

Virtual LDAP

kako natjerati strgane
aplikacije da koriste LDAP

Dobrica Pavlinušić

<http://blog.rot13.org>

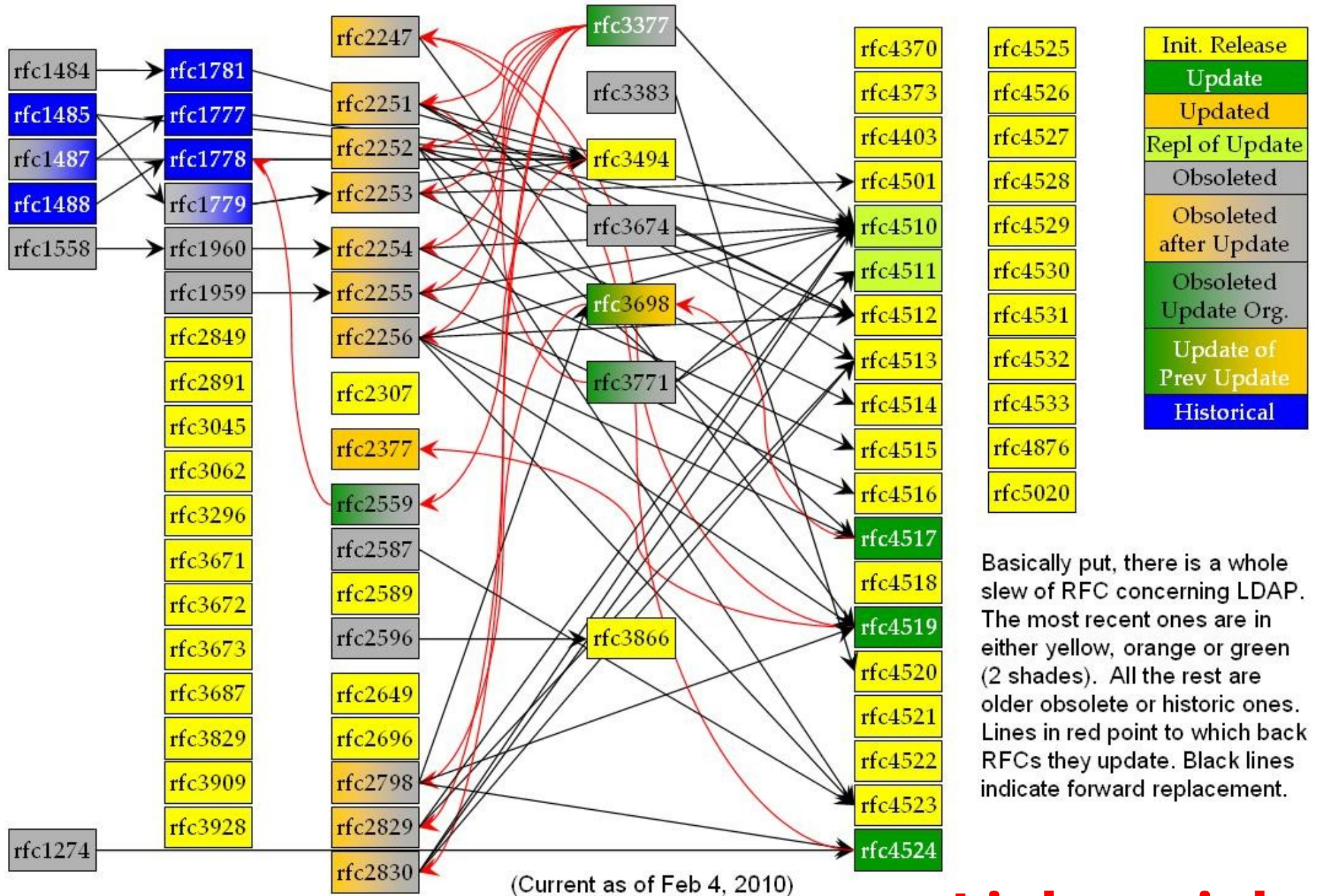
HULK, Knjižnica Filozofskog fakulteta u Zagrebu
DORS/CLUC, Zagreb, 6. svibnja 2010.

Zašto?

**Prijava u knjižnični sustav
(Koha) s LDAP računima,
kopiranje s RFID karticama**

Aplikacije imaju podršku za LDAP pa
nema problema, zar ne?

