

Kako napraviti jednostavnu black-listu za FreeRADIUS

FreeRADIUS poslužitelj može obavljati različite funkcije unutar procesa autentikacije i autorizacije korisnika.

Sam proces autentikacije baziran je na prepoznavanju podataka koje je korisnik dao o sebi. To se u osnovi svodi na korisničku oznaku i neki od oblika zaštitnih autentikacijskih podataka (lozinka, certifikat, pin, ...).

Prilikom autentikacije RADIUS poslužitelju su poznati i dodatni podaci koji se odnose na sam komunikacijski sustav kojim se obavlja autentikacija (podaci o klijentu koji šalje upit, podaci o proxy poslužiteljima prije njega, vremenima, ...).

Jednostavnu black-listu je moguće napraviti korištenjem tzv. **hints**a (postavljeno incijalno po instalaciji FreeRADIUS paketa iz AAI@EduHr distribucije).

U **hints** datoteku unutar **/etc/freeradius/** direktorija potrebno je dodati retke s odgovarajućim direktivama.

U nastavku je navedeno nekoliko primjera kako postići black-listing korisnika koji se spaja svojim prijenosnim računalom na lokalnu mrežu.

Ukoliko nam je poznata MAC adresa klijenta (korisnikova računala) potrebno je dodati slijedeće retke:

```
DEFAULT User-Name =~ "^([^\@]+)@([^\@]+)", Calling-Station-Id == "<mac_addressa>"
User-Name := "Blacklist[%{1}::%{2}]"
```

gdje se umjesto `<mac_addressa>` upisuje MAC adresa klijenta s kojeg dolaze upiti kako to prikazuje FreeRADIUS.

Primjerice:

```
DEFAULT User-Name =~ "^([^\@]+)@([^\@]+)", Calling-Station-Id == "000a.6cdf.a456"
User-Name := "Blacklist[%{1}::%{2}]"
```

U gornjem primjeru svi zahtjevi za autentikaciju koji dolaze od klijenta (prijenosnog računala) s MAC adresom 000a.6cdf.a456 biti će onemogućeni.

Ukoliko nam je poznata korisnička oznaka kojom se korisnik predstavlja potrebno je dodati slijedeće retke:

```
DEFAULT User-Name =~ "^([^\@]+)@([^\@]+)", User-Name == "pero@brzi.hr"
User-Name := "Blacklist[%{1}::%{2}]"
```

U gornjem primjeru svi zahtjevi za autentikaciju koji dolaze od korisnika koji se predstavlja s korisničkom oznakom pero@brzi.hr biti će onemogućeni.

Uvjete je moguće kombinirati sukladno potrebama. Ukoliko želimo korisnika tada za svakog od njih treba ponoviti odgovarajuću direktivu:

Primjerice:

```
DEFAULT User-Name =~ "^([^\@]+)@([^\@]+)", User-Name == "pero@brzi.hr"
User-Name := "Blacklist[%{1}::%{2}]"
DEFAULT User-Name =~ "^([^\@]+)@([^\@]+)", User-Name == "jura@spori.at"
User-Name := "Blacklist[%{1}::%{2}]"
DEFAULT User-Name =~ "^([^\@]+)@([^\@]+)", Calling-Station-Id == "000a.6cdf.a450"
User-Name := "Blacklist[%{1}::%{2}]"
DEFAULT User-Name =~ "^([^\@]+)@([^\@]+)", User-Name == "^[^\@]+@losi.hr"
User-Name := "Blacklist[%{1}::%{2}]"
```

onemogućuje pristup korisnicima s korisničkim oznakama pero@brzi.hr, jura@spori.at, korisniku koji pristupa s MAC adrese 000a.6cdf.a450 te svim korisnicima iz domene losi.hr.

Na kraju spomenimo kako je potrebno uzeti u obzir da različiti klijenti mogu zapisivati pojedine vrijednosti u različitim formatima. Stvarni format najlakše je iščitati iz logova FreeRADIUSa. Više o dozvoljenim paramterima i atributima, te njihovim vrijednostima možete saznati na sljedećim adresama:

[FreeRADIUS Run-time variables](#)

[FreeRADIUS Adding, Removing, Modifying Attributes for further processing](#)

[FreeRADIUS Operators\(link is external\)](#)