Централизованный сбор логов MikroTik с помощью ELK (Elasticsearch, Logstash, Kibana)

Козлов Роман
IntegraSky

Централизованный сбор логов MikroTik с помощью ELK (Elasticsearch, Logstash, Kibana)

Козлов Роман
IntegraSky

Проблема log

1. Сложно читаемый формат
2. Нет централизованного сборщика
3. Неудобный формат поиска
4. Для каждого конкретного приложения различные приложения для обработки логов.

Что нам нужно?

1. Open source
2. Единое приложение для всех log.
3. Возможность далать свои анализаторы.
4. Визуализация.
5. Веб приложение.

Что нам нужно?

1. Open source
2. Единое приложение для всех log.
3. Возможность далать свои анализаторы.
4. Визуализация.
5. Веб приложение.

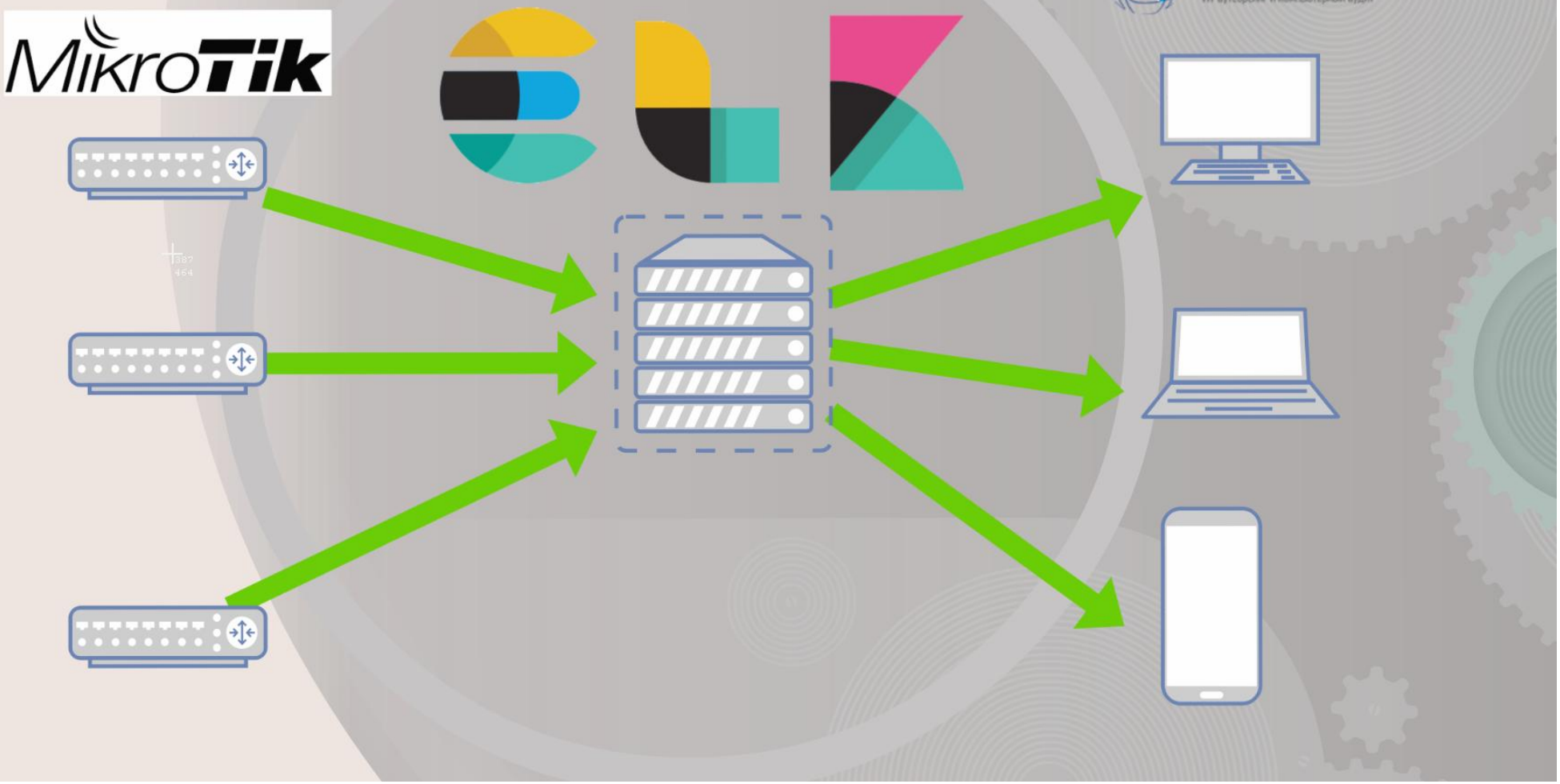
Elasticsearch
logstash и kibana
ELK

lasticsearch - система полнотекстового поиска информации.

