

Mise en place d'un serveur OpenLDAP sous Debian

Guillaume Dualé

Table des matières

1	Introduction	1
2	Installation	1
3	Configuration	1
3.1	Ajout de l'admin	1
3.2	Scripts	2
3.2.1	Génération de mot de passe	2
3.2.2	Création de groupe	2
3.2.3	Création d'utilisateurs	2
4	Quelques commandes LDAP utiles	4
4.1	Afficher l'arbre LDAP complet	4
4.2	Faire un test d'authentification	4
4.3	Supprimer un utilisateur contenu dans l'OU People	4

1 Introduction

Je vais expliquer dans ce tutorial l'installation et la configuration d'un serveur OpenLDAP sous Debian Sarge.

Un serveur LDAP permet la centralisation des informations.

Par exemple il permet une authentification centralisé pour tous les utilisateurs.

2 Installation

Commande : `apt-get install slapd ldap-utils` (en root).

A la fin de l'installation du paquet slapd, Debian va vous poser quelques questions :

- Nom de domaine : home
- Nom de votre organisation : dc=home
- Mot de passe administrateur : Tapez votre mot de passe (bis)
- Faut-il autoriser le protocole LDAPv2 ? : Non

Note : On peut générer un mot de passe solide pour l'administrateur, avec l'outil `mkpasswd` contenu dans le package `whois`.

3 Configuration

La configuration de OpenLDAP se fait via le fichier : `/etc/ldap/slapd.conf`

3.1 Ajout de l'admin

La post installation du paquet slapd a créé un utilisateur `cn=admin,dc=home` dans l'annuaire ldap et lui a donné les droits en écriture sur tout l'annuaire.

Il faut maintenant, définir cet utilisateur comme administrateur de notre base, dans le fichier `/etc/ldap/slapd.conf`

Pour ce faire, il faut tout d'abord générer un mot de passe avec l'algorithme de hash SHA.

```
Commande: /usr/sbin/slappasswd -h {SSHA} -s "Le mot de passe saisi lors de l'installation du paquet slapd"
```

On édite ensuite le fichier : `/etc/ldap/slapd.conf` et on ajoute les lignes suivantes sous la ligne : `suffix dc=home`

```
rootdn      "cn=admin,dc=home"
rootpw      {SSHA}kOMCQLOU1CchA3voiCUPdGeZ3CLC8yBL
```

Il faut bien sûr remplacer le hash précédent par votre hash généré via l'outil `'slappasswd'`.

On redémarre le serveur : `/etc/init.d/slapd restart`

Votre serveur OpenLDAP est maintenant fonctionnel !

3.2 Scripts

3.2.1 Génération de mot de passe

Voici un script qui permet de générer un mot de passe solide pour l'annuaire LDAP suivit d'un hash SSHA de ce mot de passe à mettre dans le fichier /etc/ldap/slapd.conf

```
#!/bin/sh
echo "Votre mot de passe pour le LDAP:"
password='mkpasswd paSswOrd'
echo $password
echo "Votre Hash SSHA pour à mettre dans le fichier /etc/ldap/slapd.conf"
/usr/sbin/slappasswd -h {SSHA} -s $password
echo
echo "Script fini."
```

3.2.2 Création de groupe

Voici un script permettant de créer des groupes dans le LDAP :

```
#!/bin/sh
if [ "${1}" = "" ]; then
    echo "Usage: ${0} <groupname>"
    shift
else
    group=${1}
    temp='mktemp'
    cat << EOF >> $temp
    dn: ou=$group, dc=home
    description: Groupe de personnes
    objectClass: top
    objectClass: organizationalUnit
    ou: $group

    EOF
    ldapadd -x -W -D "cn=admin,dc=home" -f $temp
    echo "Script fini."
fi
```

3.2.3 Création d'utilisateurs

Voici un script permettant de créer des utilisateurs dans l'OU People, suivit d'un envoi par mail du nouveau mot de passe généré.

```
#!/bin/sh
if [ "${1}" = "-m" -o "${1}" = "--mail" ] ; then
    mail="true"
```

```

        shift
fi
if [ "${1}" = "-h" -o "${1}" = "--help" ] ; then
    echo "Usage: ${0} [-m]      <e@mail>"
    echo "Usage: ${0} [--mail] <e@mail>"
    shift
else
#Generation du mot de passe
password='mkpasswd paSswOrd'

user=${1}
temp='mktemp'
cat << EOF >> $temp
dn: uid=${user},ou=People,dc=home
userPassword: ${password}
objectClass: inetOrgPerson
uid: ${user}
cn: ${user}
sn: ${user}

EOF

#Ajout dans le LDAP
ldapadd -x -W -D "cn=admin,dc=home" -f $temp

if [ "$mail" = "true" ]; then
    echo $password | mail -s "Votre nouveau mot de passe LDAP" $user
else
    echo "Le mot de passe ne sera pas envoyé par mail!"
fi
fi
echo "Script fini."

```

4 Quelques commandes LDAP utiles

4.1 Affichier l'arbre LDAP complet

– `ldapsearch -x -b "dc=home"`

4.2 Faire un test d'authentification

– `ldapwhoami -x -W -D "uid=nom-utilisateur,ou=People,dc=home"`

4.3 Supprimer un utilisateur contenu dans l'OU People

– `ldapdelete -v -x -W -D 'cn=admin,dc=home' 'uid=nom-utilisateur,ou=People,dc=home'`