Gestion d'Annuaires d'Entreprises

Systèmes d'Information et Management
(SIMAN)
saglio@enst.fr

1

Vocabulaire *(Petit Robert)*

- Catalogue: "liste méthodique accompagnée de détails, d'explications" (alias **Guide, Dictionnaire...**)
  - *catalogue d'objets (organisations, services…)*
- Répertoire : "inventaire méthodique (liste, table, recueil) où des matières sont classées dans un ordre qui permet de les retrouver facilement" (english: **directory**)
  - *répertoire d'adresses*
- Annuaire: "recueil publié annuellement, contenant des renseignements variables d'une année à l'autre"
  - *annuaire des Téléphones*

2

1e partie

Les annuaires électroniques
au standard LDAP

3

annuaires électroniques

- collection typée d'entités: **"entrées d'annuaire"**
  - personnes, organisations, ressources ou services
- méthodiquement organisée (stockage, accès)
  - liste à plat ou hiérarchisée pour **navigation rapide**
- mise à jour peu fréquente / taux de consultation
  à l'opposé des systèmes transactionnels !
- fractionnable, réplicable, distribuable
  - en vue d'un accès réseau standard et rapide
- d'accès contrôlé selon l'identité du demandeur

4

standard X.500

- CCITT 1988
  - Open Systems Interconnection - Directory Services
  - ISO 9594 – X.500+X.501,509,511,518,520,521,525 - 1990
  - profonde révision en 1993, mais échec en pratique
- DAP (Directory Access Protocol) couche applicative (API) au-dessus d'une pile OSI complète
- modèle objet, puissant langage de requête
- trop complexe, lourd pour les petites applications

5

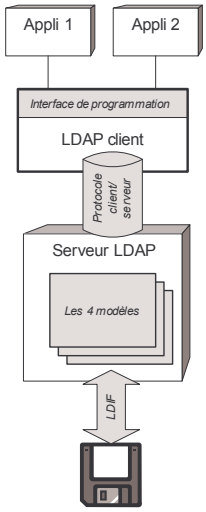
standard LDAP

- A l'origine un frontal pour X.500 sur TCP/IP
- Standard IETF LDAP
  - v1 : RFC 1487 « X.500 Lightweight Directory Access Protocol. », juillet 1993
  - v2 : RFC 1777, « Lightweight Directory Access Protocol. », mars 1995
  - v3 : RFC 2251-2256, déc. 1997 ; RFC 2228-2830, mai 2000 ; RFC 3377, sept. 2002

6

Ce que contient le standard

- Un protocole C/S basé sur tcp/ip
- Des modèles
  - Un modèle d'information - typage
  - Un modèle de nommage - organisation
  - Un modèle fonctionnel - services
  - Un modèle de sécurité
  - \+ Un modèle de réplication
- LDAP propose encore
  - API (C, Java, Perl, Python, PHP…)
  - LDIF Directory Interchange Format

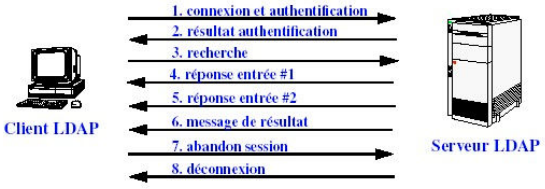


7

0. Protocole de communication

- Protocole de communication client-serveur

  Une **session** (ouverte/fermée/abandonnée) permet de faire passer plusieurs **requêtes** (interrogation ou mise à jour)



  - en mode asynchrone ou synchrone
  - avec le cas échéant renvoi sur un autre annuaire - par « referral »
- Le protocole a été défini très formellement

  dans la RFC 1777 en utilisant ASN.1 (Abstract Syntax Notation) et le codage par BER (Basic Encoding Rules)

8

1.Le modèle d'information

- Il définit le type de données pouvant être stockées dans l'annuaire
  - entrée = contient les informations sur un objet de l'annuaire
  - information = {**attribut** (nom, **syntaxe**), valeur}
  - les objets de mêmes attributs sont regroupés par **classes**
  - **schéma** = liste des classes, attributs, syntaxes...
- modèle de typage
  plutôt que modèle objet au sens plein

9

Modèle de typage

- OID associé à chaque classe d'objet, type d'attribut, "syntaxe" (~domaine) d'attribut, règle de comparaison d'attributs..
- Héritage simple entre classes et entre attributs
- **CLASSES**(OID, NAME, DESC, OID_SUP, TYPE, {OID_ATT_MUST}, {OID_ATT_MAY})
- **ATTRIBUTS**(OID, NAME, DESC, OID_SUP, OID_EQUALITY, OID_ORDERING, OID_SUBSTR, OID_SYNTAX, SINGLE_VALUE, COLLECTIVE, NO_USER_MODIF, USAGE)
- **SYNTAXE** IN ('binary', 'boolean', 'Distinguished Name', 'directory string', 'integer', 'telephone number', ...)
  - une 30aine au total cf. RFC 2256

