Nadgledanje RADIUS infrastrukture

Dokument najbolje prakse
(smernice i preporuke)

Izrađen u okviru AMRES tematske grupe za oblast NMS
(AMRES BPD 111)

Autor: Jovana Palibrk,
Saradnici: Ivan Ivanović, Esad Saitović, Marina Vermezović, Marko Stojaković

Februar, 2013.

Dokument broj: GN3-NA3-T4-AMRES-BPD-111
Verzija / datum: Februar 2013.
Izvorni jezik : Srpski
Originalni naslov: “Nadgledanje RADIUS infrastrukture”
Originalna verzija / datum: Revizija 1 (dokumenta iz novembra 2012.)/ 28. februar 2013.
Kontakt: jovana.palibrk@amres.ac.rs, ivan.ivanovic@rcub.bg.ac.rs

AMRES/RCUB snosi odgovornost za sadržaj ovog dokumenta. U izradi dokumenta učestvovala je tematska grupa za NMS organizovana u AMRESu radi sprovođenja zajedničkih aktivnosti na razvoju i širenju dokumenata sa tehničkim smernicama i preporukama za mrežne servise u višokoškolskim obrazovnim i istraživačkim ustanovama u Srbiji.

Dokument je nastao kao rezultat istraživanja koja su finansirana sredstvima Sedmog okvirnog programa Evropske zajednice (FP7/2007-2013) po ugovoru br. 238875, koji se odnosi na projekat „Multi-Gigabit European Research and Education Network and Associated Services (GN3)”.

Sadržaj

Executive Summary

This document describes the implementation of the system used for monitoring a complex server authentication hierarchy based on the RADIUS (Remote Authentication Dial In User Service) protocol. The solution presented herein has been developed within the *eduroam*®[1] service of the Academic Network of Republic of Serbia (AMRES), which at the time of writing has 60 *eduroam*® access points across Serbia. The *eduroam*® authentication infrastructure requires a suitable monitoring system, which enables testing the functionalities of all the RADIUS servers this service comprises. The monitoring system has been designed to provide a sufficiently detailed insight into the state of the RADIUS infrastructure, while not infringing upon user privacy as required under the *eduroam*® policy.

The monitoring of the infrastructure of the RADIUS-based server on the AMRES network is conducted to check the availability of RADIUS servers through the network, as well as to establish whether the RADIUS servers are processing client authentication requests in the appropriate manner. This document presents a simple and scalable monitoring solution and this solution can also be used in other environments where services rely on the RADIUS protocol.

[1] eduroam is a registered trademark of TERENA, the Trans-European Research and Education Networking Association

Rezime

U ovom dokumentu je opisana implementacija sistema za nadgledanje složene autentifikacione hijerarhije servera koja je zasnovana na RADIUS (*Remote Authentication Dial In User Service*) protokolu. Predstavljeno rešenje je razvijeno za potrebe nadgledanja nacionalne serverske infrastrukture realizovane u okviru eduroam servisa u Akademskoj mreži Republike Srbije (AMRES) koja u momentu pisanja ovog dokumenta ima 60 eduroam pristupnih tačaka širom Srbije. Autentifikaciona eduroam infrastruktura zahteva odgovarajući sistem za nadgledanje u okviru kog se vrši testiranje funkcionalnosti svih RADIUS servera od kojih se sastoji. Sistem za nadgledanje je osmišljen tako da pruža dovoljno detaljan uvid u stanje RADIUS infrastrukture ali da se, sa druge strane, prema politici eduroam servisa, ne zadire u privatnost korisnika.

Nadziranje RADIUS serverske infrastrukture u AMRES mreži se sprovodi sa ciljem da se proveri dostupnost RADIUS servera preko mreže, kao i da se utvrdi da li RADIUS serveri na odgovarajući način obrađuju autentifikacione zahteve klijenata. U radu je predstavljeno jednostavno i skalabilno rešenje za nadgledanje, a dobijeni rezultati se mogu iskoristiti i u drugim okruženjima gde se servisi oslanjaju na RADIUS protokol.

1 Uvod

eduroam (EDUcation ROAMing) predstavlja servis razvijen u međunarodnom akademskom okruženju u okviru TERENA-TF-Mobility i GEANT projekta. Cilj ovog servisa je da korisnicima akademskih institucija u Evropi, a u poslednje vreme i šire, omogući bezbedan, brz i jednostavan bežični pristup Internetu u svim tačkama u svetu na kojima je eduroam implementiran. Bilo da pristupaju eduroam servisu u svojoj ili instituciji koju posećuju, korisnici koriste kredencijale koje su dobili od svoje matične institucije.

Osnovni princip sigurnosti eduroam servisa je da se autentifikacija korisnika, bez obzira ne mesto pristupa mreži, vrši na matičnoj instituciji korisnika primenom EAP (*Extensible Authentication Protocol*) autentifikacionih metoda koje je ta institucija implementirala. Autorizacija za pristup Internetu i drugim mrežnim servisima putem lokalnih mrežnih resursa se vrši u mreži preko koje se pristupa.

Kako bi se autentifikacione poruke na siguran način razmenjivale između korisnika u posećenoj instituciji i RADIUS servera njegove/njene matične institucije, RADIUS arhitektura na koju se oslanja eduroam servis je organizovana hijerarhijski. Hijerarhijska struktura RADIUS infrastrukture se sastoji iz tri nivoa:

- Najviši (vršni) nivo čine evropski RADIUS serveri, ETLR (*European Top-Level RADIUS*) koji sadrže listu povezanih nacionalnih domena.
- Drugi nivo predstavljaju nacionalni FTLR (*Federation Top-Level RADIUS*) serveri koji sadrže listu institucionalnih domena unutar te zemlje. FTLR serverima upravlja nacionalni *roaming* operator, a u Srbiji to je AMRES.
- Treći nivo predstavljaju RADIUS serveri krajnjih institucija, davaoca identiteta i/ili resursa. Naime, svaka institucija može učestvovati u eduroam servisu, tako što svojim korisnicima obezbeđuje eduroam servis (davalac identiteta) i/ili tako što kroz eduroam servis daje pristup Internetu (davalac resursa).

