LDAP
Lightweight Directory Access Protocol

Sylvain Pernot
Sébastien Laruée
Florent Juillet de Saint-Lager

IR3 Groupe 1
Exposé Nouvelles Technologies Réseaux

Ingénieurs 2000, Université de Marne la vallée

Plan de l'exposé

- Les Annuaires électroniques
- Le protocole LDAP
- LDAP en pratique
- Synthèse de la Technologie

Annuaires : ***Définition***

- Un catalogue de données organisées dédié à la lecture, plus qu'à l'écriture

- Exemples de la vie courante
  - Annuaires papiers
    - annuaire téléphonique
    - carnet d'adresses
    - catalogue de vente
  - Annuaire électronique
    - DNS
    - WHOIS
    - Base de Registre Windows

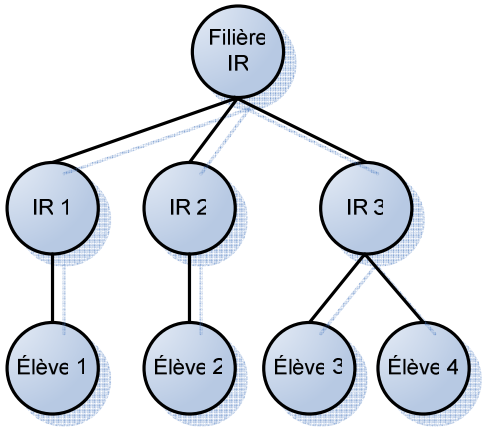
Annuaires : ***Concepts***

- ***Dynamiques*** (mise à jour en temps réels)
- ***Souples*** (changement aisé type et organisation des données)
- ***Sécurisés*** (qui voit quoi)
- ***Personnalisés*** (façon de présenter les données, action sur ses propres données,...)

Annuaires : ***Caractéristiques (1)***

- Conçu pour avoir beaucoup de requêtes en lecture, peu en écriture

- Structurations des données



Organisation Hiérarchique

1	Élève 1	1
2	Élève 2	2
3	Élève 3	3
4	Élève 4	3

IR 1	1
IR 2	2
IR3	3

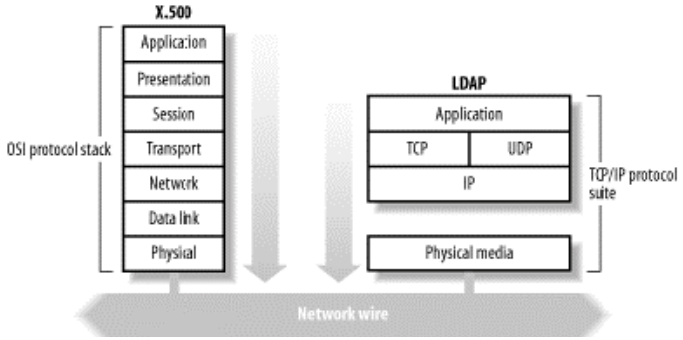
Organisation Relationnelle

Annuaires : ***Caractéristiques (2)***

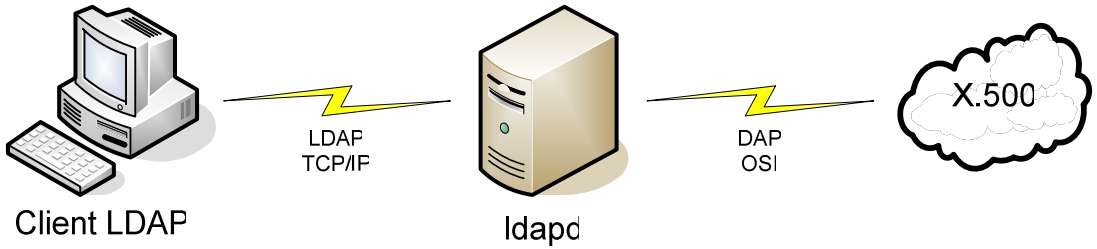
- Pas de requêtes compliquées (comme les jointures en SQL),
- Les annuaires doivent pouvoir être répartis,
- Un annuaire doit être capable de gérer l'authentification des utilisateurs

