Formation Samba 3

Ganaël Laplanche - **http://contribs.martymac.com**, 2005-2010

Ver.	***Auteur***	***Date***	***Description***
1.0	Ganaël LAPLANCHE	01/11/2005	Version initiale
1.1	Ganaël LAPLANCHE	01/11/2006	Relecture et modifications diverses
1.2	Ganaël LAPLANCHE	02/12/2006	Suppr. chaînage passdb backend (Samba v3.0.23)
1.3	Ganaël LAPLANCHE	17/01/2009	Samba 3.2 / GPLv3
1.4	Ganaël LAPLANCHE	14/01/2010	Ajout de la directive 'map to guest'

Table des matières

Avant-propos

Présentation et objectifs du cours

Ce cours a pour objectif de vous présenter Samba 3 de manière pratique. Nous étudierons les fonctions que cette suite logicielle peut remplir et les différents rapports qu'elle entretient avec le monde Microsoft.

A la fin du cours, vous serez capable d'utiliser les fonctionnalités clientes de Samba, de mettre en place un serveur de fichiers autonome, ainsi qu'un contrôleur de domaine. Vous aurez également quelques notions concernant les domaines Microsoft, ainsi que la gestion d'utilisateurs et de groupes en leur sein.

A ces notions techniques s'ajoutent des notions de culture générale autour du projet que nous disséminerons au long de la formation.

La durée prévue du cours est de 6h. Cette durée peut varier d'une personne à une autre, progressez à votre rythme !

Organisation du travail

Le cours est très orienté vers la pratique. Il présente les commandes à saisir au fur et à mesure de leur nécessité, ainsi que les fichiers de configuration à mettre en place. Il n'y a donc pas d'exercices particuliers, le cours lui-même en est-un. Je vous conseille donc de tester chacune des commandes saisies et d'effectuer vous-mêmes les configurations mises en place.

Le cours est découpé en 3 chapitres majeurs : l'utilisation de Samba en tant que client, serveur autonome et contrôleur de domaine. Ces parties sont techniquement indépendantes, mais des notions vues dans un chapitres peuvent être nécessaires au suivant, je vous coneille donc de suivre le cours dans l'ordre.

Le découpage horaire du cours est laissé à votre convenance, mais je vous conseille ceci :

- Chapitres I à V : 2h
- Chapitre VI : 2h
- Chapitres VII à XIII : 2h

Pré-requis

Les pré-requis pour suivre cette formation sont les suivants :

- Maîtriser le shell et les commandes systèmes GNU/linux de base
- Maîtriser la gestion des droits Unix
- Maîtriser la gestion des utilisateurs
- Savoir configurer une imprimante avec CUPS

Pré-requis matériels

Les exercices de ce document nécessitent deux machines :

Une machine cliente Windows XP pro ou 2000 pro
Voici la fiche signalétique de la machine utilisée dans ce document :

- OS : Windows XP
- Adresse IP : 192.168.1.1
- Nom netbios : Windows
- Utilisateur (droits d'administrateur) : martymac

Une machine serveur GNU/Linux, distribution de préférence basée sur Debian
Voici la fiche signalétique de la machine utilisée dans ce document :

- OS : GNU/Linux Ubuntu (**http://www.ubuntulinux.org**)
- Adresse IP : 192.168.1.2
- Nom betbios : ubuntu
- Utilisateur (standard) : martymac

Conventions utilisées dans ce document

Les conventions syntaxiques utilisées dans ce document sont les suivantes :

```
Ceci est le contenu d'un fichier
```

```
# Ceci est une commande exécutée en tant que root (#)
```

```
$ Ceci est une commande exécutée en tant qu'utilisateur standard ($)
```

> *Ceci est une note*

Ceci est un texte standard

Introduction

Samba est un projet libre, développé en C et diffusé sous license GPL v3.

Il est développé depuis 1992 par une équipe de passionnés : la "Samba team", composée d'une trentaine de personnes. L'initiateur du projet se nomme Andrew Tridgell, à l'époque étudiant à l'Université Nationale d'Australie. Son but initial était de pouvoir partager des fichiers entre ses machines DOS et SUN. Il annonce la version 0,5 de son logiciel le 10 Janvier 1992 : "For all those of you who have pathworks for DOS (TCP/IP) but want to be able to use file services from servers other than DecStations and VAXes this may be a solution for you." [...]

Depuis, nombreuses sont les personnes qui se sont intéressées au projet et y ont contribué ! Samba est un projet internationalement reconnu et de plus en plus utilisé dans le domaine professionnel. Sa capacité à fonctionner sur la plupart des systèmes Unix (GNU/Linux, *BSD, Solaris, Aix, HP-UX, ...) y est sans doute pour quelque chose.

L'engouement provoqué par un tel projet lui a vite permi de s'étoffer, si bien que du "simple" partage de fichiers, Samba est devenu une suite d'outils très complets permettant une interconnexion totale avec (principalement) les outils Microsoft.

Fonctionnalités de Samba

Samba est une suite d'outils très complète qui permet l'interconnexion de systèmes "hétérogènes" en implémentant des protocoles réseaux issus du monde propriétaire tels que NETBIOS et SMB/CIFS. La plupart du temps, on utilise Samba pour interconnecter une machine Unix à une machine Windows ou contrôler un domaine.

Cette interconnexion peut se faire à de nombreux niveaux, puisque Samba offre les fonctionnalités suivantes :

- le partage de fichiers
- le partage d'imprimantes
- le support de Netbios
- la gestion de domaines
- de nombreux outils en ligne de commande

On a tendance à dire qu'actuellement, en terme de fonctionnalités, un serveur Samba équivaut à un serveur NT4 (largement) amélioré.

Samba fournit donc à la fois des fonctionnalités serveur (serveur de fichiers, d'imprimantes, contrôleur de domaine, ...) et des fonctionnalités client (connexion à un partage distant, transfert de fichiers, ...). La richesse des outils fournis rendent l'interconnexion bi-directionnelle : une machine Windows peut se connecter à une machine Unix et vice-versa.

Les différentes versions de Samba

Samba est disponible en deux versions majeures :

- La version 2 : il s'agit de l'ancienne version de Samba, remplacée progressivement par la version 3. Cette version ne proposait qu'un support limité de LDAP pour la gestion des comptes utilisateurs et son code devenait difficile à maintenir. Elle est très rarement mise à jour ; des patches de sécurité lui sont parfois appliqués.

- La version 3 : il s'agit de la version actuellement conseillée pour la mise en production de Samba. C'est aussi celle que nous étudierons dans ce document. Elle est très régulièrement mise à jour et corrigée. Elle apporte de nombreuses fonctionnalités par rapport à la version 2 :

- une meilleure gestion des comptes via un système de backends modulaires
- une gestion améliorée des groupes via un mécanisme de mapping
- de nouvelles commandes (commande "net")
- amélioration du support de l'impression
- outils de migration depuis un serveurs NT4 vers un serveur Samba
- support initial d'Active Directory
- [...]

A partir de la version 3.2, évolution naturelle de la version 3, Samba est diffusé sous licence GPL v3.

Nous reviendrons sur ces différentes notions par la suite. Une toute nouvelle version de Samba est en train de voir le jour :

- La version 4 : elle est encore en cours de développement et n'est pas conseillée en production. Il s'agit d'une version totalement réécrite de Samba qui verra le jour très prochainement. Elle devrait notamment apporter le support complet d'Active Directory.

Ce que n'est pas Samba, limites

Nombreux sont ceux qui pensent que Samba peut faire fonctionner des applications Windows sur une machine Unix. Ce n'est pas le cas. Samba fournit "juste" des services réseaux et des moyens de communication entre ces deux mondes.

> *Note : Pour les plus curieux d'entre vous, il existe bel et bien un projet permettant de faire fonctionner une application Windows sur un système Unix. Il s'agit du projet Wine (**http://www.winehq.com**), mais ceci est une autre histoire...*

Il me semble également utile de préciser tout de suite les limites de Samba, afin de mieux cerner cet outil. Nous avons vu que Samba équivalait environ à un serveur NT4 : partage de fichiers, d'imprimantes, contrôle de domaine, etc... avec des fonctionnalités additionnelles, notamment en vue du support d'Active Directory. Il y a tout de même certaines fonctions que Samba ne peut pas (actuellement) remplir :

- Contrôler un domaine Active Directory - il peut en être membre
- Gérer des groupes de groupes - également impossible sous NT4 et Unix
- Etre PDC d'un BDC NT4 - en cours d'implémentation

Rappels et notions de base concernant les domaines NT

Voici des notions très importantes à maîtriser. Il s'agit de notions théoriques et de précisions techniques concernant les domaines Microsoft. Nous les mettrons très souvent en oeuvre durant la mise en place d'un domaine (ou d'un serveur autonome) Samba.

Qu'est-ce qu'un domaine NT ?

Un domaine NT4 est un regroupement logique de différents acteurs et ressources.

