OFPPT مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle et de la Promotion du Travail

TP Open LDAP

1. Prérequis

Configurer le nom du domaine en utilisant le serveur DNS

2. Installation

```
yum -y install  openldap-clients    openldap-servers    openldap-devel migrationtools
```

Démarrez le service LDAP et activez-le pour le démarrage automatique du service au démarrage du système.

```
systemctl    start    slapd.service
systemctl    enable    slapd.service
```

Vérifiez le LDAP

```
netstat -antup | grep -i 389
```

3. Configuration

a. Configurer le mot de passe root LDAP

```
[root@server ~]# slappasswd
New password:
Re-enter new password:
{SSHA}d/thexcQUuSfe3rx3gRaEhHpNJ52N8D3
```

b. Configurer le serveur OpenLDAP

Les fichiers de configuration des serveurs OpenLDAP se trouvent dans /etc/openldap/slapd.d/. Pour commencer avec la configuration de LDAP, nous aurions besoin de mettre à jour les variables "olcSuffix" et "olcRootDN".

olcSuffix , il s'agit du nom de domaine pour lequel le serveur LDAP fournit les informations. En termes simples, il devrait être changé pour votre domaine.

olcRootDN , Entrée Distinguished Name (DN) racine pour l'utilisateur qui a l'accès illimité pour effectuer toutes les activités d'administration sur LDAP, comme un utilisateur root.

olcRootPW , Mot de passe pour le RootDN ci-dessus.

Editer le fichier /etc/openldap /ldap.conf et modifier la ligne suivante par votre domaine

```
BASE    dc=tri,dc=local
```

NB : Il faut enlever « # »

Editer le fichier slapd.d/cn\=config/olcDatabase\=\{1\}monitor.ldif et renseigner votre domaine

```
"cn=Manager,dc=tri,dc=local"
```

Editer le fichier slapd.d/cn\=config/olcDatabase\=\{2\}mdb.ldif, modfier le domaine puis ajouter le mot de passe crypté

```
olcSuffix: dc=tri,dc=local
olcRootDN: cn=Manager,dc=tri,dc=local
olcRootPW: {SSHA}ppNk4zYhzD9PUUohDERGxGJFRzaCzbuA
```

c. Configurer la base de données LDAP

Copiez le fichier de configuration de base de données exemple dans / var / lib / ldap et mettez à jour les autorisations de fichier.

```
#cp   /usr/share/openldap-servers/DB_CONFIG.example     /var/lib/ldap/DB_CONFIG
#chown    ldap:ldap      /var/lib/ldap/*
```

d. Mettre à jour le Schema

```
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif
```

```
[root@ntic cn=config]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.
ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=cosine,cn=schema,cn=config"

[root@ntic cn=config]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldi
f
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=nis,cn=schema,cn=config"

[root@ntic cn=config]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorg
person.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=inetorgperson,cn=schema,cn=config"

[root@ntic cn=config]#
```

e. Redémarrer le serveur

```
systemctl    start    slapd.service
```

4. Gestion de la base

La base est gérée en utilisant les fichiers ldif

a. Ajout de l'unité d'organisation

```
dn: dc=tri,dc=local
dc: tri
objectClass: top
objectClass: domain

dn: ou=stagiaire,dc=tri,dc=local
objectClass: organizationalUnit
ou: People
```

b.Ajout du groupe

```
dn: cn=201,ou=stagiaire,dc=tri,dc=local
objectClass: posixGroup
cn: 201
gidNumber :0
```

c.Ajout de l'utilisateur

Pour la création des utilisateurs nous allons utiliser le script « migrate_passwd.pl » qui permet de générer le fichier ldif automatiquement à partir des informations d'un utilisateur local

Création de l'utilisateur

```
# useradd    user1
```

Copier les informations de l'utilisateur dans un fichier nommé passwd.txt

```
#grep  user1    /etc/passwd   >  passwd.txt
```

Maintenant créer le fichier ldif en utilisant le script migrate_passwd.pl

```
/usr/share/migrationtools/migrate_passwd.pl     passwd.txt > user1.ldif
```

```
dn: uid=user1,ou=stagiaire,dc=tri,dc=local
uid: user1
cn: user1
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:
{crypt}$6$AVyD/mkA$lIt3htNs3iPesXvjPW2G5XaeWwjEA4331AXfZkpHLcQ1hDyr3PEb
```

```
qHk8mod4oSzImcl7lNaNI2.IifOzbsgMp.
shadowLastChange: 17593
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 1003
gidNumber: 1003
homeDirectory: /home/user1
```

