Cah. Tech. I.N.R.A., 2005 56, 33-44

Intégration d'un serveur **DEBIAN GNU/LINUX** à un domaine **WINDOWS** 2000

Georges Pfeiffer[1]*, Cédric Nouguier*[2]

La présente documentation a pour objectif d'intégrer un serveur d'applications GNU/Linux à un domaine Active Directory Windows 2000.
Nous allons détailler les étapes qui nous ont permis de déléguer l'authentification des utilisateurs de la machine Linux au contrôleur de domaine Windows et d'offrir des partages personnalisés à chaque utilisateur. Nous n'aurons ainsi qu'une seule base de données utilisateurs à administrer.
Lors de leur première connexion sur la machine Linux, les utilisateurs se verront automatiquement créer un répertoire personnel.
Il sera possible d'accéder à ses données Linux et à tous les partages Windows qu'ils soient communs ou propres à l'utilisateur. Nous nuançons ce dernier point par le fait que dans notre solution, le répertoire « Mes documents » Windows est stocké de manière centralisée sur un même serveur. Si ce n'est pas le cas, un travail supplémentaire d'adaptation doit être effectué.

Mots clés

Linux, Debian, Active Directory, authentification centralisée, Windows 2000, Samba, Winbind, Kerberos, logiciel libre.

1. Introduction

Cet article s'adresse aux personnes familiarisées au monde Linux désireuses d'adjoindre un serveur Linux à un domaine Active Directory (AD) Windows 2000. Notre démarche a pour principal objectif d'adopter des solutions à base de logiciels libres, permettant de réduire de manière significative les coûts liés à l'achat de licences logicielles et de s'affranchir du coût des mises à jour. Il n'y a en effet plus à acheter de licences pour le système d'exploitation du serveur, des licences d'accès des postes clients au serveur, les licences de la suite bureautique et des autres outils. Pour convaincre le personnel à migrer sous Linux, nous devons dissiper les craintes liées au changement qu'implique le nouveau système. Nous avons donc distingué deux types d'utilisateurs :

- les utilisateurs avec des besoins standard pour qui l'interface graphique doit être intuitive.
- les utilisateurs avec des besoins spécifiques auxquels il faut proposer une alternative aux outils qu'ils utilisent sous Windows.

L'adoption de Linux par les utilisateurs n'est possible que si nous leur proposons un environnement le plus proche possible de celui qu'ils manipulent quotidiennement. Pour cela, notre démarche a été progressive.
Dans un premier temps, nous avons familiarisé les utilisateurs avec les outils libres sous leur

[1] Unité **P**lantes et **S**ystèmes de cultures **H**orticoles (PSH) d'Avignon.
[2] Institut Universitaire Professionnel – Génie Mathématique et Informatique d'Avignon.

environnement de travail Windows : Mozilla, Openoffice, Gimp...
Les outils libres répondant de mieux en mieux aux besoins standards des utilisateurs, il nous est dès lors apparu concevable de transposer les mêmes solutions sous Linux.
Nous avons donc mis en place un serveur d'applications totalement libre sous Linux, avec une distribution **Debian Sarge**.

Un de nos objectifs est de leur fournir un accès à toutes leurs données Linux et Windows depuis n'importe quel système d'exploitation.
D'un point de vue administration système, il faut proposer un accès au serveur avec leurs identifiants Windows. Ce point permet de n'administrer qu'une seule base de données utilisateurs. De plus, le principe du client-serveur, natif sous Linux depuis toujours permet de ne maintenir qu'une seule machine d'où un gain en simplicité et en temps intéressant. La robustesse du système Linux et la richesse de l'offre de logiciels nous ont conforté dans notre démarche.
La réactivité de la communauté Linux permet également de trouver rapidement une solution aux problèmes rencontrés au travers de sites Internet, forums, listes de diffusions... Nous allons présenter la configuration chronologique des outils (Samba, Winbind, Kerberos) nécessaires à l'intégration de la machine Linux au domaine Windows 2000.

