

---

# Mise en place OpenLDAP

---

## Table des matières

I) Introduction.....	1
II) Mise en place.....	3
1) Installation et configuration du serveur WEB.....	3
2) Installation et configuration du DNS.....	3
III) Installation de OpenLDAP.....	6
1) Installation des paquets LDAP.....	6
2) Configuration LDAP.....	6
3) Test du serveur LDAP.....	12
IV) Installation de phpldapadmin.....	13
1) Installation.....	13
2) Configuration de Apache2.....	13
a) 1ère méthode.....	13
b) 2ème méthode.....	13
3) Configuration de phpldapadmin.....	14
4) Interface WEB.....	15
5) Compte manager.....	16
6) Création d'une Unité Organisationnelle.....	19
7) Création de groupes.....	23
8) Création d'utilisateurs.....	30
9) Importation d'utilisateurs.....	40
V) Script.....	42
1) Prérequis.....	42
2) Script pour générer un fichier adduser.ldif.....	43
3) Script pour générer un fichier deluser.ldif.....	45
VI) Quelques commandes LDAP.....	46
1) ldapsearch.....	46
a) Tout afficher.....	46
b) Rechercher un utilisateur.....	49
2) ldapadd.....	49
a) Ajout d'utilisateur.....	49
b) Ajout de groupe.....	51
c) Ajout d'une Unité Organisationnelle.....	51
3) ldapmodify.....	52
a) Ajout d'un utilisateur dans un groupe.....	52
b) Modification d'un utilisateur.....	52
4) ldapdelete.....	53

---

## I) Introduction

**OpenLDAP** est une implémentation libre du protocole LDAP maintenue par le projet **OpenLDAP**.

**OpenLDAP** est un annuaire informatique qui fonctionne sur le modèle client/serveur. Il contient des informations de n'importe quelle nature qui sont rangées de manière hiérarchique. Pour bien comprendre le concept, il est souvent comparé aux pages jaunes, où le lecteur recherche un numéro de téléphone particulier : il va d'abord sélectionner la profession, puis la ville, puis le nom de l'entrée pour trouver finalement le numéro de téléphone. En pratique, dans un réseau informatique, il est utilisé pour enregistrer une grande quantité d'utilisateurs ou de services, parfois des centaines de milliers. Il permet d'organiser hiérarchiquement les utilisateurs par département, par lieu géographique ou par n'importe quel autre critère. C'est une alternative libre à Microsoft Active Directory.

Pour chaque donnée contenue dans l'annuaire il faut donc noter qui effectue les actions suivantes :

- ▶ **Recherche** : Une recherche s'effectue sur certains attributs. Pour chaque objet, dans chaque cas d'utilisation, il faudra donc noter les attributs sur lesquels la recherche s'effectue.
- ▶ **Lecture** : Là encore il faut tenir compte des attributs. Les cas d'utilisation devront contenir l'information « de quel attribut a besoin de lire telle personne sur tel objet. »
- ▶ **Création** : Lors du processus de création des objets dans l'annuaire, il faudra valider que la personne, ou l'application, qui crée un objet, a bien connaissance de toute l'information nécessaire. Il peut arriver que cela ne soit pas le cas. Par exemple, une personne du département ressources humaine ne pourra pas d'elle-même assigner un login à un utilisateur dans l'annuaire. Il faut prévoir un mécanisme, en dehors de l'annuaire, qui lui fournisse cette information qui se peut se révéler nécessaire dans certains cas.
- ▶ **Modification** : Dans l'écriture des cas d'utilisation comprenant des modifications, il est nécessaire de noter quels attributs sont modifiés, et de quel type de modifications il s'agit : ajout d'une valeur, retrait d'une valeur, modification de toutes les valeurs, etc.
- ▶ **Suppression**

Les données d'un annuaire sont organisées sous forme hiérarchique, en arbre. Concevoir l'arbre informationnel d'un annuaire c'est spécifier la forme de cet arbre, son organisation, comment les données vont y être nommées. L'objectif à cette étape est donc d'organiser les données pour leur :

- ▶ Consultation
- ▶ Mise à jour
- ▶ Duplication
- ▶ Répartition

Les arbres plats ont pour principal avantage que les recherches s'effectuent rapidement, parce que le serveur n'a pas à parcourir toutes les branches, et à faire une recherche par branche. Par ailleurs les arbres plats présentent beaucoup d'inconvénients :

Les collisions de RDN peuvent se produire fréquemment.

La mise en place de referral n'est pas possible (Le mécanisme de referral peut alors être remplacé par la mise en place d'un meta annuaire. Néanmoins un meta annuaire est beaucoup plus lourd à mettre en place.)

Sur ces points les arbres à fort branchage sont bien plus efficaces. Ils facilitent aussi la délégation.

L'inconvénient des arbres à fort branchage apparaît essentiellement lorsque la structure de l'arbre reflète la structure de l'organisation, et que cette structure est amenée à être modifiée. Dans ce cas, les entrées de l'arbre vont elles aussi être amenées à changer de place et de DN, ce qui peut provoquer des problèmes de cohérences.

Il y a donc un certain équilibre à atteindre entre les deux types d'arbres. Les éléments à prendre en compte sont les suivants (4) :

- ▶ Le nombre d'entrées prévu et son évolution ?
- ▶ La nature (type d'objet) des entrées actuelles et futures ?

- ▶ Vaut-il mieux centraliser les données ou les distribuer ?
- ▶ Seront-elles administrées de manière centrale ou faudra-t-il déléguer une partie de la gestion ?
- ▶ La duplication est-elle prévue ?
- ▶ Quelles applications utiliseront l'annuaire et imposent-elles des contraintes particulières ?
- ▶ Quelles permissions seront mises en place ?

**OpenLDAP** contient :

- ▶ **slapd** : stand-alone LDAP daemon (server)
- ▶ **libraries** : implémentant le protocole LDAP, les outils et les paramètres.

Nous allons maintenant découvrir comment installer **OpenLDAP** sur un serveur Debian 8.7.1 ainsi que l'interface web **phpldapadmin**.

Pour avoir une installation digne de ce nom, je vais installer le serveur DNS et un serveur WEB. Le serveur DNS va permettre de résoudre le nom `ldap.idum.eu`. Le serveur Web va permettre de faire fonctionner l'interface web **phpldapadmin**.

Voici la configuration de mon LAB utilisé pour l'article :

- ▶ Machine virtuelle : Debian 8.7.1
- ▶ Hostname : `deb-idum-lab2`
- ▶ Adresse IP : `10.10.10.11/24`
  - 2 unités d'organisations :
    - Utilisateurs
    - Groupes
  - 3 groupes :
    - Administrateurs
    - Webmasters
    - Utilisateurs
  - 3 Utilisateurs :
    - Vincent THYMME - Groupe : Utilisateurs
    - Paul HETTE - Groupe : Administrateurs
    - Jacques ADIT - Groupe : Webmasters

## II) Mise en place

Commençons l'installation.

### 1) Installation et configuration du serveur WEB

- ▶ Connectez-vous sur le serveur en root.
- ▶ Installez les paquets suivants :

```
aptitude install apache2 apache2-doc php5
```

- ▶ Votre serveur web fonctionne, laissez la configuration par défaut dans un premier temps.

### 2) Installation et configuration du DNS

- ▶ Installer les paquets suivants :

```
aptitude install bind9 bind9-doc
```

- ▶ On copie le fichier "**db.local**" dans le dossier "**/var/cache/bind**" afin de nous donner une base pour notre fichier de zone directe "**idum.eu**".

```
cp db.local /var/cache/bind/db.idum.eu
```

- ▶ On copie le fichier "**db.255**" dans le dossier "**/var/cache/bind**" afin de nous donner une base pour notre fichier de zone inverse "**10.10.10.in-addr.arpa**".

```
cp db.255 /var/cache/bind/db.10.10.10.in-addr.arpa
```

- ▶ On édite notre fichier de zone directe "**idum.eu**".

```
vim /var/cache/bind/db.idum.eu
```

- ▶ Modifiez le fichier comme ci-dessous :

```
;  
; zone directe idum.eu  
;  
$TTL      604800  
@         IN      SOA      deb-idum-lab2.idum.eu. root.idum.eu. (  
          01042017      ; Serial  
          604800        ; Refresh  
          86400         ; Retry  
          2419200       ; Expire  
          604800 )      ; Negative Cache TTL  
;  
@         IN      NS       deb-idum-lab2.idum.eu.  
@         IN      A        10.10.10.11  
deb-idum-lab2  IN      A          10.10.10.11  
ldap        IN      CNAME    deb-idum-lab2  
www         IN      CNAME    deb-idum-lab2
```

- ▶ On édite notre fichier de zone directe "**db.10.10.10.in-addr.arpa**".

```
vim /var/cache/bind/db.10.10.10.in-addr.arpa
```

- ▶ Modifiez le fichier comme ci-dessous :

```
;  
; Zone inverse du Network 10.10.10.0/24  
;  
$TTL      604800  
@         IN      SOA      deb-idum-lab2.idum.eu. root.idum.eu. (  
          20170401      ; Serial  
          604800        ; Refresh  
          86400         ; Retry  
          2419200       ; Expire  
          604800 )      ; Negative Cache TTL  
;  
@         IN      NS       deb-idum-lab2.idum.eu.  
11        IN      PTR      deb-idum-lab2.idum.eu.
```

- ▶ On édite ensuite le fichier "**named.conf.local**" afin de déclarer nos deux zones.

```
vim /etc/bind/named.conf.local
```

- ▶ Ajoutez les lignes suivantes :

```
zone "idum.eu" {
    type master;
    file "db.idum.eu";
};

zone "10.10.10.in-addr.arpa" {
    type master;
    file "db.10.10.10.in-addr.arpa";
};
```

- ▶ Redémarrer le service "**bind9**".

```
service bind9 restart
```

- ▶ Pour finir, modifiez votre fichier "**resolv.conf**".

```
vim /etc/resolv.conf
```

- ▶ Modifiez les lignes pour avoir :

```
domain idum.eu
search idum.eu
nameserver 127.0.0.1
```

- ▶ Testez la résolution de **deb-idum-lab2** :

```
nslookup deb-idum-lab2
Server:          127.0.0.1
Address:         127.0.0.1#53
```

```
Name:   deb-idum-lab2.idum.eu
Address: 10.10.10.11
```

- ▶ Testez la résolution de **ldap** :

```
nslookup ldap
Server:          127.0.0.1
Address:         127.0.0.1#53
```

```
ldap.idum.eu    canonical name = deb-idum-lab2.idum.eu.
Name:   deb-idum-lab2.idum.eu
Address: 10.10.10.11
```

- ▶ Dernier test, testez la résolution inverse :

```
nslookup 10.10.10.11
Server:          127.0.0.1
Address:         127.0.0.1#53
```

```
11.10.10.10.in-addr.arpa      name = deb-idum-lab2.idum.eu.
```

Votre serveur DNS fonctionne.

