Log Management and Visualization of AMRES Statistics using Open-source Tools

AMRES

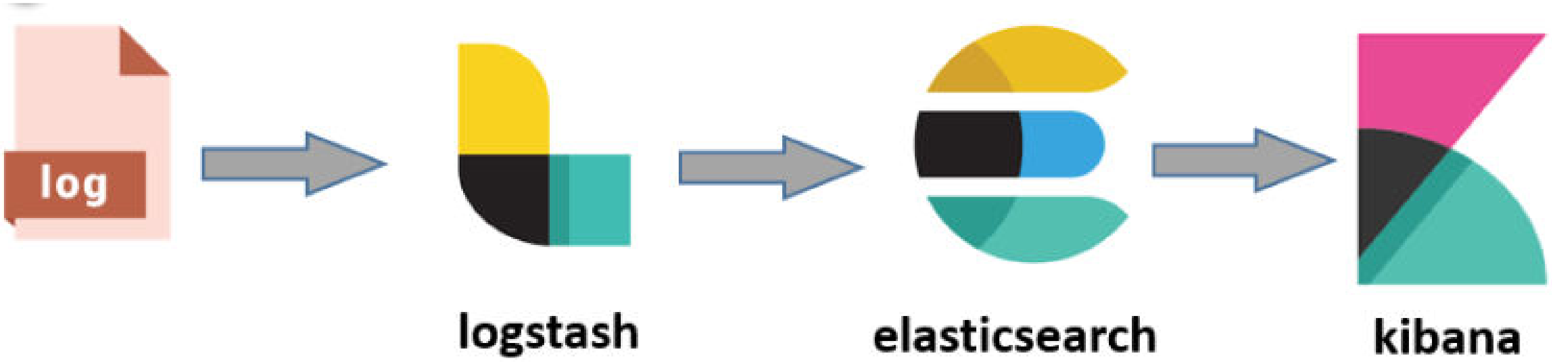
Serbian Academic Network

Andrijana Todosijević, Katarina Simonović, Anđela Arsović

PSSOH Conference October 15, 2022

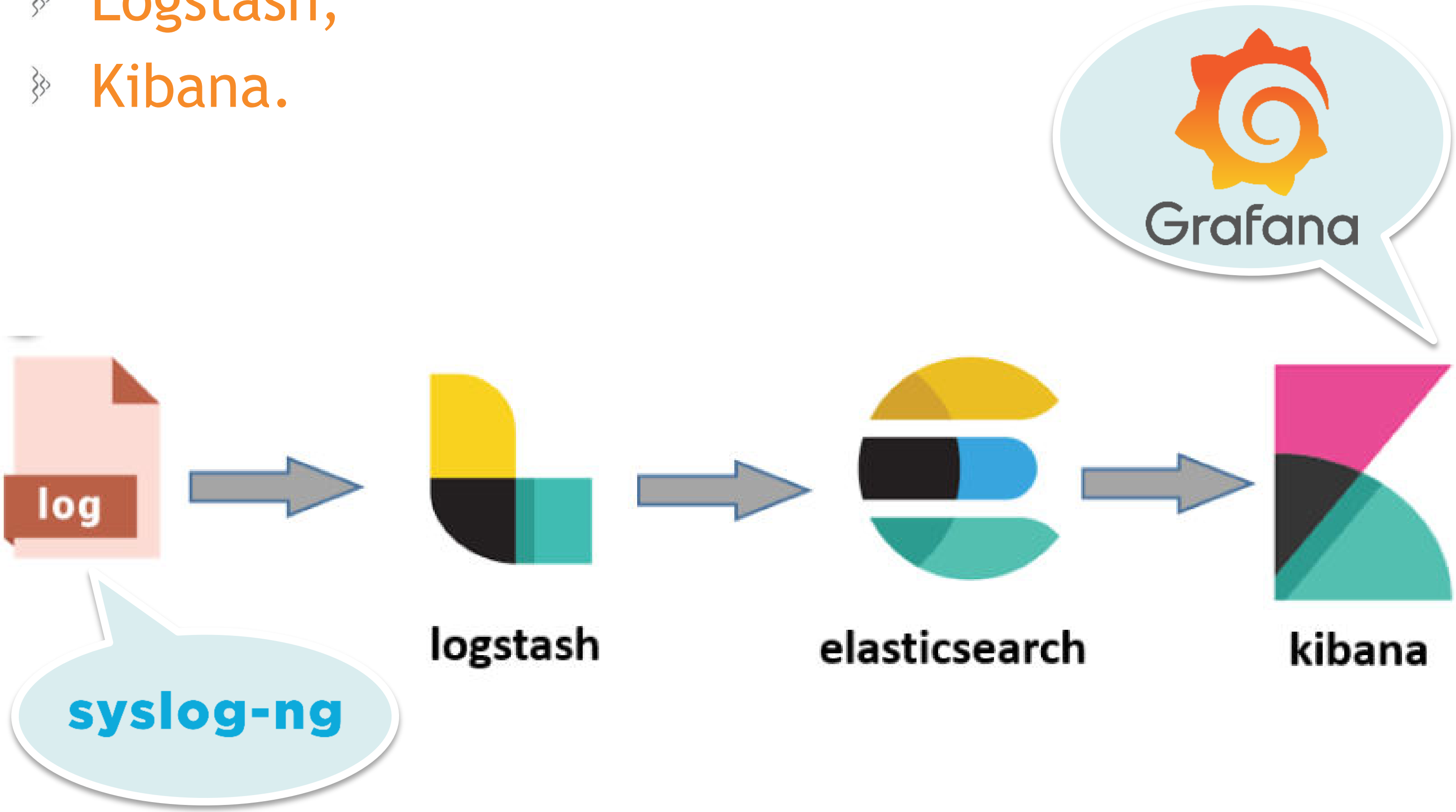
Elastic Stack software

- Beats,
- Elasticsearch,
- Logstash,
- Kibana.

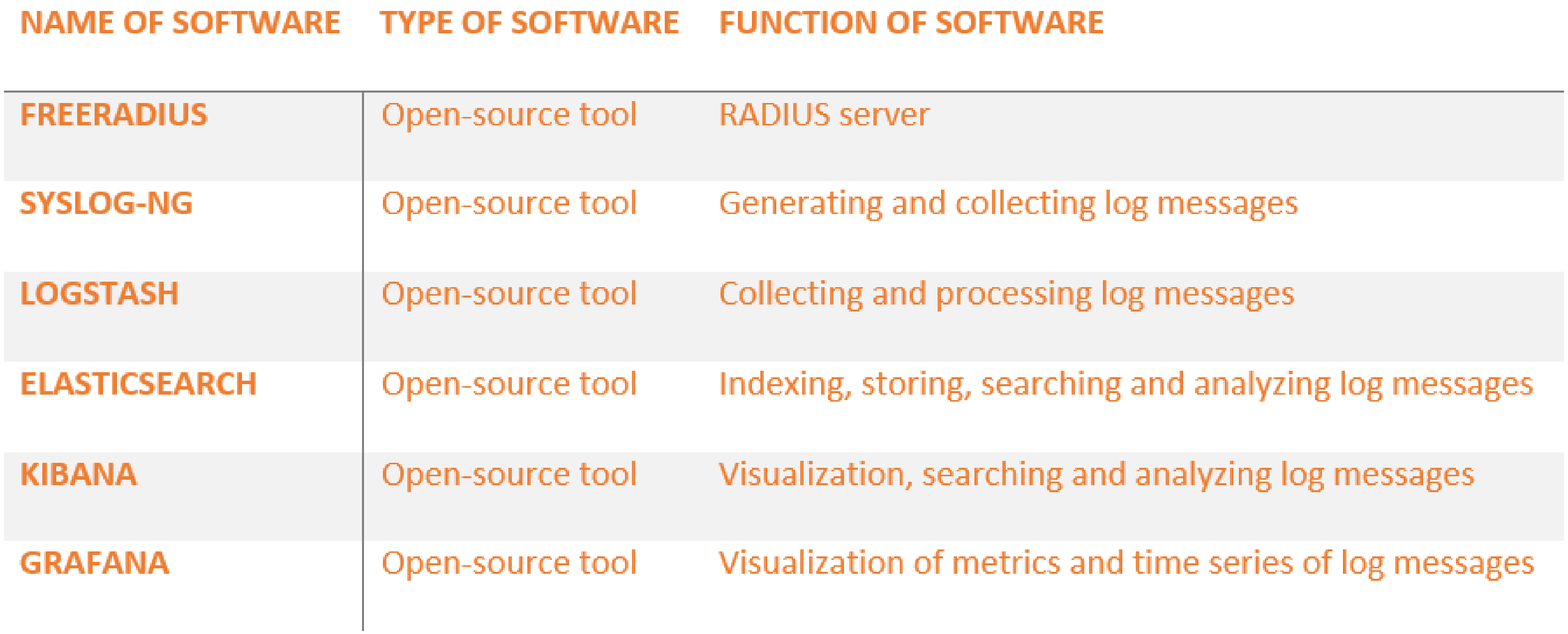


Elastic Stack software

- Beats,
- Elasticsearch,
- Logstash,
- Kibana.