Les acteurs sont les suivants :
- des utilisateurs
- des machines
- des groupes

Les ressources sont des partages :
- de fichiers
- d'imprimantes

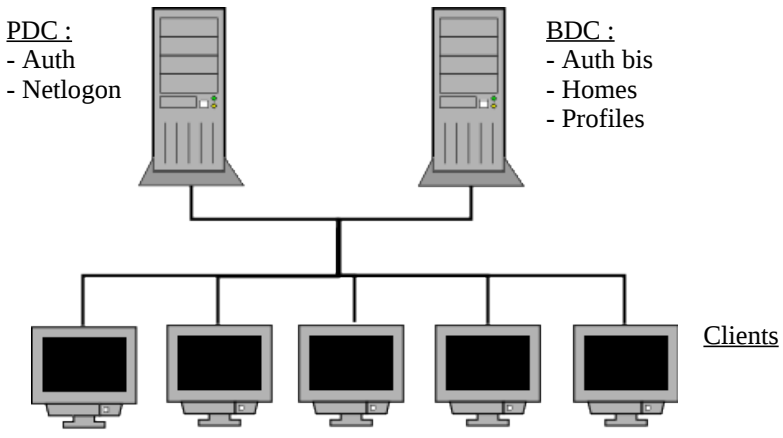
Un domaine permet d'unifier la gestion des droits sur ces ressources pour y autoriser ou non l'accès par ces acteurs. Par exemple, nous dirons que nous aurons la possibilité d'autoriser ou non M.Dupont à accéder à l'imprimante du groupe comptabilité.

Les types de machines mises en jeu dans un domaine

Tous ces éléments sont orchestrés sur le domaine par le contrôleur principal de domaine, souvent appelé PDC (Primary Domain Controler). Il peut être aidé d'un ou plusieurs BDCs, contrôleurs secondaires de domaine (Backup Domain Controler).

Le domaine accueille enfin des machine clientes et des serveurs de fichiers ou d'impression.

Un domaine peut donc être représenté par le schéma suivant :



Un domaine Microsoft

Le rôle de Samba est de permettre à une machine de type Unix de jouer indifféremment l'un ou l'autre de ces rôles dans un domaine.

Les types de comptes mis en jeu dans un domaine

Nous avons évoqué les acteurs suivants : les utilisateurs, les machines et les groupes. Sur le domaine, chacune de ces trois entités est représentée par un compte :

- un utilisateur possède un compte
- un groupe possède un compte
- une machine possède également un compte, celui-ci se termine par un $ (le $ est non visible sous NT). le compte de machine autorise une machine à faire partie du domaine.

> *Note : Les habitués des environnements NT savent qu'il existe deux types de comptes : les comptes globaux et les comptes locaux. Pour simplifier, les comptes globaux sont les comptes disponibles sur le domaine (stockés sur le contrôleur de domaine). Les comptes locaux sont des comptes disponibles uniquement sur une machine donnée.*

Un serveur NT propose un certain nombre de comptes prédéfinis, locaux et globaux, tel le compte Administrateur.

Les SIDs

Un SID (Security IDentifier) identifie un compte de manière unique sur le domaine. Il agit en quelques sortes de la même manière qu'un uid ou qu'un gid sous Unix.

Exemple : **S-1-5-21-4109349211-2507905533-872075644-513**

Le SID est composé de deux parties, le "SID local" et le "RID". Le “SID Local” est la partie du domaine (identique pour tous les acteurs du domaine). Notre domaine ici possède le sid local suivant : **S-1-5-21-4109349211-2507905533-872075644**. Le “RID” est un nombre qui identifie l'acteur au sein du domaine (513 = Utilisateurs du domaine).

De nombreux RIDs sont prédéfinis (les “Well-known RIDs” : 512, 513, 514, 515, [...]) et vont de paire avec les comptes prédéfinis cités ci-dessus. Vous pouvez vous reporter aux adresses suivantes pour plus de détails :

http://msdn.microsoft.com/library/en-us/secauthz/security/well_known_sids.asp
http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/groupmapping.html#WKURIDS

SMB/CIFS, NetBios, késako ?

Le partage de fichiers et d'imprimantes est assuré par le protocole "SMB" (Server Message Block, qui a donné son nom à un logiciel libre très connu, vous avez trouvé ?), renommé en 1996 en "CIFS" (Common Internet File System). Ce protocole est très utilisé dans le monde Microsoft. CIFS peut, ou non, utiliser NetBios (ports 137,138,139). Ceci est souvent le cas mais est en train d'évoluer vers la méthode "Direct-hosted" et l'implémentation de CIFS directement sur TCP/IP (port 445). Fonctionne au niveau des couches 6 et 7 du modèle OSI.

NetBios, "Network Basic Input/Output System", n'est pas un protocole. Il s'agit d'une méthode de communication sur un protocole existant ; c'est en fait une couche intermédiaire entre SMB et un protocole sous-jacent tel que TCP (cf. NBT) ou IPX. Il fournit une méthode de résolution de noms et de services aux couches supérieures. Il utilise un modèle de noms de machines de 15 caractères + 1 caractère de contrôle spécifiant les services offerts par la machines. NetBios a été développé en 1983 par Sytec Inc. pour IBM. A chaque démarrage, une machine Windows

annonce son nom Netbios ainsi que ses rôles (contrôleur de domaine, serveur de fichiers, ...) sur le réseau.

Maintenant que nous possédons les bases techniques concernant les domaines NT, nous allons pouvoir découvrir Samba...

Samba, les premiers pas...

Installation de Samba

Samba peut être installé de différentes manières. Soit en compilant les sources disponibles sur **http://www.samba.org**, soit en installant un (ou des) package(s) compilés pour votre distribution.

La méthode des packages est conseillée car elle vous permettra de mettre à jour votre machine plus simplement par la suite.

L'installation de Samba via des packages se fait de la manière suivante :

```
# apt-get install samba samba-doc samba-common smbfs smbclient
```

De cette manière, la totalité des outils fournis par Samba sont installés.

Découverte de Samba

Samba, nous l'avons vu, fournit un ensemble d'outils permettant à la fois de se comporter en client des réseaux Microsoft ou bien en serveur. Etudions les fichiers principaux éléments de cette véritable "suite logicielle" :

Les binaires "serveurs"

Samba se compose de 3 démons :

- smbd : qui gère les connexions SMB/CIFS (partage de fichiers, impression, ...)
- nmbd : qui gère la couche NetBios (ici résolution de noms)
- winbindd : qui permet à un serveur Unix d'utiliser un serveur NT pour bénéficier de ses comptes localement

Les deux démons les plus utilisés sont smbd et nmbd. Winbindd est utilisé dans des cas très précis ou nous désirons nous connecter sur une machine Unix avec un compte issu d'une machine NT.

Les binaires "clients"

Il s'agit d'outils très divers. Nous en détaillerons certains dans la suite de ce document :

- smbclient
- smbpasswd
- net
- nmblookup
- [...]

Le fichier de configuration smb.conf

La plupart des outils Samba (les serveurs et parfois les outils clients) se réfèrent au fichier de configuration principal de Samba qui est le fichier /etc/samba/smb.conf. Si vous avez installé Samba par le biais de packages binaires, un exemple pré-rempli de ce fichier doit être disponible. La première étape pour utiliser Samba est de renseigner ce fichier, et d'y inclure un minimum d'informations.

Les fichiers de statut

Samba maintient un ensemble d'informations concernant les connexions en cours. Ces fichiers sont des fichiers au format "tdb", une sorte de base de données à plat propre à Samba. Vous n'êtes pas sensés manipuler ces fichiers, mais il est bon de savoir que dans certains cas extrêmes, ces fichiers peuvent être interrogés ou modifiés.

Les fichiers de log

Samba (principalement ses démons) écrivent des informations diverses durant leur activité (erreurs, informations, ...). Il est bon de consulter ces logs régulièrement, ainsi qu'en cas de problème. Le niveau de détail des logs ainsi que leur emplacement est paramétrable dans le fichier smb.conf. Par défaut, ces logs se trouvent dans le répertoire /var/log.

Les pages de man

Samba fournit enfin une documentation très détaillée au travers des pages de man(uels). La page la plus importante est sans nul doute celle concernant le fichier de configuration, très complète. Elle peut être invoquée par la commande suivante :

```
$ man 5 smb.conf
```

Samba en tant que client

Nous allons voir dans ce chapitre comment utiliser les outils clients de Samba pour se connecter à un partage de fichiers, imprimer, ou effectuer des opérations diverses depuis une machine Unix.

Modification du fichier de configuration

La première étape, pour se connecter avec les outils clients est de posséder une version minimale du fichier de configuration /etc/samba/smb.conf. En voici un exemple :

```
[global]

# Nom du workgroup ou du domaine
workgroup = Workgroup
# Nom netbios de la machine
netbios name = ubuntu

# Niveau assez bas (cf élections)
os level = 40

# Nous ne sommes pas contrôleur du domaine
domain logons = no
# Ni collecteur de liste de machines pour le domaine
domain master = no
# Ni collecteur de liste de machines pour le réseau
local master = no
```

Modifiez ou créez ce fichier avec votre éditeur de texte préféré (c'est à dire forcément vi ;-)).

Remarquez la section [global]. Il s'agit d'une section au sein du fichier de configuration. Cette section est celle correspondant à la configuration générale de Samba. Tous les paramètres situés après s'y appliquent.

Remarquez également qu'un commentaire commence par un # ou un ;

Nous étudierons plus en détail par la suite les directives utilisées ici.

Test de la validité de la configuration

Une fois le fichier de configuration créé (ou modifié), vous pouvez vérifier sa validité avec la commande testparm :

```
# testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions

# Global parameters
[global]
        os level = 40
        local master = No
        domain master = No
```

Pensez à utiliser cette commande après chaque modification, ceci évite bien des soucis...

