LINAGORA

Formation samba 3

Auteur : Ganaël LAPLANCHE, v1.2

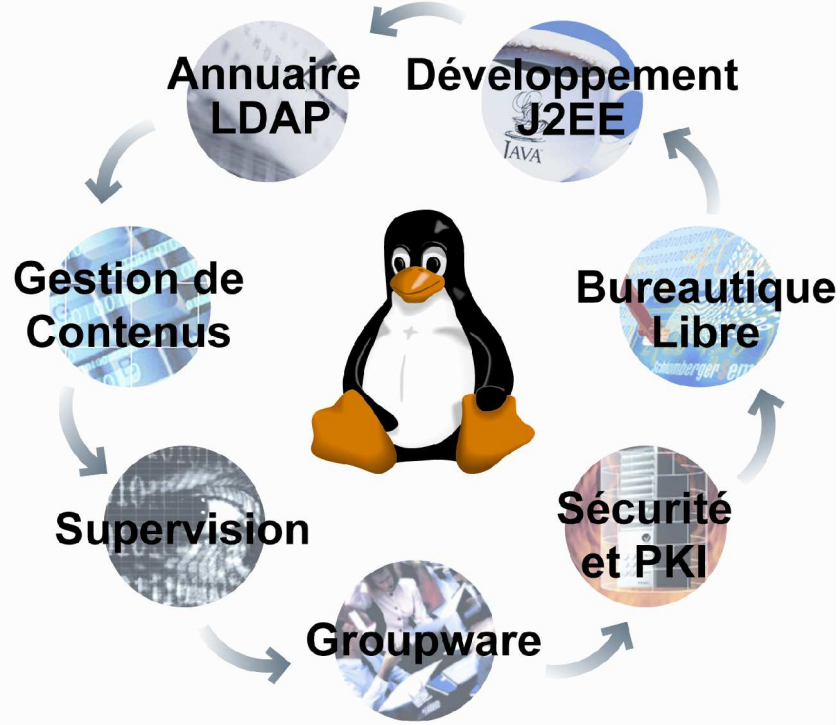
LINAGORA

- SS2L créée en mai 2000, 40 personnes
- Déjà plus de 500 clients :
  95% de grands comptes, dont
  75% dans le secteur public
- Présente sur les 3 phases d'un projet :
  - Conseil (“Consulting”)
  - Ingénierie (“Built”)
  - Assistance (“Run”)
- Plus : LINAGORA Solutions et LINAGORA Formations

Centres de compétences

- Compétences regroupées en 7 centres :

  - Annuaire LDAP
  - Gestion de contenus
  - Supervision
  - Groupware
  - Sécurité et PKI
  - Bureautique libre
  - Développement J2EE



LINAGORA formations

- Plus de 60 modules exclusivement dédiés aux technologies du libre
- Regroupés en 7 filières métiers :

  - “Indispensables” : Linux exploitation, shell Linux [...]
  - Administration et sécurité : Ldap, Samba, messagerie [...]
  - Développement web : Python, LAMP, Zope [...]
  - Développement système et embarqué : PERL, noyau Linux [...]
  - Administration de bases de données : SQL, PostgreSQL [...]
  - J2EE : Programmation objet, Programmation JAVA [...]
  - Bureautique : OpenOffice Writer, Impress [...]

La formation Samba 3

- Fait partie intégrante du cursus de formation “Administration et sécurité”
- Fournit les éléments nécessaires à :
  - L'installation et la configuration de Samba 3
  - La compréhension et la mise en place d'un domaine
  - La gestion des comptes sur le domaine
  - La mise en place d'imprimantes et de partages de fichiers
  - La migration d'un domaine NT
  - L'administration quotidienne de Samba
- Pré-requis : Linux exploitation, shell Linux, Linux administration

LINAGORA

Introduction

- Formation de 3 jours, 3 parties
- Chapitres ponctués de TPs

LINAGORA

Plan global du cours

- Partie 1 :
  I) Introduction à Samba
  II) Samba v3
  III) Rappels sur les domaines NT4
  IV) Samba : les premiers pas
  V) Le fichier de configuration smb.conf
  VI) Gestion des comptes
- Partie 2 :
  VII) Gestion des droits
  VIII) L'impression sous Samba
  IX) Samba en PDC
- Partie 3 :
  X) La migration depuis NT
  XI) Administrer Samba au quotidien
  XII) Autres outils d'administration
  XIII) S'informer, se documenter
  XIV) Conclusion

LINAGORA

Plan (partie1)

- I) Introduction à Samba
- II) Samba v3
- III) Rappels sur les domaines NT4
- IV) Samba : les premiers pas
- V) Le fichier de configuration smb.conf
- VI) Gestion des comptes

LINAGORA

Chapitre I : Introduction à Samba

Le projet Samba

- Projet sous licence GPL v2 (http://www.samba.org)
- Permet d'interconnecter des systèmes hétérogènes :

  - Partage de fichiers
  - Partage d'imprimantes
  - Support de NetBIOS
  - Gestion de domaine (authentification)
  - Outils divers

- Partage de ressources bidirectionnel

Historique

- Projet démarré en 1991 par Andrew Tridgell, étudiant à l'Université Nationale d'Australie
- Au départ : monter un partage de fichiers SMB sur une machine Unix. Le projet prend rapidement de l'ampleur
- Actuellement, la “Samba Team” compte plus de 30 personnes
- La version actuelle de Samba est la version 3

LINAGORA

Chapitre II : Samba v3

Samba 2

- Version éprouvée, dernière v.2 en date : 2.2.8a
- Support de LDAP dans les dernières versions 2
- Limites :
  - Code relativement statique, difficile à maintenir
  - Gestion des groupes limitée (via smb.conf)
- Cette version n'est plus conseillée en production

