Sveučilište u Zagrebu
Sveučilišni računski centar

Hrvatska akademska i istraživačka mreža

PROJEKT USPOSTAVE
AUTENTIKACIJSKE I AUTORIZACIJSKE INFRASTRUKTURE (AAI)
U SUSTAVU ZNANOSTI I VISOKOG OBRAZOVANJA

UPUTE ZA MIGRACIJU LDAP IMENIKA USTANOVA NA HREDU IMENIČKU SHEMU

(proizvod AAI.5.2)

- (ver.1.0.) -

Zagreb, listopad 2005.

http://www.aaiedu.hr

aai@EduHr.5.2.-ver1.0.doc - 14.04.2005. – 10 str.

Projekt AAI@EduHr

Oznaka proizvoda AAI.5.2

Naziv dokumenta: Upute za migraciju LDAP imenika na HrEdu imeničku shemu

Verzija i status: ver.1.0 / listopad 2005.

Naziv datoteke: aai@EduHr.5.2.-ver1.0.doc

URL adresa dokumenta: http://www.aaiedu.hr/docs/ aai@EduHr.5.2.-ver1.0.pdf

Dokument priredio: Dubravko Vončina

U izradi sudjelovali: Miroslav Milinović, Mijo Đerek, Dubravko Penezić

Ovaj je dokument rezultat rada na projektu *Uspostava autentikacijske i autorizacijske infrastrukture (AAI) u sustavu znanosti i visokog obrazovanja* čije je izvođenje Ministarstvo znanosti, obrazovanja i športa ugovorilo sa Sveučilišnim računskim centrom Sveučilišta u Zagrebu i Hrvatskom akademskom i istraživačkom mrežom – CARNet.

SADRŽAJ

1. Uvod

Ovaj dokument je prije svega namijenjen osobama zaduženim za održavanje postojećih LDAP poslužitelja i administriranje podataka o korisnicima u LDAP imenicima ustanova. Svrha ovog dokumenta je omogućiti bolji uvid u najznačajnije promjene koje će nastupiti prelaskom na HrEduPerson imeničku shemu te dati osnovne upute za migraciju podataka iz postojećih LDAP imenika ustanova (koji od 2003. godine uglavnom koriste CMU imeničku shemu) na hrEduPerson imeničku shemu.

U drugom poglavlju ovog dokumenta navedene su najznačajnije promjene vezane uz sadržaj LDAP imenika i način rada pojedinih servisa koje će nastupiti uvođenjem hrEduPerson imeničke sheme.

U trećem poglavlju opisano je na koji način će se vršiti prilagodba korisničkih podataka prilikom tranzicije iz postojećeg LDAP imenika s CMU shemom u LDAP imenik s hrEduPerson shemom.

U četvrtom poglavlju u osnovnim crtama je opisana procedura migracije postojećih LDAP imenika ustanova na HrEduPerson imeničku shemu.

Dodatne informacije vezane uz sadržaj hrEduPerson imeničke sheme, instalaciju LDAP poslužitelja i održavanje LDAP imenika s hrEduPerson imeničkom shemom možete pronaći na web stranici http://www.aaiedu.hr kao i u referencama navedenim na kraju ovog dokumenta.

U slučaju bilo kakvih pitanja ili problema vezanih uz migraciju LDAP imenika na hrEduPerson imeničku shemu, instalaciju LDAP poslužitelja s hrEduPerson imeničkom shemom ili importiranja podataka o korisnicima u LDAP imenik, ustanove mogu kontaktirati AAI@EduHr tim slanjem maila na adresu:

team@aaiedu.hr

2. Najvažnije promjene

Prelaskom na hrEduPerson imeničku shemu doći će do značajnih promjena u sadržaju LDAP imenika ustanova, a promjene u sadržaju LDAP imenika uzrokovat će i promjene u načinu rada pojedinih servisa koji za svoj rad koriste podatke iz LDAP imenika ustanova.

