

Kako pokrenuti sekundarni, redundantni skup AAI@EduHr komponenti na matičnoj ustanovi?

Uvod

Osnovni elementi sustava AAI@EduHr koji se nalaze matičnim ustanovama su:

- **LDAP imenik** u kojem su pohranjeni podaci o elektroničkim identitetima;
- **RADIUS poslužitelj** koji je primarno namijenjen autentikaciji za usluge pristupa mreži;
- **Aplikacija za održavanje sadržaja imenika (AOSI)** koja se sastoji od dvije komponente - web servisa za dohvat podataka (AOSI-WS) i web sučelja za održavanje sadržaja LDAP imenika (AOSI-WWW);

Dohvat podataka iz LDAP imenika obavlja se uporabom LDAP protokola. LDAP imeniku pristupaju RADIUS poslužitelj i AOSI web servis.

Organizacijska i tehnička izvedba redundantnog (sekundarnog) sustava

Da bi sekundarni sustav ispunio svoju osnovnu namjenu, potrebno ga je postaviti na zasebno računalo i ako je moguće u drugi mrežni segment.

Uloga sekundarnog sustava, odnosno skupa AAI@EduHr servisa instaliranih na matičnoj ustanovi je da u slučaju nedostupnosti ili preopterećenosti primarnih servisa privremeno obrađuje autentikacijske zahtjeve inicijalno upućene primarnim servisima. Obzirom da u normalnim uvjetima sekundarni sustav ne bi trebao obavljati nikakve zadatke, proizlazi da instalacija potrebne programske podrške i njen rad ne opterećuju znatno računalo na kojem se nalazi sekundarni sustav.

Sekundarni sustav sadrži sve osnovne komponente od kojih se sastoji i primarni sustav, s tom razlikom da je LDAP imenik sekundarnog sustava replika primarnog LDAP imenika tj. podatke u sekundarnom LDAP imeniku nije moguće proizvoljno uređivati.

Uspješna izvedba sekundarnog sustava zahtjeva repliciranje LDAP baze podataka s primarnog sustava na sekundarni sustav u realnom vremenu uz korištenje odgovarajućeg pomoćnog servisa (**slurpd**) i specijalno za tu potrebu kreiranog korisnika **replica**. Repliciranje se provodi standardnim LDAP protokolom (**ldap** ili **ldaps**), uz ograničavanje svih promjena na sekundarnom LDAP imeniku tj. promjene u sekundarnom imeniku može raditi isključivo korisnik **replica**.

Zbog specifičnosti pojedinih operacijskih sustava i njihovih file sistema, poželjno je da primarni i sekundarni sustav koriste istu verziju OS-a.

Važno!

Prije izvršavanja operacija navedenih u nastavku preporučamo da [napravite sigurnosnu kopiju](#) podataka pohranjenih u primarnom LDAP imeniku.

Uspostava sekundarnog skupa servisa i replikacije LDAP imenika

U nastavku donosimo konkretne upute za uspostavu sekundarnog sustava odnosno skup servisa potrebnih za rad AAI@EduHr. Temelj je uspostava replikacije LDAP imenika s primarnog LDAP poslužitelja na sekundarni LDAP poslužitelj.

Posao uspostave sekundarnih AAI@EduHr servisa matične ustanove svodi se na podešavanje primarnog i sekundarnog LDAP poslužitelja. U konačnici na oba poslužitelja trebaju biti instalirani i odgovarajuće podešeni paketi **openldap-aai**, **freeradius-aai** i **aosi-aai**.

Na **primarnom poslužitelju** potrebno je instalirati paket **openldap-aai** inačice **2.4.23** ili veće. Prilikom njegove instalacije kod pitanja "Nacin rada LDAP poslužitelja" potrebno je odgovoriti **primary**. Ako je odgovarajući paket već instaliran, do tog se pitanja može doći naredbom:

```
# dpkg-reconfigure openldap-aai
```

Tijekom postupka podešavanja primarnog poslužitelja potrebno je upisati i zaporku koja služi za replikaciju podataka.

Također, na **primarnom poslužitelju** treba instalirati paket **aosi-aai** inačice **3.0.7** ili veće. Prilikom njegove instalacije potrebno je kod pitanja "Nacin rada AOSI poslužitelja" odgovoriti **primary**. Ako je odgovarajući paket već instaliran, do tog se pitanja može doći naredbom:

```
# dpkg-reconfigure aosi-aai
```

Time je sve spremno za funkcioniranje primarnog LDAP i AOSI poslužitelja.

Na **sekundarnom poslužitelju** treba instalirati paket **openldap-aai** inačice **2.4.23** ili veće. Prilikom njegove instalacije potrebno je kod pitanja "Nacin rada LDAP poslužitelja" odabrati odgovor **secondary**. Ako je odgovarajući paket već instaliran, do tog se pitanja može doći naredbom:

```
# dpkg-reconfigure openldap-aai
```

U postupku podešavanja sekundarnog poslužitelja potrebno je upisati IP adresu primarnog, te istu onu zaporku za replikaciju koju ste upisali prilikom podešavanja primarnog poslužitelja.

Također, na **sekundarnom poslužitelju** treba instalirati paket **aosi-aai** inačice **3.0.7** ili veće. Prilikom njegove instalacije potrebno je kod pitanja "Nacin rada AOSI poslužitelja" odabrati odgovor **secondary**. Ako je odgovarajući paket već instaliran, do tog se pitanja može doći naredbom:

```
# dpkg-reconfigure aosi-aai
```

Time je sve spremno za funkcioniranje sekundarnog LDAP i AOSI poslužitelja.

I na primarnom i na sekundarnom poslužitelju potrebno je imati instaliran paket **freeradius-aai** inačice **2.1.3** ili veće.

Nakon što na oba poslužitelja instalirate sve odgovarajuće pakete u skladu s gore navedenim uputama, na adresu aai@srce.hr trebate poslati obavijest s podacima o IP adresi sekundarnog poslužitelja i njegovom DNS nazivu kako bismo mogli provjeriti funkcionira li sekundarni skup servisa ispravno i uključiti sekundarni poslužitelj u sustav AAI@EduHr.