Visualizing Data Using Elastic stack

Kibana

Elasticsearch

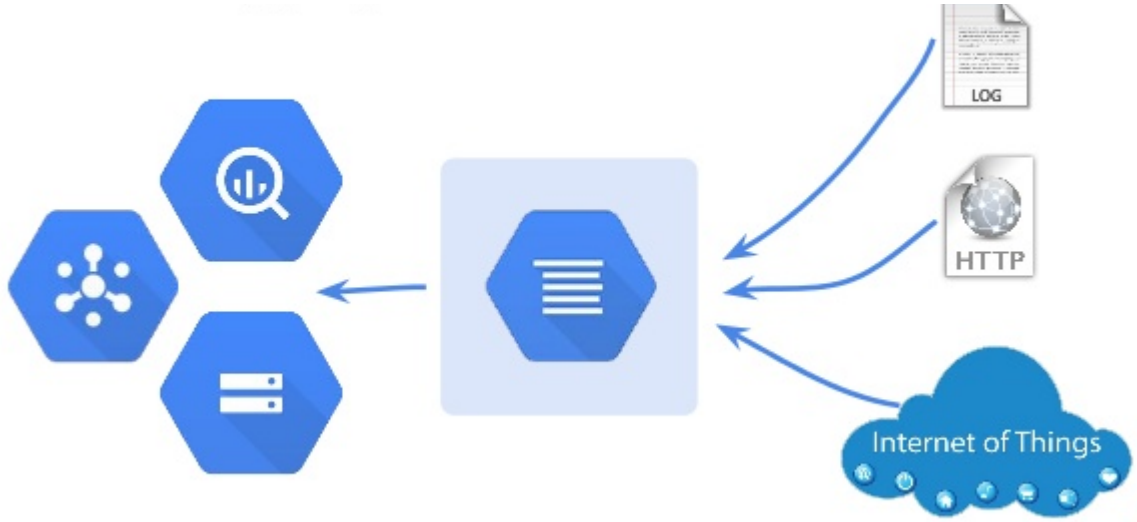
Logstash

Maghsoud Morshedi

Industrial PhD, Eye Networks and University of Oslo

Why Logging?

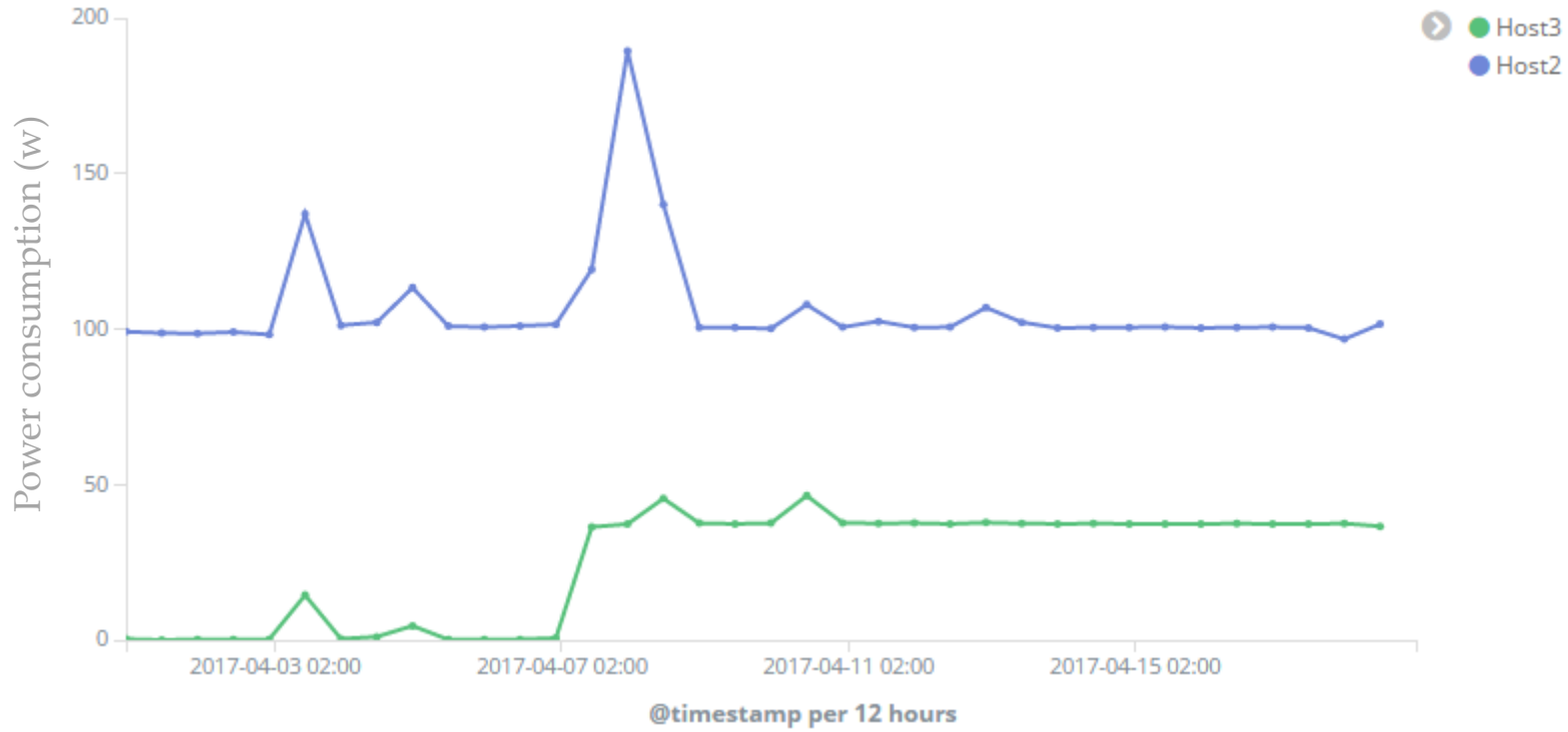
1. Monitor process
2. Extract information
3. Make proper decision



Can you make decision?