protocole LDAP : ***Présentations (1)***

- Le précurseur de LDAP : X.500
- Naissance de LDAP
  - Alléger le protocole DAP

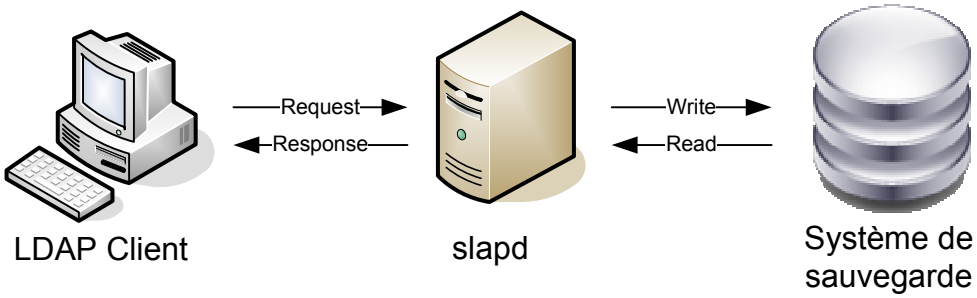


  - Une passerelle LDAP/X.500



protocole LDAP : ***Présentations (2)***

- LDAP natif



- LDAP *version 3*
  - *prise en compte des caractères spéciaux,*
  - *Le mécanisme de chaînage des requêtes,*
  - *Sécurité : l'authentification SASL et chiffrement TLS (Transport Layer Security),*
  - *Surcharge des opérations.*

Les modèles de LDAP

- 5 modèles:
  - Modèle d'information
  - Modèle de nommage
  - Modèle fonctionnel
  - Modèle de sécurité
  - Modèle de réplication

Modèle ***d'information***

- Entrée = Objet
- Une entrée contient un ensemble d'attributs (utilisateurs ou opérationnels)
- Classe d'objet: définit les attributs que doit contenir un objet
  - Classe abstraite, structurelle ou auxiliaire
  - On peut faire de l'héritage!!!
- Le schéma de l'annuaire contient les classes d'objets
- Le schéma de l'annuaire permet de vérifier le respect de la syntaxe des données

Modèle ***de nommage***

- Contraintes de nommage pour garantir l'interopérabilité entre annuaires
- DIT (directory information tree) : définit l'organisation et la désignation des données
- Chaque entrée est identifiée de manière unique par :
  - Relative Distinguished Name
  - Distinguished Name

Modèle ***fonctionnel***

- Le modèle fonctionnel décrit la manière d'accéder aux données
- Fonctions d'interrogation: search, compare
  - Paramètres: base object, scope, derefAliases, size limit, time limit, attrOnly, search filter
- Fonctions de mise à jour: add, modify, delete, rename
- Fonctions de session: bind, unbind

Modèle ***de sécurité***

- Définir pour chaque utilisateur des droits d'accès aux données (authentification, liste de contrôle d'accès)
- Garantir la confidentialité des échanges (chiffrement)

Modèle ***de réplication***

- Dupliquer un annuaire sur plusieurs serveurs
- Prévenir les coupures réseau, les surcharges de service ou les pannes de serveur
- Structure maître-esclave
- Synchronisation totale/incrémentale
- Réplication en temps réel/à heure fixe

Communication client-serveur

- Mécanisme de questions-réponses sous forme de messages
- Traitement synchrone ou asynchrone
- Cas asynchrone: attribution d'un numéro de contexte

Implémentation de LDAP

- OpenLDAP
  - Présentation
  - Configuration
  - Exemple de création d'un annuaire
  - Avantages et Inconvénients
- Exemple d'implémentation
  - Authentification sous Linux en réseau

