Administration système Avancée

Christophe Gouinaud
ISIMA

Plan

- Nommage
- Partage
- Notions Transverse : Interopératibité, architecture, communication et sécurité

Partie I : Nomage

- Des machines
  - Résolution d'adresse IP
  - Trouver des services
- Des gens
  - Annuaire => Login
  - Mots de passe
- Des organisations
  - Unité d'organisation
  - Fillialisation

Architecture de nomage

Unix :

- Machine DNS
- NIS
  - LOGIN/passwd
  - Service
  - Hosts
  - Aliase mail
  - ...

Microsoft(Active Directory)

- DNS
  - Machine
  - Serveur (KDC)
- LDAP
  - Personne
  - objet
- Kerberos
  - Authentification

DNS

- Annuaire mondiale du nomage IP
- Utilisation classique :
  - Traduction nom vers IP
  - Traduction IP vers Nom
- Utilisation avancé :
  - Champ MX
  - Avec un serveur d'annuaire

DNS :Utilisation classique

- Interrogation directe
  - Recherche des serveurs champs NS
  - Recherche hiérarchique
  - Intérogation du serveur primaire puis des secondaires
- Interrogation inverse (ex 193.55.95.1)
  - Recherche dans la zone racine de inet-darpa.
  - Rechercha dans la 95.55.193.inet-darpa.

Exemple DNS:

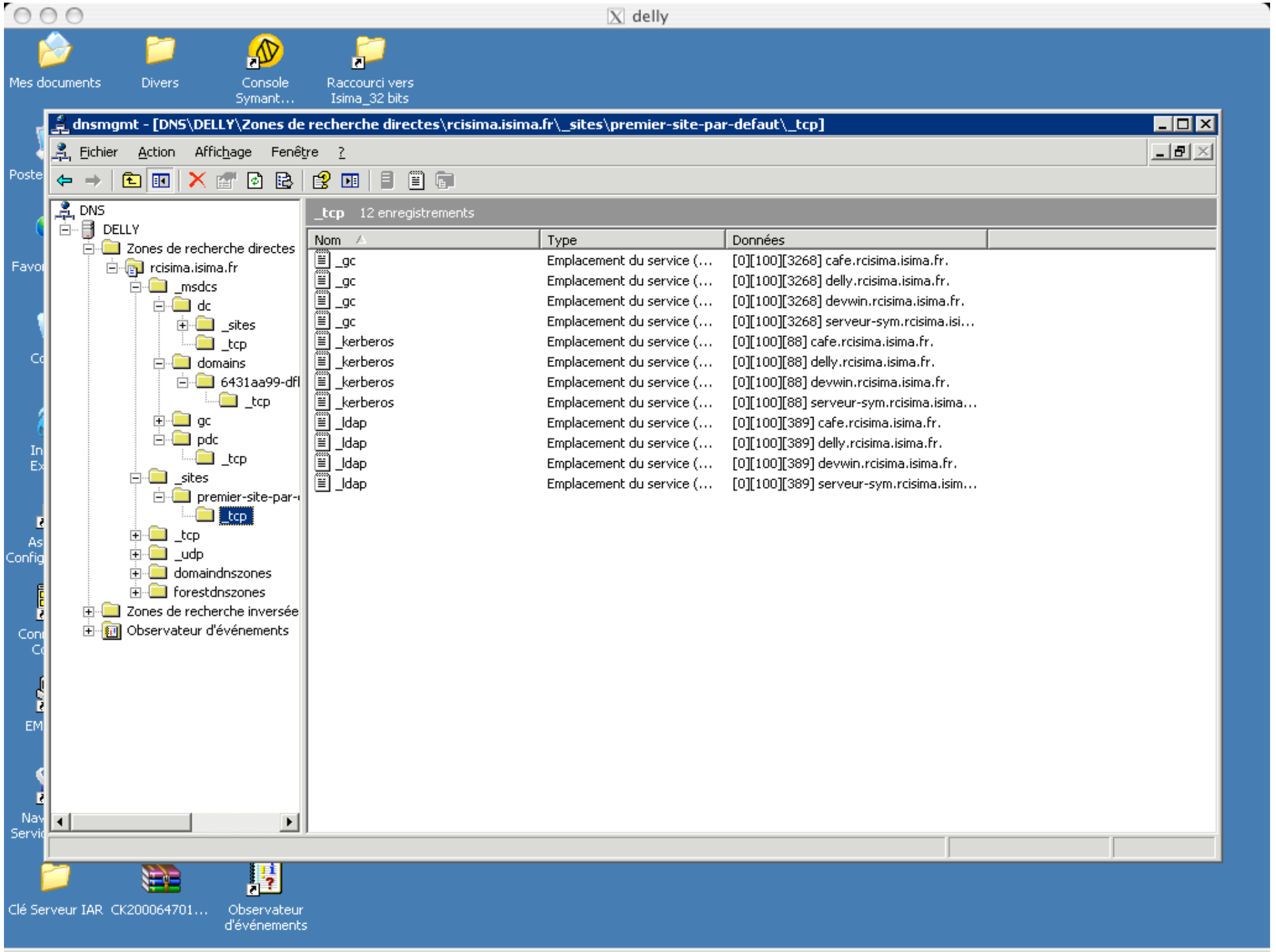
```
bash-3.2$ nslookup
> sp.isima.fr
Server:         212.27.40.242
Address:        212.27.40.242#53

Non-authoritative answer:
Name:   sp.isima.fr
Address: 193.55.95.1
> set q=ns
> isima.fr.
Server:         212.27.40.241
Address:        212.27.40.241#53

Non-authoritative answer:
isima.fr        nameserver = sp.isima.fr.
isima.fr        nameserver = ns2.nic.fr.

Authoritative answers can be found from:
sp.isima.fr     internet address = 193.55.95.1
ns2.nic.fr      internet address = 192.93.0.4
> exit
```

