UMR 6086
B. Métrot

Service d'annuaire OpenLDAP

Benoit Métrot
benoit.metrot@math.univ-poitiers.fr

UMR 6086 - Laboratoire de Mathématiques et Applications (Poitiers)

Journée Josy/Plume - 22 novembre 2010
Les outils libres de base utiles à tout ASR

UMR 6086
B. Métrot

Plan

UMR 6086
B. Métrot

Progression

Présentation du laboratoire

- UMR 6086 : Laboratoire de Mathématiques et Applications (Poitiers)
- Thèmes de recherche :
  - Algèbre Effective, Analyse Complexe et Théorie de Lie
  - Equations aux Dérivées Partielles et Applications
  - Probabilités et Statistique
- Effectifs :
  - 49 permanents
  - 25 doctorants et ATER
- Parc informatique :
  - 9 serveurs (+ 16 machines virtuelles)
  - 75 postes clients (dont 15 portables)
  - 90% sous GNU/Linux

Objectifs

- Référentiel unique des informations pour l'identification
- Source unifiée pour l'authentification
  - Ouverture de session
  - Courrier électronique (IMAPs/POPs/Webmail)
  - Intranet
  - Consultation des revues électroniques
- Interopérabilité avec des systèmes Windows

Pourquoi OpenLDAP ?

- Intégré et distribué dans toutes les bonnes distributions
- Logiciel libre largement utilisé
- Bonne documentation
- Implémentation du protocole normalisé d'annuaire LDAP

