

## Installation de samba avec une authentification sur un CPD NT4.0 ou 2000

IrOnUx

authentifier les utilisateurs samba au niveau d'un CPD NT

---

### Mise en garde

La configuration présentée a été réalisée sur une Redhat 7.3, il ne devrait pas y avoir beaucoup de changement avec les versions plus récentes. Je ne peux par contre pas certifier cette configuration sur d'autres distributions, n'ayant pas fait les tests. Vous devez au préalable avoir lu la doc pour configurer samba en tant que PDC, BDC.

### Le problème

Il est bien connu que les systèmes Microsoft et Unix ont une façon différente de gérer leur base d'utilisateurs. Une difficulté est alors rencontrée lorsque l'on veut intégrer un serveur Samba dans un réseau de machines NT. En théorie il faudrait créer sur le serveur samba les comptes systèmes correspondant aux comptes du domaine mais aussi les comptes Samba. Pourquoi ne pas simplifier la tâche en faisant en sorte de n'administrer qu'une seule base de compte.

Pour cela, on utilise winbind. Winbind est un système client-serveur qui permet entre autre d'introduire facilement des serveurs Samba dans un domaine où se trouvent déjà des CPD (CPD ou PDC : contrôleur primaire de domaine) NT. Comment ? Il se charge en fait de récupérer la base des utilisateurs sur le CPD NT et procède à une authentification de celui-ci.

### Installer Samba

La première étape consiste, d'abord, à installer Samba. Si vous avez une version de Samba déjà installée alors désinstallez-là, car nous avons besoin de fonctionnalités qui ne se trouvent pas dans les versions livrées avec la plupart des distributions.

Sur une distribution à base de RPM (RedHat, Mandrake ou SuSE), pour voir si une version de samba est installée, tapez la commande : `# rpm -q samba`. S'il existe déjà une version de Samba sur votre système alors supprimez-là avec la commande `# rpm -e samba`.

Une fois que vous avez bien désinstallé Samba, il va falloir récupérer les sources de la dernière version. La version utilisée ici est 2.2.8.

Tout d'abord, décompressez l'archive dans un répertoire. On va maintenant installer Samba:

```
cd samba-2.2.8a
# cd sources
# ./configure --enable-cups --with-smbwrapper --with-dce-dfs --with-smbmount --with-pam --with-pam_smbpass --with-syslog
--with-quotas --with-libsmbclient --with-acl-support --with-winbind --with-winbind-auth-challenge
```

Pour savoir ce que signifient ces options, vous pouvez taper la commande `./configure --help`, cette commande vous retournera une liste des différentes options possibles avec une description.

Si la commande `./configure . . . . .` retourne une erreur, tentez d'analyser ce qui est dit pour trouver l'erreur. Si vous n'avez pas d'erreurs ce qui est probablement le cas, vous pouvez compiler et installer Samba. Pour ce faire :

```
# make
# make install
# make installbin
# make installman
```

Voilà, samba est normalement bien installé. Les fichiers se trouvent dans `/usr/local/samba`. Il va falloir maintenant créer un script d'initialisation pour les trois démons `smbd`, `nmbd` et `winbindd`. Vous trouverez un script en annexe qui fonctionne très bien sur Redhat, inspirez-vous en sur les autres distributions. Vérifier notamment que les chemins (*path*) sont corrects par rapport à votre configuration.

[Le script en question.](#)

Sur une RedHat ou Mandrake, copiez le script dans `/etc/init.d`, rendez-le exécutable : `chmod +x /etc/init.d/smb`, puis activez les services samba au démarrage : `chkconfig --add smb`. Enfin, démarrez pour cette session : `/etc/init.d/smb start`.

