Formation Samba

Version Beta 0.0.2

Support Instructeur

Eric BERTHOMIER

9 janvier 2006

Table des matières

Table des matières **1**

1 Historique **7**

2 Microsoft : Le voisinage réseau **8**
2.1 A propos . . . 8
2.1.1 Mots clés . . . 8
2.2 L'architecture réseau des systèmes Microsoft . . . 8
2.2.1 NetBIOS : network basic input output . . . 8
2.2.2 CIFS : common internet file system . . . 8
2.2.3 SMB : server message block . . . 8
2.3 Les protocoles . . . 8
2.4 NetBIOS . . . 8
2.4.1 Historique . . . 8
2.5 Obtention d'un nom . . . 8
2.6 Datagrammes et sessions . . . 9
2.6.1 Datagrammes . . . 9
2.6.2 Sessions . . . 9
2.6.3 SMB . . . 9
2.7 swb . . . 9

3 Samba : Introduction **10**
3.1 A propos . . . 10
3.1.1 Mots clés . . . 10
3.1.2 Fichiers . . . 10
3.2 Présentation de Samba . . . 10
3.3 Orgine du nom . . . 10
3.4 smbd : server message block . . . 10
3.5 nmbd : netbios name server . . . 11

4 Mise en oeuvre rapide d'un serveur Samba **12**
4.1 A propos . . . 12
4.1.1 Mots clés . . . 12
4.1.2 Fichiers . . . 12
4.2 Prélude : Ports utilisés . . . 12
4.3 Installation de Samba . . . 13
4.3.1 Notes sur la compilation . . . 13
4.3.2 Installation par RPM . . . 13
4.4 Démarrage automatique . . . 14
4.5 La configuration élémentaire du serveur . . . 14

Document sous licence FDL

4.5.1 Description des différents élements du fichier de configuration 14
4.6 Configuration d'un poste client 15

5 Outils de configuration : vi, swat ou webmin 16
5.1 A propos 16
5.1.1 Mots clés 16
5.1.2 Fichiers 16
5.2 Introduction 16
5.3 vi 16
5.4 swat 16
5.4.1 Utilisation de swat 17
5.5 Webmin 18
5.5.1 Installation 18
5.5.2 Sécurisation de Webmin 18
5.5.3 Configuration de Samba 19
5.6 Conclusion 20

6 Structure du fichier de configuration 21
6.1 A propos 21
6.1.1 Mots clés 21
6.1.2 Fichiers 21
6.2 Relecture du fichier de configuration 22
6.3 Structure 22
6.3.1 Espace, guillemet et virgule 22
6.3.2 Casse des caractères 22
6.3.3 Continuation de ligne 22
6.3.4 Les commentaires 22
6.4 Variables de substitutions 22
6.5 Sections spéciales 22
6.5.1 [global] 22
6.5.2 [homes] 22
6.5.3 [printers] 23
6.6 Spécifications 23
6.7 Mise en application : Configurations de base 23
6.7.1 Paramètres globaux 23
6.7.2 Configuration d'un partage 23

7 Droits et attributs des fichiers avec MS-DOS et Unix 24
7.1 A propos 24
7.1.1 Mots clés 24
7.2 Les droits DOS 24
7.2.1 Travaux Pratiques 25
7.3 Masques de création 25
7.4 Mise en application : création d'un répertoire Public 26
7.5 Mise en application : Répertoire privilégié 26

8 Imprimantes partagées sous Linux Samba 28
8.1 A propos 28
8.1.1 Mots clés 28
8.2 Introduction 28
8.3 Mécanisme d'impression 28

Document sous licence FDL

8.4 Impression de Windows vers une imprimante définie sous Linux . . . 28
8.4.1 Une imprimante . . . 28
8.4.2 Utilisation des imprimantes déclarées . . . 29
8.4.3 Impression sous RedHat . . . 29
8.5 Test . . . 29
8.5.1 LprWizard . . . 29
8.6 Impression de Linux vers une imprimante définie sous Windows . . . 30
8.7 CUPS . . . 30

9 Paramètres Security **32**
9.1 A propos . . . 32
9.1.1 Mots clés . . . 32
9.1.2 Fichiers . . . 32
9.2 share . . . 32
9.3 user . . . 33
9.4 server . . . 33
9.5 domain . . . 33
9.6 ads . . . 33

10 Configuration avancées **34**
10.1 A propos . . . 34
10.1.1 Mots clés . . . 34
10.1.2 Fichiers . . . 34
10.2 Création d'un répertoire personnel explicite . . . 34
10.3 Création d'un partage public après authentification . . . 34
10.4 Accès public . . . 35
10.5 Réseaux multiples . . . 35
10.5.1 remote announce . . . 35
10.5.2 remote browse sync . . . 36
10.6 Synchronisation des mots de passe . . . 36
10.7 Socket options . . . 36

11 Contrôle des accès sous Samba **37**
11.1 A propos . . . 37
11.1.1 Mots clés . . . 37
11.1.2 Fichiers . . . 37
11.2 Utilisateurs . . . 37
11.2.1 Authentification . . . 37
11.2.2 Partage . . . 38
11.2.3 Superuser . . . 38
11.3 Réseaux . . . 38
11.3.1 Charge . . . 38
11.3.2 Hosts . . . 38

12 Bind **39**
12.1 A propos . . . 39
12.1.1 Mots clés . . . 39
12.1.2 Fichiers . . . 39
12.2 Introduction . . . 39
12.3 Options de bind . . . 39
12.4 Explications de quelques termes du fichier de configuration . . . 40

Document sous licence FDL

12.4.1 /var/named/root 40
12.4.2 /var/named/zone/127.0.0 40
12.5 Description d'un fichier de zone 40
12.5.1 Entête 40
12.6 Configuration en DNS Cache 41
12.7 Configuration en DNS Secondaire 41
12.7.1 Description 41
12.8 Configuration en DNS Primaire 41
12.8.1 Fichier de zone du domaine 41
12.8.2 Détail d'un enregistrement de la zone 42
12.8.3 Fichier de résolution inverse 42
12.9 Utilisation de dig 43
12.9.1 Exemples d'utilisation de dig 43
12.9.2 Obtention de la version de bind 43
12.10 Utilisation de nslookup 44
12.10.1 Recherche directe 44
12.10.2 Recherche inverse 44
12.11 Debug 44

13 Samba en Contrôleur Principal de Domaine 45
13.1 A propos 45
13.1.1 Mots clés 45
13.2 Introduction 45
13.3 Modification de smb.conf 46
13.4 Eléments de configuration 47
13.5 Travaux Pratiques 47
13.6 Ajout de compte de machine 47
13.7 Debug 48
13.7.1 Fichier lmhosts 48
13.7.2 Réinitialisation du domaine 48
13.8 Script de connexion 48
13.8.1 Exemples 49
13.8.2 Création d'un script de connexion 49
13.9 Samba en tant que serveur membre de domaine 49

14 Mise en place du support des ACLs sur Linux[1] 50
14.1 A propos 50
14.1.1 Mots clés 50
14.1.2 Fichiers 50
14.2 Procédure avec le noyau 2.4.25 50
14.3 Mise en fonction 51
14.4 Vérification 51
14.4.1 Visualisation des droits avancés 51
14.4.2 Mise en place de droits 51
14.5 Utilisation des ACLs 52
14.5.1 ACLs minimales 52
14.5.2 ACLs étendues 52
14.5.3 ACLs par défaut 52
14.6 ACLs sur les fichiers 52
14.6.1 Ajout / Modification 52
14.6.2 Suppression 52

Document sous licence FDL

14.7 ACLs sur un répertoire . . . 52
14.7.1 Création . . . 52
14.7.2 Suppression . . . 52
14.8 Sauvegarde . . . 52

15 Mise en place du support des ACLs pour Samba 53
15.1 A propos . . . 53
15.1.1 Mots clés . . . 53
15.1.2 Fichiers . . . 53
15.2 Compilation . . . 53
15.2.1 RedHat . . . 53
15.2.2 Compte-rendu . . . 54
15.3 Fichier de configuration Samba . . . 54
15.3.1 Description des éléments de syntaxe . . . 54
15.4 Joindre le domaine . . . 54
15.5 Démarrez winbindd et tester . . . 55
15.6 Le résultat . . . 55
15.6.1 getent . . . 55
15.6.2 getent group . . . 55
15.6.3 Utilisation des ACLs (droits avancés de Windows) . . . 55
15.7 Authentification Linux par Windows . . . 55
15.7.1 nsswitch.conf . . . 55
15.7.2 /etc/pam.d/system-auth . . . 56
15.8 Accéder à Linux par un compte Windows . . . 56
15.9 Le résultat . . . 56

16 Samba : Debugging 57
16.1 A propos . . . 57
16.1.1 Mots clés . . . 57
16.2 Introduction . . . 57
16.3 Commandes de diagnostics (version courte) . . . 57
16.3.1 Tester le smb.conf . . . 57
16.3.2 Tester l'@IP . . . 57
16.3.3 Tester smbd . . . 57
16.3.4 Tester nmbd . . . 57
16.3.5 Tester d'un client Windows . . . 58
16.3.6 Tester le broadcast . . . 58
16.3.7 Connection à un partage . . . 58
16.3.8 Browsing à partir du DOS . . . 58
16.3.9 Connection à un partage . . . 58
16.4 Paramètre debug level = . . . 58
16.5 Commandes de diagnostics (version originale) . . . 58

17 Outils liés à Samba 65
17.1 A propos . . . 65
17.1.1 Mots clés . . . 65
17.1.2 Fichiers . . . 65
17.2 smbmount . . . 65
17.3 smbfs . . . 65
17.4 smbclient . . . 65
17.5 findsmb . . . 65

Document sous licence FDL

17.6 nmblookup 65

18 Logiciels liés au voisinage réseau Windows **66**
18.1 A propos 66
18.1.1 Mots clés 66
18.1.2 Fichiers 66
18.2 LinNeighborhood 66
18.3 xSMBrowser 66

A OS Level Windows **69**
A.1 A propos 69
A.1.1 Mots clés 69
A.2 Election du Local Master Browser ou Explorateur Maître 69

B Créer un routeur/passerelle sous Linux **70**
B.1 A propos 70
B.1.1 Mots clés 70
B.2 Introduction 70
B.3 Configuration du réseau 70
B.4 Petit script (version Béta) 70

C GNU Free Documentation License **72**
1. APPLICABILITY AND DEFINITIONS 72
2. VERBATIM COPYING 73
3. COPYING IN QUANTITY 73
4. MODIFICATIONS 74
5. COMBINING DOCUMENTS 75
6. COLLECTIONS OF DOCUMENTS 75
7. AGGREGATION WITH INDEPENDENT WORKS 76
8. TRANSLATION 76
9. TERMINATION 76
10. FUTURE REVISIONS OF THIS LICENSE 76
ADDENDUM : How to use this License for your documents 76

Listings **78**

Liste des tableaux **79**

Table des figures **80**

Bibliographie **81**

Index **82**

Document sous licence FDL

Chapitre 1

Historique

Version	Date	Mise à jour
Beta 0.0.1		
Beta 0.0.2	10 Décembre 2004	Correctifs pédagogiques et français

Document sous licence FDL

Chapitre 2

Microsoft : Le voisinage réseau

Document sous licence FDL

2.1 A propos

2.1.1 Mots clés

NETBIOS	Network Basic Input Output
CIFS	Common Internet File System
SMB	Server Message Block

2.2 L'architecture réseau des systèmes Microsoft

2.2.1 NetBIOS : network basic input output

2.2.2 CIFS : common internet file system

2.2.3 SMB : server message block

2.3 Les protocoles

2.4 NetBIOS

2.4.1 Historique

TCP/IP utilise des @IPs (Nombres). NETBIOS utilise des Noms.

1984 IBM crée une interface de programmation pour application (API) pour mettre ses machines en réseau. L'API fournit un cadre rudimentaraire pour la connexion d'une application à un partage distant.**Netbios** a besoin d'un protocole de transport de bas niveau pour transférer les requêtes de machine en machine.

Fin 1985 NetBEUI (NetBIOS Extended User Interface). NetBEUI laisse à chaque machine le soin d'annoncer un nom (jusqu'à 15 car.).

1987 Standard NBT (NetBIOS over TCP/IP) : RFC 1001/1002

2.5 Obtention d'un nom

Une machine qui démarre doit enregistrer son nom, deux solutions :

– serveur NBNS (WINS)
– défense de son propre nom en l'envoyant par broadcast

Il est nécessaire de faire une corrélation entre Nom et @IP. Cette corrélation peut se faire de 2 façons soit par un serveur NBNS, soit par broadcast.

2.6 Datagrammes et sessions

NBT offre deux services : le service session et le service datagramme.

2.6.1 Datagrammes

Primitive	Description
Send Datagram	Envoi d'un paquet vers une machine ou un groupe de machines
Send Broadcast Datagram	Diffusion d'un datagramme à toutes les machines en attente sur "Receive Broadcast Datagram"
Receive Datagram	Réception d'un datagramme en provenance d'une machine
Receive Broadcast Datagram	Attente d'un datagramme en diffusion

FIG. 2.1 – Primitives du service datagramme

2.6.2 Sessions

Primitive	Description
Call	Démarrage d'une session avec une machine à l'écoute.
Listen	Attente d'un appel en provenance d'une machine spécifique ou de toute machine.
Hang-Up	Fin d'un Call.
Send	Envoi de données vers l'autre extrémité.
Receive	Réception de données en provenance de l'autre extrémité.
Session Status	Recherche d'informations sur des sessions spécifiques.

