Annuaire LDAP

Fred Hémery

IUT Béthune
Département
Génie des Télécommunications & Réseaux

Réseaux — 06/07

Introduction

- LDAP: Lightweight Directory Access Protocol
- LDAP est un standard de normalisation pour l'interface d'accès aux annuaires
- LDAP favorise le partage et simplifie la gestion des informations sur les personnes ou les ressources de l'entreprise
- Un annuaire LDAP permet de réduire les coûts d'administration et d'améliorer la sécurité
- LDAP manipule des données organisées en hiérarchie contrairement aux SGBD actuels qui utilisent une organisation relationnelle (L'organisation hiérarchique est plus adaptée à l'organisation d'une entreprise)

Qu'est-ce qu'un annuaire ?

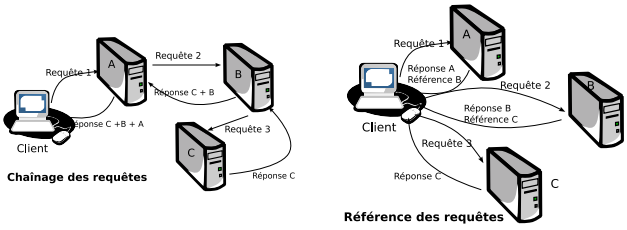
- Par exemple
  - Carnet d'adresses téléphoniques
  - Les pages blanches, jaunes
- Permet de retrouver les informations sur une personne, une entreprise à partir d'un critère de sélection: le nom, le code postal, fonction, ...
- Un annuaire doit offrir des critères de recherche efficaces (puissants et simples)
- Un annuaire est une base de données qui est le plus souvent utilisé en lecture uniquement (interrogation). Il ne gère pas les transactions complexes

Qu'est-ce qu'un annuaire ?

- Les annuaires en ligne permettent
  - Carnet d'adresses téléphoniques
  - Les pages blanches, jaunes
  - Une diffusion rapide des modifications
  - Une délégation des modifications (adresse électronique pour le responsable de la messagerie)
  - La diffusion de messages en fonction de critères de recherche (ensemble des parents d'une entreprise)
  - La modification du critère de recherche
  - Un contrôle d'accès aux informations
  - Un contrôle des informations affichées en fonction de l'utilisateur

Les annuaires LDAP

- Les annuaires LDAP suivent un standard qui uniformise le contenu des champs d'un annuaire.
- Les annuaires peuvent communiquer pour faire aboutir une requête



Introduction LDAP

- Regroupement des fonctions d'un annuaire autour du standard LDAP
  - Permet de stocker des données
  - Offre un classement et une vue hiérarchique
  - Permet de rechercher et de naviguer dans les données
  - Permet la lecture
  - Permet une interrogation à distance par une interface standard
  - Communique avec d'autres annuaires
  - Gère le contrôle d'accès
  - Flexible et évolutif
- LDAP : interface de communication avec un annuaire (l'implémentation de l'annuaire n'est pas définie)

X.500

- LDAP est un standard issu de la norme X500
- La Norme X500 est un standard conçu en 1988 (V2 en 1993) par les opérateurs télécoms ITU (International Telecommunications Unions) et l'ISO (International Organization for Standardization) pour interconnecter tout type d'annuaire. Il définit
  - Des règles de nommages pour les éléments qu'il contient
  - Des protocoles d'accès à l'annuaire
  - Des moyens d'authentifier les utilisateurs
- X500 trop lourd à mettre en place : chaque constructeur a développé une solution non compatible avec les autres.
- LDAP est né d'une adaptation de X500 pour l'internet

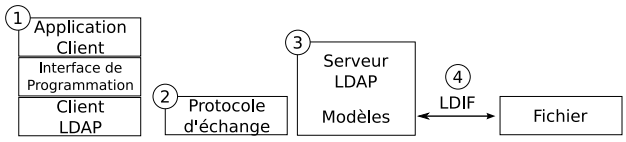
Introduction LDAP

- LDAP est un protocole client/serveur utilisant les couches réseaux TCP/IP et offrant 4 modèles qui ont pour objectif de permettre le partage, la simplification de la gestion et des droits d'accès des informations et des ressources.
- Les quatre modèles
  - Le modèle d'information
  - Le modèle de désignation ou fonctionnel
  - Le modèle des services : La recherche, la consultation, la mise à jour de l'annuaire, le contrôle d'accès
  - Le modèle de sécurité: La manière de s'identifier de façon sécurisée à l'annuaire

