

Amit mindig is tudni akartál az LDAP-ról, de sosem merted megkérdezni

Szalai Ferenc
szferi@gluon.hu

Bevezető

- Mi szösz az az LDAP?
- OpenLDAP szerver
 - adatbázis felépítése
 - szerver beállítása
- Mire jó az LDAP
 - központosított felhasználó kezelés
- Ízelítő egyéb felhasználásból

Mi a szösz az az LDAP?

- LDAP: **L**ightweight **D**irectory **A**ccess **P**rotocol
- Mi az szösz az a Directory?: Információ tárolása hierarchikus szerkezetben
 - Példák: állományrendszer, DNS
 - valójában: speciális szerkezetű adatbázis
 - fő szempontok: gyors keresés, objektum orientált szemlélet, egyszerű adatfrissítés tranzakciók nélkül
 - speciális protokoll rendszer: DAP

DAP alapok

- DAP: Directory Access Protocol
 - Kliens, szerver modell olyan megkötéssel, hogy egy kliens csak egy szerverrel beszélget a többi a szerverek oldják meg
 - szerver: információt tárolja
 - kliens: lekérdezéseket végez a szerveren
 - szerver is tud kapcsolódni a klienshez
 - bármilyen formátumú adat bármilyen hierarhikus formátumban történő kezelése, alapvetően elosztott tervezési modell
- Bajok: bonyolult, egyszerűsítés: LDAP

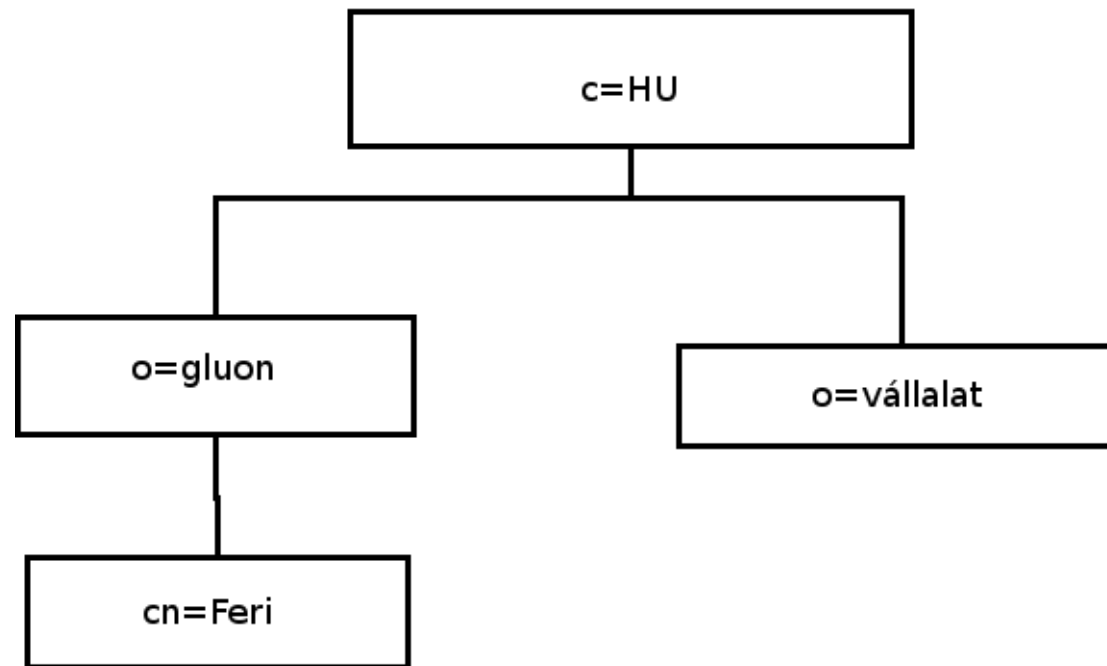
LDAP

- Információs modell: ASCII alapú
- TCP/IP felett működik
- egyszerű kliens-szerver modell
- flexibilis azonosítási mechanizmus
- elosztott műveletek
- protokoll és információs modell bővíthető speciális feladatokra
- de facto standard C API

LDAP Információs modell

- X.500 alapok
- Adatot elemi bejegyzések sora alkotja
- A bejegyzéseket fába rendezzük:
Directory Information Tree (DIT)
- Fa minden csomópontjának van neve
(Relative Distinguished Name): cn=Feri
- Fa minden csomópontjának a helye az
RDN-ek sorával adható meg (DN):
 - DN: cn=Feri,o=gluon,c=hu

DIT



DN:cn=Feri,o=gluon,c=hu

Adat a DIT-ben

- Adatbázis bejegyzés: Objektum
- Objektum: attribútumok halmaza
- Attribútumok: név, érték párok
- Attribútum: azonosító, típus, összehasonlítási szabály (séma)
- Lehetséges attribútumok osztályokba (ObjectClass) szervezendők (séma)
- Egyszerű öröklődés
- Külön séma leíró nyelv

Példa

- Person objectclass:
 - attribútumok: cn, surname, postoffice, etc.
- CN attribútum: Common Name (általános név), string típusú,
- OrganizationalPerson objectclass: a Person-ból öröklődik
 - attribútumok: ua. mint People + pl.: RoomNumber

