Institut Pythéas
Observatoire des Sciences de l'Univers
Aix*Marseille Université

Aix*Marseille université
Initiative d'excellence

Annuaire LDAP
Utilisation au sein d'un Institut de recherche

Julien LECUBIN

Adrien MALGOYRE

IUT R&T - Décembre 2022

Service Informatique Pythéas (SIP)

1300 personnes

12 sites

8 Unités de recherche

Service Informatique Pythéas (SIP)

Julien LECUBIN - Ingénieur de Recherche au CNRS depuis 2003

Responsable infrastructure Systèmes – DSI adjoint

IUT R&T Promo 1999

Adrien MALGOYRE - Ingénieur de Recherche au CNRS depuis 2010

Responsable réseau et systèmes d'authentifications

IUT R&T Promo 2008

Equipe SIP
12 Agents
12 Sites

Support aux laboratoires de recherche

Soutien scientifique

Sommaire

1. Introduction
2. Annuaire LDAP
3. Éléments de fonctionnement
4. LDAP en pratique à l'institut Pythéas

Introduction LDAP – Objectif

Réunir plusieurs bases de données au sein d'un unique annuaire informatique

- Des fichiers Microsoft Excel du personnel administratif
- Des fichiers Microsoft Access du personnel enseignant
- Des accès de comptes UNIX */etc/passwd et /etc/groups*
- Des listes de diffusion
- Des accès de comptes Microsoft Windows (Session, Partages, Exchange…)
- D'autres bases (MySQL, PostgresSQL, Oracle, fichiers CSV…)

Exemple dans l'annuaire AMU qui contient des milliers de comptes:

- **Comment faire une page web avec les noms/prénoms des étudiants IUT R&T?**
- **Comment diffuser un e-mail à la promo R&T 2023**

Introduction LDAP – Concept

Un annuaire est comme une base de données…

→ On peut y mettre des informations et les consulter

Cependant un annuaire est spécialisé :

→ Dédié à la lecture plus qu'à l'écriture

→ L'accès aux données se fait par des recherches multicritères

Son objectif est de maintenir de façon cohérente et contrôlée une grande quantité de données.

Exemples d'annuaire :

- carnet d'adresses
- annuaire téléphonique
- répertoire des rues
- et plus: certificats SSL, Trombinoscope…

Introduction LDAP – Concept

Différences annuaires/SGBD

SGBD: Système de gestion de base de données (MySQL, Postgresql, Oracle…)

Dans un annuaire LDAP:

- Pas de dépendances entre les objets stockés
- Les objets peuvent être distribués sur plusieurs annuaires pour assurer une meilleure disponibilité
- Les applications de l'annuaire n'ont pas besoin de connaître la structure interne des données stockées
- L'accès aux données est plus simple

Annuaire LDAP

L’annuaire LDAP

LDAP → Lightweight Directory Access Protocol

Héritier de l’annuaire X500 (proposé par l’ISO)

- Standard conçu par les opérateurs télécom pour interconnecter leurs annuaires téléphoniques
- X500 adapté à l’internet → LDAP (même modèle de schéma, . . .)

LDAP a été proposé en 1995 :

- Standard d’annuaire au dessus de TCP/IP
- Version 3 actuellement (RFC 2251) depuis 1997

1995

Standard d’annuaire

Objectifs

- Fournir aux utilisateurs des informations fiables, facilement accessibles
- Permettre aux utilisateurs de mettre à jour eux-mêmes leurs informations personnelles
- Rendre les informations accessibles de façon contrôlée
- Eviter la redondance d'informations : un seul annuaire pour l'ensemble des services
- Faciliter la gestion (administration) des postes de travail, des équipements réseau…

→ Tout ceci est fait sans remettre en cause les applications existantes

Concepts

LDAP définit :

- **Un protocole**: accéder à l'information contenue dans l'annuaire
- **Un modèle de nommage**: comment l'information est organisée et référencée
- **Un modèle d'information**: le type des informations contenues dans l'annuaire
- **Un modèle de fonctionnement**: comment accéder à l'information (syntaxe des requêtes, etc. . .)
- **Un modèle de sécurité**: comment données et accès sont protégés
- **Un modèle de duplication**: comment la base est répartie entre serveurs
- **Des API**: pour développer des applications clientes
- **Le format LDIF**: un format d'échange de données.

Les serveurs LDAP

Il existe plusieurs serveurs LDAP exploitant le protocole.

Les plus connus:

Microsoft
Active Directory

Kerberos + SMB + DNS + LDAP

IBM Domino

Apple opendirectory

Le protocole

Protocole LDAP

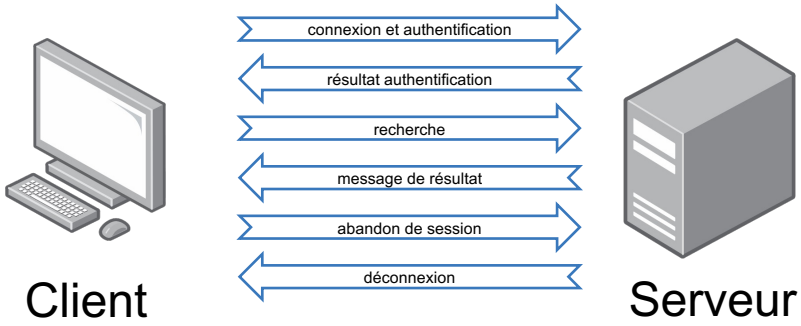
Le protocole définit :

- Comment s'établit la communication client-serveur :
  - → Commandes pour se connecter à l'annuaire ou s'en déconnecter
  - → Commandes pour rechercher, comparer, créer, modifier ou effacer des entrées.
- Comment s'établit la communication serveur-serveur :
  - → Echanger leur contenu et le synchroniser (réplication service)
  - → Créer des liens permettant de relier des annuaires les uns aux autres.
- Des mécanismes de sécurité :
  - → Méthodes de chiffrement et d'authentification
  - → Mécanismes de règles d'accès aux données.
- Un format de transport de données :
  - → Pas l'ASCII (comme pour HTTP, SMTP. . .) mais le LBER : Lightweight BER

Protocole LDAP

Les opérations de base :

- Connexion au service : bind, unbind, abandon
- Interrogation : search, compare
- Mise à jour : add, delete, modify, rename



TCP 389

LDAP non sécurisé
LDAP + chiffrement TLS

TCP 636

LDAP + chiffrement SSL
→ LDAPS

Contenu de l’annuaire:

Le modèle de nommage

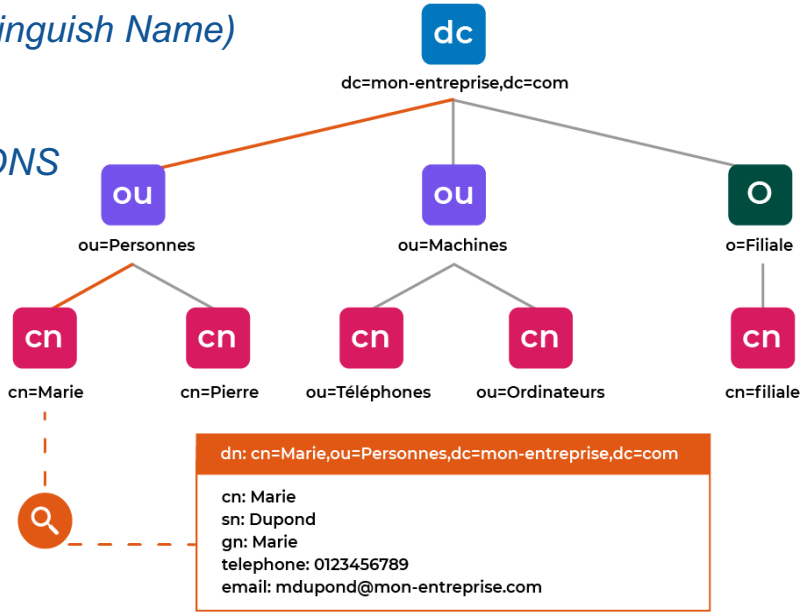
Le modèle de nommage

Le modèle de nommage définit comment les entrées de l'annuaire sont référencées et organisées

