ELK

analitička platforma

Kristijan Duvnjak & Mladen Maravić

Tko smo mi?

Kristijan Duvnjak
kristijan.duvnjak@pbz.hr

Mladen Maravić
mladen.maravic@pbz.hr

PBZ ElasticSearch tim ☺

Što je ELK ?

Elasticsearch

Što je Elasticsearch?

- Document-oriented schema-free "database"
- Izgrađeno na Apache Lucene platformi
- Omogućuje *real-time* pretraživanje i analitiku
- Full-text pretraživanje
- Horizontalno distribuiran
- Visoka raspoloživost (klastering)
- REST API

"Open Source (Apache 2)

distributed

RESTful

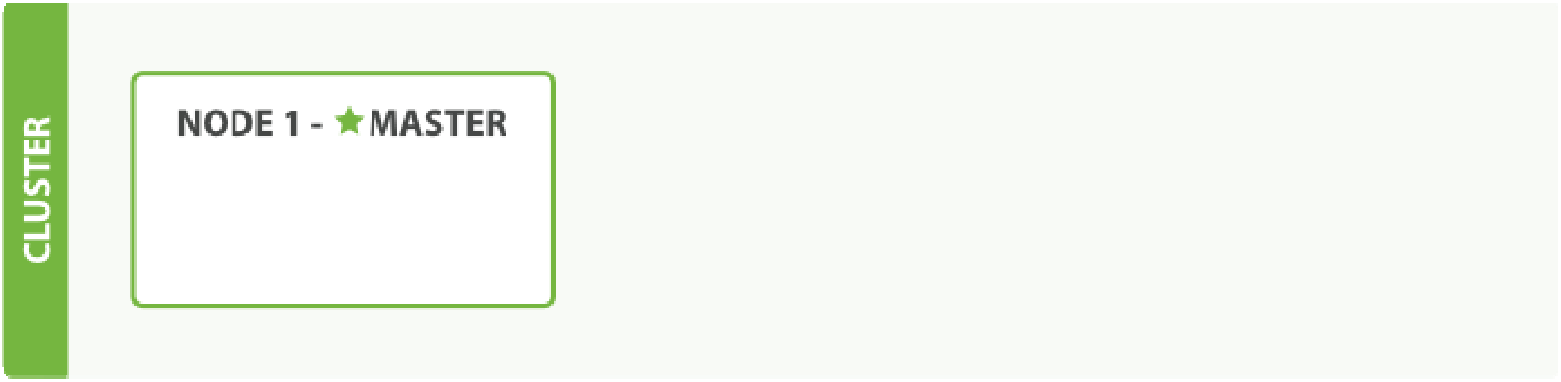
search engine

built on top of Lucene"

Usporedba sa relacijskim bazama podataka

Oracle	Elasticsearch
Database	Index
Partition	Shard
Table	Type
Row	Document
Column	Field
Schema	Mapping
Index	- (sve se "indeksira")
SQL	Query DSL

Visoka raspoloživost



- **Node** = instanca elasticsearch-a
- **Cluster** = 1 ili više node-ova koji imaju isto ime klastera
- Svaki klaster ima **1 master node**
- **Klijenti mogu razgovarati sa bilo kojim node-om u klasteru**
- 1 klaster može imati neograničeni broj indeksa

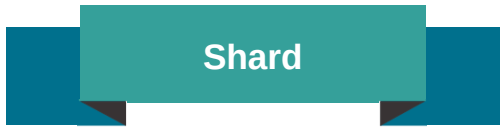
Indeksi i shardovi

- Svi podaci su pohranjeni u jednom ili više indeksa (eng. indexes)
- Indeks se sastoji od jednog ili više shardova

  (promjena broja shardova u indeksu

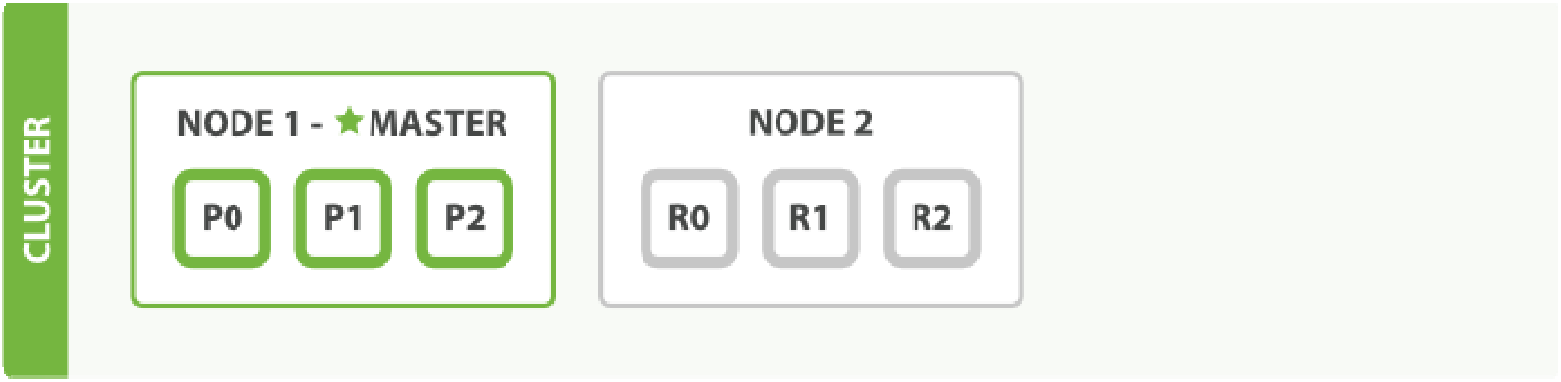
  zahtjeva reindeksaciju podataka)

