Kako u LDAP imenik dodati zapis za potrebe autentikacije aplikacija?

Iako nikako ne preporučamo u imeniku imati zapise koji ne pripadaju osobama (npr. zapise za potrebe raznih aplikacija), ukoliko imate potrebe dodati takav zapis u imenik, nužno je slijediti nekoliko pravila:

1. Obzirom da zapis u imeniku ne pripada osobi, on **ne smije** imati vrijednost atributa **objectClass=hrEduPerson;**

2. da bi se izbjegla mogućnost autentikacije tog korisnika putem središnjih AAI@EduHr servisa, kao i njegov prikaz u web sučelju za održavanje sadržaja imenika (AOSI web sučelju), takav korisnik **ne smije imati atribut uid** (njegov dn ne smije biti oblika `uid=nesto,dc=domena,dc=hr`). Za takav tip korisnika preporučamo **Distinguished Name kreirati uporabom atributa cn** (`dn: cn=nesto,dc=domena,dc=hr`);

Za primjer kako treba izgledati zapisa takvog korisnika u imeniku, pogledajte kako u vašem imeniku izgleda korisnik `cn=hreduadmin,dc=domena,dc=hr`.

Kako je AOSI web sučelje (web sučelje za održavanje sadržaja imenika) prilagođeno uređivanju objekata koji imaju **objectClass=hrEduPerson**, korisnika za potrebe aplikacija **NIJE MOGUĆE** dodati u imenik kroz web sučelje već je to potrebno uraditi nekim LDAP klijentom direktno u LDAP imeniku.

Takvog korisnika je moguće dodati u imenik i ldapmodify naredbom pomoću ldif datoteke. Primjer uporabe ldapmodify naredbe za dodavanje korisnika možete pronaći u uputi Kako napraviti sigurnosnu kopiju podataka pohranjenih u LDAP imeniku?

U nastavku je primjer atributa koje treba sadržavati ldif datoteka za dodavanje korisnika.

```
dn: cn=aplikacija, dc=domena,dc=hr
mail: mailadresa@domena.hr
userPassword: {SHA}kTzelkjlk/77dzuppppd=
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
sn: aplikacija
cn: aplikacija
```

Kod kreiranja ldif datoteke za dodavanje korisnika u imenik trebate zamijeniti riječ domena domenom svoje ustanove, postaviti odgovarajući cn (u atributima cn i dn), upisati mail adresu, te zaporku (atribut userPassword) za novog korisnika. Zaporku treba biti kriptirana, a kriptirati je možete naredbom:

```
slappasswd -h {SHA}
```

Tekst dobiven izvršavanjem gornje naredbe unesite kao vrijednost atributa userPassword.

VAŽNO: stupanjem na snagu Opće uredbe o zaštiti podataka, pristupna lista LDAP-a (ACL) je izmjenjena na način da je onemogućen anonimni dohvat podataka iz LDAP imenika, a autenticiranim korisnicima je zabranjen dohvat osobnih podataka drugih korisnika. Zbog svega navedenog, a da bi korisnik za potrebe aplikacija mogao pristupiti podacima drugih korisnika u LDAP imeniku, potrebno je promijeniti konfiguraciju LDAP-a u dijelu koji se odnosi na prava pristupa podacima / vrijednostima atributa.