Najvažnije promjene vezane uz HrEduPerson imeničku shemu su:

- hrEduPerson imenička shema zahtjeva unos dodatnih podataka o korisnicima koji ne postoje (ili se nisu morali unositi) u LDAP imeniku s CMU shemom. Popis atributa koje je za svakog korisnika potrebno obavezno unijeti u LDAP imenik s hrEduPerson shemom naveden je u definiciji hrEdu imeničkih shema [1].

- U LDAP imeniku s HrEduPerson imeničkom shemom kategorizacija korisnika radi se prema šifarnicima navedenim u [1]. Servisi CARNeta, Srca i MZOŠ-a koji koriste podatke iz LDAP ustanova imenika bit će prilagođeni tako da koriste kategorizaciju korisnika sukladno hrEduPerson imeničkoj shemi.

- Radi usklađivanja s postojećim europskim standardima, prelaskom na HrEduPerson imeničku shemu prilikom interinstitucionalne autentikacije (primjerice prilikom spajanja na CARNetove modemske ulaze, spajanja na Internet u studentskim domovima itd.) umjesto trenutno aktualnih korisničkih oznaka oblika korisnik.domena_ustanove, korisničke oznake poprimit će oblik:

  korisnik@oznaka_ustanove

  Tako će primjerice postojeća korisnička oznaka *pero.fesb* poprimiti oblik *pero@fesb.hr* .

  Po završetku migracije korisnici trebaju koristiti novi oblik korisničke oznake.

- Nakon razdoblja migracije postojeći servisi CARNeta, Srca i MZOŠ-a koji za autentikaciju i autorizaciju korisnika koriste podatke iz LDAP imenika ustanova koristit će isključivo podatke iz imenika s HrEduPerson shemom.

Zbog prethodno navedenih promjena podaci o korisnicima ne mogu se izravno iskopirati iz LDAP imenika s CMU shemom u LDAP imenik s hrEduPerson shemom vać ih je prije importiranja potrebno prilagoditi i nadopuniti podacima iz drugih izvora. Da bi migracija uspješno protekla, prije početka migracije ustanove moraju osigurati minimalan set obveznih podataka o svakom korisniku potreban za unos korisnika u LDAP imenik s hrEduPerson imeničkom shemom.

3. Dohvaćanje svih potrebnih podataka

3.1. Potrebni podaci

Proces prebacivanja podataka iz LDAP imenika s CMU shemom u LDAP imenik s hrEduPerson shemom AAI tim nastojat će maksimalno automatizirati. Obzirom da HrEduPerson imenička shema za svakog korisnika zahtjeva unos više podataka nego što ih ima u LDAP imenicima s CMU shemom, preostali potrebni podaci o korisnicima mogu se dohvaćati i iz ovih izvora:

- Informacijski sustav visokih učilišta (ISVU)
- Informacijski sustav studentske prehrane (ISSP)

Da bi se proces migracije podataka iz postojećeg LDAP imenika u LDAP imenik s hrEduPerson shemom mogao automatizirati, uoči migracije ustanova treba na adresu team@aaiedu.hr poslati:

- LDIF datoteku s ažurnim podacima o korisnicima pohranjenim u LDAP imeniku ustanove
- za one korisnike čiji podaci se ne budu mogli dohvatiti iz gore navedenih izvora, ustanova mora AAI@EduHr timu dostaviti datoteku sa svim preostalim potrebnim podacima u čitljivom obliku (tekstualna datoteka, Excel tablica...) i precizno definiranim formatom zapisa.

3.2. Konverzija atributa

Prilikom prebacivanja korisničkih podataka iz LDAP imenika s CMU shemom u LDAP imenik s hrEduPerson shemom bit će napravljeno preslikavanje pojedinih atributa. Sljedeća tablica prikazuje način preslikavanja pojedinih atributa:

hrEduPerson shema	CMU shema	Napomena
HrEduPersonUniqueID	CARNetuniqueName	prilikom konverzije atributa točka će biti zamijenjena znakom @
HrEduPersonUniqueNumber	-	ovaj atribut postaje obavezan i ustanova mora osigurati ovaj podatak za sve korisnike koji se nalaze u njenom LDAP imeniku (minimalno treba osigurati lokalno važeći identifikator (prefiks LOCAL_NO u shemi) poput broja indeksa za studente)
uid	uid	-
userPassword	userPassword	-
givenName	-	inicijalno će biti kreiran kao razlika atributa *cn* i *sn*
mail	mail	ovaj atribut postaje obavezan i ustanova mora osigurati ovaj podatak za sve korisnike koji se nalaze u njenom LDAP imeniku
hrEduPersonPrimaryAffiliation	CMUstatID	bit će napravljeno preslikavanje prema tablici 2
hrEduPersonAffiliation	CMUstatID	bit će napravljeno preslikavanje prema tablici 2