Samba 3

- Version 3.0.0 sortie en septembre 2003
- Nouveautés :
  - Gestion de backends par modules
  - Support du mapping de groupes
  - Nouvelle commande 'net'
  - Amélioration du support d'impression
  - Outils de migration
  - Support des relations d'approbation
  - Support initial d'Active Directory

Limites de Samba 3

- Encore quelques limites :

  - Serveur *membre* Active Directory
  - Pas de support des groupes imbriqués
  - Ne peut être BDC d'un PDC NT4

- La version 4 de Samba devrait résoudre ces problèmes et offrira un code intégralement réécrit

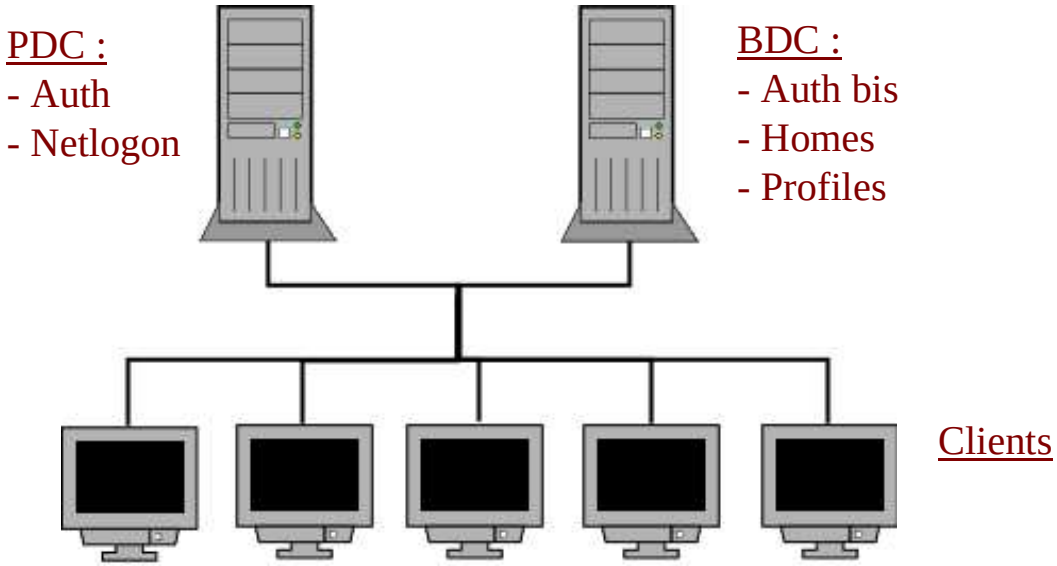
LINAGORA

Chapitre III : Rappels sur les domaines NT4

Un domaine NT - définition

- Regroupement logique d'acteurs :
  - Utilisateurs
  - Groupes
  - Machines
- Et de ressources :
  - Partages de fichiers
  - D'imprimantes
- Gestion unifiée des droits sur ces ressources

- Un domaine est composé de plusieurs éléments :
  - Contrôleur principal (PDC) - Logons
  - Contrôleur(s) secondaire(s) (BDC) - Backup
  - Serveur(s) membre(s) – Fichiers
  - Stations de travail - Clients



Un domaine Microsoft

Les acteurs du domaine

- Comptes d'utilisateurs
- Comptes de machines ($)
- Comptes de groupes

- Comptes locaux vs globaux
  => La portée du compte local est limitée à la machine qui l'héberge.
- Comptes prédéfinis

Les SIDs

- Numéro unique sur un domaine
- Identifie un acteur (utilisateur, groupe, machine)
- Format = “SID Local-RID” :
  ex : S-1-5-21-4109349211-2507905533-872075644-513
- “SID Local” : SID du domaine (unique)
- “RID” : nombre qui identifie l'acteur au sein du domaine (513 = Utilisateurs du domaine)
- Cf. “Well-known RIDs” : 512, 513, 514, 515, [...]
  http://msdn.microsoft.com/library/en-us/security/security/well_known_sids.asp
  http://de.samba.org/samba/docs/man/groupmapping.html#WKURIDS

LINAGORA

Chapitre IV : Samba, les premiers pas

Samba, vue globale

- Disponible sur : http://www.samba.org
- Packages disponibles pour la plupart des distributions GNU/Linux.
- Se compose de 3 démons :
  smbd : partage de fichiers – CIFS (SMB)
  nmbd : gestion de la couche netbios
  winbindd : connexion à une source externe (ex. : NT) pour l'authentification sous Unix (cf. nsswitch)

Les autres fichiers/commandes Samba

- Plusieurs commandes à notre disposition smbpasswd, net, smbclient [...] pour l'administration quotidienne
- Des fichiers de cache maintiennent l'état des connexions
- Documentation complète et fichiers d'exemples dans l'archive contenant les sources

Configuration de Samba

- S'effectue via un fichier unique : smb.conf
- Situé, suivant le type d'installation, dans :
  /usr/local/samba/lib/smb.conf (installation par les sources)
  /etc/samba/smb.conf (installation par binaires)
- Edition de ce fichier avec notre éditeur préféré...
  ...vi(m) par exemple !

