SaMBa

SaMBa en mode groupe de travail avec base de compte locale de type tdbsam.

Généralités

- SaMBa.

Samba est un logiciel libre et une mise en oeuvre du protocole SMB/CIFS sous Linux, initialement développée par l'australien Andrew Tridgell. Il est sous licence GNU GPL 3. Son nom provient du protocole SMB (Server message block), le nom du protocole standard de Microsoft, auquel ont été ajoutées les deux voyelles a : “SaMBa”.

A partir de la version 3, Samba fournit des fichiers et services d'impression pour divers clients Windows et peut s'intégrer à un domaine Windows Server, soit en tant que contrôleur de domaine principal (PDC) ou en tant que membre d'un domaine. Il peut également faire partie d'un domaine Active Directory. Il fonctionne sur la plupart des systèmes Unix, comme Linux, Solaris, AIX et les variantes BSD, y compris Apple, Mac OS X Server (qui a été ajoutée au client Mac OS X en version 10.2). Samba fait partie intégrante de presque toutes les distributions Linux.

SaMBa propose plusieurs fonctions.

- Serveur de partage simple.
- Serveur de groupe de travail .
- Contrôleur de domaine.

La configuration de ces fonctions est essentiellement dirigé par le paramètres `security` dans `smb.conf`.

Sa base de compte peut être synchronisé avec un annuaire OpenLDAP.

Utilisation de SaMBa pour les serveurs accédant aux baies de stockage (notamment archives)

J'ai utilisé SaMBA en serveur de groupe de travail pour celui qui accède aux archives ainsi que l'autre pour diverses données. Ainsi les utilisateurs n'ont pas besoin d'être dans un domaine pour accéder aux données et les accès sont authentifiés. Ici l'authentification se réalise avec une base de compte SaMBa (tdb : Trivial Data Base) sur le serveur Linux. L'ajout des comptes dans un annuaire OpenLDAP est plus compliqué et pas forcément utile pour le peu de comptes présent sur ces serveurs. Red Hat estime la solution OpenLDAP utile à partir de 500 utilisateurs. Vous remarquerez qu'on en est très loin!

Pour le serveur de baie 1, il est serveur de groupe de travail mais n'en est pas le maître. Ainsi, il faut simplement ne pas mettre la directive `preferred master` et mettre un `os level` plus bas que le serveur principal.

Installation

Samba est disponible en natif dans toutes les distributions Linux. On peut donc l'installer avec le gestionnaire de paquetages intégré. Sinon, récupérer le paquet disponible sur les différents sites de paquets.

```
yum install samba
aptitude install samba
```

Configuration

Documentation

- Livre O'Reilly, la référence en la matière.
- Documentation Mandriva sur les permissions Linux : http://wiki.mandriva.com/fr/Permissions

Configuration générale

Emplacement	Fonction
/etc/samba/	Dossier dans lequel tous les fichiers de configurations sont présents.
/etc/samba/smb.conf	Fichier de configuration principal de samba.
/etc/samba/smbusers	Fichier de correspondance des comptes (alias de nom).
/etc/samba/secrets.tdb	Base de données de comptes locaux de type tdbsam.

5 types d'espaces sont gérables avec SaMBa

- Espace des archives à rendre accessible au serveur Web en lecture et à un petit groupe d'utilisateurs en lecture-écriture.
- Espace projet accessible en lecture-écriture pour un groupe de personnes avec quotas.
- Espace qui recevra les sauvegardes des configurations des serveurs et des sources de développement donc en écriture pour le serveur d'archivage uniquement.
- Espace de répertoires personnels accessibles uniquement par un seul utilisateur en lecture-écriture avec quotas.
- Espace commun pour transfert de fichiers rapide pour les utilisateurs (quotas obligatoires et suppression régulière).

La majorité des espaces utilisateurs doivent comporter des quotas afin d'éviter les abus.

smb.conf générique

Avant de créer la base de compte, il faut configurer le fichier `smb.conf` qui contient toute la configuration de SaMBa. Tous les fichiers de configurations se situent dans `/etc/samba/*`.