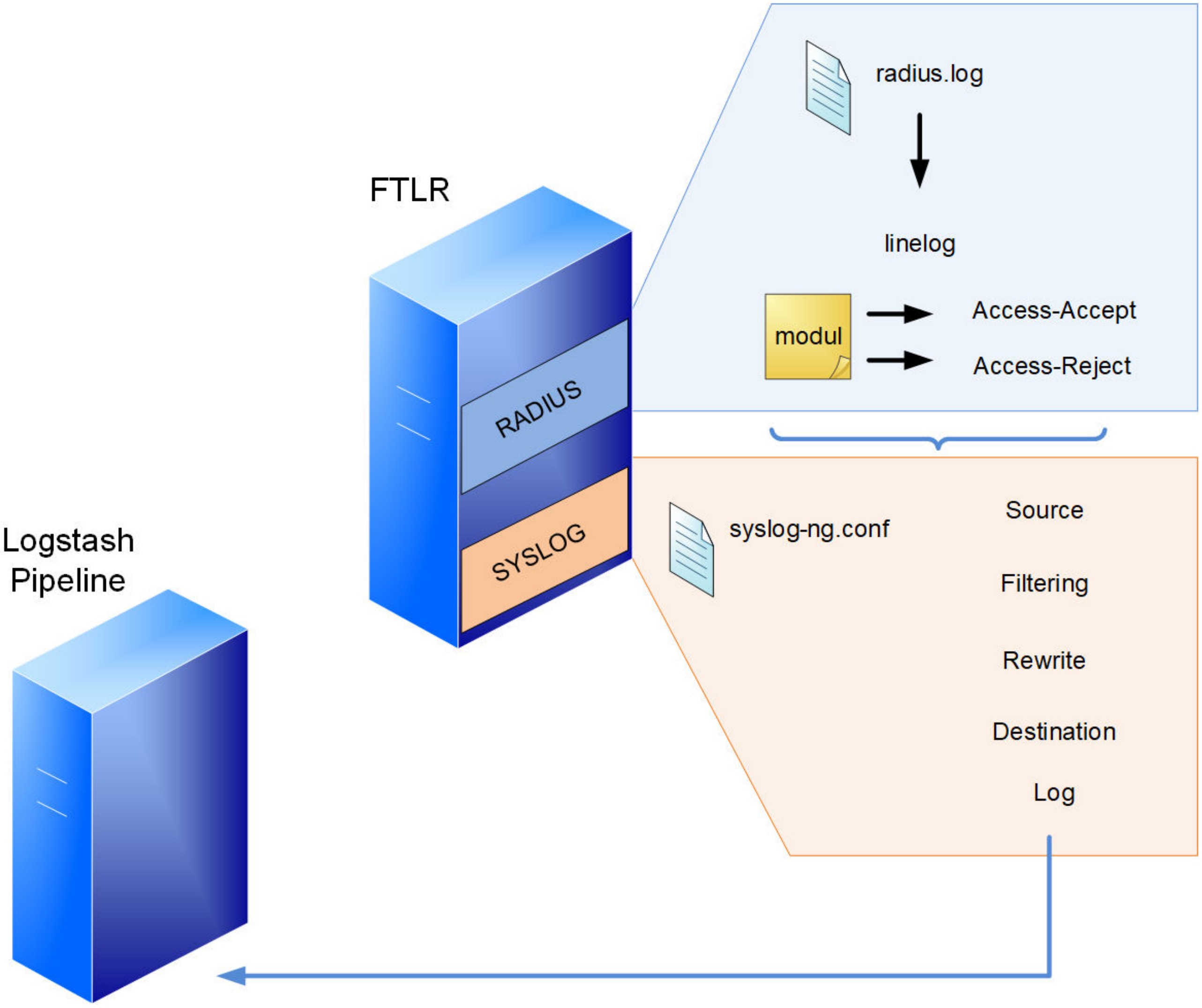


Tools used in the log management process

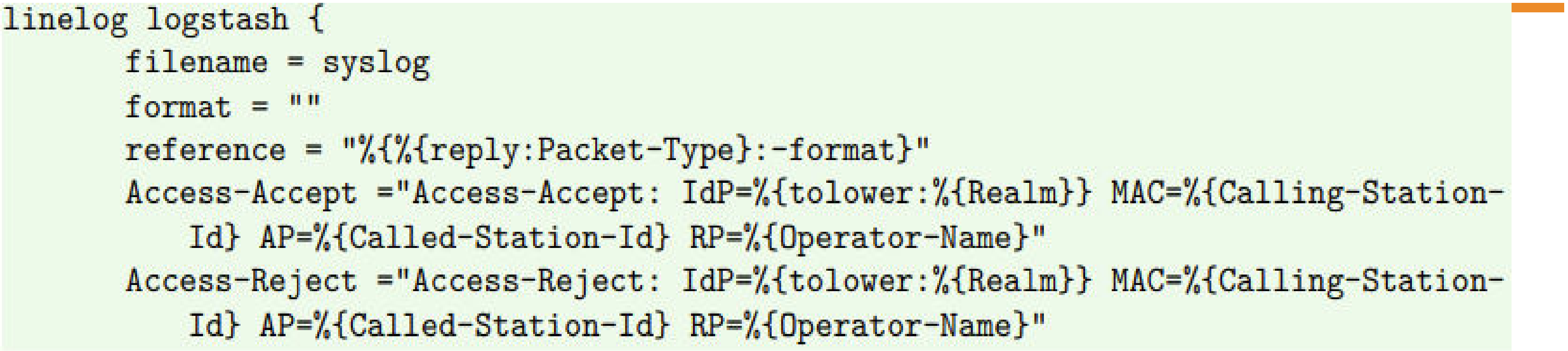


NAME OF SOFTWARE	TYPE OF SOFTWARE	FUNCTION OF SOFTWARE
FREERADIUS	Open-source tool	RADIUS server
SYSLOG-NG	Open-source tool	Generating and collecting log messages
LOGSTASH	Open-source tool	Collecting and processing log messages
ELASTICSEARCH	Open-source tool	Indexing, storing, searching and analyzing log messages
KIBANA	Open-source tool	Visualization, searching and analyzing log messages
GRAFANA	Open-source tool	Visualization of metrics and time series of log messages

Procedure of log messages generating and collecting for the eduroam scenario



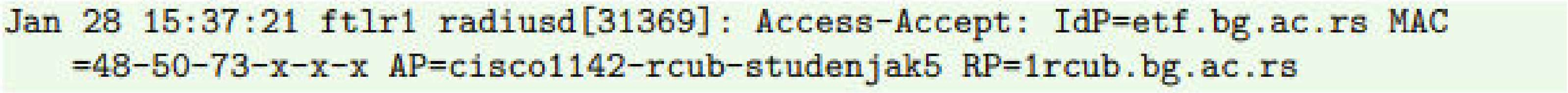
An example of configuration of the linelog module



```
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}"
```

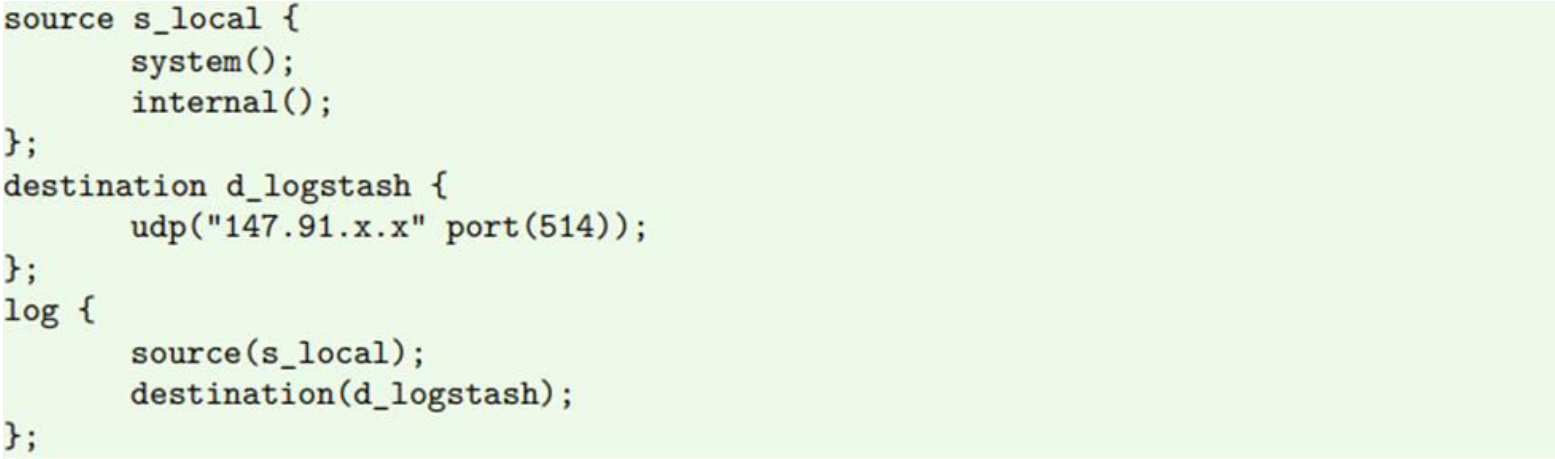
- Access-Accept/Access-Reject – authentication result;
- IdP – domain of the institution;
- MAC – MAC address of the user device;
- AP – string based on which the location of AP is determined;
- RP – RADIUS attribute Operator-Name

