

# **Samba**

Ivan Kurzweg

26 juin 2007

**Samba**  
by Ivan Kurzweg

Copyright © 2002 - 2006 Ivan Kurzweg

Permission to use, copy, modify, and distribute this documentation for any purpose with or without fee is here by granted, provided that the above copyright notice and this permission notice appear in all copies.

## Table des matières

<b>1</b>	<b>Présentation de Samba</b>	<b>3</b>
1.1	Options d'installation sur FreeBSD	3
1.2	Démons de samba	4
1.3	Outils et utilitaires de la distribution Samba	5
1.3.1	findsmb	5
1.3.2	nmblookup	5
1.3.3	pdbedit	5
1.3.4	smbtree	6
1.3.5	smbcacls	6
1.3.6	smbclient	6
1.3.7	smbcontrol	7
1.3.8	smbgroupedit	7
1.3.9	smbmount	7
1.3.10	smbpasswd	7
1.3.11	smbstatus	7
1.3.12	testparm	7
<b>2</b>	<b>Type de serveurs Samba</b>	<b>8</b>
2.1	Serveur de fichiers	8
2.1.1	Mode anonyme en lecture seule	8
2.1.2	Mode anonyme en lecture / écriture	8
2.1.3	Mode lecture / écriture sécurisé	9
2.2	Contrôleur de domaine	9
2.3	Serveur d'impression	10
<b>3</b>	<b>Configuration de Samba</b>	<b>11</b>
3.1	Le fichier de <code>smb.conf</code>	11
3.1.1	La section <code>global</code>	11
3.1.2	Les partages	12
3.2	La gestion des comptes	13
3.2.1	Gestion des utilisateurs	13
3.2.2	Gestion des comptes dans un domaine	13
3.2.2.1	Avantages d'un domaine	13
3.2.2.2	Ajout d'un poste au domaine	13
3.2.2.3	Mappage des comptes Windows avec les comptes Unix	14
<b>4</b>	<b>Exercices</b>	<b>14</b>
4.1	Concepts, réflexions, installation	14
4.2	Samba : "simple serveur de fichier"	14
4.3	Samba : contrôleur de domaine	15
4.4	Samba et Windows : utilisation avancée	15

### Résumé

Samba est une implémentation Open Source du protocole Server Message Block (SMB). Il permet l'interaction sur un réseau de Microsoft™ Windows, Linux, UNIX et d'autres systèmes d'exploitation, permettant ainsi l'accès à des fichiers basés sur Windows et à des partages d'imprimantes. L'utilisation de SMB par Samba lui permet d'apparaître comme un serveur Windows aux clients Windows. La documentation officielle de Samba est disponible [ICI](#) en local, pour la réalisation des exercices et des compléments d'informations.

### Résumé

Samba est une implémentation Open Source du protocole Server Message Block (SMB). Il permet l'interaction sur un réseau de Microsoft™ Windows, Linux, UNIX et d'autres systèmes d'exploitation, permettant ainsi l'accès à des fichiers basés sur Windows et à des partages d'imprimantes. L'utilisation de SMB par Samba lui permet d'apparaître comme un serveur Windows aux clients Windows. La documentation officielle de Samba est disponible [ICI](#) en local, pour la réalisation des exercices et des compléments d'informations.

## 1 Présentation de Samba

La version 3 de Samba, a incorporé de nombreuses améliorations par rapport aux versions précédentes, y compris :

- La possibilité de faire partie d'un domaine Active Directory au moyen de LDAP et Kerberos
- La prise en charge intégrée de Unicode pour l'internationalisation
- La prise en charge de connexions client Microsoft™ Windows XP Professional aux serveurs Samba sans devoir toucher à la base de registre local

Samba a largement participé à l'intégration de systèmes Unix dans des environnements Microsoft™, en proposant en particulier les fonctionnalités suivantes :

- Mettre des arborescences de répertoires et des imprimantes à la disposition de clients Linux, UNIX et Windows
- Aider lors de la navigation du réseau (avec ou sans NetBIOS)
- Authentifier les connexions de domaines Windows
- Fournir la résolution du serveur de noms Windows Internet Name Service (WINS)
- Agir en tant que contrôleur principal de domaine (ou PDC, de l'anglais Primary Domain Controller) de type Windows NT
- Agir en tant que Contrôleur de Domaine Secondaire (ou BDC, de l'anglais Backup Domain Controller) pour un contrôleur principal (PDC) basé sur Samba
- Agir comme un serveur *membre* du domaine Active Directory
- Joindre un PDC Windows NT/2000/2003

Cependant, et en attendant sa version 4 qui a nécessité plus de 4 ans de développement, Samba est pour le moment limitée, en particulier pour ces tâches :

- Agir comme un BDC pour un PDC Windows (et vice versa)
- Agir comme le contrôleur d'un domaine Active Directory

