Version : **2021.01**

Dernière mise-à-jour : 2021/02/05 16:01

SER704 - La Sauvegarde, la Restauration et la Réplication

Contenu du Module

- **SER704 - La Sauvegarde, la Restauration et la Réplication**
  - Contenu du Module
  - LAB #1 - Configurer les Machines Virtuelles ldapmaster et ldapslave pour la Replication
  - LAB #2 - Sauvegarde et Restauration
  - LAB #3 - Replication
    - 3.1 - Activation de l'Overlay Syncprov
    - 3.2 - Modification du ServerID
    - 3.2 - Création d'un Fichier de Mot de Passe de l'Administrateur
    - 3.3 - Création d'un Utilisateur pour la Réplication
    - 3.4 - Authorisation des Modifications de la Configuration d'OpenLDAP
      - ACLs
      - Configuration
      - Paramétrage
    - 3.5 - Vérification du Fonctionnement de la Réplication

LAB #1 - Configurer les Machines Virtuelles ldapmaster et ldapslave pour la Replication

Arretez la machine virtuelle CentOS_7 :

```
[root@centos7 ~]# exit
[trainee@centos7 ~]$ exit
```

```
desktop@serverXX:~$ VBoxManage controlvm CentOS_7 poweroff
```

Restaurez le snapshot **snapshot1** :

```
desktop@serverXX:~$ VBoxManage snapshot CentOS_7 restore snapshot1
```

Deux machines virtuelles ont été préparées et importées pour la suite de ce module. Ces deux machines doivent être mises dans le réseau réseau NAT **NatNetwork**.

Créez le réseau NAT **NatNetwork** :

```
desktop@serverXX:~$ VBoxManage natnetwork add --netname NatNetwork --network "10.0.2.0/24" --enable
desktop@serverXX:~$ VBoxManage natnetwork modify --netname NatNetwork --dhcp on
desktop@serverXX:~$ VBoxManage natnetwork start --netname NatNetwork
```

Créez les redirections de ports dans le réseau NAT **NatNetwork** de VirtualBox :

```
desktop@serverXX:~$ VBoxManage natnetwork modify --netname NatNetwork --port-forward-4
"ldapmaster:tcp:[]:3022:[10.0.2.15]:22"
desktop@serverXX:~$ VBoxManage natnetwork modify --netname NatNetwork --port-forward-4
"ldapslave:tcp:[]:4022:[10.0.2.16]:22"
```

Démarrez les deux machines virtuelles :

```
desktop@serverXX:~$ VBoxManage startvm ldapmaster --type headless
desktop@serverXX:~$ VBoxManage startvm ldapslave --type headless
```

Configurez les cartes réseaux des machines virtuelles **ldapmaster** et **ldapslave** en “NatNetwork”.

```
desktop@serverXX:~$ VBoxManage controlvm ldapmaster nic1 natnetwork NatNetwork
desktop@serverXX:~$ VBoxManage controlvm ldapslave nic1 natnetwork NatNetwork
```

En utilisant une première connexion SSH, tapez la commande suivante pour vous connecter à la machine ldapmaster :

```
desktop@serverXX:~$ ssh -l trainee localhost -p 3022
```

En utilisant une deuxième connexion SSH, tapez la commande suivante pour vous connecter à la machine ldapslave :

```
desktop@serverXX:~$ ssh -l trainee localhost -p 4022
```