04/18/2017	22:15:05	0	0	0	0	0	0	0	0	0	0	0	0	0	190	194	0	241	288	208	42	112	238	294	0
04/18/2017	22:15:07	0	0	0	0	0	0	0	0	0	0	0	0	0	185	194	0	243	289	209	42	127	239	293	0
04/18/2017	22:15:09	0	0	0	0	0	0	0	0	0	0	0	0	0	183	193	0	241	289	208	42	160	238	292	0
04/18/2017	22:15:11	0	0	0	0	0	0	0	0	0	0	0	0	0	181	194	0	259	287	209	40	121	239	294	0
04/18/2017	22:15:13	0	0	0	0	0	0	0	0	0	0	0	0	0	180	194	0	240	287	210	41	102	238	294	0
04/18/2017	22:15:15	0	0	0	0	0	0	0	0	0	0	0	0	0	184	194	0	243	285	208	41	102	240	294	0
04/18/2017	22:15:17	0	0	0	0	0	0	0	0	0	0	0	0	0	181	194	0	239	286	208	41	101	239	294	0
04/18/2017	22:15:20	0	0	0	0	0	0	0	0	0	0	0	0	0	191	192	0	243	288	209	0	100	239	293	0
04/18/2017	22:15:22	0	0	0	0	0	0	0	0	0	0	0	0	0	184	195	0	249	287	208	0	103	239	294	0
04/18/2017	22:15:24	0	0	0	0	0	0	0	0	0	0	0	0	0	183	195	0	241	287	210	40	101	238	295	0
04/18/2017	22:15:27	0	0	0	0	0	0	0	0	0	0	0	0	0	181	194	0	244	289	207	40	102	239	293	0
04/18/2017	22:15:29	0	0	0	0	0	0	0	0	0	0	0	0	0	181	193	0	242	287	209	0	103	238	294	0
04/18/2017	22:15:32	0	0	0	0	0	0	0	0	0	0	0	0	0	182	195	0	243	287	212	41	102	238	294	0
04/18/2017	22:15:34	0	0	0	0	0	0	0	0	0	0	0	0	0	184	193	0	240	286	209	0	101	238	293	0
04/18/2017	22:15:36	0	0	0	0	0	0	0	0	0	0	0	0	0	184	194	0	243	288	210	0	102	238	293	0
04/18/2017	22:15:39	0	0	0	0	0	0	0	0	0	0	0	0	0	182	195	0	244	286	208	41	97	238	294	0
04/18/2017	22:15:41	0	0	0	0	0	0	0	0	0	0	0	0	0	182	193	0	242	287	208	40	98	238	294	0
04/18/2017	22:15:43	0	0	0	0	0	0	0	0	0	0	0	0	0	183	194	0	246	288	209	41	101	238	294	0
04/18/2017	22:15:45	0	0	0	0	0	0	0	0	0	0	0	0	0	181	193	0	242	287	208	41	100	238	294	0
04/18/2017	22:15:47	0	0	0	0	0	0	0	0	0	0	0	0	0	183	193	0	245	285	208	41	111	239	292	0
04/18/2017	22:15:50	0	0	0	0	0	0	0	0	0	0	0	0	0	180	192	0	241	287	209	41	100	240	292	0
04/18/2017	22:15:52	0	0	0	0	0	0	0	0	0	0	0	0	0	186	196	0	244	286	207	40	101	238	294	0
04/18/2017	22:15:54	0	0	0	0	0	0	0	0	0	0	0	0	0	191	194	0	239	288	211	40	101	239	294	0
04/18/2017	22:15:57	0	0	0	0	0	0	0	0	0	0	0	0	0	187	193	0	243	287	209	40	101	238	294	0
04/18/2017	22:15:59	0	0	0	0	0	0	0	0	0	0	0	0	0	188	194	0	244	289	211	40	100	237	294	0
04/18/2017	22:16:01	0	0	0	0	0	0	0	0	0	0	0	0	0	190	193	0	248	287	210	40	99	239	293	0
04/18/2017	22:16:03	0	0	0	0	0	0	0	0	0	0	0	0	0	184	194	0	245	286	207	40	102	239	293	0
04/18/2017	22:16:05	0	0	0	0	0	0	0	0	0	0	0	0	0	186	194	0	242	287	210	40	101	239	294	0
04/18/2017	22:16:07	0	0	0	0	0	0	0	0	0	0	0	0	0	185	195	0	245	287	208	41	102	238	294	0
04/18/2017	22:16:10	0	0	0	0	0	0	0	0	0	0	0	0	0	181	193	0	240	287	208	41	103	238	293	0
04/18/2017	22:16:12	0	0	0	0	0	0	0	0	0	0	0	0	0	183	195	0	246	287	210	40	100	239	295	0
04/18/2017	22:16:14	0	0	0	0	0	0	0	0	0	0	0	0	0	182	194	0	239	287	208	40	101	238	294	0
04/18/2017	22:16:16	0	0	0	0	0	0	0	0	0	0	0	0	0	183	193	0	243	287	210	40	126	238	293	0
04/18/2017	22:16:18	0	0	0	0	0	0	0	0	0	0	0	0	0	181	194	0	239	287	210	40	117	239	293	0
04/18/2017	22:16:21	0	0	0	0	0	0	0	0	0	0	0	0	0	181	194	0	245	287	206	40	97	238	294	0
04/18/2017	22:16:23	0	0	0	0	0	0	0	0	0	0	0	0	0	181	193	0	237	288	210	40	99	239	293	0
04/18/2017	22:16:25	0	0	0	0	0	0	0	0	0	0	0	0	0	181	194	0	242	288	208	40	100	238	294	0
04/18/2017	22:16:28	0	0	0	0	0	0	0	0	0	0	0	0	0	181	194	0	241	289	209	0	98	238	293	0
04/18/2017	22:16:30	0	0	0	0	0	0	0	0	0	0	0	0	0	181	193	0	242	287	207	41	100	238	294	0
04/18/2017	22:16:32	0	0	0	0	0	0	0	0	0	0	0	0	0	182	193	0	244	287	208	41	101	238	293	0
04/18/2017	22:16:34	0	0	0	0	0	0	0	0	0	0	0	0	0	184	194	0	242	287	213	41	102	237	294	0

Can you make decision?

