PARAMETRER SAMBA 2.2

Configurations requises :

- Mandrake Linux 9.2 avec Samba 2.2.8 installé (poste avec une IP statique), nommé **MDK92**, connexion en tant que **root**.
- Postes clients Windows 2000 Pro / XP (avec SP4 / SP1a), nommés **PC01**, **PC02**, …, membre du groupe de travail **MANDRAKE**, connexion en tant que **administrateur** et **luc**.

1 - Configuration de base :

La configuration de SAMBA repose sur le fichier **smb.conf** placé dans **/etc/samba**. Ce fichier texte est à la fois simple et complexe suivant les fonctionnalités du serveur SAMBA.

Si un fichier /etc/samba/smb.conf existe, il est recommandé d'en faire une copie :

 # cp /etc/samba/smb.conf /etc/samba/smb.conf.bak

On va donc créer un simple partage de test accessible par tous, pour cela créons le répertoire / usr/local/samba/tmp :

(Si le répertoire /usr/local/samba n'existe pas :
mkdir /usr/local/samba)
mkdir /usr/local/samba/tmp
et donnons y des droits d'accès pour tous :
(# **chmod 777 /usr/local/samba**)
chmod 777 /usr/local/samba/tmp
On va créer la configuration SAMBA la plus simple qui soit en créant un nouveau fichier smb.conf (avec n'importe quel éditeur de texte) qui contiendra :

```
[global]
  workgroup = MANDRAKE

[test]
   comment = Répertoire partagé de Test
   path = /usr/local/samba/tmp
   guest = ok
   read only = no
```

La section **[global]** définit tous les paramètres nécessaires à la configuration générale de SAMBA. Les autres sections définissent les partages activés sur ce serveur.

Le paramètre '**workgroup**' définit le nom du groupe de travail ou du domaine suivant la configuration. Dans le cas d'un groupe de travail, tous les postes de ce groupe devront posséder le même nom. Le nom est à votre discrétion.

La section **[test]** définit l'unique partage de fichier de notre serveur SAMBA. Le nom des partage est à la discrétion des administrateurs SAMBA.

Le paramètre '**comment**' ajoute au partage un commentaire apparaissant dans le voisinage réseau des clients Windows. Il est conseillé de commenter les partages.

Le paramètre '**path**' définit l'emplacement, sur le serveur Linux, ou seront stockés les fichiers des clients Windows. C'est donc un chemin Unix.

Le paramètre '**guest**' indique que les connexions en tant qu'invité (utilisateur non définit) sont acceptées (ok) ou refusée (no). Ici, sur ce partage de test, tout le monde peut se connecter. Cette méthode est déconseillée pour des partages autres que des imprimantes.

Le paramètre '**read only**' indique si l'accès est limité en lecture seule (yes) ou si l'écriture est aussi acceptée (no). Ici nous autorisons l'écriture.

Afin de vérifier que notre fichier est sans erreur il est possible de lancer le programme testparm qui procède à une vérification de smb.conf :

testparm
```
Load smb config files from /etc/samba/smb.conf
Processing section "[test]"
Loaded services file OK.
Press enter to see a dump of your service definitions
```

Notre fichier étant correct, pour activer nos modifications il nous faut relancer le serveur SAMBA. Si le logiciel a été installé en tant que daemon Unix (méthode conseillée) faire :

 # service smb restart

A partir d'un poste du même réseau local que le serveur SAMBA, ouvrons le voisinage réseau. Si le PC utilise Windows 95, un nouveau PC apparaît dans le groupe de travail, contenant le répertoire partagé test. Identifions nous en tant que root.
Cependant si le poste est sous Windows NT, 2000 ou XP il est impossible d'ouvrir le groupe de travail car une erreur de connexion apparaît. En effet les mots de passe de NT sont cryptés. Pour cela ajoutons dans la section [global] le paramètre '**encrypt password**' :

[global]
encrypt passwords = yes

Il est aussi nécessaire de définir au niveau de SAMBA les mots de passes cryptés. Il faut au moins un utilisateur autorisé à utiliser ce partage, pour cela utilisons le programme smbpasswd afin d'authentifier le super utilisateur root :

 # smbpasswd –a root
```
New SMB password:
Retype new SMB password:
Added user root.
```

Puis redémarrons comme précédemment le serveur SAMBA. Le partage « test » est accessible et fonctionnel ! Créons et modifions-y un fichier texte d'essai.

