ELK Stack megoldások

ElasticSearch, Logstash, Kibana

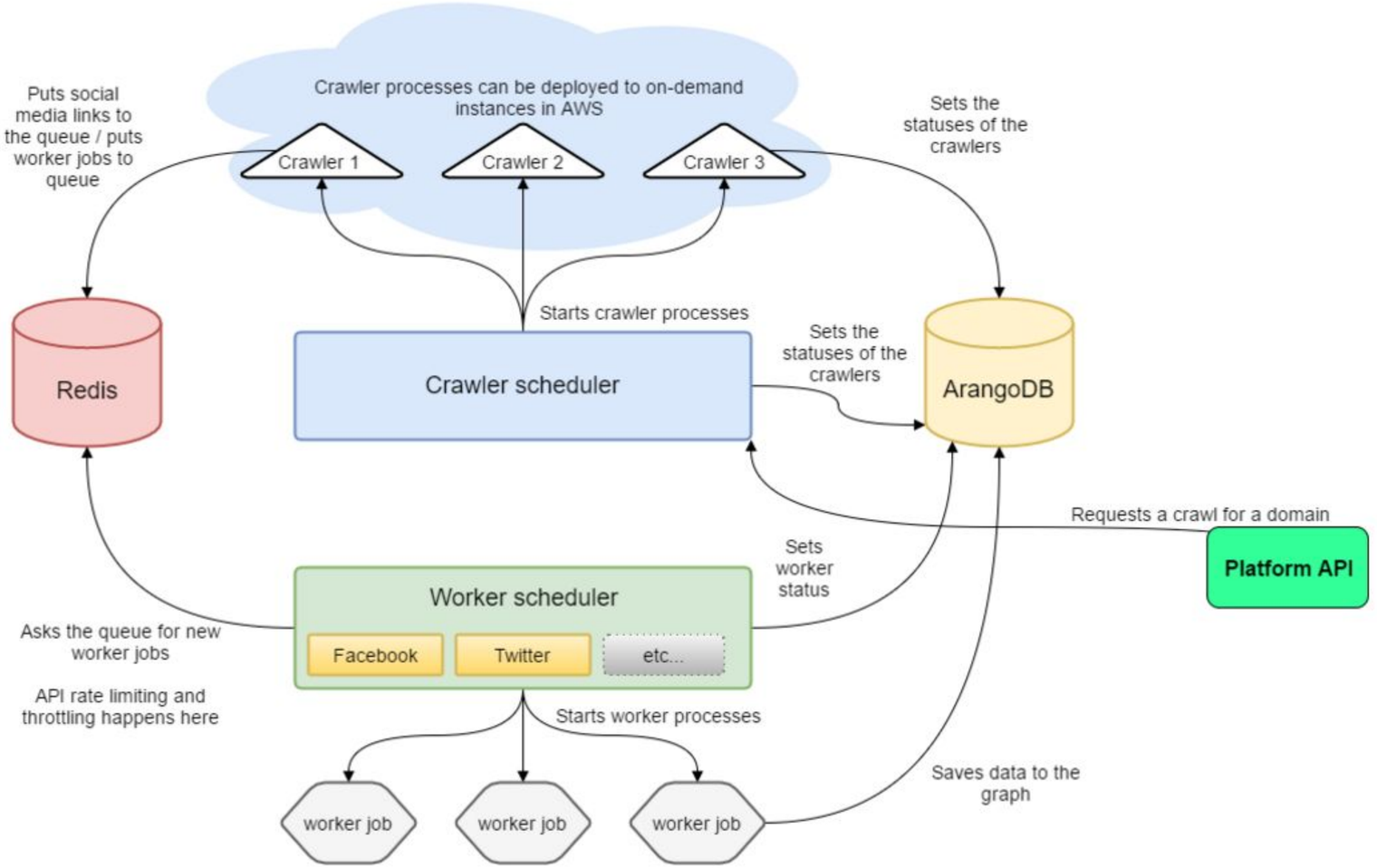
Bencs Balázs
Senior Software Developer

balazs.bencs@attrecto.com

Miért?