DNS : utilisation avancée

Ajout de champ :

- Pour information : propriétaire
  Email du gestionnaire
- Pour une application particulière : NS
  connaître son environnement
- Pour désigné un service : MX
  trouver le serveur smtp

Certain en abuse 


delly
Mes documents
Divers
Console Symant...
Raccourci vers Isima_32 bits
dnsmgmt - [DNS\DELLY\Zones de recherche directes\rcisima.isima.fr_sites\premier-site-par-defaut_tcp]
Fichier Action Affichage Fenêtre ?
DNS
DELLY
Zones de recherche directes
rcisima.isima.fr
_msdcs
dc
_sites
_tcp
domains
6431aa99-dfl
_tcp
gc
pdc
_tcp
_sites
premier-site-par-
_tcp
_tcp
_udp
domaindnszones
forestdnszones
Zones de recherche inversée
Observateur d'événements
_tcp 12 enregistrements
Nom
Type
Données
_gc Emplacement du service (... [0][100][3268] cafe.rcisima.isima.fr.
_gc Emplacement du service (... [0][100][3268] delly.rcisima.isima.fr.
_gc Emplacement du service (... [0][100][3268] devwin.rcisima.isima.fr.
_gc Emplacement du service (... [0][100][3268] serveur-sym.rcisima.isi...
_kerberos Emplacement du service (... [0][100][88] cafe.rcisima.isima.fr.
_kerberos Emplacement du service (... [0][100][88] delly.rcisima.isima.fr.
_kerberos Emplacement du service (... [0][100][88] devwin.rcisima.isima.fr.
_kerberos Emplacement du service (... [0][100][88] serveur-sym.rcisima.isima...
_ldap Emplacement du service (... [0][100][389] cafe.rcisima.isima.fr.
_ldap Emplacement du service (... [0][100][389] delly.rcisima.isima.fr.
_ldap Emplacement du service (... [0][100][389] devwin.rcisima.isima.fr.
_ldap Emplacement du service (... [0][100][389] serveur-sym.rcisima.isim...
Clé Serveur IAR
CK200064701...
Observateur d'événements

DNS : a quoi ça sert ?