U ovom dokumentu predstavljen je sistem za nadgledanje nacionalne RADIUS hijerarhije koju čine pojedinačni RADIUS serveri institucija i FTLR server. Prvo je predstavljena RADIUS infrastruktura AMRES mreže za čije potrebe je razvijeno ovo rešenje. U nastavku je detaljno opisan način realizacije sistema za nadgledanje. Na kraju su predstavljene konkretni slučajevi u okviru kojih se vrši testiranje RADIUS servera sa primerima rezultata koji su dobijeni u AMRES mreži.

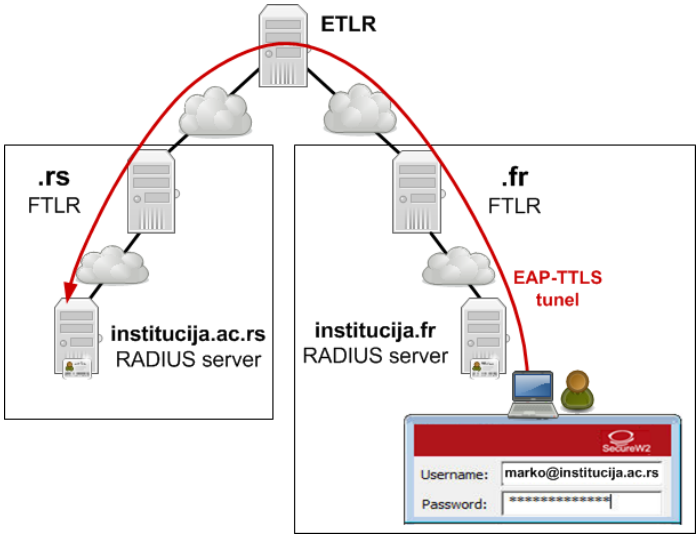
2 Hijerarhijska struktura RADIUS infrastructure

U okviru AMRES mreže RADIUS hijerarhija se sastoji od RADIUS servera lociranih u institucijama članicama eduroam servisa, koji su direktno povezani sa FTLR serverom. RADIUS serveri institucija su odgovorni za autentifikaciju svojih korisnika bilo da korisnik pokušava da koristi eduroam servis u svojoj ili nekoj drugoj, posećenoj, instituciji. Matične institucije su takođe odgovorne za održavanje podataka i kredencijala svojih korisnika. Oni se obično čuvaju u bazi podataka koju zatim RADIUS server koristi u procesu autentifikacije.

Korisničko ime je u formi *korisničko-ime@domen-institucije*, gde *domen-institucije* predstavlja DNS (*Domain Name Server*) ime institucije. RADIUS serveri koriste informaciju o domenu institucije kako bi odlučili da li zahtev treba da se obradi lokalno (sam server je zadužen za navedeni domen) ili je potrebno da se zahtev rutira kroz hijerarhijsku strukturu do RADIUS servera matične institucije korisnika.

Korišćenjem odgovarajućih EAP metoda za autentifikaciju, od uređaja kojim korisnik pristupa mreži (npr. računar, mobilni telefon) do servera za autentifikaciju u njegovoj matičnoj instituciji, uspostavlja se siguran tunel kroz koji se prenose odgovorajuće informacije radi autentifikacije korisnika. U okviru AMRES eduroam servisa koriste se EAP-TTLS (*EAP Tunneled Transport Layer Security*) [1] ili PEAP (*Protected EAP*) protokoli [2]. Ova dva autentifikaciona metoda služe za uspostavljanje sigurnih TLS (*Transport Layer Security*) sesija (tunela) od uređaja krajnjeg korisnika do autentifikacionog servera na njegovoj matičnoj instituciji tako da su osetljive informacije korisnika zaštićene od eventualnih prisluškivanja. Primer uspostavljanja EAP-TTLS sigurnosnog tunela u okviru eduroam servisa dat je na slici 1.

Vrste informacija koje se razmenjuju unutar TLS tunela zavise od protokola koji se koristi za proveru identiteta korisnika, a to mogu biti PAP (*Password Authentication Protocol*), CHAP (*Challenge Handshake Auth Protocol*), MSCHAP (*Microsoft CHAP*), EAP-GTC (*Generic Token Card*) ili *MD5-Challenge* protokoli.



Slika 1: eduroam autentifikacija

3 Sistem za nadgledanje RADIUS infrastrukture

Sistem za nadgledanje RADIUS infrastrukture u Akademskoj mreži Republike Srbije je realizovan u okviru centralnog sistema za nadgledanje računarske mreže, NetIIS (*Networking Information and Monitoring System*), koji je razvijen u Računarskom centru Univerziteta u Beogradu [3].

U okviru NetIIS sistema sprovodi se pasivno i aktivno nadgledanje stanja opreme i servisa u celoj AMRES mreži. Monitoring alati mogu da nadgledaju različite parametre, a za svaki tip nadgledanja može se konfigurisati interval vremena za koji će se monitoring izvršavati. Elementi NetIIS sistema preko kojih se vrši nadgledanje se nazivaju monitori. Monitorima se može pridružiti grafički prikaz vremenskih statistika koji se oslanja na RRD (*Round-Robin Database*) i MRTG (*Multi Router Traffic Grapher*) sistem. Takođe, svakom monitoru mogu se pridružiti alarmi koji će obaveštavati korisnika o nekom događaju vezanom za monitor.