### 1.1 Options d'installation sur FreeBSD

L'installation de Samba via les logiciels portés de Samba propose un certain nombre d'options de compilation, permettant d'ajouter/enlever des fonctionnalités en fonction de chaque environnement et besoin. Ces options peuvent varier suivant les versions de Samba :

- LDAP With LDAP support
- ADS With Active Directory support
- CUPS With CUPS printing support
- WINBIND With WinBIND support
- ACL\_SUPPORT With ACL support
- SYSLOG With Syslog support
- QUOTAS With Quota support
- UTMP With UTMP support
- MSDFS With MSDFS support
- SAM\_XML With XML smbpasswd backend
- SAM\_MYSQL With MySQL smbpasswd backend
- SAM\_PGSQL With PostgreSQL smbpasswd backend
- SAM\_OLD\_LDAP With Samba2.x LDAP smbpasswd backend
- PAM\_SMBPASS With SMB PAM module
- POPT With installed POPT library

Le script `/usr/local/etc/rc.d/samba` et le fichier `/usr/local/etc/smb.conf.sample` sont créés lors de la compilation. Le script permet de contrôler les démons Samba, et le fichier propose une configuration de Samba, à modifier bien sûr. Il est à noter que sous FreeBSD, il est nécessaire d'autoriser spécifiquement le démarrage de Samba dans le fichier `rc.conf` pour utiliser ces scripts.

```
arrakis# /usr/local/etc/rc.d/samba stop
Stopping smbd.
Stopping nmbd.
arrakis# /usr/local/etc/rc.d/samba start
Removing stale Samba tdb files: ..... done
Starting nmbd.
Starting smbd.
arrakis# /usr/local/etc/rc.d/samba restart
Performing sanity check on Samba configuration: OK
```

```
Stopping smbd.
Stopping nmbd.
Removing stale Samba tdb files: ..... done
Starting nmbd.
Starting smbd.
```

```
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options (perhaps too
# many!) most of which are not shown in this example
#
# For a step to step guide on installing, configuring and using samba,
# read the Samba-HOWTO-Collection. This may be obtained from:
# http://www.samba.org/samba/docs/Samba-HOWTO-Collection.pdf
#
# Many working examples of smb.conf files can be found in the
# Samba-Guide which is generated daily and can be downloaded from:
# http://www.samba.org/samba/docs/Samba-Guide.pdf
#
# Any line which starts with a ; (semi-colon) or a # (hash)
# is a comment and is ignored. In this example we will use a #
# for commentry and a ; for parts of the config file that you
# may wish to enable
#
# NOTE: Whenever you modify this file you should run the command "testparm"
# to check that you have not made any basic syntactic errors.
#
#===== Global Settings =====
[global]

# workgroup = NT-Domain-Name or Workgroup-Name, eg: MIDEARTH
# workgroup = MYGROUP

# server string is the equivalent of the NT Description field
# server string = Samba Server

# Security mode. Defines in which mode Samba will operate. Possible
# values are share, user, server, domain and ads. Most people will want
# user level security. See the Samba-HOWTO-Collection for details.
# security = user
....
```

Enfin, quelques utilisateurs sont fournis avec samba, dont une partie est décrite dans les paragraphes suivants.

## 1.2 Démons de samba

Samba est composé de trois démons (smbd, nmbd et winbindd). Deux services (smb et windbind) contrôlent la manière selon laquelle les démons sont démarrés et arrêtés et ainsi que d'autres fonctionnalités en relation avec les services.

1. **smbd** : Le démon `smbd` fournit des services de partage de fichiers et d'impression aux clients Windows. En outre, il est responsable de l'authentification des utilisateurs, du verrouillage des ressources et du partage des données par le biais du protocole SMB. Les ports par défaut sur lesquels le serveur est à l'écoute de tout trafic SMB sont les ports TCP 139 et 445. Le démon `smbd` est contrôlé par le service `smb`
2. **nmbd** : Le démon serveur `nmbd` comprend et répond à toutes les requêtes de service de nom NetBIOS telles que celles produites par SMB/CIFS dans des systèmes basés sur Windows. Parmi ces derniers figurent les clients Windows 95/98/ME, Windows NT, Windows 2000, Windows XP et LanManager. Ce démon joue également un rôle au niveau des protocoles de navigation qui constituent l'affichage du voisinage réseau (*Network Neighborhood*) de Windows. Le port par défaut sur

lequel le serveur attend du trafic NMB est le port UDP 137. Le démon `nmbd` est contrôlé par le service `smb`.

