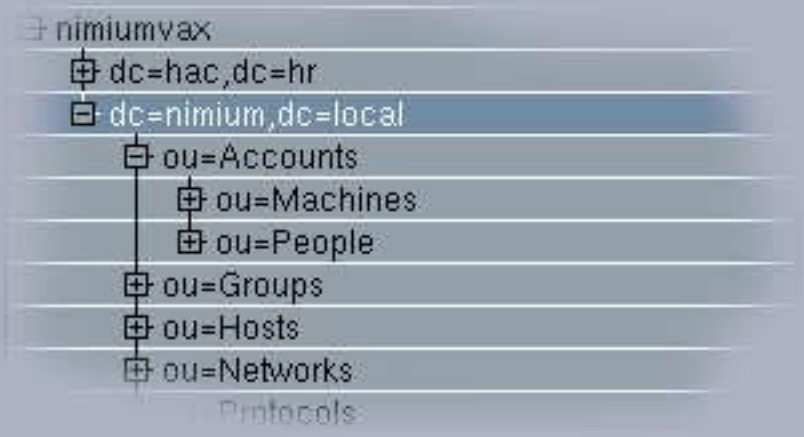
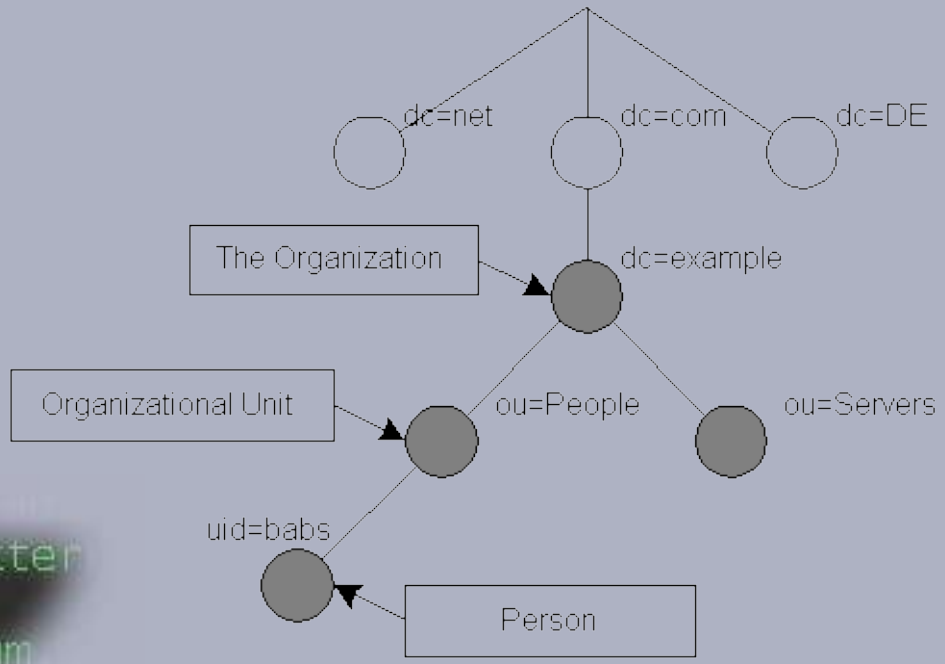
LDAP na GNU/Linuxu implementacija i primjene





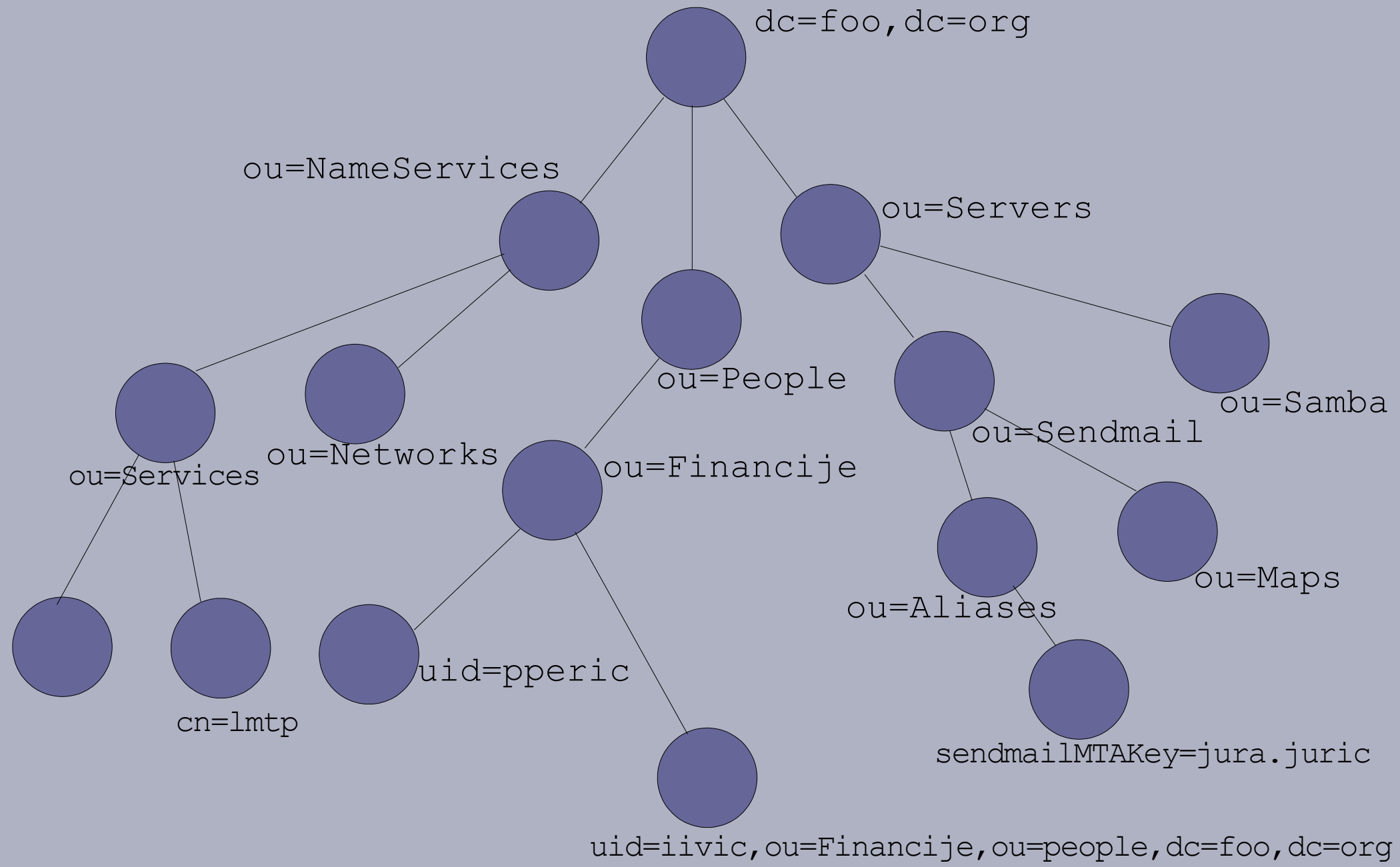

```
[nimiumvax!mvz!mvz]$ ldapsearch -Y exter
SASL/EXTERNAL authentication started
SASL username: emailAddress=mvz@nimium
eb,C=HR
SASL SSF: 0
# extended LDIF
#
# LDAPv3
# base <> with scope sub
# filter: (&(objectClass=in
# requesting: ALL
```

Miroslav Zubčić,
Nimium d.o.o.

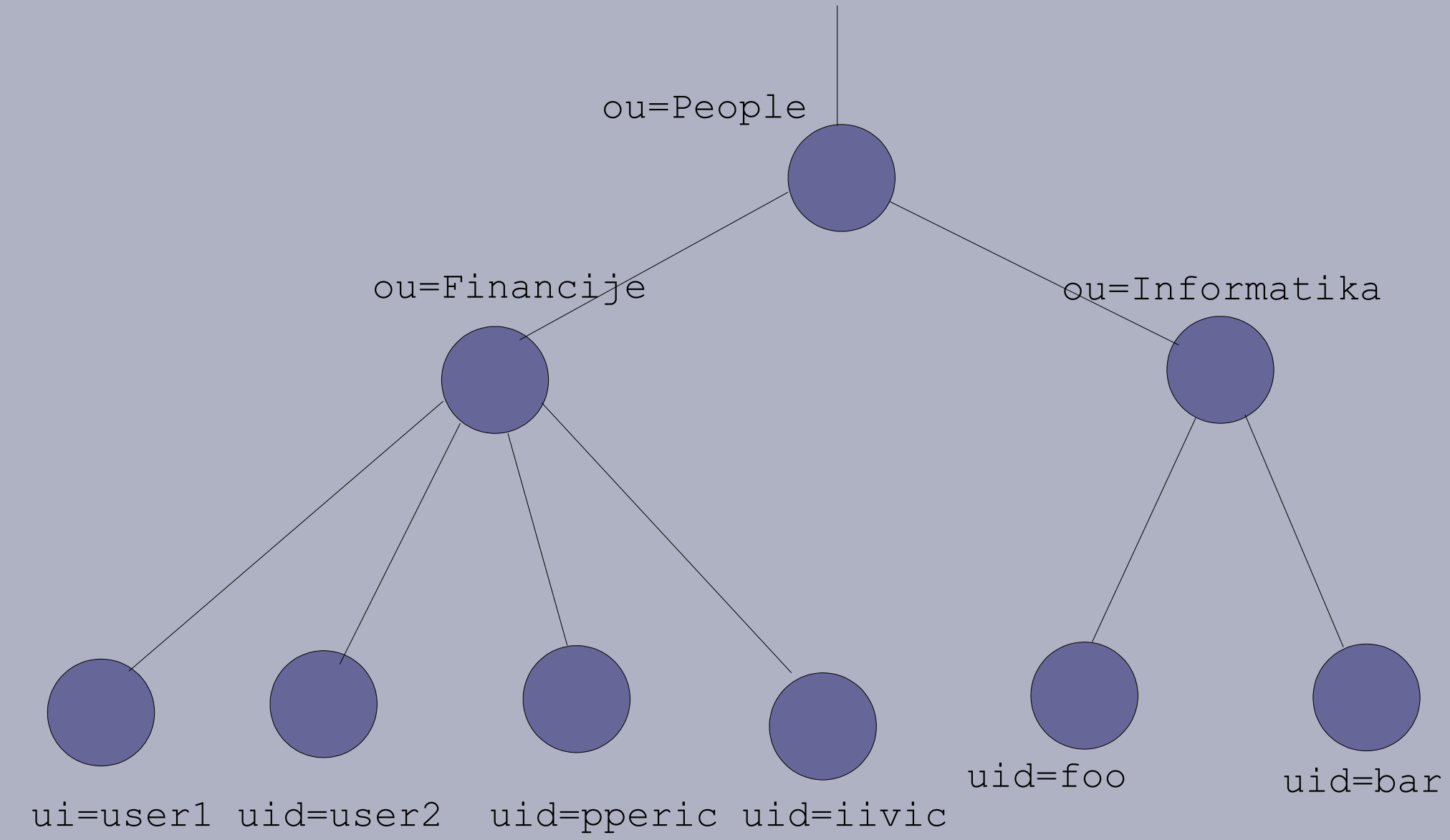
1. Osnovni pojmovi u LDAP-u

- Što je to LDAP ?
- LDAP stablo/direktorij/baza - Internet shema, moderni design LDAP direktorija
- DN – Distinguished Name
- Izgled LDAP zapisa
- Što su to atributi i objectClass-e
- LDAP filteri
- Što je to LDAP schema ?
- LDAP autentifikacija, SASL, SSL i Kerberos

1.1 Internet shema, moderni design LDAP direktorija



1.1 Internet shema, moderni design LDAP direktorija



1.2 LDAP Distinguished Name

- Kako tumačiti LDAP path: DN i RDN

DN: Distinguished Name

uid=pperic,ou=Financije,ou=People,dc=foo,dc=org

ou=Financije,ou=People,dc=foo,dc=org

ou=People,dc=foo,dc=org

dc=foo,dc=org

RDN: Relative Distinguished Name

uid=pperic

1.2 LDAP Distinguished Name

- LDAP DN path u usporedbi sa UNIX filesystem pathom:

uid=pperic,ou=Financije,ou=People,dc=foo,dc=org

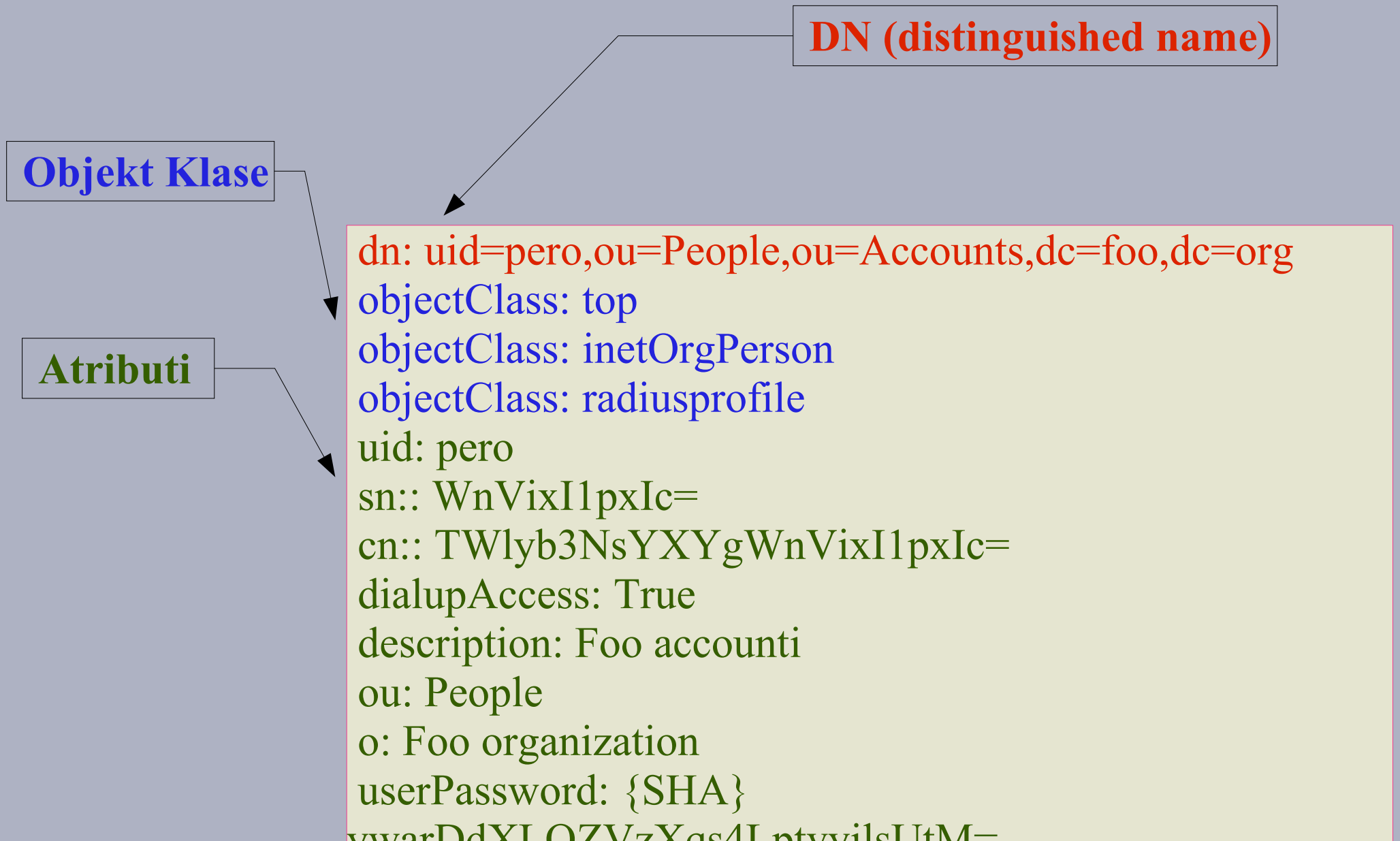
(od korijena prema krajnjem zapisu krećemo se s desna na lijevo)

. . .

