Konfiguracija – Davalac Identiteta

AMRES

Akademska mreža Srbije

eduroam servis u AMRES-u

Sadržaj

- Uvod – šta je potrebno da bi institucija postala IdP
- FreeRADIUS platforma
- Instalacija FreeRADIUS servera
- Konfiguracija IdP FreeRADIUS servera

Uvod

- Šta vam je potrebno da institucija postane davalac identiteta:
  - RADIUS server (Radiator, FreeRADIUS)
  - Digitalni sertifikat
  - Baza korisničkih podataka (LDAP, AD...)

- Uputstva za instalaciju, konfiguraciju FreeRADIUS-a www.eduroam.amres.ac.rs/rs/institucije-uputstva

FreeRADIUS server

- www.freeradius.org
- *Open-source* projekat
- Aktuelna verzija je 2.1.10
- Podržani OS:
  - Linux (**CentOS**, Debian, Mandriva, Red Hat, SUSE, Ubuntu)
  - FreeBSD
  - Solaris
  - OpenBSD..
- Jedan FreeRADIUS server se može koristiti za više servisa
- Modularna platforma

FreeRADIUS platforma (1)

- Osnovni konfiguracioni fajl je radiusd.conf – u njemu se pozivaju ostali moduli
- Ostali bitni moduli:
  - clients.conf
  - proxy.conf
  - eap.conf
  - Moduli za povezivanje na LDAP, AD
  - Virtuelni serveri...
- U svakom konfiguracionom fajlu se nalazi objašnjenje čemu on služi i šta se postiže konfiguracijom

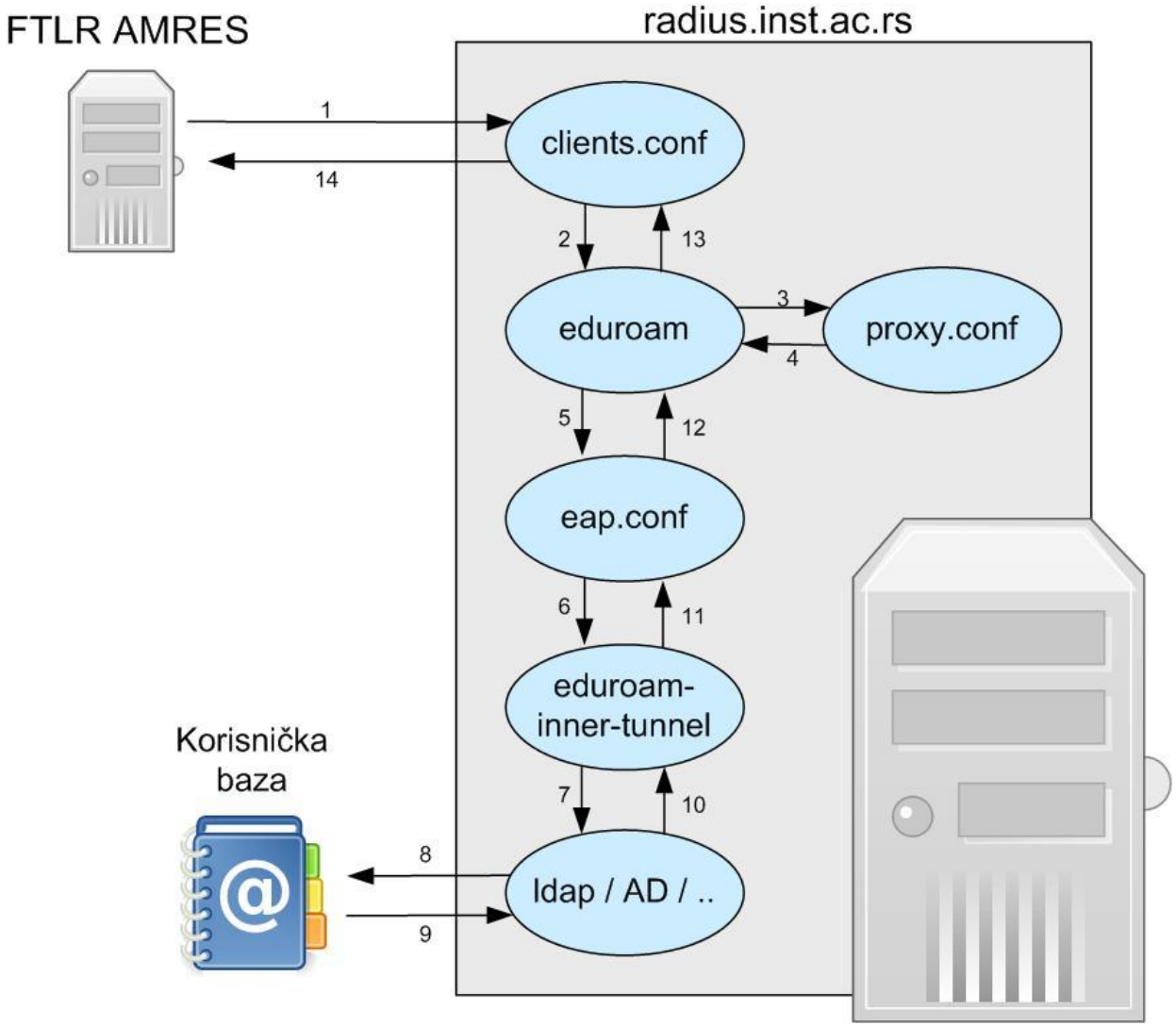
FreeRADIUS platforma (2)

