2020

Louis Bovay

DIVTEC

09/10/2020

M159 – Annuaire LDAP

Une image contenant table, portable, ordinateur, assis

Description générée automatiquement

**Table des matières**

[1. Introduction 1](#_Toc55891314)

[2. Annuaire LDAP 2](#_Toc55891315)

[2.1 Présentation 2](#_Toc55891316)

[2.2 Histoire 2](#_Toc55891317)

[2.3 Différences avec une base de données 2](#_Toc55891318)

[2.4 Structuration des données 3](#_Toc55891319)

[2.5 Type d’infrastructure 4](#_Toc55891320)

[2.5.1 Infrastructure client-serveur 4](#_Toc55891321)

[2.5.2 Infrastructure N-Tier 5](#_Toc55891322)

[3. Disponibilité des données 6](#_Toc55891323)

[4. Installations 7](#_Toc55891324)

[4.1 Système d’exploitation : 7](#_Toc55891325)

[4.2 Services Windows Server : 7](#_Toc55891326)

[4.3 Application : 7](#_Toc55891327)

[4.4 Informations serveur 7](#_Toc55891328)

[4.5 GitHub 7](#_Toc55891329)

[5. Peupler L’active Directory 8](#_Toc55891330)

[5.1 Fichier .LDIF 8](#_Toc55891331)

[5.1.1 Importation d’un fichier .LDIF 8](#_Toc55891332)

[5.2 Fichier .CSV 9](#_Toc55891333)

[5.2.1 Importation d’un fichier .CSV 9](#_Toc55891334)

[5.2.2 Générer des données 9](#_Toc55891335)

[6. Créer la base de données 10](#_Toc55891336)

[7. Site web d’importation 11](#_Toc55891337)

[7.1 Importer des données 11](#_Toc55891338)

[7.2 Supprimer les données 13](#_Toc55891339)

[7.3 Améliorations possibles 13](#_Toc55891340)

[8. Tester le tout 13](#_Toc55891341)

[8.1 Informations 13](#_Toc55891342)

[8.2 Marche à suivre 13](#_Toc55891343)

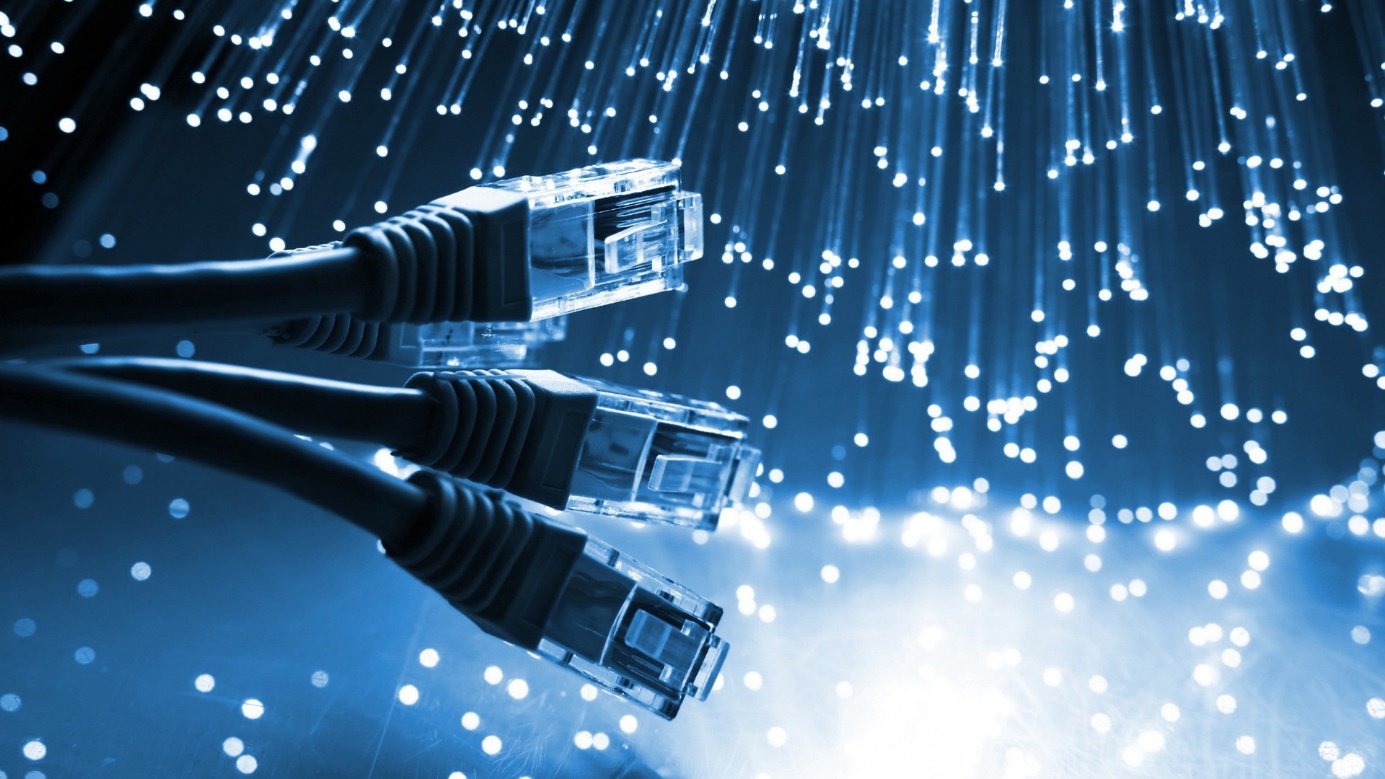
[8.3 Vidéo de teste 13](#_Toc55891344)

