PSSOH 2022, DOI: https://doi.org/10.5281/zenodo.7139492

Upravljanje logovima i vizualizacija statistika korišćenja AMRES servisa upotrebom alata otvorenog koda

Todosijević Andrijana[1], Simonović Katarina[1], Arsović Anđela[1]

1: Akademska mreža Republike Srbije - AMRES, 11000, Beograd, Srbija
elektronska pošta: andrijana.todosijevic@amres.ac.rs, katarina.simonovic@amres.ac.rs, andjela.arsovic@amres.ac.rs

REZIME

Log poruke predstavljaju automatski dokumentovane događaje u formi hronoloških zapisa koji sadrže različite informacije o IT sistemu i mreži. Upravljanje log porukama je od velikog značaja za svaku organizaciju, pa i Akademsku mrežu Republike Srbije (AMRES) i omogućava efikasnu i kvalitetnu analizu rada i upotrebu kako servisa, tako i mreže u celini. Od izuzetne važnosti je i mogućnost brze i jednostavne pretrage velikog broja generisanih log poruka, rešavanje problema i izdvajanje bitnih podataka za kasniju upotrebu. Elastic Stack softver je sveobuhvatan alat otvorenog koda koji omogućava prikupljanje i pretragu velike količine log poruka različitog tipa, kreiranje dinamičkih izveštaja i grafičkog prikaza željenih rezultata. U radu su razmatrani i detaljno objašnjeni procesi prikupljanja i analize log poruka AMRES eduroam servisa i dati primeri upotrebe Grafana alata otvorenog koda u prikazu statistika korišćenja servisa od strane AMRES krajnjih korisnika.

Ključne reči: logovi, upravljanje logovima, Elastic Stack, Grafana, eduroam.

1 Upravljanje logovima

Upravljanje log porukama je složen proces koji za cilj ima generisanje, prenos, skladištenje, zatim i analizu velike količine podataka u okviru informacionog sistema [1]. Log poruke se sastoje od hronoloških zapisa koji sadrže različite informacije i predstavljaju automatski dokumentovane događaje u samom sistemu i mreži. Prvobitno, logovi su korišćeni za identifikaciju sigurnosnih incidenata i rešavanje problema, ali danas imaju mnogo dodatnih i podjednako značajnih funkcija. Koriste se za optimizovanje performansi servisa i mreže, praćenje ponašanja korisnika i generisanje podataka korisnih za istraživanje i analizu njihovih aktivnosti. Rast broja, obima i raznovrsnosti logova praćen je povećanjem potrebe za upravljanjem log porukama. Upravljanje logovima je ključan segment zaštite i održavanja funkcionisanja servisa i mreže. Sposobnost prikupljanja različitih log poruka sa više izvora na jednom mestu, kao i njihova automatska pretraga i analiza, od velikog su značaja za svako IT okruženje. Veliki broj alata i softvera omogućavaju brzu i uspešnu analizu problema, kao i trenutno delovanje i akcije bez potrebe za manuelnim prikupljanjem, organizovanjem i pretragom velike količine podataka. Koristeći ove mogućnosti i funkcionalnosti, organizacija može na veoma efikasan način da održava mrežu i servise. Svaka organizacija ima višestruku korist od procesa sakupljanja i upravljanja logovima. Na ovaj način je omogućeno da se svi detalji čuvaju u obliku zapisa za određeni vremenski period. Rutinski pregledi i analiza logova su ključni za identifikaciju incidenata, problema u funkcionisanju mreže i servisa, kao i rešavanje istih. Takođe, mogu imati veliku ulogu u

analizi ponašanja krajnjih korisnika, biti deo internih istraživanja, uspostavljanja osnova i identifikacije operacionih trendova i dugoročnih problema [1]. U radu je opisano upravljanje logovima kojima se monitorišu servisi i aplikacije u AMRES mreži, kao i alati koji se u tu svrhu koriste, navedeni u Tabeli 1.

Tabela 1: Alati koji se koriste u procesu upravljanja logovima.

Naziv softvera	Tip softvera	Funkcija softvera
freeradius	alat otvorenog koda	RADIUS server
syslog-ng	alat otvorenog koda	generisanje i prikupljanje log poruka
Logstash	alat otvorenog koda	prikupljanje i obrada log poruka
Elasticsearch	alat otvorenog koda	indeksiranje, skladištenje, pretraga i analiza log poruka
Kibana	alat otvorenog koda	vizualizacija, pretraga i analiza log poruka
Grafana	alat otvorenog koda	vizualizacija metrika i vremenskih serija log poruka

