Howto personnel : Authentification sur une base LDAP

Pascal Pucci *Pascal@DeeNoo.com* 20 Avril 2001

Migrer des comptes unix standarts dans une base ldap (sous Debian).

1 Introduction

Ce document explique seulement comment migrer une solution classique de compte unix vers des comptes dans une base LDAP.

Attention, il n'explique pas et ne propose pas une architecture ldap spécifique et adapté pour cette occasion. (J'espère avoir le temps de faire un autre document pour aborder différentes architectures possibles, notament pour un ISP).

Je vous remercie d'avance de me communiquer les erreurs que j'aurais faites.

2 Installation LDAP

2.1 Installation de Openldap

Sous GNU/Debian :

```
apt-get install openldapd
```

Suivez les instructions et validez à chaque étape. Nous modifierons ensuite le paramettrage.

2.2 Configuration de Openldap

Modifiez le fichier /etc/openldap/slapd.conf comme suit :

```
# This is the main ldapd configuration file.
# Schema and objectClass definitions
include /etc/openldap/slapd.at.conf
include /etc/openldap/slapd.oc.conf
# Schema for supporting Netscape Roaming
include /etc/openldap/netscape_roaming.at.conf
include /etc/openldap/netscape_roaming.oc.conf
# Schema for supporting Debian Package Directory entries
# include /etc/openldap/debian.at.conf
# include /etc/openldap/debian.oc.conf
# Schema check allows for forcing entries to
# match schemas for their objectClasses's
schemacheck off
# Where clients are refered to if no
# match is found locally
```

```
# referral ldap://ldap.four11.com
# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile /var/run/slapd.pid
# Read slapd.conf(5) for possible values
loglevel 0
#######################################################################
# ldbm database definitions
#######################################################################
# The backend type, ldbm, is the default standard database ldbm
# The base of your directory
suffix "dc=exemple"
# Where the database file are physically stored
directory "/var/lib/openldap"
# Save the time that the entry gets modified
lastmod on
# By default, only read access is allowed
defaultaccess read
# For Netscape Roaming support, each user gets a roaming
# profile for which they have write
access to access to dn=".*,ou=Roaming,dc=exemple"
by dnattr=owner write
# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
access to attribute=userPassword
by dn="cn=root,ou=People,dc=exemple"
write by self
write by * none
# The admin dn has full write access
access to * by dn="cn=root,ou=People,dc=exemple" write
# End of ldapd configuration file
# L'utilisateur "root" pour la branche "People, exemple" a tout les droits.
rootdn "cn=root,ou=People,dc=exemple"
# Son mot de passe. (Il peut être en clair ou en crypté).
rootpw mon_password
```

2.3 Migration des utilisateurs vers LDAP

Je vous conseille d'utiliser les outils de migration de www.padl.com :

Outils de migration de comptes UNIX vers LDAP

Une fois l'archive décompressée :

```
tar xvfz MigrationTools.tgz
```

configurez l'outils :

```
cd MigrationTools-37/
```

éditez le fichier de configuration migrate_common.ph et remplacez

```
# Default base
$DEFAULT_BASE = "dc=padl,dc=com";
```

par :

```
# Default base
$DEFAULT_BASE = "dc=exemple";
```

Ensuite construisez en mode super-utilisateur (root) votre base à partir de vos comptes unix existant :

```
./migrate_passwd.pl /etc/passwd > /tmp/arbre_exemple.ldif
```

Comme vous pouvez le voir en éditant le fichier /tmp/arbre_exemple.ldif, les utilisateurs sont ont été ajoutés dans une branche People fille du noeud principale que nous avons définis à "dc=exemple" (pour l'exemple).

Il nous faut donc créer ces noeuds avant d'y ajouter nos utilisateurs. Pour ceci, ajoutons les lignes suivantes au début de notre fichier /tmp/arbre_exemple.ldif :

```
dn: dc=exemple
objectclass: dcobject
dc: maison
dn: ou=People, dc=exemple
objectclass: organization
ou: People
```

Notre fichier de base est prêt. Initialisons notre annuaire.