Configuration de OpenLDAP

- Le fichier slapd.conf
  - Schémas : `include /etc/openldap/schema/nis.schema`
  - Accès : `access to * by * read`
  - Base de données : `database bdb`
  - Domaines de nom : `suffix`
  - Compte d'administration : `rootdn` et `rootpw`

- Le fichier ldap.conf
  - Configuration cliente : `BASE` ***et*** `URI`

Utilisation de OpenLDAP

- Commandes client principales
  - `ldapadd` équivalent à `ldapmodify -a`
  - `ldapdelete`
  - `ldapsearch`
  - `ldapcompare`
  - `ldapmodify`
  - `ldappasswd`
  - `Ldapmodrdn`
- Le format LDIF : Import et export de données

OpenLDAP : **Création de l'arbre des données**

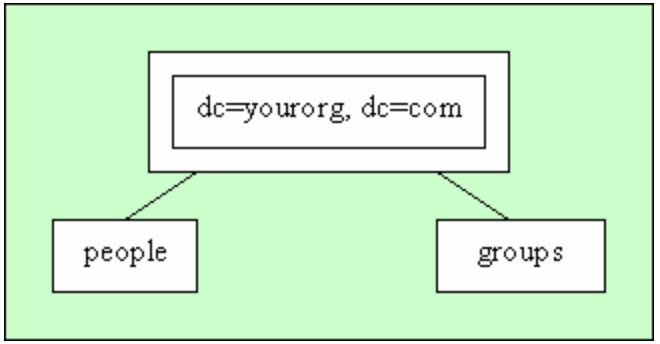
ldapadd -D «cn=Manager,dc=yourorg,dc=com» -w -f create_main_tree.ldif

```
dn:dc=yourorg, dc=com
objectclass: top
objectclass: organizationalUnit

dn:ou=groups, dc=yourorg, dc=com
objectclass: top
objectclass: organizationalUnit
ou: groups

dn:ou=people, dc=yourorg, dc=com
objectclass: top
objectclass: organizationalUnit
ou: people
```

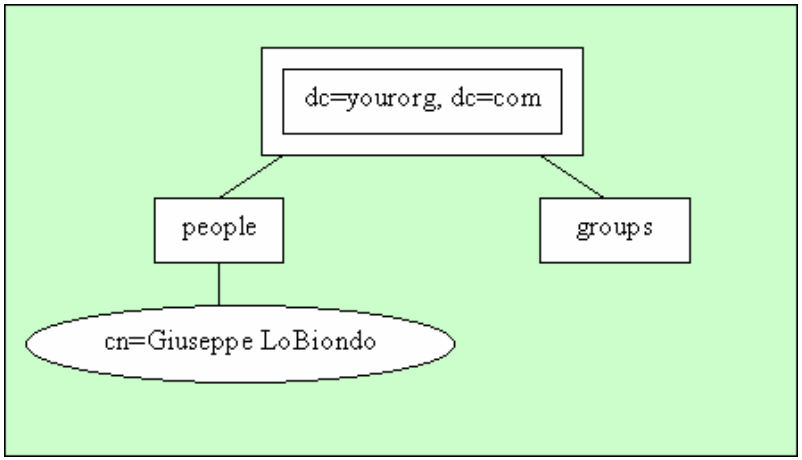
create_main_tree.ldif



OpenLDAP : **Ajout de données**

ldapadd -D «cn=Manager,dc=yourorg,dc=com» -w -f create_user.ldif

```
dn: cn=Giuseppe LoBiondo, ou=people, dc=yourorg, dc=com
cn: Giuseppe Lo Biondo
sn: Lo Biondo
objectclass: top
objectclass: person
objectclass: posixAccount
objectclass: shadowAccount
uid:giuseppe
userpassword:{crypt}$1$ss2ii(0$gbs*do&@=)eksd
uidnumber:104
gidnumber:100
gecos:Giuseppe Lo Biondo
loginShell:/bin/zsh
homeDirectory: /home/giuseppe
shadowLastChange:10877
shadowMin: 0
shadowMax: 999999
shadowWarning: 7
shadowInactive: -1
shadowExpire: -1
shadowFlag: 0
```