[9. Sources 14](#_Toc55891345)

# Introduction

Ce document a pour but d’expliquer et de montrer le fonctionnement d’un annuaire LDAP.

La première partie expliquera de manière générale ce qu’est un annuaire LDAP ainsi que sa structuration, la deuxième partie expliquera comment se connecter à un annuaire LDAP et importer ou exporter des données dans une base de données via une page WEB.



# Annuaire LDAP

## Présentation

Un annuaire LDAP (*Lightweight Directory Access Protocol ou Protocole d'accès aux annuaires léger*) permet de centraliser des données utilisateurs, ce qui autorise par la suite aux utilisateurs de se connecter à diverses applications.

Sans annuaire LDAP au sein d’une entreprise, les informations de connexions deviendraient faibles, redondantes et même obsolètes.

Car si chaque utilisateur devrait se créer un identifiant et un mot de passe pour chaque application, il choisira vite un mot de passe faible et simple à retenir pour tous ces comptes pour éviter de l’oublier.

## Histoire

L’UIT mit en place les tout premiers annuaire X.500 en 1988 pour simplifier et uniformiser l’accès aux services, centraliser et protéger les données. Pour y accéder, on utilise le protocole DAP, qui ne fonctionnent pas encore sur le réseau TCP/IP et qui est compliqué à mettre en place.

Le protocole LDAP ne sera créé qu’en 1993 par l’Université du Michigan, il ne sera qu’un simple connecteur TCP/IP avec des annuaires X.500.

En 1995, LDAP révolutionne le protocole X.500 en devenant un protocole natif et utilisable indépendamment du X.500.

## Différences avec une base de données

On peut vite faire le lien entre un LDAP et une base de données classique car au fond, les deux sont des bases de données, un annuaire LDAP est simplement une base de données bien spécifique.

L’avantage d’un LDAP c’est sa structure de données qui est, certes, extrêmement limité mais qui donne en retour un système de recherche très efficace.

On utilisera donc un LDAP majoritairement pour rechercher des données plutôt que d’en insérer, contrairement à une base de données classique.

## Structuration des données



Figure 1 Structure des données (source OpenClassRoom)

On peut y voir :

* Plusieurs nœuds (ou=users,dc=cogip,dc=fr)
* Plusieurs feuilles (uid=Jean-Christian Ranu,ou=Users,dc=cogip,dc=fr)
* La racine(dc=cogip,dc=fr)

Ce que je viens de lister sont les Distinguished Name (DN) de chaque élément, ils sont écrits « à l’envers », pour l’écrire on partira toujours de l’élément et on remontera jusqu’à la racine, contrairement à une adresse d’un dossier sur Windows par exemple, où là on par toujours de la racine vers l’élément.