After the log message undergoes the procedure of generation and processing, its final format is:



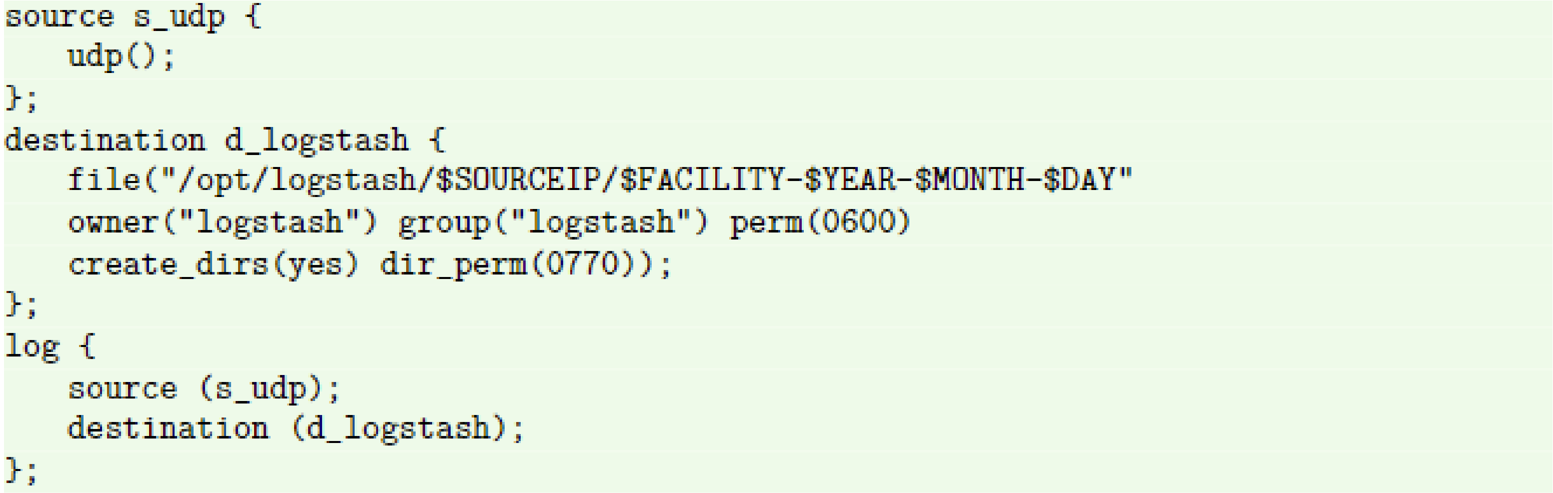
```
Jan 28 15:37:21 ftlr1 radiusd[31369]: Access-Accept: IdP=etf.bg.ac.rs MAC
   =48-50-73-x-x-x AP=cisco1142-rcub-studenjak5 RP=1rcub.bg.ac.rs
```

Configuration of syslog-ng on RADIUS server



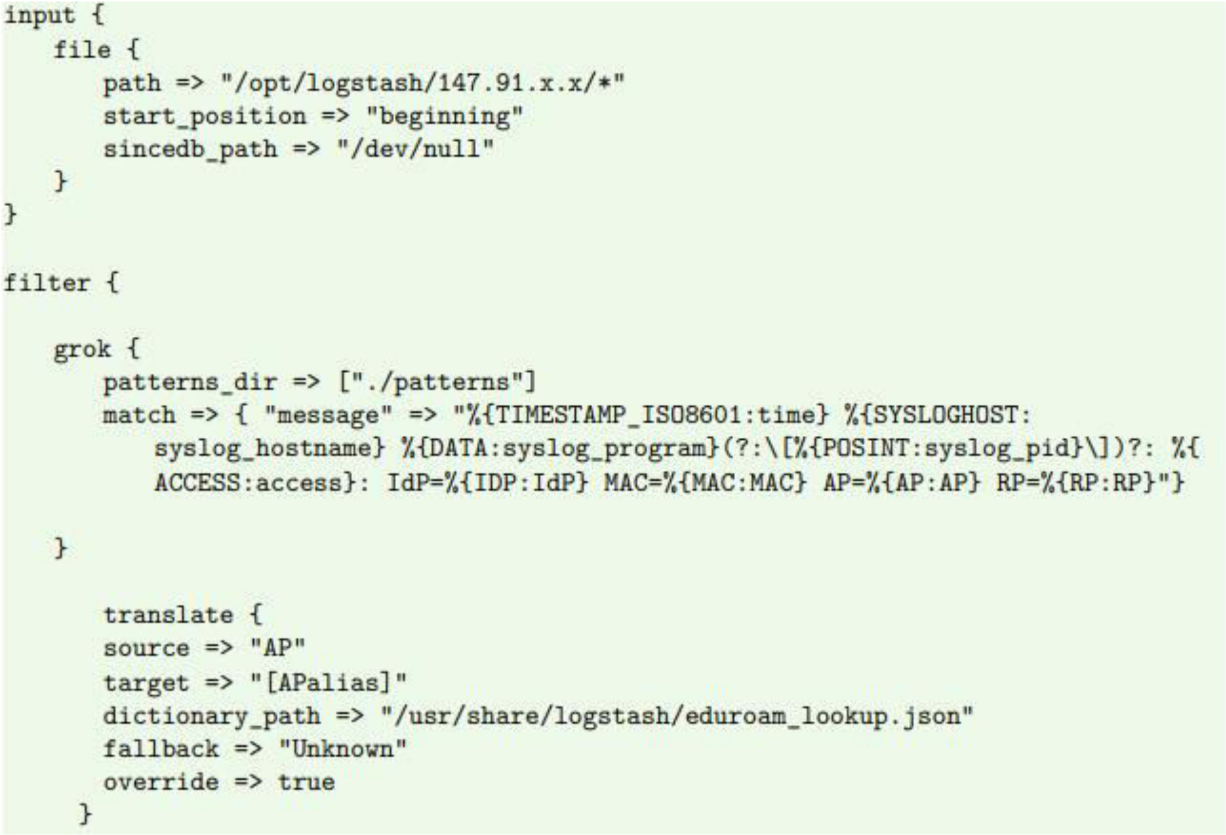
```
source s_local {
        system();
        internal();
};
destination d_logstash {
        udp("147.91.x.x" port(514));
};
log {
        source(s_local);
        destination(d_logstash);
};
```

