

Pgina i eduroam nakon prelaska na Debian Squeeze



Nakon uspješne dogradnje Carnetove distribucije Debiana na Squeeze, trebalo je provjeriti da li se radius autentikacija ispravno odvija. U logu `/var/log/freeradius/radius.log` uz zapise o ispravnim autentikacijama pojavljuju se i greške, kao u slijedećem primjeru:

```
Wed Apr 25 11:18:12 2012 : Auth: Login OK: [korisnik@simet.hr] (from client aaics3 port 0)
Wed Apr 25 11:18:57 2012 : Error: Ignoring request to authentication address * port 1812 from unknown client 161.53.xx.xx port 3064
Wed Apr 25 11:19:00 2012 : Error: Ignoring request to authentication address * port 1812 from unknown client 161.53.xx.xx port 3064
Wed Apr 25 11:19:02 2012 : Error: Ignoring request to authentication address * port 1812 from unknown client 161.53.xx.xx port 3064
Wed Apr 25 12:38:38 2012 : Error: Ignoring request to authentication address * port 1812 from unknown client 161.53.xx.xx port 2073
Wed Apr 25 12:38:41 2012 : Error: Ignoring request to authentication address * port 1812 from unknown client 161.53.xx.xx port 2073
```

Po IP adresama se vidi da se radi o greškama eduroam i Pgina klijenata. Definicije RADIUS klijenata nalaze se u `/etc/freeradius/clients.conf` u obliku npr:

```
client 161.53.x.xxx {
    secret          = TajnaRijec
    shortname       = mojPginaKlijent
}
client 161.53.x.xxx {
    secret          = TajnaRijec
    shortname       = mojEduroamKlijent
}
```

Provjerom konfiguracije u `clients.conf` ispostavlja se da su **definicije klijenata** instalacijom novog `freeradius-aa` paketa jednostavno pobrisane. Zaključujemo da se klijenti eduroama i Pgine moraju ponovo ručno prijaviti. Preko AAI službe pomoći saznajemo da je dosadašnja datoteka `/etc/freeradius/clients.conf` sada razdvojena u dvije datoteke: `/etc/freeradius/clients.conf` i `/etc/freeradius/clients-aa.conf`, te da se klijenti koje donosi `freeradius-aa` paket nalaze u `clients-aa.conf`. Naprotiv, klijente koje sami dodajemo za Pgina i eduroam prijavljujemo u `clients.conf`.

Potražimo backup koji je napravila skripta `carnet-upgrade` u `/var/backups/etc.cn6-upgrade.tar.gz`, pa iz datoteke `etc/freeradius/clients.conf` prekopiramo definicije svojih Pgina i eduroam klijenata u `/etc/freeradius/clients.conf` na serveru.

Naravno uz obavezno ponovno pokretanje servisa:

```
# /etc/init.d/freeradius restart
```

Također primjećujemo je da pokušaji klijenata koji se bežično spajaju preko eduroam infrastrukture izazivaju slijedeću grešku u dnevniku `/var/log/freeradius/radius.log`:

```
Thu Apr 26 07:54:17 2012 : Auth: Login incorrect: [korisnik@simet.hr] (from client MojPrviAP port 1 cli 00-4F-78-01-42-28)
Thu Apr 26 07:55:09 2012 : Error: TLS Alert read:fatal:unknown CA
Thu Apr 26 07:55:09 2012 : Error: TLS_accept: failed in SSLv3 read client certificate
A
Thu Apr 26 07:55:09 2012 : Error: rlm_eap: SSL error error:14094418:SSL routines:SSL3_READ_BYTES:tlsv1 alert unknown ca
Thu Apr 26 07:55:09 2012 : Error: SSL: SSL_read failed inside of TLS (-1), TLS session fails.
```

Zaključak je da dolazi do **greške pri provjeri ispravnosti certifikata**, koji je postavljen od strane installer.eduroam.hr sustava. Ako se isključi i ne "forsira" provjera certifikata kako to originalna konfiguracija podrazumijeva, spajanje uspijeva.

Problem je nastao zato što je instalacija paketa freeradius-aai izgenerirala nove certifikate koji klijente instalirane preko eduroam.installer.hr sustava prepoznaje kao "neispravne".

Iz konzultacija sa službom pomoći eduroam tima saznajemo da je došlo do promjena u konfiguraciji. Umjesto u /etc/freeradius/eap.conf putanja je u /etc/freeradius/modules/eap-aai, u obliku redaka s putanjom do lozinke i certifikata dobivenih iz prijave Eduroam installera. Podatke o putanji možete isčitati iz backupa /etc/freeradius/eap.conf datoteke.

```
private_key_password = NekaLozinka
private_key_file = /nekaputanja/server-key.pem
certificate_file = /nekaputanja/server-cert.pem
```

Retke editiramo u /etc/freeradius/modules/eap-aai.conf i nakon toga obavezno slijedi:

```
# /etc/init.d/freeradius restart
```

Nakon ovih promjena eduroam bežični klijenti bi trebali prolaziti autentikaciju bez grešaka.

pet, 2012-05-04 12:21 - Goran Šljivić **Kuharice:** [Linux](#) [1]
Kategorije: [Servisi](#) [2]
Vote: 0

No votes yet

Source URL: <https://sysportal.carnet.hr/node/1002>

Links

[1] <https://sysportal.carnet.hr/taxonomy/term/17>
[2] <https://sysportal.carnet.hr/taxonomy/term/28>