OpenLDAP Replikation

Setup-Anleitung für Provider-Consumer-Replikation

---

1. Vorbereitung - IPv4-Adressen konfigurieren

Sicherstellen, dass beide VMs unterschiedliche IPv4-Adressen haben.

Aktuelle IP-Adresse prüfen

```
ip -4 addr
```

IPv4-Adresse ändern

Konfigurationsdatei bearbeiten:

```
vim /etc/network/interfaces
```

Netzwerk neu starten

```
sudo systemctl restart networking
ip -4 addr
```

---

2. OpenLDAP Installation (auf beiden VMs)

Arbeitsverzeichnis erstellen

```
cd; mkdir openldap; cd openldap
```

OpenLDAP herunterladen

```
wget --no-check-certificate \
https://mirror.eu.oneandone.net/software/openldap/openldap-release/openldap-
2.6.10.tgz
```

Archiv entpacken

```
gunzip -c openldap-2.6.10.tgz | tar xvfB -
cd openldap-2.6.10
```

Kompilierung

```
./configure
make depend
make
sudo make install
```

Datenverzeichnis erstellen

```
sudo mkdir -p /usr/local/var/openldap-data
sudo chmod 700 /usr/local/var/openldap-data
```

---

3. Basiskonfiguration

Konfigurationsdatei bearbeiten

Datei `/usr/local/etc/openldap/slapd.conf` anpassen:

```
suffix: dc=fets,dc=local
rootdn: cn=Manager,dc=fets,dc=local
```

Konfiguration testen

```
sudo /usr/local/sbin/slaptest -u -f /usr/local/etc/openldap/slapd.conf
```

Base LDIF erstellen

Datei `/usr/local/etc/openldap/base.ldif` erstellen:

```
dn: dc=fets,dc=local
objectClass: dcObject
objectClass: organization
o: fets company
dc: fets

dn: cn=Manager,dc=fets,dc=local
```

```
objectClass: organizationalRole
cn: Manager
```

---

4. Provider-Konfiguration (VM1)

4.1 SLAPD starten

```
sudo /usr/local/libexec/slapd \
  -f /usr/local/etc/openldap/slapd.conf \
  -h "ldap://0.0.0.0:389"
```

SLAPD-Start überprüfen

```
ldapsearch -x -b '' -s base '(objectclass=*)' namingContexts
```

4.2 Base-Daten einfügen

```
ldapadd -x -H ldap://127.0.0.1:389 \
  -D "cn=Manager,dc=fets,dc=local" -w secret \
  -f /usr/local/etc/openldap/base.ldif
```

LDAP-Funktionalität bestätigen

```
ldapsearch -x -H ldap://127.0.0.1:389 \
  -D "cn=Manager,dc=fets,dc=local" -w secret \
  -b "dc=fets,dc=local"
```

Erwartetes Ergebnis: Die Ausgabe sollte die konfigurierte Domain enthalten.

4.3 Replikations-Konfiguration

In `/usr/local/etc/openldap/slapd.conf` im MDB-Datenbankbereich folgende Änderungen vornehmen:

Am Anfang des Datenbankbereichs einfügen

```
serverID 1
```

Am Ende des Datenbankbereichs hinzufügen

```
index entryUUID eq
index entryCSN eq

access to *
  by dn.exact="cn=replicator,dc=fets,dc=local" read
  by  * read

# Pflicht Overlay für Replikation
overlay syncprov
syncprov-checkpoint 100 10
syncprov-sessionlog 100
```

Komplette MDB-Datenbank-Konfiguration

```
#######################################################################
# MDB database definitions
#######################################################################
serverID 1

database        mdb
maxsize         1073741824
suffix          "dc=fets,dc=local"
rootdn          "cn=Manager,dc=fets,dc=local"
rootpw          secret
directory       /usr/local/var/openldap-data
index   objectClass     eq
index entryUUID eq
index entryCSN eq

access to *
  by dn.exact="cn=replicator,dc=fets,dc=local" read
  by  * read

overlay syncprov
syncprov-checkpoint 100 10
syncprov-sessionlog 100

#######################################################################
```

4.4 Replicator-Benutzer erstellen

SLAPD beenden:

```
sudo pkill slapd
```

Datei `/usr/local/etc/openldap/replicator.ldif` erstellen:

```
dn: cn=replicator,dc=fets,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: replicator
userPassword: secret
description: replication user
```

SLAPD neu starten:

```
sudo /usr/local/libexec/slapd \
  -f /usr/local/etc/openldap/slapd.conf \
  -h "ldap://0.0.0.0:389"
```

Replicator-Benutzer hinzufügen:

```
ldapadd -x -H ldap://127.0.0.1:389 \
  -D "cn=Manager,dc=fets,dc=local" -W \
  -f /usr/local/etc/openldap/replicator.ldif
```

Provider bestätigen

```
ldapwhoami -x -H ldap://127.0.0.1:389 \
  -D "cn=replicator,dc=fets,dc=local" -W
```

Erwartete Ausgabe: `dn: cn=replicator,dc=fets,dc=local`

---

5. Consumer-Konfiguration (VM2)

5.1 SLAPD-Konfiguration anpassen

In `/usr/local/etc/openldap/slapd.conf` folgende Konfiguration verwenden:

Wichtig: `IP_Provider` durch die tatsächliche IP-Adresse des Providers ersetzen!

```
#######################################################################
# MDB database definitions
```

```
#######################################################################
serverID 2

database        mdb
maxsize         1073741824
suffix          "dc=fets,dc=local"
rootdn          "cn=Manager,dc=fets,dc=local"
rootpw          secret
directory       /usr/local/var/openldap-data
index   objectClass     eq
index entryUUID eq
index entryCSN eq

syncrepl rid=001
  provider=ldap://IP_Provider:389
  type=refreshAndPersist
  searchbase="dc=fets,dc=local"
  bindmethod=simple
  binddn="cn=replicator,dc=fets,dc=local"
  credentials="secret"
  retry="5 5 300 5"
  timeout=1

updateref ldap://IP_Provider:389

#######################################################################
```

5.2 Base LDIF erstellen

Datei `/usr/local/etc/openldap/base.ldif` auf VM2 erstellen:

```
dn: dc=fets,dc=local
objectClass: dcObject
objectClass: organization
o: fets company
dc: fets

dn: cn=Manager,dc=fets,dc=local
objectClass: organizationalRole
cn: Manager
```

5.3 SLAPD neu starten

```
sudo pkill -9 slapd

sudo /usr/local/libexec/slapd \
  -f /usr/local/etc/openldap/slapd.conf \
  -h "ldap://0.0.0.0:389"
```

SLAPD-Start überprüfen

```
ldapsearch -x -b '' -s base '(objectclass=*)' namingContexts
```

---

6. Replikation validieren

Folgenden Befehl auf **beiden VMs** ausführen:

```
ldapsearch -x -H ldap://127.0.0.1:389 \
  -D "cn=Manager,dc=fets,dc=local" \
  -w secret \
  -b "dc=fets,dc=local"
```

Erwartetes Ergebnis: Die Ausgabe sollte auf beiden VMs identisch sein. Dies bestätigt, dass die Replikation erfolgreich funktioniert.