Le protocole LDAP

- Le protocole LDAP est défini dans la `rfc3377`
- Le protocole permet d'effectuer des opérations synchrones ou asynchrones
- Les serveurs peuvent répondre à un client par un referral, c'est à dire par un pointeur vers un autre serveur que le client devra contacter de lui même
- Les données sont transmises en utilisant le format BER (Basic Encoding Rules : indépendance de la représentation)
- Le protocole définit un ensemble de commandes de base standards (modèle fonctionnel) et
- des commandes étendues

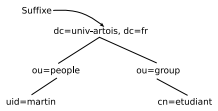
Le protocole LDAP



1. Interface de programmation
2. Protocole d'échange entre le client et le serveur et les serveurs entre-eux
3. Les quatre modèles
4. Le format de fichier LDIF pour l'import/export des données de l'annuaire

Le modèle d'information

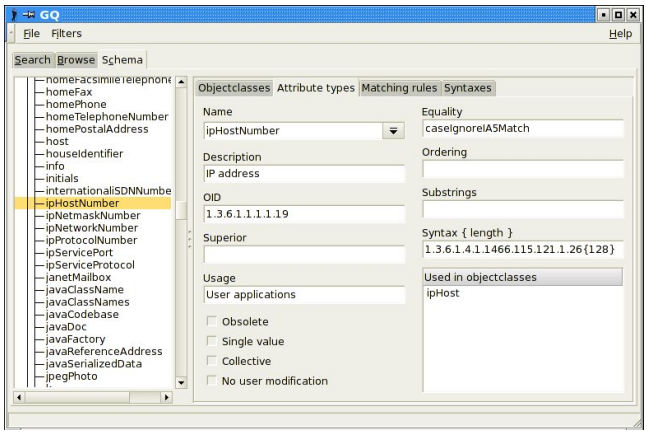
- Le Directory Information Tree
  - Les données LDAP sont structurées dans une arborescence hiérarchique : le Directory Information Tree (DIT)
  - Chaque noeud de l'arbre correspond à une entrée de l'annuaire ou Directory Service Entry (DSE) et
- Les entrées
  - Les entrées correspondent à des objets abstraits ou issus du monde réel (une personne, une imprimante, . . .)
  - Elles contiennent un certain nombre de champs appelés attributs dans lesquels sont stockées des valeurs
- Chaque serveur possède une entrée spéciale, appelée root Directory Specific Entry (rootDSE) qui contient la description de l'arbre et de son contenu



Le modèle d'information

- Le schéma
  L'ensemble des définitions relatives aux objets que sait gérer un serveur LDAP s'appelle le schéma. Il décrit les classes d'objets, leurs types d'attributs et leur syntaxe.
- Les attributs
  Une entrée de l'annuaire contient une suite d'attributs (couples types - valeurs). Les attributs sont caractérisés par :
  - Un nom qui l'identifie
  - Un Object Identifier (OID) qui l'identifie également
  - S'il est mono ou multi-valué
  - Une syntaxe et des règles de comparaison
  - Un indicateur d'usage
  - Un format ou une limite de taille de valeur qui lui est associée
  - On distingue deux types d'attributs
    - ★ Les attributs utilisateur: manipulés par l'utilisateur (nom prénom)
    - ★ Les attributs opérationnels: manipulés par l'administrateur (date mod)

Le modèle d'information



Le modèle d'information

- Les classes d'objets modélisent des objets réels ou abstraits en les caractérisant par une liste d'attributs optionnels ou obligatoires. Une classe d'objet est définie par :
  - Un nom qui l'identifie
  - Un OID qui l'identifie également
  - Des attributs obligatoires
  - Des attributs optionnels
  - Un type (structurel, auxiliaire ou abstrait)
- Le type d'une classe est lié à la nature des attributs qu'elle utilise.
  - Une classe structurelle correspond à la description d'objets basiques de l'annuaire. Une entrée appartient toujours au moins à une classe d'objet structurelle.
  - Une classe auxiliaire désigne des objets qui permettent de rajouter des informations complémentaires à des objets structurels.
  - Une classe abstraite désigne des objets basiques de LDAP comme les objets top ou alias.