La gestion des comptes sous Samba

- Dualité des comptes :
  - Un compte Samba nécessite un compte POSIX
  - Le compte Samba complète le compte POSIX
- Le compte POSIX peut être local ou distant
  => Utilisation de nsswitch (et PAM)
- Il est recommandé de centraliser les comptes POSIX et Samba dans un annuaire LDAP

LINAGORA

Chapitre V : Le fichier de configuration smb.conf

Structure du fichier

- Contient l'intégralité de la configuration Samba :
  - Comportement des serveurs smbd/nmbd
  - Comportement des commandes d'administration
  - Partages de fichiers
  - Partages d'imprimantes

- Situé par défaut dans /usr/local/samba/lib/smb.conf
- Cf. “man 5 smb.conf”

Structure du fichier (2)

- Un commentaire commence par ; ou #
- Le fichier est composé de sections et de directives

- Une section est encadrée par des []
- Une section correspond généralement à un partage
- Le partage est caché s'il se termine par un $

- Une directive s'applique à la section à laquelle elle appartient ou à toutes si elle est dans la section [global]
- Syntaxe : <directive> = <valeur>

Les sections du fichier smb.conf

- Trois sections spéciales, réservées. Ces sections réagissent différemment d'une section “normale” :

  - [global] : configuration globale
  - [homes] : répertoires personnels des utilisateurs. La section est étendue au nom de l'utilisateur
  - [printers] : configuration globale des imprimantes

Les sections du fichier smb.conf (2)

- Traditionnellement, d'autres sections sont réservées :
  - [profiles] : contient les profils itinérants des utilisateurs
  - [netlogon] : contient les scripts de connexion des utilisateurs, ainsi que les stratégies d'utilisateurs (NTConfig.POL)
  - [print$] : contient les drivers d'imprimantes

- Deux partages sont automatiquement créés par Samba :
  - [IPC$] : utilisé pour les commandes RPC
  - [ADMIN$] <=> IPC$ (utilisé par ASU)

Directives importantes [global]

- passdb backend : spécifie le backend à utiliser (smbpasswd, tdbsam, ldapsam, mysql, guest). Doit se terminer par guest pour la gestion du compte invité.
  Ex : passdb backend = tdbsam:/usr/local/samba/lib/passdb.tdb, guest
- workgroup : domaine ou workgroup auquel appartient la machine
  Ex : workgroup = mondomaine
- netbios name : nom netbios de la machine
  Ex : netbios name = mamachine
- domain logons : gestion de l'authentification sur le domaine (PDC ou BDC)
  Ex : domain logons = yes
- security : share|user|domain|server|ads. Paramètre très important sous Samba. Gère la méthode utilisée pour l'authentification des clients.
  Ex : security = user

La directive security

- 5 valeurs possibles :

  share : pas d'authentification sur le partage. Smbd doit deviner le compte à utiliser (en fonction de plusieurs paramètres). Pratique pour des partages publics.

  user : le plus souvent utilisé. Le client envoie un couple user/passwd qui est validé par Samba et sa base de comptes.

  domain : même principe que user, cependant Samba délègue l'authentification à un contrôleur (PDC ou BDC) du domaine.
  => nécessite "encrypt passwords = yes" et d'être membre du domaine (net rpc join)

  server : même principe que domain, mais indépendemment d'un domaine. Le serveur d'authentification doit être précisé. A la différence de "domain", une connexion au serveur d'authentification est maintenue.
  => nécessite l'utilisation de la directive "password server"

  ads : membre d'un domaine ADS, nécessite kerberos

Directives importantes [partage]

- Un partage standard ressemble à ceci :

  [partage] : nom du partage
  path = /export/partage : chemin local du répertoire exporté
  comment = Répertoire partagé : commentaire concernant le partage
  read only = no : peut-on y écrire ?
  browsable = yes : est-il visible dans l'explorateur ?

- Il faudra bien sûr penser à spécifier les directives de sécurité sur le partage (cf. “Gestion des droits sur un partage”)

Après la configuration...

- Ne pas oublier d'exécuter testparm pour tester la validité du fichier !
- Démarrer les démons smbd et nmbd :
  /etc/init.d/samba start ou
  smbd -D && nmbd -D

LINAGORA

Chapitre VI : Gestion des comptes

- I) Introduction à Samba
- II) Samba v3
- III) Rappels sur les domaines NT4
- IV) Samba : les premiers pas
- V) Le fichier de configuration smb.conf
- VI) Gestion des comptes

Dualité des comptes

- Comptes POSIX obligatoires
  => en local (/etc/passwd, /etc/group)
  => distants : utilisation de nsswitch (Ldap, SGBD...)
  => (utilisation de PAM si auth. sur serveur)
- Comptes Samba stockés dans un “backend”
  => fichier smbpasswd
  => fichier tdb
  => Ldap
  => MySQL
  => ...

Un compte POSIX

- Utilisé par Samba pour la gestion des droits sur le système
- Contient les informations de bases de l'utilisateur (uid, gid)

Exemple d'une entrée POSIX dans Ldap :

```
dn: uid=utilisateur,ou=Users,dc=sambatest,dc=linagora,dc=com
objectClass: account
objectClass: posixAccount
cn: utilisateur
uid: utilisateur
uidNumber: 1001
gidNumber: 100
homeDirectory: /dev/null
loginShell: /bin/false
gecos: utilisateur
description: utilisateur
```

[...suite...]

Un compte Samba

- Complète les informations du compte POSIX.