FIG. 2.2 – Primitives du service session

2.6.3 SMB

Une connexion SMB élémentaire se réalise à travers les étapes suivantes :

1. Etablissement d'une session NetBIOS
2. Négociation d'une variante de protocole
3. Définition des paramètres pour la session et établissement d'une connexion à une ressource

2.7 swb

Toutes ces étapes peut être réalisée à l'aide d'un outil nommé `swb.exe` disponible gratuitement sur le site `http://www.securityfriday.com/tools/SWB.html`.

Document sous licence GFDL

Chapitre 3

Samba : Introduction

Document sous licence FDL

3.1 A propos

3.1.1 Mots clés

samba	programme de partage de ressources Linux pour Windows
swat	programme de gestion de samba

3.1.2 Fichiers

/etc/samba/smb.conf	fichier de configuration de samba

3.2 Présentation de Samba

Un serveur Samba offre les services suivants :
- partage d'une ou plusieurs arborescences de répertoires
- partage d'une ou plusieurs arborescences Dfs ([1])
- partage d'imprimantes installées sur le serveur au profit des clients Windows du réseau.
- participation à l'exploration d'un réseau
- authentification des clients se connectant à un domaine Windows
- fourniture ou participation àla résolution de nom WINS (Windows Internet Name Service)

3.3 Orgine du nom

```
{\tt grep -i '^s.*l.*b' /usr/dict/words}
```

3.4 smbd : server message block

Démon qui gère les partages de fichiers et d'imprimantes, ainsi que les authentifications et les autorisations pour les clients SMB.

[1] DFS (Distributed File System) fournit aux utilisateurs un moyen simple d'accéder à des données reparties et distribuées sur un réseau. Un dossier partagé DFS sert de point d'accès à d'autres dossiers sur le réseau.

3.5 nmbd : netbios name server

Démon qui met en oeuvre Netbios Name Service et WINS. Participe également à l'exploration réseau.

Document sous licence FDL

Chapitre 4

Mise en oeuvre rapide d'un serveur Samba

Document sous licence FDL

4.1 A propos

4.1.1 Mots clés

samba	programme de partage de ressources Linux pour Windows
swat	programme de gestion de samba

4.1.2 Fichiers

/etc/samba/smb.conf	fichier de configuration de samba

Le site par définition pour Samba est : `http://www.samba.org`

4.2 Prélude : Ports utilisés

Avant de cherche à tout vent pourquoi votre serveur Samba ne fonctionne pas, voici les ports utilisés par celui-ci :

Port 137	Exploration des réseaux NetBIOS.
Port 138	Service de noms NetBIOS.
Port 139	Opérations sur les partages de fichiers et d'imprimantes.
Port 445	Pour Windows 2k / XP quand NetBIOS sur TCP/IP est activé.

FIG. 4.1 – Liste des ports utilisés par Samba

Rappel Il vous est possible voir les règles de parefeu par la commande `iptables -L` et de descendre celui-ci par `iptables -F`.

4.3 Installation de Samba

Une version de Samba est sans aucun doute disponible sur votre distribution. Pour voir la distribution utilisée, tapez la commande `smbd -V`. Des paquetages précompilés sont disponibles sur le site de Samba mais il vous est possible de même d'utiliser les sources du logiciel et le compiler vous même.
Sous RedHat, la distribution Samba se décompose en 3 packages :

1. samba-common : fichiers utilisés par la partie cliente ET la partie serveur de Samba.
2. samba-client : fichiers utilisés par la partie cliente (permettre à Linux de se connecter sur Windows).
3. samba : fichiers utilisées par la partie serveur.

4.3.1 Notes sur la compilation

La méthode de compilation pour Samba est identique à l'habitude :

1. ./configure
2. make
3. make install

Il est à noter cependant qu'aucune options (ACL par exmple) n'est activé par défaut et qu'il faut indiquer au moment de la configuration (./configure) les options désirées.
Pour se faire, il est nécessaire d'utiliser l'option –with-argument où argument est l'option souhaitée.
Pour obtenir la liste des options possibles la commande `./configure -help | more` vous permettra d'avoir accès à l'aide nécessaire.
Par défaut l'installation de Samba se fait logiquement dans `/usr/local/samba`, il vous est possible de changer celà avec l'option `-prefix=`.

4.3.2 Installation par RPM

– Installer Samba.

Réponse :

```
rpm -ivh .../perl-CGI-*; rpm -ivh .../samba-*
```

– Une fois celui-ci installé, vérifier si les démons NMBD et SMBD sont lancés.

Réponse :

```
ps -ef | grep smb
```

– Lancer Samba à l'aide du fichier de commande `smb` situé dans `/etc/init.d`.

Réponse :

```
service smb start
```

– Vérifier le bon déroulement de samba en vérifiant que ces démons s'exécutent.

Réponse :

Document sous licence FDL

```
ps -ef | grep smb; ps -ef | grep nmb
```

– Utiliser le voisinage réseau de Windows pour trouver votre partage Samba.

4.4 Démarrage automatique

Le fichier `/etc/init.d/smb` nous indique que Samba doit démarrer dans les runlevels 345 or celui-ci n'est aucunement demarrer lors de l'installation par défaut du RPM. La commande `chkconfig -add smb` ne vous sera hélas d'aucun secours car en fait, les choses n'ont été faîtes que de façon faussée. En effet, il existe dans les différents runlevels un fichier d'arrêt de Samba nommé K35smb qui empêche chkconfig de bien s'exécuter.

Pour résoudre le problème, il nous faut donc supprimer l'existant et réinstaller les scripts de démarrage de Samba.

```
rm -f /etc/rc?.d/K35smb
chkconfig --add smb
ls -al /etc/rc?.d | grep smb
```

4.5 La configuration élémentaire du serveur

Le fichier de configuration Samba, `/etc/smb.conf`, est prédéfini sur beaucoup de distribution. De manière à avoir une approche pas à pas, nous allons copier ce fichier afin d'en garder une trace et supprimer le contenu de l'original.

```
mv /etc/smb.conf /etc/smbold.conf
```

Créons le fichier de configuration Samba pour y indiquer le "strict nécessaire" :

```
[global]
   workgroup = METRAN
   encrypt passwords = yes

[test]
   comment = Pour le test uniquement, merci
   path = /tmp
   read only = no
   guest ok = yes
```

4.5.1 Description des différents élements du fichier de configuration

[global]

workgroup = METRAN

encrypt passwords = Nécessaire pour que les Windows 98, NT4 (sp3) Windows 2k, XP et version supérieure.

[test]

comment = Pour le test uniquement, merci

Document sous licence FDL

path = /tmp

read only =

guest ok =

De manière à valider notre fichier de configuration, nous devons utiliser la commande testparm :

```
testparm /etc/samba/smb.conf
```

Du fait du côté sécure de Linux, il est nécessaire de créer un compte utilisateur qui sera utilisé pour l'accès de Windows sur Samba. Pour se faire il faut utiliser la commande `smbpasswd`. A noter qu'il est indispensable de créer l'utilsateur sous forme unixienne avant de pouvoir le créer sous la forme Samba.

Une fois le fichier de configuration écrit, il nous faut indiquer à Samba de redémarrer pour prendre en compte celui-ci. Dans le cas d'une installation "automatisée", il vous est normalement possible d'utiliser la commande `service smb start` ou la commande qui lui correspond /etc/init.d/smb start.
Dans le cas d'une installation compilée, il vous faut soit créer les fichiers d'init, soit démarrer les services manuellement :

```
/usr/local/samba/bin/smbd -D
/usr/local/samba/bin/nmbd -D
```

Il nous reste maintenant à vérifier que tout tourne correctement :

```
smbclient -U% -L localhost
```

smbclient permet de faire une requête sur les partages offerts par une machine Windows. Les paramètres utilisés sont les suivants :

-U Permet de définir un nom d'utilisateur et un mot de passe (suite de %).

-L Permet de définir la machine que l'on désire interroger.

4.6 Configuration d'un poste client

– Indiquer le groupe de travail METRAN et une adresse IP compatible avec votre serveur Samba.
– Créer un compte utilisateur identique à celui de Samba (même mot de passe)

Document sous licence GNU

Chapitre 5

Outils de configuration : vi, swat ou webmin

5.1 A propos

5.1.1 Mots clés

samba	programme de partage de ressources Linux pour Windows
swat	programme de gestion de samba

5.1.2 Fichiers

/etc/samba/smb.conf	fichier de configuration de samba

5.2 Introduction

Le fichier de configuration smb.conf est bien sûr éditable par n'importe quel éditeur de texte classique mais il peut être intéressant (lorsque l'on démarre) d'utiliser des outils pour s'aider dans la configuration. Comme dans toute manipulation liée à un fichier de configuration, la première chose à faire est de copier le fichier smb.conf.

5.3 vi

Vi ou n'importe quel éditeur de texte peut permettre de modifier le fichier de configuration de Samba. L'inconvénient de cette méthode est simplement le risque de réaliser une erreur syntaxique. Pour éviter celà, il est **nécessaire** d'utiliser la commande `testparm` afin de valider le fichier.

5.4 swat

swat est l'outil par excellence de configuration de Samba, pourquoi cette palme offerte à cet outil, est bien simplement parceque celui-ci est développé et livré avec Samba.

Document sous licence FDL

swat est un outil de configuration de Samba par le réseau via le protocole http (Internet). Il est disponible sur le port 901.

Du fait qu'il s'agit d'un service réseau, il est nécessaire de vérifier son accessibilité réseau au niveau de inetd ou xinetd et sa présence dans le fichier /etc/services.

inetd

Il faut s'assurer de la présence de la ligne suivante :

```
swat    stream  tcp nowait.400  root  /usr/sbin/tcpd  /usr/sbin/swat
```

xinetd

Il faut s'assurer que le service swat soit déclaré et permette un accès au réseau, en voici un exemple adapté.

```
# default: off
# description: SWAT is the Samba Web Admin Tool. Use swat \
#        to configure your Samba server. To use SWAT, \
#        connect to port 901 with your favorite web browser.
service swat
{
port = 901
socket_type = stream
wait  = no
only_from = localhost 192.168.2.0/24
user = root
server = /usr/sbin/swat
log_on_failure += USERID
disable = no
}
```

FIG. 5.1 – Swat

Vous remarquerez que les paramètres de sécurité impose l'utilisation en localhost, ceci pour la simple raison que l'authentification se fait en HTTP donc en clair sur le réseau. Merci donc pour les hackers.

Document sous licence FDL

5.4.1 Utilisation de swat

Depuis quelques versions, swat a rajouté une version Wizard qui vous permet de paramétrer en un clic votre Samba dans la configuration que vous désirez. Sinon, swat dispose des éléments suivants :

Home Documentation de Samba, livré avec Samba ;-)

Globals Vous permet de définir et de visualiser les paramètres globaux de votre serveur Samba.

Shares Vous permet de définir et de visualiser les partages.

Printers Vous permet de définir les imprimantes partagées (se doivent d'être déclarées sur le Linux)

Wizard Vous permet de vous créer une base de serveur Samba en fonction du type de service déésiré (Poste de Travail, Contrôleur de domaine).

Status Vous permet de connaître l'état de santé de votre serveur et les connexions en cours.

View Vous permet de voir votre fichier de configuration : version simplifiée ou complète.

Password **Server Password Management** vous permet de créer/supprimer, valider/invalider des utilisateurs.

Client/Server Password Management vous permet de changer le mot de passe associé à un utilisateur sur une machine cliente distante.

5.5 Webmin

Webmin est logiciel libre multi-os qui permet d'administrer une machine à distance via une interface Web mais avec la possibilité

5.5.1 Installation

Allez sur le site de webmin (`http://www.webmin.com`[1]) et télécharger le dernier RPM de cet outil d'administration.

– Installer le package.

Réponse :

```
rpm -ivh webmin*
```

– Démarrez webmin :

1. `cd /etc/webmin`
2. `./start`
3. Connectez vous avec votre compte root sur l'interface web : `http://127.0.0.1:10000`.
4. Ouvrir une interface web, indiquez l'adresse `http://127.0.0.1:10000`.
5. Changez le langage en Breton (euh en Français).

– Explorez.

5.5.2 Sécurisation de Webmin

Administrateur

Modifier le mot de passe et le nom de **l'utilisateur administrateur webmin** (root par défaut) pour la connexion au serveur Webmin : Utilisateur Webmin, cliquez sur root, remplacer `Unix Authentification` par `Remplacé par` dans la section mot de passe
remplacer le nom d'utilisateur root par admin par exemple.

Cryptage

– Installer la bibliothèque OpenSSL si celà n'est pas déjà fait.

– Modifier au besoin le fichier `miniserv.conf` de manière à activer la prise en charge de ssl (`ssl=1`).

– Télécharger la bibliothèque PERL nécessaire à la sécurisation de Webmin

[1] le .org était déjà pris

Document sous licence FDL

`http://www.symlabs.com/Offerings/Net_SSLeay/`.

