
</fichier>
```

Un seul fichier de configuration pour samba !

Si samba est lancé avec ce fichier de configuration, les postes windows du réseau local pourront voir dans le voisinage réseau qu’un ordinateur nommé (le nom de votre machine linux) partage un répertoire temp dans lequel vous avez le droit d’écrire.

ATTENTION: lorsque vous mettez à jour le fichier de configuration de samba, pensez à relancer samba à l’aide du script*/etc/init.d/samba restart* (pour debian)

Le fichier de configuration, paramètres "avancés"

Voyons maintenant les paramètres suivants:

- Section [global]
  - **netbios name:**
    Vous pouvez spécifier le nom netbios de votre serveur samba. Le nom netbios est visible dans le voisinage réseau de vos ordinateurs sous windows. Si vous ne spécifiez pas de nom netbios, le serveur linux prendra comme nom netbios son nom réseau.
  - **invalid users:**
    Liste des utilisateurs interdits d’accès à Samba. Par exemple "root" devrait être interdit.
  - **interfaces:**

Si votre serveur linux dispose de plusieurs cartes réseaux et que vous vouliez restreindre son activité à un seul réseau.

- **security:**
  Choix du mode de sécurité que vous voulez utiliser. Si on utilise security=user ça oblige que chaque utilisateur ait un compte sur le serveur GNU/Linux.
  Si vous voulez lancer un samba qui ne gère pas les utilisateurs et qui ne partage que des ressources identiques pour tout le monde, vous pourrez utiliser security=share.
- **workgroup:**
  Nom du groupe de travail dont votre serveur linux doit faire partie.
- **server string:**
  Description de votre serveur linux.
- **socket options:**
  Une liste d'options pour "affiner" votre samba et faire en sorte qu'il réagisse plus vite par exemple.
- **encrypt passwords:**
  Faut il utiliser les mots de passe encryptés ? Il est important de savoir que tous les windows (ou presque) utilisent un système différent !
- **wins support:**
  Votre serveur linux fait-il aussi office de serveur wins ?
- **os level:**
  "Niveau" de votre OS pour savoir qui sera élu maître du domaine, local etc.
- **domain master:**
  Active samba comme serveur maître du domaine
- **local master:**
  Active samba comme serveur maître local
- **preferred master:**
  Samba doit-il être "préféré" à tout autre serveur s'il y en a ?
- **domain logons:**
  Samba doit-il gérer les contrôles de connexions pour le domaine ?
- **logon script:**
  Quel sera le script à lancer lors de l'ouverture de la session de cet utilisateur ?
- **logon path:**
  Ou se trouvent les fichiers script de démarrage ?
- **logon home:**
  Où faut-il stocker les profils itinérants des utilisateurs ?
- **name resolve order:**
  Dans quel ordre on fait appel aux ressources pour trouver le nom d'une machine du réseau ?
- **dns proxy:**
  Le serveur samba doit-il faire également office de proxy DNS ?
- **preserve case:**
  Permet de garder la casse des noms de fichiers.
- **short preserve case:**
  Permer de garder la casse des noms de fichiers.
- **unix password sync:**
  Faut-il syncroniser les mots de passe unix et windows ?
- **passwd program:**
  Quel programme lancer pour changer le mot de passe.

- **passwd chat:**
  Quel est le "protocole" de discussion pour changer le mot de passe.
- **max log size:**
  Taille maximum du fichier de log.

- Section [netlogon]

  On spécifie où se trouve le netlogon.

- Section [profiles]

  Bloc des profils utilisateurs.

- Section [homes]

  Le répertoire utilisateur.

Les variables de samba

Variable	Définition
Variables du client	
%a	Architecture du client Exemple: Win95, WfWg, WinNT, Samba ...
%I	Adresse IP du client
%m	Nom NetBios du client
%M	Nom DNS du client
Variables utilisateur	
%g	Groupe primaire de l’utilisateur %u
%H	Répertoire home de l’utilisateur %u
%u	Nom de l’utilisateur unix courant
Variables de partage	
%P	Racine du partage actuel
%S	Nom du partage actuel
Variables du serveur	
%h	Nom DNS du serveur Samba
%L	Nom NetBios du serveur Samba
%v	Version de Samba
Variables diverses	
%T	La date et l’heure courantes

Exemple d’utilisation de ces variables: si vous avez dans votre réseau des windows 3.11 (windows for workgroup) et des 98, vous pourrez - à l’aide de la variable %a - faire deux fichiers de configuration qui seront adaptés à ces deux systèmes.

Résultat: notre fichier de configuration

<fichier smb.conf>
[global]
printing = bsd
printcap name = /etc/printcap
load printers = yes
guest account = nobody
invalid users = root

; on "fixe" son nom netbios
netbios name = pantoufle
; le réseau à écouter n’est
; que celui-ci (sur l’autre interface on a la connexion internet,
: pas la peine d’avoir du samba de ce côté !)
interfaces = 192.168.0.1/255.255.255.0

; security user implique que tout utilisateur DOIT
; avoir un compte unix sur ce serveur :)
security = user
; Le nom du groupe de travail dont ce serveur est membre
workgroup = rycks
; La description du serveur, visible lorsqu’on affiche les détails
; %h étant le nom DNS du serveur et %v la version de samba
server string = %h server (Samba %v)

; On utilise encore le fichier de log de samba, et pas que celui de syslog
syslog only = no

; Le minimum d’informations importantes dans le syslog,
; le reste étant toujours dans /var/log/smb(nmb)/
syslog = 0;

; Vive le tuning !
socket options = IPTOS_LOWDELAY TCP_NODELAY \
SO_SNDBUF=4096 SO_RCVBUF=4096

; On utilise les mots de passe encryptés. Attention
; tous les clients W95 devront
; être mis à jour avec le patch sécurité
; SMB de MS. De même NT4 devra être patché
; par le SP3 ou mieux ... Pour le W3.11 je ne sais plus,