Le modèle d'information

- Les classes d'objets forment une hiérarchie, au sommet de laquelle se trouve la classe `top`.
- Chaque classe hérite des propriétés (attributs) de la classe dont elle est la fille.
- On précise la classe d'objet d'une entrée à l'aide de l'attribut `objectClass`.

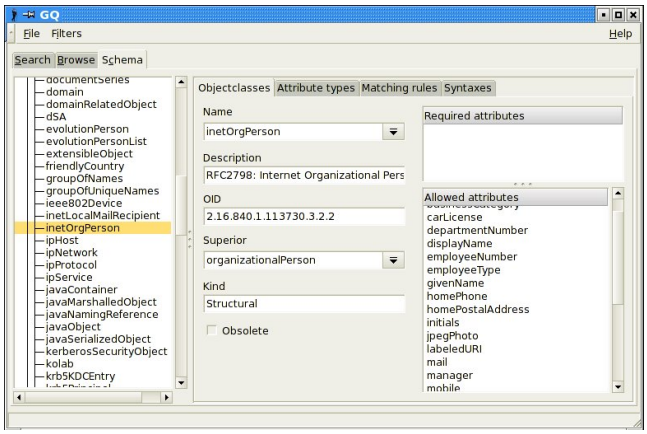
Par exemple, l'objet inetOrgPerson a la filiation suivante :

```
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
```


Le modèle d'information

Entry Type	Required Attributes	Optional Attributes
inetOrgPerson	commonName (cn), surname (sn), objectClass	businessCategory , carLicense , departmentNumber, description, employeeNumber, facsimileTelephone, Number, givenName, mail, manager, mobile, organizationalUnit (ou) , pager, postalAddress , roomNumber, secretary , seeAlso, telephoneNumber , title, labeledURI, uid
organizationalUnit	ou, objectClass	businessCategory , description, facsimileTelephoneNumber , location (l) , postalAddress, seeAlso , telephoneNumber
organization	o , objectClass	businessCategory, description, facsimileTelephoneNumber, location (l), postalAddress, seeAlso,telephoneNumber

Le modèle d'information



Le modèle d'information

- Les OIDs
  - Les objets et leurs attributs sont normalisés par le RFC2256
  - Ils sont tous référencés par un object identifier (OID) unique dont la liste est tenue à jour par l'Internet Assigned Numbers Authority (IANA).
  - Il est possible de modifier le schéma en rajoutant des attributs à un objet (déconseillé) ou en créant un nouvel objet (mieux) et d'obtenir un OID pour cet objet auprès de l'IANA (encore mieux).
  - Un OID est une séquence de nombres entiers séparés par des points.
  - Les OID sont alloués de manière hiérarchique de telle manière que seule l'autorité qui a délégation sur la hiérachie "1.2.3" peut définir la signification de l'objet "1.2.3.4". Par exemple :

```
2.5             - fait référence au service X500
2.5.4           - est la définition des types d'attributs
2.5.6           - est la définition des classes d'objets
1.3.6.1         - the Internet OID
1.3.6.1.4.1     - IANA-assigned company OIDs, used for private MIBs
1.3.6.1.4.1.4203      - OpenLDAP
```


Le modèle d'information

- Quelques exemples de comparaison

règle de comparaison		
LDAP	X500	description
cis	caseIgnoreMatch	Attribut texte non sensible à la casse
ces	caseExactMatch	Attribut texte sensible à la casse
tel	telephoneNumberMatch	Attribut texte représentant un numéro de téléphone (les virgules et les espaces sont ignorés dans la recherche)
int	integerMatch	Attribut entier (pour une comparaison numérique)
dn	distinguishedName	Nom d'entrée. Permet de comparer deux entrées
bin	octetStreamMatch	Attribut binaire. Permet de comparer octet par octet
bin	booleanMatch	Attribut booléen. Permet de comparer deux attributs booléens