/net/luna/export/financ/home/users/pperic

(od korijena prema krajnjem direktoriju krećemo se s lijeva na desno)

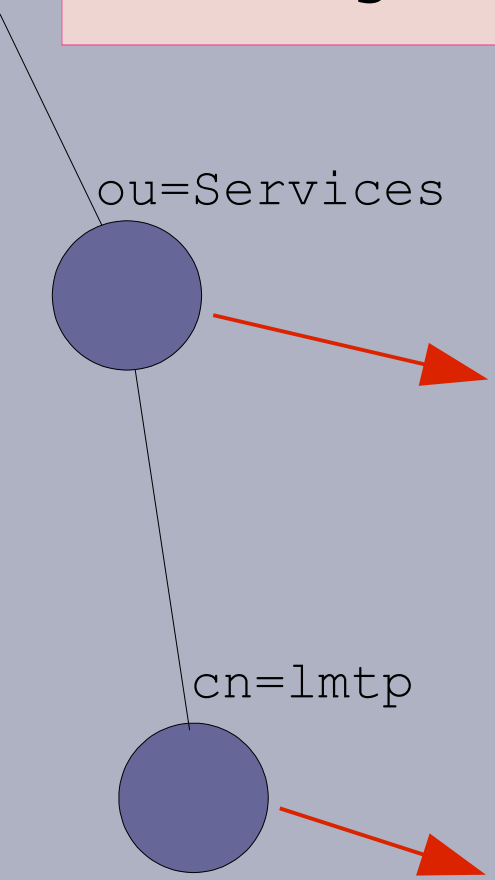
1.3 Izgled LDAP zapisa



1.4 Primjer LDAP zapisa: prosječni real-life account

```
dn: uid=pperic,ou=Financije,ou=People,dc=foo,dc=org
objectClass: person
objectClass: posixAccount
objectClass: top
objectClass: organizationalPerson
objectClass: orgFooPerson
objectClass: inetOrgPerson
objectClass: inetLocalMailRecipient
objectClass: officePerson
objectClass: mozillaPerson
objectClass: sambaSamAccount
givenName: Pero
sn:: UGVyaeY=
employeeNumber: 1234
ou: Financije
departmentNumber: 123
homePostalAddress: Putevi Svile 3
c: HR
xmozillausehtmlmail: false
initials: P. P.
o: Foo Organization
preferredLanguage: Croatian
uidNumber: 7123
loginShell: /bin/false
homeDirectory: /home/users/pperic
gidNumber: 7000
uid: pperic
displayName:: UGVybyBQZXJp5g==
cn:: UGVybyBQZXJp5g==
sambaSID: S-1-5-123-456-789-123-1-141040
sambaPrimaryGroupSID: S-1-5-123-456-789-123-1-141001
sambaLogonScript: scripts\zabrane.cmd
```

1.5 Izgled jednog LDAP podstabla i zapisa tcp/ip servisa




```
dn: ou=Services,dc=NameServices,dc=foo,dc=org
objectClass: top
objectClass: organizationalUnit
ou: Services



dn: cn=lmtp,ou=Services,dc=NameServices,dc=foo,dc=org
objectClass: ipService
objectClass: top
ipServicePort: 2000
ipServiceProtocol: tcp
cn: lmtp
```

1.6 Što su to atributi i objectClass-e

- Objekt klase (objectClass) određuju pripadnost nekog zapisa dijelu neke sheme, dostupnost pojedinih atributa zapisu, a često i obavezu da neki zapis posjeduje neki atribut.

- Svaka objekt-klasa, kao i svaki atribut imaju svoj jedinstveni OID (object identifier).

- Objekt klase, kao i atributi, definirane su u LDAPv3 shemama (tekst fileovi koje uključuje slapd.conf(5) u slučaju OpenLDAP slapd(8) servera).

- Poznatije i često upotrebljavane objekt klase opisane su u RFC dokumentima, generičkog su designa, te služe svima za slobodnu upotrebu i nadogradnju prema potrebama.

- Najpoznatije objekt klase su na primjer: `account`, `posixAccount`, `shadowAccount`, `top`, `organzationalUnit`, `ipService`, `mail`, `inetOrgPerson`, `person`, `nisMap`, `dc`, `posixGroup` i mnoge druge.

1.6 Što su to atributi, a što objectClass-e

- LDAP atributi su ključevi koji sadrže tekstualne ili binarne vrijednosti. Atributi su spremnici podataka. Na primjer: `commonName: Pero Perić` - commonName je atribut, a "Pero Perić" je njegova (UNICODE kodirana u ovom slučaju) vrijednost.
- LDAP atributi definirani su zajedno sa objekt klasama u LDAPv3 shemama, atributi mogu biti definirani kao ASCII, UNICODE, bitstring, binary, integer, boolean tipovi, a također definiraju smije li neki zapis imati samo jedan (SINGLE-VALUE) ili više definicija jednog te istog atributa. Atributima se u shemi određuju načini pretraživanja i tip substring pretrage u LDAP filterima.
- Svi non-ASCII atributi spremaju vrijednosti enkodirane base64.
- Neki primjeri atributa, kao i poznatiji atibuti su među ostalima: `cn, sn, uid, gid, o, ou, jpegPhoto, owner, l, departmentNumber, displayName, givenName, email, mobile, ipHost, st, c, street, URL, userPKCS12, loginShell, macAddress, title, postalCode uidNumber` ...
- Atributi i objekt klase se u pravilu pišu u tzv. "camel" notaciji, dvije ili više riječi spojene su u jednu i sve osim prvog pojma u riječi zadržavaju početno veliko slovo naziva.

1.7 LDAP filteri

- LDAP filteri su za LDAP protokol isto što i `SELECT` SQL upiti za SQL baze podataka.
- Filteri podržavaju logičke operatore (`AND, OR, NOT`), koji se mogu kombinirati u jednom upitu, globing (`*, ?`), aritmetičke operacije usporedbe jednakosti, više od (>), manje od (<), aproksimacije (~=) itd ...
- LDAP filteri definirani su u RFC-u 2254.

Primjeri LDAP filtera:

Filter: `(&(objectClass=shadowAccount)(ou=Financije)(uid=pp*))`
Pronaći će među ostalim zapisima koji su obuhvaćeni pretragom i zapis:
`"dn: uid=pperic,ou=Financije,ou=People,dc=foo,dc=org"`

Filter: `(&(objectClass=sambaSamAccount)(|(ou=Financije)(ou=Informatika)(uid=*)))`
Pronaći će sva UNIX login imena koja su članovi odjela financija ili informatike, te imaju samba account u svom zapisu.

Filter: `(objectClass=*)`, dan od strane direktorijskog super-korisnika, napravit će gotovo ekvivalent export cijelog direktorija, ako je baza pretrage bio LDAP korijen.

1.8 LDAP shema

- LDAP shema je skup srodnih tematskih objekt klasa i atributa, za neku posebnu namjenu, kao što su to na primjer UNIX name servisi, radius accounti, IP hostovi ...
- OpenLDAP software drži sheme u tekstualnim fileovima, te sheme se pišu bilo kojim editorom, a sintaksa je gotovo identična kao primjeri definicije LDAP shema iz RFC dokumenata.
- Pisanje i prilagođavanje sheme u nekoj organizaciji zahtijeva oprezno planiranje i promišljanje o trenutnim i budućim potrebama, kao i logičnosti u interakciji sa atributima ostalih shema, dupliciranje postojeće funkcionalnosti nije preporučljivo. Prvo treba pogledati što nude standardne sheme i to koristiti.

Neke od često korištenih shema

File	Description
`core.schema`	OpenLDAP *core* (required)
`cosine.schema`	Cosine and Internet X.500 (useful)
`inetorgperson.schema`	InetOrgPerson (useful)
`misc.schema`	Assorted (experimental)
`nis.schema`	Network Information Services (FYI)
`openldap.schema`	OpenLDAP Project (experimental

1.9 LDAP reference: podređene i nadređene informacije znanja

- LDAP podržava distribuirane direktorijske servise.
- Dijelovi LDAP stabla mogu se delegirati podređenim LDAP serverima, a u glavnom LDAP direktoriju, mogu se stavljati atributi-reference, kao što je "`ref`" - atribut `referral` objekt klase.
- LDAP server može upućivati klijente sa upitima na koje sam nema odgovore na nadređene LDAP servere, dajući im njihov URI klijent zatim pita te servere isto pitanje/filter. Ova funkcionalnost se konfigurira na razini konfiguracijskog filea kao jedna direktiva: "`referral  ldap://root.openldap.org/`".

Primjer LDAP zapisa sa referencom na podređeni izvor znanja:

```
dn: dc=mreznaoprema,dc=foo,dc=org
objectClass: referral
objectClass: extensibleObject
dc: subtree
ref: ldap://slave01.foo.org/dc=mreznaoprema,dc=foo,dc=org
```

1.10 LDAP autentifikacija, SASL, SSL/TLS i Kerberos

- OpenLDAP software podržava verziju 2 i 3 LDAP protokola, običnu v2 autentifikaciju korisničkog DN-a sa passwordom iz `userPassword` atributa, kao i v3 SASL autentifikaciju pomoću EXTERNAL (SSL x.509 certifikati), GSSAPI (Kerberos v5), CRAM-MD5, DIGEST-MD5 i ostalih mehanizama autentifikacije.

- TLSv1 je podržan kao STARTTLS ekstenzija v3 protokola, ali i kao SSL server na portu `636/tcp` u verziji 2 protokola (službeni LDAP port je `389/tcp`). Parametri ciphera i enkripcije, certifikacijski autoritet (CA), serverski certifikat, kao i privatni ključ, konfiguriraju se u slapd.conf(5) – glavnoj konfiguracijskoj datoteci servera.

- Kerberos v5 je podržan preko SASL autentifikacijskog mehanizma "GSSAPI" što znači "Generic Security Service Application Program Interface". OpenLDAP server radi kao poseban neprivilegirani sistemski korisnik, stoga mora čitati vlastitu keytab datoteku. Staza i ime kerberos keytab datoteke, uzima se iz environment varijable `KRB5_KTNAME`.

1.11 Mali podsjetnik: LDAP terminologija

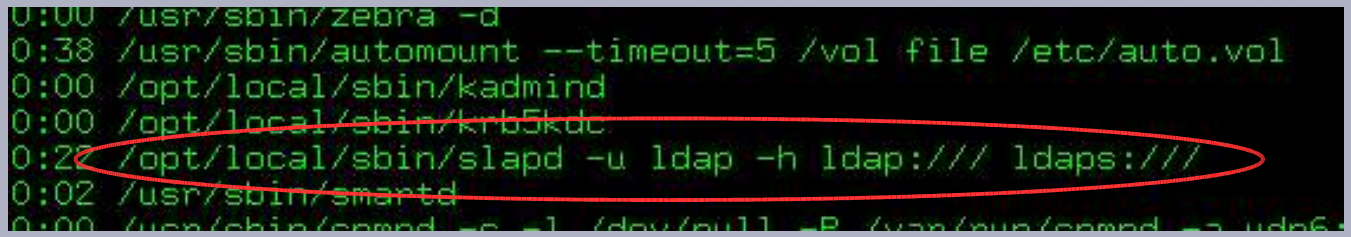
- DUA - Directory User Agent - bilo koji klijent LDAP servera - analogija: MUA, Mail User Agent
- DS - Directory Service - ukratko on-line LDAP baza
- DIT - Directory Information Tree - hijerarhijsko drvo LDAP baze, LDAP baza
- DSA - Directory System Agent - stand alone LDAP server kod normalnog TCP/IP LDAP-a. Server koji poslužuje dio informacijskog stabla kod ISO X.500 DAP protokola.
- Entry (zapis) objekt u LDAP bazi identificiran sa DN-om (distinguished name). Sadrži klase objekata koje donose mogućnost dodavanja temstskih atributa zapisu.
- objectClass (klasa objekta) - određuje kojim klasama objekata neki zapis (entry) pripada, tako da se u zapisu navode te iste objekt klase.
- SASL - Simple Authentification Security Layer (rfc 2222).
- DN - Distinguished Name. Path zapisa u direktoriju, usporediv sa UNIX filesystem pathom.
- LDIF - LDAP Data Interchange Format - lako čitljiv tekstualni oblik LDAP zapisa.