3. `Winbind` : Le service `winbind` effectue la résolution entre les informations relatives aux utilisateurs et aux groupes sur un serveur Windows NT et les rend utilisables par des plates-formes UNIX. Cette opération est possible grâce à l'utilisation d'appels RPC de Microsoft™, du système PAM (*Pluggable Authentication Module*, ou module d'authentification enfichable) et du NSS (*Name Service Switch*). Ceci permet aux utilisateurs de domaines Windows NT d'apparaître comme des utilisateurs UNIX sur une machine UNIX. Bien qu'intégré à la distribution Samba, le service `winbind` est contrôlé séparément du service `smb`. Le démon `winbindd` est contrôlé par le service `winbind` et il n'est pas nécessaire que le service `smb` soit lancé pour que le démon tourne.

## 1.3 Outils et utilitaires de la distribution Samba

### 1.3.1 `findsmb`

Le programme `findsmb subnet_broadcast_address` est un script Perl qui permet de recueillir des informations sur les systèmes compatibles avec SMB sur un sous-réseau particulier. Si aucun sous-réseau n'est spécifié, le sous-réseau local est utilisé. Parmi les éléments spécifiés figurent l'adresse IP, le nom, groupe de travail ou nom de domaine NetBIOS, le système d'exploitation et la version. L'exemple suivant montre la sortie de la commande `findsmb` exécutée en tant qu'un utilisateur valide du système :

```
ikare@ix:~$ findsmb
                                     *=DMB
                                     +=LMB
IP ADDR          NETBIOS NAME      WORKGROUP/OS/VERSION
-----
172.17.4.1       POSTE401      [      BAGGINS      ]
172.17.7.2       SRV2          *[ASR] [Windows Server 2003 R2 3790 Service Pack 1] ↔
               [Windows Server 2003 R2 5.2]
172.17.7.3       SRV3          [ASR] [Windows Server 2003 3790 Service Pack 1] [ ↔
               Windows Server 2003 5.2]
172.17.7.5       SRV5          *[CONCEPT] [Windows Server 2003 R2 3790 Service ↔
               Pack 1] [Windows Server 2003 R2 5.2]
172.17.7.9       POSTE703      +[HERMES] [Windows 5.1] [Windows 2000 LAN Manager]
172.17.3.10      POSTE310      [BAGGINS] [Windows 5.0] [Windows 2000 LAN Manager]
172.17.3.14      POSTE314      [BAGGINS] [Windows 5.0] [Windows 2000 LAN Manager]
172.17.7.20      POSTE704      [HERMES] [Windows 5.1] [Windows 2000 LAN Manager]
172.17.6.20      POSTE816      [      BAGGINS      ]
```

### 1.3.2 `nmblookup`

Le programme `nmblookup options netbios_name` effectue la résolution des noms NetBIOS en adresse IP. Le programme diffuse sa demande sur le sous-réseau local jusqu'à ce que la machine cible réponde.

```
ikare@ix:~$ nmblookup SRV2
querying SRV2 on 172.17.255.255
172.17.7.2 SRV2<00>
192.168.31.1 SRV2<00>
192.168.219.1 SRV2<00>
```

### 1.3.3 `pdbedit`

Le programme `pdbedit` gère les comptes présents dans la base de données de SAM. Tous les *backends* sont pris en charge, y compris `smbpasswd`, LDAP, NIS+ et la bibliothèque de base de données `tdb`.

```
pdbedit -v -L ikare
Unix username:      ikare
NT username:
Account Flags:      [U      ]
```

```

User SID:                S-1-5-21-761572816-94600713-4071525793-5646
Primary Group SID:      S-1-5-21-761572816-94600713-4071525793-513
Full Name:
Home Directory:         \\ix\ikare
HomeDir Drive:
Logon Script:
Profile Path:           \\ix\ikare\profile
Domain:                 IX
Account desc:
Workstations:
Munged dial:
Logon time:             0
Logoff time:            mar, 19 jan 2038 07:14:07 RET
Kickoff time:           mar, 19 jan 2038 07:14:07 RET
Password last set:     0
Password can change:   0
Password must change:  mar, 19 jan 2038 07:14:07 RET
Last bad password      : 0
Bad password count     : 0
Logon hours             : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

```

### 1.3.4 smbtree

Le programme **smbtree** permet d'obtenir l'équivalent du voisinage réseau sous Windows, en mode texte. Il affiche l'ensemble des ressources SMB, en donnant les noms et les partages de chaque poste. Un extrait de **smbtree** sur le réseau de N3 :

```

WORKGROUP
  \\POSTE704
  \\KONIFEXXX_PC
TOTO
  \\REDREUNION
    \\REDREUNION\jeux
    \\REDREUNION\Lettre et CV
    \\REDREUNION\Mes vid~~os
    \\REDREUNION\IPC$          IPC distant
SA-AUTREMENT
  \\PC-NELLO
    \\PC-NELLO\C$              Partage par défaut
    \\PC-NELLO\ADMIN$         Administration à~ distance
    \\PC-NELLO\E
    \\PC-NELLO\Counter-Strike Source
    \\PC-NELLO\Téléchargements
    \\PC-NELLO\x86_policy.X
    \\PC-NELLO\Documents
    \\PC-NELLO\print$         Pilotes d'imprimantes
    \\PC-NELLO\D$             Partage par défaut
    \\PC-NELLO\IPC$          IPC distant

```

### 1.3.5 smbcacls

Le programme **smbcacls //server/share filename options** modifie les ACL de Windows dans les fichiers et répertoires partagés par le serveur Samba.

