

# INTRODUCTION À LDAP

---

Jérôme Andrieu

# Sommaire

- Introduction sur les annuaires
- Généralités LDAP
- Usage
- Concepts/Administration
- HPC

# UN ANNUAIRE ?

---

Qu'est-ce qu'un annuaire ?



# Un annuaire

- Qu'est-ce qu'un annuaire ?
  - Une liste d'information organisée et régulièrement mise à jour.
  - Avec un index ?
- Exemples:
  - Annuaire du téléphone portable
  - Pages blanches/page jaunes
  - Liste de site web
  - Liste d'amis facebook
  - Base du personnel d'une entreprise
  - DNS
- Plus largement
  - Catalogue de produits
  - ...



# Un annuaire

- Annuaire administration de l'ENSIIE
- Liste d'entrées
  - Position
  - Nom
  - Fax
  - Téléphone

ACCUEIL	FAX	TÉLÉPHONE
<b>Standard</b>	01 69 36 73 05	01 69 36 73 50
<b>DIRECTION GENERALE</b>	FAX	TÉLÉPHONE
<b>Directeur</b>	SIDAHMED Ménad	01 69 36 73 27
<b>Directeur Adjoint</b>	IACOVELLA Andrea	01 69 36 73 27
<b>Assistante de direction</b>	AOUIOUICHE Ramla	01 69 36 73 27
<b>DIRECTION DU PILOTAGE ET DE LA QUALITÉ</b>	FAX	TÉLÉPHONE
<b>Directeur du pilotage et de la qualité</b>	IACOVELLA Andrea	01 69 36 73 27
<b>DIRECTION DES FORMATIONS ET DE LA RECHERCHE</b>	FAX	TÉLÉPHONE
<b>Directeur de la formation et de la Pédagogie</b>	BRUNEL Nicolas	01 69 36 73 27
<b>Directeur adjoint de la formation et de la pédagogie</b>	LIM Thomas	01 69 36 73 27
<b>Responsable du pôle Langues</b>	BOURARD Laurence	01 69 36 74 28
<b>Responsable de 1<sup>e</sup> année</b>	WATEL Dimitri	01 69 36 73 27
<b>Responsable de 2<sup>e</sup> année</b>	PULIDO NINO Sergio	01 69 36 73 43
<b>Responsable du S5</b>	LIM Thomas	01 69 36 74 22
<b>Responsable masters</b>	LY VATH Vathana	01 69 36 73 37
<b>Responsable parcours Mathématiques Appliquées</b>	CHEVALIER Etienne	01 69 36 73 27
<b>Responsable parcours Génie Logiciel</b>	BUREL Guillaume	01 69 36 73 27
<b>Responsable parcours Interactions Numériques</b>	ROUSSEL David	01 69 36 74 62
<b>Responsable parcours Calcul Intensif et</b>	DOSSANTOS- UZARRALDE Pierre	01 69 36 73 27
		01 69 36 73 71

# Un annuaire

- DMOZ (Directory Mozilla) <https://dmoztools.net/>

## Welcome!

*This site includes information formerly made available via DMOZ.*

Visit [resource-zone](#) to stay in touch with the community.

#OrganizeTheWeb



### Arts

Movies, Television, Music...



### Business

Jobs, Real Estate, Investing...



### Computers

Internet, Software, Hardware...



### Games

Video Games, RPGs, Gambling...



### Health

Fitness, Medicine, Alternative...



### Home

Family, Consumers, Cooking...



### News

Media, Newspapers, Weather...



### Recreation

Travel, Food, Outdoors, Humor...



### Reference

Maps, Education, Libraries...



### Regional

US, Canada, UK, Europe...



### Science

Biology, Psychology, Physics...



### Shopping

Clothing, Food, Gifts...



### Society

People, Religion, Issues...



### Sports

Baseball, Soccer, Basketball...



### Kids & Teens Directory

Arts, School Time, Teen Life...



### World

Deutsch, Français, 日本語, Italiano, Español, Русский, Nederlands, Polski, Türkçe, Dansk, 简体中文, ...

# Un annuaire

- DMOZ (Directory Mozilla) <https://dmoztools.net/>
- Catégorie « Science »

The screenshot shows the 'Science' category page on dmoztools.net. At the top, there is a navigation bar with letters A through Z. Below it, a section titled 'Subcategories 35' is shown, divided into four columns. The first column contains: Agriculture, Anomalies and Alternative Science, Astronomy, Biology, Academic Departments, By Region, Chats and Forums, Directories, Educational Resources, and Employment. The second column contains: Chemistry, Computer Science, Earth Sciences, Environment, Events, History, Instruments and Supplies, Libraries, Methods and Techniques, and Museums. The third column contains: Math, Physics, Science in Society, Social Sciences, News and Media, Organizations, People, Publications, Reference, and Research Groups and Centers. The fourth column contains: Technology, Women, Search Engines, Software, and Weblogs. Below this, a section titled 'Related categories 4' is shown, listing: Kids and Teens > School Time > Science, Recreation > Humor > Science, Reference > Encyclopedias, and Shopping > Recreation > Science and Nature.

Subcategories 35			
Agriculture	Chemistry	Math	Technology
Anomalies and Alternative Science	Computer Science	Physics	Women
Astronomy	Earth Sciences	Science in Society	Search Engines
Biology	Environment	Social Sciences	Software
Academic Departments	Events	News and Media	Weblogs
By Region	History	Organizations	
Chats and Forums	Instruments and Supplies	People	
Directories	Libraries	Publications	
Educational Resources	Methods and Techniques	Reference	
Employment	Museums	Research Groups and Centers	

Related categories 4			
Kids and Teens > School Time > Science			
Recreation > Humor > Science			
Reference > Encyclopedias			
Shopping > Recreation > Science and Nature			

# Un annuaire

- DMOZ (Directory Mozilla) <https://dmoztools.net/>
- Catégorie « Science->Computers->Parallel\_Computing »
- Liste entrées
  - Informations
    - Nom
    - Description
    - Lien

The screenshot shows a list of sites under the 'Parallel Computing' category. At the top, there are links for 'Subcategories' (14) and 'Related categories' (2). Below these, a section titled 'Sites' (8) is expanded, showing eight entries:

- Cluster & Grid Computing**  
Programming projects, calls for papers, software, documentation, other resources. Chemnitz University of Technology, Germany.
- Clustet Computing Info Centre**  
Links to parallel computing resources.
- Grid Computing Info Centre**  
An initiative to establish a global grid of computing power. Links to conferences, development, and related information.
- HOISe**  
News on high performance computing from Europe. Newsletters and conference calendar.
- IJHSC**  
International Journal of High Speed Computing. Sample copy available, archives accessible to subscribers.
- Nan's Parallel Computing Page**  
Links to online books, tutorials, and research projects.
- Supercomputing and Parallel Computing Research Groups**  
Academic research groups and projects related to parallel computing.

# Un annuaire d'entreprise (windows)

- Active Directory
- Organisé par Catégories
  - Dossier
- Entrées
  - Rangées dans les dossiers
  - Normalisées
    - Utilisateur
      - Richard Mueller
    - Groupe
      - CustomerA

The screenshot shows the Active Directory Users and Computers (ADUC) console. On the left is a tree view of the directory structure under 'Contoso.com'. A red box highlights a subtree under 'Ninja' containing 'OU\_A' and 'OU\_B'. 'OU\_A' contains 'CustomerA' (which in turn contains 'CustomerA' and 'Richard Mueller') and 'OU\_B' (which contains 'CustomerB' and 'Ed Price'). On the right is a table listing various objects with their names, types, and descriptions.

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for upgr...
Domain Controllers	Organizational ...	Default container for dom...
ForeignSecurityPrincipals	Container	
LostAndFound	lostAndFound	Default container for seco...
Managed Service Accounts	Container	Default container for orph...
Microsoft Exchange Security Groups	Organizational ...	
Ninja	Organizational ...	
OU_A	Organizational ...	
OU_B	Organizational ...	
Program Data	Container	Default location for storag...
System	Container	Builtin system settings
Users	Container	Default container for upgr...
Microsoft Exchange System Objects	msExchSystem...	
NTDS Quotas	msDS-QuotaCo...	Quota specifications cont...
Infrastructure	infrastructureU...	

Domain Admin ADUC console

# Un annuaire d'entreprise (Linux)

- OpenLDAP (phpldapadmin pour l'affichage)

The screenshot shows the phpldapadmin web interface for managing an LDAP directory. The left sidebar displays a tree view of the LDAP structure under the root 'dc=com'. The 'ou=Administrators' entry is selected. The main panel shows the details for this entry, including its distinguished name (ou=Administrators,dc=example,dc=com), server (Leonardo's Workshop LDAP Server), and template (Default). The 'objectClass' field contains 'top' and 'organizationalUnit' (structural). The 'ou' field is set to 'Administrators'. A 'required' attribute is marked with an asterisk (\*). Below the form is a 'Update Object' button.

Home | Purge caches | Show Cache

Leonardo's Workshop LDAP Server

schema search refresh info import export

dc=com (5)

- ou=Administrators (3)
  - cn=apache
  - cn=idm
  - cn=phpldapadmin
- >Create new entry here
- ou=Groups (3)
  - cn=employees
  - cn=library
  - cn=painters
- >Create new entry here
- ou=Orgs (1)
  - ou=F0000 (2)
- >Create new entry here
- ou=People (2)
  - uid=leonardo
  - uid=michelangelo
- Create new entry here
- ou=Projects (2)
  - cn=P0001
  - cn=P0002
- Create new entry here
- Create new entry here

ou=Administrators

Server: Leonardo's Workshop LDAP Server Distinguished Name: ou=Administrators,dc=example,dc=com Template: Default

Refresh Switch Template Copy or move this entry Rename Create a child entry Hint: To delete an attribute, empty the text field and click save. View 3 children Export Delete this entry Compare with another entry Add new attribute Hint: To view the schema for an attribute, click the attribute name. Export subtree

objectClass required

top  
organizationalUnit (structural)  
(add value)

ou required, rdn

Administrators  
(add value)  
(rename)

Update Object

# Un annuaire d'entreprise (Linux)

The screenshot shows the Evolveum Directory Server interface. On the left, the LDAP tree is displayed under "Leonardo's Workshop LDAP Server". The tree includes nodes for dc-example, dc-com, ou=Administrators, ou=Groups, ou=Orgs, ou=People, ou=Projects, and several user objects (cn=apache, cn=idm, cn=phpldapadmin). The "ou=Administrators" node is expanded, showing three entries: cn=apache, cn=idm, and cn=phpldapadmin. On the right, the "Search Results" window is open, showing the results of a search for "ou=Administrators,dc=example,dc=com". The results table has three rows, each corresponding to one of the three entries in the "ou=Administrators" node. Each row displays the object's dn, cn, description, objectClass, sn, and Password (represented by asterisks). The "Description" column provides a brief explanation for each account.

Object	Description	objectClass	sn	Password
cn=apache	Special LDAP account used by the apache to access the LDAP data (library).	person	apache library user	*****
cn=idm	Special LDAP account used by the IDM to access the LDAP data.	person	IDM Administrator	*****
cn=phpldapadmin	Special LDAP account used by the phpldapadmin to access the LDAP data.	person	phpldapadmin user	*****

# Un annuaire d'entreprise (Linux)

- OpenLDAP (phpldapadmin pour l'affichage)

The screenshot shows the phpldapadmin web interface. On the left, there's a sidebar titled "Leonardo's Workshop LDAP Server" with a tree view of the LDAP structure under "dc=example,dc=com". The tree includes nodes for "ou=Administrators", "ou=Groups", "ou=Orgs", "ou=People", and "ou=Projects". Each node has a "Create new entry here" link. On the right, a main panel titled "Create Object" displays a list of "Templates" for creating new entries. The templates are categorized into two columns:

Templates:	
<input type="radio"/> Courier Mail: Account	<input checked="" type="radio"/> Samba: Domain
<input type="radio"/> Courier Mail: Alias	<input type="radio"/> Samba: Group Mapping
<input type="radio"/> Generic: Address Book Entry	<input type="radio"/> Samba: Machine
<input type="radio"/> Generic: DNS Entry	<input checked="" type="radio"/> Sendmail: Alias
<input type="radio"/> Generic: LDAP Alias	<input checked="" type="radio"/> Sendmail: Cluster
<input type="radio"/> Generic: Organisational Role	<input checked="" type="radio"/> Sendmail: Domain
<input type="radio"/> Generic: Organisational Unit	<input checked="" type="radio"/> Sendmail: Relays
<input type="radio"/> Generic: Posix Group	<input checked="" type="radio"/> Sendmail: Virtual Domain
<input type="radio"/> Generic: Simple Security Object	<input checked="" type="radio"/> Sendmail: Virtual Users
<input type="radio"/> Generic: User Account	<input type="radio"/> Thunderbird: Address Book Entry
<input type="radio"/> Kolab: User Entry	<input type="radio"/> User Group
<input type="radio"/> Samba: Account	<input type="radio"/> Default

At the bottom right of the main panel, it says "1.2.2" and "SOURCEFORGE".

