

# Introduction aux annuaires LDAP avec OpenLDAP

Philippe Latu

philippe.latu(at)linux-france.org

<http://www.linux-france.org/prj/inetdoc/>

Historique des versions		
\$Revision: 1637 \$	\$Date: 2011-04-30 15:11:22 +0200 (sam. 30 avril 2011) \$	\$Author: latu \$
Année universitaire 2010-2011		
Résumé		
L'objectif de ce deuxième support de travaux pratiques de la série est l'étude du service d'annuaire LDAP. On présente succinctement les éléments constitutifs d'un annuaire puis on étudie la configuration d'un service d'annuaire basé sur le logiciel OpenLDAP. Ensuite, on étudie la configuration de l'accès aux entrées de l'annuaire depuis un poste client. Les informations délivrées par l'annuaire sont les propriétés de comptes utilisateurs stockées dans la classe d'objet posixAccount.		

## Table des matières

1. Copyright et Licence .....	1
1.1. Méta-information .....	2
1.2. Conventions typographiques .....	2
2. Adressage IP des postes de travail .....	2
3. Principes d'un annuaire LDAP .....	2
4. Configuration du serveur LDAP .....	4
4.1. Installation du serveur LDAP .....	4
4.2. Analyse de la configuration du service LDAP .....	4
4.3. Réinitialisation de la base de l'annuaire LDAP .....	5
4.4. Composition d'un nouvel annuaire LDAP .....	5
4.5. Gestion de l'annuaire avec phpLDAPadmin .....	6
5. Configuration de l'accès client au serveur LDAP .....	6
5.1. Interrogation à distance de l'annuaire LDAP .....	7
5.2. Configuration <i>Name Service Switch</i> .....	7
6. Analyse de la configuration .....	8
6.1. Indexation des entrées de l'annuaire LDAP .....	8
6.2. Analyse réseau des transactions LDAP .....	8
7. Documents de référence .....	8

## 1. Copyright et Licence

Copyright (c) 2000,2011 Philippe Latu.  
Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Copyright (c) 2000,2011 Philippe Latu.  
Permission est accordée de copier, distribuer et/ou modifier ce document selon les termes de la Licence de Documentation Libre GNU (GNU Free Documentation License), version 1.2 ou toute version ultérieure publiée par la Free Software Foundation ; sans Sections Invariables ; sans Texte de Première de Couverture, et sans Texte de Quatrième de Couverture. Une copie de la présente Licence est incluse dans la section intitulée « Licence de Documentation Libre GNU ».

## 1.1. Méta-information

Cet article est écrit avec *DocBook*<sup>1</sup> XML sur un système *Debian GNU/Linux*<sup>2</sup>. Il est disponible en version imprimable au format PDF : [admin.reseau.ldap.pdf](http://admin.reseau.ldap.pdf)<sup>3</sup>.

## 1.2. Conventions typographiques

Tous les exemples d'exécution des commandes sont précédés d'une invite utilisateur ou *prompt* spécifique au niveau des droits utilisateurs nécessaires sur le système.

- Toute commande précédée de l'invite `$` ne nécessite aucun privilège particulier et peut être utilisée au niveau utilisateur simple.
- Toute commande précédée de l'invite `#` nécessite les privilèges du super-utilisateur.

## 2. Adressage IP des postes de travail

Tableau 1. Affectation des adresses IP des postes de travaux pratiques

Poste 1	Poste 2	Passerelle par défaut	Organisation
alderaan	bespin	10.7.10.1/23	o: zone1.lan-213.stri
centares	coruscant	192.168.110.129/25	o: zone2.lan-213.stri
dagobah	endor	172.19.113.65/26	o: zone3.lan-213.stri
felucia	geonosis	10.3.2.1/23	o: zone4.lan-213.stri
hoth	mustafar	172.20.130.25/29	o: zone5.lan-213.stri
naboo	tatooine	192.168.111.1/25	o: zone6.lan-213.stri

Toutes les questions de ce support peuvent être traitées avec le document de référence : *OpenLDAP Software 2.4 Administrator's Guide*<sup>4</sup>. Il est cependant nécessaire de faire la correspondance entre les services décrits dans le document et les paquets de la distribution *Debian GNU/Linux*.