10

Types d'attributs

- Pour définir un type d'attribut, il nous faut :
  - décider s'il est mono ou multi-valué
  - lui donner une syntaxe prédéfinie (ex. tel)
    = format (ex.texte) + règles de comparaison (ex. telephoneNumberMatch)
  - éventuellement, le faire hériter d'un autre type d'attribut
- Deux familles d'attributs
  - attributs **utilisateur**, manipulés par les clients
  - attributs **opérationnels**, utilisés par les serveurs

11

Exemples de déclarations de types d'attributs

- ```
  attributetype (  1.3.6.1.4.1.12274.1.1.1.5
    NAME 'enstDate'
    DESC 'Date ENST format YYYYMMDDHHMMSSZ ou
  YYYYMMDDZ'
    EQUALITY generalizedTimeMatch
    ORDERING generalizedTimeOrderingMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
    )
  ```
- ```
  attributetype (  1.3.6.1.4.1.12274.1.1.1.6
    NAME 'enstAdmissionDate'
    DESC 'Date de declaration de l entree'
    SUP  enstDate
    SINGLE-VALUE )
  ```

Exemples d'attributs utilisateur

AttributeType Desc	Attribute Type Name
CommonName	CN
LocalityName	L
StateorProvinceName	ST
OrganizationName	O
OrganizationalUnitName	OU
CountryName	C
StreetAddress	STREET
domainComponent	DC
Userid	UID

Tableau 1 : Exemple d'attributs d'une entrée

type d'attribut	valeur d'attribut
cn:	Barnabé Dupond
uid:	bdupond
telephonenumber:	+33 (0)1 2345 6789
mail:	Barnabe.Dupond@acme.com
roomnumber:	C105

13

Attributs opérationnels

- signatures : *createTimestamp, creatorsName, modifyTimestamp, modifiersName*
- dans la classe *subschema* : liste des classes *objectClasses*, liste des attributs *attributeTypes*, liste des règles de comparaison *matchingRules*, liste des attributs qui utilisent une règle *matchingRuleUse*
- DN d'objet de type subschema : *subschemaSubentry*
- contextes (DN de racines d'arbre LDAP) supportés: *namingContexts*
- URL d'autres serveurs d'annuaire LDAP: *altServer*

14

Classe

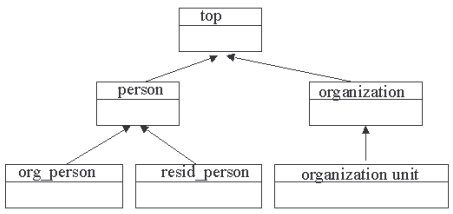
- Une classe
  - est constituées d'attributs
    - obligatoires MUST ou optionnels MAY
  - est typée
    - structurelle {attributs MUST, MAY} , auxiliaire (ne contient que des attributs MAY) ou abstraite (sans instance)
  - s'inscrit dans un arbre d'héritage de classes
    (à partir de *top*)
- LDAP définit des classes d'après X.500
- On peut en fabriquer de nouvelles !

15

Arbre d'héritage des classes des RFC 2256 et 2798

- top
  - alias
  - country
  - locality
  - organization
    - organizationalUnit
  - person
    - organizationalPerson
      - inetOrgPerson
    - residentialPerson
  - organizational role
  - groupOfName
  - ...

Héritage entre classes



Exemple de classes

- inetOrgPerson

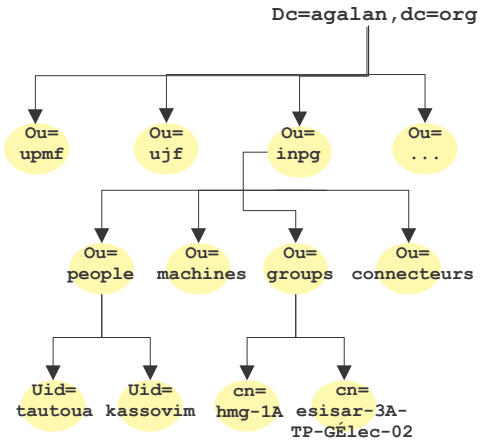
```
objectclass ( 2.16.840.1.113730.3.2.2
    NAME 'inetOrgPerson'
    SUP organizationalPerson
    STRUCTURAL
    MAY (
        audio $ businessCategory $ carLicense $ departmentNumber $
        displayName $ employeeNumber $ employeeType $ givenName $
        homePhone $ homePostalAddress $ initials $ jpegPhoto $
        labeledURI $ mail $ manager $ mobile $ o $ pager $
        photo $ roomNumber $ secretary $ uid $ userCertificate $
        x500uniqueIdentifier $ preferredLanguage $
        userSMIMECertificate $ userPKCS12
    )
)

-- syntaxe LDAPv3
```


2.Le modèle de nommage

- Organisation: ranger les entrées dans une structure logique hiérarchique
  - Directory Information Tree (DIT)
    *N.B. c'est un arbre de **nommage**, ce n'est pas un arbre de stockage/placement mémoire*
- Identification: les nommer de façon distincte
  - RDN = Relative Distinguish Name
  - DN = [full] Distinguish Name

Directory Information Tree



- Au sommet l'entrée racine ou "Suffix" ou "BaseDN"
- Les noeuds sont les entrées = racines de sous-arbres
(DSA Specific Entries)