UMR 6086
B. Métrot

Progression

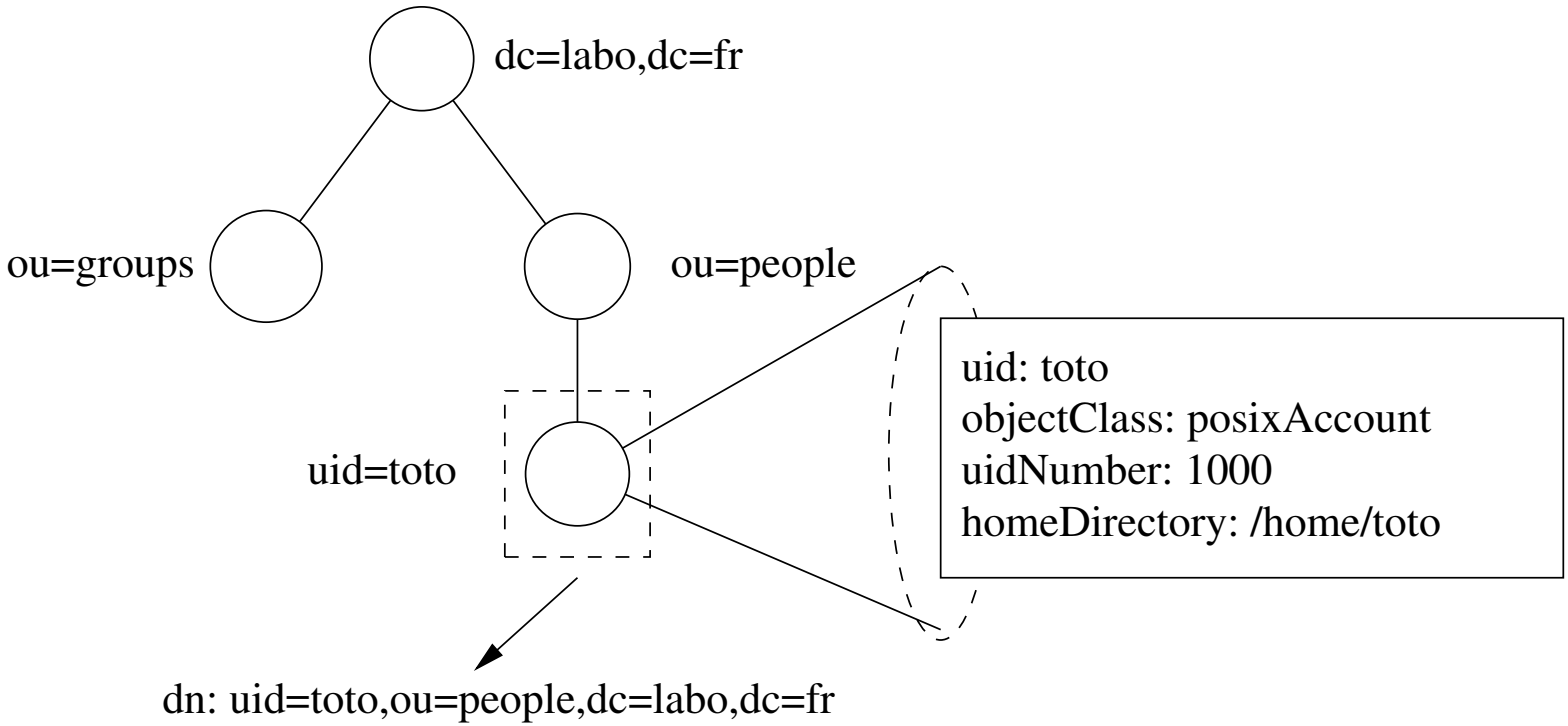
UMR 6086
B. Métrot

Protocole LDAP

- Lightweight Directory Access Protocol
  - Service d'annuaire $\neq$ base de données
  - Architecture client/serveur
- Les modèles LDAP :
  - Le modèle d'information
  - Le modèle de nommage
  - Le modèle fonctionnel
  - Le modèle de sécurité

UMR 6086
B. Métrot

Exemple d'arbre LDAP



UMR 6086
B. Métrot

Ce que fournit OpenLDAP

- Le serveur *slapd*
- Extension du protocole LDAP par les *overlays* (réplication, contraintes, groupes dynamiques)
- Une bibliothèque partagée (support de SSL)
- Des outils de recherche et modification
  - *ldapsearch*
  - *ldapadd*, *ldapdelete*, *ldapdelete*
  - *slapadd*, *slapcat*
- De la documentation

Le *Backend* de stockage est indépendant.

UMR 6086
B. Métrot

Ce que fournit OpenLDAP

- Le serveur *slapd*
- Extension du protocole LDAP par les *overlays* (réplication, contraintes, groupes dynamiques)
- Une bibliothèque partagée (support de SSL)
- Des outils de recherche et modification
  - *ldapsearch*
  - *ldapadd*, *ldapdelete*, *ldapdelete*
  - *slapadd*, *slapcat*
- De la documentation

Le *Backend* de stockage est indépendant.

UMR 6086
B. Métrot

Progression

Partie serveur

- Un serveur principal
  - Une machine virtuelle avec slapd et le backend bdb
  - Maitre des données
  - Réplication via l'overlay *syncprov*
  - Sécurisation des communications par SSL et certificats de l'IGC du CNRS
- Un serveur secondaire
  - Une machine virtuelle avec slapd et le bachend bdb
  - Reçoit les modifications du serveur principal (overlay syncrepl)
  - N'accepte aucune modification des données par les clients