2. Configuration de la machine

Toutes les manipulations ont été réalisées sur un serveur disposant de la configuration suivante : système d'exploitation GNU/Linux, basé sur une distribution Debian Sarge, avec un système de fichiers EXT3 et un noyau 2.6.8-2-686-SMP.
Le système EXT3 a été privilégié car il permet, depuis la version 2.6.1 du noyau, de gérer les droits ACL (Access Control List cf http://acl.bestbits.at/) utilisés par Windows.

2.1. Le réglage de l'horloge système avec NTP

L'intégration de la machine Linux au domaine Active Directory est sensible aux dérives temporelles. Pour éviter tout problème, il faut installer le paquet « **ntpdate** ». Il permet de synchroniser l'horloge système avec un serveur de temps NTP dédié :

→ apt-get install ntpdate

Modifier le nom du serveur de temps NTP contacté grâce au fichier suivant
« /etc/default/ntpdate ». Une liste de serveurs de temps est disponible sur le site indiqué en annexe.

NTPSERVERS= ″nom_du_serveur_ntp″

Par défaut, la machine va synchroniser l'horloge du système à chaque redémarrage.
Il est recommandé de synchroniser l'horloge chaque jour. Pour cela, ajouter dans le répertoire « **/etc/cron.daily »** un fichier nommé « **ntpdate »** avec les lignes suivantes :

```
#!/bin/sh
test -x /usr/sbin/ntpdate || exit 0
/usr/sbin/ntpdate nom_du_serveur_ntp
```

2.2. L'installation de SAMBA

L'outil **Samba** est la clé de voûte de notre solution. Il est nécessaire à la gestion de l'authentification (via le contrôle de Winbind avec ses fichiers de configuration) et la gestion des partages. Seules les versions de Samba supérieures à la 3.0.13 ont fonctionné pour les tests mais certaines versions 3.0.10 peuvent fonctionner (Ubuntu par exemple). Actuellement nous utilisons la version 3.0.14a-1 en production.

→ apt-get install samba samba-common smbclient smbfs samba-doc

La configuration de Samba peut être effectuée via un plugin de **KDE** qui est présent dans la version 3.3 dans le « **centre de configuration KDE »** rubrique « **Internet et Réseau »** ou directement en éditant les fichiers comme nous allons le détailler par la suite.

2.3. L'installation de Winbind

Winbind permet d'intégrer Samba à un domaine contrôlé par un serveur NT ou 2K. Cet outil récupère les identifiants auprès du contrôleur de domaine et les adapte au standard UNIX. Il constitue donc un maillon essentiel à l'authentification des utilisateurs du serveur Linux depuis le contrôleur de domaine Windows.

→ apt-get install winbind

L'authentification nécessite la modification de quelques fichiers utilisés par Samba et Winbind :

Fichier « **/etc/nsswitch.conf »**

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

Fichier **« /etc/samba/smb.conf »**

[global]
workgroup = « nom du domaine »
realm = « nom réel du domaine »
#ADS = securité pour windows installé en mode natif sinon DOMAIN
security = ADS
encrypt passwords = true
password server = « adresses IP des contrôleurs de domaine »
domain master = no

server string = %h serveur de test (Samba %v)
wins support = no

wins server = « adresseIP du serveru WINS »

include = /etc/samba/dhcp.conf
dns proxy = no

log file = /var/log/samba/log.%m
max log size = 1000
syslog = 1
log level = 1

panic action = /usr/share/samba/panic-action %d

####### Authentication #######

passdb backend = tdbsam guest
obey pam restrictions = yes

 # guest account = nobody
invalid users = root
passwd program = /usr/bin/passwd %u
*passwd chat = *Enter\snew\sUNIX\spassword:* %n\n *Retype\snew\sUNIX\spassword:* %n\n .*

socket options = TCP_NODELAY

winbind separator = +
idmap uid = 10000-20000
idmap gid = 10000-20000
winbind cache time = 10
winbind enum users = yes
winbind enum groups = yes
winbind use default domain = yes
#winbind trusted domains only = Yes
winbind nested groups = yes
client use spnego = yes
template shell = /bin/bash
 # le répertoire de l'utilisateur a la forme /home/nom_domaine/login
template homedir = /home/%D/%U

#======================== Partages ========================

[tous]
comment = partage accessible a tous en lecture sans authentification
browseable = yes
writable = no
path = /home/partage
only guest = yes