La configuration de SAMBA consiste donc à entrer des directives dans les diverses sections du fichier smb.conf. Ce fichier étant facilement sauvegardable, la restauration ou le clonage de la configuration d'un serveur SAMBA est donc des plus aisées.

Pour obtenir le détail de ces sections et directives, consulter le manuel de smb.conf :

 # man smb.conf

2 - Serveur de fichiers et d'impression :

Plaçons-nous dans le cas d'un réseau local des plus simples : poste à poste sans aucun type de serveur. Nous allons y ajouter notre serveur SAMBA afin de centraliser les données (le serveur Linux pourra en assurer la sauvegarde), et partager une imprimante laser.

Il est alors intéressant de demander à notre serveur SAMBA d'assumer en plus le rôle de serveur WINS (Windows Internet Name Service) c'est-à-dire d'assurer la résolution des noms NETBIOS. Il suffit d'ajouter Le paramètre '**wins support**' dans la section **[global]** .

[global]
wins support = yes

Le paramètre '**time server**' permet d'activer le serveur de temps NTP de SAMBA. Il devient ainsi possible de maintenir à la même date et heure tous les PC du groupe de travail :

[global]
time server = yes

Les PC Windows pourront alors synchroniser automatiquement leurs horloges sur celle du serveur SAMBA grâce à la commande en ligne :

C:\> NET TIME \\MDK92 /SET /Y
(MDK92 est le nom du serveur UNIX exécutent SAMBA)
Cette commande peut être incluse dans un fichier de commande, un login script par exemple.

Configuration des Pare-feu (FireWall)
Afin de pouvoir utiliser les services réseau SMB les ports suivants doivent être ouverts sur les pare-feu présents sur le réseau local :

Port 123 TCP

Utilisé par le service de temps NTP

Port 137 TCP

Utilisé pour parcourir les ressources NETBIOS (browser)

Port 138 TCP

Utilisé par le service de nom NETBIOS

Port 139 TCP

Utilisé pour les partages de fichier et d'imprimante

Port 445 TCP

Utilisé par Windows 2000/XP lorsque NetBIOS over TCP/IP est dévalidé.

Port 1512 TCP

Utilisé pour le service de noms WINS

2.1 Serveur de fichiers

Il nous faut d'abord définir un mode de gestion des partages NETBIOS :

2.1.1 Partage au niveau des ressources

C'est le partage de base initié dans Windows For Workgroups, c'était aussi le type de partage par défaut pour les versions antérieures de SAMBA.

Le paramètre '**security**' doit être défini dans la section **[global] :**

[global]
security = share

Avec ce type de partage le client SMB s'identifie systématiquement lors de la connexion à chaque ressource partagée. Il ne doit fournir que le mot de passe, il n'y a pas d'identification de l'utilisateur.

Windows offre un accès complet ou en lecture seule avec ou sans mot de passe.

SAMBA utilisant l'authentification UNIX ne se contente pas d'associer un partage à un mot de passe mais associe un partage à un utilisateur avec mot de passe.

Les clients de réseau Microsoft récents fonctionnent parfois mal avec SAMBA en mode 'share level'. Il est donc déconseillé d'utiliser ce mode de sécurité.

2.1.2 Partage au niveau des utilisateurs

C'est le partage par défaut depuis la version 2.2 de SAMBA. Explicitement déni par :

[global]
security = user

Avec ce type de partage le client SMB envoie une demande d'ouverture de session juste après la négociation du protocole en fournissant un nom d'utilisateur et un mot de passe. A ce moment le serveur ne peut baser son acceptation ou son rejet que sur :

- L'identification utilisateur et mot de passe,
- Le nom de la machine demandant la connexion.

