

SUPPORT SAMBA

Thierry GRANDADAM

TABLE DE MATIERES

GENERALITES	3
1. INSTALLATION ET DEMARRAGE DE SAMBA.....	3
1.1. Pré installation.....	3
1.2. Installation	4
2. CONFIGURATION DE SAMBA	4
2.1. Le fichier smb.conf.....	4
2.2. La section [global].....	6
SAMBA EN TANT QUE SERVEUR DE FICHIERS AVEC DES CLIENTS WINDOWS 98	7
1. INTRODUCTION	7
2. CONFIGURATION DU SERVEUR SAMBA.....	7
2.1. La section [global].....	8
2.2. La section [homes].....	9
2.3. La section [partage].....	9
2.4. La section [public].....	10
3. DEMARRAGE DE SAMBA	10
3.1. Création des utilisateurs Samba.....	10
3.2. Lancement du serveur Samba.....	11
4. CONFIGURATION DU CLIENT WINDOWS98	12
4.1. Configuration des paramètres réseau	12
4.2. Configuration des paramètres réseau	12
5. PLUS LOIN AVEC SAMBA	12
5.1. Configuration d'une imprimante partagée.....	12
5.2. Des partages personnalisés.....	13
SAMBA EN TANT QUE PDC D'UN DOMAINE WINDOWS 2000	15
1. INTRODUCTION	15
2. LE FICHIER SMB.CONF	16
3. CREATION DES COMPTES UTILISATEURS SUR LE SERVEUR.....	21
3.1. Création des comptes utilisateurs dans Linux.....	21
3.2. Création des comptes utilisateurs dans Samba.....	22
3.3. Création des comptes machines dans Samba.....	22
3.4. Le compte root.....	23
4. CONFIGURATION DES POSTES WINDOWS2000.....	23
5. APPLICATION DES STRATEGIES DE SECURITE	24
5.1. Eléments requis	24
5.2. Utilisation de POLEDIT.....	24
5.3. Configuration de SAMBA.....	26
SAMBA EN TANT QUE MEMBRE D'UN DOMAINE WINDOWS 2000.....	27
1. INTRODUCTION	27
2. CONFIGURATION DE WINBIND	27
3. CONFIGURATION DE SAMBA	29
4. DEMARRAGE DE SAMBA	30

Généralités

Introduction

Samba est un outil qui permet de réunir les systèmes Windows et Unix/Linux. Samba permet donc à votre serveur Unix/Linux d'être reconnu comme une machine Windows sur le réseau. Cela veut dire que chaque utilisateur Windows pourra utiliser les ressources d'un serveur Unix/Linux comme s'il s'agissait d'un serveur Windows NT ou 2000.

En fait, Samba est une implémentation du protocole SMB (Server message Block) pour Unix. Le protocole SMB est le coeur de NetBIOS. Il nous permettra de partager répertoires et imprimantes Unix/Linux avec Windows le tout sans logiciel spécial du côté du client.

Un serveur Unix/Linux sur lequel "tourne" Samba peut aussi être transformé en Contrôleur de Domaine qui validera les connections des clients Windows, permettre à un script d'être exécuté et aussi gérer les profils utilisateurs comme sur un serveur Windows. Il peut aussi facilement devenir un membre de domaine et utiliser n'importe quel contrôleur de domaine existant pour effectuer toutes les tâches d'authentification.

Samba peut aussi devenir maître d'exploration sur un réseau Windows comme n'importe quelle autre machine Windows. Mais à l'inverse d'une machine Windows, son rôle dans le processus peut être facilement configuré.

Aussi peut-il être configuré comme serveur WINS. Il peut alors servir pour connaître l'adresse IP d'une machine donnée.

La communication avec une machine Windows nécessitera certainement que le serveur soit capable d'utiliser des mots de passe cryptés . C'est possible avec Samba.

Finalement, Samba peut être compilé sur une grande variété de versions Unix/Linux.

Toutes ces fonctions de Samba résident dans deux daemons : `smbd` et `nmbd`. Le premier est le serveur lui-même, réalisant les authentifications, donnant l'accès aux partages et ou imprimantes, jouant le rôle du contrôleur de domaine, ... et le second performe toutes les opérations de résolution des noms (WINS...).

1. Installation et démarrage de SAMBA

1.1. Pré installation

Dans tous les chapitres qui vont suivre nous utiliserons la version 3.05 de samba (disponible sur le site officiel samba.org) installer sur un serveur Linux Redhat 9 et d'un client Windows 98

Le protocole utilisé pour la communication entre Samba et le reste du réseau Windows est TCP/IP. Il est donc nécessaire d'avoir au préalable installé ce protocole sur la machine Windows et d'avoir correctement installé la carte réseau du serveur Unix/Linux. Pour rappel, vous devrez avoir attribué une adresse IP unique et dans la même classe pour chacune des machines.

Sous Linux, il faut se souvenir que l'utilitaire **linuxconf** vous permet de configurer votre carte réseau ; il existe aussi l'utilitaire graphique **netcfg** ainsi que la commande **ifconfig**.

Le plus simple pour vérifier tout ça et de « faire un ping » entre les deux machines.

1.2. Installation

Si vous avez installé en même temps que Linux, vous devez trouver les deux démons **smb** et **nmb** dans le répertoire `/etc/rc.d/init.d`

S'ils ne sont pas présents, vous devez les installer en suivant la démarche suivante :

- Monter le CD-ROM en tapant **mount /dev/cdrom /mnt/cdrom**
- Déplacez-vous dans le répertoire `cd /mnt/cdrom/Redhat/RPMS`
- Installez le package : **rpm -ivh samba-3.05rc1-2_rh9.i386.rpm**

Maintenant vous pouvez vérifier votre installation en vérifiant la présence des fichiers suivants dans le répertoire `/usr/bin` :

- smbclient
- smbprint
- smbstatus
- smbrun
- smbadduser
- smbpasswd
- smbtar

1.3. Démarrage

Maintenant vous devez lancer les deux démons **smb** et **nmb**. Le plus simple est de le faire automatiquement au démarrage en tapant **setup** et en choisissant ensuite **System services** puis en cochant **smb**.

Il existe la commande **service** pour démarrer (**start**), ou arrêter (**stop**) un service, voir le statut (**status**).

Vous pouvez aussi le faire manuellement grâce au script `/etc/rc.d/init.d/smb` et en tapant la ligne `/etc/rc.d/init.d/smb start` ou `/etc/rc.d/init.d/service smb start`

2. Configuration de SAMBA

2.1. Le fichier smb.conf

Pour configurer samba, il est nécessaire de renseigner un unique fichier qui s'appelle **smb.conf** dans notre cas il se trouve dans `/etc/samba`.

Il est préférable de le copier dans un autre répertoire (par exemple `/root/originaux/`) afin d'en avoir une version propre en cas d'erreur

Ce qu'il faut savoir avant d'éditer et de modifier ce fichier :

C'est un fichier de type texte qui s'utilise comme un fichier `.ini` sous Windows c'est-à-dire qu'il est divisé en *sections* contenant des *clés* auxquelles sont attribuées des *valeurs*

Exemple :

[global]
WORKGROUP = GUDUBULLE

Nom de la section

Nom d'une des clés de la section "global"

Valeur attribuée à cette clé

Les sections du fichier smb.conf sont :

[global] Contient les définitions des paramètres généraux du serveur SAMBA

[homes] Contient les définitions du partage propre à chaque utilisateur du serveur (répertoire de base sous Windows). En fait le système se base sur la liste des utilisateurs Linux qui ont été définis dans le fichier /etc/passwd. Puis il rattache automatiquement le nom de l'utilisateur à son répertoire personnel.

[printers] Contient les définitions des imprimantes partagées par le serveur SAMBA

[nom_du_partage] Contient la définition d'un partage qui ici s'appellera nom_du_partage.

On verra plus tard qu'on peut aussi créer une imprimante avec un nom de partage différent de [printers].

Dans ce fichier, on peut utiliser des variables prédéfinies dont voici quelque unes parmi les plus importantes.