LDAP fonctionne sur une structure arborescente

- Structure logique hiérarchique sous forme d'Arbre : le DIT *(Directory Information Tree)*
- Une entrée est identifiée par un nom unique : le DN *(Distinguish Name)*

  et le RDN (Relative Distinguish Name)
- Par convention le DC *(Domain Component) = Domaine DNS*



Exemple de la fiche d'un étudiant d'AMU:

- Base DN (Racine):
  dc=univ-amu,dc=fr
- OU (Unité Organisationnelle) des personnels et étudiants:
  ou=people,dc=univ-amu,dc=fr
- RDN de l'étudiant John Doe (code INE *s21228888*) :
  uid=s21228888
- DN de John Doe (code INE *s21228888*) :
  uid=s21228888,ou=people,dc=univ-amu,dc=fr

Contenu de l’annuaire:
Le modèles d’information

Le modèle d'information

Le modèle d'information définit le type des données pouvant être stockées dans l'annuaire

- L'entrée: élément de base de l'annuaire

  Elle contient les informations sur un objet de l'annuaire.

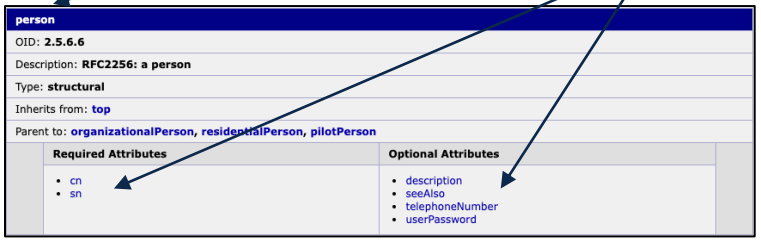
- Les informations de l'entée

  Représentées sous la forme d'attributs décrivant les caractéristiques de l'objet.

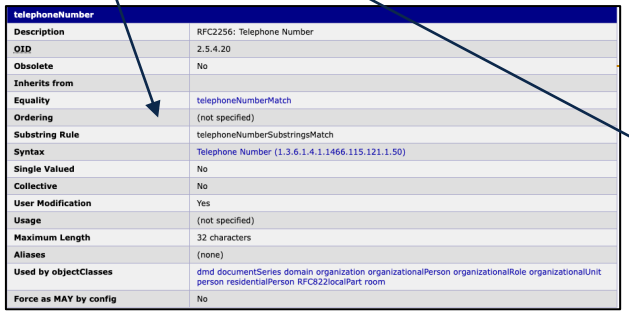
- Les schémas de l'annuaire

Définissent la liste des classes d'objets qu'il connaît:

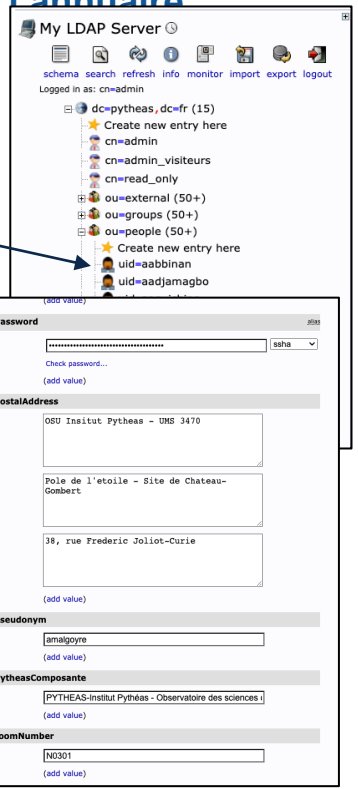
→ Leurs types d'attributs et leur syntaxe.



person	
OID: **2.5.6.6**	
Description: **RFC2256: a person**	
Type: **structural**	
Inherits from: **top**	
Parent to: **organizationalPerson, residentialPerson, pilotPerson**	
Required Attributes	**Optional Attributes**
• cn • sn	• description • seeAlso • telephoneNumber • userPassword



telephoneNumber	
Description	RFC2256: Telephone Number
OID	2.5.4.20
Obsolete	No
Inherits from	
Equality	telephoneNumberMatch
Ordering	(not specified)
Substring Rule	telephoneNumberSubstringsMatch
Syntax	Telephone Number (1.3.6.1.4.1.1466.115.121.1.50)
Single Valued	No
Collective	No
User Modification	Yes
Usage	(not specified)
Maximum Length	32 characters
Aliases	(none)
Used by objectClasses	dmd documentSeries domain organization organizationalPerson organizationalRole organizationalUnit person residentialPerson RFC822localPart room
Force as MAY by config	No



Example:
« Louis » (**entrée**) est une personne (**classe d'object**) étudiante (**classe d'objet**)
Il a donc *forcément* nom (**attribut**) et un code INE (**attribut**) dont la **syntaxe** est:
11 caractères, soit 10 chiffres et 1 lettre soit 9 chiffres et 2 lettres

Le modèle d'information

Chaque entrée de l'annuaire fait obligatoirement référence à au moins une classe d'objet du schéma et ne doit contenir que des attributs qui sont rattachés au type d'objet en question.

L'objet *inetOrgPerson* à la filiation suivante :

→ L'objet person a comme attributs :

commonName, surname, telephoneNumber, userPassword…

→ L'objet fils *organizationalPerson* **ajoute** des attributs tels que:

title, postalAddress…

→ Les objets petit-fils *inetOrgPerson* et *EtudiantAMU* **ajoutent** des attributs tels que :

mail, labeledURI, uid (userID), photo…

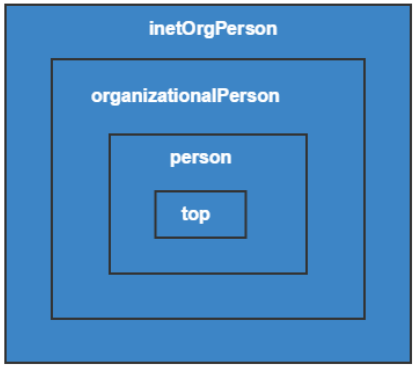
Code INE, Promo, Section, Campus,Tuteur

Remarques :

• Une entrée peut appartenir à un nombre non limité de classes d'objets.

• Les attributs obligatoires sont la réunion des attributs obligatoires de chaque classe.

objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: EtudiantAMU



Contenu de l’annuaire:
Le modèle de fonctionnement

Le modèle de fonctionnement

Une fois les données stockées et référencées, il faut permettre d'utiliser ces données

Pour cela, LDAP définit un modèle de fonctionnement (syntaxe des requêtes). Il définit les opérations possibles sur les données.

On recense 4 types d'opérations:

- opérations d'interrogation: requête pour accéder aux données (search)
- opérations de comparaison: renvoie vrai ou faux si égal (compare)
- opérations de mise à jour: add, delete, rename, modify
- opérations d'authentification et de contrôle: bind, unbind, abandon

(attribut=valeur)	égalité
(attribut~=valeur)	approximation
(attribut!=valeur)	différence
(attribut>=valeur)	supérieur
(attribut<=valeur)	Inférieur

(attribut=user1*)	Attribut débute par user1
(attribut=*)	attribut a une valeur

Contenu de l’annuaire:

Le modèle de sécurité

Le modèle de sécurité

Le modèle de sécurité permet de protéger et gérer l'accès aux données de l'annuaire.

