

AGR3r

Administration et gestion des réseaux

Samba

Pierre BETTENS
pbettens@heb.be

ESI - École Supérieure d'Informatique

12/10/2009

- Cours-laboratoire (12 $\frac{1}{2}$ h)
 - Exposé oral
 - Manipulation
- Évaluation
 - Évaluation du *savoir*
Présentation d'un question théorique orale
 - Évaluation du *savoir-faire*
Manipulation telles que celles présentées au cours
- Supports
 - Références
 - Livre Samba - **Samba. installation et mise en oeuvre** Robert ECKSTEIN, David COLLIER-BROWN, Peter KELLY Ed. O'REILLY - ISBN : 2-84177-090-7
 - *Samba3-HOWTO et Samba3-byExample*
 - <http://samba.org>
 - Copie des slides
- Contact
 - [irc.freenode.net / #esi](irc://freenode.net/#esi)
 - esi.namok.be

• Préalables

- Intégration *MS Windows / Linux*
- Cohabitation implique
 - Identification des utilisateurs
 - Partage de fichiers
 - Partage d'autres ressources
 - *mails*
 - imprimantes
 - Utilisation d'applications particulières
 - Émulateur
 - Serveur d'application
 - Choix d'une application
- Différentes solutions d'intégration

• Samba, une solution ...

- Samba fournit des services de partage de données et d'impression pour des clients MS Windows (ou *nix).
- Samba implémente le protocole SMB (sur TCP/IP) afin de permettre la communication entre machines hétérogènes.

- **Définition** : NetBIOS représente le mode de nommage Microsoft pour partager des ressources entre machines dans un réseau local
- NetBIOS est une API au niveau *applications* (couche 4) sur les ports 137, 138 et 139
 - couche 3 : transport, **NetBT**, implémentation de NetBIOS sur IP
 - Sans serveur WINS (voir plus loin) NetBT fait la résolution de noms par broadcast
 - Implique de travailler sur le même segment IP (par défaut), pas de routage
 - Les machines sur un même segment finiront toujours par se "voir"
 - couche 2 : internet **IP**
 - couche 1 : accès réseau
- **Remarques** :
 - Jadis, NetBIOS était directement implémenté via NetBEUI¹ (couche 2) sans utiliser TCP/IP
 - On ne distingue pas ici les notions de *domaine* et de *groupe de travail*.

¹NetBUI est un protocole IBM datant de 1985

- Un nom NetBIOS est composé de **15 + 1** caractères
 - Les premiers représentent le nom NetBIOS
 - Nom de la machine **ou**
 - Nom du domaine/*workgroup*
 - Le 16^e caractérise le rôle
 - 00 service station de travail
 - 1B maître explorateur du domaine
 - 1D serveur WINS
 - ...
- Chaque machine déclare (par broadcast) deux noms ²
 - le *workgroup* ou le domaine
 - nom de machine

²Ils **doivent** être différents

- Packages disponibles dans les principales distributions Linux
 - `samba-common`
 - `samba-doc`
 - `smbfs`
 - `smbclient`
 - ...
- Source et packages disponibles sur <http://samba.org>

- Samba est constitué de 3 daemons
 - *nmbd*

Prend en charge les requêtes de résolution de nom et d'enregistrement des noms. Il est impliqué dans le voisinage réseau.
Il prend en charge les protocoles basés sur UDP.
 - *smbd*

Prend en charge les connexions (basées sur TCP/IP) pour le partage de fichiers et d'imprimantes.
Administre l'authentification locale.
 - *winbindd*

Démarré lorsque Samba est membre d'un domaine Windows NT ou Active Directory.
- Lancement des daemons (SysV, ...)
- **Remarque** : Samba4 = un daemon `smbd`

- Fichier de configuration `smb.conf`
 - Découpé en **sections**
 - Débute par le nom du partage entre crochets
 - [*sharename*]
 - Se termine par la fin de fichier ou la section suivante
 - Trois sections particulière, `global`, `homes`, `printers`
 - Section composée de couple *paramètre-valeur*
 - *paramètre* = *valeur*
 - `workgroup = bbeer`
 - Commentaires : `#` ou `;`
 - Le fichier de configuration est relu chaque minute
- Localisation dépendante du binaire
 - `# smbd -b | grep smb.conf`
- Validation du fichier de configuration
 - `$ testparm /etc/samba/smb.conf`

- Liste des partages
 - `$ smbclient -L hostname`
- Accès à un partage
 - Accès *like ftp*
 - `$ smbclient //hostname/sharename`
 - `C : \ net use z : \\hostname\sharename`
- Ajout d'un partage au *file system*
 - `$ smbmount //hostname/sharename mountpoint`
 - Equivalent à `mount -t smbfs ...` sans les prérogatives root
 - `$ smbmount mountpoint` pour démonter

- **Exercice 1**
- *Samba3-HOWTO*,
Section 2.3.1.1 et 2.3.1.2 (pp 17-27)
 - Anonymous read-only document server
 - Anonymous read-write document server
 - `/export` remplacé par `~/exercicel/export`
 - `workgroup = BBEER`
- **Remarque** : Pour tous les exercices, on préférera modifier le fichier de configuration proposé par la distribution plutôt que de partir d'un fichier de configuration "vide"