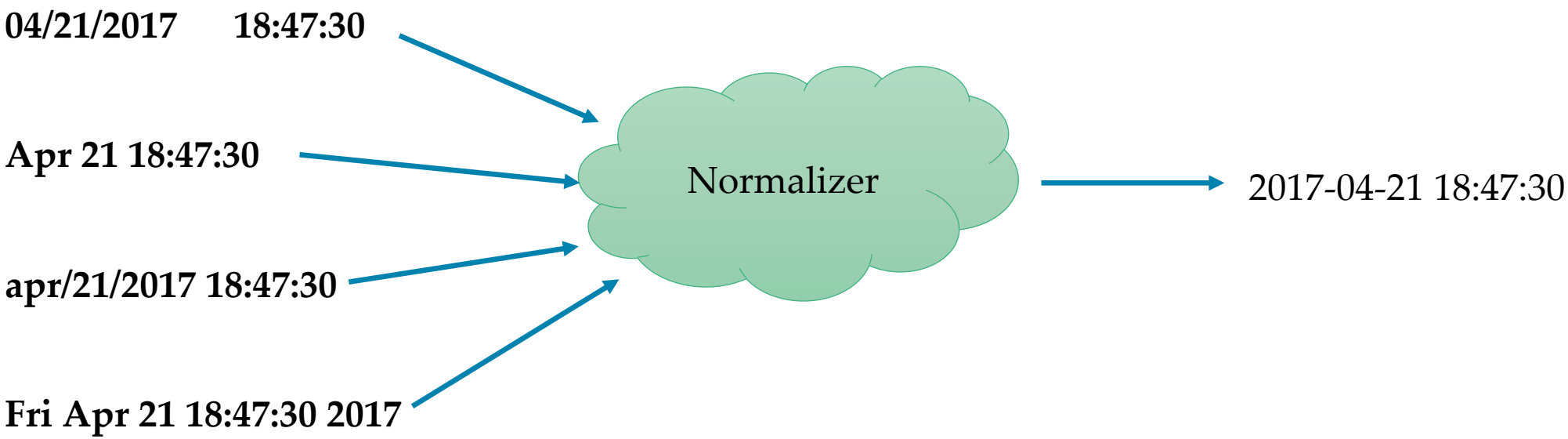


Different devices different data

04/18/2017 22:16:34 0 0 0 0 0 0 0 0 0 0 0 0 0 184 194 0
242 287 213 41 102 237 294 0

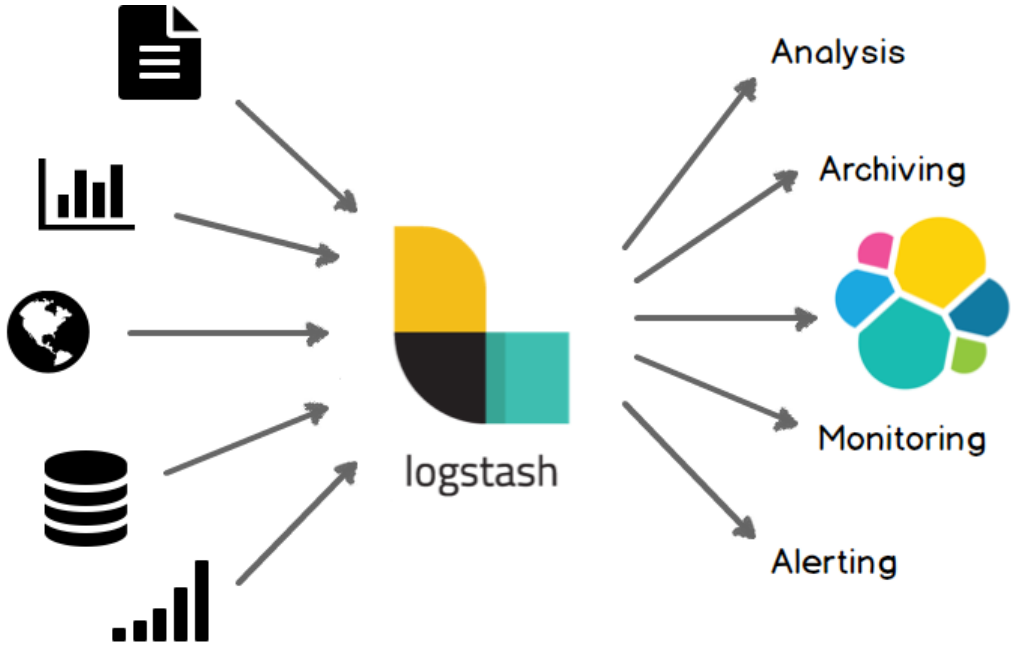
interface=wlan1 mac-address=FF:FF:FF:FF:FF:FF ap=no wds=no bridge=no
rx-rate="65Mbps-20MHz/1S" tx-rate="65Mbps-20MHz/1S" packets=1243,1218
bytes=100314,100806 frames=1243,1218 frame-bytes=93090,93498
hw-frames=1298,1540 hw-frame-bytes=128352,130756 tx-frames-timed-out=0
uptime=15m54s last-activity=11s320ms signal-strength=-41dBm@1Mbps
signal-to-noise=59dB signal-strength-ch0=-43dBm signal-strength-ch1=-46dBm
strength-at-rates=-41dBm@1Mbps 15m47s170ms,-54dBm@HT20-0 15m27s690ms,-40dBm@HT20-
1 15m44s390ms,-56dBm@HT20-2 14m36s170ms,-57dBm@HT20-3 15m17s540ms,
-54dBm@HT20-4 10m38s230ms,-53dBm@HT20-5 13m55s450ms,-53dBm@HT20-6
12m52s610ms,-55dBm@HT20-7 11s320ms
tx-ccq=99% p-throughput=61077 distance=4 last-ip=192.168.1.45
802.1x-port-enabled=yes management-protection=no wmm-enabled=yes
tx-rate-set="CCK:1-11 OFDM:6-54 BW:1x HT:0-7"

Timestamps


04/21/2017 18:47:30
Apr 21 18:47:30
apr/21/2017 18:47:30
Fri Apr 21 18:47:30 2017
Normalizer
2017-04-21 18:47:30

Shipping data to a centralized location

- **Write data to a file**
- **Shipping data over network**
- **Encrypt data**



Data lifecycle

1. **Creation**
2. **Ship**
3. **Centralization**
4. **Enrich**
5. **Store**
6. **Analyze**
7. **Visualize**
8. **Archive**