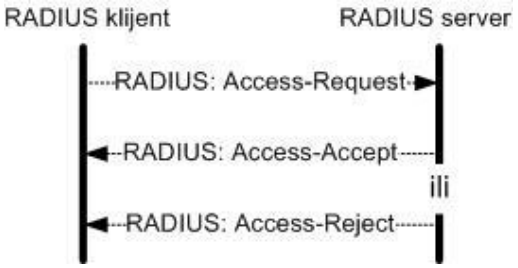
U svrhu testiranja dostupnosti RADIUS servera u NetIIS sistemu, implementirani su monitori koji testiraju dostupnost RADIUS servera preko mreže pomoću ICMP protokola. Međutim, čak i ako je neki server dostupan preko mreže, to ne znači da je on i operativan. RADIUS proces može iz nekog razloga da bude isključen tako da i pored dostupnosti servera, servis zapravo ne radi. Iz tog razloga vrši se i nadgledanje operativnosti samog RADIUS servisa na serveru.

Za testiranje funkcionalnosti RADIUS servisa koristi se *eapol_test* program [4]. Ovaj program se nalazi u sklopu *wpa_supplicant* softvera [5] koji predstavlja WPA (*Wi-Fi Protected Access*) *supplicant*, softver na korisničkom uređaju koji pruža podršku za WPA i WPA2 (*Wi-Fi Protected Access II*) protokole.

Eapol_test program se koristi za simulaciju pristupnog uređaja koji šalje *Access-Request* poruke RADIUS serveru kako bi autentifikovao korisnika koji želi pristup mreži (Slika 2). Ulazni parametri za ovaj test su: IP adresa RADIUS servera koji treba da autentifikuje korisnika ili da zahtev prosledi RADIUS serveru koji će izvršiti autentifikaciju, protokol koji se koristi za autentifikaciju klijenata i test nalog (korisničko ime i lozinka). Svaka institucija članica Akademske mreže Republike Srbije, učesnica eduroam servisa mora da kreira poseban korisnički nalog koji će se koristiti isključivo za testiranje RADIUS servera. Ukoliko se taj test nalog nalazi u bazi podataka, zajedno sa ostalim korisničkim nalozima, uz operativnost RADIUS servera proverava se i komunikacija između RADIUS servera i korisničke baze. Preko *eapol_test* programa *Access-Request* poruka sa korisničkim kredencijalima iz testnog naloga se šalje RADIUS serveru koji se testira. Na ovaj način se zatvara EAP TTLS ili PEAP tunel.

Na serveru na kom je instaliran NetIIS sistem kreirana je *shell* skripta koja pokreće *eapol_test*. NetIIS monitori periodično, na svakih 5 minuta, pokreću ovu skriptu. Kako NetIIS podržava integraciju sa *Nagios* monitorima, skripta za monitoring je napravljena tako da rezultat rada prikazuje u *Nagios* formatu. Ako RADIUS server na primljeni zahtev odgovori sa *Access-Accept* porukom monitor pruža informaciju da je sve u redu. U suprotnom, u okviru monitora aktivira se alarm koji šalje *email* obaveštenja definisanoj grupi korisnika (tehničkim kontaktima institucije) da postoji problem sa funkcionisanjem RADIUS servera. Kada se problem reši i vrednost monitora se promeni, alarm u okviru monitora će se takođe aktivirati, a ista grupa korisnika biće obaveštena o ispravnom radu njihovog RADIUS servera. Dakle, putem NetIIS sistema šalju se obaveštenja tehničkim

kontaktima institucija svaki put kada se promeni vrednost monitora.



Slika 2: Tok razmene RADIUS poruka tokom autentifikacije

Shell skripta čijim pokretanjem NetIIS sistem šalje zahteve testiranim RADIUS serverima je data u nastavku.

```
#!/bin/bash
#Input variables
a1=$2
a2=$4
a3=$6
a4=$8
shift 2
a5=$8
shift 2
a6=$8

#Defining of the eap.conf.randomnumber file that contains the data for the
#eapol_test script
xy=`cat /dev/urandom | tr -dc _A-Z-a-z-0-9 | head -c8`
touch ./eap.conf.$xy

#Defining the authentication protocol used within TLS tunnel.
#With EAP-TTLS protocol PAP protocol is used, and in case of PEAP protocol
#MSCHAPv2 is used
if [ "$a6" == "TTLS" ]; then
phase2="auth=PAP"
else
phase2="autheap=MSCHAPV2"
fi

#Population of eap.conf.randomnumber file
echo network={                          >./eap.conf.$xy
echo        ssid=\"eduroam\"            >>./eap.conf.$xy
echo        key_mgmt=WPA-EAP            >>./eap.conf.$xy
echo        eap=$a6                     >>./eap.conf.$xy
echo        identity=\"$a2\"            >>./eap.conf.$xy
echo        anonymous_identity=\"$a3\"  >>./eap.conf.$xy
echo        password=\"$a4\"            >>./eap.conf.$xy
echo        phase2=\"$phase2\"          >>./eap.conf.$xy
echo        }                           >>./eap.conf.$xy
#Time variable t1 defines the beginning of the eapol_test script execution
```

```
t1=`date +%s%N`
# Execution of eapol_test script
a=`eapol_test -c eap.conf.$xy -a $a1 -s $a5 -r 1 -t 10 2>/dev/null| tail -1`
#Time variable t2 defines the end of the eapol_test script execution
t2=`date +%s%N`
#dtN defines how long eapol_test script takes to execute
dtN=`expr $t2 - $t1`
dt=`expr $dtN / 1000000`

rm -fr ./eap.conf.$xy
#Creating the Nagios output form
if [ "$a" == "SUCCESS" ]; then
        echo "OK" "|""value=1;Response time:$dt ms"
else
        echo "False" "|""value=0;Response time:$dt ms;Radius virtual server
credential error or eduroam user doesn't exist or radius down!"
fi
```

Ulazni parametri koje skripta zahteva su:

- `a1` - IP adresa RADIUS servera koji se testira. To može da bude RADIUS server institucije davaoca identiteta i/ili davaoca resursa i FTLR server.
- `a2` - Korisničko ime test naloga.
- `a3` - Anonimni identitet.
- `a4` - Lozinka test naloga.
- `a5` - Deljeni tajni ključ koji se koristi kako bi testirani RADIUS server prihvatio zahteve koji se šalju sa NetIIS servera. Isti ključ mora da bude definisan i na strani RADIUS servera.
- `a6` - Protokol koji se koristi za autentifikaciju klijenta. U AMRES mreži implementirani su ili EAP TTLS/PAP ili PEAP/MSCHAPv2 protokoli.