2. OpenLDAP – open source implementacija LDAP klijenta, servera i API-ja za UNIX sisteme

http://www.OpenLDAP.org

- slapd(8) – stand alone LDAP daemon
- Komande i alati
- C API i sistemske biblioteke (“libovi”)
- Korisni linkovi i mailing liste

2.1 slapd(8) – stand alone LDAP daemon



- LDAPv3 podrška
- Protokoli: ipv4, ipv6, unix(7) socket
- Podržava obične i TLS konekcije (sa autentifikacijom certifikatima i/ili čistu enkripciju)
- SASL autentifikacija i autorizacija (rfc 2222)
- Zadana vremenska ograničenja za pretraživanje
- Kerberos v5 podrška pomoću SASL GSSAPI mehanizma
- Modularna sučelja i spremnici podataka (berkeley DB, ldbm, LDAP proxy, passwd, shell)
- Sučelje za on-line nadzor (back-monitor) i pregled stanja servera u obliku virt. LDAP stabla
- ACL (Access Control Lists) – omogućuju finu kontrolu pristupa pojedinim atributima i zapisima
- ACL subsistem podržava POSIX regular expressione
- Podrška za više instanci LDAP baza sa vlastitim korijenom u jednom procesu
- Indeksiranje atributa za brže pretraživanje i sortiranje
- Moderni design daemona sa POSIX threadovima
- Replikacija pomoću transakcijskog loga. Transakcijski log čita pomoćni daemon `slurpd(8)`
- TCPWRAPPERS podrška (`/etc/hosts.{allow,deny}`)
- Mapiranje SASL realmova i korisnika LDAP korisničke DN-ove

2.2 Komande i alati

Offline server alati:

- slapcat(8), slapadd(8), slapindex(8)

On-line LDAP klijenti:

- ldapsearch(1), ldapmodify(1), ldapdelete(1), ldapmodrdn(1), ldappasswd(1), ldapcompare(1), ldapwhoami(1), ldapadd(1)

2.3 C API i sistemske biblioteke (“libovi”)

- libldap – glavni LDAP API library
- liblber – BER (Basic Encoding Rules u ASN.1) subrutine
- Više od 150 često korištenih API funkcija i man stranica

2.4 Korisni linkovi i mailing liste

- Glavna stranica: http://www.OpenLDAP.org
- Dokumentacija za administratore: http://www.OpenLDAP.org/doc/
- Faq-O-Matic: http://www.openldap.org/faq/
- Bug tracking sistem: http://www.openldap.org/its/
- Lista za korisnike: <openldap-software@openldap.org>
- Lista za prijavu bugova (ITS sistem/mail): <openldap-bugs@openldap.org>
- Razni korisni savjeti: http://yolinux.com/TUTORIALS/LinuxTutorialLDAP.html

3. Integracija sistemskih name servisa sa LDAP-om - nsswitch(5) i pam(8)

- UNIX name servisi mogu biti mrežno distribuirani preko LDAP-a umjesto NIS-a (yp).
- GNU/Linux, kao i još neki slobodni unix sistemi, koristi name service switch u obliku pluginova za sistemski C library (`/lib/libnss_ldap.so.X`).
- Moguće je koristiti TLS/SSL enkripciju, kao i X.509 certifikate za autentifikaciju
- Kod intenzivno korištenih servera, koristi se nscd(8) (Name Service Cacheing Daemon), kako bi se vrijeme upita smanjilo, a performanse poboljšale.
- Nije potrebno definirati nikakvu NIS domenu, LDAP filter za selekciju korisnika se zadaje u sistemskom ldap.conf-u, najčešće prema LDAP podstablima ili atributu organizacijske jedinice (ou).
- Podržane sistemske imeničke baze su: `passwd`, `shadow`, `group`, `networks`, `rpc`, `services`, `protocols` i `netgroup`.
- Moguće je koristiti `pam_ldap` kao pam(8) plugin za mrežnu distribuiranu autentifikaciju. (U te svrhe se ipak radije preporuča `pam_krb5` - tj. Kerberos v5.).

3.1 ldap.conf: konfiguracija i važniji parametri

- `host`: nekoliko servera poredano prema preferencama klijenta (redundantno)
  primjer: `host ldapserver.foo.org ldapserver2.foo.org ldapserver3.foo.org`
- `base`: Dio direktorija od kojega nsswitch library pretražuje:
  primjer: `base dc=foo,dc=org`
- `binddn`: LDAP DN korisnik/entitet s kojim se ldap nsswitch autorizira LDAP serveru
  primjer: `binddn uid=binddn,ou=Sysacct,dc=foo,dc=org`
- bindpw: Plain tekst password s kojim se binddn autentificira
  primjer: `bindpw littlesecret`
- `rootbinddn`: LDAP DN korisnik/entitet s kojim se ldap nsswitch autorizira LDAP serveru ako efektivni uid == 0. Lozinka se nalazi u /etc/ldap.secret koji nije čitljiv za obične korisnike (mode 0600 npr.)
- `nss_base_<service>`: LDAP URI ili dio stabla sa specifikacijom filtera za pretragu korisnika. Ovime možemo na vrlo fleksibilni način ograničiti domene po bilo kojem kriteriju – kako po pojedinom atributu ili objekt klasi nekog zapisa, tako i po dijelu stabla koje se pretražuje.
- primjer: `nss_base_passwd ou=Financije,ou=People,dc=foo,dc=org?one?ou=Racuni`

3.2 pam_ldap

- Sistemska autentifikacija pomoću PAM sistema je moguća pomoću `pam_ldap` plugina.
- pam_ldap za sada ne podržava `chsh` i `chfn` servise
- Za distribuiranu mrežnu autentifikaciju korisnika, preporuča se korištenje kerberosa u kombinaciji sa LDAP-om kao nsswitch modulom. Kerberos je usko specijalizirani standardni servis za takve namjene. Integracija sa PAM sistemom ide preko plugin modula `pam_krb5`
- LDAP se kao autentifikacijski servis može koristiti za http, PPP/RADIUS i ostale sekundarne autentifikacije, gdje nema smisla eksponirati kerberos sistem.

Primjer ssh servisa u /etc/pam.d:

```
#%PAM-1.0
auth       required     /lib/security/pam_nologin.so
auth       sufficient   /lib/security/pam_ldap.so
auth       required     /lib/security/pam_unix_auth.so try_first_pass
account    sufficient   /lib/security/pam_ldap.so
account    required     /lib/security/pam_unix_acct.so
password   required     /lib/security/pam_cracklib.so
password   sufficient   /lib/security/pam_ldap.so
password   required     /lib/security/pam_pwdb.so use_first_pass
session    required     /lib/security/pam_unix_session.so
```

3.3 nsswitch.conf(5)

- Primjer `/etc/nsswitch.conf` filea. Korisnici , grupe, servisi, network segmenti, koriste `ldap` kao bazu, nakon defaultnih sistemskih postavki u lokalnim fileovima.
- Ne preporučuje se izbacivati **`files`** pretraga, kao niti stavljanje **`files`** baza nakon **`ldap`** baze.
- Neke rijetko promjenjive servise nema smisla opterećivati sa mrežnom pretragom.

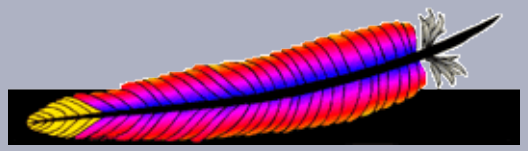
SAVJET: `hosts` servis najbolje radi sa DNS sistemom koji je specijaliziran za to, baš kao što je kerberos specijalizirani servis za sigurnu mrežnu autentifikaciju – koristimo ih, nemojmo sve trendovski potrpati u LDAP bez razmišljanja! Kerberos i DNS se dobro slažu sa LDAP-om i bez uske integracije !

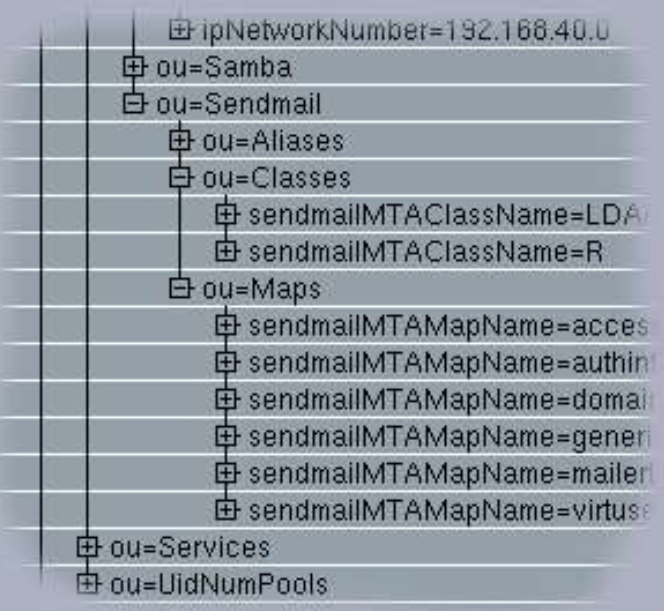
```
passwd:      files ldap
shadow:      files ldap
group:       files ldap
hosts:       files dns
ethers:      files
netmasks:    files
networks:    files ldap
protocols:   files # nema previse smisla
rpc:         files # nema previse smisla
services:    files ldap
netgroup:    files # ldap
```

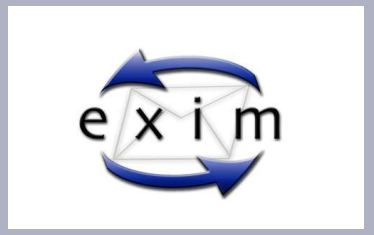
3.4 Savjeti za debugiranje i dijagnostiku nsswitcha

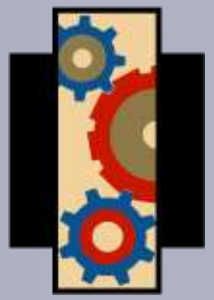
- Prije debugiranja problema sa name servisima, ugasiti privremeno nscd(8) cache.
- Uvijek imati rezervni otvoreni terminal emulator ili tty sa ulogiranim root korisnikom za slučaj fatalne greške u konfiguraciji.
- Koristiti alat getent(1) za izlistavanje podataka iz sistemskih baza.
- Provjeriti permissione od `/etc/nsswitch.conf` i `/etc/ldap.conf` fileova.

4. Integracija nekih servisa i servera sa LDAP-om: sendmail, samba, cyrus imap, apache, FreeRADIUS, squirrelmail, SASL, squid ...









4.1 Sendmail

- Sendmail je vrlo dobro integriran sa LDAP-om. Moguće je raditi mail clustere sa zajedničkim konfiguracijama klasa, mapama i bazama aliasa.
- Sendmail definira mapu tipa “ldap”, što znači da u LDAP-u može držati mape virtualnih hostova, internih mailera, domena, access liste, genericstable, a i ono najvažnije – aliase.
- Klase kao što su $=R, $={internal_aliases} i mnoge druge, mogu se također pretraživati u LDAP direktoriju (`objectClass sendmailMTAClass`).
- Sendmail podržava mail (re)routing LDAP shemu, sa individualnim pravilima za mail routing po svakog posebnog zapisa/accounta.

Dokumentacija:

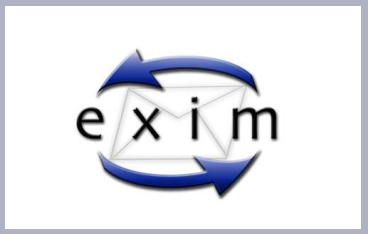
http://www.sendmail.org/m4/ldap.html
http://www.sendmail.org/m4/ldap_routing.html
draft-lachman-laser-ldap-mail-routing-02.txt
cf/README

4.2 Postfix

- Postfix je vrlo dobro i fleksibilno integriran sa LDAP-om. Podržava pretrage mapa sa virtualnim hostovima, aliasima i ostalim mapama.
- Sve konfiguracije, za LDAP host, port, autentifikaciju i ostale parametre, su u konfiguracijskom fileu main.cf.
- Filter sa upitima, skop i korijen pretrage su konfigurabilni.

Dokumentacija i više informacija:
http://www.postfix.org
postfix-2.0.19/README_FILES/LDAP_README (glavna dokumentacija)
postconf(1), access(5), virtual(8)

4.3 Exim

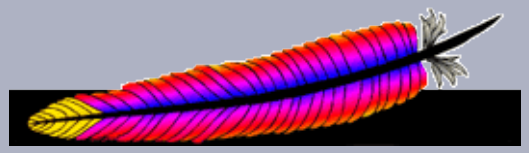


- Podržava vrlo velik broj LDAP implementacija: OpenLDAP 1 i 2, Univ. of Michigan, Netscape i Solaris.
- Ukoliko koristi OpenLDAP API, podržava LDAP konekcije preko Unix Socketa (ldapi).
- Exim implementira "`ldap`" tip pretraživanja, sa tri podmape za različite vrste rezultata pretrage (single value, multiple values i dn).

Dokumentacija i više informacija:

`http://www.exim.org`
`exim-4.31/doc/spec.txt (sekcije 9.3, 9.10 - 9.15.)`
`http://www.exim.org/pipermail/exim-users/ (arhiva mailing liste)`

4.4 Apache: mod_auth_ldap



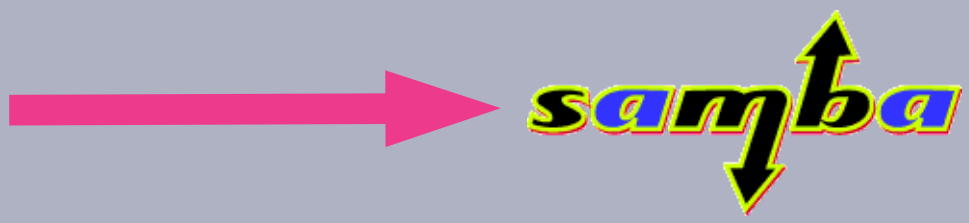
- Apache HTTP server podržava LDAP protokol za autentifikaciju korisnika u glavnom serveru, virtualnim hostovima i njihovim pojedinim direktorijima.
- Podržava OpenLDAP, Novell, iPlanet/Netscape API.
- Podrška za SSL konekcije (ldaps 636/tcp) i TLS ekstenzije LDAPv3 protokola.
- Ručna konfiguracija LDAP filtera pruža veliku fleksibilnost za autorizaciju.
- Autorizacija pomoću `require_user`, `require_valid_user`, `require_dn` i `require_group (AuthLDAPGroupAttribute)` konfiguracijskih direktiva u `httpd.conf`.
- Vrlo velike mogućnosti integrirane autentifikacije sa više apache servera ili njihovih virtualnih hostova. Isti LDAP zapisi se naravno mogu koristiti za RADIUS ili Squid proxy autentifikaciju.
- Nema portebe za .htaccess fileovima.