Elastic architecture

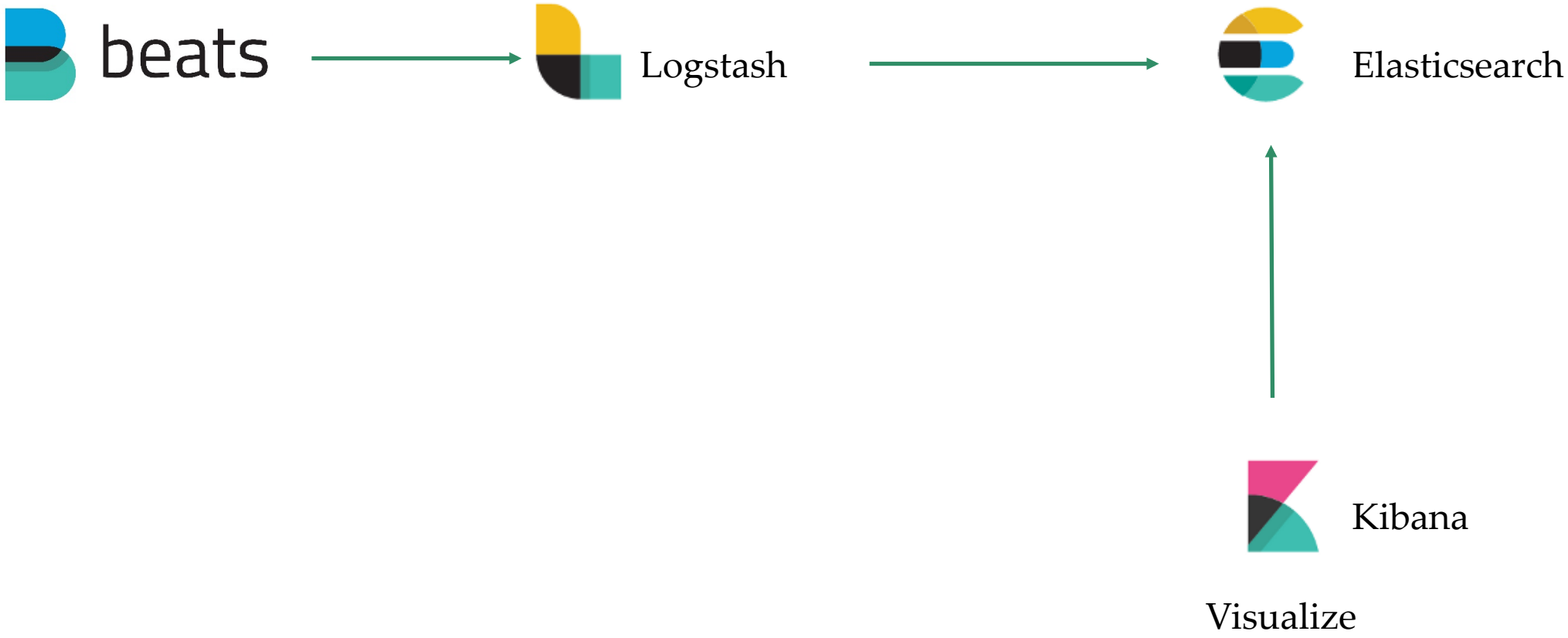
Log creation

Elastic architecture

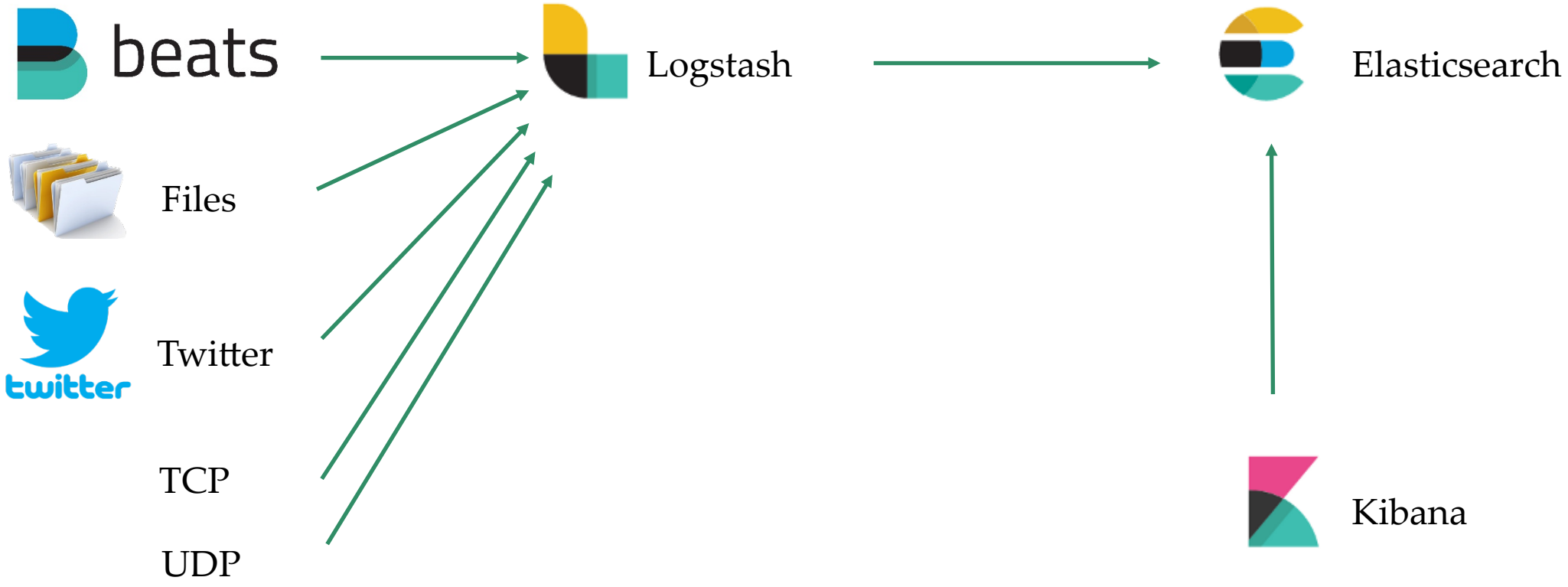
Log Centralization
and
enrichment

Elastic architecture

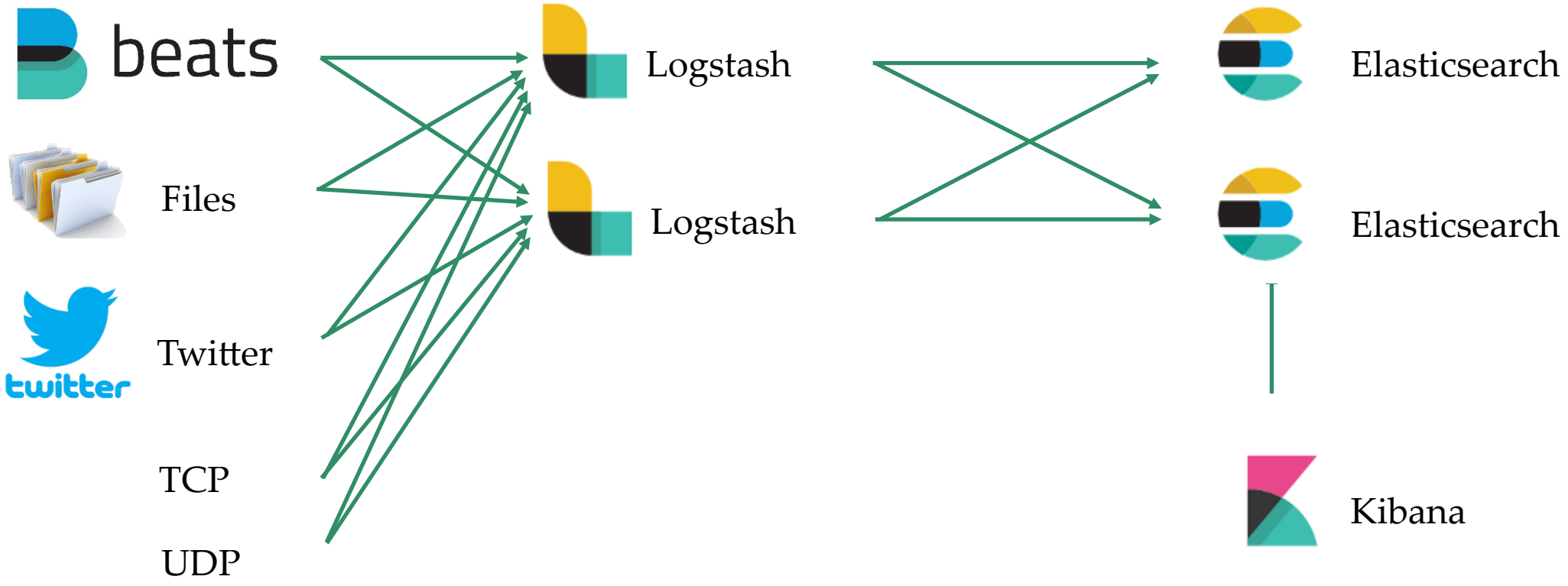
Elastic architecture



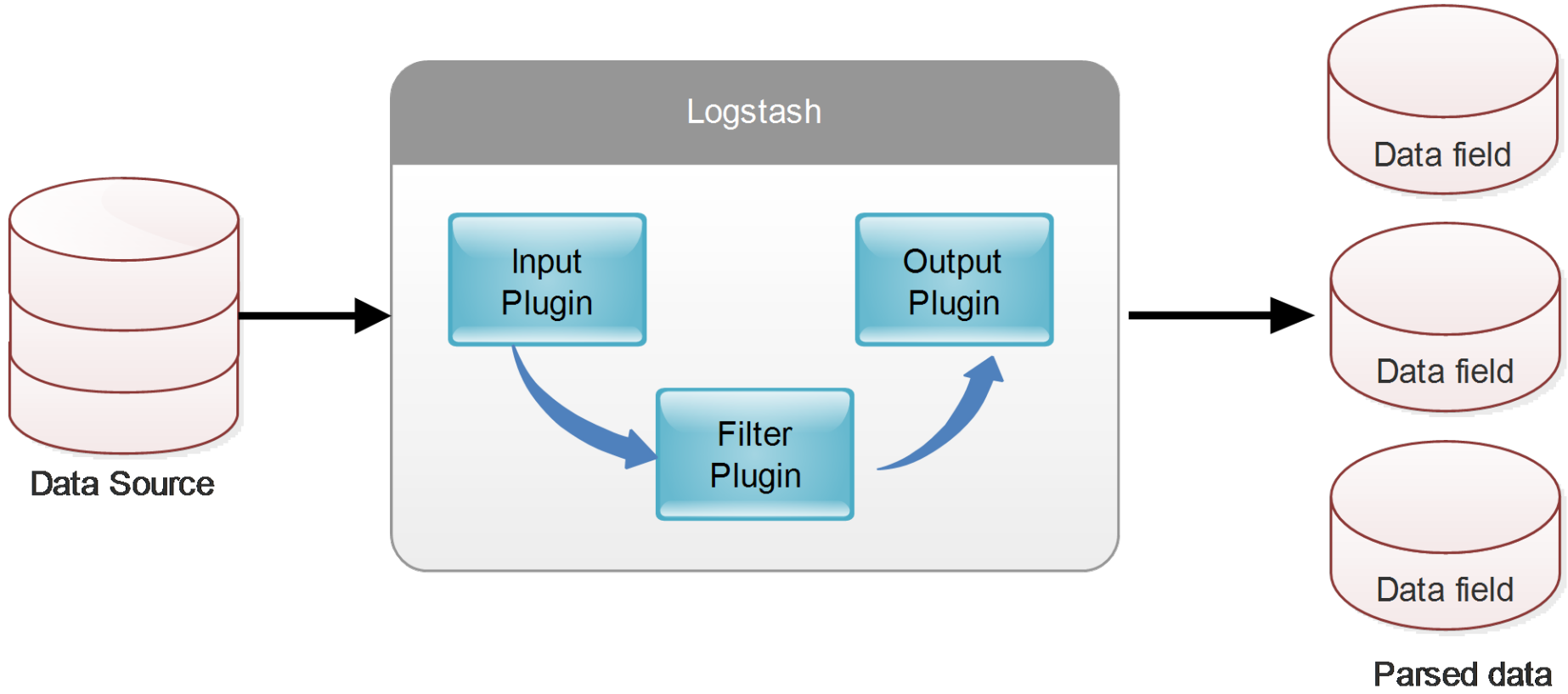
Elastic architecture



Elastic architecture



Logstash


Logstash
Input Plugin
Output Plugin
Filter Plugin
Data Source
Data field
Data field
Data field
Parsed data

Logstash Input Plugins

- An input plugin provides ability to read a specific source of events
- Logstash appends config files in an alphabetically order
- Input config file can have multiple input plugin (file, syslog, etc)

Logstash Input Plugins

- Beats
- File
- Github webhook
- http or https
- IMAP
- Twitter
- SNMP trap
- TCP
- UDP
- and more input plugins

```
Input {
  file {
        path => "csv file path"
        sincedb_path => "Path of the sincedb database file "
        start_position => "end or beginning"
        type => "type_name"
  }
}
```

Logstash Filter Plugins

- A filter plugin provides ability to parse a specific source of such as csv, grok, geoip, xml, etc.