Pour chaque paire de postes de travaux pratiques, il faut attribuer les rôles de serveur et de client. Le serveur doit mettre à disposition de son poste client une base de données utilisateurs. L'objectif en fin de séance de travaux pratiques est de pouvoir se connecter sur un poste client avec ses authentifiants `login/password`.

Relativement au précédent support sur l' *Introduction au système de fichiers réseau NFS*<sup>5</sup>, on ne dispose pas d'un système de fichiers réseau. Ici, seule l'authentification est fonctionnelle et il n'est pas possible d'accéder au répertoire utilisateur stocké sur le serveur NFS.

## 3. Principes d'un annuaire LDAP

Dans l'histoire des systèmes Unix, les services de *nommage* ont connu de nombreuses évolutions avec le développement de l'Internet et des volumes d'informations à partager.

Au début des années 80, un premier service baptisé *Network Information Service* (NIS) a vu le jour. Ce service est une méthode de distribution de la base de données des utilisateurs, de fichiers de configuration, d'authentification et d'autres données entre les hôtes d'un réseau local. Le logiciel NIS développé par Sun Microsystems<sup>TM</sup> fonctionne sur le mode Client/Serveur à partir d'une base de données «à plat» (*flat bindery base*). Son utilisation est étudiée dans le support de travaux pratiques *Introduction au service NIS*<sup>6</sup>. Avec un service NIS, il n'est pas possible de constituer des groupes logiques ayant des attributs propres. Cette limitation est rapidement devenue critique avec l'augmentation du nombres des utilisateurs et des clients.

<sup>1</sup> <http://www.docbook.org>

<sup>2</sup> <http://www.debian.org>

<sup>3</sup> <http://www.linux-france.org/prj/inetdoc/telechargement/admin.reseau.ldap.pdf>

<sup>4</sup> <http://www.openldap.org/doc/admin24/>

<sup>5</sup> <http://www.linux-france.org/prj/inetdoc/cours/index.html#admin.reseau.nfs>

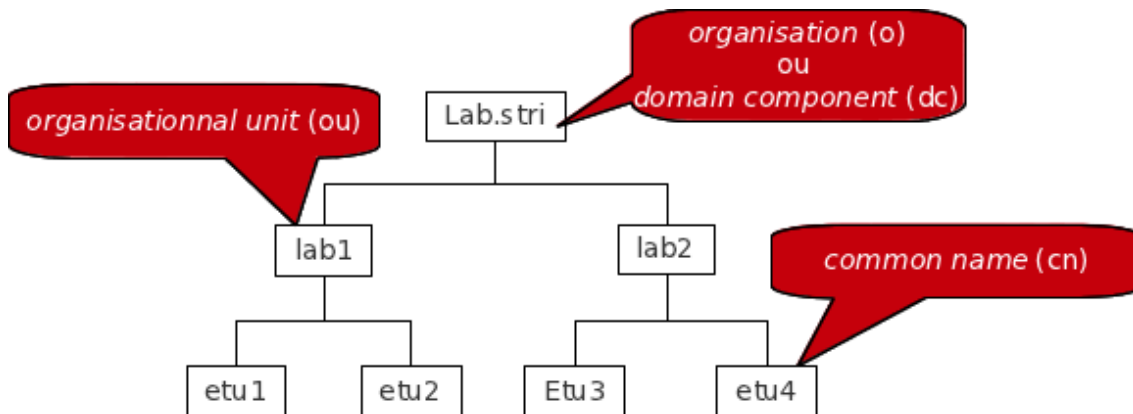
<sup>6</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.nis/>

D'autres services plus complets tels que NIS+ ou *kerberos* qui n'assure que la partie authentification ont été développés par la suite. Depuis quelques années, les annuaires LDAP ou *Lightweight Directory Access Protocol* se sont imposés comme étant l'outil d'échange universel des paramètres utilisateurs.

Pour définir ce qu'est le service LDAP, on peut retenir les caractéristiques suivantes.