- Indeks je mapa na disku



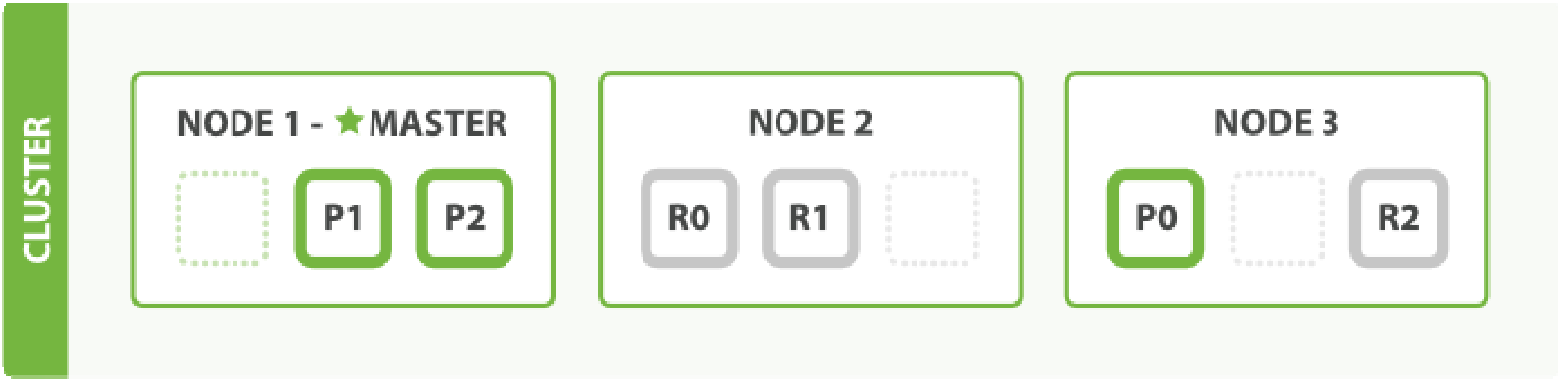
- Shard je instanca Lucene-a
- Svaki shard može imati 0 ili više replika

Visoka raspoloživost – dodavanje node-ova



- Primjer:
  - 3 indeksa
  - Svaki indeks ima jedan primarni (P) shard i jednu rednu repliku (R) shard-a

Visoka raspoloživost – dodajemo treći node



- Više primarnih shardova:
  - brže indeksiranje
  - povećana skalabilnost
- Više replika:
  - brže pretraživanje podataka
  - povećana raspoloživost

Dokumenti...

- Dokumenti su bazirani na JSON-u
- Shema nije obavezna
- Ukoliko shema nije zadana:
  - elasticsearch pogađa tipove podataka...
  - ...i indeksira sve podatke
- Ukoliko eksplicitno definiramo shemu (eng. explicit mapping):
  - Shema se odnosi na točno određeni tip dokumenta
  - Shema definira za svako polje:
    - tip (string, number, date...)
    - da li se indeksira?
    - da li se pohranjuje u indeks?

Dokumenti...

- Svaki dokument ima ID
- Moguće je definirati u koji shard se pohranjuje određeni dokument (eng. routing)
- Svaki dokument može imati i verziju

Indeksiranje

- inverted index

  Elasticsearch Server 1.0 (doc 1)
  Mastering Elasticsearch (doc 2)
  Apache Solr 4 Cookbook (doc 3)

Term	Count	Document
1.0	1	<1>
4	1	<3>
apache	1	<3>
cookbook	1	<3>
elasticsearch	2	<1>,<2>
mastering	1	<2>
server	1	<1>
solr	1	<3>

Primjer

```
POST /blog/blog_comment?routing=1
{
  "user_id" : 1,
  "date" : "2015-04-01T13:12:12",
  "comment" : "What's so cool about Elasticsearch?"
}
```

```
GET /blog/_mapping
{
   "blog": {
      "mappings": {
         "blog_comment": {
            "properties": {
               "comment": {
                  "type": "string"
               },
               "date": {
                  "type": "date",
                  "format": "dateOptionalTime"
               },
               "user_id": {
                  "type": "long"
               }
            }
         }
      }
   }
}
```

```
GET /blog/_search
{
   "took": 6,
   "timed_out": false,
   "_shards": {
      "total": 2,
      "successful": 2,
      "failed": 0
   },
   "hits": {
      "total": 1,
      "max_score": 1,
      "hits": [
         {
            "_index": "blog",
            "_type": "blog_comment",
            "_id": "AUzhH9M9HW_GzrF8oLAj",
            "_score": 1,
            "_source": {
               "user_id": 1,
               "date": "2015-04-01T13:12:12",
               "comment": "What's so cool about Elasticsearch?"
            }
         }
      ]
   }
}
```

Mogućnosti pretraživanja dokumenata

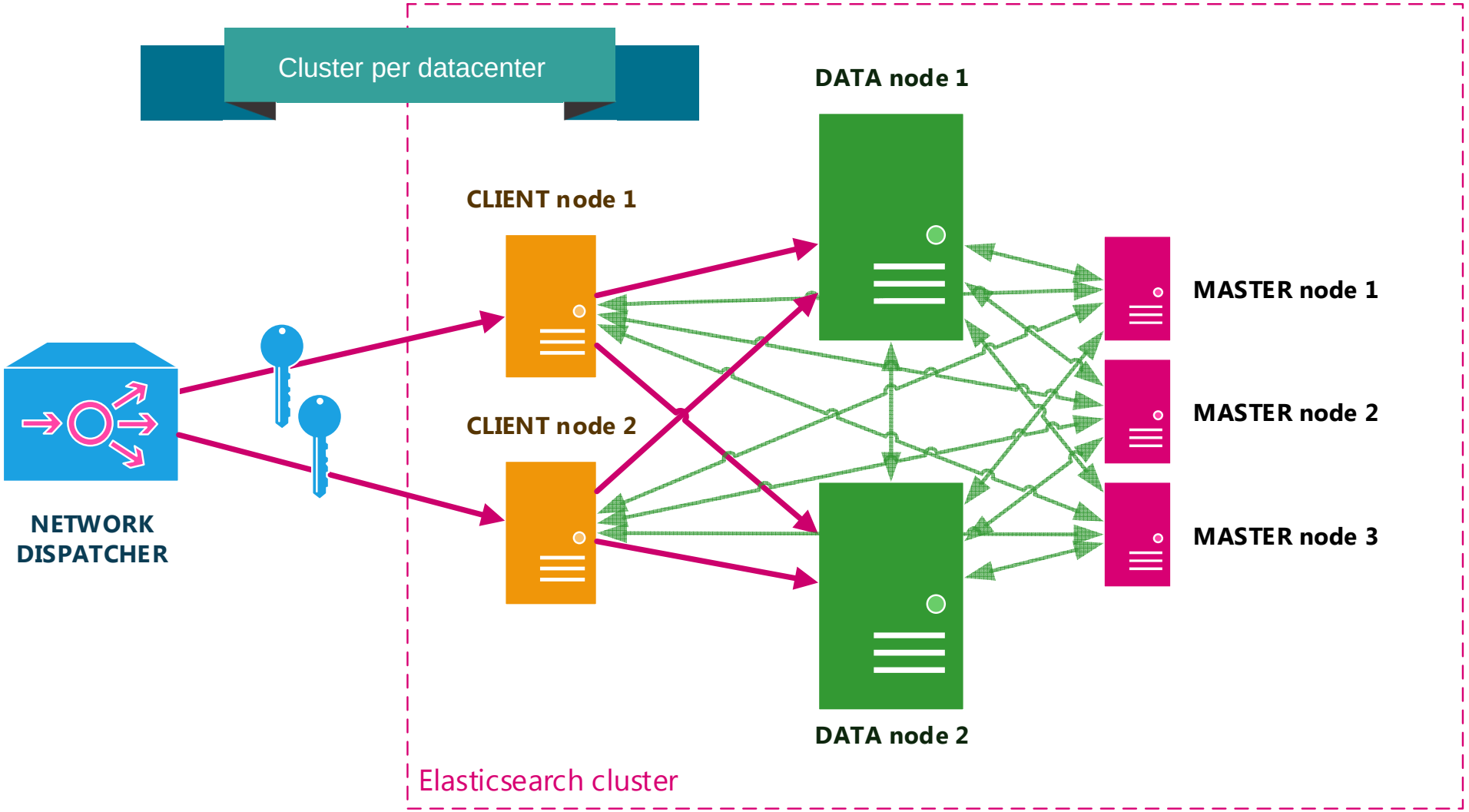
- Imamo sve standardne mogućnosti (sjetimo se WHERE klauzule u SQL-u)!
- Tu je i full-text pretraživanje sa podrškom za:
  - highlighting
  - stemming
  - ngrams & edge-ngrams
- Agregacije: term facets, date histograms, ranges
- Geo pretraživanje: bounding box, distance,distance ranges, polygons
- Percolators (or reverse-search!)

