# rôle member server, security ADS


Je vais vous montrer une des configurations de samba le rôle `member server`, quand on veut faire un serveur de partage de fichier avec l'authentification dans un domaine windows existant, en gardant la possibilité de créer des logins locaux. Pour l'installation, regardé Installation d'un serveur SAMBA 4, car l'article est basé sur cet article.

D'abord, il nous faudra installer le service suivant :

- ntp : pour synchroniser notre temps avec le contrôleur de domaine windows

## installation d'un service NTP

Avant de récupérer un ticket auprès d'un contrôleur de domaine "**DC**" Windows, il faut configurer notre client NTP (/etc/ntp.conf) pour que notre serveur est la même heure que le DC Windows, cela peut éviter certain problème de synchronisation du temps. Installation de `ntp`:

```
aptitude install ntp ntpdate
```

Nous allons éditer la configuration de `ntp` qui est dans le fichier `ntp.conf`

```
vim /etc/ntp.conf
```

Commenter les lignes `server` et ajoute vos DC:

```
server XXX.XXX.XXX.XXX iburst
server XXX.XXX.XXX.XXX iburst
```

Relancer le service `ntp` pour prendre en compte la modification.

```
/etc/init.d/ntp restart
```

## Configuration réseau

il faut vérifier le fichier **/etc/hosts**, Si cela n'est pas déjà fait.

```
127.0.0.1       localhost
XXX.XXX.XXX.XXX    nom.domaine.loc nom
```

Ou - `nom.domaine.loc`: représente le nom de votre serveur sur le réseau. - xxx.xxx.xxx.xxx : représente son IP

Vérifier les DNS que vous avez saisis dans le fichier **/etc/resolv.conf**, Si cela n'est pas déjà fait.

```
search domain.loc
domain domain.loc
```

```
nameserver XXX.XXX.XXX.XXX
nameserver XXX.XXX.XXX.XXX
```

XXX.XXX.XXX.XXX : représente les IPs de vos DCs Windows.
Modifier le fichier `/etc/network/interfaces` pour lui donner une configuration `IP static`, Si cela n'est pas déjà fait.

```
auto ethX
iface ethX inet static
     address XXX.XXX.XXX.XXX
     netmask XXX.XXX.XXX.XXX
     gateway XXX.XXX.XXX.XXX
```

Relancer le service `networking` pour prendre la modification en compte.

```
/etc/init.d/networking restart
```

## Configuration de Kerberos client

Après, nous allons pouvoir commencer à configurer Kerberos client pour qu'il aille chercher un ticket auprès du DC.
Editez le fichier /etc/krb5.conf et modifier le pour avoir ceci :

```
[libdefaults]
 default_realm = DOMAINE.LOC
[realms]
  DOMAINE.LOC = {
  kdc = DC.domain.loc
  admin_server = DC.domaine.loc
 }
[domain_realms]
 .DC.domaine.fr = DOMAINE.LOC
 test.local = DOMAINE.LOC
```

Maintenant, nous allons récupérer un ticket sur le DC Windows:

```
kinit administrator
```

Une fois cette étape passée vous pouvez vérifier que vous avez bien un ticket avec la commande:

```
klist
```

## Configuration de Samba

Édité ou créé le fichier `smb.conf` (/usr/local/samba/etc/smb.conf)

```
vim /usr/local/samba/etc/smb.conf
```

Voici, la configuration :

```
[global]
workgroup = DOMAINE
realm = domaine.loc
security = ADS
passdb backend = tdbsam
auth methods = sam winbind
server role = member server
server string = samba %v
netbios name = <NOM-SERVEUR>
encrypt passwords = yes
null passwords = yes
machine password timeout = 604800
obey pam restrictions = yes
template homedir = /home/%D/%U
winbind enum users = yes
winbind enum groups = yes
winbind separator = +
idmap uid = 50-9999999
idmap gid = 50-9999999
template shell=/bin/sh
load printers = no
printcap name = /dev/null
disable spoolss = yes
log file = /var/log/samba/%m.log
log level = 3
max log size = 100

[homes]
comment = Home Directories
read only = no
create mask = 0770
directory mask = 0770
invalid users =
valid users = %S,%D+%S
write list = %S,%D+%S
read list =

[rep_partage]
comment = rep_partage de test
path = /share/rep_partage
readonly = no
create mask = 0770
directory mask= 0770
force user =
force group =
invalid users = user2,DOMAINE+user4
valid users = @groupe1,user1,user3,@DOMAINE+GROUPE
write list = @group1,user1,@DOMAINE+GROUPE
```

```
read list= user3
```