History of LDAP Related RFCs



Lightweight?

Lightweight Directory Access Protocol

- Fiksna shema
 - AAI@EduHr
- Stablata struktura
 - HrEduPerson  
 - passwords 
 - auth by bind
 - compare (prava na LDAP serveru)
 - Grupe
 - group
 - groupOfNames
 - groupOfUniqueNames

Povezati sustave

- **OpenLDAP**
 - ldap.ffzg.hr
 - AAI@EduHr schema
- **Koha**
 - Import korisnika
 - Logiranje sa LDAP lozinkom
 - Grupe korisnika
- **Referada**
 - CSV datoteka sa adresama
- **SAFEQ**
 - Import korisnika
 - Grupe korisnika iz Kohe

AAI@EduHr LDAP shema

<http://www.aaiedu.hr/>

dn:uid=kohatest,dc=ffzg,dc=hr

uid: kohatest
hrEduPersonUniqueNumber: LOCAL_NO: 1234kohatest
givenName: Koha
mail: knjiznica@ffzg.hr
hrEduPersonPrimaryAffiliation: student
hrEduPersonExpireDate: 20101031
o: Filozofski fakultet u Zagrebu
l: Zagreb
postalAddress: Filozofski fakultet u Zagrebu, Ivana
Lucica 3, HR-10000 Zagreb
hrEduPersonHomeOrg: ffzg.hr
hrEduPersonAffiliation: student
hrEduPersonUniqueID: kohatest@ffzg.hr
objectClass: hrEduPerson
sambaSamAccount
sambaSID: kohatest
userPassword: {SHA}
sambaLMPassword: HASH
sambaNTPassword: HASH
cn: Koha Testičić Probišić ĐŽ
sn: Testičić Probišić ĐŽ

LDAP konfiguracija aplikacija

- Koha
 - `sprintf` format za bind (%s)
 - Auth by bind
 - Mapiranje LDAP atributa u polja u bazi
 - Sva ponavljanja atributa se dobiju kao jedan string
- SAFEQ
 - pager LDAP atribut za RFID SID