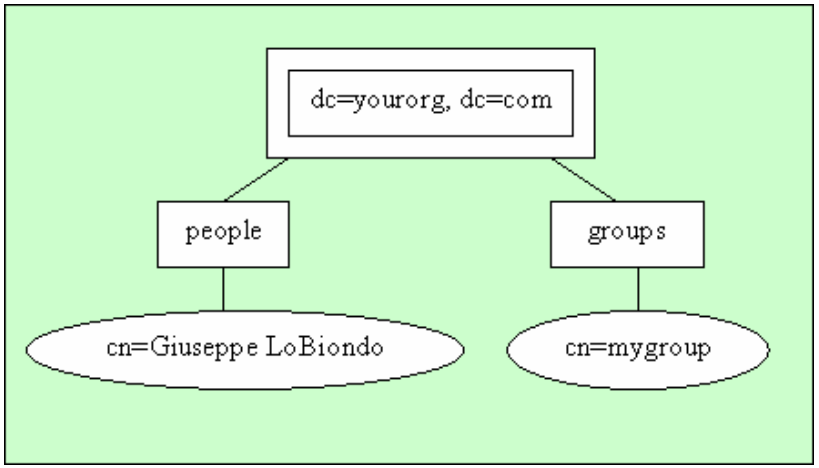
create_user.ldif

OpenLDAP : **Ajout de données**

```
ldapadd -D «cn=Manager,dc=yourorg,dc=com»
    -w -f create_group.ldif
```

```
dn: cn=mygroup, ou=groups, dc=yourorg, dc=com
objectclass: top
objectclass: posixGroup
cn: mygroup
gidnumber: 100
memberuid: giuseppe
memberuid: anotheruser
```

create_group.ldif



Avantages et inconvénients de OpenLDAP

- Avantages
  - Licence modulaire
  - Sécurité : SSL et SASL
  - Extensions
- Inconvénients
  - Support de certaines RFC optionnelles manquant
  - Documentation en ligne incomplète
  - Redémarrage après modification de la configuration

Implémentation de LDAP : Authentification sous Linux en réseau

- Au commencement : NIS
  - Critiqué pour son manque de sécurité
- L'alternative en vogue avec un annuaire
  - Association de 3 technologies
    - LDAP
    - NSS : Name Server Switch avec `nss_ldap`
    - PAM : Pluggable Authentication Modules avec `pam_ldap`

Synthèse de la technologie

- ***+ Centralisation***
- ***+ Fiabilité***
- ***+ Sécurisation***
- ***+ Support de nombreux environnements de développement***
- ***- Un langage d'interrogation pauvre***

Synthèse de la technologie

- Tableau comparatif LDAP / Base de Données

Critère	LDAP	Base de Données
Rapport lecture/écriture	optimisé en lecture	lecture/écriture
Extensibilité	facile (schéma LDAP)	difficile (via schéma entité-association)
Distribution des tables	inhérente	rare
Réplication	possible	possible
Modèle transactionnel	simple	avancé
Standard	oui	non (spécifique à un SGBD)

Tableau 1: Avantages/inconvénients de LDAP sur les bases de données

- Tableau comparatif LDAP / NIS (Network Information Services)

Critère	LDAP	NIS
Port	spécifique (389/636 par défaut)	arbitraire (appel RPC)
Chiffrement des données	possible	impossible
Mécanisme de contrôle d'accès	oui	non
Distribution des tables	oui	non
Réplication	oui (réplication partielle possible)	oui (uniquement totale)
Sémantique des recherches	avancée	simple

Tableau 2: Avantages/inconvénients de LDAP sur NIS

Questions ?