Ulazni parametri se popunjavaju preko NetIIS *web* interfejsa. U okviru skripte, unesene vrednosti upisuju se u odgovarajuće promenljive. Na osnovu dela promenljivih (`a2`, `a3`, `a4` i `a6`) formira se *eap.conf* konfiguracioni fajl. Konfiguracioni fajl ima predefinisanu strukturu jer se zajedno sa ostalim podacima (`a1` i `a5`) poziva prilikom pokretanja *eapol_test* programa. Rezultat tako pokrenutog *eapol_test* programa se dodeljuje promenljivoj `a` i njena vrednost može biti SUCCESS ili FAILURE. Na osnovu dobijenog rezultata NetIIS monitor koji pokreće skriptu dobija odgovarajuću vrednost: 1 ukoliko je primljena *Access-Accept* poruka ili 0 ukoliko je primljena *Access-Reject* poruka.

U okviru skripte se takođe beleže vremena neposredno pre pokretanja *eapol_test* programa i nakon dobijenog odgovora, na osnovu čega se izračunava vreme neophodno testiranom RADIUS serveru da pošalje odgovor na autentifikacioni zahtev.

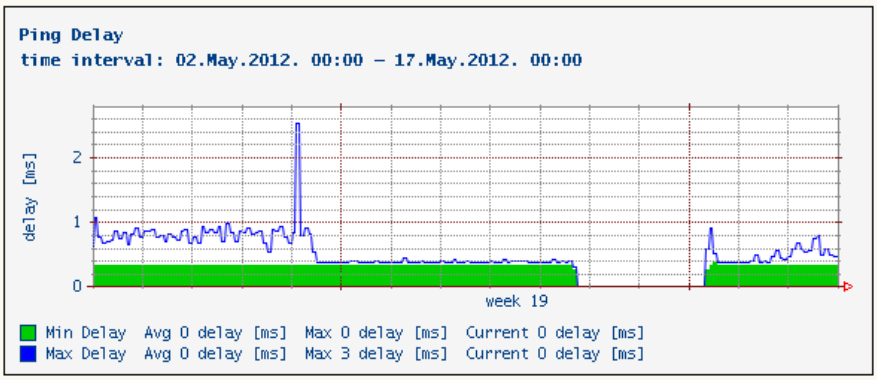
Skripta je optimizovana za pokretanje preko NetIIS sistema. Međutim, vrlo je jednostavna i lako se može prilagoditi bilo kojem sistemu za nadgledanje koji je dovoljno fleksibilan i konfigurabilan tako da dozvoljava kreiranje i izvršavanje *Linux* skripti ili *Nagios* monitora. Čak i u situacijama kada ne postoji sistem za nadgledanje računarske mreže, skripta se može dopuniti funkcijama za slanje *email* poruka kojima bi se tehnički kontakti institucija obaveštavali o promeni stanja njihovih RADIUS servera, a zatim periodično izvršavati pomoću *Linux cron* servisa.

4 Nadgledani parametri

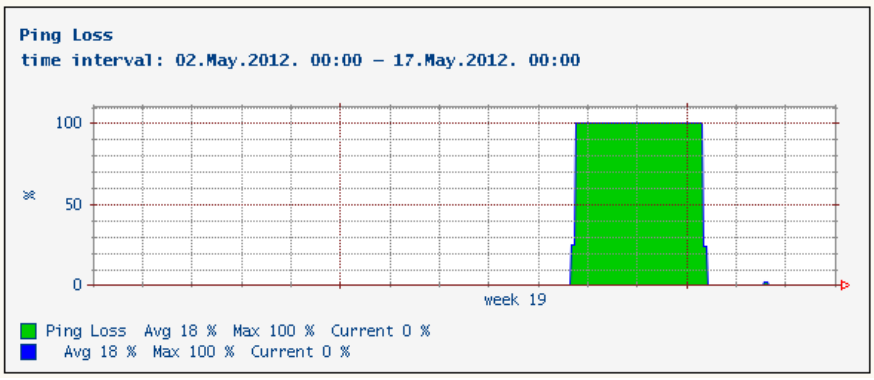
U NetIIS sistemu konfigurisane su dve grupe monitora u cilju nadgledanja RADIUS infrastrukture. Jedna grupa monitora testira dostupnost RADIUS servera kroz mrežu, dok je druga grupa monitora osmišljena da testira operativnost i merenje performansi rada RADIUS servera.

4.1 Testiranje dostupnosti RADIUS servera

Za proveru dostupnosti servera konfigurisan je *ping* monitor. Ovaj monitor šalje ICMP zahteve na IP adresu RADIUS servera. Na osnovu primljenog odgovora prikazuju se grafici kašnjenja (Slika 3a) i gubitka paketa (Slika 3b) u toku odabranog vremenskog perioda.



Slika 3a: Kašnjenje ICMP paketa koji se razmenjuju sa RADIUS serverom, za period od 15 dana



Slika 3b: Gubitak ICMP paketa koji se razmenjuju sa RADIUS serverom, za period od 15 dana

Ukoliko je server nedostupan, gubitak paketa će iznositi 100%. Ako postoje problemi u mreži, npr. mreža je zagušena, to će biti prikazano kao određeni procenat gubitka paketa, manji od 100%. Dakle, i postojanje

smetnji u mreži na putu do RADIUS servera može da se ustanovi na osnovu ovih grafika. Kako se RADIUS oslanja na UDP protokol ova informacija može biti veoma bitna. Sa slika 3a i 3b može da se zaključi da je RADIUS server bio nedostupan 3 dana (od 11. do 14. maja) jer je procenat gubitaka ICMP paketa u to vreme iznosio 100%, a vrednosti kašnjenja paketa nisu zabeležene.

