LDAP-Replikation

Ziel ist die Verteilung einer LDAP-Datenbank auf mehr als einem Server. Dies erhöht die Ausfallsicherheit und verteilt die Last. Dabei existiert ein `Main` - dies ist der LDAP-Server auf dem Schreib-Operationen erlaubt. Alle anderen LDAP-Server beziehen lediglich im Pull-Verfahren regelmäßig Änderungen von dem Main-Server.

Die Dokumentation bezieht sich auf OpenLDAP v2.4 oder später. Alle Änderungen verwenden das neue LDIF-basierte Konfigurationsformat von OpenLDAP.

In den Beispielen werden die folgenden Variablen verwendet - sie sind durch lokale Gegebenheiten zu ersetzen:

Variable	**Beschreibung**
EXAMPLE und ORG	Die LDAP-Basis des Servers - beispielsweise für „dc=meine-domain,dc=de“ wäre es `EXAMPLE=meine-domain` und `ORG=de`
SYNCAGENT_SECRET	Passwort des LDAP-Replikations-Accounts (beliebig)
LDAP_MASTER	Der Name oder die IP des LDAP-Main-Servers

Alle Änderungen lassen sich jeweils mit folgendem Kommando anwenden:

```
ldapmodify -Y EXTERNAL -H ldapi:///
```

Die untenstehenden ldif-Änderungsdaten werden dabei auf der Standardeingabe erwartet.

Konfiguration des Main-Servers

Folgendes ist zu tun: Synchronisations-Overlay für die Konfiguration und die Datenbank aktivieren und einen Account für die Datenabfrage anlegen:

1. sync-Account anlegen:

   ```
   echo "
   # einen Account für die Replikationsabfrage hinzufuegen
   dn: cn=syncagent,dc=lohro,dc=de
   cn: syncagent
   objectClass: top
   objectClass: person
   sn: syncagent" | ldapadd -D cn=admin,dc=lohro,dc=de -W
   ```

2. Konfigurationen anpassen:

   ```
   ldapmodify -Y EXTERNAL -H ldapi:///
   ```

3. in die Standardeingabe folgenden Text kopieren:

   ```
   # Sync-Modul aktivieren
   dn: cn=module{0},cn=config
   ```

```
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov.la

# fuege replikationsrelevante Attribute zum Index hinzu
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryUUID,entryCSN eq

# Zugriffsrechte für den sync-Account anlegen
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcAccess
olcAccess: to * by dn.base="cn=syncagent,dc=EXAMPLE,dc=ORG" read by *
+0 break

# sync-Provider für die LDAP-Datenbank aktivieren
dn: olcOverlay=syncprov,olcDatabase={1}hdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov

# sync-Provider für die LDAP-Konfiguration aktivieren
dn: olcOverlay=syncprov,olcDatabase={0}config,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
```

4. Passwort für den Sync-Account festlegen:

```
ldappasswd -D cn=admin,dc=EXAMPLE,dc=ORG -W -s "SYNCAGENT_SECRET"
"cn=syncagent,dc=EXAMPLE,dc=ORG"
```

Konfiguration des Clients

1. Konfigurationen anpassen:

```
ldapmodify -Y EXTERNAL -H ldapi:///
```

2. in die Standardeingabe folgenden Text kopieren:

```
# Sync-Modul aktivieren
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov.la
```

```
# fuege replikationsrelevante Attribute zum Index hinzu
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryUUID,entryCSN eq

# Datenbank-Replikation aktivieren
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcSyncrepl
olcSyncrepl: {0}rid=2 provider=ldap://LDAP_MASTER
  type=refreshOnly
  bindmethod=simple
  binddn="cn=syncagent,dc=EXAMPLE,dc=ORG"
  credentials=SYNCAGENT_SECRET
  interval="00:00:03:00"
  retry="30 10 300 +"
  timeout=1
  tls_reqcert=never
  schemachecking=off
  searchbase="dc=EXAMPLE,dc=ORG"

# Konfigurationsreplikation aktivieren
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcSyncrepl
olcSyncrepl: {0}rid=1 provider=ldap://LDAP_MASTER
  type=refreshOnly
  bindmethod=simple
  binddn="cn=syncagent,dc=EXAMPLES,dc=ORG"
  credentials=SYNCAGENT_SECRET
  interval="00:00:03:00"
  retry="30 10 300 +"
  timeout=1
  tls_reqcert=never
  schemachecking=off
  searchbase="cn=config"
```

Abschluss

Nun sollte der Client-Server sich sofort mit dem Server synchronisieren. Fehlermeldungen finden sich auf der Slave-Seite unter `/var/log/debug.log`-

---

Quellen

* OpenLDAP-Doku * passende LDIF-Konfigurationsschnipsel * mehr Erklärungen, weniger konkrete Handlungen

From:
https://howto.wikis.systemausfall.org/ - **Das HowTo-Wiki**

Permanent link:
https://howto.wikis.systemausfall.org/linux/ldap_replikation

Last update: **2022/11/20 17:09**