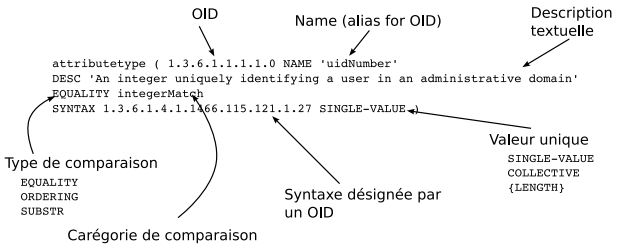
Le modèle d'information

- Quelques exemples de syntaxe d'attribut

syntaxe d'attribut	OID	description
Binary	1.3.6.1.4.1.1466.115.121.1.5	BER/DER data
Boolean	1.3.6.1.4.1.1466.115.121.1.7	boolean value
Distinguished Name	1.3.6.1.4.1.1466.115.121.1.12	DN
Directory String	1.3.6.1.4.1.1466.115.121.1.15	UTF-8 string
IA5String	1.3.6.1.4.1.1466.115.121.1.26	ASCII string
Integer	1.3.6.1.4.1.1466.115.121.1.27	Integer
Name and Optional UID	1.3.6.1.4.1.1466.115.121.1.34	DN plus UID
Numeric String	1.3.6.1.4.1.1466.115.121.1.36	Numeric String
OID	1.3.6.1.4.1.1466.115.121.1.38	Object Identifier
Octet String	1.3.6.1.4.1.1466.115.121.1.40	Arbitrary Octets
Printable String	1.3.6.1.4.1.1466.115.121.1.44	Printable String

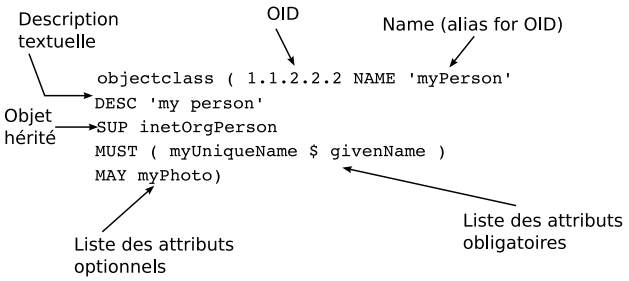
Le modèle d'information

- La déclaration d'un attribut

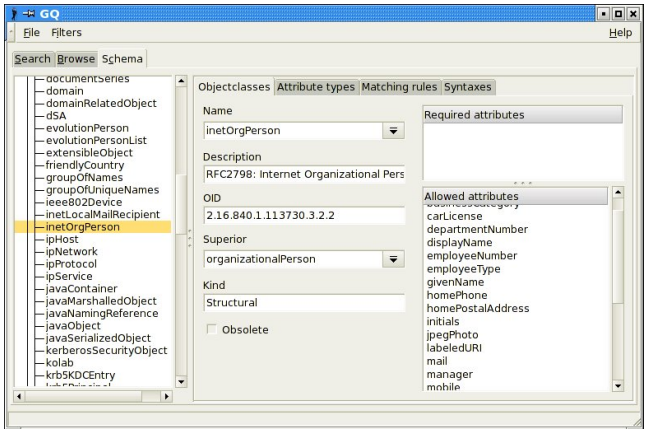


Le modèle d'information

- La déclaration d'une classe



Le modèle d'information

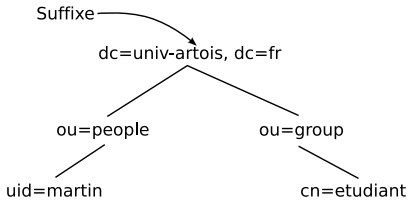


Le modèle de nommage

- Le modèle de nommage ou encore modèle de désignation a pour but de définir des règles de nommage ou de désignation des objets dans l'annuaire.
- Les objets dans un annuaire sont classés hiérarchiquement. L'annuaire possède un espace d'informations homogène (c-à-d que d'un annuaire à un autre un nom dans un annuaire désigne la même chose dans l'autre)
- Tout serveur d'annuaire LDAP contient un objet particulier : root DSE (DSA (Directory System Agent) Specific Entry), il n'appartient à aucune classe et contient des informations générales sur l'annuaire (version, niveau de sécurité, convention de nommage, ...)