### 1.3.6 smbclient

Le programme **smbclient //server/share password options** est un client UNIX souple qui fournit des fonctionnalités semblables à **ftp**.

### 1.3.7 smbcontrol

Le programme **smbcontrol options destination messagetype parameters** envoie des messages de contrôle aux démons `smbd` ou `nmbd` en cours d'exécution. L'exécution de **smbcontrol -i** lance la commande de manière interactive jusqu'à ce qu'une ligne blanche ou que la lettre 'q' soit saisie.

### 1.3.8 smbgroupedit

Le programme **smbgroupedit options** établit la correspondance entre les groupes Linux et les groupes Windows. Il permet également à un groupe Linux d'être un groupe de domaine.

### 1.3.9 smbmount

Le programme **smbmount //server/share mount\_point -o options** utilise le programme de bas niveau **smbmnt** pour monter un système de fichiers `smbfs` (partage Samba). La commande **mount -t smbfs** est également valide.

### 1.3.10 smbpasswd

Le programme **smbpasswd options username password** gère les mots de passe cryptés. Ce programme peut être exécuté aussi bien par un super-utilisateur pour changer le mot de passe d'un utilisateur quelconque que par un utilisateur ordinaire pour changer son propre mot de passe Samba.

### 1.3.11 smbstatus

Le programme **smbstatus options** affiche le statut des connexions actuelles à un serveur Samba.

### 1.3.12 testparm

Le programme **testparm options filename hostname IP\_address** vérifie la syntaxe du fichier `smb.conf`. Si votre fichier `smb.conf` se trouve dans l'emplacement par défaut (`/etc/samba/smb.conf` pour Linux, `/usr/local/etc/samba/smb.conf`), il n'est pas nécessaire de préciser l'emplacement. La spécification du nom d'hôte et de l'adresse IP pour le programme **testparm** permet de vérifier que les fichiers `hosts.allow` et `host.deny` sont bien configurés correctement. Le programme **testparm** affiche également un résumé de vos fichiers `smb.conf` et le rôle du serveur (autonome, domaine, etc.) après avoir effectué les tests. Ce programme est utile lors du débogage étant donné qu'il exclut les commentaires et fournit les informations de manière concise pour des administrateurs expérimentés.

```
testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[printers]"
Processing section "[print$]"
Loaded services file OK.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions

[global]
    workgroup = MSHOME
    server string = %h server (Samba, Ubuntu)
    obey pam restrictions = Yes
    passdb backend = tdbsam
    passwd program = /usr/bin/passwd %u
    passwd chat = *Enter\snew\sUNIX\spassword:* %n\n *Retype\snew\sUNIX\ ←
        spassword:* %n\n *password\supdated\ssuccessfully* .
    syslog = 0
    log file = /var/log/samba/log.%m
    max log size = 1000
    dns proxy = No
    panic action = /usr/share/samba/panic-action %d
    invalid users = root
```

```
[printers]
    comment = All Printers
    path = /var/spool/samba
    create mask = 0700
    printable = Yes
    browseable = No

[print$]
    comment = Printer Drivers
    path = /var/lib/samba/printers
```

## 2 Type de serveurs Samba

La plus grande partie de la configuration de Samba passe par la modification du fichier `/etc/samba/smb.conf` (`/usr/local/etc/samba/smb.conf` sur FreeBSD). Elle regroupe plusieurs sections, permettant de définir le mode de fonctionnement du serveur, les partages réalisés, et les informations relatives à la gestion du réseau.

On peut regrouper les différents rôles d'un serveur Samba au sein d'un réseau en 3 groupes : serveur de fichier, contrôleur de domaine et serveur d'impression.

### 2.1 Serveur de fichiers

Par abus de langage, nous allons désigner par "serveur de fichier" une configuration où Samba est placé en tant que serveur d'un groupe de travail, ou membre d'un groupe de travail. Un serveur autonome n'est pas un contrôleur de domaine et ne joue aucun rôle dans un domaine,

#### 2.1.1 Mode anonyme en lecture seule

Le fichier `smb.conf` suivant montre un extrait du fichier de configuration nécessaire pour permettre l'implémentation d'un partage de fichiers anonyme en lecture-seule. Le paramètre `security = share` rend un partage anonyme. Notez bien que les niveaux de sécurité pour un seul serveur Samba ne peuvent pas être mélangés. La directive de sécurité (`security`) est un paramètre global pour Samba qui se trouve dans la section de configuration `[global]` du fichier `smb.conf`.

```
[global]
workgroup = FREMENS
netbios name = FREMENS_SRV
security = share

[data]
comment = Serveur de documentation
path = /export
read only = Yes
guest only = Yes
```

Avec une telle configuration, le serveur Samba est accessible par un poste Windows, sans besoin de mot de passe. Le répertoire est en lecture seule.

