OpenLDAP Server

Minimalkonfiguration für nss

Der OpenLDAP Server `slapd` muß wie in ldap gezeigt vorkonfiguriert sein. Darüber hinaus sind folgende Einstellungen notwendig:

`/etc/ldap/slapd.conf` (Debian)

```
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema
```

`/etc/openldap/slapd.conf` (Fedora)

```
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/inetorgperson.schema
```

`/etc/openldap/slapd.conf` (SuSE)

```
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/rfc2307bis.schema
include         /etc/openldap/schema/yast.schema
```

OrganizationalUnits anlegen

OrganizationalUnits „people“ und „groups“ für Benutzer und Gruppen im LDAP-Baum anlegen: [1)]

```
DOMAIN="dc=linuxhotel,dc=de"
ldapadd -x -W <<LDIF
```

```
dn: ou=people,$DOMAIN
objectClass: top
objectClass: organizationalUnit
ou: people

dn: ou=groups,$DOMAIN
objectclass: top
objectclass: organizationalUnit
ou: groups
```

```
LDIF
```

Gruppe anlegen

```
DOMAIN="dc=linuxhotel,dc=de"
ldapadd -x -W <<LDIF
```

Debian, RedHat:

```
dn: cn=ldapusers,ou=groups,$DOMAIN
objectClass: top
objectClass: posixGroup
gidNumber: 10000
cn: ldapusers
```

SuSE:

```
dn: cn=ldapusers,ou=groups,$DOMAIN
objectClass: top
objectClass: groupOfNames
objectClass: posixGroup
memberUid: nutzer
member: uid=nutzer,ou=people,$DOMAIN
gidNumber: 10000
cn: ldapusers
```

```
LDIF
```

Benutzer anlegen

```
DOMAIN="dc=linuxhotel,dc=de"
USERNAME=nutzer
PASSWORD=$(slappasswd -h '{SSHA}' -s xxx)
```

```
cat > user.ldif <<LDIF
```

```
dn: uid=$USERNAME,ou=people,$DOMAIN
objectClass: top
objectClass: posixAccount
objectClass: account
cn: mein nutzer
uid: $USERNAME
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/$USERNAME
userPassword: $PASSWORD
loginShell: /bin/bash
```

```
LDIF
```

```
ldapadd -x -W -f user.ldif
```

nss-ldap Client

Benötigte Pakete

Debian: [2)]

```
libnss-ldap nscd
```

SuSE:

```
nss_ldap
```

RedHat:

```
nss_ldap
```

Minimalkonfiguration

Einstellungen über debconf bei Debian:

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

```
# database requires login
libnss-ldap libnss-ldap/dblogin boolean false
# distinguished name of the search base
libnss-ldap shared/ldapns/base-dn string dc=linuxhotel,dc=de
# LDAP version to use
libnss-ldap shared/ldapns/ldap_version select 3
# LDAP server host address
libnss-ldap shared/ldapns/ldap-server string localhost
# make configuration readable/writeable by owner only
libnss-ldap libnss-ldap/confperm boolean false
```

```
DEBCONF
```

`/etc/libnss-ldap.conf` (Debian):

`/etc/ldap.conf` (SuSE und Fedora):

```
host  localhost
base  dc=linuxhotel,dc=de
ldap_version 3
```

```
#ssl start_tls
```

`/etc/nsswitch.conf` :

```
passwd:         files ldap
group:          files ldap
shadow:         files ldap
```

oder

```
passwd:         compat
group:          compat
shadow:         compat
passwd_compat:  ldap
group_compat:   ldap
shadow_compat:  ldap
```

```
echo '+::::LDAP User::' >> /etc/passwd
echo '+:::' >> /etc/group
echo '+:::::::::' >> /etc/shadow
```

Testen

Achtung: evtl. sollte man zum Testen den `nscd` anhalten:

```
/etc/init.d/nscd stop
```

[3)]

Benutzeraccounts abfragen:

```
getent passwd
```

Gruppen abfragen:

```
getent group
```

Als root zum neuen Benutzer wechseln

```
su - iw
```

Dokumentation & Links

Passwort ändern

```
ldappasswd -h ldapserver -D uid=LOGINNAME,ou=People,dc=linuxhotel,dc=de -W -
S
```

Migration von Benutzerdaten und mehr

- http://www.padl.com/OSS/MigrationTools.html

Programme zur Benutzerverwaltung mit LDAP

- Directory Administrator
- phpLDAPadmin
- cpu
- http://lam.sourceforge.net
- gosa
- luma

TODO:

- Benutzer ohne Passwörter

Benutzerverwaltung mit SSSD unter RHEL6

```
authconfig  --disableldaptls --ldapserver=ldap1.example.com --
ldapbasedn="dc=linuxhotel,dc=de" --disablerfc2307bis --enablemkhomedir --
enableforcelegacy --enablesssd --enablesssdauth --updateall
```

Webmin - Modul LDAP Useradmin

SuSE:

```
http://www.webmin.com
```

Einstellungen `/etc/webmin/ldap-useradmin/config`: (SuSE)

```
auth_ldap=/etc/ldap.conf
login=cn=admin,dc=linuxhotel,dc=de
pass=villa
user_base=ou=people,dc=linuxhotel,dc=de
group_base=ou=groups,dc=linuxhotel,dc=de
base_uid=1000
base_gid=1000
```

```
other_class=account
```

1)

Die Kursschreibweise `ldapadd -x -W` ohne Angabe des Admin-Kontos funktioniert nur, wenn vorher eine Konfigurationsdatei `.ldaprc` oder `ldap.conf` angelegt wurde

2)

alternativ und vielleicht sogar besser: `sssd` oder `libnss-ldapd`

3)

Was in dem Fall meiner Erfahrung nach nicht funktioniert: dem `nscd` sagen, das es was neues gibt:

```
touch /etc/passwd
touch /etc/group
```

oder

```
nscd -i
```