

OpenLDAP installeren op CentOS7

Deze installatie resulteert in een Ldapserver waaraan client servers identification kunnen vragen voor users.

Installeer de software

```
yum -y install openldap compat-openldap openldap-clients openldap-servers  
openldap-servers-sql openldap-devel
```

en start:

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

en check of hij luistert:

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

Base Database configuratie

Genereer een paasword hash voor de database administrator:

slappasswd

```
New password:  
Re-enter new password:  
{SSHA}z8Al/JfVLlDv+4R38UpjHdj k28dnDDqG
```

Sla het wachtwoord en de gegenereerde hash ergens op.

```
vi db.ldif
```

```
dn: olcDatabase={2}hdb,cn=config  
changetype: modify  
replace: olcSuffix  
olcSuffix: dc=voorbeeld,dc=.nl  
  
dn: olcDatabase={2}hdb,cn=config  
changetype: modify  
replace: olcRootDN  
olcRootDN: cn=ldapadm,dc=voorbeeld,dc=nl  
  
dn: olcDatabase={2}hdb,cn=config  
changetype: modify  
replace: olcRootPW: {SSHA}z8Al/JfVLlDv+4R38UpjHdj k28dnDDqG
```

en pas de ldif file toe op de ldap:

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f db.ldif
```

```
vi monitor.ldif
```

```
dn: olcDatabase={1}monitor,cn=config
changetype: modify
replace: olcAccess
olcAccess: {0}to * by
dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external, cn=auth" read by
dn.base="cn=ldapadm,dc=voorbeeld,dc=nl" read by * none
```

en pas de ldif file toe op de ldap:

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f monitor.ldif
```

Controleer de huidige configuratie:

```
slaptest -u
```

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

```
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
```

```
vi base.ldif
```

```
ldapadd -x -W -D "cn=ldapadm,dc=test-net,dc=isae" -f base.ldif
```

Users toevoegen

Je zou de gebruikers met een ldif kunnen aanmaken, maar de preciese format van de ldif luistert nogal nauw. Beter is een testuser via een migratie tooltje aan te maken en die vervolgens in een latere interface als template te kunnen gebruiken om nieuwe gebruikers toe te voegen.

op linux op de ldapserver:

```
useradd testuser
passwd testuser
```

```
yum -y install migrationtools
```

```
cd /usr/share/migrationtools/
vi migrate_common.ph
```

verander de base dn en de extended schema's

```
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = "test.isae";
```

```
# Default base
$DEFAULT_BASE = "dc=test-net,dc=isae";

# turn this on to support more general object classes
# such as person.
$EXTENDED_SCHEMA = 1;
```

Vervolgens filteren we alleen de testuser uit de lijst: (system users moeten niet in de ldap worden opgenomen)

```
grep ":10[0-9][0-9]" /etc/passwd > /root/passwd
```

en ook voor de groups:

```
grep ":10[0-9][0-9]" /etc/group > /root/group
```

Maak daar ldifs van met de migratie tool:

```
./migrate_passwd.pl /root/passwd /root/users.ldif
./migrate_group.pl /root/group /root/groups.ldif
```

En pas de ldifs toe op de LDAP database:

```
ldapadd -x -W -D "cn=ldapadm,dc=test-net,dc=isae" -f /root/groups.ldif
ldapadd -x -W -D "cn=ldapadm,dc=test-net,dc=isae" -f /root/users.ldif
```

Client servers koppelen

Vervolgens kun je met deze handleiding Servers aan de LDAP koppelen en de koppeling testen.

Bronnen

<https://www.itzgeek.com/how-tos/linux/centos-how-tos/step-step-openldap-server-configuration-centos-7-rhel-7.html>

https://www.server-world.info/en/note?os=CentOS_7&p=openldap&f=1

<http://www.learnitguide.net/2016/01/configure-openldap-server-on-rhel7.html>

From:
<https://wiki.auriel.nl/> -

Permanent link:
https://wiki.auriel.nl/doku.php?id=installatie_handleidingen:openldap_op_centos7&rev=1520849645

Last update: **2018/03/12 11:14**