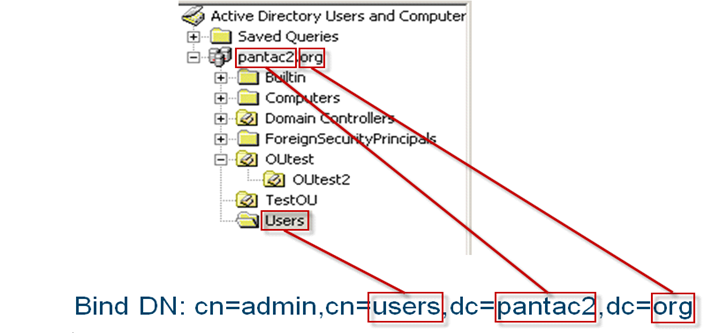


Figure 2 Exemple de lecture d'un distinguished name (source knowledgebase.paloaltonetworks)

Chaque élément a donc un Distinguished Name ainsi qu’un Relative Distinguished Name, qui comporte uniquement le nom de l’élément.

Par exemple :

* **Distinguished Name** : uid=Jean-Christian Ranu,ou=Users,dc=cogip,dc=fr
* **Relative Distinguished Name** : uid=Jean-Christian Ranu

## Type d’infrastructure

Il est possible de mettre en place plusieurs type d’infrastructure d’annuaire LDAP, en voici quelques exemples :

### Infrastructure client-serveur

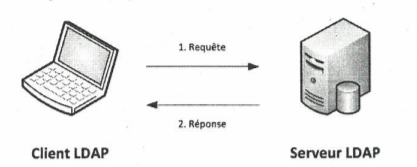
****

Figure 3 exemple d'infrastructure client-serveur ([source](https://www.editions-eni.fr/livre/ldap-planification-et-mise-en-oeuvre-d-un-annuaire-openldap-9782409011009))

C’est une infrastructure locale qui donc établie une simple connexion entre une application LDAP du client et le serveur LDAP.

Le problème c’est que chaque application LDAP doit être installée et configurée sur chaque poste, il en va de même si on met à jours notre application, il faudra la redéployée sur chaque poste.

La mise en place de cette infrastructure a comme avantage d’être extrêmement simple à mettre en place, mais devient laborieuse à entretenir.

### Infrastructure N-Tier



L’infrastructure N-Tier permet de centralisée une application qui s’occupera de faire le lien entre, par exemple, l’annuaire LDAP, des clients et une base de données

L’avantage c’est que la configuration ne se fait qu’à une place pour ensuite être accessible à tous depuis une navigateur web.

La mise en place de cette infrastructure reste néanmoins bien plus fastidieuse

C’est d’ailleurs cette infrastructure que sera détailler dans le chapitre consacré à l’installation.

# Disponibilité des données

Les données présentes dans un LDAP sont généralement asynchrones, ce qui signifie qu’une nouvelle entrée faite à Porrentruy ne sera pas visible tout de suite à Delémont.

On met en place aussi des serveurs de réplication qui, serviront de copie de l’annuaire principal pour à chaque site de l’entreprise d’accéder aux données sans engorger les liaisons.

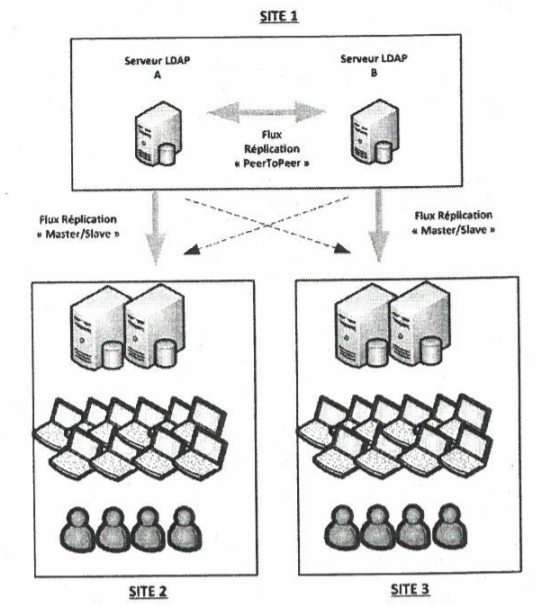


Figure 4 Distribution et réplication d'annuaire ([source](https://www.editions-eni.fr/livre/ldap-planification-et-mise-en-oeuvre-d-un-annuaire-openldap-9782409011009))