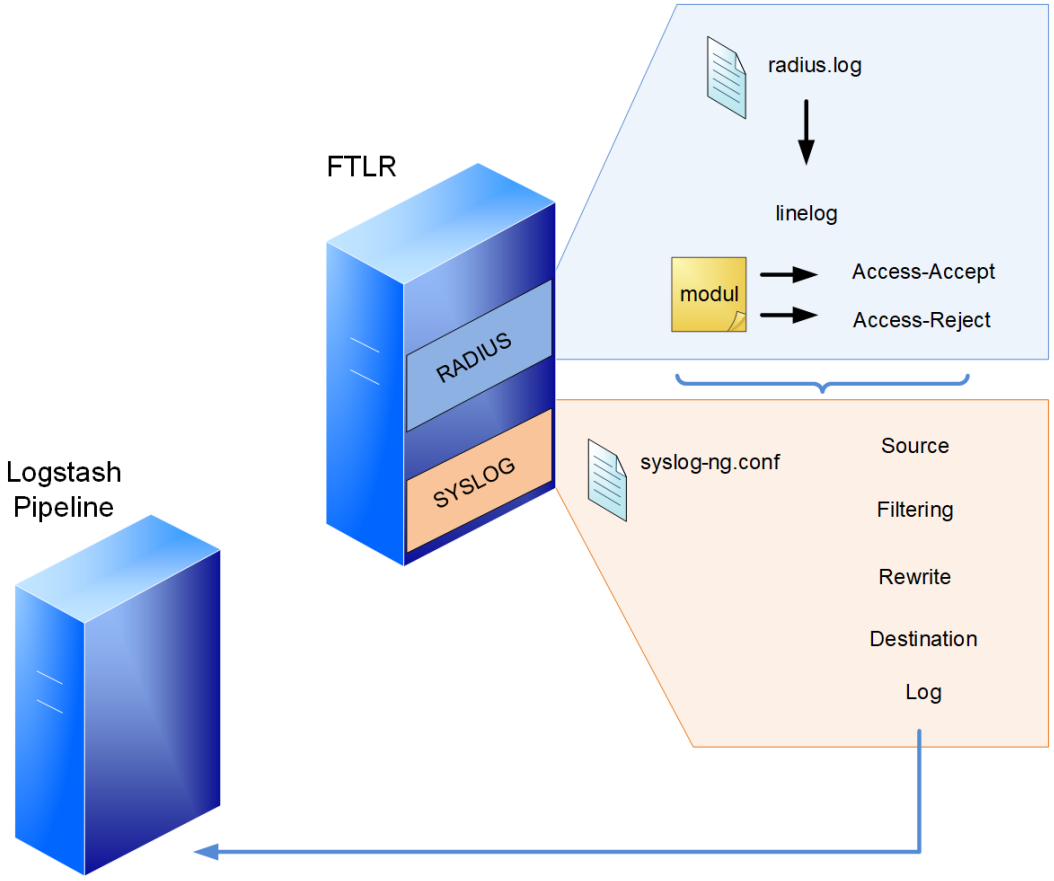
AMRES prati rad i korišćenje više servisa, a implementacija i funkcionisanje Elastic Stack [2] i Grafana [3] softvera razmatrana je sa aspekta primene u eduroam servisu. U Poglavlju 2 objašnjen je način generisanja logova i dat prikaz osnovne konfiguracije syslog-ng protokola koji se za tu priliku koristi. Implementacija Elastic Stack okruženja razmatrana je u Poglavlju 3. Opisana je konfiguracija Logstash pipeline alata za obradu i filtriranje log poruka, kao i Elasticsearch klastera za prikupljanje i skladištenje logova. Razmatrani su i način pretraživanja, prikaza i analize izdvojenih rezultata korišćenjem Grafana alata.

2 Generisanje i prikupljanje log poruka

Infrastruktura upravljanja log porukama obuhvata hardver, softver, mrežu i uređaje koji se koriste za njihovo generisanje, prikupljanje, skladištenje, analizu i upotrebu [1]. Ova infrastruktura takođe obuhvata i nekoliko funkcionalnosti koje predstavljaju dopunu prethodno navedenim procesima. Neke od njih su i parsiranje logova (izdvajanje podataka iz loga tako da se parsirane vrednosti mogu koristiti kao inputi za druge log procese), filtriranje i agregaciju događaja. Proces prikupljanja i skladištenja podrazumeva redukciju, kompresiju, konverziju, arhiviranje logova, kao i rotaciju log fajlova prema određenom rasporedu i proveru njihovog integriteta. Poslednji korak je analiza logova koja se sastoji od mapiranja zapisa iz jednog ili više izvora (na osnovu IP adrese, DNS imena, tipa događaja itd.), prikaza logova i kreiranja izveštaja. Postoje različiti načini generisanja i prikupljanja logova. Iako se u okviru Eastic Stack softvera u ovu svrhu koriste Beats alati, za potrebe praćenja rada određenih AMRES servisa od značaja, koristi se syslog-ng softver koji je dostupan za Linux platforme.

2.1 Osnovna konfiguracija syslog-ng softvera za potrebe eduroam servisa

Kao jedan od najvažnijih servisa, eduroam zahteva slanje najdetaljnijih log poruka i u tu svrhu se koristi syslog-ng softver [4]. Log poruke se prosleđuju Logstash pipeline serveru, koji zatim vrši njihovu dalju obradu. Poruke koje se šalju su dobijene kao rezultat pokušaja autentifikacije krajnjih korisnika, a generiše ih RADIUS deamon. Detaljno objašenjenje svih poruka i pojedinačnih parametara iz tih poruka je dato u Poglavlju 2.2. Postupak generisanja i slanja logova razlikuje su u zavisnosti od servisa koji se monitoriše. Kako se ovaj rad fokusira na analizu log poruka eduroam servisa, na Slici 1 prikazan je način komunikacije između sistemskih komponenti koje se nalaze na istom serveru (RADIUS server, syslog-ng deamon) i udaljenog Logstash pipeline servera.



Slika 1: Postupak generisaja i prikupljanja log poruka eduroam servisa.

Osnovni nivo konfiguracije zasniva se na tri komponente:

- izvor,
- odredište i
- Log sekcija.

Konfiguracioni fajl *syslog-ng.conf* mora imati bar tri osnovna parametra, *source*, *log* i *destination*, koja su data u nastavku:

```
source s_local {
       system();
       internal();
};
destination d_logstash {
       udp("147.91.x.x" port(514));
};
log {
       source(s_local);
       destination(d_logstash);
};
```

U ovom okruženju, puna putanja do konfiguracionog fajla je */usr/local/etc/*. U konfiguraciji je označen deo koji predstavlja default UDP (User Datagram Protocol) port za syslog protokol, preko koga se omogućava slanje logova na udaljenu lokaciju [5].