Redémarrage de Samba

Après avoir validé le fichier de configuration, il faut (re)démarrer Samba. Ceci se fait en utilisant le script de démarrage prévu à cet effet dans le répertoire /etc/init.d

Saisissez donc :

```
# /etc/init.d/samba start
```

ou

```
# /etc/init.d/samba restart
```

Note : les outils clients Samba ne nécessitent pas réellement le démarrage des services Samba. De la même manière, le fichier de configuration que nous avons créé ici est en théorie inutile aux commandes clientes. Cependant, par souci de propreté et si nous voulons éviter des problèmes de résolution de noms netbios, ou d'alertes récurrentes à cause de l'absence du fichier de configuration, mieux vaut passer au préalable par ces étapes !

Les commandes clientes Samba

Voici les principales commandes que Samba propose :

- findsmb : permet de lister toutes les machines Windows du réseau
- nmblookup : résoud un nom netbios vers son adresse IP.
- smbstatus : affiche les connexions actuelles.
- rpcclient : client RPC. Envoie une commande RPC à une machine à distance.
- smbclient : à l'instar de ftp, permet de se connecter à un partage de fichiers Windows.
- smbmount : monte un répertoire partagé par Windows ou Samba sur la machine.
- net : commande "à tout faire". Englobe de nombreuses fonctionnalités.

Voici quelques exemples d'utilisation de ces commandes...

Exemples

Lister les partages d'une machine

Pour lister les partages d'une machine (ici nommée "Windows"), nous pouvons exécuter ceci. Le compte "martymac" est utilisé pour se connecter à la machine :

```
$ smbclient -U martymac -L Windows
Password:
Domain=[Workgroup] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       Remote IPC
        Work            Disk
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share

        Server               Comment
```

```
        ---------           -------

        Workgroup           Master
        ---------           -------
```

Se connecter sur un partage de fichiers avec smbclient

La commande smbclient permet de se connecter en lignes de commandes à un partage. Une fois connecté, la commande propose un shell du même type que celui proposé par la commande ftp. Il est possible d'envoyer ou recevoir des fichiers avec les commandes "put" et "get". Vous pouvez afficher la liste des autres commandes disponibles par le biais de la commande "help" :

```
$ smbclient -U martymac  //192.168.1.1/Work
Password:
Domain=[WINDOWS] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]
smb: \> put testparm.txt
putting file testparm.txt as \testparm.txt (11.9 kb/s) (average 11.9 kb/s)
Put file smbclient-l.txt? y
smb: \> quit
```

Monter un partage

Il est possible de monter un partage localement comme on monterait une partition de disque :

```
# mkdir -p /mnt/samba
# smbmount //192.168.1.1/Work /mnt/samba -o username=martymac
Password:
# ls /mnt/samba/
Docs  EOF
```

Lister les imprimantes d'une machine

```
$ net rpc printer LIST -U martymac -S Windows
```

Je vous invite à taper "man net" pour plus d'informations sur les nombreuses fonctionnalités de cette commande ou à saisir "net help".

Imprimer un fichier avec smbspool

La commande smbspool est assez rudimentaire mais permet de lancer une impression. Voici sa syntaxe :

```
smbspool URI {num de job} {utilisateur} {titre} {copies} {options} [fichier]
```

```
$ smbspool smb://martymac:motdepasse@Windows/Imprimante 1 martymac
impression_test 1 "" /etc/crontab
```

Résoudre un nom netbios avec nmblookup

```
$ nmblookup windows
querying windows on 192.168.1.255
192.168.1.1 windows<00>
192.168.245.1 windows<00>
192.168.143.1 windows<00>
```

La cible de toutes ces commandes peut évidemment être une machine Samba ou une machine Microsoft Windows (adresse IP ou nom Netbios). Nous n'allons pas détailler l'utilisation de chaque commande. Pensez surtout à vous documenter en parcourant les pages de man, très utiles et très bien fournies. Pour chaque commande, l'option --help vous donne également une aide précieuse...

Etude approfondie du fichier de configuration

Le fichier de configuration est constitué de sections, déclarées entre [ ], et de directives, de la forme directive = valeur.

Chacune des directives s'applique uniquement à sa section, sauf si elle apparaît dans la section [global] où dans ce cas elle s'applique à toutes les sections.

Certaines directives ne peuvent être employées que dans la section [global], d'autres, dans toutes les sections. Ceci est précisé dans les pages de manuel (man 5 smb.conf).

Certaines sections sont déclarées implicitement par Samba et "réservées". Toute autre section au sein du fichier définit un partage de ce nom.

Comme sous Windows, une section (un partage) qui se termine par un $ est un partage caché.

Les sections réservées

Elles sont sont les suivantes :

- [global] : configuration globale de Samba
- [homes] : répertoires homes des utilisateurs. Cette section crée dynamiquement un partage du nom de l'utilisateur connecté.
- [printers] : section de déclaration d'imprimantes. Cette section crée un partage pour chaque imprimante présente dans le fichier /etc/printcap.
- [IPC$] : partage utilisé pour les commandes RPC
- [ADMIN$] : comme [IPC$]

Traditionnellement, les sections suivantes ont un rôle particulier :

- [profiles] : partage les profils itinérants des utilisateurs
- [netlogon] : partage les scripts de connexion des utilisateur et les stratégies (NTConfig.POL)
- [print$] : partage les drivers des imprimantes

Nous éviterons donc de déclarer l'une ou l'autre de ces sections pour des partages de fichiers !

Exercice : Créez un partage de fichiers et d'imprimantes sur votre machine GNU/Linux et effectuez les manipulations du paragraphe V.D)

Samba en tant que serveur autonome

Exercice : *Le chapitre suivant constitue un exercice à part entière et peut être effectué en même temps que la lecture du document, qui décrit toutes les étapes à mettre en oeuvre.*

Configuration avancée de Samba

Nous avons étudié jusqu'ici la partie cliente de Samba, c'est à dire comment, depuis une machine Unix, se connecter sur une machine Samba ou Windows. Nous allons désormais "passer à la vitesse supérieure" et monter un serveur autonome qui partagera fichiers et imprimante(s).

Une configuration un peu plus avancée pourrait ressembler à ceci :

```
[global]

# Identification Netbios
workgroup = Workgroup
netbios name = ubuntu

# Controle de domaine desactive
os level = 40
domain logons = no
domain master = no
local master = no

# Base de donnee de comptes
passdb backend = tdbsam:/var/lib/samba/mypassdb.tdb

# Authentification via la base de comptes locale
security = user

# Securite
encrypt passwords = yes

# Gestion des logs
log file = /var/log/samba/%m.log
log level = 2

# Serveur de temps activé
time server = yes

# Interdire l'acces a certains fichiers
veto files = /lost+found/.recycle/
```

La section [global] s'est un peu étoffée depuis la première version ! Samba va désormais agir en tant que Serveur autonome, ceci implique plusieurs choses :

- Qu'il partage des données
- Qu'il soit capable de gérer les droits d'accès lors de la connexion à ces partages
- Qu'il soit capable de gérer les droits d'accès au niveau des fichiers partagés (après connexion)

Le fichier smb.conf a donc été complété dans le but de permettre à Samba de gérer ces différents éléments.

Nous retrouvons les directives Netbios ansi que celles relatives à la gestion de domaine que avons déjà utilisées dans la précédente version du fichier smb.conf.

La directive "passdb backend" permet de spécifier où seront stockés les comptes utilisateurs autorisés à se connecter au serveur. Nous avons ici choisi de les stocker dans un fichier de type tdb. Il s'agit d'un fichier de base de données. Nous aurions pu choisir de nombreux autres "backends" tel ldap ou encore mysql. Evitez d'utiliser smbpasswd qui est l'ancien format de fichier utilisé par Samba 2 mais qui n'est plus adapté à la version 3.

La directive "security" permet de sélectionner qui va effectuer l'authentification. Puisque nous avons choisi de maintenir une base de comptes locale, nous spécifions "user", ce qui signifie que Samba va se référer au "passdb backend" spécifié ci-dessus pour authentifier les utilisateurs. Nous aurions pu, dans le cas d'un serveur membre d'un domaine, rediriger les authentifications vers le contrôleur principal de domaine en spécifiant "domain" ou vers un serveur particulier en spécifiant "server". Il existe d'autres possibilités, moins utilisées. N'hésitez pas à vous référer à la page de man du fichier smb.conf.

La directive "encrypt passwords" permet d'activer le chiffrement des mots de passe. Activez-le à chaque fois, sauf si vous avez des clients Windows inférieurs à Windows 95 OSR2.

La gestion des logs est effectuée par deux directives : "log file", qui permet de spécifier le fichier de logs utilisé et "log level", qui permet de préciser le niveau de log souhaité. Nous remarquons pour "log file" l'utilisation d'une variable qui est %m. Cette variable sera interprétée par Samba comme étant le nom netbios de la machine cliente. Nous aurons ainsi un fichier de log par machine connectée, ce qui est très pratique. Il existe de nombreuses autres variables disponibles pour la plupart des directives. Nous n'allons pas les décrire ici, elles sont disponibles dans le "man smb.conf". Un niveau de log de 2 est correct pour un serveur en production, on pourra le passer à 10 maximum afin d'effectuer des tests. N'oubliez pas de rabaisser ce niveau, sous peine de voir baisser l'espace disque disponible sur vos serveurs très rapidement !