```
; ils ne doivent probablement pas supporter les mots de passe encryptés :(
encrypt passwords = yes

; Ce serveur fait également office de serveur WINS.
; WINS permet à deux réseaux qui utilisent
; des plages d'IP différentes (par exemple
; 192.168.0.0/255.255.255.0 et 192.168.0.1/255.255.255.0)
; de voir les ressources partagées dans "l'autre"
; réseau, si la passerelle est active.
wins support = yes

; Niveau de l'OS. Comme notre serveur se charge d'être le
; maître du domaine, local logons etc. Il est donc au-dessus
; du serveur NT s'il y en a un !
os level = 34

; On fait la gestion du domaine
domain master = yes
local master = yes
preferred master = yes

; On assure la centralisation des connexions du domaine
domain logons = yes

; Quel script lancer lorsqu'un client se connecte ?
; %g correspond au nom du groupe primaire dont fait partie
; cet utilisateur.
logon script = %g.bat
; Dans quel répertoire se trouvent les fichiers de démarrage ?
; %L est le nom netbios du serveur samba
logon path=\\%L\netlogon
; Ou faudra-t-il stocker les profils itinérants des utilisateurs ?
; %U est le login de l'utilisateur
logon home=\\%L\%U\winprofile

; Dans quel ordre faire appel aux ressources
; pour trouver le nom d'une machine ?
; Notez le broadcast en FIN ... pas comme les
; windows classiques qui balancent
; régulièrement des broadcasts.
name resolve order = lmhosts host wins bcast

; Samba doit-il faire office de proxy DNS ?
dns proxy = no

; Respect des noms de fichiers et de leur casse
preserve case = yes
short preserve case = yes
```

```
; Faut-il synchroniser les mots de passe windows et linux ?
unix password sync = yes

; Que faut-il mettre en place pour la synchronisation des mots de passe
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\sUNIX\spassword:* \
%n\n *Retype\snew\sUNIX\spassword:* %n\n .

