Migration d'un PDC windows NT4 vers une solution Samba 3 - v1.3

(http://contribs.martymac.com)

Copyright (c) 2004, Linagora – Ganael LAPLANCHE.
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".

Table des matières

I) Introduction

Ce document présente les différentes étapes à suivre pour migrer les utilisateurs d'un domaine NT4 vers un domaine géré par une machine Samba. Il suppose une connaissance préalable de Samba et d'OpenLdap.

Différents éléments sont à prendre en compte lors d'une migration. Cette dernière doit permettre d'aboutir à un serveur (quasi) iso-fonctionnel au serveur "source" afin d'offrir le plus de transparence possible aux utilisateurs. Parmi les données à migrer, on trouvera :

- Les comptes utilisateurs,
- Leurs groupes,
- Les comptes machines,

- Les scripts de connexion, les stratégies
- Les données et les informations de partages
- Les droits affectés aux données.

Ceci revient globalement à deux étapes qui sont la migration de la base SAM (comptes) et la migration des données (et des droits). Nous allons voir comment procéder.

II) Présentation des architectures source et cible

Nous allons étudier dans notre exemple la migration d'un PDC NT4 disposant de 3 groupes et de 3 utilisateurs :

A) Architecture source

1) Serveur

Nom du serveur : NT4PDC
Nom du domaine : SAMBATEST

2) Acteurs du domaine (Groupes/Utilisateurs/Machines)

Direction <- Directeur
Techniciens <- Technicien
Commerciaux <- Commercial
(... sans oublier les comptes pré-définis)

3) Partages (chemin physique / partage)

Homes (utilisateur) : C:\Export\homes\<utilisateur>, \\NT4PDC\<utilisateur> : répertoires mappés sur Z: à la connection de l'utilisateur.
Homes (global) : C:\Export\homes, \\NT4PDC\homes : partage contenant tous les homes des utilisateurs. C'est ce partage que nous allons migrer plutôt que le précédent qui implique une re-copie pour chaque utilisateur.
Profils : C:\Export\profiles, \\NT4PDC\profiles\<utilisateur> : profils itinérants des utilisateurs.
Netlogon : C:\WINNT\System32\Repl\Import\Scripts, \\NT4PDC\netlogon : scripts de connexion + stratégies utilisateurs (NTConfig.POL).
Interne : partage commun, C:\Export\interne, \\NT4PDC\interne : contient 3 répertoires (Direction, Techniciens, Commerciaux) avec le droit de contrôle total pour le groupe associé. Les autres groupes n'y ont pas accès.

B) Architecture cible

Le serveur cible est un serveur Samba (samba 3.0.2a), dont les comptes utilisateurs seront stockés sur un annuaire LDAP installé en local. La distribution choisie est une Debian Woody sid (unstable) et un noyau Linux 2.4.24. On suppose que l'annuaire LDAP est correctement installé et configuré pour stocker les comptes Samba (schema Samba copié dans /etc/ldap/schema).

Le serveur cible devra proposer exactement les même services (partages, authentification) et la même configuration (même nom) que le serveur source.

Comme vous le savez, chaque compte Samba nécessite un compte Unix correspondant – nous y reviendrons. Deux stratégies sont donc possibles pour la migration des comptes vers LDAP :

- Stocker les comptes unix localement, puis stocker uniquement les comptes Samba sur LDAP
- Stocker les deux types de comptes sur l'annuaire LDAP afin de bénéficier d'une centralisation totale et d'une administration simplifiée (recommandé)

Ce document présente la seconde stratégie, la première "étant réalisable techniquement" (cf. Annexe A) mais n'offrant que peu d'intérêts en entreprise.

III) Préparation du serveur NT4 à la migration

La première étape de notre migration est de “préparer” le contrôleur de domaine originel à être migré.