- Un service de publication d'annuaire
- Un protocole d'accès aux annuaires de type X.500 ou *Lightweight Directory Access Protocol*
- Un dépôt de données basées sur des attributs ou un «genre» de base de données
- Un logiciel optimisé pour les recherches avancées et les lectures
- Une implémentation client/serveur
- Un mécanisme extensible de schémas de description de classes d'objets

Les entrées (*Directory Service Entry*) d'un annuaire LDAP sont distribuées suivant une arborescence (*Directory Information Tree*) hiérarchisée que l'on peut voir comme un système de fichiers avec ses répertoires et ses fichiers. Au sommet de l'arborescence on trouve un nom de racine (*Domain Component*) ou suffixe.



### Arborescence LDAP élémentaire - vue complète<sup>7</sup>

L'adresse d'une entrée de l'annuaire LDAP est appelée : *distinguished name* ou dn. En reprenant l'exemple d'arborescence ci-dessus, les adresses des différentes entrées sont notées comme suit.

- dn: dc=lab,dc=stri
- dn: ou=lab1,dc=lab,dc=stri
- dn: ou=lab2,dc=lab,dc=stri
- dn: cn=etu1,ou=lab1,dc=lab,dc=stri
- dn: cn=etu2,ou=lab1,dc=lab,dc=stri
- dn: cn=etu3,ou=lab1,dc=lab,dc=stri
- dn: cn=etu4,ou=lab1,dc=lab,dc=stri

L'adresse de chaque entrée appartient à une classe d'objet (*ObjectClass*) spécifiée dans un schéma (*schema*). En reprenant les mêmes exemples d'entrées, on peut associer les classes d'objets correspondantes.

<i>entry</i>	<i>objectclass</i>
o: lab.stri	organisation
dc: lab	dcObject
dc: stri	dcObject

<sup>7</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap/images/ldap-tree.png>

<i>entry</i>	<i>objectclass</i>
ou: lab1	organisationalUnit
cn: etu1	person
sn: etu1	

Un schéma peut être vu comme un ensemble de règles qui décrivent la nature des données stockées. C'est un outil qui aide à maintenir la cohérence, la qualité et qui évite la duplication des données dans l'annuaire. Les attributs des classes d'objets déterminent les règles qui doivent être appliquées à une entrée. Un schéma contient les éléments suivants.

- Les attributs requis
- Les attributs autorisés
- Les règles de comparaison des attributs
- Les valeurs limites qu'un attribut peut recevoir
- Les restrictions sur les informations qui peuvent être enregistrées

## 4. Configuration du serveur LDAP

Avant d'aborder la configuration du service LDAP, il faut passer par les étapes rituelles de sélection et d'installation des paquets contenant les outils logiciels du service. Ensuite, il faut identifier les processus, les numéros de ports ouverts et les fichiers de configuration à éditer.

### 4.1. Installation du serveur LDAP

1. Quels sont les paquets Debian relatifs au service LDAP ?

Interroger la base de données des paquets pour obtenir les informations demandées.

2. Quels sont les paquets Debian à installer pour mettre en œuvre un serveur LDAP ?

3. Comment identifier le ou les processus correspondant au service installé ?

Utiliser une commande d'affichage de la liste des processus actifs sur le système pour identifier le démon correspondant au serveur LDAP.

4. Comment identifier le ou les numéros de ports ouverts par le service installé ?

Utiliser une commande d'affichage de la liste des ports ouverts sur le système.

### 4.2. Analyse de la configuration du service LDAP

Les versions récentes du logiciel *OpenLDAP* utilisent un mode de configuration basé sur un *Directory Information Tree* ou DIT propre. Cette arborescence de configuration est pointée par le nom `cn=config`. Elle est utilisée pour configurer dynamiquement le démon `slapd`, modifier les définitions de schéma, les index, les listes de contrôle d'accès ACLs, etc. Ce mode de configuration présente un avantage déterminant lorsque l'on exploite des annuaires volumineux : toutes les opérations se font sans interruption de service.

Les documents fournis avec le paquet `slapd` contiennent des informations indispensables à l'analyse du fonctionnement du service.

1. Quel est le mode de gestion de la configuration du service adopté depuis la version 2.4.23-3 du paquet de la distribution Debian GNU/Linux ?
2. Quel est le gestionnaire de base de données (*backend*) proposé dans le fichier de configuration ?
3. Comment identifier le nom de l'annuaire fourni par défaut avec le paquet `slapd` ?
4. Quels sont les *schemas* actifs avec la configuration courante du paquet `slapd` ?