; La taille maximum du fichier de log, évite de saturer son /var :p
max log size = 1000

; On fait office de serveur de temps, c'est
; pratique que toutes les machines du réseau soient un tant soit peu
; synchronisées. On utilisera cette fonctionnalité dans le fichier .bat
; de logon
time server = yes

; On spécifie où se trouve le netlogon
; Il ne sera utilisé que lors de la connexion,
; c'est pour cela que ce n'est pas nécessaire qu'il soit public etc.
[netlogon]
path = /home/netlogon/%g
public = no
writeable = no
browseable = no

; Le répertoire Home de chaque utilisateur
[homes]
comment = Home Directories
browseable = no

; Il a quand même le droit d'y écrire !
read only = no

; Le masque Unix de création de fichier par défaut
create mask = 0700

; Pour des raisons de sécurité, on met un masque de répertoire à 700 aussi !
directory mask = 0700

; On partage le FTP, c'est plus pratique de l'avoir dans le voisinage réseau
; que de devoir lancer un utilitaire spécial.
[ftp]
path = /home/ftp/pub
public = yes
printable = no
guest ok = yes
```

; Le répertoire temporaire
[tmp]
path = /tmp
public = yes
printable = no
guest ok = yes
writable = yes

; un autre temporaire spécial pour un utilisateur exigeant beaucoup d'espace !
[bigtemp]
path = /home/bigtemp
public = yes
printable = no
guest ok = yes
valid users = erics
writable = yes

</fichier>

Ce qu'on a sur le serveur

En bref, sur le serveur, on doit avoir:

- un compte par utilisateur
- le fichier smb.conf
- un répertoire /home/netlogon (dans mon exemple)
- un fichier .bat par groupe d'utilisateur dans ce répertoire (un exemple suit)
- un fichier CONFIG.POL de statégie sécurité système dans ce répertoire également. Pour créer le fichier config.pol, chercher poledit.exe qui se trouve sur le cdrom windows.

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


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


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

```
</fichier eleves.bat>


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


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

Ce fichier permet au lancement, de monter automatiquement le répertoire personnel de l'utilisateur en P: et le répertoire temporaire sur T:. De même, on règle l'horloge système sur celle du serveur samba.

REMARQUE: les retours à la ligne du fichier .bat doivent être en "mode DOS", le plus simple est de créer ce fichier sous windows avec notepad par exemple et de l'envoyer sur le serveur après.

Création de la politique de sécurité du système (C) (TM) (R)

Un titre ronflant ... normal je l'ai trouvé dans une doc MS a propos de leur outil de politique système

Sécuriser Windows, c'est presque possible, grâce à un contrôleur de domaine.

Donc, pour créer une politique système Windows, par exemple interdire à certains utilisateurs (tous ?) de lancer regedit, un programme DOS etc. il faut utiliser POLEDIT qui se trouve sur le CDROM de windows 98

Lancez PolEdit, regardez son aide, notez les informations, cette documentation n'a pas pour but de vous expliquer comment marche un logiciel propriétaire.

Une fois que vous avez votre fichier .POL de fait, copiez-le sur votre serveur samba, dans le répertoire pointé par la directive PATH du groupe [netlogon]

ATTENTION: Pour des clients W9x le fichier de stratégie système doit être CONFIG.POL ... pour les WindowsNT ce n'est pas le même nom, et comme je n'ai pas de NT, je ne peux pas vous en parler :'(Non, ce n'est pas la peine de m'offrir un windowsNT pour que je teste. Merci quand même c'était sympa de votre part :o)

REMARQUE PolEdit Permet de créer des groupes d'utilisateurs et des utilisateurs, nous n'avons pas encore réussi à faire en sorte que ça marche. Seul l'utilisateur par défaut est pris en compte.

Par exemple, si dans PolEdit je crée un groupe d'utilisateurs "admin" qui aura le droit de lancer regedit, je me connecte en tant que "erics" (dont le groupe primaire est "admin" et je n'ai quand même pas le

droit de lancer regedit :(

Par contre, si j'avais créé un utilisateur "erics" dans poledit, ça aurait marché.