Configuration of syslog-ng on Logstash server



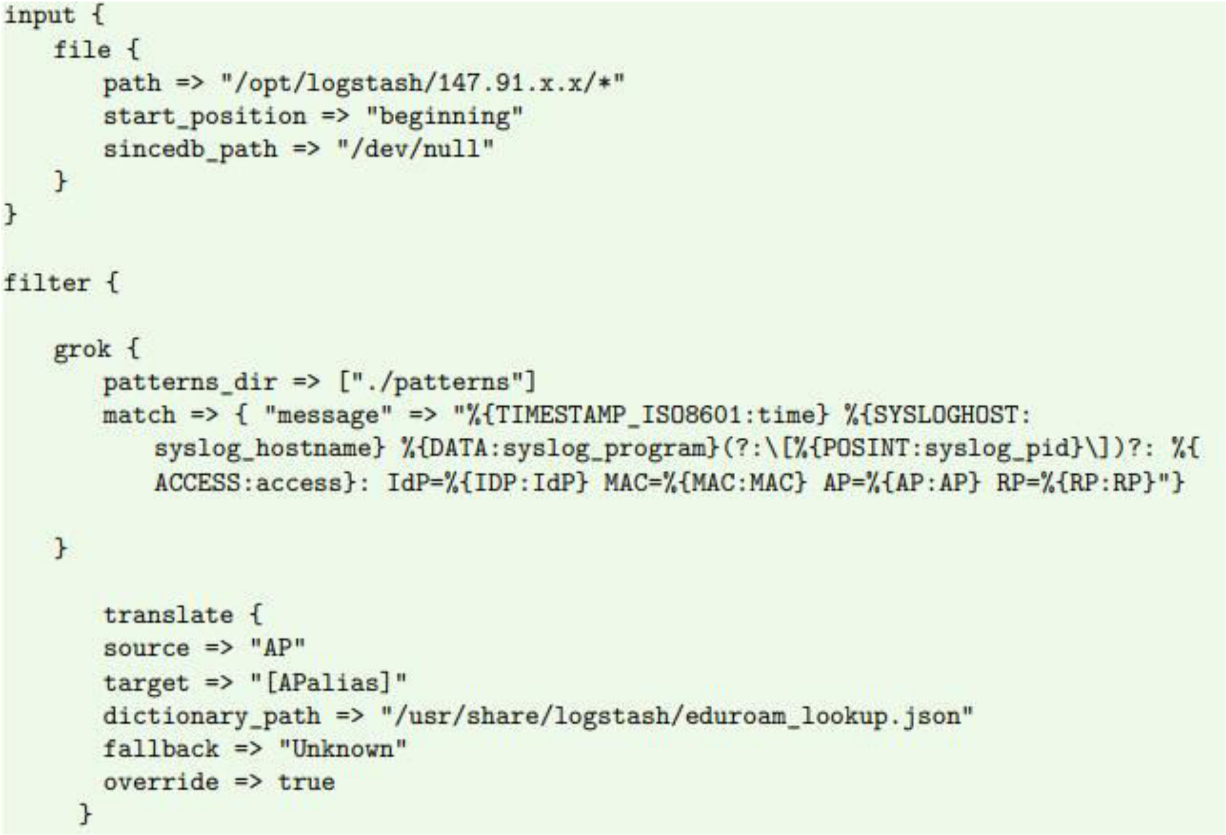
```
source s_udp {
   udp();
};
destination d_logstash {
   file("/opt/logstash/$SOURCEIP/$FACILITY-$YEAR-$MONTH-$DAY"
   owner("logstash") group("logstash") perm(0600)
   create_dirs(yes) dir_perm(0770));
};
log {
   source (s_udp);
   destination (d_logstash);
};
```

Logstash (1/2)



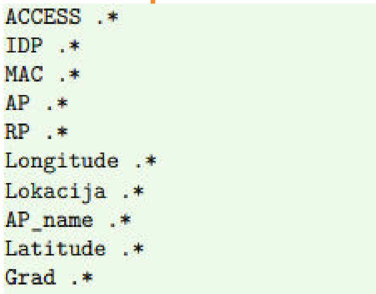
```
input {
    file {
        path => "/opt/logstash/147.91.x.x/*"
        start_position => "beginning"
        sincedb_path => "/dev/null"
    }
}

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
     }
```

Logstash (1/2)



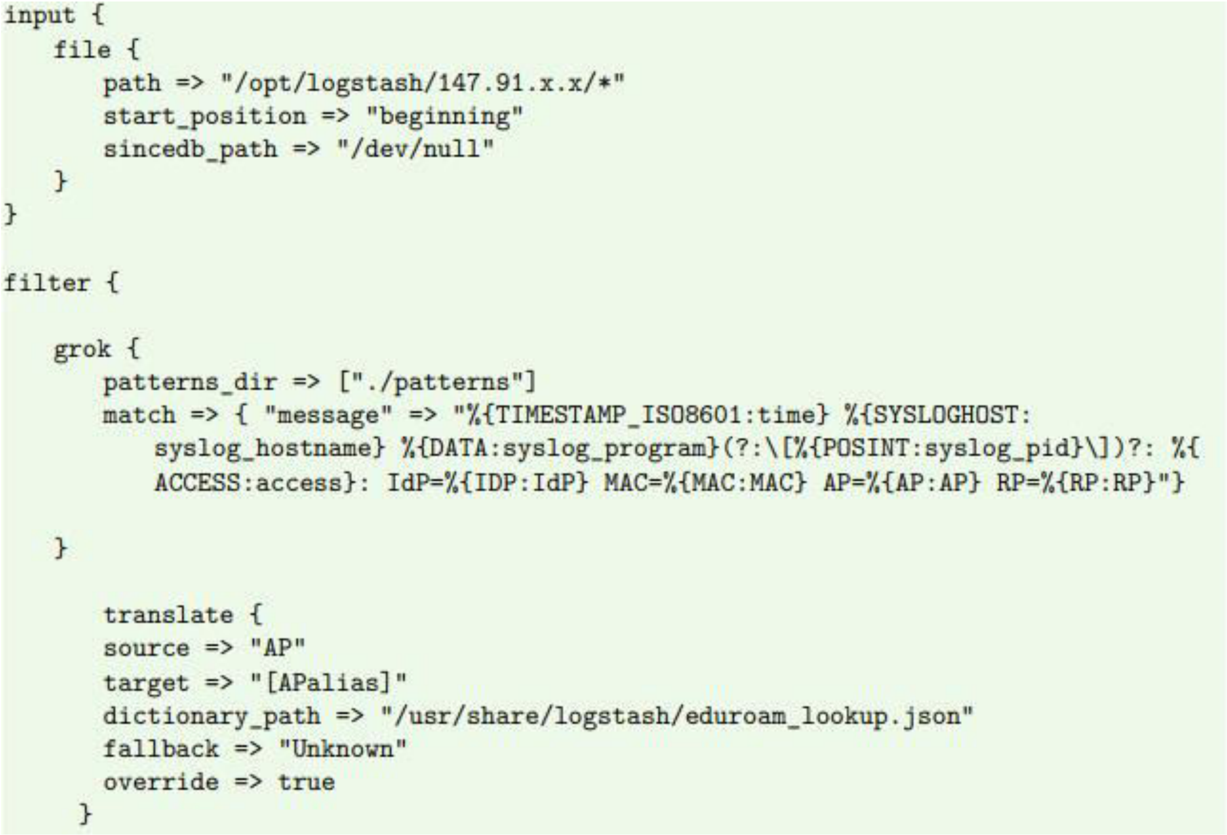
```
input {
    file {
        path => "/opt/logstash/147.91.x.x/*"
        start_position => "beginning"
        sincedb_path => "/dev/null"
    }
}

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
      }
```

Custom pattern file



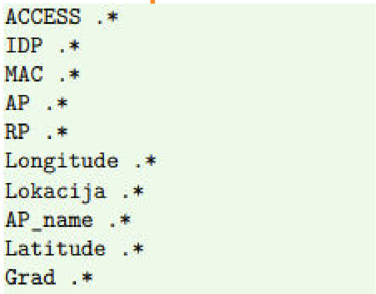
```
ACCESS .*
IDP .*
MAC .*
AP .*
RP .*
Longitude .*
Lokacija .*
AP_name .*
Latitude .*
Grad .*
```

Logstash (1/2)



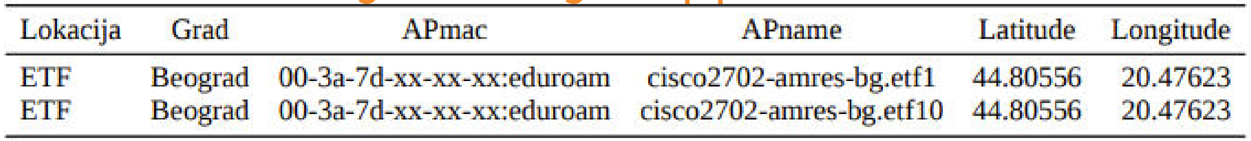
```
input {
    file {
        path => "/opt/logstash/147.91.x.x/*"
        start_position => "beginning"
        sincedb_path => "/dev/null"
    }
}

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
      }
```

