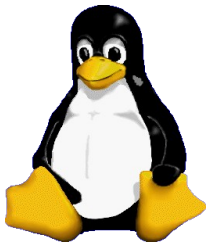


Le système GNU/Linux

By ShareVB

Partage de fichier : samba

Table des matières

I.Introduction....3
1)Historique et base....3
2)Type de réseau Windows....3
3)Gestion de la résolution des noms NetBIOS....3
4)Contrôleur de domaine et maître explorateur....4
5)Fonctionnalité de Samba....4
6)Notation UNC....5
7)Fonctionnement....5
a)Composition du service Samba....5
b)Le protocole NetBIOS....5
c)Le protocole SMB....6
d)Processus de connexion à une ressource....6
i.Etablissement de session NetBIOS....6
ii.Négociation des variantes de SMB....6
iii.Définir les paramètres de session et TID....6
e)Accès aux ressources....7
8)Autres informations....7
II.Installation sous Linux....7
III.Mode client....7
1)Sous Windows....7
a)Configuration de base....7
b)Accès....7
c)Installer une imprimante Linux sur les machines Windows....8
d)La commande Net....8
i.Montage d'un lecteur réseau....8
1.avec choix de la lettre de lecteur automatiquement....8
2.avec choix de la lettre de lecteur manuellement....8
ii.Démontage d'un lecteur réseau....8
iii.Obtenir la liste des utilisateurs du groupe de travail ou domaine....8
iv.Ajouter un partage local....8
v.Supprimer un partage....8
vi.Visualiser....9
1.les partages locaux....9
2.les partages sur un serveur....9
3.jobs d'impression....9
4.lecteurs réseaux connectés....9
5.les utilisateurs locaux....9
6.les utilisateurs existants sur votre domaine....9
vii.Messages....9
1.à un groupe....9
2.à un utilisateur....9
3.au groupe....9
4.à tous les utilisateurs connectés....9

2)Sous Linux....10
IV.Partage de fichier : mode serveur....11
1)Configuration générale....11
2)La section [global]....11
a)Général....12
b)Identité du serveur Samba....12
c)Authentification....12
i.security....12
d)Gestion des mots de passe....12
e)Option de contrôle de domaine ou explorateur de groupe....13
f)Paramètre de connexion utilisateur....13
g)Résolution de nom....13
h)Casse des noms de fichier....14
i)Réseau....14
3)Les autres sections....14
a)Paramètres généraux....14
b)Le répertoire personnel....15
c)Rendre un répertoire public....15
d)Partager un répertoire pour un utilisateur....15
e)Partager un répertoire pour upload pour un groupe et logguer les accès....16
f)Partager des applications....16
g)La base de login/mots de passes....17
4)Vérifier et activer les changements....17
V.Les imprimantes et Samba....17
1)Installation des imprimantes....17
a)Les composants de l'impression Unix....17
b)Installation des composants nécessaires....17
c)Installation d'une imprimante....18
d)Les bases de l'impression Unix....19
2)Partage d'imprimantes....19
3)Installation automatique des pilotes....20
VI.Un antivirus dans vos partages....21
1)Samba-vscan....21
2)Installation....21
a)Samba AV....21
b)ClamAV....22
3)Configuration....22
a)Samba-vscan....22
b)Les partages Samba....23
4)Test de la configuration....23
VII.Quelques notions sur NetBIOS....24
1)Les ports utilisés....24
2)Les noms NetBIOS....25
VIII.Et iptables dans tout ça....26
IX.Bibliographie....26

I. Introduction

1) Historique et base

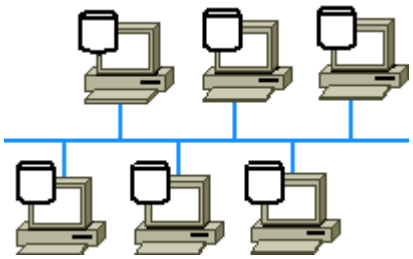
Samba est un service type « *serveur de fichier* » pour Linux permettant l'interopérabilité avec les réseaux Microsoft et la résolution de nom NetBIOS. Il utilise le protocole SMB (Server Message Bloc datant de 1988) ou CIFS (Common Internet File System = dernière version de SMB). Cette compatibilité permet donc à des clients réseau Windows 95/98/ME et Windows NT/2K/XP et plus d'accéder aux ressources partagées des serveurs Samba sous Linux.

Le projet Samba a été initié dès 1991 puis développé par un australien, Andrew Tridgell. Celui-ci lui donna ce nom, en choisissant un nom voisin de SMB en interrogeant un dictionnaire Unix, par la commande grep : `grep "^s.*m.*b" /usr/dict/words`

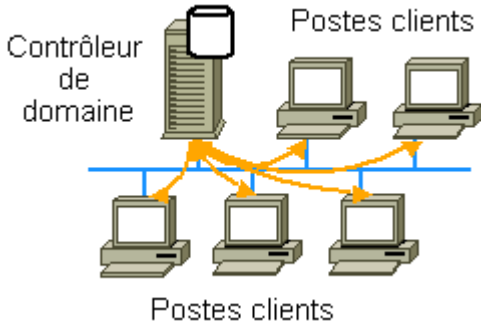
2) Type de réseau Windows

Il existe deux types de réseaux Windows :

- les groupes de travails (workgroup) : toutes les machines peuvent être clients et serveurs et tous les comptes des utilisateurs sont locaux. Ceux sont des réseaux *Peer-to-Peer* (d'égal à égal) = pas de serveur centrale par qui tout passe.



- les domaines : il faut installer un contrôleur de domaine qui assure l'authentification, le stockage des profils des utilisateurs et éventuellement la centralisation de la résolution des noms NetBIOS. Ainsi, pour pouvoir se connecter, un utilisateur doit exister sur le domaine et avoir le droit de se connecter depuis la machine depuis laquelle il essaie de le faire.