# Annuaire: Résumé

- Un système qui organise des informations
  - Index
  - Organisation hiérarchique avec des catégories
  - Différents types d'objets (personne, groupes, ...)
  - Des accès en lecture principalement et des écritures.
    - Modification et accès
      - par des personnes
      - Application
- Les objets ont des attributs:
  - Nom Prénom
  - Numéro de téléphone
  - ...
  - Obligatoire ou facultatif

# Authentification, Identification

- Identification: Qui êtes vous ?
  - Prénom, Nom, Age, ..
- Authentification: Prouvez-moi qui vous êtes ?
  - Montrez moi votre carte d'identité avec votre photo
  - Donnez moi le code secret
- Autorisation: Avez-vous le droit d'entrer
  - D'accord, vous êtes sur la liste

# EN ENTREPRISE



# Annuaire: en entreprise

- Utilisation
  - Regrouper toutes les informations sur les employés en un seul endroit (Base RH, Base de comptes informatique, ...)
    - Permet d'éviter les synchronisation de base
    - Un seul point d'entrée pour saisie/correction des données.
  - Toutes les applications utilisent la même référence
    - Logiciel RH (SAP par exemple)
    - Outlook/Thunderbird/Webmail pour les contacts
    - Site web (portail intranet de l'entreprise)
    - Le login sur les ordinateurs Windows, Linux, ...
    - Les serveurs de messagerie
    - La gestion des badges
    - ...

# Annuaire: en entreprise

- Possibilité
  - Référencer les postes de travail et serveur
    - Stocker des informations sur le matériel (Localisation)
    - Les authentifier dans certains cas (Active Directory)
  - Faire des groupes:
    - De personnes, pour limiter des accès à des fichiers, des stations, ...
    - Gérer l'accès à des ressources partagées (boite mail commune, ...)
    - De personne/mail pour faire des listes de distribution
      - Envoyer un mail à tous le employés de l'entreprise
  - Faire des objets techniques:
    - Alias mail, qui seront utilisés par les serveur de messagerie
  - Faire des objects pour inventaire
    - Licence logicielles

# Annuaire: en entreprise

- Possibilité en terme de données:
  - Préférence ou paramètres des utilisateurs:
    - Des informations simples:
      - Shell par défaut: /bin/bash
      - Prénom
      - Nom de Famille
      - Numéro de badge
    - Dépendances:
      - Référence à son manager
        - Référencer un autre objet (un lien)
    - De types différents:
      - Photo en base 64 (pour afficher dans outlook par exemple)
      - Des certificats
      - Des clés publiques

# HPC



# Annuaire: dans le HPC

- Les utilisateurs du centre d sont comme les employés dans l'entreprise
  - L'annuaire sert à:
    - Avoir toutes les informations sur les utilisateurs
      - Fournis par l'utilisateur
        - Prénom
        - Nom
        - Entreprise
        - Projet
        - Shell par défaut (/bin/bash)
      - Internes au Centre de Calcul
        - Uid
        - Gid
        - Home directory
        - Chemin des différents systèmes de fichiers

# Annuaire: dans le HPC

- L'annuaire ne sert PAS à:
  - Stocker des informations dynamiques:
    - Espace utilisé sur les systèmes de fichiers
    - Nombre d'heures de calcul...
    - L'historique des jobs
    - L'historique des connexions
    - ...

# Annuaire: dans le HPC

- Tous les services utilisent l'annuaire:
  - Nœud de login
    - SSH, vérifie que l'utilisateur est dans un groupe autorisé
    - Shell à lancer quand la personne se connecte
    - Home directory pour placer l'utilisateur dedans
  - Stockage Distribué
    - Uid/gid pour autorisé l'accès ou non aux fichiers
  - Le scheduler de jobs
  - Les services de visualisation à distance
  - ...
- Comment l'annuaire est renseigné ?
  - Un outil/des scripts sont développés pour automatiser la création
  - La création dans l'annuaire n'est qu'une étape dans la création d'un compte
  - On se sert également de l'annuaire pour les mails, groupes, ...

# Annuaire: dans le HPC: Zone Admin

- Tous les services de la zone d'administration utilise également un annuaire
  - Pour identifier les administrateurs et leurs droits:
    - Les administrateur des différentes parties du centre de calcul
      - Système
      - Calculateur
      - Stockage
    - Les infogérants et leur périmètres
      - Applicatif
      - Calculateur
      - Hotline

# UN ANNUAIRE LDAP

---

Quel annuaire ? Quel protocole ?

# LDAP: Protocole

- Lightweight Directory Access Protocol (LDAP)
  - Interrogation/modification de services d'annuaire
  - Un formalisme, une syntaxe pour accéder aux données
- Devenu la norme pour les systèmes d'annuaire
  - Souvent utilisé avec Kerberos (Authentification)
    - Bien que LDAP permet l'authentification
- Différence par rapport a un SGBD (Mysql, Posgresql, ...)
  - Orienté lecture de données

# LDAP: Concepts

- Quatre modèles
  - Nommage
    - Comment sont nommées/organisées les données
  - Fonctionnel
    - Ce que l'on peut faire avec les données
  - Information
    - Qu'est-ce que l'on peut mettre comme données (type, ...)
  - Sécurité
    - Qui accède à quelles données ? En lecture, en écriture ?

# LDAP: Usage and misusage

- Usage:
  - Trouver des informations, avec des filtres
  - Gérer des comptes, des adresses, ...
  - Une base de donnée simple (ordinateurs, produits, .. )
  - Sécurité: certificats, ...
  - Accédé par des humains via une IHM ou des programmes
  - Fait pour la lecture massive
- Misusage
  - Ecritures fréquentes ou données volumineuses
  - Données redondantes
  - Changer la fonction de champs standards des objets

# LDAP: Historique

- /etc/passwd (comme pour DNS avec /etc/hosts)
  - Base répliquée sur toutes les machines
  - Mot de passe dans /etc/shadow (Authentification)

```
root:x:0:0:root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
```

- /etc/group
  - Appartenance aux groupes

```
root:x:0:
bin:x:1:bin,daemon
daemon:x:2:bin,daemon
sys:x:3:bin,adm
adm:x:4:adm,daemon
tty:x:5:
disk:x:6:
lp:x:7:daemon
```

# LDAP: Historique X500

- Normes de 1988
- Conçu pour
  - Interconnecter les annuaires téléphoniques
  - Faire un annuaire globale
  - Extensible (modèle de données)

Numéro <a href="#">UIT-T1</a>	Numéro ISO/CEI	Titre du Standard
X.500	ISO/CEI 9594-1	Vue d'ensemble des concepts, modèles et services
X.501	ISO/CEI 9594-2	Modèles
<a href="#">X.509</a>	ISO/CEI 9594-8	<a href="#">framework</a> d'Authentification
X.512	ISO/CEI 9594-3	Définition de service
X.518	ISO/CEI 9594-4	Procédures pour les opérations distribuées
X.519	ISO/CEI 9594-5	Spécifications de protocoles
X.520	ISO/CEI 9594-6	Types d'attributs sélectionnés
X.521	ISO/CEI 9594-7	Classes d'objets sélectionnés
X.525	ISO/CEI 9594-9	Replication d'annuaire
X.530	ISO/CEI 9594-10	Administration d'annuaire

# LDAP: Historique X500

- Les protocoles définis par X.500 inclus:
  - DAP (*Directory Access Protocol*)
    - Devient LDAP
  - DSP (*Directory System Protocol*)
  - DISP (*Directory Information Shadowing Protocol*)
  - DOP (*Directory Operational Bindings Management Protocol*)
- Avantages
  - Passage à l'échelle, fonctions avancées de recherche, ...
- Problèmes
  - Conception très lourdes (nombre de normes, protocoles, ...)

# LDAP: Historique

- "X.500 is too complex to support on desktops and over the Internet, so LDAP was created to provide this service 'for the rest of us'." ([What is LDAP?](#). Gracion.com. Retrieved on 2013-07-17)
- En 1993 LDAP, version simplifiée de X500 DAP, en s'appuyant sur TCP
  - LDAPv1: RFC 1487
  - LDAPv2: RFC 1777
  - LDAPv3: RFC 4511
- Les premiers solutions apparaissent quelques années plus tard.
- En parallèle l'utilisation de NIS+ (1992) diminue (solution d'annuaire décentralisée de SUN)

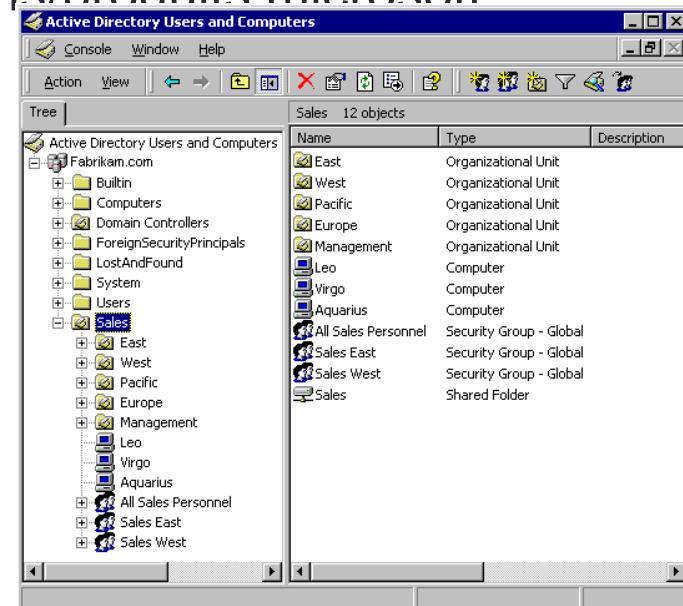
# Principaux serveurs LDAP

- OpenLDAP
- ActiveDirectory
- Apache Directory Server
- 389 Directory Server
- IBM Domino
- ...



# Active Directory

- LDAP et Kerberos intégré
  - Version propriétaire
  - Identifie et Authentifie
  - Légères modifications par rapport au LDAP et Kerberos open source
- Solution utilisée dans beaucoup d'entreprises
  - Facilité d'intégration dans le parc de stations/produits microsoft
- Attention aux différences
  - dans les schémas
  - Sur certaines opérations
- Plus
  - Notion de domaines, forets, gc, rodc, schema master, ...



# OpenLdap

- Projet
  - Démarré en 1998
- Donnée
  - Il utilise des librairies tierces pour stocker les informations.
    - Fichiers plats
    - BDB
    - Mysql
- Extensions
  - Backend: DB, Proxy (Relay, ...), Dynamic backends (statistics).
- Utilisation
  - Présent dans toutes les distributions
  - Largement utilisé



# Les clients

- SSSD (System Security Services Daemon)
  - Garde en mémoire les identités et les authentifications
- NSLCD
  - Garde en mémoire les identités
- L'ensemble des logiciels qui ont besoin de l'identité d'un utilisateur
  - Routage de mail
    - Postfix
  - Système de fichiers
    - Locaux
    - Filers (Netapp)
  - ...