5. Où sont stockées les bases définies par défaut lors de l'installation du paquet `slapd` ?

### 4.3. Réinitialisation de la base de l'annuaire LDAP

L'installation du paquet `slapd` implique l'installation d'un annuaire minimal avec une base associée. Ce mode opératoire est nécessaire, ne serait-ce que pour accéder à la configuration du service et tester la validité de l'installation. Après avoir traité les questions ci-dessus, on sait que l'installation est fonctionnelle. On peut donc passer à l'initialisation de notre propre annuaire.



#### Note

Les manipulations proposées dans cette section permettent de reprendre à zéro la configuration d'un annuaire LDAP. Il peut être utile de revenir à cette étape en cas de «doute» sur l'intégrité de l'annuaire lors du traitement des questions des sections suivantes.

1. Comment arrêter le service LDAP ?

Utiliser les scripts fournis avec le gestionnaire de lancement des processus système (*run-levels*).

2. Quels sont les éléments à effacer pour pouvoir installer une nouvelle configuration et une nouvelle base LDAP ?

Utiliser le résultat de la question sur la **localisation des bases** et la documentation fournie avec le paquet `slapd`.

3. Comment reprendre à zéro la configuration du paquet `slapd` ?

Utiliser l'outil du gestionnaire de paquets *Debian GNU/Linux* qui permet la modification des paramètres de configuration d'un service à l'aide de menus `debconf`.

4. Comment valider la nouvelle configuration du paquet `slapd` ?

Reprendre la question sur le **nom distinctif** de l'annuaire.

### 4.4. Composition d'un nouvel annuaire LDAP

Une fois que les fichiers de configuration et de base de données du nouvel annuaire sont en place, on peut passer à l'ajout de nouvelles entrées dans cet annuaire. Comme le fil conducteur de cette série de travaux pratiques est la gestion d'une base de comptes utilisateurs, on doit ajouter les objets suivants.

- Deux unités organisationnelles : `people` et `groups`.
- Quatre compte utilisateurs : `papa` et `maman Skywalker` ainsi que leurs deux enfants

Toutes les manipulations sur les objets de l'annuaire utilisent un format de fichier texte particulier baptisé LDIF pour *LDAP Data Interchange Format*. C'est un format de représentation des données contenues dans un annuaire particulièrement utile pour les opérations de sauvegarde et de restauration en volume.

Du point de vue formatage, chaque enregistrement doit être séparé du suivant par une ligne vide et chaque attribut d'un enregistrement apparaît sur une ligne sous la forme «`nomAttribut: valeur`».

1. Comment visualiser la liste des entrées contenues dans l'annuaire LDAP ?

Utiliser les pages de manuels de la commande **`ldapsearch`** et rechercher les informations sur les méthodes d'authentification, la désignation de la base dans laquelle on effectue la recherche et le nom distinctif utilisé pour se connecter à l'annuaire.

2. Comment activer la journalisation des manipulations sur les entrées de l'annuaire LDAP ?

Rechercher l'entrée relative au niveau de journalisation dans le DIT et modifier sa valeur de façon à obtenir un état dans les journaux système à chaque opération sur l'annuaire.

La modification de l'entrée du DIT doit se faire à l'aide d'un fichier LDIF approprié.

3. Quelle est la syntaxe du fichier LDIF qui permet d'ajouter les deux unités organisationnelles (*organisational unit*) ?

Rechercher un tutoriel LDIF en ligne donnant un exemple de fichier LDIF avec une ou plusieurs entrées ou :

4. Quelle est la commande à utiliser pour ajouter une ou plusieurs entrées dans l'annuaire ?

Rechercher dans la liste des programmes fournis avec le paquet des outils LDAP.

5. Quelle est la commande à utiliser pour saisir manuellement un mot de passe et obtenir la chaîne chiffrée correspondante ?

Rechercher dans la liste des programmes fournis avec les paquets de la distribution puis consulter les pages de manuels correspondantes.

6. Quelle est la syntaxe du fichier LDIF qui permet d'ajouter les quatre utilisateurs avec leurs attributs système : identifiants `uid/gid`, authentifiants `login/passwd`, etc ?