Dokumentacija:
`http://httpd.apache.org/docs-2.0/mod/mod_auth_ldap.html`

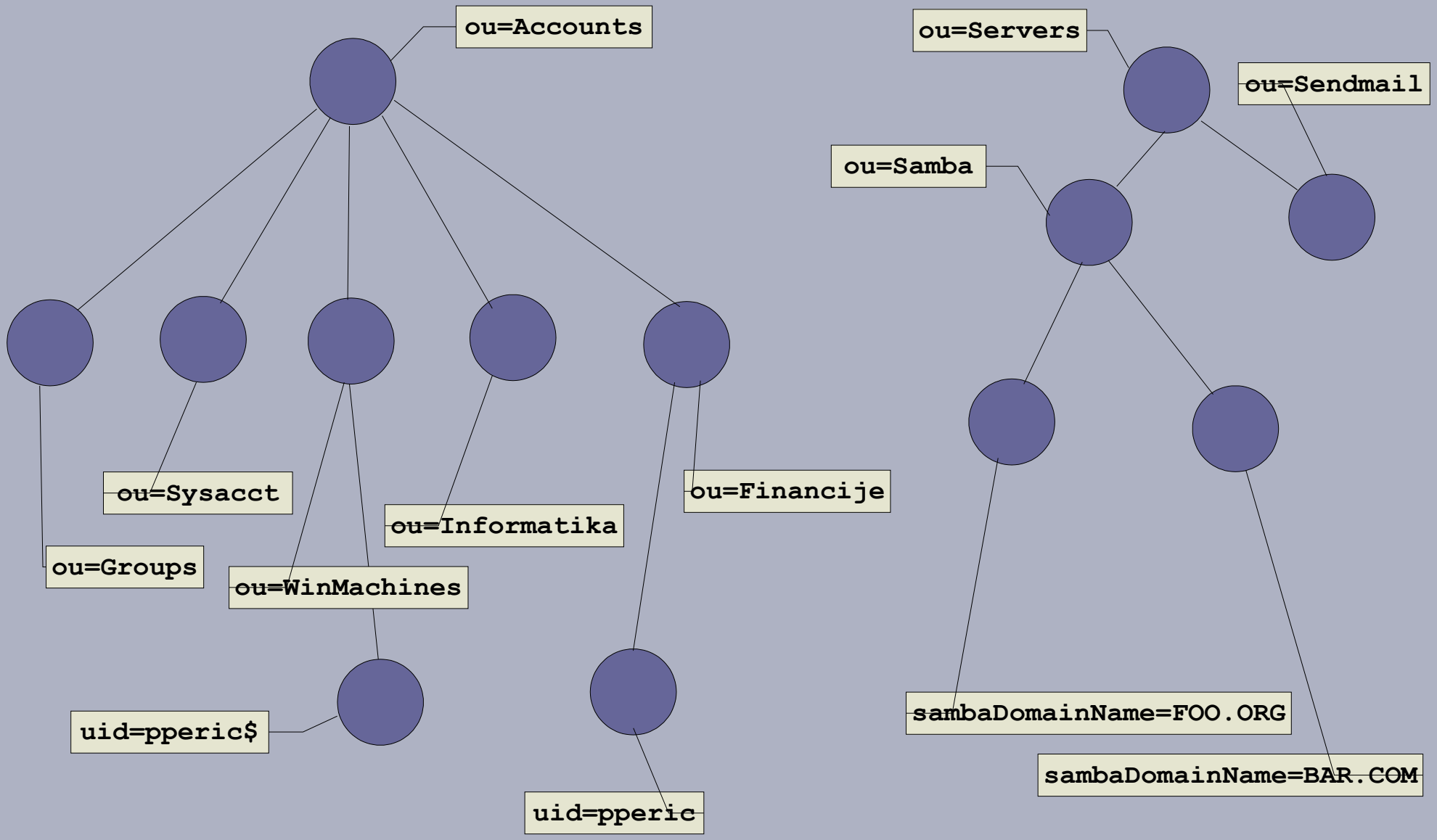
4.5 Samba (v2.2.X i v3.X)

- Samba je sa LDAP-om integrirana direktno, ali i indirektno preko name service switcha (libnss_ldap).
- Samba 2.2.X koristi shemu koja definira objekt klasu `sambaAccount`.
- Samba 3.X koristi novu shemu koja definira objekt klasu `sambaSamAccount`.
- Samba u LDAP zapisima korisnika čita atribute NT i LANMAN passworda, flagove SAM accounta, autorizacijske atribute nekih dozvola korisnika, logon skripte, patha do remote NT domain profila, ime NT/w2k domene kojoj pripada zapis/korisnik, windows drive oznake za mapiranje unix home direktorija i još poneke standardne atribute iz core sheme, kao što je `displayName`.
- Više samba NT domain kontrolera može raditi sa zajedničkim LDAP serverom.

- Jedan samba NT domain kontroler može raditi sa više LDAP servera, tj. ako prvi nije dostupan, onda sa drugim, trećim itd ...
- U sambi 3.X bolje je izvedena sinhronizacija UNIX i NT passworda u LDAP-u.
- Samba 3.X ima može imati finu kontrolu sufixa za grupe, mašine i korisnike u LDAP stablu prilikom dodavanja accounta.
- Samba 3.X može držati podatke o domeni i domain SID-u u LDAP-u, u posebnom serverskom podstablu.
- Samba 3.X još nema punu funkcionalnost win2000 AD domene, premda ostali dijelovi za AD domenu odavno postoje – Kerberos KDC (MIT, Heimdal), ISC Bind 9 i OpenLDAP.
- Kao i mnogi ostali LDAP-osposobljeni serveri, samba 3.X i 2.2.X podržava ručno specificiranje LDAP filtera za pretragu, čime je moguće odjeljivati korisničke i mašinske accounte po bilo kojem kriteriju: nekom atributu, objekt klasi, skopu pretrage i početnom korijenu pretrage (search base).



- Primjer organizacije korisnika i mašina u jednoj većoj organizaciji:



4.6 FreeRADIUS

freeRADIUS

- Autorizacija i autentifikacija pomoću eksternih resursa i servisa. Između ostalih, LDAP backend je vrlo dobro podržan.
- FreeRADIUS server je modularan poput apachea, tako da za autentifikaciju i autorizaciju može koristiti LDAP pomoću svog modula `rlm_ldap.so`.
- FreeRADIUS donosi posebnu radius shemu koja mapira RADIUS atribute iz radius dictionaryja u LDAP atribute.
- Podrška za TLS u komunikaciji sa LDAP serverom.
- Konfigurabilan LDAP filter.
- Radi primjera kompleksnosti, FreeRADIUS može raditi autorizaciju iz LDAP baze, autentifikaciju pomoću kerberosa, a accounting u postgres ili mysql SQL bazu, a sve to može biti ovisno o realmu kojemu pripada korisnik ili NAS.

Dokumentacija i mailing lista:

http://www.freeradius.org/radiusd/rfc/
http://www.freeradius.org/radiusd/doc/
http://www.mail-archive.com/freeradius-users@lists.cistron.nl/

4.7 Squid

- Squid web cache/proxy ima autentifikacijske pluginove u obliku jednostavnih programčića zvanih “helper programi” koji se spajaju na razne autentifikacijske servise.
- Squid može autentificirati korisnika pomoću `squid_ldap_auth` plugina.
- Squid može raditi autorizaciju i pre-autentifikaciju sa access control listama pomoću `squid_ldap_group` plugina čiji povratni status se definira kao eksterni ACL.
- Moguća opcionalna upotreba TLS enkripcije.
- Squid ne može koristiti autentifikaciju u “transparent proxy” načinu rada.

Dokumentacija i mailing lista:
Docs: **`http://squid-docs.sourceforge.net/latest/book-full.html`**
konfiguracijski vodič: **`http://squid.visolve.com/squid/index.htm`**
FAQ: **`http://www.squid-cache.org/Doc/FAQ/FAQ.html`**
lista: **`http://www.squid-cache.org/mail-archive/squid-users/`**

4.8 Squirrelmail

- Popularna web mail aplikacija u PHP-u podržava LDAP pretrage globalno zapisanih adresa i podataka, vrlo jednostavna konfiguracija i pretraga.
- Primjer upotrebe LDAP-a direktno od strane korisnika

Plugin:

http://www.squirrelmail.org/plugin_view.php?id=42

Pohrana korisničkih postavki u LDAP-u:

http://email.uoa.gr/projects/squirrelmail/ldapuserdata.php

4.9 ISC Bind 9 – primjer loše i uzaludne integracije

- DNS je hijerarhijska baza podataka (među ostalim).
- LDAP je po designu hijerarhijska baza podataka.
- Većina LDAP servera ima neki oblik replikacije.
- Većina DNS servera replicira zone između master i slave servera.
- Bind podržava dinamički update (rfc 2136).
- Za update LDAP direktorija na način kako se to radi sa DNS-om, često je potrebno pisati posebne programe,
- LDAP server i sistem na kojemu se nalazi mogu isto ovisiti o DNS-u, a DNS opet o LDAP-u – kokoš-jaje problem.
- DNS upiti sa zonama u LDAP backendu se ne cacheiraju u memoriji, a sporiji su i do nekoliko puta od običnih.
- **Nemojmo ponavljati integracijske pogreške nekih drugih sistema!**
- DNS i LDAP su već dovoljno integrirani putem C i resolver library funkcija i skladno rade jedan pored drugog bez nasilne integracije.

5. Pristup LDAP-u iz programskih jezika APIji: Perl::LDAP, C/C++ API (openldap, netscape), Python, PHP i java.

```
$result = $ldap->add( 'cn=Barbara Jensen, o=University of Michigan, c=US',
                            attr => [
                            'cn'   => ['Barbara Jensen', 'Barbs
Jensen'],
```

```
if ((conn->ld = ldap_connect
(instance, inst->login, inst->password, 0, &res)) == NULL) {
            radlog(L_ERR, "rlm_ldap: (re)connection attempt
failed");
            if (search_retry == 0)
                 conn->failed_conn
                return (RLM_MODULE
}
      conn->bound = 1;
```

```
   private int runPassword(String[]
args)
    { LDAPConnection lc;
        // parse args
        Options options = null;
        try { options = new Options();
                                    {
```

```
try:
    ldap_result_id = l.search(baseDN, searchScope, searchFilter,
retrieveAttributes)
    result_set = []
    while 1:
            result_type, result_data = l.result(ldap_result_id, 0)
            if (result_data == []):
                    break
            else:
```

5.1 Perl: Net::LDAP i PerlLDAP

- Perl Net::LDAP API je kolekcija perl modula koja omogućuje perl programima pristup LDAP direktorijima, operacije u direktoriju, kao i LDAPv3 ekstenzije za autentifikaciju i enkripciju.
- Net::LDAP Ovisi o ASN.1 perl modulu.

Kratak primjer konektiranja na LDAP server i jednog upita u direktoriju:

```
use Net::LDAP;

$ldap = Net::LDAP->new("127.0.0.1") or die "$@";
$mesg = $ldap->bind(version => 3);
$mesg = $ldap->bind ( "uid=admin", password => "idetigar", version => 3 );

my ($search,$attrs,$base) = shift;
if (!$base ) { $base = "dc=foo,dc=org"; }
if (!$attrs ) { $attrs = [ 'uid','cn' ]; }
my $result = $ldap->search ( base    => "$base",
                             scope   => "sub",
                             filter  => "$search",
                             attrs   =>  $attrs
                           );
```

Homepage: **http://ldap.perl.org/**

Stariji Mozilla/Netscape perl API (Zahtjeva Netscape LDAP SDK 4 ili 5):
http://www.mozilla.org/directory/perldap.html

5.2 OpenLDAP i Netscape/Mozilla API

- OpenLDAP API je danas najkorišteniji C/C++ LDAP API na slobodnim unix sistemima, dolazi u paketu sa OpenLDAP serverom.
- libldap – glavni LDAP API library (već smo rekli)
- liblber – BER (Basic Encoding Rules u ASN.1) subrutine (već smo rekli)
- Više od 150 često korištenih API funkcija i man stranica (već smo rekli)
- OpenLDAP C/C++ API koriste de facto svi slobodni otvoreni serverski i klijentski programi na GNU/Linuxu i BSD sustavima.

- Netscape LDAP SDK: alternativni LDAP C/C++ API.
- Netscape LDAP SDK implementira stariji "LDAPS" protokol, kao i gotovo sve ekstenzije LDAPv2 i LDAPv3 protokola.
- Za C API postoji dobra programerska dokumentacija i vodič

OpenLDAP developer stranice: **http://www.openldap.org/devel/**

Mozilla C SDK API: **http://www.mozilla.org/directory/csdk.html**
http://developer.netscape.com/tech/directory/

5.3 Python: python-ldap i ldaptor

- Najpopularniji python LDAP API, vrlo često korišten u web aplikacijama.
- python-ldap podržava LDAPv3, kao i većinu glavnih radnji u protokolu.
- HOWTO: http://linuxjournal.com/article.php?sid=6988&mode=thread&order=0

- ldaptor: alternativni LDAP python API
- Dolazi sa setom programa primjera
- Napisan u čistom pythonu
- API dokumentacija: http://tv.debian.net/software/ldaptor/api/

URL-ovi:

http://python-ldap.sourceforge.net/
http://tv.debian.net/software/ldaptor/

5.4 Java LDAP API implementacije

- Java Naming and Directory Interface (JNDI), core java paket ugrađen u novije verzije j2sdk i j2re (1.4.0, 1.4.1, 1.4.2). JNDI je generalni API za direktorijsko-hijerarhijske servise, ne samo za LDAP, već i za YP, NDS, DNS itd ...