# Les « commandes »

- Pour contacter directement un annuaire
  - Ldapsearch
  - Ldapmodify
  - ...
- Pour consulter les « comptes sur la machines »
  - Getent passwd
  - Getent group

```
# getent passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
halt:x:7:0:halt:/sbin:/sbin/halt
...
bernedea:x:1004:1000::/home/bernedea:/bin/bash
guest00:x:1200:2000::/home/guest00:/bin/bash
guest01:x:1201:2000::/home/guest01:/bin/bash
guest02:x:1202:2000::/home/guest02:/bin/bash
guest03:x:1203:2000::/home/guest03:/bin/bash
guest04:x:1204:2000::/home/guest04:/bin/bash
```

# Réseau/Sécurité

- TCP/IP
  - LDAP sur le port 389
    - Ne pas faire transiter de données sensibles en LDAP (Active directory interdit le changement de mot de passe en LDAP par exemple).
  - LDAPS sur le port 636
- Il était courant de laisser un annuaire en accès anonymes.
  - Il faut authentifier les accès dès que possible
- DNS
  - \_ldap.\_tcp.ccc.cdc.fr. IN SRV 0 0 389 ldap.ccc.cdc.fr.
  - Utilisé par Active Directory

# CONCEPTS

---



# LDAP: Concepts

- Nommage
  - Comment sont nommées/organisées les données
- Fonctionnel
  - Ce que l'on peut faire avec les données
- Information
  - Qu'est-ce que l'on peut mettre comme données (type, ...)
- Sécurité
  - Qui accède à quelles données ? En lecture, en écriture ?
- Protocole d'accès
  - Comment on requête ?
- Duplication
  - Les mécanismes de réplication
- API
- LDIF: LDAP Data Interchange Format

# INFORMATIONS



# Définition

- OU
  - Organisational Unit
- DN
  - Distinguished Name
- CN
  - Canonical Name

The screenshot shows a LDAP management interface titled "Leonardo's Workshop LDAP Server". The left pane displays a tree view of the directory structure under "dc=example,dc=com". The "Administrators" OU contains entries for "cn=apache", "cn=idm", and "cn=phpldapadmin". The "Groups" OU contains "cn=employees", "cn=library", and "cn=painters". The "Orgs" OU contains "ou=F0000". The "People" OU contains "uid=leonardo" and "uid=michelangelo". The "Projects" OU contains "cn=P0001" and "cn=P0002". The right pane shows a search result for "ou=Administrators,dc=example,dc=com" with 3 entries found. The first entry is "cn=apache", which has attributes: dn (cn=apache,ou=Administrators,dc=example,dc=com), cn (apache), description (Special LDAP account used by the apache to access the server), objectClass (person, top), sn (apache library user), and Password (\*\*\*\*\*). The second entry is "cn=idm", which has attributes: dn (cn=idm,ou=Administrators,dc=example,dc=com), cn (idm), description (Special LDAP account used by the IDM to access the server), objectClass (person, top), and sn (IDM Administrator).

Leonardo's Workshop LDAP Server

schema search refresh info import export

ou=Administrators,dc=example,dc=com (3)

cn=apache  
cn=idm  
cn=phpldapadmin  
Create new entry here

ou=Groups (3)

cn=employees  
cn=library  
cn=painters  
Create new entry here

ou=Orgs (1)

ou=F0000 (2)  
Create new entry here

ou=People (2)

uid=leonardo  
uid=michelangelo  
Create new entry here

ou=Projects (2)

cn=P0001  
cn=P0002  
Create new entry here  
Create new entry here

Search R

Server: Leonardo's Work Query: ou=Administrators,dc=example,dc=com

Entries found: 3 (0 seconds)

**cn=apache**

dn	cn=apache,ou=Administrators,dc=example,dc=com
cn	apache
description	Special LDAP account used by the apache to access the server
objectClass	person, top
sn	apache library user
Password	*****

**cn=idm**

dn	cn=idm,ou=Administrators,dc=example,dc=com
cn	idm
description	Special LDAP account used by the IDM to access the server
objectClass	person, top
sn	IDM Administrator

# Schéma: objet

- Le schéma de l'annuaire définit les classes d'objets utilisables
  - /etc/openldap/schema/core.schema, ...
- Toutes les entités de l'annuaire font forcément référence à un objet du schéma
  - Object
    - Nom
    - Description
    - Héritage
  - Attributs
    - Obligatoires
    - Facultatifs

# Schéma: core.schema

```
objectclass ( 2.5.6.6 NAME 'person'  
    DESC 'RFC2256: a person'  
    SUP top STRUCTURAL  
    MUST ( sn $ cn )  
    MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )  
  
objectclass ( 2.5.6.7 NAME 'organizationalPerson'  
    DESC 'RFC2256: an organizational person'  
    SUP person STRUCTURAL  
    MAY ( title $ x121Address $ registeredAddress $ destinationIndicator $  
        preferredDeliveryMethod $ telexNumber $ teletexTerminalIdentifier $  
        telephoneNumber $ internationalISDNNumber $  
        facsimileTelephoneNumber $ street $ postOfficeBox $ postalCode $  
        postalAddress $ physicalDeliveryOfficeName $ ou $ st $ i ) )
```

# Schéma: Attributs

- Chaque objets à des attributs
  - Type
    - Attributetype
  - OID
    - Identifie l'attribut
  - NAME
    - Nom de l'attribut, sert de référence
  - DESC
    - Description
  - EQUALITY
    - Méthode de comparaison
  - SUBSTR
    - Méthode de comparaison pour un sous ensemble
  - SYNTAX
    - OID{Taille MAX} SINGLE-VALUE/MULTI

# Schéma: Attributs

```
attributetype ( 2.5.4.20 NAME 'telephoneNumber'  
    DESC 'RFC2256: Telephone Number'  
    EQUALITY telephoneNumberMatch  
    SUBSTR telephoneNumberSubstringsMatch  
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.50{32} )
```

# Schéma: Attributs

```
# 9.3.7. Photo
#
# The Photo attribute type specifies a "photograph" for an object.
# This should be encoded in G3 fax as explained in recommendation T.4,
# with an ASN.1 wrapper to make it compatible with an X.400 BodyPart as
# defined in X.420.
#
# IMPORT G3FacsimileBodyPart FROM { mhs-motis ipms modules
# information-objects }
#
# photo ATTRIBUTE
#   WITH ATTRIBUTE-SYNTAX
#     CHOICE {
#       g3-facsimile [3] G3FacsimileBodyPart
#     }
#     (SIZE (1 .. ub-photo))
#   ::= {pilotAttributeType 7}
#
attributetype ( 0.9.2342.19200300.100.1.7 NAME 'photo'
               DESC 'RFC1274: photo (G3 fax)'
               SYNTAX 1.3.6.1.4.1.1466.115.121.1.23{25000} )
```

# Schéma: Attributs

```
attributetype ( 1.3.6.1.1.1.3 NAME 'homeDirectory'  
    DESC 'The absolute path to the home directory'  
    EQUALITY caseExactIA5Match  
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