DIT et espace de nommage

- un serveur LDAP peut gérer plusieurs DIT (plusieurs espaces de nommage)
- chaque DIT est décrit (LDAPv3) dans une entrée opérationnelle spécifique (rootDSE)
- l'organisation du DIT est un libre choix de l'administrateur de l'annuaire :
  - peu profond = maintenance facile + peu sémantique
  - profond = plus sémantique + maintenance difficile

DN & RDN

- DN (Distinguished Name)
  - référence unique d'une entrée (// full path name Unix)
  - formé d'une suite de RDN séparés par des ","
- RDN (Relative Distinguished Name)
  - attribut du RDN à choisir pour que tout DN soit unique (Penser aux déplacements éventuels dans le DIT !)
  - exemples:
    - uid=saglio
    - ou=infres
    - o=enst, c=fr

3.Le modèle fonctionnel

- Définit les opérations que l'on peut effectuer sur l'annuaire :
  - Connexion au serveur
  - Déconnexion du serveur
  - Recherche d'entrées
  - Modification d'une entrée
  - Abandon des opérations en cours
  - « Extended Operations »

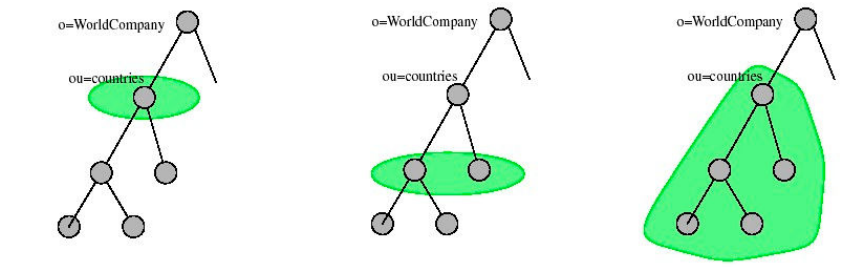
Opérations de lecture

- Recherche, paramètres:
  - base object (DN)
  - scope
  - derefAliases
  - sizeLimit
  - timeLimit
  - typesOnly
  - filter
  - attributes
- Comparaison, paramètres :
  - Entrée à comparer (DN)
  - Liste d'atributs avec leurs valeurs
  - OK si les attributs sont de valeurs comparables

```
LDAPResult ::=
    SEQUENCE {
        resultCode      ENUMERATED {
                            success                      (0),
                            operationsError              (1),
                            protocolError                (2),
                            timeLimitExceeded            (3),
                            sizeLimitExceeded            (4),
                            compareFalse                 (5),
                            compareTrue                  (6),
                            authMethodNotSupported       (7),
                            strongAuthRequired           (8),
                            noSuchAttribute              (16),
                            undefinedAttributeType       (17),
                            inappropriateMatching        (18),
                            constraintViolation          (19),
                            attributeOrValueExists       (20),
                            invalidAttributeSyntax       (21),
                            noSuchObject                 (32),
                            aliasProblem                 (33),
                            invalidDNSyntax              (34),
                            isLeaf                       (35),
                            aliasDereferencingProblem    (36),
                            inappropriateAuthentication  (48),
                            invalidCredentials           (49),
                            insufficientAccessRights     (50),
                            busy                         (51),
                            unavailable                  (52),
                            unwillingToPerform           (53),
                            loopDetect                   (54),
                            namingViolation              (64),
                            objectClassViolation         (65),
                            notAllowedOnNonLeaf          (66),
                            notAllowedOnRDN              (67),
```

23

Scope



search base = "ou=countries,o=WorldCompany"

search scope = base	search scope = onelevel	search scope = subtree

Filtres de recherche RFC 2254

- Type de recherche d'entrées :
  - égalité, sous-chaîne, approximation, plus grand/petit ou égal, présence...
- Opérateurs de combinaison des filtres
- opérateurs: = ~= >= <= | & !
- (opérateur(assertion)(opérateur(assertion)))

ex: **(&(objectClass=person)(!(telephoneNumber=*)))**

- Limitation à la lecture des seuls attributs autorisés
- Le résultat peut être une référence vers un autre serveur

25

LDAP URL

exemples:

ldap://ldap.enst.fr/ou=People,dc=enst,dc=fr??one?cn=Jean-Marc Saglio

- RFC-1959

syntaxe : ldap[s]://<hostname>:<port>/<base_dn>?<attributes>?<scope>?<filter>

<base_dn> : DN de l'entrée qui est le point de départ de la recherche
<attributes> : les attributs que l'on veut consulter
<scope> : la profondeur de recherche dans le DIT à partir du <base_dn>
- base : s'arrête au niveau courant (par défaut)
- one : descend d'un niveau
- sub : parcourt tous les sous-niveaux

<filter> : filtre de recherche, par défaut (objectClass=*)

26

Opérations de modification

- Modification - modify- d'une entrée
  - Paramètres de la modification
    - Object à modifier (DN)
    - Liste d'opérations sur les attributs
      - type d'opération
        - » ajout
        - » suppression
        - » remplacement
      - type d'attribut
      - valeurs

