Support de cours

Serveur de fichiers Samba

Introduction

Samba est une suite logicielle implémentant le protocole SMB* (Server Message Block) sur les systèmes Unix.

Samba implémente le coté serveur de ce protocol et permet ainsi de partager des ressources (répertoires, imprimantes, etc.) vers des clients réseaux Windows®, Linux®, OS/2®, etc.

Il implémente également la partie cliente de SMB, offrant ainsi la possibilité aux systèmes Unix d'accéder aux ressources partagées par des systèmes d'exploitation Microsoft.

* Appelé encore CIFS (Common Internet File System, RFC 1001 et 1002), LanManager ou NetBIOS.

Composantes

Les composantes de Samba sont les suivantes :

- `smbd` : le démon qui gère le partage des ressources ;
- `nmbd` : le démon qui implémente la résolution des noms NetBIOS ;
- `winbind` : qui permet d'utiliser les listes d'utilisateurs et groupes de serveurs NT et 2000 ;
- `smbclient` : fournit une interface en ligne de commande pour accéder à des partages Windows ;
- `smbfs`/`smbmount` : permettent de monter des partages Windows sur un système de fichiers Unix.

Fichier de configuration `smb.conf`

L'ensemble des directives de configuration de Samba sont contenues dans le fichier `smb.conf`.

Le nombre de directives de configuration est assez élevé car Samba propose de nombreuses options.
De plus, plusieurs de ces directives possèdent des synonymes.

Conformément à la tradition Unix, ce fichier est un fichier texte qu'il est possible de modifier avec n'importe quel éditeur de texte Unix.

Il est organisé sous forme de sections qui contiennent des paires de directive/valeur.

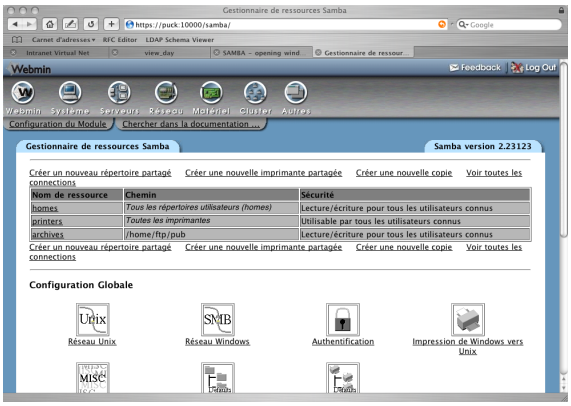
Exemple :

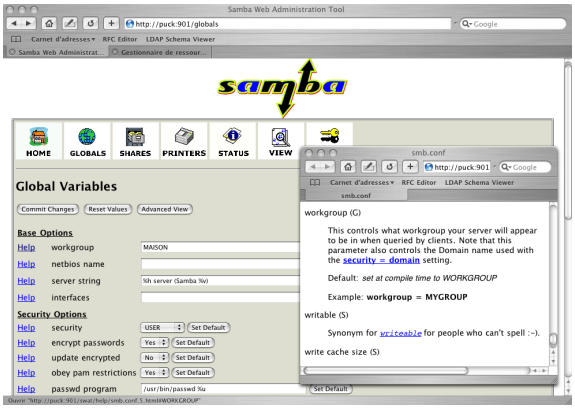
```
[global]
  server string = Serveur Lucky Luke
```

Swat et Webmin

Deux alternatives existent à l'édition pure du fichier `smb.conf` :

- Swat ;
- Webmin.





Le serveur de fichier `smbd`

Le démon `smbd` utilise toutes les sections du fichier `smb.conf`.

Parmi ces sections, certaines ont une signification particulière :
- `[global]` : contient l'ensemble des directives de configuration générale du serveur ainsi que les paramètres par défaut des partages ;
- `[homes]` : permet de partager simplement le répertoire de chacun des utilisateurs ;
- `[printers]` : pour fournir les paramètres par défaut de toutes les imprimantes partagées du système.

Les autres sections représentent chacune un partage.