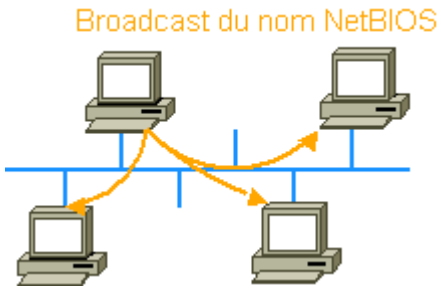


3) Gestion de la résolution des noms NetBIOS

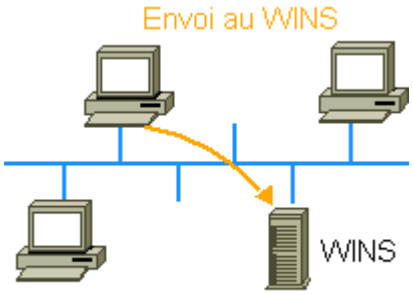
La résolution des noms NetBIOS peut se réaliser de la façon suivante dans un groupe de travail :

- soit une machine est choisie au hazard dans le workgroup pour devenir la machine maitre contenant la liste des autres machines de ce workgroup

- soit on désigne un serveur pour être toujours choisi



- soit il faut utiliser un serveur WINS qui permet également d'avoir un workgroup sur plusieurs sous-réseaux (du fait que le protocole NetBIOS n'est pas routable)



Dans un domaine, il y aura obligatoirement au moins un serveur WINS (qui pourra par défaut être le contrôleur de domaine) pour centraliser la résolution des noms.

4) Contrôleur de domaine et maître explorateur

Sur les groupes de travail, on trouve toujours un « Maître explorateur local » voire un « Maître explorateur de sauvegarde ». Un maître explorateur est un serveur WINS. Il est chargé de récupèrer des informations sur les machines de son voisinage réseau local.

Sur les domaines, on trouve obligatoirement un « contrôleur de domaine » chargé de l'authentification des utilisateurs du domaine, et éventuellement de WINS s'il n'y a pas de « Maitre explorateur ».

Il est souvent nécessaire de mettre des « Maîtres explorateur locaux » sur chaque sous-réseau du fait que NetBIOS utilise les broadcast et ne sort généralement pas du sous réseaux d'émission. Dans ce cas, le « contrôleur de domaine » ou « WINS » global ira chercher les informations et en donnera à tous les « Maîtres explorateur locaux ».

5) Fonctionnalité de Samba

Le serveur Samba est donc un service de « *serveur de fichiers* » capable de :

- partage de fichiers et de répertoires : répertoire publique ou semi-privée (mot de passe)
- partage d'imprimantes : accès publique ou avec mot de passe
- gestion des comptes utilisateurs : accès privé par login/mot de passe
- gestion des permissions d'accès : les droits Unix
- exécution de scripts de connexion personnalisés
- servir de serveur WINS

6) Notation UNC

La notation UNC (souvent appelé « notation réseau Windows » et toujours associée aux réseaux Windows) est une notation à base de nom Net BIOS (et pas DNS). Il se compose du nom NetBIOS du serveur, du nom du partage suivi du chemin du fichier (relativement au partage) :

`\\nom_netbios_serveur\nom_partage\chemin\vers\fichier`

Dans Windows, si l'on tappe dans la barre d'adresse d'Explorateur :

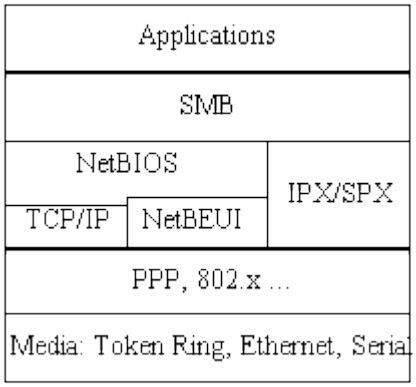
- `\\nom_netbios_serveur` : affiche la liste des partages du serveur
- `\\nom_netbios_serveur\nom_partage` : affiche le contenu du partage (dans le cas d'un dossier)
- `\\nom_netbios_serveur\nom_partage\chemin\vers\fichier` : affiche le contenu du fichier

7) Fonctionnement

a) Composition du service Samba

Le serveur Samba se compose de deux parties :

- **smbd** : serveur de fichier
- **nmbd** : serveur de noms NetBIOS



b) Le protocole NetBIOS

Le protocole NetBIOS se place au dessus de TCP (ou anciennement au dessus de NetBUI sur les réseaux du même nom). Il a pour but de satisfaire aux exigences suivantes :

- enregistrer sur une machine les associations NetBIOS et adresses IP
- résoudre les noms de machines NetBIOS en adresses IP

c) Le protocole SMB

Service Message Block est un protocole de type « client/serveur » :

- le serveur est une machine ayant une ressource à partager
- le client est une machine voulant accéder à une ressource

Le rôle de serveur et de client peut être inversé à tout moment et un client peut être un serveur simultanéement (et réciproquement).

Le protocole SMB permet de :

- ouvrir et fermer les fichiers
- écrire ou lire depuis ou vers des fichiers
- créer ou supprimer des fichiers et dossiers
- rechercher des fichiers
- mettre un fichier à imprimer dans une file d'impression

d) Processus de connexion à une ressource

Pour établir une connexion à une ressource, il faut :

- établir une session NetBIOS
- négocier les variantes du protocole SMB
- définir les paramètres de session
- faire une connexion en arbre vers le ressource

i. Etablissement de session NetBIOS

Avant de pouvoir accéder à un partage, il est nécessaire d'obtenir une session NetBIOS vers le serveur. Pour cela, le client envoie un message de demande d'ouverture de session à laquelle le serveur répond par un approbation ou un rejet.

ii. Négociation des variantes de SMB

Ensuite, il faut indiquer quelle version de SMB utiliseront le client et le serveur. Pour cela, le client envoie une liste de version de SMB et le serveur répond en indiquant l'index de la version de SMB (dans la liste du client) qu'il accepte ou 255 s'il ne trouve pas son bonheur.

iii. Définir les paramètres de session et TID

Enfin, il faut définir les paramètres de connexions au partage. Pour cela, on utilise un message SMB qui en contient en réalité 2 :

- définition des paramètres de connexion : login/mot de passe, groupe de travail/nom domaine NetBIOS, nombre de requête à mettre en queue...
- connexion à un partage : nom du partage...

