# Intégration de Samba dans un Active Directory

## >>> Debian & Microsoft Windows server 2008 R2 Français

**Description :**

**Dans ce cours nous allons apprendre à configurer Samba qui utilisera les comptes utilisateur de Active Directory.**

**L'utilisation de clef RSA vous permet d'augmenter la sécurité au niveau de l'administration à distance de vos serveurs.**

# Intégration de Samba dans un Active Directory

### >>> Debian & Microsoft Windows server 2008 R2 Français

L'utilisation de clef RSA vous permet d'augmenter la sécurité au niveau de l'administration à distance de vos serveurs.

**Sommaire :**



---

Quelques informations :
- Adresse IP du serveur samba : 192.168.1.2
- Adresse IP du serveur DNS + AD : 192.168.1.3
- Nom du serveur samba : Fraise
- Nom du serveur DNS + AD : Cerise
- Nom du domaine : dumca.eu
- Nom NETBIOS : DUMCA

---

# I) Installation et Configuration du serveur de fichiers

## 1) Configuration du serveur

Commencez par vérifier si votre configuration IP est statique :

```
cat /etc/network/interfaces
```

Ensuite configurez votre fichier resolv.conf pour ajouter le serveur DNS local :

```
vim /etc/resolv.conf
```

Votre fichier resolv.conf doit ressembler à ça :

```
search dumca.eu
domain dumca.eu
nameserver 192.168.1.3
nameserver 8.8.8.8
```

Maintenant mettons le serveur à jour :

```
aptitude update
aptitude -y safe-upgrade
```

On met le serveur à l'heure via un serveur NTP, sinon le serveur AD va nous refuser.

```
aptitude install -y ntpdate
ntpdate pool.ntp.org
```

Et pour finir la préparation du serveur nous allons modifier le fichier /etc/hosts :

```
vim /etc/hosts
```

A la première et deuxième ligne du fichier on doit trouver ceci :

```
127.0.0.1 localhost
192.168.1.2     fraise.dumca.eu                 fraise
```

On configure aussi le fichier /etc/hostname

```
vim /etc/hostname
```

Pour obtenir ceci :

```
fraise
```

Pour finir tapez cette commande :

```
hostname fraise
```

On vérifie que la configuration du Hostname est correcte :

```
hostname -f
```

Vous devez obtenir ceci :

```
fraise.dumca.eu
```

## 2) Création des dossiers partagé

Nous allons créer deux répertoires, un répertoire pour tous les utilisateurs de l'Active Directory puis un deuxième répertoire contenant tous les répertoires personnels. Ce dossier devra porter le nom NetBIOS en majuscule.

```
mkdir /home/partage
mkdir /home/DUMCA
```

Puis on attribut les droits 777 aux répertoires :

```
chmod 777 /home/partage
chmod 777 /home/DUMCA
```

## 3) Installation et Configuration de Samba

On commence par installer samba :

```
aptitude install samba
```

Et on sauvegarde le fichier de configuration :

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

Pour finir on configure le fichier smb.conf :

```
[global]
        NetBIOS name = fraise
        server string = Serveur de fichiers
        socket options = TCP_NODELAY SO_RCVBUF=16384 SO_SNDBUF=16384
        idmap uid = 10000-20000
        idmap gid = 10000-20000
        workgroup = DUMCA
        os level = 20
        preferred master = no
        max log size = 50
        log file = /var/log/samba3/log.%m
        encrypt passwords = yes
        dns proxy = no
        realm = DUMCA.EU
        security = ADS
        obey pam restrictions = yes

        winbind use default domain = yes
        winbind enum groups = yes
        winbind enum users = yes
        winbind gid = 10000-20000
        winbind separator = +
        winbind cache time = 10
        template shell = /bin/bash
```

```
        template homedir = /home/%D/%U

        invalid users = root

[partage]
        comment = Dossier pour les utilisateurs du domaine
        path = /home/partage
        browseable = yes
        writeable = yes
        create mask = 700
        directory mask = 700
        valid users = @\"DUMCA+utilisateurs du domaine\"

[homes]
   comment = Home Directories
   browseable = no
   writeable = yes
```

Voilà la configuration de samba est faite, mais on va quand même expliquer un peu.
**– NetBIOS name** : Nom de la machine samba.
**– server string** : Description du serveur samba.
**– Workgroup** : Correspond au nom NetBIOS du domaine (n'oubliez pas de l'écrire en MAJUSCULE).
**– realm** : Nom du domaine (n'oubliez pas de l'écrire en MAJUSCULE).
**– security** : ce paramètre permet de déterminer quel type de sécurité samba doit appliquer sur les partages, nous avons mis ADS pour Active Directory Security.
**– obey pam restrictions = yes** : Permet d'intégrer les comptes AD dans Pam.
**– invalid users = root** : Pour plus de sécurité nous interdisons les connexions avec l'utilisateur root.
**– [partage]** : Nom du dossier qui sera affiché sur le réseau.
**– comment** : Description du dossier.
**– path** : Désigne le chemin du dossier partagé.
**– browseable** : Permet d'afficher ou de cacher le dossier sur le réseau.
**– writeable** : Permet d'autoriser l'écriture dans le dossier.
**– valid users** : Désigne les utilisateurs ou les groupes autorisés à accéder au répertoire.
**– [homes]** : homes est un nom spécial, car il va afficher sur le réseau un dossier au nom du login. (exemple : nom de login : lrattif, le dossier lrattif sera affiché sur le réseau.

# 4) Installation de Winbind

Winbind est un logiciel permettant de faire la liaison entre le monde Unix et le monde Microsoft. Nous avons juste besoin de l'installer :

```
aptitude install winbind
```

Winbind n'a pas de fichier de configuration à lui, il se rajoute dans les fichiers de configuration des autres logiciels.