[tous_ad]

comment = partage accessible aux utilisateurs AD seuls
path = /home/partage
browseable = yes
writable = no
valid users = @"Utilisa. du domaine"
create mask = 0700
directory mask = 0700

[donnees_linux]
comment = partage répertoire home des utilisateurs AD
path = /home/PSH/%U
browseable = yes
writable = yes
valid users = @"Utilisa. du domaine"

2.4. L'installation de Kerberos

Kerberos est le protocole de cryptage des données entre le contrôleur de domaine et la machine Linux. Nous avons installé les librairies nécessaires à l'authentification avec Kerberos :

→ apt-get install krb5-config krb5-user libkrb53 libnss3 libpam-krb5 libpam-krb5 libpam-runtime libpam-smbpass libpam0g libpam0g-dev

Fichier « **/etc/krb5.conf »**

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

[libdefaults]
default_realm = DOM.AVI
dns_lookup_realm = true
dns_lookup_kdc = true
ticket_lifetime = 24000
kdc_timesync = 1
ccache_type = 4
forwardable = true
proxiable = true

v4_instance_resolve = false
[realms]
DOM.AVI = {
kdc = « controleur de domaine»:88
#exemple
#kdc = CTRL1.DOM.AVI:88
admin_server = DOM.AVI
default_domain = DOM.AVI
}

[domain_realm]

« .nom réel du domaine » = « NOM REEL DU DOMAINE »
« nom réel du domaine » = « NOM REEL DU DOMAINE »
#exemple
 # .dom.avi = DOM.AVI
 # dom.avi = DOM.AVI
[pam]
debug = false
ticket_lifetime = 36000
renew_lifetime = 36000
forwardable = true
krb4_convert = false

[login]
krb4_convert = false
krb4_get_tickets = false

La procédure suivante est très bien décrite sur le site officiel de Samba.

Désactiver les services Samba et Winbind :
→ /etc/init.d/samba stop
→ /etc/init.d/winbind stop

Joindre le domaine et donner le mot de passe administrateur du contrôleur primaire de domaine :
→ net ads join -U Administrateur

Vérifier que la machine a bien été jointe au domaine :
→ net ads testjoin

Démarrer le service Nmbd puis Winbind puis Smbd ou Winbind puis Samba.
→ /etc/init.d/winbind start

Attendre au moins une minute avant de lancer Samba, le temps que Winbind récupère tous les identifiants des utilisateurs du domaine.
Démarrer Samba :
→ /etc/init.d/samba start

Vérifier que Samba partage un secret avec le contrôleur de domaine Windows :
→ wbinfo -t

Vérifier que Winbind a bien récupéré la liste des utilisateurs et des groupes du domaine Active Directory :
→ wbinfo -u
→ wbinfo -g

Ensuite vérifier que le système est capable de mapper les logins qu'il a rapatriés selon le format GNU/Linux avec les commandes suivantes :
→ getent passwd
→ getent group

Vérifier enfin que la communication entre Samba, Winbind et le contrôleur de domaine est correcte :

→ net ads info

2.5. L'authentification des utilisateurs Linux

Les fichiers permettant de personnaliser le type d'authentification se situent dans le répertoire « **/etc/pam.d/** » et correspondent à chaque service de la machine Linux : ssh, kmd, gdm...
Il est donc possible de n'autoriser la connexion des utilisateurs du domaine Active Directory que pour certains services.
Attention ! De mauvaises configurations des méthodes d'authentification peuvent empêcher toute connexion à la machine et ce, même avec l'identifiant « root ».
Pour prévenir tout problème de ce type, il est conseillé d'autoriser l'authentification des utilisateurs du domaine Active Directory ainsi que des utilisateurs disposant d'un compte Unix standard local pour tous les services excepté le service « **login ».** Ce dernier ne sera accessible qu'aux utilisateurs locaux de la machine, dont « **root »** fait partie.

Voici les fichiers qu'il faut modifier et les changements qui s'imposent.