- Virtuelni serveri (/raddb/sites-available):
  - Svaki virtuelni server je predviđen za jedan servis (eduroam, vpn, dial-up...)
  - Inicijalno postoji samo jedan virtuelni server (*default* i *inner-tunnel*)
  - Za eduroam kreiramo jedan novi:
    - eduroam (kopiramo *default*) i
    - eduroam-inner-tunnel (kopiramo *inner-tunnel*)

FreeRADIUS moduli (1)

- Biće prikazane konfiguracije relevantnih modula pri vezivanju na LDAP i AD korisničke baze
- Relevantni eduroam konfiguracioni fajlovi:
  - clients.conf
  - eduroam
  - eduroam-inner-tunnel
  - eap.conf
  - proxy.conf
  - ldap-attrmap
  - ldap
  - ntlm_auth

FreeRADIUS moduli (2)



Instalacija FreeRADIUS-a (1)

- Pre instalacije FreeRADIUS-a:
  - gcc biblioteke
  - Openssl, **openssl-devel** (!)
  - LDAP (ako imate LDAP bazu) – u uputstvu za instalaciju je prikazana instalacija openldap softvera
  - MySQL (za davaoce resursa)

Instalacija FreeRADIUS-a (2)

- Instalacija:

  `./configure --with-openssl --with-"xyz"`

  `make`

  `make install` (root privilegije)

- Nakon instalacije, FreeRADIUS folder (raddb) se obično nalazi u /usr/local/etc/

- Startovanje servera:

  `radiusd` (centos)

  /usr/sbin/freeradius (debian)

- Startovanje servisa u debug modu:

  `radiusd -X` (centos)

  /usr/sbin/freeradius -X (debian)

clients.conf

- U ovom modulu se definišu klijenti FreeRADIUS servera
- Potrebno je uneti parametre za dva FTLR AMRES servera i Netiis (za monitoring)
- Lozinke se dobijaju od AMRES-a (telefonom ili lično)

clients.conf

```
## eduroam Federation Top Level RADIUS serveri:
## eduroam ftlr1
client ftlr1.ac.rs {
   ipaddr              = 147.91.4.204
   secret              = pass
   shortname           = ftlr1
   nastype             = other
   virtual_server      = eduroam
}


## Monitoring eduroam servisa
client netiis.monitor {
   ipaddr               = 147.91.3.12
   secret               = pass
   shortname            = netiis
   nastype              = other
   virtual_server       = eduroam
}
```

FTLR 1,
(analogno i FTLR2)

Netiis

eduroam modul

- U /raddb/sites-available
- Prekopirati default konfiguracioni fajl u eduroam
- Obavezno dodati “*wrapper*”:
  - Na početak: `server eduroam {`
  - Na kraj: `}`
- Napraviti soft link ka eduroam virtuelnom serveru u /raddb/sites-enabled folderu

eduroam modul

- eduroam konfiguracioni fajl sadrži više sekcija:
  - **authorize**
  - **authenticate**
  - preacct
  - accounting
  - session
  - post-auth
  - pre-proxy
  - post-proxy

eduroam modul

- U authorize sekciji je važno ostaviti eap komandu jer on označava korišćenje eap.conf modula i samim tim omogućava EAP-TTLS ili EAP-PEAP autentifikaciju:

```
server eduroam {
authorize {
        preprocess
        auth_log
        suffix
        eap {
                ok = return
        }
        expiration
        logintime
}
```