→ Authentification pour se connecter au service LDAP:

- Anonyme : Anonymous authentication,
- Administrateur : Root DN/passwd authentication,
- Utilisateur : User DN/passwd

→ Contrôle de l'accès aux données:

- droits d'accès aux données (fonctions de l'utilisateur authentifié)
- règles définies sous forme d'ACL (Access Control List)

→ **Chiffrement** des transactions (LDAP+SSL, . . .) et des attributs type mot de passe (MD5/SSHA….)

Contenu de l’annuaire:
Le modèle de duplication

Le modèle de duplication

Il définit comment dupliquer l'annuaire sur plusieurs serveurs.

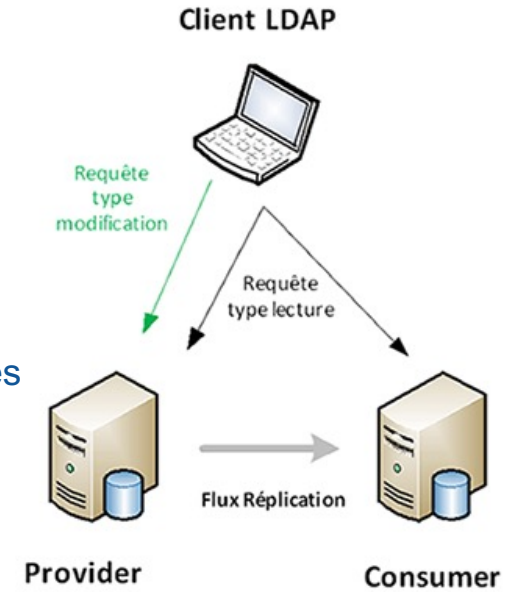
- → améliorer le temps de réponse
- → être tolérant aux pannes

Deux types de serveurs LDAP

- → serveur maitre (provider): fournit les données
- → serveur esclave (consumer server): reçoit les données du/des maîtres

Possibilité de partitionner l'annuaire (éclatement sur plusieurs serveurs)

Proxy LDAP



Le format LDIF

LDIF

LDIF → LDAP Interchange Format

Standard de représentation des entrées LDAP sous format texte.

Permet de :

- faire des imports/exports de la base ou d'une partie de la base
- créer, ajouter, modifier, . . .

Ajout d'attributs dans une fiche existante avec LDIF

```
dn: uid=Marcia Garza,ou=People,dc=example,dc=org
changetype: modify
add: telephonenumber
telephonenumber: +1 408 555 8283
-
add: building
building: sc09
```

Création d'un arbre LDAP avec LDIF

```
dn: dc=example,dc=org                    Identifiant de l'entrée « dc=example »
dc: example                              //
description: Serveur exemple             //
objectClass: dcObject                    // Attributs de l'entrée example
objectClass: organization                //
o: Serveur exemple                       //

dn: ou=people, dc=example,dc=com         Identifiant de l'entrée « ou=people »
ou: people                               //
objectClass: organizationalUnit          // Attributs de l'entrée people

dn: cn=admin, ou=people,                 Identifiant de l'entrée « cn=admin »
dc=example,dc=com                        //
description: Administrateur LDAP         //Attributs de l'entrée admin
objectClass: organizationalRole          //
cn: admin
```

LDIF

Récupérons le LDIF de l'étudiant s123456789

```
[root@cluster ~]# ldapsearch -h annuaireldap.univ-amu.fr -p 389 -D "uid=arnaud.fevrier,ou=People,dc=univ-amu,dc=fr » -w "ARNAUDPA$$WORD" -x -b "dc=univ-amu,dc=fr" uid=s123456789
```

```
dn: uid=s123456789,ou=People,dc=univ-amu,dc=fr

objectClass: inetOrgPerson
objectClass: eduPerson
objectClass: supannPerson
objectClass: posixAccount

cn: NOM Prénom
supannEtuSecteurDisciplinaire: {CODE}01
supannEtuTypeDiplome: 24


uidNumber: 12345678
gidNumber: 513
loginShell: /bin/bash
homeDirectory: /home/etudiant/ 12345678
```

- Saut de ligne = autre entrée
- Commentaires: #

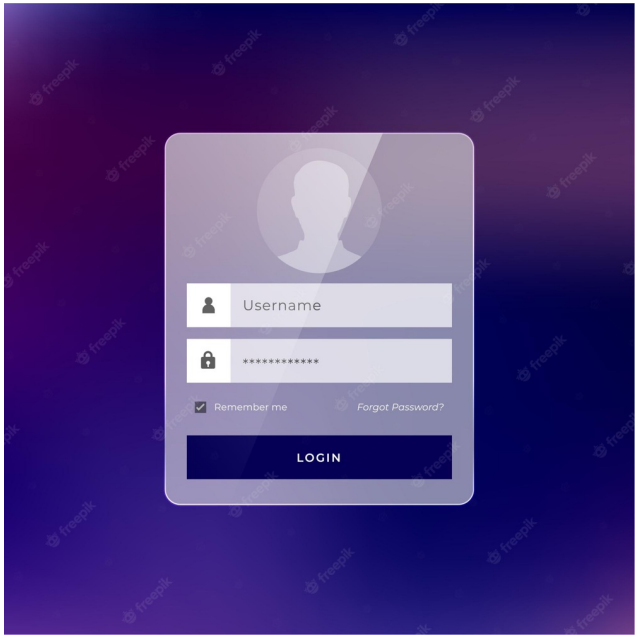
API

API

Les langages couramment utilisés savent exploiter LDAP via modules/librairies (PHP, Java, Perl, Python)

Example PHP: Tester la validité d'un compte sur l'annuaire (Login/MDP)

```php
<?php

// using ldap bind
$ldaprdn  = 'username';  // ldap rdn or dn
$ldappass = 'password';  // associated password

// connect to ldap server
$ldapconn = ldap_connect("ldap://ldap.example.com")
    or die("Could not connect to LDAP server.");

if ($ldapconn) {
    // binding to ldap server
    $ldapbind = ldap_bind($ldapconn, $ldaprdn, $ldappass);

    // verify binding
    if ($ldapbind) {
        echo "LDAP bind successful...";
    } else {
        echo "LDAP bind failed...";
    }
}


?>
```



API

Example PHP: Afficher le prénom, nom et mail des étudiants inscrits en 2021 et 2022

```php
<?php
//using ldap bind anonymously

//connect to ldap server
$ldapconn = ldap_connect("ldap://ldap.example.com")
    or die("Could not connect to LDAP server.");

if ($ldapconn) {

    // binding anonymously
    $ldapbind = ldap_bind($ldapconn);

    $dn = "dc=univ-amu,dc=fr";
    $filter="(|(EtuInscription=2022)(EtuInscription=2023))";
    $justthese = array("sn", "givenname", "mail");

    $sr=ldap_search($ds, $dn, $filter, $justthese);

    $info = ldap_get_entries($ds, $sr);

    echo $info["count"]." entries returned\n";
    for ($i=0; $i<$info["count"]; $i++) {
        echo $info[$i]["sn"][0];
        echo $info[$i]["givename"][0];
        echo $info[$i]["mail"][0];
    }

}

?>
```

Annuaire LDAP dans le contexte de l'Institut Pythéas

Annuaire LDAP de l'institut (1/2)

- **Gestion centralisée des comptes utilisateurs (2000 entrées) et des groupes (400 entrées)**
- **Annuaire LDAP multi-sites**
- **En RW sur un site (maitre)**
- **En RO sur l'ensemble des autres sites (esclaves)**
- **Réplication par syncrepl (1 Maitre → N esclaves en mode synchrone)**
- **1 LDAP de site = 1 machine virtuelle**
    - Ressources attribuées :
        - 1 cœur CPU / 8 Go RAM / 20 Gb disques (OS Debian + base LDAP)
- **Taille de la base LDAP : 35 Mo**

