INSA
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
CENTRE VAL DE LOIRE

ANNUAIRE LDAP

(Lightweight Directory Access Protocol)

STI 4A

Promotion 2022

M. Szpieg

Historique LDAP

- Les annuaires électroniques sont nés avec l'arrivée de l'informatique (/etc/passwd et NIS).
- Avec l'arrivée d'INTERNET, apparaissent le DNS et WHOIS (diffusion des données associées à une adresse IP ou à un nom de domaine) répartition des données à l'échelle de la planète.
- La normalisation X500

son but était de mettre à disposition un standard d'annuaire pour l'industrie de la télécommunication indépendant et de permettre d'inter-opérer les annuaires de la planète (pages blanches ou jaunes)

Historique LDAP

- X500

Première version 1988 puis seconde version 1993.

- X500 est, lui même, composé de plusieurs standards (X501, X509, X511,…)
  - Notons, au passage, la norme X509 qui est à la base des certificats électroniques, PKI « Public Key Infrastructure ».
- X500 principe d'échange de données :
  - Un client DUA (Directory User Agent) dialogue avec un DSA (Directory System Agent) qui contient au moins une partie de la base de données DIB (Directory Information Base) en utilisant le protocole DAP (Directory Access Protocol).

Historique LDAP

- X500 et DAP :

DAP est un protocole entièrement défini par l'ISO qui s'appuie, entre autre, sur des couches réseaux, de niveau inférieur OSI, définies aussi par l'ISO et non pas simplement sur TCP/IP.

- X500 est très riche en fonctionnalités et engendre une complexité dans sa mise en œuvre.
- Naissance de LDAP :
  - Suite à la complexité de DAP et à l'obligation d'utilisation de cartes réseaux X25 un nouveau standard beaucoup plus pratique est né LDAP (Lightweight Directory Access Protocol).
  - La version 3 de LDAP est normalisée par l'IETF (Internet Engineering Task Force) en 1997.

Historique LDAP

- LDAP protocol :

Le protocole LDAP emploie la notation ASN.1 et les messages sont codés avec le format binaire LBER (Lightweight une version simplifié de BER Basic Encoding Rules vue avec SNMP).

Définition et aspects (1/2)

- Annuaire : Base de données permettant la localisation d'une information à partir de différents critères
- Annuaire numérique possède un aspect dynamique :
  - Réduction du temps de diffusion de l'information
  - Réduction du temps de mise à jour
- Un aspect Flexible
  - Possibilités de rajouter des informations non prévues à la création de l'annuaire.
  - Affichage des données suivant les critères de l'utilisateur.
- Un aspect sécurité
  - Contrôle de la diffusion d'informations en fonction de l'identité (authentification) de la personne qui consulte (ou modifie).

Définition et aspects (2/2)

- Gestion de profils
  - On peut créer différents profils d'utilisateurs (administrateurs, personnels de l'entreprise, autres…)

Utilités des annuaires

- Localiser des personnes ou des ressources ou tout type « d'objets ».
- Localiser des ressources (applications, stockage…) et des droits d'accès.
- Recherche d'informations facilitée (multicritères, critères incomplets)

Annuaire ou base de données

- Un annuaire a un rapport requêtes lecture/requêtes écriture élevé.
- Un annuaire ne gère pas des transactions complexes.
- Les annuaires doivent être disponibles pour un grand nombre de personnes (Entreprise dans son ensemble ou inter-entreprises) et engendrer un débit faible pour chaque requête.
- Les annuaires doivent pouvoir communiquer entre-eux (similitude avec le DNS).
- Les informations dans un annuaire sont classées de manière hiérarchique.
- Un annuaire offre un espace de noms homogène (similitude nom FQDN).

Espace de noms

Représente l'information hiérarchique dans les entrées consistant en un ensemble d'attributs avec un nom unique appelé « Distinguished Name (DN) »

Premiers pas avec LDAP (1/2)

LDAP contient 4 modèles :

- Modèle d'information : Définit la nature des données stockées.
  - Une donnée est un ensemble d'enregistrements et chaque enregistrement est une instance de classe d'objet comportant une série d'attributs.
  - Chaque attribut est défini par un type (entier, chaîne de caractères…) et contient une ou plusieurs valeurs (Nom,prénoms) obligatoires ou non (Téléphone portable).
- Modèle de désignation : Définit l'organisation des données.
  - Elle sont classées de manière hiérarchique dans un arbre le DIT (Directory Information Tree).
  - Le nom d'une entrée contient des informations sur une instance d'une ou plusieurs classes du DIT.
  - L'entrée est définie par la chaîne des noms des nœuds de l'arbre qui conduisent à la donnée (analogie chemin absolu dans un système de fichiers).