Custom pattern file



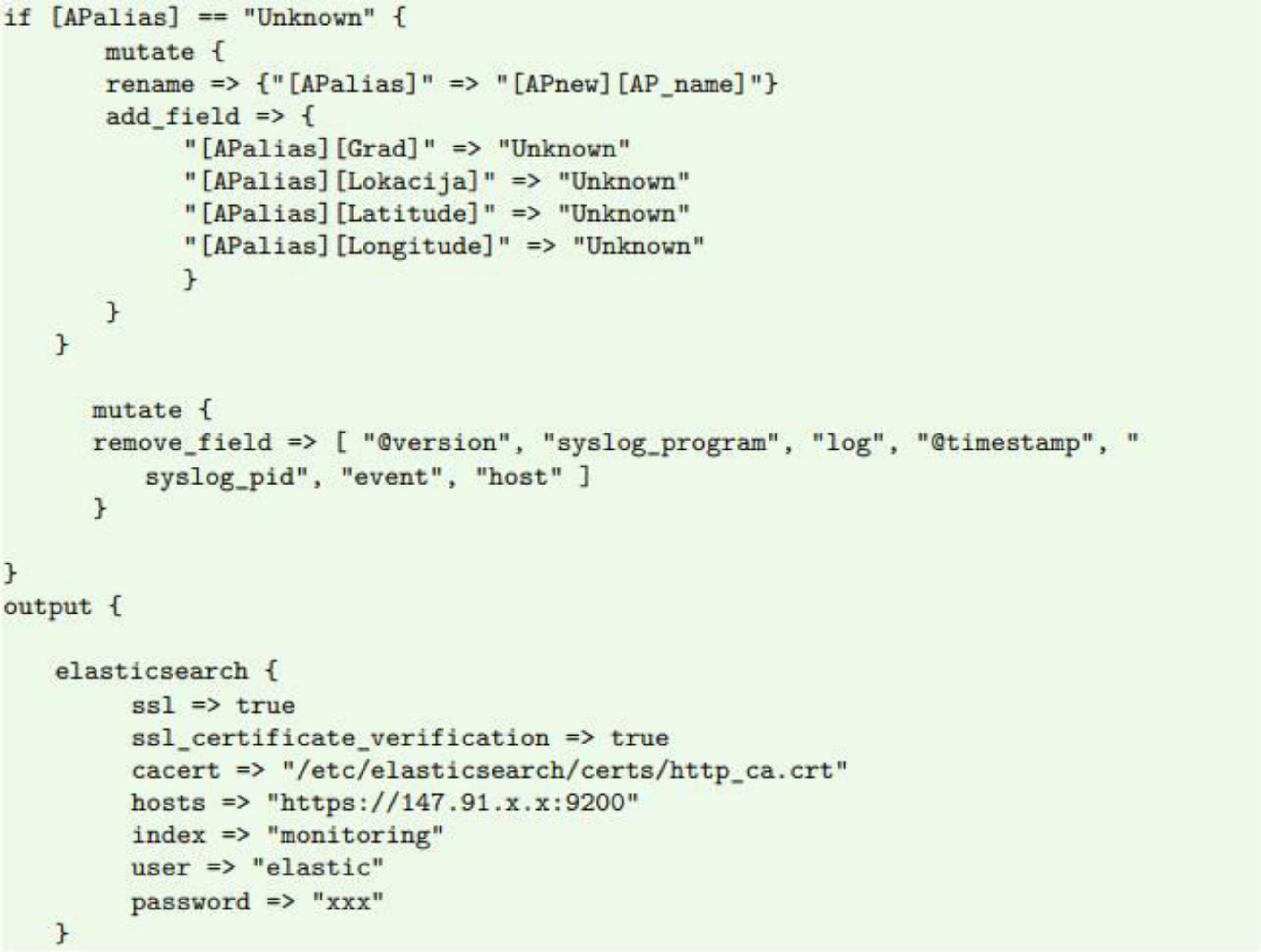
```
ACCESS .*
IDP .*
MAC .*
AP .*
RP .*
Longitude .*
Lokacija .*
AP_name .*
Latitude .*
Grad .*
```

Showing part of the eduroam lookup file used to format the log message in the Logstash pipeline software



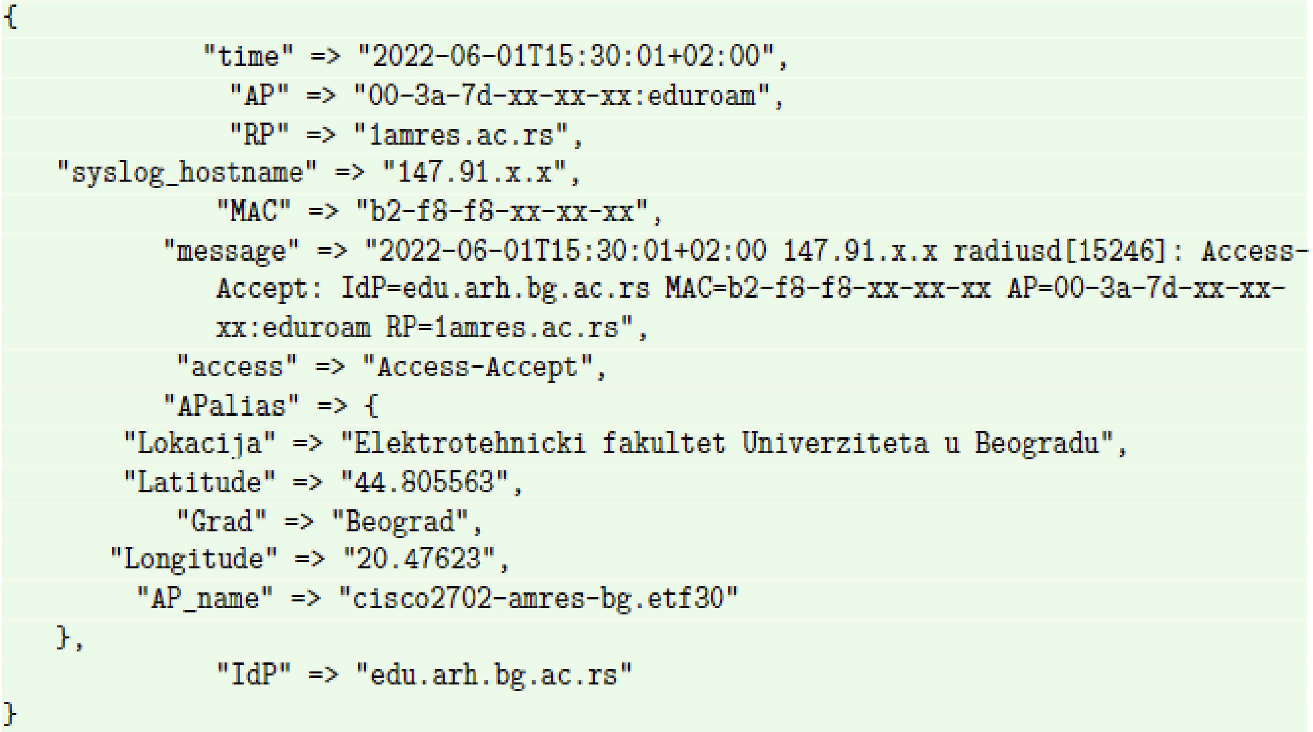
Lokacija	Grad	APmac	APname	Latitude	Longitude
ETF	Beograd	00-3a-7d-xx-xx-xx:eduroam	cisco2702-amres-bg.etf1	44.80556	20.47623
ETF	Beograd	00-3a-7d-xx-xx-xx:eduroam	cisco2702-amres-bg.etf10	44.80556	20.47623

Logstash (2/2)