Annuaire LDAP de l'institut (2/2)

- **Généralités**
  - Chaque annuaire LDAP est spécifique et correspond à des besoins liés à la structure
  - Structures des branches spécifiques
  - ACL en fonction de la sécurité à adopter
  - Utilisation d'outils spécifique pour la gestion de l'annuaire
    - Chez nous OpenLDAP (opensource) et ActiveDirectory (propriétaire)

Administration de l'annuaire (1/5)

Nécessité dans notre contexte d'utiliser une interface web pour simplifier l'administration de l'annuaire LDAP

- Ajouter / modifier / supprimer un/des utilisateur / groupe
- Modifier le contenu d'un attribut spécifique

L'interface web doit être accessible pour :

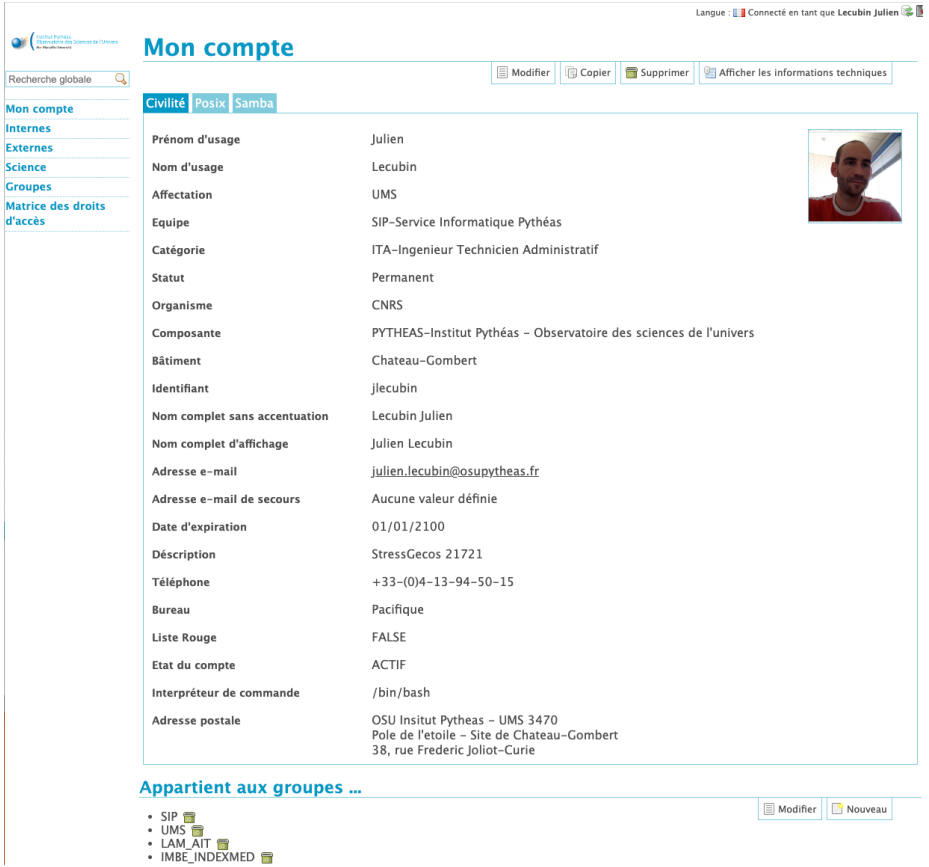
- Le service informatique pour des manips d'administration dans l'annuaire
- Les utilisateurs des labos pour modification d'attributs spécifiques tels que numéro de téléphone, numéro de bureau, photo)

Administration de l’annuaire (2/5)

Interface web ldapsaisie (openLDAP)

- PHP / JavaScript
- Licence GNU
- Société Easter-eggs (1997 - Paris)
- Matrice de droits d’accès
- Cohérence du contenu dans l’annuaire

A Pythéas, utilisé par les utilisateurs, les services administratifs et l’équipe informatique

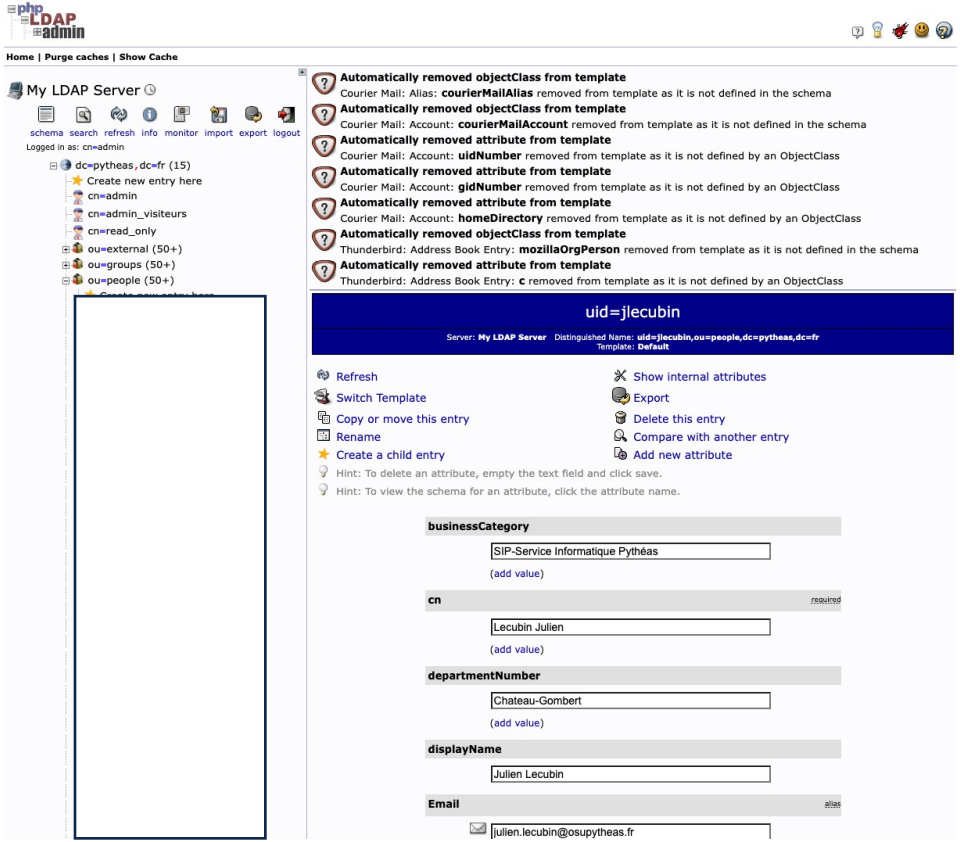


Administration de l'annuaire (3/5)

Interface web phpldapadmin (openLDAP)

- PHP
- Licence GNU
- Possibilité de modifier l'intégralité des champs
- Cas spécifique non couvert par ldapsaisie (champs spécifique à modifier)
- Insertion / modification / export possible par fichier LDIF

A Pythéas utilisé uniquement par l'équipe informatique



Administration de l'annuaire (4/5)