Si le serveur valide la connexion le client s'attend à pouvoir monter tous les partages sans avoir à fournir de mot de passe. Il s'attend à ce que tous les droits d'accès aient été définis lors de l'ouverture de session.

Il est possible pour un client SMB d'utiliser plusieurs ouvertures de session. Le serveur donnant lors de chaque ouverture de session un identifiant (UID) associé au mon d'utilisateur avec son mot de passe.

2.1.3 Partage au niveau du domaine

C'est le partage par défaut depuis la version 2.2 de SAMBA. Explicitement déni par :

[global]
security = domain

Avec ce type de partage le serveur SAMBA possède une compte sécurité sur un domaine. Toutes les demandes d'authentification seront transmises au contrôleur du domaine. Le serveur SAMBA doit donc être un serveur membre d'un domaine.

Afin de pouvoir fonctionner ainsi il faut que :

- Un compte machine soit définit sur le contrôleur de domaine pour le serveur SAMBA,
- Que le le serveur SAMBA soit joint au domaine NT via la commande :

 # net rpc join –U administrator%password

Utiliser ce type de sécurité impose qu'un compte d'utilisateur Unix soit créé pour chaque utilisateur SMB afin de pouvoir donner un UID lors de chaque ouverture de session validée par le contrôleur de domaine. Ces comptes peuvent être verrouillés afin d'éviter que tout autre clients que MS-Windows puissent les utiliser. Il suffit d'invalider le shell Unix en indiquant /bin/false en tant que shell pour ce type de compte dans /etc/passwd.

Une meilleure solution est d'avoir recours à l'utilitaire WinBind qui gère l'association des comptes Unix avec ceux du Domaine NT.

2.2 Serveur de fichiers

Voici un exemple de serveur de fichiers gérant des partages de fichiers par groupes d'utilisateurs et par utilisateurs.

Pour cela notre section [global] devient :

[global]
workgroup = MANDRAKE
netbios name = SAMBA
server string = Serveur SAMBA %v
encrypt passwords = yes
name resolve order = wins lmhosts bcast
wins support = yes
time server = yes
local master = yes
preferred master = yes
os level = 65
security = user

Le paramètre '**netbios name**' permet d'attribuer au serveur SAMBA un nom NETBIOS différent de son nom d'hôte LINUX.

Le paramètre '**server string**' permet d'associer au serveur SAMBA un commentaire. La variable **% v** permet l'affichage de la version du logiciel Samba. les paramètres (Netbios name et Server string) apparaîtront dans le 'Voisinage réseau' des postes clients sous Windows.

Le paramètre '**encrypt passwords**' vu précédemment permet la gestion des de passe cryptés des clients Windows NT/2000/XP.

Le paramètre '**name resolve order**' indique comment les noms NETBIOS seront traduits en adresses IP. Par défaut l'ordre est 'hosts, lmhosts, wins, bcast'. 'hosts' appelle la fonction Unix gethostbyname() utilisant aussi bien le fichier /etc/hosts ou DNS ou NIS suivant le paramètrage des fichiers /etc/host/config, /etc/nsswitch.conf et /etc/resolv.conf. Ici l'absence de 'hosts' permet d'exclure tous les PC qui ne font pas partie du segment de réseau local où qui ne sont enregistrés dans le fichier lmhosts ou dans le serveur WINS.
Le fichier texte lmhosts contient l'adresse IP et le nom de tous les postes utilisant NETBIOS.

Le paramètre '**wins support**' active le serveur NMBD de SAMBA permettant la résolution des noms NETBIOS. Attention ce serveur ne sait pas dialoguer avec les serveurs WINS de Microsoft., il doit donc être le seul sur le réseau. Si un serveur WINS existe déjà il faut remplacer ce paramètre par '**wins server = w.x.y.z**' permettant de préciser l'adresse TCP/IP su serveur WINS en fonction sur le réseau.

