

LDAP



Présentation

OpenLDAP est une implémentation open source du protocole LDAP (Lightweight Directory Access Protocol), un protocole standard utilisé pour accéder et gérer des annuaires d'informations. Voici une présentation de ses caractéristiques principales :

1. **Service d'annuaire** : OpenLDAP fournit un service d'annuaire, qui est une base de données hiérarchique utilisée pour stocker des informations sur les utilisateurs, les groupes, les ressources réseau et d'autres entités dans un réseau informatique.
2. **Protocole LDAP** : OpenLDAP implémente le protocole LDAP, qui permet aux applications et aux clients d'accéder et de manipuler les données stockées dans l'annuaire. LDAP est largement utilisé dans les environnements informatiques pour l'authentification, l'autorisation, la recherche d'informations et d'autres opérations liées à la gestion des identités.
3. **Open Source et Gratuit** : OpenLDAP est distribué sous une licence open source (généralement la licence OpenLDAP Public License) et est gratuit à utiliser et à distribuer. Cela permet aux organisations de déployer des services d'annuaire sans frais de licence.
4. **Sécurité** : OpenLDAP prend en charge divers mécanismes de sécurité pour protéger les données stockées dans l'annuaire, y compris l'authentification des clients, le chiffrement des communications et le contrôle d'accès basé sur des politiques.
5. **Extensibilité** : OpenLDAP est hautement extensible, ce qui signifie qu'il peut être étendu pour prendre en charge de nouveaux schémas de données, des mécanismes d'authentification personnalisés et d'autres fonctionnalités spécifiques aux besoins de l'organisation.
6. **Interopérabilité** : OpenLDAP est compatible avec d'autres implémentations LDAP et peut interagir avec une large gamme d'applications et de services qui prennent en charge le

protocole LDAP. Cela permet d'intégrer facilement OpenLDAP dans des environnements informatiques existants.

7. **Administration et Gestion** : OpenLDAP est livré avec des outils d'administration et de gestion qui facilitent la configuration, la surveillance et la maintenance de l'annuaire LDAP.

En résumé, OpenLDAP est une solution puissante et flexible pour la gestion des identités et des ressources dans un réseau informatique. En tant que service d'annuaire open source, il offre une alternative économique et évolutive aux solutions d'annuaire propriétaires.

Installation

Dans le terminal, en superuser :

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

Choisir un mot de passe pour l'admin ldap

Ensuite, on va devoir définir le domaine, dans le fichier :

```
nano /etc/ldap/ldap.conf
```