Exemple

```
[global]
  # Paramètres généraux
  workgroup = LUKE
  load printers = yes
  security = user
  # Valeur par défaut pour les partages
  writable = yes

[homes]
  comment = Espaces personnels
  browseable = no

[printers]
  # Valeurs par défaut pour toutes les imprimantes
  writable = no
  printable = yes

[partage]
  comment = Espace commun
  path = /home/shared
```

Variables de substitution

Beaucoup de valeurs du fichier `smb.conf` peuvent contenir une ou plusieurs variables de substition. Par exemple :

```
log file = /var/log/samba/%m.log
```

Voici la liste des variables les plus utiles :

`%u`	nom de l'utilisateur
`%g`	groupe de l'utilisateur
`%S`	nom du partage
`%m`	nom de la machine cliente
`%L`	nom du serveur
`%M`	nom Internet de la machine cliente
`%I`	adresse IP de la machine cliente
`%$(var)`	valeur de la variable d'environnement `var`

Autre exemple :

```
[groupe]
  path = /home/groupes/%g
```

Section [global]

Paramètres généraux

```
workgroup = string
server string = string
```

Paramètres d'impression

```
load printers = yes/no
printing = bsd/lprng/cups/etc.
```

Paramètres de sécurité

```
allow hosts = list
deny hosts = list
guest account = string
```

Section [global]

Paramètres d'authentification

```
security = share/user/server/domain
encrypt passwords = yes/no
```

Paramètres des journaux

```
log file = string
max log size = integer
debug level = integer
```

Partages

Paramètres généraux

```
comment = string
browseable = yes/no
path = string
```

Paramètres de case des caractères

```
mangle case = yes/no
case sensitive = yes/no
default case = upper/lower
preserve case = yes/no
short preserve case = yes/no
```

Par défaut, Samba n'est pas sensible à la case des caractères mais il la préserve.

Partages

Paramètres de contrôle d'accès

```
valid users = list
public = yes/no
invalid users = list
write list = list
read list = list
```

Paramètres de gestion des droits

```
read only = yes/no
writable = yes/no
create mask = rights
directory mask = rights
force user = string
```

Une liste d'utilisateurs peut contenir des groupes : `@groupe`.
Les droits s'expriment sous forme octale : `0644`.

Partages, exemple

```
[global]
  # Une très bonne idée
  invalid users = root

[ressources]
  comment = Ressources d'installation
  path = /home/data/ressources
  read only = yes
  write liste = @admins
  public = yes

[temp]
  comment = Attention, ce répertoire est nettoyé toutes les nuits
  path = /home/data/temp
  create mask = 0666
  directory mask = 0777
  public = yes
  read only = no
```

Imprimantes

Paramètres généraux

```
printable = yes/no
printer = string
```

De plus, les partages d'imprimantes étant des partages particuliers, l'ensemble des directives applicables aux partage, vues précédemment, le sont également aux imprimantes (bien que certaines n'aient pas de sens dans ce contexte).

Imprimantes, exemple

```
[global]
  load printers = yes

[printers]
  browseable = no
  path = /tmp
  printable = yes
  public = yes
  writable = no
  create mode = 0700
```

```
[couleur]
  printer = lpcolor
  valid users = seb @staff
  browseable = no
  path = /tmp
  printable = yes
  writable = no
  create mode = 0700
  comment = Imprimante couleur
```

Le résolveur `nmbd`

Le démon smbd a les tâches suivantes :
- fournir les parties cliente et serveur de WINS ;
- participer aux élections ;
- répondre aux requêtes du réseau pour les résolutions de nom.

Il est configuré via certaines directives de la section `[global]` du fichier `smb.conf`.

Attention : l'activation de certaines valeurs sur certaines directives peuvent rendre bancale le réseau Microsoft si des contrôleurs de domaine ou « master browsers » sont déjà présents.

Le résolveur nmbd

Paramètres de résolution de noms

```
name resolve order = list of lmhosts host wins bcast
dns proxy = yes/no
```

Paramètres WINS

```
wins support = yes/no
wins server = address
```

(ces directives s'excluent mutuellement)

Paramètres affectant le comportement du « browser »

```
local master = yes/no
preferred master = yes/no
os level = integer
domain master = yes/no
```

Le résolveur nmbd, exemple

Configuration typique si Samba est PDC

```
[global]
  workgroup = MYNET
  name resolve order = lmhosts host bcast
  wins support = yes
  local master = yes
  preferred master = yes
  os level = 10
  domain master = yes
```

Configuration à utiliser si un PDC NT ou 2000 existe pour le domaine MYNET

```
[global]
  workgroup = MYNET
  name resolve order = wins bcast
  wins server = 192.168.2.10
  local master = no
  preferred master = no
  domain master = no
```

Authentification

Samba, à travers la directive `security`, reconnaît quatre configurations possibles pour l'authentification :

- `share` : mot de passe par partage ;
- `user` : mot de passe par utilisateur (base Unix) ;
- `server` : authentification auprès d'un serveur NT ;
- `domain` : authentification auprès du PDC ou BDC d'un domaine.