4.2 Testiranje operativnosti RADIUS servera

Funkcionalnost RADIUS servera se razlikuje u slučaju kada je institucija kojoj server pripada davalac identiteta i kada je davalac resursa. RADIUS server institucije davaoca identiteta treba da obradi pristigle zahteve za autentifikaciju lokalnih korisnika. Ako je institucija i davalac resursa, RADIUS server treba da bude konfigurisan da zahteve korisnika drugih institucija prosleđuje FTLR serveru koji će, zatim, zahtev da prosledi RADIUS serveru matične institucije korisnika. Ukoliko bi institucija bila isključivo davalac resursa, njen RADIUS server bi prosleđivao sve pristigle zahteve FTLR serveru. Stoga su, prilikom konfiguracije monitora koji testiraju operativnost RADIUS servera, u obzir uzeta četiri moguća scenarija:

- Scenario 1 simulira situaciju u kojoj eduroam korisnik koristi eduroam servis u svojoj matičnoj instituciji. Na ovaj način se proverava kako testirani RADIUS server obrađuje direktno pristigle zahteve za autentifikaciju lokalnih korisnika.

- Scenario 2 predstavlja situaciju u kojoj korisnik institucije čiji se RADIUS server testira koristi eduroam servis na nekoj drugoj instituciji. Odgovarajućim monitorom se proverava kako testirani RADIUS server obrađuje zahtev za autentifikaciju lokalnog korisnika koji je primio od FTLR servera.

  Prva dva scenarija se koriste za testiranje funkcionalnosti RADIUS servera institucije koja je davalac identiteta.

- Scenario 3 simulira situaciju kada korisnik neke druge institucije koristi eduroam servis na instituciji čiji se RADIUS server testira. Odgovarajući monitor se koristi za proveru funkcionalnosti RADIUS servera institucije koja je davalac resursa. Naime, testira se da li RADIUS server prosleđuje zahtev za autentifikaciju korisnika druge institucije FTLR serveru.

  Monitori u okviru kojih su implementirani ovi testovi za AMRES institucije članice eduroam servisa se mogu naći ovde, http://netiis.rcub.bg.ac.rs/netiis/NetIIS?service=main&ID=group.35865.

- Scenario 4 se koristi za testiranje da li FTLR server uspešno prosleđuje autentifikacione zahteve korisnika.

  Monitori koji testiraju funkcionalnost AMRES FTLR servera se nalaze na ovoj lokaciji, http://netiis.rcub.bg.ac.rs/netiis/NetIIS?service=main&ID=group.37378.

Kombinacija ovih testova pomaže da se lociraju problemi u radu RADIUS infrastrukture. Ako je test za prvi scenario prošao uspešno, a za drugi neuspešno, zaključuje se da RADIUS server može da autentifikuje lokalne korisnike, ali da postoji problem između testiranog servera i FTLR servera. U tom slučaju je verovatno došlo do jednog od sledećih problema:

- Prilikom konfiguraciju FTLR servera je došlo do greške, stoga on nije u mogućnosti da zahtev prosledi testiranom RADIUS serveru.

- Postoji problem u komunikaciji između RADIUS servera institucije i FTLR servera (pogrešno konfigurisani parametri za povezivanje, RADIUS serveri nisu dostupni jedan drugom preko mreže itd.)

- FTLR server nije operativan, na šta će ukazati monitor za četvrti scenario.

Ukoliko su i test za prvi i test za drugi scenario neuspešni zaključuje se da RADIUS server institucije ne funkcioniše ispravno. To, naravno, ne eliminiše mogućnost da postoji problem i sa operativnošću FTLR servera. Zato se koristi monitor za scenario 4 koji ukazuje na ispravnost rada FTLR servera.

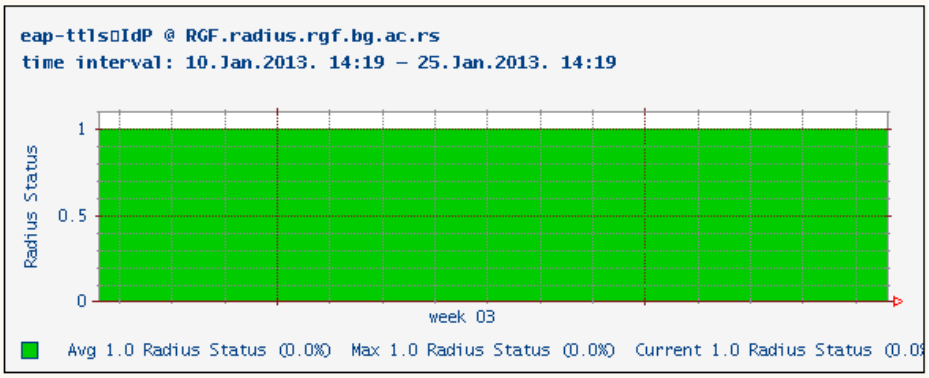
Pad monitora za scenario 3, može biti prouzrokovan problemom u funkcionisanju ili testiranog RADIUS servera ili FTLR servera. Stanje monitora za scenario 4 u tom slučaju pomaže da se utvrdi lokacija problema kako bi se moglo pristupiti njegovom rešavanju.