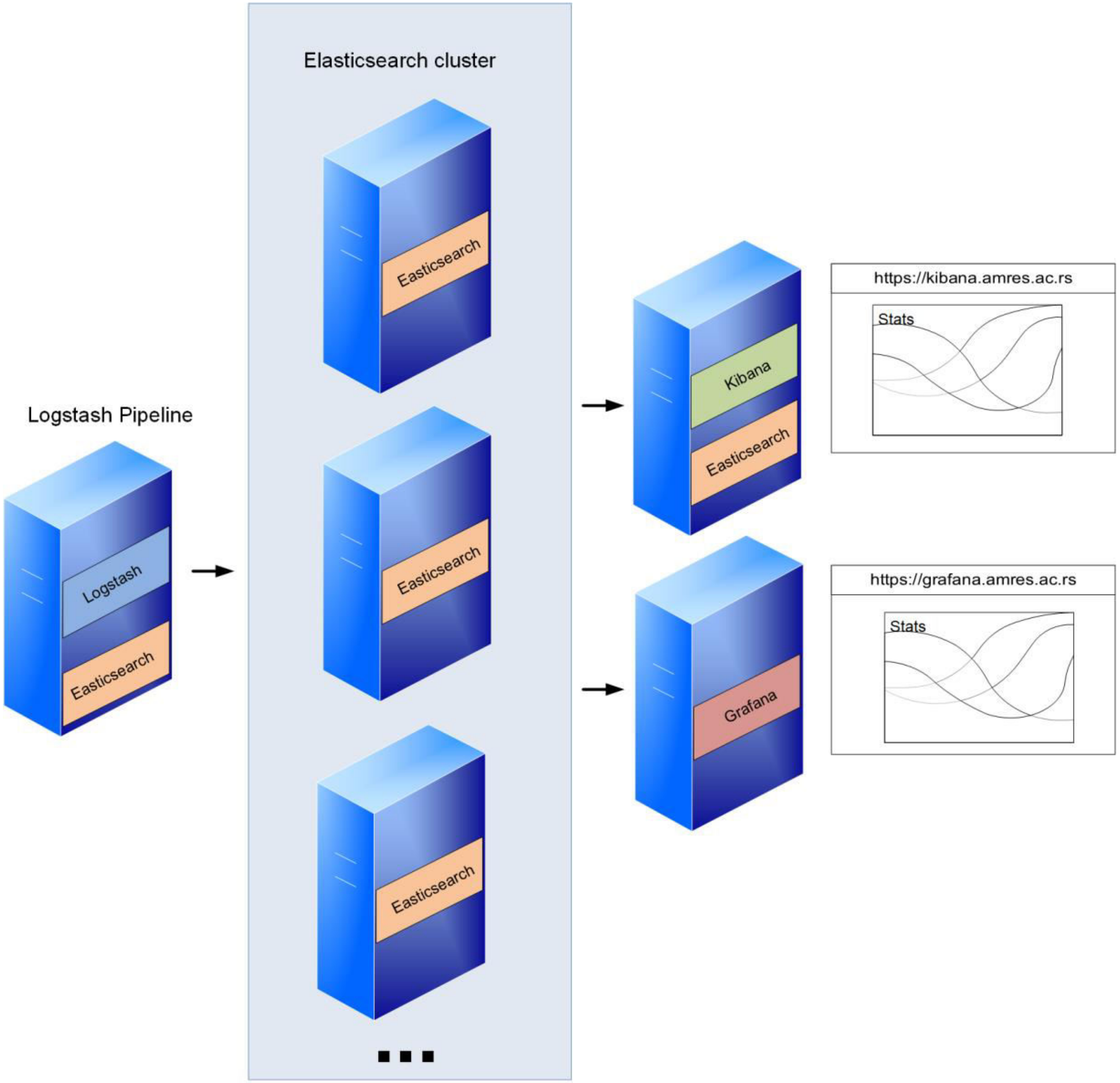
```
if [APalias] == "Unknown" {
       mutate {
       rename => {"[APalias]" => "[APnew][AP_name]"}
       add_field => {
            "[APalias][Grad]" => "Unknown"
            "[APalias][Lokacija]" => "Unknown"
            "[APalias][Latitude]" => "Unknown"
            "[APalias][Longitude]" => "Unknown"
            }
       }
    }

      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"
    }
```

Logstash pipeline output



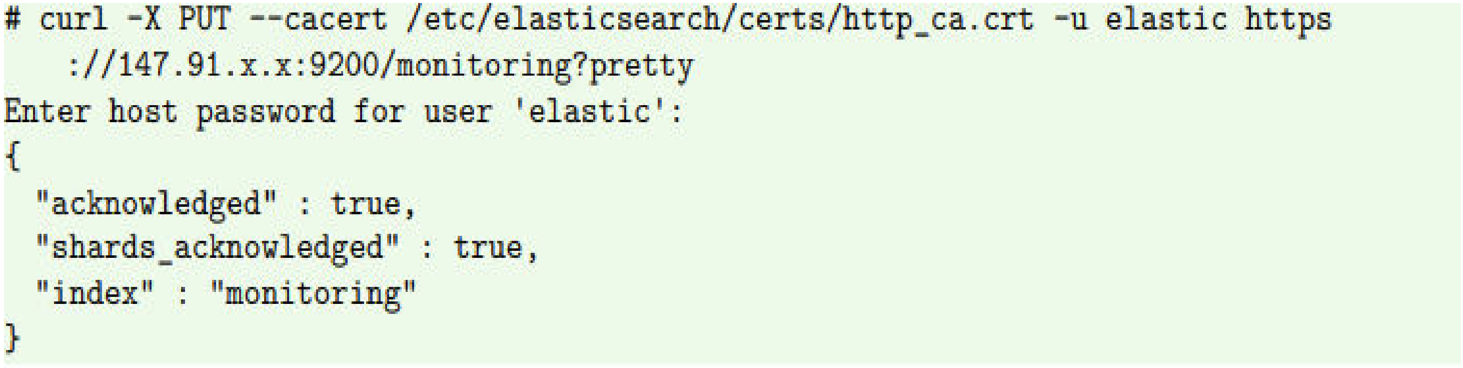
```
{
              "time" => "2022-06-01T15:30:01+02:00",
                "AP" => "00-3a-7d-xx-xx-xx:eduroam",
                "RP" => "1amres.ac.rs",
   "syslog_hostname" => "147.91.x.x",
               "MAC" => "b2-f8-f8-xx-xx-xx",
           "message" => "2022-06-01T15:30:01+02:00 147.91.x.x radiusd[15246]: 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"
}
```