```
attributetype ( 1.3.6.1.1.1.4 NAME 'loginShell'  
    DESC 'The path to the login shell'  
    EQUALITY caseExactIA5Match  
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )
```

# Schéma: OID Syntax

- Définis dans la RFC 4517
- ( 1.3.6.1.4.1.1466.115.121.1.6 DESC 'Bit String' )
- ( 1.3.6.1.4.1.1466.115.121.1.7 DESC 'Boolean' )
- ( 1.3.6.1.4.1.1466.115.121.1.11 DESC 'Country String' )
- ( 1.3.6.1.4.1.1466.115.121.1.36 DESC 'Numeric String' )

# Schéma: OID Syntax

## 3.3.31. Telephone Number

A value of the Telephone Number syntax is a string of printable characters that complies with the internationally agreed format for representing international telephone numbers [E.123].

The LDAP-specific encoding of a value of this syntax is the unconverted string of characters, which conforms to the <PrintableString> rule in Section 3.2.

Examples:

+1 512 315 0280  
+1-512-315-0280  
+61 3 9896 7830

The LDAP definition for the Telephone Number syntax is:

( 1.3.6.1.4.1.1466.115.121.1.50 DESC 'Telephone Number' )

The Telephone Number syntax corresponds to the following ASN.1 type from [X.520]:

PrintableString (SIZE(1..ub-telephone-number))

The value of ub-telephone-number (an integer) is implementation defined. A non-normative definition appears in [X.520].

# Schéma: Attributs EQUALITY

- numericStringMatch,
- numericStringSubstringsMatch,
- caseExactMatch,
- caseExactOrderingMatch,
- caseExactSubstringsMatch,
- caseExactIA5Match,
- caseIgnoreIA5Match,
- caseIgnoreIA5SubstringsMatch,
- caseIgnoreListMatch,
- caseIgnoreListSubstringsMatch,
- caseIgnoreMatch,
- caseIgnoreOrderingMatch,
- caseIgnoreSubstringsMatch,
- directoryStringFirstComponentMatch,
- telephoneNumberMatch,
- telephoneNumberSubstringsMatch and
- wordMatch.

# OID: Attribution

- X OID de l'entreprise.
- Range privé assigné par l'IANA:
  - 1.3.6.1.4.1.X.1 - assign to SNMP objects
  - 1.3.6.1.4.1.X.2 - assign to LDAP objects
  - 1.3.6.1.4.1.X.2.1 - assign to LDAP syntaxes
  - 1.3.6.1.4.1.X.2.2 - assign to LDAP matchingrules
  - 1.3.6.1.4.1.X.2.3 - assign to LDAP attributes
  - 1.3.6.1.4.1.X.2.4 - assign to LDAP objectclasses
  - 1.3.6.1.4.1.X.2.5 - assign to LDAP supported features
  - 1.3.6.1.4.1.X.2.9 - assign to LDAP protocol mechanisms
  - 1.3.6.1.4.1.X.2.10 - assign to LDAP controls
  - 1.3.6.1.4.1.X.2.11 - assign to LDAP extended operations

# Schéma: Classes d'objets

- Les plus courantes sont:
  - top
  - organizationalUnit
  - Person
  - organizationalPerson
  - user
  - Account
  - posixAccount
  - shadowAccount
  - Alias
  - posixGroup
  - Group
  - ...

# Schéma: Vérification

- Création
  - LDAP vérifie que la syntaxe est conforme au schéma.
- Modification
  - LDAP vérifie que la syntaxe est conforme au schéma.
- Processus de « Schema Checking »
- Si non conforme
  - « Error no 53 *Unwilling to perform error* »

# Configuration des schéma dans slapd

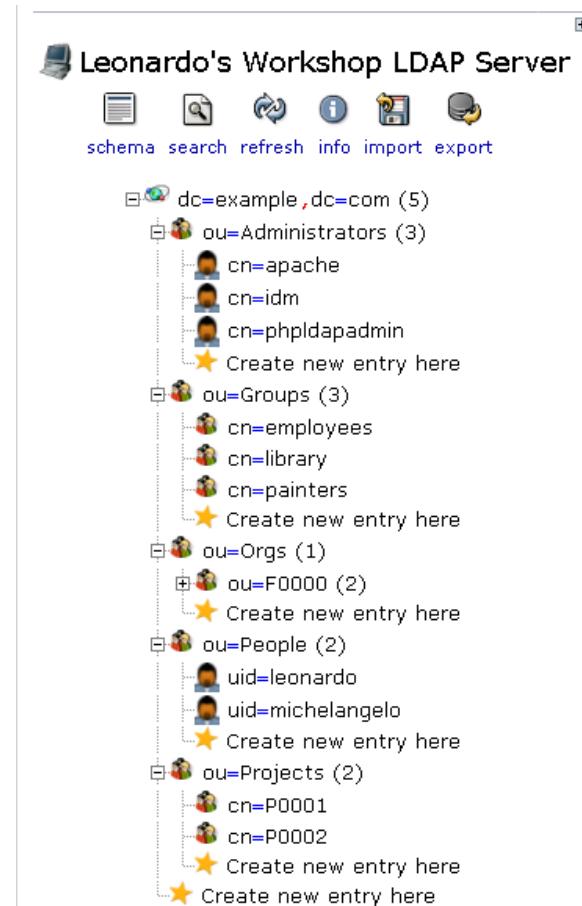
- Avant LDAPv3, le serveur garder ses schéma pour lui
  - Maintenant, le serveur les exposes dans subschema
- Pour que les mécanismes de réPLICATION fonctionnent:
  - Tous les serveurs doivent avec les même schéma
  - Sinon
    - Les objets ne sont pas répliqués (la réPLICATION s'arrête à l'erreur)

# NOMMAGE



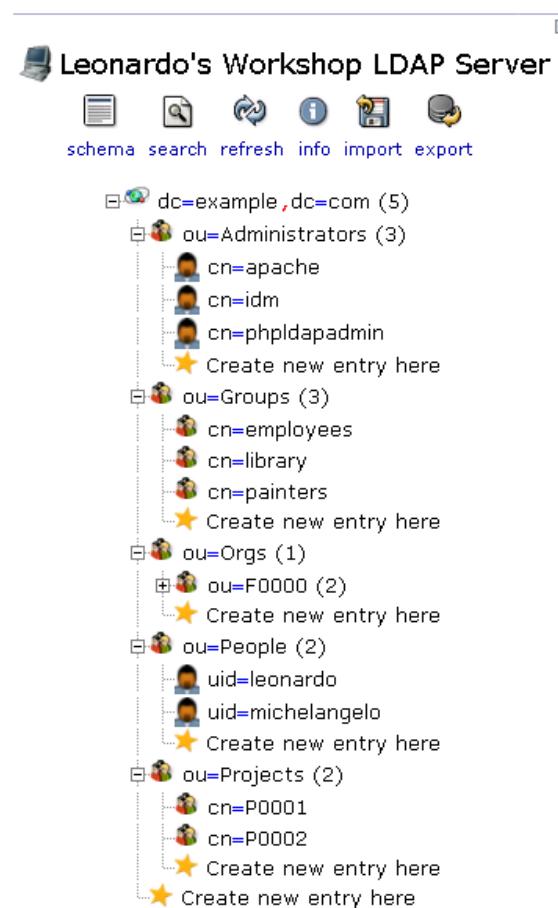
# Nommage

- Suffixe ou base définit l'espace de nommage
  - Un serveur peut gérer plusieurs suffixes
- Il y a une entrée technique « root DSA » qui contient la description du DIT (Directory Information Tree)
- Ensuite on organise les OU comme on veut.
- En général on à:
  - People
  - Groups
  - Administrators
  - Computers
- Le défaut d'AD est presque devenu le standard.



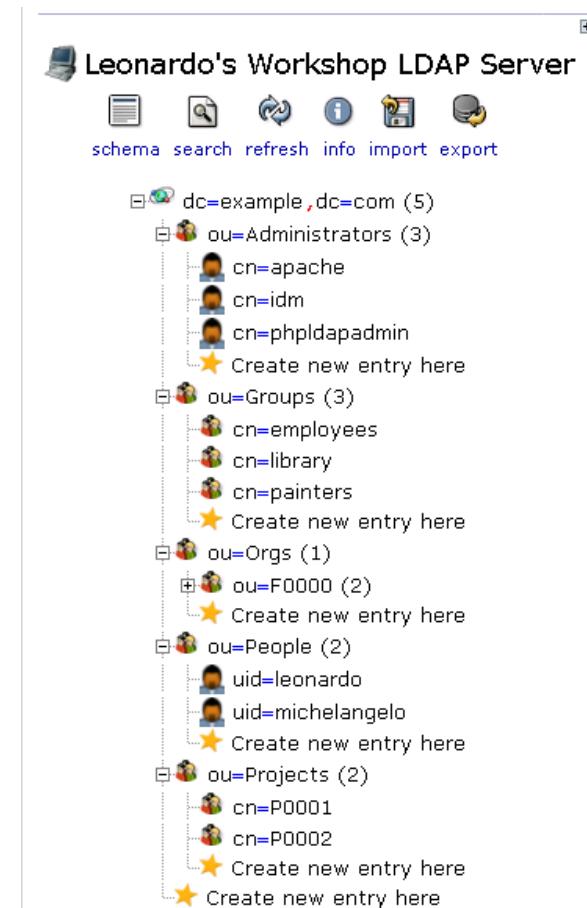
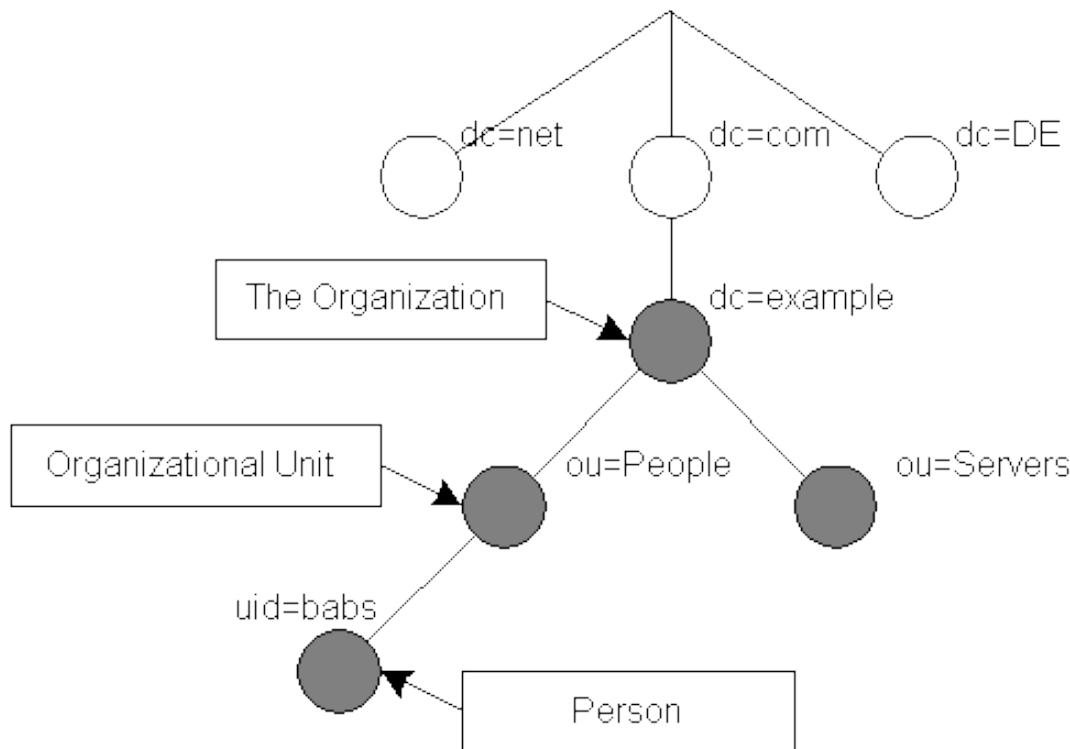
# Nommage

- DN Distinguished name
  - Ressemble au path d'un fichier
  - Elle est unique
  - Exemple:
    - dn: uid=macronm,ou=People,dc=ccc,dc=cdc,dc=fr
    - dn: cn=ldapadm,dc=ccc,dc=cdc,dc=fr
  - Séparé par des virgules
  - Le RDN de l'objet + chemin d'accès
- RDN Relative Distinguished name
  - Différent par objet
    - Uid pour les comptes par exemple
    - Cn pour les alias
  - Doit permettre de s'assurer que deux entrées n'ont pas le même nom
- Certains attributs permettent de référencer un DN pour faire une « référence »



# Nommage

- DN Distinguished name



# FONCTIONNEL

---



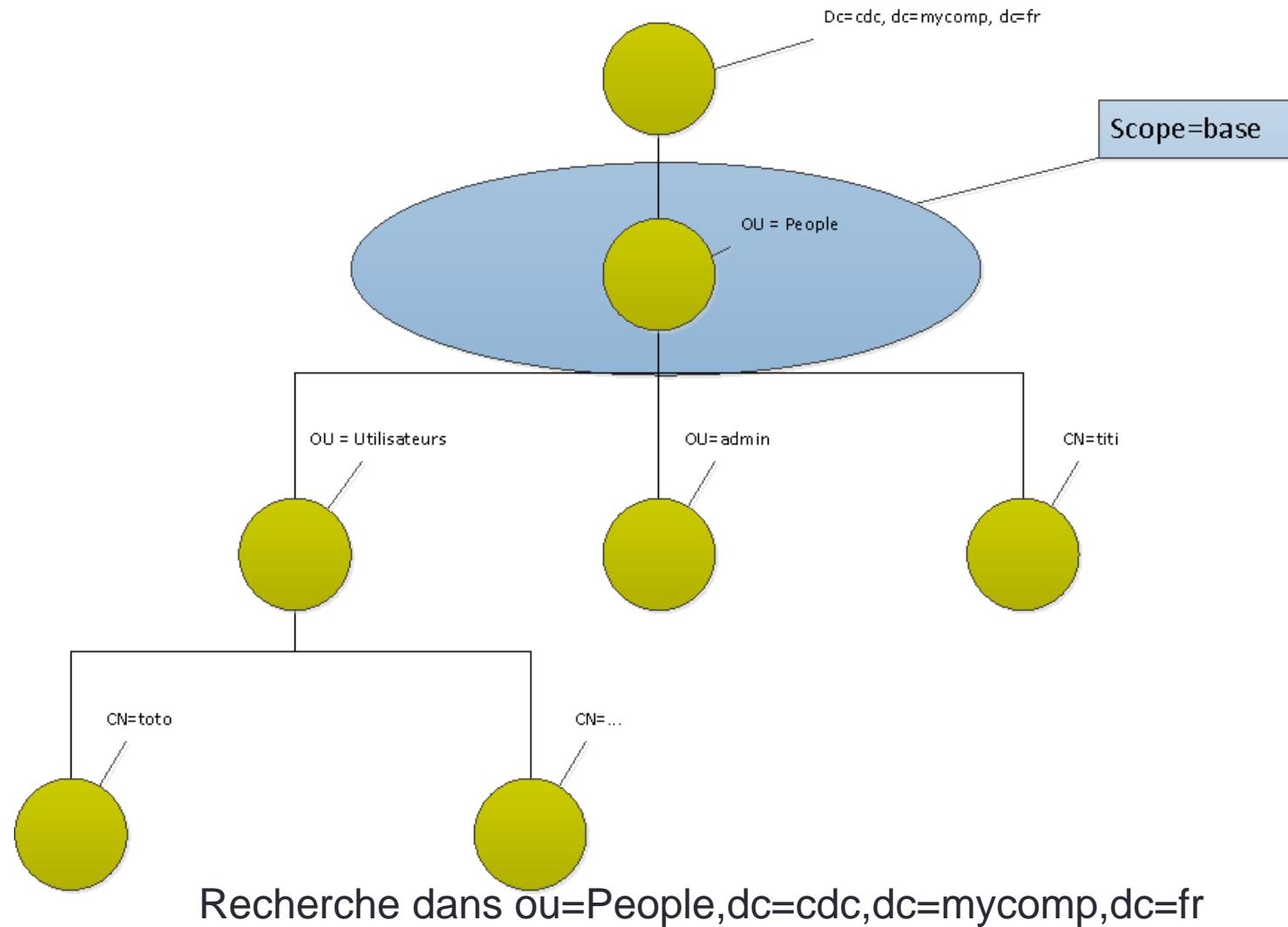
# Fonctionnel

- Comment écrire une requête
- Paramètres à fournir
  - Principaux
    - Suffixe: dc=ccc,dc=cdc,dc=fr
    - Scope: périmètre de recherche
    - Search filter: Filtre
    - List of attributs: Liste des attributs à retourner
  - Secondaires
    - Sizelimit
    - Timelimit
    - Attronly
    - derefAliases

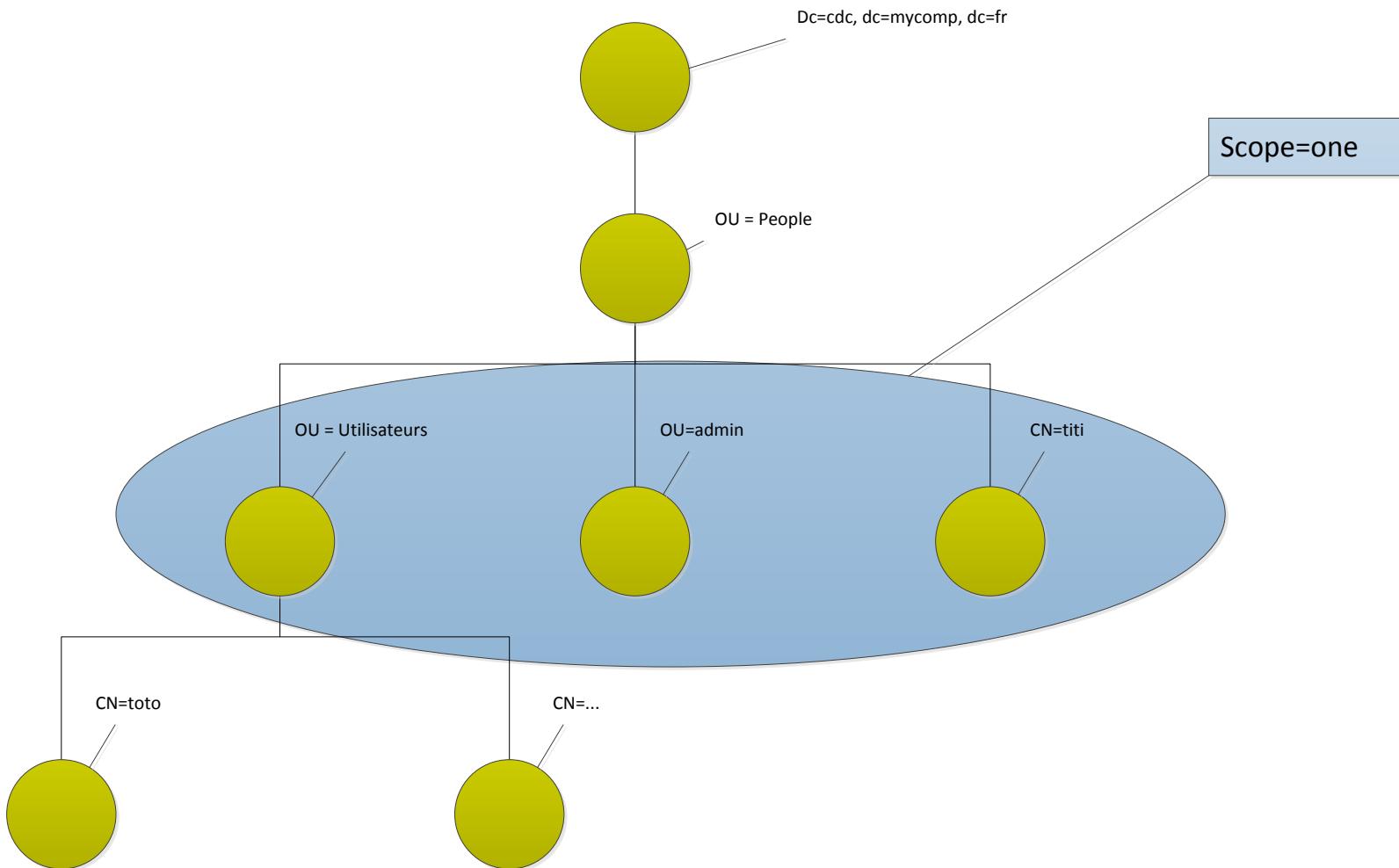
# Les scopes

- Utilisé pour la recherche
  - On spécifie à partir d'où on veut faire la recherche
- Défini quand est le périmètre de la recherche
  - Où on s'arrête dans les sous dossier
- Possibilités:
  - Base
    - L'OU courante
  - One
    - L'OU courante et les dossier
  - Subtree
    - L'OU courante et toutes les sous dossiers de manière récursive

# Scope: Base

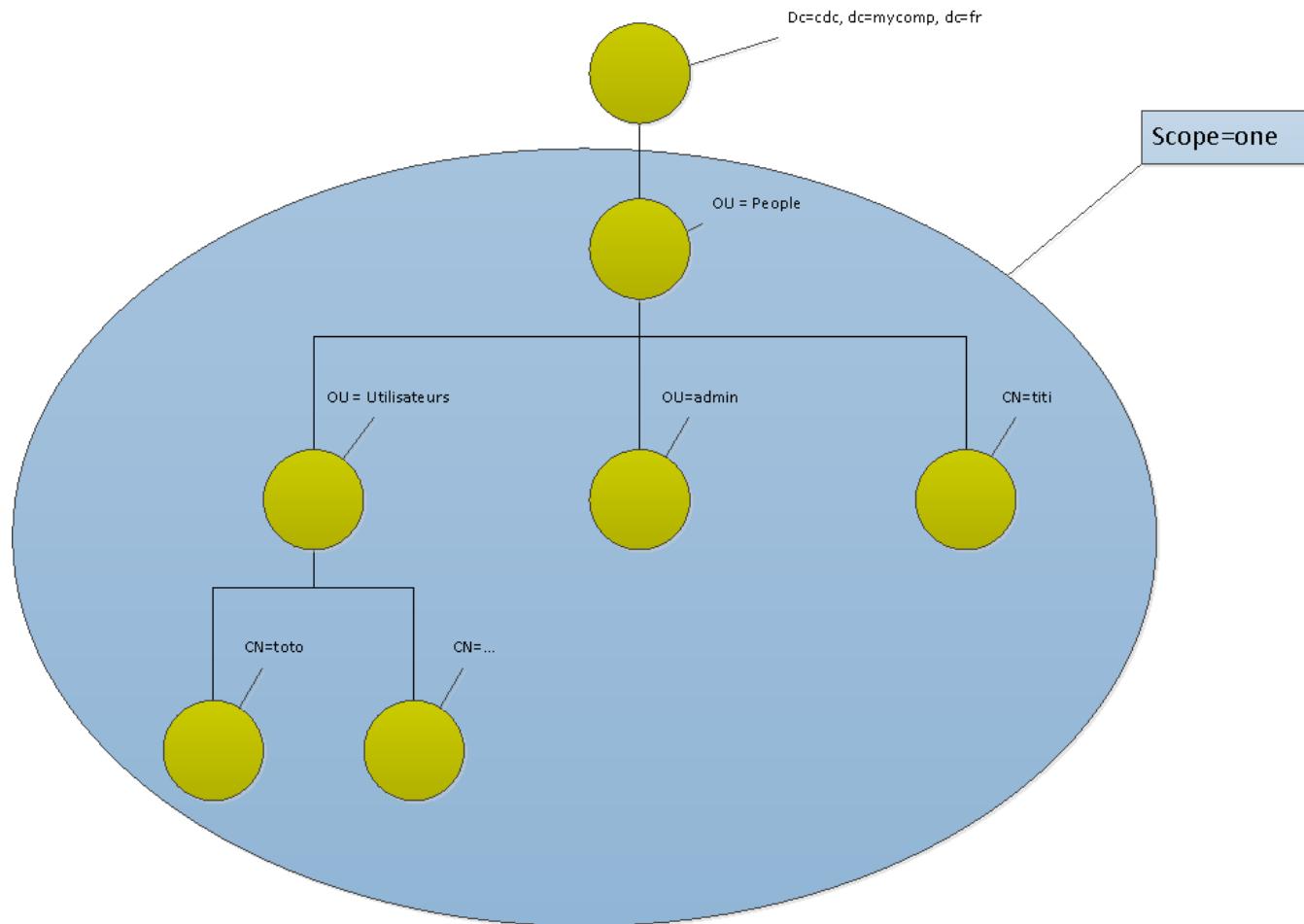


# Scope: onerulevel



Recherche dans `ou=People,dc=cdc,dc=mycomp,dc=fr`

# Scope: subtree



Recherche dans `ou=People,dc=cdc,dc=mycomp,dc=fr`

# Filtres de recherche

Filtre	Comparaison	Description
(cn=Macron)	Égalité	Le cn est Macron
(cn=*acr*)	Sous-chaine	Le nom contient « acr »
(cn=Mac*)	Sous-Chaine	Le nom commence par Mac
(uid=*)	Existence	Tous les objets qui ont un uid
(cn~=Makron)	Approximation	Se prononce de la même façon
(&(Firstname=Emmanuel)(JobTitle=President))	ET	Tous les Emmanuel dont le job est President
( (Firstname=Emmanuel)(Firstname=Brigitte))	OU	Emmanuel ou Brigitte
(!(mail)=*)	NON	Tous les utilisateurs qui n'ont pas de mail

# Opération: Search

- L'opération la plus courante
- La seul façon de consulter l'annuaire
- Fournir une configuration avec:
  - Serveur (obligatoire)
  - Base dn (obligatoire)
  - Filtre
  - ...
- La configuration est fourni par:
  - Le fichier /etc/openldap/ldap.conf
  - Par l'application
    - En paramètre pour ldapsearch

# Opération: Compare

- Comparaison
  - Compare un attribut avec une valeur donnée
- Ldapcompare
  - ldapcompare "uid=babs,dc=example,dc=com" sn:Jensen
- Héritage de X500
- Retour
  - Vrai si c'est la même valeur
  - Faux pour les autres cas

# Opération: Add

- Créer un nouveau objet à part de:
  - Un DN
  - Une liste d'attributs
  - Ldapadd –f object.ldif
- Conditions
  - L'OU parente existe
  - Il n'existe pas d'entrée du même nom
  - Les attributs correspondent au schéma
  - l'utilisateur dispose des accès

# Opération: Modify

- Modifie un objet existant
  - Ajoute, supprime ou remplace des attributs
  - Ldapmodify –f object.ldif
- Conditions
  - L'entrée existe
  - La modification respecte le schéma
  - Toutes les modifications sont prévus

# Opération: Delete

- Supprime une entrée
  - A partir du DN
- Condition
  - L'entrée existe
  - L'entrée n'a pas de sous entrées
  - L'utilisateur a le droit de supprimer l'objet

# Opération: Rename

- Renommer une entrée (changer un RDN et un DN)
  - A partir du DN
- Condition
  - L'entrée existe
  - La cible n'existe pas
  - L'utilisateur a les droits sur l'objet et la cible

# Opération: Rename

- Plusieurs possibilité
  - Changer de RDN au même endroit (changement de nom de famille pour un utilisateur par exemple)
    - dn: uid=trogneuxb,ou=People,dc=ccc,dc=cdc,dc=fr (rdn: uid=trogneuxb)
    - dn: uid=macronb,ou=People,dc=ccc,dc=cdc,dc=fr
  - Déplacer l'entrée dans l'arbre en changeant ou gardant le RDN
    - dn: uid=macronb,ou=People,dc=ccc,dc=cdc,dc=fr
    - dn: uid=macronb,ou=VIP,dc=ccc,dc=cdc,dc=fr
  - dn: uid=trogneuxb,ou=People,dc=ccc,dc=cdc,dc=fr
  - dn: uid=macronb,ou=VIP,dc=ccc,dc=cdc,dc=fr

# Opération: Bind/Unbind/Abandon

- Bind
  - Connexion au serveur
  - Simple Bind
  - SASL Bind
    - Par défaut en ligne de commande
  - Anonymous Bind
- Unbind
  - Déconnexion
- Abandon
  - Abandonne la requête qu'il avait envoyé.

# Ligne de commande

- Ldapadd -> Ajout
- Ldapdelete -> Suppression
- Ldapmodify -> Modification
- Ldappasswd -> Changement de MDP
- Ldapurl -> Génération d'url ldap
- Ldapcompare -> Comparaison
- Ldapexop -> Opérations étendus
- Ldapmodrdn -> Renomage
- Ldapsearch -> Recherche
- Ldapwhoami -> Qui suis-je

Les pages de MAN sont à jour !

# Ligne de commande (2)

- Paramètres souvent utilisés
- -x pour se connecter en anonyme
- -h pour spécifier le serveur (déprécié)
  - MONSERVERLDAP.MONDOMAINE.ORG
- -H pour spcifcier une URI LDAP
  - LDAP://MONSERVERLDAP.MONDOMAINE.ORG

# Libs

- Python
  - Python-ldap
- C
  - Openldap
- Perl
  - Perl::ldap
- Go
  - Go-ldap
- Erlang
  - eldap

# Python ldap: bind