Tablica 1: Konverzija pojedinih atributa prilikom prebacivanja s CMU na hrEduPerson imeničku shemu

Kao što se vidi iz Tablice 1., za svakog će korisnika *uid* (identifikator korisnika u ustanovi) i zaporka u LDAP imeniku ostati nepromijenjeni.

Važno je naglasiti da e-mail adresa korisnika u hrEduPerson imeničkoj shemi postaje obavezna. Dakle, u LDAP imeniku s hrEduPerson shemom svaki korisnik mora imati upisanu (važeću) e-mail adresu.

Također, bit će napravljena konverzija atributa *CMUstatID* u atribute *hrEduPersonPrimaryAffiliation* i *hrEduPersonAffiliaton* na način prikazan u sljedećoj tablici

Shema:	**CMU**	**hrEduPerson**	
Naziv atributa:	**CMUstatID**	**hrEduPersonPrimaryAffiliation**	**hrEduPersonAffiliation**
Vrijednost atributa:	A	djelatnik	djelatnik
	B	djelatnik	djelatnik
	C	djelatnik	djelatnik
	D	djelatnik	djelatnik
	E	vanjski suradnik	vanjski suradnik
	F	student	student
	G	djelatnik	djelatnik
	H	učenik	učenik
	I	korisnik usluge	korisnik usluge
	J	korisnik usluge	korisnik usluge

Tablica 2: Konverzija atributa CMUstatID u atribute hrEduPersonPrimaryAffiliation i hrEduPersonAffiliation

Prilikom automatske konverzije vrijednost atributa *hrEduPersonAffiliation* inicijalno će biti postavljena tako da bude jednaka vrijednosti atributa *hrEduPersonPrimaryAffiliation*, a ustanova može naknadno promijeniti vrijednosti tih atributa za pojedine korisnike.

4. Migracija LDAP imenika na HrEdu imeničku shemu

4.1. Pripreme uoči migracije

Da bi se izbjegli potencijalni problemi tijekom migracije podataka iz LDAP imenika s CMU shemom u LDAP imenik s hrEduPerson shemom, prije migracije ustanova mora napraviti sljedeće:

1. Prije tranzicije ustanova mora uspostaviti ažurno stanje LDAP imenika. Iz imenika ustanove treba obrisati sve one korisnike koji više nisu ni na koji način povezani s ustanovom.

2. Za svakog korisnika obavezno treba u LDAP imenik ustanove unijeti njegovu e-mail adresu (po mogućnosti e-mail adresu koju ima na ustanovi).

3. Za sve one korisnike koji nisu evidentirani u ISVU i/ili ISSP, ustanova mora pribaviti sve podatke čiji unos zahtjeva hrEduPerson imenička shema (to su oni atributi koji su u opisu hrEduPerson imeničke sheme u dokumentu [1] označeni kao obvezni), a koji se ne nalaze u postojećem LDAP imeniku ustanove.

4. Ustanove koje žele da tijekom migracije njihovi korisnici imaju pristup uslugama CARNeta, Srca ili MZOŠ-a za koje se autentikacija/autorizacija korisnika radi iz njihovog LDAP imenika, nakon što obave korak 1. trebale bi osigurati da nekoliko dana uoči migracije njihov LDAP poslužitelj neprekidno radi ispravno kako bi se ažurni podaci iz LDAP imenika ustanove iskopirali na backup LDAP poslužitelj u Srcu.