Nous avons enfin deux dernières directives. La première, "time server", active un serveur de temps sur notre serveur Samba. Les clients pourront se synchroniser avec une commande du type `"net time \\ubuntu /set /y"` dans un prompt DOS. La seconde, "veto files", empêche l'accès à certains fichiers ou répertoires sur notre serveur. Ici, nous interdisons l'accès aux fichiers et répertoires nommés lost+found et .recycle (ils doivent être séparés par des / dans la déclaration).

Voilà, notre configuration Samba est un peu plus avancée. Nous pouvons la tester avec la commande testparm. Si aucun Warning n'apparait, nous sommes prêts pour déclarer un premier partage, ce que nous ferons juste après une petite parenthèse concernant la gestion des comptes utilisateurs...

La gestion des comptes sous Samba

Nous abordons là l'une des principales sources de problèmes dans la mise en place d'un serveur Samba. La manière dont Samba gère les comptes utilisateurs est un peu particulière et souvent méconnue.

Le rôle principal de Samba en tant que serveur est de permettre à des comptes de type Windows de se connecter à une machine Unix. Or, et nous l'avons vu notamment avec la notion de SID, la gestion des comptes sous Windows est totalement différente de celle sous Unix. Tout le travail de Samba va être d'effectuer correctement une relation entre les deux types de comptes. Cette relation est nécessaire pour pouvoir, par exemple, définir les droits de l'utilisateur au niveau du système de fichiers.

Samba établit donc une correspondance en les utilisateur Unix et les utilisateurs Windows. Cette table de correspondance est en fait le fichier tdb déclaré au début du fichier de configuration. Ceci implique quelque chose de très important : **a chaque utilisateur Samba doit correspondre un utilisateur Unix** (un compte POSIX).

Ceci revient donc à dire que la création d'un compte Samba se fait en DEUX étapes : d'abord l'ajout du compte utilisateur sur la machine Unix, ensuite l'ajout de ce compte à la base Samba. Au sein de sa base, Samba complètera les infomations concernant le compte Unix par des informations purement Windows, telles un SID, un répertoire home, un script de logon, etc...

Le compte Unix de l'utilisateur peut être situé n'importe où. Il est typiquement situé dans /etc/passwd mais pourrait l'être sur un annuaire LDAP (classe posixAccount), une base de données, etc... Samba utilise l'abstraction fournie pas le mécanisme nsswitch de la machine pour obtenir les informations concernant ces comptes dits "POSIX".

Le compte Samba de l'utilisateur est manipulé traditionnellenemt pas la commande smbpasswd. Depuis peu, il est possible également de les manipuler par les commandes pdbedit ou net. Ce compte sera stocké à l'emplacement spécifié par la directive "passdb backend". Il peut être situé, à l'heure actuelle, dans un fichier (smbpasswd, tdbsam), sur un annuaire (ldapsam, nisplussam) ou dans une base de donnée (mysql). Des possibilités d'export vers un fichier xml existent également.

Il est très intéressant de centraliser les deux types de comptes sur un même annuaire LDAP ; l'administration est ainsi grandement simplifiée. Nous n'aborderons pas ici le déport des comptes POSIX et Samba sur une autre source qu'/etc/passwd et tdbsam, mais si le sujet vous intéresse, voici quelques liens :

- nss_ldap sur **http://www.padl.com**
- les ldapscripts et quelques documentations sur **http://contribs.martymac.com**

Création d'un partage accessible à tous

La configuration que nous avons éditée ne contient toujours pas de partage de fichiers. Nous allons en déclarer un, qui n'utilise que le compte invité. Il s'agit d'un partage "tmp".

Ajoutez ceci au fichier de configuration :

```
[global]

# [...]
# Dans quel cas mapper une connexion vers un compte anonyme ?
map to guest = Bad User

# Un partage tmp accessible a tous
[tmp]
path = /tmp
guest ok = yes
writeable = yes
browseable = yes
```

Nous pouvons désormais redémarrer Samba par la commande /etc/init.d/samba restart.

Nous avons ici configuré notre premier partage, appelé tmp. Il est accessible depuis toute machine Windows (ou Samba) par le chemin UNC \\ubuntu\tmp.

Chaque section de partage doit au moin contenir une directive "path", indiquant quel répertoire est partagé par cette section. Ici, il s'agit du répertoire /tmp.

La directive "guest ok" permet d'autoriser n'importe quel compte inconnu à se connecter (si le compte est connu mais le mot de passe invalide, la connexion sera refusée. Cf. la directive "map to guest" pour changer ce comportement).

Nous autorisons l'écriture dans ce partage, via la directive "writeable", et nous le rendons visible via la directive "browseable" ("browseable = no" équivaut à [tmp$]).

La connexion à ce partage peut être effectuée avec n'importe quel compte, c'est l'essence même d'un partage invité. Samba utilisera en interne le compte POSIX "nobody" pour la gestion des droits (par défaut). Ce compte est modifiable par la directive globale "guest user".

Si l'on y réfléchit, nous avons un peu "triché" jusqu'ici, en déclarant une base de compte pour Samba qui n'est finalement pas encore utilisée. Nous allons voir comment nous pouvons l'utiliser et la mettre à profit...

Création d'un partage avec authentification

Modification du fichier de configuration

Commençons par compléter notre fichier de configuration en ajoutant un partage "donnees" qui pointe vers `/data/samba/donnees` :

```
# Partage accessible uniquement au groupe sambausers
[donnees]
path = /data/samba/donnees
comment = Partage Donnees
writeable = yes
browsable = yes
guest ok = no
valid users = @sambausers
```

Nous interdisons l'accès aux invités, et autorisons uniquement le groupe sambausers à se connecter (directive "`valid users`"). Nous pouvons redémarrer Samba.

Gestion des comptes

Création des comptes

L'étape suivante est de créer un groupe, ainsi qu'un utilisateur. Appelons ce groupe "sambausers" et l'utilisateur "martymac".

Création du groupe Unix de l'utilisateur martymac (gid 513) :

```
# groupadd -g 513 sambausers
```

Note : 513 pour le gid de ce groupe n'est pas une obligation technique mais ceci rend plus simple la gestion des groupes lorsqu'on met en place des mappings. Nous verrons ceci dans le chapitre concernant le contrôle de domaine.

Création de deux utilisateurs (seul martymac possède sambausers comme groupe primaire) :

```
# useradd -g sambausers martymac
```

```
# useradd fred

# smbpasswd -a martymac
# smbpasswd -a fred
```

Le mot de passe des utilisateurs vous est demandé ; ce mot de passe sera celui à taper depuis le client Windows. Le mot de passe Unix n'est pas utilisé par Samba.

Créons ensuite le répertoire partagé /data/samba/donnees

```
# mkdir -p /data/samba/donnees
```

Il est désormais possible de se connecter au partage [donnees] avec l'utilisateur martymac uniquement. L'utilisateur fred, quant à lui, ne pourra pas se connecter car il ne dispose pas des droits nécessaires (il n'appartient pas au groupe sambausers) :

```
# tail /var/log/samba/windows.log

[2005/10/22 11:11:48, 2] auth/auth.c:check_ntlm_password(305)
  check_ntlm_password:  authentication for user [fred] -> [fred] -> [fred]
succeeded
[2005/10/22 11:11:48, 2] smbd/service.c:make_connection_snum(321)
  user 'fred' (from session setup) not permitted to access this share
(donnees)
```

Supprimons fred par la suite de commandes :

```
# smbpasswd -x fred
# userdel fred
```

Lister les comptes créés

Les utilisateurs connus par Samba peuvent être obtenus par la commande suivante :

```
# pdbedit -L
```

ou

```
# pdbedit -vL
```

pour obtenir des détails sur chaque compte (SID, nom complet, ...)

```
# pdbedit -v martymac
```

permet de ne lister que les informations concernant l'utilisateur martymac

Remarquez que, suivant la distribution GNU/Linux que vous utilisez, un certain nombre d'utilisateurs ont pu être pré-définis dans le fichier passdb.tdb lors de l'installation des packages Samba. Nous utilisons dans nos exemples le fichier mypassdb.tdb. Il ne devrait donc apparaître aucun autre utilisateur que celui que nous avons défini ensemble (martymac).

La gestion des droits

Deux types de droits

Si vous avez essayé de créer un fichier avec l'utilisateur martymac dans le partage [donnees], vous avez dû remarquer que vous n'en aviez pas le droit. Vous avez pu vous connecter, mais

vous n'avez rien pu faire par la suite. Comment cela se fait-il ? Nous avons pourtant bien spécifié "writeable = yes" dans le fichier de configuration !

La réponse vient de la manière dont sont gérés les droits sous Samba. De même que deux types de comptes interviennent, comme nous l'avons vu, il existe deux types de droits sous Samba :

- les droits liés au partage, c'est à dire les droits liés à la connexion sur celui-ci : "qui peut se connecter à quoi ?"
- les droits sur le système de fichiers : "qui peut faire quoi une fois connecté ?"

Nous comprenons ici mieux l'intérêt des deux types de comptes utilisés par Samba : Samba doit être capable de déduire les droits Unix d'un utilisateur Windows.

