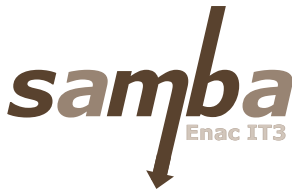


AUTHENTIFICATION DES CLIENTS WINDOWS DANS UN DOMAINE LINUX/SAMBA VIA UN SERVEUR ldap

LE CAS CONCRET DE L'ENAC-IT3



Paulo.deJesus@epfl.ch, ENAC



Les objectifs

Dans le groupe Informatique et télématique IT3 de la Faculté ENAC (*Environnement naturel, architectural et construit*) nous nous sommes fixés comme objectif la création d'un domaine avec des clients Windows (2000 et XP), Mac OSX et un contrôleur de domaine Samba sur Linux, sans utiliser un Windows 2000 serveur.

Comme je l'avais déjà écrit dans mon article **Partage de ressources dans un environnement Mac, PC et Unix-Linux** paru dans le FI1/2002, <http://sic.epfl.ch/SA/publications/FI02/fi-1-2/1-2-page1.html>) Samba nous permet non seulement de partager des ressources (dossiers et imprimantes) mais peut aussi jouer le rôle de PDC (Contrôleur Principal de Domaine) et ainsi authentifier des postes clients Windows9x, NT, 2000 et XP. Samba peut aussi faire partie d'un domaine (Windows2k) comme serveur membre ou comme serveur Stand Alone dans un WorkGroup selon la configuration choisie.

A l'époque, nous avons fait les essais avec des clients Windows NT et des comptes utilisateurs créés directement dans le système sur un Macintosh en système 10.01 basé sur un *file system* Unix BSD.

Plus récemment, nous avons refait l'expérience d'utiliser Samba comme PDC en nous passant de la fastidieuse opération de création de comptes (surtout si le nombre dépasse la centaine) et en laissant les utilisateurs s'authentifier directement sur le serveur ldap de L'EPFL.

Notre objectif était de permettre aux utilisateurs d'avoir un **profil itinérant**, d'avoir **accès** aux **imprimantes** et à des **dossiers partagés**, un **partage DFS** (*Microsoft Distributed File*) et une **redirection** du dossier **My Documents** pour les clients Windows.

Le but de cette expérience et de cet article n'est pas d'aller contre des stratégies déjà mises en place, mais de démontrer encore une fois que d'autres solutions sont possibles et qu'elles sont quelquefois mieux adaptées à des environnements de travail qui ne se prêtent pas à une gestion trop centralisée des ressources informatiques.

LE MATÉRIEL

- PDC: Linux RedHat avec Samba 2.2.7 (un Mac OSX, qui par défaut inclut un client et un serveur Samba, pourrait sans problème avoir le même rôle, pour plus d'infos: http://samba.epfl.ch/samba/docs/using_samba/appf.html).

- Clients: Windows 2000, Windows XP et Mac OSX. L'installation de Samba n'est pas décrite dans cet article.

LES UTILISATEURS

Un groupe de collaborateurs de la section d'architecture s'est prêté volontairement au jeu. Actuellement le domaine Samba ENAC-IT3 contient 25 membres Windows, 15 Macs pour une cinquantaine d'utilisateurs.

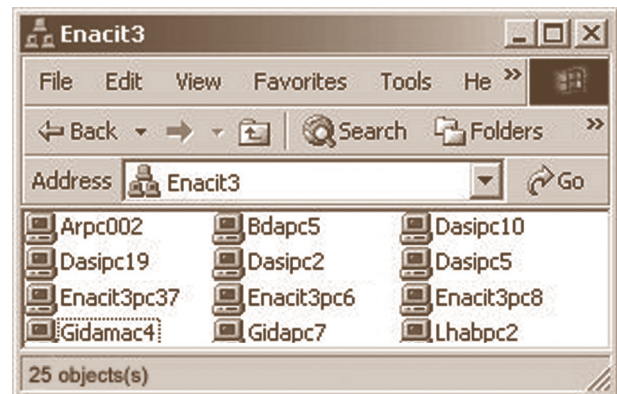


IMAGE 1 – DOMAINE ENACIT3

CONFIGURATION DU PDC

La partie la plus importante de la configuration passe par l'édition (en mode texte ou *via script*) des fichiers **smb.conf** pour Samba et des **ldap.conf**, **system-authority** et **nsswitch.conf** pour l'authentification. Voici les points importants pour que Samba devienne PDC:

LE FICHIER **smb.conf**:

```
[global]
workgroup = nom du domaine
netbios name =nom du serveur
domain master =yes
domain logons = yes
local master = yes
preferred master = yes
os level = 66
encrypted passwords = yes
```

pour permettre de recevoir les mots de passe cryptés de clients Windows (à partir de Windows 98)

```
security = user
```

les options sont user pour un contrôleur de domaine, domain pour un serveur membre et share pour un serveur en stand alone

```
host msdfs = yes
    pour activer le support DFS
logon path = \\serveur\profile\%u
    emplacement où les profils itinérants seront stockés (le %u a
    la même signification que le %USERNAME% Windows.
logon scripts = .bat, .kix ou .vbs
    les logon scripts peuvent être des scripts .bat ou .kix et
    doivent entrer dans le dossier «net logon». Ces scripts seront
    téléchargés par la machine cliente et exécutés en local.
```

EXEMPLE D'UN SCRIPT .BAT:

```
net use H: \\dasipc2\transfertateliers
net time \\serveur /set /yes
```

EXEMPLE D'UN SCRIPT .KIX:

```
if @WKSTA="arpc003" or
    @WKSTA="arpc004" or
    @WKSTA="arpc005"

    ADDPRINTERCONNECTION ("\\DASIPC16\
AAD001XeroxNB")
    ADDPRINTERCONNECTION ("\\DASIPC16\
AAD001XeroxColor")
    ;Installer l'imprimante par default
    SetDefaultPrinter ("\\DASIPC16\
AAD001XeroxNB")
    USE H:\\dasipc2\TransfertSAR
Endif
```

On peut forcer l'exécution d'un script pour un utilisateur (toto par exemple) spécifique avec l'option:

```
logon script = %U.bat
```

avec un script appelé Toto.bat par exemple

idem pour une machine:

```
logon script = %m.bat
```

avec un script appelé dasipc2.bat par exemple

```
adduser user script = /usr/sbin/useradd -d /
dev/null -g computers -s /bin/false -M %u
```

cette commande est très importante, elle permet d'introduire à partir du client la machine cliente dans le domaine sans créer le compte au préalable dans le pdc (opération à effectuer évidemment par un utilisateur ayant les droits d'administrateur dans le domaine).

```
include = /etc/samba/smb.conf.%m
```

cette ligne permet de charger un fichier smb.conf spécifique pour une machine, le %m sera remplacé par le netbios name de la machine.

```
preexec = echo %T: %u connected on %m >> /var/
log/samba/users.log
postexec = echo %T: %u disconnected from %m>>
/var/log/samba/users.log
```

Les commandes preexec et postexec permettent d'exécuter un script shell sur le serveur lors d'une connexion (contrairement à logon, script qui est exécuté sur le client). On peut se servir de cette possibilité pour alimenter un fichier de log de connexion-déconnexion. On peut avoir une vision on-line de l'activité du serveur avec la commande:

```
[linux1 :~]root % tail -f /var/log/samba/
users.log
```

```
[netlogon]
comment = dossier où seront stockés les logon
scripts
path = /export/samba/logon
public = no
writable = no
browseable = no
create mask = 0644
```

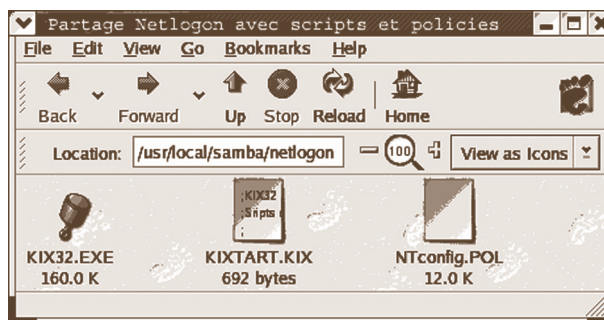


IMAGE 2 – PARTAGE NET LOGON

```
[profiles]
comment = partage pour stocker le profil itinérant des utilisateurs
path = /home/samba/profiles
writable = yes
browseable = no
create mode = 0644
directory mode = 0755
```

Au premier logon le système crée un profil local de l'utilisateur sur le poste client, au logoff le profil est copié sur le partage désigné dans [profiles]. Pour éviter qu'un poste client utilisé par plusieurs utilisateurs ne soit vite rempli avec la copie locale du profil itinérant il faut ajouter dans la clé de la base du registre:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon mettre la valeur Delete-
RomingCache à 1, ou alors utiliser une stratégie de sécurité
qui le fasse.
```

Il faut évidemment créer les dossiers avant, par exemple:

```
[linux1:~] root% mkdir -m 0775 /usr/local/
samba/netlogon
[linux1:~] root% chown root:admin /usr/local/
samba/netlogon
[linux1:~] root% mkdir /usr/local/samba/profiles
[linux1:~] root% chmod 1757 /usr/local/samba/
profiles
```

```
[dfs]
comment = Partage DFS (Distributed File System)
path = /home/samba/dfs
msdfs root = yes
```

Pour le partage DFS on doit commencer par créer le dossier à partager.

```
[linux1:~] root% mkdir /home/samba/dfs
[linux1:~] root% chown root:root /home/samba/
dfs
[linux1:~] root% chmod 755 /home/samba/dfs
```

Après on crée les liens vers les partages

```
linux1:~] root% cd /home/samba/dfs
linux1:~] root% ln -s 'msdfs:serveur1\nom de
partage1' alias1
linux1:~] root% ln -s 'msdfs:serveur2\nom de
partage2' alias2
exemple: ln -s 'msdfs:dasipc2\
transfertAteliers' transfertAteliers
```

Avec ces quelques lignes votre serveur Samba est prêt à intégrer des clients Windows, à authentifier des utilisateurs et à leur proposer des partages. Les utilisateurs Mac OSX pourront sans problème accéder au partage du domaine et configurer leur propre serveur Samba intégré (comme serveur *stand alone*) et l'intégrer dans le domaine principal.

Par exemple dans le fichier **smb.conf** (du Mac):

```
[global]
workgroup = nom du domaine principal
netbios name = nom de Mac
os level = 17
domain logons = no
domain master = no
(...)
[BoiteAlait]
comment = mon partage publique
path = /Users/boitealait
public = yes
writable = yes
```

Le Mac sera visible dans le domaine principal et les utilisateurs autorisés pourront accéder aux ressources partagées. A chacun de configurer le fichier **smb.conf** de façon à l'adapter à son environnement et à ses besoins spécifiques.

LE FICHIER LDAP.CONF

```
host ldap.epfl.ch
    adresse du serveur ldap
base o=epfl, c=ch
    base de recherche
pam_filter &(gidNumber=xxx*) (objectClass=posix
Account)
    le filtre où l'on doit mentionner le numéro du ou des groupes
    autorisés à se connecter. Par défaut tout le monde est autorisé
    à se connecter.
nss_base_passwd ou=SIC-II, ou=PL-IT, ou=PL,
o=epfl, c=ch
nss_base_shadow ou=SIC-II, ou=PL-IT, ou=PL,
o=epfl, c=ch
nss_base_groupou=SIC-II, ou=PL-IT, ou=PL,
o=epfl, c=ch
    emplacement dans la hiérarchie ldap où le système cherche les
    utilisateurs. On peut mettre toute la racine ou uniquement
    la branche qui nous intéresse; dans notre cas:
nss_base_passwd ou=ENAC, o=epfl, c=ch
nss_base_shadow ou=ENAC, o=epfl, c=ch
nss_base_group ou=ENAC, o=epfl, c=ch
*= numero de groupe (gid)
```

LE FICHIER SYSTEM-AUTH

Ce qu'il faut ajouter dans le fichier:

```
auth sufficient /lib/security/pam_ldap.so use_
first_pass
password sufficient /lib /security/pam_ldap.so
use_authok
session optional /lib/security/pam_ldap.so
```

LE FICHIER NSSWITCH.CONF

Ce qu'il faut ajouter dans le fichier:

```
passwd: files ldap
shadow: files ldap
group : files ldap
```

les fichiers complets **smb.conf**, **ldap.conf**, **system-auth** et **nsswitch.conf** sont à disposition à l'adresse: <http://enacit3.epfl.ch/samba/>.

SÉCURITÉ

CÔTE CLIENT

Pour sécuriser les postes clients nous avons utilisé l'utilitaire **Poledit.exe**. Après configuration on sauvegarde le fichier sous le nom de **ntconfig.pol** dans le dossier partagé **net logon**. Le nom **ntconfig.pol** est utilisable par les machines NT. Pour les machines Windows9x le fichier doit s'appeler **config.pol**. On aurait pu aussi utiliser l'utilitaire **Tweakui**

pour configurer un poste client de base et déployer l'image avec Ghost, ou créer des fichiers **.reg** à appliquer sur les machines concernées mais les scripts et les polices apportent beaucoup plus de souplesse .

CÔTÉ SERVEUR, LE MINIMUM À FAIRE