Le modèle de nommage

- LDAP présente les informations sous forme d'un arbre (ou de plusieurs) appelé DIT (Directory Information Tree).
- Chaque noeud de l'arbre est un objet qui peut appartenir à n'importe quelle classe.
- Dans un annuaire LDAP, il n'y a pas de racine unique. Le niveau supérieur de chaque arbre est appelé domaine. Un annuaire peut avoir plusieurs domaines.

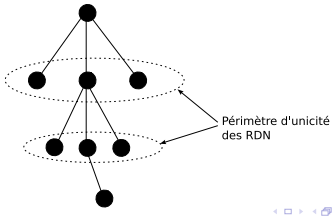


Le modèle de nommage

- Le nom des objets. Il existe deux concepts pour nommer les objets:
  - un nom relatif RDN (Relative Distinguished Name) et
  - un nom absolu DN (Distinguished Name).

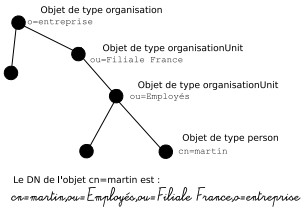
Le modèle de nommage

- Le nom relatif est constitué d'un couple composé d'un attribut et d'une valeur. Par exemple le RDN d'un objet person peut être "`cn=Pierre Durand`" ou encore "`uid=pdurand`".
- Propriétés d'un nom relatif
  - Un objet ne peut avoir qu'un seul RDN et doit être unique dans la branche ou se situe l'objet et au même niveau.
  - Il est préférable d'utiliser un attribut obligatoire
  - Un RDN peut avoir plusieurs couple attribut/valeur "`cn=Pierre Durand+mail=pdurand@entreprise.com`".



Le modèle de nommage

- Le nom absolu DN permet de désigner un objet sans ambiguïté
- Le DN d'un objet est composé de l'ensemble des RDN des noeuds supérieurs, y compris celui de l'objet lui-même. Les RDN sont séparés par des virgules et ils sont classés dans un ordre ascendant (celui de plus bas niveau est placé en premier).



Le modèle des services

Les opérations de base permettent d'accéder au serveur ou de modifier la structure de l'arbre et/ou les entrées de l'annuaire.

Opération LDAP	Description
Search	recherche dans l'annuaire d'objets à partir de critères
Compare	comparaison du contenu de deux objets
Add	ajout d'une entrée
Modify	modification du contenu d'une entrée
Delete	suppression d'un objet
Rename	(Modify DN) modification du DN d'une entrée
Bind	connexion au serveur
Unbind	deconnexion
Abandon	abandon d'une opération en cours
Extended	opérations étendues (v3)

Le modèle des services

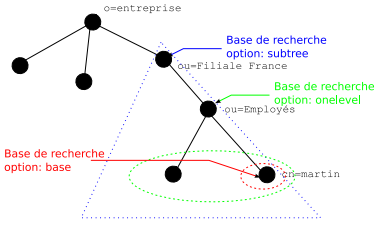
- Les services permettent l'accès à l'information stockée dans l'annuaire. On peut classer ces services en quatre catégories:
  1. Les services de connexion et déconnexion
     permettre au client de s'identifier avant le lancement de la session et se déconnecter en fin de session
  2. Les services de recherche qui déploient tout un ensemble de critères pour sélectionner les informations
  3. Les services de mise à jour qui permettent de faire évoluer l'information disponible dans l'annuaire
  4. Les services annexes qui proposent des services supplémentaires