Modifier <NOM-SERVEUR> dans l'option `netbios name`
**@DOMAINE_AD+groupe_AD** : vous n'êtes pas obligé d'ajouter le groupe, le login suffit, mais c'est pour montrer la syntaxe

## script de Lancement

Je me suis fabriqué un petit script de lancement samba.tar.gz, il vous suffit de le récupérer, de le décompresser :

```
tar -xvzf samba.tar.gz
```

De le mettre dans le répertoire de lancement `init.d`:

```
mv samba /etc/init.d/
```

Lui mettre les bons droits et le bon propriétaire, si ce n'est pas déjà fait.

```
chown root:root /etc/init.d/samba
chmod 755 /etc/init.d/samba
```

Et pour terminer d'activer le service afin que le script soit exécuté au démarrage.

```
update-rc.d samba defaults
```

J'ai fait exactement la même chose sur winbind

Pour le lancement de samba avec winbind winbind.tar.gz, il faut respecter un ordre

```
/etc/init.d/winbind  stop;  /etc/init.d/samba  restart;
/etc/init.d/winbind start
```

## Joindre le domaine

Puis, nous allons pouvoir intégrer notre serveur SAMBA dans le domaine Windows.

```
net ads join -U administrator
```

Pour vérifier, saisir ces quelques commandes :

```
wbinfo -u
wbinfo -g
```

Si, elles donnent les login et les groupes du domaine, tout est ok.

On ne peut pas encore s'authentifier sur la debian avec les logins du domaine.
Donc, pour cela nous allons faire des liens symboliques vers la `libnss_winbind.so`

```
ln -s /usr/local/samba/lib/libnss_winbind.so /lib/
ln -s /lib/libnss_winbind.so /lib/libnss_winbind.so.2
ldconfig
```

## Modification de NSS

Nous allons ensuite modifier le Name Service Switch (NSS), c'est ce qui autorise le remplacement des traditionnels fichiers Unix/Linux de configuration (par exemple /etc/passwd, /etc/group, /etc/hosts) par une ou plusieurs bases de données centralisées.
Le fichier nsswitch.conf (/etc/nsswitch.conf) :

```
 passwd:         compat winbind
 group:          compat winbind
 shadow:         compat winbind
```

Démarrer les services winbind et samba

```
/etc/init.d/samba start; /etc/init.d/winbind start
```

Le petit test vous permettra de savoir si cela est bon.

```
su DOMAIN+administrator
```

Si vous avez un prompt, c'est bon

## ACL

Penser à ajouter **DOMAINE_AD+groupe_AD** ou son groupe sur un répertoire partagé dans le fichier smb.conf

```
[rep_partage]
 comment = "rep_partage"
 path = /share/rep_partage
 readonly = no
 create mask = 0770
 directory mask = 0770
 force group =
 force user =
 invalid users=
  valid  users=DOMAINE_AD+user1  ,@DOMAINE_AD+groupe_AD,  user2,
@group2
  write  list=DOMAINE_AD+user1  ,@DOMAINE_AD+groupe_AD,  user2,
```

```
@group2
 read list=
```

**@DOMAINE_AD+groupe_AD** : vous n'êtes pas obligé d'ajouter le groupe, le login suffit, mais c'est pour montrer la syntaxe

Activer les acl dans /etc/fstab:

```
 /dev/mapper/VG0-share /share           ext4
defaults,acl,user_xattr,barrier=1        0       2
```

Installer les acls:

```
 aptitude install acl
```

Puis modifier les acls:

```
 setfacl -R -m g:"DOMAINE_AD+groupe_AD":rwx /home/share
```

**Pour les logins locaux :**
Ajouter un login :

```
 addgroup sambausers
 useradd -m -g sambausers toto
 smbpasswd -a toto
```

Ensuite, vous n'avez plus qu'a ajouté les droits associé au répertoire de partage, sinon Samba autorisera l'accès, mais pas le système Linux.
exemple:

```
chown toto:sambausers /share/rep_partage
```

Pour changer le mot de passe :

```
 smbpasswd toto
```

Pour supprimer un login de la base Samba :

```
smbpasswd -x toto
```

Quand vous supprimez un login de la base de samba, il n'est supprimer de Linux

## Autres

Affiché les connexions actives via Samba :

```
smbstatus -v
```

Pour effacer toutes la configuration de samba (fichier de configuration et base local)

```
rm -f /usr/local/samba/etc/smb.conf
rm -rf /usr/local/samba/private/*
```

Source: wikipedia samba.org