A cela, le serveur répond par une autorisation ou un refus de connexion, et dans le cas d'un succès,

il renvoie un TID (Tree Identifier) qui est un identifiant pour la connexion au partage par le client et qui devra être envoyé pour toute opération sur le partage par le client.

e) Accès aux ressources

Pour effectuer une action (comme lecture, création, suppression) sur une ressource/partage, il faut d'abord établir une connexion à la ressource comme indique la section précédente. Ensuite, on pourra utiliser le TID résultant pour effectuer les actions sur la ressource.

8) Autres informations

Pour plus d'informations voir la section « Quelques notions sur NetBIOS et SMB »

II. Installation sous Linux

```
[root]# apt-get install samba-common samba
```

`Debconf` vous demande s'il doit lancer samba avec `Inetd` ou en **standalone.** La seconde est de loin la meilleure car `Inetd` n'est qu'un wrapper TCP.

III. Mode client

1) Sous Windows

a) Configuration de base

Samba nécessite TCP/IP et NetBIOS. Sur chaque machine cliente Windows, il faut donc ajouter `TCP/IP et NETBIOS` si ces protocoles sont absents. Il est aussi nécessaire de vérifier que `NetBios` est activé avec `TCP/IP` (`Voisinage réseau/Propriétés TCP/IP`, onglet `NetBios`).
Ensuite, il est nécessaire que l'IP cliente appartienne au même sous réseau que le serveur Samba.
Enfin, on peut modifier le nom de l'ordinateur dans l'onglet `Nom de l'ordinateur` des `Propriétés systèmes` (clic droit sur `Poste de travail/Propriétés`) et en cliquant sur `Modifier`.

b) Accès

Vous devriez voir le serveur Samba dans le `Voisinage réseau` et/ou dans votre groupe de travail. Lorsque vous cliquez sur l'icône du serveur ou de l'un de ses partages, un nom d'utilisateur et un mot de passe devraient vous être demandés.

c) Installer une imprimante Linux sur les machines Windows

- Lancer l'`Assistant d'ajout d'imprimante` (Paramètres/Imprimantes)
- Choisir `Imprimante réseau`
- Parcourir le *voisinage réseau* pour détecter l'imprimante : par exemple, choix de *`nom_imprimante`* sur *`serveur`*. Le nom de la file d'attente serait alors `\\serveur\nom_imprimante`
- Choisir le modèle d'imprimante et le nom sous lequel elle apparaîtra sur la machine locale.
- Pour vérifier faire imprimer une page de test.
- Normalement l'imprimante partagée sera visible dans le voisinage réseau

d) La commande Net

On peut trouver plus d'informations à http://fanocayoo.free.fr/sys_nt_net.htm.

i. Montage d'un lecteur réseau

1. avec choix de la lettre de lecteur automatiquement

```
net use * \\serveur\partage
```

2. avec choix de la lettre de lecteur manuellement

```
net use lettre: \\serveur\partage
```

ii. Démontage d'un lecteur réseau

```
net use lettre: /DELETE
```

iii. Obtenir la liste des utilisateurs du groupe de travail ou domaine

```
net user
```

iv. Ajouter un partage local

```
net share nom_partage=lecteur:répertoire
```

v. Supprimer un partage

```
net share nom_partage /DELETE
```

vi. Visualiser

1. les partages locaux

```
net share
```

2. les partages sur un serveur

```
net view \\serveur
```

3. jobs d'impression

```
net print \\serveur\partage
```

4. lecteurs réseaux connectés

```
net use
```

5. les utilisateurs locaux

```
net user
```

6. les utilisateurs existants sur votre domaine

```
net -W domaine rpc user
```

vii. Messages

1. à un groupe

```
net send /domain:nom_groupe message
```

2. à un utilisateur

```
net send utilisateur message
```

3. au groupe

```
net send * message
```

4. à tous les utilisateurs connectés

```
net send /USERS message
```

2) Sous Linux

```
[root]# yum install samba
```

La commande nmblookup permet d'obtenir des informations sur un nom netbios :

```
[user]# nmblookup <nom netbios>
```

La commande net permet de récupérer diverses informations sur les réseaux Microsoft, par exemple, comme `nmblookup` :

```
[user]# net lookup <nom netbios>
```

On peut aussi obtenir le nom et l'IP du contrôleur de domaine d'un réseau Microsoft :

```
[user]# nmblookup -M <nom du réseau>
```

ou avec la commande `net` :

```
[user]# net lookup master INFO
```

On peut aussi trouver la liste de machines d'un réseau :

```
[user]# findsmb
```

Pour obtenir la liste des partages d'une machine, on utilisera la syntaxe suivante :

```
[user]# smbclient -L \\\\nom_netbios_ou_ip_machine\\
```

On peut aussi monter un dossier samba dans l'arborescence locale :

```
[user]# smbmount //nom_netbios_ou_ip_machine/nom_partage
/chemin/montage -o username=nom_utilisateur_pour_montage
```

Dans le fichier `/etc/fstab` :

```
smb:///nom_netbios_ou_ip_machine/chemin/nom_partage
/chemin/montage     smb
credentials=/chemin/fichier/mot/passe,fmask=0022,dmask=0022,rw
```

Dans le fichier `/chemin/fichier/mot/passe` :

```
username=<utilisateur>
password=<mot de passe>
```

IV. Partage de fichier : mode serveur

1) Configuration générale

Toute la configuration de Samba se fait dans le fichier `/etc/samba/smb.conf`. Ce fichier est constitué comme un fichier INI de Windows :

- le fichier est divisé en section commençant par `[nom_section]` et se terminant au début de la section suivante ou la fin du fichier
- dans chaque section, on indique des couples : `clé = valeur` définissant les propriétés de la section

On peut utiliser les macros suivantes dans le fichier `smb.conf` :