`http://java.sun.com/products/jndi/`

- Mozilla/Netscape LDAP C SDK - baziran na istoimenom C SDK-u.

`http://www.mozilla.org/directory/javasdk.html`

- JLDAP - Novellov prilog OpenLDAP projektu

- J `http://developer.novell.com/ndk/` a programere koji već dobro poznaju JDBC tehnologiju. Prilog OctetString-a OpenLDAP projektu.

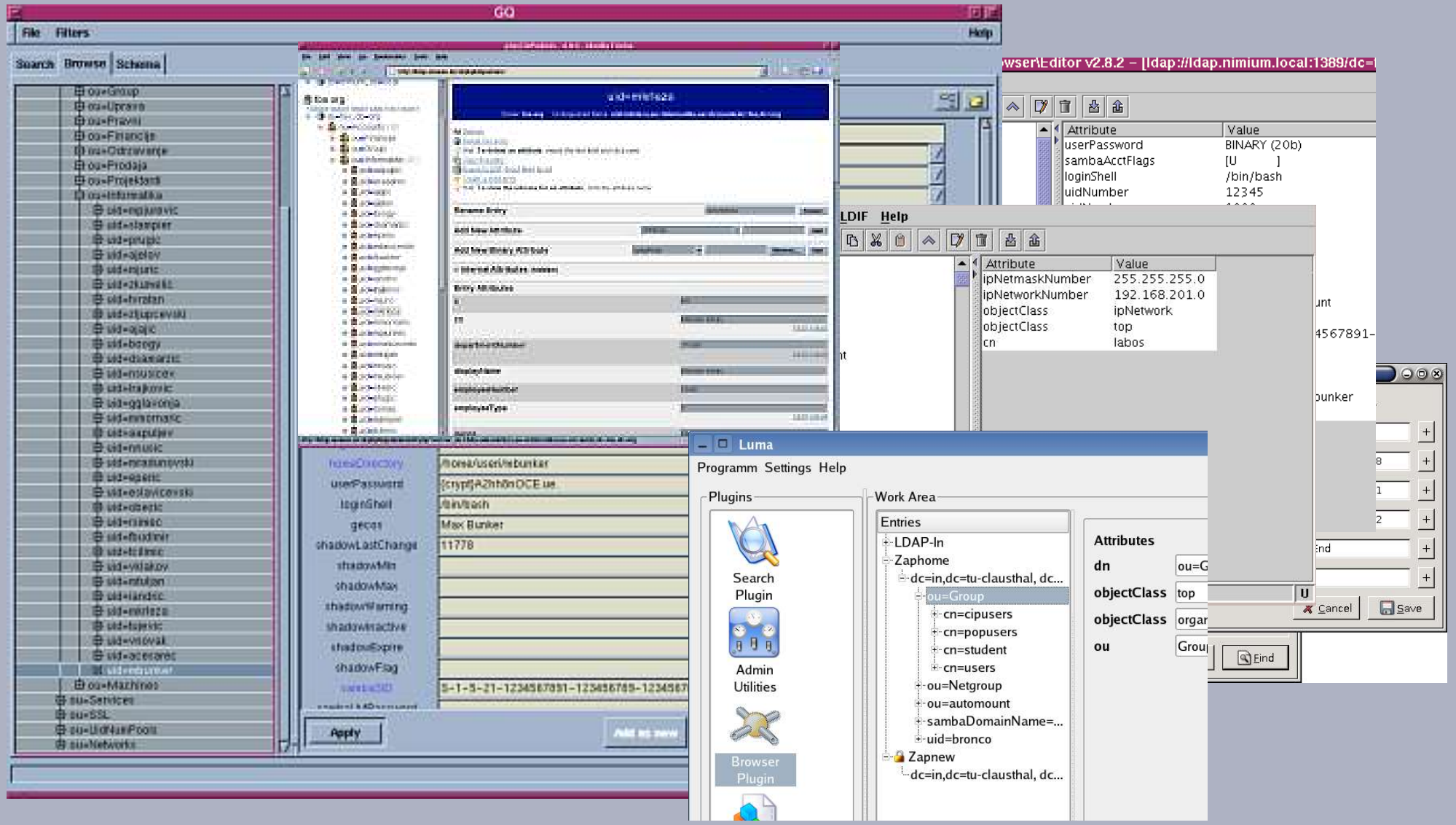
`http://www.octetstring.com/products/jdbcldapdriver/`

5.5 PHP

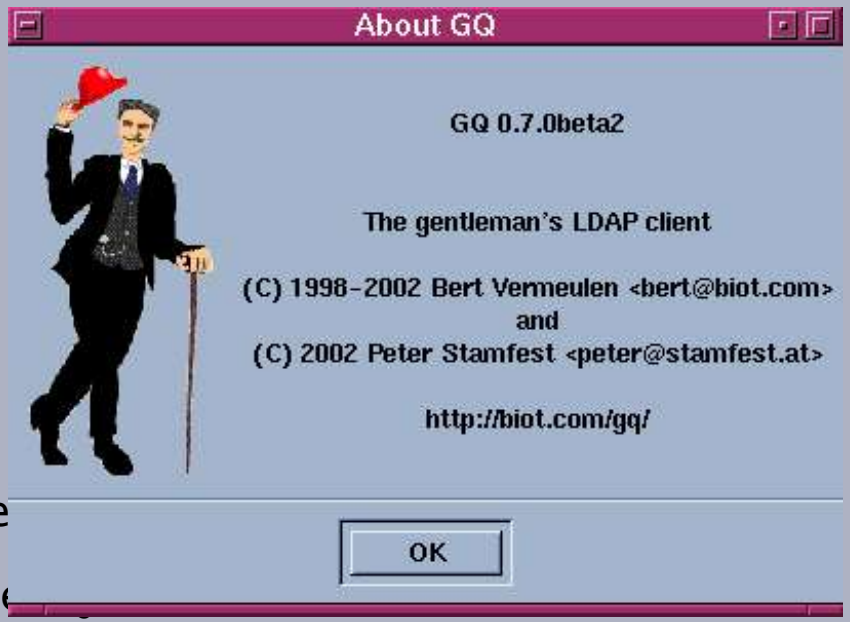
- PHP mora biti iskompiliran sa “--with-ldap” switchem, kako bismo dobili podršku sa LDAP. Za kompilaciju nam treba stari UoM API, Netscape SDK ili OpenLDAP API i njihovi dinamički ili statički libraryji.

```
Dokumentacija, uputstva i korisni linkovi:
http://www.php.net/ldap
```

6. Administracijski alati za LDAP i krajnje korisničke aplikacije koje ga direktno podržavaju



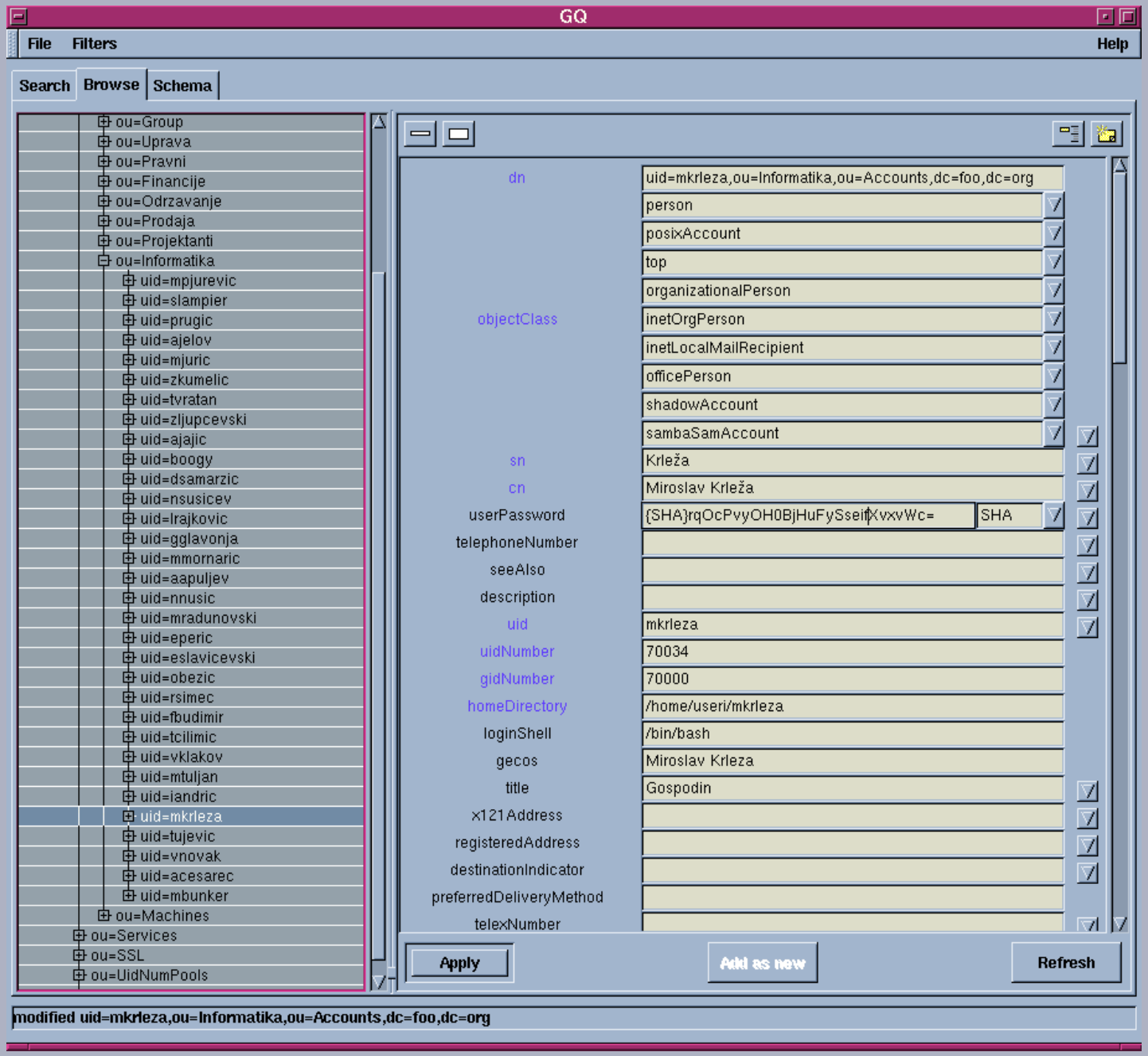
6.1 GQ



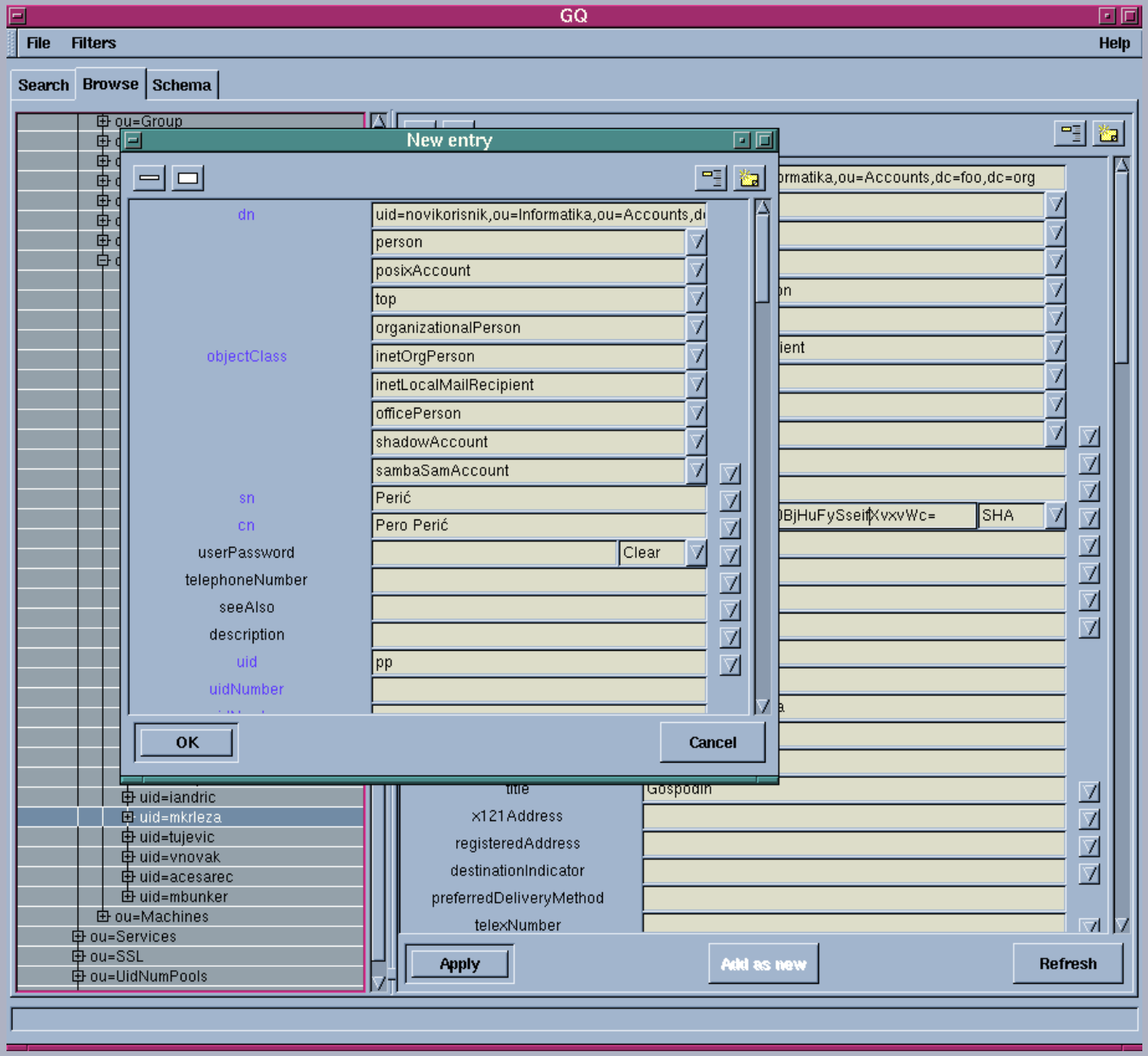
- GQ je popularan i vrlo praktičan GTK+ LDAP klijent.
- Brzina, pouzdanost i praktičnost - glavne odlike.
- Grafički LDAP browser
- LDAP V3 Schema browser
- Predlošci
- Eksport dijelova direktorija ili cijelog servera u ldif file
- Gotovo neograničen broj servera u konfiguraciji i kone
- Jednostavno i fleksibilno uređivanje, dodavanje i brisanje zapisa.
- Prikazuje slike, sadržaj X.509 certifikata i većinu binarnih atributa