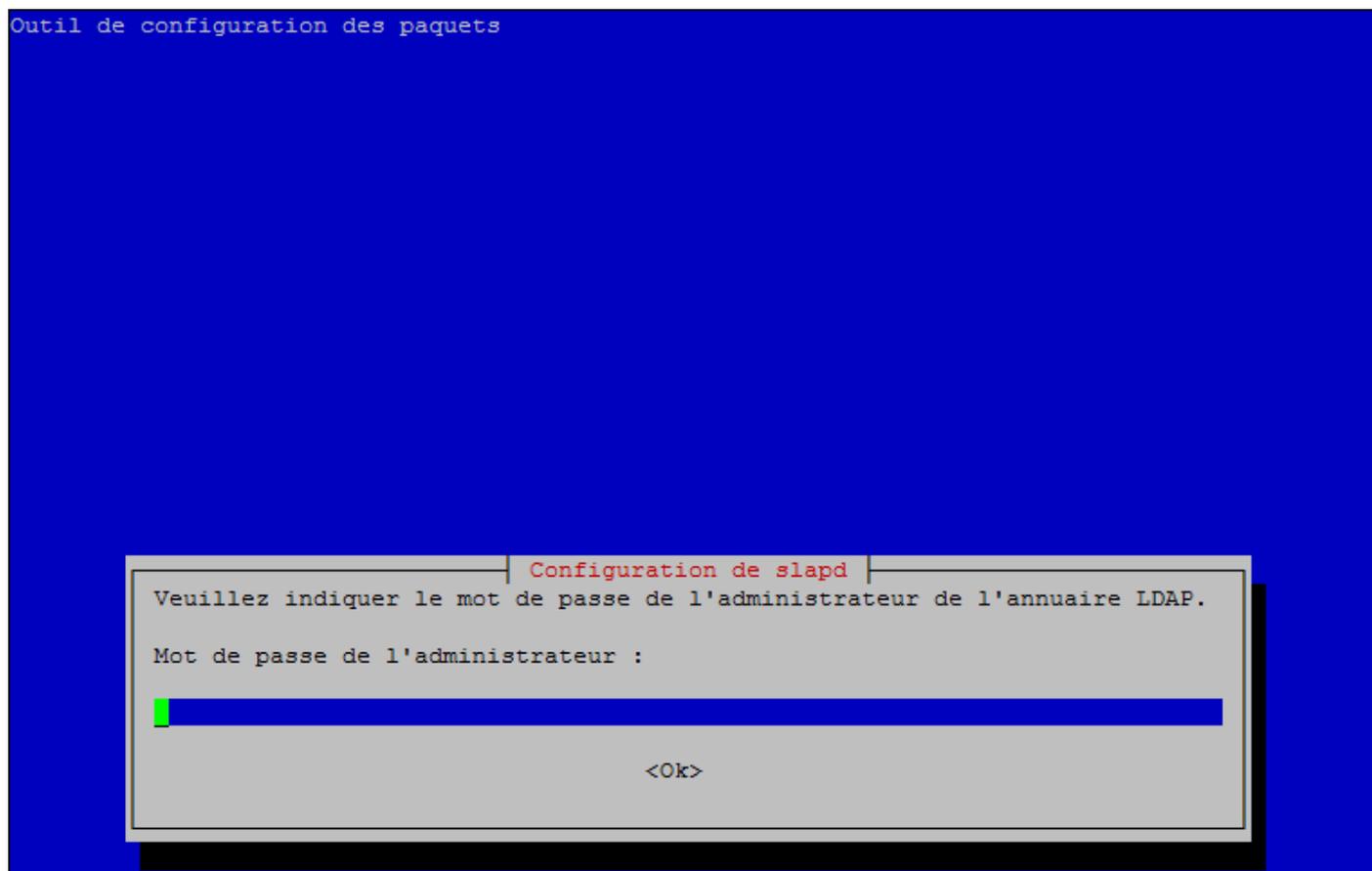
## III) Installation de OpenLDAP

### 1) Installation des paquets LDAP

- ▶ Installez les paquets suivants :

```
aptitude install slapd ldap-utils
```

- ▶ Au cours de l'installation, vous devrez définir le mot de passe de l'administrateur.



- ▶ Puis confirmer le mot de passe.

### 2) Configuration LDAP

- ▶ Editez le fichier "**ldap.conf**".

```
vim /etc/ldap/ldap.conf
```

- ▶ Modifiez les lignes "**BASE**" et "**URI**".

```
#  
# LDAP Defaults  
#
```

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

BASE      dc=idum,dc=eu
URI       ldap://ldap.idum.eu ldap://ldap.idum.eu:666 ldap://127.0.0.1

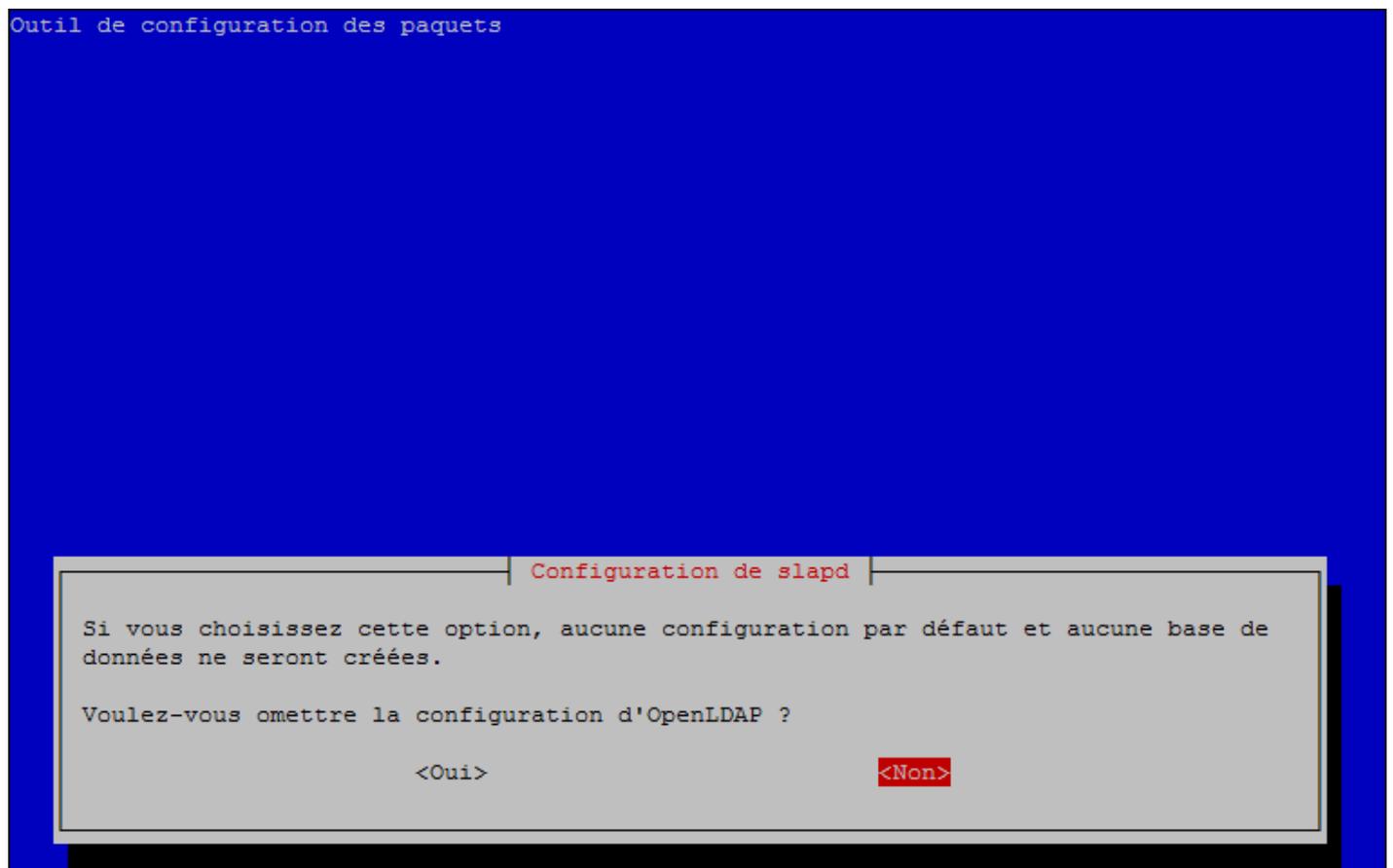
#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

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

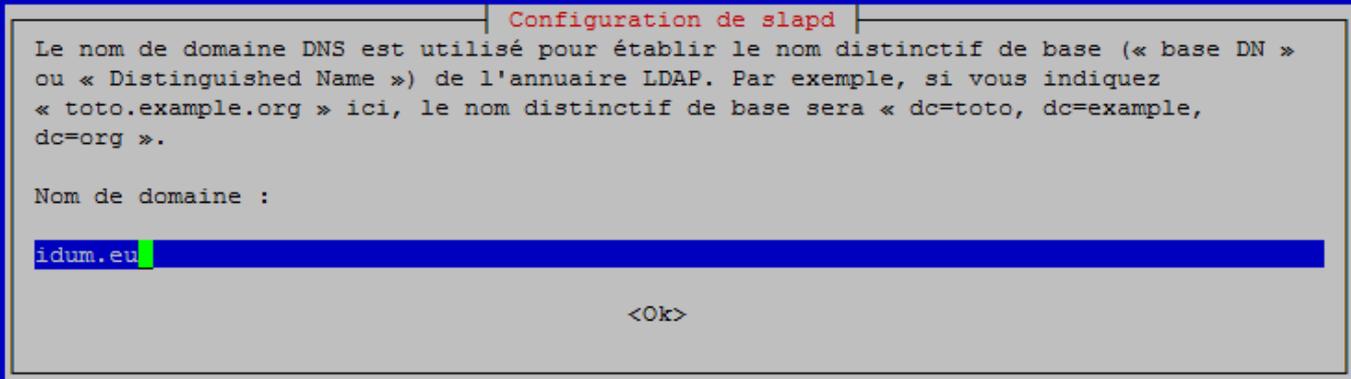
► Tapez la commande suivante pour reconfigurer le paquet "**slapd**".

```
dpkg-reconfigure slapd
```

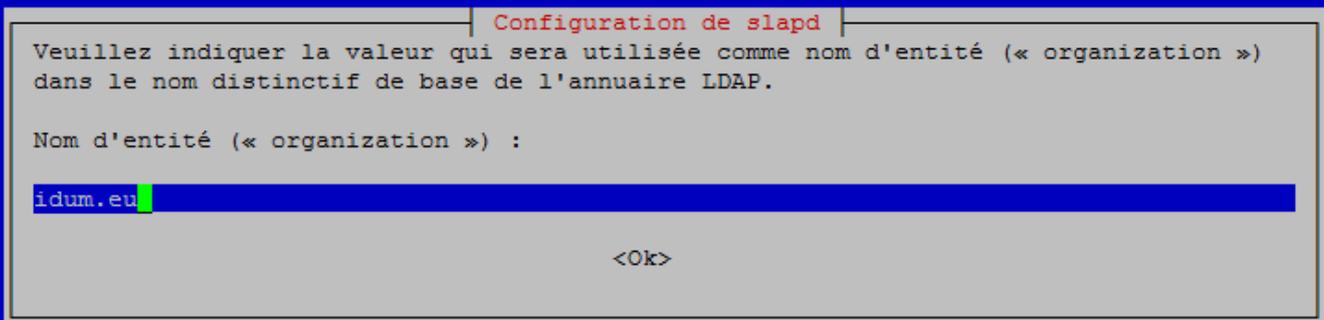
► Lors de la première question "Voulez-vous omettre la configuration d'OpenLDAP répondez "**Non**".