1. Décompresser celle-ci avec la commande tar : `tar xvzf ...`
2. Aller dans le répertoire nouvellement créé.
3. Installer la bibliothèque à l'aide des commandes suivantes :
   (a) `perl Makefile.PL` **ou** `perl Makefile.PL -t` si vous êtes connecté à Internet.
   (b) `make install`

Attention : Ceci nécessite le compilateur C (voir *"Installation des outils de programmation"* **et** le package openssl-devel.

– Une fois l'installation terminée, se rendre dans la configuration de Webmin et cliquer sur chiffrage SSL. Sélectionner `Redirect non-SSL requests to SSL mode? O` de manière à passer toujours en https lors de vos connexions à Webmin.

Note : Un package contenant cette bibliothèque existe mais ne donne pas satisfaction (voir site de l'auteur).

5.5.3 Configuration de Samba

Dans le menu Serveur, cliquer sur le menu "Partage Windows avec Samba". A noter la présence de l'onglet "Configuration du module" qui permet d'adapter le module Webmin à VOTRE configuration de Samba. Les menus sont standards et nous découvrirons toutes les fonctionnalitées indiquées un peu plus tard, quelques notes cependant sur certains menus :

Créer une nouvelle copie

Permet d'avoir 2 répertoires de noms différents pointant sur le même espace disque.

Options réseau Unix

Permet de définir la configuration réseau au niveau de Linux.

Options réseau Windows

Permet de définir les configurations globales au niveau de Samba.

Convertir des utilisateurs

Permet de synchroniser la liste des utilisateurs Unix en utilisateurs Samba.

Synchrinisation Utilisateur

Webmin peut être configuré de telle sorte que la liste d'utilisateurs Unix sera automatiquement utilisée pour la liste d'utilisateurs Samba. **Ceci ne marchera que si le module Webmin Utilisateurs et Groupes est utilisé pour ajouter, effacer ou modifier des utilisateurs Unix**

Add and edit Samba groups ET Configure automatic Unix and Samba group synchronisation

Utilisable dans le cas des ACLs uniquement (hors cours).

Document sous licence FDL

5.6 Conclusion

Les outils de configuration peuvent être un bon moyen de démarrer mais ceux-ci ne remplacent en aucun cas la nécessité de connaître les composants essentiels du fichier de configuration Samba.

Document sous licence FDL

Chapitre 6

Structure du fichier de configuration

6.1 A propos

6.1.1 Mots clés

samba	programme de partage de ressources Linux pour Windows
swat	programme de gestion de samba

6.1.2 Fichiers

/etc/samba/smb.conf	fichier de configuration de samba

Nous allons voir la structure du fichier de configuration dont voici un exemple :

```
[global]
   workgroup = METRAN
   encrypt passwords = yes
   wins support = yes
   log level = 1
   max log size = 1000
   read only = no

[homes]
   browseable = no
   map archive = yes

[printers]
   path=/var/tmp
   printable = yes
   min print space = 2000

[test]
   comment = Pour le test uniquement, merci
   path = /tmp
   read only = no
   guest ok = yes
```

Document sous licence FDL

6.2 Relecture du fichier de configuration

La relecture du fichier de configuration se fait automatiquement par Samba toutes les 60 secondes, il est possible de forcer cette relecture par l'appel de la commande système `killall -HUP smbd nmbd`.

6.3 Structure

Les noms placés ente [...] délimitent les sections. Chaque section correspond à un partage sauf la section [global] qui correspond au parmètre du serveur Samba.
Chaque section contient des options spécifiques initialisées par affectation. La plupart du temps ces options ont des valeurs par défaut.

6.3.1 Espace, guillemet et virgule

Les espaces compris à l'intérieur d'une valeur sont significatifs, ils permettent de séparer différentes valeurs. Ces espaces peuvent être remplacés par une virgule.

6.3.2 Casse des caractères

La casse des caractères n'est pas importante sauf dans le cas d'accès au système Linux (chemin de fichier notamment).

6.3.3 Continuation de ligne

Il est possible de scinder une ligne en 2 par un \.

6.3.4 Les commentaires

Les commentaires sont précédés par un #.

6.4 Variables de substitutions

Une nouvelle instance de smbd est crée pour chaque client connecté, chaque client peut donc disposer d'un fichier de configuration sur mesure. Une variable commence par le caractère % suivi d'une lettre unique majuscule ou majuscule.

6.5 Sections spéciales

6.5.1 [global]

Permet de définir les options générales du serveur et la définition des options communes à tous les partages, sauf si elles sont redéfinies à l'intérieur d'un partage.

6.5.2 [homes]

A l'image de la connexion Linux d'un utilisateur, il est possible de réaliser via ce partage, un accès sur le répertoire personnel de l'utilisateur Linux/Samba.

Document sous licence FDL

6.5.3 [printers]

Permet de créer un partage des imprimantes définies dans /etc/printcap.

Attention cependant : si un utilisateur et une imprimante ont le même nom, le seul partage visible sera le compte utilisateur.

6.6 Spécifications

Il est possible de découper ou de remplacer le fichier de configuration courant à l'aide des options suivantes :

config file Lit le fichier de configuration indiqué dans le cas où celui-ci existe, sinon utilise l'actuel.

include Permet d'insérer un partage. Attention, ne fonctionne pas avec les variables %u (utilisateur) ou %P (répertoire racine du répertoire) ou %S (nom du partage courant) qui ne sont pas initialisées au moment où le paramètre include est traîté.

copy Permet de cloner les options du partage indiqué. Ceci permet d'éviter des redondances importantes.

6.7 Mise en application : Configurations de base

6.7.1 Paramètres globaux

```
[global]
   # Paramètres de configuration du serveur
   netbios name = toltec
   server string = Samba %v sur %L
   workgroup = METRAN
   encrypt passwords = yes
   wins support = yes
   os level = 128
```

6.7.2 Configuration d'un partage

```
[data]
   path = /export/samba/data
   comment = Disque de données
   volume = Exemple-de-disque-de-données
   writable = yes
```

Nous allons créer le répertoire concerné : `mkdir -p /export/samba/data`. Puis pour ne pas soulever le problème des droits, nous allons donner tous les droits d'accès sur ce répertoire : `chmod 777 /export/samba/data`.
Nous noterons la présence de l'option `writable = yes` du fait que par défaut tous les partages Samba sont en lecture seule.

Document sous licence FDL

Chapitre 7

Droits et attributs des fichiers avec MS-DOS et Unix

Document sous licence FDL

7.1 A propos

7.1.1 Mots clés

samba	programme de partage de ressources Linux pour Windows
droits	gestion des droits Unix et Windows

7.2 Les droits DOS

Sous Unix, les droits sont composés de 3 triplets (rwx) associés respectivement à l'utilisateur, le groupe et les autres. Sous DOS, les droits sont Lecture Seule, Fichier Système, Fichier caché et Archive.

Lecture seule	Le contenu du fichier ne peut être lu que par l'utilisateur lui-même.
Fichier système	Le fichier tient un rôle spécial dans le fonctionnement du système d'exploitation.
Fichier caché	Le fichier est invisible pour l'utilisateur, sauf s'il demande explicitement de voir les fichiers cachés.
Archive	Le fichier a été modifié depuis la dernière sauvegarde DOS

TAB. 7.1 – Signification des droits DOS

Nous remarquons que ces droits DOS n'ont à part le droit de Lecture Seule aucune corrélation avec les droits Unix. Nous remarquons à contrario, que les droits d'exécution de Unix n'ont aucun sens pour le DOS. De ce fait, les droits d'exécutions de Unix vont servir à indiquer les droits DOS de la façon suivante :

Fichier système	Droit x du groupe
Fichier caché	Droit x des autres
Archive	Droit x du propriétaire

TAB. 7.2 – Translation des droits DOS vers Linux

Ces droits sont gérés au niveau de Samba par les options :

map archive par défaut Yes

map system par défaut No

map hidden par défaut No

Attention : Vous noterez que seul le mapping de l'archive est activé par défaut. D'autre part, pour être valides :

- le map hidden doit être combiné avec un create mask égal au moins à 0001.
- le map system doit être combiné avec un create mask égal au moins à 0011.

7.2.1 Travaux Pratiques

```
# Samba config file created using SWAT
# from 192.168.2.128 (192.168.2.128)
# Date: 2004/07/23 15:43:47

# Global parameters
[global]
netbios name = toltec
server string = Samba %v sur %L
workgroup = METRAN
encrypt passwords = yes
wins support = yes
os level = 128

[data]
create mask = 0755
path = /export/samba/data
comment = Disque de données
volume = Exemple
writable = yes
map archive = yes
map system = yes
map hidden = yes
```

- Modifier votre fichier de configuration Samba pour inclure les spécifications map system et hidden.
- Transférer un fichier de Windows sur Linux/Samba, changer les droits avancés, constater.

Document sous licence FDL

7.3 Masques de création

Ils servent à définir les droits par défaut à affecter à un fichier lors de sa création. Ces masques ont la même structure et la même fonction que les masques d'Unix. Une seule petite différence cependant le droit x n'a un sens pour Samba que si les paramètres map ... ont été définis.
La définition des masques se fait au niveau d'un partage.

Option	Fonction	Valeur par défaut
create mask	masque de création des fichiers	0755
directory mask	masque pour la création des répertoires	0755
force create mode	droits associés pour la création des fichiers	0000
force directory mode	droits associés pour la création d'un répertoire	0000
force group	groupe associé à la création d'un répertoire ou d'un fichier	NA
force user	utilisateur associé à la création d'un répertoire ou d'un fichier	NA
inherit permissions	héritage des droits du répertoire parent pour les nouveaux fichiers et répertoires	no

TAB. 7.3 – Signification des droits DOS

7.4 Mise en application : création d'un répertoire Public

Créer un répertoire partagé à l'aide des commandes suivantes :

– `mkdir /export/samba/public`
– `chmod 777 /export/samba/public`
Ajouter à la section [global] la ligne suivante :

```
guest ok = yes
```

Ajouter la section [public] suivante à votre fichier de configuration Samba.

```
[public]
   comment = Public
   path = /export/samba/public
   browseable = yes
   writable = yes
   create mode = 0666
   directory mode = 0777
```

Pour l'instant, notre répertoire est public pour *tous les utilisateurs déclarés de Samba*, par contre notre machine n'est pas accessible à un inconnu.

Du faire du create mode et du directory mode, chacun peut supprimer à sa guise les fichiers et les répertoires des autres. Il est possible de prévenir (seule une boîte de dialogue indiquant que le fichier est en lecture seule apparaît) en utilisant le sticky bit (`chmod +t`) sur le répertoire /export/samba/export.

Pour rendre le répertoire accessible à **TOUS** les utilisateurs même non déclarés sur le système, il est nécessaire d'indiquer dans les paramètres [global] `security = share` comme indiqué dans la documentation de `guest ok = yes`.

L'interaction que nous venons de constater entre Samba et Linux ne s'arrête pas là et peut nous permettre de réaliser une gestion au niveau de groupes d'utilisateurs ou même d'utilisateurs.

7.5 Mise en application : Répertoire privilégié

Le but de cette manipulation va être de créer un partage accessible uniquement à un groupe d'utilisateurs.

Document sous licence FDL

Créer le groupe stage : `/usr/bin/groupadd stage`

Créer les utilisateurs tux et beastie : `adduser tux ; adduser beastie ; smbpasswd -a tux ; smbpasswd -a beastie`

Ajouter les utilisateurs tux et beastie à ce groupe : `vi /etc/group ; stage :x :502 :tux,beastie`

Créer un répertoire stage accessible au groupe : `mkdir /export/samba/stage ; chown tux.stage /export/samba/stage ; chmod 770 /export/samba/stage`

```
[stage]
comment = Stage
path = /export/samba/stage
valid users = @stage
public = no
writable = yes
create mask = 0660
directory mode = 0770
force group = stage
```

La directive `valid users` nous permet d'indiquer que seuls les membres du groupe stage peuvent accéder à ce partage.

Document sous licence FDL

Chapitre 8

Imprimantes partagées sous Linux Samba

Document sous licence FDL

8.1 A propos

8.1.1 Mots clés

samba	programme de partage de ressources Linux pour Windows
imprimantes	serveur d'impression

8.2 Introduction

Samba permet à la fois de partager des imprimantes configurés sur le linux mais aussi d'imprimer sur des imprimantes connectées à Windows.

8.3 Mécanisme d'impression

Le pilote d'impression va transformer le fichier que l'on désire imprimer en un fichier compréhensible par l'imprimante. De ce fait, il ne faut pas installer de pilotes d'impression au niveau du serveur Samba mais au niveau des postes clients. Il peut bien sûr être utile d'installer des pilotes d'impression sur le Linux / Samba dans le cas où l'on désire imprimer directement de Linux. Dans ce cas, il faut définir 2 files d'impression, 1 pour les clients distants, 1 pour le local.

8.4 Impression de Windows vers une imprimante définie sous Linux

8.4.1 Une imprimante

```
[printer1]
printable = yes
print command = /usr/bin/lpr -P%p -r %s
printer = imprimante réseau
printing = BSD
path = /var/spool/lpd/tmp
```

L'option essentielle de ce partage est `printable = yes` qui indique à Samba le fait que l'on est à faire à une imprimante.

%s	Chemin complet sur le serveur vers le fichier à imprimer.
%f	Nom du fichier lui-même (sans le chemin) sur le serveur Samba.
%p	Nom de l'imprimante Unix à utiliser.
%j	Numéro de job d'impression.