4.2.1 Scenario 1

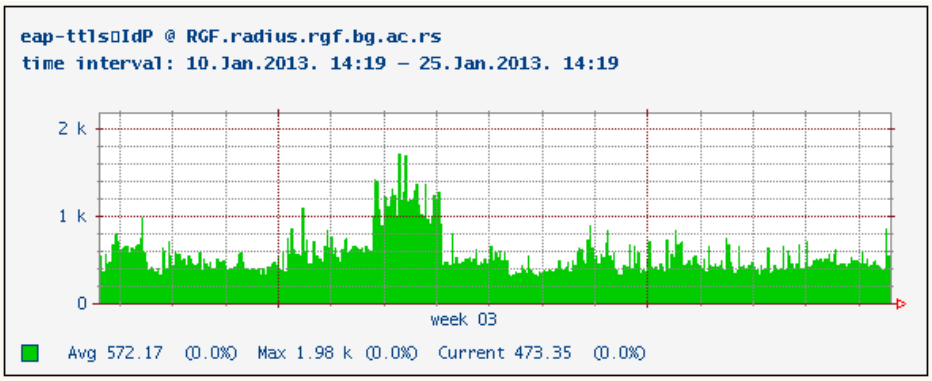
Odgovarajući monitor u NetIIS sistemu preko skripte pokreće *eapol_test* koji simulira klijenta koji šalje zahtev RADIUS serveru čime se između njih zatvara direktan EAP TTLS ili PEAP tunel, u zavisnosti od protokola koji je implementiran na instituciji čiji se RADIUS server testira (Slika 4). Za autentifikaciju se koriste kredencijali iz test naloga. RADIUS server obrađuje primljeni zahtev i na osnovu dobijenog rezultata iscrtava se grafik statusa servera (Slika 5a). Ako je primljena *Access-Accept* poruka status ima vrednost jedan. U suprotnom vrednost statusa je nula. Takođe se dobija i grafik kašnjenja odgovora (Slika 5b). Kada je sve funkcionalno kašnjenje ima konstantnu vrednost u toku vremena. Ukoliko vrednost kašnjenja varira tokom vemena može se zaključiti da postoje problemi u radu samog servera, npr. server je opterećen, što može ukazivati na mogućnost DoS (*Denial-of-Service*) napada na RADIUS serveru. Kašnjenje poruka može biti posledica problema u komunikaciji između RADIUS servera i korisničke baze podataka (u slučaju kada se test nalog čuva u korisničkoj bazi podataka) ili postojanja smetnji u mreži na putu do RADIUS servera.

Napomena: ukoliko odgovor ne stigne do NetIIS sistema, na grafiku kašnjenja biće prikazana vrednost 10s, što predstavlja vremenski period čekanja odgovora (*timeout* parametar) definisan u skripti prilikom pokretanja *eapol_test* programa.

Slika 4: Formiranje EAP tunela direktno između klijenta i RADIUS servera



Slika 5a: Status RADIUS servera u periodu od 15 dana, prvi scenario

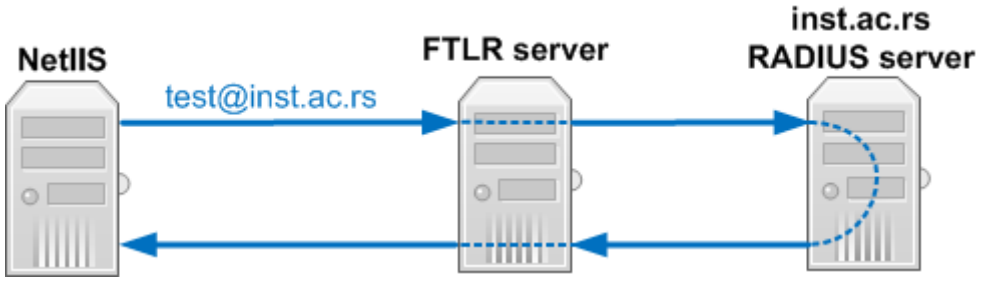


Slika 5b: Kašnjenje odgovora RADIUS servera u periodu od 15 dana, prvi scenario

Sa slike 5a se može videti da je za prikazanih 15 dana nadgledani RADIUS server uspešno obrađivao sve dobijene zahteve jer je status servera 1, ali na slici 5b se može primetiti da je u toku jednog dana (16. januara) vrednost kašnjenja poruka porasla ili zbog opterećenosti servera, ili zbog eventualnih smetnji u mreži.

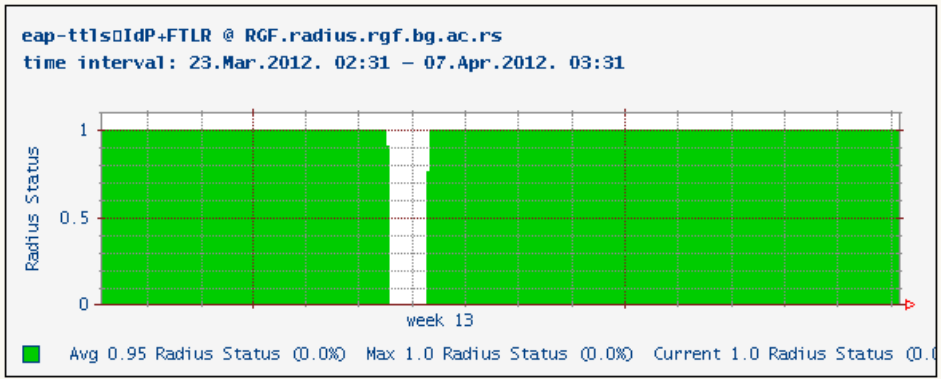
4.2.2 Scenario 2

Kako bi se nadgledao EAP tunel formiran između klijentskog uređaja i RADIUS servera preko FTLR servera implementirani monitor za scenario 2 preko *eapol_test* programa šalje zahtev korišćenjem istih korisničkih kredencijala kao u prethodnom scenariju, ali sada na IP adresu FTLR servera koji, ako je sve operativno, taj zahtev prosleđuje testiranom RADIUS serveru (Slika 6).