2.2 RADIUS log poruke

FTLR (*Federation Top-Level RADIUS*) server je RADIUS server kroz koji prolaze autentifikacioni zahtevi prilikom pokušaja povezivanja na eduroam. Ovi autentifikacioni zahtevi mogu poticati od korisnika iz AMRES mreže, kao i od inostranih korisnika. AMRES FTLR serveri su realizovani primenom FreeRADIUS softvera [6]. Ovaj softver prema početnoj konfiguraciji beleži sve autentifikacione zahteve u *radius.log* fajl. Rezultat autentifikacije može biti poruka „Login OK“ ili „Login incorrect“. Uz primenu FreeRADIUS linelog modula, ove poruke se prepisuju tako da budu usklađene sa RADIUS RFC 2865 preporukom [7], pa za neuspešnu autentifikaciju imaju vrednost „Access-Reject“ , dok za uspešnu autentifikaciju imaju vrednost „Access-Accept“. U nastavku je dat primer konfiguracije linelog modula:

```
linelog logstash {
       filename = syslog
       format = ""
       reference = "%{%{reply:Packet-Type}:-format}"
       Access-Accept ="Access-Accept: IdP=%{tolower:%{Realm}} MAC=%{Calling-Station-
           Id} AP=%{Called-Station-Id} RP=%{Operator-Name}"
       Access-Reject ="Access-Reject: IdP=%{tolower:%{Realm}} MAC=%{Calling-Station-
           Id} AP=%{Called-Station-Id} RP=%{Operator-Name}"
```

Ovi podaci se zatim šalju syslog-ng softveru, koji filtrira, prepisuje i usmerava log poruke ka udaljenom Logstash pipeline serveru. Atribut „Called-Station-Id“ je u formatu Base Radio MAC:SSID (npr. 00--00-00-00-00-00:eduroam), koji je nedovoljno razumljiv [5]. Kako bi se dobila prepoznatljiva vrednost za AP (Access Point) atribut „Called-Station-Id“ u AP delu poruke, koriste se dva načina mapiranja:

- *rewrite* sekcija syslog-ng softvera, čime se ovaj atribut prepisuje u format koji se odnosi na lokaciju na kojoj je AP postavljen (npr. cisco1142-rcub-studenjak5), preporučuje se kada postoji manji broj AP uređaja. Nakon što log poruka prođe postupak generisanja i obrade, njen konačan format je:

  ```
  Jan 28 15:37:21 ftlr1 radiusd[31369]: Access-Accept: IdP=etf.bg.ac.rs MAC
     =48-50-73-x-x-x AP=cisco1142-rcub-studenjak5 RP=1rcub.bg.ac.rs
  ```

- *Lookup* fajl sa zapisima koje koristi Logstash pipeline, koji će biti objašnjen u Poglavlju 3.1.

RADIUS log poruka se sastoji od sledećih podataka:

- Access-Accept/Access-Reject – rezultat autentifikacije,
- IdP – domen institucije,
- MAC – MAC adresa korisničkog uređaja,
- AP – niz karaktera koji predstavlja naziv AP uređaja, na osnovu koga se određuje lokacija AP-a,
- RP – RADIUS atribut *Operator-Name* na osnovu koga se određuje Davalac Resursa, tj. kojoj instituciji pripadaju AP uređaji.

3 Elastic Stack softver otvorenog koda

Za prikupljanje i skladištenje log poruka AMRES koristi deo Elastic Stack softvera koji predstavlja skup alata otvorenog koda i formira veoma moćnu platformu za upravljanje logovima, prikupljanje i obradu podataka iz više izvora, centralizovano skladištenje na skalabilan način, uključujući i skup alata za njihovu analizu i pravljenje izveštaja. Elastic Stack softver obuhvata sledeće komponente:

- Beats
- Elasticsearch
- Logstash
- Kibana

Beats komponenta predstavlja skup alata koji služe sa formatiranje log poruka i polja u okviru log zapisa i slanje istih ka Logstash pipeline serveru. Elasticseach je NoSQL baza podataka [8] za indeksiranje, skladištenje, pretragu i analizu velike količine podataka, obezbeđujući RESTful API [9] interfejse i JSON [10] format za rad sa podacima. Ovaj alat nudi maksimalnu pouzdanost, lako upravljanje, jednostavnu implementaciju, ali i mogućnost naprednih upita. Logstash pipeline je agregator podataka koji se koristi za prikupljanje log poruka sa više izvora, omogućuje transformacije nestruktuiranih podataka, filtriranje i slanje podataka u Elasticsearch bazu. Kibana je alat za vizualizaciju podataka, implementiran tako da dopunjuje Elasticsearch i omogućuje pretragu, pregled i interakciju sa indeksiranim podacima u realnom vremenu. Koristi se primarno za analizu log poruka i omogućuje tekstualne upite i pretragu podataka [2]. Grafana je još jedan alat otvorenog koda koji se koristi za vizualizaciju metrika i vremenskih serija za log poruke koje se dobijaju iz različitih izvora podataka, uključujući Elasticsearch, kao i kreiranje dinamičkih izveštaja i grafičkog prikaza željenih rezultata.

3.1 Konfiguracija Logstash pipeline softvera

U prethodnom poglavlju opisan je syslog protokol, pomoću koga se šalju podaci sa udaljene lokacije, tj. RADIUS servera na Logstash pipeline server. Na samom Logstash pipeline serveru takođe je potrebno konfigurisati syslog-ng servis, koji upisuje log poruke u fajlove, koje zatim čita Logstash pipeline softver. Konfiguracioni fajl *syslog-ng.conf* mora imati bar tri osnovna parametra, *source*, *log* i *destination*, prikazana u nastavku:

```
source s_udp { udp(); };
log {
  source(s_udp);
  destination (d_logstash);
};
destination d_logstash {
       file("/opt/logstash/$SOURCEIP/$FACILITY-$YEAR-$MONTH-$DAY"
       owner("logstash") group("logstash") perm(0600)
       create_dirs(yes) dir_perm(0770));
};
```

Uloga Logstash pipeline softvera je da učita, formatira i filtrira log poruke, a primer konfiguracionog fajla je dat u nastavku:

```
input {
    file {
        path => "/opt/logstash/147.91.x.x/*"
        start_position => "beginning"
        sincedb_path => "/dev/null"
    }
}

filter {

    grok {
        patterns_dir => ["./patterns"]
        match => { "message" => "%{TIMESTAMP_ISO8601:time} %{SYSLOGHOST:
            syslog_hostname} %{DATA:syslog_program}(?:\[%{POSINT:syslog_pid}\])?: %{
            ACCESS:access}: IdP=%{IDP:IdP} MAC=%{MAC:MAC} AP=%{AP:AP} RP=%{RP:RP}"}

    }

        translate {
        source => "AP"
        target => "[APalias]"
        dictionary_path => "/usr/share/logstash/eduroam_lookup.json"
        fallback => "Unknown"
        override => true
      }
if [APalias] == "Unknown" {
        mutate {
        rename => {"[APalias]" => "[APnew][AP_name]"}
        add_field => {
             "[APalias][Grad]" => "Unknown"
             "[APalias][Lokacija]" => "Unknown"
             "[APalias][Latitude]" => "Unknown"
             "[APalias][Longitude]" => "Unknown"
             }
        }
    }

       mutate {
       remove_field => [ "@version", "syslog_program", "log", "@timestamp", "
           syslog_pid", "event", "host" ]
       }

}
output {

    elasticsearch {
         ssl => true
         ssl_certificate_verification => true
         cacert => "/etc/elasticsearch/certs/http_ca.crt"
         hosts => "https://147.91.x.x:9200"
         index => "monitoring"
         user => "elastic"
         password => "xxx"
    }
```

```
    stdout { codec => rubydebug }
}
```