Le premier problème qui se pose est la compatibilité des noms de comptes Unix et NT. Alors que NT accepte les accents, espaces, caractères spéciaux dans les noms d'utilisateurs, cela est rarement le cas pour Unix, surtout si les comptes sont stockés dans le fichier /etc/passwd (sous LDAP, les restrictions sont moins importantes). Nous pouvons donc prendre les devants en modifiant, sur le serveur NT, les noms des comptes (utilisateurs et groupes) qui ne possèdent pas les qualités requises pour la migration. Malheureusement, NT ne permet pas de modifier les noms de groupes une fois créés, il faudra donc se rabattre sur un outil tiers tel qu'Ultraadmin de Doriansoft (http://www.doriansoft.com) qui offrira cette fonctionnalité.

Une fois la compatibilité des comptes assurée, il va falloir créer un compte pour notre serveur Samba qui devra temporairement se joindre au domaine existant en tant que BDC pour avoir le droit de copier les données de la base SAM du PDC. Dans le gestionnaire de serveur, ajouter un contrôleur secondaire de domaine dont le nom sera celui de notre serveur Samba (SAMBAMIGR dans notre exemple, cf. fichier smb.conf ci-dessous).

IV) Préparation du serveur Samba à la migration

A) Installation de Samba

Sur notre serveur GNU/Linux doit être compilé Samba, une bonne configuration pour la compilation peut être par exemple “configure --with-ldap --with-automount --with-smbmount --with-quotas --with-libsmbclient –with-acl-support”.

Les ACLs et les quotas sont supportés par le système de fichiers (ici ext3fs patché ; xfs conseillé en environnement de production) et représentent une option très intéressante pour Samba. On continue par 'make && make install' et Samba 3.0.2a est désormais compilé et installé dans /usr/local/samba (par défaut).

B) Préparation de l'annuaire LDAP

Commençons tout d'abord par définir une arborescence de base de notre annuaire LDAP. Voici un exemple de fichier ldif qui permettra de stocker les utilisateurs, les groupes et les machines POSIX et Samba :

```
---------- début de base.ldif ----------
# Base de l'annuaire LDAP
dn: dc=sambatest,dc=linagora,dc=com
objectclass: dcObject
objectclass: organization
dc: sambatest
o: Tests Samba 3
description: Tests Samba 3

# Conteneur d'utilisateurs Samba
dn: ou=Users,dc=sambatest,dc=linagora,dc=com
objectclass: top
objectclass: organizationalUnit
ou: Users

# Conteneur de groupes Samba
dn: ou=Groups,dc=sambatest,dc=linagora,dc=com
objectclass: top
objectclass: organizationalUnit
ou: Groups

# Conteneur de machines Samba
dn: ou=Machines,dc=sambatest,dc=linagora,dc=com
objectclass: top
objectclass: organizationalUnit
ou: Machines
---------- fin de base.ldif ----------
```

Une commande ldapadd (ldapadd -W -D 'cn=Manager,dc=sambatest,dc=linagora,dc=com' -xH ldap://localhost -f base.ldif) permet d'insérer les données.

C) Configurer nsswitch

Les comptes POSIX seront copiés dans l'annuaire LDAP. Il faut que le système puisse interroger l'annuaire afin que chaque compte apparaisse de manière transparente comme étant un compte POSIX standard, à l'instar de ceux présents dans /etc/passwd et /etc/group. Ceci se fait par l'intermédiaire de nsswitch et de la librairie libnss_ldap (http://www.padl.com).

Deux fichiers sont à modifier :

- Le fichier de configuration de nsswitch (/etc/nsswitch.conf)

Ajouter ldap pour les sources passwd, group et shadow

```
passwd:         files ldap
group:          files ldap
shadow:         files ldap

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

- Le fichier de configuration de libnss_ldap (souvent /etc/ldap.conf ou /etc/libnss-ldap.conf suivant la distribution GNU/Linux)

Ce fichier précise quel serveur LDAP il faut interroger et dans quelles branches sont situés les comptes