La réplication sert aussi à instaurer de la redondance, comme ça si un serveur tombe en panne, l’autre prend le relais. Par exemple si A tombe en panne, B prendra le relais pour pousser les données aux serveurs du SITE 2.

On peut aussi garder des données via le cache, ce qui permet d’avoir un accès permanant et instantané, mais qui comporte certains risques :

* Si une personne garde trop longtemps un cache sans le mettre à jours
  + Obsolescence des données du cache
  + Aucun accès au nouvelles données
* Si une personne quitte l’entreprise avec le cache
  + Vol de données
  + Ventes de données
  + Divulgation volontaire ou involontaire de données

# Installations

L’installation ne sera pas détaillée car très simple.

## Système d’exploitation :

* Windows 2016 SERVER (English)

## Services Windows Server :

* Active Directory
* DNS
* DHCP

## Application :

* Visual studio code (PHP, CSS, SQL)
* XAMPP (PHP et MySQL) + 2 .dll à installer dans le dossier PHP de XAMPP
* Firefox (Navigateur)
* Apache directory studio (visualisation du LDAP)

## Informations serveur

* Nom du serveur > M159LDAP
* Root Domain > M159LDAP.LOCAL
* NetBIOS >M159LDAPDOMAIN

## GitHub

Tout les fichiers source sont disponibles sur [le GitHub du projet](https://github.com/EctoBoggan/M159-LDAP)

* GestionActiveDirectory L’application permettant d’importer un fichier CSV
* PHP Le site et son CSS
* SQL Code SQL de création de la table
* dll .dll requis pour se connecter à l’AD en PHP
* docs documentation du projet

# Peupler L’active Directory

J’ai testé deux manières de peupler l’active directory, la première en important un fichier LDIF, la deuxième avec un fichier .CSV

## Fichier .LDIF

### Importation d’un fichier .LDIF

Les fichiers .LDIF se présentent généralement comme cela :

dn: cn=durant,dc=jalios,dc=com

cn: Michel Durant

objectClass: inetOrgPerson

uid: durant

userPassword: michel

givenName: Michel

sn: Durant

description: Michel Durant sert pour les tests LDAP

mail: michel.durant@jalios.com

title: Directeur des tests

telephoneNumber: 01 39 63 01 02

mobile: 06 39 63 01 02

C’est ce que l’on obtient après avoir exporter un annuaire LDAP, c’est un fichier universel qui permet l’export / l’import de donnée entre des annuaire LDAP différent.

Pour exporter des données, il suffit de créer une connexion à l’annuaire LDAP puis de se connecter à ce dernier via Apache directory, puis d’appuyer sur fichier -> exporter et choisir le format .LDIF

C’est exactement la même chose pour importer un fichier, il faut néanmoins faire bien attention à ce que les chemins soit correctement écrit (ici il faudra regarder que notre annuaire LDAP est bien structurer de manière à accueillir M.durant dans le dossier « dn: cn=durant,dc=jalios,dc=com »

## Fichier .CSV

### Importation d’un fichier .CSV

Je me suis amusé à créer une petite application PowerShell qui permet d’importer un fichier .CSV à l’active directory.

L’application GestionActiveDirectory.ps1 permet de :

* newOU.ps1 Créer des unités organisationnelles
* AddUser.ps1 Ajouter des utilisateurs
* removeOU.ps1 Supprimer les unités organisationnelles
* removeUser.ps1 Supprimer les utilisateurs

### Générer des données

Il a fallu d’abord générer un fichier CSV, je me suis servi de <https://mockaroo.com/> pour générer des noms, prénoms et téléphone aléatoires puis de excel ainsi que de quelque mise en forme conditionnelle pour générer leur mail, username, ainsi que de leur chemin.

