

TP Installation du service d'annuaire LDAP:

DÉSACTIVER LE SERVICE DHCP QUI CASSE LES COUILLES A TOUT LE MONDE -> SUDO SERVICE

ISC-DHCP-SERVER close

Installation ldap et outils de configuration minimum: sudo apt install slapd ldap-utils
pas besoin de changer le dit suffix *dc=exemple,dc=com* car accès direct via notre ip.

installer ldap-utils pour afficher les données de l'annuaire.

!: Qu'est-ce que LDAP et installation:

LDAP (Lightweight Directory Access Protocol) est un service protocol permettant la gestion de personnes, groupes, objets, etc. Ce service est disponible sur Windows et Linux, pour ce projet, nous procéderons sous une distribution Ubuntu, distribution Linux simple d'installation et bien documentée. Notre service LDAP sera ici administré depuis OpenLDAP et phpLDAPadmin.

Nous commencerons par installer les paquets nécessaires pour ensuite lancer le daemon sur notre système.

```
med@ldap:~$ sudo apt-get install slapd ldap-utils
[sudo] password for med:
Reading package lists... Done
Building dependency tree
Reading state information... Done
ldap-utils is already the newest version (2.4.49+dfsg-2ubuntu1.8).
```

Assurons-nous que le daemon est bien actif et en cours:

```
med@ldap:~$ systemctl status slapd
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
   Loaded: loaded (/etc/init.d/slapd; generated)
   Drop-In: /usr/lib/systemd/system/slapd.service.d
            └─slapd-remain-after-exit.conf
   Active: active (running) since Tue 2022-03-08 16:23:53 CET; 25min ago
```

```
med@ldap:~$ sudo dpkg-reconfigure slapd
```

Pour lancer le processus de configuration du service.

Lors de ce processus l'outil de configuration nous demandera plusieurs informations:

Les plus importantes information étant:

- Un nom de domaine: pas nécessaire dans notre situation car nous utiliserons directement l'ip attribuée.
- Un mot de passe administrateur.
- Le format de stockage de la base de données: MDB

Fichier de configuration apres modification de BASE et URI:

```
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE      dc=medinfo,dc=fr
URI        ldap://localhost

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
TLS_CACERT     /etc/ssl/certs/ca-certificates.crt
```

Nous installerons également phpLDAPadmin qui nous permet une administration facile, accessible partout de notre serveur ldap.

- sudo apt install phpldapadmin
- sudo vim /etc/phpldapadmin/config.php pour modifier la configuration php à nos besoins.

```
binds. */
$servers->setValue('login','bind_id','cn=admin,dc=medinfo,dc=fr');
```

```
$servers->setValue('server','host','10.0.0.67');
```

```
$servers->setValue('server','name','LDAP serveur mehdi');
```

```
$servers->setValue('server','base',array('dc=medinfo,dc=fr'));
```

Test en allant sur 10.0.0.67/phpldapadmin:

Accueil | Purger les caches | Montrer le cache

LDAP serveur mehdi

schéma rechercher rafraîchir info importer exporter se déconnecter

Connecté en tant que :: cn=admin

- dc=medinfo,dc=fr (2)
 - cn=admin (1)
 - cn=my_group (1)
 - Créer une nouvelle entrée ici

S'authentifier auprès du serveur
Connexion au serveur %s effectuée.

phpLDAPadmin

Utiliser le menu de gauche pour naviguer

[Crédits](#) | [Documentation](#) | [Donation](#)

Création d'un nouveau groupe ldap:

Créer un objet

Serveur: LDAP serveur mehdi Conteneur: cn=admin,dc=medinfo,dc=fr
Modèle: Samba: Group Mapping (sambaGroupMapping)

New Samba3 Group Mapping (Étape 1 sur 1)

GID ajouter, supprimer, sélectionner

501

Groupe ajouter, supprimer, sélectionner

my_group

Utilisateurs ajouter, supprimer

Ajout d'un nouvel utilisateur dans ce group:

cn=notorious B.I.G

Serveur: LDAP serveur mehdi Nom distingué: cn=notorious B.I.G,cn=my_group,dc=medinfo,dc=fr
Modèle: Valeur par défaut

Rafraîchir
 Switch Template
 Copier ou déplacer cette entrée
 Renommer
 Créer une sous-entrée
 Astuce : pour supprimer un attribut, videz le champ texte et enregistrez.
 Astuce : pour afficher le schéma d'un attribut, cliquez sur le nom de l'attribut.