DNS : architecture du service

- Trois types de serveurs :
  - Serveur maître
    source des données
  - Serveur secondaire
    copie du maître
  - Serveur feuille
    cache en interrogation
- Protocole UDP

DNS : Configuration client LINUX

- Fichier /etc/nsswitch.conf
  Ligne hosts : files dns
- Fichier /etc/resolv.conf
  search rcisima.isima.fr, isima.fr
  nameserver 172.16.64.249
  nameserver 172.16.32.249
  nameserver 193.55.95.1
- Test immédiat avec nslookup

DNS : architecture physique

Guideline : Au moins un serveur doit être disponible !!!!

- Au moins deux serveurs joignables sur chaque VLAN
- Serveur externe et interne différents
- Attention au problème électrique
- Attention aux fausses réplique

DNS : Quelques Trucs

- Manifestation des pannes !
  Le serveur nianianiark n'est pas ....
- Utilisés des forwarder
- Faire des sous zones pour active directory
- Mettre toutes les IP dedans !
- Attention au ligne intermitante
- Attention à l'ordre de démarages des services !

DNS : Configuration cache serveur

Configuration d'une cache :

- Répertoire /var/named
  Cache des information
- Fichier /etc/named.conf
  Indique le type de serveur et les info de démarage
- Fichier named.local
  permet la resolution inverse
- Fichier /etc/resolv.conf
  vers 127.0.0.1

DNS : fichier /etc/named.conf

```
/* Fichier /etc/named.conf */

options {
    directory "/var/named";
    forward only;
    forwarders {
        193.55.95.1;
        193.168.100.11;
    };
};

/*  cache */

zone "." {
    type hint;
    file "named.ca";
};

/* cache inverse */

zone "0.0.127.in-addr.arpa" {
    type master;
    file "named.local";
```

DNS cache seulement

Bind versions 9

DNS : configuration de master serveur

Semblable au cache mais :

- Fichier /var/named/mondomain
  définit par une régle type master
- Fichier /var/named/mondomain.rev
  précision suplémentaire
- Le mieux est de se reporter à ce tutorial
  http://www.linux-france.org/article/memo/dns/node1.html

Annuaire !

- Information stockée :
  - Information personnel
  - Information de sécurité
  - Stratégie
- Protocole utilisé :
  - NIS
  - LDAP en fait X500 light
    opendirectory, active directory

Annuaire II

- Les annuaires se distinguent :
  - Leurs utilisation
  - Leurs architecture
  - Leurs mode de remplissage
- Il ne faut pas confondre :
  - Identification
  - Et authentification

Authentification

- Local on utilise des fichier
  base de registre
  /etc/shadow sous linux
- Nis
  basé sur rpc sous UNIX
- Service spécifique
  - Kerberos
  - Radius