```
host 127.0.0.1
port 389
ldap_version 3

base dc=sambatest,dc=linagora,dc=com
scope sub

nss_base_passwd dc=sambatest,dc=linagora,dc=com?sub
nss_base_shadow dc=sambatest,dc=linagora,dc=com?sub
nss_base_group  ou=Groups,dc=sambatest,dc=linagora,dc=com?one
```

Note : Si vous voulez que les utilisateurs puisse se connecter localement sur le serveur Unix avec leurs comptes migrés (composante POSIX), il faudra utiliser PAM, qui permettra au système d'utiliser LDAP comme source d'authentification .
(cf. http://www.padl.com, ainsi que le fichier /etc/ldap.conf ou /etc/libpam-ldap.conf suivant la distribution GNU/Linux).

D) Configuration de Samba pour la migration

Samba doit être BDC sur le domaine pour la phase de migration. Voici un exemple de fichier de configuration (/usr/local/samba/lib/smb.conf) :

```
---------- début de smb.conf ----------
[Global]
passdb backend = ldapsam:ldap://localhost, guest
ldap admin dn = "cn=Manager,dc=sambatest,dc=linagora,dc=com"
ldap ssl = off
ldap delete dn = no
ldap user suffix = ou=Users
ldap machine suffix = ou=Machines
ldap group suffix = ou=Groups
ldap suffix = dc=sambatest,dc=linagora,dc=com

workgroup = SAMBATEST
netbios name = SAMBAMIGR
encrypt passwords = yes
os level = 40
domain logons = Yes
domain master = No
local master = No
```

```
; Utilisé lors du net vampire
add machine script = /usr/local/sbin/smbldap-useradd -g sambamachines -w -c "Samba Machine" -d /dev/null -s /bin/false '%u'
add user script = /usr/local/sbin/smbldap-useradd -g sambausers -c "Samba User" -d /dev/null -s /bin/false '%u'
add group script = /usr/local/sbin/smbldap-groupadd '%g'
add user to group script = /usr/local/sbin/smbldap-groupmod -m "%u" "%g"
delete user script = /usr/local/sbin/smbldap-userdel "%u"
delete group script = /usr/local/sbin/smbldap-groupdel "%g"
delete user from group script = /usr/local/sbin/smbldap-groupmod -x "%u" "%g"
set primary group script = /usr/local/sbin/smbldap-usermod -g "%g" "%u"

security = user

log file = /var/log/samba/%m.log
log level = 2
---------- fin de smb.conf ----------
```

On remarque la configuration LDAP qui pointe sur nos différentes branches que l'on vient de créer. Il ne faut pas oublier de sauvegarder le mot de passe de l'admin dn dans le fichier secrets.tdb afin que Samba puisse accéder en écriture au serveur LDAP : smbpasswd -w <motdepasse>.

Aucun partage n'est défini ici ; ils ne sont en effet pas nécessaires pour aspirer la base. On configurera les partages adéquats par la suite lorsque Samba devra prendre le relais du PDC.

E) Jonction de Samba au domaine

Nous pouvons désormais joindre le domaine de notre serveur NT4 en tant que BDC. Ceci se fait par la commande "net rpc join -S NT4PDC -w SAMBATEST -U Administrateur". Le mot de passe de l'administrateur vous est demandé et le BDC est joint. N'oubliez pas que notre serveur Samba est éteint. Il ne sera démarré que pour prendre le relais du PDC.

Enfin, il va nous falloir réinitialiser le SID local de notre BDC pour qu'il soit égal à celui de notre PDC afin de conserver le domaine intègre. Notons le SID du domaine SAMBATEST : net getlocalsid SAMBATEST, et forçons la valeur du SID local de notre BDC avec net setlocalsid <SID noté>.

F) Installation et configuration des smbldap-tools

Le fichier smb.conf présenté ci-dessus utilise plusieurs directives [...] script [...]. Ces directives permettent de faire appel à des scripts externes lors de certaines actions telles que l'ajout d'un utilisateur. Chaque script va permettre d'ajouter les informations POSIX du compte avant sa complétion par l'ajout des informations Samba (telles que le SID de l'utilisateur). Les scripts à utiliser ici doivent donc créer les informations POSIX sur l'annuaire LDAP. Ces différentes directives seront utilisées lors de la phase de copie des comptes depuis le contrôleur de domaine NT.

Nous faisons ici appel aux scripts smbldap-tools, développés par idealx (http://samba.idealx.org). Il s'agit de scripts PERL qui reprennent les commandes Unix standards (useradd,userdel, ...) et leurs options. On pourrait tout à fait envisager d'utiliser d'autres outils (ex. Annexe A).

Vous aurez besoin de PERL et Net::LDAP (perl -MCPAN -e shell, puis install Net::LDAP dans le shell CPAN) pour faire fonctionner les smbldap-tools.

Décompressez l'archive des smbldap-tools, puis suivez les instructions du fichier INSTALL pour copier et configurer les smbldap-tools.

Directives importantes dans le fichier /etc/smbldap-tools/smbldap.conf :