[...]
objectClass: sambaSAMAccount
displayName: Samba User
sambaSID: S-1-5-21-4109349211-2507905533-872075644-3004
sambaPrimaryGroupSID: S-1-5-21-4109349211-2507905533-872075644-513
sambaHomeDrive: U:
sambaLogonScript: utilisateur.bat
sambaProfilePath: \\LINUXPDC\profiles\utilisateur
sambaHomePath: \\LINUXPDC\utilisateur
sambaPwdCanChange: 1081326771
sambaLMPassword: BD265149BC043C3C064F1AD6E79B75DA
sambaNTPassword: 65AEECE40F54AA222DEC0726C0385963
sambaPwdLastSet: 1081326771
sambaAcctFlags: [U]

Gestion des comptes POSIX

- Rien à faire si utilisation de /etc/passwd et /etc/shadow
- Si utilisation de LDAP (ou autre), nsswitch nécessaire pour rediriger les requêtes systèmes

  => Configuration de /etc/nsswitch.conf
  => Configuration de la librairie nss utilisée

Spécification du backend Samba

- Dans le fichier smb.conf, section [global] :

  Fichier Tdb :

  ```
  passdb backend = tdbsam:/usr/local/samba/lib/passdb.tdb, guest
  ```

  Annuaire LDAP (Samba compilé avec --with-ldap)

  ```
  passdb backend = ldapsam:ldap://localhost, guest
  ldap admin dn = "cn=manager,dc=sambatest,dc=linagora,dc=com"
  ldap ssl = off
  ldap delete dn = no
  ldap user suffix = ou=Users
  ldap machine suffix = ou=Machines
  ldap group suffix = ou=Groups
  ldap suffix = dc=sambatest,dc=linagora,dc=com
  ```

- Penser à spécifier le mot de passe LDAP :

  ```
  smbpasswd -w <mot de passe>
  ```

Gestion des groupes

- Comme pour les utilisateurs, une entrée, deux types d'informations :

  Une entrée LDAP de groupe :

```
dn: cn=sambausers,ou=Groups,dc=sambatest,dc=linagora,dc=com
objectClass: posixGroup
objectClass: sambaGroupMapping
cn: sambausers
gidNumber: 513
sambaSID: S-1-5-21-4109349211-2507905533-872075644-513
sambaGroupType: 2
displayName: sambausers
description: Local Unix group
memberUid: utilisateur
```

Le mapping de groupes

- “Associer un groupe Unix à un groupe Windows”
- Concrêtement, ajoute les informations Samba aux informations POSIX du groupe ; notamment le SID du groupe.

  => net groupmap add sid=<sid> unixgroup=<groupe>

- Attention, si utilisation de LDAP, le groupe POSIX doit exister sous LDAP (entrée “de base”).

Le superutilisateur Samba

- Ce compte spécial permet d'effectuer certaines fonctions d'administrations (jonction d'une machine au domaine...)
- Il doit posséder un uid égal à 0
- On utilise généralement le compte root que l'on ajoute aux utilisateurs Samba

Ajouter/Supprimer des utilisateurs

- Sans utilisation de LDAP :
  Ajout sous Unix : useradd <utilisateur>
  Ajout dans Samba : smbpasswd -a <utilisateur>

- Avec utilisation de LDAP :
  Via un fichier ldif pour les informations POSIX
  Ajout des informations Samba : smbpasswd -a <utilisateur>

  => Les smbldap-tools automatisent ces tâches.
  Ex. : smbldap-useradd -a utilisateur
  Ajoute les comptes POSIX et samba dans LDAP.

LINAGORA

Plan (partie2)

- VII) Gestion des droits
- VIII) L'impression sous Samba
- IX) Samba en PDC

LINAGORA

Chapitre VII : Gestion des droits

- VII) Gestion des droits
- VIII) L'impression sous Samba
- IX) Samba en PDC

Deux types de droits

- Droits de connexion à un service (smb.conf)
  => Définit qui peut se connecter à un partage
  => Agit avant les droits du système de fichiers

- Droits du système de fichiers
  => Définit les droits que va avoir l'utilisateur sur les fichiers une fois connecté (rwx)
  => Possibilité d'utiliser les ACLs POSIX et les quotas
  => Utilisation de chown, chmod, setfacl et getfacl pour fixer les droits initiaux

Les droits POSIX sur le système

- Droits “ugo” : rwx
- Simples à mettre en oeuvre, moins évolués que les ACLs
- Utilisation de chown, chmod
- Le SGID bit (2) permet l'héritage du groupe propriétaire s'il est placé sur un répertoire.
  (le SUID bit n'a pas de sens sur un répertoire)

Les droits POSIX sous Samba

- Des options permettent de spécifier les droits associés aux fichiers créés :

  (force) create mode = 770
  => droits pour un fichier créé
  (force) directory mode = 2770
  => droits pour un répertoire créé

  (force) security mode = 700
  => bits sur lesquels peut agir un utilisateur (pour un fichier)
  (force) directory security mode = 0700
  => bits sur lesquels peut agir un utilisateur (pour un répertoire)

- On peut également demander à Samba de gérer l'héritage des permissions (et outrepasser les 2 options de création) :

  inherit permissions = yes
  => active l'héritage (sauf set uid bit)

Mise en place des ACLs sur le système

- Permettent de mapper plus précisément les droits Windows
  => rwx pour une liste d'utilisateurs ou de groupes.
- Doivent être supportées par le système de fichier et le noyau
  => Recompiler le noyau si besoin est
- Support des ACLs pour EXT2, EXT3, XFS
  => cf. http://acl.bestbits.at

- Activation des ACLs lors du montage des partitions :
  => Extrait de fstab :

```
/dev/hda3 /files ext3 defaults,acl  0  2
```

Mise en place des ACLs sous Samba

- Samba doit être compilé avec l'option –with-acl-support
  (Option couramment utilisée pour les packages binaires livrés dans les distributions GNU/Linux)
- Activation des ACLs dans le fichier smb.conf,
  section [global] ou [partage] :
  => nt acl support = yes
- Gestion de l'héritage des ACLs
  => inherit acls = yes
- Il faudra ensuite positionner les droits initiaux sur le système de fichiers pour les partages où les ACLs sont utilisées.
  => cf. setfacl, chown, chmod