- Filters are usually applied conditionally based on input type.

Logstash Filter Plugins

- Anonymize
- CSV
- Date
- emoji
- Geoip
- Grok
- Mutate
- XML
- and more filters

```
if [type]  ==  “type_name” {
  csv {
            separator = “        “
            columns => [ “date”, “time”, “field1”, “field2” ]
            convert => { “field1” => “float”
                         “field2” => “float”
                       }
      }
  mutate {
            add_field => { “timestamp” => “%{date} %{time}”}
            }
 date {
            match => [ “timestamp” , “MM/dd/yyyy  HH:mm:ss”]
            remove_field => [“timestamp”]
            target => “@timestamp”
            timezone => “Europe/Amsterdam”
            }
}
```

Logstash Output Plugins

- A output plugin provides ability to send event data a specific destination such as elasticseach, csv, tcp, etc.

- Outputs are usually applied conditionally based on input type.

Logstash Output Plugins

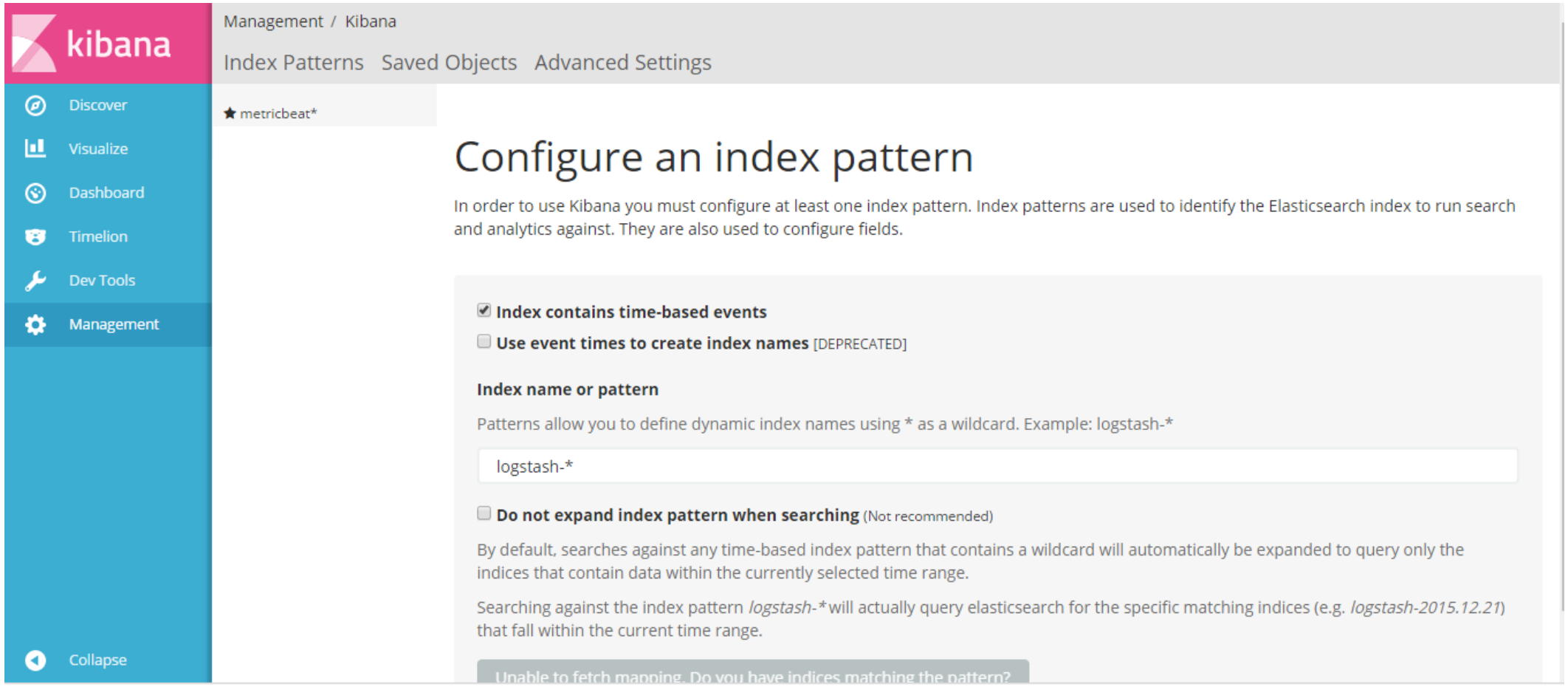
- CSV file
- Elasticsearch
- Email
- File
- Google cloud storage
- http or https
- Jira
- TCP
- UDP
- and more output plugins

```
output {
  if [type] == “type_name” {
        elasticsearch {
              hosts => [ “localhost:9200” ]
              index => “your_index”
        }
  }
}
```