Primjer korištenja u PBZ-u

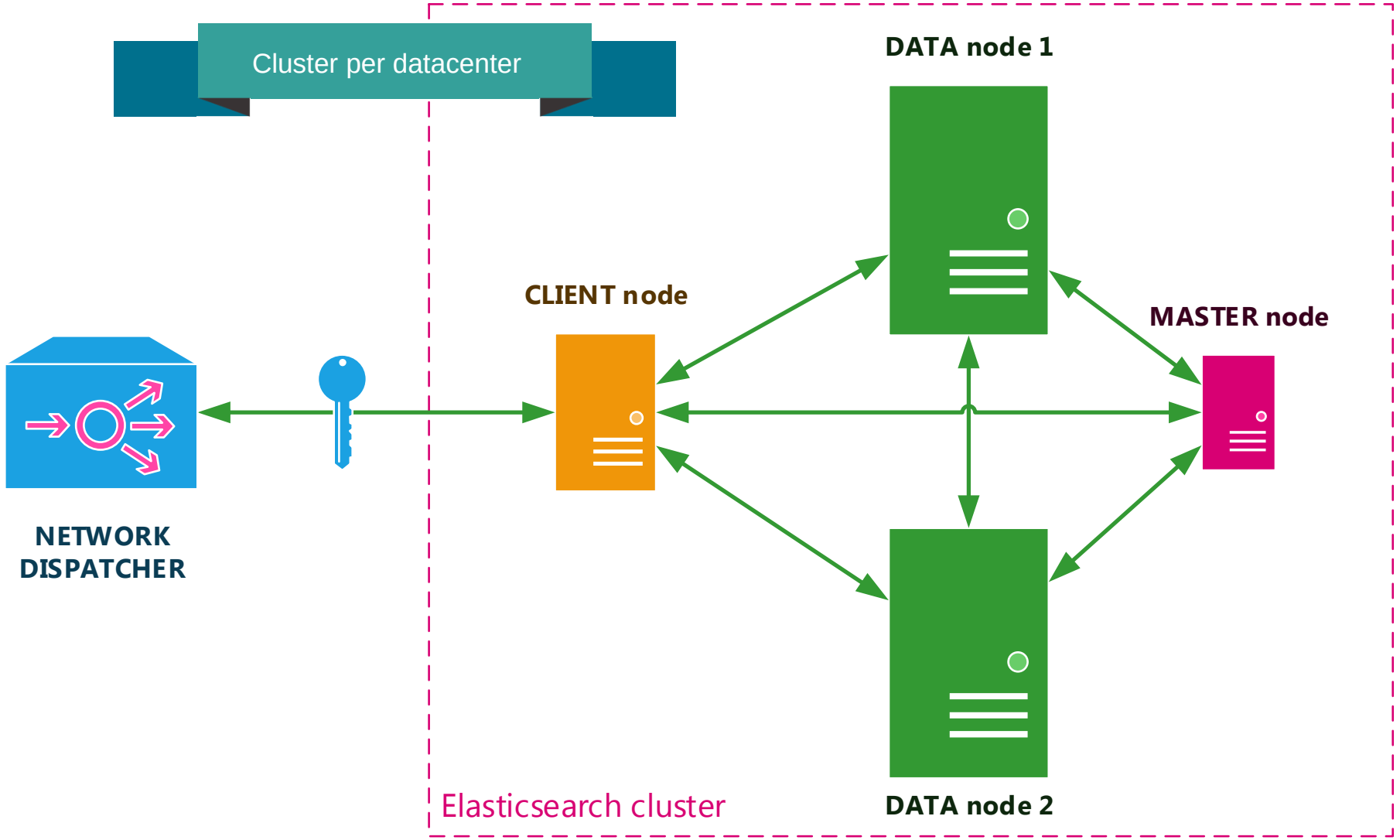
- prometi po računima građana: 600M dokumenata, 200M/godini
- *routing* po broju računa

- indeksiramo 30-40 tisuća dokumenata u sekundi
- Oracle perfomanse smo mjerili u sekundama, elasticsearch u milisekundama (3500 upita/sek):
  - pronađi zadnjih 100 prometa za zadani tekući račun **< 50 ms**
  - pronađi zadnjih 100 prometa za zadani tekući račun gdje opis plaćanja sadrži određene riječi **<100ms**
- **Performanse elasticsearch-a skoro pa ne variraju!**

PBZ ES arhitektura - idealno



PBZ ES arhitektura – konačno rješenje



Logstash

Što je logstash?