Notre problème d'écriture dans le répertoire partagé est probablement lié à un problème de droits Unix. Si l'on y regarde d'un peu plus près :

```
# ls -al /data/samba/
total 12
drwxr-xr-x  4 root root       4096 Oct 22 11:19 .
drwxr-xr-x  3 root root       4096 Oct 22 10:11 ..
drwxr-xr-x  2 root root       4096 Oct 22 11:19 donnees
```

nous nous apercevons que martymac ne possède aucun droit d'écriture sur le répertoire partagé ! Il a donc pu se connecter, Samba lui autorise d'écrire ("writeable = yes") au niveau du partage déclaré, mais le système de fichiers refuse car l'utilisateur martymac Unix ne possède pas les bons droits.

Pour remédier à ceci, nous devons donner les droits à l'utilisateur martymac, ou, mieux, à son groupe, puisque nous voulons que le groupe sambausers puisse écrire dans notre partage :

```
# chmod 775 /data/samba/donnees
# chgrp sambausers /data/samba/donnees
```

Testez à nouveau la connexion et essayez de créer un fichier, tout devrait rentrer dans l'ordre !

Options de configuration et gestion des droits

Samba fournit de nombreuses options pour gérer les droits au niveau du partage comme au niveau du système de fichiers lui-même. Il sera capable de positionner les droits du système de fichiers pour simuler un héritage par exemple. Voici quelques-unes des directives intéressantes concernant ces mécanismes :

Droits purement "virtuels", au niveau de la connexion

- **read only** : lecture seule sur un partage (inverse de writeable)
  ex : read only = yes
- **valid users** : déclare les utilisateurs et groupes autorisés à se connecter (inverse de invalid users)
  ex : valid users = martymac, fred, @sambausers, @autregroupe
- **force user, force group** : force la connexion en tant que l'utilisateur ou groupe spécifié
  ex : force user = martymac
- **read list, write list** : déclare les utilisateurs ou groupes autorisés à lire ou écrire
  ex : read list = fred
  ex : write list = @sambausers
- **guest ok** : autorise la connexion avec un compte invité
  ex : guest ok = yes
- **guest only** : interdit la connexion avec un compte autre qu'invité
  ex : guest only = yes
- **guest account** : spécifie le compte Unix à utiliser lors d'une connexion en invité (par défaut nobody)
  ex : guest account = martymac
- **map to guest** : spécifie quand considérer qu'un utilisateur est invité
  ex : map to guest = bad user

Manipulation des droits au niveau du système de fichiers

- **create mode** : droits placés sur un fichier lors de sa création
  ex : create mode = 770
- **directory mode** : droits placés sur un répertoire lors de sa création
  ex : directory mode = 2770
- **security mode** : pour un fichier, bits sur lesquels peut agir l'utilisateur
  ex : security mode = 700
- **directory security mode** : pour un répertoire, bits sur lesquels peut agir l'utilisateur
  ex : directory security mode = 0700

Toutes ces directives peuvent être placées au niveau global comme au niveau d'un partage. Elles permettent de mettre en place une politique de droits relativement fine.

Les administrateurs systèmes Unix savent combien il est difficile de gérer les droits sur ce type de système, surtout s'il faut mettre en place un ensemble de droits calquant ceux d'un serveur Windows (lors d'une migration par exemple). En effet, sur un fichier, Unix ne gère les droits (rwx) que pour un utilisateur donné, un groupe donné ou "tous les autres utilisateurs et groupes" (ugo). Les ACLs permettent d'aller plus loin en proposant les mêmes droits (rwx) mais pour une liste d'utilisateurs ou de groupes donnée. Le système de fichiers doit être compatible et le support des ACLs au niveau de Samba activé. Nous n'aborderons pas ici plus en détails cette fonctionnalité.

L'impression et le partage d'imprimantes

Nous allons maintenant partager une imprimante avec notre serveur Samba.

Il est possible de déclarer nos imprimantes manuellement dans le fichier smb.conf, mais l'une des facilités offertes par Samba est l'utilisation de CUPS (Common Unix Printing System - **http://www.cups.org**). CUPS est un service d'impression "nouvelle génération" destiné à remplacer les anciens systèmes tels LPD.

Installez CUPS par la commande suivante :

```
# apt-get install cupsys cupsys-client foomatic-db
```

Déclarez ensuite vos imprimantes en mode RAW via l'interface dédiée (**http://localhost:631**)

et testez-les. Le mode RAW est important car Samba et CUPS ne vont servir que de relais d'impression. Le driver utilisé sera du côté de la machine cliente, si bien que les informations transmises seront déjà correctement formatées pour l'imprimante.

Nous considérons pour la suite que nous avons une imprimante déclarée sous CUPS sous le nom d'"imprimante" et qu'elle fonctionne correctement. Cups est une suite logicielle très puissante, mais que nous n'étudierons pas plus en détails ici... ceci pourrait faire l'objet d'un autre cours. Plus d'informations sur **http://www.cups.org**.

Revenons à Samba, nous avons à ce stade une imprimante sous CUPS, mais Samba n'en a pas connaissance.

Complétons la section globale de notre fichier de configuration :

```
[global]
# [...]

# Impression
printing = cups
printcap name = cups
load printers = yes

# Partage d'imprimantes (configurées en "raw" sous CUPS)
[printers]
comment = Partage d'imprimantes
path = /data/spool
printable = yes
browseable = yes
guest ok = no
valid users = @sambausers
```

La section est compélée en spécifiant le système d'impression utilisé ("printing" et "printcap name") ainsi qu'en demandant explicitement à Samba de charger toutes les imprimantes connues ("load printers").

De cette manière, Samba va créer dynamiquement, lors de son démarrage, un partage pour chaque imprimante CUPS déclarée. Le partage [printers] permet de configurer de manière globale ces imprimantes : "path" permet de préciser le répertoire de spool (le répertoire où sont stockés temporairement les fichiers en cours d'imrpession) et "printable" précise que ce partage est un partage d'impression.

N'oubliez pas de créer le répertoire /data/spool :

```
# mkdir -p /data/spool
# chmod 775 /data/spool
# chgrp sambausers /data/spool
```

et de redémarrer Samba.

Vous devriez être capable d'ajouter l'imprimante du côté du client Windows en navigant sur les partages de la machine Unix et en double-cliquant sur l'imprimante. Le driver devra être installé manuellement. Vous pouvez désormais imprimer une page de test.

Note : Sachez qu'il est possible de gérer un partage de drivers au niveau du serveur d'impression, afin de permettre aux stations l'installation d'imprimantes de manière totalement automatique. Ceci est une opération assez complexe et se fait via le partage [print$] et la directive "show add printer wizard". Nous n'aborderons pas ce point ici...

Samba en tant que contrôleur de domaine

Exercice : *Le chapitre suivant constitue un exercice à part entière et peut être effectué en même temps que la lecture du document, qui décrit toutes les étapes à mettre en oeuvre.*

Introduction

Jusqu'à présent, notre serveur Samba est bien seul... Il agit de manière totalement autonome et ne gère aucune athentification pour un groupe de machine. Il ne gère que les accès à ses propres partages. Nous allons voir comment nous pouvons activer cette fonctionnalité et ainsi devenir PDC (contrôleur principal de domaine) ou bien BDC (contrôleur secondaire de domaine).

Plusieurs modifications sont nécessaires : d'abord au niveau de la configuration et des partages, ensuite au niveau des comptes.

Configuration de Samba en tant que PDC

Pour devenir contrôleur principal de domaine, il faut tout d'abord modifier quelque peu la section globale du fichier de configuration de Samba pour obtenir ceci :

```
[global]

# Identification Netbios
workgroup = mondomaine
netbios name = ubuntu

# Controle de domaine desactive
os level = 65
domain logons = yes
domain master = yes
local master = yes
preferred master = yes
wins support = yes

# Base de donnee de comptes
passdb backend = tdbsam:/var/lib/samba/mypassdb.tdb

# [...] La suite du fichier est identique à celle que nous avions
# précédemment
```

La directive "domain logons = yes" active le contrôle de domaine, c'est à dire la gestion des authentifications sur le domaine. Nous nommons au passage le domaine "mondomaine" grâce à la directive "workgroup".

Les directives "domain master" et "local master" sont un peu particulières. Lorsqu'une machine Windows désire naviguer dans le voisinage réseau, elle a besoin d'une liste de ses machines voisines. La machine qui fait office de "master browser" est là pour lui en fournir une. Il y a deux types de "master browsers", le "domain master browser" et le "local master browser". Ils sont respectivement "master browsers" pour le domaine Windows (qui peut s'étaler sur plusieurs réseaux) et pour le réseau local (qui peut faire partie d'un domaine plus vaste).

Il faut savoir qu'un système d'élections est prévu pour choisir la machine qui sera "master browser". Activer les deux options ci-dessus permet de participer à ces élections. Le résultat des

élections dépend du type de système d'exploitation et du rôle de la machine (et d'autres paramètres) sur le réseau. Nous pouvons influencer ce résultat en indiquant "preferred master = yes" et en indiquant un "OS level" au maximum, c'est à dire à 65.

Attention, ne déclarez qu'un seul "preffered master" par réseau sous peine de voir vos serveur Samba se battre pour devenir "master browser" et organiser des élections en continu ! De même, ne déclarez qu'un seul "domain master" par domaine.

L'"OS level" permet également de différencier un PDC d'un BDC. Un OS level à 65 est correct pour un PDC. Pour un BDC, nous choisirons plutôt un OS level plus faible, 40 par exemple. Nous étudierons ceci un peu plus tard.