ObjectClass típusok

- Öröklődés szabályozása
- ABSTRACT: csak az öröklődési hierarchia felépítésére használjuk
- STRUCTURAL: általános leírása a dolgoknak, egy osztály csak egy ilyen objectclass-ot valósíthat meg (öröklődési fát is figyelembe véve)
- AUXILIARY: kiegészítő attribútumok

LDIF – LDAP Data Interchange Format

- RFC 2849

LDIF – LDAP Data Interchange Format

- RFC 2849

Értékek

```
dn: cn=Feri,o=Gluon,c=hu
ObjectClass: top
ObjectClass: person
ObjectClass: posixAccount
cn: Feri
mail: szferi@niif.hu
mail: szferi@gluon.hu
telephonNumber: 12345678
userPassword:: e2NyeXB0fUNwLkyUi9G33UUU=
```

Attribútumok

LDAP szerverek

- Microsoft AD, Netscape DS, Sun JDS, IBM stb. Számos ezek közül ingyenes
- Nyílt forrású LDAP szerverek:
 - OpenLDAP
 - Fedora DS
- OpenLDAP: egyszerű, bővíthető a legfontosabb tulajdonságokkal rendelkezik, kis- és közepes szervezetek számára

OpenLDAP architektúra



OpenLDAP telepítés és konfiguráció

- `apt-get install slapd`
- Fő konfigurációs állomány
`/etc/ldap/slapd.conf`
- Sémák: `/etc/ldap/schema/`
- Adatbázis backendek:
 - `ldbm, bdb, shell, ldap, sql`

slapd.conf

```
# This is the main slapd configuration file.
include          /etc/ldap/schema/core.schema
schemacheck      on
modulepath       /usr/lib/ldap
moduleload       back_bdb
database         bdb
suffix           "o=gluon,c=hu"
directory        "/var/lib/ldap"
index            objectClass eq
access to attrs=userPassword
                by dn="cn=admin,o=gluon,c=hu" write
                by anonymous auth
                by self write
                by * none
                by * read
```

Idap-utils

- Parancssori Idap kliensek:
 - Idapsearch: kereses lekérdezés
 - Idapadd: adatbetöltés
 - Idapmodify: adatmódosítás

```
ldapsearch -x -LLL -w
```

```
-b ou=People,o=gluon,c=hu
```

```
-D uid=admin,o=gluon,c=hu
```

```
(uid=bela*) cn
```

```
(&(uid=*)(|(AuthorizedService=ssh)(role=admin)))
```

Mire jó az LDAP?

- Röviden: sokmindenre
- Hosszabban:
 - Sok felhasználó: sok gép
 - Egységes adminisztráció egyedi jelszó (passwd) állományok helyett
 - Ún. felhasználói profil kezelése
 - virtuális felhasználók (nincs home könyvtár, írási jog): levelezés, web hozzáférés

Linux felhasználói azonosítás mechanizmusa

- NSS (Name Service Switch): névfeloldás
 - uid, gid, DNS, /etc/services, /etc/protocols stb.
 - glibc része get*byname jellegű függvények
 - username -> uid (ha sikerül létezik)
- PAM: Pluggable Authentication Module
 - /etc/pam.d, /etc/pam.conf
 - azonosítás (pl.: jelszóellenőrzés) elvégzése
 - felhasználói környezet kialakítása belépés

után

PAM

- alkalmazásokat (login, ssh stb.) fel kell készíteni a használatára
- modulok: azonosítási adatbázisok kezelése pl.: unix, ldap, sql
- minden alkalmazás azonosítási mechanizmusa külön konfigurálható
- több modult is lehet egyszerre használni (pl.: először megpróbálom az LDAP-ot, ha nem megy, akkor a passwd állományt)

LDAP: NSS, PAM

- apt-get install libnss-ldap, pam-ldap
- /etc/pam_ldap.conf
- /etc/libnss-ldap.conf,
- /etc/nsswitch.conf

```
cat /etc/nsswitch.conf  
passwd: compat ldap  
group: compat ldap  
shadow: compat ldap
```

Felhasználói azonosítás OpenLDAP szerveren

- BIND parancs: DN, titok pár üzenet
- Titok: jelszó, kódolt jelszó stb.
- Módszerek: sima jelszó, SASL, TLS
- Miden DIT belei elemhez lehet UserPassword attribútumot rendelni
- Azonosítás lépései:
 - SSH (felhasználó név, jelszó)
 - LDAP keresés, LDAP bind
 - Sikeres bind után engedélyezzük a belépést

LDAP adatbázis kezelése

- ldap-utils
- phpldapadmin
- gq
- Egyedi megoldások

Mit tud LDAP-ot használni?

- ssh, login
- levelező kliens: címadatbázis
- levelező szerver: felhasználó adatbázis
- IMAP/POP szerverek
- Web szerver: azonosítás, virtuális domaineik stb.
- FTP szerver, Samba (gépek is)
- DNS szerver (pl.: PowerDNS)