ogstash - сервер сборки, фильтрации и перенаправления информации.

ibana - веб интерфейс поиска и визуализации данных из Elasticsearch

Схема получения log файлов



Что мы получаем от ELK?

1. Быстрый поиск сетевых проблем.
2. Веб поведение пользователей
4. Анализ проблем безопастности

Наст

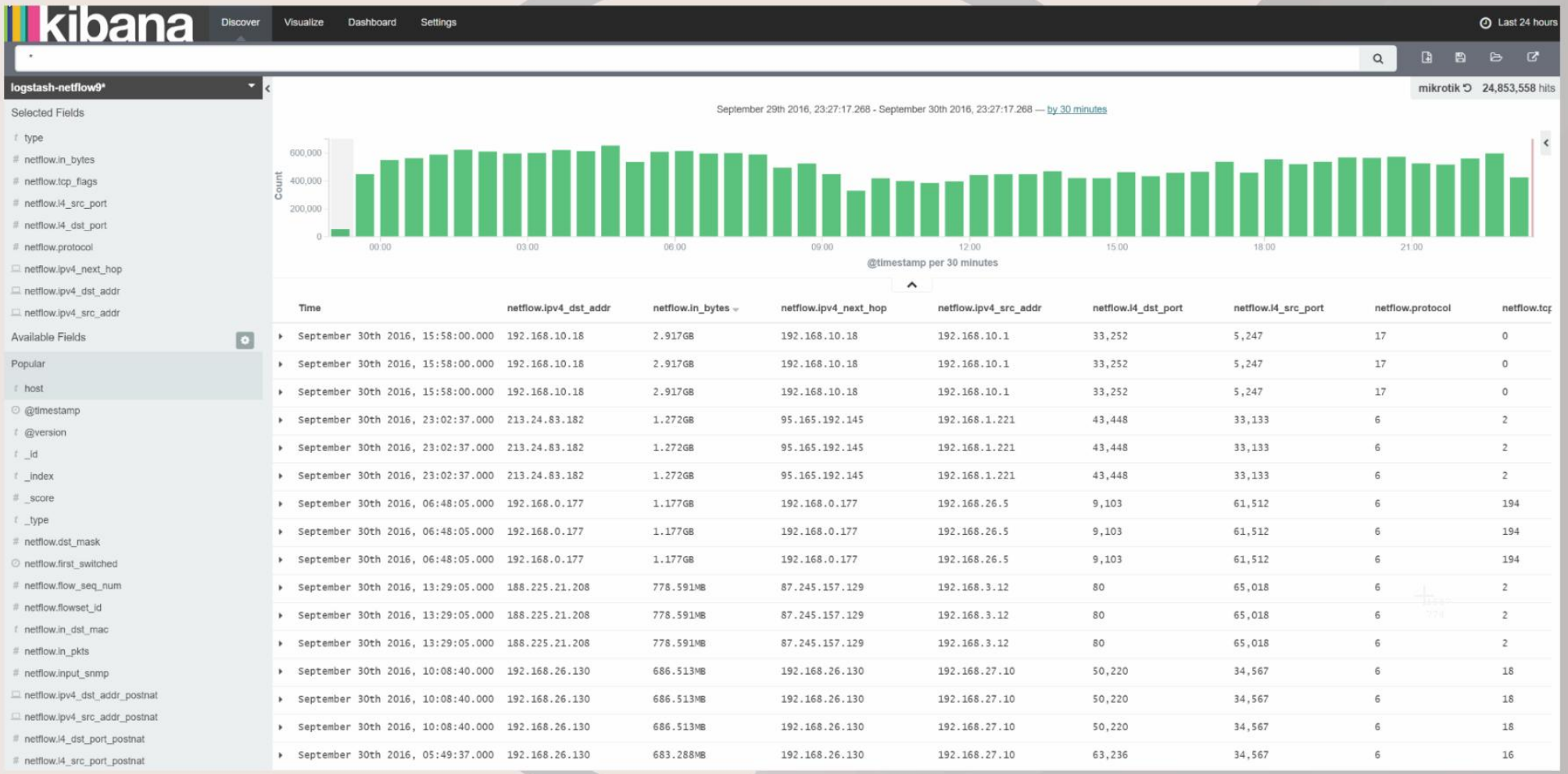
/system logg

Наст

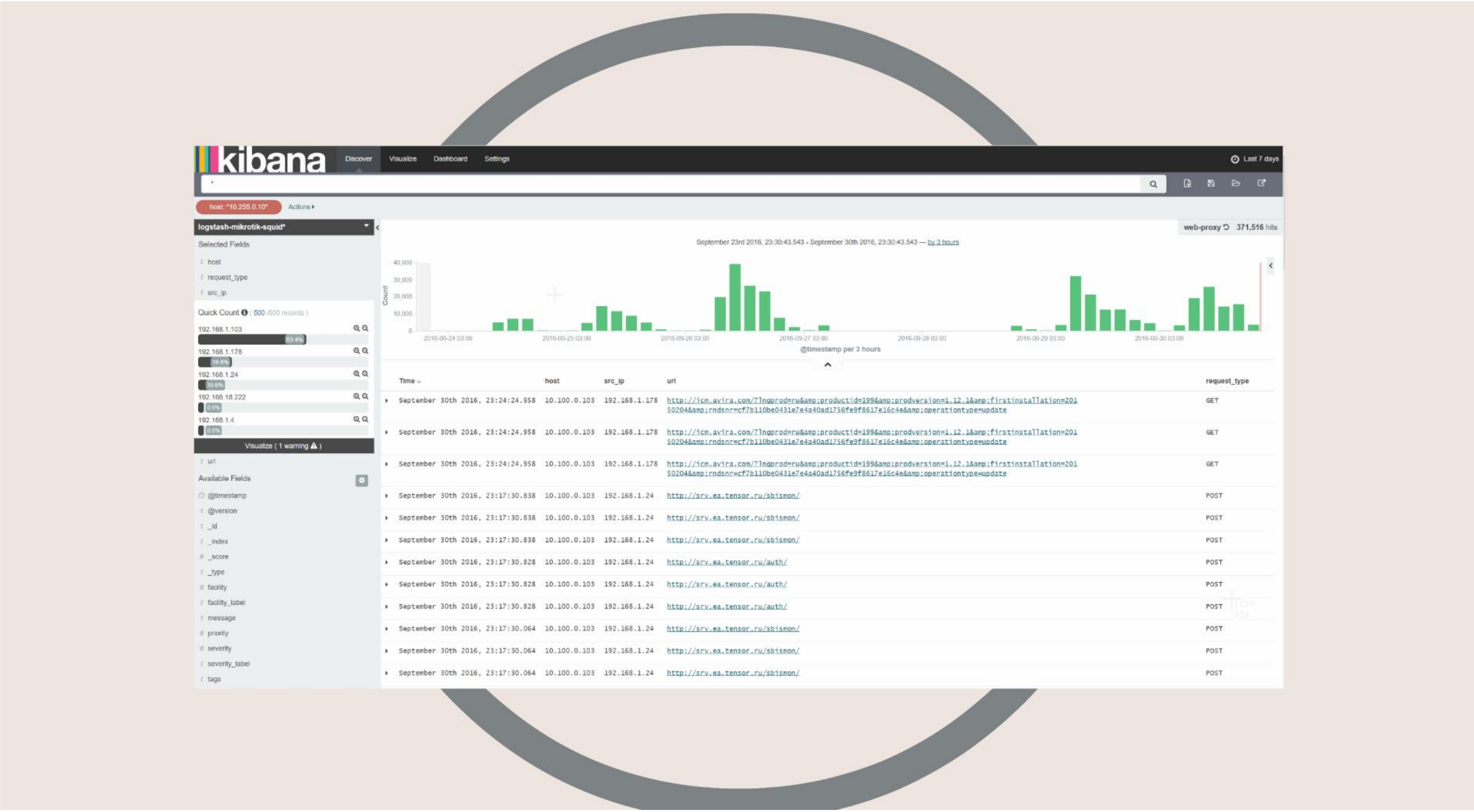
/opt/log
MIKRO

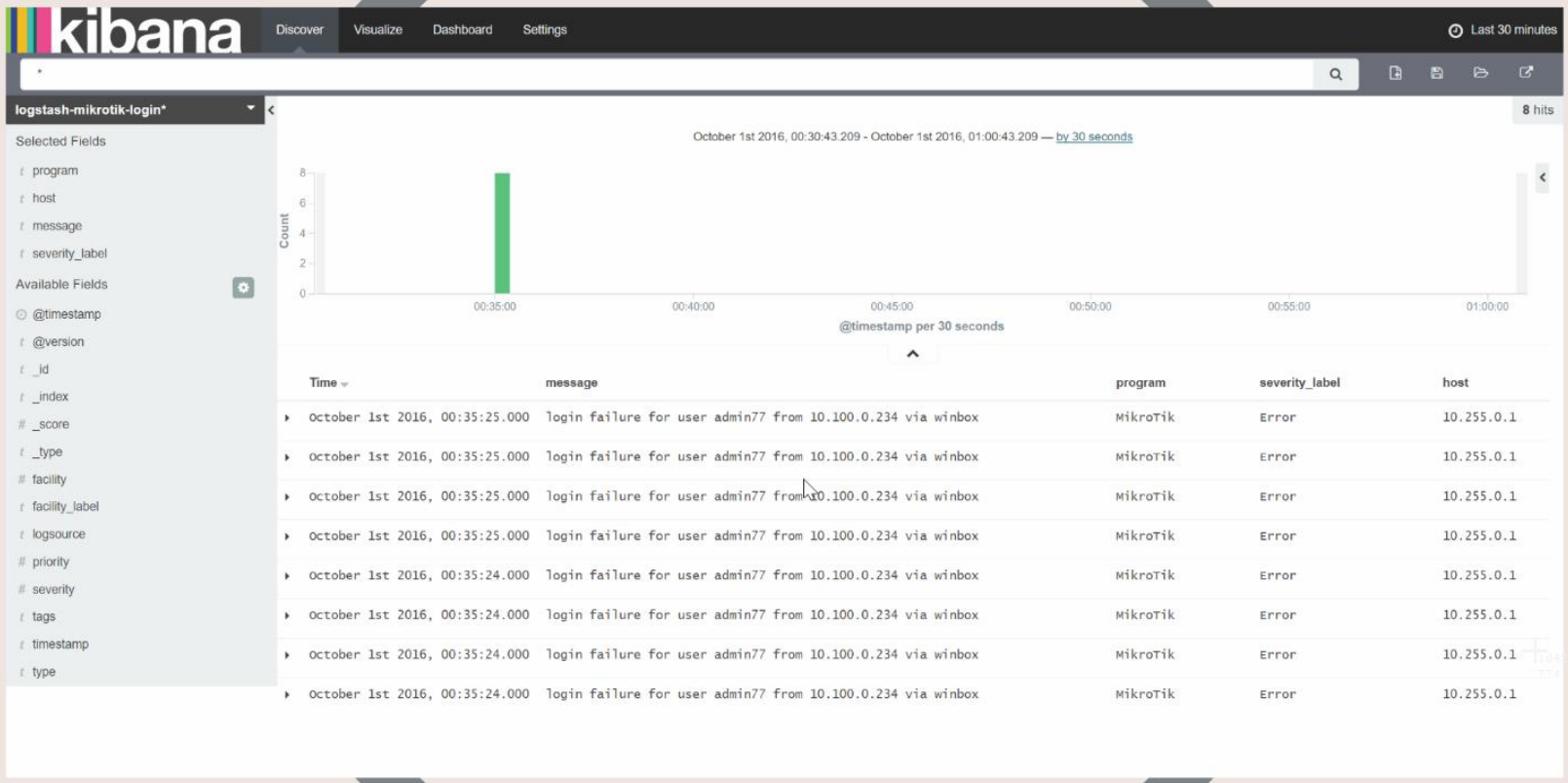