Activation des quotas

- S'appliquent à une partition (pas à un répertoire).
  => Bien penser le partitionnement (cf. LVM)
- Doivent être supportées par le système de fichiers et le noyau
  => Recompiler le noyau si besoin est
- Quotas par groupes et/ou utilisateurs
- Activation séparément lors du montage des partitions

Extrait de fstab :

```
/dev/hda3 /files ext3 defaults,acl,usrquota,grpquota  0  2
```

Gestion des quotas

- Les quotas doivent être initialisés avec la commande “quotacheck -aug”
  => Création des fichiers de quotas [a]quota.user et [a]quota.group pour toutes les partitions supportant les quotas
- Mise en route des quotas par “quotaon -a”
- Edition des quotas par “edquota -u <utilisateur>” ou “edquota -g <groupe>”

Gestion des quotas sous Samba

- Les quotas sont automatiquement gérés si Samba a été compilé avec l'option –with-quotas
- Les limites de chaque partage apparaissent côté client en tant que taille maximale disponible sur le point de montage

Gestion des droits sur un partage

- Possibilité d'interdire/autoriser des utilisateurs ou groupes sur un partage :
  invalid users = invite, @gestion, @compta
  valid users = administrateur, @direction
- Forcer la connexion en tant qu'un utilisateur ou groupe spécifique :
  force user = utilisateur
  force group = groupe
- Spécifier les accès en lecture seule ou en lecture-écriture :
  read list = dupont, durand
  write list = @direction
- Lecture seule sur un partage :
  read only = yes
- Désactiver totalement un partage :
  -valid = no

Le signe '@' précise un groupe (recherche sur NIS puis dans les groupes Unix). Les signes '+' (recherche dans les groupes Unix uniquement) et '&' (recherche sur NIS uniquement) peuvent également être utilisés et associés pour définir l'ordre de recherche du groupe : ex : +&compta : recherche d'abord dans les groupes Unix puis sur NIS.

Les accès invités

- Autoriser l'accès en guest (cf. 'guest account')
  guest ok = yes

- Accepter uniquement les connexions guests
  guest only = yes

- Spécifier le compte utilisé pour le guest (nécessite guest ok = yes)
  guest account = utilisateur

- Définir la stratégie utilisée pour déterminer si un utilisateur est guest
  map to guest = Never|Bad User|Bad Password

LINAGORA

Chapitre VIII : L'impression sous Samba

- VII) Gestion des droits
- VIII) L'impression sous Samba
- IX) Samba en PDC

Configuration de CUPS

- Samba peut créer dynamiquement plusieurs imprimantes en utilisant la configuration du partage [printers]
- Déclarer auparavant les imprimantes dans cups via une connexion http sur le port 631 du serveur CUPS
- Imprimantes généralement déclarées en mode “raw” dans CUPS ; drivers gérés côté clients

L'impression sous Samba

- La section globale définit le système d'impression :

```
[global]
printing = cups
printcap name = cups
printer admin = @printadmins
load printers = yes
show add printer wizard = yes
```

- La section printers est ensuite utilisée pour créer dynamiquement les imprimantes (load printers = yes) :

```
[printers]
comment = Partage d'imprimantes
path = /data/spool
printable = yes
browseable = yes
guest ok = no
valid users = @sambausers
```

Add printer wizard

- Possibilité d'ajouter un partage [print$] qui permettra le téléchargement automatique de drivers chez les clients :

```
[print$]
comment = Drivers d'imprimantes
path = /data/samba/drivers
browseable = no
guest ok = yes
read only = yes
write list = @printadmins
```

- La directive "show add printer wizard = yes" propose au client de télécharger le driver via un wizard. Il faut que l'utilisateur fasse partie des utilisateurs spécifiés dans la directive "printer admin".

Add printer wizard (2)

- Il faut ensuite créer une arborescence de base dans le répertoire contenant les drivers :

  /data/samba/drivers/W32X86 : pour WinNT/2000/XP
  /data/samba/drivers/WIN40 : pour Win9x/Me

- S'assurer que le groupe “printadmins” a le droit de lecture et d'écriture sur les répertoires

- Il reste à uploader les drivers depuis le client, en tant qu'administrateur, via un clic droit sur une imprimante et “avancé/nouveau pilote”

LINAGORA

Chapitre IX : Samba en PDC

- VII) Gestion des droits
- VIII) L'impression sous Samba
- IX) Samba en PDC

Modification du fichier smb.conf

- Gestion des authentifications sur le domaine
  domain logons = yes
- Activation du serveur wins (un seul) sur le domaine, géré par nmbd
  wins support = yes
- Le parcours des machines présentes sur le réseau via l'explorateur nécessite la mise en place de master browsers pour le réseau qui vont collecter les noms des machines présentes. Un master browser est élu au démarrage de la machine en fonction de plusieurs paramètres (notamment les versions d'OS). Les “master browsers” s'enregistrent sur le serveur WINS afin de se faire connaître des clients (découverte par broadcast si serveur WINS absent).