- **%u.** Nom d'utilisateur pour le service courant.
- **%g.** Nom du groupe primaire de l'utilisateur `%u`.
- **%U.** Nom d'utilisateur pour le service courant. Ceci est le nom demandé par l'utilisateur, pas forcement le nom utilisé par Samba
- **%G.** Nom du groupe primaire de l'utilisateur `%U`.
- **%H.** Répertoire personnel (home) de `%u`.
- **%v.** Version de Samba.
- **%S.** Le nom du service courant (par exemple le nom du partage).
- **%P.** Le répertoire principal du service courant.
- **%h.** Le nom Internet de la machine (hostname) sur laquelle tourne Samba.
- **%m.** Le nom Netbios de la machine cliente.
- **%L.** Le nom Netbios du serveur Samba. C'est le nom utilisé par le client, peut être utile pour différencier le comportement de Samba avec plusieurs noms Netbios.
- **%R.** Niveau de protocole utilisé *(CORE, COREPLUS, LANMAN1, LANMAN2 ou NT1)*.
- **%d.** Numéro de process du processus serveur courant.
- **%a.** Architecture du système client. Reconnait actuellement *Samba, WfWg, WinNT et Win95*. Le reste renvoie *UNKOWN*
- **%I.** Adresse IP de la machine cliente
- **%T.** La date et l'heure courante
- **%$(envar).** La valeur de la variable d'environnement `envar`.
- **%N.** Nom du serveur hébergeant le répertoire personnel (home) NIS.
- **%p.** Chemin du répertoire personnel NIS, obtenu à partir de l'entrée NIS auto.map.

2) La section [global]

Dans cette section, on trouve les paramètres généraux de Samba dont voici les principaux

a) Général

```
# compte à utiliser pour les accès invités aux partages
guest account = nobody
# accès multi utilisateur
share modes = yes
# utiliser un fichier de trace pour chaque machine qui se connecte
log file = /var/log/samba/log.%m
```

b) Identité du serveur Samba

```
#nom du groupe de travail ou domaine
workgroup=nom_groupe_de_travail_ou_domaine
#nom NetBIOS (nom Windows) du serveur Samba
netbios name=SERVEURSMB
#autres noms pour la machine serveur (à décommenter si utilisé)
#netbios aliases = autre_nom1 autre_nom2 ...
#description du serveur
server string=Serveur %L (Samba %v)
```

c) Authentification

```
#niveau de sécurité
security = user
#active la fonction « contrôleur de domaine » de Samba
#indique que les clients Windows peuvent se logguer au domaine
#dont le nom est celui indiqué dans workgroup
domain logons = yes
#indique le fichier contenant le mapping entre utilisateur Samba et Unix
username map = /etc/samba/smbusers
```

i. security

Voilà bien le paramètre le plus important de la sécurité des données hébergées dans les répertoires servis par Samba. Cette propriété peut prendre les valeurs suivantes

- *share* : sécurité à la Win9x = (au mieux) un mot de passe par partage sans s'occuper du nom d'utilisateur = login anonyme
- *user* : droits d'accès aux partages par couples login/mots de passes (approximativement les fonctionnalités d'authentification de NT)
- *server* : ne pas utiliser
- *domain* : forcer l'authentificiation uniquement sur les contrôleurs de domaines

d) Gestion des mots de passe

```
#indique si l'on doit faire les négociations
# avec des mots de passes cryptés ou pas
# (98 et +, NT4 SP3 et +)
encrypt passwords = yes
# indique le fichier contenant les logins Samba, l'uid utilisateur
# les mots de passes cryptés (LanMan, NT)...à la /etc/passwd
smb passwd file = /etc/samba/smbpasswd

#indique l'adresse du serveur principal (contrôleur de domaine)
```

```
#à décommenter si utilisé avec security = server ou security = domain
#password server = ip_ou_nom_serveur_principal
#indiquer s'il faut automatiquement appeler la commande passwd
#lors du changement de mot de passe. A décommenter si utile
#unix password sync = yes #ou no
#indique la commande passwd à exécuter si l'option précédente est à yes
# à décommenter si utile
#passwd program = /usr/bin/passwd %u
```

e) Option de contrôle de domaine ou explorateur de groupe

```
#indique si le serveur Samba peut être « Master Browser »
# (Maitre Explorateur)
# du réseau local (du moins participer à l'élection locale)
local master = yes
#indique la version de Windows que l'on simule :
# plus la valeur est grande plus le serveur a de chances
# d'être Master Browser
os level = 33
#indique si le serveur Samba est le « Domain Master Browser »
# de son domaine
#ce qui permet de récupérer la liste des machines
# depuis les Master Browser locaux et leur redistribue
# la liste complète
domain master = yes
# indique l'adresse à laquelle le serveur peut se signaler par broadcast
# pour avertir de sa présence un autre groupe de travail
# à décommenter si vous ne voyez pas le serveur depuis les clients
# remote announce = <IP de broadcast du sous réseau>
```

f) Paramètre de connexion utilisateur

#ces options sont uniquement valables si le serveur est contrôleur de domaine primaire

```
#script Windows qui sera exécuter à chaque connexion d'un utilisateur
#dans le domaine
logon script = script.bat
# lettre utilisée pour connecter le lecteur réseau du répertoire
# personnel sous NT
logon drive = p:
#chemin NetBIOS des profils utilisateurs pour Win9x
logon home = \\%L\profiles\%U\
#chemin NetBIOS de stockage des profils utilisateurs pour WinNT
# (contenu genre Documents And Settings\utilisateur)
logon path = \\%L\Profiles\%U
```

g) Résolution de nom

```
#indique si l'on supprote WINS ou pas
wins support = yes #ou no
#indique l'IP ou le nom du serveur WINS
wins server = 10.0.0.2
# indique si l'on sert de proxy WINS
wins proxy = yes
# indique si l'on essaie de résoudre les noms NetBIOS par DNS
dns proxy = no
```

h) Casse des noms de fichier

```
#indique si l'on préserve la casse des noms longs ou pas
preserve case = yes # NOTE: These can be set on a per share basis
#indique si l'on préserve la casse des noms courts
short preserve case = no
#indique la casse par défaut
default case = lower
#indique si l'on respecte la casse
case sensitive = no
```

i) Réseau

```
#indique des options de sockets
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
#indique les interfaces d'écoute pour Samba
interfaces = 10.0.0.1/32
```