```
#[...]
# Sid du domaine Samba, que l'on peut obtenir par la commande 'net getlocalsid'
SID="S-1-5-21-4109349211-2507905533-872075644"
#[...]
# GID Posix par défaut pour chaque utilisateur ajouté
defaultUserGid="513"
# GID Posix par défaut pour chaque machine ajoutée
defaultComputerGid="515"
#[...]
```

G) Ajout de deux groupes d'import : sambausers et sambamachines

Pour la migration, Samba va utiliser deux groupes : sambamachines et sambausers qui deviendront les groupes Unix primaires des utilisateurs et machines importés. Il faut donc les créer, en tenant compte des deux GIDs précisés dans le fichier de configuration des smbldap-tools :

smbldap-groupadd -g 513 sambausers && smbldap-groupadd -g 515 sambamachines

Ces deux commandes vont créer dans LDAP les informations POSIX des deux groupes primaires des utilisateurs et machines importés. Il faut ensuite créer un mapping correspondant à ces deux groupes par les commandes :

net groupmap add sid=S-1-5-21-4109349211-2507905533-872075644-513 unixgroup=sambausers
net groupmap add sid=S-1-5-21-4109349211-2507905533-872075644-515 unixgroup=sambamachines

Les informations Samba sont ainsi ajoutées aux entrées Posix de l'annuaire LDAP. Chacun des deux groupes est associé au "well-known rid" correspondant (cf. http://de.samba.org/samba/docs/man/howto/groupmapping.html#WKURIDS).

H) Création d'un administrateur Samba

A ce stade, nous pouvons créer notre premier utilisateur qui est l'administrateur Samba. Cet utilisateur doit exister sur la machine et posséder un uid égal à 0 et un gid égal à 0. Utilisons l'utilisateur root déjà existant en local. Il faut l'ajouter sous Samba : smbpasswd -a root. L'utilisateur est inséré dans LDAP. Il sera utilisé pour se connecter au serveur Samba lors d'une commande d'administration (net user par exemple).

V) Migration des comptes

Nos deux serveurs sont désormais prêts pour la migration des comptes. Lançons le processus de réplication : net rpc vampire -S NT4PDC -w SAMBATEST -U Administrateur. Les différents comptes défilent et sont copiés sous LDAP.

A) Quelques erreurs fréquentes

Erreur de création de mapping ? -> Avez-vous bien spécifié les scripts (smb.conf) qui permettent de créer les entrées POSIX dans LDAP ?
Erreur de validité de compte ? -> Le compte à importer ne dispose-t-il pas de caractères interdits (accents, espaces...) ?

B) Vérifications

Nous pouvons vérifier que les comptes ont bien été migrés de plusieurs manières :

posix (locaux et LDAP) : getent passwd ; getent group
samba : pdbedit -vL
(net user ne fonctionne pas pour le moment car le serveur Samba est éteint...)
ldap : ldapsearch -b 'dc=sambatest,dc=linagora,dc=com' -xH localhost
mappings samba : net groupmap list

VI) Migration des données

Les données sont regroupées à travers 4 partages sur notre PDC : un partage profiles, un partage homes (qui regroupe les partages de chaque utilisateur), un partage netlogon et un partage interne. Il va falloir migrer l'intégralité des données contenues dans ces partages et les recréer côté Samba.

A) Définition des futurs partages dans Samba

Commençons par modifier notre fichier smb.conf pour y définir les partages corrects. Ajouter, sous la section [Global] :

```
[interne]
comment = Partage interne de fichiers
path = /export/interne
read only = no
writable = yes