Paramètres à modifier dans `/etc/samba/smb.conf`.

```
workgroup = WORKGROUP (nom du groupe de travail).
hosts allow = 192.168.0. 192.168.1. 147.171.149. 127.  (adresses réseaux à autoriser à l'accès).
security = user (valeur par défaut pour transformer le serveur en groupe de travail).
passdb backend = tdbsam (type de la base de données utilisateurs SaMBa).
encrypt passwords = yes (crypter les mots de passes)
username map = /etc/samba/smbusers (fichier des alias de comptes notamment pour root)

#augmenter ou diminuer de 1024 en 1024
socket options = IPTOS_LOWDELAY TCP_NODELAY SO_SNDBUF=14336 SO_RCVBUF=14336 (directive de performance très importante.
#Je suis passé de 2h50 de copie à 25 minutes pour un fichier de 8,8 Go avec ces paramètres. Il faut changer les deux dernières valeurs de 1024 en 1024. Plus on monte, plus on alloue des ressources pour les copies.
#Nous en avons particulièrement besoin car nous copions des fichiers gigantesques (environ de 20 Go)).

interfaces = 192.168.1.33/24 (adresse de l'interface du serveur à écouter).
preferred master = yes (pour l'un des serveurs seulement. Sert à rendre le serveur maître d'explorateur de réseau)
os level = 33 (valeur par défaut. Elle sert à remporter les élections d'explorateur de réseau. Il faut mettre une valeur inférieur pour un second serveur non maître du réseau).
```

smb.conf utilisé

```
workgroup = WORKGROUP
server string = File Server infrastructure
netbios name = <machine_name>
#socket options = IPTOS_LOWDELAY TCP_NODELAY SO_SNDBUF=14336 SO_RCVBUF=14336
log file = /var/log/samba/%m.log
max log size = 50
security = share
passdb backend = tdbsam
encrypt passwords = yes
username map = /etc/samba/smbusers
browseable = no #pour ne pas afficher les home dir
os level = 33
preferred master = yes

[homes]
        comment = Home Directories
        browseable = no
        writable = no
```

Utiliser la commande de test pour tester la syntaxe et vérifier.

```
testparm
```

Après avoir réaliser ceci, redémarrer le service.

```
/etc/init.d/smb restart
```

Aucunes erreurs ne doivent être rencontrées. Vérifier le fichier de log.

```
tail -n 100 /var/log/samba/smbd.log
```

Paramétrer le système pour que le service se lance au démarrage.

```
chkconfig smb on
```

Il faut ensuite modifier `administrator` en `administrateur` dans le fichier `/etc/samba/smbusers` afin de permettre les connexions en administrateur et non administrator et surtout pas avec `root`. Ce fichier trompe un peu l'ennemi en faisant croire que c'est un serveur Windows qui gère les fichiers alors que c'est un serveur GNU/Linux (Si on rentre root on sait tout de suite que ce n'est pas du Windows!).

Fonctionnement des comptes

Le système Linux dispose d'un serveur Samba. Pour paramétrer Samba, il faut gérer les comptes de la base Linux et ceux de la base Samba.

La base Linux

Afin de mettre en relation un serveur Samba avec un utilisateur, il faut tout d'abord que le serveur dispose des utilisateurs désirant se connecter avec les bons identifiants et les bons groupes.

La base Samba

Afin de faire fonctionner Samba, il faut aussi que les comptes de la base Linux soit dans la base Samba. En effet, afin que Samba puisse reconnaître les utilisateurs qui se connectent, il faut tout simplement qu’ils les connaissent dans sa base.

Ainsi, les deux bases (Linux et Samba) sont indépendantes mais se complètent car la base Samba a besoin des comptes de la base Linux pour créer ses comptes.

Création des bases utilisateurs

Avant de commencer, il faut définir une architecture des noms de comptes. J'ai choisit le nom entier + la première lettre du prénom. ex : fooa (alice foo), foob (bruno foo) et food (dingo foo)

Base Linux

Exemple avec le premier cas d'espace gérable. Ici c'est le cas de l'administrateur de la base documentaires qui doit pouvoir écrire et le serveur Web qui doit uniquement lire les données. En fait la différence réside dans le répertoire de base et l'attribution du groupe.

```
groupadd smbarchives
useradd -G smbarchives -d /dev/null -s /sbin/nologin food
```

Pas de commande passwd, on ne leur attribue pas de mot de passe. Ainsi le compte ne peut se connecter sur le système.

Le groupe smbarchives est créé pour les utilisateurs accédant aux archives (en lecture et en écriture). Les accès sont régis dans la configuration du partage dans `smb.conf`.

Base SaMBa

Nous avons ajouté `passwd backend = tdbsam` dans le fichiers `smb.conf`. Ce paramètres permet de ne pas se servir d'un fichier texte basique (smbpasswd) pour la base de compte mais d'un fichier base de données. Le fichier texte se déprécie de plus en plus, il est conseillé d'utiliser cette méthode.

Redémarrer SaMBa si ce n'est déjà pas fait.

```
service smb restart
```

Création du compte root d'administrateur de SaMBa.

```
pdbedit -a root
```

Création d'un utilisateur de base préalablement créé dans la base Linux.

```
pdbedit -a food
```

Il n'y a rien d'autres à faire. On peut passer à la section suivante.