3) Les autres sections

a) Paramètres généraux

Paramètre	Description
`guest ok = yes|no`	partage en accès libre sans authentification (synonyme de public)
`valid users =`	liste des utilisateurs autorisés à se connecter à la ressource
`printable = true|false`	partage d'un service d'impression et non de répertoire
`writeable = yes|no`	permet ou non l'écriture sur le répertoire (contraire de read only)
`write list =`	liste des utilisateurs autorisés à écrire
`browseable =`	visibilité du partage par tous, même les utilisateurs non autorisés
`create mode | mask =`	droits maximums accordés à un fichier créé dans la ressource (masquer par l'umask Unix)
`directory mode | mask =`	droits maximums accordés à un répertoire créé dans la ressource (masquer par l'umask Unix)
`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 commençant par un point (comme Linux)
`hosts allow hosts deny =`	ressource autorisée/interdite à une liste d'adresses IP

b) Le répertoire personnel

```
# Donne accès à chaque utilisateur
#  à son répertoire personnel /home/%u
[homes]
     #donne une description au partage
     comment = Répertoire personnel
     # suel l'utilisateur concerné voit son dossier personnel
     browsable = no
     # il peu écrire dans son dossier :)
     writable = yes
     # tous les fichiers et dossiers créés dans son dossier
     #personnel ne sont au maximum « rwx » que par lui
     create mode = 0700
```

c) Rendre un répertoire public

Il est nécessaire de créer le dossier, par exemple, `/chemin/dossier/publique` avec les droits `rwxrwxrwx (chmod 777)`.

```
# Donne à un partage nommé « public »
[public]
     #description du partage
     comment = Répertoire public
     #chemin du dossier partagé
     path = /chemin/dossier/publique
     #indique que tout le monde peut y accéder
     public = yes
     #indique que l'on peut écrire dedans
     writeable = yes
     #indique que les fichiers sont lisibles par tout le monde
     # et modifiables uniquement par leur propriétaire
     create mode = 0755
```

d) Partager un répertoire pour un utilisateur

```
#partage un dossier sous le nom « prive »
[prive]
     #description du partage
     comment = répertoire privé
     #chemin du partage
     path = /chemin/partage
     #utilisateur propriétaire du dossier du partage
     user = utilisateur
     #indique que seul l'utilisateur ci-dessus
     #peut accéder au partage
```

```
        only user = yes
        #indique que le dossier est inscriptible
        writable = yes
```

Note : cela permet « d'émuler `security=share` » dans la mesure où un seul login/mots de passe est possible. Cepedant, il est nécesaire de donner le bon login en plus du bon mot de passe.

e) Partager un répertoire pour upload pour un groupe et logguer les accès

Il est nécessaire de créer le dossier, par exemple, `/chemin/dossier/upload` avec les droits `rwxrwx---` `(chmod 770)` et de donner la propriété du répertoire au groupe *`groupe`*.

```
#partage un dossier en écriture seule avec log sous le nom de « upload »
[upload]
        #description du répsertoire
        comment = répertoire upload
        #dossier non publique
        public = no
        #chemin du dossier
        path = /chemin/dossier/upload
        #upload de fichier uniquement pour le groupe
        write list = @groupe
        #log les connexions
        preexec = echo \"%u s'est connecté à %S depuis %m (%I)\"
>> /var/log/samba/monsamba
        #et les déconnexions
        postexec = echo \"%u s'est déconnecté de %S depuis %m
(%I)\" >> /var/log/samba/monsamba
```

f) Partager des applications

Il est nécessaire de créer le dossier, par exemple, `/chemin/dossier/appli` avec les droits `rwxrwxr-x` `(chmod 775)` et de donner la propriété du répertoire à *`admin:admin`*.

```
#partage un dossier de logiciels sous le nom « appli »
[logiciels]
        #description du répertoire
        comment = Applications partagées sur le serveur
        #chemin du dossier à partager
        path = /chemin/dossier/appli
        #indique que le dossier est accessible de tous
        public = yes
        #répertoire en lecture seule pour tout le monde
        writeable =no
        #sauf pour le groupe admin
        write list = @admin
```

g) La base de login/mots de passes

Pour activer un login/mot de passe, il est nécessaire d'ajouter les utilisateurs et mots de passes à la main avec smbpasswd :

```
[root]# smbpasswd <utilisateur>
```

4) Vérifier et activer les changements

Lancer l'utilitaire **`testparm`** permet de tester la syntaxe du fichier de configuration et de déceler les erreurs. Il est recommandé de le lancer systématiquement lors de la mise au point de `smb.conf`. Il diagnostique des erreurs de syntaxe et des incohérences dans les choix des clauses.

Ne pas oublier à chaque changement effectué dans `smb.conf` à relancer les processus de Samba :

```
# conseillé plutôt que la commande globale smb restart
/etc/rc.d/init.d/samba stop
/etc/rc.d/init.d/samba start
```

V. Les imprimantes et Samba

1) Installation des imprimantes

a) Les composants de l'impression Unix

Les composants de l'impression Unix :

- CUPS

  Le Common UNIX Printing System (http://www.cups.org) est un spouleur d'impression ainsi qu'une suite de logiciel pour l'administrer.

- Samba

  Samba (http://www.samba.org) est un logiciel permettant les systèmes non Windows de servir de serveur de fichiers et d'impression.