Modification du smb.conf (2)

- => Le local master browser collecte la liste des ordinateurs présents sur un domaine de broadcast
  local master = yes : participer aux élections du local master browser
- => Le domain master browser (un seul par domaine) collecte les listes des local master browsers
  domain master = yes : participer aux élections du domain master browser
- Tricher aux élections
  os level = 65 : relève le niveau de l'OS (valeur max = 255)
  preferred master = yes : forcer une élection au démarrage
  (un seul par réseau pour éviter des conflits et des élections récurrentes)
- Finalement, vérification du rôle de Samba
  testparm => Server role: ROLE_DOMAIN_PDC

Les partages du PDC

- Généralement, le PDC offre 3 partages de base :
  - [homes] : homes des utilisateurs
  - [profiles] : profils itinérants
  - [netlogon] : scripts de connexion + NTConfig.POL
- Techniquement, homes et profiles peuvent être déportés sur d'autres serveurs (modification des propriétés des utilisateurs).
- Netlogon, s'il existe, est obligatoirement situé sur le PDC (le chemin du script utilisateur y est relatif)

Les partages du PDC (2)

- [homes] : étendu au nom de l'utilisateur. Un partage est dynamiquement créé lors de son logon sur le domaine.
  => chown utilisateur ; chmod 700
  => Limiter les "valid users" au service (%S)

- [profiles] : informations relatives à la personnalisation de l'environnement de l'utilisateur (fond d'écran...).
  => chown utilisateur ; chmod 700
  => Cf. "profiles acls = yes" pour la compatibilité ACLs - 2000/XP

- [netlogon] : scripts (*.cmd, *.bat) exécutés au logon de l'utilisateur. Ce partage contient aussi le fichier NTConfig.POL qui définit les stratégies utilisateurs.
  => chmod 444 (lecture seule)

Lien au compte utilisateur

- Le compte utilisateur Samba contient les chemins UNC (Uniform Naming Convention, de la forme \\serveur\ressource) des partages, ainsi que la lettre de montage du répertoire home :

```
sambaHomeDrive: U:
sambaLogonScript: utilisateur.bat
sambaProfilePath: \\LINUXPDC\profiles\utilisateur
sambaHomePath: \\LINUXPDC
```

- Netlogon : chemin relatif au PDC

Un partage commun

- Un partage commun peut être défini :

```
[commun]
path = /data/samba/commun
comment = Partage Commun
writeable = yes
browsable = yes
guest ok = no
valid users = @sambausers
create mode = 2774
directory mode = 2774
```

- Il pourra être monté automatiquement au logon de l'utilisateur en spécifiant :

```
@ECHO OFF
@NET USE J: \\LINUXPDC\commun
@ECHO ON
```

dans le script de connexion de l'utilisateur (utilisateur.bat).

La gestion des droits

- Droits de connexion aux partages
- Droits sur le système de fichier : POSIX ou ACLs
- => Les erreurs d'"Accès refusé" proviennent souvent de droits (de partages ou de fichiers) mal positionnés
- Partages personnels : droits pour l'utilisateur uniquement
- Partages communs : gestion par groupes d'utilisateurs ; les ACLs offrent une grande souplesse
- => Des problèmes peuvent survenir avec les ACLs et MsOffice >= 2000. Dans certains cas, les ACLs sont réinitialisées. On utilisera dans ce cas les droits POSIX.
  Cf. : http://support.microsoft.com/default.aspx?scid=kb;EN-US;814112

LINAGORA

Plan (partie3)

- X) La migration depuis NT
- XI) Administrer Samba au quotidien
- XII) Autres outils d'administration
- XIII) S'informer, se documenter
- XIV) Conclusion

LINAGORA

Chapitre X : La migration depuis NT

La migration

- La migration permet de remplacer un PDC ou un BDC par un serveur Samba
- Transparente aux utilisateurs
- Doit offrir les mêmes services que la machine d'origine
- Planifier la migration ; un arrêt de service est à prévoir. Définir les étapes et la stratégie adoptée

Grandes étapes de la migration

- Préparation du serveur NT4 (Comptes)
- Préparation du serveur Samba (BDC - partages)
- Aspiration des comptes (net rpc vampire)
- Copie des fichiers partagés
- Copie des ACLs / droits des fichiers
- Prise de relais du serveur par Samba

Préparation du serveur NT

- Certains comptes peuvent poser problème lors de la migration (Invité, Administrateur...). Il est préférable de les renommer auparavant (cf. outils commerciaux)
- Il faut que Samba soit BDC sur le domaine pour l'aspiration des comptes : lui créer un compte sur le PDC via le gestionnaire de serveurs

Préparation du serveur Samba

- Modifier le fichier smb.conf :

  => Passer Samba en BDC

  os level = 40
  domain logons = yes
  domain master = no
  local master = no

  => Spécification des scripts de gestion des comptes (commandes systèmes ou scripts type smbldap-tools)

  add machine script = [...]
  add user script = [...]
  add group script = [...]
  add user to group script = [...]
  delete user script = [...]
  delete group script = [...]
  delete user from group script = [...]
  set primary group script = [...]

Préparation du serveur Samba (2)

- Joindre le domaine du PDC NT
  => net rpc join -S <serveur> -w <domaine> -U Administrateur
- Forcer le sid local de Samba
  => net getlocalsid <domaine>
  => net setlocalsid <sid local du domaine>
- Créer le compte administrateur (uid 0 - utiliser root)
  => Utilisé notamment pour la jonction d'une machine au domaine
- Créer deux groupes pour l'import des utilisateurs et des machines.
  => Ex. : sambausers (513) : groupe primaire des utilisateurs
  => Ex. : sambamachines (515) : groupe primaire de machines
  => Ajouter les mappings correspondants
- Création à l'identique des partages du PDC sur Samba

Aspiration des comptes

- L'aspiration des comptes va copier tous les comptes d'utilisateurs, de groupes et de machines dans le backend Samba :

