Samba

Didier Depoisier
Jean-Luc Parouty
Institut de Biologie Structurale (IBS)

25 mai 2010

Institut de Biologie Structurale
41, rue Jules Horowitz
38027 Grenoble Cedex 1 France

Équipe
Informatique

1 / Expression des besoins

Institut de Biologie Structurale
41, rue Jules Horowitz
38027 Grenoble Cedex 1 France

Équipe
Informatique

Contexte

Unité mixte de recherche, de taille moyenne :

- 200-500 personnes
- Tutelles multiples
- Usages et population très hétérogène
- Organisation complexe (groupes, équipes, projets, …)
- Forte autonomie des usagers vis à vis de leur poste de travail...

Mais Samba/LDAP est une solution réputée robuste et efficace au sein d'organisations importantes (>10000).

Expression des besoins

Intégrer l'ensemble des services du SI :

- Messagerie
- Stockage
- Outils collaboratifs et Web (Spip, Plone, ...)
- Authentification des postes de travail*
- ...

Dans un environnement :

- Hétérogène (Windows, Linux, MacOS)
- Fortement évolutif
- Ouvert
- Disposant de ressources limitées**

(*) Des utilisateurs sur les postes de travail
(**) Ressources limitées en moyens humain et budgétaire

Expression des besoins

Du point de vue de l'utilisateur : *Simple is beautifull !*

- Un seul login, un seul mot de passe, pour l'ensemble des services
- Un seul espace de stockage* pour l'ensemble des architectures

Du point de vue de l'administrateur :

- Un seul référentiel, une seule solution (urbanisée)...
- Standard et évolutif
- Simple, robuste (haute disponibilité...)

Du point de vue du décideur :

- Économique (réalisation, exploitation)
- Pérenne (vis a vis des moyens de l'organisation)

(*) Avec séparation des espaces personnels, scientifiques et de partage

Autrement dit,

Comment :

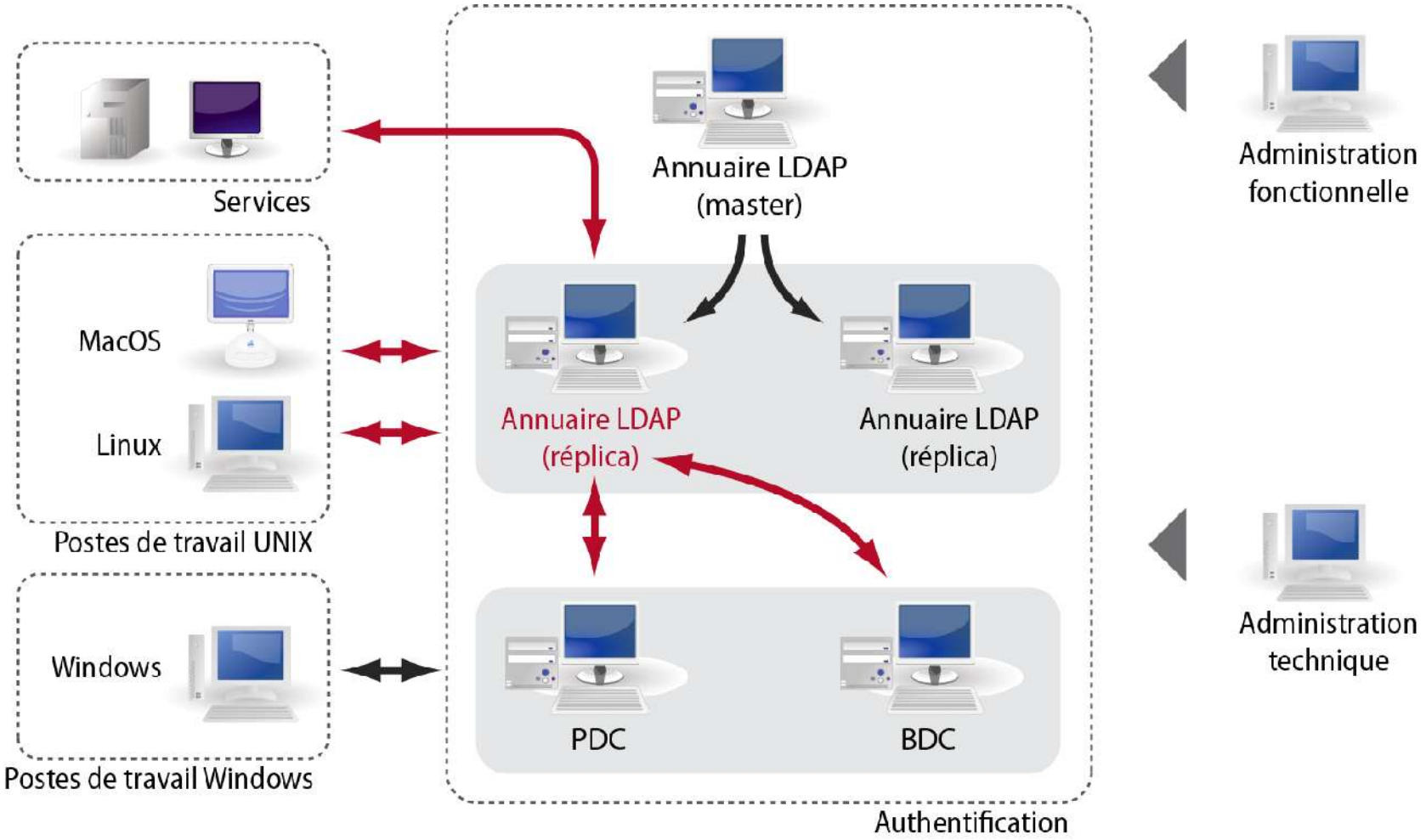
- Avoir un même référentiel d'authentification pour l'ensemble des services ?
- Partager des espaces de stockage vers l'ensemble des architectures (Windows, MacOS et Linux) ?
- ...et faire en sorte que ça ne coûte pas (trop) chers et que ça marche (presque) tout seul ;-)

