



Publié sur **COAGUL** (<http://coagul.org/drupal>)

[Accueil](#) > [Rubriques](#) > [Publications](#) > [Réseaux](#) > PDF imprimable

Intégrer un poste Debian dans un domaine Windows

ven, 02/09/2005 - 01:00 — Tony

[Réseaux](#) ^[1]

But de ce document

Ce document me sert de mémo pour intégrer un poste bureautique sous Debian Testing dans un domaine contrôlé par un serveur Windows NT.

Le but de ce document est d'arriver à se connecter sur le poste Debian avec un utilisateur quelconque du domaine. De plus, il est prévu de monter automatiquement les dossiers partagés par les serveurs du domaine en fonction des droits de l'utilisateur qui se connecte.

Pré-requis

Avoir installé une Debian de Base : http://www.coagul.org/article.php3?id_article=158 ^[2]

Avoir installé KDE : http://www.coagul.org/article.php3?id_article=159 ^[3]

Installation de Winbind

Winbind permet d'intégrer les utilisateurs et les groupes du domaine au poste Linux.

Paquet à installer :

```
# apt-get install winbind
```

Si samba n'est pas installé, Winbind demandera son installation. La configuration de Winbind se fait avec le fichier de configuration de samba (smb.conf).

Remarque : Pour ce mémo, Il n'est pas obligatoire d'installer la partie serveur de Samba (le paquet « samba-client » suffit). Si des questions sont posées lors de l'installation des paquets, il faut laisser les réponses par défaut.

Configuration de /etc/nsswitch.conf

Ce fichier permet d'indiquer le programme qui s'occupe de la gestion des utilisateurs :

Il faut simplement ajouter **winbind** et **wins** comme indiqué dans l'exemple ci-dessous :

```
passwd: compat winbind
group: compat winbind
shadow: compat
hosts: files dns wins
networks: files
protocols: db files
services: db files
ethers: db files
rpc: db files
netgroup: nis
```

Configuration de /etc/samba/smb.conf

Le fichier « **smb.conf** » est utilisé pour configurer **Samba** mais également **Winbind**.

A chaque modification du fichier **smb.conf**, il faut recharger la configuration de **Samba** :

```
# /etc/init.d/samba reload
```

Si la partie concernant **Winbind** est modifiée, il faut redémarrer **Winbind** :

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

Même si le poste Linux ne propose pas de dossier partagé, il est nécessaire de configurer Samba pour pouvoir joindre le domaine Windows, récupérer les utilisateurs et se connecter avec un utilisateur du domaine.

Voici le début de mon fichier **smb.conf** :

```
[global]
workgroup = NomDuDomaine
netbios name = NomDuServeur
security = DOMAIN
# Adresse IP du serveur Wins
wins server = 192.168.0.1
```

La suite du fichier **smb.conf** permet de configurer **Winbind**. Il faut donc redémarrer **Winbind** à chaque modification de cette partie :

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

Le premier paramètre permet d'indiquer le caractère à utiliser comme séparateur entre le nom du domaine et le nom de l'utilisateur (J'ai choisi / car c'est le caractère utilisé par Windows) :

```
winbind separator = /
```

Les deux paramètres suivants permettent d'indiquer la plage des numéros à utiliser pour les utilisateurs ou les groupes. Ces deux lignes sont obligatoires au bon fonctionnement de Winbind. **ATTENTION** : Une fois que le poste Linux sera connecté au domaine, il ne faudra surtout pas changer la plage des numéros, car cela peut poser de gros problèmes de connexion.

```
winbind uid = 10000-20000
winbind gid = 10000-20000
```

Pour pouvoir se connecter sur le poste Linux avec un compte du domaine Windows, il est obligatoire d'indiquer l'adresse du shell à utiliser :

```
template shell = /bin/bash
```

La ligne suivante permet d'indiquer le chemin où seront enregistrés les profils des utilisateurs du domaine (%D = Nom du domaine et %U = Login de l'utilisateur). Le dossier et le profil seront créés automatiquement lors de la première connexion.

Attention : Il faut créer manuellement le dossier racine correspondant au nom du domaine (%D). Car s'il est créé automatiquement lors de la connexion du premier utilisateur, les autres utilisateurs ne pourront plus se connecter pour des problèmes de droits sur ce dossier. En cas de problème, il faut regarder les logs dans auth.log

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

La ligne suivante permet d'éviter de saisir le nom du domaine devant le nom de l'utilisateur pour pouvoir se connecter. Sans cette ligne, il faut utiliser le login « NomDuDomaine/NomDuLogin » et avec cette ligne il suffit juste de saisir comme login « NomDuLogin ».

La commande « **wbinfo -u** » permet de voir l'influence de cette ligne une fois que tout est correctement configuré.