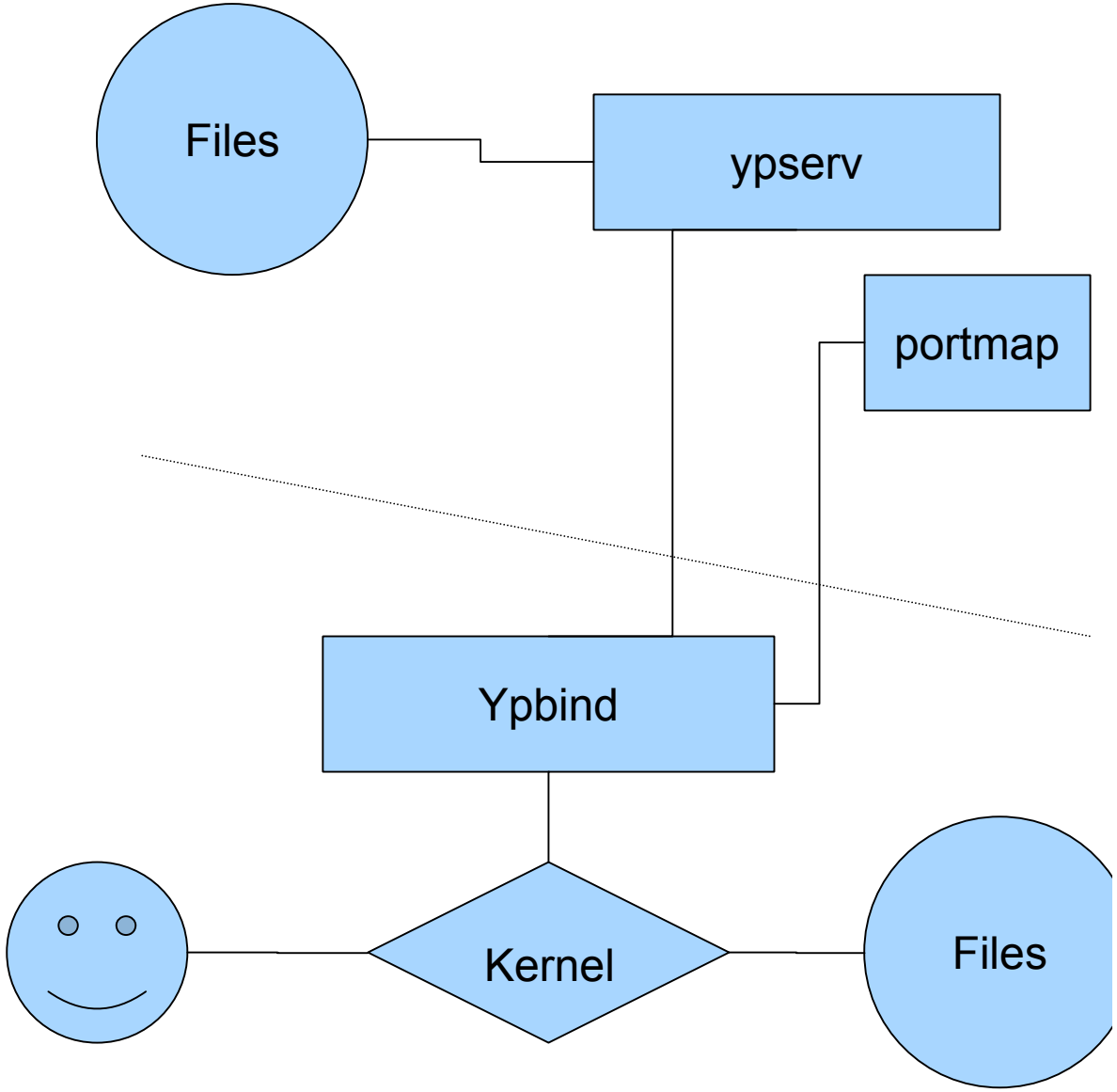
Auth : exemple client LINUX

- Fichier /etc/nsswitch.conf
  passwd : files nis
  shadow : files radius (ou nis)

- Comportement différents :
  - Nis authentification local
  - Radius authentification centralisé

Architecture de NIS

- Serveur maître ypserv
- Serveur esclave ypserv
- Client NIS ypbind
- Base sur rpc