Logstash pipeline softver čita log poruke koje syslog zapisuje u fajlove na serveru, za šta je zaslužan *input* segment, na početku konfiguracionog fajla. U okviru *filter* segmenta, log poruka se formatira na osnovu polja koja Logstash pipeline softver prepoznaje kao obrasce, a koja su definisana u *patterns-dir* parametru, a zatim mapirana u *match* parametru. *Patterns* fajl je dat u nastavku:

```
ACCESS .*
IDP .*
MAC .*
AP .*
RP .*
Longitude .*
Lokacija .*
AP_name .*
Latitude .*
Grad .*
```

Na osnovu podataka koji su poslati Logstash pipeline serveru od strane RADIUS servera ne mogu se dobiti svi željeni podaci o uspešnim i neuspešnim autentifikacijama. Zato je potrebno uvesti dodatne podatke kroz *lookup* fajl, koji se zatim povezuju sa podatkom o AP MAC adresi u *translate* segmentu. Ukoliko se taj podatak ne nalazi u fajlu, parametrima loga se dodaju “Unknown” vrednosti. Deo *lookup* fajla koji AMRES koristi dat je u Tabeli 2.

Tabela 2: Prikaz dela eduroam lookup fajla koji se koristi za formatiranje log poruke u Logstash pipeline softveru.

Lokacija	Grad	APmac	APname	Latitude	Longitude
ETF	Beograd	00-3a-7d-xx-xx-xx:eduroam	cisco2702-amres-bg.etf1	44.80556	20.47623
ETF	Beograd	00-3a-7d-xx-xx-xx:eduroam	cisco2702-amres-bg.etf10	44.80556	20.47623

Na osnovu uvedenih dodatnih podataka kreiran je sadržajniji log zapis i obogaćena je mogućnost pretrage i analize log poruke, a pridodat je grafički prikaz željenih izveštaja. U *output* sekciji pored konfiguracije destinacije na koju Logstash pipeline prosleđuje formatirane i filtrirane logove, najvažnija opcija je specificiranje indeksa za obrađene log poruke koji se šalju Elasticsearch softveru. Primer novokreirane log poruke prikazan je u nastavku:

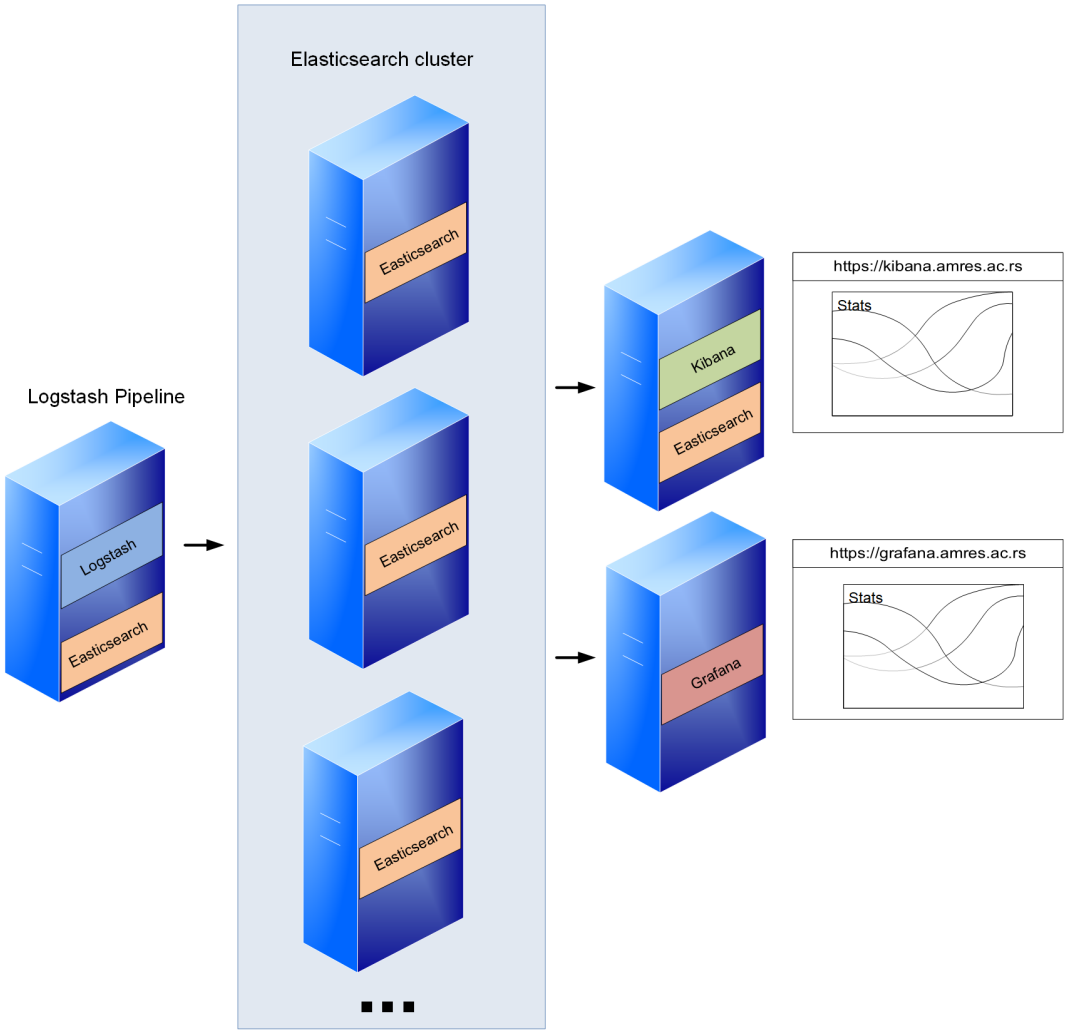
```
{
             "time" => "2022-06-01T15:30:01+02:00",
               "AP" => "00-3a-7d-xx-xx-xx:eduroam",
               "RP" => "1amres.ac.rs",
   "syslog_hostname" => "147.91.x.x",
              "MAC" => "b2-f8-f8-xx-xx-xx",
          "message" => "2022-06-01T15:30:01+02:00 147.91.x.x radiusd[15246]: Access-
              Accept: IdP=edu.arh.bg.ac.rs MAC=b2-f8-f8-xx-xx-xx AP=00-3a-7d-xx-xx-
              xx:eduroam RP=1amres.ac.rs",
           "access" => "Access-Accept",
          "APalias" => {
       "Lokacija" => "Elektrotehnicki fakultet Univerziteta u Beogradu",
```

```
        "Latitude" => "44.805563",
           "Grad" => "Beograd",
       "Longitude" => "20.47623",
         "AP_name" => "cisco2702-amres-bg.etf30"
   },
              "IdP" => "edu.arh.bg.ac.rs"
}
```