2/ Architecture de type Samba-LDAP

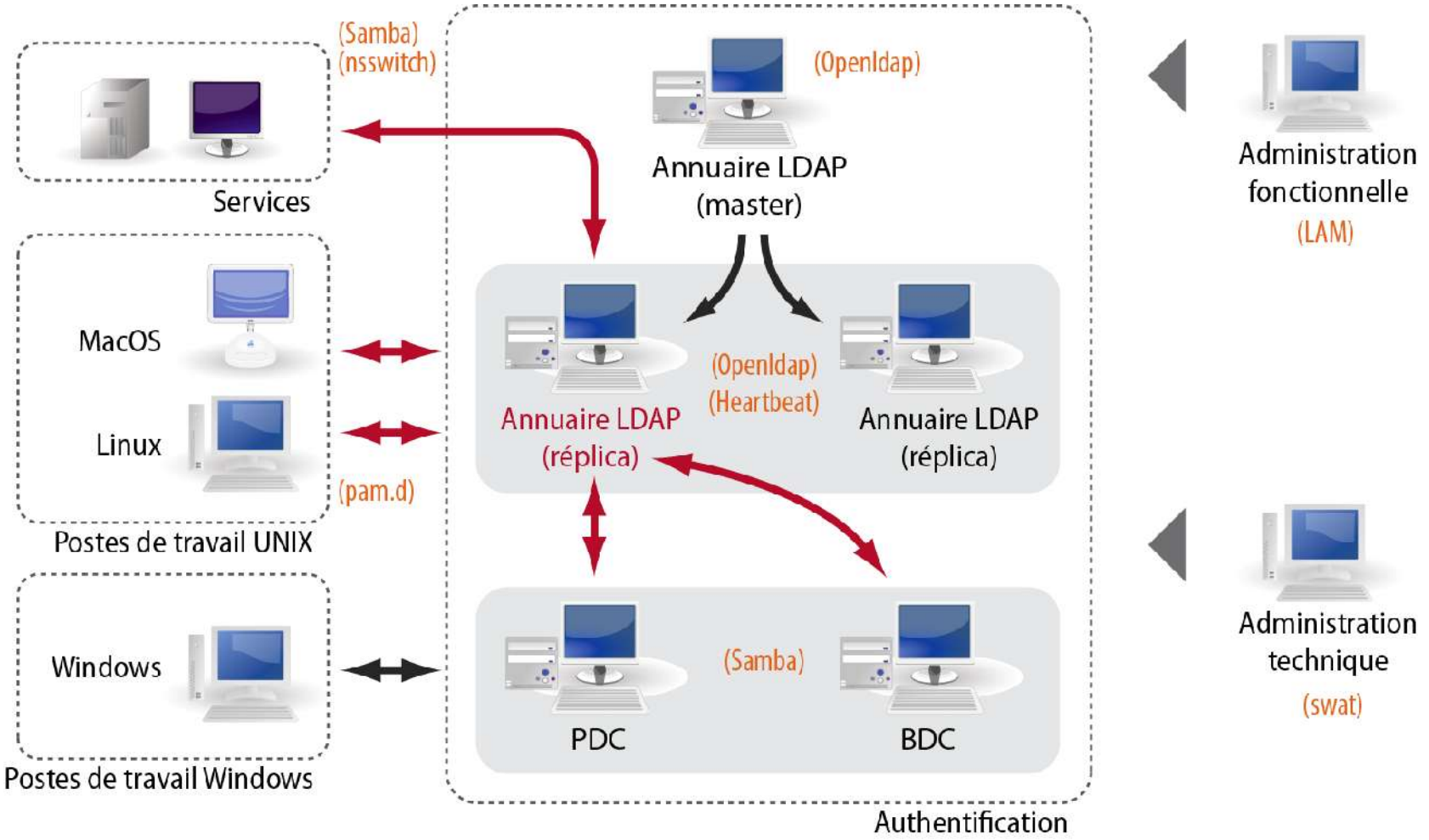
Institut de Biologie Structurale
41, rue Jules Horowitz
38027 Grenoble Cedex 1 France

Équipe
Informatique

Architecture



Architecture



A propos de Samba...

Objectifs :

- Partage de fichiers (et d'imprimantes)
- Gestionnaire de domaine (NT4)
- Explorateur réseau

Historique :

- 1992 : projet initié par Andrew Tridgell
- 2001 : version 2.0
- 2003 : version 3.0
- Mai 2010 : version 3.5.3 et 4.0.0alpha11

Licence :

- GPLv2

Site de référence :

- http://www.samba.org

A propos de Samba...

Un domaine NT4 permet de gérer :

- Des entités :
  - Utilisateurs
  - Groupes
  - Machines
- Des ressources :
  - Partage de fichiers
  - Imprimantes
- Des droits entre ces entités et ces ressources

A propos de Samba...

Samba est composé :

- De 3 démons
  - Smbd : Partage de fichiers
  - Nmbd : Gestion de la couche netbios, WINS et explorateur
  - ~~Winbind~~ : Interaction Linux/contrôleur de domaine
- D'un backend
  - Idéalement LDAP
- D'un fichier de configuration
  - `/etc/samba/smb.conf`
- D'une interface graphique : swat
- De commandes
  - `net, smbpasswd, smbstatus, smbmount, smbclient, etc.`

3/ Mise en œuvre Samba-LDAP

Samba 3 et OpenLDAP en 4 étapes...