Par ailleurs, la directive `encrypt passwords` contrôle si les mots de passe doivent être cryptés par les clients.
Elle doit avoir la valeur `yes` obligatoirement pour les authentification `server` ou `domain`. Si l'authentification est `share` ou `user`, alors la directive `smb passwd file` doit être utilisée pour donner le nom du fichier qui stocke les mots de passe cryptés.

UID et GID

Quelque soit la méthode d'authentification utilisée, au final, un utilisateur (UID) et un groupe (GID) Unix doivent être associés au client qui se connecte à un partage.

Ce qui veut dire :
- que l'utilisateur et le groupe doivent exister dans la base Unix (fichers `/etc/passwd` et `/etc/group`) ;
- ou que des directives telles que `guest ok`, `user`, etc. sont utilisées au niveau du partage ;
- ou qu'un mécanisme est mis en place pour aller chercher ces informations dans une base externe (NIS, LDAP, domaine NT via `winbind`, etc.).

Ces UID et GID effectifs associés à la connexion permettent de contrôler les droits d'accès Unix aux répertoires et aux fichiers.

Authentification `share`

Cette méthode est plutôt désuète. Elle fait référence à la méthode d'authentification qui était utilisée par les clients « Windows for Workgroups » 3.11 !

Exemple :

```
[global]
  security = share

[unpartage]
  path = /home/partage
  user = partage
```

Authentification `user`

Cette authentification est utilisée lorsque le serveur Samba est utilisé seul dans le domaine. Les mots de passe des utilisateurs sont vérifiés auprès de la base des mots de passe Unix ou du fichier `smbpasswd` s'ils sont cryptés (ce qui est désormais généralement le cas).

Exemple :

```
[global]
  security = user
  encrypt passwords = yes
  smb passwd file = /etc/samba/smbpasswd
  unix password sync = yes
  passwd program = /usr/bin/passwd %u
  passwd chat = *Enter\snew\spassword:* %n\n *Retype\snew\spassword:* %n\n .

[unpartage]
  path = /home/partage
```

Authentification `server`

Lorsque cette méthode d'authentification est utilisée, Samba authentifie les utilisateurs auprès d'un serveur NT.
Il est recommandé que les mots de passe soient cryptés.
Les utilisateurs et les groupes doivent exister dans la base des utilisateurs et groupes d'Unix.

Exemple :

```
[global]
  security = server
  encrypt passwords = yes
  password server = ServeurNT

[unpartage]
  path = /home/partage
```

Le programme `smbpasswd`

Le fichier des mots de passe cryptés `smbpasswd` peut être géré avec la commande... `smbpasswd` !

Exemples :

Ajouter un utilisateur (le mot de passe est demandé)
```
puck:~# smbpasswd -a seb
```
Modifier le mot de passe d'un utilisateur
```
puck:~# smbpasswd seb
```
Désactiver/activer un utilisateur
```
puck:~# smbpasswd -d seb
puck:~# smbpasswd -e seb
```
Supprimer un utilisateur
```
puck:~# smbpasswd -x seb
```
Ajouter une machine au domaine (si Samba est PDC)
```
puck:~# smbpasswd -m "ys$"
```

<u>Rappel</u> : L'utilisateur doit, au préalable, être connu du système Unix !

Authentification `domain`

Cette configuration d'authentification nécessite au préalable que le serveur Samba soit enregistré comme membre du domaine auprès du PDC.
Les mots de passe doivent être cryptés.
Les utilisateurs et les groupes doivent exister dans la base des utilisateurs et groupes d'Unix.

Exemple :

```
[global]
  security = domain
  encrypt passwords = yes
  password server = *

[unpartage]
  path = /home/partage
```

Authentification `domain`

Afin que le serveur Samba soit membre du domaine, suivre ces étapes :

1) Configurer `smb.conf` ainsi

```
security = server
workgroup = DOMAIN
password server = PDCServer
```

2) Avec l'utilitaire « Gestionnaire de server pour les domaines » de Windows NT, ajouter le nom du serveur Samba comme membre du domaine.
Puis utiliser la commande : `smbpasswd -j DOMAIN`

2alt) Utiliser la commande : `smbpasswd -j DOMAIN -U username%password`
(où username est un compte du domaine ayant les droits nécessaires pour ajouter une machine au domaine).