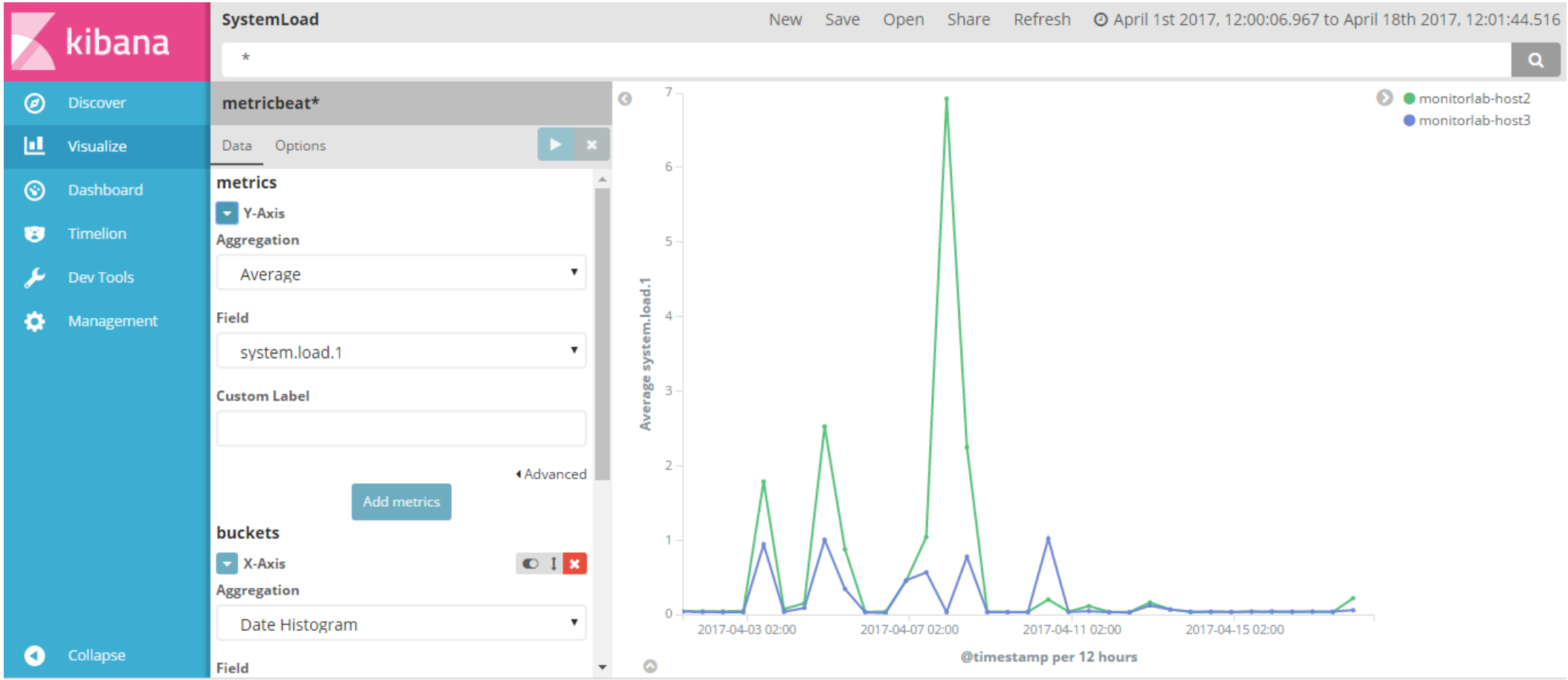
Visualize data with Kibana

- Login to Kibana
- Add your index through Management window
- Build a graph though Visualize window
- Add the graph to your dashboard