=> net rpc vampire -S <serveur> -w <domaine> -U Administrateur

Copie des fichiers

- Utiliser un compte qui a le droit de lecture sur toute l'arborescence à copier

  => smbclient -U Administrateur \
  -c “tar c /export/partage.tar” //SERVEURNT/partage

- Décompresser ensuite les données copiées

  => cd /export && tar xvf partage.tar

Copie des droits

- Pas de méthode “clefs en mains”
- 3 possibilités :
  - Copie des ACLs depuis Samba :
    => Utilisation de smbcacls + scripts (à développer)
  - Copie des fichiers + ACLs depuis le serveur NT
    => Utilisation de scopy ou robocopy (reskits) - Aléatoire
  - Réinitialisation manuelle des droits (-R)
- Paramétrer les droits sur les connexions aux partages dans le fichier smb.conf

Prise de relais par Samba

- Changer le rôle de Samba en celui du serveur NT originel
  Ex. : PDC

  ```
  os level = 65
  domain logons = yes
  domain master = yes
  local master = yes
  ```

- Changer son nom netbios en celui du contrôleur de domaine NT

  ```
  netbios name = SERVEURNT
  ```

- Eteindre le contrôleur NT (pour éviter les conflits avec Samba)
- Démarrer Samba

LINAGORA

Chapitre XI : Administrer Samba au quotidien

Lister les utilisateurs

- En local :
  pdbedit -vL
- Via RPC :
  net rpc user -U root -S <serveur>
  rpcclient -U root -c "enumdomusers" <serveur>
- Au niveau du backend :
  smbldap-tools
  ldapsearch
  gq
  [...]

Ajouter/Supprimer des utilisateurs

- En local :

```
pdbedit -a utilisateur
pdbedit -x utilisateur
smbpasswd -a utilisateur
smbpasswd -x utilisateur
```

- Via RPC :

```
net rpc user add -U root -S <serveur> utilisateur
net rpc user delete -U root -S <serveur> utilisateur
rpcclient -U root -c "createdomuser bbb" <serveur>
rpcclient -U root -c "deletedomuser bbb" <serveur>
```

- Au niveau du backend

Lister les groupes

- En local :
  net groupmap list
- Via RPC :
  net rpc group -U root -S <serveur>
  rpcclient -U root -c "enumdomgroups" <serveur>
- Au niveau du backend

Ajouter/Supprimer des groupes

- En local :

net groupmap add unixgroup=<groupe> sid=<sid>
=> LDAP : Ajoute la partie Samba au groupe POSIX existant
net groupmap delete sid=<sid>
=> LDAP : Supprime tout le groupe si “delete dn = yes” dans le fichier smb.conf

- Via RPC :

net rpc group add -U root -S linuxbdc <groupe>
[net rpc group delete -U root -S linuxbdc <groupe>]

- Au niveau du backend

Envoyer des commandes RPC

- De nombreuses commandes sont disponibles pour l'administration d'un serveur à distance
  => cf. “rpcclient -U root -c "help" <serveur>”
- Démarrer le shell :

  rpcclient -U root <serveur>

- Lister les partages, gérer les utilisateurs, les imprimantes...

Connaître le réseau

- Trouver les hôtes présents sur le réseau :

  findsmb

- Résoudre un nom netbios :

  nmblookup <nom>

- Lister les partages d'un hôte :

  smbclient -L <nom> -U <utilisateur>

Se connecter sur un partage

- Démarrer le shell (ftp-like) :
  smbclient -U <utilisateur> //<serveur>/<partage>

  => Nombreuses commandes disponibles, dont cd, chmod, get, put, tar ...

- Monter un partage localement :
  smbmount //<serveur>/<partage> <dest> \
  -o username=<utilisateur>

  mount -t smbfs -o username=<utilisateur> \
  //<serveur>/<partage> <dest>

Suivre l'activité du serveur

- Afficher des informations sur les utilisateurs connectés et sur les ressources en cours d'utilisation :

  smbstatus

Recharger le fichier smb.conf

- Le fichier est “re-parsé” toutes les minutes
- En cas d'”urgence” : envoi d'un “sigHUP”

```
killall -HUP smbd && killall -HUP nmbd
```

- Dans certains cas, il est nécessaire de redémarrer totalement le serveur Samba :

```
/etc/init.d/samba restart
```

```
killall -15 smbd && killall -15 nmbd && \
sleep 1 && smbd && nmbd
```

Exporter des comptes

- Utilisation de pdbedit pour exporter des comptes vers différents backends (backend source = celui du fichier smb.conf) :

  => Ex. : Export vers le fichier passdb.tdb

  pdbedit -e tdbsam

  => Ex. : Export vers le fichier smbpasswd

  pdbedit -e smbpasswd

Etude des logs

- Deux directives importantes (smb.conf) :

```
log file = /var/log/samba/%m.log
log level = 2
```

- Consulter régulièrement les logs
- En cas de problème, augmenter le log level (de 0 à 10). Ne pas dépasser 3 en production.

LINAGORA

Chapitre XII : Autres outils d'administration

Smbldap-tools

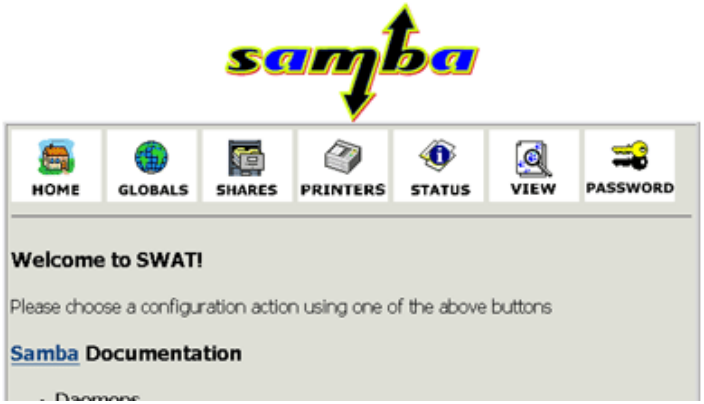
- Permettent de gérer les comptes POSIX + Samba dans un annuaire LDAP en lignes de commandes.

