

**Maquette et mise en place  
d'un annuaire LDAP à l'IMB**

**Rencontres mathrice  
Lyon, 25-27 mars 2003**

## **Plan :**

- Les besoins
- Les moyens
- Les choix
- La maquette
- Le déploiement
- Les problèmes
- Conclusions

## **Les besoins**

L'IMB = Une fédération de recherche et 3 laboratoires :

Annuaire :

- de l'ordre de 300 individus (permanents, étudiants, invités...)
- 5 secrétariats (institut, labos, école doctorale)
- une connaissance des mouvements de personnel approximative

Authentification :

- 4 domaines NIS
- 4 manières de gérer les mouvements
- Mise en commun du travail à travers la cellule

## **Les moyens**

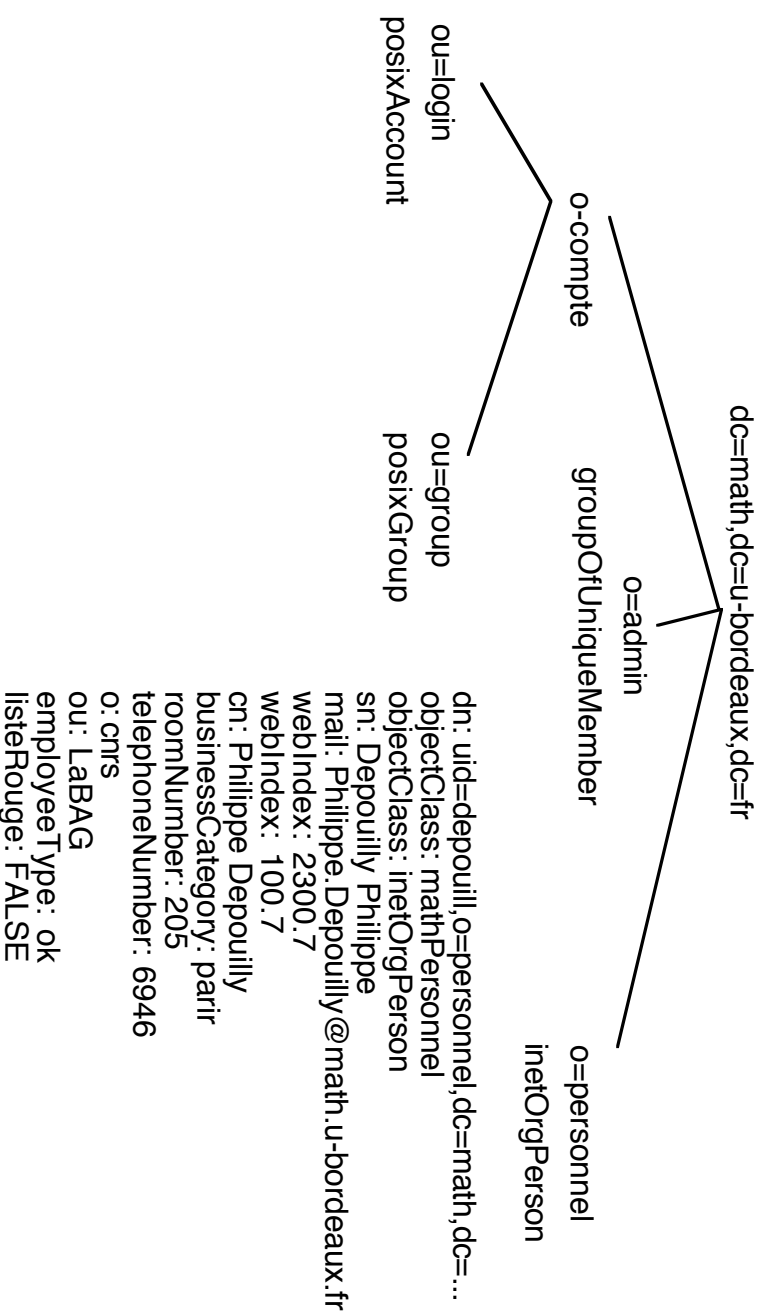
Une première maquette montée par une vacataire :

- beaucoup de littérature
- réflexion sur la structure d'annuaire
- validation, faisabilité
- réflexion sur les technologies
- transfert de compétences

## **Les choix (1)**

- Deux branches  
dc=math,dc=u-bordeaux,dc=fr -> o-compte et  
o=personnel
- Schémas standards  
(posixAccount, posixGroup, inetOrgPerson)  
-> quelques attributs supplémentaire pour personnel
- OpenLDAP 2.1.x :  
avec Berkeley (ldbm), TLS, réplicas, PAM, auth-ldap
- Administration via PHP avec différents niveaux