De plus, cette ligne est obligatoire pour arriver à faire fonctionner libpam-mount pour monter automatiquement des partitions avec des utilisateurs du domaine.

```
winbind use default domain = yes
```

Voici un exemple complet et fonctionnel de fichier smb.conf :

```
[global]
#** Debut de la configuration de Winbind **
workgroup = NomDuDomaine
winbind separator = /
netbios name = NomDuServeur
winbind uid = 10000-20000
security = DOMAIN
winbind gid = 10000-20000
wins server = 192.168.0.1
template shell = /bin/bash

winbind use default domain = yes
#** Fin de la configuration de Winbind *****
```

Remarque : Cet exemple de configuration ne contient aucun dossier partagé, car la partie serveur de Samba n'est pas installée et n'est pas nécessaire.

Ajouter le serveur Samba au contrôleur de domaine Windows

Il faut commencer par arrêter le serveur Samba et éventuellement Winbind :

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

Voici la commande pour ajouter le serveur Samba au gestionnaire de serveurs du contrôleur de domaine Windows (l'utilisateur root, doit avoir l'autorisation d'ajouter des serveurs au domaine) :

```
net rpc join -U root
```

Et si tout se passe bien, le message suivant doit apparaître :

```
Joined domain MonDomaine
```

Ensuite, il faut redémarrer le serveur Winbind et le serveur Samba :

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

Quelques commandes pour vérifier que tout fonctionne

Remarque : Avant de saisir les commandes suivantes, il faut vérifier que le serveur Samba est correctement ajouté dans la liste des serveurs du « gestionnaire de serveurs » du contrôleur de domaine Windows. Si ce n'est pas le cas, il faut peut-être attendre quelques minutes pour que la mise à jour se fasse.

La commande suivante doit donner la liste des utilisateurs du domaine :

```
wbinfo -u
```

Celle-ci la liste des groupes du domaine :

```
wbinfo -g
```

Celle-ci permet de vérifier que les utilisateurs du domaine sont ajoutés à la liste des utilisateurs du serveur Linux avec les bons uid :

```
getent passwd
```

La même chose avec les groupes d'utilisateurs :

```
getent group
```

Cette commande permet de vérifier qu'un utilisateur particulier est correctement reconnu

```
wbinfo -a MonDomaine/tony%LeMotDePasse
```

La commande suivante permet d'afficher les ressources partagées par le serveur Samba « pgdebian » pour l'utilisateur « tony » :

```
smbclient -L //pgdebian -U tony
```

Montage des partitions automatiquement en fonction de l'utilisateur

Le paquet « **libpam-mount** », permet de monter et démonter des partitions automatiquement en fonction du login de l'utilisateur.

Paquet à installer :

```
apt-get install libpam-mount
```

Autres paquets à installer pour monter des partitions samba :

```
apt-get install smbfs smbclient
```

Le fichier « **/etc/security/pam_mount.conf** » est le principal fichier de configuration de « libpam-mount ». A la fin de ce fichier, il faut insérer une ligne du type :

```
volume [smbfs|ncp|nfs|local]
```

- **user** : Nom de l'utilisateur ou « * » pour tous les utilisateurs.
 - **server** : Nom ou adresse IP du serveur
 - **partage** : Nom du partage à monter.
 - **mount point** : Point de montage du partage. Si ce dossier n'existe pas, il sera créé automatiquement
 - **mount options** : Options de montage correspondant au système de fichiers à monter (Les mêmes que pour /etc/fstab). Mettre un tiret si ce paramètre n'est pas utilisé.
 - **fs key cipher** : Indique le type de clé à utiliser pour crypter (non testé). Mettre un tiret si ce paramètre n'est pas utilisé.
 - **fs key path** : Indique le chemin d'accès au fichier contenant la clé (non testé). Mettre un tiret si ce paramètre n'est pas utilisé.
- Remarque** : Si « * » est utilisé pour le paramètre , le caractère « & » correspondra au login de l'utilisateur.

Voici un exemple pour monter le dossier partagé « Utilisateurs » du serveur « pglinux » sur le point de montage « /Reseau/pglinux » pour tous les utilisateurs (Le signe correspond au répertoire home de l'utilisateur) :

```
volume * smbfs pglinux Utilisateurs ~/Reseau/pglinux - - -
```

Voici le même exemple avec des options de montage :

```
volume * smbfs pglinux Utilisateurs ~/Reseau/pglinux  
uid=&,gid=&,fmask=0700,dmask=0700,workgroup=VOTREDOMAIN,iocharset=iso8859-1,codepage=cp850 - -
```

Voici le même exemple valable uniquement pour l'utilisateur tony (Dans ce cas, le signe « & » n'est plus utilisable) :

```
volume tony smbfs pglinux Utilisateurs ~/Reseau/pglinux
uid=tony,gid=tony,mask=0700,dmask=0700,workgroup=VOTREDOMAINE,icharset=iso8859-
1,codepage=cp850 - -
```

Débugage : La première ligne de ce fichier permet également d'activer le débogage pour comprendre ce qui ne fonctionne pas :

```
debug 1
```

Si vous ne souhaitez pas que les points de montage soient créés automatiquement s'ils n'existent pas, il faut modifier la ligne suivante :

```
mkmountpoint 0
```

Pour faire fonctionner « **libpam-mount** », il faut également configurer « **pam** » comme indiqué au chapitre suivant.