```
import ldap
try:
    l = ldap.open("127.0.0.1")
    l.protocol_version = ldap.VERSION3
    username = "cn=Manager, o=anydomain.com"
    password = "secret"
    l.simple_bind(username, password)
except ldap.LDAPError, e:
    print e
```

# Python ldap: ajouter une entrée

```
import ldap
import ldap.modlist as modlist

l = ldap.initialize("ldaps://localhost.localdomain:636/")

l.simple_bind_s("cn=manager,dc=example,dc=com","secret")

dn="cn=replica,dc=example,dc=com"

attrs = {}
attrs['objectclass'] = ['top','organizationalRole','simpleSecurityObject']
attrs['cn'] = 'replica'
attrs['userPassword'] = 'aDifferentSecret'
attrs['description'] = 'User object for replication using slurpd'

ldif = modlist.addModlist(attrs)

l.add_s(dn,ldif)

l.unbind_s()
```

# LDIF



# LDIF

- Format utilisé pour exporter et importer les données d'un annuaire

```
dn: cn=John Doe,dc=example,dc=org
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 555 6789
telephoneNumber: +1 555 1234
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

# LDIF

```
dn: cn=Modify Me,dc=example,dc=com  
changetype: modify  
replace: mail  
mail: modme@example.com
```

```
-  
add: title  
title: Grand Poobah  
  
-  
delete: description  
-
```

```
dn: cn=Barbara ,dc=example,dc=com  
changetype: delete
```

```
dn: cn=Barbara,dc=example,dc=com  
objectClass: person  
cn: Barbara  
sn: Jensen  
title: the manager  
mail: bjensen@example.com  
uid: bjensen
```

# SECURITE

---



# Authentification dans le service d'annuaire

- Anonyme
  - N'importe quelle personne malveillante peut récupérer toutes les informations de l'entreprise ou du centre de calcul
- login/password
  - Avec un compte dans l'annuaire
    - Pour le système
      - Mot de passe dans un fichier accessible que par root
- GSS-API (Generic Security Service Application Program Interface )
  - Kerberos (authentification par kerberos)
  - +
    - Chaque machine/personne est authentifier avec sa propre keytab
    - Ticket de service
    - ...