3.2 Konfiguracija Elasticsearch softvera

Filtrirane i formatirane log poruke se prosleđuju Elasticsearch softveru. Elasticsearch softver skladišti podatke pri čemu je najoptimalnije rešenje konfigurisati klaster koji se sastoji od jednog master noda i više običnih nodova, nad kojima se vrše upiti od strane Kibana komponente softvera, a koji omogućuje veću pouzdanost i skalabilnost celog sistema.

Slika topologije za prikupljanje i skladištenje logova, uključujući Elasticsearch klaster, prikazana je na Slici 2.



Slika 2: Postupak prikupljanja i skladištenja log poruka AMRES servisa.

Sve informacije o konfiguraciji klastera dostupne su u izlazu sledece komande koju omogućuje Elastic-

search API:

```
# curl --cacert /etc/elasticsearch/certs/http_ca.crt -u elastic https://147.91.x.x
   :9200/_cat/nodes?v
Enter host password for user 'elastic':
ip  heap.percent ram.percent cpu load_1m load_5m load_15m node.role master name
147.91.x.x        77         97  4    0.54   0.40    0.28 cdfhilmrstw -   node-3
147.91.x.x        50         97  21   0.96   0.75    0.45 cdfhilmrstw -   node-4
147.91.x.x        55         98  1    0.07   0.10    0.07 -         -     node-2
147.91.x.x        66         96  3    0.01   0.06    0.05 cdfhilmrstw *   node-1
```

U izlazu ove komande se može uočiti da je node-1 master nod, a njegova funkcionalnost se može promeniti. Funkcionalnost noda zavisi od uloge koju vrši u klasteru. Da bi Logstash upešno prosleđivao logove i upisivao u bazu, u okviru Elasticsearch softvera definisan je index na master nodu, što se postiže sledećom komandom:

```
# curl -X PUT --cacert /etc/elasticsearch/certs/http_ca.crt -u elastic https
   ://147.91.x.x:9200/monitoring?pretty
Enter host password for user 'elastic':
{
  "acknowledged" : true,
  "shards_acknowledged" : true,
  "index" : "monitoring"
}
```

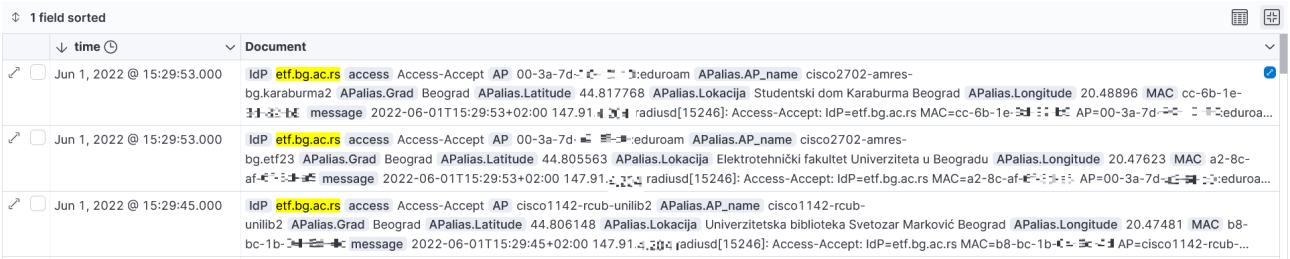
Nakon uspešne konfiguracije, korišćenjem Elasticsearch API komande mogu se pretražiti prikupljeni logovi, a u nastavku je dat primer strukture jednog takvog loga u JSON formatu, na osnovu upita i pretrage po domenu Davaoca Identiteta, tj. domena institucije:

```
# curl -X GET --cacert /etc/elasticsearch/certs/http_ca.crt -u elastic https
   ://147.91.x.x:9200/monitoring/_search?pretty -H 'Content-Type: application/json'
    -d'
> {
>   "query": {
>     "match": {
>       "IdP":"etf.bg.ac.rs"
>     }
>   }
> }
> '
Enter host password for user 'elastic':
{
  "took" : 23,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 319,
      "relation" : "eq"
    },
```

```
"max_score" : 2.3934784,
"hits" : [
  {

    "_index" : "monitoring",
    "_id" : "TTWV2YIBCUCBlsdkFJDV",
    "_score" : 2.3934784,
    "_source" : {
      "access" : "Access-Accept",
      "RP" : "1amres.ac.rs",
      "AP" : "00-3a-7d-x-x-x:eduroam",
      "IdP" : "etf.bg.ac.rs",
      "syslog_hostname" : "147.91.x.x",
      "time" : "2022-06-01T15:14:24+02:00",
      "APalias" : {
        "Longitude" : "20.461087",
        "Grad" : "Beograd",
        "AP_name" : "cisco2702-amres-bg.med22",
        "Latitude" : "44.797416",
        "Lokacija" : "Medicinski fakultet Univerziteta u Beogradu"
      },
      "message" : "2022-06-01T15:14:24+02:00 147.91.x.x radiusd[15246]: Access-
         Accept: IdP=etf.bg.ac.rs MAC=98-0d-51-x-x-x AP=00-3a-7d-x-x-x:eduroam RP
         =1amres.ac.rs",
      "MAC" : "98-0d-51-x-x-x"
    }
  },
```


Za razliku od Elasticsearch softvera koji prikazuje podatke u JSON formatu, Kibana omogućuje grafički prikaz log poruka i njihovu dalju obradu u smislu kreiranja statistika i vizualizaciju podataka. Primer log poruke koju prikazuje Kibana dat je na Slici 3.