TAB. 8.1 – Variables pour l'impression

8.4.2 Utilisation des imprimantes déclarées

Le partage [printers] permet l'utilisation de toutes les imprimantes déclarées.

```
[printers]
printable = yes
printing = BSD
printcap name = /etc/printcap
print command = /usr/bin/lpr -P%p -r %s
printer = imprimante réseau
path = /var/spool/lpd/tmp
min print space = 2000
```

L'option `min print space` permet de contrôler qu'un espace de 2Mo est disponible sur le répertoire de path pour lancer l'impression.

Attention : Dans le cas de l'utilisation d'un répertoire tmp dans `/var/spool/lpd`, il est nécessaire de créer ce partage par les commandes suivantes :

```
cd /var/spool/lpd
mkdir tmp
chmod 777 tmp
```

8.4.3 Impression sous RedHat

Le fichier `/etc/printcap` est généré automatique à l'initialisation de lpd. Il faut donc déclarer notre imprimante dans `/etc/printcap.local` puis relancer l'impression par `service lpd restart`

8.5 Test

```
smbclient //serveur/lp -U username%password
smb: /> print fichier.txt
```

Le fichier fichier.txt peut être un fichier local ou réseau.

8.5.1 LprWizard

Il est possible d'utiliser le gestionnaire Wizard d'impression de Windows en indiquant un partage nommé `[print$]` dans la liste des partages. Ce partage devra contenir les drivers nécessaires pour l'installation de l'imprimante concernée.

Document sous licence FDL

8.6 Impression de Linux vers une imprimante définie sous Windows

Tout d'abord, partager l'imprimante distante sous Windows puis définisser votre imprimante sous Linux de la manière habituelle. La seule chose qui va changer au niveau du fichier de configuration va être le `if=` qui permet de définir l'imprimante en entrée. Ce paramètre va utiliser une fonctionnalité de samba nommée `smbprint`.

```
# /etc/printcap: printer capability database. See printcap(5).
# You can use the filter entries df, tf, cf, gf etc. for
# your own filters. See /etc/filter.ps, /etc/filter.pcl and
# the printcap(5) manual page for further details.

lpR|Lexmark R:\
        :lp=/dev/null:\
        :sd=/var/spool/lpd/R:\
        :mx#0:\
:af=m412:\
:if=/usr/bin/smbprint:\
        :sh:
```

FIG. 8.1 – Déclaration d'une imprimante

Le programme `smbprint` a besoin d'un fichier .config qui va lui donner les accès à l'imprimante Windows. Ce fichier doit être placé dans le répertoire de spool de l'imprimante c'est à dire dans le répertoire désigné par `sd=`.

```
server=serveur
service=OPTRA01_PCL
user="user"
password="motdepasse"
workgroup="workgroup"
```

FIG. 8.2 – Déclaration d'une imprimante de smbprint

Il ne reste plus qu'à redémarrer le serveur d'impression : `/etc/init.d/lpd restart`.

8.7 CUPS

Samba utilise l'utilitaire `smbspool` pour utiliser les imprimantes déclarées par cups. Créer pour celà un lien symbolique nommé smb de cups vers la commande smbspool de Samba :

```
ln -s /usr/local/samba/bin/smbspool /usr/lib/cups/backend/smb
```

Puis envoyer un signal HUP au démon cupsd de CUPS et vérifier la prise en compte de SMB à l'aide de la commande `lpinfo -v`. Le résultat doit contenir une ligne `network smb`.

Enfin, utiliser l'interface Web de cups (`http://localhost:631`) ou la comamnde `lpadmin` pour ajouter l'imprimante :

```
lpadmin -p imprimante -E -v smb://serveur/imprimante -D ''Description''
```

La description de l'imprimante se fait de la façon suivante :

Document sous licence FDL

```
smb://[utilisateur[:mot_de_passe]@]groupedetravail/]serveur/partage_imprimante
```

Document sous licence FDL

Chapitre 9

Paramètres Security

9.1 A propos

9.1.1 Mots clés

samba	programme de partage de ressources Linux pour Windows
swat	programme de gestion de samba

9.1.2 Fichiers

/etc/samba/smb.conf	fichier de configuration de samba

9.2 share

Déconseillé.
Accès à tout le monde, les partages sont protégés par un mot de passe et disponible pour tous ceux qui ont le mot de passe.
Le partage share utilise le couple login/mot de passe du système pour authentifier un utilisateur. Ce login/mot de passe n'est demandé qu'au moment du premier accès au partage, ceci peut être invalidé par l'option `revalidate = yes`. Si en plus de celà le partage est `guest only`, le partage devient libre.

```
# Global parameters
[global]
        workgroup = METRAN
security = share

[testpub]
comment = Partage ouvert à tous
path = /home/testpub
        public = yes
        browseable = Yes
writable = yes
```

Document sous licence FDL

9.3 user

Les utilisateurs possèdent des comptes et des mots de passe et ils en ont besoin pour s'authentifier auprès du serveur avant de pouvoir accéder aux services. Cette authentification s'effectue au niveau serveur : `smbpasswd`. Le login/mot de passe utilisé par défaut sont ceux spécifiés dans Windows pour l'ouverture de session.

9.4 server

Déconseillé.
L'authentification des utilisateurs est délégué à un autre serveur SMB ou à soit même pour devenir serveur. Cette option était largement utilisé dans le temps ou Samba ne pouvait être intégré dans un Domaine.

```
# Global parameters
[global]
        workgroup = METRAN
security = server
password server = *
```

password server : l'option `password server` spécifie une liste de serveurs SMB qui valident le mot de passe. `password server = *` permet de lancer un broadcast afin de savoir quelle est la machine "Contrôleur de domaine".
Il est possible d'utiliser `password server =` avec des noms de machines explicites.

9.5 domain

Samba agit en tant que contrôleur de domaine et contrôle les logins et les machines qui se connectent.

```
# Global parameters
[global]
        workgroup = METRAN
security = domain
```

9.6 ads

L'authentification est réalisée par Active Directory de Windows 2000.

```
# Global parameters
[global]
        workgroup = METRAN
security = ADS
realm = your.kerberos.REALM
password server = your.kerberos.server
```

L'option `realm` permet d'indiquer le nom de domaine Kerberos, il est nécessaire en plus de celà d'indiquer l'adresse du serveur d'authentification auquel on délègue cette authentification.

Document sous licence FDL

Chapitre 10

Configuration avancées

10.1 A propos

10.1.1 Mots clés

samba	programme de partage de ressources Linux pour Windows
swat	programme de gestion de samba

10.1.2 Fichiers

/etc/samba/smb.conf	fichier de configuration de samba

10.2 Création d'un répertoire personnel explicite

L'utilisation de [homes] permet à chaque user déclaré d'avoir son répertoire personnel. Il est possible aussi de le faire pour un utilisateur particulier exemple ici pour eric.

```
[eric]
   comment =  Répertoire personnel de %U
   writable = yes
   valid users = eric
   path = %H
```

Une autre possibilté est de mettre cette partie de script dans un fichier séparé et faire un `include %U`

10.3 Création d'un partage public après authentification

Un partage public permet à n'importe quelle personne authentifiée de déposer / supprimer des fichiser sur ce partage. Afin de se prémunir des droits de chacun des utilisateurs connectés, il est possible d'indiquer à Samba que l'accès à ce partage se fera par le compte invité uniquement. Pour celà nous utiliserons la configuration de partage suivante :

Document sous licence FDL

```
[testpub]
        comment = Partage de test public
        path = /home/testpub
        public = yes
        guest ok = yes
        guest only = yes
guest account = smbguest
        browseable = yes
writable = yes
```

10.4 Accès public

Un partage public ouvrir celui-ci à tout le monde.
Dans le mode de sécurité share, aucun problème car aucune authentification n'est réalisée au départ. Par contre dans les autres modes de sécurité, les problèmes sont plus ardus. En effet `security = user` impose à une personne de s'authentifier à Samba pour pouvoir accéder aux ressources. Or ici dès que Windows se connecte, il se présente comme étant X, X étant le login utilisé avec Windows. Il faut donc ruser et dire que si l'user est inconnu, il faut prendre l'invité. L'option à utiliser pour celà est : `map to guest` qui peut valoir les valeur suivantes :

Never Une connexion d'un utilisateur avec un mot de passe invalide sera purement rejetée. (défaut)

Bad User Un utilisateur avec un mot de passe invalide sera rejeté sauf si l'utilisateur n'existe pas, dans ce cas, il sera traîté comme étant un invité.

Bad Password Un utilisateur avec un mot de passe invalide sera traîté comme un utilisateur invité.

```
# Global parameters
[global]
workgroup = METRAN
guest account = smbguest
map to guest = Bad User

[testpub]
        comment = Partage de test public lecture seule
        path = /home/testpub
        public = yes
        guest ok = yes
        guest only = yes
        browseable = yes
```

Document sous licence FDL

10.5 Réseaux multiples

Samba ne peut être serveur de domaine secondaire ou même serveur wins secondaire, ceci pose un problème concernant les réseaux sur plusieurs sections et notamment les réseaux interconnectés par un VPN (Virtual Public Network).
Pour aider cette mise en oeuvre, deux options sont tout de même disponibles.

10.5.1 remote announce

`remote announce` ajoute des groupes de travail sur lesquels Samba va s'annoncer.

Syntaxe : remote announce = @IP/Groupe.
L'IP peut être un broadcast ou l'adresse du maître d'exploration.

10.5.2 remote browse sync

`remote browse sync` effectue une synchronisation des listes d'explorations avec d'autres explorateurs maîtres du réseau

Syntaxe : remote browse sync = @IP ou Broadcast.

10.6 Synchronisation des mots de passe

A FAIRE

10.7 Socket options

Il est possible de régler les buffers réseaux utilisés par Samba. De manière courante on trouve : `socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192`.

Document sous licence FDL

Chapitre 11

Contrôle des accès sous Samba

Document sous licence FDL

11.1 A propos

11.1.1 Mots clés

samba	programme de partage de ressources Linux pour Windows
swat	programme de gestion de samba

11.1.2 Fichiers

/etc/samba/smb.conf	fichier de configuration de samba

11.2 Utilisateurs

11.2.1 Authentification

Il est possible de créer un tableau de correcpondance entre utilisateurs Windows et utilisateurs Linux en utilisant l'option : `username map =` . Les droits associés à ce fichier doivent être 0744 ou 0644.

Attention : Le mot de passe user et le mot de passe de l'utilisateur emprunté doivent être identiques, en effet le nom est changé mais pas les mots de passe qui leur sont associés.

```
eric = tartenpion
ma = madalton
users = @account
nobody = *
```

TAB. 11.1 – Exemple de fichier de correspondance

Comme nous pouvons le voir dans cet exemple, un groupe Windows peut être aussi couplé avec un groupe Linux (`users = @account`).

Ensuite, l'authentification d'un utilisateur se fait en trois phases :

1. Recherche de l'utilisateur avec la casse fournie
2. Recherche de l'utilisateur avec la casse en minuscules

3. Recherche de l'utilisateur avec la 1ère lettre en majuscule

L'option `username level =` permet d'augmenter le nombre de lettres dont on peut changer la casse.

11.2.2 Partage

Les options `valid users =` et `invalid users =` permettent de spécifier les utilisateurs ayant droit ou non d'accéder aux partages. Cette option peut être appliquée au niveau partage ou au niveau global. Il est possible de spécifier un groupe avec la syntaxe suivante : `@groupe`

Les options `write only =`, et `read list =` permettent de spécifier les utilisateurs qui ont ou non les droits d'écriture sur un partage.

11.2.3 Superuser

Il est possible d'affecter des droits de super-utilisateur à un utilisateur Samba. Pour celà, il faut utiliser l'option `admin users =`.

Attention : l'utilisateur ainsi déclaré possède véritablement les droits de `root`. C'est pour cette raison, qu'il est déconseillé d'utiliser cette option.

11.3 Réseaux

11.3.1 Charge

L'option `max connection =` permet de définir le nombre de connexions maximums pouvant être acceptées pour un partage.

11.3.2 Hosts

Les options `allow hosts` et `deny hosts` permettre d'autoriser ou d'interdire des machines ou des plages d'adresses réseaux.

Document sous licence FDL

Chapitre 12

Bind

12.1 A propos

12.1.1 Mots clés

bind	nom du serveur DNS
named	nom du démon associé
dig	outil d'interrogation des DNS
nslookup	outil d'interrogation des DNS (désuet)

12.1.2 Fichiers

/etc/bind/named.conf	fichier de configuration
/etc/resolv.conf	fichier de configuration pour la résolution des noms

12.2 Introduction

Sous Linux, c'est le démon `named` qui joue le rôle de serveur DNS. Il peut être configuré de 3 façons :
- "caching only" : mise en cache simple
- Primary Master : serveur maître
- Secondary Master : serveur esclave

12.3 Options de bind

```
1  options {
2          directory "/var/cache/bind";
3
4          // If there is a firewall between you and nameservers you want
5          // to talk to, you might need to uncomment the query-source
6          // directive below.  Previous versions of BIND always asked
7          // questions using port 53, but BIND 8.1 and later use an unprivileged
8          // port by default.
9
10         // query-source address * port 53;
11
12         // If your ISP provided one or more IP addresses for stable
13         // nameservers, you probably want to use them as forwarders.
```

Document sous licence FDL

```
14          // Uncomment the following block, and insert the addresses replacing
15          // the all-0's placeholder.
16
17          forwarders {
18                  10.122.1.3;
19                  192.168.220.20;
20          };
21
22          auth-nxdomain no;    # conform to RFC1035
23  };
```

12.4 Explications de quelques termes du fichier de configuration

directory chemin de base pour les fichiers de configuration.

version permet de masquer la version de Bind utilisée et de limiter ainsi l'exploration des failles de sécurité.

zone spécifie la zone de réseau qui sera décrite. `in-addr.arpa` est une zone spéciale qui permet de faire des recherches inverses.
Exemple : pour trouver la machine 192.168.2.2, la requête sera sur 192.in-addr.arpa puis 168.192.in-addr.arpa ...