Vérifiez votre configuration dans les deux machines **ldapmaster** et **ldapslave** :

```
[root@master ~]# ldapsearch -xLLL
dn: dc=i2tch,dc=com
objectClass: dcObject
objectClass: organization
dc: i2tch
o: i2tch.com
description: Exemple

dn: cn=Manager,dc=i2tch,dc=com
objectClass: organizationalRole
cn: Manager
description: Gestionnaire

dn: ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: France

dn: ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
```

```
ou: Recherche

dn: ou=Production,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Production

dn: ou=Suisse,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Suisse

dn: ou=Commercial,ou=Suisse,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: USA

dn: ou=Commercial,ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche

dn: cn=Responsable Personnel,ou=France,dc=i2tch,dc=com
cn: Responsable Personnel
```

```
aliasedObjectName: cn=Directeur,ou=France,dc=i2tch,dc=com
objectClass: top
objectClass: alias
objectClass: extensibleObject

dn: cn=directeur,ou=France,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: directeur
sn: Guillaud
telephoneNumber: 12345678
telephoneNumber: 87654321

dn: ou=Angleterre,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Angleterre

dn: ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Sales

dn: cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: Sales Director
sn: Smith

dn: cn=Sales Manager,cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: Sales Manager
sn: Brown
```

```
dn: cn=mail,ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: person
objectClass: top
cn: mail
mail: info@i2tch.com
sn: info

dn: cn=dupond,ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: top
cn: dupond
sn: dupond
mail: dupond@i2tch.com

dn: cn=dupois,ou=Production,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: top
cn: dupois
sn: dupois
```

```
[root@slave ~]# ldapsearch -xLLL
dn: dc=i2tch,dc=com
objectClass: dcObject
objectClass: organization
dc: i2tch
o: i2tch.com
description: Exemple

dn: cn=Manager,dc=i2tch,dc=com
objectClass: organizationalRole
cn: Manager
description: Gestionnaire
```

```
dn: ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: France

dn: ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche

dn: ou=Production,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Production

dn: ou=Suisse,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Suisse

dn: ou=Commercial,ou=Suisse,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: USA
```

```
dn: ou=Commercial,ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=USA,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Recherche

dn: cn=Responsable Personnel,ou=France,dc=i2tch,dc=com
cn: Responsable Personnel
aliasedObjectName: cn=Directeur,ou=France,dc=i2tch,dc=com
objectClass: top
objectClass: alias
objectClass: extensibleObject

dn: cn=directeur,ou=France,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: directeur
sn: Guillaud
telephoneNumber: 12345678
telephoneNumber: 87654321

dn: ou=Angleterre,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Angleterre

dn: ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Sales
```

```
dn: cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: Sales Director
sn: Smith

dn: cn=Sales Manager,cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: Sales Manager
sn: Brown

dn: cn=mail,ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: person
objectClass: top
cn: mail
mail: info@i2tch.com
sn: info

dn: cn=dupond,ou=Recherche,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: top
cn: dupond
sn: dupond
mail: dupond@i2tch.com

dn: cn=dupois,ou=Production,ou=France,dc=i2tch,dc=com
objectClass: inetOrgPerson
objectClass: top
cn: dupois
sn: dupois
```

Important - Dans ce cas les deux machines possèdent un DIT identique.

LAB #2 - Sauvegarde et Restauration

Dans le cas où les deux machines ne contiennent pas de DIT identique, il convient de dupliquer le DIT du master dans l'esclave.

Retournez à la machine virtuelle **ldapmaster**.

Sauvegardez les données de la configuration :

```
[root@master ~]# slapcat -b cn=config > save_config.ldif
```

Sauvegardez les données de la configuration :

```
[root@master ~]# slapcat -b dc=i2tch,dc=com > save_data.ldif
```

Transférez les deux fichiers à la machine virtuelle **ldapslave** :

```
[root@master ~]# scp save_*.ldif trainee@10.0.2.16:/tmp
The authenticity of host '10.0.2.16 (10.0.2.16)' can't be established.
ECDSA key fingerprint is SHA256:RgOsp/XI7JHNq+oIfHKw+jkHdtTnBIh+Dd7kVmHRxtU.
ECDSA key fingerprint is MD5:19:cd:05:58:af:2c:10:82:52:ba:e3:31:df:bd:72:54.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.16' (ECDSA) to the list of known hosts.
trainee@10.0.2.16's password:
save_config.ldif
100%   55KB  10.9MB/s   00:00
save_data.ldif
100% 8118     2.8MB/s   00:00
```

Retournez à la machine virtuelle **ldapslave** et arrêtez le service **slapd** :

```
[root@slave ~]# systemctl stop slapd
```

Supprimez la configuration existante :

```
[root@slave ~]# rm -rf /etc/openldap/slapd.d/*
```