WWW stranice:
`http://biot.com/gq`

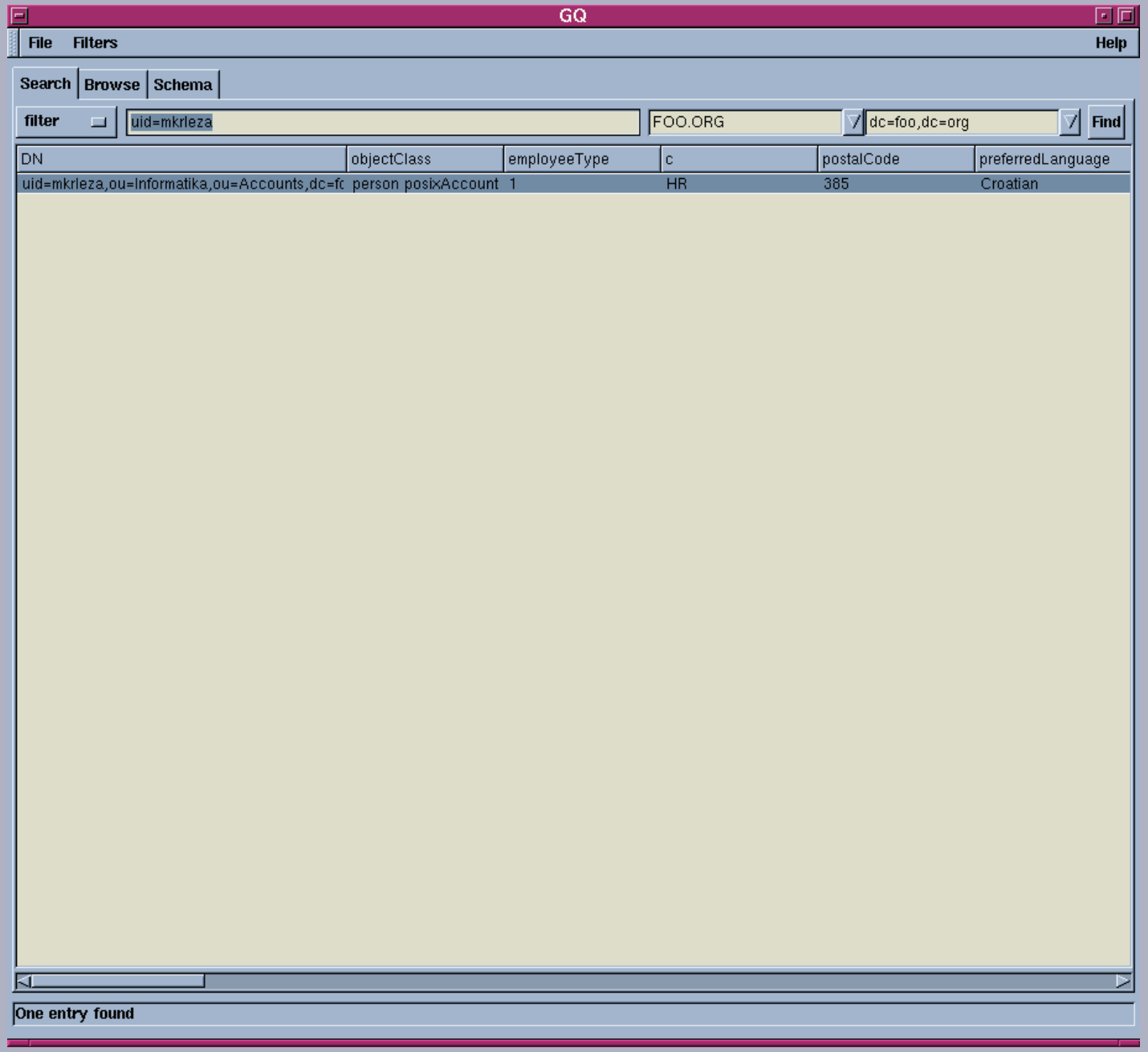
6.1 GQ – tab sa browserom (glavni tab)



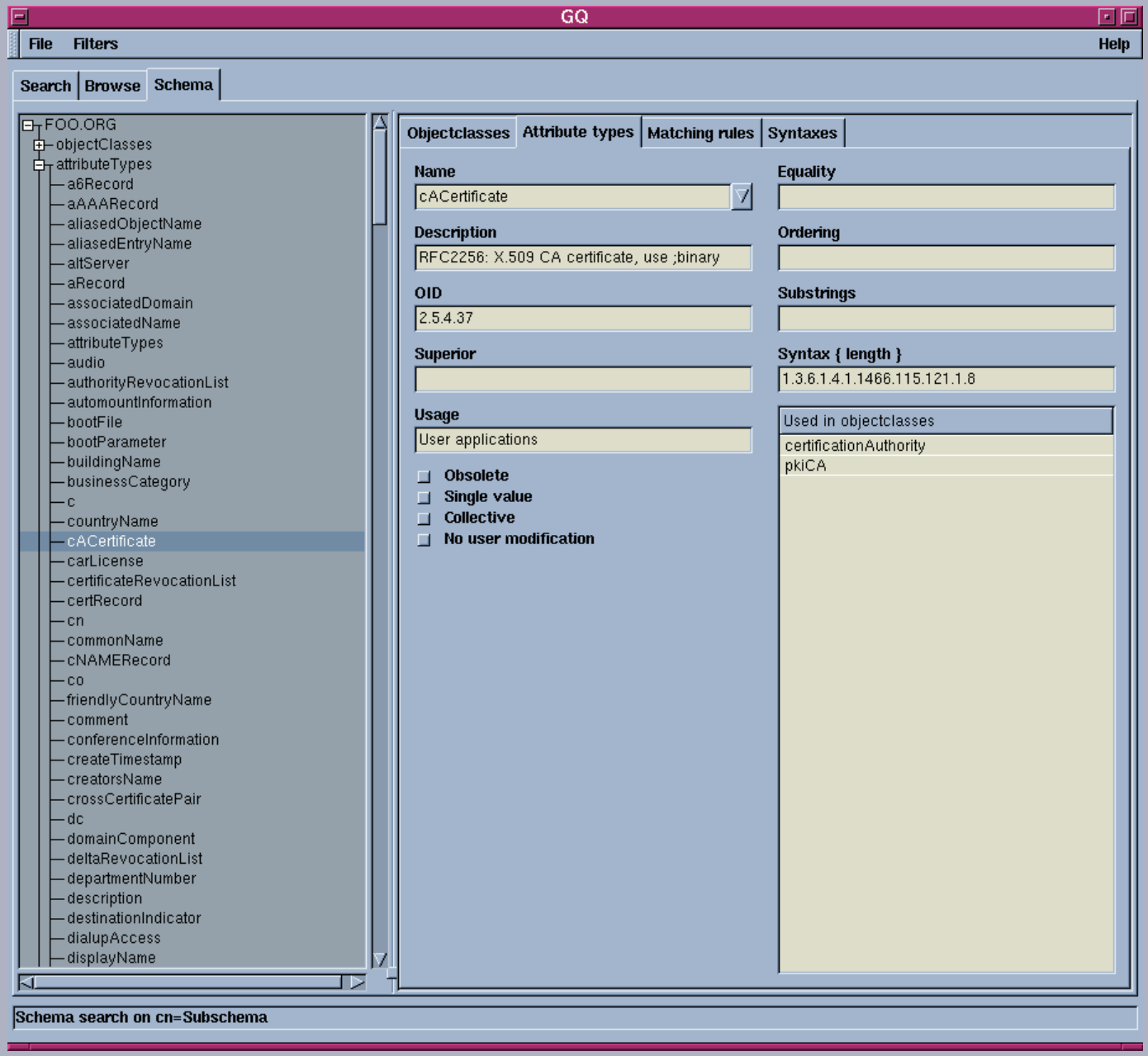
6.1 GQ – dodavanje novog zapisa (korisnika u ovom slučaju)