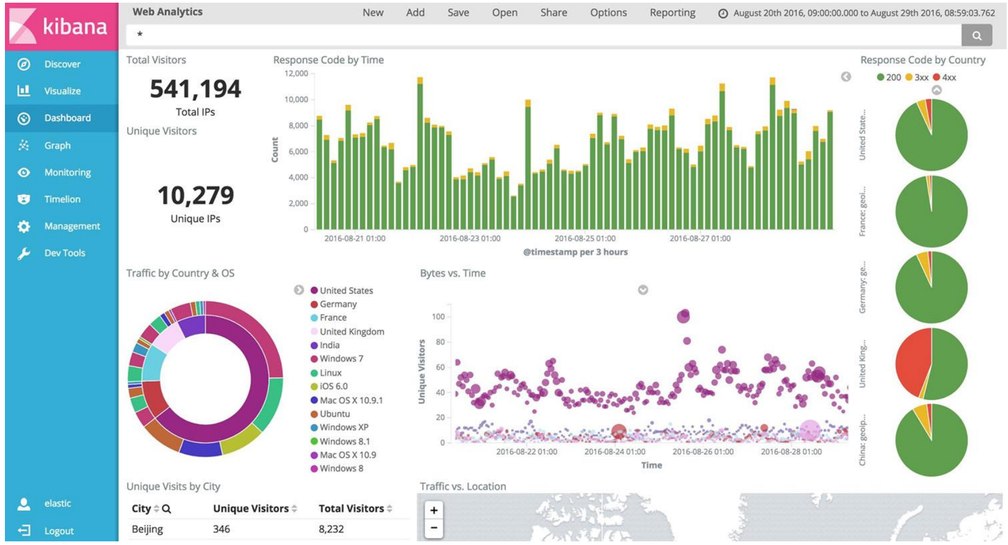
“Ki kellene keresni a tegnapi előtti logokból a hibákat 10 óra és 1 között”

“Hol vannak az XY szerver logjai??”


Crawler processes can be deployed to on-demand instances in AWS
Crawler 1
Crawler 2
Crawler 3
Puts social media links to the queue / puts worker jobs to queue
Sets the statuses of the crawlers
Starts crawler processes
Redis
Crawler scheduler
Sets the statuses of the crawlers
ArangoDB
Requests a crawl for a domain
Platform API
Sets worker status
Worker scheduler
Facebook
Twitter
etc...
Asks the queue for new worker jobs
API rate limiting and throttling happens here
Starts worker processes
worker job
worker job
worker job
Saves data to the graph


```
192.168.1.16 - - [10/Jan/2017:18:06:59 +0000]
"POST
/kibana/elasticsearch/_msearch?timeout=30000&
ignore_unavailable=true&preference=1447070343
481 HTTP/1.1" 200 8352
"https://elastic/kibana/index.html"
"Mozilla/5.0 (X11; Linux armv7l)
AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu
Chromium/45.0.2454.101 Chrome/45.0.2454.101
Safari/537.36" 0.465 0.454
```