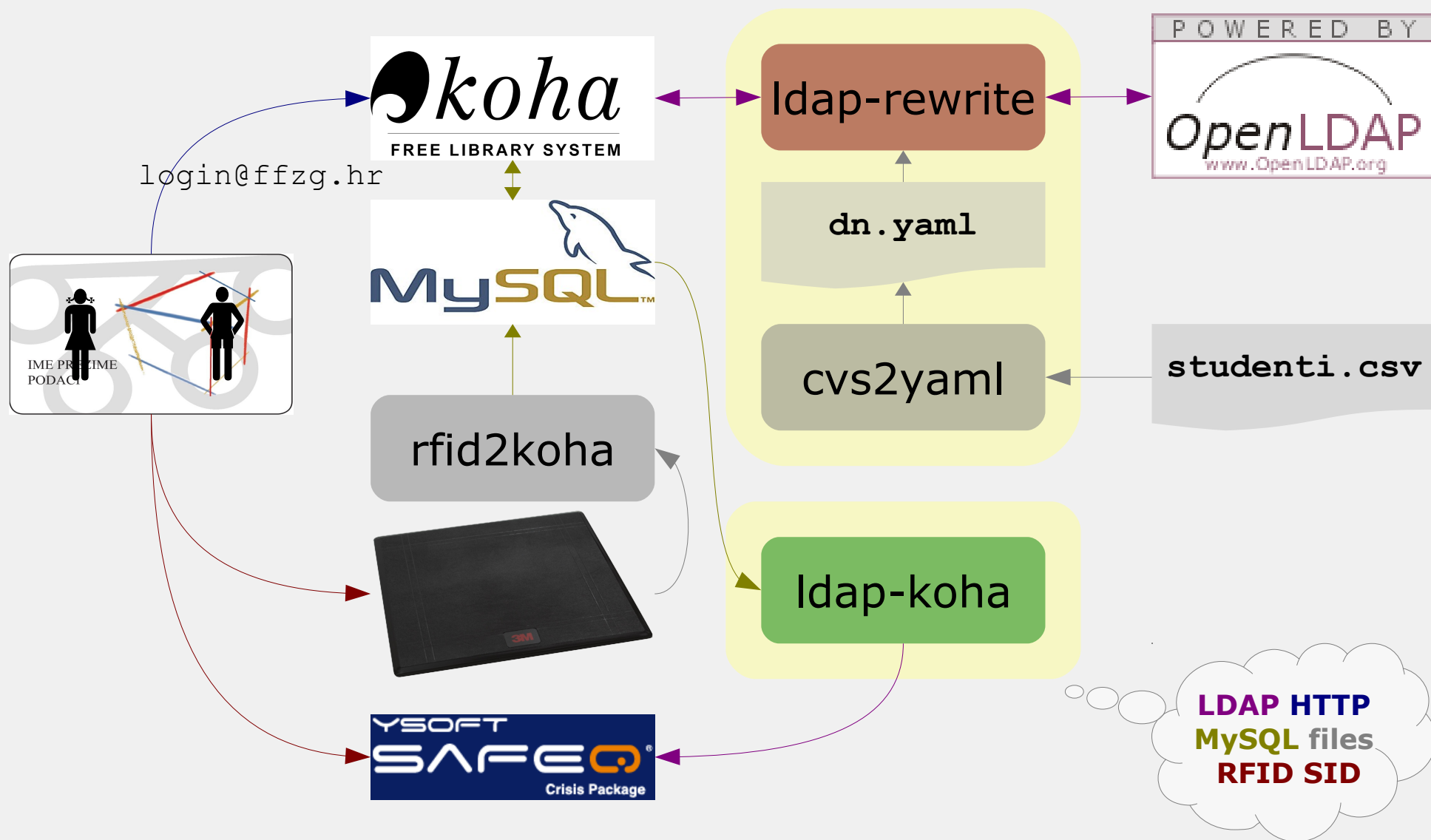
Naša knjižnica



Virtualno vješanje?

Kada bi smo barem mogli nekako utjecati na to kako ti sustavi pričaju LDAP-om jedan s drugim!

Virtual LDAP



ldap-rewrite

- Prepiši bind login (isti kao na web-u)
 - HrEduPersonUniqueID: dpavlin@ffzg.hr
 - bind DN: uid=dpavlin,dc=ffzg,dc=hr
- Dodaj search rezultatima LDAP servera podatke iz yaml datoteke korisnika
 - uid=login,dc=ffzg,dc=hr.yaml
- Dodatna polja za HrEduPersonUniqueNumber
 - HrEduPersonUniqueNumber JMBG:1234567890
 - HrEduPersonUniqueNumber_JMBG 1234567890
- SSL enkripcija do LDAP servera

studenti.csv

UTF-16 Windows CSV file

```
dn;jmbg;jmbag;prezime;ime;spol;datum_rodjenj  
a;mjesto_i_drzava_rodjenja;prebivaliste_drza  
va;prebivaliste_mjesto;prebivaliste_postansk  
i_broj;prebivaliste_zupanija;ml_telefoni;ml_  
email_adrese;ml_postanska_adresa  
uid=kohatest,dc=ffzg,dc=hr;3112999000000;012  
3456789;Koha;Test;Ž;1998-21-31;Zagreb #  
Hrvatska;HR;zagreb;10000;ZG;091/500-0000 #  
01/5000001;kohatext@example.com;Ulica 42#  
Zagreb
```

csv2yaml

- Ponavljajuće vrijednosti odvojene sa #
- Odrola ponavljanja u nove elemente:
 - address [street, city]
 - address_0 street
 - address_1 city
- spol u M/F
- Kategorizira telefone u:
 - tel_fixed
 - tel_mobile