Procedure for collecting and storing log messages of the AMRES service



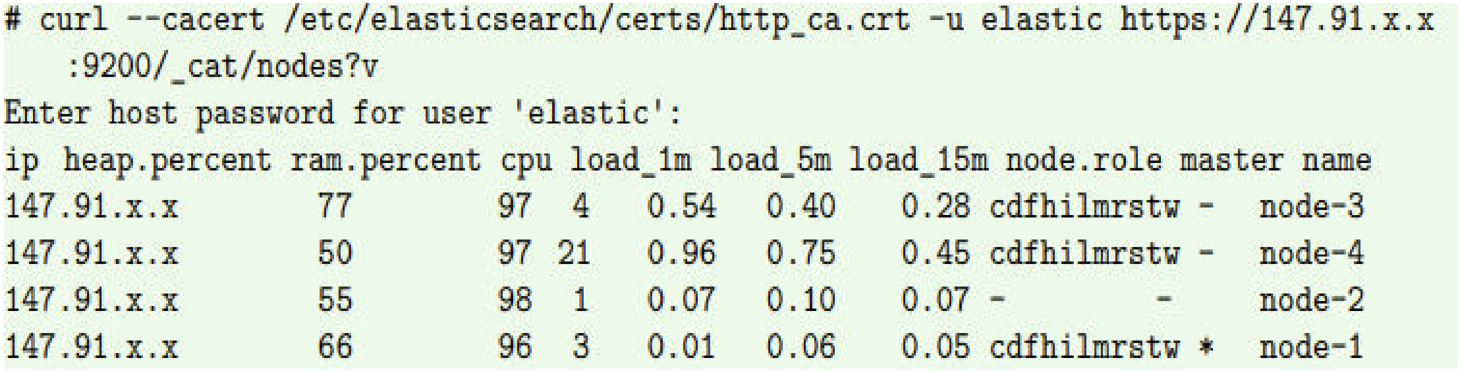
Basic Elasticsearch commands

Example of creating an index



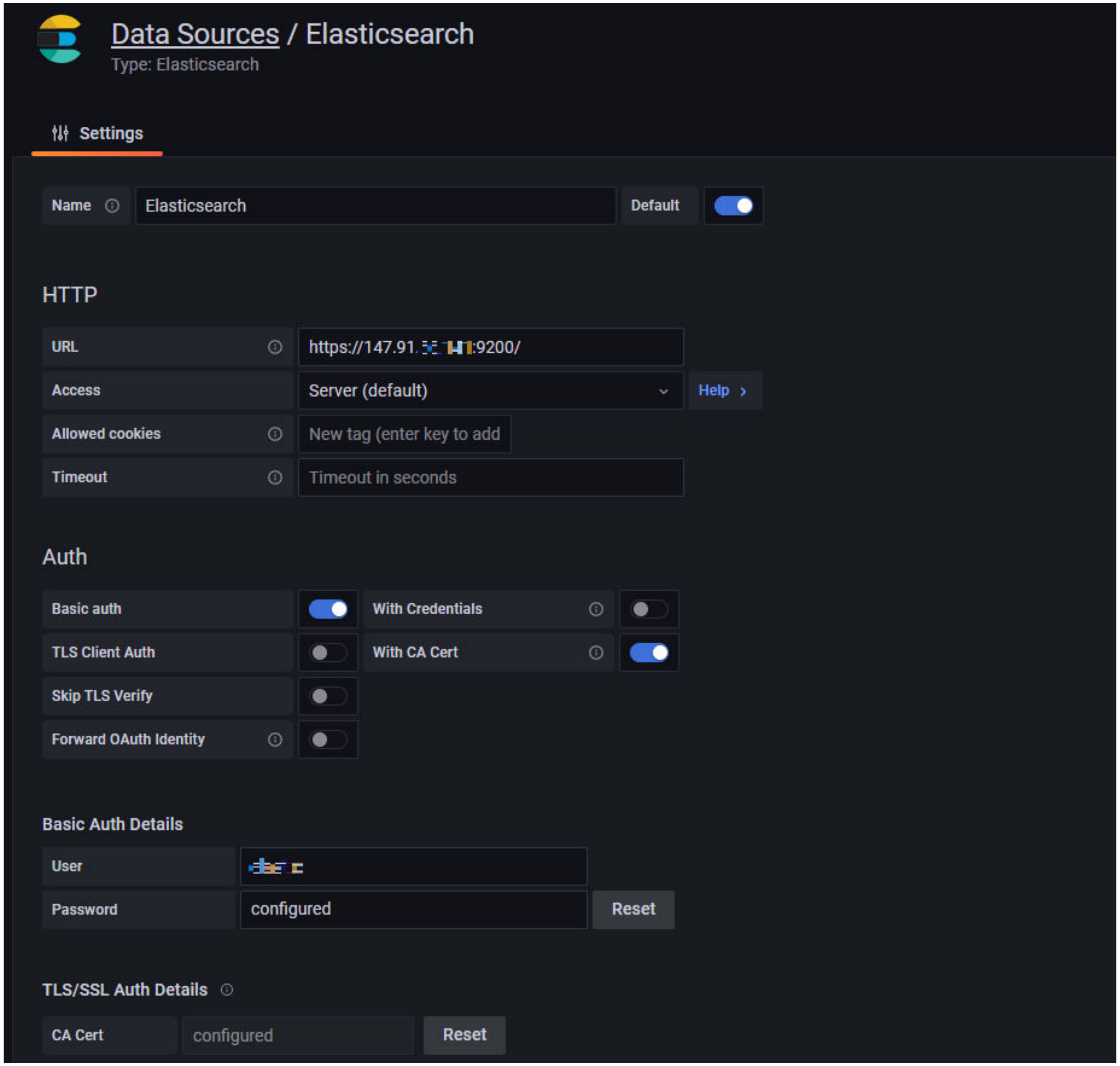
```
# curl -X PUT --cacert /etc/elasticsearch/certs/http_ca.crt -u elastic https
    ://147.91.x.x:9200/monitoring?pretty
Enter host password for user 'elastic':
{
  "acknowledged" : true,
  "shards_acknowledged" : true,
  "index" : "monitoring"
}
```

Example of all cluster configuration information



```
# 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
```

Elasticsearch data source configuration within Grafana software



Data Sources / Elasticsearch
Type: Elasticsearch

Settings

Name: Elasticsearch
Default: ● on

HTTP

URL: https://147.91.[redacted]:9200/
Access: Server (default)

Allowed cookies: New tag (enter key to add
Timeout: Timeout in seconds

Auth

Basic auth: ● on
With Credentials: ○ off
TLS Client Auth: ○ off
With CA Cert: ● on
Skip TLS Verify: ○ off
Forward OAuth Identity: ○ off