Injectez la sauvegarde de la configuration en provenence de la machine virtuelle **master** :

```
[root@slave ~]# slapadd -F /etc/openldap/slapd.d -b cn=config -l /tmp/save_config.ldif
_#################### 100.00% eta   none elapsed            none fast!
Closing DB...
```

Modifiez le propriétaire et le groupe :

```
root@debian10:~# chown -R ldap:ldap /etc/openldap/slapd.d/
```

Supprimez maintenant les données existantes :

```
[root@slave ~]# rm -rf /var/lib/ldap/*
```

Injectez la sauvegarde des données en provenance de la machine virtuelle **master** :

```
[root@slave ~]# slapadd -b dc=i2tch,dc=com -l /tmp/save_data.ldif
5e1c9ee9 hdb_db_open: warning - no DB_CONFIG file found in directory /var/lib/ldap: (2).
Expect poor performance for suffix "dc=i2tch,dc=com".
_#################### 100.00% eta   none elapsed            none fast!
Closing DB...
```

Important - Notez l'avertissement concernant le fichier DB_CONFIG.

Remettez en place donc ce fichier :

```
[root@slave ~]# cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
```

Modifiez le propriétaire et le groupe :

```
root@debian10:~# chown -R ldap:ldap /var/lib/ldap/
```

Ré-indexez la base de données :

```
[root@slave ~]# slapindex
5e1ca06f The first database does not allow slapindex; using the first available one (2)
```

Démarrez le serveur OpenLDAP :

```
[root@slave ~]# systemctl start slapd
```

Vérifiez les restaurations :

```
[root@slave ~]# ldapsearch -xLLL | more
dn: dc=i2tch,dc=com
objectClass: dcObject
objectClass: organization
dc: i2tch
o: i2tch.com
description: Exemple

dn: cn=Manager,dc=i2tch,dc=com
objectClass: organizationalRole
cn: Manager
description: Gestionnaire

dn: ou=France,dc=i2tch,dc=com
```

```
objectClass: organizationalUnit
objectClass: top
ou: France

dn: ou=Commercial,ou=France,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: Commercial

dn: ou=Recherche,ou=France,dc=i2tch,dc=com
--More--
```

LAB #3 - Replication

Le mécanisme de réplication **syncrepl** est basé sur l'architecture de **serveurs homologues**. Le serveur dit *consommateur* lance le démon **syncrepl** dans un thread. Ce dernier contact le serveur *fournisseur* et charge une première version de l'annuaire. Ensuite il se maintient à jour. La fonctionalité syncrepl fournit la réplication :

- maître - esclave,
- maître - maître.

Le **consommateur** initie la réplication soit en prenant les mises à jour du fournisseur, processus appelé **refreshOnly**, soit en demandant au fournisseur de fournir les mises à jour d'une manière périodique, processus appelé **refreshAndPersist**.

Pour que syncrepl fonctionne, il faut que l'Overlay **syncprov** soit chargé dans les deux serveurs.

3.1 - Activation de l'Overlay Syncprov

Créez le fichier **syncrepl.ldif** suivant dans les machines virtuelles **ldapmaster** et **ldapslave** :

```
[root@master ~]# vi syncrepl.ldif
```

```
[root@master ~]# cat syncrepl.ldif
dn: cn=module,cn=config
cn: module
objectclass: olcModuleList
objectclass: top
olcmoduleload: syncprov.la
olcmodulepath: /usr/lib/ldap
```

```
[root@slave ~]# vi syncrepl.ldif
[root@slave ~]# cat syncrepl.ldif
dn: cn=module,cn=config
cn: module
objectclass: olcModuleList
objectclass: top
olcmoduleload: syncprov.la
olcmodulepath: /usr/lib/ldap
```

Injectez la configuration dans chaque machine :

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

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

Vérifiez la mise en place de la configuration :

```
[root@master ~]# ldapsearch -LLLY external -H ldapi:/// -b "cn=config" "objectClass=olcModuleList"
```