Le paramètre '**time server**' active le serveur de temps de SAMBA utilisant le protocole NTP.

Le paramètre '**local master**' permet au serveur SAMBA de participer à l'élection au titre de 'maître local' (yes).

Le paramètre '**preferred master**' positionné à 'yes' permet au chargement de forcer une élection au titre de 'maître local' avec une bonne chance de gagner cette élection surtout s'il est combiné au paramètre 'domain master = yes'.

Le paramètre '**os level**' détermine le niveau du serveur SAMBA dans les élections au titre de 'maître local'. Ici la valeur de 65 assure une élection quasi certaine.

Le paramètre '**security**' détermine comment les clients se connectent au serveur SAMBA.
'share' est peu utilisé, pour un serveur d'imprimante uniquement par exemple, avec des partages sans mot de passe (partage invité). La fourniture d'un éventuel mot de passe n'a lieu que lors de la

connexion à une ressource partagée.
'user' est la méthode par défaut de SAMBA 2.2. Le client doit d'abord s'identifier avant de recevoir la liste des ressources partagées disponibles. Les paramètres 'user' et 'guest only' n'interviennent qu'après cette authentification. Les partages invités ne peuvent donc pas fonctionner sans utiliser une correspondance automatique avec un compte invité (guest account). Le paramètre 'map to guest' permet cela.
'domain' est utilisé pour s'intégrer à un domaine Windows NT 4 (fonctionnement en tant que serveur membre). Les mots de passe doivent être cryptés (encrypted passwords = yes).

On doit maintenant définir les différentes sections qualifiant chacun des partages de fichiers :

[temp]
comment = Fichiers temporaires
path = /tmp
public = yes
read only = no
browsable = yes

Le paramètre '**comment**' identifie le partage dans le 'voisinage réseau' de Windows.

Le paramètre '**path**' définit l'emplacement de ce partage sur le serveur SAMBA.
ce répertoire devra disposer de droits d'accès pour tous :
 # chmod 777 /tmp

Le paramètre '**public**' indique ici que les connexions en tant qu'invité sont acceptées, tout le monde pourra donc y accèder.

Le paramètre '**read only**' autorise dans ce cas la création et la modification des fichiers.

Le paramètre '**browsable**' permet l'affichage ce partage dans le 'voisinage réseau' de Windows. Par defaut ce paramètre est à '**yes**' dans ce cas il n'est pas nécessaire de le mentionner.

[compta]
comment = Comptables
path = /home/compta
public = no
valid users = administrateur @compta
writable = yes

Le paramètre '**path**' définit l'emplacement de ce partage sur le serveur SAMBA.
Un groupe 'compta' pour les comptables devra avoir été défini au niveau de Linux, le répertoire /home/compta préalablement créé avec les droits adéquats :
 # groupadd compta
 # mkdir /home/compta
 # chmod –g compta /home/compta

Le paramètre '**public**' indique ici que les connexions en tant qu'invité sont refusées.

Le paramètre '**valid users**' définit ici l'administrateur et le groupe 'compta' (car précédé de @) comme seuls utilisateurs autorisés à utiliser cette ressource.

Le paramètre '**writable**' autorise les comptables à créer et modifier les fichiers.

[ventes]
comment = Statistiques commerciales
path = /home/compta/ventes
public = no
valid users = administrateur @compta @vendeurs
writable = no
write list = @compta
create mode = 0750

Le paramètre '**valid users**' définit ici l'administrateur et les groupes 'compta' et 'vendeurs' comme seuls autorisés à utiliser cette ressource.

Le paramètre '**writable**' interdit la création et la modification des fichiers. Ainsi les commerciaux pourront visualiser les résultats des ventes sans pouvoir les modifier.

Le paramètre '**write list**' autorise les les comptables à créer et modifier les fichiers. Les comptables pourront mettre à jour les résultats des ventes.