A noter que les lignes préfixées de « **@** » signifient que l'on importe des fichiers pour la configuration.
Il faut donc remplacer les lignes commençant par « **@ »** de ce fichier par les lignes indiquées ci-après. Cela a pour effet de ne plus inclure les fichiers communs d'authentification mais de les remplacer par des comportements standard d'authentification (utilisés par défaut pour l'authentification des utilisateurs locaux).

Fichier « **/etc/pam.d/login** »

```
auth    required        pam_unix.so nullok_secure
#@include common-auth
account required pam_unix.so
#@include common-account
sessionrequired         pam_unix.so
#@include common-session
password   required   pam_unix.so nullok obscure min=4 max=8 md5
#@include common-password
```

Fichier « **/etc/pam.d/common-auth** »

```
## 2 Ligne ajoutees pour winbind ou utilisateur local
auth    sufficient      pam_winbind.so
auth    required       pam_unix.so nullok_secure use_first_pass
# remplacent celle ci
#auth   required        pam_unix.so nullok_secure
```

Fichier « **/etc/pam.d/common-account** »

```
# Ajout de cette ligne pour winbind ne pas modifier la suivante

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

Fichier « **/etc/pam.d/common-session** »

 # cela cree le repertoire personnel de l'utilisateur avec les droits par defaut
 # de umask : 077 pour rwx------ 022 pour des droits rwxr-xr-x
 # la ligne doit etre situee avant les 2 lignes session suivantes
sessionrequired pam_mkhomedir.so skel=/etc/skel umask=077
 # Ajout de cette ligne pour winbind, ne pas modifier la suivante
session sufficient pam_winbind.so
sessionrequired pam_unix.so

Fichier « **/etc/pam.d/common-password** »

#Ajout de cette ligne pour winbind ne pas modifier la suivante
password sufficient pam_winbind.so
password required pam_unix.so nullok obscure min=4 max=8 md5

Fichier « **/etc/pam.d/samba** »

auth sufficient pam_winbind.so
auth required pam_unix.so
account sufficient pam_winbind.so
account required pam_unix.so
session sufficient pam_winbind.so
session required pam_unix.so

Les modifications réalisées, la configuration est testée en se connectant via **ssh** avec un compte Windows non créé localement sur la machine Linux.

Attention ! Dans le cas où uniquement le service KDM doit gérer la connexion d'utilisateurs AD, il faut prendre garde à ce que le service de verrouillage de la session gère l'authentification des utilisateurs avec AD. Pour éviter tout désagrément, nous préconisons d'utiliser l'authentification AD et locale pour tous les services sauf un de sécurité pour « **login »**.
Si l'authentification d'un utilisateur AD n'est plus possible, il se peut que le problème vienne de Winbind. Vérifier l'erreur avec la commande « **wbinfo -t** ».
Si l'erreur « **NT_STATUS_INVALID_COMPUTER_NAME »** apparaît, redémarrer simplement Winbind :