5. Osoba odgovorna za administraciju podataka u LDAP imeniku ustanove mora svim korisnicima u svojoj ustanovi najaviti promjene vezane uz sadržaj LDAP imenika ustanove, kao i datum od kada se očekuje da će nastupiti promjene. Također, potrebno je obavjestiti korisnike da tijekom procesa migracije neće moći pristupati svojim podacima u LDAP imeniku (primjerice, neće moći promijeniti svoju zaporku) te da će nakon migracije morati koristiti isključivo korisničke oznake oblika *korisnik@oznaka_ustanove*.

4.2. Proces migracije kod ustanova koje imaju vlastite LDAP poslužitelje

Proces prijenosa podataka iz postojećeg LDAP imenika u LDAP imenik s hrEduPerson imeničkom shemom odvijat će se sljedećim redoslijedom:

1) Prije samog početka migracije potrebno je ugasiti lokalni RADIUS poslužitelj ustanove kako bi se tijekom migracije autentikacija korisnika mogla vršiti preko backup poslužitelja u Srcu.

2) Nakon što ustanova osigura da su svi podaci u njenom LDAP imeniku ažurni, potrebno je sadržaj LDAP imenika ustanove arhivirati u LDIF datoteku i poslati tu datoteku na adresu team@aaiedu.hr. Također, na istu adresu potrebno je dostaviti u elektroničkom obliku i sve one podatke o korisnicima koji nisu dostupni kroz ISVU ili ISSP, a koje zahtijeva hrEduPerson imenička shema.

3) Na temelju dobivene org.ldif datoteke i ostalih dostupnih podataka (ISVU, ISSP, dodatni podaci o korisnicima koje je dostavila ustanova...) AAI@EduHr tim će za ustanovu kreirati novu LDIF datoteku prilagođenu hrEduPerson imeničkoj shemi. Nakon što napravi konverziju, AAI@EduHr tim će ustanovi dostaviti:

   - LDIF datoteku s podacima o korisnicima iz ustanove prilagođenim importiranju u LDAP imenik s hrEduPerson imeničkom shemom

   - popis korisnika koji nisu mogli biti prebačeni u novu LDIF datoteku zato što za te korisnike AAI timu nisu bili na raspolaganju svi potrebni podaci koje zahtijeva

hrEduPerson imenička shema. Te korisnike ustanova će morati u novi LDAP imenik dodati ručno.

4) Nakon što od AAI tima dobije novu LDIF datoteku prilagođenu hrEduPerson imeničkoj shemi, osoba zadužena za održavanje LDAP poslužitelja ustanove mora na računalu na kojem se nalazi lokalni LDAP poslužitelj ustanove instalirati:

   - LDAP poslužitelj s HrEduPerson imeničkom shemom
   - aplikaciju za održavanje sadržaja imenika (AOSI)

   Nova konfiguracija LDAP poslužitelja instalira se iz odgovarajućih CARNetovih paketa, a prilikom instalacije nove konfiguracije postojeći LDAP imenik, kao i svi podaci koji se u njemu nalaze, bit će obrisani.

5) Po završetku instalacije LDAP poslužitelja s HrEduPerson imeničkom shemom, potrebno je iz nove LDIF datoteke s podacima prilagođenim hrEduPerson imeničkoj shemi importirati podatke u LDAP imenik ustanove.

6) Nakon unosa podataka o korisnicima osoba zadužena za održavanje LDAP poslužitelja ustanove mora na adresu team@aaiedu.hr poslati obavijest o završetku instalacije kako bi AAI@EduHr tim mogao provjeriti radi li sve ispravno.

4.3. Proces migracije kod ustanova koje koriste LDAP hosting

Ustanove koje koriste uslugu LDAP hostinga bit će unaprijed obavještene o datumu migracije, a prije migracije moraju učiniti sljedeće:

- osigurati ažurnost sadržaja svog LDAP imenika
- pribaviti sve podatke o svojim korisnicima koji su potrebni za migraciju na hrEduPerson imeničku shemu, a koji se ne nalaze u sadašnjim LDAP imenicima ustanova

Ustanove koje do definiranog datuma ne osiguraju sve potrebne podatke morat će svoje korisnike u novi LDAP imenik unijeti ručno.

5. Reference

[1] Definicija HrEdu imeničke sheme (ver.1.2.)