TTL durée de vie de la zone, exprimée en secondes par défaut. Il est possibile d'indiquer le temps en jour par le suffixe D.

12.4.1 /var/named/root

C'est le fichier de zone des serveurs root.

12.4.2 /var/named/zone/127.0.0

C'est le fichier lié à votre boucle locale, vous devez y déclarer votre machine.

12.5 Description d'un fichier de zone

12.5.1 Entête

```
1   TTL     3D
2   @ IN SOA dns_primaire. adresse_mail. (
3           xxxxxxxx;       serial
4           xxxxx;          refresh
5           xxxxx;          retry
6           xxxxx;          expire
7           xxxxx;          default_ttl
8   )
9
10  @ IN NS serveur.domaine.
```

TTL : Durée de vie **de la zone**.

@ IN SOA dns_primaire. adresse_mail. SOA : Start Of Authority

Document sous licence FDL

dns_primaire : le nom de votre DNS

adresse mail : l'adresse mail de l'administrateur en remplaçant @ par .

serial : Numéro de version de la zone, la syntaxe est souvent AAAAMMJJNN où NN représente le numéro de correctif dans la journée.

refresh : Temps d'attente avant de contrôler un éventuel changement au niveau du DNS primaire (8 chiffres max).

retry : Temps d'attente du serveur secondaire avant de faire à nouveau une demande sur le serveur primaire s'il n'a pas répondu (8 chiffres max).

expire : Temps pendant lequel le serveur secondaire va conserver les données en cache (8 chiffres max).

default_ttl : TTL par défaut **pour les enregistrement** (possibilité d'en définir un par enregistrement).

12.6 Configuration en DNS Cache

Il suffit d'indiquer dans le champs `forwarder` l'adresse IP du ou des serveurs DNS qui contiennent les informations pertinentes.

12.7 Configuration en DNS Secondaire

Il suffit d'indiquer pour la zone concernée les informations suivantes :

```
1 zone mazone.org {
2                 type slave
3                 file zone/mazone.org
4                 masters{@IP serveur primaire}
5         }
6 )
```

12.7.1 Description

zone : nom de la zone pour laquelle on est DNS secondaire

type : type de la zone (ici esclave)

file : un nom de fichier, celui-ci sera rempli par le DNS primaire lors des différentes requêtes.

masters : adresse(s) IP du ou des DNS primaires.

12.8 Configuration en DNS Primaire

12.8.1 Fichier de zone du domaine

```
1 $TTL     604800
2
3 @        IN      SOA     serveur.domaine.        root.domaine. (
4                          2003100901      ; Serial
5                          604800          ; Refresh
6                          86400           ; Retry
7                          2419200         ; Expire
8                          604800 )        ; Negative Cache TTL
```

Document sous licence FDL

```
9  ;
10                      NS      serveur.domaine.
11                      MX      10      serveur.domaine.
12
13 serveur              A       192.168.10.2
14 mouette              A       192.168.10.3
```

12.8.2 Détail d'un enregistrement de la zone

Tous les enregistrements ont la forme suivante :

hôte ou wildcard	(ttl)	classe	type	(priorité)	valeur
@		IN	NS		lampion.bi.com.
lampion		IN	A		192.168.2.128

Hôte ou Wildcard : indique si l'on définit une machine ou un ensemble de machines.

Classe : généralement IN (Internet)

Type : type d'enregistrement

A : addresse

CNAME : alias de nom

NS : serveur de nom

MX : serveur de mail

TXT : commentaires

Priorité priorité

Valeur valeur donnée à l'enregistrement

12.8.3 Fichier de résolution inverse

```
1  $TTL    3D
2  @       IN      SOA     serveur.domaine. root.domaine. (
3                          20040408        ; Serial
4                          86400           ; Refresh 3 heures
5                          7200            ; Retry 2 heures
6                          604800          ; Expire
7                          345600 )        ; Negative Cache TTL
8
9  @       IN      NS      serveur.domaine.
10
11 2       IN      PTR     serveur.domaine.
12 3       IN      PTR     mouette.domaine.
```

PTR : enregistrement pointer record

Attention ! Bind est très sensible à la syntaxe et même s'il n'en parait rien, votre DNS peut ne pas fonctionner. Il est donc nécessaire de contrôler votre DNS avec `nslookup` ou `dig`

Document sous licence FDL

12.9 Utilisation de dig

12.9.1 Exemples d'utilisation de dig

- Requête sur le champ "A" du nom www.mondomaine.org auprès du serveur DNS 12.42.112.242 :
  `dig @12.42.112.242 www.mondomaine.org A`
- Requête sur la champ "MX" du nom mondomaine.org auprès du serveur DNS 12.42.112.242 :
  `dig @12.42.112.242 mondomaine.org MX`
- Requête sur tous les champs du nom mondomaine.org auprès du serveur DNS 12.42.112.242 :
  `dig @12.42.112.242 mondomaine.org ANY`
- Requête AXFR sur le domaine mondomaine.org auprès du serveur DNS 12.42.112.242 :
  `dig @12.42.112.242 mondomaine.org AXFR`
- Requête inverse (i.e. reverse DNS) sur l'IP 12.42.111.422 auprès du serveur DNS 12.42.112.242 :
  `dig @12.42.112.242 -x 12.42.111.422`

La sortie de la commande dig est très détaillée ; la réponse à la requête (la partie qui vous intéressera le plus !) se trouve en dessous de la ligne suivante :

```
;; ANSWER SECTION :
```

12.9.2 Obtention de la version de bind

Ici utilisation sur le serveur DNS local :
`dig @127.0.0.1 version.bind txt chaos` donne lieu à cette réponse :

```
1  ; <<>> DiG 9.2.3 <<>> @127.0.0.1 version.bind txt chaos
2  ;; global options:  printcmd
3  ;; Got answer:
4  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13962
5  ;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
6
7  ;; QUESTION SECTION:
8  ;version.bind.                  CH      TXT
9
10 ;; ANSWER SECTION:
11 version.bind.           0       CH      TXT     "9.2.1"
12
13 ;; Query time: 1 msec
14 ;; SERVER: 127.0.0.1#53(127.0.0.1)
15 ;; WHEN: Fri Mar 19 16:10:07 2004
16 ;; MSG SIZE  rcvd: 48
```

La syntaxe utilisée est la suivante : `dig @serveur nom type classe`.

nom : Nom de la ressource de l'enregistrement que l'on désire visualiser.

type : Indique le type de la question qui est sollicité.

classe :

- Ajouter l'option "version "SECRET" dans la section options de BIND. Constater.

Réponse :

```
Le champs version.bind devient SECRET au lieu de 9.2.1.
version.bind. 0 CH TXT "SECRET"
Attention à ne pas oublier de relancer le démon une fois le
fichier de configuration modifié.
```

Document sous licence FDL

```
1 options {
2                 // éRpertoire des fichiers de configuration
3                 directory "/var/named";
4
5                 version "SECRET";
6         };
```

12.10 Utilisation de nslookup

12.10.1 Recherche directe

Ici utilisation sur le serveur DNS local :
`nslookup mouette` donne lieu à cette réponse :

```
Server: 192.168.10.2
Address: 102.168.10.2#53

Name: mouette.domaine
Address: 192.168.10.3
```

12.10.2 Recherche inverse

Ici utilisation sur le serveur DNS local :
`nslookup 192.168.10.3` donne lieu à cette réponse :

```
Server: 192.168.10.2
Address: 102.168.10.2#53

3.10.168.192.in-addr.arpa name=mouette.asfavi.
```

12.11 Debug

Bind 9 arrive avec son coktail de programmes de test, à utiliser sans modération :

named-checkconf	permet de valider la syntaxe du fichier de configuration de named
named-checkzone	permet de valider la syntaxe de la définition d'une zone
rndc	utilitaire de contrôle du démon rndc

Document sous licence FDL

Chapitre 13

Samba en Contrôleur Principal de Domaine

13.1 A propos

13.1.1 Mots clés

samba	programme de partage de ressources Linux pour Windows
contrôleur de domaine	contrôle d'un domaine

13.2 Introduction

Samba gère les principales fonctions d'un contrôleur de domaine :

- connexion au domaine
- authentification pour l'accès aux ressources partagées
- scripts de connexion
- profils errants
- stratégie système

Document sous licence FDL

13.3 Modification de smb.conf

```
# Global parameters
[global]
netbios name = toltec
server string = Samba %v sur %L
workgroup = METRAN
encrypt passwords = yes

; ce qui change ;
domain master = yes
local master = yes
preferred master = yes
os level = 128

; debugging
debuglevel = 1

security = user
domain logons = yes

; logon path fixe l'emplacement du profil errant de Windows NT/2000/XP
logon path = \\%L\profiles\%u\%m
logon script = logon.bat

logon drive = H:

; logon home fixe l'emplacement du répertoire personnel
; et du profil errant de Windows 9x/98/Me
logon home = \\%L\%u\.win_profile\%m

time server = yes

[netlogon]
path = /export/samba/netlogon
writable = no
browsable = no

[profiles]
; NT 2000 XP
path = /export/samba/profiles
browsable = no
writable = yes
create mask = 0600
directory mask = 0700

[homes]
read only = no
browsable = no
guest ok = no
map archive = yes
```

Document sous licence FDL

Samba doit être à la fois l'explorateur maître du domaine ET l'eplorateur local car une tâche dévolue aux PDC Windows NT/2000 et parce que les clients Windows localisent le contrôleur principal de domaine de cette manière.

13.4 Eléments de configuration

security = user indique que la connexion au serveur nécessite un user/mdp valide. Il est possible d'indiquer security=domain lors de la validation des mots de passe pas un contrôleur de domaine externe.

domain logons = yes indique que c'est Samba qui gère les connexions au domaine.

logon path indique le partage ([profiles] dans lequel seront stockés les profils errants.

%L nom du serveur

%u nom de l'utilisateur connecté

logon script nom du script **MS-DOS** à exécuter lors de la connexion d'un utilisateur au domaine. Ce script se trouvera dans le partage [netlogon].

logon drive = H : associe par défaut le lecteur H : au répertoire personnel. (Win NT/XP/2k)

logon home définit l'emplacement du répertoire personnel. Pour Win9x, il définit l'emplacement des profils errants.

time server se définit comme serveur de temps

13.5 Travaux Pratiques

- Créer les répertoires nécessaires sur le serveur Samba :
  - mkdir /export/samba/netlogon
  - chmod 775 /export/samba/netlogon
  - mkdir /export/samba/profiles
  - chmod 777 /export/samba/profiles
- Mettre en application le fichier de configuration défini ci-dessus et utiliser Windows 9x ou Me pour vous connecter au domaine.
- Rechercher les fichiers de profils errants dans le compte personnel de l'utilisateur.

13.6 Ajout de compte de machine

Pour interagir avec Windows XP/2000/NT, il est nécessaire de déclarer chaque machine du domaine. Sous Samba 2.2, l'administrateur du domaine est root, son compte doit être créer par la commande suivante :

```
smbpasswd -a root
```

Par mesure de sécurité, il est préférable de ne pas mettre le même mot de passe que le root Linux.
Pour chacune des machines ; vous dévez déclarer celle-ci sous Linux :

```
/usr/sbin/useradd -d /dev/null -g 100 -s /bin/false -M nommachine$
smbpasswd -m -a nommachine
```

Attention : il y a un $ à la fin du nommachine pour le useradd, celui-ci est absent dans la commande `smbpasswd`.

Document sous licence FDL

13.7 Debug

Il peut arriver que votre Windows refuse de se connecter à votre serveur de domaine pour d'obscures raisons. Pour palier à ce problème, 2 petites astuces sont utilisables : informer le fichier hosts ou lmhosts et annuler le nom du domaine pour le réinsérer par la suite.

13.7.1 Fichier lmhosts

Ce fichier se situe dans le répertoire :

win 9x/3.1x : c :
windows

win NT/2k : c :
windows
system32
drivers
etc

Dans ce fichier insérer en tête des déclarations les lignes suivantes de manière à indiquer où se situe le PDC :

```
@IP NOM #PRE #DOM:NomDuDomaine
```

où @IP est l'adresse IP du contrôleur de domaine et NomDuDomaine et le nom du domaine géré par le contrôleur.

- `#PRE` permet de charger cette information avant la tentative de connexion au serveur de domaine. Ceci permet donc au poste de savoir à qui s'adresser pour se connecter au domaine.
- `#DOM` permet d'identifier le contrôleur de domaine dont il est question, une machine pouvant se connecter à plusieurs domaines.