[privé]
comment = Dossiers confidentiels
path = /home/luc/private
public = no
valid users = luc
writable = yes
create mode = 0700
browsable = no

Le paramètre '**valid users**' n'autorise que l'utilisateur 'luc' à utiliser cette ressource. Les droits Linux devront avoir étés restreints pour ce répertoire :
 # chgrp luc /home/luc/private
 # chown luc /home/luc/private
 # chmod 700 /home/luc/private

Le paramètre '**browsable**' permet de ne pas faire apparaître ce partage dans le 'voisinage réseau' de Windows pour une meilleure confidentialité. Il faudra connaître le nom de cette ressource pour s'y connecter.

2.3 Serveur d'imprimantes

2.3.1 Paramètrage du serveur d'imprimantes

On ajoute à la section **[global]** les paramètres :

[global]
printing = cups
printer admin = administrateur

Le paramètre '**printing**' détermine la méthode de gestion des imprimantes utilisée par le serveur UNIX. CUPS (Common Unix Printing System) est le choix par défaut pour Mandrake Linux 9.2. De nombreuses autres méthodes sont disponibles en fonction du type de système d'exploitation (BSD, AIX, LPRNG, PLP, SYSV, HPUX, QNX, SOFTQ).

Le paramètre '**printer admin**' définit le ou les utilisateurs ou groupes autorisés à gérer les imprimantes SAMBA. Ici c'est l'administrateur Windows. Le super administrateur de Linux (root)

n'est pas explicitement défini car il possède automatiquement les droits de gestion de toutes les imprimantes.

On doit maintenant définir les différentes sections qualifiant chacun des partages d'impression :

```
[printers]
  comment = Toutes les imprimantes
  path = /var/spool/samba
  guest ok  = yes
  printable = yes
  print command = lpr –cups –P %p –o raw -r %s   browsable = yes
```

La section **[printers]** est une section spéciale comme la section **[global]**. Il en existe une troisième que nous verrons plus loin (**[homes]**).

Ainsi, tous les utilisateurs de SAMBA pourront se connecter à toutes les imprimantes définies dans le fichier '/etc/printcap' du serveur Linux.

Le paramètre '**path**' définit le répertoire utilisé par le spool de SAMBA

Le paramètre '**guest ok**' permet ici à tout le monde d'utiliser les imprimantes du serveur Linux.

Le paramètre '**printable**' doit obligatoirement être '**yes**' sinon le serveur refusera le chargement du fichier de configuration

Le paramètre '**print command**' définit la commande d'impression utilisée sur le serveur Linux. '**lpr**' est la commande Unix d'impression, l'argument **–cups** défini la méthode d'impression CUPS, l'argument **–P** défini comme imprimante de destination celle de nom **%p**, l'argument **–o** permet d'indiquer via l'option **raw** que le fichier est déjà formaté et qu'aucun filtre ne doit être appliqué, l'argument **–r** indique que les fichiers doivent être effacés après l'impression, la variable **%s** indique le répertoire du spool.

La section **[hpluc]** permet de définir une imprimante privée, réservée exclusivement à l'utilisateur 'luc'. De nombreuse variantes d'administration des imprimantes sont possibles.

```
 [hpluc]
  comment = HP  LaserJet 2100 de Luc
  path = /homes/luc
  printer= hp_luc
  public = no
  valid user = luc
  printable = yes
  browsable = no
```

Le paramètre '**path**' indique que le répertoire utilisé par le spool de cette imprimante est placé dans le répertoire personnel de l'utilisateur 'luc'

Le paramètre '**valid user**' indique que seul l'utilisateur 'luc' peut utiliser cette imprimante.

Le paramètre '**browsable**' indique indique ici que cette imprimante ne sera pas affichée dans la liste des ressources NETBIOS (puisque privée).

2.3.2 PDF Distiller

Un des autres services de SAMBA est de permettre la création de fichiers PDF.