Premiers pas avec LDAP (2/2)

LDAP contient 4 modèles (suite) :

- Modèle service :

  Définit les fonctions offertes par un annuaire (recherche-consultation, mise à jour, authentification des utilisateurs).

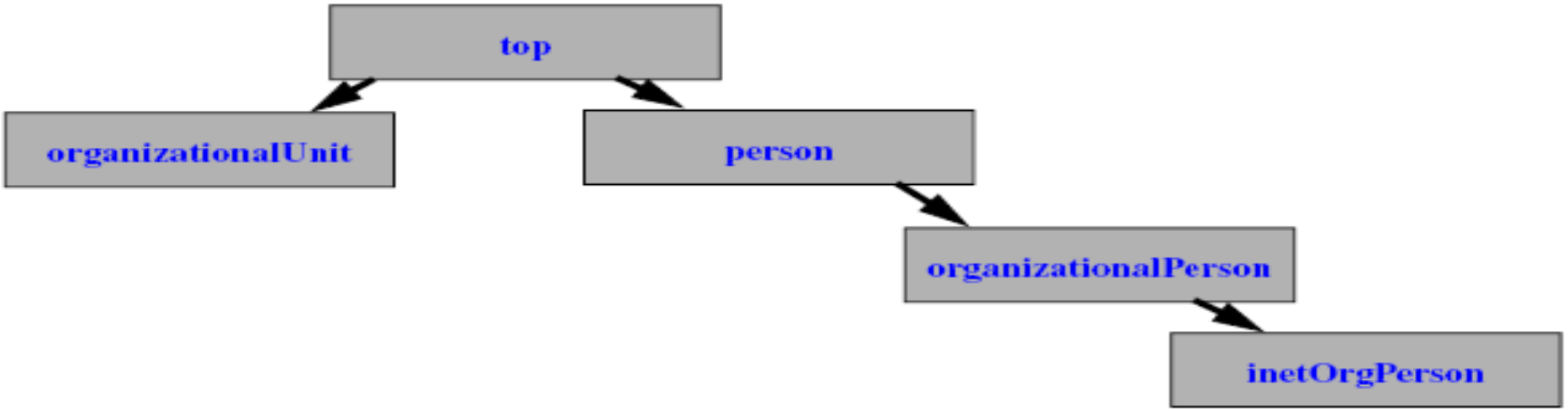
- Modèle sécurité :

  Définit les manières de s'identifier de façon sécurisée sur un annuaire LDAP.

Le DIT (Directory Information Tree)

Les classes d'objet, qui sont des attributs, forment un arbre dont la racine est « top ».

Chaque attribut possède un nom (dc, sn, cn, o, ou…)