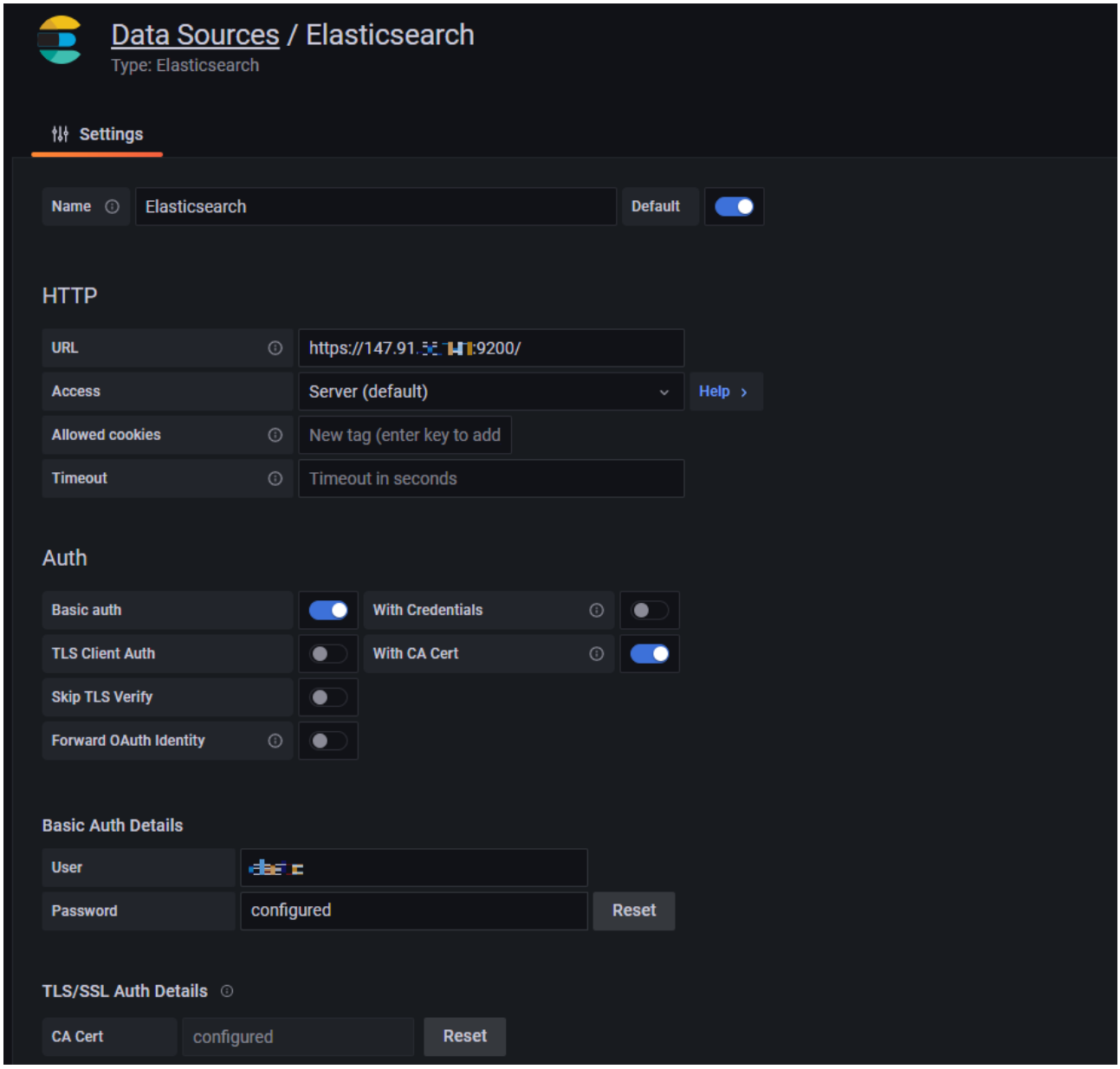
Slika 3: Primer formatirane log poruke koju prikazuje Kibana.

Sa slike se mogu videti uspešne autentifikacije AMRES krajnjih korisnika koji imaju otvoren digitalni identitet kod matične institucije koja je u ovom slučaju Elektrotehnički fakultet, a prijavili su se na eduroam servis sa tri različite lokacije:

- Studentski dom Karaburma Beograd,
- Univerzitetska Biblioteka Svetozar Marković Beograd,
- Elektrotehnički fakultet Univerziteta u Beogradu.