/etc/log

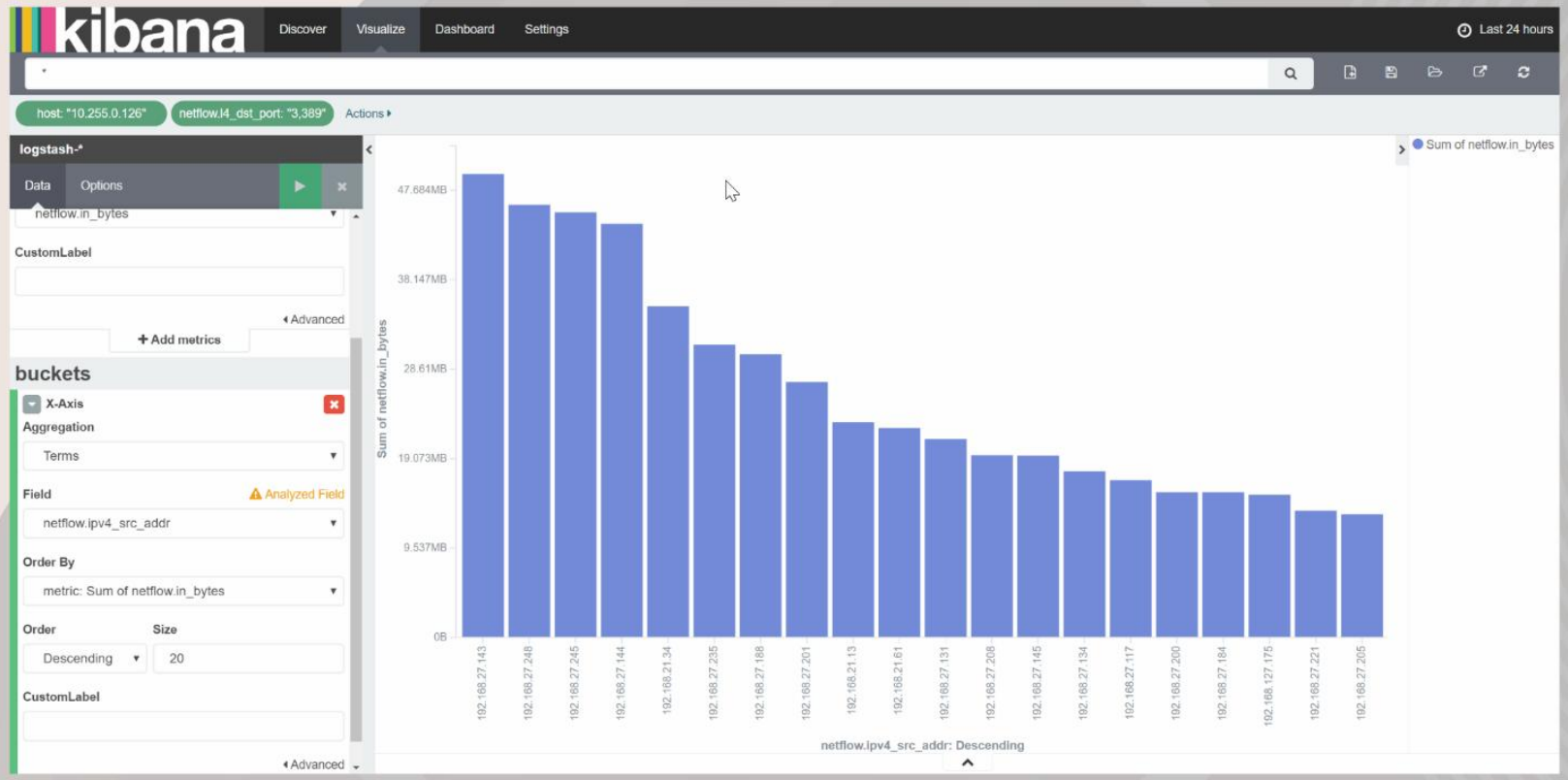
```
input {
  syslog {
    port => 5015
    type => "mikrotik-squid"
  }
}
```