► Saisissez votre nom de domaine.



- Saisissez le nom de l'entité correspondant à la base de votre domaine.



- Définissez de nouveau le mot de passe de l'administrateur LDAP.

Outil de configuration des paquets

Configuration de slapd

Veillez indiquer le mot de passe de l'administrateur de l'annuaire LDAP.

Mot de passe de l'administrateur :

\*\*\*

<Ok>

- Confirmer le mot de passe.

Outil de configuration des paquets

Configuration de slapd

Veillez entrer à nouveau le mot de passe de l'administrateur de l'annuaire LDAP afin de vérifier qu'il a été saisi correctement.

Mot de passe de l'administrateur :

\*\*\*

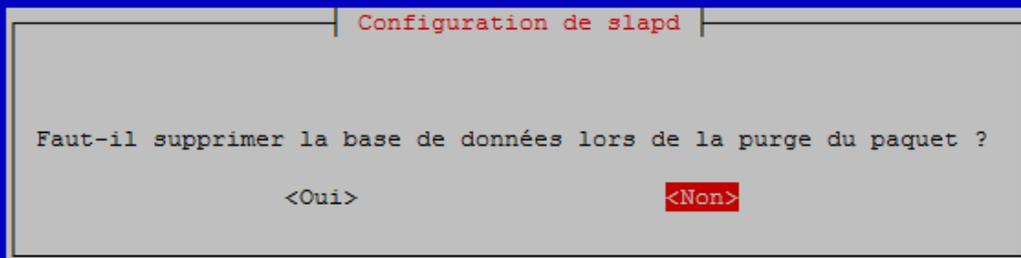
<Ok>

- Sélectionnez le type "MDB" pour la base de données.

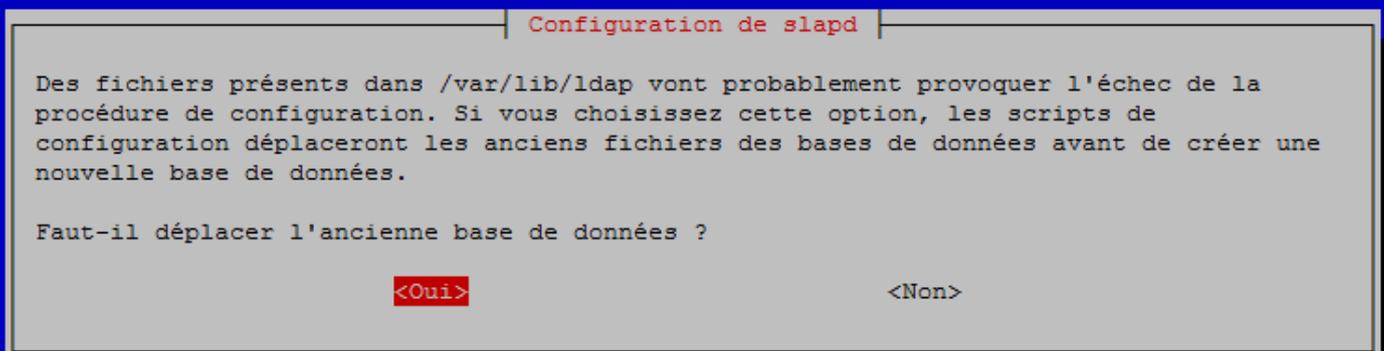
Outil de configuration des paquets



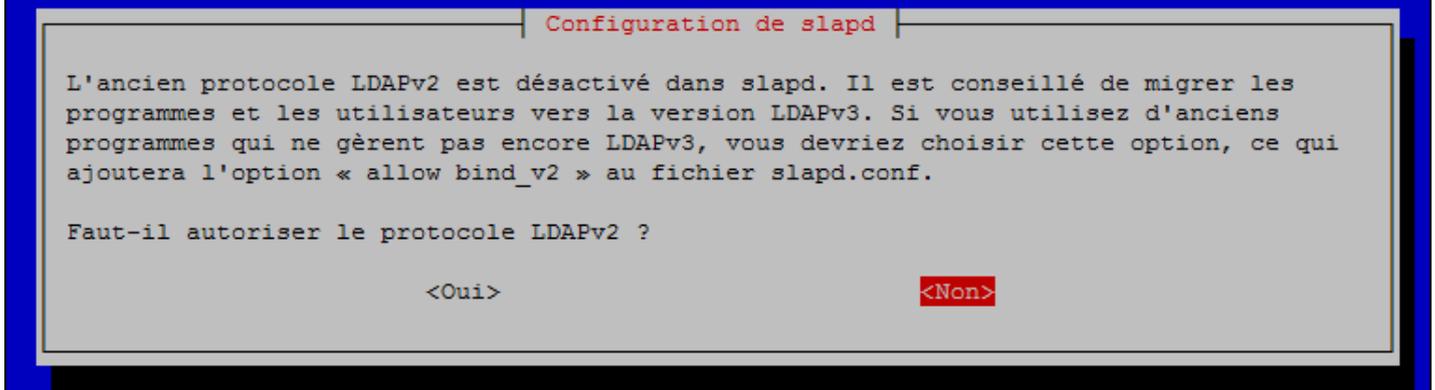
- Choisissez ensuite de ne pas supprimer la base de données.



- Choisissez de déplacer l'ancienne base de données.



- Choisissez de ne pas activer le protocole LDAPv2.



- ▶ Redémarrez le service "**slapd**".

```
service slapd restart
```

- ▶ Votre serveur LDAP doit normalement fonctionner.

### 3) Test du serveur LDAP

Le serveur étant configuré, tapez la commande ci-dessous pour vérifier que LDAP est bien actif.

```
ldapsearch -x
```

- ▶ Vous devez obtenir ceci :

```
# extended LDIF
#
# LDAPv3
# base <dc=idum,dc=eu> (default) with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# idum.eu
dn: dc=idum,dc=eu
objectClass: top
objectClass: dcObject
objectClass: organization
```

```
o: idum.eu
dc: idum

# admin, idum.eu
dn: cn=admin,dc=idum,dc=eu
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

## IV) Installation de phpldapadmin

L'administration de **OpenLDAP** en ligne de commande est assez difficile, "**phpldapadmin**" est une interface qui permet de simplifier l'administration.

### 1) Installation

► Pour installer "**phpldapadmin**", tapez la commande ci-dessous :

```
aptitude install phpldapadmin
```

### 2) Configuration de Apache2

Afin d'activer l'interface web, vous avez 2 solutions :

- En utilisant un lien symbolique (méthode rapide)
- En créant un site web (méthode plus sécurisé)

#### a) 1ère méthode

► Créer le lien symbolique en tapant la commande ci-dessous.

```
ln -s /usr/share/phpldapadmin/ /var/www/html/phpldapadmin
```

#### b) 2ème méthode

► Tapez la commande ci-dessous afin de créer une copie du fichier "**000-default.conf**".

```
cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/phpldapadmin.conf
```

► Éditez ensuite le fichier.

```
vim /etc/apache2/sites-available/phpldapadmin.conf
```

- ▶ Modifiez les lignes suivantes :

```
ServerName ldap.idum.eu
```

```
ServerAdmin webmaster@idum.eu
```

```
DocumentRoot /usr/share/phpldapadmin/
```

- ▶ Ajoutez les lignes suivantes en dessous de la ligne "**DocumentRoot**".

```
<Directory /usr/share/phpldapadmin/>
    AllowOverride None
    Require all granted
    Options -Indexes -FollowSymlinks
</Directory>
```

- ▶ Tapez la commande suivante pour activer le site.

```
a2ensite phpldapadmin.conf
```

- ▶ Vous devez obtenir ceci :

```
Enabling site phpldapadmin.
```

```
To activate the new configuration, you need to run:
```

```
service apache2 reload
```

- ▶ Comme demandé, relancez le service "**apache2**".

```
service apache2 reload
```

### 3) Configuration de phpldapadmin

- ▶ Éditez le fichier **config.php**

```
vim /etc/phpldapadmin/config.php
```

- ▶ Commencez par modifier la ligne "**timezone**", pour définir le timezone de "**Europe/Paris**" :

```
$config->custom->appearance['timezone'] = 'Europe/Paris';
```

- ▶ Modifiez la ligne ci-dessous qui correspond au nom du serveur (description du serveur) :

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

- ▶ Si votre **OpenLDAP** est sur un serveur différent que le serveur "**phpldapadmin**" alors définissez l'adresse IP du serveur LDAP :

```
$servers->setValue('server', 'host', '127.0.0.1');
```

- ▶ Définissez le nom du domaine :

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

- ▶ Définissez un utilisateur avec des droits admin de **OpenLDAP** :

```
$servers->setValue('login', 'bind_id', 'cn=admin,dc=idum,dc=eu');
```

- ▶ Relancez le serveur apache2 :