Configuration de pam

Pam est un système très complet et très modulaire permettant de gérer les connexions et les autorisations sur un poste Linux. Pam permet de gérer les connexions locales ou peut utiliser une base de données LDAP ou encore les utilisateurs d'un domaine Windows.

ATTENTION : Avant de modifier la configuration de pam, il est vivement conseillé d'ouvrir une console sous root (ALT+F1) et de ne pas la fermer tant que tout ne fonctionne pas correctement. **Une mauvaise configuration de pam peut empêcher toute connexion même sous root** .

Pam se configure à l'aide des différents fichiers du dossier « **/etc/pam.d/** ». Chaque application peut avoir sa propre méthode d'authentification et c'est pour cela que nous retrouvons dans ce dossier un fichier pour chaque type de programme nécessitant une authentification (cron, cupsys, kdm, login, su, ssh,...)

Dans le cadre de ce mémo, nous allons modifier uniquement le fichier « **kdm** », car je souhaite me connecter avec un utilisateur du domaine uniquement avec kdm et pas en ssh ou en console.

Donc, il suffit d'ouvrir le fichier « **/etc/pam.d/kdm** », de commenter toutes les lignes existantes et d'ajouter les lignes suivantes :

```
auth required pam_mount.so
account sufficient pam_winbind.so nulok.obscure min=4 max=8 md5
password required pam_unix.so use_first_pass
auth sufficient pam_winbind.so
account sufficient pam_unix.so
session optional pam_khomedir.so
auth required pam_unix.so use_first_pass
session optional pam_mount.so
```

L'explication détaillée du fonctionnement de pam, dépasse très largement le cadre de ce mémo, mais voici quelques explications :

- La première ligne permet de monter les partitions. Les deux lignes suivantes indiquent que la connexion avec un utilisateur du domaine (winbind) est suffisante, mais que si celui-ci n'est pas trouvé, il cherchera un utilisateur local (unix). Remarque : Le paramètre « **use_first_pass** » permet de récupérer le mot de passe saisi pour pam_mount pour éviter de le saisir une nouvelle fois pour les comptes winbind et unix.
- La ligne avec « **pam_khomedir.so** » permet de créer automatiquement les répertoires homes et les répertoires des lecteurs réseaux s'il n'existent pas lors de leur première utilisation.
- Le paramètre « **optional** » indique que la ligne n'est pas bloquante s'il elle n'aboutit pas (si le montage d'un lecteur réseau n'aboutit pas, cela n'empêchera pas l'utilisateur de se connecter)

Test de fonctionnement

Pour tester le fonctionnement, il faut se connecter avec kdm avec un utilisateur existant en locale et faire un autre test avec un utilisateur du domaine. Il faut vérifier que les partitions sont correctement montés lors de la connexion et démontés lors de la déconnexion.

Si ça ne fonctionne pas, il faut penser à regarder les logs :

```
# tail -f /var/log/auth.log
```

Il faut peut-être aussi redémarrer kdm :

```
# /etc/init.d/kdm restart
```

Problèmes rencontrés

Problème de localisation -> Créer .xsession et choisir « Default » dans kdm.

- cf mon article sur le sujet : http://www.coagul.org/article.php3?id_article=305^[4]
Il ne faut pas utiliser de majuscule pour se connecter avec un utilisateur du domaine.

Autres articles sur le même sujet

Installation de Winbind pour intégrer Samba dans un Domaine Windows :

- http://www.coagul.org/article.php3?id_article=178^[5]
Monter automatiquement des partitions en fonction du login de connexion avec libpam-mount :
- http://www.coagul.org/article.php3?id_article=297^[6]

Historique des modifications

| Version | Date | Commentaire |
|---------|----------|--|
| 0.1 | 13/06/05 | Création par Tony GALMICHE |
| 0.2 | 15/06/05 | Nombreuses modifications suite aux remarques de Piou |
| 0.3 | 02/09/05 | Correction bug de sécurité dans PAM |
| 0.4 | 23/03/07 | smb devient smbfs dans libpam-mount |

Licence Creative Commons by-sa 3.

URL source: <http://coagul.org/drupal/publication/int%C3%A9grer-poste-debian-dans-domaine-windows>

Liens:

- [1] <http://coagul.org/drupal/rubrique/reseaux>
- [2] http://www.coagul.org/article.php3?id_article=158
- [3] http://www.coagul.org/article.php3?id_article=159
- [4] http://www.coagul.org/article.php3?id_article=305
- [5] http://www.coagul.org/article.php3?id_article=178
- [6] http://www.coagul.org/article.php3?id_article=297