# Contrôle d'accès

- Configuration
  - access to \*
    - by self write
    - by users read
    - by anonymous auth
- Granularité
  - Permet de donner des droits par attributs, OU, ...
    - Donne le droits aux utilisateurs de modifier eux-même leur numéro de téléphone

# Access rules

```
<access directive> ::= access to <what>
  [by <who> [<access>] [<control>] ]+
<what> ::= * |
  [dn[.<basic-style>]=<regex> | dn.<scope-style>=<DN>]
  [filter=<ldapfilter>] [attrs=<attrlist>]
<basic-style> ::= regex | exact
<scope-style> ::= base | one | subtree | children
<attrlist> ::= <attr> [val[.<basic-style>]=<regex>] | <attr> , <attrlist>
<attr> ::= <attrname> | entry | children
<who> ::= * | [anonymous | users | self
  | dn[.<basic-style>]=<regex> | dn.<scope-style>=<DN>]
  [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>]
<access> ::= [self]{<level>|<priv>}
<level> ::= none | disclose | auth | compare | search | read | write | manage
<priv> ::= {=|+|-}{m|w|r|s|c|x|d|0}+
<control> ::= [stop | continue | break]
```

# CONFIGURATION OPENLDAP/LDAP

---



# Configuration serveur

- /etc/openldap
  - Dans les derniers version, la configuration de OpenLDAP est dans openldap (il faut faire des Idapmodify)
  - On peut toujours faire un fichier slapd.conf (plus licence) et générer la configuration avec slapttest
  - Slapttest permet de vérifier la validité des configurations
- Avoir des certificats valide pour faire du LDAP
- Certaines actions ont besoin de LDAPS (par exemple changer un mot de passe).

# Configuration Client

- Provider: /etc/nsswitch.conf
  - Passwd: compat ldap
  - Group: compat ldap
  - Shadow: compat
- /etc/nscd.conf
- /etc/nslcd.conf
- /etc/openldap/ldap.conf
  - BASE dc=ccc,dc=cdc,dc=fr
  - URI ldap://hpc01
  - #SIZELIMIT 12
  - #TIMELIMIT 15
  - #DEREF never
  - TLS\_CACERTDIR /etc/openldap/certs

# HPC

---



# HPC ?

- Qui utilise le LDAP dans le centre de calcul ?
- Tout le monde
  - Les nœuds de calcul
  - Les home utilisateurs
  - Le stockage distribué
  - Les services (Web, visu distante, ...)
- Quelle Qualité de Service ?
  - Performance
    - Tous les nœuds accèdent en parallèle
      - Cache
  - Fiabilité
    - Tous les services accèdent au LDAP pour fonctionner
      - Redondance

# Renseignement de l'annuaire

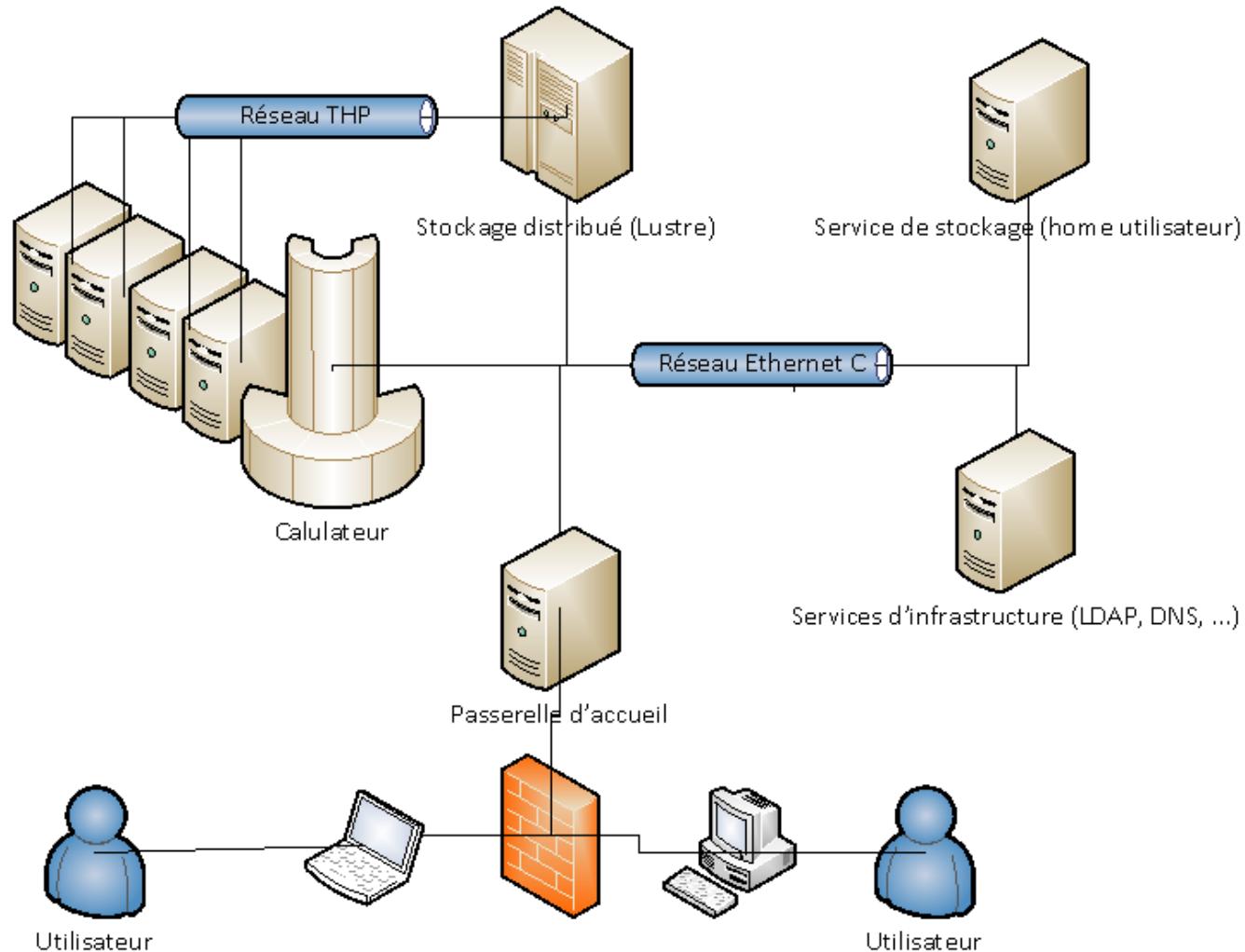
- Comment est rempli le LDAP ?
- Un outil de création de compte qui:
  - Créer les home directory
  - Créer les objets dans l'annuaire
    - Trouve un
      - Uid
      - Gid
    - De libre et l'affecte
  - Donne des quotas
  - ...
- L'outil modifie également les comptes:
  - Doit être capable de faire un DELTA
- Le LDAP est seulement écrit par cet outil.

# Schema

- Schema standard
  - include /etc/openldap/schema/corba.schema
  - include /etc/openldap/schema/core.schema
  - include /etc/openldap/schema/cosine.schema
  - include /etc/openldap/schema/duaconf.schema
  - include /etc/openldap/schema/dyngroup.schema
  - include /etc/openldap/schema/inetorgperson.schema
  - include /etc/openldap/schema/java.schema
  - include /etc/openldap/schema/misc.schema
  - ..
- Un schema maison avec les spécificités
  - include /etc/openldap/schema/ccc.schema
  - Contient par exemple les adresses mails autorisées à sortir du centre de calcul

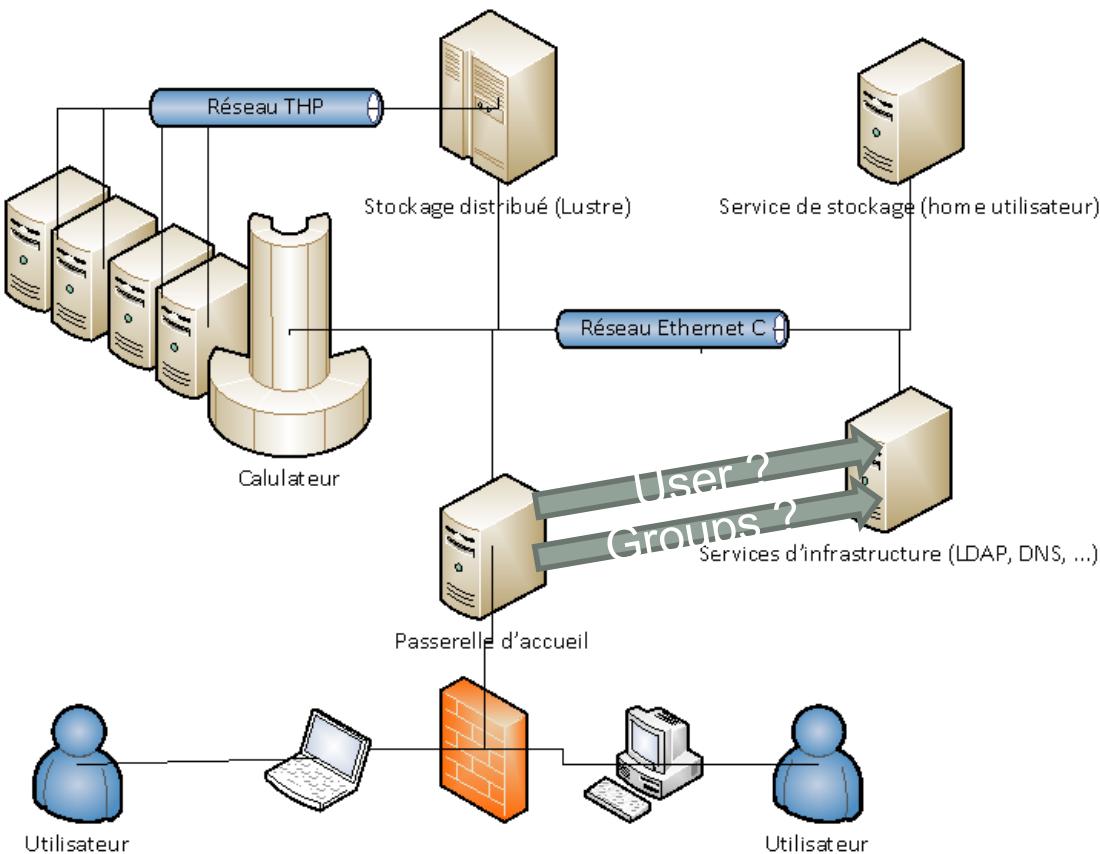
# LDAP dans le CDC

Aperçu et déroulement sans aucun cache



# LDAP dans le CDC

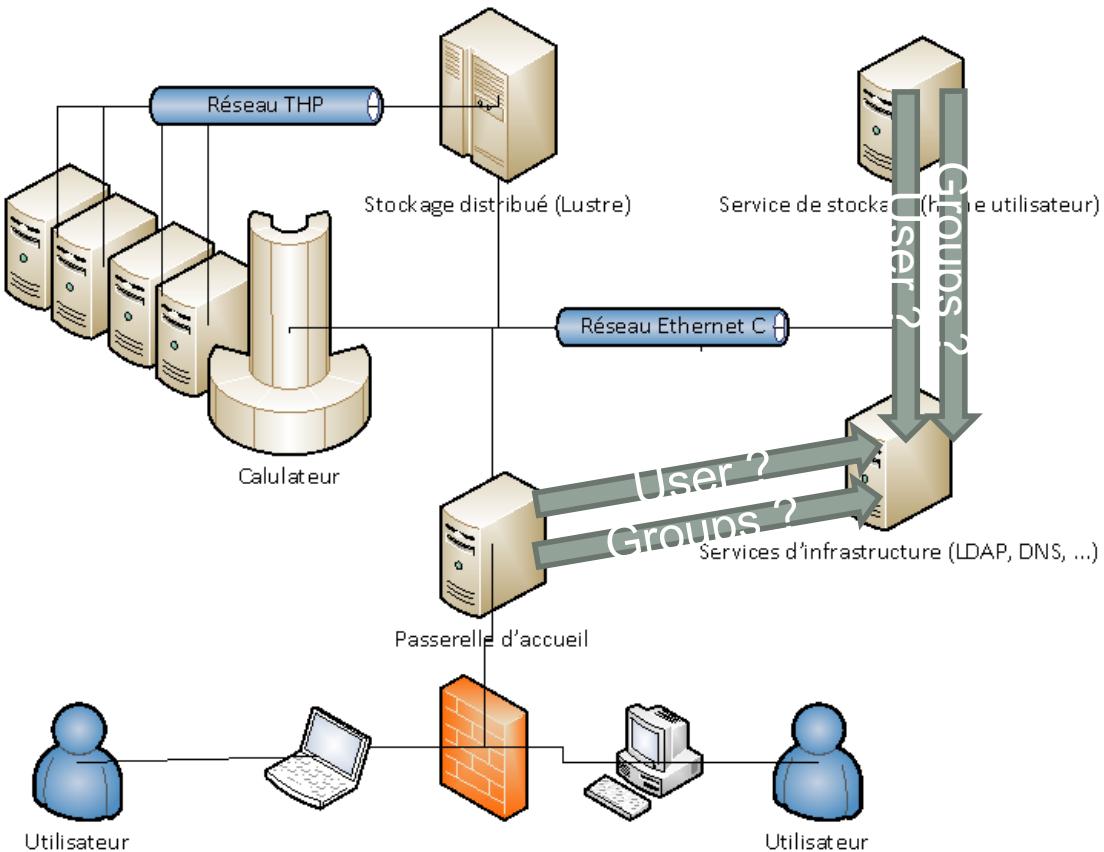
Connexion de l'utilisateur sur la machine d'accueil