Enfin, la directive "wins support = yes" permet d'activer un serveur Wins sur la machine Samba. Ce serveur, si l'on configure correctement les clients Windows, permettra de résoudre des noms Netbios, au même titre que le ferait un serveur DNS.

Les partages spécifiques du contrôleur de domaine

Un contrôleur de domaine digne de ce nom se doit de disposer de certains partages de base :

- un partage **[homes]** contenant les répertoires homes des utilisateurs. Le répertoire home de l'utilisateur sera connecté vers un lecteur spécifié lorsque l'utilisateur s'authentifiera sur le domaine.
- un partage **[netlogon]** contenant les scripts de connexion (netlogon) qui seront téléchargés et éxécutés par les machines clientes à la connexion des utilisateurs sur le domaine.
- un partage **[profiles]** contenant les profils itinérants des utilisateurs. Ces profils permettent de stocker de manière centralisée la configuration du bureau, le fond d'écran, les préférences internet (...) pour chaque utilisateur du domaine.

Chaque compte utilisateur Samba fait référence aux emplacements de ces partages particuliers, nous le verrons par la suite.

Nous devons donc ajouter les partages suivants à notre fichier de configuration :

```
# Partages Homes
[homes]
path = /data/samba/home/%u
comment = Repertoires Homes
valid users = %S
guest ok = no
writeable = yes
create mode = 0700
directory mode = 2700
browsable = no

# Partage Netlogon - lecture seule
[netlogon]
path = /data/samba/netlogon
comment = Partage Netlogon
guest ok = no
read only = yes
browseable = no
valid users = @sambausers

# Partage Profiles
[profiles]
```

```
path = /data/samba/profiles
comment = Repertoires Profiles
guest ok = no
writeable = yes
create mode = 0700
browsable = no
valid users = @sambausers
```

Le partage [homes] est un partage virtuel : si l'utilisateur martymac se connecte, le partage [martymac] sera créé automatiquement.

Pour plus de sécurité, nous limitons l'accès au partage uniquement aux personnes ayant un login correspondant au nom du partage ("valid users = %S"), c'est à dire à la personne qui a été elle-même à l'origine de la création du partage. CQFD !

L'étape suivante est de créer les répertoires nouvellement partagés :

```
# mkdir -p /data/samba/home
# mkdir -p /data/samba/netlogon
# mkdir -p /data/samba/profiles
```

Et de leur attribuer les bons droits :

```
# chgrp sambausers /data/samba/home ; chmod 775 /data/samba/home
# chgrp sambausers /data/samba/netlogon ; chmod 555 /data/samba/netlogon
# chgrp sambausers /data/samba/profiles ; chmod 775 /data/samba/profiles
```

Pensez à créer le répertoire home de l'utilisateur martymac :

```
# mkdir -p /data/samba/home/martymac
# chown martymac:sambausers /data/samba/home/martymac
# chmod 700 /data/samba/home/martymac
```

Enfin, nous pouvons créer un script très simple pour notre utilisateur martymac qui connectera automatiquement son lecteur j: à notre partage "données" lors de son logon sur le domaine :

```
# cat > /data/samba/netlogon/martymac.cmd << EOF
@echo off
@NET USE J: \\ubuntu\donnees
@echo on
EOF
```

Attribuez-lui les bons droits :

```
# chown martymac:sambausers /data/samba/netlogon/martymac.cmd
# chmod 444 /data/samba/netlogon/martymac.cmd
```

Nous verrons comment nous pouvons modifier le compte de martymac pour qu'il tienne compte du script au logon et qu'il connecte un lecteur au répertoire home.

La gestion des comptes sur un contrôleur de domaine

La commande pdbedit

La commande pdbedit permet de lister les informations détaillées de chacun des comptes du domaine.

Nous pouvons ainsi lister les informations pour notre utilisateur martymac :

```
# pdbedit -v martymac
Unix username:        martymac
NT username:
Account Flags:        [U          ]
User SID:             S-1-5-21-1339008745-1179508330-2449281493-3000
Primary Group SID:    S-1-5-21-1339008745-1179508330-2449281493-1201
Full Name:            martymac,,,
Home Directory:       \\ubuntu\martymac
HomeDir Drive:        u:
Logon Script:         martymac.cmd
Profile Path:         \\ubuntu\profiles\martymac
Domain:               WORKGROUP
Account desc:
Workstations:
Munged dial:
Logon time:           0
Logoff time:          Fri, 13 Dec 1901 21:45:51 GMT
Kickoff time:         Fri, 13 Dec 1901 21:45:51 GMT
Password last set:    Sun, 23 Oct 2005 14:12:49 GMT
Password can change:  Sun, 23 Oct 2005 14:12:49 GMT
Password must change: Fri, 13 Dec 1901 21:45:51 GMT
Last bad password   : 0
Bad password count  : 0
Logon hours         : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
```

Notons au passage le SID de l'utilisateur : **S-1-5-21-1339008745-1179508330-2449281493-3000** qui signifie qu'il appartient au domaine (ou workgroup ici) ayant le SID **S-1-5-21-1339008745-1179508330-2449281493** et que son compte possède la RID **3000**. C'est le même principe pour son groupe primaire, qui possède le même SID local (de domaine).

Le mapping de groupes et le rôle des RIDs

Nous avons vu qu'un domaine NT prédéfinissait certains comptes et groupes par défaut, en leur attribuant des RID particuliers, synonymes d'un rôle particulier sur le domaine, les "well-known RIDs". Il est nécessaire pour un contrôleur Samba de ré-utiliser ces RIDs pour les comptes du domaine.

Ces RIDs particuliers sont notamment importants au niveau des groupes des utilisateurs. Ainsi, pour que les utilisateurs du groupe sambausers soient des "utilisateurs du domaine" au sens Windows du terme (RID égal à **513**), il va falloir explicitement l'indiquer à Samba. De même, nous aurons besoin, pour les comptes de machines, d'un groupe sambamachines, correspondant au groupe "machines du domaine" (RID égal à **515**).

Commençons par créer notre groupe de machines (le groupe sambausers existe déjà) :

```
# groupadd -g 515 sambamachines
```

Attribuons ensuite les bons RIDs aux deux groupes :

```
# net groupmap add rid=515 unixgroup=sambamachines ntgroup="Domain Computers"
# net groupmap set "Domain Users" sambausers
```

Note : "net groupmap add" ajoute un mapping, et "net groupmap set" en modifie un. Nous

utilisons "net groupmap set" pour les utilisateurs du domaine car Samba propose déjà un mapping non initialisé.

Enfin, nous pouvons vérifier les "mappings" créés listant les mappings existants :

```
# net groupmap list
System Operators (S-1-5-32-549) -> -1
Replicators (S-1-5-32-552) -> -1
Guests (S-1-5-32-546) -> -1
Domain Users (S-1-5-21-1339008745-1179508330-2449281493-513) -> sambausers
Domain Computers (S-1-5-21-1339008745-1179508330-2449281493-515) ->
sambamachines
Power Users (S-1-5-32-547) -> -1
Print Operators (S-1-5-32-550) -> -1
Administrators (S-1-5-32-544) -> -1
Domain Admins (S-1-5-21-1339008745-1179508330-2449281493-512) -> -1
Domain Guests (S-1-5-21-1339008745-1179508330-2449281493-514) -> -1
Account Operators (S-1-5-32-548) -> -1
Backup Operators (S-1-5-32-551) -> -1
Users (S-1-5-32-545) -> -1
```

Nous avons bien "mappé" les deux groupes sambausers et sambamachines vers leur équivalent NT.

Attention : Lors de la création d'un mapping faisant intervenir le groupe primaire Unix d'un utilisateur, Samba ne modifie pas, pour cet utilisateur, la valeur de son "primary group sid" correspondant au nouveau mapping. Ceci provoque une décorrélation entre ces deux IDs (la valeur mappée et la valeur effective apparaissant au niveau du compte Samba). La solution est de créer les mappings AVANT de créer les comptes utilisateurs.

Pour corriger ce problème, je vous propose de supprimer l'utilisateur martymac et de le re-créer :

```
# smbpasswd -x
# smbpasswd -a martymac
```

Cette fois, si nous étudions le SID de groupe primaire de l'utilisateur martymac, nous voyons qu'il se termine bien par 513 :

```
# pdbedit -v martymac | grep -i "primary group sid"
Primary Group SID:    S-1-5-21-1339008745-1179508330-2449281493-513
```

Les paramètres avancés de chaque compte

Nous avons créé les partages homes, netlogon et profiles sur notre contrôleur de domaine. Pour qu'un utilisateur en bénéficie, il va falloir modifier ces informations au sein de son compte.

Ceci se fait par le biais de la commande pdbedit, avec laquelle nous indiquons le chemin de tous ces éléments, ainsi que la lettre de lecteur attribuée au répertoire home de l'utilisateur :

```
# pdbedit -h "\\\\ubuntu\\martymac" -D "U:" -S "martymac.cmd" -p
"\\\\ubuntu\\profiles\\martymac" martymac
```

Notez que le script de netlogon est toujours relatif au partage "netlogon" du contrôleur de domaine.