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
dn: cn=module{0},cn=config
objectClass: olcModuleList
objectClass: top
cn: module{0}
olcModulePath: /usr/lib64/openldap
olcModuleLoad: {0}syncprov.la
```

```
[root@slave ~]# ldapsearch -LLLY external -H ldapi:/// -b "cn=config" "objectClass=olcModuleList"
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
dn: cn=module{0},cn=config
objectClass: olcModuleList
objectClass: top
cn: module{0}
olcModulePath: /usr/lib64/openldap
olcModuleLoad: {0}syncprov.la
```

3.2 - Modification du ServerID

Chaque serveur homologue doit être identifié par une entrée **olcServerID** différente. Créez donc les fichiers **serverid.ldif** suivants dans **ldapmaster** et **ldapslave** respectivement :

```
[root@master ~]# vi serverid.ldif
[root@master ~]# cat serverid.ldif
dn: cn=config
changetype: modify
add: olcServerID
olcServerID: 1
```

```
[root@slave ~]# vi serverid.ldif
[root@slave ~]# cat serverid.ldif
dn: cn=config
changetype: modify
add: olcServerID
olcServerID: 2
```

Injectez la configuration dans chaque machine :

```
[root@master ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f serverid.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"
```

```
[root@slave ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f serverid.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"
```

Vérifiez la mise en place de la configuration :

```
[root@master ~]# ldapsearch -LLLY external -H ldapi:/// -b "cn=config" "objectClass=olcGlobal" olcServerID
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
dn: cn=config
olcServerID: 1
```

```
[root@slave ~]# ldapsearch -LLLY external -H ldapi:/// -b "cn=config" "objectClass=olcGlobal" olcServerID
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
```

```
SASL SSF: 0
dn: cn=config
olcServerID: 2
```

3.3 - Création d'un Fichier de Mot de Passe de l'Administrateur

Afin d'éviter de passer le mot de passe de l'administrateur d'OpenLDAP sur la ligne de commande, créez le fichier **/root/passwdldap** dans chaque machine virtuelle :

```
[root@master ~]# echo -n "fenestros" > /root/passwdldap
[root@master ~]# chmod 600 /root/passwdldap
```

```
[root@slave ~]# echo -n "fenestros" > /root/passwdldap
[root@slave ~]# chmod 600 /root/passwdldap
```

3.4 - Création d'un Utilisateur pour la Réplication

Créez le fichier **repuser.ldif** suivant dans les machines virtuelles **ldapmaster** et **ldapslave** :

```
[root@master ~]# vi repuser.ldif
[root@master ~]# cat repuser.ldif
dn: ou=system,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: system

dn: cn=replicant,ou=system,dc=i2tch,dc=com
userPassword: password
cn: replicant
objectclass: top
objectclass: person
```

```
sn: replicant
```

```
[root@slave ~]# vi repuser.ldif
[root@slave ~]# cat repuser.ldif
dn: ou=system,dc=i2tch,dc=com
objectClass: organizationalUnit
objectClass: top
ou: system

dn: cn=replicant,ou=system,dc=i2tch,dc=com
userPassword: password
cn: replicant
objectclass: top
objectclass: person
sn: replicant
```

Injectez la configuration dans chaque machine :

```
[root@master ~]# ldapadd -x -H ldap://localhost -D cn=Manager,dc=i2tch,dc=com -y /root/passwdldap -f repuser.ldif
adding new entry "ou=system,dc=i2tch,dc=com"

adding new entry "cn=replicant,ou=system,dc=i2tch,dc=com"
```

```
[root@slave ~]# ldapadd -x -H ldap://localhost -D cn=Manager,dc=i2tch,dc=com -y /root/passwdldap -f repuser.ldif
adding new entry "ou=system,dc=i2tch,dc=com"

adding new entry "cn=replicant,ou=system,dc=i2tch,dc=com"
```

Authorisation des Modifications de la Configuration d'OpenLDAP

Il est maintenant necéssaire d'authoriser des modifications de la configuration d'OpenLDAP par l'utilisateur **cn=replicant,ou=system,dc=i2tch,dc=com**.

ACLs

Créez le fichier **acls.ldif** dans les machines virtuelles **ldapmaster** et **ldapslave** :