Connexion en SSH.  
Configuration de ssh:  
AllowGroups: projecttoto

# LDAP dans le CDC

Le bash s'ouvre dans la home



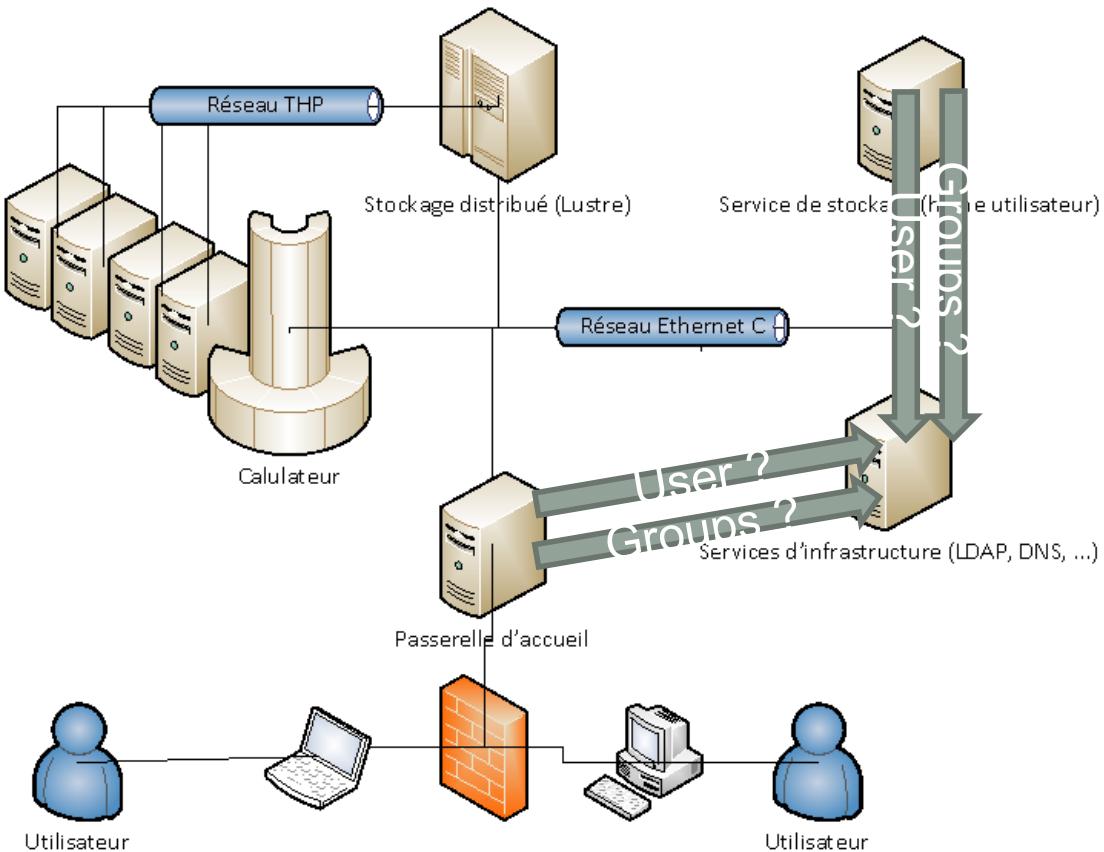
Ouverture de Bash  
dans la racine de la  
home:

Quel est l'uid ?  
Quel groupe ?

READIR NFS le filer:  
Quel est l'uid ?  
Quel groupe ?

# LDAP dans le CDC

Le bash s'ouvre dans la home



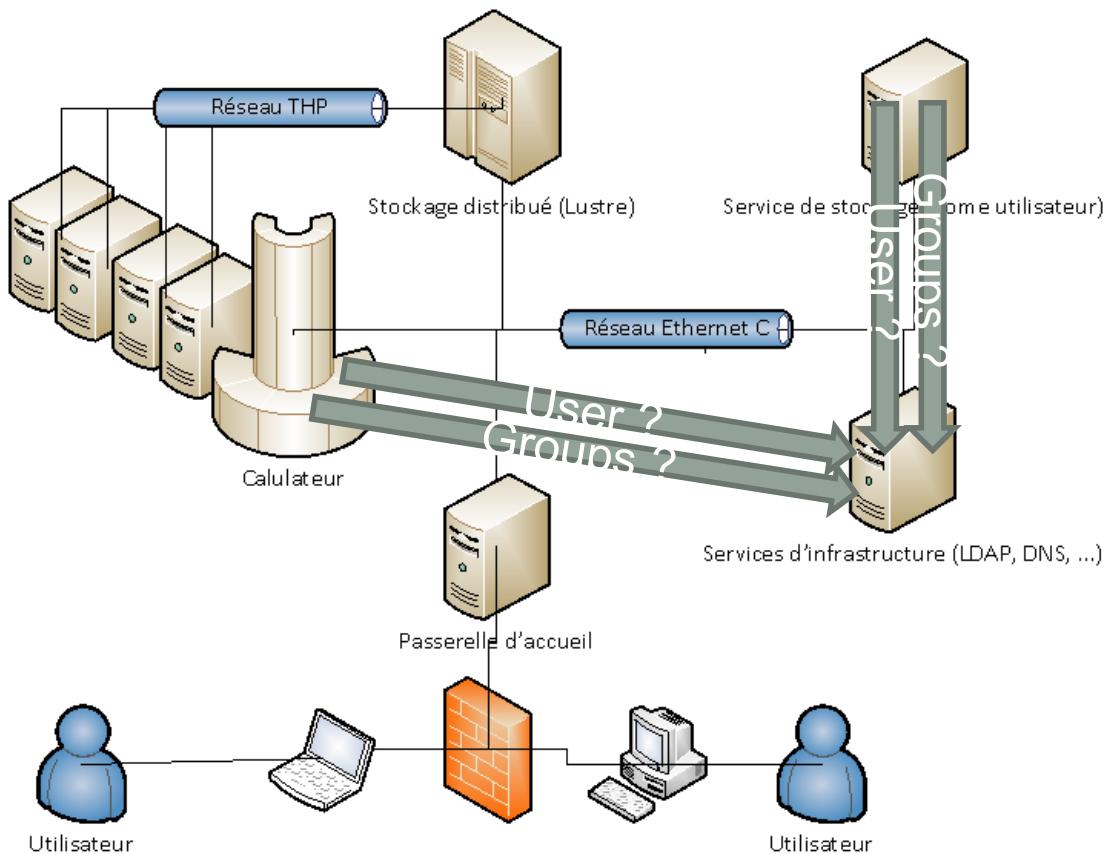
Ouverture de Bash  
dans la racine de la  
home:

Quel est l'uid ?  
Quel groupe ?

READIR NFS le filer:  
Quel est l'uid ?  
Quel groupe ?

# LDAP dans le CDC

Connexion au calculateur



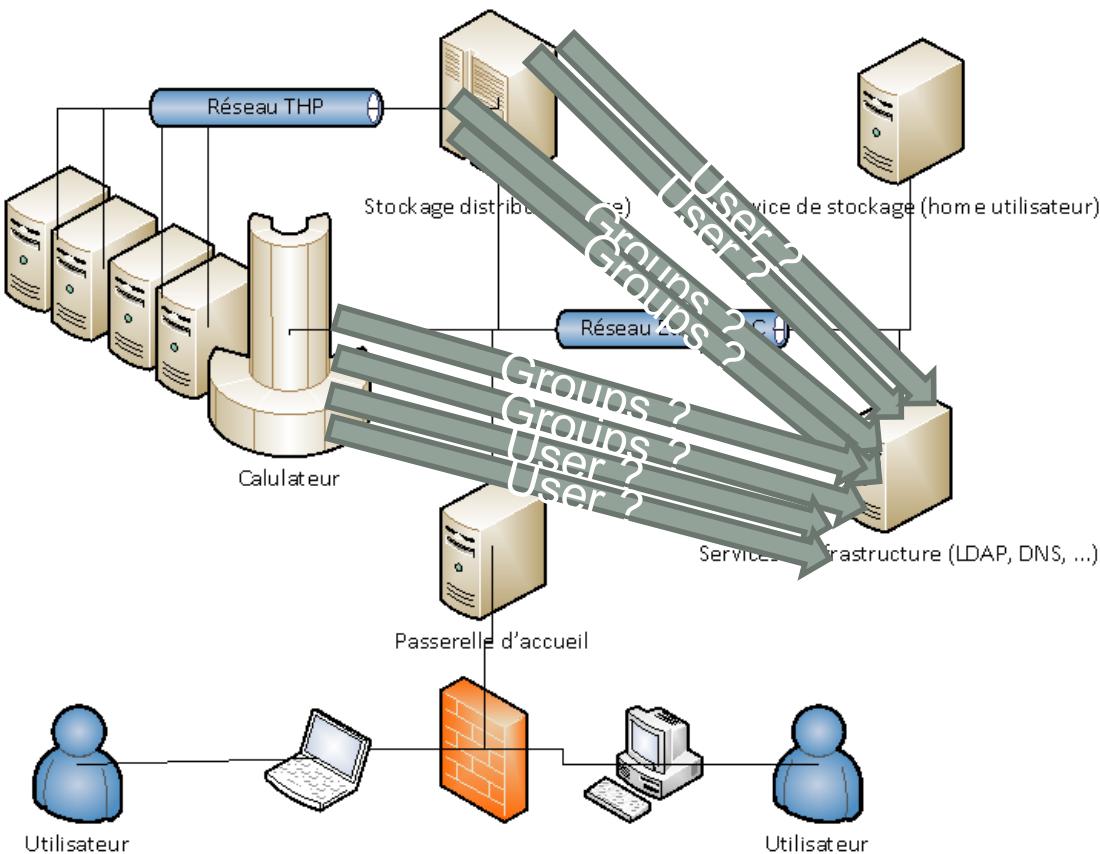
Connexion en SSH.  
Configuration de ssh:  
AllowGroups: projecttoto

Ouverture de Bash  
dans la racine de la  
home:  
Quel est l'uid ?  
Quel groupe ?

READIR NFS le filer:  
Quel est l'uid ?  
Quel groupe ?

