

OpenLDAP Server

Benötigte Pakete

Debian:

```
slapd ldap-utils
```

SuSE: ¹⁾

```
openldap2
```

CentOS (ab 6):

```
openldap-servers openldap-clients
```

Initiale Konfiguration

Debian

Bei Debian wird das Paket mit folgenden Werten vorkonfiguriert ²⁾:

```
debconf-set-selections <<DEBCONF
```

```
# Name of your organization:  
slapd shared/organization string linuxhotel  
# Allow LDAPv2 protocol?  
slapd slapd/allow_ldap_v2 boolean false  
# DNS domain name:  
slapd slapd/domain string linuxhotel.de  
# Admin password:  
slapd slapd/password1 password villa  
# Confirm password:  
slapd slapd/password2 password villa
```

```
DEBCONF
```

CentOS (7)

```
shopt -s dotglob  
rm -rf /var/lib/ldap/*  
rm -rf /etc/openldap/slapd.d/*  
cp -a /usr/share/openldap-servers/slapd.ldif /usr/share/openldap-
```

```
servers/slapd.ldif.orig
vim /usr/share/openldap-servers/slapd.ldif
```

```
olcAccess: to dn.base="" by * read
olcAccess: to dn.base="cn=Subschema" by * read
olcAccess: to *
    by self write
    by users read
    by anonymous auth
#
# Server status monitoring
#

dn: olcDatabase=monitor,cn=config
objectClass: olcDatabaseConfig
olcDatabase: monitor
olcAccess: to *
    by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read
    by dn.base="cn=admin,dc=example,dc=net" read
    by * none

#
# Backend database definitions
#

dn: olcDatabase=hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: hdb
olcSuffix: dc=linuxhotel,dc=de
olcRootDN: cn=admin,dc=linuxhotel,dc=de
olcDbDirectory: /var/lib/ldap
olcDbIndex: objectClass eq,pres
olcDbIndex: ou,cn,mail,surname,givenname eq,pres,sub
```

```
/usr/libexec/openldap/convert-config.sh -f /usr/share/openldap-
servers/slapd.ldif
cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
systemctl start slapd
systemctl enable slapd
```

root-Zugriff auf LDAP-Server über Socket

~/ldaprc

```
URI      ldapi:///
BASE     cn=config
SASL_MECH EXTERNAL
```

```
ldapsearch -LLL '(olcSuffix=*)' olcSuffix
```

Mehr dazu unter [ldap-config](#)

erste LDAP Einträge

Unter Debian werden bereits bei der Installation die ersten Werte, wie z.B. der Administrator-Benutzer in das Verzeichnis eingefügt. Unter SuSE und Fedora kann man das mit dem Befehl `slapadd` tun, das Administrator-Passwort wird mit dem Befehl `slappasswd` erzeugt:

```
DOMAIN="dc=linuxhotel,dc=de"  
DC=${DOMAIN%%, *}  
PASSWORD=$(slappasswd -s villa)  
slapadd <<LDIF
```

```
dn: $DOMAIN  
objectClass: top  
objectClass: dcObject  
objectClass: organization  
o: linuxhotel  
dc: ${DC#dc=}  
  
dn: cn=admin,$DOMAIN  
objectClass: top  
objectClass: simpleSecurityObject  
objectClass: organizationalRole  
cn: admin  
description: LDAP administrator  
userPassword: $PASSWORD
```

```
LDIF
```

slapd starten

SuSE, Centos, Fedora:

```
service ldap restart  
chkconfig ldap on
```

Debian:

```
service slapd restart
```

Fehler beim Starten finden

(unter SuSE /usr/lib/openssl/slapd)

```
slapd -d -1
```

Tips & Tricks

LDAP Daten sichern und wieder herstellen

(hier für Debian. Bei CentOS heißen Nutzer und Gruppe ldap statt openssl)

```
service slapd stop
slapcat -b "dc=linuxhotel,dc=de" > sicherung.ldif
less sicherung.ldif
grep directory /etc/ldap/slapd.conf
# DB_CONFIG nicht löschen ...
rm /var/lib/ldap/*.bdb
rm /var/lib/ldap/__db.*
vi sicherung.ldif
# nur bei dynamischer config:
slapadd -f sicherung.ldif
# slapindex # wird seit openssl2.4 nicht mehr benötigt
chown -R openssl:openssl /var/lib/ldap/*
service slapd start
```

```
# nur bei dynamischer config:
# slapcat -b cn=config > config-backup.ldif
# wenn auch die config wieder hergestellt werden muss: Reihenfolge beachten!
# slapadd -f config-backup.ldif && slapadd -f sicherung.ldif
# anschließend "chown -R openssl:openssl /etc/ldap/slapd.d/", für
/var/lib/ldap wie oben weiter
```

1)

Bug in openSuSE 12.3 und 13.1 https://bugzilla.novell.com/show_bug.cgi?id=777418

2)

Die Werte kann man natürlich auch interaktiv beim apt-get install eingeben

From:

<https://wiki.lab.linuxhotel.de/> - **Linuxhotel Wiki**

Permanent link:

<https://wiki.lab.linuxhotel.de/doku.php/lpi2:ldap?rev=1529531768>

Last update: **2018/06/20 21:56**