Variable	Définition
Client	
%a	Architecture client (Samba, Wfw pour windows 3.11, WinNT pour windows Nt ou 2000, Win95 pour Windows 95 ou 98 ...)
%l	Adresse IP du client
%m	Nom NetBios du client
%M	Nom DNS du client
Utilisateur	
%u	Nom d'utilisateur Windows
%U	Nom d'utilisateur Linux
%g	Groupe Primaire de %u
%G	Groupe Primaire de %U
Partage	
%p	Répertoire principal
%P	Répertoire principal du partage courant
%S	Nom du partage en cours
Serveur	
%d	ID du processus
%h	Nom DNS du Serveur
%H	Contenu de la variable HOME
%L	Nom NetBios du serveur
%N	Répertoire
%v	Version de Samba
Divers	
%R	Niveau de protocole négocié
%T	Date et heure courantes

Attention, si le premier caractère de la ligne est le symbole ; ou # cela signifie qu'il s'agit d'une ligne de commentaire.

2.2.La section [global]

Voici les principales entrées de cette section :

dns proxy	Le serveur samba doit-il faire également office de proxy DNS ?
domain logons	Samba doit-il gérer les contrôles de connexions pour le domaine ?
domain master	Active samba comme serveur maître du domaine
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 !
Interfaces	Si votre serveur linux dispose de plusieurs cartes réseaux et que vous voulez restreindre son activité à un seul réseau.
invalid users	Liste des utilisateurs interdits d'accès à Samba. Par exemple "root" devrait être interdit.
local master	Active samba comme serveur maître local
logon home	Où faut-il stocker les profils itinérants des utilisateurs ?
logon path	Où se trouvent les fichiers script de démarrage ?
logon script	Quel sera le script à lancer lors de l'ouverture de la session de cet utilisateur ?
max log size	Taille maximum du fichier de log.
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.
os level	"Niveau" de votre OS pour savoir qui sera élu maître du domaine, local etc.
passwd chat	Quel est le "protocole" de discussion pour changer le mot de passe.
passwd program	Quel programme lancer pour changer le mot de passe.
preferred master	Samba doit-il être "préféré" à tout autre serveur s'il y en a ?
preserve case	Permet de garder la casse des noms de fichiers.
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 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.
server string	Description de votre serveur linux.
short preserve case	Permet de garder la casse des noms de fichiers.
socket options	Une liste d'options pour "affiner" votre samba et faire en sorte qu'il réagisse plus vite par exemple.
unix password sync	Faut-il synchroniser les mots de passe unix et windows ?
wins support	Votre serveur linux fait-il aussi office de serveur wins ?
Workgroup	Nom du groupe de travail dont votre serveur linux doit faire partie.

Afin de comprendre aisément la mise en place d'un serveur Samba, nous allons expliquer quelques exemples de configuration :

- Un serveur Samba en tant que serveur de fichiers avec des clients Windows 98
- Un serveur Samba PDC d'un domaine Windows 2000
- Un serveur Samba dans un domaine comprenant un serveur PDC sous Windows 2000.

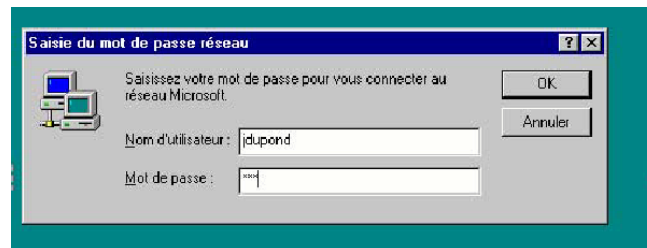
Samba en tant que serveur de fichiers avec des clients Windows 98

1. Introduction

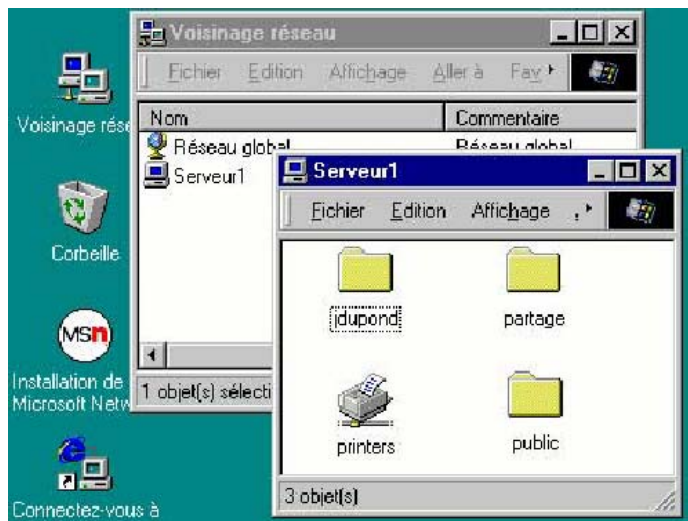
Un des plus importants paramètres de smb.conf est le paramètre "security". Il existe 4 modes disponibles sur un serveur Samba, qui sont :

share / user / server / domain

Dans ce cas, l'installation va se faire en mode user. Ce mode est assez simple. En mode user sur le serveur Samba. Le client Windows 98 se comporte de la manière suivante :



Une fois connecté voilà ce qu'on observe dans le voisinage réseau:



Un serveur qui a comme nom Serveur1 et sur ce serveur, on voit apparaître un certain nombre de partages. Il y a les répertoires "jdupond", "partage", "public" et une imprimante réseau.

Ces quatre éléments sont en fait sur un serveur Linux sur lequel "tourne" SAMBA.

2. Configuration du serveur Samba

Dans le répertoire de base de Samba (/etc/samba), après avoir renommé le fichier smb.conf d'origine en smb.conf.backup nous allons créer un nouveau fichier texte smb.conf contenant les lignes suivantes:

```
[global]  
netbios name = Serveur1  
workgroup = GUDUBULLE  
security = user  
os level = 65  
hosts allow = 192.168.1.101 192.168.1.201  
encrypt passwords = yes  
smb passwd file = /etc/smbpasswd  
guest account = invite
```

```
[homes]  
comment = repertoire perso  
path = %H  
writeable = yes  
valid users = %S  
browseable = no
```

```
[partage]  
path = /home/partage  
writeable = yes  
valid users = @users  
locking = yes  
create mode = 0660  
directory mode = 0770
```

```
[public]  
path = /usr/doc  
guest ok = yes  
writeable = no
```

Avant de configurer le client Windows 98 et de démarrer le serveur SAMBA, il est je crois nécessaire d'expliquer le paramétrage ci-dessus section par section

2.1. La section [global]

C'est la section qui définit les paramètres généraux du serveur Samba

netbiosname = Serveur1

Nom netbios du serveur Samba tel qu'il apparaîtra dans le voisinage réseau des postes windows. Il est bien sûr différent du nom du serveur Unix/Linux sur lequel "tourne samba"

workgroup = GUDUBULLE

Nom du groupe de travail, en l'occurrence c'est GUDUBULLE

security = user

Mode de sécurité, c'est le mode « user », ou dit utilisateur.

Lorsque le client se connecte au serveur, celui-ci va être identifié grâce à la combinaison "nom d'utilisateur" et "mot de passe". Le serveur n'envoie aucune information au client lui indiquant qu'il fait partie des utilisateurs autorisés à se connecter.

os level = 65

Définition du niveau des élections dans l'exploration du réseau.

64 : Client 2000

32 : Serveur NT

16 : Client NT

1 : Poste W9X

Donc pour que Samba gagne les élections, on affecte ce paramètre à 65.

Hosts allow = 192.168.1.101 192.168.1.201

On autorise seulement 2 machines à se connecter au serveur, on spécifie donc ici leurs adresses IP. Il est possible d'indiquer tout un réseau, à l'aide des masques de sous réseau, sous la forme :

192.168.1.