- Zasebna komponenta koja omogućuje 3 osnovne operacije:
  - **Prikupljanje** podataka (uglavnom logova, ali ne nužno – recimo poruke sa JMS queue-ova)
  - **Transformacija** podataka
  - **Prijenos** podataka (u pravilu u elasticsearch, ali ne nužno)
- Jednostavna instalacija (unzip & run)
- Jednostavna konfiguracija (1 JSON datoteka)
- Lako pisanje dodatnih pluginova

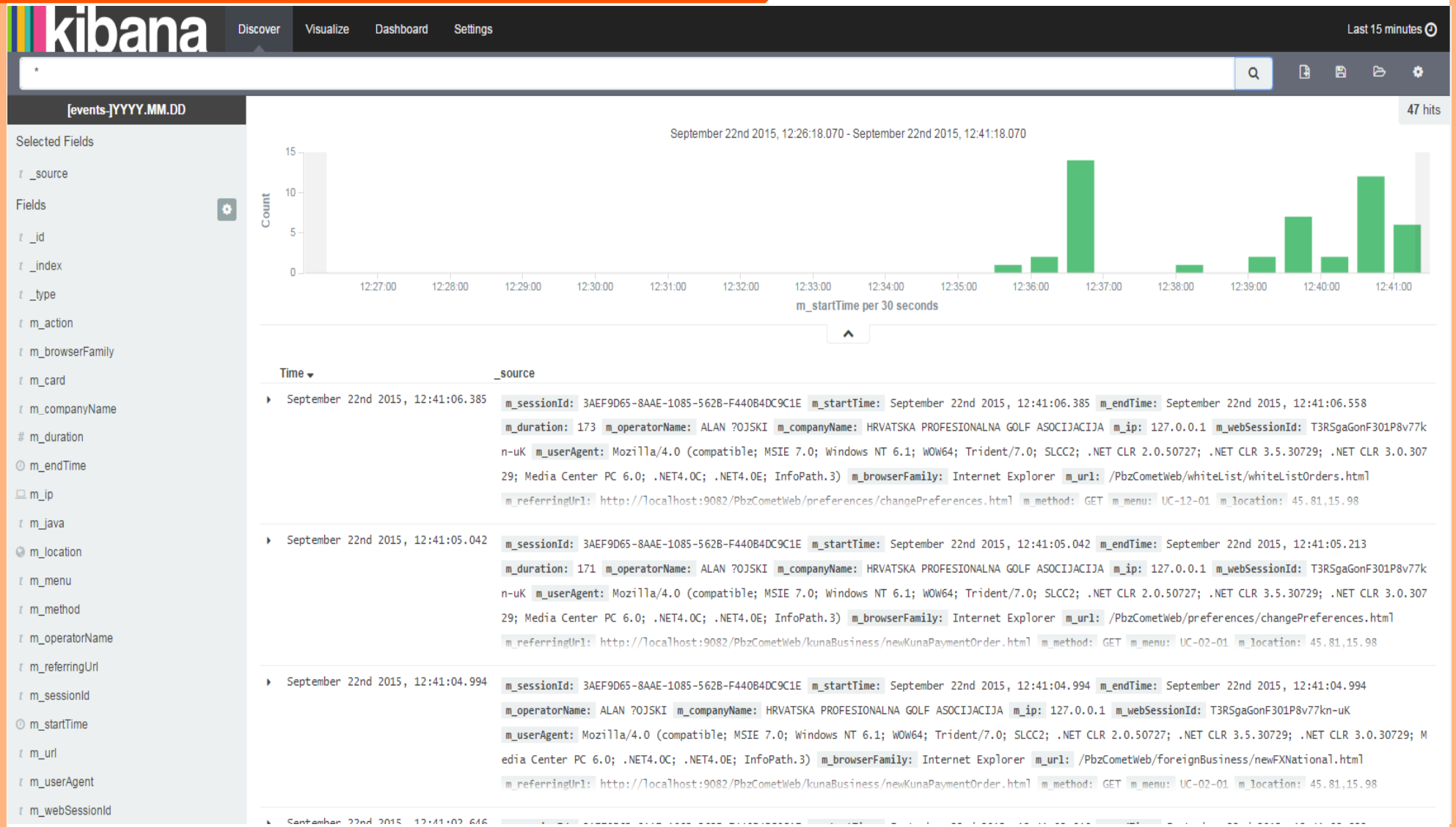
Kibana

Kibana uvod

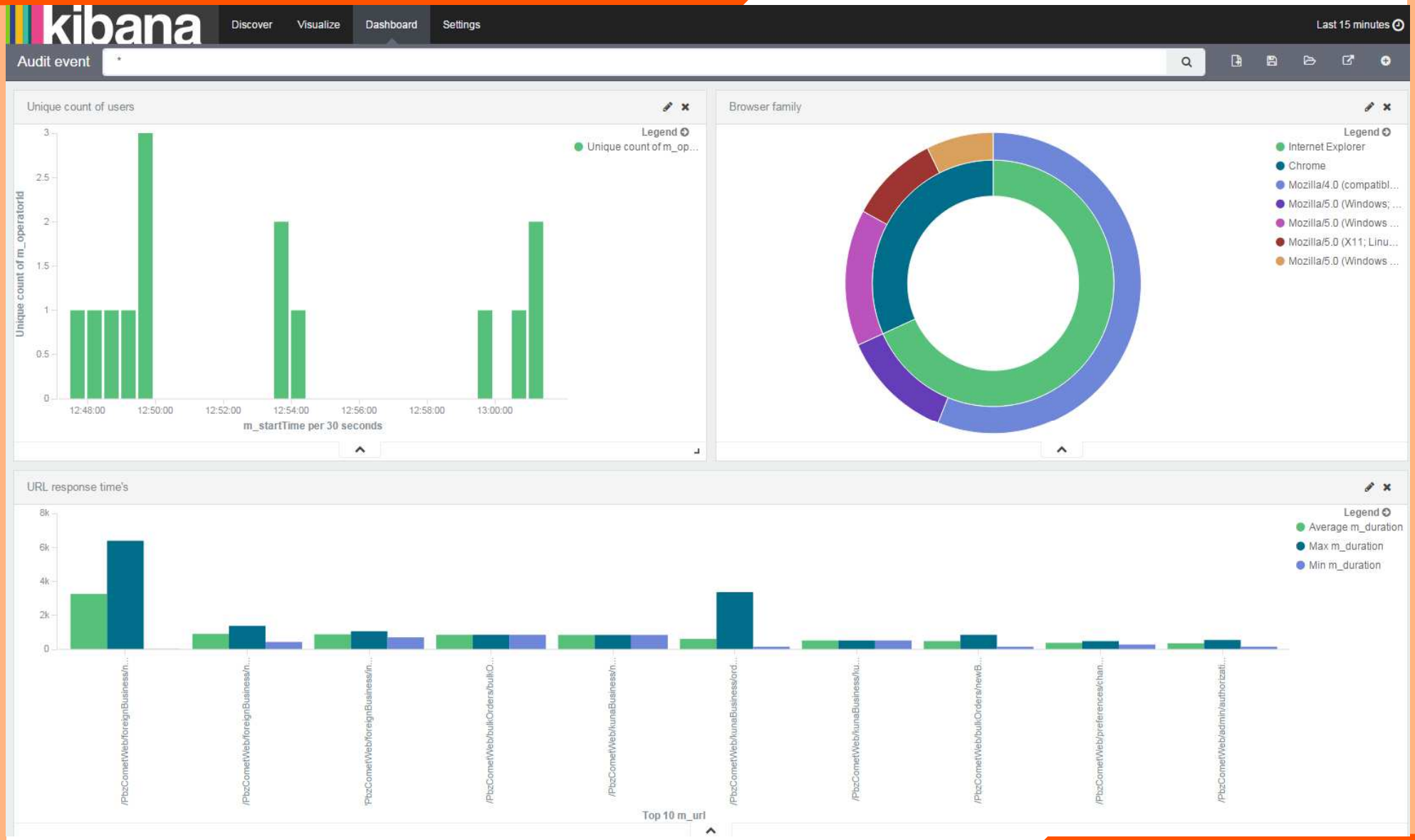
- **elasticsearch korisničko sučelje za pretraživanje i vizualizaciju podataka**
- omogućuje izradu *dashboard*-ova, agregacija, dijeljenje prikaza
- Kibana podržava format index-a sa vremenskom komponentom (po satu, danu ...),