#### 2.1.2 Mode anonyme en lecture / écriture

Dans le cas du fichier de configuration suivant, on obtient un partage réseau accessible de manière anonyme en lecture/écriture. Bien entendu, une telle politique de partage de ressources n'est pas à privilégier ! L'écriture est possible grâce à la directive `read only = no`. Les directives `force user` et `force group` sont également ajoutées pour appliquer les règles de propriété à tout fichier ajouté et spécifié comme appartenant au partage.

```
[global]
workgroup = FREMENS
netbios name = FRE_SRV
security = share
```

```
[data]
comment = Serveur NON sécurisé
path = /export
force user = nobody
force group = nobody
read only = No
guest ok = Yes
```

Ici, le serveur est accessible sans mot de passe. La création de documents est possible selon les droits Unix des répertoires cibles, et la modification/suppression des fichiers est également dépendante des droits Unix de l'utilisateur `nobody` sur les fichiers.

### 2.1.3 Mode lecture / écriture sécurisé

```
[global]
workgroup = FREMENS
netbios name = FRE_SRV
security = user

[homes]
comment = Home Directories
valid users = %S
read only = No
browseable = No

[public]
comment = Partage sécurisé
path = /export
force user = nobody
force group = nobody
read only = No
browseable = Yes
```

Dans ce cas, la connexion au serveur n'est possible que par authentification *login/password*. Le prérequis est bien entendu la création de compte Samba ! A la suite du login, tous les utilisateurs ont accès à LEUR répertoire de domiciliation, et au répertoire `public`.

## 2.2 Contrôleur de domaine

S'il est possible d'intégrer un serveur Linux comme membre d'un domaine Active Directory, nous allons concentrer notre étude que la configuration d'un serveur en temps que contrôleur de domaine (de type NT). La version 4 de Samba permettra d'en faire un contrôleur de domaine Active Directory.

S'il est possible d'utiliser LDAP pour l'authentification des utilisateurs et ordinateurs sur le domaine, nous allons utiliser le backend de gestionnaire de mots de passe `tdbsam`, par défaut dans Samba.

```
[global]
workgroup = FREMENS
netbios name = FRE_PDC
passdb backend = tdbsam
security = user
add user script = /usr/sbin/useradd -m %u
delete user script = /usr/sbin/userdel -r %u
add group script = /usr/sbin/groupadd %g
delete group script = /usr/sbin/groupdel %g
add user to group script = /usr/sbin/usermod -G %g %u
add machine script = \
  /usr/sbin/useradd -s /bin/false -d /dev/null \
  -g machines %u

logon script = logon.bat
logon path = \\%L\Profiles\%U
```

```
logon drive = H:
logon home = \\%L%\%U
domain logons = Yes
os level = 99
preferred master = Yes
domain master = Yes
idmap uid = 15000-20000
idmap gid = 15000-20000

[homes]
comment = Home Directories
valid users = %S
read only = No
browseable = No
writable = Yes

[public]
comment = Data
path = /export
force user = nobody
force group = nobody
guest ok = Yes

[netlogon]
comment = Network Logon Service
path = /var/lib/samba/netlogon/scripts
admin users = ed, john, sam
guest ok = No
browseable = No
writable = No

[Profiles]
comment = Roaming Profile Share
path = /var/lib/samba/profiles
read only = No
browseable = No
guest ok = Yes
profile acls = Yes

# Other resource shares
...
...
```

## 2.3 Serveur d'impression

Le fichier `smb.conf` suivant montre un extrait du fichier de configuration nécessaire pour implémenter un serveur d'impression anonyme. Comme nous l'avons montré, le fait de donner à `browsable` la valeur `no`, n'inclut pas l'imprimante dans la liste Voisinage réseau de Windows. Bien que n'apparaissant pas lors de la navigation, la configuration explicite de l'imprimante est possible. Le serveur Samba n'a aucune responsabilité quant au partage de pilotes d'impression avec le client.

```
[global]
workgroup = FREMENS
netbios name = PRINT_SRV
security = share
printcap name = cups
disable spools= Yes
show add printer wizard = No
printing = cups

[printers]
comment = All Printers
```

```
path = /var/spool/samba
guest ok = Yes
printable = Yes
use client driver = Yes
browseable = Yes
```

L'imprimante est donc en accès anonyme. Sécuriser l'accès se ferait en mettant `security = user` dans la section `global`.

## 3 Configuration de Samba

### 3.1 Le fichier de `smb.conf`

#### 3.1.1 La section `global`

La section `global` du `smb.conf` permet de définir le rôle et le comportement du serveur samba dans le réseau, en positionnant un certain nombre de paramètres. La liste qui suit n'est pas exhaustive, la lecture du **man** et de la documentation est un passage obligé.