### Configurer samba

Avant de lancer samba il va falloir éditer le fichier de configuration et les autres fichiers nécessaires au bon fonctionnement de la paire samba/winbind. Je vous présente, à titre indicatif au niveau des partages, mon `smb.conf`. A noter que ce fichier doit se trouver dans le répertoire `/usr/local/samba/lib`.

```
[global]
```

```
#Chaîne de description du serveur samba
server string = SambaBSD-2.2.8
```

```
#Définit le nom netbios principale du serveur samba
netbios name = SambaBSD
```

```
# Définit le groupe netbios de machines auquel
# le serveur appartient ici le nom du domaine.
workgroup = sztitechinf

# Nom et emplacement du fichier journal de samba. Les variables
# standards de samba peuvent être utilisées.
log file = /var/log/samba/%m.log

# Taille maximale des fichiers log.
max log size = 100

# Samba fait parité d'un domaine windows
security = domain

# Cette option sert à indiquer le CPD ici le caractère de
# substitution * ordonne à samba de rechercher le CPD lui-même.
password server = *

# Comme son nom l'indique cette option sert à crypter les mots de
# passe, il faudra au préalable appliquer un patch sur les stations
# NT ce patch peut être trouvé dans le répertoire doc de samba il sert
# à activer les plaintextpassword sous NT
encrypt passwords = yes

# Chemin du fichier de mot de passe de samba
smb passwd file = /usr/local/samba/bin/smbpasswd

# les lignes suivantes sont utiles pour pouvoir changer le mot de passe
# et ajouter des utilisateurs à partir de serveurs windows. A utiliser avec
# "encrypt passwd" et "smb passwd file"
unix password sync = yes
passwd program = /usr/bin/passwd
passwd chat = *New*password* %n\n *Retype*new*password* %n\n *passwd:*all*authentication*tokens*updated*successfully*
add user script = /usr/sbin/useradd %u -g smbusers
delete user script = /usr/sbin/userdel %u
allow trusted domains = yes

# Support de l'ACL Microsoft
nt acl support = yes

# Séparateur winbind. Avec + les utilisateurs auront la forme
# domaine+nom_d'utilisateur.
# les séparateurs peuvent être + ou /. Toutes les options qui
# suivent sont indispensables pour le bon fonctionnement de
# winbind
winbind separator = +
winbind cache time = 10
template shell = /bin/bash
template homedir = /home/%D/%U
winbind uid = 10000-20000
winbind gid = 10000-20000

socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

#Si égale à yes, samba tentera de devenir explorateur principal
#du sous-réseau local.
local master = no

# Fixe le niveau de l'os de samba lors de l'élection de
# l'explorateur local principal.
os level = 33

#Si égale à yes, samba tentera alors de devenir explorateur
# principal de domaine du groupe de travail.
domain master = no

# Samba utilisera le bit de l'explorateur principal favori pour devenir
# explorateur local principale si cette valeur est égale à yes.
preferred master = no

# Ici on indique le serveur wins du réseau.
wins server = 10.35.36.250
```

```
# égale a yes, samba conservera la casse fourni par le client
# sans convertir par la classe par défaut.
preserve case = yes
# Si égale à yes, samba distinguera les majuscules des
# minuscules lors de l'utilisation des fichiers.
case sensitive = no

# Ce premier partage va servir à créer un répertoire personnel
# pour l'utilisateur du domaine qui viendra se connecter.
[homes]
comment = Home Directory
browseable = no
writable = yes
valid users = %S
create mode = 0664
directory mode = 0775
```

```
[public]
path = /partage/public
public = yes
only guest = yes
writable = yes
printable = no
```

### Le fichier nsswitch.conf

Nous avons donc maintenant un fichier `smb.conf` opérationnel, il ne nous reste plus qu'à nous tourner vers `winbind` car nous avons terminé la partie dédiée purement à samba. Pour que `winbind` fonctionne correctement avec samba il va falloir éditer quelques fichiers.

Tout d'abord éditez le fichier `/etc/nsswitch.conf`, dans ce fichier vous allez devoir ajouter `winbind` à la ligne `groupe` et `user` :

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

Vérifiez ensuite que vous disposez bien des bibliothèques nécessaires `/lib/libnss_winbind.so` et `/lib/libnss_winbind.so.2`, ces bibliothèques se trouvent, si elles ne sont pas installées, dans les sources de samba. Si la bibliothèque `libnss_winbind.so.2` n'existe pas mais que l'autre est présente alors exécutez la commande suivante: `# ln -s /lib/nss_winbind.so /lib/libnss_winbind.so.2`.