Comme nous n'avons pas envie de créer les 1056 utilisateurs dans poledit, et que la gestion globale des utilisateurs est plus intéressante, nous vous proposons l'astuce suivante:

Pour faire face à cela, nous avons rusé: on a fait 3 fichiers config.pol avec seulement des utilisateurs par défaut, et sur le serveur linux, on a:
/home/netlogon/professeurs/CONFIG.POL
/home/netlogon/professeurs/professeurs.bat
/home/netlogon/eleves/CONFIG.POL
/home/netlogon/eleves/eleves.bat
/home/netlogon/admin/CONFIG.POL
/home/netlogon/admin/admin.bat
Et on a modifié le smb.conf pour que cela soit pris en compte:

<fichier smb.conf>
[netlogon]
; on a rajouté le %g pour que selon
; le groupe de l'utilisateur netlogon pointe
; vers un répertoire différent
; dans lequel le config.pol correspond à
; chaque groupe de profil utilisateur.
path = /home/netlogon/%g
public = no
writeable = no
browseable = no
</fichier smb.conf>

Configuration des postes Windows

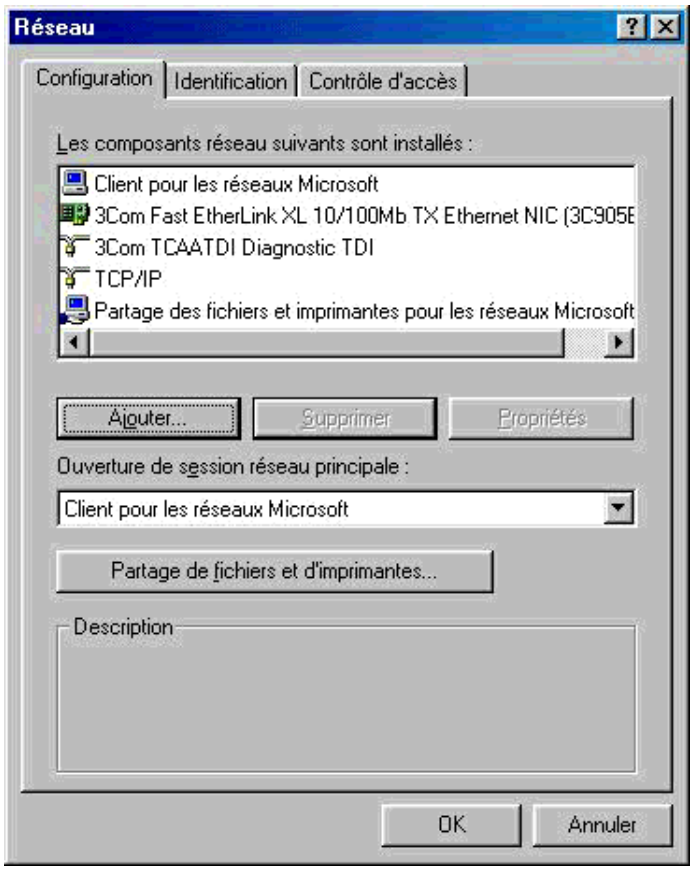
Pour un poste client type Win98

Cliquer sur Démarrer/Paramètres/Panneau de configuration puis double-cliquer sur Réseau

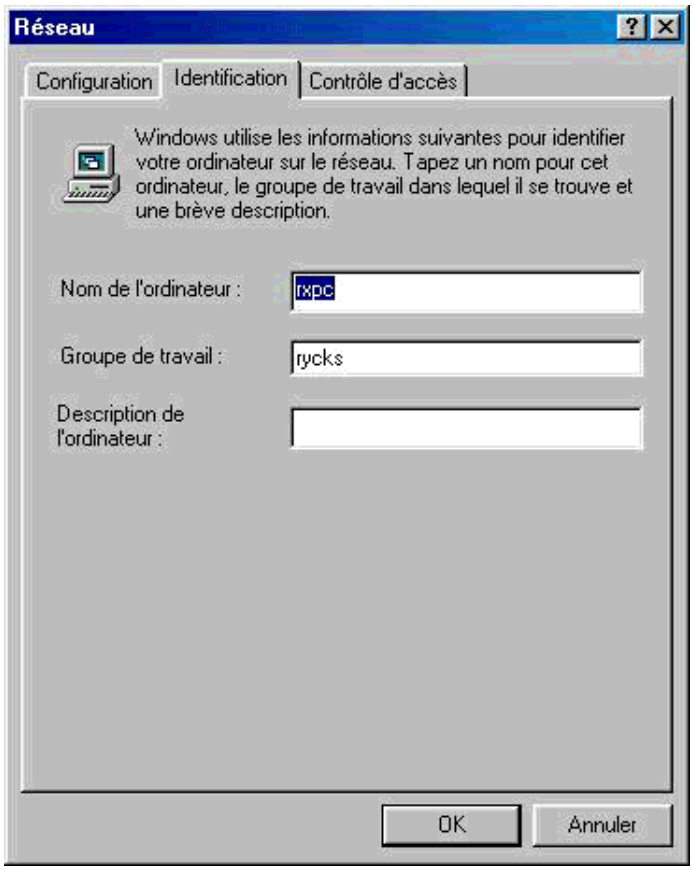
Installer:

- Client pour les réseaux MS
- Driver de votre carte réseau
- Support TCP/IP et SEULEMENT TCP/IP (pas d'ipx ou de netbios)
- Partage de fichiers et d'imprimantes

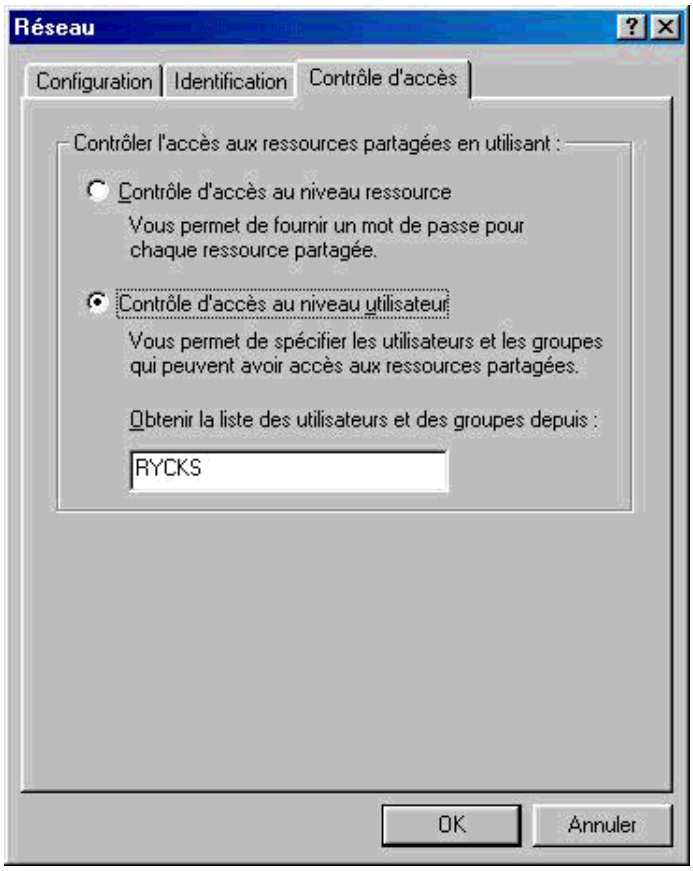
Avec un peu de chance, 20 clics de souris et 1 reboot pour configurer windows !