; Scripts et stratégies
[netlogon]
path = /export/netlogon
comment = Network logon service
read only = yes
guest ok = yes

; A mapper via \\serveur\utilisateur
[homes]
path = /export/homes/%u
comment = Home directories
valid users = %S
writeable = yes
read only = no
create mask = 0600
directory mask = 0700
browsable = no

; A mapper via \\serveur\profiles\utilisateur
[profiles]
path = /export/profiles
comment = User profiles
writeable = yes
read only = no
create mask = 0600
directory mask = 0744
profile acls = yes
```

On redéfinit ici à l'identique les partages disponibles sur notre PDC originel. Les répertoires locaux /export/interne, /export/netlogon, /export/homes et /export/profiles doivent bien entendu exister (les créer le cas échéant).

B) Copie des fichiers partagés

Il convient désormais de migrer les données présentes dans chacun de ces partages. Un utilitaire Samba existe pour nous faciliter la tâche : smbclient. Ici, nous devrons taper 4 commandes successives :

```
smbclient -U Administrateur -c "tar c /export/profiles/profiles.tar" //NT4PDC/profiles
smbclient -U Administrateur -c "tar c /export/netlogon/netlogon.tar" //NT4PDC/netlogon
smbclient -U Administrateur -c "tar c /export/homes/homes.tar" //NT4PDC/homesamigrer
smbclient -U Administrateur -c "tar c /export/interne/interne.tar" //NT4PDC/interne
```

Notons que l'utilisateur Administrateur doit disposer des droits en lecture sur chacun des fichiers/répertoires partagés pour pouvoir les sauvegarder. Ces commandes ont pour effet de créer 4 archives situées dans les répertoires exportés, il reste à les décompresser :

```
cd /export/profiles && tar xvf profiles.tar && rm profiles.tar
cd /export/netlogon && tar xvf netlogon.tar && rm netlogon.tar
cd /export/homes && tar xvf homes.tar && rm homes.tar
cd /export/interne && tar xvf interne.tar && rm interne.tar
```

VII) Migration des droits

Un gros problème se pose malheureusement lors de la migration des données. Nous avons perdu l'intégralité des ACLs présentes sur les données. Il n'existe pas de méthode simple pour les migrer rapidement. Smbcacls permet de dumper les acls (format NT) d'un fichier partagé. Il conviendrait donc de développer un script qui mémoriserait l'intégralité des acls de l'arborescence partagée, les filtrerait pour les transcrire en ACL POSIX et les réappliquerait sur les fichiers migrés sur le disque.

Dans notre cas, ré-appliqons simplement les droits à la main :

```
chown -R Directeur:sambausers /export/profiles/Directeur
chown -R Commercial:sambausers /export/profiles/Commercial
chown -R Technicien:sambausers /export/profiles/Technicien
chown -R Administrateur:sambausers /export/profiles/Administrateur
chmod -R u+rw /export/profiles/*
chmod -R g-rwx /export/profiles/*
chmod -R o-rwx /export/profiles/*

chown -R Directeur:sambausers /export/homes/Directeur
chown -R Commercial:sambausers /export/homes/Commercial
chown -R Technicien:sambausers /export/homes/Technicien
chown -R Administrateur:sambausers /export/homes/Administrateur
chmod -R u+rw /export/homes/*
chmod -R g-rwx /export/homes/*
chmod -R o-rwx /export/homes/*

chown Directeur:sambausers /export/netlogon/Directeur.cmd
chmod -R 500 /export/netlogon/*

chown -R :Commerciaux /export/interne/Commerciaux
chown -R :Techniciens /export/interne/Techniciens
chown -R :Direction /export/interne/Direction
chmod -R u+rw /export/interne/*
chmod -R g+rw /export/interne/*
chmod -R o-rwx /export/interne/*
```

VIII) Prise de relais du PDC

Une fois les comptes et les données migrées, il reste à modifier la section [Global] de notre fichier smb.conf pour prendre le même nom que le PDC NT, ainsi que ses fonctions :