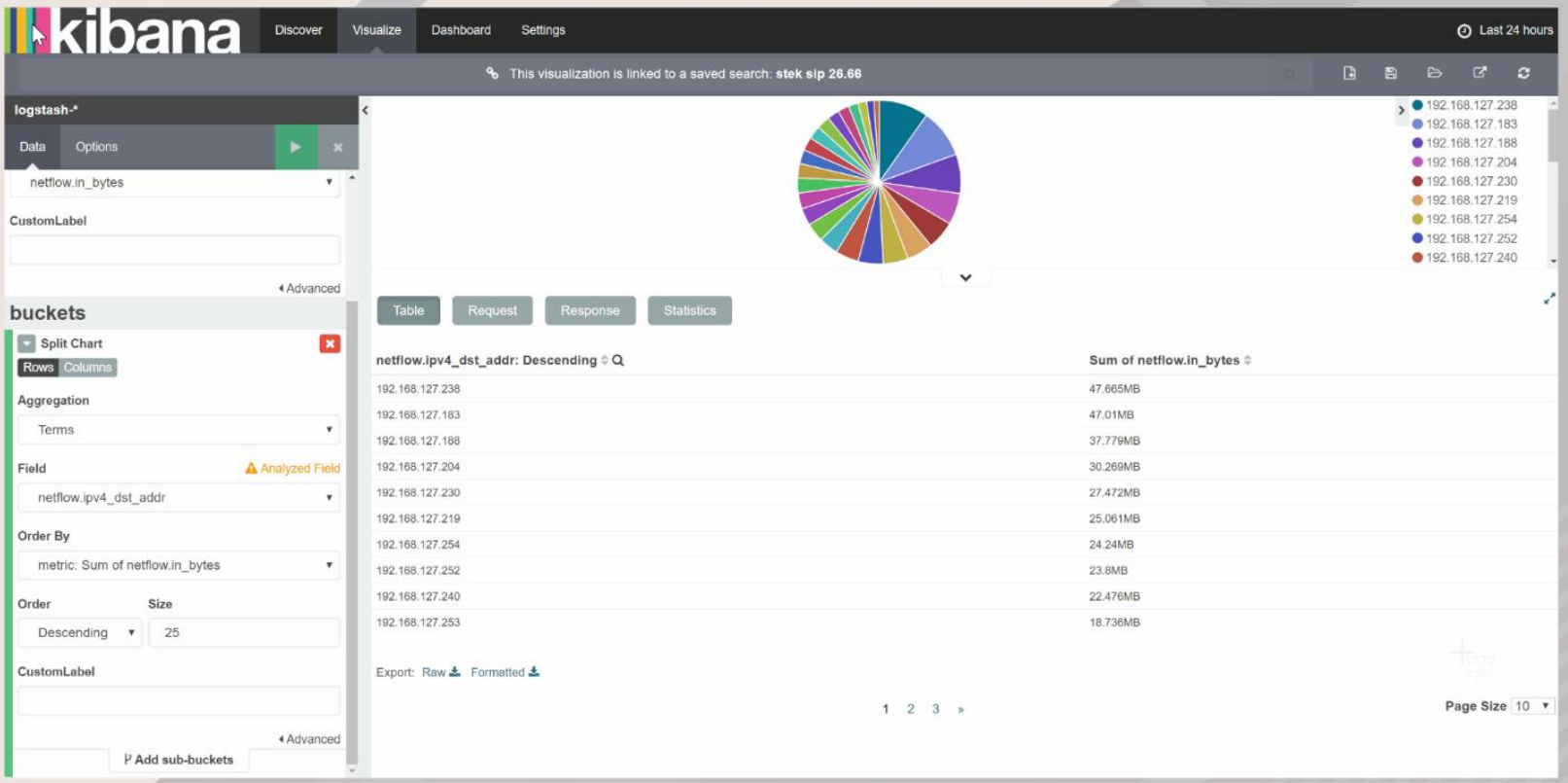


Time	netflow.ipv4_dst_addr	netflow.in_bytes	netflow.ipv4_next_hop	netflow.ipv4_src_addr	netflow.l4_dst_port	netflow.l4_src_port	netflow.protocol	netflow.tcp
September 30th 2016, 15:58:00.000	192.168.10.18	2.917GB	192.168.10.18	192.168.10.1	33,252	5,247	17	0
September 30th 2016, 15:58:00.000	192.168.10.18	2.917GB	192.168.10.18	192.168.10.1	33,252	5,247	17	0
September 30th 2016, 15:58:00.000	192.168.10.18	2.917GB	192.168.10.18	192.168.10.1	33,252	5,247	17	0
September 30th 2016, 23:02:37.000	213.24.83.182	1.272GB	95.165.192.145	192.168.1.221	43,448	33,133	6	2
September 30th 2016, 23:02:37.000	213.24.83.182	1.272GB	95.165.192.145	192.168.1.221	43,448	33,133	6	2
September 30th 2016, 23:02:37.000	213.24.83.182	1.272GB	95.165.192.145	192.168.1.221	43,448	33,133	6	2
September 30th 2016, 06:48:05.000	192.168.0.177	1.177GB	192.168.0.177	192.168.26.5	9,103	61,512	6	194
September 30th 2016, 06:48:05.000	192.168.0.177	1.177GB	192.168.0.177	192.168.26.5	9,103	61,512	6	194
September 30th 2016, 06:48:05.000	192.168.0.177	1.177GB	192.168.0.177	192.168.26.5	9,103	61,512	6	194
September 30th 2016, 13:29:05.000	188.225.21.208	778.591MB	87.245.157.129	192.168.3.12	80	65,018	6	2
September 30th 2016, 13:29:05.000	188.225.21.208	778.591MB	87.245.157.129	192.168.3.12	80	65,018	6	2
September 30th 2016, 13:29:05.000	188.225.21.208	778.591MB	87.245.157.129	192.168.3.12	80	65,018	6	2
September 30th 2016, 10:08:40.000	192.168.26.130	686.513MB	192.168.26.130	192.168.27.10	50,220	34,567	6	18
September 30th 2016, 10:08:40.000	192.168.26.130	686.513MB	192.168.26.130	192.168.27.10	50,220	34,567	6	18
September 30th 2016, 10:08:40.000	192.168.26.130	686.513MB	192.168.26.130	192.168.27.10	50,220	34,567	6	18
September 30th 2016, 05:49:37.000	192.168.26.130	683.288MB	192.168.26.130	192.168.27.10	63,236	34,567	6	16


kibana
Discover
Visualize
Dashboard
Settings
Last 7 days
host: "10.255.0.10"
Actions
logstash-mikrotik-squid*
Selected Fields
host
request_type
src_ip
Quick Count (500 /500 records)
192.168.1.103
192.168.1.178
192.168.1.24
192.168.18.222
192.168.1.4