Rechercher un tutoriel LDIF en ligne donnant un exemple de fichier LDIF avec un exemple de description des attributs d'un compte utilisateur.

## 4.5. Gestion de l'annuaire avec phpLDAPAdmin

Après avoir vu quelques manipulations à base de fichiers LDIF dans la section précédente, on se propose maintenant d'introduire un outil de gestion d'annuaire avec une interface de type service Internet. Le client Web *phpLDAPAdmin* est représentatif de cette catégorie d'outil. Il ne peut pas se substituer aux fichiers LDIF pour les traitements en volume, mais il peut très bien servir de console d'analyse et de support.

Dans cette section, on commence par installer l'outil avec le serveur Web *apache2* et on configure un accès sécurisé SSL. On ajoute un groupe d'utilisateurs baptisé *StarWars* dans l'unité organisationnelle `groups` et on visualise le schéma d'une entrée du type `posixAccount`.

1. Quel est le paquet à installer pour mettre en place le client Web *phpLDAPAdmin* ?

Rechercher le nom `phpldapadmin` dans la liste des paquets de la distribution et installer ce paquet.

2. Comment activer l'accès SSL au service Web ?

Consulter les fichiers de documentation fournis avec le paquet *apache2* et repérer les instructions d'activation du service SSL.

3. Quel est le fichier de configuration du paquet `phpldapadmin` qui contient la définition du contexte de nommage (suffixe) ?

Rechercher le répertoire contenant les fichiers de configuration du paquet. Repérer le fichier contenant la définition du suffixe de l'annuaire.

4. Quelles modifications apporter à ce fichier de configuration pour utiliser le suffixe de travaux pratiques ?

Rechercher les options de la commande `sed` qui permettent de substituer `dc=example,dc=com` dans le fichier de configuration du paquet `phpldapadmin`.

5. Comment ajouter un groupe *StarWars* dans l'unité organisationnelle `groups` ?

6. Comment visualiser les attributs d'une entrée de type `posixAccount` ?

## 5. Configuration de l'accès client au serveur LDAP

Dans cette section, on suppose qu'un annuaire LDAP est disponible et accessible. On se propose de configurer un poste client pour qu'il obtienne de façon transparente les informations sur les comptes utilisateurs desservis par l'annuaire.

## 5.1. Interrogation à distance de l'annuaire LDAP

On reprend ici les requêtes de visualisation des entrées vues dans la [Section 4.4, « Composition d'un nouvel annuaire LDAP »](#). Cette fois ci les requêtes sont émises depuis un hôte réseau différent du serveur.

1. Quel est le paquet qui fournit les commandes de manipulation des entrées de l'annuaire ?  
Interroger la base de données des paquets pour obtenir les informations demandées.
2. Quelle est la syntaxe d'interrogation de l'annuaire qui permet d'obtenir tous les attributs de l'enregistrement correspondant à un utilisateur particulier ?
3. Quelle est la syntaxe de la commande permettant de changer le mot de passe de l'utilisateur dont on a affiché les attributs à la question précédente ?

## 5.2. Configuration *Name Service Switch*

Les manipulations présentées ici ont pour but de rendre transparent l'accès aux attributs des comptes utilisateurs. Le mécanisme *Name Service Switch* assure un aiguillage de l'accès à ces attributs entre les fichiers locaux et les différents services réseau disponibles. Ici, l'annuaire LDAP constitue un dépôt de référence pour le stockage des attributs des comptes utilisateurs.