On pourra éviter cette tâche fastidieuse de modification de comptes en ajoutant les directives suivantes à la section globale de notre fichier de configuration :

```
[global]
# [...]
# Paramètres Samba par défaut pour un utilisateur
logon drive = U:
logon home = \\ubuntu\%U
logon path = \\ubuntu\profiles\%U
logon script = %U.cmd
# [...]
```

Ainsi, chaque utilisateur Samba ajouté (par smbpasswd par exemple) prendra ces valeurs par défaut.

Création du compte POSIX de manière autonome

Un contrôleur de domaine Samba peut être manipulé à distance, soit graphiquement par un outil de gestion de domaine, tel celui proposé par NT4, soit en ligne de commande avec la commande net Samba. Cependant, à l'heure actuelle, notre contrôleur de domaine n'est pas capable d'ajouter un compte de manière autonome. En effet, Samba peut ajouter la partie lui concernant mais n'est pas configuré pour ajouter, auparavant, la partie POSIX du compte.

Voici quelques directives qui permettent de palier ce problème :

```
[global]
# [...]
# Gestion des comptes POSIX
add machine script = /usr/sbin/useradd -g sambamachines -c Machine -d
/dev/null -s /bin/false '%u'
add user script = /usr/sbin/useradd -g sambausers -c Utilisateur -d
/dev/null -s /bin/false '%u'
add group script = /usr/sbin/groupadd '%g'
add user to group script = /usr/bin/gpasswd -a '%u' '%g'
delete user script = /usr/sbin/userdel -r '%u'
delete group script = /usr/sbin/groupdel '%g'
delete user from group script = /usr/bin/gpasswd -d '%u' '%g'
set primary group script = /usr/sbin/usermod -g '%g' '%u'
# [...]
```

Chacune de ces commandes va être appelée par Samba pour ajouter la partie POSIX d'un compte avant la partie Samba :

- **add machine script** : ajout d'une machine (jonction d'une machine au domaine)
- **add user script** : ajout d'un utilisateur
- **add group script** : ajout d'un groupe
- **add user to group script** : ajout d'un groupe pour un utlisateur
- **delete user script** : suppression d'un utilisateur
- **delete group script** : suppression d'un groupe
- **delete user from group script** : suppression d'un groupe pour un utilisateur
- **set primary group script** : positionnement d'un groupe en groupe primaire pour un utilisateur

Les comptes POSIX étant stockés sur la machine elle-même, nous faisons appel aux commandes standard de manipulation de comptes sous GNU/Linux. Pour des comptes situés sur un annuaire LDAP, il faudrait faire appel à des scripts particuliers, tels les ldapscripts.

Le superutilisateur Samba

Le superutilisateur Samba est nécessaire pour effectuer diverses opérations d'administrations, notamment pour la jonction d'une machine au domaine. Ce superutilisateur doit avoir un uid Posix égal à 0. L'utilisateur root est traditionnellement utilisé, ajoutons-le à nos utilisateurs Samba :

```
# smbpasswd -a root
```

Nous pouvons tester cet utilisateur en ajoutant un compte via une commande RPC :

```
# net rpc user add test -U root -S ubuntu
```

L'utilisateur root est celui avec lequel nous allons joindre notre machine cliente au domaine...

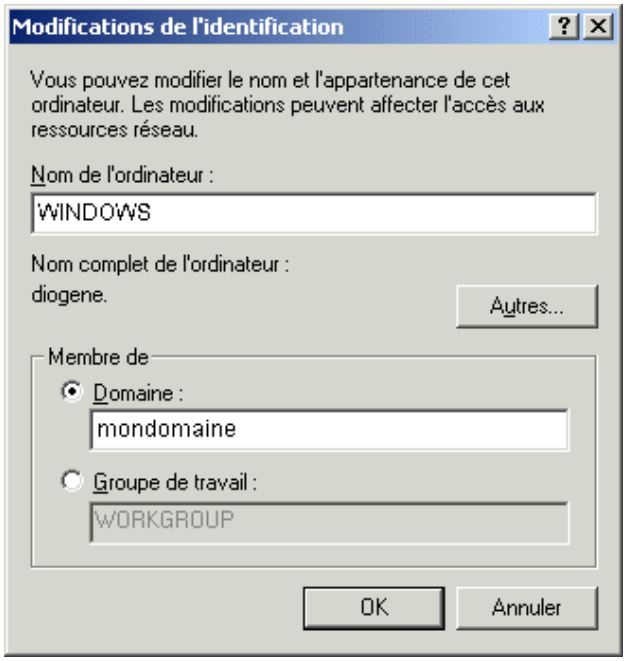
Jonction au domaine et test de notre contrôleur

Notre contrôleur de domaine est prêt. La dernière action à effectuer est de joindre notre machine cliente au domaine que nous venons de créer...

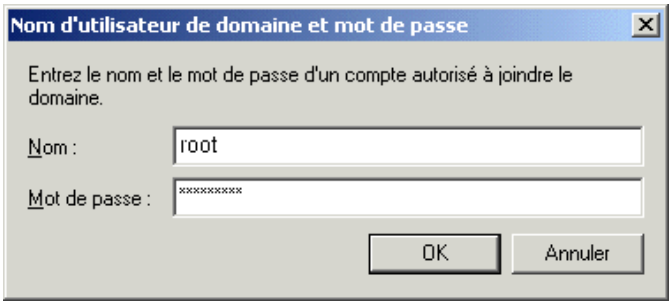
Concrètement, la jonction d'une machine au domaine correspond à la création d'un compte pour cette machine sur le PDC. Ce compte est un compte utilisateur standard, du nom netbios de la machine jointe, se terminant par un $.

Prenons l'exemple d'une machine XP. La jonction d'une machine Windows Xp à un domaine se fait par un clic droit sur le poste de travail -> propriétés. Cliquez ensuite sur l'onglet "Nom de l'ordinateur", puis cliquez sur modifier.

Une fenêtre apparaît vous demandant le nom Netbios de votre machine et le domaine à joindre. Indiquez "mondomaine" pour le nom du domaine, et, par exemple "Windows" pour le nom netbios de votre machine.



Validez. Une fenêtre apparaît ensuite, vous demandant le nom du compte habilité à joindre une station sur le contrôleur de domaine. C'est ici que nous devons utiliser le compte "root". Saisissez donc "root" et votre mot de passe et validez.



Votre machine devrait être jointe au domaine. Du côté du contrôleur de domaine Samba, un compte a bien été créé (POSIX + Samba) :

```
# getent passwd
[...]
windows$:x:1001:515:Machine:/dev/null:/bin/false
[...]

# pdbedit -L
martymac:1000:martymac,,,
root:0:root
windows$:1001:WINDOWS$
```

Nous pouvons désormais tester notre compte martymac sur la machine Windows. Connectez-vous avec ce compte au domaine "mondomaine", vous devriez avoir une lettre U: mappée vers votre répertoire home, ainsi qu'un lecteur J: mappé vers le partage données (via le script de logon). Votre profil devrait également être sauvegardé à la déconnexion.

Samba en tant que BDC

Le rôle d'un contrôleur secondaire de domaine est double : répartir la charge liée aux authentifications avec le PDC et prendre le relais du PDC en cas de panne.

Techniquement, un BDC est une machine jointe au domaine (qui possède donc un compte sur le PDC) et qui gère les authentifications sur le domaine. Il possèdera un OS level plus faible que celui de PDC.

Voici un fichier de configuration qui pourrait convenir pour ajouter un BDC à notre domaine :

```
[global]

# Identification Netbios
workgroup = mondomaine
netbios name = ubuntubdc

# Controle de domaine active
os level = 40
domain logons = yes
domain master = no
local master = no

# Base de donnee de comptes - doit être synchonisée avec celle du PDC !
passdb backend = tdbsam:/var/lib/samba/mypassdb.tdb

# Authentification via la base de comptes locale
```

```
security = user

# Securite
encrypt passwords = yes

# Gestion des logs
log file = /var/log/samba/%m.log
log level = 2
```

Notez que nous devons synchroniser les base de comptes (POSIX et Samba) afin que notre BDC soit autonome en cas de panne du PDC ! C'est pour ceci que nous utilisons généralement un backend LDAP, afin de permettre au BDC comme au PDC de disposer de la même base de comptes (Posix et Samba)... La configuration ci-dessus n'est donc pas totalement adaptée. Nous n'étudierons pas ici le cas complet de la mise en place d'un BDC, qui reste une opération assez complexe à mettre en oeuvre.

Après avoir correctement configuré la machine et si nous disponsons d'une base de comptes commune, il faut joindre le BDC au domaine. Ceci se fait de la manière suivante, depuis la machine ubuntubdc :

```
# net rpc join -S ubuntu -W mondomaine -U root
```

Un compte pour le BDC devrait être créé sur le PDC.

Administrer le serveur Samba

Nous avons déjà abordé les points essentiels liés à l'administration du serveur Samba :

- la configuration inititale
- la définition d'un partage
- l'ajout d'utilisateurs et de groupes

Il reste cependant certains points à aborder, et certaines "bonnes habitudes" à prendre, nous allons en décrire quelques-unes.

Visualiser les connexions...

