2020

Bovay Louis

DIVTEC

09/10/2020

M159 – LDAP

Une image contenant table, portable, ordinateur, assis

Description générée automatiquement

**Table des matières**

[1. Introduction 1](#_Toc26781129)

[2. Chapitre 2](#_Toc26781130)

[2.1 Sous-chapitre 2](#_Toc26781131)

[2.2 Sous-chapitre 2](#_Toc26781132)

[3. Chapitre 3](#_Toc26781133)

[3.1 Sous chapitre 3](#_Toc26781134)

[4. Chapitre 4](#_Toc26781135)

[4.1 Sous-chapitre 4](#_Toc26781136)

[5. Conclusion 5](#_Toc26781137)

[6. Remerciements 6](#_Toc26781138)

[7. Index 7](#_Toc26781139)

[8. Sources 8](#_Toc26781140)

# 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.

# Annuaire LDAP

## Présentation

Un annuaire LDAP 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.

## 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. (Plus de détails sur la recherche dans le chapitre **INSERER CHAPITRE)**

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 écris « à l’envers », pour l’écrire on partira toujours de l’élément 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.

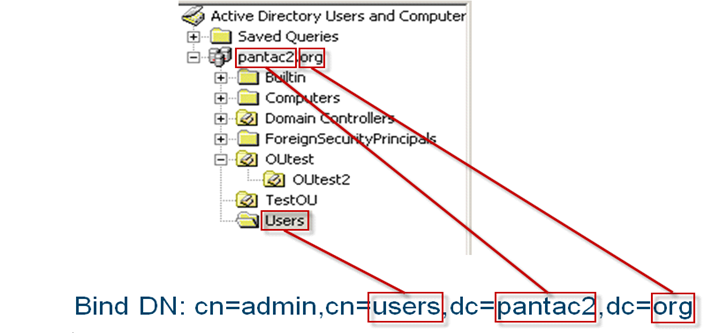


Figure 2 Exemple de lecture d'un distinguished name (source knowledgebase.paloaltonetworks)

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**

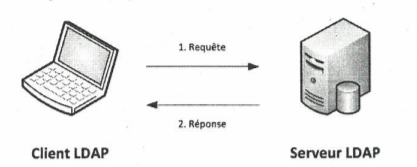
****

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 n’a comme seul avantage d’être excrément 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.

# 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)
* Firefox (Navigateur)
* Apache directory studio (visualisation du LDAP)

## Informations serveur

* Nom du serveur > M159LDAP
* Root domain > M159LDAP.LOCAL
* NetBios >M159LDAPDOMAIN

# 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 a ce que les chemins soit correctement écrit (ici il faudra regarder que notre annuaire LDAP est bien structurer de manière a 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 permet de :

* Créer des unités organisationnelles
* Ajouter des utilisateurs
* Supprimer les unités organisationnelles
* 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.

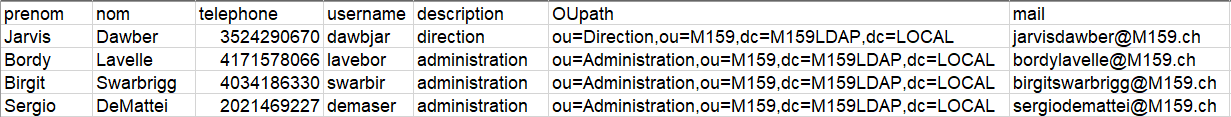


Figure 4 Fichier Excel

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

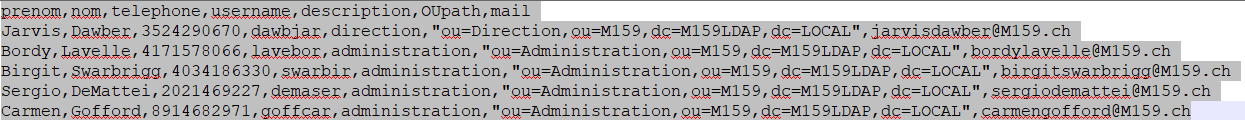


Figure 5 Fichier Excel exporter en .CSV

# Sources

[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)

[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)