  [events-]YYYY.MM.DD
- podržava dinamički *mapping* (shemu podataka):
  - prednosti: puno veća mogućnost pretraživanja
  - nedostatci: problem održavanja mappinga i performanse
- vizualizacija: area chart, data table, line chart, markdown widget, metric, pie chart, tile map, vertical bar chart
- pretraživanje postavljanjem upita:
  - “GET”, “Plaćanje struje”, Plaćanje struje (Plaćanje OR struje)
  - m_operatorId: 3454534534534, m_companyName: *Tvornica
  - m_duration: [100 TO *] ili {100 TO *}

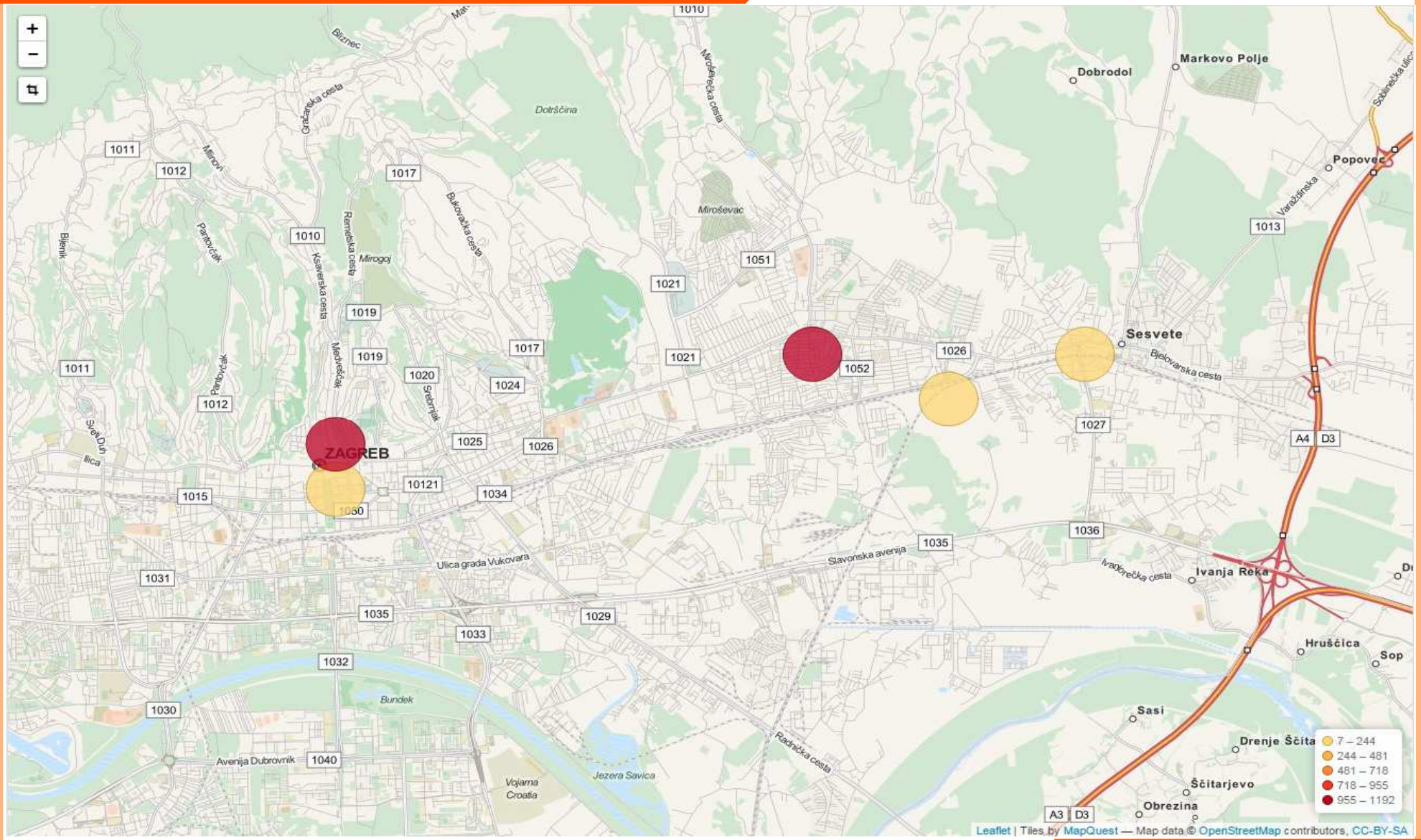
Kibana korisničko sučelje



Kibana dashboard



Kibana mapa

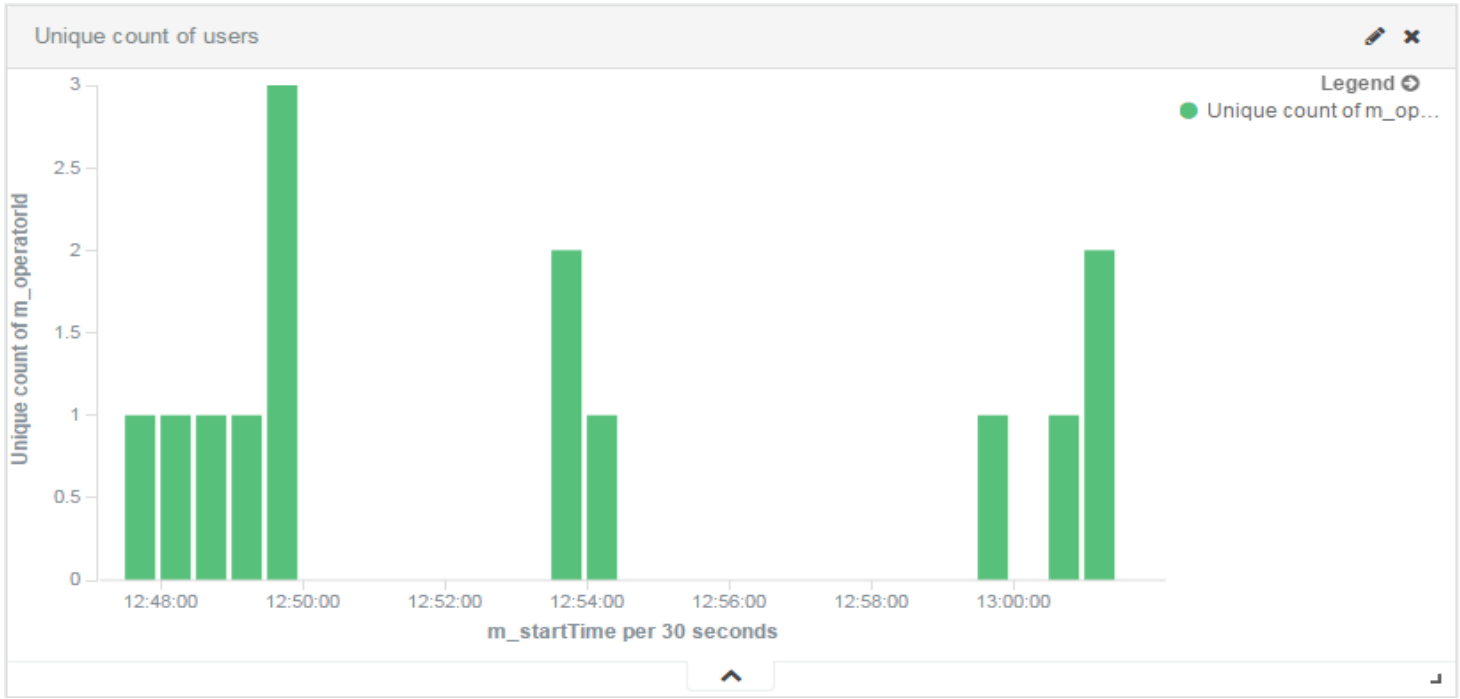

ZAGREB
Dobrodol
Markovo Polje
Popovec
Sesvete
Ivanja Reka
Hruščica
Sop
Sasi
Drenje Ščita
Ščitarjevo
Obrezina
Dotrščina
Mirogoj
Miroševac
Bundek
Jezera Savica
Vojama
Croatia
Ulica grada Vukovara
Slavonska avenija
Avenija Dubrovnik
Radnička cesta
Bjelovarska cesta
Ivanječka cesta
Varaždinska
Sesvetska ulica
A4
D3
A3
1010
1011
1012
1013
1015
1017
1019
1020
1021
1024
1025
1026
1027
1029
1030
1031
1032
1033
1034
1035
1036
1040
1050
1051
1052
10121
7 – 244
244 – 481
481 – 718
718 – 955
955 – 1192
Leaflet | Tiles by MapQuest — Map data © OpenStreetMap contributors, CC-BY-SA

Audit događaja

- praćenje događaja u aplikaciji (web, mobile)
- Java servlet filteri, SOAP interceptori, java interceptori
- thread local varijable
- asinkroni zapis podataka
- komunikacija sa Elasticsearch-om:
  - REST
  - zapisi u log, Logstash ➔ Elasticsearch
- mogućnosti:
  - pretraživanje zbog forenzike, sigurnosti, integracija sa helpdeskom
  - prikaz statistika i grafova o aplikaciji ili grupi korisnika/klijenata
  - podatci za poslovnu stranu, marketing ...