- `workgroup` : indique le groupe de travail dans lequel Samba est intégré
- `server string` : le nom NetBIOS du serveur tel qu'il apparaîtra dans le réseau
- `security` : prend une valeur parmi `share`, `user`, `server`, `domain`, `ads`.
  - `share` permet un accès aux ressources en se basant uniquement sur les droits des fichiers Unix
  - `user` correspond à l'identification par login/motdepasse. Si l'authentification réussit, l'attribution d'un GID/UID permet de contrôler l'accès aux ressources pour toute la session
  - `server` permet d'indiquer à Samba de faire partie d'un domaine NT en tant que serveur membre (ancienne utilisation, obsolète)
  - `domain` permet d'indiquer à Samba de faire partie d'un domaine NT en tant que serveur membre. Toutes les demandes d'authentification seront relayées au contrôleur de domaine.
  - `ads` fait du serveur Samba un membre actif d'un domaine Active Directory et ainsi accepter des tickets Kerberos.
- `hosts allow` : permet de donner les plages d'adresses IP pouvant accéder au serveur
- `printing` : indique le système d'impression à utiliser
- `guest account` : indique éventuellement la compte utilisé lors de connexion anonymes. Par défaut il s'agit de `nobody`
- `log file` : dans le cas d'une valeur de type `/var/log/samba/log.%m`, permet de spécifier un fichier de journalisation par machine
- `passdb backend` : indique le *backend* des mots de passe samba. Par défaut il s'agit de `tddbSam`.
- `interfaces` : spécifie la liste des interfaces réseau sur lesquelles Samba peut accepter les connexions
- `os level` : une valeur élevée augmente les chances d'élection de Samba en temps que maître explorateur dans un Workgroup Windows.
- `preferred master` : augmente les chances d'élection de Samba en temps que maître explorateur dans un Workgroup Windows.
- `logon script`, `logon path` : indique les différents scripts et leur emplacements pour des exécutions au démarrage des machines membres d'un domaine NT, ou au login des utilisateurs.
- `wins supprt`, `wins server` : indique si samba peut être serveur Wins, et dans le cas contraire quel est le serveur Samba sur le réseau.
- Les différents scripts permettant la gestion des utilisateurs et des groupes depuis des stations clientes sur le domaine.

```
[global]
workgroup = FREMENS
server string = FRE_PDC
hosts allow = 172.17.9
security = user
socket options = TCP_NODELAY
local master = yes
os level = 99
domain master = yes
preferred master = yes
domain logons = yes
logon script = login.bat
```

```

logon home = \\serveur\profil\%U
name resolve order = host wins lmhosts bcast
wins support = yes
dns proxy = yes add user script = /usr/sbin/useradd %u
add group script = /usr/sbin/groupadd %g
add machine script = /usr/sbin/adduser -n -g machines -c Machine -d /dev/null -s ←
    /bin/false %u
delete user script = /usr/sbin/userdel %u
delete user from group script = /usr/sbin/deluser %u %g
delete group script = /usr/sbin/groupdel %g

```

### 3.1.2 Les partages

Chaque ressource SMB sur le serveur est spécifiée dans une section de `smb.conf` portant son nom.

Les principales options sont les suivantes :

- `path` : chemin du répertoire à partager
- `comment` : texte visible dans le voisinage réseau client
- `guest ok` : si `yes` partage en accès libre sans authentification
- `valid users` : liste des utilisateurs autorisés à se connecter à la ressource
- `printable` : partage d'un service d'impression et non d'un répertoire
- `writable` : permet ou non l'écriture sur le répertoire, contraire de `read only`
- `write list` : tous les utilisateurs autorisés à écrire
- `browseable` : visibilité du partage par tous, même les utilisateurs non autorisés
- `create mode | mask` : droits maximum accordés à un fichier créé dans la ressource
- `directory mode | mask` : droits maximum accordés à un répertoire créé dans la ressource
- `force directory mode` : droits imposés lors de la création du répertoire
- `force group` : Impose un groupe propriétaire d'un fichier lors de sa création dans le partage
- `hide dot files` : cache les fichiers cachés
- `hosts deny, allow` : toutes les stations interdites, autorisées à accéder à la ressources
- `max connections` : nombre maximum de connexions simultanées à la ressources

```

[homes]
comment = Domiciliation
browseable = no
writable = yes
force create mode = 0775
force group = resp

[stagiaires]
path = /export/stagiaires
comment = Groupe
writable = yes
browseable = yes
force create mode = 0777

[netlogon]
comment = LogonService
path = /export/netlogon
writable = yes
browseable = no
write list = admin

[profil]
path = /export/profil
browseable = no
writable = yes

[document]
comment = Document
path = /export/document
writable = yes
browseable = yes