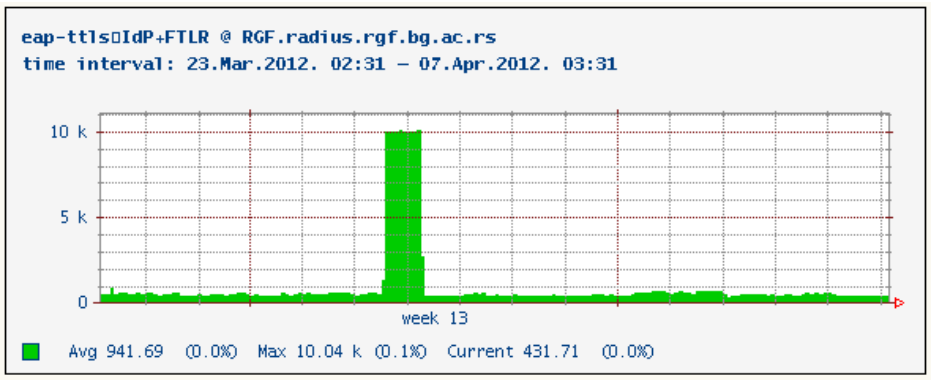


Slika 6: Formiranje EAP tunela između klijenta i RADIUS servera preko FTLR servera

Na osnovu dobijenih rezultata iscrtavaju se grafici statusa servera (Slika 7a) i kašnjenja odgovora (Slika 7b).



Slika 7a: Status RADIUS servera u periodu od 15 dana, drugi scenario

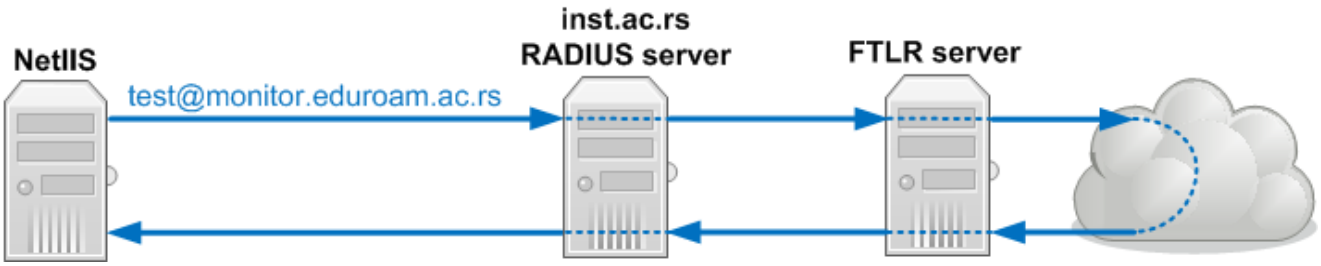


Slika 7b: Kašnjenje odgovora RADIUS servera u periodu od 15 dana, drugi scenario

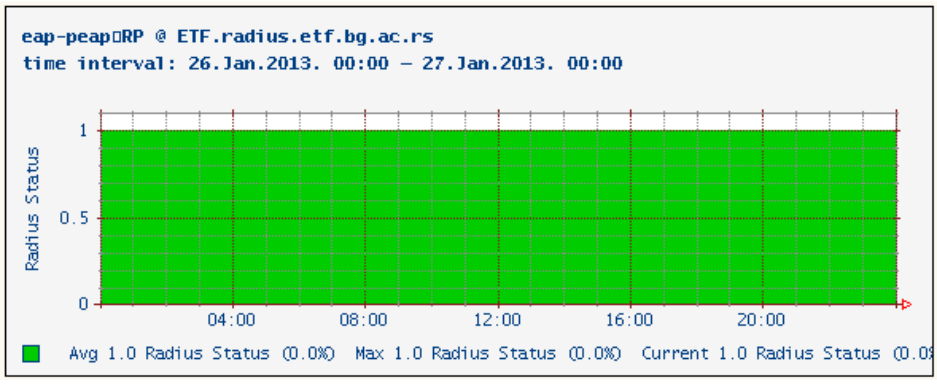
Sa slike 7a se vidi da NetIIS sistem nije primao odgovore od testiranog RADIUS servera u periodu od 28. do 29. marta 2012. Na grafiku sa slike 7b, stoga, vrednost kašnjenja iznosi 10s, što je vrednost *timeout* parametra definisanog prilikom pokretanja *eapol_test* programa.

4.2.3 Scenario 3

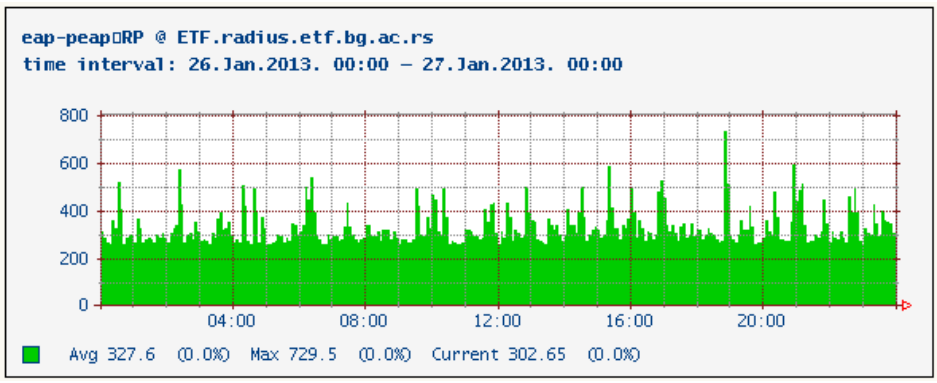
Kako bi se testirala operativnost RADIUS servera koji zahteve za autentifikaciju korisnika treba da prosledi FTLR serveru (Slika 8), instaliran je dodatni, testni RADIUS server koji se koristi samo za potrebe nadgledanja. Preko *eapol_ test* programa monitor u NetIIS-u šalje zahtev direktno RADIUS serveru koji se testira ali se sada koriste autentifikacioni podaci testnog naloga sa testnim domenom koji je definisan u okviru testnog RADIUS servera. RADIUS server primljeni zahtev prosleđuje FTLR serveru koji dalje zahtev prosleđuje testnom RADIUS serveru. Naravno, FTLR server je konfigurisan da komunicira sa testnim RADIUS serverom. Na osnovu dobijenih rezultata formiraju se grafici statusa servera (Slika 9a) i kašnjenja odgovora (Slika 9b).