3) Changer ces 2 options ainsi :

```
security = domain
password server = *
```

Outils

Samba est installé avec un ensemble d'outils :

- `testparm` : permet de tester la validité du fichier `smb.conf` ;
- `smbstatus` : liste l'ensemble des connexions et des fichiers ouverts ;
- `smbpasswd` : pour manipuler le fichier des mots de passe cryptés ;
- `make_smbcodepage` : création des pages de codes pour les clients ;
- `make_printerdef` : permet l'« auto-installation » des imprimantes ;
- `smbcontrol` : envoie de messages aux démons Samba ;
- `smbclient` : pour accéder aux fichiers d'un partage distant ;
- `smbmount` : pour monter un système de fichier distant ;
- `smbtar` : sauvegarde automatique de partages distants ;
- `nmblookup` : résoudre un nom NetBIOS.

testparm

L'utilitaire `testparm` permet de :

1) valider que le fichier `smb.conf` ne contient pas d'erreur ;
2) afficher les valeurs par défaut de tous les directives de configuration.

Exemple :

```
puck:~# testparm |more
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Processing section "[archives]"
Loaded services file OK.
Press enter to see a dump of your service definitions
# Global parameters
[global]
        coding system =
        client code page = 850
        code page directory = /usr/share/samba/codepages
.../...
```

smbstatus

Cet utilitaire affiche l'ensemble des connexions au serveur Samba ainsi que la liste des fichiers sur lesquels un verrou est positionné.

Exemple :

```
puck:~# smbstatus

Samba version 2.2.3a-12.3 for Debian
Service  uid    gid   pid     machine
----------------------------------------
seb      seb    seb   11923   ys       (192.168.200.51) Tue May 13 11:31:12 2003

No locked files
```

smbclient

Le programme `smbclient` fournit un outil simple, en ligne de commande, qui permet d'accéder à un répertoire partagé sur un serveur Windows, Samba, etc. La syntaxe est très proche de celle des clients FTP.

Exemple :

```
ys:~$ smbclient //puck/seb -U seb -W ANET
added interface ip=192.168.200.51 bcast=192.168.200.255 nmask=255.255.255.0
Password:
Domain=[ANET] OS=[Unix] Server=[Samba 2.2.3a-12.3 for Debian]
smb: \> cd OpenOffice.org1.0.1
smb: \OpenOffice.org1.0.1\> ls
  LICENSE                                  5908  Wed Jun 26 07:00:00 2002
  README.html                             16075  Wed Jun 26 07:00:00 2002
                37870 blocks of size 262144. 14209 blocks available
smb: \OpenOffice.org1.0.1\> get LICENSE
getting file LICENSE of size 5908 as LICENSE (12.3 kb/s) (average 12.3 kb/s)
smb: \OpenOffice.org1.0.1\> exit
```

smbclient

Les options de `smbclient` les plus souvent utilisées sont :

`-D` *`directory`*	spécifie le répertoire par défaut lors de la connexion
`-U` *`username%password`*	
`-W` *`workgroup`*	
`-M` *`machine`*	pour envoyer un message « popup »
`-N`	ne pas demander de mot de passe
`-I` *`address`*	si la résolution du nom NetBIOS n'est pas possible
`-L`	pour afficher la liste des partages
`-T<`*`c`*`|`*`x`*`>IXFqgbNan file`	permet de faire une archive d'un paratage

`smbclient`, exemples

```
ys:~$ smbclient -L //puck -N
added interface ip=192.168.200.51 bcast=192.168.200.255 nmask=255.255.255.0
Anonymous login successful
Domain=[ANET] OS=[Unix] Server=[Samba 2.2.3a-12.3 for Debian]

        Sharename      Type      Comment
        ---------      ----      -------
        archives       Disk
        groupes        Disk
        IPC$           IPC       IPC Service (puck server (Samba ...
        ADMIN$         Disk      IPC Service (puck server (Samba ...
        lp             Printer   Generic dot-matrix printer entry

        Server               Comment
        ---------            -------
        PUCK                 puck server (Samba 2.2.3a-12.3 for Debian)

        Workgroup            Master
        ---------            -------
        ANET                 PUCK
```

`smbclient`, exemples

Sauvegarde du répertoire `user` qui est sur le partage `\\puck\seb` vers le fichier `user.tar` :

```
ys:~$ smbclient //puck/seb -U seb%VerySecret -D user -Tc user.tar
```

Envoi d'un message « popup » :

```
ys:~$ nmblookup yvain
querying yvain on 192.168.201.255
192.168.201.243 yvain<00>
ys:~$ smbclient -M yvain
added interface ip=192.168.201.51 bcast=192.168.201.255 nmask=255.255.255.0
added interface ip=127.0.0.1 bcast=127.255.255.255 nmask=255.0.0.0
Got a positive name query response from 127.0.0.1 ( 192.168.201.243 )
Connected. Type your message, ending it with a Control-D
Test... (Désolé)
-- Seb
^Dsent 26 bytes
```

smbtar

`smbtar` est un script shell qui utilise l'option `-T` de `smbclient` afin de mettre en oeuvre des sauvegardes automatiques de partages distants.