/etc/init.d/winbind restart

L'authentification devrait fonctionner à nouveau.

3. Accès au répertoire « Mes Documents » de Windows depuis Linux

A l'aide du navigateur Internet Konqueror, il est possible d'accéder au répertoire « Mes Documents » **(figure 1**) de Windows (en lecture et écriture). Cela n'est cependant possible que si les répertoires « Mes Documents » sont partagés sur le réseau. Pour cela, entrer la ligne suivante dans la barre d'URL :

smb://$USER@xxx.xxx.xxx.xxx/Mes Documents$/$USER

Un mot de passe est alors demandé. Il correspond au mot de passe du compte Windows. Il est possible de créer une icône disponible pour chaque utilisateur sur le bureau :
Clic droit sur le bureau > créer nouveau >fichier> lien vers une application.

Donner un nom à l'icône puis dans l'application mettre la ligne suivante :

konqueror "smb://$USER@xxx.xxx.xxx.xxx/Mes Documents$$/$USER"

La variable d'environnement $USER correspond au login de l'utilisateur Linux. Les deux caractères «$» servent pour ne pas interpréter le caractère «$» comme préfixant un nom de variable d'environnement dans konqueror. Mettre ensuite l'icône dans le répertoire Desktop de « /etc/skel » pour qu'elle soit disponible pour chaque nouvel utilisateur.

Figure 1: *Connexion à Linux via Cygwin et accès aux partages Windows*

4. Accès au home Linux depuis Windows

Grâce à Samba il est possible d'accéder aux données personnelles d'un utilisateur connecté sous Windows. Pour cela, dans « voisinage réseau » sélectionner « afficher tout le réseau » puis sélectionner le domaine auquel la machine Linux appartient et enfin le serveur Linux.
Choisir le partage « **donnees_linux** » (**figure 2**) pour que les données Linux de l'utilisateur soient accessibles depuis Windows (même login).

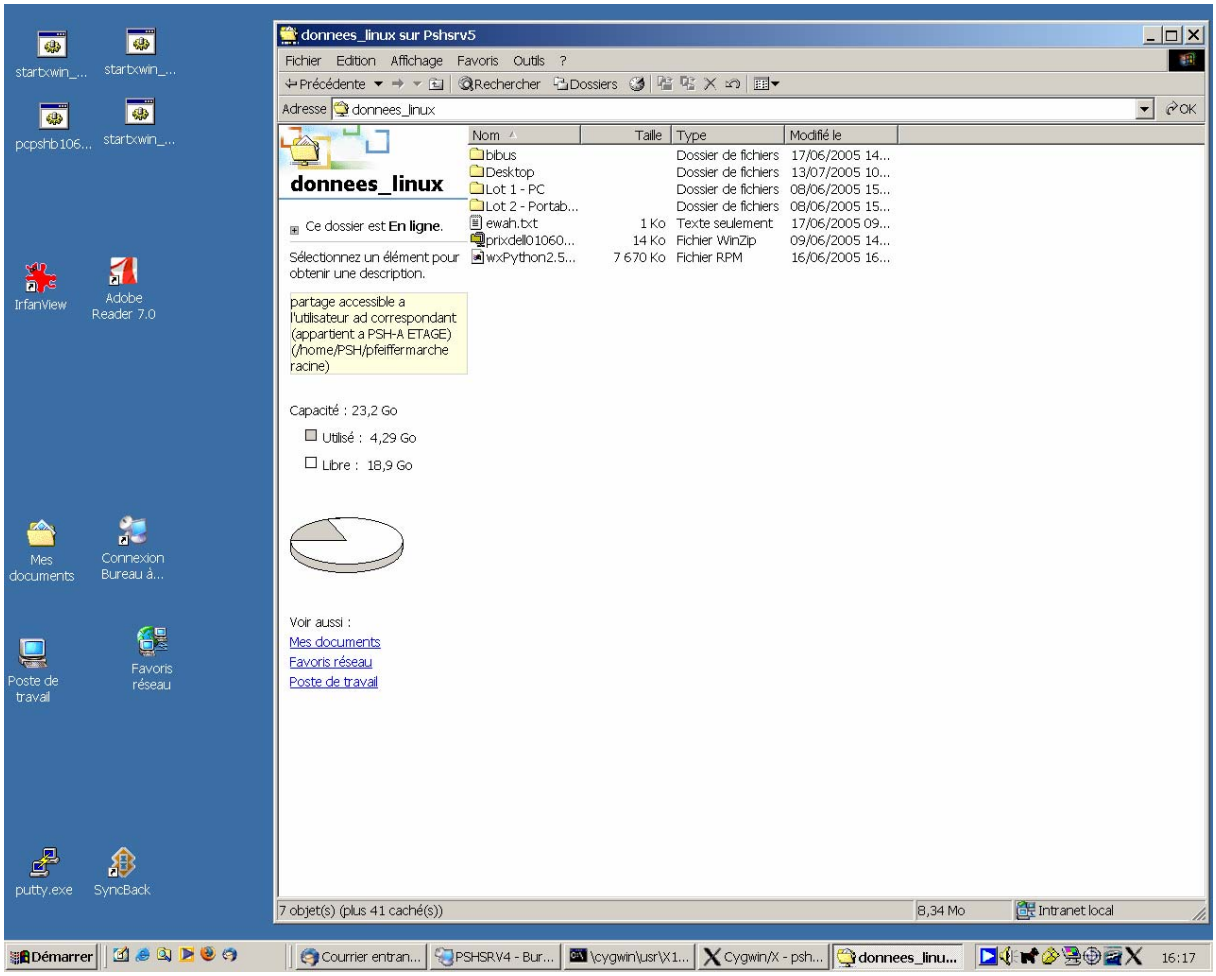

Figure 2: *Accès aux données Linux depuis Windows*

5. Conclusion

La démarche que nous avons exposée est le fruit de notre expérience à l'unité PSH d'Avignon. Elle peut par la suite être affinée en ce qui concerne la gestion des partages à travers l'utilisation d'un module de PAM « **pam_mount.so** ». Ce module permet de créer sur des points de montages définis, des répertoires propres à chaque utilisateur et qui seront démontés après chaque déconnexion. De plus, une gestion plus fine des droits sur les fichiers partagés pourra être mise en place grâce aux paquets relatifs aux Access Control Lists (ACL) recréant le système de gestion des droits Windows sur Linux.

6. Liens utiles

Guide d'installation d'une Debian Sarge

http://jmichau.free.fr/sarge_netinst/x437.html

Liste Debian

http://groups.google.com/groups?hl=fr&lr=&ie=UTF-8&oe=UTF-8&group=linux.debian.user.french

Liste des serveurs de temps

http://www.cru.fr/NTP/serveurs_francais.html

Samba

http://www.coagul.org/article.php3?id_article=177