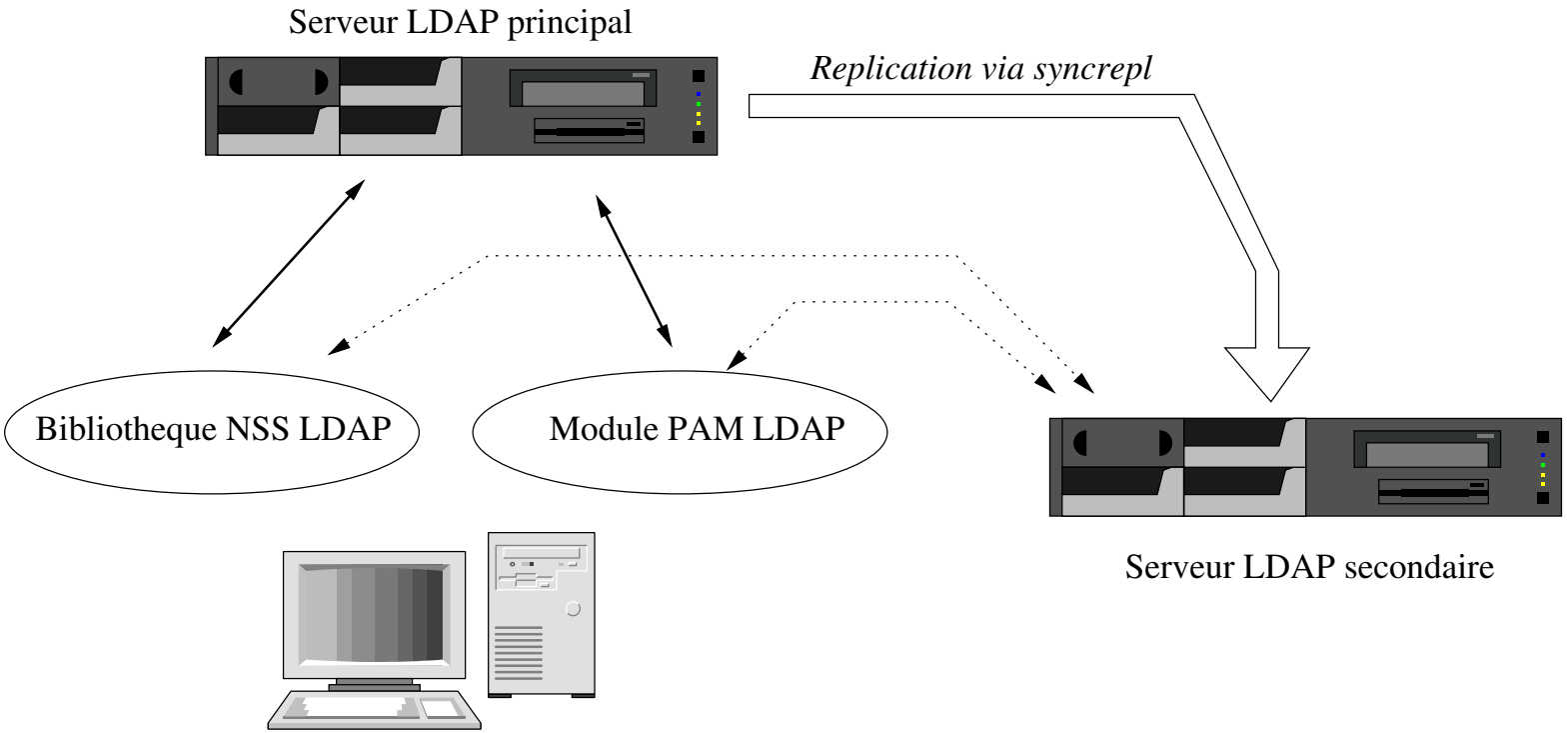
UMR 6086
B. Métrot

Partie cliente

- Identication des utilisateurs par la bibliothèque NSS LDAP
- Authentification avec le module PAM LDAP
- Si le maitre ne répond pas, interrogation du serveur secondaire

UMR 6086
B. Métrot

Architecture



Retour d'expérience

Points forts :

- Manipulation des données au format LDIF (texte)
- Sauvegarde très facile
- Reprise sur panne rapide
- Extensibilité du schéma d'annuaire
- Interactions multiples (Outils graphiques, Perl, Python)

Quelques limites :

- Interopérable avec Windows mais pas directement
- Absence de cache intégré coté client
- Pas de répartition de charge

UMR 6086
B. Métrot

Progression

UMR 6086
B. Métrot

Bilan

- OpenLDAP ne fait plus l'authentification au LMA, délégation du service à Kerberos
- Très bon service d'annuaire
- Minimiser la redondance d'information (facilité de mise à jour)
- Préférer une arborescence simple et peu profonde en suivant les recommandations SUPANN du CRU