AGR3r
Administration et gestion des réseaux
Samba

Pierre BETTENS
pbettens(à)heb.be

ESI - École Supérieure d'Informatique

08/10/2010

Organisation

- 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*
  - `esi.namok.be`

Préalables

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

- 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.

Préalables protocolaires

- **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 NetBEUI [1] (couche 2) sans utiliser TCP/IP
  - On ne distingue pas ici les notions de *domaine* et de *groupe de travail*.

1. NetBUI est un protocole IBM datant de 1985

Préalables protocolaires

- 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
    - ...
  - `$ nmblookup -A <ip>` ou
    `C: nbtstat -A <ip>`
- Chaque machine déclare (par broadcast) deux noms [2]
  - le *workgroup* ou le domaine
  - nom de machine

2. Ils **doivent** être différents

Installation

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

Daemons

- 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`

Configuration

- 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`

Commandes élémentaires

- 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`
  - `$ smbumount` *`mountpoint`* pour démonter

Exercice 1

- **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 `~/exercice1/export`
  - `workgroup = BBEER`
- **Remarque :** Pour tous les exercices, on préfèrera modifier le fichier de configuration proposé par la distribution plutôt que de partir d'un fichier de configuration "vide"

Liste de browsing

- 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 (derrrière un routeur), l'interroger via son IP sur le port 139
    - Permet de visualiser **plusieurs** *workgroups* ou domaines
  - Paramètre `browseable = yes|no` ($ en fin de nom sous MS Windows)
- Chaque machine informe le maître explorateur (*master browser*) de sa présence toutes les **12'**

Maître explorateur

- *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
  - Entraine une certain inertie
    - Après chaque élection, *broadcast* du nouveau *master browser* et *ack* des autres
    - Avant de considérer une machine comme éteinte, *master browser* attend 3 mise à jour, soit +- 36 minutes
  - Pour limiter l'inertie
    - Rendre un serveur inéligible (`master browser = no`)
    - Utiliser un serveur WINS

Serveur WINS

- Serveur WINS
  - Système de centralisation des listes 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'inscrira pour ses clients
  - S'il n'est pas sur le même segment, il est invisible

Authentification des utilisateurs

- 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

Authentification des utilisateurs

- Protocole d'authentification "*challenge-response*"
  - **Primo** Le client envoie une requête au serveur se présentant (`negotiate_message`)
  - **Secundo** Le serveur répond en envoyant un *challenge*, un nombre aléatoire de 8 bits (`challenge_message`)
  - **Tertio** Le client calcule un *hash* sur base du challenge et du password (`authenticate_message`)
  - **Quarto** Le serveur accepte le client (ou pas)
- NTLM (NT Lan Manager) est un protocole d'authentification *challenge-response*
  - Le client utilise un hash du mot de passe de 24 bits
  - En fonction de la version du protocole, NTLM utilise différentes fonctions de hashage
    - **LanMan** (permet le hashage de 14 caractères en majuscules)
    - **NT** (MD4)
    - Aucune de ces deux fonctions n'utilise de graine (*salt*)

Authentification des utilisateurs

- **NTLMv1**, première version de l'algorithme
  - Paramètre samba,
    `encrypt passord = yes`
  - Le client fournit **deux** réponses (LanMan et NT) et `smbpasswd` contient
    - Si le password <14 caractères
      `login:1004:01FC5A6BE7BC6929AAD3B435B51404EE :`
      `0CB6948805F797BF2A82807973B89537:[U ]:LCT-44528BD2:`
    - Si le password >14 caractères, LanMan est désactivé
      `login:1009:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX :`
      `0FF1DFDA18B63EC50E1FD9ECFCDFDE05:[U ]:LCT-44528C6B:`
  - Pour désactiver l'utilisation de LanManager,
    `lanman auth = no`

Authentification des utilisateurs

- **NTLMv2**, deuxième version de l'algorithme
  - Variante introduite avec MS *Windows NT 4.0 SP4*
  - Utilise une fonction de hashage HMAC - MD5
  - Lorsque la réponse d'un client (dans le challenge d'authentification) est au format NTLMv2, Samba utilise NTLMv2 sinon le serveur utilise NTLMv1
    - Désactiver NTLMv1 renforce la sécurité du serveur
  - Pour désactiver NTLMv1, désactiver LanManager et `ntlm auth = no`

Authentification des utilisateurs

- Dans un cadre Windows 2000 et/ou Active Directory, **Kerberos** est l'algorithme d'authentification utilisé

