

LDAP

Cours 05/03

Pierre Mauduit

6 mars 2007

1 Annuaire ?

Un annuaire est un conteneur d'informations organisées

Exemples d'annuaires :

- annuaire téléphonique
- carnet d'adresses
- ...

Un annuaire électronique a les propriétés suivantes :

- protocole d'accès au contenu
- syntaxe d'interrogation de la base
- modèle de duplication
- modèle de distribution des données

Par rapport aux annuaires non électroniques :

- Dynamique : taux de mise à jour important
- Sécurité (contrôle d'accès)

Par rapport à une base de données :

- Rapport lecture / écriture beaucoup plus élevé pour les annuaires
- Plus facilement extensible
- Diffusion plus large échelle
- distribution multi serveur plus facile
- Duplication des infos plus fréquentes
- Standard : LDAP
- Performances globales des annuaires plus élevées en lecture

Un annuaire est :

- Moyen de chercher des infos plus efficacement et rapidement
- Accessible des humains et des applications
- Un outil de gestion (carnet d'adresses, comptes utilisateurs, profils ...)
- Un moyen de stockage et de diffusion des certificats dans une PKI

Un annuaire n'est pas :

- Approprié aux écritures fréquentes
- Destiné à manipuler des données volumineuses

2 Historique

- 1970-80 : /etc/passwd
IBM MVS PROFS
- 1980 : Grapevine (Xerox)
- 1984 : - DNS - Whois
- Annuaire applicatifs :
 - Lotus cc : Mail, Notes
 - Unix sendmail, /etc/aliases
 - Microsoft Exchange
- Annuaire Internet (Vers le LDAP) :
 - Bigfoot, Yahoo's Four11, AnyWho ...
- Annuaire systÃmes / rÃseau (NOS) :
 - Sun NIS, NIS+
 - Novell Netware Directory Service
 - MS Active directory (natif LDAP)
- Annuaire multi usages :
 - X500
 - Whois++
 - CSO
 - LDAP
- X.500 :
 - RÃgles de nommage des objets et des entitÃs
 - Les protocoles pour fournir le service d'annuaire
 - MÃcanisme d'authentifications
 - ...

X.500 ne tourne pas sur des serveurs PCs (Architecture propriÃtaire). Serveurs trÃs extensibles, fonctions trÃs ÃvoluÃes de recherche, et distribuÃ. L'impantation est toutefois trÃs lourde, bugguÃ, et difficilement interopÃrable. BasÃ sur des protocoles ISO, contraires Ã la culture internet.

=> X.500 abandonnÃ car c'est un Ãchec en terme de dÃploiement. Mais a permis l'arrivÃe de LDAP.

LDAP garde beaucoup d'aspects de X.500 mais va dans le sens de la "culture internet", en amÃliorant ce qui posait problÃme.

Protocole d'accÃs

- Comment s'effectue la communication client / serveur
- Comment s'Ãtablit la communication serveur / serveur (synchronisation, Ãchange de contenu)
- CrÃer des liens permettant de relier des annuaires les uns aux autres.
- Format de transport de donnÃes : On Ãvite l'ASCII et on privilÃgie le Lightweight Basic Encoding Rules (LBER)
- MÃcanismes de sÃcuritÃ

- Opérations de base : search, compare add, delete modify rename bind, unbind, abandon
- Referral service défini dans LDAPv3
- "replication service" encore en développement

LDAPv3 conçu pour être extensible sans avoir à modifier la norme, grâce à 3 concepts :

- Ajout d'opérations, en plus des 9 de base
- LDAP controls : modification / ajout de comportements.
- SASL : (Simple Authentication And Security Layer)
- Entrée : l'ajout de base de l'annuaire.
- Informations représentées sous la forme d'attributs
- Il existe toute sorte de classes d'objets (concrètes ou abstraites)
- Schéma de l'annuaire définit la liste des classes d'objets qu'il connaît

"Directory Schema" est l'ensemble des définitions relatives aux objets qu'il sait gérer (équivalent du typedef).

Les attributs sont identifiés par un nom et un OID. Il existe 2 catégories d'attributs : les attributs utilisateurs et les attributs systèmes.

Les OID sont normalisés dans un RFC, référencés par l'IANA.

Schémas :

- issus de X.500
- slapd.conf
- ASN.1
- LDAPv3 : stockage des schémas au sein de LDAP

exemple de syntaxe dans slapd.conf :

```
attribute NAME [ALIASSES] [OID] SYNTAXID [OPTIONS] attribute cb commonName 2.5.4.3 cis
objectclass NAME [OID] [superior SUP] [required REQATTRS] [allows OPTATTRS] object person
oid 2.5.6.6 superior top requires sn, cn allows description, seeAlso, telephoneNumber, userPassword
```

exemple de syntaxe ASN.1 : [...]

exemple de syntaxe LDAPv3 : [...]

Vérification de schéma : Les schémas sont vérifiés par défaut dans OpenLDAP. (schema checking)

Le module de nommage définit comment sont organisés les entrées dans l'annuaire et comment elles sont référencées.

Les entrées représentent des objets.

L'organisation des objets se fait suivant une structure logique hiérarchique

- Structure arborescente : "Root Entry" ou "Base DN" pour la racine

DN : distinguished name cn=admin,dc=pedrov,dc=net par exemple

- Entrée des alias : pointe vers un élément local au LDAP

- Entrée des referrals : rel : pointe vers une URL LDAP traitée au niveau du serveur LDAP

Module fonctionnel

- interrogation,
- comparaison,
- mise à jour,
- authentification et contrôle,

- opérations attendues (v3)
- Requete composée de 8 paramètres
- Filtres de recherche RFC 2254 (cn=Norbert Durant) (&(sn=Durant)(1=paris))
- Mises à jour add, ...
- LDAP : protocole avec connexion : ouverture de session (bind) + identification et éventuellement mot de passe.
- "RootDN Authentication" : accès administrateur
- Mot de passe + SSL ou TLS - Certificats SSL nécessite un échange de certificats - SASL : OTP par exemple (One Time Password)
- ACL assez simples : <quoi> <qui> <comment> Comment : Read, Write, Search, Compare, Selfwrite, Add, Delete Qui : tout le monde, self ...
- Chiffrement
- Duplication : n'est pas encore standard mais proposée par la plupart des serveurs IETF propose le protocole LDUP
- Critères de choix d'un logiciel serveur :
 - Prix d'achat
 - Coûts de maintenance et support
 - Adaptation du logiciel types d'applications envisagées
- LDIF : représentation des données sous forme de texte uuencode (base64)
- Utilisation des referrals : faire attention à utiliser intelligemment, car une requete distante peut être très lourde.
- Utilisations de LDAP :
 - Peut être étroitement lié au système d'exploitation
 - Extranet
 - Peut remplacer un SGDB (fichier clientèle, catalogues de fournitures ...)
 - Couplé à un autre SGDB : exportation de certaines données vers le LDAP
 - Gestion centralisée authentification et droits d'accès (Projet 2)
- Le futur :
 - Meta-annuaires
 - intégration au coeur des OS
 - prédominance de LDAP
 - tout est annuaire!