Annuaire LDAP

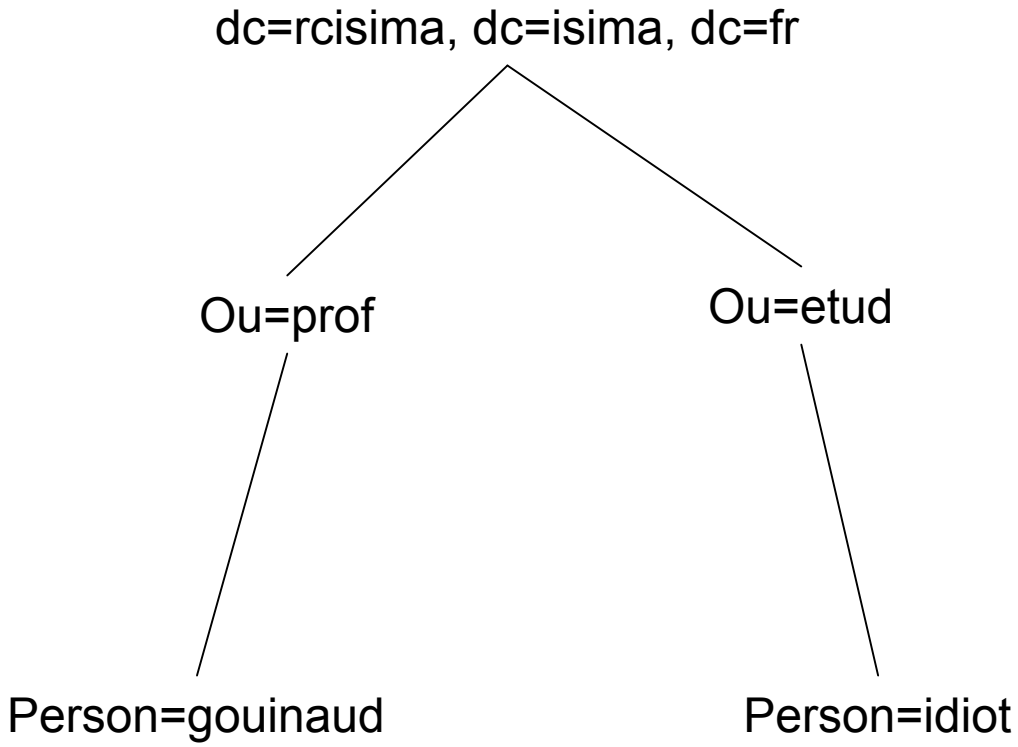
- Annuaire TCP/IP a la mode
- Modèle d’accès et de modifications
- Gestion du format des données
- Gestion des accès sécurisé
- Support de Active directory
- Orienté lecture rapide
- Stockage hiérarchique

Protocole LDAP

- Norme RFC2251
- Communication client/serveur
- Communication serveur/serveur
- Port 389/ldap et 636/ldaps
- Transport binaire BER (basic encoding rules)
- Protocole connecté en lecture et écriture
- Modification de la structure dans le protocole

Base de données LDAP

- DIT = directory information tree
- DES = directory service entry
- Objets = ce qui est stocké
  - Réel
  - Abstrait



Objets LDAP

- Les objets sont constitué d'attributs :
  - Nom
  - OID
  - Caractère mono ou multivarié
  - Syntaxe de la relation d'ordre
  - Usage
  - Format ou taille
- Les objets sont caractérisé par une liste d'attributs

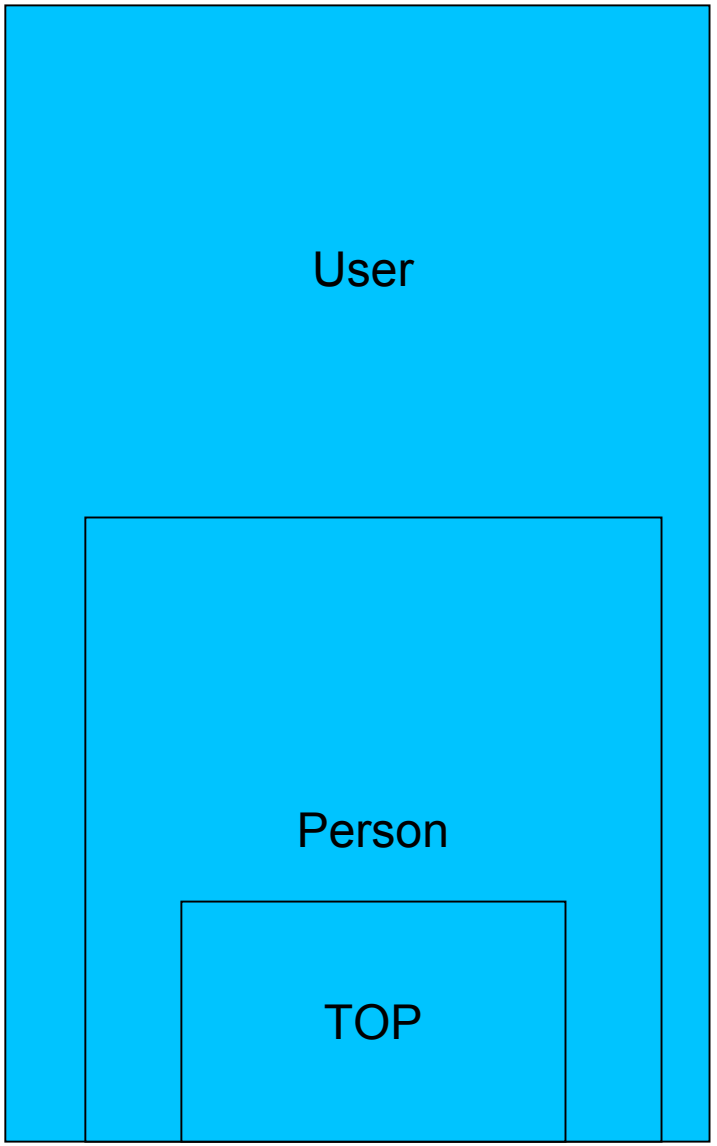
Objets LDAP(2)