```
service apache2 reload
```

## 4) Interface WEB

► Si vous avez utilisé la 1ère méthode, tapez l'adresse suivante dans votre navigateur :

`http://10.10.10.11/phpldapadmin`

► Si vous avez utilisé la 2ème méthode, tapez l'adresse suivante dans votre navigateur :

`http://ldap.idum.eu`

► Vous devez obtenir la page ci-dessous. Cliquez sur le bouton "**connexion**" :



The screenshot shows the phpLDAPadmin web interface. At the top left is the logo 'phpLDAPadmin'. Below it are navigation links: 'Accueil | Purger les caches | Montrer le cache'. On the left side, there is a sidebar with 'LDAP Idum' and a 'connexion' button highlighted with a red box. The main content area features a message: 'S'authentifier auprès du serveur Successfully logged out of server.' Below this is the large 'phpLDAPadmin' logo. Underneath the logo, it says 'Utiliser le menu de gauche pour naviguer' and provides links for 'Crédits | Documentation | Donation'. The footer shows '1.2.2 sourceforge'.

► Saisissez le mot de passe de l'utilisateur "**admin**" saisie précédemment lors de l'installation.

LDAP Idum

connexion

## S'authentifier auprès du serveur LDAP Idum

Avertissement: Avertissement : la connexion Web n'est pas chiffrée..

**DN de connexion:**

**Mot de passe:**

Connexion anonyme

## 5) Compte manager

Il est toujours utile d'avoir plusieurs comptes pour se connecter. Je vous propose donc de créer un deuxième compte admin que nous nommerons "**manager**".

- ▶ Développez l'arborescence

LDAP Idum

schéma rechercher rafraîchir info importer exporter se déconnecter

Connecté en tant que :: cn=admin

- + dc=idum,dc=eu (1)

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

Utiliser le menu de gauche pour naviguer

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

- ▶ Cliquez sur "**cn=admin**".

LDAP Idum ⌚

schéma rechercher rafraîchir info importer exporter se déconnecter

Connecté en tant que :: cn=admin

dc=idum,dc=eu (1)

cn=admin

Créer une nouvelle entrée ici

► Cliquez sur "Copier ou déplacer cette entrée".

## cn=admin

Serveur: LDAP Idum Nom distingué: cn=admin,dc=idum,dc=eu  
Modèle: Valeur par défaut

 <a href="#">Rafraîchir</a>	 <a href="#">Afficher les attributs internes</a>
 <a href="#">Switch Template</a>	 <a href="#">Exporter</a>
 <a href="#">Copier ou déplacer cette entrée</a>	 <a href="#">Supprimer cette entrée</a>
 <a href="#">Renommer</a>	 <a href="#">Comparer avec une autre entrée</a>
 <a href="#">Créer une sous-entrée</a>	 <a href="#">Ajouter un nouvel attribut</a>

 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.

► Saisissez le nom "cn=manager,dc=idum,dc=eu", puis cliquez sur "Copier".

## Copier cn=admin

Serveur: LDAP Idum Nom distingué: cn=admin,dc=idum,dc=eu

Copier **cn=admin** vers un nouvel objet:

DN de destination:

 [parcourir](#)

Serveur de destination: LDAP Idum

Supprimer après la copie (déplacement) :

► Saisissez le mot de passe, puis cliquez sur "Créer un objet".

## Créer un objet

Serveur: LDAP Idum Conteneur: dc=idum,dc=eu  
Modèle: Valeur par défaut

**cn** requis, rdn

manager \*

(renommer)

**description**

LDAP administrator

**objectClass**

simpleSecurityObject

organizationalRole (structurel)

**Mot de passe** alias, requis

[Vérifier le mot de passe...](#)

► Cliquez sur "Valider".

## Créer Entrée LDAP

Serveur: **LDAP Idum** Conteneur: **dc=idum,dc=eu**

Voulez-vous créer cette entrée ?

Attribut	Nouvelle valeur	Passer
<b>cn=manager,dc=idum,dc=eu</b>		
<b>cn</b>	manager	<input type="checkbox"/>
<b>description</b>	LDAP administrator	<input type="checkbox"/>
<b>objectClass</b>	simpleSecurityObject organizationalRole	<input type="checkbox"/>
<b>Password</b>	*****	<input type="checkbox"/>

[Valider](#) [Annuler](#)

## 6) Création d'une Unité Organisationnelle

Nous allons créer 2 unités d'organisation :

- Groupes
- Utilisateurs

► Cliquez sur "Créer une nouvelle entrée ici".



Accueil | Purger les caches | Montrer le cache

LDAP Idum



schéma rechercher rafraîchir info importer exporter se déconnecter

Connecté en tant que :: cn=admin

dc=idum,dc=eu (2)

cn=admin

cn=manager

[★ Créer une nouvelle entrée ici](#)

► Sélectionnez "Générique : Unité Organisationnelle".

## Créer un objet

Serveur: LDAP Idum Conteneur: dc=idum,dc=eu

### Sélectionner un modèle pour le processus de création

- Modèles:**
- E-Mail : Compte
  - E-Mail : Alias
  - Générique : Entrée Carnet d'Adresse
  - Générique : Entrée DNS
  - Générique : LDAP Alias
  - Générique : Rôle Organisationnel
  - Générique : Unité Organisationnelle
  - Générique : Groupe Posix
  - Generic: Simple Security Object
  - Générique : Compte Utilisateur
  - Kolab: User Entry
  - Samba: Account
  - Samba: Domain
  - Samba: Group Mapping
  - Samba: Machine
  - Sendmail: Alias
  - Sendmail: Cluster
  - Sendmail: Domain
  - Sendmail: Relays
  - Sendmail: Virtual Domain
  - Sendmail: Virtual Users
  - Thunderbird: Address Book Entry
  - Valeur par défaut

► Saisissez le nom de l'unité organisationnelle, puis cliquez sur "Créer un objet".

## Créer un objet

Serveur: LDAP Idum Conteneur: dc=idum,dc=eu  
Modèle: Generic: Organisational Unit (ou)

### Nouvelle unité organisationnelle (Étape 1 sur 1)

Unité organisationnelle

alias, requis, rdn, astuce

Utilisateurs\*

Créer un objet

► Cliquez sur "Valider".

# Créer Entrée LDAP

Serveur: **LDAP Idum** Conteneur: **dc=idum,dc=eu**

Voulez-vous créer cette entrée ?

Attribut	Nouvelle valeur	Passer
<b>ou=Utilisateurs,dc=idum,dc=eu</b>		
objectClass	organizationalUnit	<input type="checkbox"/>
Organisational Unit	Utilisateurs	<input type="checkbox"/>

► Cliquez sur "Créer une nouvelle entrée ici".



Accueil | Purger les caches | Montrer le cache

LDAP Idum ⌚



[schéma](#) [rechercher](#) [rafraîchir](#) [info](#) [importer](#) [exporter](#) [se déconnecter](#)

Connecté en tant que :: cn=admin

dc=idum,dc=eu (3)

cn=admin

cn=manager

ou=Utilisateurs

► Sélectionnez "Générique : Unité Organisationnelle".

## Créer un objet

Serveur: LDAP Idum Conteneur: dc=idum,dc=eu

### Sélectionner un modèle pour le processus de création

- Modèles:**
-  E-Mail : Compte
  -  E-Mail : Alias
  -  Générique : Entrée Carnet d'Adresse
  -  Générique : Entrée DNS
  -  Générique : LDAP Alias
  -  Générique : Rôle Organisationnel
  -  Générique : Unité Organisationnelle
  -  Générique : Groupe Posix
  -  Generic: Simple Security Object
  -  Générique : Compte Utilisateur
  -  Kolab: User Entry
  -  Samba: Account
  -  Samba: Domain
  -  Samba: Group Mapping
  -  Samba: Machine
  -  Sendmail: Alias
  -  Sendmail: Cluster
  -  Sendmail: Domain
  -  Sendmail: Relays
  -  Sendmail: Virtual Domain
  -  Sendmail: Virtual Users
  -  Thunderbird: Address Book Entry
  -  Valeur par défaut

► Saisissez le nom de l'unité organisationnelle, puis cliquez sur "Créer un objet".

## Créer un objet

Serveur: LDAP Idum Conteneur: dc=idum,dc=eu  
Modèle: Generic: Organisational Unit (ou)

### Nouvelle unité organisationnelle (Étape 1 sur 1)

**Unité organisationnelle** alias, requis, rdn, astuce

\*

► Cliquez sur "Valider".

# Créer Entrée LDAP

Serveur: LDAP Idum Conteneur: dc=idum,dc=eu

Voulez-vous créer cette entrée ?

Attribut	Nouvelle valeur	Passer
ou=Groupes,dc=idum,dc=eu		
objectClass	organizationalUnit	<input type="checkbox"/>
Organisational Unit	Groupes	<input type="checkbox"/>

## 7) Création de groupes

Comme indiqué dans l'introduction nous allons créer 3 groupes :

- Administrateurs
- Webmasters
- Utilisateurs

► Cliquez sur "**ou=Groupes**".



Accueil | Purger les caches | Montrer le cache

LDAP Idum



schéma rechercher rafraîchir info importer exporter se déconnecter

Connecté en tant que :: cn=admin

dc=idum,dc=eu (4)

cn=admin

cn=manager

**ou=Groupes**

ou=Utilisateurs

★ Créer une nouvelle entrée ici

► Cliquez sur "**Créer une sous-entrée**".

## ou=Groupes

Serveur: LDAP Idum Nom distingué: ou=Groupes,dc=idum,dc=eu  
Modèle: Valeur par défaut

-  Rafraîchir
-  Switch Template
-  Copier ou déplacer cette entrée
-  Renommer
-  **Créer une sous-entrée**
-  Afficher les attributs internes
-  Exporter
-  Supprimer cette entrée
-  Comparer avec une autre entrée
-  Ajouter un nouvel attribut

 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.

► Sélectionnez "Générique : Groupe Posix".

## Créer un objet

Serveur: LDAP Idum Conteneur: ou=Groupes,dc=idum,dc=eu

### Sélectionner un modèle pour le processus de création

- Modèles:**
-  E-Mail : Compte
  -  E-Mail : Alias
  -  Générique : Entrée Carnet d'Adresse
  -  Générique : Entrée DNS
  -  Générique : LDAP Alias
  -  Générique : Rôle Organisationnel
  -  Générique : Unité Organisationnelle
  -  **Générique : Groupe Posix**
  -  Generic: Simple Security Object
  -  Générique : Compte Utilisateur
  -  Kolab: User Entry
  -  Samba: Account
  -  Samba: Domain
  -  Samba: Group Mapping
  -  Samba: Machine
  -  Sendmail: Alias
  -  Sendmail: Cluster
  -  Sendmail: Domain
  -  Sendmail: Relays
  -  Sendmail: Virtual Domain
  -  Sendmail: Virtual Users
  -  Thunderbird: Address Book Entry
  -  Valeur par défaut

► Saisissez le nom du groupe, puis cliquez sur "Créer un objet".

## Créer un objet

Serveur: **LDAP Idum** Conteneur: **ou=Groupes,dc=idum,dc=eu**  
Modèle: **Generic: Posix Group (posixGroup)**