L'installation sur le serveur SAMBA des drivers Windows Postscript, de préférence couleur, est souhaitable afin de permettre aux clients Windows d'auto installer ces drivers.

```
[pdf-generator]
  comment = Imprimante PDF
  path = /var/tmp
  guest ok = no
  printable = yes
  print command = /usr/share/samba/scripts/print-pdf %s ~%u //%L/%u %m %I &

[pdf-screen]
  copy = pdf-generator
  comment = Imprimante PDF – Qualité écran
  print command = /usr/share/samba/scripts/print-pdf %s ~%u //%L/%u %m %I "" %S &

[pdf-printer]
  copy = pdf-generator
  comment = Imprimante PDF – Qualité imprimante
  print command = /usr/share/samba/scripts/print-pdf %s ~%u //%L/%u %m %I "" %S &

[pdf-prepress]
  copy = pdf-generator
  comment = Imprimante PDF – Qualité imprimerie
  print command = /usr/share/samba/scripts/print-pdf %s ~%u //%L/%u %m %I "" %S &
```

Le paramètre '**copy**' permet d'inclure automatiquement dans les 3 sections pdf suivantes le contenu de la section [pdf-generator]. Les paramètres présents dans les 3 sections pdf suivantes remplacent les paramètres identiques de [pdf-generator].

3 Contrôleur de Domaine NT 4.0

Le modèle de groupe de travail de type 'égal à égal' (Peer To Peer) ne fonctionne qu'avec un nombre limité de postes. L'authentification devient rapidement contraignante car chaque utilisateur doit être défini sur chacun des postes où il est censé pouvoir travailler.

La notion de 'Domaine' est apparue avec Windows NT 3.51. Elle permet de centraliser la gestion des utilisateurs et des partages réseau.

Un serveur SAMBA peut se substituer à un serveur NT 4.0. Il peut se joindre à un domaine NT 4 en tant que serveur membre ou même devenir un contrôleur primaire de domaine (PDC),. Il ne peut cependant pas devenir un contrôleur de sauvegarde d'un serveur NT 4 (BDC) et encore moins être utilisé au sein d'une 'Active Directory' (AD) basée sur le protocole LDAP.

Afin de fonctionner en tant que PDC, il faut disposer d'une version de SAMBA 2.2.x ou 3.x, si un BDC est souhaité, il devra être aussi de type SAMBA et non NT/2000/2003.

Pour cela notre section [global] devient :

```
[global]
   workgroup = MANDRAKE
   netbios name = SAMBA
   server string = Serveur SAMBA %v
```

encrypt passwords = yes
name resolve order = wins lmhosts bcast
wins support = yes
time server = yes
local master = yes
preferred master = yes
os level = 65
security = user
printing = cups
printer admin = root administrateur
domain master = yes
domain logons = yes
domain admin group = root administrateur
logon drive = H:
logon script = logon.bat
logon path = \\%L\profiles\%u\%m
logon home = \\%L\%u\windows\%m
add user script = /usr/sbin/useradd -g machines -d /dev/null -s /bin/false -M %u

Le paramètre '**domain master**' confère au serveur SAMBA le rôle de 'domain master browser' répertoriant toutes les ressources partagées du groupe de travail. Attention si un serveur PDC Windows existe déjà un conflit de résolution de nom peut se produire.

Le paramètre '**domain logons**' confère au serveur SAMBA un rôle limité de 'contrôleur de domaine Windows NT 4'.

Ces 3 paramètres assurent au serveur SAMBA un fonctionnement en tant que contrôleur de domaine principal (PDC) vis-à-vis des clients Windows.

Le paramètre '**domain admin group**' permet de définir les noms des administrateurs SAMBA. Ici super utilisateur de Linux et l'administrateur de Windows NT/2000/XP. Un nom précédé de @ indique un groupe (@administrateurs pour le groupe des administrateurs de Windows NT/2000/XP par exemple).

Le paramètre **security**' est obligatoirement '**user**' puisqu'il faut authentifier les utilisateurs et non pas les ressources (comme avec 'share') et que le serveur SAMBA devenant le PDC du domaine doit donc traiter les ouvertures de session et non pas les transmettre à un autre PDC (comme avec 'domain').