  => smbldap-useradd, smbldap-groupadd, [...]

- Disponibles sur http://samba.idealx.org et dans les sources de Samba

SWAT

- Outil de configuration livré avec la suite Samba
- Fichier smb.conf (global, partages, imprimantes)
  Comptes utilisateurs (Samba)
- Visualisation du statut de Samba
- Attention, peut rapidement mettre la pagaille dans le fichier de configuration, car il écrase le fichier original !



LAM

- Outils PHP (graphique) qui permet de gérer les comptes POSIX + Samba dans un annuaire LDAP. Disponible sur http://lam.sf.net

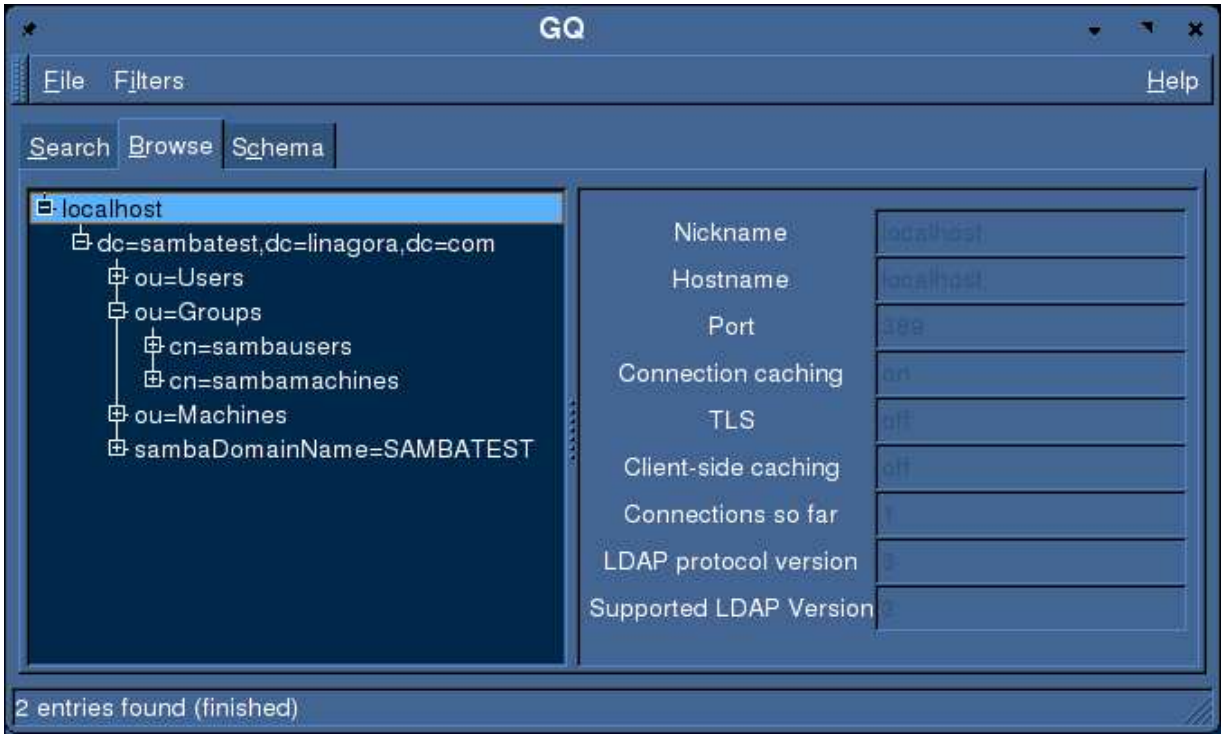
=> Traduction française par Linagora, intégrée au projet à partir de la version 0.4.5

Gosa

- Outil PHP (graphique) permettant de gérer un grand nombre d'attributs sur chaque compte, en plus des attributs POSIX et Samba. Disponible sur https://gosa.gonicus.de

Gq

- Outil d'administration LDAP (GTK) non spécialisé Samba. Permet une gestion fine de tout type d'enregistrement. Disponible sur http://biot.com/gq



LINAGORA

Chapitre XIII : S'informer, se documenter

Liens

- Le site de Samba : http://www.samba.org
- Penser aux pages de man !
- Le document “Samba Howto Collection” (http://de.samba.org/samba/docs/Samba-HOWTO-Collection.pdf)
- Le répertoire docs/ des sources (cf. sources Samba 2.2.8a)
- Dernière version de ce document et diverses contributions sur http://contribs.martymac.com

Listes de diffusion

- Officielles (en) :
  samba@lists.samba.org
  samba-technical@lists.samba.org
  http://lists.samba.org/mailman

- Française :
  samba-fr@ujf-grenoble.fr
  http://listes.ujf-grenoble.fr/wws/info/samba-fr

LINAGORA

Chapitre XIV : Conclusion

- X) La migration depuis NT
- XI) Administrer Samba au quotidien
- XII) Autres outils d'administration
- XIII) S'informer, se documenter
- XIV) Conclusion

LINAGORA

Conclusion

- Merci de votre attention !

LINAGORA

GNU Free Documentation License