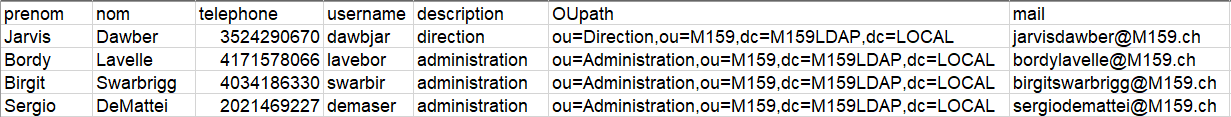


Figure 5 Fichier Excel

Puis je l’ai enregistré sous format .CSV ce qui me donne :

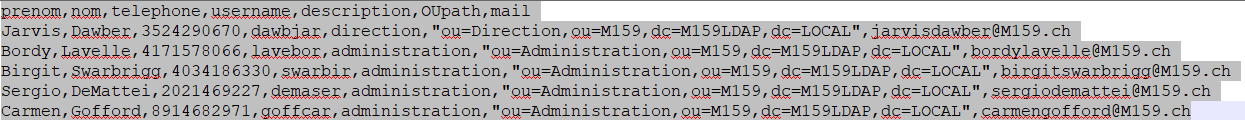


Figure 6 Fichier Excel exporter en .CSV

# Créer la base de données

Je me suis rendu sur le panneau de contrôle phpMyAdmin et j’ai créer une nouvelle base de données nommée « m159 », puis j’y ai créer les tables ainsi que les champs avec les codes suivant :

#Suppression des tables

DROP TABLE IF EXISTS tb\_user;

DROP TABLE IF EXISTS tb\_role;

#Création de la table role

CREATE TABLE tb\_role(

pk\_role INT PRIMARY KEY AUTO\_INCREMENT,

nom\_role VARCHAR(25) NOT NULL

);

#Ajout des 4 roles dans tb\_role

INSERT INTO tb\_role VALUES(null,'Direction'),

(null,'Administration'),

(null,'Comptabilité'),

(null,'Utilisateur');

#Création de la table user

CREATE TABLE tb\_user(

pk\_user INT PRIMARY KEY AUTO\_INCREMENT,

fk\_role INT NOT NULL,

nom\_user VARCHAR(25) NOT NULL,

pre\_user VARCHAR(25) NOT NULL,

username\_user VARCHAR(50) NOT NULL UNIQUE,

mail\_user VARCHAR(50) UNIQUE,

tel\_user BIGINT UNIQUE,

FOREIGN KEY (fk\_role) REFERENCES tb\_role(pk\_role)

);

*La base de données reste très basique et mériterait l’ajout d’index pour faciliter les recherches.*

La base de données est maintenant créée et prête à recevoir des données.

# Site web d’importation

Le site contient uniquement deux boutons « import » et « suppression »

Il s’agit donc d’un formulaire qui, suivant le bouton cliqué, importe ou supprime des données

TOUT ce code est disponible dans le dossier GitHub « PHP » et est commenté si besoin de plus d’information

## Importer des données

Il a fallu d’abord créer une connexion à l’AD

 //paramètre de connexion

 //Utilisateur (ici Administrator)

 $ldap\_dn = "cn=Administrator,cn=Users,dc=M159LDAP,dc=LOCAL";

 //Mot de passe

$ldap\_password = "Admlocal1";

 // Assigne et ouvre la connexion

 //$ldap\_con = ldap\_connect("ldap://localhost:10389");

            $ldap\_con = ldap\_connect("M159LDAP.LOCAL");

Puis s’y connecter

ldap\_bind($ldap\_con, $ldap\_dn, $ldap\_password);

On récupère les utilisateurs

$entries = getUsers($ldap\_con);

/\*\*

 \* Cherche tous les utilisateurs et les enregistre dans une array

 \* @param connexion connexion au serveur ldap

 \* @return array une liste d'utilisateurs

 \*/

function getUsers($connexion)

{

    //filtre (\* pour tous les utilisateurs)

    $filter = "(cn=\*)";