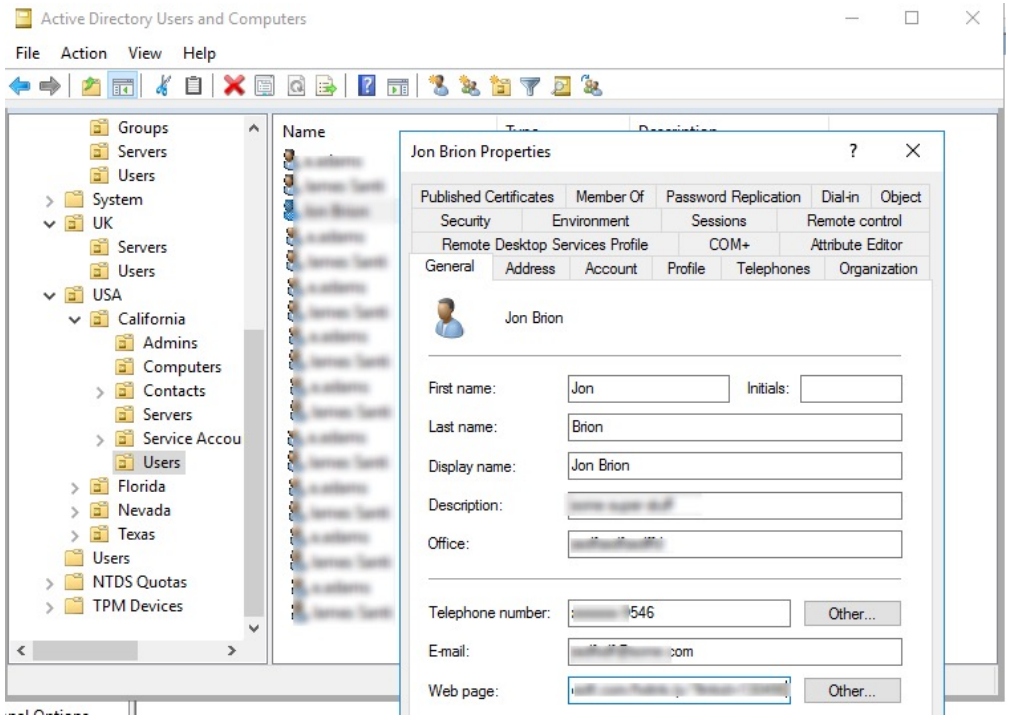
L'interface web n'est pas le seul outil disponible pour intervenir sur un annuaire !

- **Apache Directory studio, AD Explorer (Microsoft), Jxplorer Java LDAP Browser,**
- **Utilisation de la ligne de commande**
  - ldapsearch, ldapadd, ldapmodify, ldapdelete (pour OpenLDAP)
  - Avantages : scripts avec regex pour modification en masse, rapidité d'intervention, simplicité d'accès, nécessité de voir les logs de l'annuaire pour comprendre ce qu'il se passe
- **Développements « maison » (perl, C, python…)**

Administration de l'annuaire (5/5)

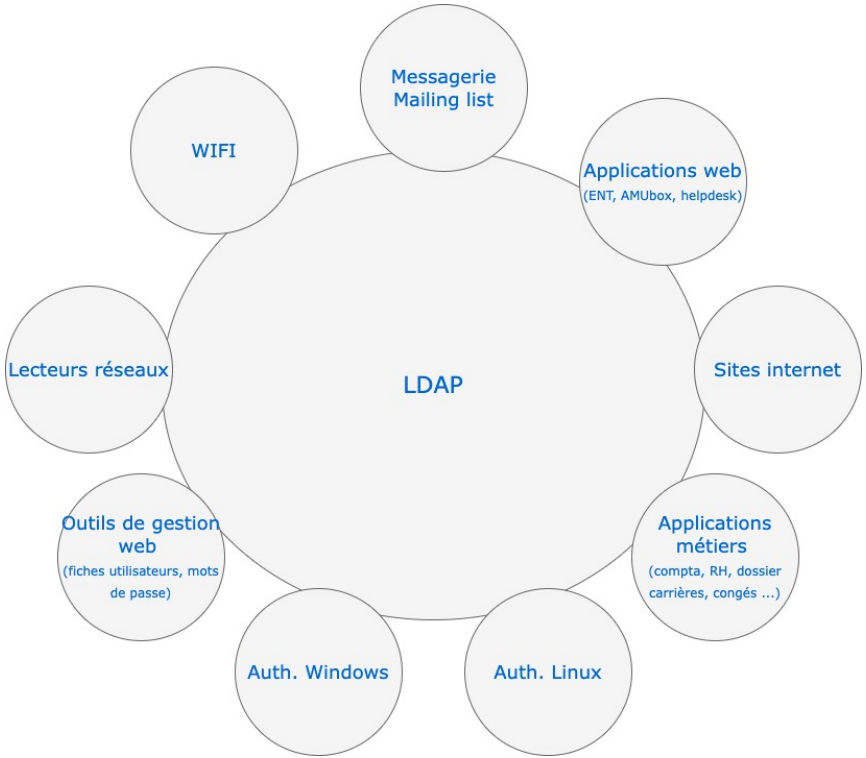
Interface Active Directory explorer

- Microsoft Windows Server
- Client LDAP graphique



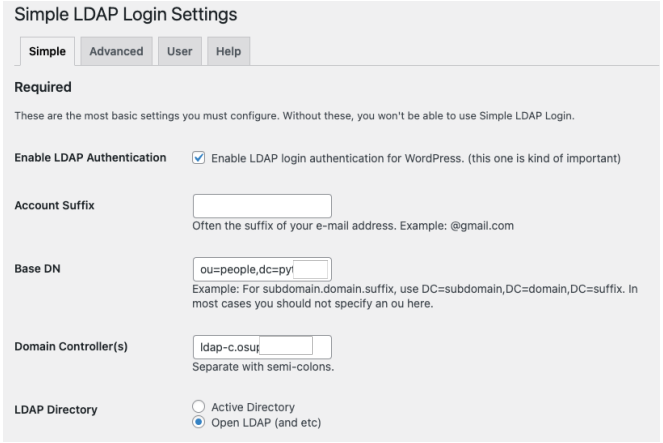
Services utilisant notre annuaire LDAP

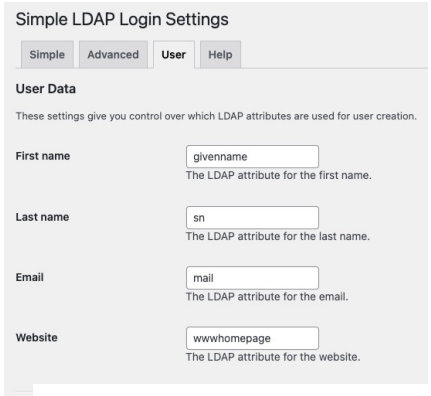
- **On authentifie les utilisateurs mais ce n'est pas que ça !**
- **Avantage d'un annuaire central :**
  - Applications consultent un seul référentiel
  - Unification des procédures de connexion
  - Plus sécurisé, rapidité de déploiement des services à grande échelle
  - Même login / mot de passe partout
- **Inconvénients de la centralisation :**
  - La coupure de l'annuaire provoque l'arrêt de l'accès à tous nos services



CMS Wordpress
Configuration LDAP pour la gestion des sites web

- Authentification LDAP pour l'administration des 100 sites wordpress
- Plugin spécifique, par exemple *Simple LDAP login*
- **Evite l'ajout d'utilisateur manuellement** via l'interface wordpress
- Permet d'attribuer la **gestion du contenu à des utilisateurs / groupes LDAP**
- **Pas de stockage de mot de passe** dans la base de données du CMS (plus de sécurité)



