OpenLDAP als Login-Server

Minimalkonfiguration für nss/pam/sssd

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

Entscheidung: rfc2307 oder rfc2307bis-01 ?

- rfc2307bis-01 (expired: 20.08.2005)LDIF
- rfc2307bis-02 (expired: 10.02.2010)

- openSuSE: default ist rfc2307bis
- debian: default ist rfc2307, alternativ rfc2307bis.schema z.B. aus dem Paket `fusiondirectory`
- ceontos: default ist rfc2307

→ Schema-Änderung nötig?

Variante slapd.conf

Debian:

/etc/ldap/slapd.conf

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

CentOS:

/etc/openldap/slapd.conf

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

openSuSE:

/etc/openldap/slapd.conf

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

Variante slapd.d/

```
ldapsearch -b cn=schema,cn=config -LLL dn
```

```
…
dn: cn={0}core,cn=schema,cn=config
dn: cn={1}cosine,cn=schema,cn=config
dn: cn={2}nis,cn=schema,cn=config
dn: cn={3}inetorgperson,cn=schema,cn=config
…
```

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
```

rfc2307 / Debian, RedHat:

```
dn: cn=ldapusers,ou=groups,$DOMAIN
```

```
objectClass: top
objectClass: posixGroup
gidNumber: 10000
cn: ldapusers
```

rfc2307bis / 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
UIDNUMBER=10023
```

```
tee user.ldif <<LDIF
```

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

```
LDIF
```

```
ldapadd -x -W -f user.ldif
ldappasswd -x -W -S "uid=$USERNAME,ou=people,$DOMAIN"
```

[1)]

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