### Nouveau groupe Posix (Étape 1 sur 1)

**GID**

alias, requis, astuce, ro

500

**Groupe**

alias, requis, rdn

Administrateurs\*

**Utilisateurs**

alias, astuce

Créer un objet

► Cliquez sur "Valider".

## Créer Entrée LDAP

Serveur: **LDAP Idum** Conteneur: **ou=Groupes,dc=idum,dc=eu**

Voulez-vous créer cette entrée ?

Attribut	Nouvelle valeur	Passer
<b>cn=Administrateurs,ou=Groupes,dc=idum,dc=eu</b>		
<b>GID Number</b>	500	<input type="checkbox"/>
<b>Group</b>	Administrateurs	<input type="checkbox"/>
<b>objectClass</b>	posixGroup	<input type="checkbox"/>

Valider Annuler

► Cliquez sur "ou=Groupes".

LDAP Idum ⌚

schéma rechercher rafraîchir info importer exporter se déconnecter

Connecté en tant que :: cn=admin

- dc=idum , dc=eu (4)
  - cn=admin
  - cn=manager
  - ou=Groupes (1+)**
  - ou=Utilisateurs
  - ★ Créer une nouvelle entrée ici

► Cliquez sur "**Créer une sous-entrée**".

## ou=Groupes

Serveur: LDAP Idum Nom distingué: ou=Groupes,dc=idum,dc=eu  
Modèle: Valeur par défaut

<a href="#">Rafraîchir</a>	<a href="#">Afficher les attributs internes</a>
<a href="#">Switch Template</a>	<a href="#">Exporter</a>
<a href="#">Copier ou déplacer cette entrée</a>	<a href="#">Supprimer cette entrée</a>
<a href="#">Renommer</a>	<a href="#">Comparer avec une autre entrée</a>
<b><a href="#">Créer une sous-entrée</a></b>	<a href="#">Ajouter un nouvel attribut</a>
Astuce : pour supprimer un attribut, videz le champ texte et enregistrez.	
<a href="#">Afficher 1 sous-entrée</a>	<a href="#">Exporter une sous-arborescence</a>
Astuce : pour afficher le schéma d'un attribut, cliquez sur le nom de l'attribut.	

► Sélectionnez "**Générique : Groupe Posix**".

## Créer un objet

Serveur: LDAP Idum Conteneur: ou=Groupes,dc=idum,dc=eu

### Sélectionner un modèle pour le processus de création

- Modèles:**
- E-Mail : Compte
  - E-Mail : Alias
  - Générique : Entrée Carnet d'Adresse
  - Générique : Entrée DNS
  - Générique : LDAP Alias
  - Générique : Rôle Organisationnel
  - Générique : Unité Organisationnelle
  - Générique : Groupe Posix**
  - Generic: Simple Security Object
  - Générique : Compte Utilisateur
  - Kolab: User Entry
  - Samba: Account
  - Samba: Domain
  - Samba: Group Mapping
  - Samba: Machine
  - Sendmail: Alias
  - Sendmail: Cluster
  - Sendmail: Domain
  - Sendmail: Relays
  - Sendmail: Virtual Domain
  - Sendmail: Virtual Users
  - Thunderbird: Address Book Entry
  - Valeur par défaut

► Saisissez le nom du groupe, puis cliquez sur "Créer un objet".

## Créer un objet

Serveur: LDAP Idum Conteneur: ou=Groupes,dc=idum,dc=eu  
Modèle: Generic: Posix Group (posixGroup)

### Nouveau groupe Posix (Étape 1 sur 1)

**GID** alias, requis, astuce, ro

501

**Groupe** alias, requis, rdn

Webmasters\*

**Utilisateurs** alias, astuce

Créer un objet

► Cliquez sur "Valider".

# Créer Entrée LDAP

Serveur: **LDAP Idum** Conteneur: **ou=Groupes,dc=idum,dc=eu**

Voulez-vous créer cette entrée ?

Attribut	Nouvelle valeur	Passer
<b>cn=Webmasters,ou=Groupes,dc=idum,dc=eu</b>		
GID Number	501	<input type="checkbox"/>
Group	Webmasters	<input type="checkbox"/>
objectClass	posixGroup	<input type="checkbox"/>

**Valider** Annuler

► Cliquez sur "**ou=Groupes**".



Accueil | Purger les caches | Montrer le cache

LDAP Idum



schéma rechercher rafraîchir info importer exporter se déconnecter

Connecté en tant que :: cn=admin

dc=idum,dc=eu (4)

cn=admin

cn=manager

**ou=Groupes (2)**

ou=Utilisateurs

★ Créer une nouvelle entrée ici

► Cliquez sur "**Créer une sous-entrée**".

## ou=Groupes

Serveur: **LDAP Idum** Nom distingué: **ou=Groupes,dc=idum,dc=eu**  
Modèle: **Valeur par défaut**

 <a href="#">Rafraîchir</a>	 <a href="#">Afficher les attributs internes</a>
 <a href="#">Switch Template</a>	 <a href="#">Exporter</a>
 <a href="#">Copier ou déplacer cette entrée</a>	 <a href="#">Supprimer cette entrée</a>
 <a href="#">Renommer</a>	 <a href="#">Comparer avec une autre entrée</a>
 <a href="#">Créer une sous-entrée</a>	 <a href="#">Ajouter un nouvel attribut</a>
 Astuce : pour supprimer un attribut, videz le champ texte et enregistrez.	
 <a href="#">Afficher 2 sous-entrées</a>	 <a href="#">Exporter une sous-arborescence</a>
 Astuce : pour afficher le schéma d'un attribut, cliquez sur le nom de l'attribut.	

► Sélectionnez "**Générique : Groupe Posix**".

## Créer un objet

Serveur: **LDAP Idum** Conteneur: **ou=Groupes,dc=idum,dc=eu**  
Modèle: **Generic: Posix Group (posixGroup)**

### Nouveau groupe Posix (Étape 1 sur 1)

**GID** alias, requis, astuce, ro

502

**Groupe** alias, requis, rdn

Utilisateurs \*

**Utilisateurs** alias, astuce

[Créer un objet](#)

► Saisissez le nom du groupe, puis cliquez sur "**Créer un objet**".

## Créer un objet

Serveur: LDAP Idum Conteneur: ou=Groupes,dc=idum,dc=eu

### Sélectionner un modèle pour le processus de création

- Modèles:**
- E-Mail : Compte
  - E-Mail : Alias
  - Générique : Entrée Carnet d'Adresse
  - Générique : Entrée DNS
  - Générique : LDAP Alias
  - Générique : Rôle Organisationnel
  - Générique : Unité Organisationnelle
  - Générique : Groupe Posix**
  - Generic: Simple Security Object
  - Générique : Compte Utilisateur
  - Kolab: User Entry
  - Samba: Account
  - Samba: Domain
  - Samba: Group Mapping
  - Samba: Machine
  - Sendmail: Alias
  - Sendmail: Cluster
  - Sendmail: Domain
  - Sendmail: Relays
  - Sendmail: Virtual Domain
  - Sendmail: Virtual Users
  - Thunderbird: Address Book Entry
  - Valeur par défaut

► Cliquez sur "Valider".

## Créer Entrée LDAP

Serveur: LDAP Idum Conteneur: ou=Groupes,dc=idum,dc=eu

Voulez-vous créer cette entrée ?

Attribut	Nouvelle valeur	Passer
<b>cn=Utilisateurs,ou=Groupes,dc=idum,dc=eu</b>		
<b>GID Number</b>	502	<input type="checkbox"/>
<b>Group</b>	Utilisateurs	<input type="checkbox"/>
<b>objectClass</b>	posixGroup	<input type="checkbox"/>

## 8) Création d'utilisateurs

Nous allons maintenant créer manuellement 3 utilisateurs :

- Vincent THYMME - appartenant au groupe : Utilisateurs
- Paul HETTE - appartenant au groupe : Administrateurs

- Jacques ADIT - appartenant au groupe : Webmasters

► Cliquez sur "**ou=Utilisateurs**".

The screenshot shows the phpLDAPadmin interface. At the top, there are navigation links: "Accueil | Purger les caches | Montrer le cache". Below this is the "LDAP Idum" section with a clock icon. A row of icons represents various actions: "schéma", "rechercher", "rafraîchir", "info", "importer", "exporter", and "se déconnecter". Below the icons, it says "Connecté en tant que :: cn=admin". The LDAP tree structure is shown below, with "dc=idum, dc=eu (4)" expanded to show "cn=admin", "cn=manager", and "ou=Groupes (3)". The "ou=Utilisateurs" entry is highlighted with a red box. At the bottom of the tree, there is a star icon and the text "Créer une nouvelle entrée ici".

► Cliquez sur "**Créer une sous-entrée**".

The screenshot shows the "ou=Utilisateurs" entry details page. The title is "ou=Utilisateurs" in a blue header. Below the title, it says "Serveur: LDAP Idum" and "Nom distingué: ou=Utilisateurs,dc=idum,dc=eu". Below that, it says "Modèle: Valeur par défaut". There are two columns of action buttons: "Rafraîchir", "Switch Template", "Copier ou déplacer cette entrée", "Renommer", "Créer une sous-entrée" (highlighted with a red box), "Afficher les attributs internes", "Exporter", "Supprimer cette entrée", "Comparer avec une autre entrée", and "Ajouter un nouvel attribut". At the bottom, there are two lightbulb icons representing tips: "Astuce : pour supprimer un attribut, videz le champ texte et enregistrez." and "Astuce : pour afficher le schéma d'un attribut, cliquez sur le nom de l'attribut."

► Sélectionnez "**Générique : Compte Utilisateur**".

# Créer un objet

Serveur: LDAP Idum Conteneur: ou=Utilisateurs,dc=idum,dc=eu

## Sélectionner un modèle pour le processus de création

- Modèles:**
-  E-Mail : Compte
  -  E-Mail : Alias
  -  Générique : Entrée Carnet d'Adresse
  -  Générique : Entrée DNS
  -  Générique : LDAP Alias
  -  Générique : Rôle Organisationnel
  -  Générique : Unité Organisationnelle
  -  Générique : Groupe Posix
  -  Generic: Simple Security Object
  -  **Générique : Compte Utilisateur**
  -  Kolab: User Entry
  -  Samba: Account
  -  Samba: Domain
  -  Samba: Group Mapping
  -  Samba: Machine
  -  Sendmail: Alias
  -  Sendmail: Cluster
  -  Sendmail: Domain
  -  Sendmail: Relays
  -  Sendmail: Virtual Domain
  -  Sendmail: Virtual Users
  -  Thunderbird: Address Book Entry
  -  Valeur par défaut

► Saisissez les différentes informations, puis cliquez sur "**Créer un objet**".

# Créer un objet

Serveur: **LDAP Idum** Conteneur: **ou=Utilisateurs,dc=idum,dc=eu**  
Modèle: **Generic: User Account (posixAccount)**

## Nouveau compte utilisateur (Étape 1 sur 1)

<b>Nom Commun</b>	alias, requis, rdn
<input type="text" value="Vincent THYMME"/>	*
<b>Prénom</b>	alias
 <input type="text" value="Vincent"/>	
<b>GID</b>	alias, requis, astuce
<input type="text" value="Utilisateurs"/>	*
<b>Répertoire personnel</b>	alias, requis
<input type="text" value="/home/users/vthymme"/>	*
<b>Nom de famille</b>	alias, requis
<input type="text" value="THYMME"/>	*
<b>Login shell</b>	alias
<input type="text" value="/bin/sh"/>	
<b>Mot de passe</b>	alias, astuce