On peut aussi spécifier une plage d'adresses :

192.168.1.32/255.255.255.224

encrypt passwords = yes

Utilisation de mots de passes cryptés. Obligatoire lorsque le client est Windows98 ou Windows NT. Si vous l'omettez, vous n'aurez aucun accès possible au serveur.

smb passwd file = /etc/smbpasswd

On indique où se trouve le fichier contenant les mots de passe SAMBA des utilisateurs. Attention les mots de passe SAMBA sont distincts des mots de passe Linux/Unix.

guest account = invite

Indique que l'on a créé un utilisateur invite, cet utilisateur n'a pas de mot de passe, pour être exact son mot de passe doit être nul. Par sécurité, il n'est pas conseillé d'autoriser l'écriture pour cet utilisateur.

2.2. La section [homes]

C'est le partage par défaut de Samba, en fait le système utilise la variable "homes" qui rattache le nom de l'utilisateur à son répertoire sur le serveur Linux. Samba utilise le fichier /etc/passwd pour savoir où se trouve le répertoire de chaque utilisateur déclaré sur le serveur. Si vous avez créé un utilisateur jdupond sur le serveur Linux, lorsque l'utilisateur jdupond se connectera sur le poste W98, son répertoire personnel qui se trouve par exemple en /home/jdupond (sur le serveur Linux) sera monté automatiquement sous la forme d'un répertoire ayant pour nom jdupond (sur le poste W98).

comment = repertoire perso

Commentaire affiché lorsqu'on visualise le répertoire dans l'explorateur Windows sous la forme "détail", sur le poste W98.

path = %H

Chemin du partage. Ici on utilise la variable %H de Samba, cette variable correspond au répertoire personnel du nom de l'utilisateur Linux/Unix.

writeable = yes

On indique que le partage [homes] est en mode écriture.

valid users = %S

Ce paramètre indique la liste des utilisateurs autorisés à connecter au partage [home]. Ici on utilise la variable %S qui correspond au nom du Service Actuel.

browseable = no

On fait en sorte que le partage [homes] ne soit pas explorable dans le voisinage réseau.

2.3. La section [partage]

Désignation d'un nouveau partage qui se nommera "partage" sous Windows

path = /home/partage

Chemin d'accès Linux/Unix à ce partage

writeable = yes

On autorise l'écriture dans ce partage

valid users = @users

On précise ici la liste des utilisateurs autorisés à accéder à ce partage. Notez bien le "@" qui signifie groupe Linux/Unix. Toute personne faisant partie du groupe Linux/Unix users a le droit d'accéder à ce partage, à condition qu'elle ait été définie dans le fichier /etc/smbpasswd.

locking = yes

Verrouillage des fichiers, lorsqu'un utilisateur utilise un des fichiers, personne d'autre n'a le droit d'aller y écrire. Par contre tous les utilisateurs ont le droit de le lire.

create mode = 0660

Masque de création des nouveaux fichiers, ce masque est en fait équivalent à la commande `chmod 660`.

directory mode = 0770

Masque de création des répertoires.

2.4. La section [public]

Désignation d'un nouveau partage qui se nommera "public" sous Windows

path = /usr/doc

Chemin Unix du partage.

guest ok = yes

Ce partage est autorisé au compte invité défini dans la section [global].

writable = no

Comme c'est un répertoire accessible à n'importe qui, on ne l'autorise pas en écriture.

3. Démarrage de Samba

Avant tout il est nécessaire de vérifier qu'il n'y a pas de faute de frappe ou autre dans le fichier `smb.conf`. Pour cela on utilise "**testparm**" en tapant:

```
testparm smb.conf
```

si tout va bien on devrait voir ceci s'afficher à l'écran

```
Load smb config files from /etc/smb.conf  
Unknown parameter encountered: "domain controller"  
Ignoring unknown parameter "domain controller"  
Processing section "[homes]"  
Processing section "[printers]"  
Processing section "[Partage]"  
Loaded services file OK.  
Press enter to see a dump of your service definitions
```

Si vous voulez observez en détail la liste des variables, validez par entrée. Attention la liste est longue. Sinon Ctrl-C.

3.1. Création des utilisateurs Samba

Admettons que nous ayons un utilisateur "jdupond" qui fait partie du groupe "users" On suppose que le groupe "users" a déjà été défini sur Linux/Unix.

Il faut que l'utilisateur ait été déclaré sur le serveur Linux/Unix par exemple à l'aide de la commande :

```
adduser jdupond -g users  
adduser invite
```

Attention, les utilisateurs qui ont été définis sur le serveur Samba n'ont pour l'instant aucun mot de passe SAMBA. Il faut se placer dans le répertoire **/etc** et taper la commande suivante :

```
cat passwd | mksmbpasswd.sh > smbpasswd
```

Vous devriez vous retrouver avec un fichier **smbpasswd** qui est la forme suivante :

```
#  
# SMB password file.  
#  
root:0:XXXXXXXXXXXXXXXXXXXXXXXXXX:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:[U]:LCT-  
00000000:root
```

On supprime toutes les lignes correspondant à un utilisateur Linux/Unix qui n'utilisera pas Samba. Pour affecter un mot de passe SAMBA à l'utilisateur **jdupond**, on utilise la commande:

```
smbpasswd jdupond  
New SMB password: *****  
Retype new SMB password: *****  
Password changed for user jdupond.
```

Attention, à partir de cet instant, si vous avez ajouté un utilisateur Linux/Unix, et que vous voulez rajouter cet utilisateur dans le fichier **smbpasswd**, il n'est pas nécessaire de relancer la commande *cat passwd..* Car si vous utilisez cette commande vous serez obligé de retaper tous les mots de passe des utilisateurs SAMBA. Utilisez donc la commande :

```
smbpasswd -a nouvel_utilisateur  
New SMB password: *****  
Retype new SMB password: *****
```

Lorsque les mots de passe ont été configurés, vous pouvez lancer le serveur SAMBA.

3.2. Lancement du serveur Samba

Il suffit de lancer la commande suivante :

```
/etc/rc.d/initd/smb start
```

Pour vérifier que les processus tournent correctement :

```
/etc/rc.d/init.d/smb status
```

Pour arrêter le serveur :

```
/etc/rc.d/init.d/smb stop
```

Pour relancer le serveur :

```
/etc/rc.d/init.d/smb restart
```

Sous Redhat 9.0 on peut utiliser la commande **service** ("service smb start" par exemple).

4. Configuration du client Windows98

4.1. Configuration des paramètres réseau

Les modifications à faire se situent au niveau réseau, un clic bouton droit sur l'icône voisinage réseau et on choisit "Propriétés". Dans l'onglet "Configuration", vérifier que l'ouverture de la session est sur "Client pour les réseaux Microsoft".

Ensuite dans l'onglet "Identification", assurez-vous que le nom du groupe de travail soit le même que celui spécifié dans le fichier smb.conf (GUDUBULLE).

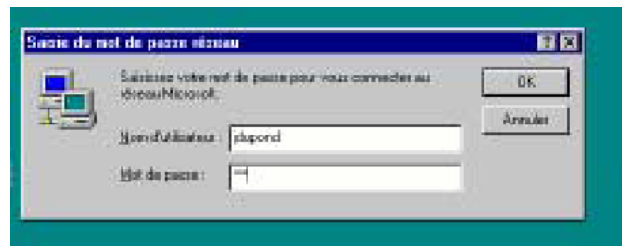
On passe à l'onglet "Contrôle d'accès" pour vérifier que la case cochée soit celle du "contrôle d'accès au niveau ressource".

Revenir sur l'onglet Configuration et double-cliquer sur "Client pour les réseaux Microsoft". Bien vérifier que l'option Re-connexion des lecteurs réseaux est positionnée à Connexion rapide.

Enfin il vous suffit de configurer l'IP de votre machine. Souvenez-vous que seulement deux adresses IP ont été autorisées à accéder au serveur Samba (voir section [global] du smb.conf)

4.2. Configuration des paramètres réseau

Une fois le client Windows 98 redémarré, vous devez obtenir un dialogue qui ressemble à ça :



Attention : ne faites pas d'erreur de frappe, lorsque vous entrez le nom de l'utilisateur et son mot de passe, le serveur ne vous enverra aucun message, vous indiquant que vous n'y avez pas accès.