Le modèle des services

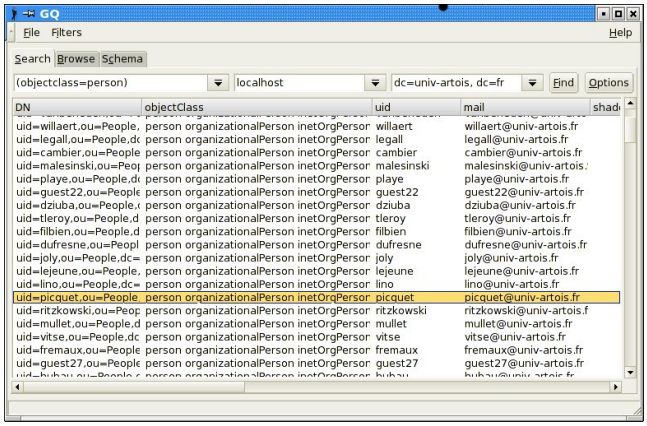
- La connexion permet au client de fournir son identité: toujours obligatoire. Les paramètres
  - Le numéro de version LDAP
  - Le DN de l'objet avec lequel le client souhaite s'identifier (anonyme: chaîne vide)
  - Les paramètres de sécurité (méthode d'authentification : simple, SASL (simple authentification and security layer))
- Le retour: identifiant de la session qui sera utilisé dans toutes les autres opérations.

Le modèle des services

- La recherche permet d'effectuer une recherche sur un ou plusieurs objets ou attributs dans l'annuaire. Les paramètres:
  - Le DN de l'objet constituant la base de la recherche
  - Le périmètre de la recherche (Uniquement au niveau de l'objet de base,1 niveau en dessous de l'objet de base,Tous les niveaux en dessous de l'objet de base)



Le modèle d'information



Le modèle des services

- La modification d'objet permet de modifier tous les attributs d'un objet sauf le DN. Les paramètres
  - DN de l'objet
  - Une liste des modifications à effectuer avec une modification qui contient:
    - ★ Un type de modification (ajout, suppression, remplacement)
    - ★ Un ensemble d'attributs à modifier
- L'ajout d'un objet permet d'ajouter un objet dans l'annuaire. Les paramètres: DN de l'objet, la liste des attributs et des valeurs associées
- La suppression d'un objet permet de supprimer un objet dans l'annuaire Le paramètre: DN de l'objet

Le modèle des services

- La modification d'un DN permet de modifier le DN d'un objet. Les paramètres:
  - Le DN de l'objet
  - Le nouveau RDN (présent si l'on souhaite modifier le RDN de l'objet)
  - Indicateur de suppression de l'ancien RDN (booléen)
  - DN de l'objet qui sera le nouveau supérieur (n'est pas obligatoire)
- La comparaison permet de vérifier si un objet contient bien une ou plusieurs valeurs données. Les paramètres : DN de l'objet, un filtre LDAP. Le retour contient un code qui indique si la comparaison a fonctionné ou pas

Le modèle des services

- Un filtre prend la forme générique suivante:
  `(operateur (assertion ...)(operateur (assertion ...)))`
- Une assertion
  - Un attribut, qui appartient à la liste des attributs dans l'annuaire ou objectClass
  - un opérateur de comparaison, $=$ égalité, $\sim=$ approximation, $>=$, $<=$
  - une valeur
- Les opérateurs booléens
  - ! négation
  - & et
  - | ou

Le modèle des services

Le tableau qui suit récapitule les opérateurs de recherche disponibles :

Filtre	Syntaxe	Interprétation
Approximation	(sn$\sim=$Mirtain)	nom dont l'orthographe est voisine de Mirtain
Egalité	(sn=Mirtain)	vaut exactement Mirtain
Comparaison	(sn$>$Mirtain) , $<=$, $>=$, $<$	noms situés alphabétiquement après Mirtain
Présence	(sn=*)	toutes les entrées ayant un attribut sn
Sous-chaîne	(sn=Mir*), (sn=*irtai*), (sn=Mirt*i*)	expressions régulières sur les chaînes
ET	(&(sn=Mirtain) (ou=Semir))	toutes les entrées dont le nom est Mirtain et du service Semir
OU	(|(ou=Direction) (ou=Semir))	toutes les entrées dont le service est le Semir ou la Direction
Négation	(!(tel=*))	toutes les entrées sans attribut téléphone