Institut de Biologie Structurale
41, rue Jules Horowitz
38027 Grenoble Cedex 1 France

Équipe
Informatique

Etape 1 : LDAP (OpenLDAP)

Quelques spécificités liées à Samba :

- Intégrer le schéma des *SambaSamAccount :*
  `include /(...)/schema/samba.schema`
- Installer une interface d'administration pour gérer les entrées de l'annuaire : par exemple, LAM
- Créer les différentes branches :
  - Pour les personnes :
    `inetOrgPerson, posixAccount, sambaSamAccount`
  - Pour les groupes :
    `posixGroup, sambaGroupMapping`
  - Pour les machines :
    `posixAccount, sambaSamAccount`
  - Pour les domaines
    `sambaDomain`

Etape 1 : LDAP (OpenLDAP)

```
# ------ Schemas utilisés
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/inetorgperson.schema
include         /etc/ldap/schema/samba.schema

# ------ Racine
suffix          "dc=abc,dc=fr"

# ------ Administrateur LDAP
rootdn          "cn=root,dc=abc,dc=fr"
rootpw          {MD5}iuYJHGyhggGHJhggHHGJGg==

# ------ Quelques index
index   objectclass,uidNumber,gidNumber                 eq
index   cn,sn,uid,displayName                           pres,sub,eq
index   memberUid,mail,givenname                        eq,subinitial
index   sambaSID,sambaPrimaryGroupSID,sambaDomainName   eq

# ------ Quelques ACL
access to attrs=userPassword,sambaLMPassword,sambaNTPassword,shadowLastChange
        by anonymous auth
        by self write
        by * none

access to attrs=street,telephoneNumber,sn,givenName,mail
        by self write
        by group.exact="cn=secretaire,ou=otherGroups,dc=abc,dc=fr" write
        by * read

access to attrs=givenName,gecos,description,sn,employeeType,postalAddress,postalAddress,
title,roomNumber,businessCategory,employeeNumber
        by group.exact="cn=secretaire,ou=otherGroups,dc=abc,dc=fr" write
        by * read
```

Glanés dans /etc/slapd.conf

Note : Il existe 2 types de groupes : posixGroup et groupOfNames

Etape 2 : Configuration des serveurs hôtes

Les systèmes hébergeant les serveurs Samba ont besoin de connaître les utilisateurs et les groupes (dualité des comptes et des groupes)

- Configuration de nsswitch :

  ```
  /etc/nsswitch.conf
  /etc/libnss-ldap.conf
  ```

- Activation du cache nscd :

  ```
  /etc/init.d/nscd start
  ```

- Vérification :

  ```
  # getent passwd
  # getent groups
  ```

Etape 2 : Configuration des serveurs hôtes

```
# Dans /etc/nsswitch.conf

(…)
passwd:         compat  ldap
group:          compat  ldap
(…)

# Dans /etc/libnss-ldap.conf

(…)
base dc=abc,dc=fr
uri ldap://authentification.abc.fr
ldap_version 3
(…)

# Dans /etc/nscd.conf

…pas grand chose à changer…!

# Service nscd
# /etc/init.d/ncsd start                # Demarrage du service
# /etc/init.d/nscd stop                 # Arrêt du service
# /usr/sbin/nscd --invalidate <map>     # Pour effacer une table du cache
# /getent <map>                         # Pour afficher une map (test)
```

Etape 3 : Configuration de Samba

3.1/ Comme contrôleur de domaine :

- Dans /etc/samba/smb.conf :

```
[global]
    workgroup = ABC-DOMAIN
    logon script = \scripts\%U-xp.bat
    logon path =
    logon home =
    domain logons = Yes
    os level = 65
    preferred master = Yes
    domain master = Yes
    wins support = Yes
    (…)
[netlogon]
    path = /var/data/netlogon
    browsable = No
    root preexec = /etc/samba/script/…
    (…)
```

Étape 3 : Configuration de Samba

3.2/ Pour « s'accrocher » à l'annuaire LDAP :

- Dans /etc/samba/smb.conf :

```
[global]
    (…)
    ldap admin dn = uid=admin,dc=abc,dc=fr
    ldap suffix = dc=abc,dc=fr
    ldap user    suffix = ou=people
    ldap group   suffix = ou=groups
    ldap machine suffix = ou=machines
    ldap passwd sync = Yes
    ldap ssl = no
    (…)
```

- Ne pas oublier de donner à samba le mot de passe administrateur de l'annuaire :

```
# smbpasswd -w
```

Étape 4 : Gestion des personnes et des machines

Utiliser une interface graphique (!)