Lorsque vous êtes connecté en tant qu'utilisateur jdupond, en explorant le voisinage réseau, sur le serveur Serveur1 vous devriez voir trois partages "jdupond", "partage" et "public".

5. Plus loin avec Samba

Il peut être nécessaire de rajouter une imprimante partagée au serveur. Il est recommandé d'utiliser des imprimantes PostScript, car elles sont "universelles". Il n'y a pas besoin de drivers spécifiques

5.1. Configuration d'une imprimante partagée

La configuration est définie comme un partage, la distinction se faisant dans l'utilisation du paramètre : printable = yes

Il suffit de rajouter les lignes suivantes au fichier smb.conf :

```
[Laser PS]
printable = yes
printer driver = Apple LaserWriter Pro 630
print command = /usr/bin/lpr -r %s
printer = lp
read only = yes
guest ok = yes
```

Quelques explications

[Laser PS]

Nom de l'imprimante dans le voisinage réseau de Windows98

```
print command = /usr/bin/lpr -r %s  
printer = lp  
read only = yes  
guest ok = yes
```

```
printable = yes
```

Indique si il s'agit d'un partage de type imprimante

```
printer driver = Apple LaserWriter Pro 630
```

Désignation du driver qui est nécessaire sur le Client, lors de l'installation de l'imprimante. Attention : lors de l'installation de l'imprimante, il se peut que le poste sous W98 demande le CD Windows.

```
print command = /usr/bin/lpr -r %s
```

Commande qui sera exécutée par le serveur (commande Linux/Unix) lors du lancement d'une impression. On utilise la commande *lpr -r*
L'option *-r* supprime les fichiers lorsqu'ils ont été imprimés

```
printer = lp
```

Nom de l'imprimante qui est rattachée au serveur Linux. En général, il s'agit de lp.

5.2. Des partages personnalisés

Lorsque l'utilisateur invité se connecte, il voit apparaître le partage "public" ce qui est normal, mais il voit aussi le partage "partage".

Pour éviter cela, on peut utiliser une fonction très pratique du fichier smb.conf qui est la fonction *include*

Sa syntaxe est la suivante :

```
include = chemin_d'accès_du_fichier.
```

Elle permet de créer un fichier smb.conf qui est fonction d'une variable de Samba
Admettons que l'utilisateur "jdupont" fasse partie du groupe "users" et que l'utilisateur "invite" d'un groupe appelé "invites"

On pourrait créer un fichier smb.conf comme ceci

```
[global]
```

```
netbios name = Serveur1
```

```
workgroup = GUDUBULLE
```

```
security = user
```

```
os level = 65
```

```
hosts allow = 192.168.1.101 192.168.1.201
```

```
encrypt passwords = yes
```

```
smb passwd file = /etc/smbpasswd
```

```
guest account = invite
```

```
include = /etc/smb/%G.conf
```

A la connexion Samba va remplacer %G dans smb.conf par sa valeur c'est-à-dire le nom du groupe de l'utilisateur. On aura donc une section [global] commune aux deux groupes contenue dans smb.conf et des partages propres à chacun des deux groupes contenues dans les fichiers users.conf et invites.conf comme ceci

```
[homes]
comment = Repertoire perso de %u
path = %H
writeable = yes
valid users = %S
browseable = no
```

```
[imprimante]
comment = Imprimante PostScript
path = /var/spool/samba
printable = yes
writeable = no
```

```
[partage]
path = /home/partage
writeable = yes
valid users = @users
locking = yes
create mode = 0660
directory mode = 0770
```

```
[public]
path = /usr/doc
guest ok = yes
writeable = no
```

/etc/smb/users.conf

```
[public]
path = /usr/doc
guest ok = yes
writeable = no
```

/etc/smb/invite.conf

Aujourd'hui il existe des utilitaires de plus en plus complet qui permettent d'administrer un serveur SAMBA. Le principe est toujours le même : il faut un navigateur et connaître le port.

L'utilitaires graphique (SWAT – SMBEdit) utilisant un navigateur html en tapant l'URL <http://localhost:901> (il faut décommenter la ligne `swat stream tcp nowait.400` et `root /usr/sbin/swat swat` dans le fichier `/etc/inet.conf` et relancer inet avec la commande `/etc/rc.d/init.d/inet restart`).

Le plus complet est Webmin qui faut aller chercher sur le net et l'installer. Le port est le 10000. Il fait tout s'est simple.

Samba en tant que PDC d'un domaine Windows 2000

1. Introduction

Nous allons étudier comment configurer un domaine comportant des clients Windows 2000 et un serveur Samba. Ce serveur devra donc identifier les clients et les utilisateurs du domaine à la manière d'un PDC Windows 2000. Dans notre exemple, on considère que notre entreprise GUDUBULLE est composée de 5 salariés

Le directeur :

- Jésus WILEBOSS

La secrétaire :

- Jessica NETDANLFRIGO

Les commerciaux :

- Jean VENPLUSKEMARC
- Marc AVENUE

Les infographistes :

- Nordine HATEUR
- Salah Me

Les noms d'utilisateur seront les prénoms (sans accent), chaque utilisateur aura un PC (windows2000) dont le nom sera pc suivi du prénom de l'utilisateur (pcjesus pour le PC du directeur). On va répartir les utilisateurs en 3 groupes.

Le groupe **admin**:

- composé des utilisateurs jesus et jessica
- accède à l'imprimante réseau laser_admin
- accède en écriture aux partages **administration**, **commerce** et **info**
- gère le partage **public**

Le groupe **comm**:

- composé des utilisateurs jean et marc
- accède à l'imprimante réseau laser_comm
- accède en écriture au partage **commerce**
- accède en lecture aux partages **info** et **public**

Le groupe **info**:

- composé de l'utilisateur nordine et salah
- accède à l'imprimante locale
- accède en écriture au partage **info**
- accède en lecture au partage **public**

De plus chaque utilisateur dispose d'un lecteur personnel.

2. Le fichier smb.conf

Voici le fichier en Samba 3.08

```
[global]
#Section Global : Définition du fonctionnement général de SAMBA

#Indique le nom du groupe de travail pour Microsoft
WORKGROUP = guichard
#Indique le nom du serveur Samba
NETBIOS NAME = SRVLINUX
#Définit le niveau des élections :
# 1=Win9x
# 16=Clt NT4
# 32=Serveur NT4
# 64=Clt Win2000 & XP
#En définissant 255, on est sûr que Samba sera maître d'explorateur
OS level = 255
#On définit la sécurité au niveau du partage ou de l'utilisateur
security = user
#On indique que les mots de passe sont cryptés
encrypt passwords = yes
#On indique le chemin du fichier des utilisateurs autorisés de Samba
smb passwd file = /etc/samba/smbpasswd
#Synchronise le mot passe de Samba avec Linux
unix password sync = yes
#
passwd program = /usr/bin/passwd %u
#J'autorise toutes les adresses IP de la plage à Samba
hosts allow = 200.200.200.
#La correspondance des noms se trouve ds "smbusers"
username map = /etc/samba/smbusers
#On définit l'ordre de résolution des noms en TCP/IP puis WINS puis fichier HOSTS
name resolve order = bcast wins hosts
#Samba est le maître explorateur
domain master = yes
#Permet à Win9x de se rajouter au domaine
local master = yes
preferred master = yes
wins support = yes
#Permet à Windows 2000 et XP de se rajouter au domaine
domain logons = yes
#Compte administrateur valide sur le domaine
net groupmap add unixgroup = root ntgroup = Administrateurs
#Définit le chemin d'accès des profils de Win 2000
logon path = \\%L\profils\%U

#=====Définitions des partages=====

#Le nom entre [] est le nom de partage
[commun]
#Indique le chemin du dossier qui sera partagé
path = /commun
#On indique le type d'accès
writeable = yes
#On indique si le partage est visible ou pas
browseable = yes
#Indique qui peut accéder au dossier
valid users = %U

#=====Définitions des partages=====

#Le nom entre [] est le nom de partage
[%U]
#Indique le chemin du dossier qui sera partagé
path = /users/%U
#On indique le type d'accès
writeable = yes
#On indique si le partage est visible ou pas
browseable = no
#Indique qui peut accéder au dossier
valid users = %U
#Les droits par défaut pour la création d'un répertoire
directory mode = 0700
```