```
[Global]

passdb backend = ldapsam:ldap://localhost, guest
ldap admin dn = "cn=Manager,dc=sambatest,dc=linagora,dc=com"
ldap ssl = off
ldap delete dn = no
ldap user suffix = ou=Users
ldap machine suffix = ou=Machines
ldap group suffix = ou=Groups
ldap suffix = dc=sambatest,dc=linagora,dc=com

workgroup = SAMBATEST
netbios name = NT4PDC
encrypt passwords = yes

os level = 65
domain logons = Yes
domain master = Yes
local master = Yes

; Utilisé lors du net vampire
add machine script = /usr/local/sbin/smbldap-useradd -g sambamachines -w -c "Samba Machine" -d /dev/null -s /bin/false '%u'
add user script = /usr/local/sbin/smbldap-useradd -g sambausers -c "Samba User" -d /dev/null -s /bin/false '%u'
add group script = /usr/local/sbin/smbldap-groupadd '%g'
add user to group script = /usr/local/sbin/smbldap-groupmod -m "%u" "%g"
delete user script = /usr/local/sbin/smbldap-userdel "%u"
delete group script = /usr/local/sbin/smbldap-groupdel "%g"
delete user from group script = /usr/local/sbin/smbldap-groupmod -x "%u" "%g"
set primary group script = /usr/local/sbin/smbldap-usermod -g "%g" "%u"

security = user

log file = /var/log/samba/%m.log
log level = 2
```

Nous pouvons désormais éteindre le PDC NT4 et démarrer le PDC Samba : smbd-D && nmbd -D

IX) Test de connexion

Si la migration s'est bien passée, nous pouvons désormais nous connecter avec notre machine cliente et nos comptes habituels (machine et utilisateur). Pour joindre une nouvelle machine au domaine, on pourra le faire depuis Windows (directive add machine script) ou bien au préalable lui créer un compte sur le serveur Samba : smbldap-useradd -w machine && smbpasswd -a -m machine.

X) Notes finales

A) Migration et groupe primaire

Lors de la migration, le groupe primaire de chaque utilisateur est réinitialisé au groupe Unix qui sert à l'import ('sambausers' dans notre exemple). Le vrai groupe NT primaire devient un groupe secondaire. Ceci ne pose pas de problème en soi car Samba gère désormais correctement les groupes multiples pour les utilisateurs, ce qui n'était pas le cas dans les versions précédentes.

B) Ce qui n'est PAS faisable avec Samba dans l'état actuel des choses

- Etre PDC d'un BDC NT4
- Utiliser/migrer des GPO
- Importer l'intégralité des ACLs (faisable, mais pas de solution “clefs en mains”)
- Imbriquer des groupes (non géré par NT4)

C) Les ACLs et MS.Office >= 2000

Noyau 2.4.21 + ext3 + acls, samba 3.0.2

Description du problème :
Un problème est régulièrement soulevé concernant les ACLs est la suite MsOffice >= 2000. Si la gestion des ACLs est activée sur le serveur Samba, Office repositionne les droits sur le fichier à “r--” pour l'utilisateur propriétaire après tout enregistrement du fichier, ce qui empêche une personne qui enregistre son fichier de pouvoir l'enregistrer à nouveau (il est alors en lecture seule). Le problème est référencé chez Microsoft à cette adresse : http://support.microsoft.com/default.aspx?scid=kb;EN-US;814112, cependant, ni le hotfix, ni le SP4 2000 (qui inclut le hotfix), ni le SP3 de MS Office 2000 ne permet de résoudre intégralement le problème (le SP4 a réglé le pb pour certains fichiers créés par Office 2000 mais pas par Office 97). Notons que pour les fichiers dont le pb a été réglé, l'utilisateur qui modifie le fichier est ajouté dans les acls avec les droits rwx. Ceci pose un nouveau pb ds le cas d'une gestion des droits par groupes car les droits explicites des utilisateurs sont prioritaires aux droits du groupe. En cas de changement de groupe de l'utilisateur, il conserve ses droits explicites sur le fichier. Les fichiers créés par Office 97 et ouvert par Office 2000 ont continueé à poser le même problème après l'application du patch.

L'héritage des Acls ou les masks du smb.conf n'y changent rien.

Explication technique :
Lors de l'enregistrement, Office crée un nouveau fichier temporaire et y copie le contenu du fichier en cours. Lors de la sauvegarde, le fichier original est supprimé, le nouveau fichier renommé, et les droits réinitialisés à la lecture pour l'utilisateur créateur du fichier.

Solution :
La solution est ici de ne plus utiliser les ACLs (nt acl support = no) mais juste les droits posix qui permettent, en outre, une gestion simplifiée (mais plus limitée). On utilise des droits posix par groupes.
Pour un partage commun comprenant des droits différents sur des sous-répertoires, on positionne le groupe qui doit avoir les droits particuliers en tant que groupe owner du répertoire ; on positionne ensuite les droits sur ce répertoire en utilisant le SGID pour conserver le groupe owner sur les fichiers et sous-répertoires créés au sein du répertoire (chmod 2770 sur le répertoire de base) ; on force enfin le create mask et le directory mask en 2770 dans le smb.conf pour le partage en question (create mode = 2770, directory mode = 2770). On désactive également l'héritage de permissions (inherit permissions = no).
On peut positionner initialement les droits par un chown et un chmod récursif (en utilisant le SGID bit) sur les répertoires du partage concerné (ex : chown -R root:compta /data/samba/commun/compta ; chmod -R 2774 /data/samba/commun/compta).

XI) Liens

La dernière version de ce document est disponible à l'adresse : http://contribs.martymac.com. Vous y trouverez également d'autres contributions Samba... à bientôt !

XII) Annexe A : scripts pour une migration avec séparation de comptes

Voici trois scripts qui permettent d'ajouter les informations POSIX (utilisateur, groupe ou machine) sous LDAP à partir d'un compte local. Ils peuvent être utiles pour des tests lors de la mise en place d'une solution Samba/LDAP avec volonté de créer les comptes POSIX localement (/etc/passwd et /etc/group) et les comptes Samba sur l'annuaire LDAP.

Ces scripts sont à copier dans le répertoire /usr/local/sbin.