- Par exemple : LDAP Account Manager (LAM)

NOTE : A ne pas oublier dans l'annuaire :

- Créer le domaine dans l'annuaire
  - Récupérer le SID du domaine :
    ```
    # net getdomainsid
    ```
  - Créer une entrée dans l'annuaire, avec ce SID
- Créer des administrateurs
  - UNIX : uid=0
  - Windows : groupe des administrateurs

Ces petites choses qui facilitent la vie..

Pour se simplifier la vie :

- Eviter les profiles itinérants (quand on peut !)
- Laisser les imprimantes à CUPS et IPP !
- Scripts de démarrage, cotés client :

```
logon script
```

- Scripts automatiques :

```
add machine script (G)
add user script (G)
root preexec (S)
root preexec close (S)
root postexec (S)
...
```

Ces petites choses qui facilitent la vie..

```
# Par exemple, dans /etc/smb.conf


[global]
    (…)
    logon script = \scripts\%U-xp.bat

[netlogon]
    root preexec = /etc/samba/scripts/createLogon.pl
     -user="%U" -group="%G"
     -client="%M" -arch="XP"

[homes]
    (…)
    root preexec = /etc/samba/scripts/createDir  "%U"
```

4/ Et Seven, dans tout ça ?

Institut de Biologie Structurale
41, rue Jules Horowitz
38027 Grenoble Cedex 1 France

Équipe
Informatique

....et bien ça marche !

Trois petites choses nécessaires :

- Utiliser un Samba récent (à partir de 3.3.7)
- Activer la compatibilité...
  ...en modifiant 2 valeurs de la base de registre :

```
HKLM\System\CCS\Services\LanmanWorkstation\Parameters
            DWORD  DomainCompatibilityMode = 1
            DWORD  DNSNameResolutionRequired = 0
```

  ...et relancer le service *LanmanWorkstation* (ou en redémarrant...)
- Joindre le domaine !
  ...sans s'inquiéter du warning lié à une non résolution DNS du domaine ;-)

cf : http://wiki.samba.org/index.php/Windows7

Note : Un Seven ne sait pas joindre un « authentique » domaine NT4 Windows (dixit Microsoft)

...des problèmes ?

Avec Seven, par défaut, l'administrateur du domaine n'est pas autorisé à ouvrir une session...

Solution :

- Modifier le niveau de sécurité de l'UAC (User Account Control) :

  Panneau de configuration /
  Système et sécurité /
  Centre de maintenance /
  - Modifier les paramètres de contrôle de compte d'utilisateur et baisser la jauge sur le niveau le plus bas "Ne jamais m'avertir"...
  - Redémarrer l'ordinateur

That's all folks !

5/ Et Samba 4, dans tout ça ?

Institut de Biologie Structurale
41, rue Jules Horowitz
38027 Grenoble Cedex 1 France

Équipe
Informatique

Et Samba 4 ?

Samba 4 :

- Réécriture complète de la couche CIFS / AD
- Documentation perfectible (mais on en trouve)
- Intégration DNS / NTP

Nous avons testé pour vous :

- Installation avec le *backend* par défaut : ok
- Intégration de XP, Seven : ok
- Gestion de comptes : ok (a priori)
- GPO : ok (a priori)

Ce qui reste « difficile » :

- Un *Backend* OpenLDAP reste « difficile » a mettre en œuvre..

6/ Et donc... ...on fait quoi ?

Institut de Biologie Structurale
41, rue Jules Horowitz
38027 Grenoble Cedex 1 France

Équipe
Informatique

Conclusion (du moment)

Pourquoi faire compliqué quand on peut faire simple ?

- Samba-LDAP va très bien
- Simple : 2 ou 3 jours suffisent pour démarrer une maquette...
- Efficace : Samba et LDAP répondent à la plupart des besoins
- Robuste : HD en quasi-natif...

Dans tous les cas, ces projets restent lourd et complexes à mettre en œuvre (impact global sur le SI)...

...L'avenir : Samba 4 :-)