```
[global]
hosts allow = 192.168.10. 192.168.11.
    autorise la connexion des clients des subnets 10 et 11
    hosts deny = ALL
    interdit cette connexion à tous les autres
interfaces = 192.168.10.2/255.255.255.0
192.168.11.2/255.255.255.0
    interfaces réseau utilisées par Samba:
browseable = no
    cette option rend les partages sensibles invisibles au butinage
    (browsing).
    Et mettre les bonnes permissions sur les mêmes, surtout sur
    le partage net logon
[netlogon]
writable = no
    Un utilisateur malveillant pourrait mettre un exécutable
    dans ce partage et il serait exécuté par toutes les machines
    qui se connecteraient.
    Ne pas accepter certains types de fichiers.
veto files = /*.exe/*.dll/*.bat/*.vbs/
    Par exemple pour éviter la propagation de fichiers infectés
    dans le serveur.
```

LES CLIENTS

INTRODUCTION DES POSTES CLIENTS DANS LE DOMAINE

L'introduction des clients Windows 2k/XP dans le domaine Samba se fait sans problème et il suffit d'utiliser la procédure habituelle, c'est-à-dire la configuration réseau (IP DNS Masque réseau, etc.) et rejoindre ensuite un domaine par la procédure habituelle. Comme pour Windows l'opération doit être exécutée par un utilisateur avec des droits d'Administrateur sur le serveur.

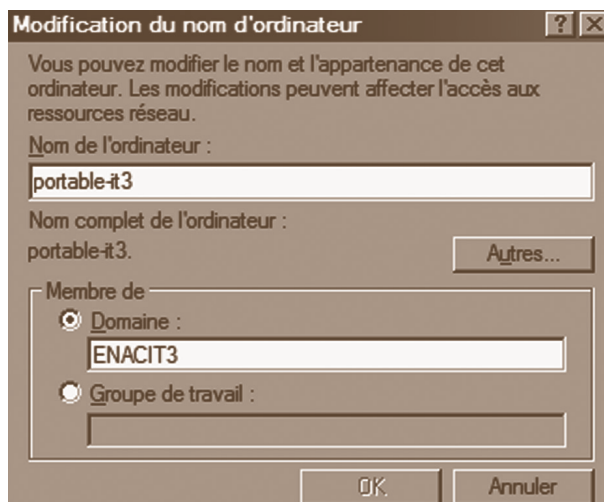


IMAGE 3 – INTRODUCTION D'UN CLIENT WINDOWS DANS LE DOMAINE

Pour les clients Windows XP, une modification est nécessaire au niveau de la base de registres; il faut ajouter la clé:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\Netlogon\Parameters] «requiresignor
seal»=dword:00000000
```

Les Mac OSX accèdent aux ressources par une interface graphique ou alors en mode **commande**.

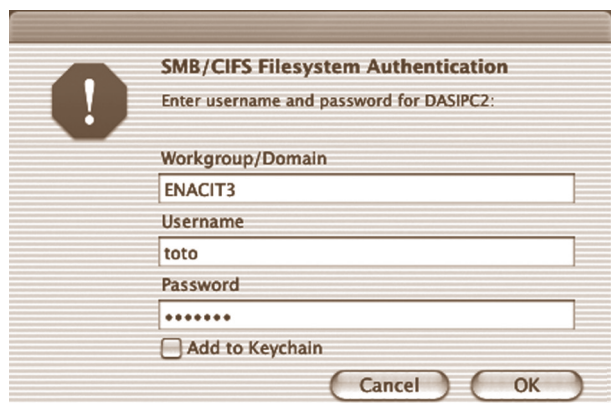


IMAGE 4 – INTERFACE SAMBA CLIENT POUR MAC OSX

GESTION SAMBA EN MODE GRAPHIQUE

Bien évidemment si l'on doit gérer un grand nombre d'utilisateurs et de clients, toutes les manipulations ci-dessus peuvent être très efficacement scriptées.

Plusieurs applications sont à disposition pour administrer Samba en mode graphique:

- **WebMin** (<http://www.webmin.com>).

