TP Installation/Configuration d'un annuaire LDAP sur serveur GNU/Linux

Nom :		Prénom :		Date :		Numéro :	

Objectifs :

- Installer un annuaire LDAP sur un PC serveur GNU/Linux (Mandriva).
- Visiter les principaux fichiers de configuration utiles à LDAP.
- Utiliser l'annuaire LDAP depuis un poste client GNU/Linux, ou Windows.

☞ Une grande partie de la formation d'un administrateur système Unix vient de l'auto-formation grâce au manuel !

1 Installation du serveur LDAP et des utilitaires (Mandriva)

a - Installation

☞ Utiliser `urpmq` pour trouver les paquets *rpm* liés au service ldap (i.e. `ldap`)

☞ Installer le paquet serveur `ldap-servers`, le paquet client `openldap-clients` , les paquets `nss_ldap` et `pam_ldap` avec la commande `urpmi`

☞ Visualiser les fichiers des paquets installés

2 Configuration d'un serveur LDAP

On va configurer un serveur LDAP, pour une entité fictive dont le DNS serait `tpal.fr` . Le but est de modifier les champs `database`, `suffix`, `rootdn` et `rootpw`.

a - Configuration : fichier slapd.conf

Localiser et éditer le fichier `slapd.conf` situé dans `/etc/openldap`.

☞ Déduire du nom de domaine un `suffix` utilisable pour l'annuaire, conforme aux recommandations de l'IETF

☞ En choisissant `admin` comme nom d'administrateur de l'annuaire, déduire le DN de root (`rootdn`)

☞ On utilisera `bdb` (Berkeley DB) comme type de base de données

☞ Utiliser la commande
`slappasswd -h '{SSHA}' -s secret -v`
pour générer le mot de passe crypté cprrespondant à `secret` . Ce mot de passe crypté sera utilisé pour le champ `rootpw`.

Fichier /etc/openldap/slapd.conf:

```
include /usr/share/openldap/schema/core.schema
...
include /usr/share/openldap/schema/nis.schema
include /usr/share/openldap/schema/openldap.schema
include /usr/share/openldap/schema/autofs.schema
include /usr/share/openldap/schema/samba.schema
...
include /usr/share/openldap/schema/dnszone.schema
include /usr/share/openldap/schema/dhcp.schema

include /etc/openldap/schema/local.schema

include         /etc/openldap/slapd.access.conf

access to dn.subtree="dc=tpal,dc=fr"
        by group="cn=Replicator,ou=Group,dc=tpal,dc=fr"
        by users read
        by anonymous read

limits group="cn=Replicator,ou=Group,dc=tpal,dc=fr"
 size=unlimited
 time=unlimited

pidfile         /var/run/ldap/slapd.pid
argsfile        /var/run/ldap/slapd.args

modulepath      /usr/lib/openldap

TLSCertificateFile      /etc/ssl/openldap/ldap.pem
TLSCertificateKeyFile   /etc/ssl/openldap/ldap.pem
TLSCACertificateFile    /etc/ssl/openldap/ldap.pem

database        bdb
suffix          "dc=tpal,dc=fr"
rootdn          "cn=admin,dc=tpal,dc=fr"

rootpw  {SSHA}pY6bNv0FBHvRcvVWG3YmmHd4OOPxSSO1

directory       /var/lib/ldap

checkpoint 256 5

index   objectClass,uid,uidNumber,gidNumber,memberuid   eq
index   cn,mail,surname,givenname                       eq,subinitial
```

b - lancement du serveur

☞ Chercher dans le manuel l'option permettant de lancer l'exécutable *stand-alone LDAP* sous une identité donnée.	
☞ Vérifier l'identité sous laquelle est lancée l'exécutable *stand-alone LDAP* (piste : consulter le fichier de démarrage du service *ldap* dans `/etc/init.d`)	
☞ Démarrer le service *ldap* et vérifier les messages syslog	
☞ Extraire (`grep`) de la commande `ps` la ligne concernant le service *ldap*	
☞ Rechercher dans le fichier `/etc/services` le numéro officiel du port *ldap*	

3 Initialisation d'un annuaire

a - Création des objets préliminaires :

Pour pouvoir accéder aux objets de l'annuaire, il faut créer le suffixe de la base (ici, c'est le dn : `dc=tpal,dc=fr`). Éditer le fichier `init.ldif` comme suit :

```
dn:dc=tpal,dc=fr
objectClass:top
objectClass:dcObject
objectClass:organization
dc:tpal
o:tpal
```

☞ Ajouter les informations du fichier `init.ldif` avec la commande `ldapadd` :

```
ldapadd -x -W -D "cn=admin,dc=tpal,dc=fr" -f init.ldif
```

(on donne le mot de passe correspondant à celui déclaré par le champ `rootw` du fichier `ldap.conf`).

