Központosított felhasználómenedzsment

- Samba 4
- NIS
- LDAP

LDAP

- Lightweight Directory Access Protocol
- Kliens-szerver protokol címtár szolgáltatás eléréséhez
- **slapd** – a szolgáltatást nyújtó démon
- slurpd - szerverek közötti replikáció kiszolgálója
- Kliens-szerver modellen alapul
- Egy vagy több LDAP szerveren tárolt adatból épül fel az LDAP fa
- Az LDAP kliens egy LDAP szerverhez csatlakozik, és felteszi a kérdéseit
- A szerver a válasszal reagál, vagy egy mutatóval, hol talál több információt a kliens

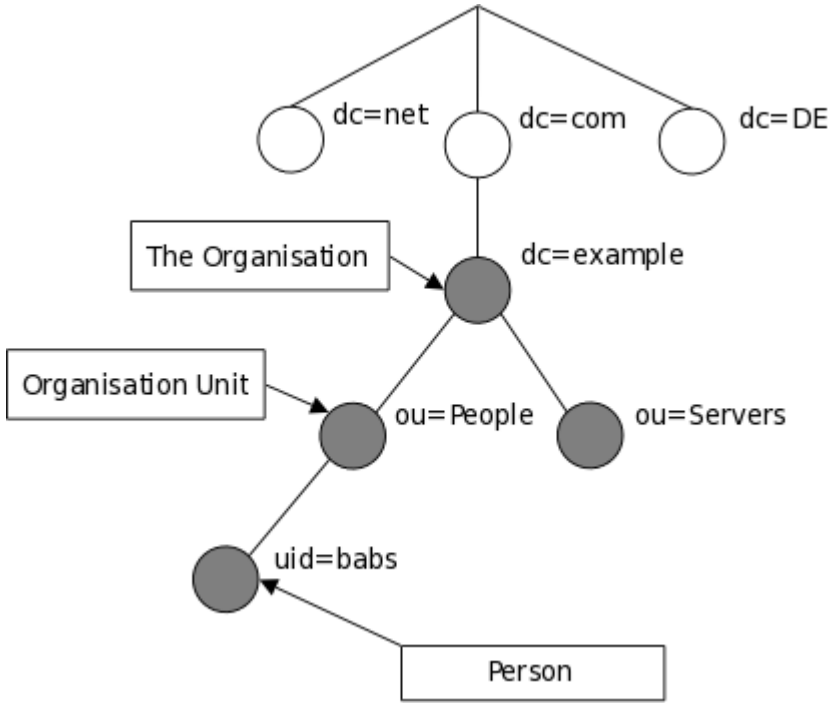
Adatbázisok

- Három különböző, szabadon választható háttér adatbázis használható:
  - **LDBM**, a nagy teljesítményű merevlemez alapú adatbázis
  - SHELL, az adatbázis interfész tetszőleges UNIX parancs vagy shell-script eléréséhez
  - PASSWORD, az egyszerű jelszó adatbázis

Az LDBM adatbázis

- 4 bájtos egyedi azonosítók minden adathoz
- Fő indexe az id2entry, ami a bejegyzések egyedi azonosítóit (entry's unique indentifier - EID) összerendeli saját szöveges ábrázolásával
- Importálás és exportálás LDIF formátumban (LDAP Data Interchange Format)
- A bejegyzéseket objektum orientált hiearchikus formában tárolja

Internet tartomány név alapú fastruktúra



- DIT: directory information tree
- Hivatkozás a bejegyzésre:RFC4514,
- DN: distinguished name: uid=babs,ou=People,dc=example,dc=com
- RDN: Relative Distinguished Name uid=babs

DC – Domain Component
CN – Common Name
OU – Organizational Unit

LDIF

```
dn: o=Nns, c=Hu
o: Nns
objectclass: organization

dn: cn=Halász Gábor, o=Nns, c=Hu
cn: Halász Gábor
sn: Halász
gn: Gábor
mail: halasz.g@nns.hu
objectclass: person
```

Felépítés

- dn - distinguished name (megkülönböztő név) - a bejegyzés nevéből áll, megtoldva a név elérési útjával vissza a címtár hiearchia csúcsáig
- alapvető objektum osztályok:
  - **Group** (csoport), független objektumok rendezetlen listája vagy objektumok csoportja
  - **Location** (elhelyezkedés), az országok nevei és leírásuk
  - **Organization** (szervezet)
  - **People** (személy)

Bejegyzések

- Egy bejegyzés (attribútum) több objektumosztályhoz is tartozhat
- cn: Halász Gábor (commonName)
- givenname: Gábor
- surname: Halász
- mail: halasz.g@nns.hu
- A person objektumosztályban
  - cn és sn attribútumok **szükségesek**
  - telephoneNumber, seeAlso és userpassword jellemzők **engedélyezettek**, de nem szükségesek

Attribútum szintaxis

- Minden attribútumnak meghatározott szintaxis definíciója van
- bin - binary (bináris)
- ces - case exact string (betűnagyságnak meg kell egyeznie az összehasonlítás során)
- cis - case ignore string (betűnagyságnak nem kell egyeznie az összehasonlítás során)
- tel - telephone number string (olyan, mint a cis, de a <-> kihagyásával)

Az LDAP szerver konfigurálása

- hely: /usr/local/etc/openldap vagy /etc/openldap
- állomány: slapd.conf
- (slapd.oc.conf és slapd.at.conf)

slapd.conf

```
# megjegyzés - ezek az egész adatbázisra érv.
<globális konfigurációs lehetőségek>
# első adatbázis
database <backend 1 type>     <backend 1 beáll.>
# második adatbázis
database <backend 2 type>     <backend 2 beáll.>
# további adatbázis definíciók
```

LDAP szerver indítása

- önállóan (LDBM esetén ez ajánlott)
  $(ETCDIR)/slapd [<opciók>]*

- inetd-vel indítva

Accessing LDAP

- Add, modify, and delete entries with `ldapadd`, `ldapmodify`, and `ldapdelete`
- Search the LDAP database with `ldapsearch`
  - Bind as some DN or anonymously

```
ldapsearch -D "cn=Directory Manager" -h ldaphost -b
  "dc=cims,dc=nyu,dc=edu" "uidNumber=9876" gecos
```

- Access to information is controlled by an access control list, e.g. password hashes are not available through anonymous bind