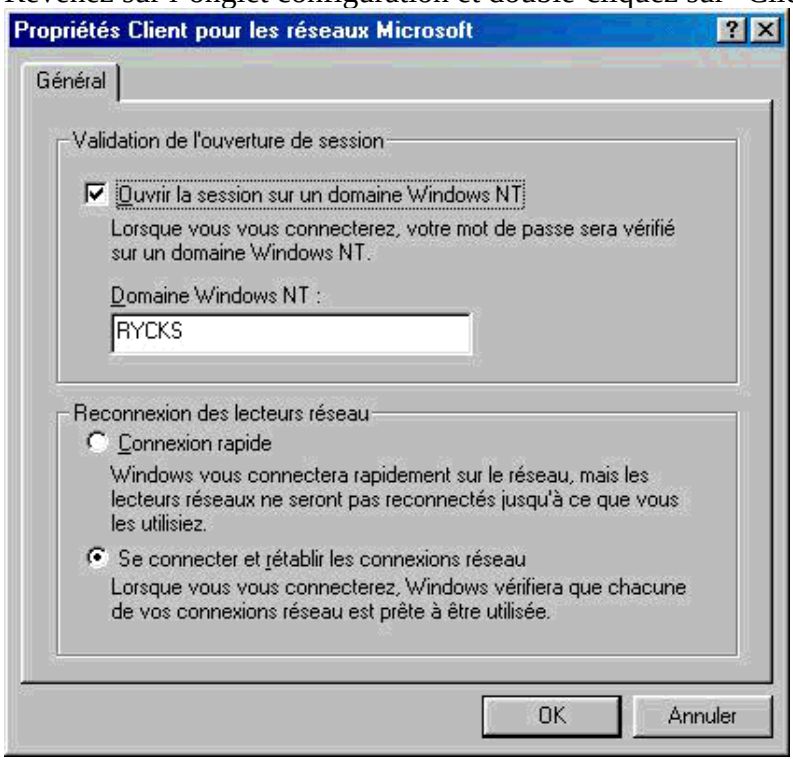
Cliquez ensuite sur l’onglet "Identification" et renseignez le nom de l’ordinateur ainsi que le groupe de travail dans lequel vous voulez être.



Cliquez sur "Contrôle d’accès" et cochez la case de contrôle d’accès au niveau utilisateur



Revenez sur l'onglet configuration et double-cliquez sur "Client pour les réseaux MS"



N’oubliez pas de configurer votre support TCP/IP:
Double-cliquez sur TCP/IP

Adresse IP:

- l’adresse IP que vous voulez pour cette station (ex: 192.168.0.2)
- Masque de sous-réseau (ex: 255.255.255.0)

Configuration WINS:

- Activer la résolution WINS
- Ajouter un serveur WINS, IP 192.168.0.1 (si le serveur samba a cette IP)

Passerelle: Si vous avez une passerelle, configurez-la ici

Configuration DNS: configurez votre accès DNS

Remarques "tuning/performances/bon sens ?"

A l’utilisation, il apparait très rapidement un engorgement du réseau dû à l’utilisation des profils itinérants de windows.

En effet, dans le profil on "trimbale" plein de trucs que MS a décidé comme étant importants, comme par exemple, le cache de IE, celui de Outlook etc.

En bref, cela implique par exemple que 10 Mo de fichiers seront téléchargés lors de la connexion à un poste (mon profil est "classique", une image de fond, ie et outlook ...) et 10 Mo seront envoyés sur le serveur lorsque je me déconnecte.

10 Mo par utilisateurs, prenons une salle de 15 machines (taille "normale" d’une salle de TP informatique par exemple), 150 Mo, et si y a 10 salles dans le bâtiment ... calculez le temps de déconnexion des utilisateurs lorsque la sonnerie de la pause se déclenche.

Mieux vaut anticiper le mouvement et se déloger à -5 ... (heu, j’avoue lors des TP VC++ c’est ce que je faisais à tous les coups) ... que à pile ou à 5, comme pour les bouchons sur le périf, il faut passer soit 10 minutes avant, soit 2 heures après !

Donc, au vu de ce problème important, et selon la politique que vous mettez en place, il serait parfois astucieux de monter pour tout le monde son répertoire home sur P: (par exemple, P comme Perso) et de former les utilisateurs: "sauvegardez vos documents sur P et pas dans "Mes documents" sinon vous ne les retrouverez pas".

Reste ensuite à trouver les logiciels qui peuvent être configurés pour avoir leur bookmark sur P:\bookmarks.html et ainsi de suite pour les paramètres.

Je ne sais tout simplement pas si ça existe dans le monde windows!

Si jamais vous avez une solution miracle, faites-en un article, c’est un savoir qu’il faut partager !