Le paramètre '**logon drive**' permet de définir automatiquement un nom de disque pour le répertoire personnel à la connexion. Ici le lecteur H :.

Le paramètre '**logon script**' permet l'exécution d'un fichier de commande (.bat) à la connexion. Ce fichier est situé dans le répertoire défini par le paramètre path de la section [netlogon]. Ici le fichier / usr/local/samba/lib/netlogon/logon.bat pourrait contenir :

@NET TIME \\SAMBA /SET /YES

Le paramètre '**logon path**' permet de définir automatiquement un répertoire personnel pour les utilisateurs itinérants de type Windows NT/2000/XP.

Le paramètre '**logon home**' permet de définir automatiquement un répertoire personnel pour les utilisateurs itinérants de type Windows 95/98/Me. Cela permet d'utiliser par exemple dans un script ou depuis l'invite de commande MSDOS de Windows :
C:\> NET USE H: /HOME

Le paramètre '**add user script**' permet de créer automatiquement 'à la volée' le compte machine Linux correspondant au PC Windows lors de la première connexion. La variable %u contient le nom de machine NETBIOS terminé par $. Le groupe 'machines' (UID 421) doit être créé dans / etc/group. Ce compte est verrouillé sous Linux.

On doit aussi ajouter les sections [netlogon] et [homes] nécessaires à la connexion des différents utilisateurs :

```
[netlogon]
   path = /usr/local/samba/lib/netlogon
   writable = no
   browsable = no
```

Cette section est destinée à permettre les connexions des clients Windows au domaine.

Le paramètre **'path'** définit le répertoire où seront stockés les scripts de connexion et les policies systèmes. Les connexions échoueront si l'arborescence /usr/local/samba/lib/netlogon n'existe pas, il faut donc créer ce répertoire :

```
# mkdir /usr/local/samba/lib/netlogon
# chmod 775 /usr/local/samba/lib/netlogon
```

Le paramètre '**writable**' permet d'accepter (yes) ou de refuser (no) l'écriture sur un partage. Ici les utilisateurs ne font que lire les scripts de connexions et les policies, il est inutile de leur accorder des droits d'écriture.

Le paramètre '**browsable**' permet d'afficher (yes) ou de masquer (no) une ressource réseau. Ici les utilisateurs du réseau n'ont pas besoin de voir le partage netlogon.

```
[homes]
   read only = no
   create mask = 0600
   directory mask = 0700
   guest ok = no
   browsable = no
   map archive = yes
```

La section **[homes]** est le troisième type de section spéciale de SAMBA

SAMBA ajoute le répertoire personnel de l'utilisateur (trouvé dans /etc/passwd) en tant que partage apparaissant comme un dossier au nom de l'utilisateur sur le poste client. SAMBA remplace 'homes' par le nom de l'utilisateur.

Les directives '**create mask**' et '**directory mask**' définissent les masques Unix de création de fichier et de répertoire. Ici les droits de Lecture + Ecriture (4+2=6) pour les fichiers et Lecture + Ecriture + Lister (4+2+1=7) pour les répertoires ne sont accordés qu'au seul propriétaire.

Le paramètre '**guest ok**' autorise (yes) ou refuse (no) les connexions en tant qu'invité.

Le paramètre '**browsable**' indique que ce partage ne doit pas être diffusé à tous les utilisateurs.

Le paramètre '**map archive**' permet de s'assurer que l'attribut DOS archive est transformé en bit d'exécution pour le propriétaire. Ceci permet de rendre les scripts exécutables sous Linux.

```
[profiles]
   path = /home/ntprofiles
   writable = yes
   create mask = 0600
   directory mask = 0700
   browsable = no
```

La section **[profiles]** est nécessaire pour les clients utilisant les profils itinérants de Windows NT/2000/XP. Cela permet à un utilisateur d'obtenir le même environnement de travail quel que soit le PC d'où il se connecte.