5. Importation du fichier ldif

Ajout de l'unité d'organisation

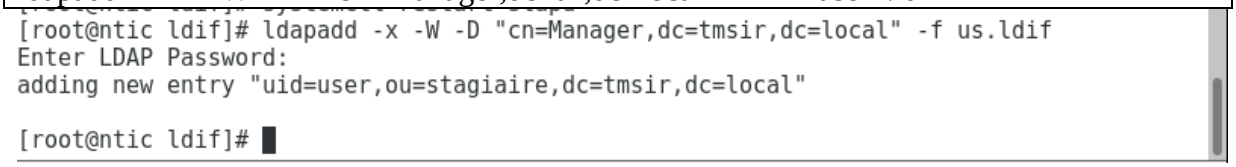
```
ldapadd -x -W -D "cn=Manager,dc=tri,dc=local" -f stagiaire.ldif
```

Ajout du groupe

```
ldapadd -x -W -D "cn=Manager,dc=tri,dc=local" -f 201.ldif
```

Ajout de l'utilisateur

```
ldapadd -x -W -D "cn=Manager,dc=tri,dc=local" -f user1.ldif
```



6. Vérification de l'importation

Pour vérifier l'ajout des fichiers « ldif » il faut utiliser la commande de recherche « ldapsearch »

```
#ldapsearch -x -b "dc=tri,dc=local "
```

```
[root@ntic ldif]# ldapsearch -x -b  "dc=tmsir,dc=local"
# extended LDIF
#
# LDAPv3
# base <dc=tmsir,dc=local> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# tmsir.local
dn: dc=tmsir,dc=local
dc: tmsir
objectClass: top
objectClass: domain

# stagiaire, tmsir.local
dn: ou=stagiaire,dc=tmsir,dc=local
objectClass: organizationalUnit
ou: stagiaire

# 201, stagiaire, tmsir.local
```

On peut utiliser l'option « -LLL »

```
#ldapsearch  -x   -b   "dc=tri,dc=local "  -LLL
```

```
[root@ntic ldif]# ldapsearch -x -b  "dc=tmsir,dc=local" -LLL
dn: dc=tmsir,dc=local
dc: tmsir
objectClass: top
objectClass: domain

dn: ou=stagiaire,dc=tmsir,dc=local
objectClass: organizationalUnit
ou: stagiaire

dn: cn=201,ou=stagiaire,dc=tmsir,dc=local
objectClass: posixGroup
cn: 201
gidNumber: 0

dn: uid=user,ou=stagiaire,dc=tmsir,dc=local
uid: user
cn: user
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:: e2NyeXB0fSEh
shadowLastChange: 17928
```

7. Suppression d'un élément

Pour supprimer l'utilisateur « user1 » on utilise la commande

```
#ldapdelete   -v –D   "cn=Manager,dc=tri,dc=ma"   -W   "cn=user1,
ou=stagiaire,dc=tri,dc=local"
```

```
[root@ntic ldif]# ldapdelete -v -D "cn=Manager,dc=tmsir,dc=local" -W "uid=user,ou=stagi
aire,dc=tmsir,dc=local"
ldap_initialize( <DEFAULT> )
Enter LDAP Password:
deleting entry "uid=user,ou=stagiaire,dc=tmsir,dc=local"
[root@ntic ldif]#
```

8. Option

-x : Authentification simple (sans utiliser SASL)
-b : base de recherche dans l'arborescence
-H : serveur LDAP
-D : identifiant connexion à la base
-W : demande le mot de passe
-LLL : Affichage au format LDIF (sans commentaires, sans version LDIF)

9. Modification d'un attribut

```
dn: uid=user,ou=stagiaire,dc=tmsir,dc=local
changetype: modify
add:description
description: stagiaire ofppt
```

```
ldapmodify -x -W -D "cn=Manager,dc=tmsir,dc=local" -f ajout.ldif
```

```
[root@ntic ldif]# ldapmodify -x -W -D "cn=Manager,dc=tmsir,dc=local" -f mod1.ldif
Enter LDAP Password:
modifying entry "uid=user,ou=stagiaire,dc=tmsir,dc=local"

[root@ntic ldif]#
```

```
dn: uid=USER123,ou=users,dc=example,dc=com
changetype: modify
replace: userpassword
userpassword: UnMotDePa55e
```

```
dn: uid=user,ou=stagiaire,dc=tmsir,dc=local
changetype: modify
replace:description
```

```
description: stagiaire NTIC de  CMFMNTIOE
```