 <input type="password" value="..."/>	md5
<input type="password" value="..."/>	(confirmer)
<a href="#">Vérifier le mot de passe...</a>	
<b>UID</b>	alias, requis, astuce, ro
 <input type="text" value="1000"/>	
<b>ID utilisateur</b>	alias, requis
<input type="text" value="vthymme"/>	*

**Créer un objet**

► Cliquez sur "**Valider**".

# Créer Entrée LDAP

Serveur: **LDAP Idum** Conteneur: **ou=Utilisateurs,dc=idum,dc=eu**

Voulez-vous créer cette entrée ?

Attribut	Nouvelle valeur	Passer
<b>cn=Vincent THYMME,ou=Utilisateurs,dc=idum,dc=eu</b>		
Common Name	Vincent THYMME	<input type="checkbox"/>
First name	Vincent	<input type="checkbox"/>
GID Number	502	<input type="checkbox"/>
Home directory	/home/users/vthymme	<input type="checkbox"/>
Last name	THYMME	<input type="checkbox"/>
Login shell	/bin/sh	<input type="checkbox"/>
objectClass	inetOrgPerson posixAccount	<input type="checkbox"/>
Password	*****	<input type="checkbox"/>
UID Number	1000	<input type="checkbox"/>
User ID	vthymme	<input type="checkbox"/>

**Valider** Annuler

► Cliquez sur "**ou=Utilisateurs**".

The screenshot shows the phpLDAPadmin interface. At the top, there is a navigation bar with "Accueil | Purger les caches | Montrer le cache". Below this, the main content area displays the LDAP tree structure for "LDAP Idum". The tree shows a hierarchy starting with "dc=idum, dc=eu (4)", which contains "cn=admin" and "cn=manager". Below these are "ou=Groupes (3)" and "ou=Utilisateurs (1)". The "ou=Utilisateurs (1)" entry is highlighted with a red box. At the bottom of the tree, there is a star icon and the text "Créer une nouvelle entrée ici".

► Cliquez sur "**Créer une sous-entrée**".

## ou=Utilisateurs

Serveur: LDAP Idum Nom distingué: ou=Utilisateurs,dc=idum,dc=eu  
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.
-  Afficher 1 sous-entrée
-  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
-  Exporter une sous-arborescence

► Sélectionnez "Générique : Compte Utilisateur".

## Créer un objet

Serveur: LDAP Idum Conteneur: ou=Utilisateurs,dc=idum,dc=eu

### Sélectionner un modèle pour le processus de création

- Modèles:**
-  E-Mail : Compte
  -  E-Mail : Alias
  -  Générique : Entrée Carnet d'Adresse
  -  Générique : Entrée DNS
  -  Générique : LDAP Alias
  -  Générique : Rôle Organisationnel
  -  Générique : Unité Organisationnelle
  -  Générique : Groupe Posix
  -  Generic: Simple Security Object
  -  **Générique : Compte Utilisateur**
  -  Kolab: User Entry
  -  Samba: Account
  -  Samba: Domain
  -  Samba: Group Mapping
  -  Samba: Machine
  -  Sendmail: Alias
  -  Sendmail: Cluster
  -  Sendmail: Domain
  -  Sendmail: Relays
  -  Sendmail: Virtual Domain
  -  Sendmail: Virtual Users
  -  Thunderbird: Address Book Entry
  -  Valeur par défaut

► Saisissez les différentes informations, puis cliquez sur "Créer un objet".

# Créer un objet

Serveur: **LDAP Idum** Conteneur: **ou=Utilisateurs,dc=idum,dc=eu**  
Modèle: **Generic: User Account (posixAccount)**

## Nouveau compte utilisateur (Étape 1 sur 1)

<b>Nom Commun</b>	alias, requis, rdn
<input type="text" value="Paul HETTE"/>	*
<b>Prénom</b>	alias
 <input type="text" value="Paul"/>	*
<b>GID</b>	alias, requis, astuce
<input type="text" value="Administrateurs"/>	*
<b>Répertoire personnel</b>	alias, requis
<input type="text" value="/home/users/phette"/>	*
<b>Nom de famille</b>	alias, requis
<input type="text" value="HETTE"/>	*
<b>Login shell</b>	alias
<input type="text" value="/bin/sh"/>	*
<b>Mot de passe</b>	alias, astuce
 <input type="password" value="..."/> <input type="text" value="md5"/>	*
<input type="password" value="..."/> (confirmer)	*
<a href="#">Vérifier le mot de passe...</a>	
<b>UID</b>	alias, requis, astuce, rdn
 <input type="text" value="1001"/>	*
<b>ID utilisateur</b>	alias, requis
<input type="text" value="phette"/>	*

**Créer un objet**

► Cliquez sur "**Valider**".

# Créer Entrée LDAP

Serveur: **LDAP Idum** Conteneur: **ou=Utilisateurs,dc=idum,dc=eu**

Voulez-vous créer cette entrée ?

Attribut	Nouvelle valeur	Passer
<b>cn=Paul HETTE,ou=Utilisateurs,dc=idum,dc=eu</b>		
Common Name	Paul HETTE	<input type="checkbox"/>
First name	Paul	<input type="checkbox"/>
GID Number	500	<input type="checkbox"/>
Home directory	/home/users/phette	<input type="checkbox"/>
Last name	HETTE	<input type="checkbox"/>
Login shell	/bin/sh	<input type="checkbox"/>
objectClass	inetOrgPerson posixAccount	<input type="checkbox"/>
Password	*****	<input type="checkbox"/>
UID Number	1001	<input type="checkbox"/>
User ID	phette	<input type="checkbox"/>

**Valider** Annuler

► Cliquez sur "ou=Utilisateurs".

The screenshot shows the phpLDAPadmin web interface. At the top, there is a navigation bar with links: Accueil | Purger les caches | Montrer le cache. Below this, the main content area displays the LDAP tree for 'LDAP Idum'. The tree structure is as follows:

- LDAP Idum
  - dc=idum, dc=eu (4)
    - cn=admin
    - cn=manager
    - ou=Groupes (3)
    - ou=Utilisateurs (2)** (highlighted with a red box)
    - Créer une nouvelle entrée ici

► Cliquez sur "Créer une sous-entrée".

## ou=Utilisateurs

Serveur: LDAP Idum Nom distingué: ou=Utilisateurs,dc=idum,dc=eu  
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.
-  Afficher 2 sous-entrées
-  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
-  Exporter une sous-arborescence

► Sélectionnez "Générique : Compte Utilisateur".

## Créer un objet

Serveur: LDAP Idum Conteneur: ou=Utilisateurs,dc=idum,dc=eu

### Sélectionner un modèle pour le processus de création

- Modèles:
-  E-Mail : Compte
  -  E-Mail : Alias
  -  Générique : Entrée Carnet d'Adresse
  -  Générique : Entrée DNS
  -  Générique : LDAP Alias
  -  Générique : Rôle Organisationnel
  -  Générique : Unité Organisationnelle
  -  Générique : Groupe Posix
  -  Generic: Simple Security Object
  -  **Générique : Compte Utilisateur**
  -  Kolab: User Entry
  -  Samba: Account
  -  Samba: Domain
  -  Samba: Group Mapping
  -  Samba: Machine
  -  Sendmail: Alias
  -  Sendmail: Cluster
  -  Sendmail: Domain
  -  Sendmail: Relays
  -  Sendmail: Virtual Domain
  -  Sendmail: Virtual Users
  -  Thunderbird: Address Book Entry
  -  Valeur par défaut

► Saisissez les différentes informations, puis cliquez sur "Créer un objet".

# Créer un objet

Serveur: **LDAP Idum** Conteneur: **ou=Utilisateurs,dc=idum,dc=eu**  
Modèle: **Generic: User Account (posixAccount)**

## Nouveau compte utilisateur (Étape 1 sur 1)

<b>Nom Commun</b>	alias, requis, rdn
<input type="text" value="Jacques ADIT"/>	*
<b>Prénom</b>	alias
 <input type="text" value="Jacques"/>	*
<b>GID</b>	alias, requis, astuce
<input type="text" value="Webmasters"/>	*
<b>Répertoire personnel</b>	alias, requis
<input type="text" value="/home/users/jadit"/>	*
<b>Nom de famille</b>	alias, requis
<input type="text" value="ADIT"/>	*
<b>Login shell</b>	alias
<input type="text" value="/bin/sh"/>	*
<b>Mot de passe</b>	alias, astuce
 <input type="password" value="..."/> <input type="text" value="md5"/>	
<input type="password" value="..."/> (confirmer)	
<a href="#">Vérifier le mot de passe...</a>	
<b>UID</b>	alias, requis, astuce, rdn
 <input type="text" value="1002"/>	*
<b>ID utilisateur</b>	alias, requis
<input type="text" value="jadit"/>	*

**Créer un objet**

► Cliquez sur "**Valider**".

## Créer Entrée LDAP

Serveur: **LDAP Idum** Conteneur: **ou=Utilisateurs,dc=idum,dc=eu**

Voulez-vous créer cette entrée ?

Attribut	Nouvelle valeur	Passer
<b>cn=Jacques ADIT,ou=Utilisateurs,dc=idum,dc=eu</b>		
<b>Common Name</b>	Jacques ADIT	<input type="checkbox"/>
<b>First name</b>	Jacques	<input type="checkbox"/>
<b>GID Number</b>	501	<input type="checkbox"/>
<b>Home directory</b>	/home/users/jadit	<input type="checkbox"/>
<b>Last name</b>	ADIT	<input type="checkbox"/>
<b>Login shell</b>	/bin/sh	<input type="checkbox"/>
<b>objectClass</b>	inetOrgPerson posixAccount	<input type="checkbox"/>
<b>Password</b>	*****	<input type="checkbox"/>
<b>UID Number</b>	1002	<input type="checkbox"/>
<b>User ID</b>	jadit	<input type="checkbox"/>

## 9) Importation d'utilisateurs

La méthode du chapitre précédent pour ajouter des utilisateurs est bien pour du cas par cas, mais lors d'un ajout en masse ce n'est pas pratique. Avec "**phpldapadmin**" vous avez la possibilité d'importer un fichier au format LDIF.

Dans le chapitre suivant j'expliquerai comment générer le fichier LDIF.

- ▶ Cliquez sur "**importer**".

LDAP Idum ⌚

schéma rechercher rafraîchir info **importer** exporter se déconnecter

Connecté en tant que :: cn=admin

- dc=idum,dc=eu (4)
  - cn=admin
  - cn=manager
  - ou=Groupes (3)
  - ou=Utilisateurs (3)
  - ★ Créer une nouvelle entrée ici

- ▶ Sélectionnez votre fichier en cliquant sur "**Choisissez un fichier**" où copier le contenu de votre fichier dans l'encadrer.
- ▶ Puis cliquez sur le bouton "**Procéder >>**".

### Importer

Serveur: LDAP Idum

Sélectionner un fichier LDIF :  addusers-...412.ldif  
Taille maximale du fichier : 2M

ou coller votre LDIF ici

Ne pas vous arrêter sur les erreurs

- ▶ Vous pouvez observer que l'import à fonctionner en vérifiant le nombre d'utilisateurs avant et après l'import.



## V) Script

### 1) Prérequis

- ▶ Commencez par créer un répertoire sur votre serveur :