```

```
[appli]
comment = Applications
path = /export/appli
writable = yes
browseable = yes
write list = admin
```

## 3.2 La gestion des comptes

### 3.2.1 Gestion des utilisateurs

Nous allons nous intéresser à la gestion des utilisateurs utilisant le *backend* par défaut, `tddbSam`. L'outil le plus communément utilisé pour ajouter des utilisateurs Samba est `smbpasswd` :

```
smbpasswd [-a] [-c <config file>] [-x] [-d] [-e] [-D debuglevel] [-n]
          [-r <remote machine>] [-R <name resolve order>] [-m]
          [-U username[%password]] [-h] [-s] [-w pass] [-W] [-i] [-L]
          [username]
```

`smbpasswd` permet de faire la correspondance entre les utilisateurs Unix et les utilisateurs Samba. Les informations relatives aux comptes sont stockées dans le fichier `/usr/local/etc/samba/smbpasswd` alors que les mots de passes sont stockés dans `/usr/local/etc/samba/secret.tdb`.

Il n'est donc pas possible de créer un compte samba n'existant pas à priori dans Unix ! L'authentification sur le serveur Samba aura donc pour conséquence de chercher dans les fichiers précédemment cités une correspondance. Si l'utilisateur est correctement authentifié, alors chaque accès à une ressource du système hôte Samba passera par la vérification des droits Unix correspondant à son compte et à ses *groupes* unix.

### 3.2.2 Gestion des comptes dans un domaine

**3.2.2.1 Avantages d'un domaine** La gestion d'un réseau via un domaine amène plusieurs avantages non négligeable :

- SSO
- Tous les accès réseau et les droits sont gérés depuis le gestionnaire SAM (*Security Account Manager*)
- Les configurations de sécurité des postes Windows peuvent être gérées via les fichiers de stratégie système.
- L'exécution de scripts de démarrage permet de connecter des ressources réseau et d'automatiser certaines tâches.
- La centralisation des comptes dans une base de données sur un serveur du domaine

Pour arriver à ce niveau d'intégration des fonctionnalités Windows, Samba intègre quelques utilitaires complémentaires, permettant par exemple l'ajout des postes Windows au domaine, le *mappage* entre les groupes Windows et Unix, etc ...

**3.2.2.2 Ajout d'un poste au domaine** L'intégration d'un poste Windows à un domaine passe par sa configuration (Poste de Travail). Une demande est alors envoyée au contrôleur de domaine, qui doit ajouter le poste dans sa base (et particulièrement affecter un SID au poste). Dans le cas d'un serveur Samba, le service doit alors soit avoir un compte utilisateur représentant la machine à intégrer, soit créer le compte correspondant automatiquement.

La création manuelle d'un compte pour un machine consiste à ajouter un compte Unix standard, n'ayant pas de Shell ni de répertoire de domiciliation, et appartenant au groupe `machine`. Ceci est possible en utilisant les utilitaires classiques des distributions Linux ou des systèmes \*BSD.

La deuxième méthode consiste à prévoir dans le fichier de configuration la commande qui sera exécutée au moment de l'intégration d'un poste dans le domaine.

```
add machine script = /usr/sbin/useradd -d /var/lib/nobody -g 100 -s /bin/false -M ↔
                  %u
```

La ligne précédente ajoutée dans la section globale de `smb.conf` permet d'exécuter la ligne de commande `/usr/sbin/useradd -d /var/lib/nobody -g 100 -s /bin/false -M %u` lors de l'intégration d'un poste au domaine. Bien sûr, il faut adapter la commande à chaque cas précis.

De la même manière, il est possible de spécifier les différentes commandes à lancer lors de la manipulation des groupes et des utilisateurs. Ainsi, il devient possible de manipuler les comptes du domaine depuis un poste distant, à condition de disposer des autorisations `root` sur le serveur.

**3.2.2.3 Mappage des comptes Windows avec les comptes Unix** Dans le cas d'une configuration de Samba en PDC, il peut être intéressant de *mapper* les comptes prédéfinis des domaines Windows avec les comptes Unix. Par exemple, le groupe `Domain Admins` est automatiquement ajouté au groupe `Administrateurs` dans les clients Windows lors de leur connexion au domaine. Ceci permet par exemple de définir des utilisateurs sur le domaine faisant partie du groupe `Domain Admins`, et qui seront de fait Administrateur de chaque poste du domaine.

La correspondance entre les groupes Unix et les groupes Windows permet de regrouper la gestion des groupes dans un même environnement, et se fait via la commande `net`. Cette commande va permettre de tenir à jour un fichier de mappage entre les SID des groupes Windows et les groupes Unix.

```
arrakis# net groupmap add ntgroup="Domain Admins" unixgroup=admin rid=512 type=d
```

La commande précédente permet donc de mapper le groupe unix `admin` avec le groupe NT `Domain Admins`. Ainsi, tous les membres du groupe Unix `admin` seront administrateur de tous les postes du domaine NT. Bien entendu, le principe peut-être étendu à l'ensemble des groupes Windows.