VS



Architektúra

attrecto
smartphone solutions

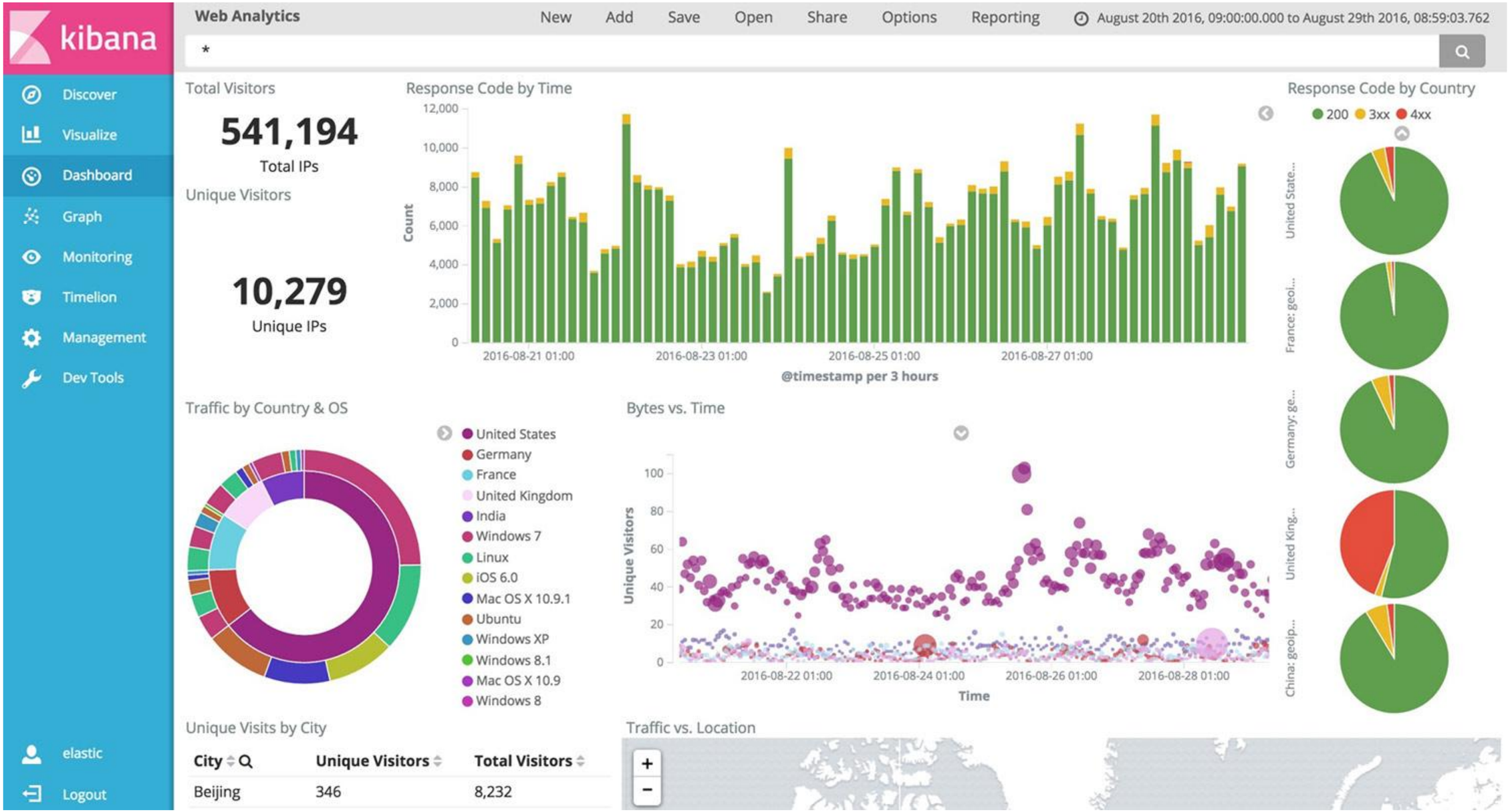
ElasticSearch

- Java alapú
- Fulltext search engine és document storage
- Keresés és indexelés
- Elosztott - Sharding és replication támogatott
- Clustering
- Egyszerű REST API
- Open Source