Slika 8: Formiranje EAP tunela direktno između klijenta i RADIUS servera njegove matične institucije preko RADIUS servera koji se testira



Slika 9a: Status RADIUS servera u toku jednog dana, treći scenario

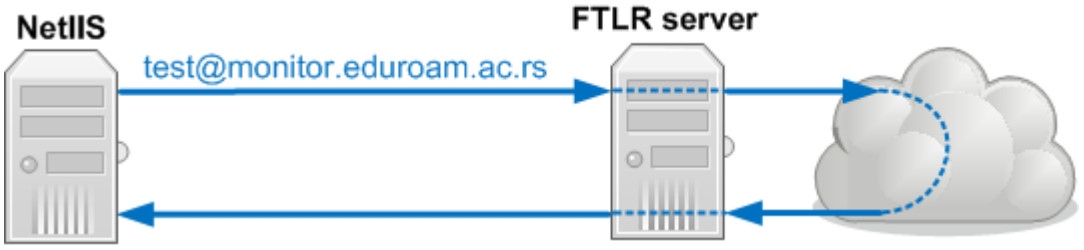


Slika 9b: Kašnjenje odgovora RADIUS servera u toku jednog dana, treći scenario

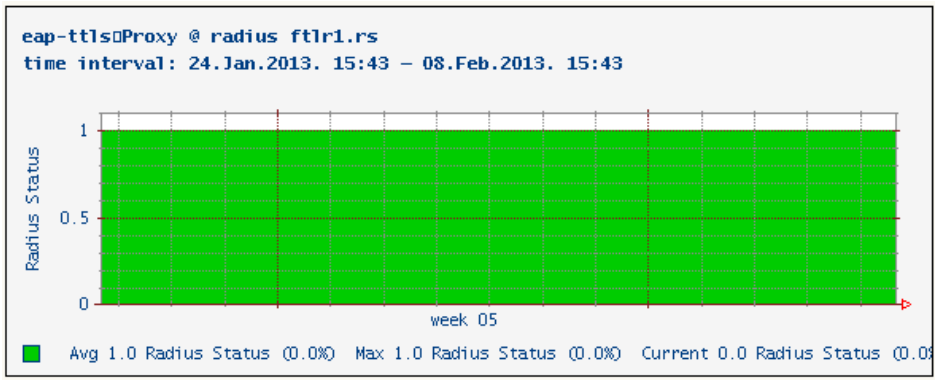
Na slikama 9a i 9b prikazani su primeri kada je nadgledani RADIUS server ispravno funkcionisao. Vrednost radius statusa je 1, a kašnjenje je konstantno i u proseku iznosi 330 ms.

4.2.4 Scenario 4

Testni RADIUS server iz prethodnog scenarija se takođe koristi prilikom provere funkcionalnosti FTLR servera. Preko *eapol_test* programa se šalje zahtev za autentifikaciju testnog korisnika direktno FTLR serveru. FTLR server prosleđuje zahtev testnom RADIUS serveru, čiji odgovor šalje natrag NetIIS sistemu (Slika 10). Na osnovu dobijenih rezultata prikazuje se grafik statusa servera. Kašnjenje poruka u slučaju testiranja FTLR servera nije od značaja s obzirom da su server na kome se nalazi NetIIS sistem i FTLR server locirani u istoj LAN (*Local Area Network*) mreži.



Slika 10: Formiranje EAP tunela preko FTLR servera



Slika 11: Status FTLR servera u periodu od 15 dana, četvrti scenario

Ovim je kompletiran sistem za nadgledanje nacionalne RADIUS infrastrukture koji čini jednostavno, skalabilno i centralizovano rešenje. Implementiran je sistem monitora koji pružaju uvid u ispravnost rada i dostupnost nacionalne hijerarhije RADIUS servera. Sistem alarma je takođe implementiran kako bi se zadužene osobe na vreme obavestile o eventualnim greškama u funkcionisanju servisa. Izloženi principi nadgledanja RADIUS

servera su primenljivi i u manje kompleksnim konfiguracijama autentifikacione infrastrukture, ali i na druge servise koji postoje u okviru telekomunikacionih mreža.

5 Rečnik

RADIUS	Remote Authentication Dial In User Service
FTLR	Federation Top Level RADIUS
ETLR	European Top Level RADIUS
EAP	Extensible Authentication Protocol
EAP-TTLS	EAP Tunnelled Transport Layer Security
PEAP	Protected EAP
TLS	Transport Layer Security
PAP	Password Authentication Protocol
MSCHAPv2	Microsoft Challenge Handshake Auth Protocol version 2
NetIIS	Networking Information and Monitoring System
MRTG	Multi Router Traffic Grapher
WPA	Wi-Fi Protected Access

6 Literatura

[1] P. Funk, S. Blake-Wilson, “Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP TTLSv0)”, RFC 5281, August 2008.

[2] A. Palekar, D. Simon, G. Zorn, S. Josefsson “Protected EAP protocol (PEAP)”, INTERNET-DRAFT, March 2003

[3] S. Gajin, D. Pajin, D. Novaković, “Sistem za nadgledanje računarske mreže - NetIIS”, YuInfo, 2006.
http://www.e-drustvo.org/proceedings/YuInfo2006/html/pdf/149.pdf

[4] Deploying RADIUS
http://deployingradius.com/scripts/eapol_test/

[5] Linux WPA/WPA2/IEEE 802.1X Supplicant
http://hostap.epitest.fi/wpa_supplicant/