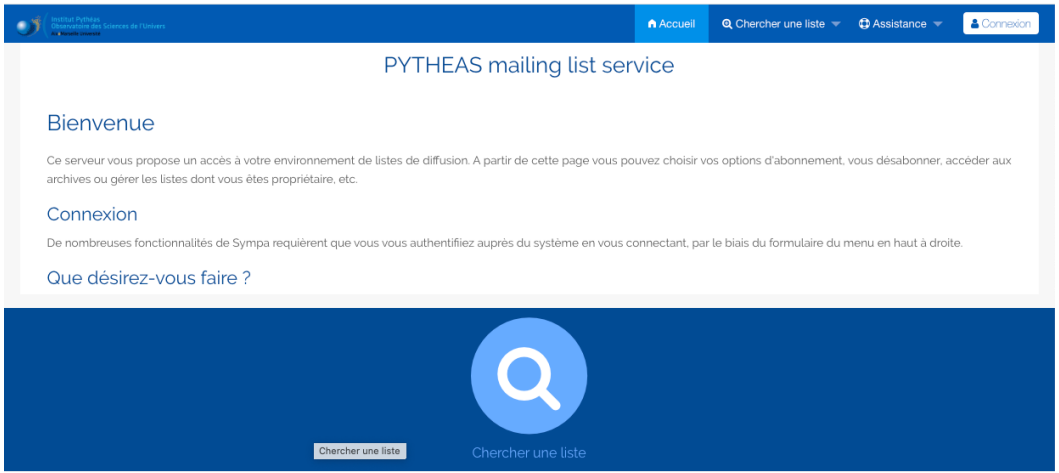


Messagerie (1/3)
Exemple de configuration LDAP pour les listes de diffusion (mailing list)

Liste de diffusion → on s'adresse à un ensemble de personnes par mail

Service de mailing list utilisé → « sympa » (OpenSource)

Sympa sait utiliser LDAP → mais que sait-il faire avec ?



Messagerie (2/3)
Exemple de configuration LDAP pour les listes de diffusion (mailing list)

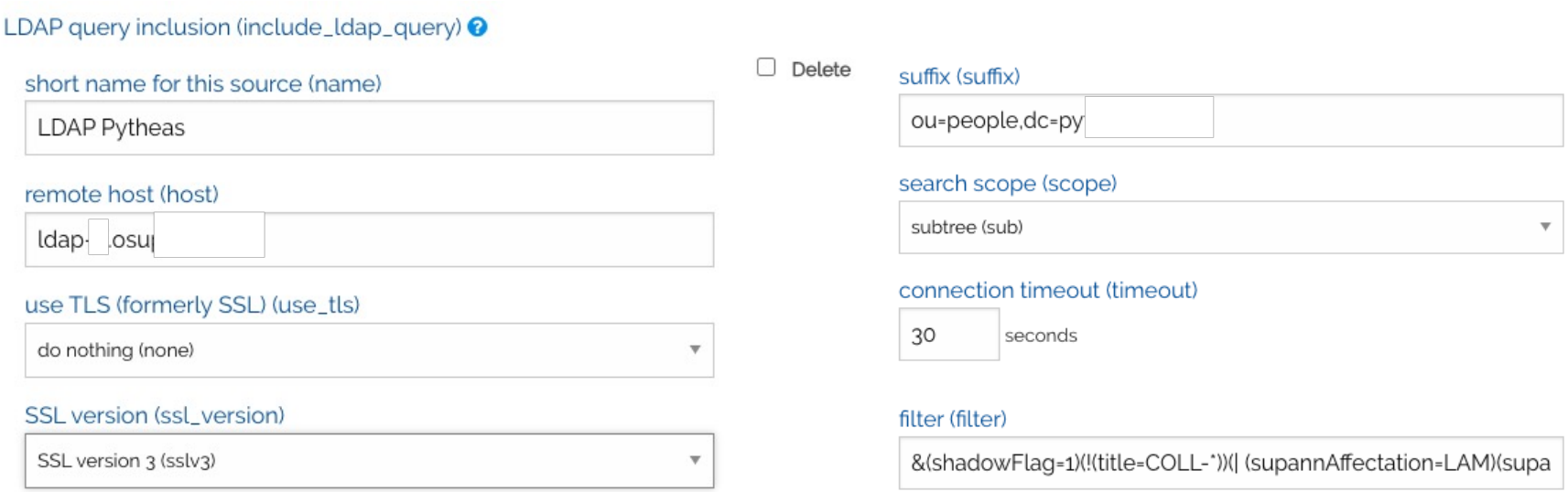
- **Authentification LDAP des utilisateurs pour l'accès au service**
  - possibilité pour un utilisateur de créer une nouvelle mailing list
  - attribution des droits (modération, consultation des archives …)

- **2 types de listes :**
  - listes **statiques** gérées par un / des modérateurs

    Exemple : mailing list de projet scientifique
  - listes **dynamiques** (mise à jour automatique de la liste par requête LDAP)

    Exemple : mailing list des doctorants de l'Institut

Messagerie (3/3)
Exemple de configuration LDAP pour les listes de diffusion (mailing list)



Filter = &(shadowFlag=1)(!(title=COLL-*))(|(supannAffectation=LAM)(supannAffectation=UMS))

ET
- l'attribut *shadowFlag* vaut strictement 1
- l'attribut *title* ne commence pas (symbole **!**) par COLL- (*)
- l'attribut *supannAffectation* vaut strictement LAM OU l'attribut *supannAffectation* vaut strictement UMS

Authentification sous Linux d'un client LDAP
Cas d'authentification via service SSSD

- SSSD : *System Security Services Daemon*
- Possibilité d'utiliser plusieurs fournisseurs LDAP différents
- Authentification par filtre ldap
- Mise en cache des informations d'identités
- Authentification possible hors-ligne

Une mauvaise configuration peut vous bloquer l'accès à distance !

```
[domain/ldap.osup                ]
id_provider = ldap
auth_provider = ldap
chpass_provider = ldap
ldap_uri = ldaps://ldap                    :636
ldap_backup_uri = ldap://ldap-                    :389
ldap_chpass_uri = ldap://ldap-                    :389
ldap_search_base = dc=pyt          dc=fr
ldap_schema = rfc2307
ldap_user_name = uid
ldap_user_uid_number = uidNumber
ldap_user_gid_number = gidNumber
ldap_user_gecos = gecos
ldap_user_home_directory = homeDirectory
ldap_user_shadow_expire = shadowExpire
ldap_user_fullname = cn
ldap_user_email = mail
ldap_group_name = cn
ldap_group_gid_number = gidNumber
ldap_group_member = memberUid
ldap_search_timeout = 6
ldap_network_timeout = 6
ldap_connection_expire_timeout = 900
ldap_page_size = 1000
ldap_tls_reqcert = never
ldap_user_search_base = dc=pyt      ,dc=fr
ldap_access_order = filter
ldap_group_search_base = ou=groups,dc=pyt
enumerate = true
access_provider = ldap
ldap_access_filter = (&(!(shadowFlag=0))(ou:dn:=people))
debug_level = 4
[sssd]
domains = ldap.osu
services = nss, pam
config_file_version = 2
```

Authentification sous Linux d'un client LDAP
Cas d'authentification via service SSSD

- /etc/nsswitch.conf : définit entre autre l'ordre de recherche pour la recherche des utilisateurs et groupe :

```
passwd:     files sss
shadow:     files sss
group:      files sss
```