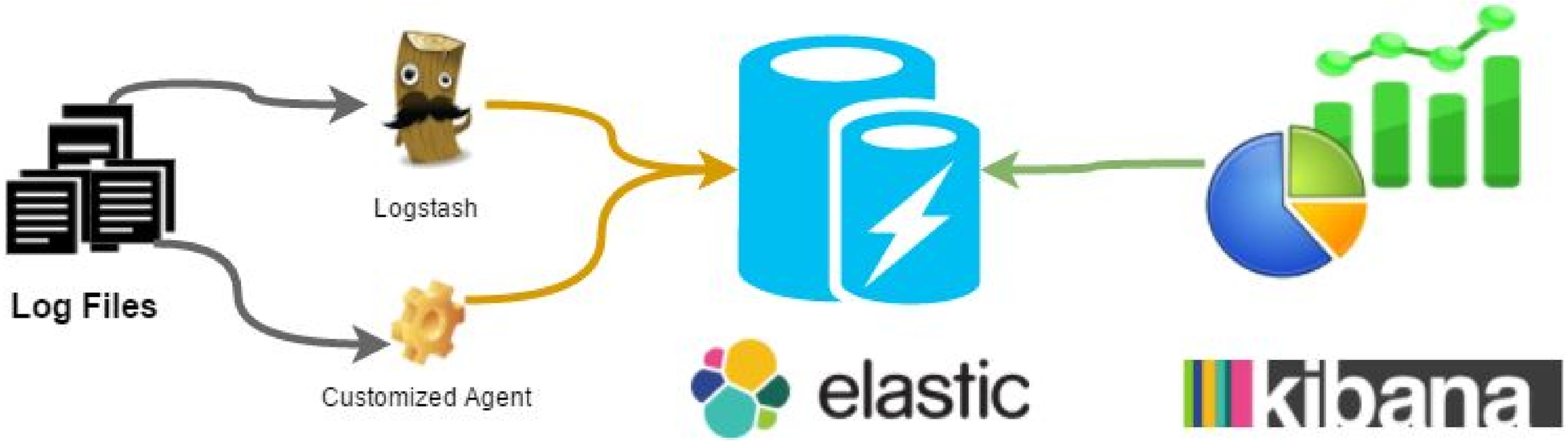
Logstash

- Többféle input, többféle output
- Központosítja a logokat
- Begyűjti az adatokat
  - Lehetnek sima logfájlok, syslog, redis, vagy filebeat, stb.. (az utóbbiról később)
- Feldolgozza
  - Rengeteg kész pattern különböző log fájlokhoz
  - Sok plugin gyárilag, de tovább bővíthető
  - Grok pattern engine
  - GeoIP
- Továbbítja és tárolja

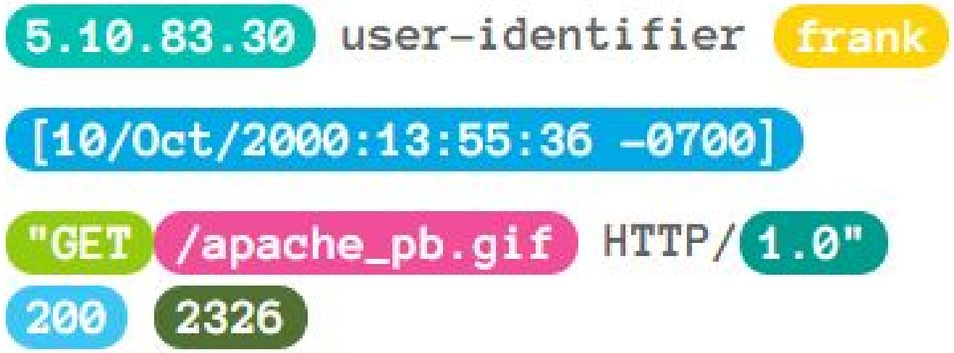
Kibana


kibana
Web Analytics
New
Add
Save
Open
Share
Options
Reporting
August 20th 2016, 09:00:00.000 to August 29th 2016, 08:59:03.762
*
Discover
Visualize
Dashboard
Graph
Monitoring
Timelion
Management
Dev Tools
elastic
Logout
Total Visitors
541,194
Total IPs
Unique Visitors
10,279
Unique IPs
Response Code by Time
12,000
10,000
8,000
6,000
4,000
2,000
0
Count
2016-08-21 01:00
2016-08-23 01:00
2016-08-25 01:00
2016-08-27 01:00
@timestamp per 3 hours
Response Code by Country
200
3xx
4xx
United State...
France: geol...
Germany: ge...
United King...
China: geoip...
Traffic by Country & OS
United States
Germany
France
United Kingdom
India
Windows 7
Linux
iOS 6.0
Mac OS X 10.9.1
Ubuntu
Windows XP
Windows 8.1
Mac OS X 10.9
Windows 8
Bytes vs. Time
100
80
60
40
20
0
Unique Visitors
2016-08-22 01:00
2016-08-24 01:00
2016-08-26 01:00
2016-08-28 01:00
Time
Unique Visits by City
City
Unique Visitors
Total Visitors
Beijing
346
8,232
Traffic vs. Location