#Les droits par défaut pour la création d'un fichier
create mode = 0700
#Indique le chemin du répertoire privé de Linux
path = %H

[NETLOGON]
#Indique le chemin du dossier qui sera partagé
path = /NETLOGON
#On indique le type d'accès
writeable = no
#On indique si le partage est visible ou pas
browseable = yes
#Indique qui peut accéder au dossier
valid users = %U

[admin]
browseable = yes
valid users = %U
path = /admin

[comm]
browseable = no
valid users = %U
path = /comm

[info]
browseable = no
valid users = %U
path = /info

[profils]
public = yes
guest ok = yes
writeable = yes
browseable = yes
valid users = %U
path = /profils

Voici le fichier en Samba 2.xx

```
[global]  
netbios name = ServeurSMB  
workgroup = GUDUBULLE  
server string = Serveur Samba %v  
log file = /var/log/samba/log.%U  
username map = /etc/smbusers  
lm announce = yes  
lm interval = 5  
security = user  
socket options = TCP_NODELAY  
name resolve order = bcast wins hosts  
client code page = 850  
encrypt passwords = yes  
smb passwd file = /etc/smbpasswd  
unix password sync = yes  
passwd program = /usr/bin/passwd %u  
passwd chat = *New* %n\n *Re* %n\n *pa*  
os level = 255  
domain master = yes  
local master = yes  
preferred master = yes  
domain logons = yes  
wins support = yes  
logon script = %G.bat  
logon path = \\ServeurSMB\profils\%u  
logon drive = H:  
logon home = \\ServeurSMB\%U  
domain admin group = root administrateur  
  
[netlogon]  
path = /samba/netlogon  
locking = no  
writeable = no  
public = yes  
browseable = no
```

[admin]
browseable = yes
valid users = @admin
path = /samba/partages/admin
admin users = jesus

[comm]
browseable = no
valid users = @admin @comm
path = /samba/partages/comm
admin users = @comm

[info]
browseable = no
valid users = @admin @comm @info
path = /samba/partages/info
admin users = @info

[public]
path = /samba/partages/public
browseable = yes
valid users = @admin @comm @info
admin users = jesus
write list = jesus

[homes]
browseable = no
comment = Répertoire de %U
writable = yes

[Laser_Admin]
printable = yes
printer = lp1
print command = /usr/bin/lpr -r %s
read only = yes
printer driver = HP Laserjet 4 Plus
guest ok = no
valid users = @admin
comment = Imprimante Laser de la Direction

[Laser_Comm]
printable = yes
printer = lp2
print command = /usr/bin/lpr -r %s
read only = yes
printer driver = HP Laserjet 4 Plus
guest ok = no
valid users = @admin
comment = Imprimante Laser des commerciaux

netbios name = ServeurSMB

Nom netbios du serveur Samba, il s'appelle ici ServeurSMB, c'est par rapport à ce nom que seront faits les accès.

workgroup = GUDUBULLE

On définit le domaine du serveur, ici c'est GUDUBULLE

server string = Serveur Samba %v

On précise le commentaire lié au serveur qui sera affiché dans le voisinage réseau. %v est une variable de samba, indiquant sa version

log file = /var/log/samba/log.%U

Commande importante, elle permet de créer des fichiers qui sont la trace écrite de toutes les commandes qui ont pu être exécutées entre le serveur et le poste client. Remarquez la notation /var/log/samba/log.%U qui indique que les fichiers seront créés dans le répertoire /var/log/samba du serveur Linux, sous un nom qui sera log.nom_du_client_connecté

username map = /etc/smbusers

Sous Linux le nom des utilisateurs est limité à 15 caractères. Heureusement à l'aide de Samba, on peut créer une liste d'utilisateurs Windows qui correspondent à des utilisateurs Linux. Ce fichier est /etc/smbusers et il est de la forme suivante

```
#Unix_name = SMB_name1 SMB_name2 ...  
root = administrateur admin  
nobody= guest pcguest smbguest
```

lm announce = yes

Permet d'autoriser la diffusion des informations (voisinage réseau) sur le réseau. Par définition cette option est à *auto*. Ici on la fixe à *yes*, de cette manière la diffusion a toujours lieu.

lm interval = 5

On définit l'intervalle qui fixe le temps d'attente avant la prochaine diffusion, (par défaut 60 secondes).

security = user

voir chapitre précédent

socket options = TCP_NODELAY

Sans rentrer dans les détails des protocoles, on améliore la transmission des paquets entre le serveur et les clients. Les délais d'attente sont censés être moins élevés.

name resolve order = bcast wins hosts

On définit l'ordre de résolution des noms de machines. Via d'abord le broadcast (TCP), puis Wins et enfin le fichier /etc/hosts

client code page = 850

Pour indiquer les tables de caractères utilisés. Ici il s'agit des caractères européens (850)

encrypt passwords = yes

Commande qui précise que les mots de passe des utilisateurs sont enregistrés de manière cryptée, afin de sécuriser au mieux le serveur (on limite les trous de sécurité). Windows 2000 transmet les mots de passe sous forme cryptée. Si vous mettez cette option à *no*, les clients ne pourront pas se connecter au serveur.

smb passwd file = /etc/smbpasswd

Permet d'indiquer à Samba où se trouve le fichier contenant les mots de passe des utilisateurs, lors de l'authentification par le serveur Samba.

unix password sync = yes

Paramètre très pratique, permet de synchroniser les mots de passe Samba et les mots de passe Linux. Attention un utilisateur Linux qui modifie son mot de passe Linux, ne modifie pas automatiquement le mot de passe dans le fichier smbpasswd. La synchronisation n'a lieu que lorsque l'utilisateur modifie son mot de passe dans l'environnement Windows.

passwd program = /usr/bin/passwd %u

On indique où se trouve le programme de changement des mots de passe sur le serveur Linux. Cette commande est obligatoire lorsque l'on utilise la synchronisation des mots de passe.

passwd chat = *New* %n\n *Re* %n\n *pa*

Permet d'indiquer les entrées sorties qui sont testées lors de l'utilisation de la commande passwd entre le serveur Linux et le poste Windows.

Cette commande teste si les lignes affichées comportent les mots **New**, avant la fin de la ligne on place le nouveau mot de passe via la variable *%n* On re-confirme le mot de passe en testant la ligne **Re**, avant la fin de la ligne on place le

nouveau mot de passe, et si le changement a bien eu lieu, on teste la dernière ligne affichée à l'aide du mot `*pa*`

```
passwd jesus  
Changing password for user jesus  
New UNIX password:  
Retype new UNIX password:  
passwd: all authentication tokens updated successfully
```

os level = 255

voir chapitre précédent

domain master = yes

Permet de faire en sorte que Samba est un explorateur maître de domaine.

local master = yes

Permet à Samba de participer aux élections de l'explorateur de réseau

preferred master = yes

Permet de définir Samba comme explorateur maître préféré de son groupe de travail.

domain logons = yes

On autorise les clients Windows 2000 à se connecter sur le domaine.

wins support = yes

Activer le système WINS du serveur.

logon script = %G.bat

On indique le nom du script de démarrage ici nom_du_groupe.bat. Pour l'instant on ne précise pas où il se trouve.

logon path = \\ServeurSMB\profils\%u

On définit le chemin d'accès des répertoires des profils Windows 2000, contenant les dossiers et fichiers tels que Menu Démarrer, Voisinage réseau...

logon drive = H:

Définit le nom du lecteur réseau qui sera montée dans le poste de travail du client. Cette unité réseau contiendra le répertoire personnel de l'utilisateur qui est connecté.

logon home = \\ServeurSMB\%U

Définit le chemin d'accès réseau du répertoire personnel de l'utilisateur.

domain admin group = root

Définit la liste des utilisateurs autorisés à administrer le poste client Windows 2000.