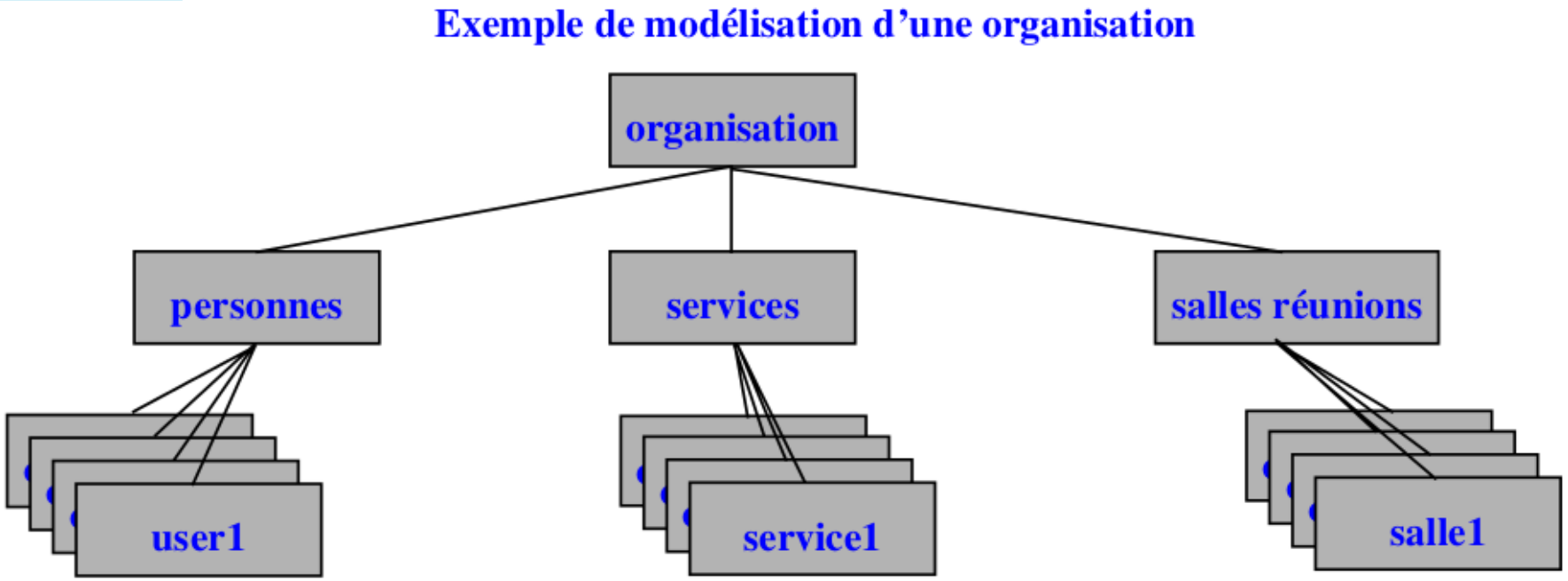


Chaque objet hérite des attributs de l'objet dont il est fils.
Chaque entrée est définie par un attribut classe d'objet (objectClass).
On indique obligatoirement la parenté de chaque objet.

Le DIT (Directory Information Tree)

Une classe d'objet possède un OID (Object Identifier) unique dont la liste est tenue à jour par l'IANA (Internet Assigned Numbers Authority).
Un OID est une séquence de nombres entiers séparés par des points.
Les OIDs sont alloués de manière hiérarchique et sont sous l'autorité de l'organisation qui en possède la délégation.
Une entreprise qui le désire peut demander à l'IANA l'allocation d'un préfixe d'OID.
Un OID est une chaîne de numéros séparés par des points. EX : 1.3.5.1.4.1.1466.115.121.1.15
(Similitude avec MIB SNMP!!)

Le DIT (Directory Information Tree)



Le schéma d'un annuaire

Le schéma décrit les classes d'objets, les types des attributs et leur syntaxe.
Le schéma de l'annuaire définit la liste des classes d'objets qu'il connaît.
Dans un objet classe des données peuvent être facultatives ou obligatoires.
objectclass (1.3.6.1.4.1.999.2.1 NAME 'Personne' SUP inetorgperson
DESC 'membre du personnel'
MUST (sn $ cn $ fonction)
MAY (uidNumber $ gidNumber $ homeDirectory $ loginShell))
Ici la fonction (exemple chef de service info) est obligatoire, le loginshell non

Les trois type de classes d'objet

- Type classe structurelle :
  Décrit un objet réel : personne ,organisation, calculateur.

- Type classe auxiliaire :
  ajoute des attributs supplémentaires, elle complète une classe structurelle et ne peut être employée seule.

- Type classe abstraite :
  Ne peut être utilisée directement mais sert d'ancêtre à une classe d'objet. EX : la classe d'objet « top »

Objet « user » dans un schéma LDAP

posixAccount - schéma LDAP standard pour représenter des comptes d'utilisateurs.

```
nisSchema.2.0 NAME 'posixAccount' SUP top AUXILIARY
DESC 'Abstraction of an account with POSIX attributes'
MUST ( cn $ uid $ uidNumber $ gidNumber $ homeDirectory )
MAY ( userPassword $ loginShell $ gecos $ description )
```

L'attribut particulier dc

La RFC 2247 préconise l'utilisation de l'infrastructure DNS pour obtenir un espace de nommage cohérent.
Il est préconisé pour une organisation d'utiliser son nom de domaine Internet pour identifier, de manière unique, le suffixe de base de l'annuaire.
Ce contexte de nommage définit le DN de plus haut niveau (distinguished name).
dcObject est une classe auxiliaire permettant de compléter une entrée existante contenant des informations organisationnelles.
Exemple de DN (distinguished name) :

CN=Pierre Dupont,OU=sti,DC=insa-cvl,DC=fr

Le format LDIF (LDAP Data Interchange Format)

Le format LDIF permet la transmission de base de données de serveur LDAP à serveur LDAP de manière normalisée.