```
mkdir Generateur_LDIF
cd ./Generateur_LDIF
```

- ▶ Téléchargez ensuite les deux scripts que j'ai créés :

```
wget http://idum.eu/Telechargements/Scripts/article_326/gen-adduser-ldif.sh
wget http://idum.eu/Telechargements/Scripts/article_326/gen-deluser-ldif.sh
```

- ▶ Vous devez maintenant déposer votre fichier "liste de noms" dans le répertoire. Votre fichier doit être un fichier CSV avec séparation point-virgule. Une ligne par personne. Respectant le schéma ci-dessous :

- ID ;Prenom ;Nom ;UserID ;

- ▶ Voici un exemple de mon fichier liste de noms.csv :

```
1;Jesper;Gauvin;jgauvin
2;Romaine;Authier;rauthier
3;Agrican;Auclair;aaclair
4;Paul;Daoust;pdaoust
5;Madeleine;Latourelle;mlatourelle
6;Michèle;Pelletier;mpelletier
7;Calandre;Petit;cpetit
8;Scoville;Lafrenière;slafrenière
9;Belisarda;Chauvin;bchauvin
```

► Vous pouvez télécharger le fichier que j'ai utilisé comme exemple :

```
wget http://idum.eu/Telechargements/Scripts/article_326/listedenoms.csv
```

Voilà vous êtes prêts.

## 2) Script pour générer un fichier adduser.ldif

Nous voulons générer un fichier LDIF pour ajouter des utilisateurs en masse dans **OpenLDAP**.

Avant de commencer à jouer avec le script, voici à quoi ressemble un fichier LDIF compatible avec l'import de **"phpldapadmin"** :

```
dn: cn=Jesper GAUVIN,ou=Utilisateurs,dc=idum,dc=eu
cn: Jesper GAUVIN
gidnumber: 502
givenname: Jesper
homedirectory: /home/users/jgauvin
mail: jgauvin@idum.eu
objectclass: inetOrgPerson
objectclass: posixAccount
objectclass: top
loginshell: /bin/sh
sn: GAUVIN
uid: jgauvin
uidnumber: 10001
userpassword: {MD5}7Dmb674iW1CvQotyN9XTSw==
```

```
dn: cn=Romaine AUTHIER,ou=Utilisateurs,dc=idum,dc=eu
cn: Romaine AUTHIER
gidnumber: 502
givenname: Romaine
homedirectory: /home/users/rauthier
mail: rauthier@idum.eu
objectclass: inetOrgPerson
objectclass: posixAccount
objectclass: top
loginshell: /bin/sh
sn: AUTHIER
uid: rauthier
uidnumber: 10002
userpassword: {MD5}7Dmb674iW1CvQotyN9XTSw==
```

```
dn: cn=Agrican AUCLAIR,ou=Utilisateurs,dc=idum,dc=eu
cn: Agrican AUCLAIR
gidnumber: 502
givenname: Agrican
homedirectory: /home/users/aaclair
mail: aaclair@idum.eu
```

```
objectclass: inetOrgPerson
objectclass: posixAccount
objectclass: top
loginshell: /bin/sh
sn: AUCLAIR
uid: aauclair
uidnumber: 10003
userpassword: {MD5}7Dmb674iW1CvQotyN9XTSw==
```

Maintenant que nous avons vu le modèle, exécutez le script.

► Dans le répertoire "**Generateur\_LDIF**" tapez la commande suivante pour exécuter le script :

```
bash gen-adduser-ldif.sh
```

► Chaque utilisateur doit avoir un uidnumber unique, le script vous demande s'il doit commencer le compteur à "10 000" où si vous souhaitez taper une valeur.

```
Voulez-vous commencer le compteur UID à '10 000' ? (Y/N)
```

```
y
```

► Pour chaque utilisateur, vous devez définir un shell par défaut. Le script vous demande si vous voulez utiliser **"/bin/sh"**, sinon tapez le shell que vous souhaitez utiliser :

```
Votre shell est '/bin/sh' ? (Y/N)
```

```
y
```

► Pour chaque utilisateur, vous devez définir un répertoire personnel. Le script vous demande si les répertoires personnels seront stockés dans **"/home/users/NOM\_DE\_L UTILISATEUR"** :

```
Le chemin des répertoires personnels se trouve dans '/home/users/' ? (Y/N)
```

```
y
```

► Le script va générer un mot de passe pour tous les utilisateurs, souhaitez-vous utiliser le mot de passe **"password-NOM\_DE\_L UTILISATEUR"**. Sinon le script peut vous propose de générer le même mot de passe pour tous les utilisateurs :

```
Voulez-vous utilisez le mot de passe 'password-username' ? (Y/N):
```

```
y
```

► Définissez le groupe ID (GID) auquel les utilisateurs seront rattachés :

```
Definissez le Group ID :
```

```
502
```

► Définissez le domaine :

```
Definissez le domaine :
```

idum.eu

- Saisissez le nom de votre fichier liste de noms.csv :

Votre fichier doit être un fichier csv avec séparation point-virgule.

Une ligne par personne respectant le schéma ci-dessous :

ID;Prenom;Nom;UserID;

Comment ce nomme votre fichier liste de noms :

listedenoms.csv

- Tapez la commande suivante pour voir si le fichier est bien généré :

```
cat addusers-20170412.ldif
```

Vous avez plus qu'à importer votre fichier avec "**phpldapadmin**" comme indiqué dans le chapitre III.9).

### 3) Script pour générer un fichier deluser.ldif

Nous voulons générer un fichier LDIF pour supprimer des utilisateurs en masse dans **OpenLDAP**.

Contrairement au fichier ajout, celui-ci ne peut pas être utilisé avec "**phpldapadmin**", j'expliquerai dans le prochain chapitre comment supprimer avec la commande "**ldapdelete**".

Le fichier que nous souhaitons générer doit avoir cette syntaxe :

```
cn=Jesper GAUVIN,ou=Utilisateurs,dc=idum,dc=eu
```

```
cn=Romaine AUTHIER,ou=Utilisateurs,dc=idum,dc=eu
```

```
cn=Agrican AUCLAIR,ou=Utilisateurs,dc=idum,dc=eu
```

```
cn=Paul DAOUST,ou=Utilisateurs,dc=idum,dc=eu
```

Dans le répertoire "**Generateur\_LDIF**", tapez la commande suivante pour exécuter le script :

```
bash gen-deluser-ldif.sh
```

- Définissez le domaine :

Definissez le domaine :

idum.eu

- Saisissez le nom de votre fichier liste de "noms.csv" :

Votre fichier doit être un fichier csv avec séparation point-virgule.

Une ligne par personne respectant le schéma ci-dessous :

ID;Prenom;Nom;UserID;

Comment ce nomme votre fichier liste de noms :

listedenoms.csv

- Tapez la commande suivante pour voir si le fichier est bien généré :

```
cat addusers-20170412.ldif
```

## VI) Quelques commandes LDAP

### 1) Ldapsearch

La commande "**ldapsearch**" vous permet de faire des recherches et de vérifier le bon fonctionnement de **OpenLDAP**.

#### a) Tout afficher

► Pour vérifier que **OpenLDAP** fonctionne, tapez l'une des commandes suivantes :

```
ldapsearch -x -H ldap:/// -D "cn=admin,dc=idum,dc=eu" -W
ldapsearch -v -H ldap:/// -D "cn=admin,dc=idum,dc=eu" -W "objectClass=*"
ldapsearch -x
```

► Vous devez obtenir ceci :

```
ldapsearch -x -H ldap:/// -D "cn=admin,dc=idum,dc=eu" -W
Enter LDAP Password:
# extended LDIF
#
# LDAPv3
# base <dc=idum,dc=eu> (default) with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# idum.eu
dn: dc=idum,dc=eu
objectClass: top
objectClass: dcObject
objectClass: organization
o: idum.eu
dc: idum

# admin, idum.eu
dn: cn=admin,dc=idum,dc=eu
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9N0NRYmVlMGFWQXBuTnVRcWZJb1JXdVNCSEd0ZjZZSXo=

# manager, idum.eu
dn: cn=manager,dc=idum,dc=eu
cn: manager
description: LDAP administrator
```

```
objectClass: simpleSecurityObject
objectClass: organizationalRole
objectClass: top
userPassword:: e1NTSEF9SmhFaXAxQLZEd1Yxa01UZFUvVm9VV1JUV2JJLy90cWo=
```

```
# Utilisateurs, idum.eu
dn: ou=Utilisateurs,dc=idum,dc=eu
objectClass: organizationalUnit
objectClass: top
ou: Utilisateurs
```

```
# Groupes, idum.eu
dn: ou=Groupes,dc=idum,dc=eu
objectClass: organizationalUnit
objectClass: top
ou: Groupes
```

```
# Administrateurs, Groupes, idum.eu
dn: cn=Administrateurs,ou=Groupes,dc=idum,dc=eu
gidNumber: 500
cn: Administrateurs
objectClass: posixGroup
objectClass: top
```

```
# Webmasters, Groupes, idum.eu
dn: cn=Webmasters,ou=Groupes,dc=idum,dc=eu
gidNumber: 501
cn: Webmasters
objectClass: posixGroup
objectClass: top
```

```
# Utilisateurs, Groupes, idum.eu
dn: cn=Utilisateurs,ou=Groupes,dc=idum,dc=eu
gidNumber: 502
cn: Utilisateurs
objectClass: posixGroup
objectClass: top
```

```
# Vincent THYMME, Utilisateurs, idum.eu
dn: cn=Vincent THYMME,ou=Utilisateurs,dc=idum,dc=eu
cn: Vincent THYMME
givenName: Vincent
gidNumber: 502
homeDirectory: /home/users/vthymme
sn: THYMME
loginShell: /bin/sh
```

objectClass: inetOrgPerson  
objectClass: posixAccount  
objectClass: top  
userPassword:: e01ENX1rQUZRbUR6U1Q3RFdsajk5S09GL2NnPT0=  
uidNumber: 1000  
uid: vthymme  
mail: vthymme@idum.eu

# Paul HETTE, Utilisateurs, idum.eu  
dn: cn=Paul HETTE,ou=Utilisateurs,dc=idum,dc=eu  
cn: Paul HETTE  
givenName: Paul  
gidNumber: 500  
homeDirectory: /home/users/phette  
sn: HETTE  
loginShell: /bin/sh  
objectClass: inetOrgPerson  
objectClass: posixAccount  
objectClass: top  
userPassword:: e01ENX1rQUZRbUR6U1Q3RFdsajk5S09GL2NnPT0=  
uidNumber: 1001  
uid: phette

# Jacques ADIT, Utilisateurs, idum.eu  
dn: cn=Jacques ADIT,ou=Utilisateurs,dc=idum,dc=eu  
cn: Jacques ADIT  
givenName: Jacques  
gidNumber: 501  
homeDirectory: /home/users/jadit  
sn: ADIT  
loginShell: /bin/sh  
objectClass: inetOrgPerson  
objectClass: posixAccount  
objectClass: top  
userPassword:: e01ENX1rQUZRbUR6U1Q3RFdsajk5S09GL2NnPT0=  
uidNumber: 1002  
uid: jadit

# Compta, Groupes, idum.eu  
dn: cn=Compta,ou=Groupes,dc=idum,dc=eu  
objectClass: top  
objectClass: posixGroup  
gidNumber: 503  
cn: Compta  
memberUid: jgauvin  
memberUid: aclavette

```
# Ordinateurs, idum.eu
dn: ou=Ordinateurs,dc=idum,dc=eu
objectClass: top
objectClass: organizationalUnit
ou: ordinateurs
```

```
# search result
search: 2
result: 0 Success
```

```
# numResponses: 14
# numEntries: 13
```

## b) Rechercher un utilisateur

► Nous souhaitons rechercher l'utilisateur "**Jacques ADIT**" afin de vérifier qu'il est bien présent dans la base et pour connaître son uidnumber.