### Configurer pam.d

Maintenant la dernière étape. Il va falloir éditer quelques fichiers se trouvant dans le répertoire `/etc/pam.d`. Ce sont ces fichiers qui définissent la sécurité des authentifications. Je vous montre ci-après les trois fichiers qu'il faut modifier afin que samba utilise le CPD pour authentifier et afin que l'on puisse se logger sur une Linux box avec un compte NT.

Le fichier `/etc/pam.d/samba`

```
##%PAM-1.0
#auth required pam_nologin.so
#auth required pam_stack.so service=system-auth
auth required /lib/security/pam_winbind.so
auth required /lib/security/pam_pwdb.so nullok shadow
account required /lib/security/pam_winbind.so
account required /lib/security/pam_pwdb.so
#account required pam_stack.so service=system-auth
session required pam_stack.so service=system-auth
password required pam_stack.so service=system-auth
```

Le fichier `/etc/pam.d/auth-config`

```
##%PAM-1.0
#auth sufficient /lib/security/pam_rootok.so
#auth required /lib/security/pam_stack.so service=system-auth
#account required /lib/security/pam_permit.so
#session optional /lib/security/pam_xauth.so
#session required /lib/security/pam_permit.so
auth required /lib/security/pam_securetty.so
auth required /lib/security/pam_nologin.so
auth sufficient /lib/security/pam_winbind.so
auth required /lib/security/pam_pwdb.so use_first_pass shadow nullok
account required /lib/security/pam_winbind.so
```

Et enfin le fichier `/etc/pam.d/login`

```
##%PAM-1.0
auth required /lib/security/pam_securetty.so
auth sufficient /lib/security/pam_winbind.so
auth sufficient /lib/security/pam_unix.so use_first_pass
auth required /lib/security/pam_stack.so service=system-auth
auth required /lib/security/pam_nologin.so
account sufficient /lib/security/pam_stack.so service=system-auth
account sufficient /lib/security/pam_winbind.so
password required /lib/security/pam_stack.so service=system-auth
```

Vous pouvez éditer d'autres fichier `pam.d` afin que les applications voulues utilisent winbind pour s'authentifier.

### Adjoindre le serveur au domaine

Il nous faut maintenant joindre notre serveur samba au domaine, vous devez pour cela taper la commande:

```
# /usr/local/samba/bin/smbpasswd -j nom_du_domaine -r nom_cpd -U administrateur%motdepasse
```

`administrateur%motdepasse` étant un compte autorisé à joindre des machines au domaine. Après avoir tapé cette commande cela devrait vous retourner quelque chose comme: `Domain toto joined.`

### Test

Voilà nous allons maintenant lancer samba avec le script donné en annexe. Editez ce script, vérifiez si les chemins correspondent avec votre configuration. Coller ce script dans le répertoire `/etc/rc.d/init.d` et rendez-le exécutable.

Pour démarrer samba, exécutez tout simplement la commande :

```
#service smb start
```

ou alors :

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

Si vous n'utilisez pas une distribution "RedHat" ou "Mandrake", adaptez le script fourni, ainsi que la procédure de lancement

Vous devriez voir les trois démons `nmbd`, `smbd` et `winbindd`, se lancer. Pour vérifier s'ils sont bien lancés, vous pouvez taper la commande :

```
# ps -ae | grep -E "(smbd|nmbd|winbindd)"
```

Si la commande vous retourne 3 lignes, c'est que les 3 démons sont bien lancés.

Le premier test que l'on peut faire consiste à taper la commande :

```
#wbinfo -u
```

Cette commande devrait nous retourner les différents utilisateurs sur le CPD.

Vérifiez que l'authentification se fait bien en tapant la commande :

```
#wbinfo -a utilisateur%motdepasse
```

Si tout cela fonctionne bien, vérifiez avec les commandes :

```
# getent passwd
# getent group
```

que winbind arrive bien à récupérer les noms d'utilisateurs sur le CPD NT.

Vous pouvez normalement maintenant accéder au serveur samba en utilisant vos logins NT et sans avoir besoin d'administrer deux bases de comptes.