Le fichier `hosts` Le fichier `hosts` est un fichier contenant une liste de machines et d'adresse IP. Il est comparable au fichier `lmhosts` en de nombreux points sauf qu'il gère la couche IP tandis que le fichier `lmhosts` gère la couche NetBios.

13.7.2 Réinitialisation du domaine

- Sous Windows 9x, la solution trouvée est la suivante, décochez l'authentification à un domaine NT, rebooter, se connecter à la machine en local, rebooter, recocher l'authentification à un domaine NT et là tout roule comme par magie.

- Sous Windows 2k ; changer le nom du domaine, rebooter, réindiquer le bon nom de domaine.

Les 2 méthodes sont sensiblement identiques, je n'indique ici que celles que j'utilise.

13.8 Script de connexion

Au démarrage de la session, un Windows peut exécuter un fichier batch qui lui permettra notamment de connecter des lecteurs réseaux.

Document sous licence FDL

13.8.1 Exemples

1. `net use T: \\toltec\test`
2. `net use H: /home`
3. `net time /set/yes`

13.8.2 Création d'un script de connexion

Le nom du fichier script de connexion est déterminé par `logon script =`, son répertoire est lui défini par le partage [netlogon]. Dans notre configuration le script de connexion doit donc être : `/export/samba/netlogon/logon.bat`

Listing 13.1 – unix2dos.pl

```
1 #!/usr/bin/perl
2 open FILE, $ARGV[0];
3 while (<FILE>) {s/$/\r/; print}
```

13.9 Samba en tant que serveur membre de domaine

La première étape consiste à ajouter le serveur Samba au domaine en lui créant un compte sur le contrôleur de domaine à l'aide des commandes `smbpasswd` :

```
service smb stop
smbpasswd -j DOMAINE -r NOMPDC -Ucompteadmin%motdepasse
```

Il est nécessaire d'arrêter le serveur Samba avant d'exécuter la commande `smbpasswd -j ...`. La seconde étape consiste à modifier le fichier smb.conf :

```
workgroup = METRAN
security = domain
password server = *
```

La seule ligne nécessitant des commentaire est `password server = *`, l'* indique de rechercher le serveur de domaine dans le réseau. Il est possible d'indiquer textuellement ce serveur.

Document sous licence FDL

Chapitre 14

Mise en place du support des ACLs sur Linux[1]

14.1 A propos

14.1.1 Mots clés

acl access control list

14.1.2 Fichiers

Les ACLs sont supportés en natifs par les noyaux 2.6 par contre, il ne le sont pas pour les noyaux de la génération 2.4. Il est donc nécessaire de patcher le noyau 2.4 avec l'un des patchs disponibles sur le site suivant `http://acl.bestbits.at/download.htm`.

14.2 Procédure avec le noyau 2.4.25

1. Installer le noyau dans le répertoire `/usr/src`
2. Renommer le répertoire linux-2.4.25 des sources du noyau en linux-2.4.25.orig

Réponse :

```
mv linux-2.4.25 linux-2.4.25.orig
```

3. Copier le patch dans le répertoire `/usr/src`
4. Installer le patch

Réponse :

```
patch -p0 ea...
```

Document sous licence FDL

5. Exécuter la commande de configuration du noyau

Réponse :

```
make menuconfig
```

6. Dans la section FileSystems, il vous est possible de sélectionner `extended attributes` pour les systèmes de fichiers EXT2 et EXT3.
7. Sélectionner les options complémentaires liées aux ACLs :
   - ExtX extended attribute block sharing
   - ExtX extended user attributes
   - ExtX trusted extended attributes
   - ExtX security labels
   - ExtX POSIX Access Control Lists
8. Dans la dite section, sélectionner si vous le désirez le XFS avec Posix ACL Support
9. Recompiler, installer

14.3 Mise en fonction

Pour activer les ACLs sur une partition déjà montée, utiliser la commande : `mout -o remount,acl /dev/hdaX`.
Pour activer les ACLs automatiquement au démarrage du système, ajouter l'option `acl` dans le fichier fstab.

14.4 Vérification

14.4.1 Visualisation des droits avancés

Se déplacer dans le volume monté avec l'option ACL.

Listing 14.1 – Test des ACLS

```
1 su - root
2 cd /dataacl
3 touch test.acl
4 chmod 600 test.acl
5 getfacl test.acl
```

Ces commandes nous permettent de créer un fichier vide (`touch`) et d'indiquer que seul root aura le droit de lecture écriture sur ce fichier
La commande `getfacl` nous permet de voir les droits fixés sur ce fichier.

14.4.2 Mise en place de droits

Listing 14.2 – Test des ACLs

```
1 login : eric
2 cd /dataacl
3 su - root
4 setfacl -m u:eric:rw test.acl
5 exit
6 touch ''coucou'' > test.acl
```

Document sous licence FDL

En se connectant sous le login eric, nous allons sur le volume monté avec les ACLs, avec les droits root, nous indiquons des permissions “excceptionnelles” pour eric qui lui permettent alors d’écrire dans le fichier (`touch`).

14.5 Utilisation des ACLs

14.5.1 ACLs minimales

Les ACLs minimales représentent le portage des droits unix (owner, group, other).

14.5.2 ACLs étendues

Prolongent les droits des ACLs minimales, elle contient au moins un élément de type texte.

14.5.3 ACLs par défaut

Appliqués aux répertoires pour définir quels droits un objet du système de fichiers devra hérité lors de sa création.

14.6 ACLs sur les fichiers

14.6.1 Ajout / Modification

La commande à utiliser est la suivante : `setfacl -m` avec la syntaxe suivante : `setfacl [ugo] :[user/group/rie`

14.6.2 Suppression

Il est possible de supprimmer les ACLs de manière complète par la commande `setfacl -b fichier` ou de manière détaillée par la commande `setfacl -x [ugh] :[user/group] fichier`.

14.7 ACLs sur un répertoire

Ceci permet de créer des ACLs par défaut lors de la création des fichiers. La syntaxe des commandes est la même que vue précédemment sauf que l’on doit rajouter l’option `d :`.

14.7.1 Création

`setfacl -m d :u :data :rw mon.repertoire`.

14.7.2 Suppression

`setfacl -k mon.repertoire`.

14.8 Sauvegarde

Le logiciel `star` permet de conserver les droits ACLs.

Document sous licence FDL

Chapitre 15

Mise en place du support des ACLs pour Samba

15.1 A propos

15.1.1 Mots clés

acl access control list

15.1.2 Fichiers

15.2 Compilation

Pour que Samba puisse supporter les ACLs, il est nécessaire de recompiler celui-ci avec les options `-with-acl`. La procédure préconisée pour réaliser ceci est d'utiliser le package source, de rajouter l'option et de reconstruire le package avec ainsi le support des ACLs.

Ceci permet de garder la spécificité du package par rapport à l'OS.

15.2.1 RedHat

1. Se rendre sur le site de Samba (`http://www.samba.org`) et télécharger le dernier SRPM disponible.
2. L'installer : `rpm -i samba-x.x.x.src.rpm`
3. Aller dans le répertoire `/usr/src/redhat/SPECS` et visualiser le fichier des spécifications liés à Samba.
4. Rajouter dans le fichier `sambaX.spec` les lignes suivantes dans les directives de construction :
   (a) `--with-acl-support`
   (b) `--with-winbind`
   (c) `--with-winbind-auth-challenge`

Document sous licence FDL

Attention chacune des lignes est suivie d'un \pour indiuquer que la ligne se continue sur la ligne suivante !

5. Reconstruire le package : `rpmbuild -bb sambaX.spec`
6. Aller dans le répertoire `/usr/src/redhat/RPMS/i386` et installer le RPM ainsi généré.

15.2.2 Compte-rendu

L'installation du package samba a permis de mettre en place l'architecture complète du serveur Samba **ET** l'installation de la librairie PAM `pam_winbind.so` dans le répertoire `/lib/security`.

15.3 Fichier de configuration Samba

Il est nécessaire d'ajouter les éléments `winbind` dans la section global au fichier de configuration de Samba :

```
[global]
  security = domain
  workgroup = METRAN
  encrypt passwords = yes
  password server = saturne
  winbind separator = +
  winbind uid = 10000-65000
  winbind gid = 10000-65000
  winbind enum users = yes
  winbind enum groups = yes
```

Si l'on désire en plus pouvoir accéder au Linux via une authentification par Winbind, on rajoutera les éléments suivants :

```
[global]
<...>
template shell = /bin/bash
template homedir = /home/%D/%U
```

15.3.1 Description des éléments de syntaxe

A FAIRE

15.4 Joindre le domaine

Arrêter Samba (`/etc/init.d/smb stop`) et utiliser **l'une** des commandes suivantes pour joindre le domaine :

– `smbpasswd -j DOMAIN -r PDC -U administrateur`
– `net join -U administrateur`

Redémarrez Samba : `/etc/init.d/smb start`

Document sous licence FDL

15.5 Démarrez winbindd et tester

- Lancez winbindd `winbindd`.
- Visualiser les comptes des utilisateurs Windows : `wbinfo -u`
- Visualiser les groupes des utilisateurs Windows : `wbinfo -g`
- Unifier les mots de passe et les groupes entre Linux et Windows :
  - `getent passwd`
  - `getent group`

15.6 Le résultat

15.6.1 getent

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
<...>
toto:x:10047:10047::/home/toto:/bin/bash
<...>
METRAN+ebr:x:10032:10000:Eric BERTHOMIER:/home/BI.COM/ebr:/bin/bash
<...>
```

15.6.2 getent group

```
root:x:0:root
bin:x:1:root,bin,daemon
<...>
METRAN+stagiaire:x:10005:METRAN+Administrateur,METRAN+mgt,METRAN+gmd
```

15.6.3 Utilisation des ACLs (droits avancés de Windows)

```
# file: titi.txt
# owner: BI.COM\ebr
# group: BI.COM\Utilisa. du domaine
user::rwx
user:BI.COM\mgt:rwx
group::---
mask::rwx
other::---
```

Document sous licence FDL

15.7 Authentification Linux par Windows

15.7.1 nsswitch.conf

Modifier le fichier `nsswitch.conf` pour lui demander d'interroger `winbind` en plus des fichiers :

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

15.7.2 /etc/pam.d/system-auth

Modifier le fichier `system-auth` pour lui indiquer qu'il est "suffisant" d'être authentifier par winbind.

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      /lib/security/$ISA/pam_env.so
auth     sufficient   /lib/security/pam_winbind.so
auth        sufficient    /lib/security/$ISA/pam_unix.so use_first_pass likeauth nullok
auth        required      /lib/security/$ISA/pam_deny.so

account     sufficient   /lib/security/pam_winbind.so
account     required      /lib/security/$ISA/pam_unix.so

password    required      /lib/security/$ISA/pam_cracklib.so retry=3 type=
password    sufficient    /lib/security/$ISA/pam_unix.so nullok use_authtok md5 shadow
password    required      /lib/security/$ISA/pam_deny.so

session     required      /lib/security/$ISA/pam_limits.so
session     required      /lib/security/$ISA/pam_unix.so
```

Il est inutile de modifier le fichier `/etc/pam.d/samba`

```
#%PAM-1.0
auth       required pam_nologin.so
auth       required pam_stack.so service=system-auth
account    required pam_stack.so service=system-auth
session    required pam_stack.so service=system-auth
password   required pam_stack.so service=system-auth
```

15.8 Accéder à Linux par un compte Windows

Nous allons créer un compte personnel pour un utilisateur Windows. Comme défini dans le fichier de configuration de Samba (`template homedir = /home/%D/%U`), la forme du répertoire de connexion se devra d'être `/home/domaine/utilisateur`.

- `mkdir /home/METRAN`
- `chmod 755 /home/METRAN`
- `mkdir /home/METRAN/ebr`
- `chown 'METRAN+ebr :METRAN+Utilisa. du domaine' /home/METRAN/ebr`
- `chmod 700 /home/METRAN/ebr`

Il faut en plus de celà l'utilisateur qui pourra authentifier les utilisateurs au niveau du domaine :

```
wbinfo --set-auth-user METRAN+Administrateur%motdepasse
```

15.9 Le résultat

```
login: METRAN+ebr
passwd: mdpdeMETRAN

-bash-2.05b$
```

Document sous licence FDL

Chapitre 16

Samba : Debugging

Document sous licence FDL

16.1 A propos

16.1.1 Mots clés

samba programme de partage de ressources Linux pour Windows

16.2 Introduction

Un fichier de diagnostication de pannes est disponible pour Samba : il s'agit du fichier diagnosis.txt.

16.3 Commandes de diagnostics (version courte)

16.3.1 Tester le smb.conf

Commande : `testparm`

16.3.2 Tester l'@IP

Commande : `ping`

16.3.3 Tester smbd

Commande : `smbclient -L Serveur -N`.
L'option `-N` permet de ne pas indiquer de mot de passe.

Erreurs courantes

error connection g	problème Firewall ou IP
session request failed	hosts deny/allow

16.3.4 Tester nmbd

Commande : `nmblookup -B serveur __SAMBA__`.
Doit retourner votre @IP. L'option `-B` permet de cibler la diffusion.
Exemple : `nmblookup -B lampion __SAMBA__`

16.3.5 Tester d'un client Windows

Commande : `nmblookup -B serveur '*'`
Permet de rechercher un explorateur maître.

16.3.6 Tester le broadcast

Commande : `nmblookup -d 2 '*'` doit retourner "Get a positive answer from ..."
L'option `-d` permet d'indiquer un niveau de debug (ici 2).