Opérations de modification

- Ajout - add - d'une entrée
  - Paramètres de l'ajout :
    - DN souhaité pour l'entrée
  - Liste d'attributs et valeurs (conforme au schéma)
  - un parent doit préexister
- Suppression - delete - d'une entrée
  - Seul paramètre : le DN de l'entrée à supprimer
  - Ne peut être utilisé que pour les feuilles du DIT

autres opérations

- Modification du DN d'une entrée
  - changer le RDN sans changer de place
  - Déplacement de l'entrée avec/sans modif RDN
  - N'est pas faite pour le déplacement entre serveurs
- « Extended Operations »
  - Permettent des opérations prévues ou non dans les RFC
  - Chaque opération doit être enregistrée sous un OID
  - Exemple :
    - TLS avec opération « start TLS »

N.B. TLS, standing for Transport Layer Security, is the latest version of SSL. It is an enhancement of SSL version 3.0 (see RFC2246).

4.Le modèle de sécurité

- La sécurité se fait à plusieurs niveaux :
  - par le *chiffrement* des transactions entre clients et serveurs ou entre serveurs LDAPv3 :

    SSL (ldaps) ou TLS (startTLS extended operation)
  - par l'*authentification* pour se connecter au service,
    - anonymous
    - DN+password en clair
    - SASL (p.ex. avec Kerberos), SSL ou TLS pour l'authentification par certificat
  - par un modèle de *contrôle d'accès* aux données,

Contrôle d'accès

- droits (lecture, écriture, recherche, comparaison)
- attachés à des entrées, à la racine, au sommet d'un sous-arbre
- effet sur l'entrée entière ou certains attributs
- s'appliquent à des individus, groupes, adresses IP, noms de domaine, jours-heures
- non encore standard : OpenLdap <> Netscape

31

Access Control Lists

- Expression générique des ACLs :

```
<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 :

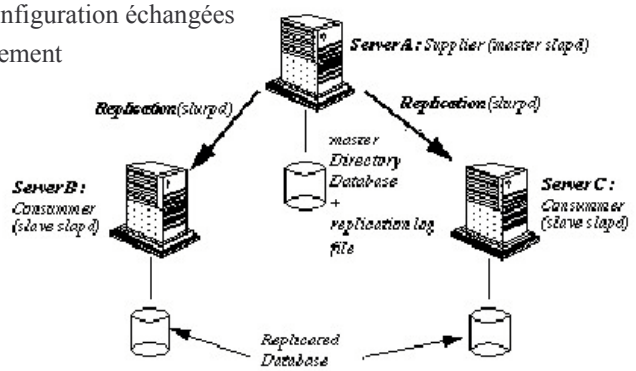
```
access to * by self write
      by * read
```

5.Le modèle de réplication

- pas encore standard IETF, **LDUP** en préparation
- but: QoS (proximité, performance, disponibilité)
- en pratique: supplier/consumer servers

  informations de configuration échangées

  = replication agreement



Méthodes de réplication

- On peut répliquer
  - 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 réplique que les objets de type personne »
    - « on ne réplique que les attributs non confidentiels » (annuaire interne vs. annuaire externe)
- Plusieurs manières de synchroniser les serveurs :
  - mise à jour totale / mise à jour incrémentale…
  - en temps réel ou à l'heure prévue
- Plusieurs stratégies de réplications :
  - single-master / multiple-master replication
  - les serveurs doivent tous utiliser le même schéma
  - les régles d'accès aux données répliquées doivent être répliquées

Aliases et Referrals

- deux objets abstraits permettant de pointer vers une autre entrée dans le même annuaire ou dans un autre
  - L'attribut `aliasObjectName` de l'objet `alias` a pour valeur le DN de l'entrée pointée.
  - L'attribut `ref` de l'objet `referral` a pour valeur l'URL LDAP de l'entrée désignée.
  - Les referrals sont traités au niveau du serveur en LDAP V2, par le client en V3

6.APIs

- En C
  - l'API d'OpenLDAP
  - Sun ONE Directory SDK for C
  - Netscape Directory SDK pour C
  - Innosoft LDAP Client Software Development Kit (ILC-SDK)
- En Perl
  - PerLDAP : librairie en C et Perl fournissant une API Perl d'accès à un annuaire LDAP
  - Net::LDAPapi : ancienne librairie Perl remplacée par PerLDAP
  - Perl-LDAP : librairie Perl avec API orientée objet
- En Java
  - Netscape Directory SDK pour Java
  - Sun ONE Directory SDK for Java
  - Java Naming and Directory Interface (JNDI), de SUN : API Java multi-annuaires (NIS, DNS, LDAP,...)
  - JLDAP : classes LDAP Java, contribution de Novell pour OpenLDAP
- Autres
  - Extensions LDAP de PHP3 : API LDAP pour le langage de script PHP
  - Python-LDAP : API LDAP pour Python (en développement)
  - DSML : représentation XML des entrées ou des réponses aux requêtes

sous Unix: **ldapsearch -h ldap.enst.fr -b "ou=People,dc=enst,dc=fr" -s "one" "cn=Jean-Marc Saglio"**

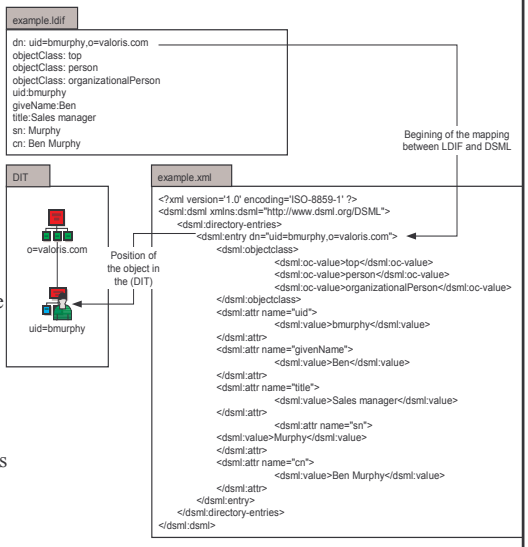
7.LDAP Interchange Format (LDIF)

- export/import/modification
- fichier ASCII+codage base64
- Exemple d'entrée listée:

```
dn: cn=Jean-Marc Saglio,mail=saglio@enst.fr
cn: Saglio, Jean-Marc
sn: Saglio
givenname: Jean-Marc
objectclass: top
objectclass: person
locality: Paris 13
mail: saglio@enst.fr
title: Directeur d'études BD et SI
postOfficeBox: 46, Rue Barrault
streetaddress: 75634 PARIX Cedex 13
postalcode: 75634
telephonenumber: 01 4581 8062
facsimiletelephonenumber: 01 4581 3119
homephone: 01 6931 2355
o: ENST
```


Introduction à DSML

- Directory Services Markup Language, basé sur XML,
  - Microsoft, Novell, SunONE, Oracle, IBM, Oblix, Calendra, etc.
- DSML v1
  - Standard XML : schéma et données
  - Utilisé pour l'import et l'export des données
- DSMLv2
  - Standard XML : requêtes LDAP V3
  - Utilisé pour s'authentifier, lire et écrire dans un annuaire via les Web Services (SOAP, HTTP, etc.)
- Usage et apports
  - Intégration avec des applications non LDAP mais XML
  - « Parsers » gratuits, réduction des coûts d'intégration
  - Flexibilité en cas de changement du modèle de données



Bibliographie LDAP, DSML

- http://www.openldap.org
- http://www.cru.fr/ldap/
- **FORMATION DÉPLOIEMENT AGALAN - 13 et 14 février 2003 - « Survol de LDAP » - INP Grenoble, Éric Simoëns**
- http://www.int-evry.fr/mci/user/procacci/ldap/
- http://www.cs.rpi.edu/~hollingd/netprog/notes/ldap/ldap.ppt
- http://www.oasis-open.org/committees/dsml/docs/DSMLv2.doc
- Marcel Rizcallah, "Construire un annuaire d'entreprise avec LDAP", Eyrolles, 2000
- http://www.infres.enst.fr/people/saglio/slides/ldap/ (Cours ENST 2000)

39

Performances comparées des serveurs LDAP

d'après UC Davis Tech Infrastruture Forum

Product	Bulk Load Time	Messaging Test with 1 Client	Messaging Test with 10 clients	Addressing (wildcard); test with 1 client	Addressing (wildcard); test with 10 clients	Search rate test with 1 client	Seach rate test with 10 clients	Modify test
	(record/sec)	(Operation/sec)	(Operation/sec)	(Operation/sec)	(Operation/sec)	(Operation/sec)	(Operation/sec)	(Operation/sec)
Novell NDS eDirectory for NT	0.8	321.7	333	86.7	93	318	464	6.6
I planet Directory Server	413.2	1,323	3,175	108.9	166	1,350	3,147	138
Innosoft IDDS	416.7	426	115.1	11.7	1.8	461	147	147.1
Critical Path Global Directory Server	47.6	373	670	5.1	3.8	370	651	77
Computer Associates eTrust Directory	5.2	94.3	101	3.6	3	162	108	3.4
Siemens DirX	3.1	4.3	30.1	4.9	12.3	5.1	19.24	12.9
Oracle Internet Directory	139	64	228	17	41	64	234	23
Microsoft Active Directory	33.3	915	1,536	2.6	11.6	999	2,199	27.7
Open LDAP	23.5	4.6	47.7	5.9	48.6	4.5	18.2	9.3

27 février 2003 http://tif.ucdavis.edu/ 40

2e partie

Les annuaires d'entreprise
intégration, méta-annuaire

41

Outils et responsabilités

- outils informatiques :
  - serveur de données multi-interfaces