- Printer Drivers

  LinuxPrinting.org (http://www.linuxprinting.org) offre une liste impressionnante de PPDs (pilote d'impression).

b) Installation des composants nécessaires

Voic les composants nécessaire sous Debian :

- `cupsys`

  Serveur CUPS

- `cupsys-bsd`

  commande BSD CUPS

- `cupsys-client`

  programme clients pour CUPS

- `foomatic-bin`

  Programme pour LinuxPrinting.org

- `samba`

  Samba SMB/CIFS server for UNIX

- `smbclient`

  Samba SMB/CIFS client for UNIX

- `gs-esp`

  ESP Ghostscript (http://www.cups.org/ghostscript.php)

- `a2ps`

  GNU A2PS (http://www.gnu.org/software/a2ps/)

- `cupsys-driver-gimpprint`

  Une série de PPD pour vos imprimantes

```
[root]# apt-get update
[root]# apt-get install cupsys cupsys-bsd cupsys-client foomatic-
bin samba smbclient gs-esp a2ps cupsys-driver-gimpprint
```

c) Installation d'une imprimante

La commande lpadmin permet d'administrer les imprimantes :

```
lpadmin -p Nom_imprimante -v /dev/périphérique -P /chemin/fichier.ppd
cupsenable Nom_imprimante
cupsaccept Nom_imprimante
lpadmin -d Nom_imprimante
```

- La première commande ajoute l'imprimante *Nom_imprimante* qui est reliée au périphérique /dev/*périphérique* dans le fichier */chemin/fichier.ppd*. On peut trouver un grand nombre de fichiers PPD dans le répertoire /usr/share/cups/model.Pour obtenir la liste des pilotes (PPD) disponibles, utiliser la commande lpinfo -v (avec un grep *le_nom_de_votre_imprimante*). Pour obtenir la liste des périphériques disponibles, utiliser la commande lpinfo -m.

- La seconde permet d'activer l'imprimante.
- La troisième permet de dire à CUPS que la file d'impression de l'imprimante peut imprimer.
- Enfin, la dernière commande permet de définir la nouvelle imprimante comme imprimante par défaut.

d) Les bases de l'impression Unix

Les document peuvent être mis en file d'impression par les commandes lpr ou lp suivies du nom de fichier à imprimer. On peut aussi voir la file d'impression et l'état d'une imprimante avec les commande lpstat -o ou lpstat -p. Enfin, pour annuler une impression, on utilisera cupscancel ou lprm suivi de l'ID de job.

Le spouleur d'impression de CUPS est cupsd. Il convertit les documents en PostScript puis les convertit pas une série de filtres (qui peuvent rallonger le temps d'impression) en un format natif à l'imprimante cible. Les imprimantes qui ne parlent pas PostScript utilise un format Raster ou Bitmap. Ces formats peuvent prendre un certain temps à être réalisés et envoyés à l'imprimante.

Si CUPS ne trouve pas de filtre pour convertir un fichier en PostScript, lp ou lpr renvoie une erreur de format non supporté. Souvent, les applications ne sont pas fourni avec un filtre pour CUPS. Dans ce cas, on ne peut utiliser que le « Fichier/Imprimer » depuis l'application.

2) Partage d'imprimantes

Dans la section `[global]` de `smb.conf` :

```
#indique que l'on utilise cups pour imprimer sur le serveur
printing = cups
```

Ensuite, il faut créer le dossier des jobs d'impression :

```
[root]# mkdir /var/spool/samba
[root]# chmod a+rwt /var/spool/samba
```

Et à la fin du fichier `smb.conf` :

```
#si on utilise CUPS, on n'a pas besoin de définir chaque imprimante séparement
[printers]
      #descriptions des imprimantes
      comment = All Printers
      #chemin du spool
      path = /var/spool/samba
      #seuls les utilisateurs autorisés peuvent voir les imprimantes
      #peut être yes si on veut les voir dans l'assistant d'ajout d'imprimantes
      browseable = no
      #pas d'écriture dans le partage des imprimantes
      writable = no
      #définit un partage d'imprimantes
      printable = yes
      #accessible uniquement par un utilisateur authentifié
      create mode = 0700
```

3) Installation automatique des pilotes

Si vous installez une imprimante sur un serveur Linux, pourquoi ne pas proposer l'installation automatique des pilotes sur les postes clients ? Cela vous permettra de ne pas avoir à vous soucier de le faire sur toutes les machines de votre réseau.

Pour réaliser cette installation, il est nécessaire d'utiliser la technologie *Point And Print* disponibles en client sous Windows.

Il est nécessaire d'avoir un niveau de sécurité user et d'avoir réalisé la configuration de la section `[printers]` ou d'un partage imprimante spécifique.

Pour que Windows sache trouver les pilotes, il faut ajouter un partage « `print$` » (invisible sous Windows car terminé par $) :

```
[print$]
     #dossier des pilotes d'imprimantes
     path = /chemin/du/dossier/pilote
     #accessible en anonyme
     guest ok = yes
     #visible par tout le monde
     browseable = yes
     #lecture seule pour tout le monde
     read only = yes
     #sauf pour le groupe chargé de gérer les pilotes d'imprimantes
     write list = @groupe_administrateur_pilote
     #indique le groupe charger de la gestion des pilotes
     printer admin = @groupe_administrateur_pilote
```

On peut aussi être amené à ajouter la dernière ligne :

```
     printer admin = @groupe_administrateur_pilote
```

au partage correspondant à l'imprimante ou `[printers]`.

Il est ensuite nécessaire de créer les dossiers appropriés :

```
[root]# mkdir /chemin/du/dossier/pilote
```

Pour Windows NT et + :

```
[root]# mkdir /chemin/du/dossier/pilote/W32X86
```

Pour Windows Win9x :

```
[root]# mkdir /chemin/du/dossier/pilote/WIN40
```

```
[root]# chown -R admin:groupe_administrateur_pilote
/chemin/du/dossier/pilote
[root]# chmod -R 775 /chemin/du/dossier/pilote
```

Maintenant, connectez-vous sur une machine Windows et ouvrez le serveur Samba dans le `Voisinage réseau`. Si un login/mot de passe vous est demandé, donner le login/mot de passe

d'un utilisateur du groupe *groupe_administrateur_pilote*.