- Liste de *browsing* (d'exploration)
 - Permet de visualiser les partages Samba et Microsoft Windows dans le voisinage réseau
 - Le voisinage réseau est l'ensemble des machines faisant tourner NetBIOS dans un segment
 - Pour visualiser les partages sur une machine hors segment (derrière un routeur), l'interroger via son IP sur le port 139
 - Permet de visualiser **plusieurs** *workgroups* ou domaines
 - Paramètre `browseable` = *yes/no*
- Chaque machine informe le maître explorateur (*master browser*) de sa présence toutes les **12'**

- *Master browser*

- Détient la liste de browsing qu'il met à jour grâce aux annonces des autres (via `__MSBROWSE__ [01]`)
- Est élu
 - Le choix se fait en fonction de l'OS, le rôle, la version, ...
 - Paramètre `os level = number`
 - Une élection est déclenchée
 - dès que l'on ne trouve pas de *master browser*
 - un client détecte la disparition d'un *master browser*
 - un serveur samba démarre et "demande" l'élection
- Entraîne une certaine inertie
 - Après chaque élection, *broadcast* du nouveau *master browser* et *ack* des autres
 - Avant de considérer une machine comme éteinte, *master browser* attend 36 minutes
- Pour limiter l'inertie
 - Rendre un serveur inéligible (`master browser = no`)
 - Utiliser un serveur WINS

- Serveur WINS
 - Système de centralisation des liste de noms des machines
 - Permet la correspondance adresse IP / noms NetBIOS
- Permet de limiter les *broadcast* et fonctionne "derrière les routeurs"
 - Les clients se signalent au serveur WINS (via son IP)
 - Les clients font leur requête de demande de noms/IP au serveur WINS (via son IP)
- Si un client ne s'identifie pas auprès du serveur WINS il ne pourra pas interroger le serveur WINS mais
 - S'il est sur le même segment, le serveur WINS recevra (un jour) sont *broadcast* de signalement et l'insrira pour ses clients
 - S'il n'est pas sur le même segment, il est invisible

- Types d'authentification
 - Paramètre `security`
 - `share`
 - Demande de jeton à chaque accès à un partage
 - (jeton éventuellement mis en cache)
 - `user`
 - Demande du jeton une fois pour l'accès à la machine ensuite le même jeton est utilisé quel que soit le partage
 - `server`
 - *idem* `user` mais via un serveur tiers
 - `domain`
 - Demande d'authentification auprès d'un contrôleur de domaine

- Samba comprend un certain nombre de variables dans son fichier de configuration
 - Par exemple
 - %I, adresse IP du client
 - %m, nom netbios du client
 - %M, nom DNS du client
 - %u, nom d'utilisateur *nix
 - %g, nom du groupe de l'utilisateur %u
 - Ces variables permettent un contrôle plus fin des accès au serveur

- **Exercice 2**

- *Samba3-ByExample*

Chapter 2, small office networking
(pp 29-51)

- Conserver les noms de machines habituels
- Omettre les configurations d'imprimantes
- Pas de configuration automatique au niveau réseau
- Travailler par groupes de 3 machines
 - 4-6, 192.168.210.0/24 - 192.168.211/24
 - 7-9, 192.168.210.0/24 - 192.168.212/24
 - 10-12, 192.168.210.0/24 - 192.168.213/24
 - 13-16, 192.168.210.0/24 - 192.168.214/24
- /data remplacé par ~/exercice2/data

- Peu d'utilisateurs, peu de changements (création/destruction de comptes)
smbpasswd file
 - passdb backend = smbpasswd, guest
 - fichier, /etc/samba/smbpasswd
 - Possibilité de synchroniser les *passwords* Samba avec les *passwords* *nix
 - password program = /usr/bin/passwd %u
- Nombre d'utilisateurs plus conséquent (mais <250), le serveur peut jouer le rôle de PDC
tdbsam (trivial database)
 - passdb backend = tdbsam
 - fichier(s) *.tdb* dans le répertoire /var/lib/samba/
 - Possibilité identique de synchronisation des *passwords*
 - Ne permet pas la réplication (un seul PDC dans le domaine)

- Lorsque la charge est plus importante, le serveur est PDC et il existe un (des) BDC dans le domaine

Annuaire ldap

- `passdb backend = ldapsam :ldap ://<hostname>`
- serveur ldap local ou distant pour un BDC
- Active Directory
 - *attendre Samba4 pour un implémentation complète de AD*

- Restriction d'accès aux partages
 - `invalid users`
 - Utilisateurs ou groupes (@)
 - *invalid users*, prévaut sur *valid users*
- Accès superutilisateur
 - `admin users`
 - Permet de définir des utilisateurs Samba ayant accès *root* au partage
- Accès
 - `hosts allow / hosts deny`
 - Permet de restreindre l'accès de différentes machines

- Partage d'imprimantes
 - Installation basique
 - Partage `printers`
 - Paramètre `load printers = yes`
 - Possibilité de configuration "automatique" des imprimantes
 - ...
- Intégration de LDAP
- $12\frac{1}{2}$, *c'est décidément trop court ...*

- Freemind
- Script *freemind2beamer*
- L^AT_EX
- Package Beamer pour L^AT_EX (pour les slides)