    //Recherche

    $result = ldap\_search($connexion, "ou=M159,dc=M159LDAP,dc=LOCAL", $filter) or exit("<p class='fail'>Recherche échouée</p>");

    //Récupération du résultat

    return ldap\_get\_entries($connexion, $result);

}

On se connecte à la base de données

/\*\*

 \* Ouvre une connexion à la base de données

 \*

 \* @return db la connexion

 \*/

function dbConnect()

{

    echo "<p class='info'>Connexion à la base de donnée .  .  .<br></p>";

    $user = 'root';

    $pass = '';

    $dbname = 'm159';

    $db = new mysqli('localhost', $user, $pass, $dbname) or die("<p class='fail'>echec de connexion</p>");

    echo "<p class='success'> → connexion à la base de donnée réuissie<br></p>";

    return $db;

}

On créer une requête

$query = "INSERT INTO tb\_user

          VALUES(null," .

           $SQLuser['role'] . ",'" .

           $SQLuser['nom']  . "','" .

           $SQLuser['prenom'] . "','" .

           $SQLuser['username'] . "','" .

           $SQLuser['mail'] . "'," .

           $SQLuser['tel'] . ");";

On l’envoie et on fait ça pour chaque utilisateur

$connexion->query($query)

## Supprimer les données

Le bouton supprimer ne fait qu’une simple requête pour supprimer

//Suppression de donnée

$query = "DELETE FROM tb\_user;";

//Exécution de la requête

$connexion->query($query);

Voilà en grandes lignes comment la mise en place du site à été faite.

## Améliorations possibles

* Choisir ce que l’ont souhaite supprimer (car là, la base de données est entièrement vidée).
* Gestion des duplications

# Tester le tout

## Informations

Posséder la machine virtuelle aide grandement au teste, mais il reste possible de le faire en installant soit même un serveur puis de suivre els étape suivante après avoir copier le dépôt GitHub

## Marche à suivre

1. Copier la machine virtuelle et démarrez-la
2. Démarrez GestionActiveDirectory.ps1 avec PowerShell ou l’invite de commande
3. (Optionnel) insérer votre propre fichier CSV dans le dossier GestionActiveDirectory>ressources
4. Ajoutez des OU, Puis ajoutez des utilisateurs (cela peut prendre du temps).
5. (Optionnel) Essayez de supprimer les utilisateurs, puis les OU
6. Ouvrez XAMPP et allumez les services Apache et MySQL
7. Ouvrez le navigateur Firefox, et ouvrez l’onglet favoris « Site PHP»
8. Importez les données
9. (Optionnel) Essayez de supprimer les données
10. Ouvrez l’onglet favoris « Base de données »
11. Vérifiez que vos données ont bien été importé

## Vidéo de teste

Voici une vidéo montrant la marche à suivre décrite précédemment

<https://www.youtube.com/watch?v=Si594umXe5o>

# Sources

## Sources pour la partie théorique

[Cours OpenClasseRoom LDAP](https://openclassrooms.com/fr/courses/2257706-presentation-du-concept-dannuaire-ldap#:~:text=Il%20est%20con%C3%A7u%20pour%20fonctionner,de%20Lightweight%20Directory%20Access%20Protocol)

[Wikipédia X.500](https://fr.wikipedia.org/wiki/X.500)

[Wikipédia LDAP](https://fr.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol)

[Livre planification et mise en œuvre d'annuaire ldap](https://www.editions-eni.fr/livre/ldap-planification-et-mise-en-oeuvre-d-un-annuaire-openldap-9782409011009)

Note prises en cours du module M159

## Sources pour la partie pratique :

[Créer des users avec un fichier CSV](https://www.youtube.com/watch?v=9WAcQE-Q9xo&ab_channel=ServerAcademy)

[Ajouter/supprimer User/OU active directory](https://www.youtube.com/watch?v=eGjrw85U4_0)

[Syntaxe New-ADUser](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee617253(v=technet.10)?redirectedfrom=MSDN)

[Bind DN](https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGOCA0)

[Connexion php - ldap](https://www.youtube.com/watch?v=AEjGhzZpGlg)