3. Création des comptes utilisateurs sur le serveur

Avant de se lancer dans la configuration du fichier smb.conf il est nécessaire de créer les comptes des utilisateurs.

3.1. Création des comptes utilisateurs dans Linux

Sur le poste Linux, sous root, nous créons les 3 groupes (pour des raisons de compatibilité Linux/Samba, il est préférable de fixer le nombre de caractères d'un nom de groupe à 8):

```
groupadd admin
groupadd comm
groupadd info
```

Il est nécessaire tout d'abord de créer les répertoires qui regrouperont les groupes d'utilisateurs, toujours sous root :

```
mkdir samba
mkdir /samba/users
mkdir /samba/users/admin
mkdir /samba/users/comm
mkdir /samba/users/info
```

Ceux qui contiendront les partages

```
mkdir /samba/partages
mkdir /samba/partages/admin
mkdir /samba/partages/comm
mkdir /samba/partages/info
```

Ceux qui contiendront les partages

```
mkdir /samba/profils
mkdir /samba/profils/jesus
```

```
mkdir /samba/profils/jessica
mkdir /samba/profils/jean
mkdir /samba/profils/marc
mkdir /samba/profils/nordine
```

Et celui qui contiendra les logons scripts:

```
mkdir /samba/netlogon
```

Ensuite il ne reste plus qu'à créer les comptes utilisateurs Linux, à l'aide de la commande adduser

Pour le groupe admin :

```
adduser jesus -g admin -d /samba/users/admin/jesus -s /dev/false
adduser jessica -g admin -d /samba/users/admin/jessica -s /dev/false
```

Pour le groupe comm :

```
adduser jean -g comm -d /samba/users/comm/jean -s /dev/false
adduser marc -g comm -d /samba/users/comm/marc -s /dev/false
```

Pour le groupe info :

```
adduser nordine -g info -d /samba/users/info/nordine -s /dev/false
```

Remarques : L'option `-s /dev/false` empêche les utilisateurs de se connecter sous Linux; il ne pourront accéder au serveur qu'en passant par Samba.

Il existe un utilitaire sous Linux qui se nomme `userconf`, et qui permet d'éviter toutes ces commandes. De plus lorsque vous définissez un mot de passe Linux pour chaque utilisateur, `userconf` affecte le même mot de passe dans le fichier `smbpasswd`

3.2. Création des comptes utilisateurs dans Samba

Attention, les utilisateurs qui ont été définis sur le serveur Samba n'ont pour l'instant aucun mot de passe SAMBA. Il faut se placer dans le répertoire `/etc` et taper la commande suivante :

```
cat passwd | mksmbpasswd.sh > smbpasswd
```

Vous devriez vous retrouver avec un fichier `smbpasswd` qui est la forme suivante :

```
#
# SMB password file.
#
root:0:XXXXXXXXXXXXXXXXXXXXXXXXXX:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:[U]:LCT-0000000:root
```

On supprime toutes les lignes correspondant à un utilisateur Linux/Unix qui n'utilisera pas Samba. Pour affecter un mot de passe SAMBA à un utilisateur, on utilise la commande :

```
smbpasswd jesus
New SMB password: *****
Retype new SMB password: *****
Password changed for user jesus.
```

3.3. Création des comptes machines dans Samba

Lorsque qu'une machine de type Windows 2000 doit rejoindre un domaine géré par SAMBA, il faut que cette machine soit définie dans le fichier `/etc/samba/smbpasswd`. Or pour que la machine soit définie dans ce fichier, il faut impérativement qu'elle soit d'abord inscrite dans le fichier `/etc/passwd`

Donc il faut impérativement connaître le nom de chaque client Windows 2000 qui appartiendra au domaine. Pour le poste de jean par exemple la manipulation va être la suivante :

- Ajouter la machine dans le fichier /etc/passwd :

Attention : la machine se nomme dans notre exemple PCJEAN il va falloir utiliser la commande suivante :

```
groupadd machines  
adduser pcjean$ -g machines -s /dev/false -d /dev/null
```

Il s'agit bien d'un \$ à la fin du nom de la machine pour la différencier d'un utilisateur

- Ajouter la machine dans le fichier /etc/samba/smbpasswd :

```
smbpasswd -m -a pcw2000$
```

il s'agit bien d'un \$ à la fin du nom de la machine pour la différencier d'un utilisateur

3.4. Le compte root

Lorsque vous allez configurer le client Windows 2000 pour joindre le domaine GUDUBULLE, le client vous demandera une identification. Cette identification est celle du gestionnaire du domaine, donc de SAMBA.

La seule personne qui soit l'administrateur du serveur sous Linux, c'est bien évidemment root. Il faut donc que root ait un mot de passe défini.

Attention, pour des raisons évidentes de sécurité, n'affectez pas un mot de passe samba à l'utilisateur root qui soit identique à celui qui est utilisé pour administrer le serveur linux.

```
smbpasswd -a root  
New SMB password:*****  
Retype new SMB password:*****  
Password changed for user root
```

Enfin, nos utilisateurs et notre machine, existent sur le serveur Samba, il nous faut lancer les daemons Samba, à l'aide de la commande : service smb start

4. Configuration des postes Windows2000

Cette configuration est très simple il suffit d'avoir une adresse IP dans la bonne plage d'adresse et ensuite de changer le domaine en GUDUBULLE. Lors de cette manipulation un nom d'utilisateur et un mot de passe sont demandés pour entrer dans le domaine. Il s'agit de root (vous pouvez utiliser administrateur par exemple si vous l'avez défini au préalable dans le fichier smbusers) et de son mot de passe SAMBA (attention il est préférable qu'il soit différent du mot de passe LINUX). Après un redémarrage tout devrait fonctionner.

N'oubliez pas l'adresse IP du serveur SAMBA dans l'onglet WINS des propriétés de TCP/IP.

Si vous avez une machine XP il faut modifier la base de registre.

Aller a : - HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ Netlogon \ Parameters et modifier la clé suivante : requiresignorseal.

Par défaut elle a comme valeur 1 mettez a la place un 0 (zéro)
Fermer la base de registre et relancer le poste XP.

Voici aussi une autre solution de fichier REG

```
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Netlogon\Parameters]
"requiresignorseal"=dword:00000000
"requirestrongkey"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\Netlogon\Parameters]
"requiresignorseal"=dword:00000000
"requirestrongkey"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
]
"requiresignorseal"=dword:00000000
"requirestrongkey"=dword:00000000
```

5. Application des stratégies de sécurité

5.1. Éléments requis

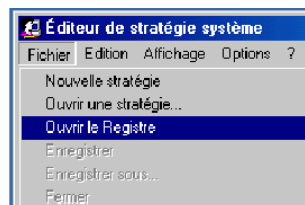
Pour que nos stratégies soient valables sur les clients Windows 2000, il faut récupérer à partir d'un Windows 2000 Serveur l'utilitaire **poledit** ainsi que les deux fichiers de modèles d'administration : **common.adm** et **winnt.adm**

Les deux modèles se trouvent dans le répertoire : **C:\WINNT\INF**

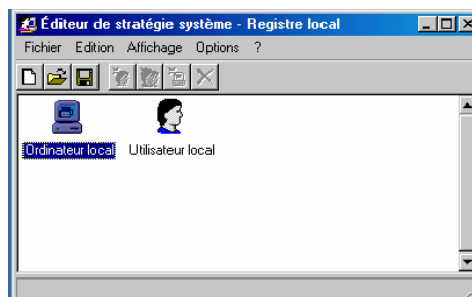
Ensuite il faut installer poledit sur un client Windows 2000 Pro membre du domaine, il suffit donc de copier l'application ainsi que les deux fichiers **.adm** sur le client dans le répertoire **C:\WINNT\INF**. Il faut impérativement effectuer l'installation sous le compte local **Administrateur** du client.