Le modèle des services

- Recherche des objets de la classe account et ayant un numéro de groupe égal à 510
  `((\&(objectclass=account)(gidNumber=510))`
- Recherche des objets de la classe account et ayant un numéro de groupe égal à 510 et dont l'uid commence par un 'd' ou un 'p'
  `(\&(objectclass=account)(gidNumber=510)`
  `(|(uid=d*)(uid=p*)))`
- Recherche des objets qui ne sont pas des machines (ipHost) et dont le nom commence par un 'v'
  `(\&(!(objectClass=ipHost))(cn=v*)`

Le modèle de sécurité

- L'authentification
  - Elle est traitée lors des opérations de connexion
  - Elle se fait par usage de mot de passe (mode simple) par certificat (mode SSL) ou par une méthode désignée (mode SASL)
- La confidentialité
  - Elle est traitée lors des opérations de connexion
- L'intégrité
  - N'est pas encore décrit dans la version 3 de LDAP (trace et identification de toutes modifications dans l'annuaire)

Le modèle de sécurité

- Les habilitations consistent à décrire les droits d'accès de certains objets de l'annuaire sur d'autres objets. Cette description est faite à l'aide de règles ACL (Acces Control List)
- Chaque ACL comprend plusieurs règles dénommées ACI (Acces Control Item)
- Un ACI décrit un droit d'un ensemble d'objets sur un ensemble d'objets
  - Un droit concerne une des opérations (recherche, comparaison, modification, ...)
  - Les objets peuvent être désignés explicitement (DN) ou implicitement (filtre LDAP)
- Les règles sont parcourues séquentiellement, la première qui correspond à la connexion est appliquée, les suivantes ne seront pas utilisées.

Le modèle de sécurité

- La syntaxe

```
<access directive> ::= access to <what>
        [by <who> <access> <control>]+
<what> ::= * | [ dn[.<target style>]=<regex>]
        [filter=<ldapfilter>] [attrs=<attrlist>]
<target style> ::= regex | base | one | subtree | children
<attrlist> ::= <attr> | <attr> , <attrlist>
<attr> ::= <attrname> | entry | children
<who> ::= [* | anonymous | users | self |
        dn[.<subject style>]=<regex>]
        [dnattr=<attrname> ]
        [group[/<objectclass>[/<attrname>][.<basic style>]]=<regex> ]
        [peername[.<basic style>]=<regex>]
        [sockname[.<basic style>]=<regex>]
        [domain[.<basic style>]=<regex>]
        [sockurl[.<basic style>]=<regex>]
        [set=<setspec>]
        [aci=<attrname>]
<subject style> ::= regex | exact | base | one | subtree | children
<basic style> ::= regex | exact
<access> ::= [self]{<level>|<priv>}
<level> ::= none | auth | compare | search | read | write
<priv> ::= {=|+|-}{w|r|s|c|x}+
<control> ::= [stop | continue | break]
```


Le modèle de sécurité

- <what> : point d'entrée de l'annuaire auquel s'applique la règle
- <access> : permet ou refuse un type d'accès (lecture, écriture...)
- <who> : identifie le bindDN utilisé en connexion

La cible <what>

- Détermine l'(les) entrée(s) et les attributs qui seront concernés par la règle. L'entrée peut être désignée avec un DN ou à partir d'un filtre.

L'identification (<who>)

*	tous les utilisateurs y compris `anonymous` et les utilisateurs identifiés
anonymous	`anonymous` les utilisateurs non identifiés
users	les utilisateurs identifiés
self	l'utilisateur associé avec l'entrée cible
dn=<regex>	les utilisateurs qui vérifient l'expression régulière

Le modèle de sécurité

Les Permissions (<access>)

Read	permet de lire les données
Write	changer ou créer. Permet également de détruire des données, mais pas l'entrée qui les contient (permission Delete)
Search	les données peuvent être une clef de recherche. La différence avec le droit Read est que celui-ci permet de lire les données issues d'une recherche. Ex : droit search sur le common name et read sur le room number autorise l'affichage du room number pour les résultats de la sélection sur le common name, mais ne permet pas de rechercher les résidents du bureau.
Compare	utilisable pour des critères de comparaison. Implique le droit search mais renvoie en retour un simple booléen.
Selfwrite	uniquement pour la gestion des groupes. Permet soi-même de s'ajouter ou se supprimer d'un groupe.
Add	permet de créer des entrées filles (en dessous de la branche de l'entrée
Delete	droit d'effacer une entrée.