La documentation officielle de Samba

http://us1.samba.org/samba/docs/man/Samba-HOWTO-Collection/

Pages concernant active directory et Samba

http://us1.samba.org/samba/docs/man/Samba-HOWTO-Collection/domain-member.html#ads-member

http://www.wlug.org.nz/ActiveDirectorySamba

Winbind

http://www.coagul.org/article.php3?id_article=178

http://us1.samba.org/samba/docs/man/Samba-HOWTO-Collection/domain-member.html#ads-member

http://us1.samba.org/samba/docs/man/Samba-HOWTO-Collection/winbind.html

7. Lexique

GNU : GNU is Not Unix Projet de réalisation d'un système d'exploitation totalement libre lancé en 1984.

Linux : Système d'exploitation complet, fiable, disponible gratuitement, développé à l'origine par Linus Torvalds.

Debian : Une des distributions de GNU/Linux les plus populaires pour sa stablilité. L'une de ses caractéristiques principales est due à ses concepteurs : ils insistent pour qu'elle contienne exclusivement du logiciel libre (mais tolère et facilite l'installation de logiciel commercial), que sa conception demeure élégante et conforme aux normes, et qu'elle soit appelée GNU/Linux (car est officiellement recommandée par le projet GNU). www.fr.debian.org

NTP : Network Time Protocol, abrégé NTP, est un protocole permettant de synchroniser des horloges de systèmes informatiques à travers un réseau de paquets dont la latence est variable.

Active Directory : Nom donné au service d'annuaire de Windows 2000.

PAM : Abréviation de Pluggable Authentication Modules. PAM permet de gérer l'authentification sous GNU/Linux.

SMB : Abréviation de Server Message Block, SMB est le protocole utilisé pour partager des ressources avec des réseaux Windows.

Samba est un logiciel libre sous licence GNU supportant le protocole SMB/CIFS. Ce protocole est employé par Microsoft pour le partage de diverses ressources (fichiers, imprimantes, etc.) entre ordinateurs équipés de Windows. Samba permet aux systèmes Unix d'accèder aux ressources de ces systèmes et vice-versa.

Winbind est un outil qui permet de transformer des identifiants issus d'un contrôleur de domaine Windows en identifiants Unix.

Kerberos est un protocole d'authentification réseau créé au MIT. Kerberos utilise un système de tickets au lieu de mots de passe en texte clair. Ce principe renforce la sécurité du système et empêche que des personnes non autorisées interceptent les mots de passe des utilisateurs.

ACL : Les Access Control Lists permettent un réglage fin et précis des droits d'accès à des ressources (typiquement des fichiers ou dossiers).

Cygwin : Collection de logiciels libres à l'origine développés par Cygnus Solutions permettant à différentes versions de Windows de Microsoft d'agir un peu comme un système Unix. Depuis 2001 un système de fenêtre X Xfree86 a été implanté permettant de se connecter à une machine Linux depuis Windows.