6.1 GQ – pretraga



6.1 GQ – pregled LDAP sheme

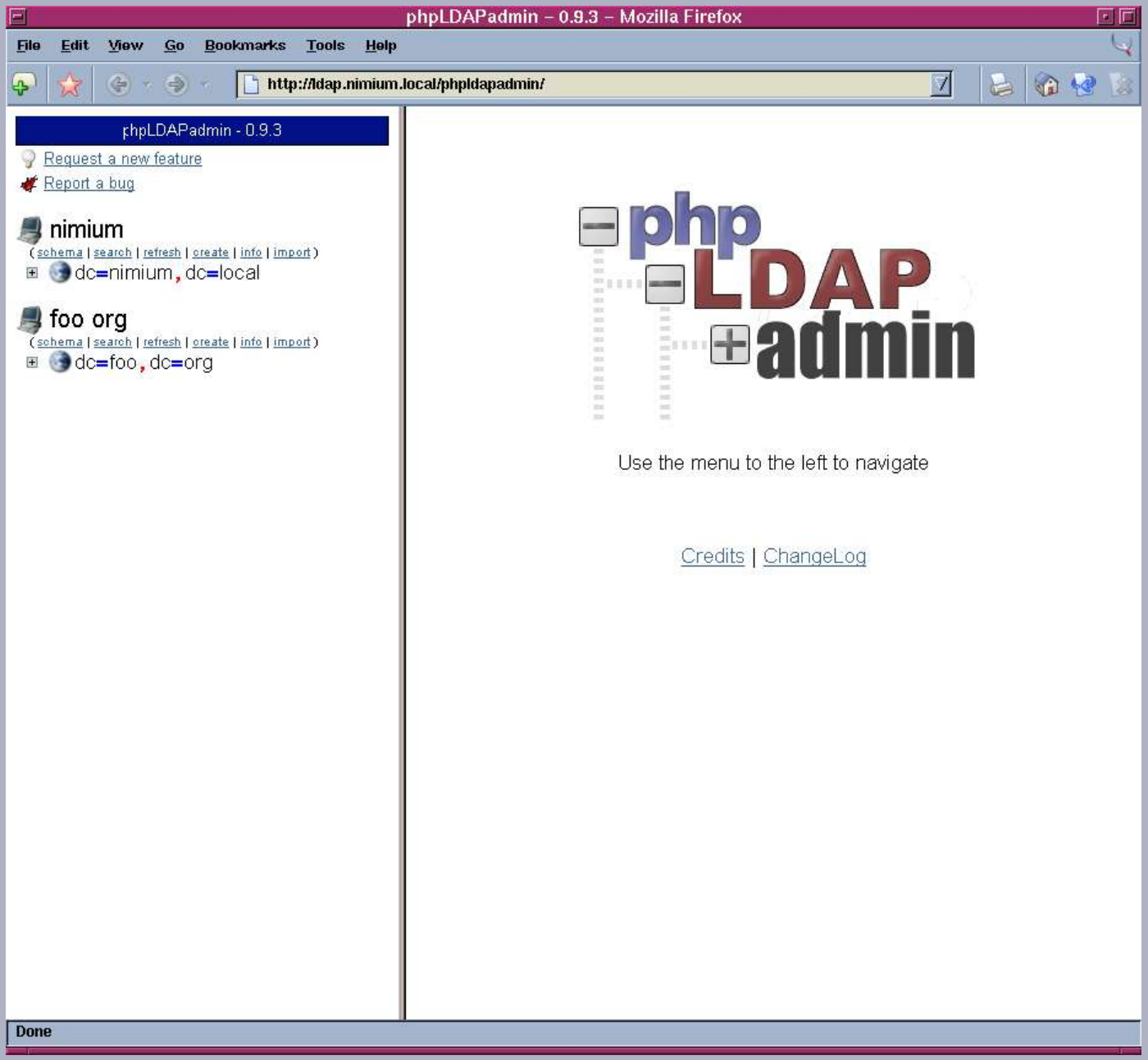


6.2 PHPLdapAdmin

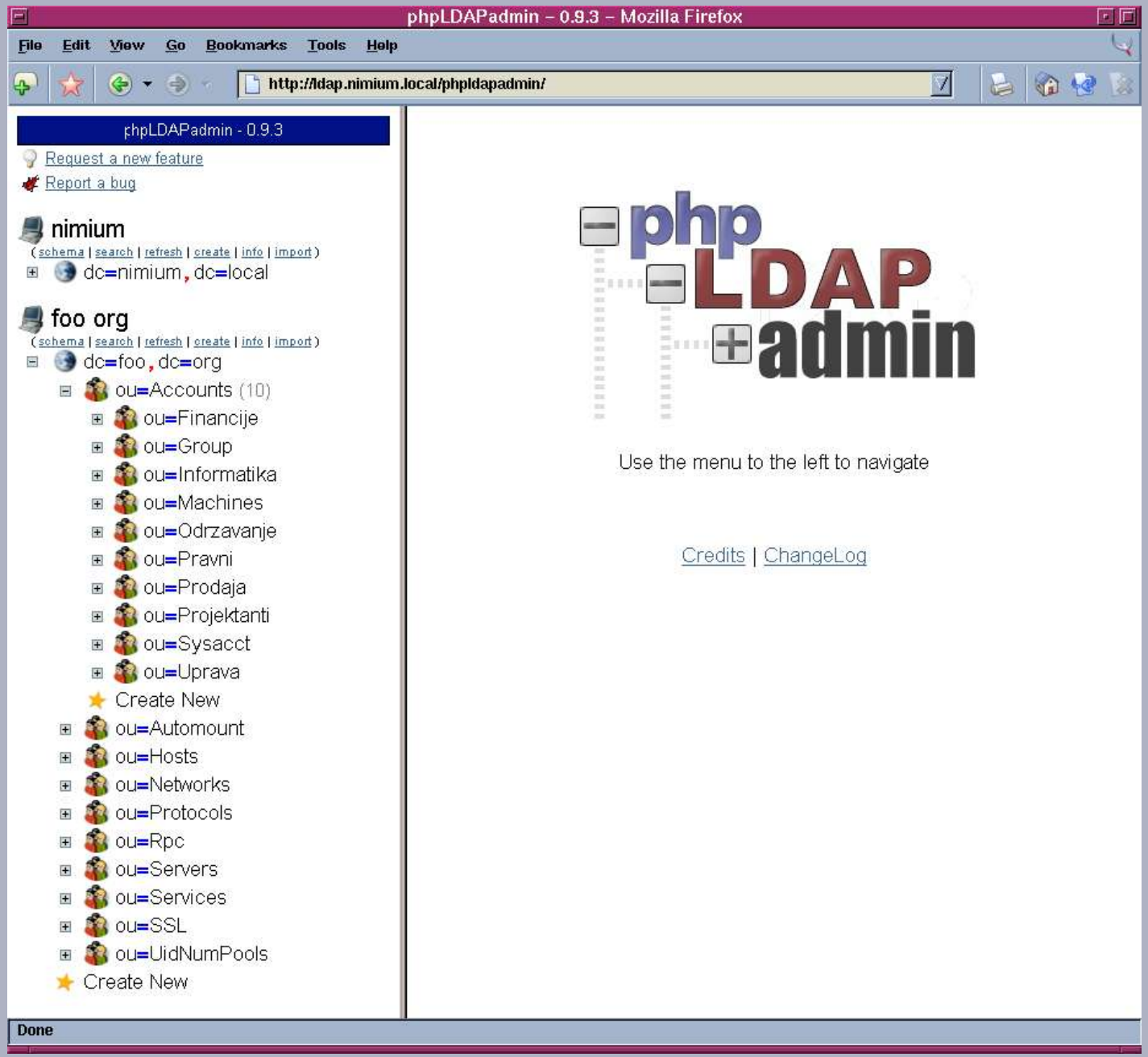
- PHP Ldap Admin (nekada se je zvao DaveDAP) je web-bazirani alat za administraciju LDAP-a napisan u PHP-u.
- Zahtjeva apache, PHP i LDAP PHP dinamički API modul.
- Ne zahtjeva lokalnu instalaciju, budući da se radi o web aplikaciji.
- Ugrađen LDAP shema preglednik
- Gotovi predlošci za najčešće korištene tipove zapisa
- Eksport pojedinih ili stabala zapisa kao tekst file u ldif formatu.
- Import podataka iz tekstualnog filea u ldif formatu.
- Dobra forma za napredno pretraživanje.