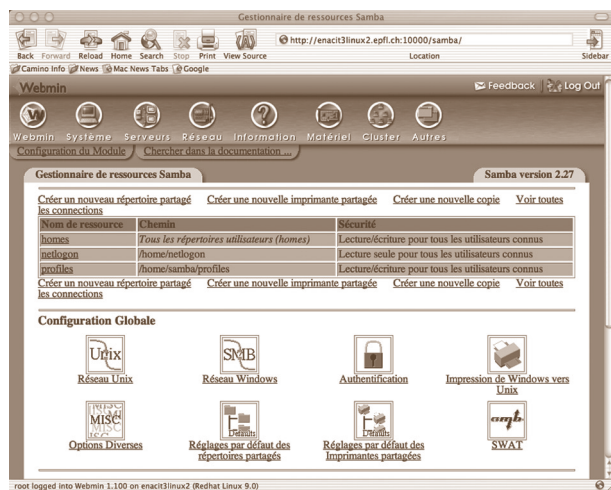


IMAGE 5 –INTERFACE WEBMIN

- **Swat**, distribué avec Samba.
- L'outil RedHat, RedHat-conf-Samba.
- Sur le miroir suisse de Samba (<http://samba.epfl.ch/samba/samba.html>) on peut trouver d'autres informations sur ce sujet.

LES PROBLÈMES À RÉSOUDRE

Le cryptage du mot de passe sur ldap n'est pas le même que sur Samba. Les utilisateurs peuvent s'authentifier sur le PDC, mais pour accéder aux ressources partagées par Samba ils doivent retaper leur mot de passe au premier logon pour qu'il s'enregistre dans le fichier **smbpasswd** au bon format.

AVANTAGES ET DÉSAVANTAGES PAR RAPPORT À UN SYSTÈME WINDOWS 2000 SERVEUR

La configuration se fait en mode texte donc avec plus de clarté et plus de souplesse.

En cas de crash total de la machine, la sauvegarde des fichiers (smb.conf, smbpasswd, ldap.conf, system-auth) permet d'installer rapidement un autre PDC. L'expression **administrer un domaine** prend ici son vrai sens vu que la plupart des paramètres sont visibles et éditables avec un simple éditeur de texte.

Encore un mot à dire par rapport à une solution *Forêt Active Directory* où à partir d'un certain niveau, l'**administrateur** devient un simple exécutant qui obéit aux stratégies qui lui sont imposées et encore une fois la séduction de l'interface GUI ne lui laisse aucune chance de s'orienter dans les méandres du système. Son rôle se cantonne à appliquer des règles prédéfinies et le cas échéant, à passer des *patches* pour colmater les défauts obscurs du système.

Au niveau des stratégies de sécurité, Samba n'atteint pas encore;-) le degré de complexité d'un serveur Windows, mais dans un milieu académique la balance doit pencher du côté du prix, du gain de liberté et de souplesse dans l'utilisation des ressources informatiques que nous offrent les produits Samba et Linux.

DU NOUVEAU DANS SAMBA 3!

La version Samba-3.0.0 RC2 est disponible. Entre autres nouveautés, citons les plus importantes:

- Support Active Directory: Samba peut rejoindre un domaine Active Directory comme serveur membre et authentifier les utilisateurs avec ldap/kerberos.
- Nouveau système d'authentification interne.
- Nouvelle commande **net**.
- Nouveau support d'impression pour Windows XP/2003 et publication des imprimantes dans Active Directory.
- Nouveaux modules RCP.
- Support pour la migration d'un domaine NT4 vers SAMBA 3 en gardant les SID des utilisateurs, groupes et domaine (vraiment intéressant).
- Bien sûr à suivre aussi l'évolution de Samba TNG: <http://www.samba-tng.org>.

LA DOCUMENTATION

- Le miroir suisse de Samba: <http://samba.epfl.ch/samba/samba.html>.
- *Using Samba* des éditions O'Reilly (2ème édition), disponible aussi au format html (voir site du miroir suisse).
- *Using Samba as a PDC, IBM developerWorks*: <http://www1.ibm.com/servers/esdl/tutorials/samba/>.
- Une multitude d'articles écrits par la communauté du *open source* qu'on peut évidemment trouver sur Internet.

REMERCIEMENTS

Je remercie Michèle Coulmance du SIC, Carla pour le logo et tous ceux qui m'ont encouragé dans ce projet.■