Ouvrir le dossier Imprimantes sur le serveur et clic à droite sur l'imprimante pour laquelle vous voulez installer les pilotes. Cliquer sur Propriétés. Une boîte de dialogue vous demandant si vous voulez installer les pilotes s'affiche. Répondez **Non.**

Allez dans l'onglet Avancé et cliquer sur Nouveau pilote. Ensuite installer le pilote de l'imprimante depuis la liste fourni, un CD ou ce que vous voulez du moment que vous installer les bons pilotes pour la bonne imprimante.

Si vous obtenez une erreur de permissions, c'est que vous ne vous êtes pas connecté avec un compte du groupe *groupe_administrateur_pilote*.

Une fois l'installation terminée, **n'oubliez pas de cliquer sur Appliquer** (une fois revenu dans l'onglet Avancé) afin d'ensuite tous les clients pourront installer les pilotes sur leurs machines.

Si tous s'est bien passé vous devriez voir un nouveau sous dossier dans W32X86 avec les fichiers des pilotes dedans.

Les clients n'auront plus qu'à :

- Cliquer sur « Ajouter une imprimante » depuis la liste des imprimantes locales
- Choisir Imprimante réseau
- Cliquer sur parcourir pour choisir l'imprimante à ajouter depuis le voisinage réseau
- Choisir si ce doit être votre imprimante par défaut
- Cliquer sur Terminer

VI. Un antivirus dans vos partages

ClamAV est un antivirus tournant en démon sous Linux et capable de détecter les virus Windows. Le projet se trouve à l'adresse http://www.clamav.net

1) Samba-vscan

Module VFS pour Samba qui permet d'analyser les fichiers lors des accès sur le serveur de fichiers. http://sourceforge.net/projects/openantivirus/

2) Installation

a) Samba AV

Pour installer le projet *Samba-vscan*, il faut avoir installer les sources de *Samba* :

```
[root]# cd /usr/src
[root]# apt-get install dpkg-dev
[root]# apt-get source samba
[root]# apt-get build-dep samba
[root]# cd samba-*
```

```
[root]# ./debian/rules configure-stamp
[root]# cd source/
[root]# make proto
[root]# cd /usr/src/
[root]# wget http://switch.dl.sourceforge.net/sourceforge/openantivirus/samba-vscan-0.3.6.tar.bz2
[root]# tar xjvf samba-vscan-0.3.6.tar.bz2
[root]# cd samba-vscan-0.3.6
[root]# ./configure --with-samba-source=/usr/src/samba-*/source
[root]# make
```

Si vous recevez l'erreur :

```
      global/vscan-parameter.c: Dans la fonction « set_common_default_settings »:
      global/vscan-parameter.c:78: attention : format int, arg time_t (arg 2)
      global/vscan-parameter.c:105:40: suffixe « a » invalide pour une constante entière
```

Modifier le fichier `/usr/src/samba-3.0.14a/source/include/version.h` en supprimant le "a" de :
`SAMBA_VERSION_RELEASE=14a`

```
[root]# make install
[root]# cp clamav/vscan-clamav.conf /etc/samba/
```

b) ClamAV

```
[root]#  apt-get install clamav clamav-daemon clamav-testfiles clamav-freshclam
```

Debconf va vous demander comment mettre à jour la base antivirale : choisir `cron`. Pour les autres questions, garder les options par défaut. Si vous voulez recommencer, taper `dkpg-reconfigure clamav-freshclam`.

3) Configuration

a) Samba-vscan

Dans le fichier de configuration de **samba-vscan**, */etc/samba/vscan-clamav.conf*, il faut modifier plusieurs variables :

```
; envoyer un message de notification grâce au service ,
; Windows Messenger service lorsqu'un virus est trouvé
; (default: yes)
send warning message = yes
; le nom du socket de clamav défini dans /etc/clamav/clamd.conf
clamd socket name = /var/run/clamav/clamd.sock
; action à  faire en cas d'infection,
; quarantine : essayer de déplacer le fichier dans le répértoire de quarantaine,
```

```
; si le déplacement échoue le fichier est effacé
; delete : effacer le fichier (dangeureux),
; nothing : ne rien faire.
infected file action = quarantine
quarantine directory = /tmp/quarantine
quarantine prefix = vir-
```

b) Les partages Samba

Dans chacun des partages que vous voulez protéger, dans le fichier `smb.conf` :

```
vfs object = vscan-clamav
vscan-clamav: config-file = /etc/samba/vscan-clamav.conf
```

4) Test de la configuration

Si la syntaxe du fichier de configuration est correcte vous pouvez redémarrer le daemon `smb` et tester le bon fonctionnement de l'antivirus :

```
[root]# /etc/init.d/samba restart
[user]$ smbclient \\\\serveur\\un_partage
Password:
....
lcd /usr/share/clamav-testfiles/
put clamav.zip
```

Ensuite dans l'un des fichiers (`syslog`) de logs vus devriez trouver des lignes provenant de `smbd_vscan` indiquant d'un virus a été détecté.

Si ce fichier contient des lignes d'erreurs du style :

`smbd_vscan-clamav[`*`PID`*`]: ERROR: daemon failed with a minor error - access to file `*`fichier`*` denied`