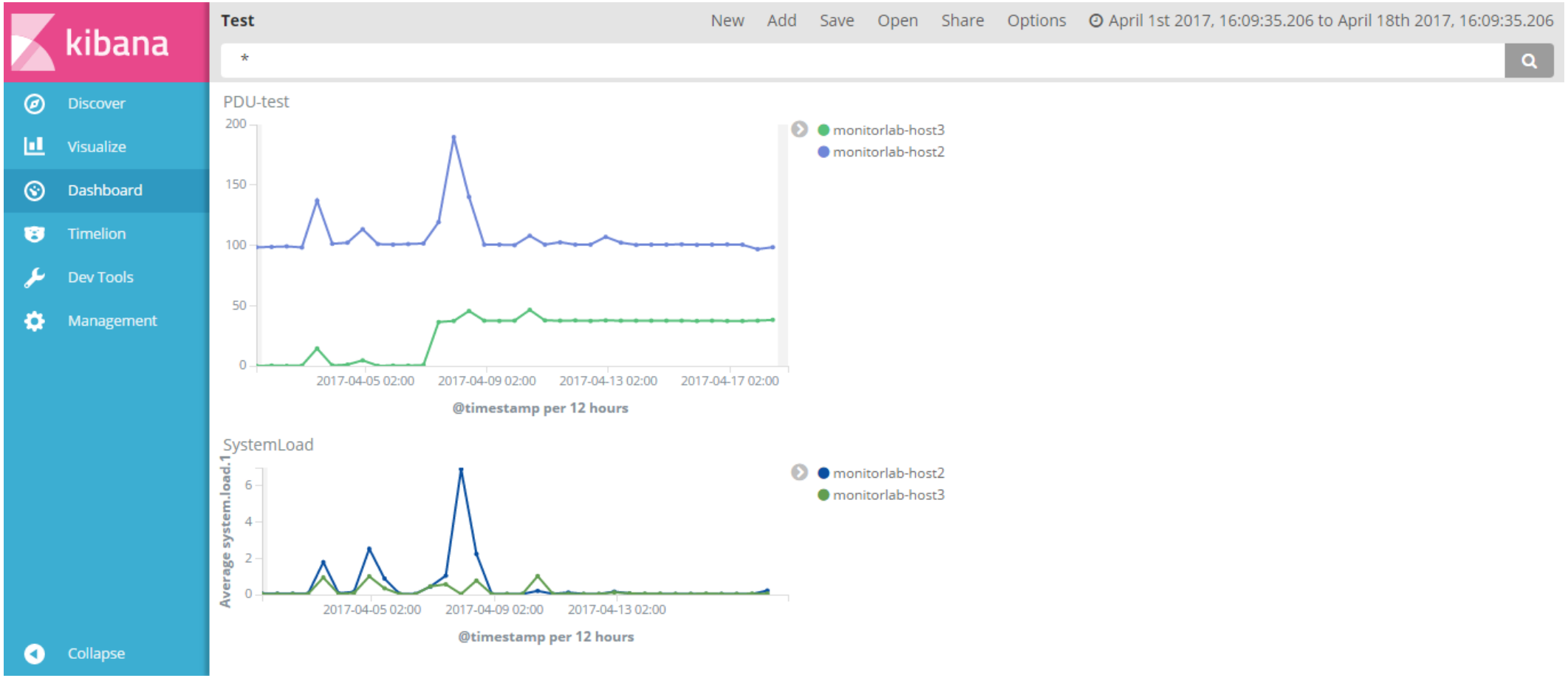
Configure index in Kibana



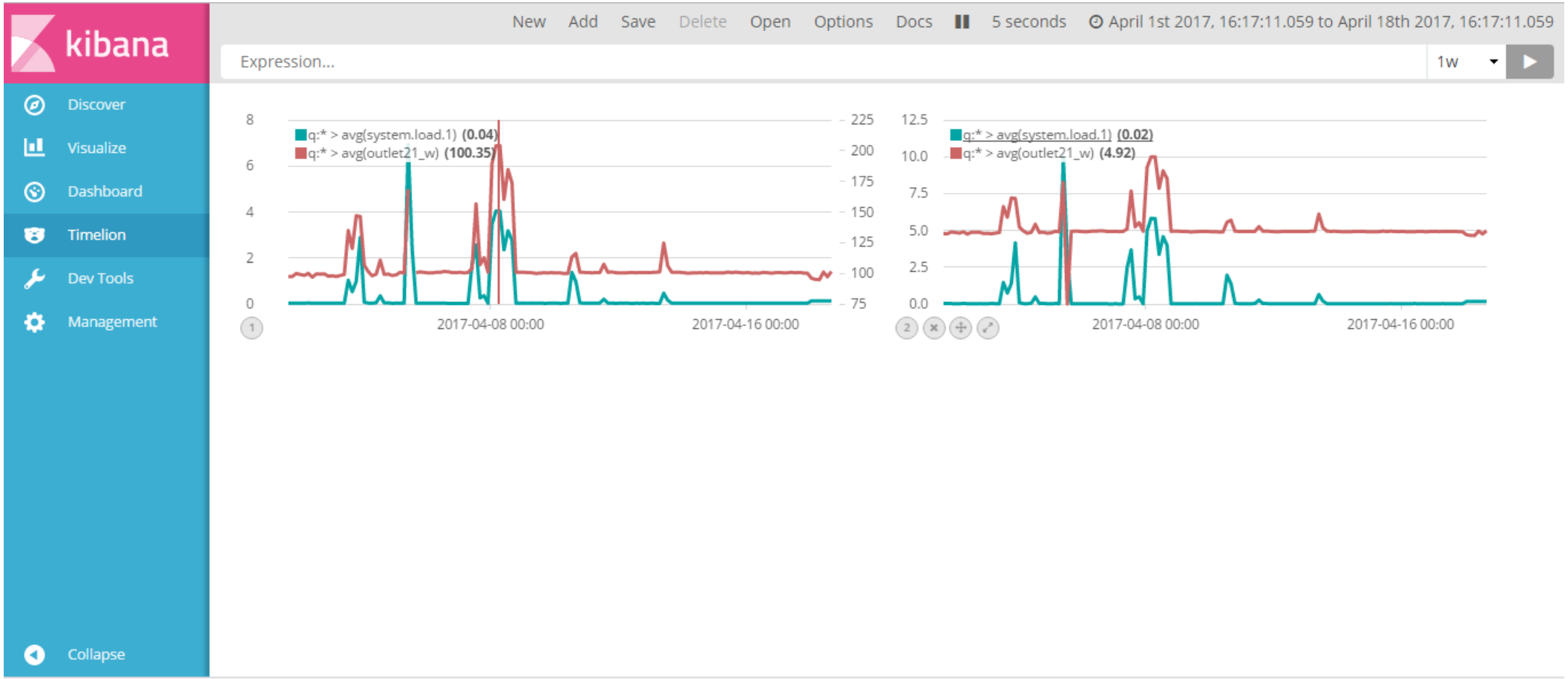
Visualize data with Kibana



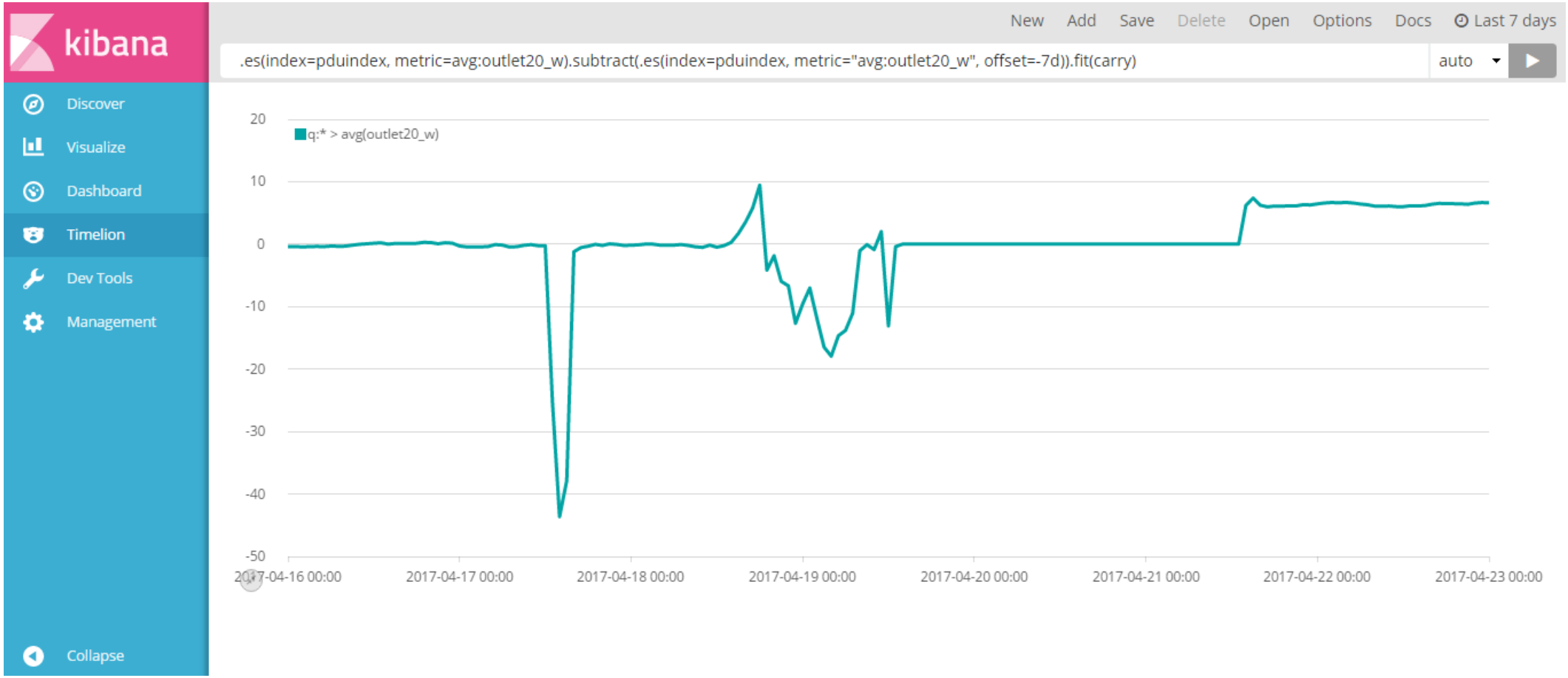
Kibana Dashboard



Kibana Timelion



Kibana Timelion



Summary

- Easy to use
- Minimum dependency (only Java)
- Open source
- Flexible

Visualizing Data Using Elastic stack

Kibana

Elasticsearch

Logstash

Maghsoud Morshedi

Industrial PhD, Eye Networks and University of Oslo