```
---------- début de addgroup_ldap.sh ----------
#!/bin/sh

SERVER="localhost"
BINDDN="cn=manager,dc=sambatest,dc=linagora,dc=com"
PASSWORD="secret"

if [ "$1" == "" ]
then
  echo "Usage : $0 <group>"
  exit -1
fi

GROUP=$1
GID=`getent group | grep -E "^$1:" | cut -d ":" -f 3`

if [ "$GID" == "" ]
then
  echo "Couldn't find group $1"
  exit -1
fi

grep -E '^##' $0 | sed 's/^##//' | \
        sed -e "s/<group>/$GROUP/g" -e "s/<groupid>/$GID/g" | \
        ldapadd -w $PASSWORD -D $BINDDN -xH ldap://$SERVER > /dev/null

if [ $? -ne 0 ]
then
  echo "Error adding group $1 to LDAP"
  exit -1
fi

echo "Successfully added group $1 to LDAP"
exit 0

# Ldif info
##dn: cn=<group>,ou=Groups,dc=sambatest,dc=linagora,dc=com
##objectClass: posixGroup
##cn: <group>
##gidNumber: <groupid>
---------- fin de addgroup_ldap.sh ----------
```

```
---------- début de adduser_ldap.sh ----------
#!/bin/sh

SERVER="localhost"
BINDDN="cn=manager,dc=sambatest,dc=linagora,dc=com"
PASSWORD="secret"

if [ "$1" == "" ]
then
  echo "Usage : $0 <user>"
  exit -1
fi

USER=$1
UUID=`id -u $1 2> /dev/null`
UGID=`id -g $1 2> /dev/null`

if [ "$UUID" == "" ] || [ "$UGID" == "" ]
then
  echo "Couldn't find user $1"
  exit -1
fi

grep -E '^##' $0 | sed 's/^##//' | \
        sed -e "s/<user>/$USER/g" -e "s/<uid>/$UUID/g" -e "s/<gid>/$UGID/g" | \
        ldapadd -w $PASSWORD -D $BINDDN -xH ldap://$SERVER > /dev/null

if [ $? -ne 0 ]
then
  echo "Error adding user $1 to LDAP"
  exit -1
fi
echo "Successfully added user $1 to LDAP"
exit 0