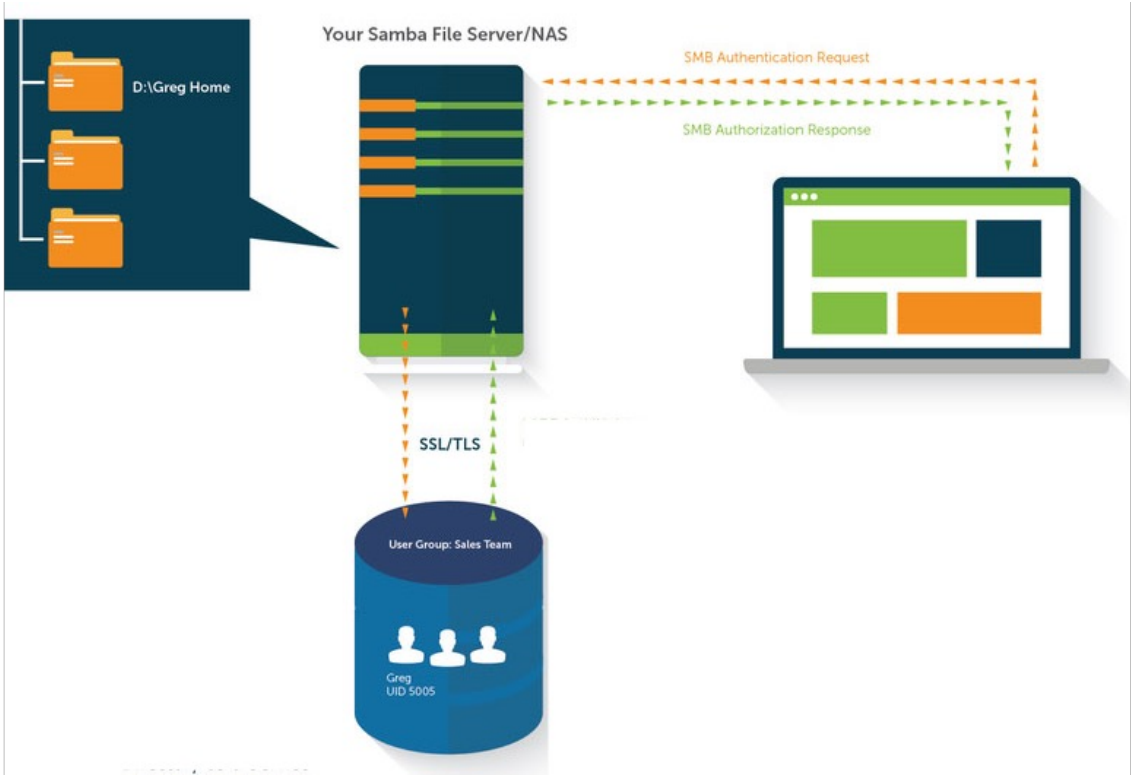
- Pour indiquer à nsswitch d'utiliser le service sssd :

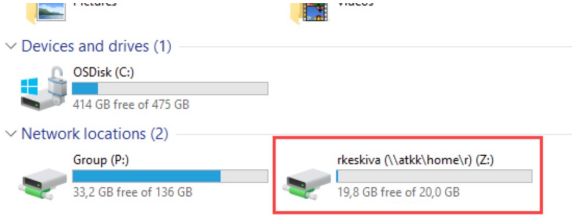
```
[root@server ~]# authconfig --enablesssd --update
```

- *getent passwd* : lister les utilisateurs
- *getent group* : lister les groupes
- *getent passwd $user* : lister un utilisateur spécifique

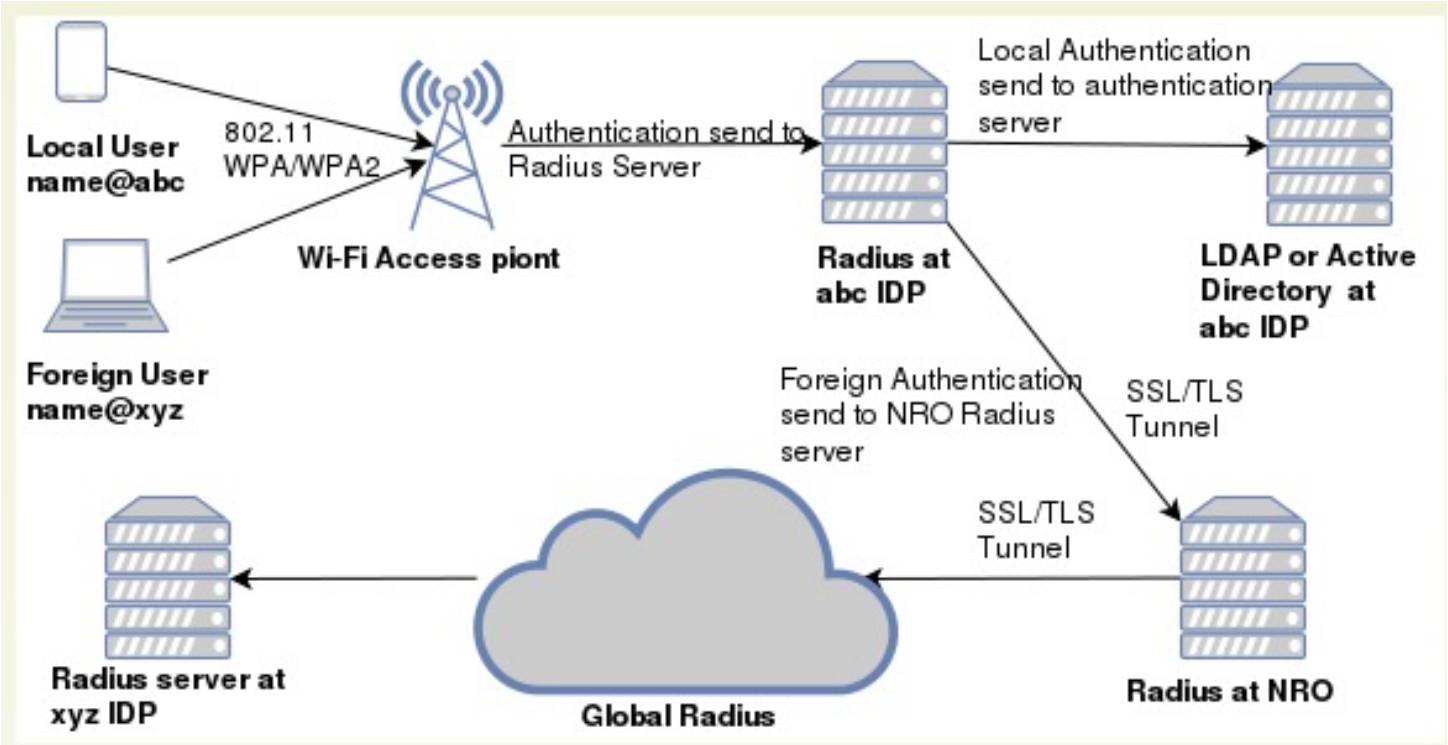
```
[[jlecubin@ssh]:[~] >getent passwd jlecubin
jlecubin:*:6203:5000:Lecubin Julien:/home/jlecubin:/bin/bash
```

Authentification LDAP
Cas des lecteurs réseau (LDAP / SAMBA / CIFS)





Cas du WiFi
Authentification Eduroam



Politique de gestion des comptes et mots de passe

- **Comptes LDAP utilisateurs**
  - Si un utilisateur quitte le laboratoire → son compte est supprimé
  - Suppression du compte → aucun service accessible
  - CDD / prolongation de compte → définition d'une date de fin dans un champs LDAP spécifique (attribut LDAP shadowExpire – format de type date faisant partie du objectClass: shadowAccount)

- **Gestion des mots de passe**
  - Chiffrage des mots de passe au format SSHA (attribut LDAP userPassword)
  - Mot de passe aléatoire lors de la création d'un compte
  - Si pas de modification du mot de passe au bout de 2 semaines : compte bloqué

Interfaces de changement des mots de passe

3 interfaces Open Source compatibles avec openLDAP :