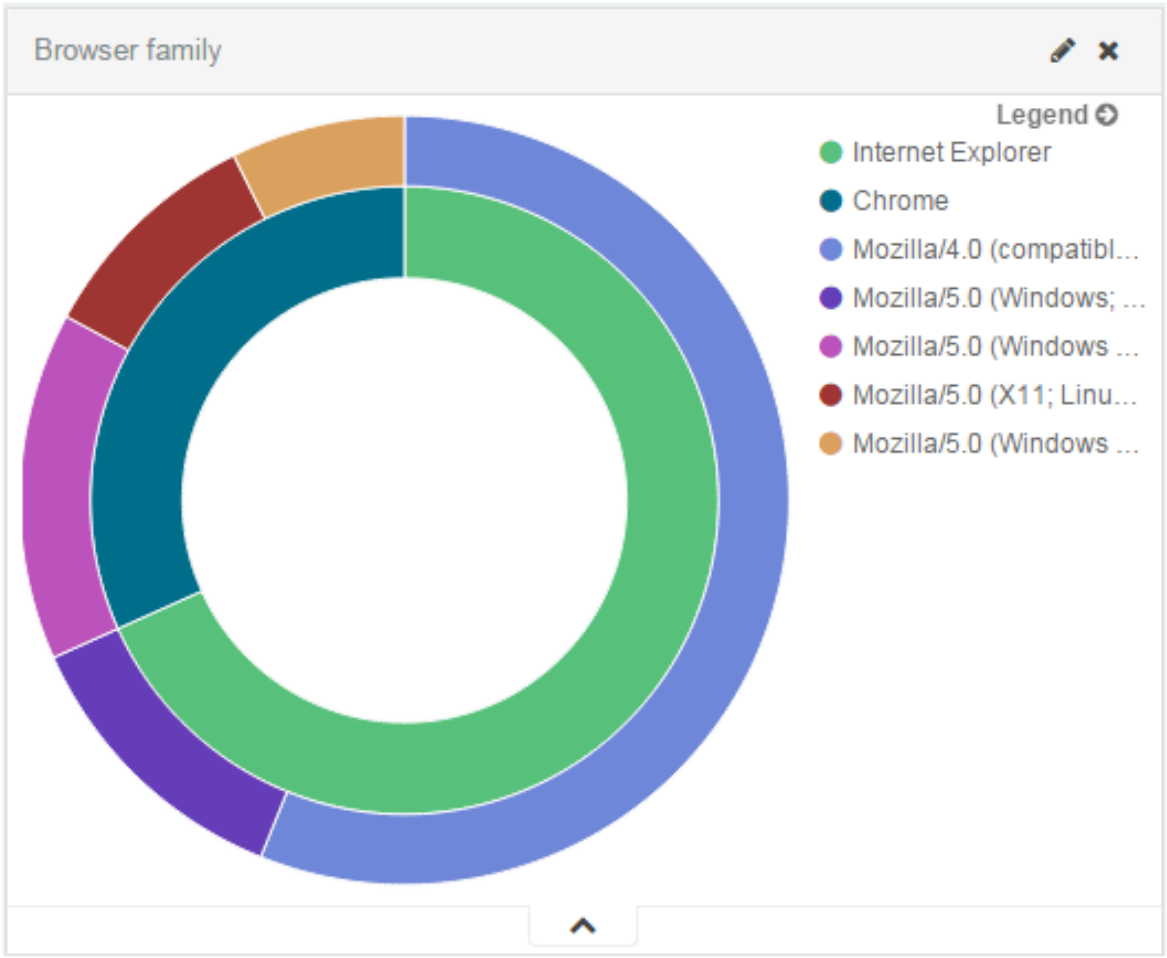
Jedinstveni broj korisnika

```
GET events*/_search?search_type=count
{
    "aggs" : {
        "user_count" : {
            "cardinality" : {
                "field" : "m_operatorId"
            }
        }
    }
}
```



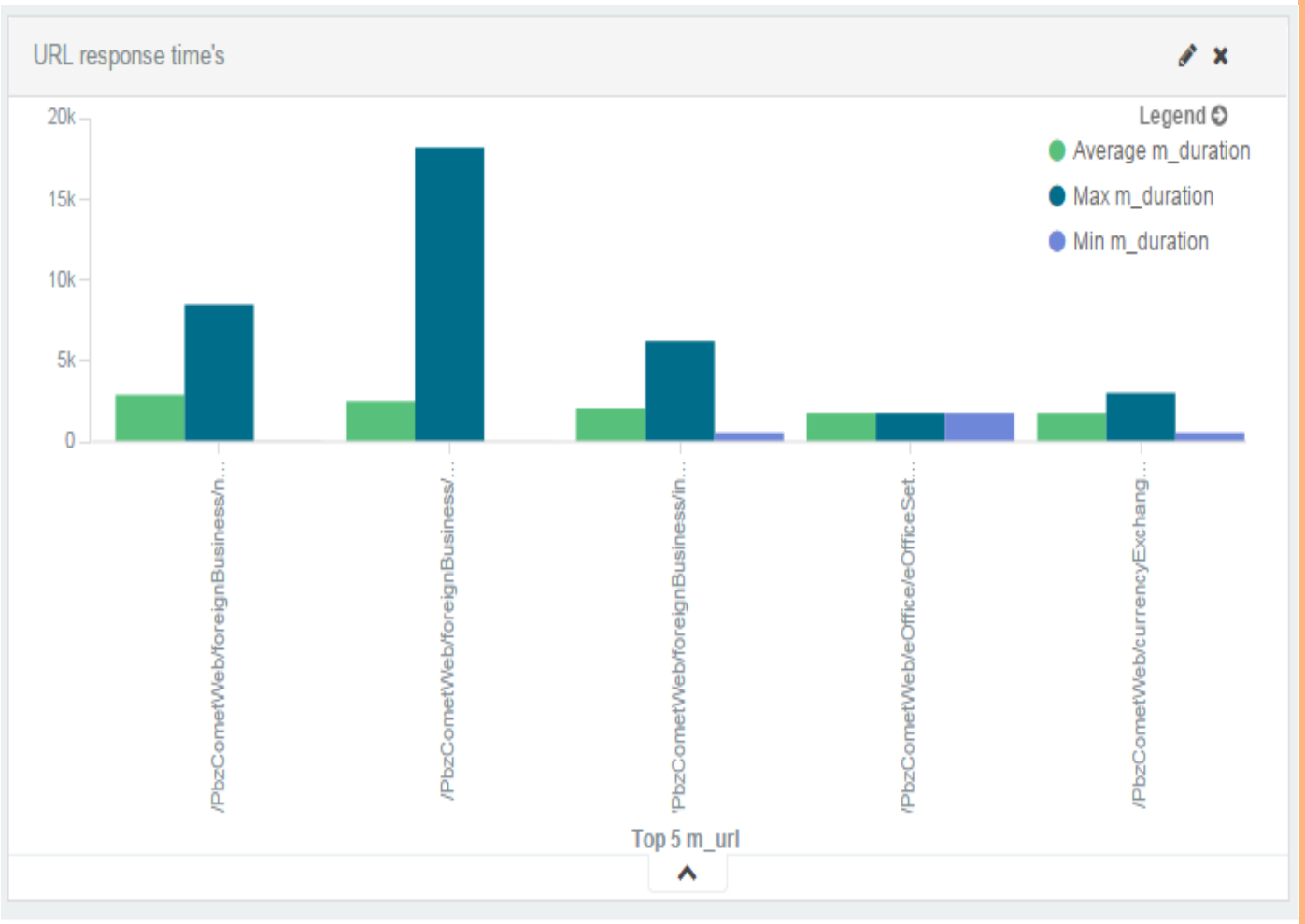
Tipovi preglednika

```
GET events*/_search?search_type=count
{
  "aggs": {
    "browser": {
      "terms": {
        "field": "m_browserFamily",
        "size": 5,
        "order": {
          "_count": "desc"
        }
      },
      "aggs": {
        "user_agent": {
          "terms": {
            "field": "m_userAgent",
            "size": 5,
            "order": {
              "_count": "desc"
            }
          }
        }
      }
    }
  }
}
```

