LDAP softver i organizacija podataka

Ivan Nejgebauer
ARMUNS/CIT-UNS
<ian@uns.ac.rs>

LDAP

- Običnо se uvod svede na...

LDAP (drugi pokušaj)

- Protokol kojim se nekoj bazi pristupa
  - standardizovan
  - pogodan za integraciju
- Baza podataka organizovana na specifičan način
  - prilagođena radu sa protokolom

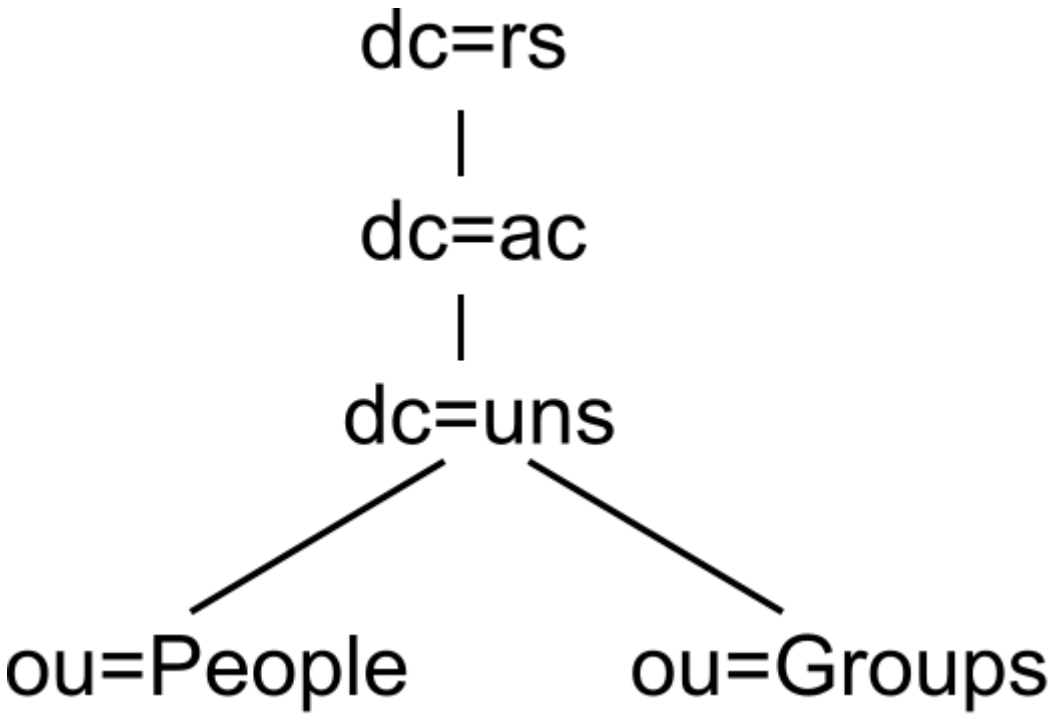
LDAP kao baza

- Orijentisana na čitanje/pretraživanje
- Tipičan slučaj (statistika servera UNS u toku jednog radnog dana):
  - pretraga: ~100k
  - modifikacija: ~100

LDAP: organizacija

- Baza se sastoji od *zapisa*
- Zapisi su organizovani kao stablo
- Donekle slično: fajlsistem sa direktorijumima i fajlovima
- Nije sasvim analogno:
  - fajlovi imaju sadržaj, direktorijumi ne
  - svi LDAP zapisi mogu imati sadržaj

LDAP: stablo



LDAP: preporuke za stablo

- Što manje razgranato
- Ne pokušavati preslikavanje organizacione šeme firme
  - moguć izuzetak: studenti/svi ostali
- Funkcionalno grananje po kategorijama

LDAP: zapisi

- Sve što nam treba od podataka o jednom objektu ide u jedan zapis
- Zapis ima jedinstveno ime, određeno položajem u stablu
- DN: **Distinguished Name**, putanja kroz stablo koja vodi do zapisa

```
uid=test,ou=People,dc=uns,dc=ac,dc=rs
```

- Pojedinačni elementi: relativna imena (RDN: **Relative Distinguished Name**)

LDAP: struktura zapisa

- Pojedinačne vrednosti zovu se *atributi*
- Skup obaveznih i dopuštenih atributa određen klasama objekata (**object classes**)
  - jedna *strukturna* (**structural**)
  - nula ili više *pomoćnih* (**auxiliary**)
- Srodni atributi i klase se definišu u *šemama*

LDAP: izbor strukturne klase

- Jednom izabranu nije trivijalno promeniti
  - obična MODIFY operacija ne radi
  - može se upotrebiti (eksperimentalna) kontrola „Relax Rules“...
  - ...ali je to problematično kod replikacije
- Preporuka: izabrati standardizovanu, kao što je **inetOrgPerson** ili **organizationalRole**

LDAP: pomoćne klase

- Sve ostalo što vam treba
- Obratite pažnju: svaka klasa objekata ima MUST i/ili MAY atribute
  - MUST atributi moraju postojati u svakom zapisu
  - ...čak i ako u vašoj instalaciji nemaju svrhu

Klase za obrazovno-istraživačke organizacije

- Internet2 projekat: klase **eduPerson** i **eduOrg**
- Prilagođeno od strane AMRES-a: **rsEduPerson** i **rsEduOrganization**
- Originalna verzija ovih klasa: strukturna
  - ne preporučuje se korišćenje u ovom obliku iz ranije navedenih razloga
  - prerađena verzija: pomoćne klase

Atributi za usluge (1/2)

- rsEduPersonAffiliation, po uzoru na eduPersonAffiliation

faculty	nastavni kadar
student	student
staff	**učenik**
alum	
member	**korisnik usluge**
affiliate	spoljni saradnik
employee	zaposleni
library-walk-in	gost

Atributi za usluge (2/2)

- eduPersonEntitlement, privilegije za pristup servisima
- Oblik: URN ili URL
- Internet2 projekat od skora preporučuje URL
- AMRES:
  - urn:mace:amres.ac.rs:...
  - urn:geant:amres.ac.rs:...

LDAP softver

- Preporuka: OpenLDAP
- Preporuka: što novija verzija
- Preporuka: 64-bitni OS
- Preporuka: mdb fizički format
- Preporuka: statička konfiguracija (ali budite spremni za dinamičku)

Kako instalirati?

- Izvorni kod:
  http://www.openldap.org/software/download/
- LTB paketi:

  RPM (CentOS)
  http://ltb-project.org/wiki/documentation/openldap-rpm

  DEB (Debian, Ubuntu)
  http://ltb-project.org/wiki/documentation/openldap-deb

Preporuke za konfiguraciju

- LTB, CentOS: obratiti pažnju na SELinux
- Definisati **rootdn**, ali *ne* **rootpw** za glavnu bazu
- Mapirati uid/gid administrativnog korisnika na **rootdn**
  - direktiva **sasl-regexp**
  - "gidNumber=**N**\\\\ +uidNumber=**N**,cn=peercred,cn=external,cn=auth"
- Za lokalne klijente, ako je moguće, koristiti **ldapi** transport i SASL EXTERNAL
  - loše podržano, na žalost

Klijentski pristup

- Klijentske aplikacije koje idu uz OpenLDAP server
- Shell/Perl/Python/C API
- Apache Directory Studio
- shelldap