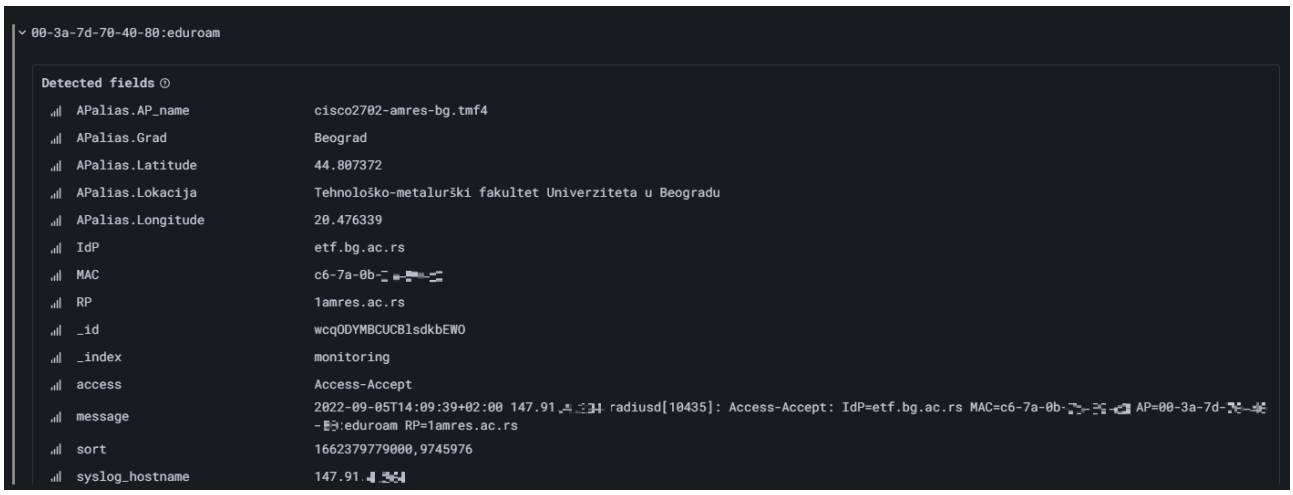
3.3 Konfiguracija Grafana softvera

Elasticsearch softver pruža mogućnost pristupa podacima koje skladišti u JSON formatu, koristeći Elasticsearch API. Dodatno, veliki broj aplikacija sada obuhvata i dodatke za integraciju sa Elasticsearch izvorom podataka. U ovu grupu se ubraja i Grafana softver, koji predstavlja veoma moćan alat za analizu i grafički prikaz podataka. Podešavanje izvora log poruka koje Grafana čita i koristi je veoma jednostavno i prikazano je na Slici 4.



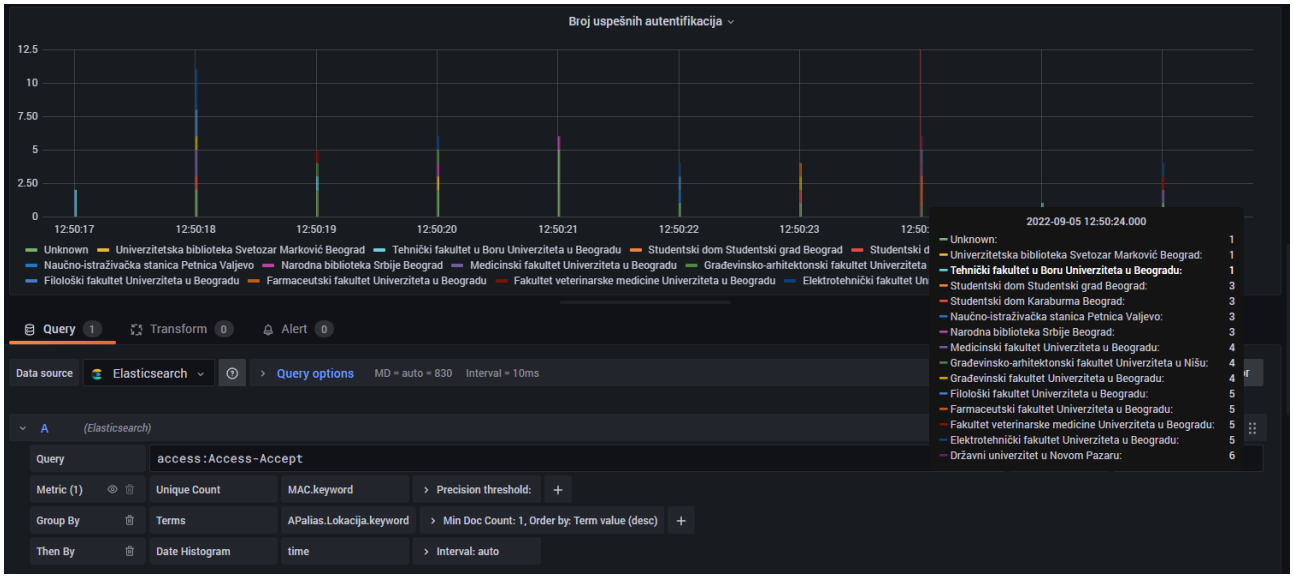
Slika 4: Konfiguracija Elasticsearch izvora podataka u okviru Grafana softvera.

Da bi Grafana softver mogao da učita log poruke sa udaljenog servera, potrebno je podesiti adresu Elasticsearch softvera i autentifikacione parametre, pošto je Elasticsearch zaštićen sertifikatom i za pristup podacima je neophodna autentifikacija i CA sertifikat. Nakon uspešne autentifikacije, log poruke su dostupne za prikaz i dalje korišćenje u okviru upita za pretragu, filtriranje, transformacije, itd. Na Slici 5 dat je prikaz logova u Grafana softveru.



Slika 5: Primer log poruka koju prikazuje Grafana softver.

Slika 6 ilustruje samo jedan od mnogobrojnih upita koji se mogu upotrebiti za grafički prikaz statistika dobijenih na osnovu prikupljenih podataka.



Slika 6: Primer Grafana upita kojim se vizualizuju statistike korišćenja eduroam servisa