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

BASE    dc=e-ecole,dc=org
URI     ldap://192.168.1.1

#SIZELIMIT    12
#TIMELIMIT    15
#DEREF        never

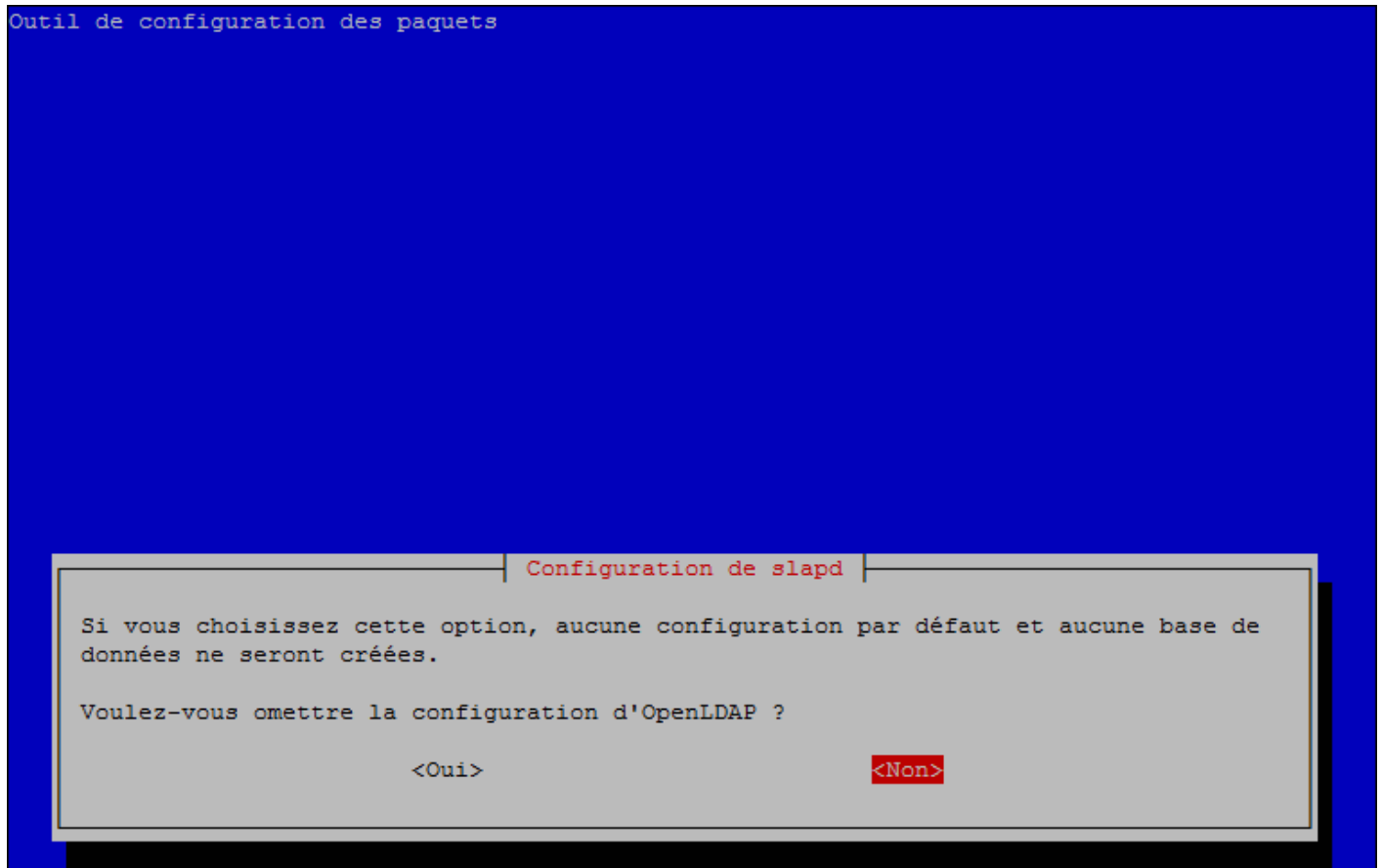
# TLS certificates (needed for GnuTLS)
TLS_CACERT    /etc/ssl/certs/ca-certificates.crt
```

Les deux lignes `BASE` et `URI` sont à décommenter et à remplir comme l'exemple ci-dessus, avec le nom de domaine et l'ip serveur.

On va pouvoir à présent configurer le paquet slapd installé plus tôt :

```
dpkg-reconfigure slapd
```

Lors de la première question "Voulez-vous omettre la configuration [...]", il faut répondre non, auquel cas, la configuration se ferme.



Saisissez votre nom de domaine, dans notre exemple : e-ecole.org, deux fois

Configuration de slapd

Le nom de domaine DNS est utilisé pour établir le nom distinctif de base (« base DN » ou « Distinguished Name ») de l'annuaire LDAP. Par exemple, si vous indiquez « toto.example.org » ici, le nom distinctif de base sera « dc=toto, dc=example, dc=org ».

Nom de domaine :

e-ecole.org

<Ok>

Définissez le nouveau 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>

Choisissez de ne pas supprimer la BDD

Outil de configuration des paquets

Configuration de slapd

Faut-il supprimer la base de données lors de la purge du paquet ?

<Oui> **<Non>**

Choisissez de déplacer l'ancienne base

Outil de configuration des paquets

Configuration de slapd

Des fichiers présents dans /var/lib/ldap vont probablement provoquer l'échec de la procédure de configuration. Si vous choisissez cette option, les scripts de configuration déplaceront les anciens fichiers des bases de données avant de créer une nouvelle base de données.

Faut-il déplacer l'ancienne base de données ?

<Oui>

<Non>

De retour dans le terminal :

```
service slapd restart
```

```
ldapsearch -x
```

Vous devriez avoir un retour similaire à cela :

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

```
o: e-ecole.org
dc: e-ecole

# admin, e-ecole.org
dn: cn=admin,dc=e-ecole,dc=org
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

Le LDAP est maintenant configuré !

Il est possible que le compte admin soit invisible sur le résultat, mais qu'il ai été créé malgré tout !

Revision #1

Created 2025-10-29 12:36:03 UTC

Updated 2025-10-29 12:36:05 UTC