```
ldapsearch -v -H ldap:/// -D "cn=admin,dc=idum,dc=eu" -W -LLL "cn=Jacques
ADIT" cn sn uid uidnumber
```

► Vous devez obtenir ceci :

```
ldap_initialize( ldap://:389/??base )
Enter LDAP Password:
filter: cn=Jacques ADIT
requesting: cn sn uid uidnumber
dn: cn=Jacques ADIT,ou=Utilisateurs,dc=idum,dc=eu
cn: Jacques ADIT
sn: ADIT
uidNumber: 1002
uid: jadit
```

## 2) ldapadd

La commande "**ldapadd**" permet d'ajouter une ou des entrée(s) dans **OpenLDAP**.

### a) Ajout d'utilisateur

► Pour ajouter un utilisateur, vous devez créer un fichier "user.ldif" comme ceci :

```
vim user.ldif
```

► Ajoutez ensuite les informations suivantes :

```
dn: cn=Jesper GAUVIN,ou=Utilisateurs,dc=idum,dc=eu
cn: Jesper GAUVIN
gidnumber: 502
givenname: Jesper
homedirectory: /home/users/jgauvin
```

```
mail: jgauvin@idum.eu
objectclass: inetOrgPerson
objectclass: posixAccount
objectclass: top
loginshell: /bin/sh
sn: GAUVIN
uid: jgauvin
uidnumber: 10001
userpassword: {MD5}7Dmb674iW1CvQotyN9XTSw==
```

► Ensuite tapez la commande suivante pour ajouter l'utilisateur :

```
ldapadd -v -x -H ldap:/// -W -D "cn=admin,dc=idum,dc=eu" -f user.ldif
```

► Vous devez obtenir ceci :

```
ldap_initialize( ldap://:389/??base )
Enter LDAP Password:
add cn:
    Jesper GAUVIN
add gidnumber:
    502
add givenname:
    Jesper
add homedirectory:
    /home/users/jgauvin
add mail:
    jgauvin@idum.eu
add objectclass:
    inetOrgPerson
    posixAccount
    top
add loginshell:
    /bin/sh
add sn:
    GAUVIN
add uid:
    jgauvin
add uidnumber:
    10001
add userpassword:
    {MD5}7Dmb674iW1CvQotyN9XTSw==
adding new entry "cn=Jesper GAUVIN,ou=Utilisateurs,dc=idum,dc=eu"
modify complete
```

► Voilà votre utilisateur est ajouté.

► Précédemment nous avons créé un fichier contenant une liste d'utilisateur. Pour l'ajouter il vous suffit d'utiliser la même commande.

## b) Ajout de groupe

- ▶ Pour ajouter un groupe, vous devez créer un fichier "groupe.ldif" comme ceci :

```
vim groupe.ldif
```

- ▶ Ajoutez ensuite les informations suivantes :

```
dn: cn=Compta,ou=Groupes,dc=idum,dc=eu
objectClass: top
objectClass: posixGroup
gidNumber: 503
```

- ▶ Ensuite tapez la commande suivante :

```
ldapadd -v -x -H ldap:/// -W -D "cn=admin,dc=idum,dc=eu" -f groupe.ldif
```

- ▶ Vous devez obtenir ceci :

```
ldap_initialize( ldap://:389/??base )
Enter LDAP Password:
add objectClass:
    top
    posixGroup
add gidNumber:
    503
adding new entry "cn=Compta,ou=Groupes,dc=idum,dc=eu"
modify complete
```

- ▶ Votre nouveau groupe est ajouté.

## c) Ajout d'une Unité Organisationnelle

- ▶ Pour ajouter une Unité Organisationnelle, vous devez créer un fichier "ou.ldif" comme ceci :

```
vim ou.ldif
```

- ▶ Ajoutez ensuite les informations suivantes :

```
dn: ou=Ordinateurs,dc=idum,dc=eu
objectClass: top
objectClass: organizationalUnit
ou: ordinateurs
```

- ▶ Ensuite tapez la commande suivante :

```
ldapadd -v -x -H ldap:/// -W -D "cn=admin,dc=idum,dc=eu" -f ou.ldif
```

- ▶ Vous devez obtenir ceci :

```
ldap_initialize( ldap://:389/??base )
Enter LDAP Password:
add objectClass:
    top
    organizationalUnit
add ou:
```

```
ordinateurs
adding new entry "ou=Ordinateurs,dc=idum,dc=eu"
modify complete
```

► Votre nouvelle Unité Organisationnelle est ajoutée.

### 3) Ldapmodify

#### a) Ajout d'un utilisateur dans un groupe

► Pour ajouter un utilisateur dans un groupe, vous devez utiliser la commande "**ldapmodify**" et créer un fichier "modif-user.ldif".

- Nous souhaitons ajouter l'utilisateur "aclavette" au groupe "Compta".

```
vim modif-user.ldif
```

► Ajoutez ensuite les informations suivantes :

```
dn: cn=Compta,ou=Groupes,dc=idum,dc=eu
changetype: modify
add: memberuid
memberuid: aclavette
```

► Ensuite tapez la commande suivante :

```
ldapmodify -v -x -H ldap:/// -W -D "cn=admin,dc=idum,dc=eu" -f modif-
user.ldif
```

► Vous devez obtenir ceci :

```
ldap_initialize( ldap://:389/??base )
Enter LDAP Password:
add memberuid:
    jgauvin
modifying entry "cn=Compta,ou=Groupes,dc=idum,dc=eu"
modify complete
```

#### b) Modification d'un utilisateur

► Pour modifier par exemple le nom d'un utilisateur, créer un fichier "modif-user2.ldif".

- Nous voulons modifier le sn de l'utilisateur "Jesper GAUVIN" par la valeur "EASTWOOD".

```
vim modif-user2.ldif
```

► Ajoutez ensuite les informations suivantes :

```
dn: cn=Jesper GAUVIN,ou=Utilisateurs,dc=idum,dc=eu
changetype: modify
replace: sn
sn: EASTWOOD
```

► Ensuite tapez la commande suivante :

```
ldapmodify -v -x -H ldap:/// -W -D "cn=admin,dc=idum,dc=eu" -f modif-
```

user2.ldif

- ▶ Vous devez obtenir ceci :

```
ldap_initialize( ldap://:389/??base )
Enter LDAP Password:
replace sn:
    EASTWOOD
modifying entry "cn=Jesper GAUVIN,ou=Utilisateurs,dc=idum,dc=eu"
modify complete
```

## 4) ldapdelete

- ▶ Pour supprimer un utilisateur, tapez la commande suivante :

```
ldapdelete -v -H ldap:/// -D "cn=admin,dc=idum,dc=eu" -W "cn=Jesper
GAUVIN,ou=Utilisateurs,dc=idum,dc=eu"
```

- ▶ Vous devez obtenir ceci :

```
ldap_initialize( ldap://:389/??base )
Enter LDAP Password:
deleting entry "cn=Jesper GAUVIN,ou=Utilisateurs,dc=idum,dc=eu"
```

- ▶ Pour supprimer plusieurs utilisateurs via un fichier "deluser.ldif". Tapez la commande suivante :

```
ldapdelete -v -c -H ldapi:/// -D "cn=admin,dc=idum,dc=eu" -W -f delusers-
20170412.ldif
```

- ▶ Vous devez obtenir ceci :

```
ldap_initialize( ldapi:///??base )
Enter LDAP Password:
deleting entry "cn=Jesper GAUVIN,ou=Utilisateurs,dc=idum,dc=eu"
ldap_delete: No such object (32)
    matched DN: ou=Utilisateurs,dc=idum,dc=eu
deleting entry "cn=Romaine AUTHIER,ou=Utilisateurs,dc=idum,dc=eu"
deleting entry "cn=Agrican AUCLAIR,ou=Utilisateurs,dc=idum,dc=eu"
deleting entry "cn=Paul DAOUST,ou=Utilisateurs,dc=idum,dc=eu"
deleting entry "cn=Madeleine LATOURELLE,ou=Utilisateurs,dc=idum,dc=eu"
deleting entry "cn=Michele PELLETIER,ou=Utilisateurs,dc=idum,dc=eu"
deleting entry "cn=Calandre PETIT,ou=Utilisateurs,dc=idum,dc=eu"
deleting entry "cn=Scoville LAFRENIERE,ou=Utilisateurs,dc=idum,dc=eu"
deleting entry "cn=Belisarda CHAUVIN,ou=Utilisateurs,dc=idum,dc=eu"
deleting entry "cn=Iven GILBERT,ou=Utilisateurs,dc=idum,dc=eu"
deleting entry "cn=Renee CHANDONNET,ou=Utilisateurs,dc=idum,dc=eu"
deleting entry "cn=Fleurette TREPANIER,ou=Utilisateurs,dc=idum,dc=eu"
....
....
....
deleting entry "cn=Caresse BOUTOT,ou=Utilisateurs,dc=idum,dc=eu"
ldap_delete: No such object (32)
```

```
    matched DN: ou=Utilisateurs,dc=idum,dc=eu
deleting entry "cn=Lirienne CUILLERIER,ou=Utilisateurs,dc=idum,dc=eu"
deleting entry "cn=Andree CHARLEBOIS,ou=Utilisateurs,dc=idum,dc=eu"
deleting entry "cn=Leon RENE,ou=Utilisateurs,dc=idum,dc=eu"
ldap_delete: No such object (32)
    matched DN: ou=Utilisateurs,dc=idum,dc=eu
deleting entry "cn=Babette DE LAUNAY,ou=Utilisateurs,dc=idum,dc=eu"
deleting entry "cn=Sumner PERILLARD,ou=Utilisateurs,dc=idum,dc=eu"
deleting entry "cn=Delit BERTHELETTE,ou=Utilisateurs,dc=idum,dc=eu"
deleting entry "cn=Bradamate PAULET,ou=Utilisateurs,dc=idum,dc=eu"
deleting entry "cn=Melisande VERREAU,ou=Utilisateurs,dc=idum,dc=eu"
deleting entry "cn=Aubine CAOUETTE,ou=Utilisateurs,dc=idum,dc=eu"
deleting entry "cn=Berangaria SOUCY,ou=Utilisateurs,dc=idum,dc=eu"
ldap_delete: No such object (32)
    matched DN: ou=Utilisateurs,dc=idum,dc=eu
deleting entry "cn=Patrice LEMELIN,ou=Utilisateurs,dc=idum,dc=eu"
```

5 juin 2017 -- [N.Salmon](#)