## Les choix (2)



## Les choix (3)

o-compte

ou=login

posixAccount

dn: uid=depouill,ou=login,...  
objectClass: posixAccount

ou=groupes

posixGroup

dn: cn=mpb,ou=groupes,o=compte,...  
objectClass: posixGroup  
objectClass: top

cn: mpb  
gidNumber: 7000  
uniqueMember: 7000

uid: depouill

**userPassword**

uidNumber: 7000

gidNumber: 7000

gecos: Philippe Depouilly

oginShell: /bin/bash

homeDirectory: /home/mpb/depouill

pwdLastSet: 1036602232

logonTime: 2147483647

logoffTime: 2147483647

kickoffTime: 2147483647

pwdCanChange: 2147483647

pwdMustChange: 2147483647

rid: 15000

primaryGroupID: 15001

acctFlags: [U]

**lmPassword, ntPassword**

## Les choix (4)

SLAPD.CONF :

```
include /etc/openldap/schema/core.schema
include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/nis.schema
include /etc/openldap/schema/samba.schema
include /etc/openldap/schema/new.schema

# Define global ACLs to disable default read access.
TLSCertificateFile /usr/share/ssl/certs/server.pem
TLSCertificateKeyFile /usr/share/ssl/certs/server.pem
TLSCACertificateFile /usr/share/ssl/certs/server.pem
..
rootpw {crypt}aaczX2rr2Hlpo
index objectClass,uid,uidNumber,gidNumber,memberUid eq
index cn,mail,surname,givenname eq,subinitial

replica host=test.math.u-bordeaux.fr:389
binddn="uid=Manager.math.u-bordeaux.fr"
bindmethod=simple
```



## Les choix (5)

SLAPD.CONF :

```
...  
access to attr=userPassword  
by anonymous auth  
by self write  
by group/groupOfUniqueNames="cn=igs,o=admin,dc=..." write  
by * none  
  
access to attrs=lmPassword,ntPassword  
by dn="cn=Manager,dc=math,dc=u-bordeaux,dc=fr" write  
by * none  
  
access to dn="*,dc=math,dc=u-bordeaux,dc=fr"  
by group/groupOfUnique..."="cn=igs,o=admin,dc=math,dc=..." write  
  
etc...
```

## Les choix (6)

LDAP.CONF :

```
host LDAP.math.u-bordeaux.fr
base dc=math,dc=u-bordeaux,dc=fr
ldap_version 3
pam_password md5
ssl_start_tls
tls_cacertfile /usr/share/ssl/certs/ldap.pem
```

SMB.CONF :

```
ldap admin dn = "cn=Manager,dc=math,dc=u-bordeaux,dc=fr"
ldap server = LDAP.math.u-bordeaux.fr
ldap ssl = start_tls
ldap suffix = "ou=login,o=compte,dc=math,dc=u-bordeaux,dc=fr"
ldap filter = "&(uid=%u)(objectclass=posixAccount)"
```

PROFTPD.CONF :

```
LDAPHomeDirOnDemandPrefix "/math/www/public_html"
```

## **Maquette**

- OpenLDAP 2.0.5
  - Scripts de migration NIS de padl.com
  - GnuDB
  - Test de réplication
  - Tests d'authentification (apache, samba, pam, proftpd)
  - Première interface PHP
- > premières conclusions (2.0 vs 2.1, base, stabilité, arborescence définitive, etc.)

## **Déploiement (1)**

-> Il est encore à faire à grande échelle

Ce qui est fait :

- Openldap 2.1.5 (passage vers 2.1.12 prévu)
- Utilisation exclusive de TLS
- Authentification via samba, proftpd et pam sur le serveur principal
- Interface PHP pour l'administration
- Intégration dans les pages webs des labos

## **Déploiement (2)**

-> Il est encore à faire à grande échelle

A faire :

- Authentification des clients (remplacement des NIS) avec la gestion des groupes pour gérer les autorisation locales
- Déploiement des réplicas
- Formation des administrateurs
- Mise en place d'une solution de replis

## **Les problèmes**

- 2.0.x peu stable avec des incohérences
- Compréhension des ACLs (écriture rigoureuse)
- PHP 4.2 au moins
- Compréhension de PAM pour plus de sécurité
- Stratégie de l'arborescence : LDAP != SGBD (pas de jointure, etc.)
- Authentification samba nécessite pam (compte unix valide)

## **Conclusions**

- Réponse satisfaisante aux besoins : meilleure administration des comptes, des mouvements, sécurisation de l'authentification
- Il a été sage d'attendre la 2.1 pour se lancer
- Ne pas se lancer dans des mécanismes plus lourds (kerberos, SASL)
- Élégance de la solution (séparation des branches, mécanisme de gestion de groupes, possibilité de cacher des attributs)