Le modèle de sécurité

Quelques exemples:

```
access to * by * read

access to *
       by self write
       by anonymous auth
       by * read

access to dn=".*,dc=example,dc=com"
       by * search
access to dn=".*,dc=com"
       by * read

access to dn="(.*,)?dc=example,dc=com" attr=homePhone
       by self write
       by dn="(.*,)?dc=example,dc=com" search
       by domain=.*\.example\.com read
access to dn="(.*,)?dc=example,dc=com"
       by self write
       by dn=".*,dc=example,dc=com" search
       by anonymous auth

access to attr=member,entry
       by dnattr=member selfwrite
```


Le format d'échange LDIF

- Il permet d'importer ou d'exporter des données de l'annuaire dans des fichiers ASCII
- LDIF : LDAP Data Interchange Format
- Facilite la réplication ou la synchronisation avec des bases de données externes
- Exemples

```
dn: ou=personnes, o=entreprise.com
Objectclass: top
Objectclass:organizationalUnit
Ou: personnes
Description: ou fictives dédiée aux
             objets Personnes
```

```
dn: uid=pdurand, ou=personnes, o=entreprise.com
Objectclass: top
Objectclass:person
Objectclass:organizationalPerson
Cn: Pierre Durand
Uid: pdurand
Givenname: Pierre
Sn: Durand
Mail: pdurand@entreprise.com
TelephoneNumber: +33 1 41 02 03 04
Description: Responsable du projet annuaire
```


Les outils disponibles

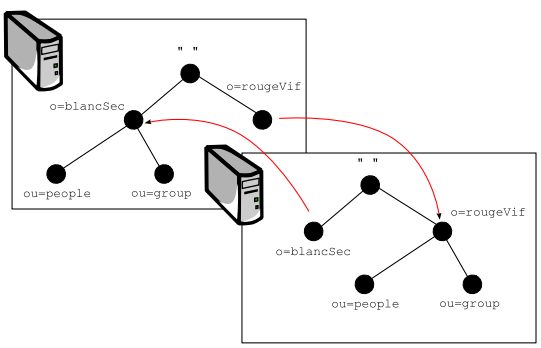
- Un serveur LDAP
  - slapd est un serveur qui permet de gérer un annuaire et vérifie le standard LDAP, il fait partie du logiciel OpenLDAP (http://www.openldap.org)
- Des clients LDAP
  - `ldapadd` qui permet d'ajouter des objets dans l'annuaire
  - `ldapsearch` qui permet de faire des recherches dans l'annuaire
  - `ldapmodify`, `ldapmodrdn` qui permettent de modifier un objet dans l'annuaire
  - `ldapdelete` qui permet de supprimer un objet dans l'annuaire
  - `ldappasswd` qui permet de crypter un mot de passe
  - `gq` qui est un client graphique

Le choix d'un schéma

- le choix des classes d'objet et des attributs (il est préférable de partir d'un schéma standard et d'ajouter des classes qui héritent des classes standards).
- le choix du nommage des entrées (influence l'organisation de l'accés, du contrôle, de la répartition et de la duplication)
  - Un arbre plat sera plus efficace, mais moins facile à gérer
  - Un arbre avec une branche par catégorie d'objet facilitera la gestion des droits d'acces
  - Un arbre avec une branche par entité dans l'entreprise facilitera la duplication ou la répartition
- le choix de l'attribut pour le DN (assurer l'unicité)
- le choix du suffixe (on utilise le nom de domaine dc=univ-artois, dc=fr)

La topologie de l'annuaire

- La répartition consiste à placer les données de l'annuaire sur plusieurs serveurs.



La topologie de l'annuaire

- La duplication consiste à copier une partie ou toutes les données de l'annuaire sur un autre serveur.