5.2. Utilisation de POLEDIT

Une fois que tout est installé, on lance **poledit** puis on clique sur **Fichier/Ouvrir le Registre** comme ceci:

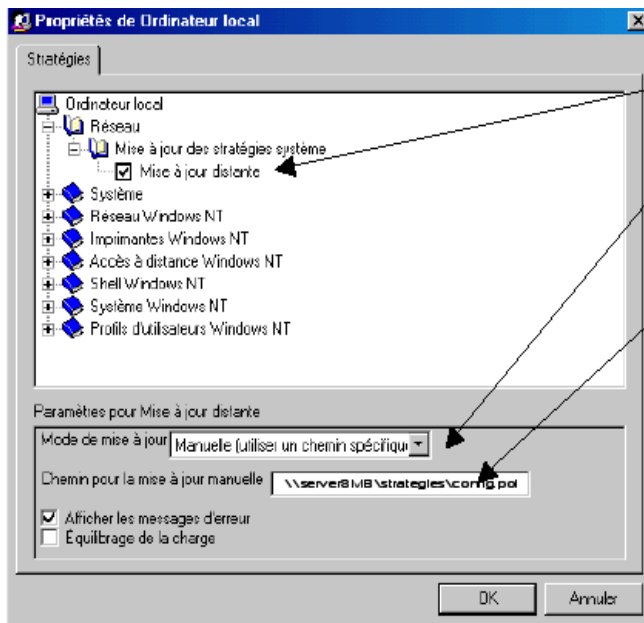


De cette manière, on accèdera au registre du client. On se retrouve avec le même environnement que Windows NT.



Le principe reste relativement simple, on va demander au client Windows 2000 d'aller télécharger la stratégie depuis le serveur Samba. Pour cela il suffit de double cliquer l'icône **Ordinateur Local** puis de configurer les options comme ceci :

Bien vérifier que cette option est **cochée**.



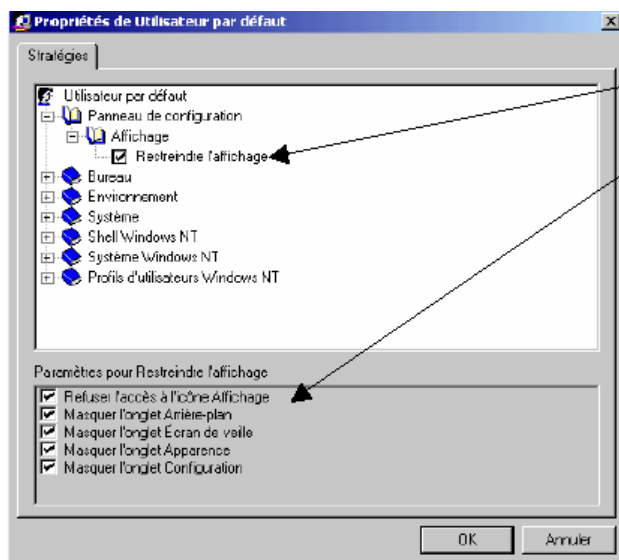
Le but de la manipulation est de créer des stratégies en fonctions des groupes d'utilisateurs. Pour cela nous allons créer deux fichiers **config.pol** qui contiennent deux politiques distinctes.

Admettons que les groupes **comm** et **admin** ait le droit de régler le panneau de configuration **Affichage** tandis que le groupe **info** ne l'ait pas.

Pour cela, il suffit en tant qu'**administrateur** local du poste Windows 2000 d'ouvrir **poedit** puis de créer une nouvelle stratégie (Fichier/Nouvelle Stratégie)

Dans la rubrique ordinateur par défaut, on sélectionne les mêmes options que précédemment (**Mise à jour des stratégies distantes** et chemin réseau [\\serverSMB\strategies\config.pol](#)) puis on valide par **OK**.

Une fois que c'est fait on clique sur **Utilisateur par défaut** de manière à sélectionner les options de stratégies suivantes :



On restreint au maximum les possibilités de l'utilisateur

Il n'y a plus qu'à enregistrer les modifications sous **lockscreen.pol**.

On crée une autre stratégie dans laquelle on décochera toutes les options liées à l'affichage que l'on appellera **nolockscreen.pol** :

Maintenant on va s'intéresser au serveur Samba.

5.3. Configuration de SAMBA

Du côté de Samba on va créer deux partages. Le premier contenant les stratégies en fonction du groupe de l'utilisateur :

```
[strategies]  
path = /samba/strategies/%g  
browseable = yes  
writeable = yes
```

Le second sera un partage d'administration pour l'utilisateur root qui lui permettra d'accéder à tous les partages contenus dans /samba

```
[tout]  
path = /samba  
valid users = root  
writeable = yes
```

Une fois notre serveur correctement configuré, il ne vous reste plus qu'à se connecter en tant que **root** sur le client 2000 et à copier **nolockscreen.pol** dans les répertoires **/samba/strategies/admin** et **/samba/strategies/comm** et le fichier **lockscreen.pol** dans **/samba/strategies/info** en les renommant en **config.pol**.

Samba en tant que membre d'un domaine Windows 2000

1. Introduction

Si dans votre réseau existe déjà un serveur NT, configuré comme Contrôleur de Domaine (PDC - Primary Domain Controller), vous pouvez décider de configurer votre serveur Samba pour qu'il fasse partie du domaine contrôlé par ce serveur NT. Alors pour authentifier un utilisateur se connectant à lui, le serveur Samba demandera au Contrôleur de Domaine de vérifier pour lui le nom de l'utilisateur et du mot de passe reçu.

Il y a deux valeurs pour le paramètre **security** qui peuvent être utilisées pour que Samba utilise un autre PDC en tant que serveur d'authentification. La première valeur est **server** (security=server). Historiquement, il s'agit de la première implémentation de l'utilisation d'un "serveur de mots de passe". Lorsqu'il est mis à cette valeur, le serveur Samba qui reçoit un nom d'utilisateur et un mot de passe d'un client, utilisera ces deux valeurs pour effectuer une connexion vers le serveur d'authentification renseigné dans son fichier de configuration. Si la connexion est acceptée, alors Samba lui-même autorisera la connexion venant du client et allant vers lui. Cette méthode d'authentification a le désavantage de consommer une licence sur le serveur. De plus, la connexion entre Samba et le serveur d'authentification restera ouverte aussi longtemps que le client sera connecté à Samba.

La deuxième valeur qui peut être utilisée, depuis la version 2.0.0, est **domain**. Avec cette valeur, Samba sera réellement un membre de domaine et participera au domaine comme tout autre machine NT peut le faire. Quand le serveur Samba aura besoin de valider un utilisateur et un mot de passe, il se connectera au PDC (le serveur d'authentification) pour lui passer l'authentification exactement de la même manière qu'une machine NT est capable de le faire. Cela signifie qu'aucune connexion ne doit rester ouverte plus longtemps que le temps nécessaire à la validation du nom de l'utilisateur et de son mot de passe.

Il est recommandé d'utiliser **security=domain** si vous avez la version 2.0.x de Samba ou supérieure, vu qu'elle permet de faire des économies de ressources (licences, ...) sur le serveur faisant l'authentification.

Cela dit, il devient difficile de gérer un nombre élevé d'utilisateurs et de les créer dans Samba chaque fois qu'ils sont créés dans Windows. On va donc, pour se simplifier la vie, utiliser **Winbind**. Winbind est un outil d'Unix/Linux qui permet l'authentification via le contrôleur de domaine d'un domaine Windows (NT/2000/2003) en fait il interroge régulièrement la base de données utilisateurs du PDC et modifie les fichiers passwd et smbpasswd du serveur Samba en fonction des changements. L'avantage: on ne gère qu'une seule base de données utilisateurs celle du PDC Windows 2000.

2. Configuration de winbind

Je ne traiterai pas ici l'installation de winbind puisqu'il est fourni avec la plupart des distributions actuelles et que de nombreuses aides existent partout sur le net.