Architektúra



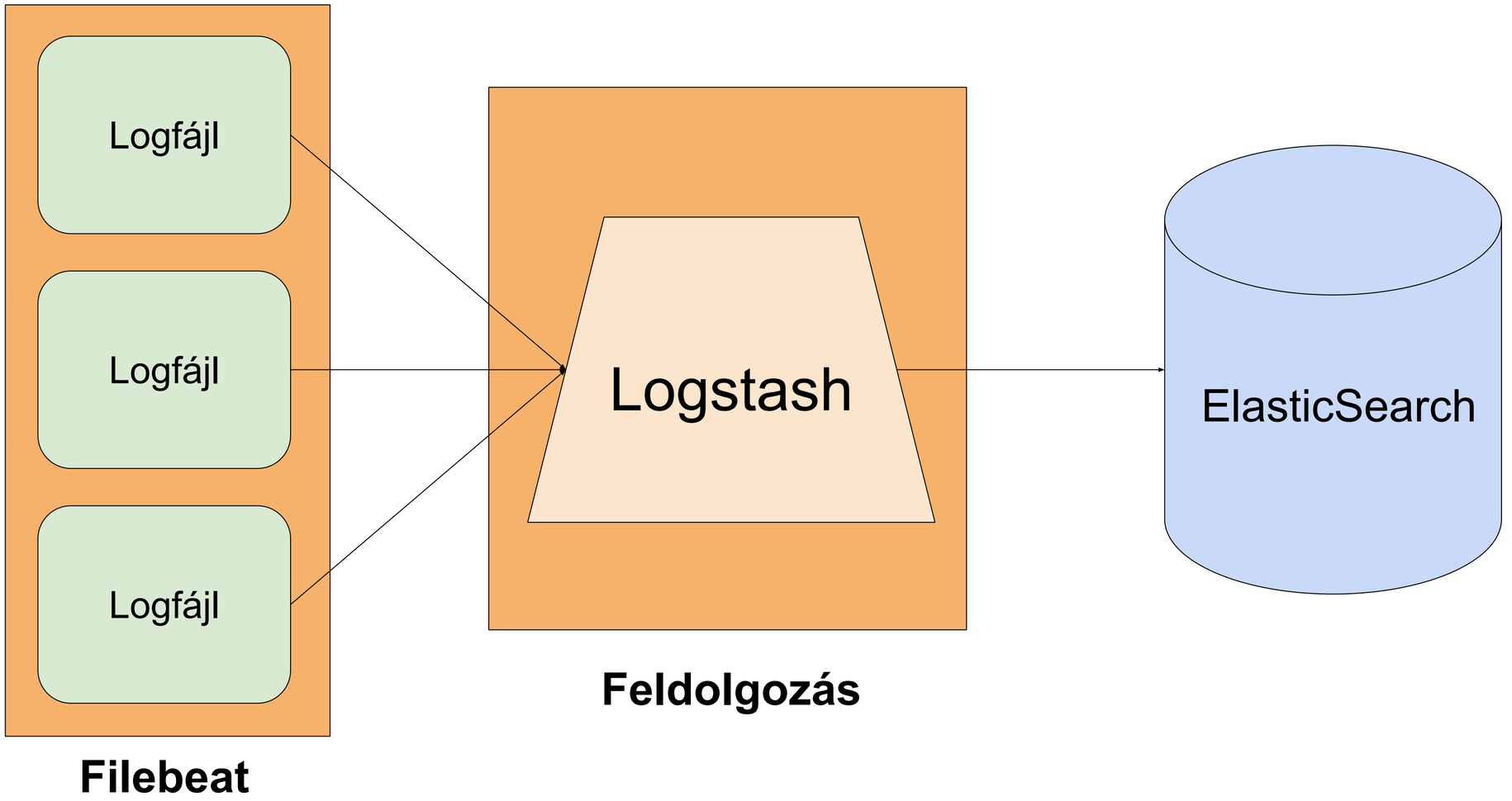
Logstash


5.10.83.30 user-identifier frank
[10/Oct/2000:13:55:36 -0700]
"GET /apache_pb.gif HTTP/1.0"
200 2326