Visualize (1 warning)
url
Available Fields
@timestamp
@version
_id
_index
_score
_type
facility
facility_label
message
priority
severity
severity_label
tags
web-proxy 371,516 hits
September 23rd 2016, 23:30:43.543 - September 30th 2016, 23:30:43.543 — by 3 hours
Count
@timestamp per 3 hours
Time
host
src_ip
url
request_type
September 30th 2016, 23:24:24.958 10.100.0.103 192.168.1.178 GET
September 30th 2016, 23:17:30.838 10.100.0.103 192.168.1.24 http://srv.ea.tensor.ru/sbismon/ POST
September 30th 2016, 23:17:30.828 10.100.0.103 192.168.1.24 http://srv.ea.tensor.ru/auth/ POST
September 30th 2016, 23:17:30.064 10.100.0.103 192.168.1.24 http://srv.ea.tensor.ru/sbismon/ POST


kibana
Discover
Visualize
Dashboard
Settings
Last 30 minutes
logstash-mikrotik-login*
Selected Fields
program
host
message
severity_label
Available Fields
@timestamp
@version
_id
_index
_score
_type
facility
facility_label
logsource
priority
severity
tags
timestamp
type
8 hits
October 1st 2016, 00:30:43.209 - October 1st 2016, 01:00:43.209 — by 30 seconds
Count
00:35:00
00:40:00
00:45:00
00:50:00
00:55:00
01:00:00
@timestamp per 30 seconds
Time
message
program
severity_label
host
October 1st 2016, 00:35:25.000 login failure for user admin77 from 10.100.0.234 via winbox MikroTik Error 10.255.0.1
October 1st 2016, 00:35:25.000 login failure for user admin77 from 10.100.0.234 via winbox MikroTik Error 10.255.0.1
October 1st 2016, 00:35:25.000 login failure for user admin77 from 10.100.0.234 via winbox MikroTik Error 10.255.0.1
October 1st 2016, 00:35:25.000 login failure for user admin77 from 10.100.0.234 via winbox MikroTik Error 10.255.0.1
October 1st 2016, 00:35:24.000 login failure for user admin77 from 10.100.0.234 via winbox MikroTik Error 10.255.0.1
October 1st 2016, 00:35:24.000 login failure for user admin77 from 10.100.0.234 via winbox MikroTik Error 10.255.0.1
October 1st 2016, 00:35:24.000 login failure for user admin77 from 10.100.0.234 via winbox MikroTik Error 10.255.0.1
October 1st 2016, 00:35:24.000 login failure for user admin77 from 10.100.0.234 via winbox MikroTik Error 10.255.0.1