WWW stranice:
`http://phpldapadmin.sourceforge.net/`

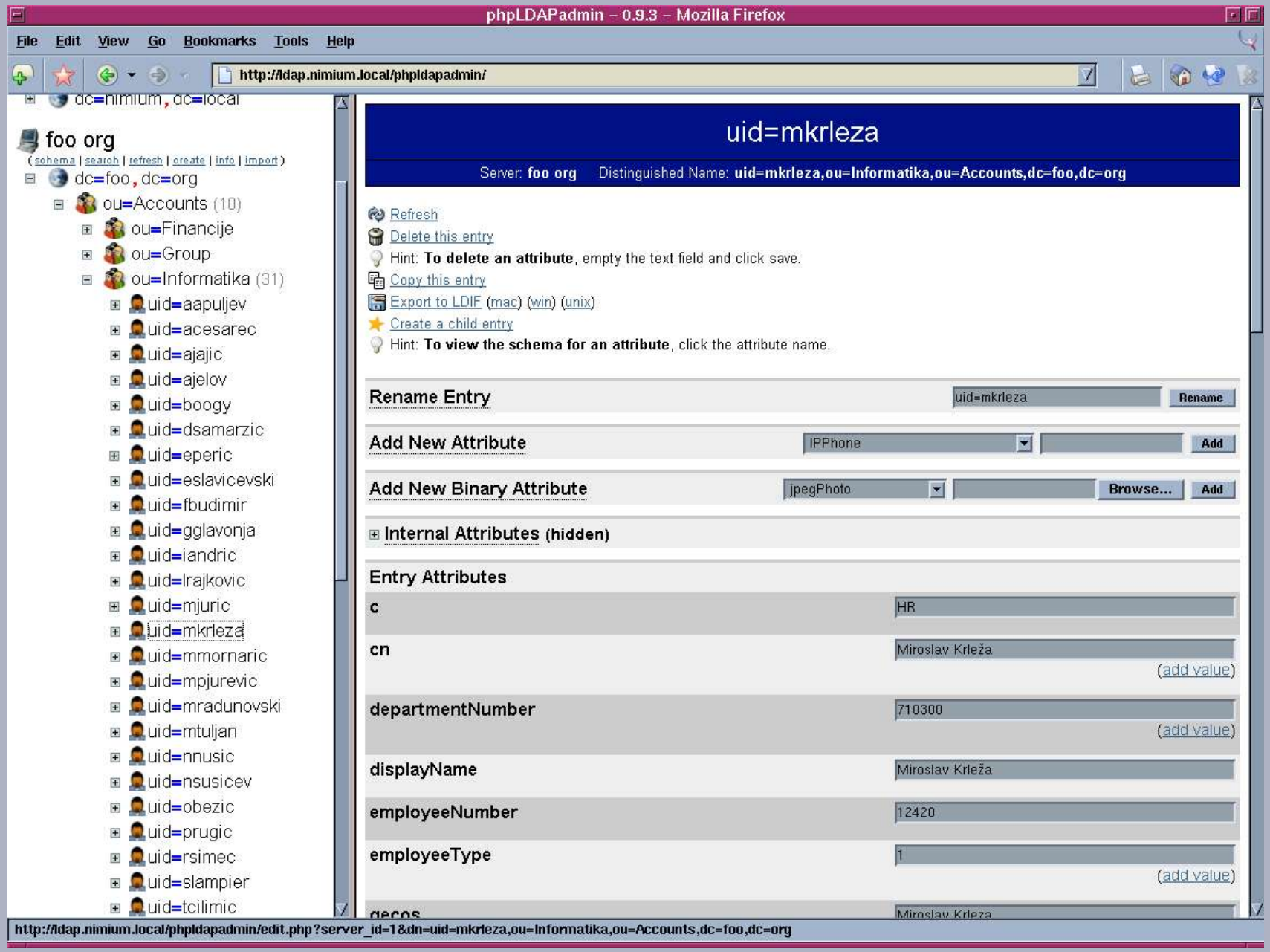
6.2 PHPLdapAdmin - početna stranica



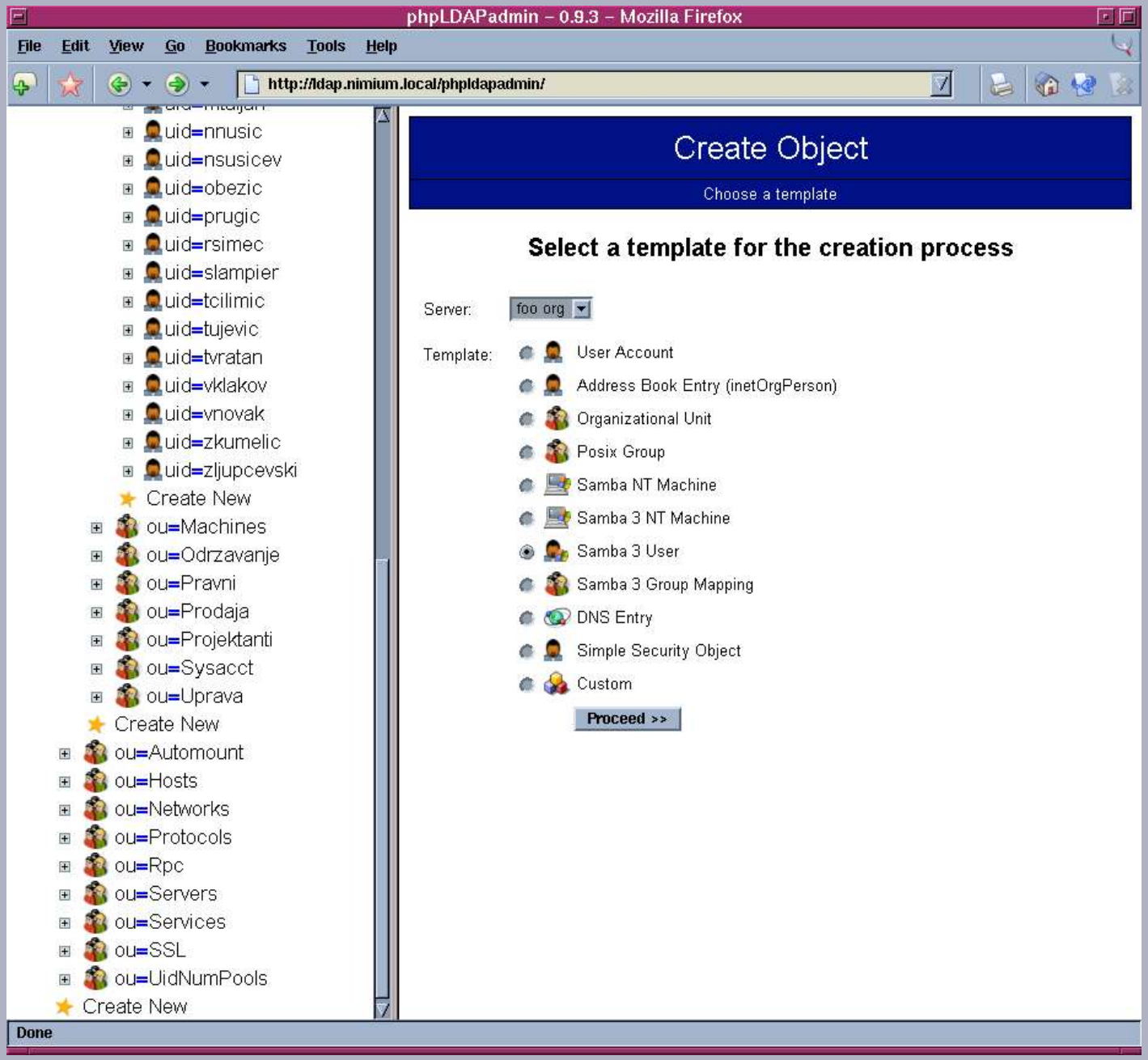
6.2 PHPLdapAdmin - directory browser



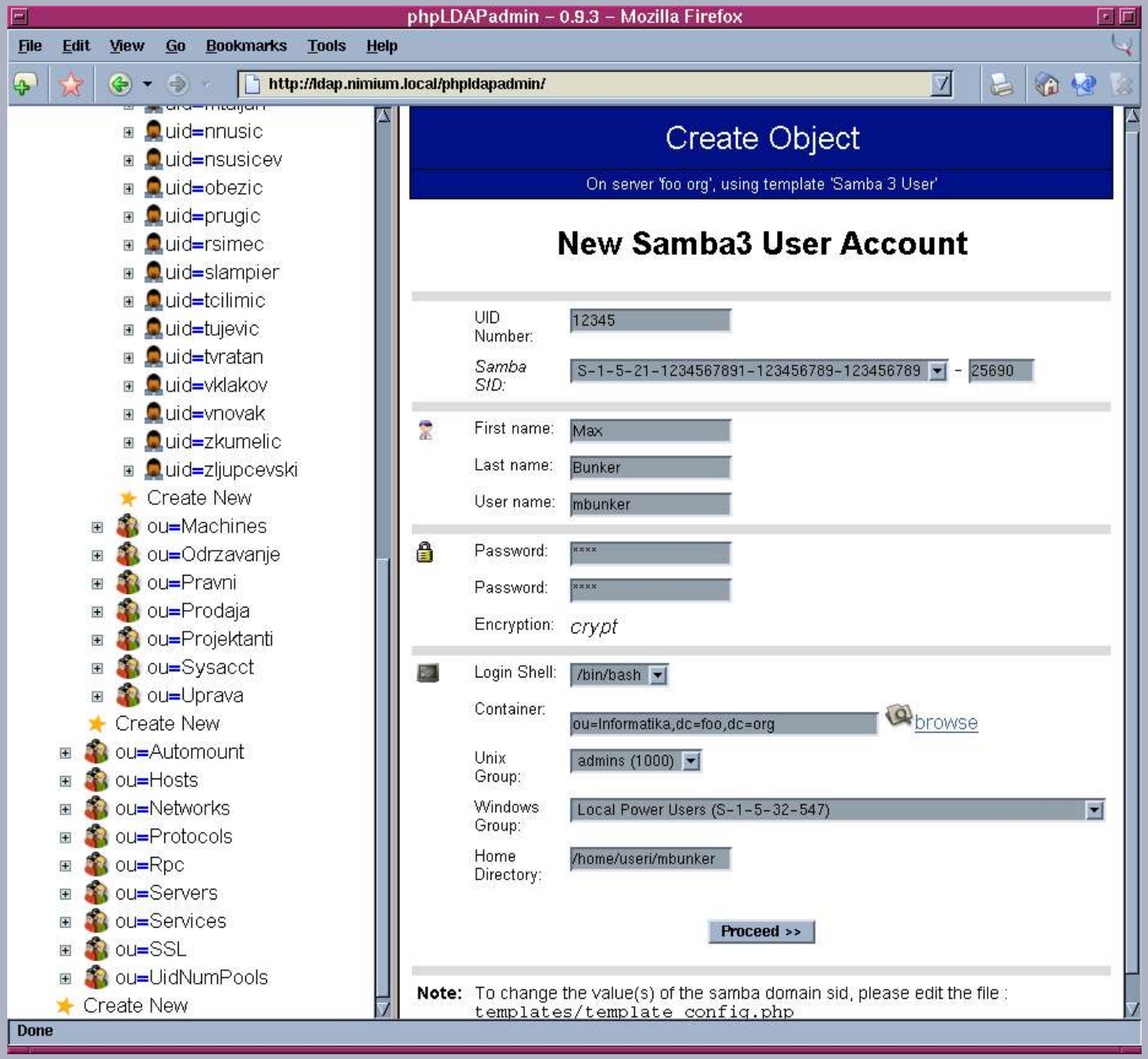
6.2 PHPLdapAdmin – uređivanje zapisa



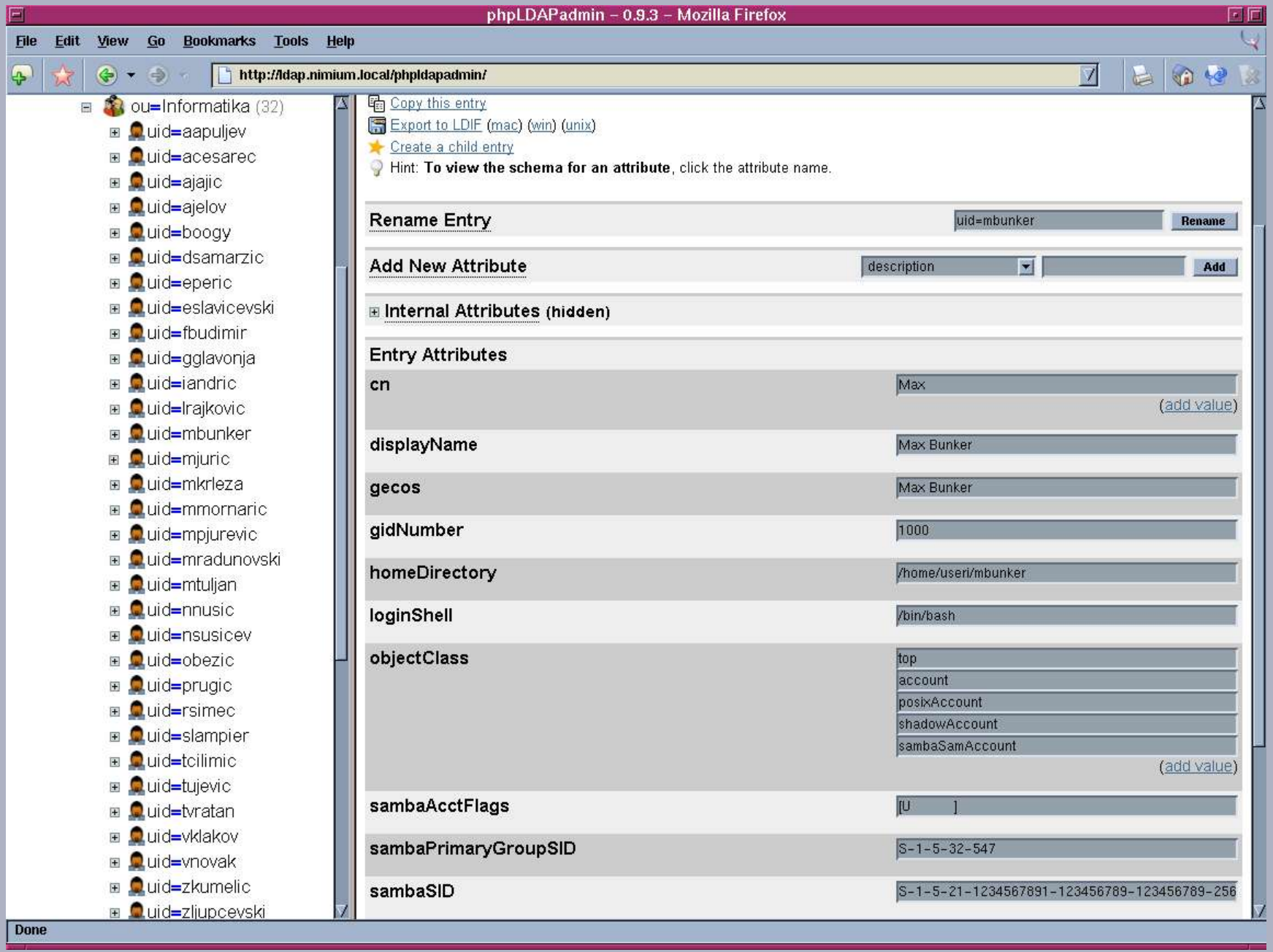
6.2 PHPLdapAdmin – predložak za dodavanje novih zapisa



6.2 PHPLdapAdmin – dodavanje novog zapisa (account)

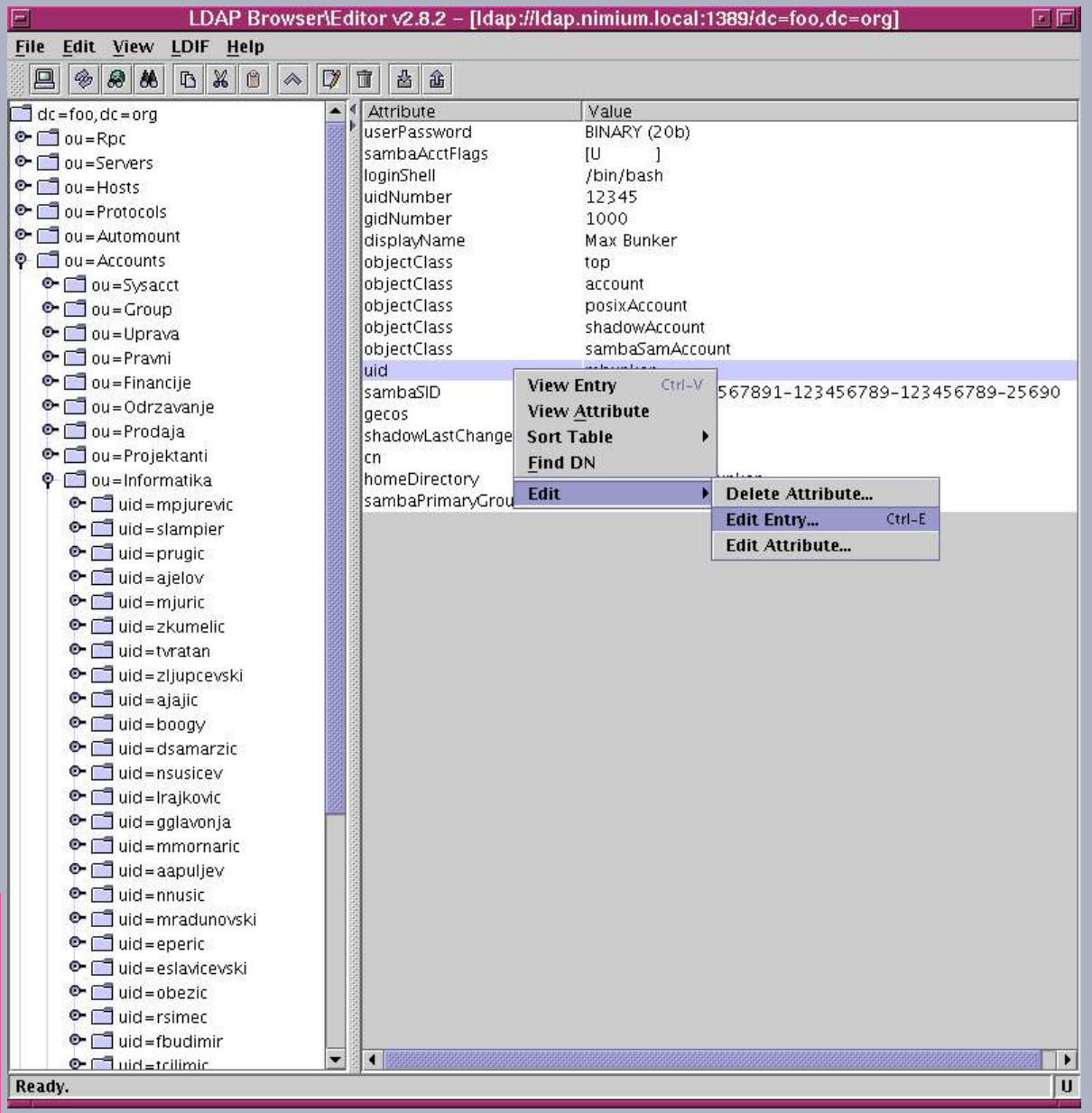


6.2 PHPLdapAdmin - pregled novog zapisa



6.3 Ostali alati: Ldap Browser/Editor

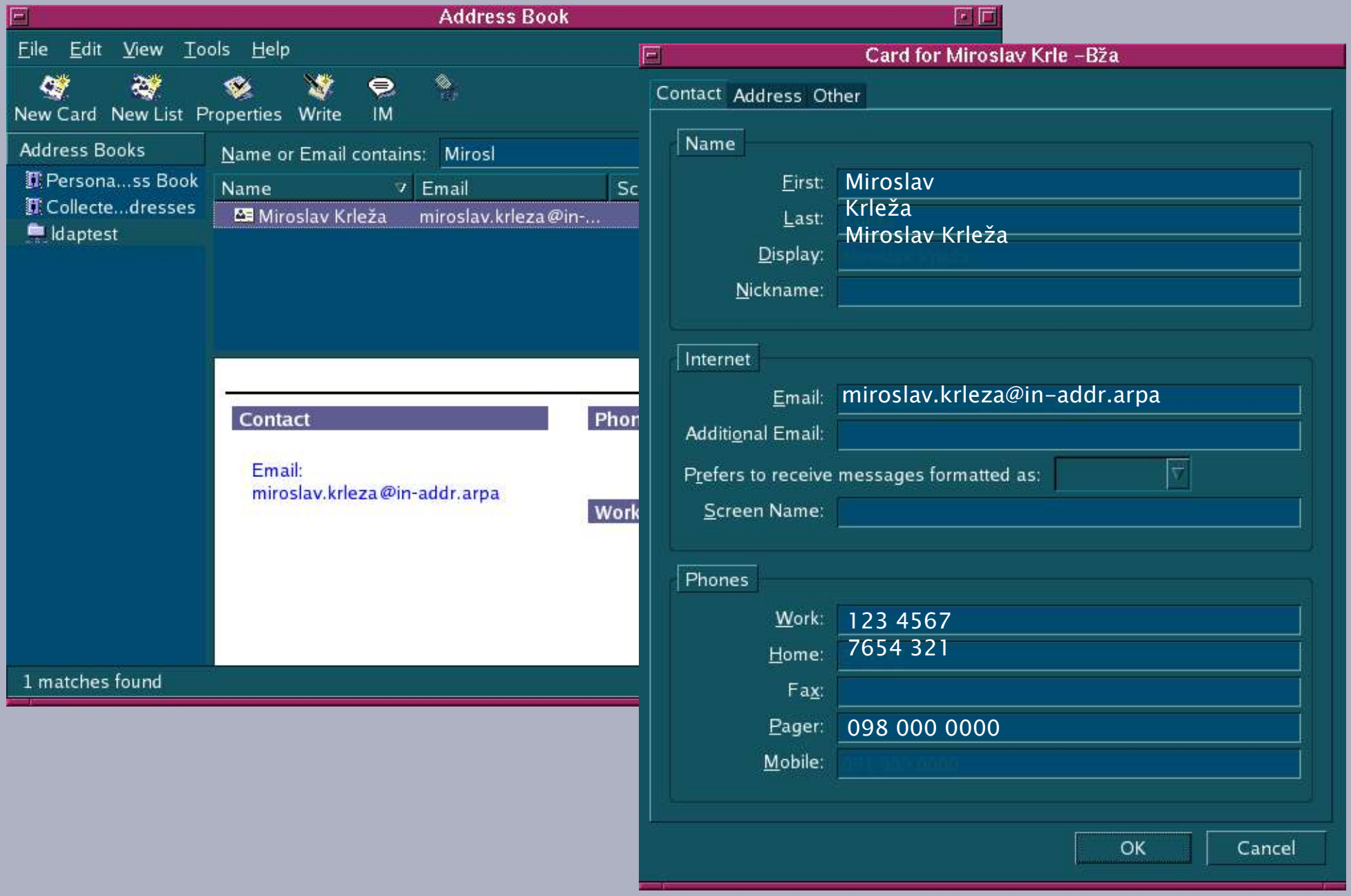
- Rad sa lokalnog diska ili iz browsera sa java pluginom - pisan u javi.
- Standardne mogućnosti pretraživanja dodavanja i modifikacije zapisa.
- Eksport i import zapisa iz ldif fileova
- Vrlo Dobar browser
- Nije free software (free only for educational use) :-(



WWW stranice:

`http://www.iit.edu/~gawojar/ldap/`

6.3 Korisnički LDAP klijenti: Mozilla addressbook



7. Linkovi na WWW

- DAP i X.500 Stranice:
http://www.surfnet.nl/innovatie/afgesloten/x500/introducing/
- Popis javnih LDAP servera: http://www.emailman.com/ldap/public.html
- Linux LDAP howto dokumentacija:
http://www.ibiblio.org/pub/Linux/docs/HOWTO/other-formats/html_single/LDAP-HOWTO.html
- Linux LDAP HOWTO koji opisuje integraciju sa servisima i implementaciju na sistemu:
http://www.ibiblio.org/pub/Linux/docs/HOWTO/other-formats/html_single/LDAP-Implementation-HOWTO.html
- Stranice sa puno korisnih LDAP linkova, specifikacijama, standardima, implementacijama primjerima ... http://www.kingsmountain.com/ldapRoadmap.shtml
- Mailing list softver koji adrese pretplatnika čita iz LDAP-a: http://listes.cru.fr/sympa/
- Još jedna stranica sa puno LDAP temetike i referenci: http://www.uwo.ca/its/projects/ldapurls.html

LDAP + Kerberos + SASL HOWTO (Debian orijentiran dokument, ali vrlo korisno štivo i za ostale)
http://www.bayour.com/LDAPv3-HOWTO.html

- Mapiranje LDAP atributa u windows/outlook adresaru: http://www.openldap.org/faq/data/cache/294.html

K R A J

(pitanja ?)