# 5) Installation et configuration de Kerberos

Comme toujours on commence par installer avant de configurer :

```
aptitude install -y krb5-user
```

L'installation faite, passons à la sauvegarde du fichier de configuration :

```
cp /etc/krb5.conf /etc/krb5.conf.old
```

Enfin nous passons à la configuration :

```
vim /etc/krb5.conf
```

Configurez votre fichier comme ceci :

```
[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
default_realm = DUMCA.EU
dns_lookup_realm = false
dns_lookup_kdc = false
ticket_lifetime = 24h
forwardable = yes

[realms]
DUMCA.EU = {
    kdc = cerise.dumca.eu
    admin_server = cerise.dumca.eu
    default_domain = dumca.eu
}

[domain_realm]
.kerberos.server = DUMCA.EU
.dumca.eu = DUMCA.EU
dumca.eu = DUMCA.EU

[kdc]
profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]
pam = {
    debug = false
    ticket_lifetime = 36000
    renew_lifetime = 36000
    forwardable = true
    krb4_convert = false
}
```

**Respectez bien les minuscules et les MAJUSCULES c’est important.**

# 6) Configuration de "nsswitch.conf

Commençons par la sauvegarde du fichier :

```
cp /etc/nsswitch.conf /etc/nsswitch.conf.old
```

Nous éditons le fichier :

```
vim /etc/nsswitch.conf
```

Recopiez ceci :

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

#hosts: db files nisplus nis dns
hosts: files dns wins

# Example - obey only what nisplus tells us...
#services: nisplus [NOTFOUND=return] files
#networks: nisplus [NOTFOUND=return] files
#protocols: nisplus [NOTFOUND=return] files
#rpc: nisplus [NOTFOUND=return] files
#ethers: nisplus [NOTFOUND=return] files
#netmasks: nisplus [NOTFOUND=return] files

bootparams: nisplus [NOTFOUND=return] files
ethers: db files
netmasks: files
networks: files dns
protocols: db files
rpc: files
services: files
netgroup: files
publickey: nisplus
automount: files
aliases: files nisplus
```

# 7) Intégrations du serveur dans le domaine Active Directory

Nous redémarrons les différents services que nous avons configurés ci-dessus.

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

Ensuite on fait une requête de jetons Kerberos :

```
kinit Administrateur
```

**– Administrateur** : Correspond au nom du compte administrateur du domaine.

On vérifie que nous avons bien récupéré un ticket valide

```
klist
```

**–** Les informations suivantes devraient s’afficher :

```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: Administrateur@DUMCA.EU

Valid starting     Expires            Service principal
08/25/10 19:34:14  08/26/10 05:36:04  krbtgt/DUMCA.EU@DUMCA.EU
        renew until 08/26/10 19:34:14

Kerberos 4 ticket cache: /tmp/tkt0
klist: You have no tickets cached
```

Maintenant que nous avons le ticket Kerberos nous pouvons faire une demande pour joindre le serveur Active Directory.

```
net join -U Administrateur
```

Le message suivant devrait s'afficher :

```
Using short domain name -- DUMCA
Joined 'HOLA' to realm 'dumca.eu'
```

# 8) Configuration de "Pam.d"

La configuration suivante n'est pas obligatoire pour le fonctionnement de samba, sauf si vous voulez utiliser les comptes AD pour se connecter sur le serveur Samba. Elles vont permettre aussi de créer automatiquement un dossier personnel lors de la première connexion de l'utilisateur AD au serveur, ou lors du premier accès au fichier partagé.

Commençons par sauvegarder les fichiers configurations :

```
cp /etc/pam.d/common-account /etc/pam.d/common-account.old
cp /etc/pam.d/common-auth /etc/pam.d/common-auth.old
cp /etc/pam.d/common-session /etc/pam.d/common-session.old
```

On édite le fichier "common-account" :

```
vim /etc/pam.d/common-account
```

Pour mettre ceci :

```
account    sufficient    pam_winbind.so
account    required    pam_unix.so
```

On édite le fichier "common-auth" :

```
vim /etc/pam.d/common-auth
```

Pour mettre ceci :

```
auth    sufficient    pam_winbind.so
auth    required    pam_unix.so use_first_pass nullok_secure
```

Pour finir on édite le fichier **"common-session"** :

```
vim /etc/pam.d/common-session
```

Pour mettre ceci :

```
session    required    pam_mkhomedir.so skel=/etc/skel/ umask=0066
session    sufficient    pam_winbind.so
session required    pam_unix.so
```

# II) Installation avec le script

Pour simplifier l'intégration du serveur de fichiers (samba) dans un domaine active directory, j'ai réalisé ce petit script en BASH. Ce script reprend toutes les étapes ci-dessus.

## 1) Récupération du script

Pour récupérer mon script, faite :

```
wget http://idum.fr/Telechargements/Scripts/SambaAD/script_v11.sh
```

## 2) Exécution du script

Une fois téléchargé, lancez le script :

```
bash script_v10.sh
```

(La commande "bash" permet de lancer le script sans attribuer les droits d'exécutions)

Le script s'exécute, Il commence par vous poser quelques questions :
- le nom de votre domaine
- le nom de la machine samba
- l'adresse IP du serveur samba
- le nom de votre serveur Active Directory
- l'adresse IP de votre serveur DNS local
- l'adresse d'un serveur DNS public
- le login de l'administrateur du domaine
- la description du serveur Samba
- le nom du dossier partage
- la langue de votre Active directory est en Français ou en Anglais.

Au cours de l'installation le script vous affichera trois écrans bleus, faite "Entrée" directement.

A la fin de la configuration le script vous demandera deux fois le mot de passe de votre compte administrateur, puis votre serveur va redémarrer pour prendre en compte toutes les modifications.