Le paramètre **'path'** indique ou seront stockés les profils sur le serveur SAMBA. Les clients devront pouvoir lire et écrire des données.

```
# mkdir /home/ntprofiles
# chmod 777 /home/ntprofiles
```

3.1 Comptes d'ordinateurs :

Afin de pouvoir se connecter dans un domaine, chaque poste doit disposer d'un 'compte d'ordinateur' ressemblant aux 'comptes d'utilisateurs'. Ces comptes sont créés par un administrateur sur les postes Windows NT/2000/XP. Pour un système Linux nous utiliserons le super utilisateur root auquel nous devons donner un compte SAMBA :

 # smbpasswd –a root

```
New SMB password:
Retype new SMB password:
Added user root.
```

Il peut être intéressant de donner un mot de passe différent de celui utilisé pour Linux afin d'éviter de compromettre la sécurité du serveur Linux.

Quand un compte d'utilisateur est créé par SAMBA, 2 actions ont lieu.

- Une ligne est ajoutée au fichier smbpasswd, stockant le mot de passe, avec un nom composé du nom NETBIOS auquel est accolé un $. Ceci est réalisé automatiquement par la commande smbpasswd.
- Une ligne correspondante est recherchée dans le fichier des mots de passe Unix /etc/passwd afin de donner au compte d'ordinateur un Identifiant d'Utilisateur (UID) sur le serveur SAMBA. Cette fonctionnalité est apparue depuis la version 2.2.

Il convient donc de créer un compte d'utilisateur qui ne sera jamais utilise pour des connexions Linux. On peut utiliser la commande useradd de Linux. Le répertoire personnel et le shell devront être neutralisés, si le nom NETBIOS du poste est PC01 on aura :

 # useradd –g machines –d /dev/null –s /bin/false –M –c "Compte Ordinateur" pc01$

Cette commande provoque l'ajout de la ligne suivante dans /etc/passwd :

```
pc01$:x:505:421:Compte Ordinateur:/dev/null:/bin/false
```

Une ligne a aussi été ajoutée au fichier de sécurité /etc/shadow :

```
pc01$:!!:11625:0:99999:7:::
```

La version 2.2 de SAMBA permet de simplifier ce processus en permettant une création du compte d'utilisateur 'à la volée' lors de la première connexion au domaine. Pour cela il faut ajouter le paramètre 'add user script' dans la section [global] :

```
[global]
   add user script = /usr/sbin/useradd –g machines –d /dev/null –s /bin/false –M
      –c "Compte Ordinateur" %u
```

Le compte de l'ordinateur sera automatiquement créé lors de la connexion au domaine. La variable %u représente le nom de l'ordinateur auquel est automatiquement rajouté le $ (identique à %m$).

Il suffit alors sur le poste client d'activer la connexion au domaine suivant la version de Windows l'équipant. ATTENTION : les postes sous Windows XP Edition Familiale (XP Home) ne peuvent pas se connecter à un domaine NT 4 où à une « Active directory », cette prestation est réservée à Windows XP Professionnel.

4 Paramètres complémentaires

De nombreux paramètres supplémentaires sont disponibles afin d'obtenir une configuration du serveur SAMBA la plus proche possible des besoins de l'administrateur.

[global]
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
character set = ISO8859-1
oplocks = no

Le paramètre '**socket options**' permet d'optimiser le fonctionnement du serveur SAMBA. Les paramètres fournis donnent usuellement de bons résultats.

Le paramètre '**character set**' permet de définir la façon de transcrire les noms de fichiers. Ce paramétrage vaut pour l'Europe.

Windows inclus un mécanisme de 'verrouillage opportuniste' des fichiers lors des accès simultanés afin de gagner un peu de rapidité. Ce système peut poser des problèmes (sur de gros fichiers par exemple). Le paramètre '**oplocks**' permet de désactiver ce mécanisme afin d'éviter des corruption de fichier, mais avec un ralentissement d'environ 30 %. La valeur par défaut est '**yes**'.

Il ne reste plus maintenant qu'à paramétrer votre serveur SAMBA 2.2 en fonction de vos besoins.

Luc ROLLAND
luc@rolland-fr.com