16.3.7 Connection à un partage

Commande : `smbclient '//serveur/tmp' -U user` puis `dir`

16.3.8 Browsing à partir du DOS

Commande : `net view`
`serveur`

16.3.9 Connection à un partage

Commande : `net use t: \\serveur\test /user:username`

16.4 Paramètre debug level =

Il est possible de fixer le paramètre `debug level =` dans le fichier smb.conf.

debug level	level
0	critique
1-2	général : connexion / déconnexion
3-5	débug et code source
>=6	développement

TAB. 16.1 – Debug Level

Il est indiqué qu'un `debug level` >=3 ralentit énormément le serveur.
D'autre part, afin de limiter la taille des logs, il est possible d'utiliser `max log size =`. Enfi de manière à cibler les logs, il est possible d'utiliser : `log file` en le fixant par exemple de la façon suivante : log file = /var/log/samba/log.

16.5 Commandes de diagnostics (version originale)

Ce fichier est maintenant disponible sous la forme html dans les sources de Samba (répertoire /docs/html-docs/howto).

```
1 !==
2 !== DIAGNOSIS.txt for Samba release 2.0.7 26 Apr 2000
3 !==
4 Contributor:     Andrew Tridgell
5 Updated:         November 1, 1999
6
```

Document sous licence FDL

```
Subject:          DIAGNOSING YOUR SAMBA SERVER
============================================================================

This file contains a list of tests you can perform to validate your
Samba server. It also tells you what the likely cause of the problem
is if it fails any one of these steps. If it passes all these tests
then it is probably working fine.

You should do ALL the tests, in the order shown. I have tried to
carefully choose them so later tests only use capabilities verified in
the earlier tests.

If you send me an email saying "it doesn't work" and you have not
followed this test procedure then you should not be surprised if I
ignore your email.


ASSUMPTIONS
-----------

In all of the tests I assume you have a Samba server called BIGSERVER
and a PC called ACLIENT both in workgroup TESTGROUP. I also assume the
PC is running windows for workgroups with a recent copy of the
microsoft tcp/ip stack. Alternatively, your PC may be running Windows
95 or Windows NT (Workstation or Server).

The procedure is similar for other types of clients.

I also assume you know the name of an available share in your
smb.conf. I will assume this share is called "tmp". You can add a
"tmp" share like by adding the following to smb.conf:

[tmp]
 comment = temporary files
 path = /tmp
 read only = yes


THESE TESTS ASSUME VERSION 2.0.6 OR LATER OF THE SAMBA SUITE. SOME
COMMANDS SHOWN DID NOT EXIST IN EARLIER VERSIONS

Please pay attention to the error messages you receive. If any error message
reports that your server is being unfriendly you should first check that you
IP name resolution is correctly set up. eg: Make sure your /etc/resolv.conf
file points to name servers that really do exist.

Also, if you do not have DNS server access for name resolution please check
that the settings for your smb.conf file results in "dns proxy = no". The
best way to check this is with "testparm smb.conf"


TEST 1:
-------

In the directory in which you store your smb.conf file, run the command
```

Documents sous licence FDL

```
62 "testparm smb.conf". If it reports any errors then your smb.conf
63 configuration file is faulty.
64
65 Note:    Your smb.conf file may be located in: /etc
66          Or in:    /usr/local/samba/lib
67
68
69 TEST 2:
70 ———————
71
72 run the command "ping BIGSERVER" from the PC and "ping ACLIENT" from
73 the unix box. If you don't get a valid response then your TCP/IP
74 software is not correctly installed.
75
76 Note that you will need to start a "dos prompt" window on the PC to
77 run ping.
78
79 If you get a message saying "host not found" or similar then your DNS
80 software or /etc/hosts file is not correctly setup. It is possible to
81 run samba without DNS entries for the server and client, but I assume
82 you do have correct entries for the remainder of these tests.
83
84 Another reason why ping might fail is if your host is running firewall
85 software. You will need to relax the rules to let in the workstation
86 in question, perhaps by allowing access from another subnet (on Linux
87 this is done via the ipfwadm program.)
88
89
90 TEST 3:
91 ———————
92
93 Run the command "smbclient -L BIGSERVER" on the unix box. You
94 should get a list of available shares back.
95
96 If you get a error message containing the string "Bad password" then
97 you probably have either an incorrect "hosts allow", "hosts deny" or
98 "valid users" line in your smb.conf, or your guest account is not
99 valid. Check what your guest account is using "testparm" and
100 temporarily remove any "hosts allow", "hosts deny", "valid users" or
101 "invalid users" lines.
102
103 If you get a "connection refused" response then the smbd server may
104 not be running. If you installed it in inetd.conf then you probably edited
105 that file incorrectly. If you installed it as a daemon then check that
106 it is running, and check that the netbios-ssn port is in a LISTEN
107 state using "netstat -a".
108
109 If you get a "session request failed" then the server refused the
110 connection. If it says "Your server software is being unfriendly" then
111 its probably because you have invalid command line parameters to smbd,
112 or a similar fatal problem with the initial startup of smbd. Also
113 check your config file (smb.conf) for syntax errors with "testparm"
114 and that the various directories where samba keeps its log and lock
115 files exist.
116
```

Document sous licence FDL

```
117 There are a number of reasons for which smbd may refuse or decline
118 a session request. The most common of these involve one or more of
119 the following smb.conf file entries:
120         hosts deny = ALL
121         hosts allow = xxx.xxx.xxx.xxx/yy
122         bind interfaces only = Yes
123
124 In the above, no allowance has been made for any session requests that
125 will automatically translate to the loopback adaptor address 127.0.0.1.
126 To solve this problem change these lines to:
127         hosts deny = ALL
128         hosts allow = xxx.xxx.xxx.xxx/yy 127.
129 Do NOT use the "bind interfaces only" parameter where you may wish to
130 use the samba password change facility, or where smbclient may need to
131 access local service for name resolution or for local resource
132 connections. (Note: the "bind interfaces only" parameter deficiency
133 where it will not allow connections to the loopback address will be
134 fixed soon).
135
136 Another common cause of these two errors is having something already running
137 on port 139, such as Samba (ie: smbd is running from inetd already) or
138 something like Digital's Pathworks. Check your inetd.conf file before trying
139 to start smbd as a daemon, it can avoid a lot of frustration!
140
141 And yet another possible cause for failure of TEST 3 is when the subnet mask
142 and / or broadcast address settings are incorrect. Please check that the
143 network interface IP Address / Broadcast Address / Subnet Mask settings are
144 correct and that Samba has correctly noted these in the log.nmb file.
145
146 TEST 4:
147 ———————
148
149 Run the command "nmblookup –B BIGSERVER __SAMBA__". You should get the
150 IP address of your Samba server back.
151
152 If you don't then nmbd is incorrectly installed. Check your inetd.conf
153 if you run it from there, or that the daemon is running and listening
154 to udp port 137.
155
156 One common problem is that many inetd implementations can't take many
157 parameters on the command line. If this is the case then create a
158 one–line script that contains the right parameters and run that from
159 inetd.
160
161
162 TEST 5:
163 ———————
164
165 run the command "nmblookup –B ACLIENT '*'"
166
167 You should get the PCs IP address back. If you don't then the client
168 software on the PC isn't installed correctly, or isn't started, or you
169 got the name of the PC wrong.
170
171 If ACLIENT doesn't resolve via DNS then use the IP address of the
```

Document sous licence FDL

```
client in the above test.


TEST 6:
-------

Run the command "nmblookup -d 2 '*'"

This time we are trying the same as the previous test but are trying
it via a broadcast to the default broadcast address. A number of
Netbios/TCPIP hosts on the network should respond, although Samba may
not catch all of the responses in the short time it listens. You
should see "got a positive name query response" messages from several
hosts.

If this doesn't give a similar result to the previous test then
nmblookup isn't correctly getting your broadcast address through its
automatic mechanism. In this case you should experiment use the
"interfaces" option in smb.conf to manually configure your IP
address, broadcast and netmask.

If your PC and server aren't on the same subnet then you will need to
use the -B option to set the broadcast address to the that of the PCs
subnet.

This test will probably fail if your subnet mask and broadcast address are
not correct. (Refer to TEST 3 notes above).

TEST 7:
-------

Run the command "smbclient //BIGSERVER/TMP". You should then be
prompted for a password. You should use the password of the account
you are logged into the unix box with. If you want to test with
another account then add the -U <accountname> option to the end of
the command line. eg: smbclient //bigserver/tmp -Ujohndoe

Note: It is possible to specify the password along with the username
as follows:
        smbclient //bigserver/tmp -Ujohndoe%secret

Once you enter the password you should get the "smb>" prompt. If you
don't then look at the error message. If it says "invalid network
name" then the service "tmp" is not correctly setup in your smb.conf.

If it says "bad password" then the likely causes are:

- you have shadow passords (or some other password system) but didn't
compile in support for them in smbd
- your "valid users" configuration is incorrect
- you have a mixed case password and you haven't enabled the "password
level" option at a high enough level
- the "path =" line in smb.conf is incorrect. Check it with testparm
- you enabled password encryption but didn't create the SMB encrypted
password file
```

Document sous licence FDL

```
227 – The uid for the user in smbpasswd is different from that in /etc/passwd.
228
229 If none of these causes appear to be the problem, check the
230 samba logs in the log directory (typically /usr/local/samba/var) for more details.
231
232 Once connected you should be able to use the commands "dir" "get"
233 "put" etc. Type "help <command>" for instructions. You should
234 especially check that the amount of free disk space shown is correct
235 when you type "dir".
236
237
238 TEST 8:
239 ———————
240
241 On the PC type the command "net view \\BIGSERVER". You will need to do
242 this from within a "dos prompt" window. You should get back a list of
243 available shares on the server.
244
245 If you get a "network name not found" or similar error then netbios
246 name resolution is not working. This is usually caused by a problem in
247 nmbd. To overcome it you could do one of the following (you only need
248 to choose one of them):
249
250 – fixup the nmbd installation
251 – add the IP address of BIGSERVER to the "wins server" box in the
252 advanced tcp/ip setup on the PC.
253 – enable windows name resolution via DNS in the advanced section of
254 the tcp/ip setup
255 – add BIGSERVER to your lmhosts file on the PC.
256
257 If you get a "invalid network name" or "bad password error" then the
258 same fixes apply as they did for the "smbclient –L" test above. In
259 particular, make sure your "hosts allow" line is correct (see the man
260 pages)
261
262 Also, do not overlook that fact that when the workstation requests the
263 connection to the samba server it will attempt to connect using the
264 name with which you logged onto your Windows machine. You need to make
265 sure that an account exists on your Samba server with that exact same
266 name and password.
267
268 If you get "specified computer is not receiving requests" or similar
269 it probably means that the host is not contactable via tcp services.
270 Check to see if the host is running tcp wrappers, and if so add an entry in
271 the hosts.allow file for your client (or subnet, etc.)
272
273
274 TEST 9:
275 ———————
276
277 Run the command "net use x: \\BIGSERVER\TMP". You should be prompted
278 for a password then you should get a "command completed successfully"
279 message. If not then your PC software is incorrectly installed or your
280 smb.conf is incorrect. make sure your "hosts allow" and other config
281 lines in smb.conf are correct.
```

Document sous licence FDL

```
282
283 It's also possible that the server can't work out what user name to
284 connect you as. To see if this is the problem add the line "user =
285 USERNAME" to the [tmp] section of smb.conf where "USERNAME" is the
286 username corresponding to the password you typed. If you find this
287 fixes things you may need the username mapping option.
288
289 TEST 10:
290 ————————
291
292 Run the command "nmblookup –M TESTGROUP" where TESTGROUP is the name
293 of the workgroup that your Samba server and Windows PCs belong to. You
294 should get back the IP address of the master browser for that
295 workgroup.
296
297 If you don't then the election process has failed. Wait a minute to
298 see if it is just being slow then try again. If it still fails after
299 that then look at the browsing options you have set in smb.conf. Make
300 sure you have "preferred master = yes" to ensure that an election is
301 held at startup.
302
303 TEST 11:
304 ————————
305
306 From file manager try to browse the server. Your samba server should
307 appear in the browse list of your local workgroup (or the one you
308 specified in smb.conf). You should be able to double click on the name
309 of the server and get a list of shares. If you get a "invalid
310 password" error when you do then you are probably running WinNT and it
311 is refusing to browse a server that has no encrypted password
312 capability and is in user level security mode. In this case either set
313 "security = server" AND "password server = Windows_NT_Machine" in your
314 smb.conf file, or enable encrypted passwords AFTER compiling in support
315 for encrypted passwords (refer to the Makefile).
316
317
318 Still having troubles?
319 ——————————————————
320
321 Try the mailing list or newsgroup, or use the tcpdump–smb utility to
322 sniff the problem. The official samba mailing list can be reached at
323 samba@samba.org. To find out more about samba and how to
324 subscribe to the mailing list check out the samba web page at
325               http://samba.org/samba
326
327 Also look at the other docs in the Samba package!
```