```
[root@master ~]# vi acls.ldif
[root@master ~]# cat acls.ldif
dn: olcDatabase={0}config,cn=config
changeType: modify
add: olcAccess
olcAccess: to * by dn.exact=cn=replicant,ou=system,dc=i2tch,dc=com manage by * break
```

```
[root@slave ~]# vi acls.ldif
[root@slave ~]# cat acls.ldif
dn: olcDatabase={0}config,cn=config
changeType: modify
add: olcAccess
olcAccess: to * by dn.exact=cn=replicant,ou=system,dc=i2tch,dc=com manage by * break
```

Injectez la configuration dans chaque machine :

```
[root@master ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f acls.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={0}config,cn=config"
```

```
[root@slave ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f acls.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={0}config,cn=config"
```

Configuration

Créez le fichier **configuration.ldif** dans les machines virtuelles **ldapmaster** et **ldapslave** :

```
[root@master ~]# vi configuration.ldif
[root@master ~]# cat configuration.ldif
dn: olcOverlay=syncprov,olcDatabase={0}config,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
```

```
[root@master ~]# vi configuration.ldif
[root@master ~]# cat configuration.ldif
dn: olcOverlay=syncprov,olcDatabase={0}config,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
```

Injectez la configuration dans chaque machine :

```
[root@master ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f configuration.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "olcOverlay=syncprov,olcDatabase={0}config,cn=config"
```

```
[root@slave ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f configuration.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "olcOverlay=syncprov,olcDatabase={0}config,cn=config"
```

Paramétrage

Créez le fichier **settings.ldif** dans les machines virtuelles **ldapmaster** et **ldapslave** :

```
[root@master ~]# vi settings.ldif
[root@master ~]# cat settings.ldif
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcSyncRepl
olcSyncRepl: rid=01 provider=ldap://10.0.2.15
  binddn="cn=replicant,ou=system,dc=i2tch,dc=com" bindmethod=simple
  credentials=password searchbase="cn=config"
  type=refreshAndPersist retry="5 5 300 5" timeout=1
olcSyncRepl: rid=02 provider=ldap://10.0.2.16
  binddn="cn=replicant,ou=system,dc=i2tch,dc=com" bindmethod=simple
  credentials=password searchbase="cn=config"
  type=refreshAndPersist retry="5 5 300 5" timeout=1
-
add: olcMirrorMode
olcMirrorMode: TRUE
```

```
[root@slave ~]# vi settings.ldif
[root@slave ~]# cat settings.ldif
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcSyncRepl
olcSyncRepl: rid=01 provider=ldap://10.0.2.15
  binddn="cn=replicant,ou=system,dc=i2tch,dc=com" bindmethod=simple
  credentials=password searchbase="cn=config"
  type=refreshAndPersist retry="5 5 300 5" timeout=1
olcSyncRepl: rid=02 provider=ldap://10.0.2.16
  binddn="cn=replicant,ou=system,dc=i2tch,dc=com" bindmethod=simple
  credentials=password searchbase="cn=config"
```

```
  type=refreshAndPersist retry="5 5 300 5" timeout=1
-
add: olcMirrorMode
olcMirrorMode: TRUE
```

Injectez la configuration dans chaque machine :

```
[root@master ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f settings.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={0}config,cn=config"
```

```
[root@slave ~]# ldapmodify -Y EXTERNAL -H ldapi:/// -f settings.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={0}config,cn=config"
```

3.5 - Vérification du Fonctionnement de la Réplication

Vérifiez la configuration :

```
[root@master ~]# ldapsearch -QLLLY external -H ldapi:/// -b "cn=config" "olcDatabase={0}config" olcSyncRepl
dn: olcDatabase={0}config,cn=config
olcSyncrepl: {0}rid=01 provider=ldap://10.0.2.15 binddn="cn=replicant,ou=syste
 m,dc=i2tch,dc=com" bindmethod=simple credentials=password searchbase="cn=conf
 ig" type=refreshAndPersist retry="5 5 300 5" timeout=1
olcSyncrepl: {1}rid=02 provider=ldap://10.0.2.16 binddn="cn=replicant,ou=syste
 m,dc=i2tch,dc=com" bindmethod=simple credentials=password searchbase="cn=conf
 ig" type=refreshAndPersist retry="5 5 300 5" timeout=1
```