  - portails intranet/internet avec sécurité
  - CD-ROM
- Responsabilités / qualité de l'information :
  - informations enregistrées par qui ?
  - informations certifiées par qui ?
  - service d'information assuré par qui ?

42

SGBD et/ou Annuaires

L'annuaire peut remplacer un SGBD traditionnel dans le cas de données simples, intensivement interrogées, distribuées à large échelle et utilisées par des multiples applications (fichier clientèle, catalogues de fournitures...).

Il peut épauler un SGBD, en étant synchronisé avec lui, pour faciliter la consultation des données ou la mise à jour de certains champs.

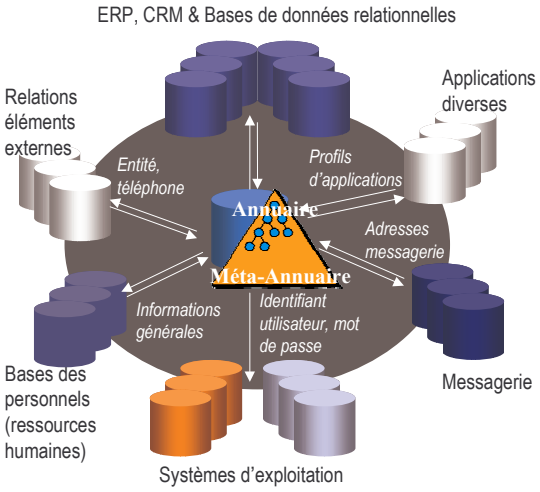
Parfois, l'organisation possède plusieurs bases de données déconnectées et gérant des informations redondantes :

- **la paye**
- **le bureau du personnel**
- **les comptes informatiques**
- **les badges d'accès**
- **les cartes de restaurants...**

Un annuaire LDAP peut fédérer les données communes (informations sur les employés), les données sensibles étant gérées dans les SGBD

=> Meta-Annuaire.

Les annuaires dans l'entreprise



La solution annuaire d'entreprise

- L'annuaire d'entreprise est le produit d'un ensemble d'annuaires et d'un méta annuaire
- L'annuaire d'entreprise centralise l'accès à l'information et synchronise les processus **en un point unique** entraînant ainsi :
  - Une meilleure productivité
    - Simplification des méthodes de travail
    - Qualité de service
  - Une économie des coûts de gestion
  - Une information sécurisée
  - La présence d'un socle applicatif fiable

L'annuaire d'entreprise – l'annuaire

Les Annuaires stockent les informations :

- Données statiques à faible taux de mise à jour
- Objets et attributs
  - Définis par un schéma
  - Organisés en arborescence (DIT : *Directory Information Tree*)
- Accessible des utilisateurs et des applications au travers des interfaces selon des règles définies (ACL : *Access Control List*)

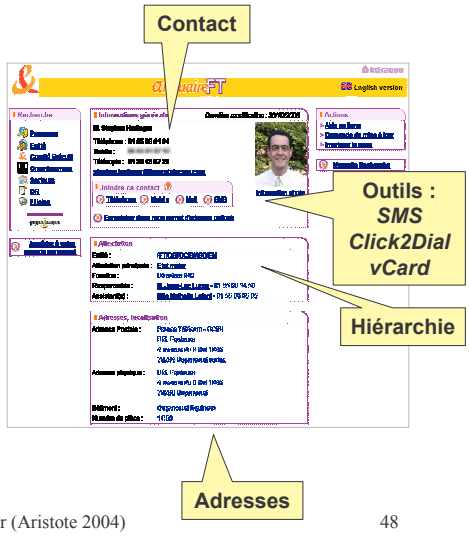
La définition des *règles du jeu* rendent l'accès à ces informations entièrement maîtrisables et contrôlés

L'annuaire d'entreprise – le méta annuaire

- ***Le méta-annuaire synchronise les informations :***
  - Processus automatisés d'échanges entre l'annuaire et les sources d'information
  - Règles de synchronisation paramétrables
- Il **récupère** dans les sources, les données propriétaires dont il vérifie la cohérence et vraisemblance pour alimenter l'annuaire
- Il **propage** les informations de l'annuaire vers les consommateurs (règles de synchronisation descendantes)

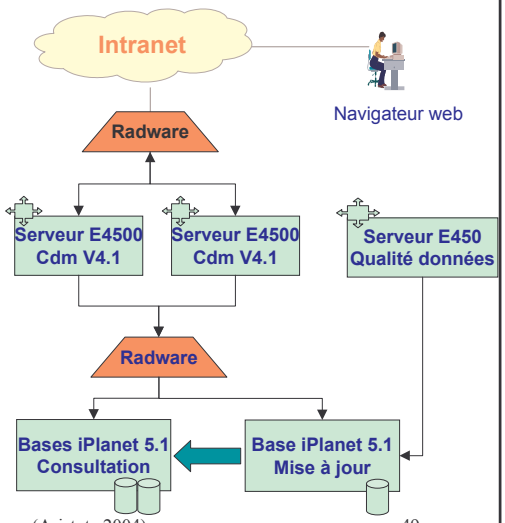
Ex: Annuaire interne FT

- Contenu
  - 150.000 personnes
  - dont 60% avec photo
- Activité
  - > 3 millions de consultation / mois