Exemples :

Mise sur bande (par exemple, un lecteur DAT) du répertoire `Data` situé sur le partage `seb` de la machine `puck`, la connexion est réalisée avec le login `seb` et le mot de passe `SuperSecret` :

```
ys:~$ smbtar -s puck -u seb -p SuperSecret -x seb -d Data -t /dev/st0
```

Création d'une archive compressée nommée `backup.tar.gz` du partage `backup` de la machine `puck`, le mot de passe est `backupPwd` :

```
ys:~$ smbtar -s puck -p backupPwd -t - | gzip > backup.tar.gz
```

nmblookup

`nmblookup` est un outil qui permet de tester la résolution des noms NetBIOS en ligne de commande.
Exemple :

```
puck:~# nmblookup puck
querying puck on 192.168.200.255
192.168.200.1 puck<00>
puck:~# nmblookup -S puck
querying puck on 192.168.200.255
192.168.200.1 puck<00>
Looking up status of 192.168.200.1
        PUCK            <00> -         M <ACTIVE>
        PUCK            <03> -         M <ACTIVE>
        PUCK            <20> -         M <ACTIVE>
        ..__MSBROWSE__. <01> - <GROUP> M <ACTIVE>
        ANET            <00> - <GROUP> M <ACTIVE>
        ANET            <1b> -         M <ACTIVE>
        ANET            <1d> -         M <ACTIVE>
        ANET            <1e> - <GROUP> M <ACTIVE>
```

Winbind

La problématique qui se présente régulièrement est la suivante : un serveur Samba est configuré pour authentifier auprès d'un serveur NT ou 2000 (avec la directive `security`).

Mais cela ne concerne que la vérification des mots de passe présentés par les clients. Par conséquent, les utilisateurs et groupes doivent être connus du serveur Unix.

Ce qui conduit à la redondance des listes des utilisateurs (dans la base des utilisateurs du serveur NT ou 2000 et dans les fichiers `/etc/passwd` et `/etc/group` du Linux).

Winbind propose une solution intéressante à ce problème. Il s'appuit sur les mécanismes traditionnels PAM et nsswitch de Linux.

PAM

Les PAM (Pluggable Authentication Modules) permettent à un système Linux (ou Solaris®) d'authentifier les utilisateurs du système à partir de bases de données d'utilisateurs distantes.
Par exemple : NIS (anciennement « Yellow Pages »), LDAP, etc.

Pour cela chaque service du serveur Linux dispose d'un fichier dans le répetoire `/etc/pam.d` qui lui permet d'obtenir les paramètres d'authentification.

Par exemple :

```
seb@puck:~$ cat /etc/pam.d/pop
#%PAM-1.0
auth     required       pam_unix_auth.so
account  required       pam_unix_acct.so
password required       pam_unix_passwd.so
session  required       pam_unix_session.so
```

nsswitch

nsswicth a le même rôle que PAM en ce qui concerne les informations des utilisateurs (login, UID, GID, gecos, répertoire personnel, shell) et des groupes du système (nom, GID, membres).

La fichier de configuration de nsswitch est `/etc/nsswitch.conf`.

Un extrait de ce fichier est :

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

Principe de Winbind

Les utilisateurs et groupes créés dans Windows NT ou 2000 ont un attribut nommé RID.
Le rôle principal de Winbind est d'effectuer une correspondance entre le RID de ces enregistrements et les UID et GID d'Unix.

Ces correpondances sont arbitraires et sont conservées en cache sur le serveur Linux.

Le démon `winbindd` est chargé des communications RPC entre le module PAM Winbind et le contrôleur de domaine.

Configuration de Winbind

Dans le fichier /etc/nsswitch.conf :

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

Dans la section `[global]` du fichier `smb.conf` :

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

Enfin, s'assurer que le service `winbindd` est bien activé au démarrage de la machine (par exemple avec `ntsysv`).