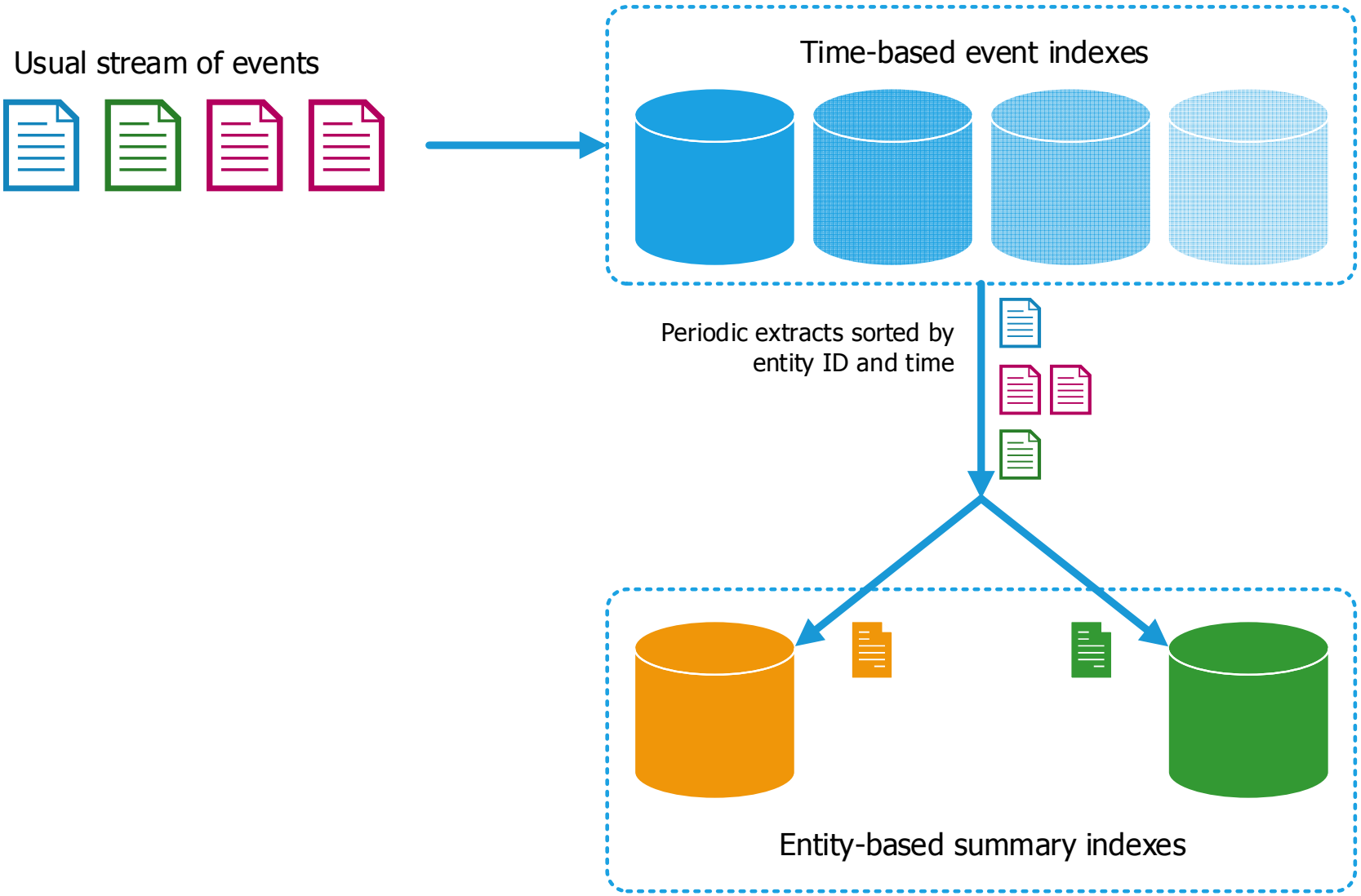


Funkcionalnosti u aplikaciji

```
GET events*/_search?search_type=count
{
  "aggs": {
    "url_stats": {
      "terms": {
        "field": "m_url",
        "size": 10,
        "order": {
          "avg_duration": "desc"
        }
      },
      "aggs": {
        "avg_duration": {
          "avg": {
            "field": "m_duration"
          }
        },
        "max_duration": {
          "max": {
            "field": "m_duration"
          }
        },
        "min_duration": {
          "min": {
            "field": "m_duration"
          }
        }
      }
    }
  }
}
```



Entity / event indeksi



Alarmi (Watcher plugin)

- Alarmi i notifikacije (aktivacija, upit, uvjeti, akcije)
- aktivacija:
  - vremenska ili u intervalima
  - cron izrazi
- upit definira izvor podataka (jednostavni upiti – konstanta, ES query, http web servis-JSON)
- uvjeti (uvijek, nikada, usporedba ili skripte (default Groovy))
- akcije
  - logging (samo za testne uvijete)
  - mail notifikacije(mogućnosti prilaganja rezultata)
  - webhook, htttp request
  - upis u ES-a

Alarmi (Watcher plugin) primjer

```
PUT /_watcher/watch/url_duration_status
{
  "trigger": {
    "schedule": {
      "interval": "5m"
    }
  },
  "input": {
    "search": {
      "request": {
        "indices": [
          "<events-{now/d}>"
        ],
        "body": {
          "fields": [
            "m_url",
            "m_duration"
          ],
          "query": {
            "filtered": {
              "query": {
                "range": {
                  "m_duration": {
                    "gte": 10000
                  }
                }
              },
              "filter": {
                "range": {
                  "m_endTime": {
                    "from": "now-10m"
                  }
                }
              }
            }
          }
```

```
"condition": {
    "compare": {
      "ctx.payload.hits.total": {
        "gt": 0
      }
    }
  },
  "actions": {
    "email_admin": {
      "email": {
        "to": ˇes_alert@pbz.hr",
        "subject": "{{ctx.watch_id}} executed",
        "body": "{{ctx.watch_id}} executed with
{{ctx.payload.hits.total}} hits.",
        "attach_data": true
      }
    }
  }
}
```

fields:
m_url:
- "/PbzCometWeb/foreignBusiness/newFXNational.html"
m_duration:
- 10045

Q & A