  - > 50.000 modifications / mois
- Services offerts
  - Recherche phonétique
  - Recherche téléphonique inversée
  - Organigramme
  - Envoi de SMS
  - vCard
  - Click2Dial
- Accessible en :
  - HTML, WAP, LDAP



Architecture de l'annuaire FT

- Matériel
  - 2 serveurs SUN E4500 4CPU
  - Radware: Répartiteur de charge réseau
- Annuaire
  - 1 annuaire iPlanet 5.1 maître
  - 2 annuaires iPlanet 5.1 de consultation
- Application Intranet
  - Calendra Cdm v4.1
  - Serveur Web Apache
- Supervision
  - BMC Patrol

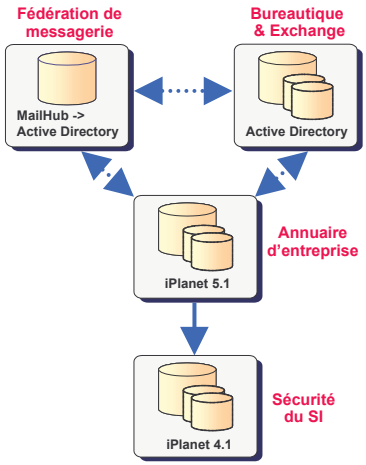


Mise à jour de l'annuaire FT

- Un réseau de correspondants
  - Saisie assurée par 450 correspondants nommés toutes les entités
  - Processus de saisie suivant au plus près les processus RH de mobilité
- Des imports/exports d'annuaires
  - Échanges de fichiers avec les filiales
  - Problématique de qualité de données (contrôle de champs, contrôle de doublons…)
  - Problématique de mise à jour massive de l'annuaire lors des imports :
    - Suppression des anciennes données
    - Insertion des nouvelles donnes
    - État transitoire à gérer : mécanisme de pré-production et synchronisation à J+1
- Un contrôle qualité permanent
  - Un tableau de bord QoS mensuel très détaillé
  - Une équipe dédié « qualité de données » et des outils d'audit permanent
    - Format des champs, doublons…
    - Format et taille des photos…

Synchronisation entre annuaires

- Synchronisations
  - Entre annuaires LDAP
  - En batch, à J+1
- Outil de synchronisation
  - Utilisation de Perl_LDAP
  - Excellent produit !
  - Peut travailler indifféremment sur un annuaire LDAP ou des fichiers LDIF
  - Performant et stable
- Évolution vers un méta-annuaire
  - Évolution envisagée vers Microsoft MIIS



Problématique d'intégration

- multiples applications (données, fonctions, topologie)
- multiples sources (données, fonctions, topologie)
- standard intégrateur: LDAP (modèles, API)
- problèmes classiques de l'intégration :
  - schéma fédéré des objets
    - ne créer de nouvelles classes que par héritage / standards
    - DIT à branchage faible
  - topologie multi-serveurs
    - localisation au plus près des resp. des mises à jours
    - réplication (perf, répartition des charges, disponibilité)

3e partie

Les annuaires intégrés
pour le service de gestion d'identité

53

Définitions

"Digital identity comprises electronic records that represent network principals[2], including people, machines, devices, applications, and services." [1]

"Identity Management (IdM) comprises the set of business processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities within a legal and policy context." [1]