On définit des classes d'objet :

- Un nom de classe
- Un OID
- Les atributs obligatoires
- Les atributs facultatif
- Un type
  - Structurel : objet réel basiques (personne, ou, …)
  - Auxiliaire : objet enrichissant une classe
  - Abstrait : élément du service (top)

Objets LDAP(3)

- Les objets sont imbriqué hiérarchiquement
- Top est la racine
- Cela facilite l’intérogation par la désignation d’une classe



Objets LDAP(4)

Les objets ont un OID (object indentifier) :

- Normalisé par l'IANA (RFC 2256)
- Séquence de nombre qui définit une classe
- Assure l'interopérabilité

```
objectclass person
 oid 2.5.6.6
superior top
requires        sn,         cn
allows          description,
seeAlso, telephoneNumber,
userPassword

person OBJECT-CLASS ::=
{   SUBCLASS OF top
MUST CONTAIN {commonName,surname}
MAY CONTAIN {description,
    seeAlso,telephoneNumber,
    userPassword}   ::= {objectClass 6}
```

Schéma LDAP

- Définition de la hiérachie d'objet
- Valable pour un serveur (non normalisé)
- Définitions des :
  - Classes
  - Type d'attribut
  - Syntaxe
- Ne pas confondre avec le DIT

Schéma LDAP et service LDAP

- Les serveurs publient le schéma
- Les serveur vérifie la conformité des entités créées
- On désigne les attributs par le DN (distinguish name) :
  uid=gouinaud, ou=prof, dc=rcisima, dc=isima, dc=fr

Stockage des bases et manipulations

- Le stockage n’est pas normalisé (dbm pour openldap)
- Le format LDIF :
  - Import/export de base
  - Modification
  - C’est un script ASCII
  - C’est le sql LDAP

Format LDIF stockage

dn: <distinguished name
objectClass: <object class
objectClass: <object class
...
<attribute type:<attribute value
<attribute type:<attribute value
...

```
dn: cn= Christophe gouinaud,
ou=prof, o= ISIMA, c= FR
objectClass: person
objectClass:
organizationalPerson
objectClass:
inetOrgPerson    cn:
Christophe Gouinaud    sn:
Rossi    givenName:
Christophe    mail:
gouinaud@isima.fr
userPassword:
{sha}CRYPTER    uid:
gouinaud    telephoneNumber:
0681192690    roomNumber:
A011
```

Format LDIF modification

dn: distinguished name
changetype <identifier
change operation identifier
list of attributes...
...
-
change operation identifier
list of attributes
...
<identifier :
add (ajout d'une entrée),
delete (suppression),
modrdn (modification du RDN),
modify (modification : add,
replace, delete)

dn: cn= Gouinaud Christophe, ou= Prof, o=ISIMA, c=FR
changetype: modify
add: telephonenumber
telephonenumber: 0681192690

dn: cn= Gouinaud Christophe, ou= Prof, o=ISIMA, c=FR
changetype: delete

Les opérations sur LDAP

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)