Déclaration de l'entrée de l'annuaire au format LDIF :

- dn: dc=insa-cvl, dc=fr
- objectClass: domain
- dc: insa-cvl.fr

LDIF exemple

```
dn: uid=test,ou=People,dc=insa-cvl,dc=fr
cn: Test User
uid: testuser
uidNumber: 501
loginShell: /bin/sh
homeDirectory: /home/testuser
gidNumber: 100
userPassword:: e2NyeXB0fVRYaHRIa05GOUdBSWc=
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
shadowLastChange: 13072
givenName: Test
sn: User
```

LDIF

Le format utilisé dans LDIF est l'ASCII.
Toute donnée non ASCII doit être encodé en base 64.
Dans ce cas le séparateur entre le type et la valeur de l'attribut est « :: ».

JpegPhoto::/9j/4AAQSkZJRgABAQAAAQABAAD//gBHQ1JFQVRPU
jogWFYgVmVyc2IvbiAzLjEwI
CBSZXY6IDEyLzE2Lzk0ICBRdWFsaXR5ID0gNzUsIFNtb290aGluZ
yA9IDAK/9sAQwAIBgYHBgUIB
WcHCQkICgwUDQwLCwwZEhMPFB0aHx4dGhwcICQuJyAiLCMcH
Cg3KSwwMTQ0NB8nOT04MjwuMzQy/

LDAP V3 utilise le jeu de caractères Unicode
Transformation UTF-8 pour les attributs de type texte et les DNs.

Le protocole

Les opérations de base:

- interrogation : search, compare
- mise à jour : add, delete, modify, rename
- connexion au service : bind, unbind, abandon

Le protocole

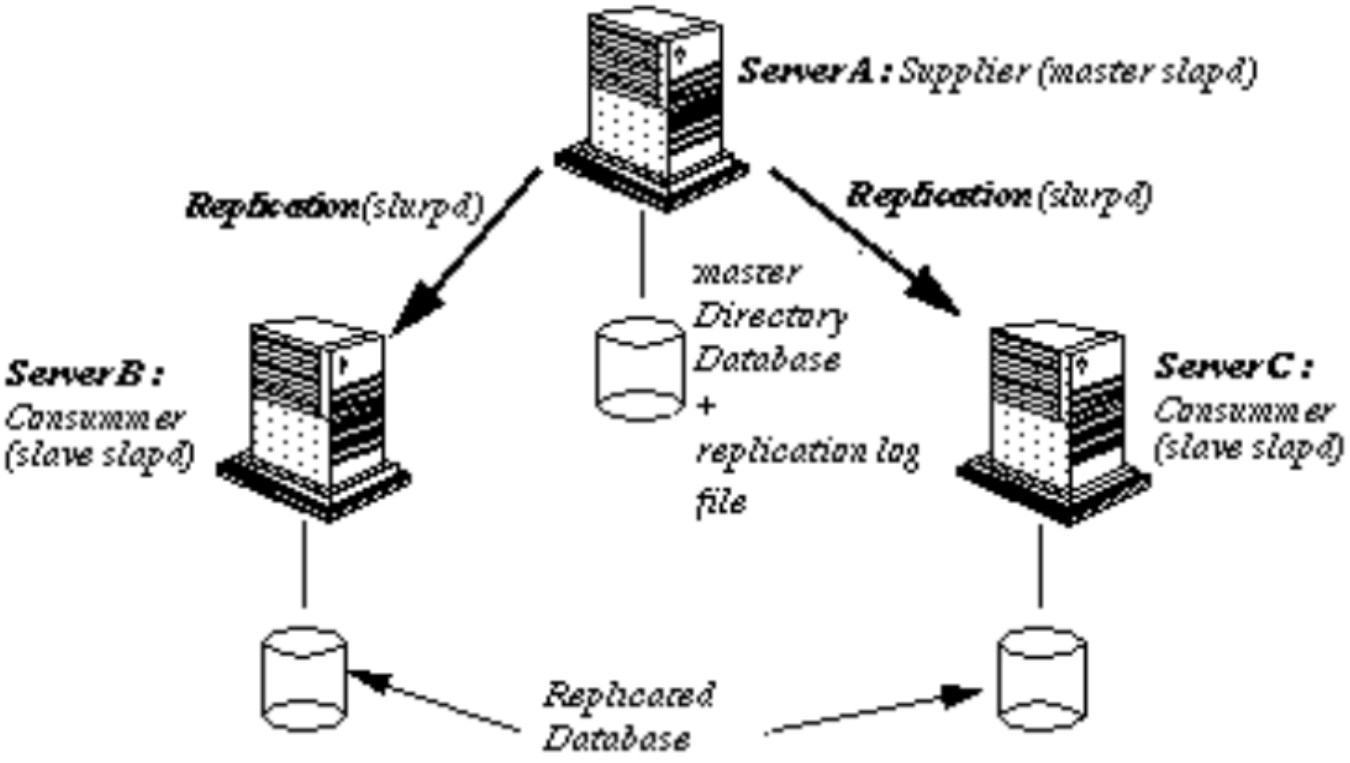
Communication serveur-serveur :