Modifier votre fichier `/etc/clamav/clamd.conf` pour ajouter ou modifier :

```
User clamav
```

en

```
User root
```

VII. Quelques notions sur NetBIOS

1) Les ports utilisés

Port	Nom	Nom usuel	Usage

	court		
135	EPMAP	Service Location	Service permettant la réalisation des appels de procédures distantes (RPC ou Remote Procedure Call). Toutes les tâches administratives distants sous Windows utilisent ces RPC. Ce port est, en réalité, un véritable dispatcher ou plutôt un "portmapper" : lorsqu'une machine cherche à atteindre un service sur une machine distante, elle réalise schématiquement (et oui, vous avez déjà vu MS faire simple vous !) les actions suivantes : • elle se connecte d'abord via le port 135 pour localiser le port réel sur lequel tourne le service qui l'intéresse • ennsuite elle se connectera au service via le numéro de port qui lui aura été communiqué Voilà pourquoi ce port s'appelle « *localisation de services* ». Sur ce port 135 se situe aussi le gestionnaire de contrôle de services COM ce qui le rend nécessaire aux mécanismes DCOM.
137	NETBIOS-NS	NetBios Name Service	Ce port est utilisé pour l'enregistrement des associations nom NetBIOS <=> IP. C'est le port du serveur WINS. Le WINS est comme le DNS, il permet de donner l'IP d'un nom. Toutes les machines peuvent s'annoncer par un broadcast (ou directement) sur le réseau local pour enregistrer son nom NetBIOS auprès du serveur WINS local. Pour résoudre un nom NetBIOS, le client envoie soit un broadcast ou se connecte directement au WINS et reçoit la réponse sur ce port. Enfin, on pourra signaler qu'un caractère non imprimable à la fin du nom NetBIOS indique le type de service qu'il fournit (client, serveur, WINS...)
138	NETBIOS-DGM	NetBios Datagram Service	Comme son nom l'indique (Datagram), ce port ne s'utilise que sur UDP. Il sert principalement pour diffuser (par broadcast) des informations sur le réseau. Chaque machine écoute sur ce port pour récolter les informations (noms NetBIOS, partage) que les autres machines broadcast sur ce port. Ce service est utiliser avant tout pour le service d'explorateur réseau (SMB browser service) pour découvrir les machines du voisinage réseau (et remplir cette vue de l'explorateur Windows).
139	NETBIOS-SSN	NetBios Session Service	Comme son nom l'indique (Session), ce port n'est utilisé qu'en TCP. Il sert pour les connexions aux partages entre deux machines (le client et le serveur). C'est ce port qui sera utiliser pour tout accès à la liste des partages ou au contenu des partages sur une machine.

2) Les noms NetBIOS

Les noms NetBIOS sont uniques dans tout le réseau local et sont éventuellement remplis avec des

espaces pour atteindre 15 caractères et suivis d'un caractère de type de service. A chaque nom NetBIOS est associée une IP (sauf pour les noms de domaines ou groupe de travail)

Nom NetBIOS	**Description**
Computername <00>	C'est le fameux « nom NetBIOS de l'ordinateur » enregistré par le service « station de travail » de l'ordinateur « client »
Computername <03>	Ce nom de machine est enregistré par le « service des messages » (Messenger service) afin de pouvoir recevoir des messages « net send *nom_machine* ». Ces noms de « messagerie Windows » existent au nom de deux : un pour l'ordinateur et l'autre pour l'utilisateur connecté.
Username <03>	Ce nom d'utilisateur est enregistré par le « service des messages » (Messenger service) afin de pouvoir recevoir des messages « net send *nom_utilisateur* ». Ces noms de « messagerie Windows » existent au nom de deux : un pour l'ordinateur et l'autre pour l'utilisateur connecté. Si vous vous connectez avec le même login sur deux machines en même temps, alors vous ne recevrez le message que sur la première machine connecté du fait de l'unicité des noms NetBIOS.
Computername	Ce nom est enregistré par le service « serveur » afin de permettre au client de se connecter à la machine pour accéder aux partages.
Workgroup or domainname <00>	C'est un nom de groupe de travail ou de domaine. Il est forcément le même sur toutes les machines d'un groupe ou domaine.
Workgroup or domainname <1E>	C'est un nom de groupe de travail ou de domaine utilisé pour l'élection de « Maître explorateur local ».
Domainname <1B>	Enregistre l'ordinateur local comme « Maître explorateur » de groupe de travail ou domaine. Ce nom est donc unique (associe une IP).
Domainname <1C>	Enregistre l'ordinateur local comme « Contrôleur de domaine ». Ce nom est donc unique (associe une IP).
Workgroup or domainname <1D>	Enregistre l'ordinateur local comme « Maître explorateur local au sous réseau » de groupe de travail ou domaine. Ce nom est donc unique (associe une IP). Si un domaine/groupe de travail recouvre plusieurs sous réseaux, on doit mettre un « Maître explorateur » par sous réseau pour répondre aux requêtes broadcast des clients.
__MSBROWSE__.<01>	Sert à annoncer le domaine ou le groupe de travail, par un mécanisme de concaténation avec un nom de domaine ou de groupe de travail géré par le protocole, aux masters browsers des autres domaines et groupes de travail.

VIII. Et iptables dans tout ça

Il est nécessaire de ne laisser accéder au serveur que les clients autorisés et surtout pas Internet.

Il nous faut donc les règles suivantes :

```
# EPMAP : toutes les RPC pour Windows
iptables -A INPUT -p tcp --dport 135 -s adresse_réseau_local -j ACCEPT
iptables -A INPUT -p udp --dport 135 -s adresse_réseau_local -j ACCEPT
# NetBios-NS : service de résolution des noms NetBIOS
iptables -A INPUT -p tcp --dport 137 -s adresse_réseau_local -j ACCEPT
iptables -A INPUT -p udp --dport 137 -j ACCEPT,
# NetBios-DGM : exploration du réseau (basé sur SMB browser service)
iptables -A INPUT -p udp --dport 138 -s adresse_réseau_local -j ACCEPT
# NetBios-SSN : partage fichiers, imprimantes par Microsoft
iptables -A INPUT -p tcp --dport 139 -s adresse_réseau_local -j ACCEPT
# SMB/IP => partage fichiers, imprimantes par SaMBa
iptables -A INPUT -p tcp --dport 445 -s adresse_réseau_local -j ACCEPT
iptables -A INPUT -p udp --dport 445 -s adresse_réseau_local -j ACCEPT.
```

IX. Bibliographie

Samba -- Opening Windows to a Wider World

Mise en place de **Samba** sous Linux

Installation de **Samba**

Système antivirus sur un serveur **Samba**

Ajout d'une imprimante **Samba** (SMB)

Point and **Print** in **Samba**

IpTables - Mémento : protocoles et ports à ouvrir

Samba and **IPTables**

The Unofficial Samba HOWTO