GROK pattern


```
NGUSERNAME [a-zA-Z\.\@\-\+_%]+
NGUSER %{NGUSERNAME}
NGINXACCESS %{IPORHOST:clientip} %{NGUSER:ident} %{NGUSER:auth}
\[%{HTTPDATE:timestamp}\] "%{WORD:verb} %{URIPATHPARAM:request}
HTTP/%{NUMBER:httpversion}" %{NUMBER:response} (?:%{NUMBER:bytes}|-)
(?:"(?:%{URI:referrer}|-)"|%{QS:referrer}) %{QS:agent}
```

Hogy is megy ez

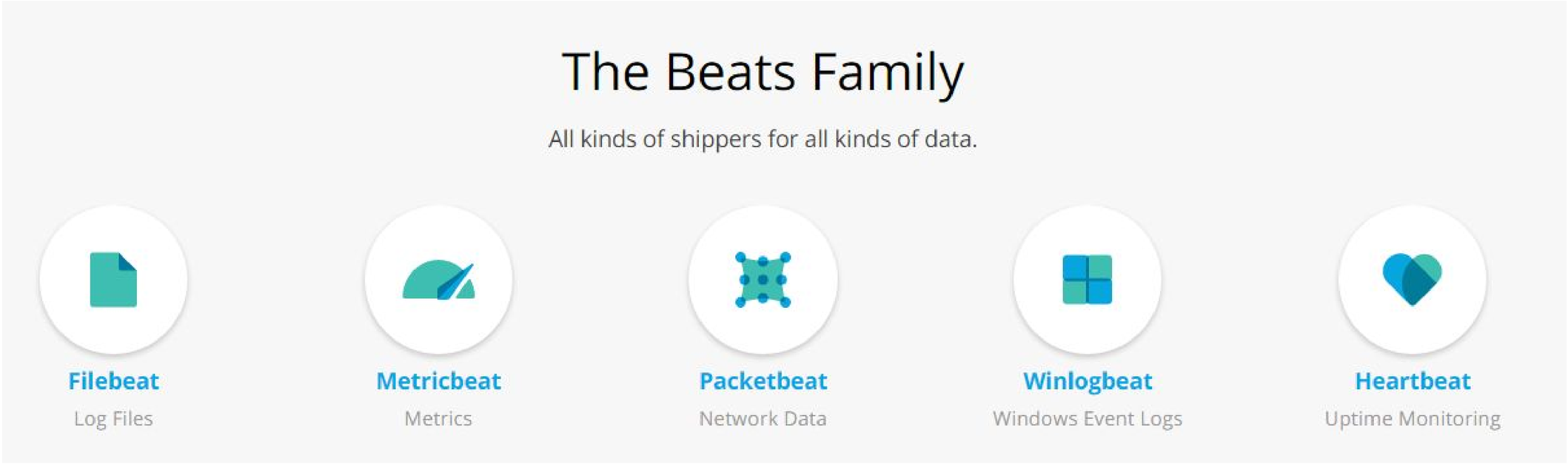


Logstash filter

```
grok {
   match => [ "message" , "%{COMBINEDAPACHELOG}+%{GREEDYDATA:extra_fields}"]
   overwrite => [ "message" ]
}
mutate {
   convert => ["response", "integer"]
   convert => ["bytes", "integer"]
   convert => ["responsetime", "float"]
}
geoip {
   source => "clientip"
   target => "geoip"
   add_tag => [ "nginx-geoip" ]
}
date {
   match => [ "timestamp" , "dd/MMM/YYYY:HH:mm:ss Z" ]
   remove_field => [ "timestamp" ]
}
```

Beats

Több különböző típusú forrásból/alkalmazásból képes összegyűjteni az eseményeket és elküldeni a logstash-nek



System module

Apache

Docker

HAProxy

Kafka

MongoDB

MySQL

Nginx

PostgreSQL

Redis

ZooKeeper

Add your own

Köszönöm a figyelmet!

attrecto
smartphone solutions