uid=kohatest,dc=ffzg,dc=hr.yaml

```
---
dn: uid=kohatest,dc=ffzg,dc=hr
ime: Test
jmbag: 0123456789
jmbg: 3112999000000
mjesto_i_drzava_rodjenja:
  - Zagreb
  - Hrvatska
mjesto_i_drzava_rodjenja_0: Zagreb
mjesto_i_drzava_rodjenja_1: Hrvatska
ml_email_adrese: kohatest@example.com
ml_postanska_adresa:
  - Ulica 42
  - Zagreb
ml_postanska_adresa_0: Ulica 42
ml_postanska_adresa_1: Zagreb
ml_telefoni:
  - 091/500-0000
  - 01/5000001
ml_telefoni_0: 091/500-0000
ml_telefoni_1: 01/5000001
ml_telefoni_fixed: 01/5000001
ml_telefoni_mobile: 091/500-0000
prebivaliste_drzava: HR
prebivaliste_mjesto: zagreb
prebivaliste_postanski_broj: 10000
prebivaliste_zupanija: ZG
prezime: Koha
spol: F

dn: uid=kohatest,dc=ffzg,dc=hr
hrEduPersonUniqueNumber: LOCAL_NO: 1234kohatest
givenName: Koha
mail: knjiznica@ffzg.hr
hrEduPersonPrimaryAffiliation: student
hrEduPersonExpireDate: 20101031
o: Filozofski fakultet u Zagrebu
l: Zagreb
postalAddress: Filozofski fakultet u Zagrebu, Ivana Lucica 3, HR-10000
Zagreb
hrEduPersonHomeOrg: ffzg.hr
hrEduPersonAffiliation: student
hrEduPersonUniqueID: kohatest@ffzg.hr
objectClass: hrEduPerson
sambaSamAccount
sambaSID: kohatest
userPassword: {SHA}0qTS06yhQv2Dqwuk0CaGsKWxqwo=
sambaLMPassword: 942FC74155F6172A613E9293942509F0
sambaNTPassword: 0C967E5AA27696638F85FBF1BA8F73A1
cn: Koha Testićić Probišić Đž
sn: Testićić Probišić Đž
hrEduPersonUniqueNumber_LOCAL_NO: 1234kohatest
ffzg-prebivaliste_postanski_broj: 10000
ffzg-ml_postanska_adresa_1: Zagreb
ffzg-ml_postanska_adresa_0: Ulica 42
ffzg-mjesto_i_drzava_rodjenja_0: Zagreb
ffzg-ml_telefoni_fixed: 01/5000001
ffzg-ml_telefoni: 091/500-0000
01/5000001
ffzg-datum_rodjenja: 1998-21-31
ffzg-prezime: Koha
ffzg-prebivaliste_zupanija: ZG
ffzg-spol: F
ffzg-ml_telefoni_mobile: 091/500-0000
ffzg-jmbg: 3112999000000
ffzg-ime: Test
ffzg-mjesto_i_drzava_rodjenja_1: Hrvatska
ffzg-prebivaliste_drzava: HR
ffzg-mjesto_i_drzava_rodjenja: Zagreb
Hrvatska
ffzg-ml_telefoni_0: 091/500-0000
ffzg-ml_postanska_adresa: Ulica 42
Zagreb
ffzg-ml_telefoni_1: 01/5000001
ffzg-ml_email_adrese: kohatest@example.com
ffzg-jmbag: 0123456789
ffzg-prebivaliste_mjesto: zagreb
ffzg-dn: uid=kohatest,dc=ffzg,dc=hr
```

Uf, a kopirke?



ldap-koha

- LDAP server koji koristi Koha MySQL bazu
- RFID SID kao LDAP filter 
 - pager=E00401001F77E218
- SQL datoteka za objectClass 
 - sql/hreduperson.sql
 - sql/organizationalunit.sql
 - sql/group.sql
- pretvara LDAP filter u SQL where 
- Grupe korisnika iz Kohe 
 - Različita prava korištenja kopirki

Zašto testirati?

- bind & search testovi
 - **BUG: ldap-rewrite konekcije na LDAP server** (nakon godinu dana u produkciji)
- Integracija sa Kohom
 - Obriši testnog korisnika
 - Ulogiraj korisnika
 - **BUG: Koha ne radi u kombinaciji auth by bind i replikacije** (bugs.koha.org#4256)

```
dpavlin@koha:/srv/virtual-ldap$ wc -c t/*.t t/koha/*.t
1216 t/ldap-koha.t
1055 t/ldap-rewrite.t
 737 t/koha/01-remove-test-user.t
 769 t/koha/02-create-test-user.t
3777 total
```

Više informacija

- Virtual LDAP project
 - <https://www.ohloh.net/p/virtual-ldap>
- Source code
 - <http://svn.rot13.org/index.cgi/virtual-ldap/>
- Blog 
 - <http://blog.rot13.org/>
 - Tagovi: Virtual-LDAP, ldap

Pitanja?
42