OpeLDAP Master/Slave Kurulum Adımları

Kamu kurumlarında OpenLDAP bileşeninin Master/Slave yapısında kurulum ihtiyacını karşılamak amacıyla hazırlanmıştır. Kurulum;

- Ortak Adımlar
- Master Sunucu Ayarları
- Slave Sunucu Ayarları
- Kurulum Testi

adımlarından oluşmaktadır.

> Kurulumlar **Pardus 17.3** üzerinde **OpenLDAO(slapd) 2.4.44+dfsg-5+deb9u2** versiyonu ile yapılmıştır

Ortak Adımlar

Aşağıdaki adımlar her iki ldap sunucusunda uygulanacak adımlardır;

Uçbirimde;

```
sudo apt install slapd ldap-utils -y
```

komutu ile ldap paketi ve ldap komutlarını getiren ldap-utils paketi yüklenir. Kurulum esnasında ldap **admin** kullanıcısı için parola(**Yönetici parolası-Parolayı doğrulayınız**) tanımlanır. Paket kurulumları tamamlandıktan sonra slapd paketi konfigüre edilir. Uçbirimde;

```
dpkg-reconfigure slapd
```

aşağıda örnek değerleri tanımlanan alanlar kurulum esnasında girilir.

Alan	Değer
OpenLDAP sunucu yapılandırması atlansın mı?	Hayır
DNS alan adı:	*liderahenk.org*
Örgüt adı:	*LiderAhenk*
Yönetici parolası:	*ssifre*
Parolayı doğrulayınız:	*ssifre*
Kullanılacak veritabanı arka ucu:	*MDB*
* slapd paketi tamamen kaldırıldığında veritabanının da kaldırılmasını ister misiniz?	Hayır
** Eski veritabanı taşınsın mı?	Evet

Yukarıdaki değerlerden * ve ** değerlerini farklı bir şekilde tanımlayabilirsiniz.

Master Sunucu Ayarları

Bu adımlar master olarak belirlenen ldap sunucusunda uygulanır.

- İlk olarak uçbirimde;

```
pico syncmod.ldif
```

komutu ile **syncmod.ldif** dosyası oluşturulur. İçine aşağıdaki veriler girilir.

```
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov.la
```

Daha sonra;

```
ldapadd -Y EXTERNAL -H ldapi:/// -f syncmod.ldif
```

komutu ile **syncmod.ldif** dosyası ldap,'a yüklenir. Yükleme sonrası uçbirim çıktısı aşağıdaki şekilde olmalıdır;

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=module{0},cn=config
```

- Uçbirimde;

```
pico index.ldif
```

komutu ile **index.ldif** dosyası oluşturulur. İçine aşağıdaki veriler girilir.

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryUUID,entryCSN eq
```

Daha sonra;

```
ldapadd -Y EXTERNAL -H ldapi:/// -f index.ldif
```

komutu ile **index.ldif** dosyası ldap,'a yüklenir. Yükleme sonrası uçbirim çıktısı aşağıdaki şekilde olmalıdır;

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={1}mdb,cn=config"
```

- Uçbirimde;

```
pico sync.ldif
```

komutu ile **sync.ldif** dosyası oluşturulur. İçine aşağıdaki veriler girilir.

```
dn: olcOverlay=syncprov,olcDatabase={1}mdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
```

Daha sonra;

```
ldapadd -Y EXTERNAL -H ldapi:/// -f sync.ldif
```

komutu ile **sync.ldif** dosyası ldap,'a yüklenir. Yükleme sonrası uçbirim çıktısı aşağıdaki şekilde olmalıdır;

```
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={1}mdb,cn=config"
```

Slave Sunucu Ayarları

Bu adımlar slave olarak belirlenen ldap sunucusunda uygulanır.

- İlk olarak uçbirimde;

```
pico syncmod.ldif
```

komutu ile **syncmod.ldif** dosyası oluşturulur. İçine aşağıdaki veriler girilir.

```
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: syncprov.la
```

Daha sonra;

```
ldapadd -Y EXTERNAL -H ldapi:/// -f syncmod.ldif
```

komutu ile **syncmod.ldif** dosyası ldap,'a yüklenir. Yükleme sonrası uçbirim çıktısı aşağıdaki şekilde olmalıdır;

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=module{0},cn=config
```

- Uçbirimde;

```
pico index.ldif
```

komutu ile **index.ldif** dosyası oluşturulur. İçine aşağıdaki veriler girilir.

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryUUID,entryCSN eq
```

Daha sonra;

```
ldapadd -Y EXTERNAL -H ldapi:/// -f index.ldif
```

komutu ile **index.ldif** dosyası ldap,'a yüklenir. Yükleme sonrası uçbirim çıktısı aşağıdaki şekilde olmalıdır;

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={1}mdb,cn=config"
```

- Uçbirimde;

```
pico sync.ldif
```

komutu ile **sync.ldif** dosyası oluşturulur. İçine aşağıdaki veriler girilir.

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcSyncRepl
olcSyncRepl: rid=001
  provider=ldap://ldap-master-ip
  bindmethod=simple
  binddn="cn=admin,dc=liderahenk,dc=org"
  credentials=ssifre
  searchbase="dc=liderahenk,dc=org"
  scope=sub
  schemachecking=on
  type=refreshAndPersist
  retry="30 5 300 3"
  interval=00:00:00:30
  starttls=yes
  tls_reqcert=allow
```

Oluşturulan sync.ldif dosyasındaki;

> *provider=ldap://ldap-master-ip*
>
> *binddn="cn=admin,dc=liderahenk,dc=org"*
>
> *credentials=ssifre*
>
> *searchbase="dc=liderahenk,dc=org"*

değerler yukarıda ortak ayarlarda girilen bilgiler ile doldurulmalıdır. Daha sonra;

```
ldapadd -Y EXTERNAL -H ldapi:/// -f sync.ldif
```

komutu çalıştırılmalı, **sync.ldif** dosyası ldap,'a yüklenmelidir. Sonuç aşağıdaki şekilde dönmelidir;

```
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={1}mdb,cn=config"
```

Kurulum Testi

Son olarak yapılan kurulumun testi iiçn örnek bir kullanıcıyı sisteme ekleyelim;

```
pico user.ldif
```

komutu ile user.ldif dosyası açılır ve;

```
dn: uid=test-user,dc=liderahenk,dc=org

objectClass: simpleSecurityObject

objectclass: account

uid: test-user

description: Test  User

userPassword: Test1234
```

satırları isteğe göre düzenlenir. Daha sonra;

```
ldapadd -x -W -D "cn=admin,dc=liderahenk,dc=org" -f user.ldif
```

"Enter LDAP Password" sorusuna yukarıda tanımlanan **admin** parolası girilir, çıkan sonuç;

```
adding new entry "uid=test-user,dc=liderahenk,dc=org  "
```

şeklinde olmalıdır.

```
ldapsearch -x uid=test-user -b dc=liderahenk,dc=org
```

komutu ile kullanıcının eklendiği kontrol edilebilir, çıkan sonuç aşağıdaki şekilde olmalıdır;

```
# extended LDIF
#
# LDAPv3
# base <dc=liderahenk,dc=org> with scope subtree
# filter: uid=test-user
# requesting: ALL
#

# test-user, liderahenk.org
dn: uid=test-user,dc=liderahenk,dc=org
objectClass: simpleSecurityObject
objectClass: account
uid: test-user
description: Test  User

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```