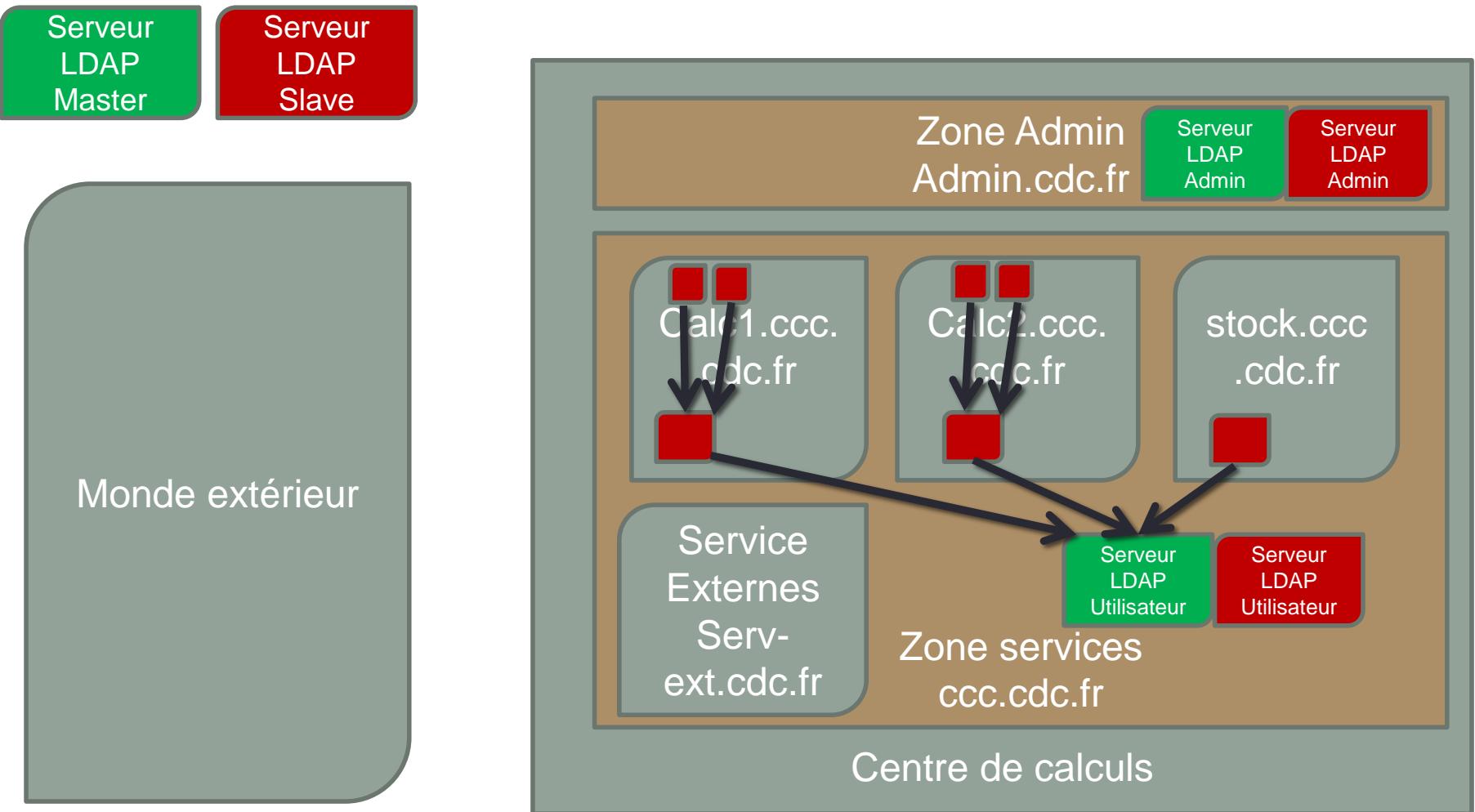
# LDAP dans le CDC

L'utilisateur lance un job qui produit et accède au stockage distribué



Chaque nœud du calculateur et du stockage distribué vérifie les accès

# Le centre de calcul

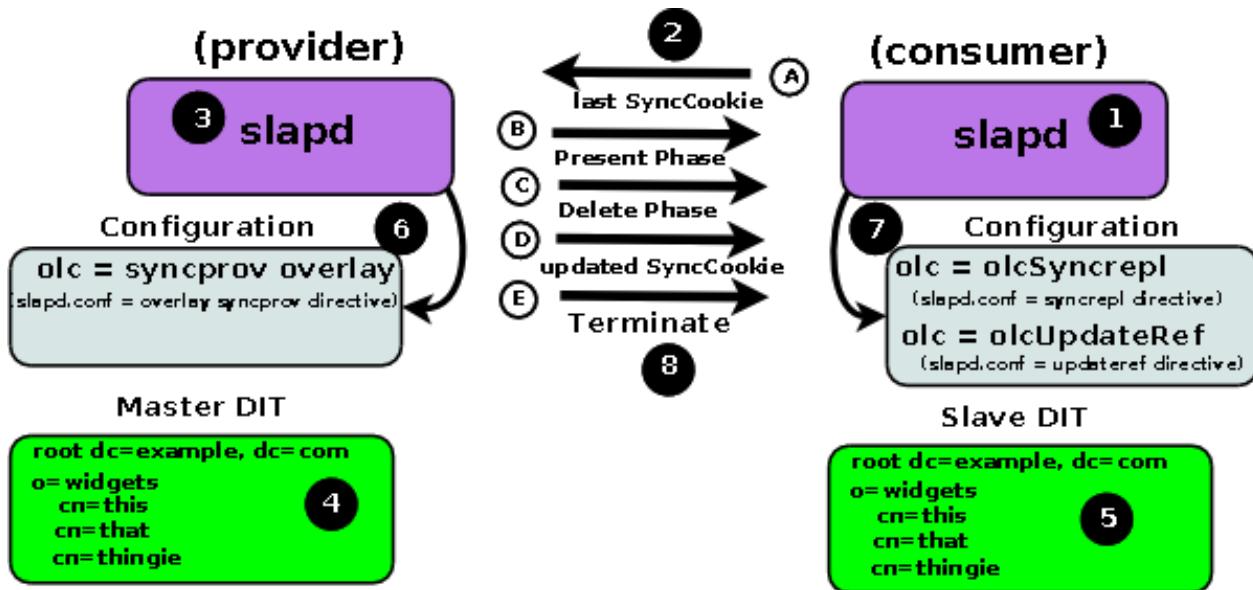


# Passage à l'échelle et fiabilité

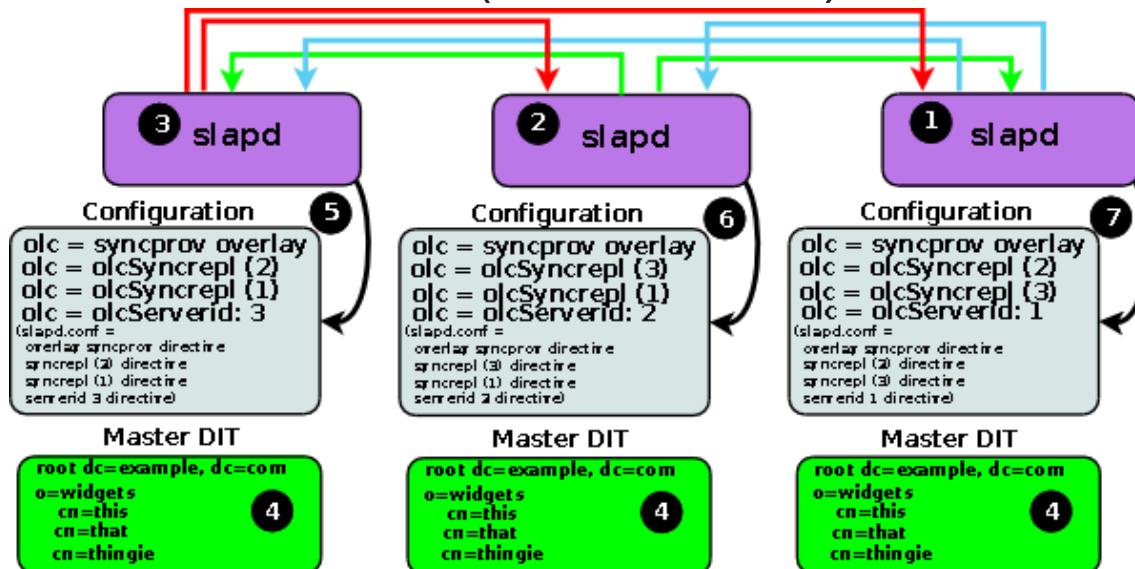
- Les serveurs d'accès au centre de calcul:
  - être fiable et les bases mises à jours dans un délai cours.
  - Protégé des éventuels piques de charge générés par le calculateur
- Les nœuds de calcul
  - Limite les accès parallèles sur un service
  - Accès très rapide aux informations

# Replication

- Maitre/Eslave



- Maitre/Maitre (MultiMaster)

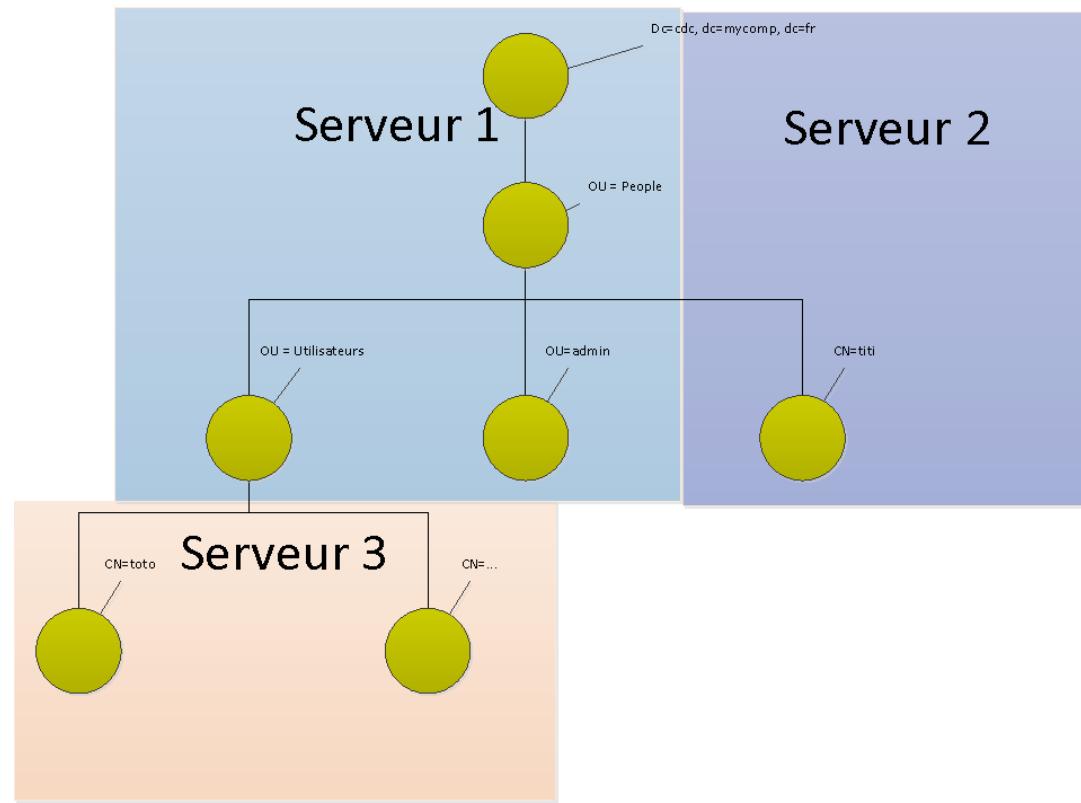


# Replication

- Master/Slave
  - Configuration classique
  - # Replication
  - syncrepl rid=123
    - provider=ldap://primary-ldap.ccc.cdc.fr
    - type=refreshOnly
    - interval=00:00:02:00
    - retry="60 +"
    - searchbase="dc=ccc,dc=cdc,dc=fr"
    - filter="(objectClass=\*)"
    - scope=sub

# Solutions non adaptées: références

- Déclaration d'un même annuaire sur plusieurs serveurs
  - Utilisation de références
  - Utile pour des bases avec beaucoup d'entrée
  - Dépend de l'organisation



# Round Robin

- Round Robin avec le DNS
  - Sur des serveurs Slave pour le calculateur.
- Round robin:
  - Ldap.ccc.cdc.fr -> 172.20.10.1
  - Ldap.ccc.cdc.fr -> 172.20.10.2
- En général pas en zone ccc.cdc.fr.
  - Pas besoin de repartir la charge
  - On veut de préférence utiliser un serveur.
    - Pour les logs, ... (si pas de centralisation)
    - Sauf en master/master

# HLB, SLB

- Hardware Load Balancer
  - Modèles
    - CISCO ACE
    - F5
- Software Load Balancer
  - HAProxy
  - Keepalived
- Solutions à base de Heartbeat/pacemaker/corosync/...
  - Fragiles en cas de double coupure, ...
- Principe
  - Deux machines/Appliance en HA (actif/actif actif/passif) qui sonde à intervalle régulier les serveurs LDAP pour envoyer les requêtes au moins chargé.
- Problématiques
  - Certificats

# QUESTIONS