Commandes d'administrations utiles. Afficher la liste des comptes base SaMBa.

```
pdbedit -L
pdbedit -Lv (mode bavard)
```

Puis dans la base Linux.

```
cat /etc/passwd
```

Modifier mot de passe d'un compte base SaMBa.

```
smbpasswd -a nomcompte
```

Comme le fichier de base de données est changé dans `smb.conf` c'est le fichier tdb (`passwd.tdb`) qui est modifié, pas smbpasswd puisqu'il n'existe pas de toute façon.

Supprimer un compte base SaMBa.

```
pdbedit -x -u nomcompte
```

Puis supprimer dans la base Linux.

```
userdel -r nomcompte
```

Configuration des partages

Partage en lecture seulement accessible uniquement par le compte zope qui se trouve être le serveur Web. Il est à noter que j'ai partagé exactement le même volume pour pouvoir y ajouter deux accès différents (un en lecture pour zope et un autre en lecture-écriture pour les admins). Le dossier de montage (ex : /mnt/aav-1-b2) doit disposer des permissions suivantes .

```
mkdir /mnt/aav-1-b2
cd /mnt
chmod 770 aav-1-b2
chgrp smbarchives aav-1-b2
```

Ceci parce que tous les utilisateurs qui ont accès à ce partage sont membres du groupe `smbarchives`.

```
chmod g+s aav-1-b2 (fixer le bit GID pour que le groupe soit propagé dans
les sous-dossiers de manière fixe).
```

Pour plus d'informations, se reporter à la documentation de Mandriva citée dans les sources.

Faire de même pour les autres dossiers. Ainsi, les propriétaires des fichiers correspondront au dernier utilisateur qui a modifié le fichier et le groupe sera toujours `smbarchives`. Voici la configuration dans `/etc/samba/smb.conf` à la fin qui permet de configurer les partages.

```
#############################################################################
#############################################
# partage archives audiovisuelles 2007 en acces lecture pour serveur Web
[aav-1-b2]
   comment = acces archives
   path = /mnt/aav-1-b2
   valid users = zope
   read only = yes
   writable = no
   browsable = yes
   hide dot files = yes
   veto files = /lost+found/.DS_Store/._.DS_Store/.bash*/
   delete veto files = yes
   oplocks = yes
```

```
#############################################################################
##########################################
#au niveau linux @smbarchives contient tous les utilisateurs : fooa, zope...
# partage archives audiovisuelles 2007 en acces ecriture pour (admin des
archives)
[aav-1-b2-w]
   comment = archives ecriture
   path = /mnt/aav-1-b2
   #@smbarchives pour un groupe
   valid users = fooa, foob, archiveur

   read only = no
   writable = yes
   browsable = yes

#positionnement des droits maximums des fichiers (lecture ecriture sur les
fichiers pour proprio et groupe seulement)
   create mode = 0660
#forcer les droits des fichiers
   force create mode = 0660
#positionnement des droits maximums des repertoires (tout les droits pour le
proprio et le groupe seulement)
   directory mode = 0770
#forcer les droits des repertoires
   force directory mode = 0770
#forcer l'attribution du groupe des fichiers et repertoires (realise sur le
dossier de montage avec un setGID (chmod g+s aav-2-b2)
   force group = smbarchives

   hide dot files = yes
   veto files = /lost+found/.DS_Store/._.DS_Store/.bash*/
   delete veto files = yes
   oplocks = yes

#############################################################################
##########################################"
#partages dedie admin archives pour archives temporaires
[aav-2-b2-w]
   comment = archives supplementaires en ecriture
   path = /mnt/aav-2-b2
   valid users = fooa, foob

   read only = no
   writable = yes
   browsable = yes

#positionnement des droits maximums des fichiers (lecture ecriture sur les
fichiers pour proprio et groupe seulement)
   create mode = 0660
#forcer les droits des fichiers
   force create mode = 0660
```

```
#positionnement des droits maximums des repertoires (tout les droits pour le
proprio et le groupe seulement)
   directory mode = 0770
#forcer les droits des repertoires
   force directory mode = 0770

#forcer l'attribution du groupe des fichiers et repertoires (realise sur le
dossier de montage avec un setGID (chmod g+s aav-2-b2)
   force group = smbarchives

   hide dot files = yes
   veto files = /lost+found/.DS_Store/._.DS_Store/.bash*/
   delete veto files = yes
   oplocks = yes

##############################################################################
##########################################"
# partage pour espace supplementaire
[aav-3-b2-w]
   comment = espace archives 3
   path = /mnt/aav-3-b2
   valid users = fooa, foob

   read only = no
   writable = yes
   browsable = yes

#positionnement des droits maximums des fichiers (lecture ecriture sur les
fichiers pour proprio et groupe seulement)
   create mode = 0660
#forcer les droits des fichiers
   force create mode = 0660
#positionnement des droits maximums des repertoires (tout les droits pour le
proprio et le groupe seulement)
   directory mode = 0770
#forcer les droits des repertoires
   force directory mode = 0770

#forcer l'attribution du groupe des fichiers et repertoires (realise sur le
dossier de montage avec un setGID (chmod g+s aav-2-b2)
   force group = smbarchives

   hide dot files = yes
   veto files = /lost+found/.DS_Store/._.DS_Store/.bash*/
   delete veto files = yes
   oplocks = yes
```

