

## Što je to SPONA?

SPONA je akronim od Sistemsko Pomagalo za Otvaranje Novih Accounata. To se odnosi na otvaranje novih korisničkih računa na Linux poslužitelju prema sadržaju [AAI@EduHr](mailto:AAI@EduHr) imenika ustanove. Drugim riječima, to je alat za sinkronizaciju korisnika između imenika i sistema. Osim dodavanja novih korisničkih računa donosi i mogućnost automatiziranog održavanja GECOS polja (imena i prezimena korisnika – bitno za dostavu pošte na adresu [ime.prezime@domena.hr](mailto:ime.prezime@domena.hr)) te automatizirano brisanje korisničkih računa koji nisu više u imeniku.

## Kako se instalira?

Paket se instalira putem standardnog APT mehanizma sa APT izvora:

```
deb ftp://ftp.srce.hr/srce-debian/ sarge main
```

Instalira se naredbom:

```
# apt-get install spona-aa1
```

## Inicijalno podešavanje

Prilikom instalacije potrebno je unijeti neke parametre koji će ovom alatu omogućiti rad. Potrebno je unijeti adresu WSDL datoteke AOSI web-servisa putem kojeg ovaj alat dohvaća popis korisnika iz imenika. Također potrebno je unijeti baznu granu imenika (Base DN).

Programski paket dolazi s nekoliko predefiniраниh profila korisničkih računa koji se kreiraju ukoliko postoje u imeniku a istoimenih nema na sistemu. Za bolju kontrolu nad tim parametrima, pregledajte te profile te ih po želji prilagodite prije prvog pokretanja. Datoteka sa profilima je `/etc/spona/profiles.conf`.

## Redovna uporaba

U paketu dolazi *frontend* naredba za korisnika, koja se zove spona. Opcije koje se dodaju su:

```
--useradd          mod rada u kojem se dodaju korisnici
--userdel          mod rada u kojem se brisu korisnici
-c, --cron         rad iz crona
-p, --profile <profile> neki drugi profile
-y, --no-dry-run   stvarno izvršenje komandi
-s, --script <file> generiraj skriptu u <file>
-h, --help         pomoc
```

Trenutno su dostupna dva načina rada, jedan je za dodavanje korisnika, drugi je za brisanje korisnika. Oni se dodaju kao argumenti naredbe. Znači, ako želimo dodati korisnike koji su u imeniku, a nema ih na sistemu, rabimo:

```
# spona --useradd
```

Jedini nužan argument te naredbe je način rada (`--useradd` ili `--userdel`).

Pokretanjem gornje naredbe, SPONA će ponuditi popise korisnika koje želi dodati, te se njihovim odabirom generira shell skripta kojom se kasnije mogu dodati korisnici. SPONA namjerno automatski ne dodaje korisnike, već generira skriptu koja se kasnije pokrene. Preporuča se administratoru da pogleda tu skriptu prije njenog izvršavanja.

Opcija `--cron` služi za korištenje iz CRON-a, odnosno neće koristiti vizualne dijaloge (*ncurses*) za interakciju sa administratorom. Sve opcije se moraju zadati putem konfiguracijskih datoteka, ili putem argumenata naredbe. Primjer korištenja iz CRON-a se nalazi u datoteci `/etc/cron.d/spona`. Tamo se mogu otkomentirati mogući primjeri. U CRON načinu rada potrebno je u datoteku `/etc/spona/agent.global.conf` dodati korisničko ime i lozinku koja će se koristiti za slanje upita na AOSI web servis. Upućujemo Vas na primjere navedene u toj datoteci.

Opcija `--script` služi za odabir gdje će se generirati skripta za dodavanje korisnika. Ako se ovaj argument ne doda, SPONA će izgenerirati skriptu unutar direktorija `/tmp` koristeći naredbu `mktemp` (npr. `/tmp/spona.sh-7azXNx`) i javiti putem svog sučelja točnu lokaciju te skripte.

Opcija `--profile` služi za odabir profila korisničkih računa (student, djelatnik, ...) prema definiciji u `/etc/spona/profiles.conf`. U slučaju da se ne doda ovaj argument, podrazumna operacija su svi profili navedeni u varijabli `AVAILABLE_PROFILES` u datoteci `/etc/spona/profiles.conf`.

Opcija `--no-dry-run` služi za direktno dodavanje računata, bez generiranja skripte. Preporučeni način rada je bez ove opcije, tako da postoji dodatna mogućnost kontrole generirane skripte.

Sve gornje opcije se mogu koristiti kod oba načina rada (dodavanje/brisanje korisničkih računa).

## Autentikacija osnovnih servisa putem [AAI@EduHr](#)

Za autentikaciju različitih servisa putem [AAI@EduHr](#) mogu se koristiti dva modula: **pam\_ldap** i **pam\_radius**. Preporuka [AAI@EduHr](#) službe je uporaba modula **pam\_radius**, pa će ove upute biti bazirane na njemu.

Način rada u ovom slučaju je posredan, jer `pam_radius` kontaktira RADIUS server, koji zatim komunicira s LDAP serverom.

Uz pretpostavku da se radi o Debian Linuxu, potrebno je instalirati paket `libpam-radius-auth` koji donosi potreban PAM modul. Instalacija je standardna:

```
# apt-get install libpam-radius-auth
```

U konfiguraciji FreeRADIUS-a prijavite poslužitelj na kojem otvarate nove korisničke račune kao klijenta:

```
# U našem slučaju je klijent na lokalnom računalu (localhost)
client 127.0.0.1 {
    secret      = neki_secret
    shortname = localhost
}
```

Ovaj secret se treba prenijeti i u konfiguraciju pam\_radius-a u datoteci /etc/pam\_radius\_auth.conf:

```
# server[:port]      shared_secret  timeout (s)
127.0.0.1:1812 neki_secret      3
```

Naravno, primjere (stari 127.0.0.1 i other-server) zakomentirajte.

Time smo obavili predradnje za autentikaciju servisa preko RADIUS-a. Konfiguracijske datoteke PAM-a nalaze se u direktoriju /etc/pam.d/.

Ako želite sve servise autenticirati preko RADIUS-a, u datoteci /etc/pam.d/common-auth, bez diranja ostalih datoteka, zakomentirajte redak:

```
#auth required pam_unix.so nullok_secure
```

i dodajte:

```
auth sufficient      pam_radius_auth.so
auth required pam_unix.so try_first_pass
```

Time smo postigli da se autentikacija korisnika obavlja preko RADIUS servera, a tek u slučaju neuspješne autentikacije pita se pam\_unix (odnosno traži unos zaporke navedene u datoteci /etc/shadow). To je dobro, jer će se sistemac moći prijaviti na poslužitelj i u slučaju ispada RADIUS-a ili LDAP-a.

Ako ne želite sve servise autenticirati putem pam\_radius-a, možete za svaki servis definirirati autorizacijski mehanizam, tj. svaki servis ima svoju pam datoteku. Na primjer, za Secure shell u /etc/pam.d/ssh zakomentirajte redak:

```
#@include common-auth
```

i dodajte dva nova:

```
auth sufficient      pam_radius_auth.so
auth required pam_unix.so try_first_pass
```

U /etc/pam.d nalazi se konfiguracija i za druge servise. Na isti način možete unijeti i konfiguraciju na primjer za ftp, imap, pop itd.