2.4 Création de la base LDAP

Tapez en ligne de commande la ligne suivante :

```
ldapadd -h localhost -p 389 -D "cn=root,dc=exemple" -w mon_password -f /tmp/arbre_exemple.ldif
```

Vérifiez ensuite que votre base LDAP a bien été remplie en faisant une recherche :

```
ldapsearch -L -h localhost -p 389 -b "dc=exemple" "(objectclass=*)"
```

ou tester l'utilisation de GQ :

```
apt-get install gq
gq &
```

Si vous n'êtes pas "Java-phobe", vous pourrez toujours tester un browser Java à l'adresse suivante : http://www.iit.edu/~gawojar/ldap/ (Attention, le logiciel n'est pas libre).

NB : Vous avez sans doute remarqué que le champ "userPassword" est crypé ({crypt}...). Le mot de passe peut rester en clair ou être crypté avec d'autres algorithmes d'encryptages : MD5, SHA, DES

3 Configuration PAM-LDAP

PAM (Pluggable Authentication Modules) permet un mode d'authentification modulaire facilement paramétrable. Il existe donc un module PAM pour LDAP, soit :

```
apt-get install libpam-ldap
```

Ensuite paramétrons ce module : /etc/pam_ldap.conf

```
host localhost
base ou=People,dc=exemple
ldap_version 2
pam_crypt local
```

4 Configuration PAM

4.1 Configuration

Vérifiez au préalable que vous possédez les bons outils :

```
apt-get install libpam-pwdb libpam-cracklib
```

Puis remplacez le contenu des modules d'authentification /etc/pam.d/*. Nous testerons ici avec rlogin, remplacez donc /etc/pam.d/rlogin par :

```
auth required pam_nologin.so
auth sufficient pam_ldap.so
auth required pam_pwdb.so shadow nodelay
account sufficient pam_ldap.so
account required pam_pwdb.so
password required pam_cracklib.so
password required pam_pwdb.so shadow nullok use_authtok
```

Si cette configuration vous parait un peu trop compliquée (sécurisée), vous pourrez utilisez la suivante :

```
auth required pam_ldap.so
account required pam_ldap.so
password required pam_ldap.so
session required pam_ldap.so
```

4.2 Configuration avec création automatique du répértoire personnel

On pourra grace au procédé PAM améliorer notre configuration par la création automatique des répertoires personnels au cas ou ils n'existeraient pas déjà.

Dans ce cas essayez d'ajouter à votre mode d'authentification /etc/pam.d/* par le contenu suivant :

```
session required pam_mkhomedir.so skel=/etc/skel/ umask=0022
session required pam_pwdb.so
```

4.3 Tests

Utilisez l'outils que vous avez configuré avec un utilisateur de la base LDAP :

```
rlogin -l ppucci localhost
```

5 Configuration du service de nomage (nsswitch librairies).

Exemple d'utilisation de ce service : Savoir nommer le propriétaire d'un fichier si son propriétaire est dans une base LDAP.

Donc, il nous faut installer cette librairie pour LDAP :

```
apt-get install libnss-ldap
```

Puis, il nous suffira de configurer le fichier /etc/nsswitch.conf et /etc/libnss-ldap.conf :

- /etc/nsswitch.conf :

```
passwd: files ldap
group: files ldap
shadow: files ldap
```

- /etc/libnss-ldap.conf :

```
host localhost
base ou=People,dc=exemple
```

6 Logitheque

Outils de migration de comptes UNIX vers LDAP

LDAP Browser

Un grosse liste d'outils LDAP

Kldap

Pam-Ldap-Module

Openldap

7 Bibliographie

Introduction to LDAP under Linux

Authenticating with LDAP using Openldap and PAM