Pour commencer, il faut spécifier à Unix/Linux que l'authentification peut se faire avec Winbind. Pour cela, il est nécessaire de modifier quelques fichiers. Le premier est le fichier **/etc/nsswitch.conf**. Il faut s'assurer que les lignes commençant par passwd: et group: contiennent le paramètre Winbind comme ceci

```
passwd: files winbind
shadow: files
group: files winbind
```

Cela pour permettre à Unix/Linux d'authentifier les utilisateurs grâce à /etc/passwd (paramètre files) et grâce à Winbind (paramètre Winbind) et même chose pour les groupes d'utilisateurs.

Ensuite, on modifiera les fichiers de configuration du module PAM (Pluggable Authentication Modules) comme ceci :

```
##%PAM-1.0
auth required /lib/security/pam_securetty.so
auth required /lib/security/pam_nologin.so
auth sufficient /lib/security/pam_winbind.so
auth required /lib/security/pam_pwdb.so use_first_pass shadow nullok
account required /lib/security/pam_winbind.so
```

Le fichier /etc/pam.d/authconfig

```
##%PAM-1.0
auth required /lib/security/pam_winbind.so
auth required /lib/security/pam_pwdb.so nullok shadow
account required /lib/security/pam_winbind.so
account required /lib/security/pam_pwdb.so
session required pam_stack.so service=system-auth
password required pam_stack.so service=system-auth
```

Le fichier /etc/pam.d/samba

```
##%PAM-1.0
auth required /lib/security/pam_securetty.so
auth sufficient /lib/security/pam_winbind.so
auth sufficient /lib/security/pam_unix.so use_first_pass
auth required /lib/security/pam_stack.so service=system-auth
auth required /lib/security/pam_nologin.so
account sufficient /lib/security/pam_stack.so service=system-auth
account sufficient /lib/security/pam_winbind.so
password required /lib/security/pam_stack.so service=system-auth
```

Le fichier /etc/pam.d/login

De plus comme nous utilisons Redhat

```
##%PAM-1.0
session required/lib/security/pam_permit.so
session optional/lib/security/pam_xauth.so
session optional/lib/security/pam_timestamp.so
account required /lib/security/pam_winbind.so
account required /lib/security/pam_pwdb.so
```

Le fichier /etc/pam.d/redhat-config-network

Cela étant fait, il faut vérifier l'existence du lien libnss_winbind.so.2 dans le cas contraire on le créera en tapant :

```
In libnss_winbind.so libnss_winbind.so.2
```

A ce moment toute la configuration liée à l'authentification par Winbind est faite. Pour que les changements s'appliquent sans redémarrer la machine on tapera :

```
/sbin/ldconfig -v | grep winbind
```

3. Configuration de Samba

A ce moment de la manipulation, Samba n'est **pas** démarré. Avant de commencer l'écriture d'un fichier smb.conf, on va créer sur le PDC Windows 2000 le compte de la machine Samba.

On peut donc maintenant passer au fichier de configuration de Samba à proprement parler.

```
[global]
netbios name = SMBTEST
server string = Samba Version 3
workgroup = <LE NOM NETBIOS DE MON DOMAINE 2000>
log file = /var/log/samba/%m.log
max log size = 100
security = domain
password server = *
encrypt passwords = yes
smb passwd file = /usr/bin/smbpasswd
unix password sync = yes
passwd program = /usr/bin/passwd
passwd chat = "New*password* %n\n *Retype*new*password* %n\n *passwd:*all*authentication*tokens*updated*successfully*"
add user script = /usr/sbin/useradd %u -g smbusers
delete user script = /usr/sbin/userdel %u
allow trusted domains = yes
nt acl support = yes
winbind separator = +
winbind cache time = 10
template shell = /bin/bash
template homedir = /home/%D/%U
winbind uid = 10000-20000
winbind gid = 10000-20000
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
local master = no
os level = 65
domain master = no
preferred master = no
wins server = <LE SERVEUR WINS DE MON DOMAINE>
preserve case = yes
case sensitive = no
root preexec = /etc/samba/createhomedir %U %D

[homes]
comment = Répertoire de base
browseable = no
writable = yes
create mode = 0664
directory mode = 0775
```

security = domain

Nom NetBios du serveur Samba

password server = *

Liste des machines qui peuvent être utilisées pour demander l'authentification d'un utilisateur. Ça doit être une liste de machine (par exemple : un PDC 2000, un BDC 2000, un autre serveur Samba en mode de sécurité utilisateur, ...). Les valeurs entrées ici sont les noms NetBIOS des machines à utiliser (cela peut aussi fonctionner avec les adresses IP). Les noms seront résolus en utilisant les méthodes standards : WINS, fichier lmhosts, DNS ou broadcast comme défini dans le paramètre name resolve order (voir chapitre précédent). Au lieu de donner le nom du contrôleur de domaine, vous pouvez utiliser une astérisque (*). Cette valeur spéciale demande à Samba de chercher lui-même le contrôleur du domaine et son nom de la même façon qu'une machine Windows le fait.

nt acl support = yes

Le serveur Samba supportera les access list (droits d'accès) de type Windows

winbind separator = +

"+" sera le séparateur utilisé dans Samba et Winbind pour séparer le nom de domaine du nom d'utilisateur ou du nom de groupe. Par exemple l'utilisateur toto du groupe truc sera connu par Samba comme truc+toto.

```
template shell = /bin/bash
```

Nom du shell attribué lors de la création d'un nouvel utilisateur

```
template homedir = /home/%D/%U
```

Lors de la création d'un nouvel utilisateur celui-ci aura pour répertoire de base le répertoire /home/<domaine>/<utilisateur>

```
winbind uid = 10000-20000
```

Les utilisateurs windows auront un UID dans cette fourchette

```
winbind gid = 10000-20000
```

Les groupes windows auront un GID dans cette fourchette

```
root preexec = /etc/samba/createhomedir %U %D
```

A chaque connexion d'un utilisateur sur le serveur Samba on va exécuter le script /etc/samba/createhomedir. J'ai créé ce script pour tester si le répertoire de base de l'utilisateur en question existe si non cela veut dire que c'est la première fois qu'il se connecte et donc nous sommes obligés de le créer. Voici le code de ce script :

```
USER=$1
DOMAIN=$2
HOME=/home/${DOMAIN}/${USER}
LOG=/etc/samba/adduser.log

if [ -d ${HOME} ]; then
echo `date` le repertoire de ${USER} existe deja. >> ${LOG}
exit 0
fi

mkdir ${HOME}
chmod 700 ${HOME}
chgrp smbusers ${HOME}
chown ${DOMAIN}.${USER} ${HOME}
echo `date` creation du repertoire de ${USER} >> ${LOG}
```

La seconde étape se déroule sur le serveur Samba lui-même. Il faut exécuter la commande suivante tout en ayant pris soin d'arrêter les daemons Samba:

```
smbpasswd -j <DOMAINE2000> -r <PDC2000> -U <administrateur2000>
```

où <DOMAINE2000> est le nom du domaine, <PDC2000> le nom NetBIOS de votre PDC et <administrateur2000> le nom de l'utilisateur administrateur du domaine. On doit alors introduire le mot de passe de l'administrateur et le compte machine du serveur Samba est alors automatiquement créé sur le contrôleur de domaine. Le mot de passe de la machine est stocké un fichier appelé secrets.tdb, le format de base de données utilisé par Samba depuis la version 2.2.0 pour stocker des paramètres importants.

Une fois que ces étapes ont été suivies, votre serveur Samba est prêt à opérer. Il faut juste créer les partages comme d'habitude.

4. Démarrage de Samba

Pour cette configuration il faut **absolument** démarrer les daemons dans l'ordre suivant :

- 1- Samba
- 2- Winbind
- 3- Xinetd

Pour s'assurer que le daemons winbind n'est pas démarré il suffit de taper la commande :

```
ps -ae |grep winbind
```

Une fois le processus "tué" (avec la commande kill -9 <N° du PID>), on lance

Samba :

service samba start

Puis winbind :

/usr/sbin/winbindd

Et enfin xinetd :

service xinetd restart

Pour s'assurer que l'intégration a réussi il suffit de taper :

getent passwd

Le fichier passwd devrait s'afficher avec tous les utilisateurs Windows en fin de fichier.