ldapmodify -x -W -D "cn=Manager,dc=tmsir,dc=local" -f modif.ldif

```
[root@ntic ldif]# ldapmodify -x -W -D "cn=Manager,dc=tmsir,dc=local" -f mod1.ldif
Enter LDAP Password:
modifying entry "uid=user,ou=stagiaire,dc=tmsir,dc=local"
```

```
dn: uid=user,ou=stagiaire,dc=tmsir,dc=local
changetype: modify
delete:description
```

ldapmodify -x -W -D "cn=Manager,dc=tmsir,dc=local" -f delete.ldif

10. Configuration client Linux

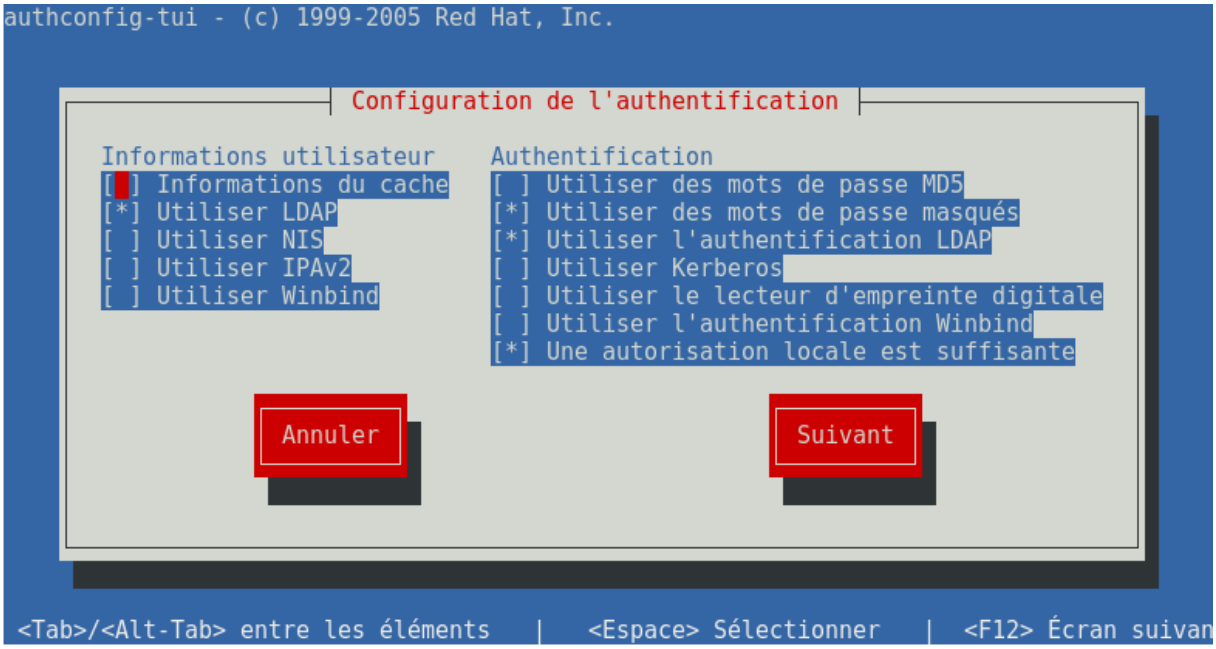
Vérifier que le serveur DNS est correctement renseigner

Installer le packet openldap client

```
# yum -y install openldap-clients nss-pam-ldapd
```

Configurer l'authentification LDAP, lancer la commande :

```
# authconfig-tui
```



Cocher « Utiliser LDAP », « Utiliser des mots de passe masqués » et « Utiliser l'authentification LDAP » et « Une autorisation locale est suffisante »

tmsir.local:/home /home auto defaults 0 0Pour vérifier la connectivité et la communication entre le serveur et le client taper la commande

```
# getent  passwd  NomUtilisateur
```

```
[root@localhost ~]# getent passwd ilham
ilham:*:1007:1008:ilham:/home/ilham:/bin/bash
[root@localhost ~]#
```

Pour accéder via l'utilisateur Ldap il faut partager le répertoire /home en utilisant le serveur NFS

Coté serveur Openldap

Vérifier l'existence du paquet nfs-utils si non installer le

Editer le fichier /etc/exports et ajouter la ligne suivante :

```
/home          *(rw)
```

Coté Client

Editer le fichier /etc/fstab et ajouter la ligne suivante

```
tri.local:/home    /home                auto    defaults        0 0
```

Lancer la commande

```
mount -a
```

Tester l'accèer

```
#su  - NomUtilisateurLdap
```

```
[root@localhost ~]# su - ilham
Dernière connexion : samedi 23 février 2019 à 20:32:35 WET sur pts/0
/usr/bin/id: cannot find name for group ID 1008
[ilham@localhost ~]$
```

https://linux-note.com/centos-7-ldap