Questions et ouverture vers une suite à cet article

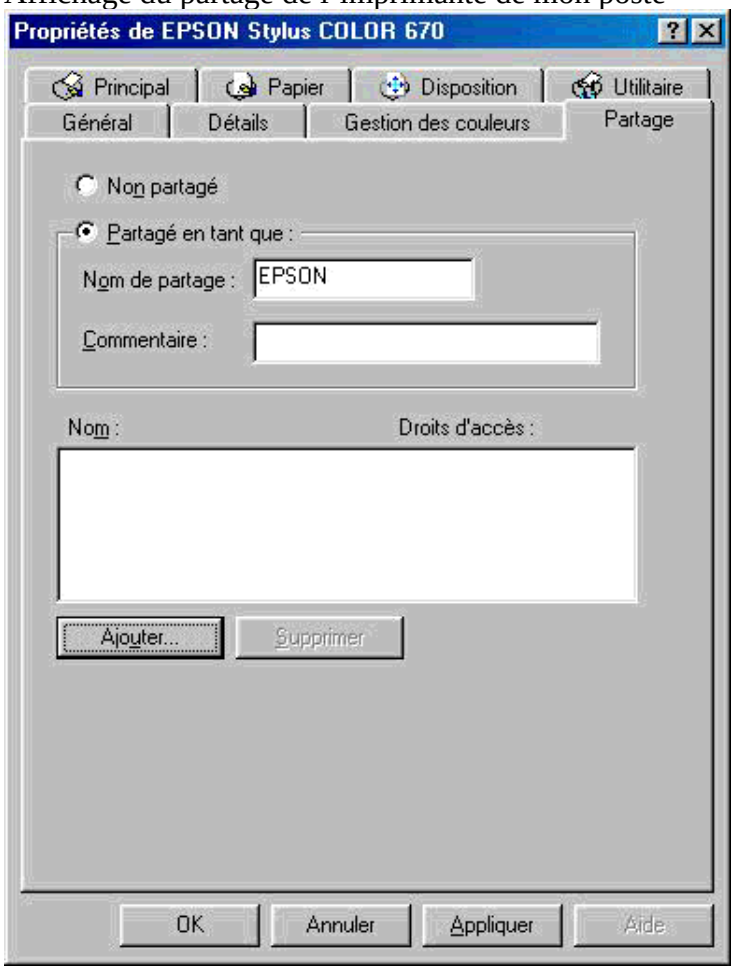
Il est possible d'avoir plusieurs WorkGroups sur un même domaine, comme cela se gère, peut-on répartir les problèmes entre plusieurs GNU/Linux Samba ?

Comment faire cohabiter des serveurs NT et Samba ?

Configurer des clients NT, le CONFIG.POL équivalent sous NT porte un autre nom.

Un problème concret de n'avoir qu'un serveur Samba (et pas de NT), je suis sur un poste Windows (98) et je souhaite partager une ressource locale, mon imprimante par exemple:

Affichage du partage de l'imprimante de mon poste



Après le clic sur le bouton Ajouter...

HOT NEWS : La solution à ce petit problème m'a été donnée, il suffit en effet de sélectionner "Contrôle d'accès niveau ressource" à l'étape 3 de la configuration de votre poste windows.

Remerciements

Bruno pour sa relecture attentive et ses précisions précieuses :o)

JohnPerr pour m'avoir incité à écrire mon 1er article sur LinuxFocus, et l'avoir traduit en anglais
Michel Billaud aka MiB pour toutes tes solutions, à chaque fois qu'on a un problème, tu nous apprends des trucs, strace etc. :o)
Etienne, Éric, et l'homme invisible dont j'ai mangé le nom, je suis désolé ! Donc, merci de nous avoir transmis votre savoir issu des cours MS sur les serveurs NT
Jean Peyratout, est-il indispensable de dire pourquoi ? c'est trop long
L'Abul en général
Rycks pour m'accorder du crédit-temps et des ressources pour développer et documenter "du libre".

Ressources

La version en ligne du livre de O'Reilly: http://www.oreilly.com/catalog/samba/chapter/book/index.html

N'oubliez pas que ce document sera mis à jour sur la partie documentation de rycks.com

Pour me contacter: Éric Seigne