Autre exemple de partage fonctionnel.

```
[exemple_share]
  comment = partage d'infrastructure
```

```
  path = /var/share
  guest ok = yes
  read only = no
  writable = yes
  browsable = yes

  hide dot files = yes
  veto files = /lost+found/.DS_Store/._.DS_Store/
  delete veto files = yes
  oplocks = yes
```

SElinux

Configuration de SELinux pour autoriser l'accès en rw.

```
setsebool -P samba_export_all_rw on
```

Nom des partages mis en place

Sur servbaie1.

- bureautique-b1
- espace-1-b1
- sauv-serv-b1

Sur servbaie2.

- aav-1-b2
- aav-2-b2
- aav-3-b2

Montage à partir des clients

Pour monter un partage samba d'un MAC OS

```
mount_smbfs -W WORKGROUP //user:mdp@servbaie2/nompartage /Volumes/share
killall Finder
```

Le montage permanent via MAC OS est difficile car confus via l'interface. Il sera réalisé via le logiciel AutomountMaker qui est simple d'utilisation. Son installation et sa configuration est détaillée dans le Wiki.

Pour monter avec GNU/Linux

J'ai classiquement conservé le protocole smbfs pour le montage. Cependant, l'utilisation de cifs est conseillé pour le serveur d'archive car il évite une erreur de taille de fichiers limité à 2 Go lors de restauration (assez étrange ma foi). Dans le cas de création de bande smbfs peut être utilisé sans problème.

En prenant exemple pour le serveur Web.

```
(connecté en root) mount -t smbfs -o username=zope //servbaie2/aav-1-b2
/mnt/aav-1-b2
```

Pour démonter.

```
umount /mnt/aav-1-b2
ou
(connecté en utilisateur de base) smbmount \\\\servbaie2\\aav-1-b2
/mnt/aav-1-b2 -o username=zope
```

Pour démonter.

```
smbumount /mnt/aav-1-b2
```

Montage permanent dans `/etc/fstab` (ne fonctionne que si on spécifie le mot de passe en plus : password=XXXXX après username)

```
//servbaie2/aav-1-b2 /mnt/aav-1-b2 smbfs username=zope 0 0
```

Le moyen de lister les partages CIFS d'une machine à l'aide du compte user.

```
smbclient --ip-address=10.188.147.69 -L NAS -U user
```

SWAT

SWAT (SaMBa Web Administration Tool) est un utilitaire Web qui permet de créer et gérer la configuration de SaMBa. Personnellement je ne conseille pas son utilisation. La connaissance des directives dans le fichiers `smb.conf` est beaucoup plus propre et on risque moins de casser la configuration surtout en ce qui concerne la base de comptes. De plus, la connexion n'est pas sécurisée. Cependant, il est tout de même possible d'essayer de l'utiliser si l'interface graphique intéresse.

Avant toutes choses, commencer par copier le fichier de configuration de samba.

```
cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
```

Installation SWAT

Installer le paquetage.

```
up2date samba-swat
```

Modifier `/etc/xinet.d/swat`.

```
vi /etc/xinetd.d/swat
```

Commenter.

```
only_from = 127.0.0.1
```

Mettre disable à la valeur no.

```
disable  = no
```

Redémarrer xinetd.

```
service xinetd restart
```

On peut accéder à la configuration de samba via l'URL suivante.

```
http://adresseIP:901
```

La page d'administration contient le lien vers SWAT.

Principal Intérêt

Le principal intérêt de SWAT réside dans la visibilité qu'il offre avec l'onglet status. On dispose d'informations intéressantes. On peut notamment savoir si des fichiers sont utilisés ou tout simplement qui a monté les partages. On peut ainsi prévenir l'utilisateur d'une coupure momentané pour une modification de configuration qui nécessite un redémarrage du service.