Document sous licence FDL

Chapitre 17

Outils liés à Samba

17.1 A propos

17.1.1 Mots clés

acl access control list

17.1.2 Fichiers

17.2 smbmount

17.3 smbfs

17.4 smbclient

17.5 findsmb

17.6 nmblookup

Document sous licence FDL

Chapitre 18

Logiciels liés au voisinage réseau Windows

18.1 A propos

18.1.1 Mots clés

LinNeighborhood programme de partage de ressources Linux pour Windows

18.1.2 Fichiers

/etc/samba/smb.conf fichier de configuration de samba

18.2 LinNeighborhood

LinNeighborhood est un logiciel libre téléchargeable à l'adresse suivante :
`http://www.bnro.de/~schmidjo/`

18.3 xSMBrowser

xSMBrowser est un logiciel libre téléchargeable à l'adresse suivante :
`http://www.public.iastate.edu/~chadspen/xsmbrowser.html`

Document sous licence FDL

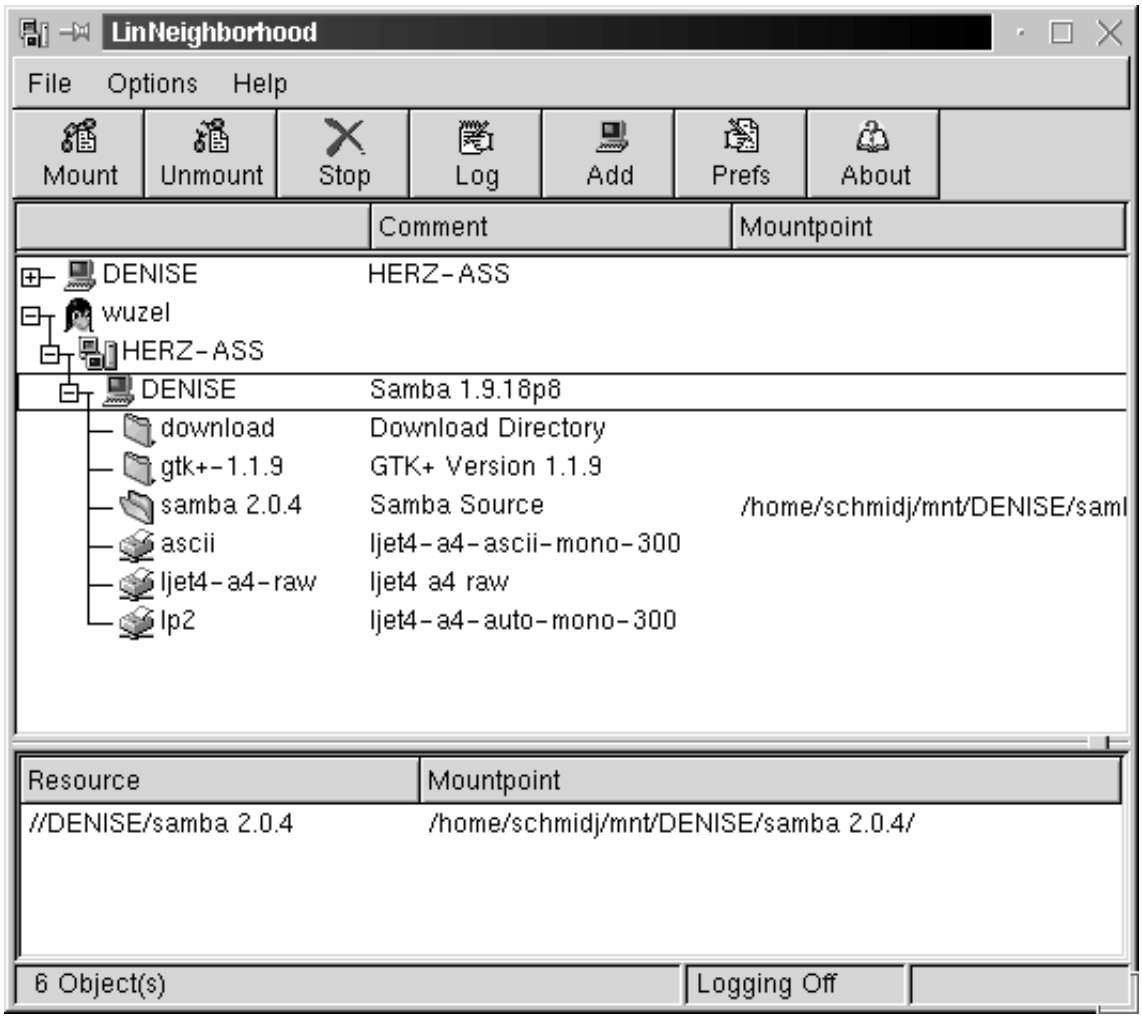

FIG. 18.1 – LinNeighborhood

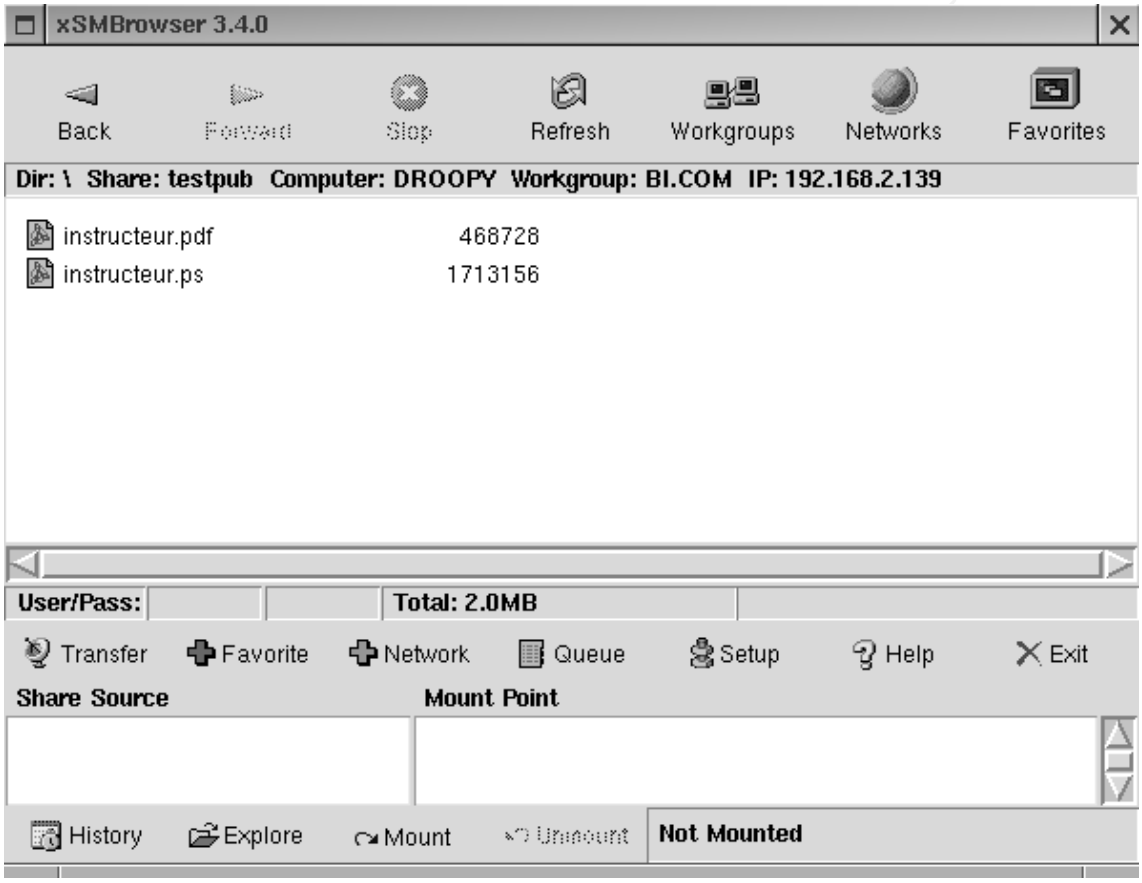

FIG. 18.2 – xSMBrowser

Annexe A

OS Level Windows

A.1 A propos

A.1.1 Mots clés

os level force d'élection d'un os

A.2 Election du Local Master Browser ou Explorateur Maître

Operating System and Configuration	OS Type value
(MS-DOS or Win 3.x, with Microsoft Network Client installed	1
Windows for Workgroups	1
Windows 95	1
Windows 98	1
Windows Me	1
Windows NT 3.x Workstation	16
Windows NT 3.x Server, member server	16
Windows NT 3.x Server, as PDC	32
Windows NT 4 Workstation	16
Windows NT 4 Server, as member server	16
Windows NT 4 Server, as PDC	32
Windows 2K Professional	16
Windows 2K Adv.Server, as member server	16
Windows 2K Adv.Server, as NT-PDC	32
Windows XP Home	16
Windows XP Professional	16

TAB. A.1 – OS Level

Durant une élection, le système avec le plus haut niveau d'OS gagne. En cas d'égalité d'autres facteurs sont utilisés pour déterminer le système gagnant.

Document sous licence FDL

Annexe B

Créer un routeur/passerelle sous Linux

Document sous licence FDL

B.1 A propos

B.1.1 Mots clés

passerelle création d'une passerelle sous linux

B.2 Introduction

Linux est capable de servir de routeur. Le petit script ci-dessous vous permet de réaliser cette tâche.

B.3 Configuration du réseau

Il est nécessaire auparavant de configurer les 2 cartes réseaux pour chacun des deux réseaux distincts que l'on désire lier. Une fois ceci fait le script ci-dessous vous permettra d'activer :

1. la possibilité pour Linux de passer une trame d'une carte à une autre (`echo 1 > ...`).
2. le firewall pour lui indiquer de transférer toutes les trames reçues d'un réseau sur l'autre.

Attention : Ce protocole permet le passage dans un sens uniquement. Le réseau A peut accéder au Réseau B et envoyer/recevoir des requêtes mais le réseau B ne peut accéder au réseau A. Si nous désirions faire celà, il faudrait rajouter une règle de Firewall pour faire faire le transfert.

B.4 Petit script (version Béta)

1. Ecrire le petit script avec votre éditeur de texte favori et l'enregistrer dans le répertoire /etc/init.d.
2. Le rendre exécutable à l'aide de la commande `chmod +x passerelle`.
3. Le rendre actif au démarrage à l'aide de la commande `chkconfig --add passerelle`.

Listing B.1 – passerelle

```
1 #!/bin/sh
2 #
3 # chkconfig: 345 81 35
4 # description: Starts and stops the gateway
```

```
5
6  # Source networking configuration.
7  . /etc/sysconfig/network
8
9  # Check that networking is up.
10 [ ${NETWORKING} = "no" ] && exit 0
11
12 # See how we were called.
13 case "$1" in
14   start)
15         echo -n "Starting gateway services: "
16         echo "1" > /proc/sys/net/ipv4/ip_forward
17         iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
18         ;;
19   stop)
20         echo -n "Shutting down gateway services: "
21         echo "0" > /proc/sys/net/ipv4/ip_forward
22         ;;
23   *)
24         echo "Usage: passerelle {start|stop}"
25         exit 1
26 esac
```

Document sous licence FDL

Annexe C

GNU Free Documentation License

Document sous licence FDL

Version 1.2, November 2002
Copyright ©2000,2001,2002 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom : to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation : a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals ; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The **"Document"**, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as **"you"**. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A **"Modified Version"** of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A **"Secondary Section"** is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus,

if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The **"Invariant Sections"** are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The **"Cover Texts"** are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A **"Transparent"** copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called **"Opaque"**.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The **"Title Page"** means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section **"Entitled XYZ"** means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as **"Acknowledgements"**, **"Dedications"**, **"Endorsements"**, or **"History"**.) To **"Preserve the Title"** of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties : any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts : Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version :

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties–for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another ; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History" ; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included

in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http ://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM : How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page :

> Copyright ©YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation ; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this :

> with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

Document sous licence FDL

Listings

13.1 unix2dos.pl 49
14.1 Test des ACLS 51
14.2 Test des ACLs 51
B.1 passerelle 70

Document sous licence FDL

Liste des tableaux

7.1 Signification des droits DOS 24
7.2 Translation des droits DOS vers Linux 24
7.3 Signification des droits DOS 26

8.1 Variables pour l'impression 29

11.1 Exemple de fichier de correspondance 37

16.1 Debug Level 58

A.1 OS Level 69

Document sous licence FDL

Table des figures

2.1 Primitives du service datagramme 9
2.2 Primitives du service session 9

4.1 Liste des ports utilisés par Samba 12

5.1 Swat 17

8.1 Déclaration d'une imprimante 30
8.2 Déclaration d'une imprimante de smbprint 30

18.1 LinNeighborhood 67
18.2 xSMBrowser 68

Document sous licence FDL

Bibliographie

[1] Erik Bullier. http ://www.LinuxFrench.net.

Document sous licence FDL

Index

Symbols

/etc/resolv.conf 34
/etc/samba/smb.conf . 5, 7, 11, 16, 19, 23, 27, 29, 32, 40, 52, 65

B

bind 34

C

CIFS 3

D

dig 37
DNS
- A 37
- CNAME 37
- expire 36
- MX 37
- NS 37
- PTR 37
- refresh 36
- retry 36
- serial 36
- TTL 36
- TXT 37

DNS Cache 36
DNS Primaire 36
DNS Secondaire 36

G

gateway 65

N

named 34
NETBIOS 3
nslookup 37

O

os level 64

S

samba 5, 7, 11, 16, 19, 23, 27, 29, 32, 40, 52
SMB 3

Document sous licence FDL