Emprunté sur : http://www-sop.inria.fr/members/Laurent.Mirtain/ldap-livre.html

Les requêtes

Deux type de requêtes search et compare :

Paramètre	Description
base object	l'endroit de l'arbre où doit commencer la recherche
scope	la profondeur de la recherche
derefAliases	si on suit les liens ou pas
size limit	nombre de réponses limite
time limit	temps maxi alloué pour la recherche
attrOnly	renvoie ou pas la valeur des attributs en plus de leur type
search filter	le filtre de recherche
list of attributes	la liste des attributs que l'on souhaite connaître

Emprunté sur : http://www-sop.inria.fr/members/Laurent.Mirtain/ldap-livre.html

Lecture des informations

- Routine search
- Nombreux opérateurs

Filtre	Syntaxe	Interprétation
Approximation	(sn~=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

Divers :

- Url ldap = Tentative de simplification :

  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" | "one" | "sub"
  <filter> : filtre de recherche, par défaut (objectClass=*)

  Bof

- DNS champ SRV

  _ldap._tcp.rcisima.isima.fr IN SRV 0 0 389 devwin.rcisima.isima.fr

Open LDAP

Suite libre qui implémente le protocole LDAP :

- Stockage dbm
- Daemon slapd
- Config dans /etc/slapd.conf
- Commande ldapsearch
- Librairie libldap.so.6
- Bien imergé dans php

Architecture d'annuaire

- Architecture logique
  Ex : personne
- Architecture physique :
  Ex : DNS
- Ne pas négliger l’un pour l’autre

Etape d’un projet d’annuaire

- Recensement de l’existant
- Enoncés des besoins
- Choix technologique
- Définitions de l’annuaire maître
- Définitions des héritages
- Création d’une maquette - test unitaire
- Déploiement

Recensement de l’existant

- Annuaire du personnel
- Répertoire téléphonique et Email
- Compte d’accès informatique
- Annuaire de contrôle d’accès
- Liste des bureau et clef
- Logiciel gérant des listes
- Personne gérant des listes de personnes

Ennoncés des besoins

- Qui sont les utilisateurs :
- Quel sont les système client
  - Ordinateurs
  - Contrôle d’accès
- Quel sont les applications clientes
  - Base de données
  - ERP
  - Intranet

Choix technologiques

- Liste des besoins par application
- Liste des annuaires existant
- Choix d’un annuaires maîtres
  - Celui qui fourni les clefs primaires
  - Le plus ouvert possible
- Eviter de bordélisé
- Le bon choix n’est pas forcément LDAP

Définitions de l’annuaire

- Définitions du schéma
- Définitions des règles d’accès
- Définitions des workflow de modification
- Pièges :
  - Faire trop hiéarchique
  - Mettre trop d’attribut dans les objets
  - Vouloir utilisé un seul système

Définitions des héritages

- Définir les règles de modification des annuaire esclave
- Mettre au point des outils automatique d’heritage
- Définir une stratégie de reprise
- Bloquer les systèmes de modification locaux d’attributs hérités

Création d’une maquette - test

- Implémenter l’annuaire maître
- Implémenter tout les annuaires esclave
- Implémenter toutes les procédures d’héritage
- Tester les recherches/ajout et modifications
- Tester les stratégie de reprise
- Tester les temps de convergences
- Astuces : utiliser des machines virtuels

Déploiement

- Former les personnes ressources technique
- Commencer le déploiement avec le mail
- Continuer avec les login
- Finir avec les applications métier
- Vérifier les systèmes de sauvegarde !

Partie II : stockage - partage

Rendre disponible les fichiers :

- A Bas niveaux => SAN (FC, ISCSI)
- Entre machine UNIX : NFS
- Entre machine Windows : CIFS
- Répartie :
  - DFS
  - LUSTRE
- En inter opérabilité : Samba

Partie III: Inter opérabilité

- Niveau d'inter opérabilité
- Niveau données
- Niveau Nomage
- Niveau Hardware
- Niveau applicatif