```
[root@slave ~]# ldapsearch -QLLLY external -H ldapi:/// -b "cn=config" "olcDatabase={0}config" olcSyncRepl
dn: olcDatabase={0}config,cn=config
olcSyncrepl: {0}rid=01 provider=ldap://10.0.2.15 binddn="cn=replicant,ou=syste
 m,dc=i2tch,dc=com" bindmethod=simple credentials=password searchbase="cn=conf
 ig" type=refreshAndPersist retry="5 5 300 5" timeout=1
olcSyncrepl: {1}rid=02 provider=ldap://10.0.2.16 binddn="cn=replicant,ou=syste
 m,dc=i2tch,dc=com" bindmethod=simple credentials=password searchbase="cn=conf
 ig" type=refreshAndPersist retry="5 5 300 5" timeout=1
```

Créez le fichier LDIF **director.ldif** et éditez-le ainsi :

```
[root@master ~]# vi director.ldif
[root@master ~]# cat director.ldif
version: 1
dn: cn=director,ou=Angleterre,dc=i2tch,dc=com
objectClass: person
objectClass: top
cn: director
sn: Smith
telephoneNumber: 11111111
telephoneNumber: 99999999
```

Injectez la configuration dans la machine **ldapmaster** :

```
[root@master ~]# ldapadd -x -H ldap://localhost -D cn=Manager,dc=i2tch,dc=com -y /root/passwdldap -f
director.ldif
adding new entry "cn=director,ou=Angleterre,dc=i2tch,dc=com"
```

Vérifiez que l'ajout de l'utilisateur s'est déroulé correctement dans la machine **ldapmaster** :

```
[root@master log]# ldapsearch -x -LLL -S ou -s children -u -b "ou=Angleterre,dc=i2tch,dc=com"
dn: cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
ufn: Sales Director, Sales, Angleterre, i2tch.com
```

```
objectClass: person
objectClass: top
cn: Sales Director
sn: Smith

dn: cn=Sales Manager,cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
ufn: Sales Manager, Sales Director, Sales, Angleterre, i2tch.com
objectClass: person
objectClass: top
cn: Sales Manager
sn: Brown

dn: cn=director,ou=Angleterre,dc=i2tch,dc=com
ufn: director, Angleterre, i2tch.com
objectClass: person
objectClass: top
cn: director
sn: Smith
telephoneNumber: 11111111
telephoneNumber: 99999999

dn: ou=Sales,ou=Angleterre,dc=i2tch,dc=com
ufn: Sales, Angleterre, i2tch.com
objectClass: organizationalUnit
objectClass: top
ou: Sales
```

Dernièrement, vérifiez que la réplication fonctionne :

```
[root@slave ~]# ldapsearch -x -LLL -S ou -s children -u -b "ou=Angleterre,dc=i2tch,dc=com"
dn: cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
ufn: Sales Director, Sales, Angleterre, i2tch.com
objectClass: person
objectClass: top
```

```
cn: Sales Director
sn: Smith

dn: cn=Sales Manager,cn=Sales Director,ou=Sales,ou=Angleterre,dc=i2tch,dc=com
ufn: Sales Manager, Sales Director, Sales, Angleterre, i2tch.com
objectClass: person
objectClass: top
cn: Sales Manager
sn: Brown

dn: cn=director,ou=Angleterre,dc=i2tch,dc=com
ufn: director, Angleterre, i2tch.com
objectClass: person
objectClass: top
cn: director
sn: Smith
telephoneNumber: 11111111
telephoneNumber: 99999999

dn: ou=Sales,ou=Angleterre,dc=i2tch,dc=com
ufn: Sales, Angleterre, i2tch.com
objectClass: organizationalUnit
objectClass: top
ou: Sales
```

<html>

</html>