kibana
Discover
Visualize
Dashboard
Settings
Last 24 hours
host: "10.255.0.126"
netflow.l4_dst_port: "3,389"
Actions
logstash-*
Data
Options
netflow.in_bytes
CustomLabel
Advanced
+ Add metrics
buckets
X-Axis
Aggregation
Terms
Field
Analyzed Field
netflow.ipv4_src_addr
Order By
metric: Sum of netflow.in_bytes
Order
Size
Descending
20
CustomLabel
Advanced
Sum of netflow.in_bytes
47.684MB
38.147MB
28.61MB
19.073MB
9.537MB
0B
Sum of netflow.in_bytes
192.168.27.143
192.168.27.248
192.168.27.245
192.168.27.144
192.168.21.34
192.168.27.235
192.168.27.188
192.168.27.201
192.168.21.13
192.168.21.61
192.168.27.131
192.168.27.208
192.168.27.145
192.168.27.134
192.168.27.117
192.168.27.200
192.168.27.184
192.168.127.175
192.168.27.221
192.168.27.205
netflow.ipv4_src_addr: Descending


kibana
Discover
Visualize
Dashboard
Settings
Last 24 hours
This visualization is linked to a saved search: stek sip 26.66
logstash-*
Data
Options
netflow.in_bytes
CustomLabel
Advanced
buckets
Split Chart
Rows
Columns
Aggregation
Terms
Field
Analyzed Field
netflow.ipv4_dst_addr
Order By
metric: Sum of netflow.in_bytes
Order
Size
Descending
25
CustomLabel
Advanced
Add sub-buckets
192.168.127.238
192.168.127.183
192.168.127.188
192.168.127.204
192.168.127.230
192.168.127.219
192.168.127.254
192.168.127.252
192.168.127.240
Table
Request
Response
Statistics
netflow.ipv4_dst_addr: Descending
Sum of netflow.in_bytes
192.168.127.238 47.665MB
192.168.127.183 47.01MB
192.168.127.188 37.779MB
192.168.127.204 30.269MB
192.168.127.230 27.472MB
192.168.127.219 25.061MB
192.168.127.254 24.24MB
192.168.127.252 23.8MB
192.168.127.240 22.476MB
192.168.127.253 18.736MB
Export: Raw Formatted
1 2 3 »
Page Size 10

Настройка MikroTik на отправку логов web-proxy

/system logging add topics=web-proxy,!debug action=remote prefix=web-proxy

Настройка приема логов web-proxy в logstash

/opt/logstash/patterns/mikrotik
MIKROTIKPROXY web-prox%{IP:src_ip}%{WORD:request_type} %{URI:url}

/etc/logstash/conf.d/03-mikrotik-squid.conf

```
input {
  syslog {
    port => 5015
    type => "mikrotik-squid"
  }
}
```

```
filter {
  if [type] == "mikrotik-squid" {
    grok {
      patterns_dir => ["/opt/logstash/patterns/"]
      match => [ "message", "%{MIKROTIKPROXY}" ]
      add_tag => ["mikrotik-squid"]
    }
  }
}
```

```
output {
   elasticsearch {
      hosts => ["localhost:9200"]
      codec => "json"
      index => "logstash-%{type}-%{+YYYY.MM.dd}"
   }
}
```

Настройка MikroTik на отправку trafic-flow

```
/ip traffic-flow set enabled=yes
/ip traffic-flow target add dst-address=1.1.1.1 port=1111 version=9
```

Настройка logstash на прием trafic-flow

```
input {
  udp {
    port  => 9996
    codec => netflow {
      versions => [9]
      netflow_definitions => "/etc/logstash/mikrotik.netflow9.yaml"
    }
    type  => "netflow9"
  }
}
output {
  elasticsearch {
    hosts => ["localhost:9200"]
    codec => "json"
    index => "logstash-%{type}-%{+YYYY.MM.dd}"
  }
}
```

Спасибо за внимание
Вопросы и пожелания
soriels87@gmail.com