1. Quel est le nom du paquet relatif au mécanisme *Name Service Switch* permettant d'accéder aux ressources de l'annuaire LDAP ?  
Rechercher dans les bases du gestionnaire de paquets un paquet dont le nom débute par la chaîne `libnss`.
2. Quels sont les paquets qui dépendent de l'installation des bibliothèques LDAP pour le mécanisme *Name Service Switch* ?  
Utiliser les informations contenues dans la description du paquet pour repérer les dépendances entre paquets.
3. Quel est le rôle de l'interface entre les fonctions PAM (*Pluggable Authentication Modules*) et l'annuaire LDAP ?
4. Quelles sont les principales étapes de la configuration des paquets de bibliothèques NSS et PAM ?  
Lors de l'installation des deux paquets de bibliothèques LDAP, on passe par une série de menus `debconf` qu'il faut renseigner correctement pour accéder au serveur LDAP de façon transparente.
5. Quelles sont les modifications à apporter au fichier de configuration `/etc/nsswitch.conf` pour activer l'accès aux ressources de l'annuaire LDAP ?  
Suivant les indications données dans la série de menus `debconf` ci-dessus, il faut éditer manuellement le fichier `/etc/nsswitch.conf`. Consulter les exemples fournis avec la documentation du paquet de bibliothèques LDAP pour le mécanisme NSS.
6. Comment illustrer simplement le fonctionnement du mécanisme *Name Service Switch* intégrant l'utilisation de l'annuaire LDAP ?  
Rechercher la commande de récupération des entrées depuis les bases de données d'administration dans les outils fournis avec les bibliothèques standard (paquet `libc-bin`).
7. Comment valider l'authentification d'un utilisateur déclaré dans l'annuaire LDAP ?  
Choisir un service qui nécessite une authentification sur le système et qui utilise une entrée de l'annuaire LDAP.



### Avertissement

Après chaque manipulation sur la configuration des paquets `libnss-ldap` et `libpam-ldap`, il faut impérativement relancer le démon de gestion du cache des services de noms : `# /etc/init.d/nscd restart`.

Sans le redémarrage de ce démon, il est fréquent que les tests de connexion échouent alors que la configuration système est correcte.

## 6. Analyse de la configuration

Dans cette partie, on considère que les services élémentaires sont en place. Côté **serveur**, on dispose de l'unité organisationnelle `people` qui contient quatre entrées de comptes utilisateurs. Côté **client**, les outils d'accès à l'annuaire LDAP ont été installés et l'authentification sur la base des attributs des entrées de l'annuaire fonctionne.

Les manipulations suivantes sont à réaliser en concertation entre les deux postes de travaux pratiques client et serveur.

### 6.1. Indexation des entrées de l'annuaire LDAP

Comme la **journalisation des transactions sur l'annuaire** a été activée sur le serveur, toutes les **authentifications** réalisées par le client apparaissent dans ces journaux.

1. Quelles sont les informations relatives à l'indexation des entrées de l'annuaire qui apparaissent dans les journaux système du serveur lorsqu'une transaction est initiée par le client ?

Que constate-t-on ?

Rechercher le mot clé `index` dans le principal fichier de journalisation système du serveur.

2. Quelle est la syntaxe du fichier LDIF permettant d'ajouter les index identifiés dans la configuration du service LDAP ?

Rechercher un tutoriel LDIF en ligne donnant un exemple de fichier LDIF avec une ou plusieurs entrées `index`.

3. Comment mettre en place les nouveaux index et valider leur présence dans la configuration du service LDAP ?

Reprendre la démarche suivie lors de l'activation des fonctions de **journalisation**.

4. Comment créer les index dans la base de données du démon `slapd` ?

Rechercher dans la liste des fichiers du paquet `slapd` la commande relative à l'indexation des entrées d'un annuaire.

### 6.2. Analyse réseau des transactions LDAP

Comme dans le cas du support sur l'*Introduction au système de fichiers réseau NFS*<sup>8</sup>, la compréhension des mécanismes d'accès à un annuaire passe par l'analyse réseau. Les opérations de capture de trafic peuvent être réalisées aussi bien sur le poste client que sur le poste serveur.

1. Quelles sont les étapes de l'accès aux ressources de l'annuaire LDAP dans les trois cas de figure ci-dessous ?

Exécuter les instructions suivantes depuis le poste client.

- `# getent passwd`
- `$ su anakin`
- `anakin@clnt:/home/etu$ passwd`

## 7. Documents de référence

*OpenLDAP Software 2.4 Administrator's Guide*

La documentation officielle : *OpenLDAP Software 2.4 Administrator's Guide*<sup>9</sup> constitue le point d'entrée essentiel pour la mise en œuvre du service LDAP.

<sup>8</sup> <http://www.linux-france.org/prj/inetdoc/cours/index.html#admin.reseau.nfs>

<sup>9</sup> <http://www.openldap.org/doc/admin24/>