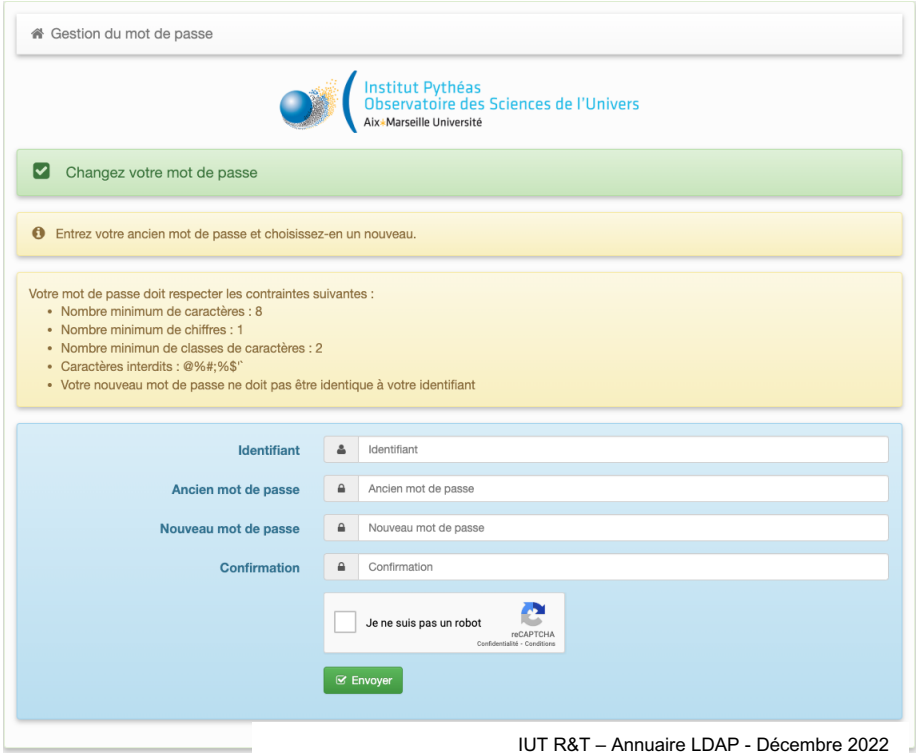
- ldapsaisie
- ldapadmin
- ldap toolbox self service password

(MAJ openldap + active directory)

Alternatives via command-line :

- ldapmodify
- Commande passwd (sssd)

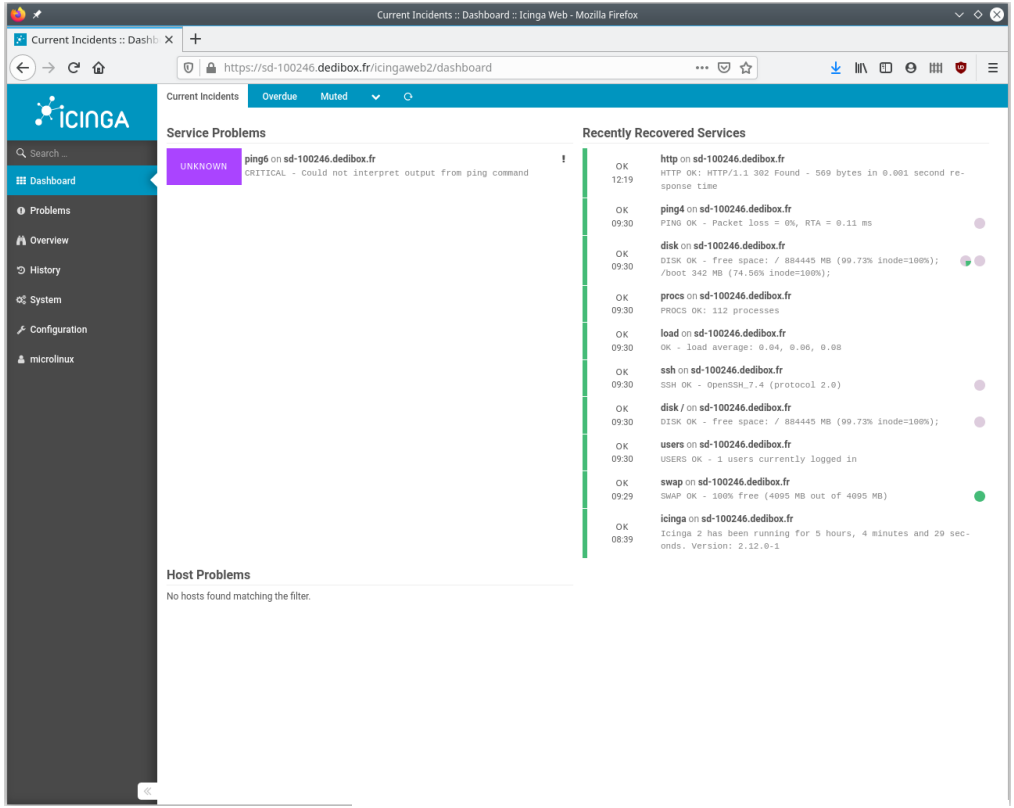
→ bloqué dans notre SI



Supervision des annuaires

Supervision LDAP via icinga2

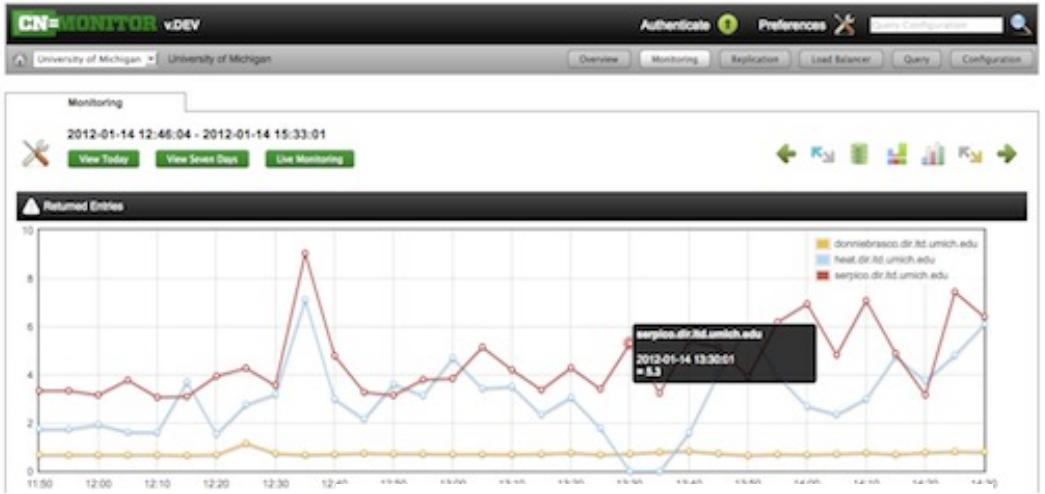
- Suivi de l'état du service par site
- Remontée des alertes par email



Métrologie des annuaires

Métrologie avec le module *cn=monitor (Dans OpenLDAP les modules sont appelés des Overlay)*

- **cn=monitor est le nom d'un outil web ET le nom de l'overlay pour le monitoring openLDAP**
- **Arbre LDAP spécial où sont collectées les statistiques de connexion à l'annuaire**
- **Possibilité d'interroger le module en ligne de commande**
- **Statistiques connexion/bind/unbind etc.**
- **Trafic**
- **Nb opérations en lecture / écriture**



Résilience du service LDAP

- **2 possibilités pour faire du HA**
  - sur une infra de virtualisation VMWARE/PROXMOX
  - via outil spécifique réplication master-master openldap
- **Sauvegarde complète de la base au format ldif (commande slapcat)**
  - utile pour retrouver une archive (compte utilisateur par exemple)
- **Sauvegarde de la machine complète :**
  - snapshots de la VM
  - sauvegarde régulière (au format tar.gz par exemple)
  - sauvegarde du répertoire de config (/etc/ldap)

Problèmes rencontrés ?

- **Max open files**
  - Paramètre unix contrôlant le nombre max de fichier ouvert pour un utilisateur donné (autre que root) – 1024 par défaut
- **Plantage du service (VM à redémarrer)**
  - Manque de ressources (RAM ou espace disque)
- **Réplication pas à jour**
  - Décalage dans l'horaire des serveurs: NTP
  - Soucis réseaux
  - Mauvaise configuration, mauvais certificats SSL…

Des questions ?