- le referral service est définit par LDAPv3,
- le service de réplication est normalisé sous la dénomination LDAP Duplication Protocol (LDUP)

La réplication

La duplication met en jeu plusieurs serveurs : les « supplier servers » fournissent les données, les « consumer servers » les reçoivent.

Les informations de configuration décrivant les « suppliers », les « consumers » et quelles données ils échangent, forment le « replication agreement ».



La réplication

On peut dupliquer
• l'arbre entier ou seulement un sous arbre,
• une partie des entrées et de leurs attributs qu'on aura spécifiés via un filtre du genre
: « on ne duplique que les objets de type personne »
« on ne duplique que les attributs non confidentiels » (annuaire interne vs. annuaire externe)

- Plusieurs manières de synchroniser les serveurs :
  - mise à jour totale
  - mise à jour incrémentale…

- Plusieurs stratégies de duplications :
  - single-master replication
  - multiple-master replication
  - cascading replication.

La réplication

La duplication se fait en temps-réel ou à heure fixe (scheduling replication).

Deux précautions :

- les serveurs doivent tous utiliser le même schéma de données,
- les règles d'accès aux données dupliquées doivent être dupliquées.

La mise en œuvre de la duplication nécessite de la prévoir au moment de la conception du DIT.

L'annuaire distribué

L'objectClass referral permet de déléguer une partie de la branche d'annuaire à un serveur distant.

Avantages :

Performances : mettre une branche très sollicitée sur un autre serveur augmente les performances au plus près des utilisateurs les plus fréquents.

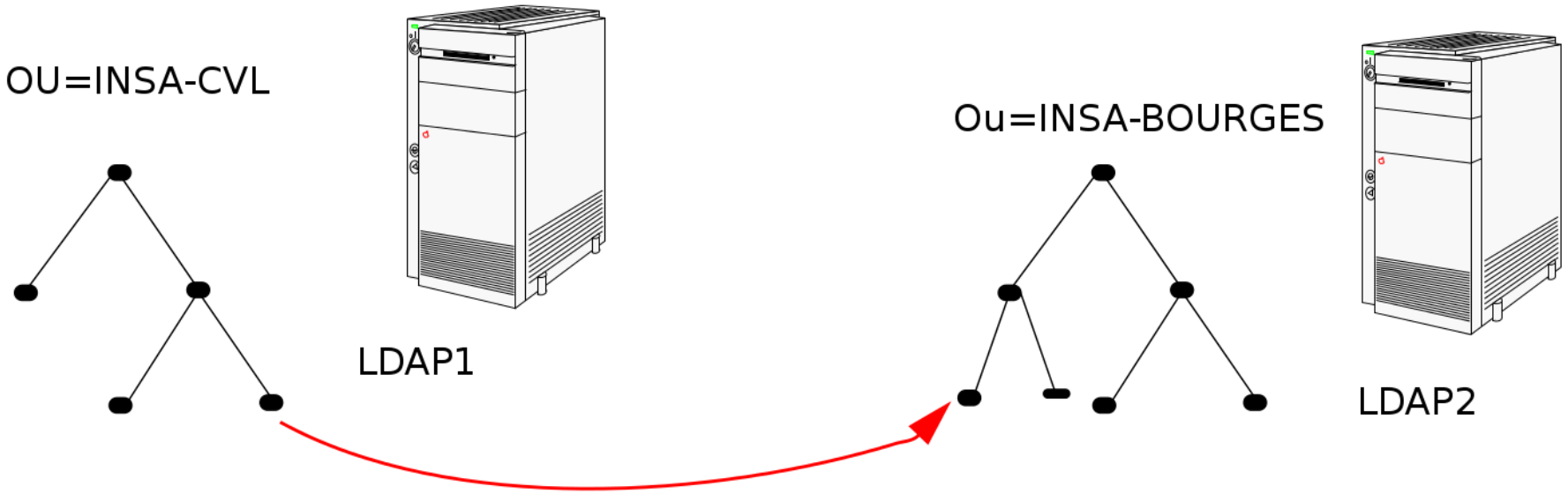
Localisation géographique : mettre la partie de branche au plus près des utilisateurs les plus fréquents.