proxy.conf

- FreeRADIUS “tabela rutiranja”
- U njemu se nalaze informacije o tome da li se dolazni zahtev obrađuje lokalno ili ga je potrebno proslediti nekom drugom serveru (u slučaju davaoca resursa)
- U slučaju davaoca identiteta potrebno je definisati samo lokalni domen

proxy.conf

```
proxy server {
        default_fallback = no
}
home_server localhost {
        type = auth+acct
        ipaddr = 127.0.0.1
        port = 1812
        secret = testing123
        response_window = 20
        zombie_period = 40
        revive_interval = 120
        status_check = status-server
        check_interval = 30
        num_answers_to_alive = 3
}
```

```
realm inst.ac.rs {
        authhost    = LOCAL
        accthost    = LOCAL
        User-Name   = "%{Stripped-User-Name}"
}
realm LOCAL {
}
realm NULL {
}
```

eap.conf

- Fajl u kome se podešava autentifikacioni metod koji će se koristiti (EAP-TTLS ili EAP-PEAP)
- Inicijalno je potrebno promeniti dva reda konfiguracije:
  - Prvi red: `default_eap_type = ttls` (ili peap ako je to slučaj)
  - U TTLS/PEAP delu: promeniti virtual server u eduroam-inner-tunnel:

```
ttls {
        default_eap_type = md5
        copy_request_to_tunnel = no
        use_tunneled_reply = no
        virtual_server = "eduroam-inner-tunnel"
    }
```

eap.conf - dodavanje sertifikata

- Inicijalno server kreira *self-signed* digitalni sertifikat koji smešta u /raddb/cert folder
- Preporučuje se korišćenje sertifikata čiji je *root* sertifikat preinstaliran u većini SSL klijenata
- AMRES je obezbedio TCS serverske sertifikate www.amres.ac.rs
- Kada se arhiva dobije i raspakuje u njoj se nalaze dva fajla:
  - Sertifikat sa **.crt** (npr. cert.crt),
  - Drugi fajl sa **.ca-bundle** ekstenzijom (cert.ca-bundle)
- Prilikom generisanja zahteva za sertifikatom generiše se privatni ključ servera (private.key)

eap.conf - dodavanje sertifikata

- Potrebno je sva tri prebaciti u /raddb/certs folder
- Sertifikat sa .crt se prebacuje u .pem format
- Zatim je potrebno uključiti oba u eap.conf modulu, u tls sekciji:

```
private_key_file = /etc/raddb/certs/private.key
certificate_file = /etc/raddb/certs/cert.pem
CA_file = /etc/raddb/certs/cert.ca-bundle
```

eduroam-inner-tunnel

- Prekopirati inner-tunnel konfiguracioni fajl u eduroam-inner-tunnel (raddb/sites-available)
- Na početku fajla promeniti naziv servera:

```
server eduroam-inner-tunnel {
```

- U authorize i authenticate sekcijama se definiše modul za interakciju sa korisničkom bazom (LDAP, AD..)

eduroam-inner-tunnel

- Za vezivanje na ldap:

```
server eduroam-inner-tunnel {
authorize {
        auth_log
        ldap
        pap
}
authenticate {
        Auth-Type PAP {
        pap
}
```

eduroam-inner-tunnel

- Za vezivanje na AD

```
server eduroam-inner-tunnel {
authorize {
        suffix
        update control {
                Proxy-To-Realm := LOCAL
                Auth-Type = ntlm_auth
        }
        eap
        ntlm_auth
        pap
}
authenticate {
        Auth-Type ntlm_auth {
                ntlm_auth
        }
```

Vezivanje na LDAP

- LDAP modul /raddb/modules/

```
ldap {
    server = "localhost"
    identity = "uid=reader,ou=SystemAccounts,dc=bg,dc=ac,dc=rs"
    password = pass
    basedn = "ou=People,dc=bg,dc=ac,dc=rs“
     ...
```

- U ldap.attrmap fajlu se definišu atributi koji se čitaju iz baze

Vezivanje na AD

- Potrebno je instalirati sambu i konfigurisati kerberos (detaljnije u uputstvu na eduroam.amres sajtu)
- Testirati povezivanje na AD sa servera preko komande:

```
ntlm_auth --request-nt-key --domain=MYDOMAIN --username=user --password=password
```

- FreeRADIUS koristi prethodnu komandu za upite ka AD bazi
- Konfiguracija ntlm_auth modula (/raddb/modules):

```
exec ntlm_auth {
  wait = yes
  program = "/usr/bin/ntlm_auth --request-nt-key  --domain=QUARK --
   username=%{Stripped-User-Name} -password=%{User-Password}"
}
```