☞ Vérifier le fonctionnement de l'annuaire avec la commande `ldapwhoami` :

```
ldapwhoami -x -W -D "cn=admin,dc=tpal,dc=fr"
```

☞ On peut maintenant rajouter les information concernant l'utilisateur `admin`. Éditer le fichier `admin.ldif` comme suit :

```
dn: cn=admin,dc=tpal,dc=fr
objectClass:simpleSecurityObject
objectClass:organizationalRole
cn:admin
description:LDAP Administrator
userPassword:{SSHA}pY6bNv0FBHvRcvVWG3YmmHd40OPxSSO1
```

Remarque : le `userPassword` est identique à celui du fichier `ldap.conf`.

4 Migration des informations passwd/shadow/group dans un annuaire LDAP

Le but est d'utiliser l'annuaire LDAP à la place des fichiers `/etc/passwd`, `/etc/group` et `/etc/shadow` pour utiliser un mécanisme d'identification/authentification LDAP (dans ce cas, LDAP joue le même rôle que NIS). Pour tester, on va créer un utilisateur `testldap`. Les informations de connexion de cet utilisateur seront migrées sous LDAP, puis effacées des fichiers `/etc/passwd`, `/etc/group` et `/etc/shadow`. On pourra alors vérifier que le système LDAP permet bien la connexion de cet utilisteur.

☞ Créer un utilisateur `testldap` : `useradd testldap`. Lui affecter un mot de passe avec la commande : `passwd testldap`.

a - Récupération des outils de migration

☞ Rapatrier l'archive avec la commande :
`wget http://www.padl.com/download/MigrationTools.tgz`.

☞ Développer l'archive : `tar xvzf MigrationTools.tgz`

☞ Aller dans le répertoire `MigrationTools-47`, et éditer le fichier `migrate_common.ph` pour donner les bonnes valeurs aux variables `DEFAULT_MAIL_DOMAIN` et `DEFAULT_BASE`.

☞ Créer une version filtrée des fichiers `passwd` et `group` en ne retenant que les informations de `testldap`, et les mettre dans des fichiers `passwd` et `group` :

```
grep testldap /etc/group > group
grep testldap /etc/passwd > passwd
```

☞ Lancer les scripts `migrate_group.pl` et `migrate_passwd.pl` en prenant bien soin d'utiliser les versions raccourcies des fichiers `passwd` et `group` :

```
./migrate_group.pl group group.ldif
./migrate_passwd.pl passwd passwd.ldif
```

☞ Examiner les fichiers LDIF créés.

b - Création des objets préliminaires

Pour pouvoir enregistrer les utilsateurs, il faut créer les objets (de type `organizationalUnit`) `People` et `Group` . Éditer le fichier `init2.ldif` comme suit :

```
dn: ou=Group,dc=tpal,dc=fr
objectclass: organizationalUnit
ou: Group
description: Groupes
dn: ou=People,dc=tpal,dc=fr
objectclass: organizationalUnit
ou: People
description: People
```

☞ Ajouter les informations du fichier `init2.ldif` avec la commande `ldapadd` :

```
ldapadd -x -W -D "cn=admin,dc=tpal,dc=fr" -f init2.ldif
```

☞ Ajouter les informations des fichiers `group.ldif` et `passwd.ldif` avec la commande `ldapadd` :

```
ldapadd -x -W -D "cn=admin,dc=tpal,dc=fr" -f group.ldif
ldapadd -x -W -D "cn=admin,dc=tpal,dc=fr" -f passwd.ldif
```

☞ Vérifier le conetnu de l'annuaire avec la commande

```
ldapsearch -x -W -D "cn=admin,dc=tpal,dc=fr" -b "dc=tpal,dc=fr"
```

☞ Supprimer l'utilisateur `testldap` : `userdel testldap`.

c - Configuration du pc en client LDAP

La dernière opération consiste à configurer le PC en client LDAP, de façon qu'il puisse se servir de ce service pour permettre la connexion des utilisateurs.

Fichier `/etc/nsswitch.conf` : à modifier pour rajouter le service ldap

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

Fichier `/etc/ldap.conf` : description du serveur LDAP et de l'annuaire utilisés par le service PAM du client. Le minimum à renseigner est :

```
host 192.168.x.y
base dc=tpal,dc=fr
```

Si besoin, éditer le reste du fichier pour mentionner la branche `dc=tpal,dc=fr` dans les lignes non commentées qui le nécessitent.

Fichier `/etc/openldap/ldap.conf` : description du serveur LDAP et de l'annuaire utilisés par le client. Le minimum à renseigner est :

```
BASE    dc=tpal, dc=fr
HOST    127.0.0.1
URI     ldap://127.0.0.1/
```

On va configurer le service `ssh` pour qu'il utilise l'identification/authentification LDAP :

- éditer le fichier `/etc/ssh/sshd.conf`, et mettre le champ `UsePAM` à `yes`,
- copier le fichier `/usr/share/doc/pam_ldap-170/pam.d/ssh` à l'emplacement `/etc/pam.d/sshd`
- tester une connexion par `ssh` sous le compte `testldap`. : `ssh testldap@localhost` par exemple.