Authentification des utilisateurs

- L'utilisateur a différentes manières de se connecter à un serveur Samba. Le serveur réagira différement en fonction du cas
  - Différentes manières de se connecter à un serveur Samba
    - 1. Si le client fournit un couple *login/password* et qu'il est valide, la connexion est faite en temps qu'utilisateur *login*
    - 2. Si le client a, au préalable, enregistré un *login* et qu'il fournit un *password* valide pour ce *login*, la connexion est faite en temps qu'utilisateur *login*
    - 3. Le nom Netbios du client et tous les *logins* fournis précédemment sont testés avec le *password* fourni. Si l'un d'entre eux correspond, la connexion est faite en temps qu'utilisateur *ce login*
    - 4. Si le client a déjà validé un couple *login/password* et que le client refournit le *token*, ce *login* est utilisé
    - 5. Si un paramètre `user = ...` est renseigné dans le fichier de configuration `smb.conf`, que le client fournit un *password* correspondant à l'un des *users*, la connexion est faite avec ce *login*
    - 6. Si le service est *guest*, la connexion est autorisée en utilisant le *login* `guest account` sans se soucier du *password* fourni
  - Si `guest only = yes` pour le partage et `security = share` alors le serveur passse directement au dernier point

Authentification des utilisateurs

- L'utilisateur a différentes manières de se connecter à un serveur Samba. Le serveur réagira différement en fonction du cas
  - Différentes manières de se connecter à un serveur Samba
    - 1. Si le client fournit un couple *login/password* et qu'il est valide, la connexion est faite en temps qu'utilisateur *login*
    - 2. Si le client a, au préalable, enregistré un *login* et qu'il fournit un *password* valide pour ce *login*, la connexion est faite en temps qu'utilisateur *login*
    - 3. Le nom Netbios du client et tous les *logins* fournis précédemment sont testés avec le *password* fourni. Si l'un d'entre eux correspond, la connexion est faite en temps qu'utilisateur *ce login*
    - 4. Si le client a déjà validé un couple *login/password* et que le client refournit le *token*, ce *login* est utilisé
    - 5. Si un paramètre `user = ...` est renseigné dans le fichier de configuration `smb.conf`, que le client fournit un *password* correspondant à l'un des *users*, la connexion est faite avec ce *login*
    - 6. Si le service est *guest*, la connexion est autorisée en utilisant le *login* `guest account` sans se soucier du *password* fourni
  - Si `guest only = yes` pour le partage et `security = share` alors le serveur passse directement au dernier point

Authentification des utilisateurs

- L'utilisateur a différentes manières de se connecter à un serveur Samba. Le serveur réagira différement en fonction du cas
  - Différentes manières de se connecter à un serveur Samba
    - 1. Si le client fournit un couple *login/password* et qu'il est valide, la connexion est faite en temps qu'utilisateur *login*
    - 2. Si le client a, au préalable, enregistré un *login* et qu'il fournit un *password* valide pour ce *login*, la connexion est faite en temps qu'utilisateur *login*
    - 3. Le nom Netbios du client et tous les *logins* fournis précédemment sont testés avec le *password* fourni. Si l'un d'entre eux correspond, la connexion est faite en temps qu'utilisateur *ce login*
    - 4. Si le client a déjà validé un couple *login/password* et que le client refournit le *token*, ce *login* est utilisé
    - 5. Si un paramètre `user = ...` est renseigné dans le fichier de configuration `smb.conf`, que le client fournit un *password* correspondant à l'un des *users*, la connexion est faite avec ce *login*
    - 6. Si le service est *guest*, la connexion est autorisée en utilisant le *login* `guest account` sans se soucier du *password* fourni
  - Si `guest only = yes` pour le partage et `security = share` alors le serveur passse directement au dernier point

Authentification des utilisateurs

- L'utilisateur a différentes manières de se connecter à un serveur Samba. Le serveur réagira différement en fonction du cas
  - Différentes manières de se connecter à un serveur Samba
    - 1. Si le client fournit un couple *login/password* et qu'il est valide, la connexion est faite en temps qu'utilisateur *login*
    - 2. Si le client a, au préalable, enregistré un *login* et qu'il fournit un *password* valide pour ce *login*, la connexion est faite en temps qu'utilisateur *login*
    - 3. Le nom Netbios du client et tous les *logins* fournis précédemment sont testés avec le *password* fourni. Si l'un d'entre eux correspond, la connexion est faite en temps qu'utilisateur *ce login*
    - 4. Si le client a déjà validé un couple *login/password* et que le client refournit le *token*, ce *login* est utilisé
    - 5. Si un paramètre `user = ...` est renseigné dans le fichier de configuration `smb.conf`, que le client fournit un *password* correspondant à l'un des *users*, la connexion est faite avec ce *login*
    - 6. Si le service est *guest*, la connexion est autorisée en utilisant le *login* `guest account` sans se soucier du *password* fourni
  - Si `guest only = yes` pour le partage et `security = share` alors le serveur passse directement au dernier point