Administration : Déléguer l'administration d'une partie de la base.

Remarque : similitude avec les Glue Records du DNS

Le service « REFERRAL »

But : Créer des liens permettant de relier des annuaires les uns aux autres (referral service) définit par LDAP V3.
L'attribut ref de l'objet referral a pour valeur l'URL LDAP de l'entrée désignée.



Les « ALIAS »

Un Alias (défini dans la RFC 4512) utilise l'« alias STRUCTURE objectClass » pour définir la position au sein de la DIT actuel. L'alias peut être considéré comme un « lien symbolique » au niveau intra-LDAP.

L’authentification

Dans l’annuaire on peut avoir ,par exemple, l’objectClass person.
Dans cette classe un attribut userPassword est défini.
Cet attribut peut contenir des données pour identifier l’utilisateur et cette donnée peut (doit) être codée(hachage).
L’authentification anonyme est possible avec un DN et un mot de passe vide.

L’authentification

LDAP est un protocole avec connexion : l’ouverture de session (bind) s’accompagne d’une identification et, éventuellement, d’un mot de passe (optionnel en V3).
- Anonymous authentification - accès sans authentification permettant d’atteindre les données sans restrictions d’accès (V2,V3).
- Root DN authentification - accès administrateur (tous les droits)(V2, V3).
- Mot de passe en clair - un DN plus un password qui transite en clair sur le réseau (V2, V3).
- Kerberos V4 (V2)

L’authentification

Mot de passe + SSL (LDAPS) ou TLS - la session est chiffrée et le mot de passe ne transite plus en clair.
- Certificats sur SSL - échange de certificats SSL (clefs publiques/privées).
- Simple Authentification and Security Layer (SASL) – mécanisme externe d’authentification (V3).

Le contrôle d’accès

Les ACLs peuvent être "placées" au niveau des entrées, au sommet de l’arbre ou sur un sous-arbre.
Elles agissent sur les entrées ou certains de leurs attributs.
Elles s’appliquent à des individus ou à des groupes, mais aussi suivant les adresses IP ou les noms de domaine des clients ou les jours et heures.
Le placement et la portée des ACLs dépendent des capacités du logiciel.

Le contrôle d'accès

<quoi> <qui> <comment>

<quoi> : point d'entrée de l'annuaire auquel s'applique la règle

<qui> : à qui s'appliquent ces droits

<comment> : opérations autorisées/refusées

<comment>	<qui>
Read	Tout le monde
Write	Un utilisateur
Search	Un groupe d'utilisateur
Compare	Une machine
Selfwrite	
Add	
Delete	

Exemple openldap :

```
access to * by self write
       by * read
```

Monitorer Ldap

Reading LDAP logs

- Debug levels allow output of useful information
- /usr/sbin/slapd -d xxx
  - 8 – connection management
  - 32 – search filter processing
  - 64 – config file processing
  - 128 – access control list processing
  - 256 – connections/operations/results
  - additive – 288 is conn/ops/results and search filters