1 "Enterprise Identity Management: It's About the Business", V1, July 2, 2003, Burton Group Research Overview

2 traduisez: agents

54

Une identité, plusieurs attributs

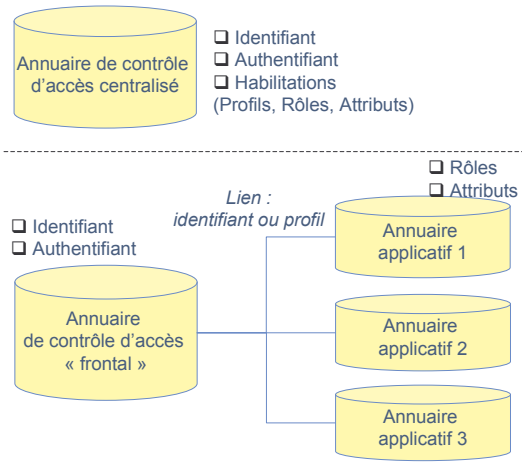
- identité universelle le DN
- autres identités selon les applications :
  - UID, email, tél, #SS, … (annuaires “inversés”)
- localisations géo, org, ...
- autres attributs de recherche (compétences…)

  > annuaire externe ou interne **pour les “humains”**
- rôles {droits}, profils
- clés d’authentification, certificats

  > annuaire interne **pour les “machines”**

55

2 scénarios d’organisation des informations de contrôle d’accès



Avantages	Inconvénients
❑ Facilité d’administration ❑ Homogénéité des informations	❑ Risque de sécurité (possibilité d’accéder à l’ensemble des informations contenues dans l’annuaires)
❑ Deux niveaux de contrôle ❑ Localisation différente des annuaires dans l’espace de confiance	❑ Synchronisation des informations entre les annuaires ❑ « Gestion locale » des droits applicatifs

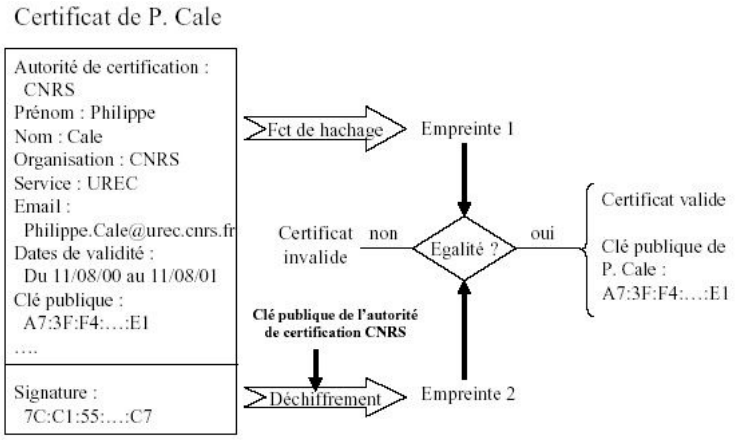
Authenti(fi)cation

- prouvez que vous êtes qui vous prétendez!
- chiffrement/déchiffrement asymétrique
  - du texte à vous destiné que vous lirez avec votre clé privée
  - de ma signature (empreinte dans mon texte) que vous authentifierez avec ma clef publique
- certification des informations d'annuaire
  - en particulier de la clef publique

  (**P**ublic **K**ey (**I**nfrastructure) de **G**estion des **C**lés)
  - enregistrement, certification, publication

57

PKI-IGC



58

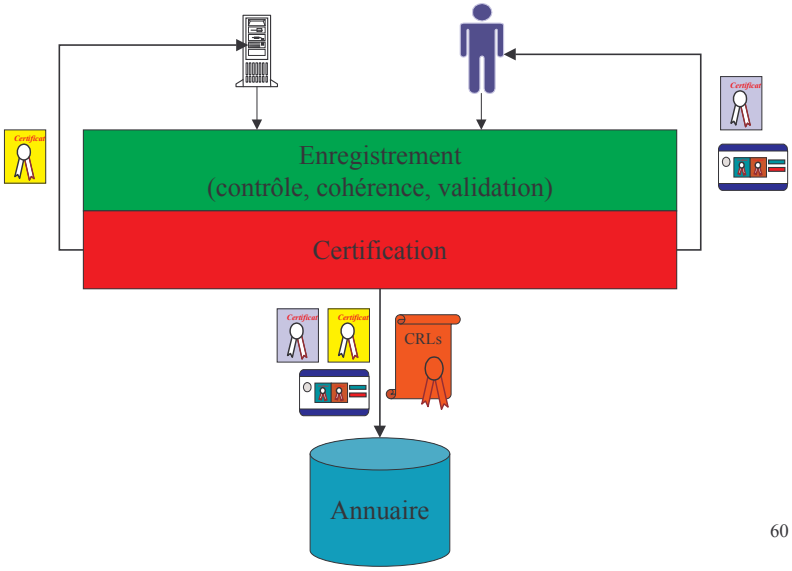
Ex: l'annuaire « Carte Personnel Santé »

Le GIP «CPS» est chargé de répondre aux exigences d'identification et de sécurité dans le monde sanitaire et social en assurant le rôle d'une tierce partie de confiance (Autorité d'Enregistrement, Autorité de Certification).

Opérationnellement, il offre trois services aux Professionnels de Santé :

- un service d'enregistrement de demande;
- un service de certification;
- **un service de publication : annuaire CPS**.

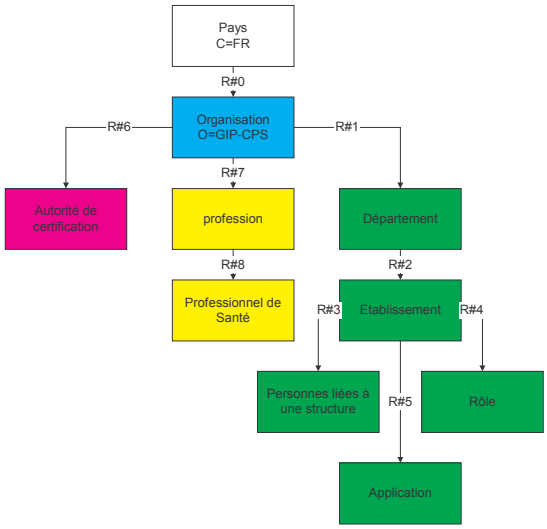
Rôle de l'annuaire CPS



Usage de l'annuaire CPS

- Messagerie sécurisée
  - Signature
  - Confidentialité
- Serveur Web
  - Authentification
  - Intégrité

Schéma : global



Interface d'accès

- Interface LDAP
  - Accès à la partie publique de l'annuaire
- Interface LDAP/S
  - Accès réservé, avec authentification mutuelle
- Passerelle HTTP/LDAP
- Synchronisation / réplication
- Import / export

Bibliographie IGC\IdM

- Calendra - http://www.calendra.com
  Identity Management
- Valoris - http://www.valoris.com/
- Dictao - http://www.dictao.com/
- Unité réseaux du CNRS - http://www.urec.cnrs.fr/
  - http://www.urec.cnrs.fr/igc/Certifs_CNRS.html