## 4 Exercices

### 4.1 Concepts, réflexions, installation

1. Samba est le premier mot d'un dictionnaire contenant les lettres S, M et B. Si le dictionnaire était un fichier texte nommé `spell.txt`, donnez la ligne de commandes permettant d'en sortir tous les mots comprenant S, M et B.
2. Samba 3 ne supporte pas *Active Directory*. Il est cependant possible d'appliquer des stratégies aux ordinateurs et aux utilisateurs, d'utiliser un annuaire LDAP, de faire des profils itinérants, etc ... . Qu'apporterait de plus le support d'*Active Directory* ?
3. Pourquoi Kerberos est-il nécessaire dans un environnement *Active Directory* ?
4. Dans quel cas conseillez vous l'emploi de LDAP comme *backend* ?
5. Installation : en utilisant la méthode vue plusieurs fois en cours, installer en prenant soin de justifier les options de configuration choisies. Indiquer les différentes méthodes pour être sûr que votre service samba tourne.

### 4.2 Samba : "simple serveur de fichier"

Cette mise en application est à réaliser *seul*, en installant un serveur Samba sur chaque poste FreeBSD. Chaque point doit être mis en oeuvre, puis testé et démontré devant le formateur.

1. Vous devez réaliser un serveur de fichiers partageant un répertoire `public` accessible en contrôle total par tout le monde, permettant de déposer et de lire des fichiers.
2. Ajoutez un répertoire `partage`, qui soit accessible en lecture par tous les utilisateurs authentifiés. Vous prendrez soin de créer deux comptes utilisateurs : `formateur1/FORM@TeUr_1` et `stagiaire1/St@Gi@ire1` pour que d'autres postes puissent tester vos partages.
3. Ajoutez le partage de votre lecteur CD-ROM, accessible par tous.
4. Ajoutez un partage web permettant (seulement) à un *user* (`login=webadmin/motdepasse=apache`) d'administrer le site web, à partir d'une station quelconque.
5. Ajoutez deux groupes d'utilisateurs à Samba, `FORMATEURS` et `STAGIAIRES`. Ajoutez des utilisateurs `formateurs` et `stagiaires` en respectant les *login/passwords* dont la forme est donnée dans le point 2. Créez deux partages pour chaque groupe d'utilisateurs.
6. Testez la configuration de votre voisin en montant tous les partages décrits dans les points précédents, depuis une machine BSD. Contrôlez en même temps les différentes connexions à votre propre serveur Samba.
7. Configurez Samba pour garder trace de toutes les connexions aux ressources, classées par machine.

8. Par groupe de deux, un serveur Samba et un client Windows XP, vérifiez et optimisez le parcours du voisinage réseau. Vous prendrez soin de vous être placés dans des sous-réseaux distincts des autres groupes.

### 4.3 Samba : contrôleur de domaine

Cette mise en application est à réaliser par groupe de deux : un serveur Samba PDC, un client Windows .

1. Configurer Samba en tant que contrôleur de domaine. Ajoutez le poste Windows XP au domaine.
2. Réalisez un script de connexion permettant de monter le lecteur réseau personnel d'un utilisateur et un lecteur réseau public et qui met à l'heure le système
3. Il existe des outils Windows permettant de gérer les comptes Utilisateurs et Ordinateurs dans un domaine depuis une station Windows. SRVTOOLS.EXE permet de les installer. Essayer de gérer votre domaine depuis les outils graphiques de Windows : ajout, suppression d'utilisateurs, de groupes, etc ...

### 4.4 Samba et Windows : utilisation avancée

Cet mise en application est à réaliser par groupe de deux ou trois, en prolongement des manipulations précédentes. Si vous avez besoin d'outils spécifiques, demandez au formateur ...

1. Vous devez, via le déploiement de stratégies systèmes, supprimer du menu démarrer de vos client Windows les menus "Panneaudeconfiguration" et "Exécuter...".
2. Comment obtenir une gestion des permissions sur les ressources aussi fine que sous Windows ? Mettez en oeuvre une ressource partagée, accessible depuis deux utilisateurs Samba ne faisant pas partie des mêmes groupes Unix.
3. Les OS Windows possèdent un grand nombres de groupes utilisateurs prédéfinis. Comment faire pour mapper ces groupes Windows avec les groupes Unix ? Mettez en oeuvre la solution en mapant le groupe *administrateur* avec le groupe *wheel*, puis le compte *Administrateur* avec le compte *sysop*.
4. Configurer Samba comme serveur de fichier membre de Active Directory, et utilisant l'authentification Kerberos d'un serveur 2003 de votre réseau.
5. ----- TO DO -----