# Ldif info
##dn: uid=<user>,ou=Users,dc=sambatest,dc=linagora,dc=com
##objectClass: account
##objectClass: posixAccount
##cn: <user>
##uid: <user>
##uidNumber: <uid>
##gidNumber: <gid>
##homeDirectory: /dev/null
##userPassword:
##loginShell: /bin/false
##gecos: <user>
##description: <user>
---------- fin de adduser_ldap.sh ----------
```

```
---------- début de addmachine_ldap.sh ----------
#!/bin/sh

SERVER="localhost"
BINDDN="cn=Manager,dc=sambatest,dc=linagora,dc=com"
PASSWORD="secret"

if [ "$1" == "" ]
then
  echo "Usage : $0 <machine\$>"
  exit -1
fi

USER=$1
UUID=`id -u $1 2> /dev/null`
UGID=`id -g $1 2> /dev/null`

if [ "$UUID" == "" ] || [ "$UGID" == "" ]
then
  echo "Couldn't find machine $1"
  exit -1
fi

grep -E '^##' $0 | sed 's/^##//' | \
        sed -e "s/<user>/$USER/g" -e "s/<uid>/$UUID/g" -e "s/<gid>/$UGID/g" | \
        ldapadd -w $PASSWORD -D $BINDDN -xH ldap://$SERVER > /dev/null

if [ $? -ne 0 ]
then
  echo "Error adding machine $1 to LDAP"
  exit -1
fi

echo "Successfully added machine $1 to LDAP"
exit 0

# Ldif info
##dn: uid=<user>,ou=Machines,dc=sambatest,dc=linagora,dc=com
##objectClass: account
##objectClass: posixAccount
##cn: <user>
##uid: <user>
##uidNumber: <uid>
##gidNumber: <gid>
##homeDirectory: /dev/null
##userPassword:
##loginShell: /bin/false
##gecos: <user>
##description: <user>
---------- fin de addmachine_ldap.sh ----------
```

Lors de la migration des utilisateurs, Samba va ajouter deux comptes pour chaque utilisateur/groupe/machine importé : un compte posix sur la machine et un compte Samba sur LDAP. Le compte posix est obligatoire pour Samba, qu'il soit situé localement sur la machine ou bien sur Ldap (avec utilisation de nsswitch comme nous l'avons étudié).

Si, en théorie, LDAP peut ne contenir que les comptes Samba, en pratique cela s'avère différent, car des outils comme LAM attendent une entrée posix en plus de l'entrée Samba dans LDAP. Plus grave encore, la création d'un mapping de groupes est impossible sous Samba si une entrée posix n'existe pas dans l'annuaire, ce qui compromet tout le processus de migration. Les scripts présentés ci-dessus permettent de gérer les comptes posix en local et d'ajouter sous LDAP les quelques informations nécessaires à Samba pour la migration et à LAM pour fonctionner.

Voici les lignes du fichier smb.conf à modifier :

```
; Nécessaire pour LAM
add machine script = /usr/sbin/useradd -g sambamachines -c "Samba Machine" -d /dev/null -s /bin/false '%u' && /usr/local/bin/addmachine_ldap.sh '%u'
; Nécessaire pour LAM
add user script = /usr/sbin/useradd -g sambausers -c "Samba User" -d /dev/null -s /bin/false '%u' && /usr/local/bin/adduser_ldap.sh '%u'
; Nécessaire pour que Samba puisse créer le mapping
add group script = /usr/sbin/groupadd '%g' && /usr/local/bin/addgroup_ldap.sh '%g'
add user to group script = /usr/sbin/usermod -G `/usr/bin/id -G '%u' | /bin/sed 's/ /,/g'`,'%g' '%u'
```

Re-précisons que cette méthode de migration est déconseillée en production ; mieux vaut centraliser les comptes POSIX et Samba sur l'annuaire, ainsi que nous l'avons présenté tout au long de ce document.

GNU Free Documentation License

Version 1.2, November 2002

Copyright (C) 2000,2001,2002 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

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.