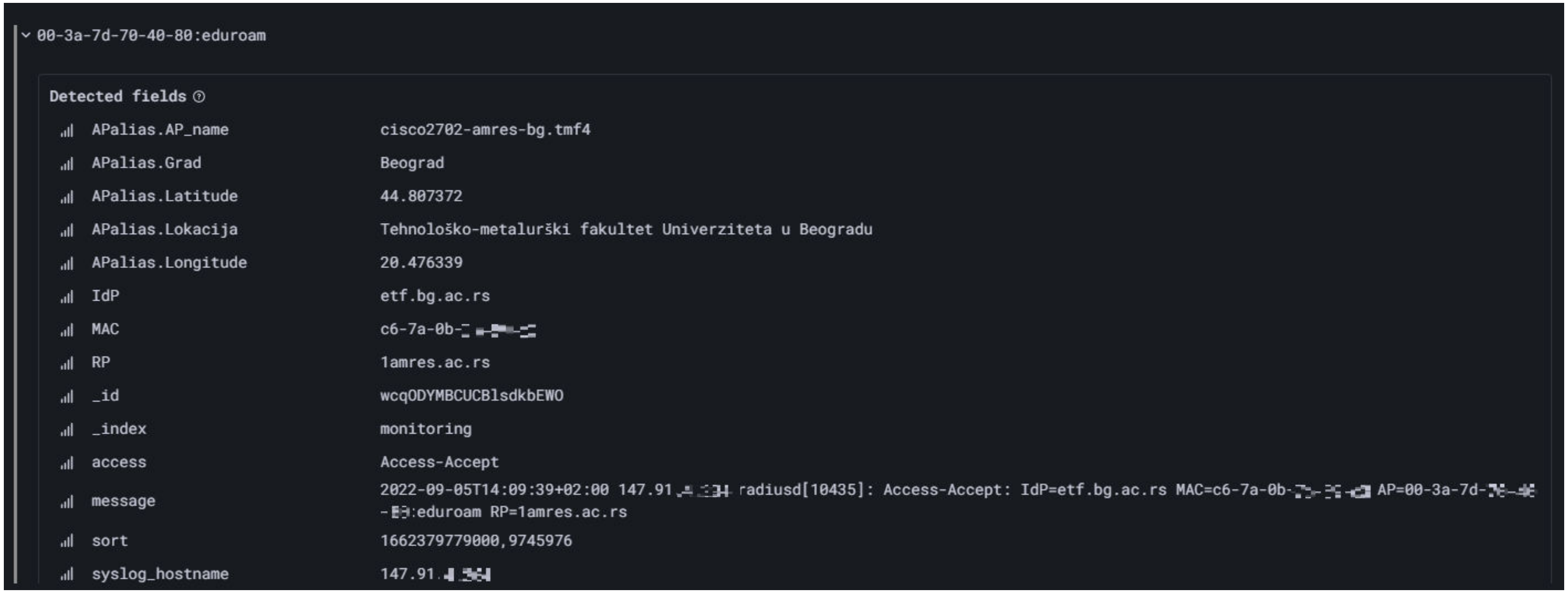
Basic Auth Details

User: [redacted]
Password: configured

TLS/SSL Auth Details

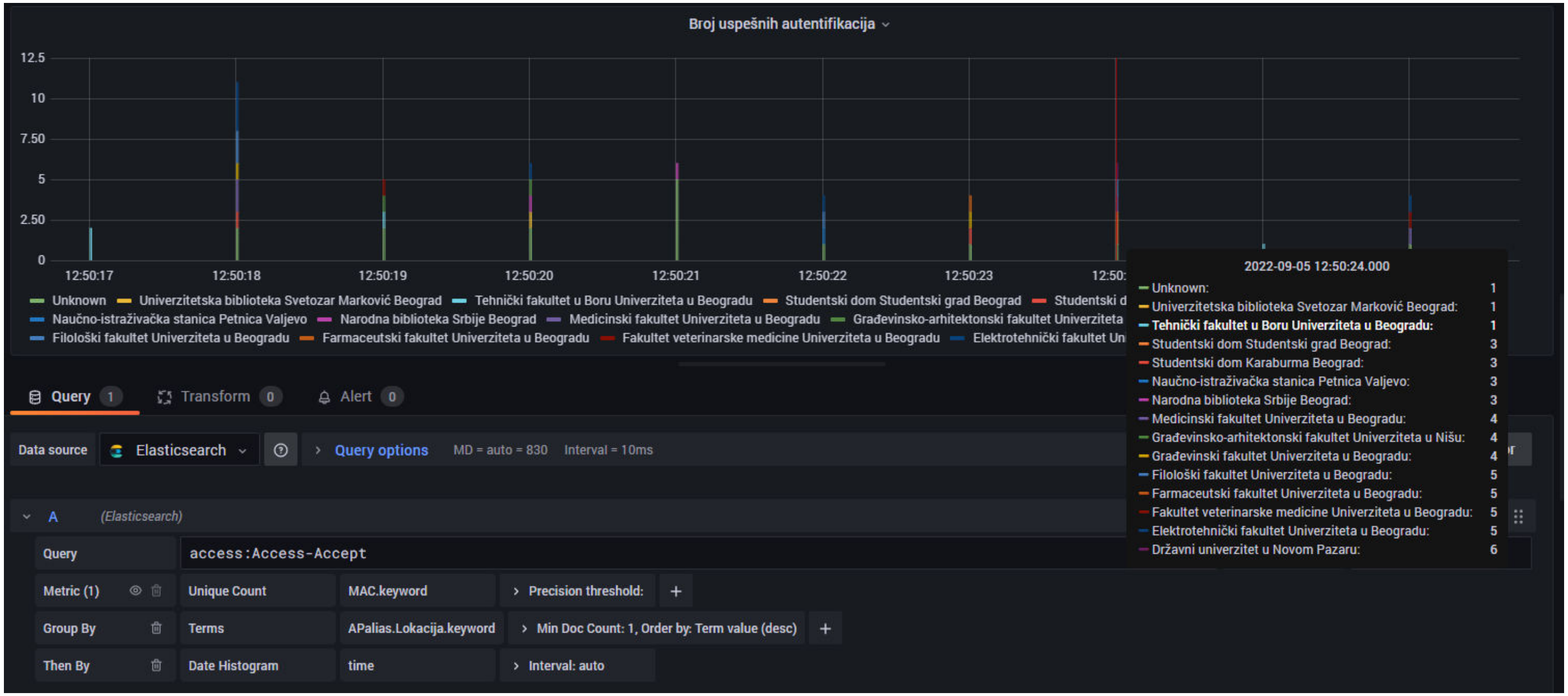
CA Cert: configured

Example of log messages displayed by Grafana software



```
⌄ 00-3a-7d-70-40-80:eduroam

Detected fields ⓘ
  APalias.AP_name       cisco2702-amres-bg.tmf4
  APalias.Grad          Beograd
  APalias.Latitude      44.807372
  APalias.Lokacija      Tehnološko-metalurški fakultet Univerziteta u Beogradu
  APalias.Longitude     20.476339
  IdP                   etf.bg.ac.rs
  MAC                   c6-7a-0b-[redacted]
  RP                    1amres.ac.rs
  _id                   wcqODYMBCUCBlsdkbEWO
  _index                monitoring
  access                Access-Accept
  message               2022-09-05T14:09:39+02:00 147.91.[redacted] radiusd[10435]: Access-Accept: IdP=etf.bg.ac.rs MAC=c6-7a-0b-[redacted] AP=00-3a-7d-[redacted]
                        -[redacted]:eduroam RP=1amres.ac.rs
  sort                  1662379779000,9745976
  syslog_hostname       147.91.[redacted]
```

Example of Grafana query that visualizes eduroam service usage statistics


Broj uspešnih autentifikacija
12.5
10
7.50
5
2.50
0
12:50:17
12:50:18
12:50:19
12:50:20
12:50:21
12:50:22
12:50:23
12:50:
Unknown
Univerzitetska biblioteka Svetozar Marković Beograd
Tehnički fakultet u Boru Univerziteta u Beogradu
Studentski dom Studentski grad Beograd
Studentski d
Naučno-istraživačka stanica Petnica Valjevo
Narodna biblioteka Srbije Beograd
Medicinski fakultet Univerziteta u Beogradu
Građevinsko-arhitektonski fakultet Univerziteta
Filološki fakultet Univerziteta u Beogradu
Farmaceutski fakultet Univerziteta u Beogradu
Fakultet veterinarske medicine Univerziteta u Beogradu
Elektrotehnički fakultet Un
Query 1
Transform 0
Alert 0

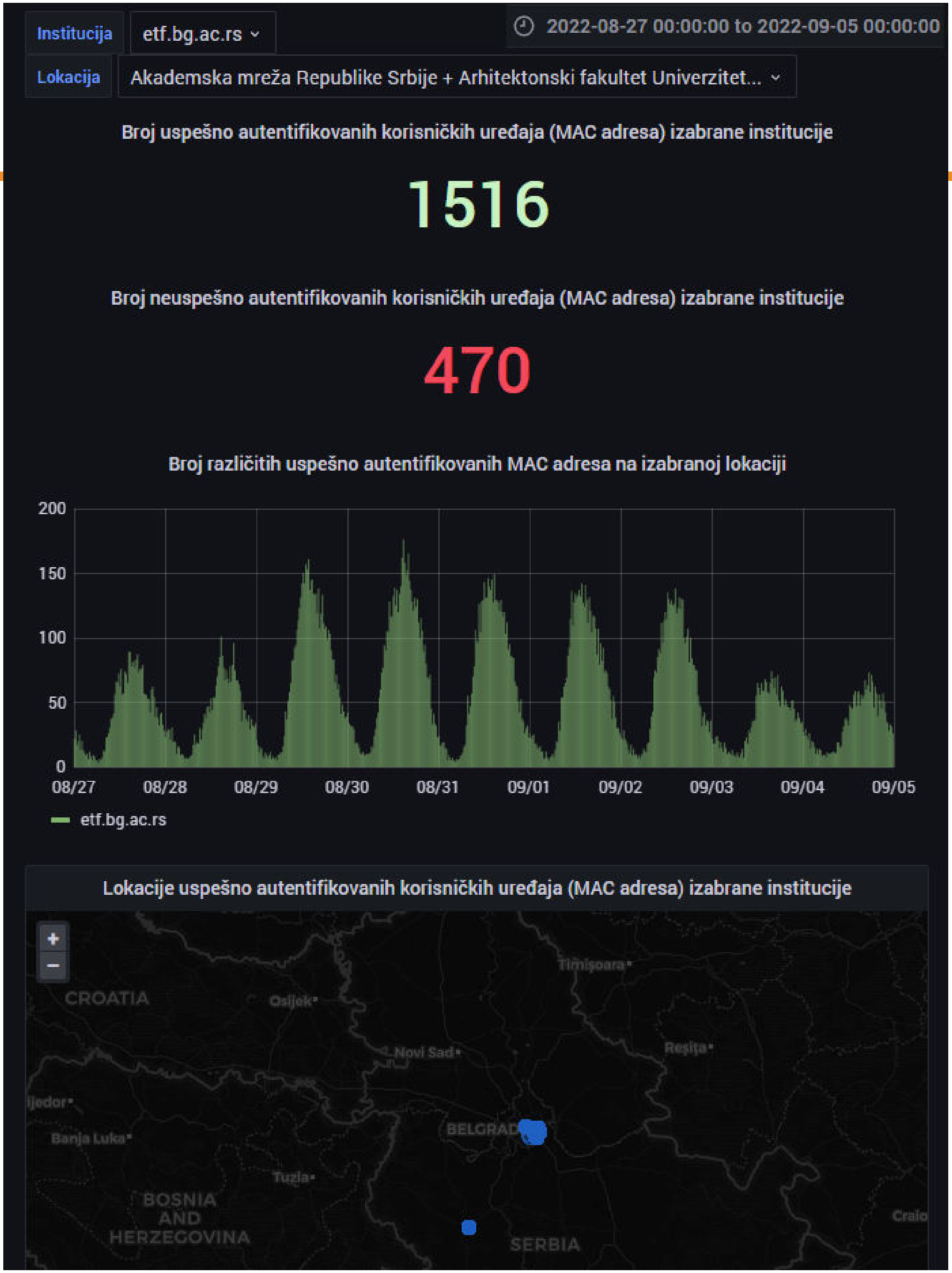
```
2022-09-05 12:50:24.000
Unknown:                                                  1
Univerzitetska biblioteka Svetozar Marković Beograd:      1
Tehnički fakultet u Boru Univerziteta u Beogradu:         1
Studentski dom Studentski grad Beograd:                   3
Studentski dom Karaburma Beograd:                         3
Naučno-istraživačka stanica Petnica Valjevo:              3
Narodna biblioteka Srbije Beograd:                        3
Medicinski fakultet Univerziteta u Beogradu:              4
Građevinsko-arhitektonski fakultet Univerziteta u Nišu:   4
Građevinski fakultet Univerziteta u Beogradu:             4
Filološki fakultet Univerziteta u Beogradu:               5
Farmaceutski fakultet Univerziteta u Beogradu:            5
Fakultet veterinarske medicine Univerziteta u Beogradu:   5
Elektrotehnički fakultet Univerziteta u Beogradu:         5
Državni univerzitet u Novom Pazaru:                       6
```

Data source: Elasticsearch

Query options MD = auto = 830 Interval = 10ms

A (Elasticsearch)

Query	access:Access-Accept		
Metric (1)	Unique Count	MAC.keyword	Precision threshold:
Group By	Terms	APalias.Lokacija.keyword	Min Doc Count: 1, Order by: Term value (desc)
Then By	Date Histogram	time	Interval: auto



Institucija etf.bg.ac.rs

2022-08-27 00:00:00 to 2022-09-05 00:00:00

Lokacija Akademska mreža Republike Srbije + Arhitektonski fakultet Univerzitet...

Broj uspešno autentifikovanih korisničkih uređaja (MAC adresa) izabrane institucije

1516

Broj neuspešno autentifikovanih korisničkih uređaja (MAC adresa) izabrane institucije

470

Broj različitih uspešno autentifikovanih MAC adresa na izabranoj lokaciji

Lokacije uspešno autentifikovanih korisničkih uređaja (MAC adresa) izabrane institucije

Q&A

THANK YOU!

Contact:

katarina.simonovic@amres.ac.rs