Afficher les attributs internes
 Exporter
 Supprimer cette entrée
 Comparer avec une autre entrée
 Ajouter un nouvel attribut

cn requies, rdn

notorious B.I.G
(ajouter une valeur)
(renommer)

gidNumber requies

500
my_group ()

givenName

notorious
(ajouter une valeur)

homeDirectory requies

/home/users/my_group/

loginShell

/bin/sh

objectClass requies

inetOrgPerson (structurel)
 posixAccount
 top
 (ajouter une valeur)

cn=my_group

Serveur: LDAP serveur mehdi Nom distingué: cn=my_group,dc=medinfo,dc=fr
Modèle: Valeur par défaut

Rafraîchir
 Switch Template
 Copier ou déplacer cette entrée
 Renommer
 Créer une sous-entrée
 Astuce : pour supprimer un attribut, videz le champ texte et enregistrez.
 Astuce : pour afficher le schéma d'un attribut, cliquez sur le nom de l'attribut.

Afficher les attributs internes
 Exporter
 Supprimer cette entrée
 Comparer avec une autre entrée
 Ajouter un nouvel attribut

cn requies, rdn

my_group
(ajouter une valeur)
(renommer)

gidNumber requies

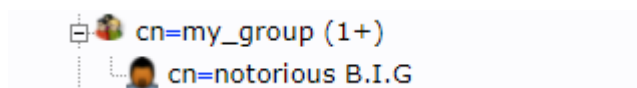
500

objectClass requies

posixGroup (structurel)
 top
 (ajouter une valeur)

Update Object

Le nouvel utilisateur est bien dans notre nouveau group:



En cas d'oubli de mot de passe de LDAP: sudo reconfigure dpkg-ldap

! J'avais oublié de désactiver le service DHCP du dernier projet qui interférait avec certains postes de la salle ! —> sudo service isc-dhcp-server stop

II: Juridiction:

a) Les données enregistrées sont-elles de type à caractère personnel?:

Une donnée à caractère personnel correspond à toutes informations relatives à une personne pouvant permettre de l'identifier (numéros de téléphone, adresse IP, adresse postale...). Dans notre situation, notre annuaire a pour objectif de gérer les utilisateurs de bibliothèques et de les enregistrer pour qu'ils puissent emprunter des livres et utiliser d'autres services. Il nous faudra donc y enregistrer des données à caractère personnel tel que leurs noms, téléphone, adresse etc. Les données enregistrées sont donc à caractère personnel.

<https://afkgaming.com/esports/news/7410-what-does-copium-mean-in-twitch-chat-and-where-did-it-originate#:~:text=Copium%20is%20a%20combination%20of,loss%20or%20failure%20on%20stream.>

b) La protection des DCP (données à caractère personnel) de la part des professionnels de l'informatique doit répondre à certains principes fondamentaux réglementés par la CNIL. Parmi lesquels:

- i) Ne collecter des données strictement nécessaires au bon fonctionnement du système informatique mis en place (demander la religion d'un individu serait peu pertinent.).
- ii) Les personnes doivent être informées quelles données sont utilisées et dans quel contexte.
- iii) Mettre tous les moyens en place pour sécuriser au mieux les données. Sécurité physique et informatique.
- iv) Établir une durée de conservation fixe des données: ex: 6 mois, 1 ans, dans le cas d'une carte d'adhérent.

Sources:

<https://ubuntu.com/server/docs/service-ldap>

<https://connect.ed-diamond.com/Linux-Pratique/lp-115/installation-et-configuration-d-un-annuaire-openldap>

<https://bitsparadise.info/index.php/2020/11/11/mise-en-place-dun-service-ldap-avec-dopenldap-et-phpldapadmin/>

<https://www.cnil.fr/fr/cnil-direct/question/une-donnee-caractere-personnel-cest-quoi>

<https://www.cnil.fr/fr/adopter-les-six-bons-reflexes>

<https://www.cnil.fr/fr/rgpd-par-ou-commencer>