... avant de stopper un serveur pour intervention. La commande smbstatus permet de savoir en temps réel qui est connecté, et quels fichiers sont ouverts. Pensez à l'utiliser avant d'intervenir sur un serveur pour vous assurer que peu ou pas de personnes sont connectées.

```
# smbstatus -v
using configfile = /etc/samba/smb.conf
Processing section "[printers]"
Processing section "[tmp]"
Processing section "[donnees]"
Processing section "[homes]"
Processing section "[netlogon]"
Processing section "[profiles]"

Samba version 3.0.14a-Ubuntu
PID     Username      Group         Machine
-------------------------------------------------------------------
 7084   martymac      sambausers    windows      (192.168.1.1)
Opened /var/run/samba/connections.tdb

Service      pid     machine       Connected at
-------------------------------------------------------
donnees       7084   windows       Mon Oct 31 09:44:56 2005
IPC$          7084   windows       Mon Oct 31 09:44:54 2005

No locked files
```

Note : On remarque au passage que Samba gère chaque connexion est gérée par un processus différent (ici PID 7084) et que les informations relatives à la connexion sont maintenues dans un fichier tdb.

Relire la configuration sans redémarrer Samba...

Samba peut relire sa configuration sans être redémarré. Pour ceci, il suffit d'envoyer un signal HUP aux démons qui sont en cours de fonctionnement :

```
# killall -HUP smbd nmbd winbindd
```

Attention, le comportement de Samba est parfois un peu étrange dans le sens où toute la configuration n'est pas re-parsée. Si vous avez ajouté une imprimante dans CUPS, elle ne sera pas chargée.

En cas de problème : étude des logs !

Pensez à étudier les logs et, si besoin est, à augmenter le niveau de log au maximum, c'est à dire 10. C'est là l'un des seuls moyens de se sortir d'une situation où tout semble bloqué...

```
log file = /var/log/samba/%m.log
log level = 10
```

```
# tail -f /var/log/samba/machine.log
```

Administration graphique ? Swat...

Nous avons étudié, dans ce manuel, comment administrer Samba via les lignes de commandes. L'un des principaux problèmes de Samba est qu'il ne dispose pas d'interface graphique "digne de ce nom" pour l'administration. Une interface rudimentaire est toutefois proposée en standard, il s'agit de Swat.

Swat est un outil Web, il embarque un petit serveur http et doit être démarré via (x)inetd. Plus d'informations à cette adresse :

http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/SWAT.html

Le futur, Samba 4

Nous l'avons vu, Samba 3 n'est pas capable de contrôler un domaine active directory. Il peut uniquement en être membre (security = ads). Les futures versions de Samba devraient être capable d'offrir cette fonctionnalité.

La version 4 semble très prometteuse car elle offrira un code totalement ré-écrit ainsi qu'une architecture plus souple à maintenir pour les développeurs. Ceci implique une meilleur qualité/stabilité du code et une réactivité plus importante pour l'ajout de nouvelles fonctionnalités.

La version 4 est dores et déjà compilable et utilisable, mais non conseillée en environnement de production ! Elle est encore en phase de développement...

Plus d'information sur : **http://devel.samba.org**

Conclusion

Samba est un formidable "concentré" de technologie, admirable par la quantité de travail fourni et le résultat obtenu par l'équipe de développement.

Bien entendu, nous n'avons, à travers ces quelques pages, abordé que les principales fonctionnalités de cet outil. Si vous êtes curieux, je vous invite à consulter le site de Samba, source d'information bien entendu complète sur le sujet, et à suivre le quelques liens ci-dessous...

S'informer, se documenter

Voici quelques liens utiles pour compléter ce cours :

- Le site de Samba : **http://www.samba.org**
- Les pages de man, notamment man 5 smb.conf
- La “Howto Collection” : **http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection**
- Le répertoire docs/ des sources (et les sources elles-mêmes ;-))
- Dernière version de ce document et diverses contributions sur : **http://contribs.martymac.com**

Les listes de diffusion sont également une source précieuse d'informations :

Officielles (en) :
- samba@lists.samba.org
- samba-technical@lists.samba.org
  -> **http://lists.samba.org/mailman**

Française :
- samba-fr@ujf-grenoble.fr
  -> **http://listes.ujf-grenoble.fr/wws/info/samba-fr**

Annexe : configuration complète du PDC

```
[global]

# Identification Netbios
workgroup = mondomaine
netbios name = ubuntu

# Controle de domaine desactive
os level = 65
domain logons = yes
domain master = yes
local master = yes
preferred master = yes
wins support = yes

# Base de donnee de comptes
passdb backend = tdbsam:/var/lib/samba/mypassdb.tdb

# Authentification via la base de comptes locale
security = user

# Securite
encrypt passwords = yes

# Dans quel cas mapper une connexion vers un compte anonyme ?
map to guest = Bad User

# Gestion des logs
log file = /var/log/samba/%m.log
log level = 2

# Serveur de temps activé
time server = yes

# Interdire l'acces a certains fichiers
veto files = /lost+found/.recycle/

# Impression
printing = cups
printcap name = cups
load printers = yes

# Paramètres Samba par défaut pour un utilisateur
logon drive = U:
logon home = \\ubuntu\%U
logon path = \\ubuntu\profiles\%U
logon script = %U.cmd

# Gestion des comptes POSIX
add machine script = /usr/sbin/useradd -g sambamachines -c Machine -d
/dev/null -s /bin/false '%u'
add user script = /usr/sbin/useradd -g sambausers -c Utilisateur -d
/dev/null -s /bin/false '%u'
add group script = /usr/sbin/groupadd '%g'
add user to group script = /usr/bin/gpasswd -a '%u' '%g'
delete user script = /usr/sbin/userdel -r '%u'
delete group script = /usr/sbin/groupdel '%g'
delete user from group script = /usr/bin/gpasswd -d '%u' '%g'
```

```
set primary group script = /usr/sbin/usermod -g '%g' '%u'

# Partage d'imprimantes (configurées en "raw" sous CUPS)
[printers]
comment = Partage d'imprimantes
path = /data/spool
printable = yes
browseable = yes
guest ok = no
valid users = @sambausers

# Un partage tmp accessible a tous
[tmp]
path = /tmp
guest ok = yes
writeable = yes
browseable = yes

# Partage accessible uniquement au groupe sambausers
[donnees]
path = /data/samba/donnees
comment = Partage Donnees
writeable = yes
browsable = yes
guest ok = no
valid users = @sambausers

# Partages Homes
[homes]
path = /data/samba/home/%u
comment = Repertoires Homes
valid users = %S
guest ok = no
writeable = yes
create mode = 0700
directory mode = 2700
browsable = no

# Partage Netlogon - lecture seule
[netlogon]
path = /data/samba/netlogon
comment = Partage Netlogon
guest ok = no
read only = yes
browseable = no
valid users = @sambausers

# Partage Profiles
[profiles]
path = /data/samba/profiles
comment = Repertoires Profiles
guest ok = no
writeable = yes
create mode = 0700
browsable = no
valid users = @sambausers
```

Glossaire

ACL (Access Control List) : Liste spécifiant les droits attribués à un ou plusieurs acteurs (ex : un utilisateur) sur une ressource (ex : un fichier).

BDC (Backup Domain Controller) : Contrôleur secondaire de domaine, prend le relais du PDC en cas de panne. Apellation propre à un domaine NT.

DC (Domain Controller) : Terme générique pour désigner un contrôleur de domaine, qu'il soit PDC, BDC (NT) ou qu'il n'ait pas de niveau d'importance particulier (Active Directory).

GID (Group Identifier) : Identifiant numérique représentant un groupe d'utilisateurs sous Unix.

LDAP (Lightweight Directory Access Protocol) : Adaptation allégée du protocole X500. Protocole de gestion d'annuaires réseaux.

NetBios : "Network Basic Input/Output System" : n'est pas un protocole. Méthode de communication sur un protocole existant ; est en fait une couche intermédiaire entre SMB et un protocole sous-jacent tel que TCP (cf. NBT) ou IPX. Il fonctionne à la couche 5 (session) du modèle OSI. Fournit une méthode de résolution de noms et de services aux couches supérieures. Utilise un modèle de noms de machines de 15 caractères + 1 caractère de contrôle spécifiant les services offerts par la machines. NetBios a été développé en 1983 par Sytec Inc. pour IBM.

NSS (NSSwitch, Name Service Switch) : Mécanisme qui intercepte les requêtes de noms effectuées par la machine (concernant les noms de machines, d'utilisateurs : cf. getent, ...) et les redirige vers différentes sources d'informations (LDAP, MySQL...). Fonctionne avec différents modules.

PDC (Primary Domain Controller) : Contrôleur principal de domaine. Apellation propre à un domaine NT.

SAM (Security Account Manager) : Base de données contenant les informations de sécurité sur un serveur Windows NT, notamment les comptes et mots de passes des utilisateurs.

SID (Security Identifier) : Un SID est un identifiant unique attribué à chaque acteur d'un domaine Windows. Il est composé d'une partie nommée "SID local", qui identifie le domaine, et d'une seconde que l'on appelle "RID" (Relative Identifier), qui identifie l'acteur (utilisateur/groupe/machine) au sein du domaine : un exemple de SID pourrait-être : S-1-5-21-3493456274-4211610059-1786859526-512 qui identifie le groupe d'Administrateurs du domaine (512) au sein du domaine S-1-5-21-3493456274-4211610059 .

UID (User Identifier) : Identifiant numérique représentant un utilisateur sous Unix.

UNC (Universal Naming Convention) : Convention de nommage universelle (sous Windows) permettant de désigner le chemin d'un répertoire partagé. Ex. : \\Serveur\partage.

Licence : GNU Free Documentation License

Version 1.2, November 2002

0. 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.

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 (c)  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.