Authentification des utilisateurs

- L'utilisateur a différentes manières de se connecter à un serveur Samba. Le serveur réagira différement en fonction du cas
  - Différentes manières de se connecter à un serveur Samba
    - 1. Si le client fournit un couple *login/password* et qu'il est valide, la connexion est faite en temps qu'utilisateur *login*
    - 2. Si le client a, au préalable, enregistré un *login* et qu'il fournit un *password* valide pour ce *login*, la connexion est faite en temps qu'utilisateur *login*
    - 3. Le nom Netbios du client et tous les *logins* fournis précédemment sont testés avec le *password* fourni. Si l'un d'entre eux correspond, la connexion est faite en temps qu'utilisateur *ce login*
    - 4. Si le client a déjà validé un couple *login/password* et que le client refournit le *token*, ce *login* est utilisé
    - 5. Si un paramètre `user = ...` est renseigné dans le fichier de configuration `smb.conf`, que le client fournit un *password* correspondant à l'un des *users*, la connexion est faite avec ce *login*
    - 6. Si le service est *guest*, la connexion est autorisée en utilisant le *login* `guest account` sans se soucier du *password* fourni
  - Si `guest only = yes` pour le partage et `security = share` alors le serveur passse directement au dernier point

Authentification des utilisateurs

- L'utilisateur a différentes manières de se connecter à un serveur Samba. Le serveur réagira différement en fonction du cas
  - Différentes manières de se connecter à un serveur Samba
    - 1. Si le client fournit un couple *login/password* et qu'il est valide, la connexion est faite en temps qu'utilisateur *login*
    - 2. Si le client a, au préalable, enregistré un *login* et qu'il fournit un *password* valide pour ce *login*, la connexion est faite en temps qu'utilisateur *login*
    - 3. Le nom Netbios du client et tous les *logins* fournis précédemment sont testés avec le *password* fourni. Si l'un d'entre eux correspond, la connexion est faite en temps qu'utilisateur *ce login*
    - 4. Si le client a déjà validé un couple *login/password* et que le client refournit le *token*, ce *login* est utilisé
    - 5. Si un paramètre `user = ...` est renseigné dans le fichier de configuration `smb.conf`, que le client fournit un *password* correspondant à l'un des *users*, la connexion est faite avec ce *login*
    - 6. Si le service est *guest*, la connexion est autorisée en utilisant le *login* `guest account` sans se soucier du *password* fourni
  - Si `guest only = yes` pour le partage et `security = share` alors le serveur passse directement au dernier point

Authentification des utilisateurs

- L'utilisateur a différentes manières de se connecter à un serveur Samba. Le serveur réagira différement en fonction du cas
  - Différentes manières de se connecter à un serveur Samba
    - 1. Si le client fournit un couple *login/password* et qu'il est valide, la connexion est faite en temps qu'utilisateur *login*
    - 2. Si le client a, au préalable, enregistré un *login* et qu'il fournit un *password* valide pour ce *login*, la connexion est faite en temps qu'utilisateur *login*
    - 3. Le nom Netbios du client et tous les *logins* fournis précédemment sont testés avec le *password* fourni. Si l'un d'entre eux correspond, la connexion est faite en temps qu'utilisateur *ce login*
    - 4. Si le client a déjà validé un couple *login/password* et que le client refournit le *token*, ce *login* est utilisé
    - 5. Si un paramètre `user = ...` est renseigné dans le fichier de configuration `smb.conf`, que le client fournit un *password* correspondant à l'un des *users*, la connexion est faite avec ce *login*
    - 6. Si le service est *guest*, la connexion est autorisée en utilisant le *login* `guest account` sans se soucier du *password* fourni
  - Si `guest only = yes` pour le partage et `security = share` alors le serveur passse directement au dernier point

Authentification des utilisateurs

- L'utilisateur a différentes manières de se connecter à un serveur Samba. Le serveur réagira différement en fonction du cas
  - Différentes manières de se connecter à un serveur Samba
    - 1. Si le client fournit un couple *login/password* et qu'il est valide, la connexion est faite en temps qu'utilisateur *login*
    - 2. Si le client a, au préalable, enregistré un *login* et qu'il fournit un *password* valide pour ce *login*, la connexion est faite en temps qu'utilisateur *login*
    - 3. Le nom Netbios du client et tous les *logins* fournis précédemment sont testés avec le *password* fourni. Si l'un d'entre eux correspond, la connexion est faite en temps qu'utilisateur *ce login*
    - 4. Si le client a déjà validé un couple *login/password* et que le client refournit le *token*, ce *login* est utilisé
    - 5. Si un paramètre `user = ...` est renseigné dans le fichier de configuration `smb.conf`, que le client fournit un *password* correspondant à l'un des *users*, la connexion est faite avec ce *login*
    - 6. Si le service est *guest*, la connexion est autorisée en utilisant le *login* `guest account` sans se soucier du *password* fourni
  - Si `guest only = yes` pour le partage et `security = share` alors le serveur passse directement au dernier point

Configuration II

- 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

- **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`

Authentification

- 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)

Authentification

- 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*

Sécurité

- 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

Notions non abordées

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

Crédits

- Freemind
- Script *freemind2beamer*
- LaTeX
- Package Beamer pour LaTeX(pour les slides)