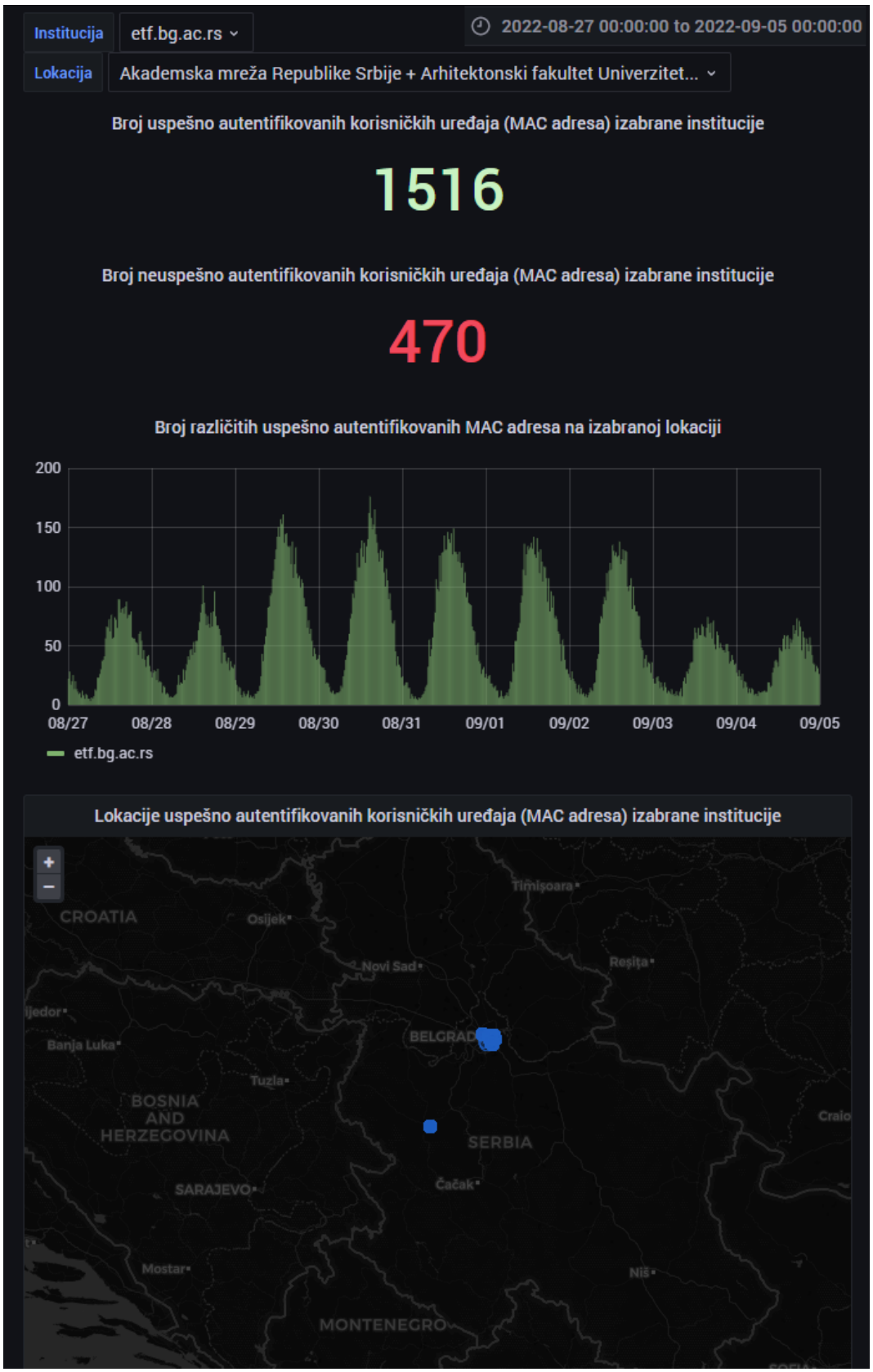
Pretraga u okviru Grafana softvera omogućava detaljnu analizu log poruka i olakšava praćenje performansi i korišćenja servisa. Svaki realizovan upit može se sačuvati kao panel, za kasnije korišćenje. Sačuvani paneli se zatim mogu spojiti u *Dashboard*. U okviru Grafana softvera *dashboard* predstavlja zajednički prikaz kreiranih izveštaja, koji mogu biti u različitim formatima.

AMRES prati i izdvaja veliki broj podataka iz log poruka i pravi statistike o različitim aspektima korišćenja eduroam servisa. AMRES prati veliki broj parametara bitnih za eduroam servis, koji se mogu podeliti u pet grupa:

- Svi korisnici,
- AMRES korisnici,

- Korišćenje po instituciji,
- Korišćenje po lokaciji,
- Strani korisnici.

Za ove grupe informacija od značaja kreiran je Dashboard, čiji je primer prikazan na Slici 7.



Slika 7: Primer grafičkog prikaza podataka dobijenih primenom različitih upita u okviru Grafana softvera.

4 Zaključak

Elastic Stack softver pruža velike mogućnosti za prikupljanje log poruka i na taj način efikasno i kvalitetno prati i analizira rad i korišćenje servisa u mreži. Softver koji je razmatran je više nego dovoljan alat koji administratorima omogućava da na brz i efikasan način prikupljaju i pretražuju logove iz različitih izvora, vrše monitoring servisa i prate ponašanje korisnika. Implementirani sistem predstavlja sveobuhvatno i skalabilno okruženje, u smislu količine i obima log poruka koje je potrebno skladištiti i obraditi. Takođe, pruža veliku pouzdanost u radu i mogućnost gubitaka podataka je svedena na minimum. Iako je uloga Grafana softvera u ovom radu vizualizacija i analiza logova, on se primarno koristi i kao alat za monitoring rada servisa i prikaz i analizu različitih metrika.

Literatura

[1] Murugiah Souppaya and Karen Scarfone. Nist special publication 800-92, Guide to computer security log management, 09 2006.

[2] Elastic stack. https://www.elastic.co/. Accessed: 2022-09-01.

[3] Grafana. https://grafana.com/. Accessed: 2022-09-01.

[4] syslog-ng website. https://www.syslog-ng.com/. Accessed: 2022-09-01.

[5] Splunk log management. https://archive.geant.org/projects/gn3/geant/services/cbp/Documents/cbp-48_splunk_log_management_amres.pdf. Accessed: 2016-03.

[6] freeradius website. https://freeradius.org/. Accessed: 2022-09-01.

[7] RFC2865. https://www.rfc-editor.org/rfc/rfc2865. Accessed: 2022-09-01.

[8] Elasticsearch as a NoSQL database. https://www.elastic.co/blog/found-elasticsearch-as-nosql. Accessed: 2022-09-01.

[9] Elasticsearch RESTful API. https://www.redhat.com/en/topics/api/what-is-a-rest-api. Accessed: 2022-09-01.

[10] JSON. https://www.json.org/json-en.html. Accessed: 2022-09-01.