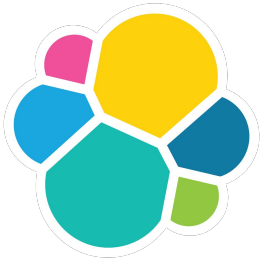


elastic

MONITORING SZYTY NA MIARĘ

Tomasz Gintowt

Senior IT Systems Engineer - Adform

https://www.linkedin.com/in/tomasz-gintowt/

Karol Cienkosz

Cloud Engineer - Vodeno

https://www.linkedin.com/in/karol-cienkosz-56997a165/

ELASTIC STACK

DEMO

PROMETHEUS

DEMO

WNIOSKI

demo.elastic.com

demo.robustperception.io

play.grafana.org

ELASTIC STACK

Zapytajmy internety..

rankinrez 33 points · 1 year ago

Elk is for logs

Prometheus / Time series are for performance metrics.

cuddling_tinder_twat 2 points · 1 year ago

The cost for alerting is what kills me

brianw824 11 points · 1 year ago · *edited 1 year ago*

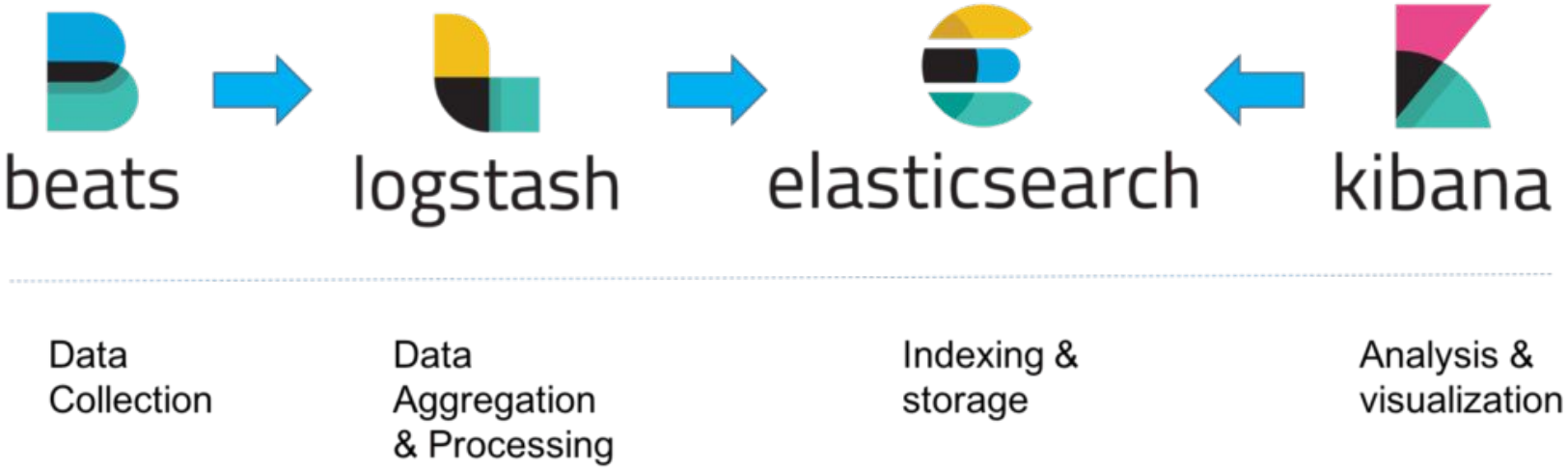
I used to use ELK for all logging, metrics and alerting and generally didn't like it but it can work.

The **biggest difference is** that ELK specializes in logs, and Prometheus specializes in metrics. Most major productions require using both ELK and Prometheus, each for its own specialty.

Prometheus VS ELK

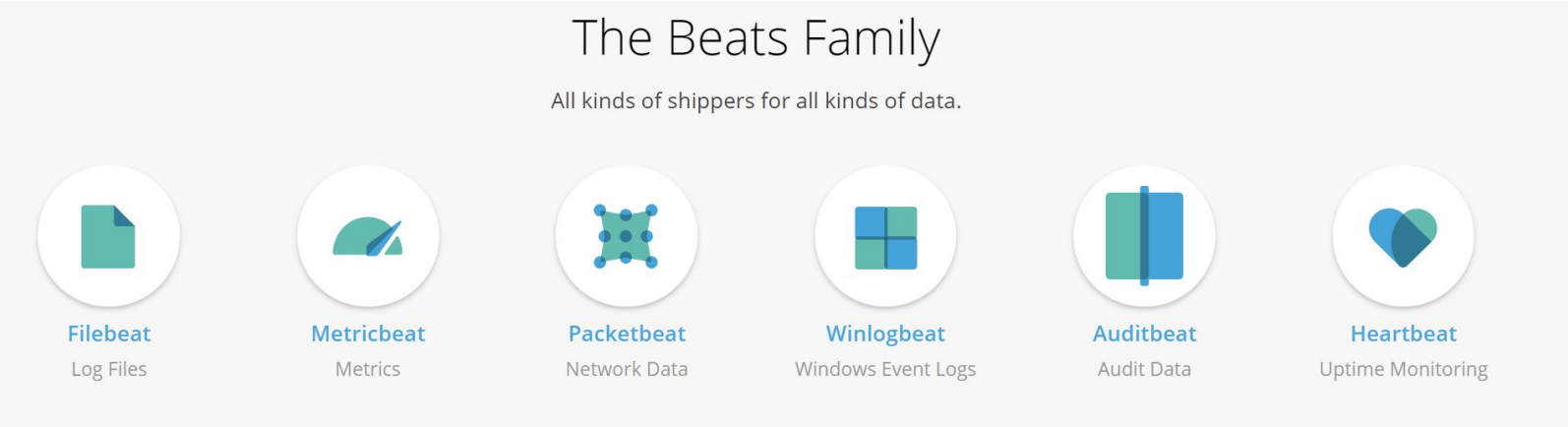
Both monitoring systems, Prometheus and ELK stack, have similar purposes. Their goals are detecting problems, debugging, and solving issues. But these systems use different approaches to this task.

Elastic Stack

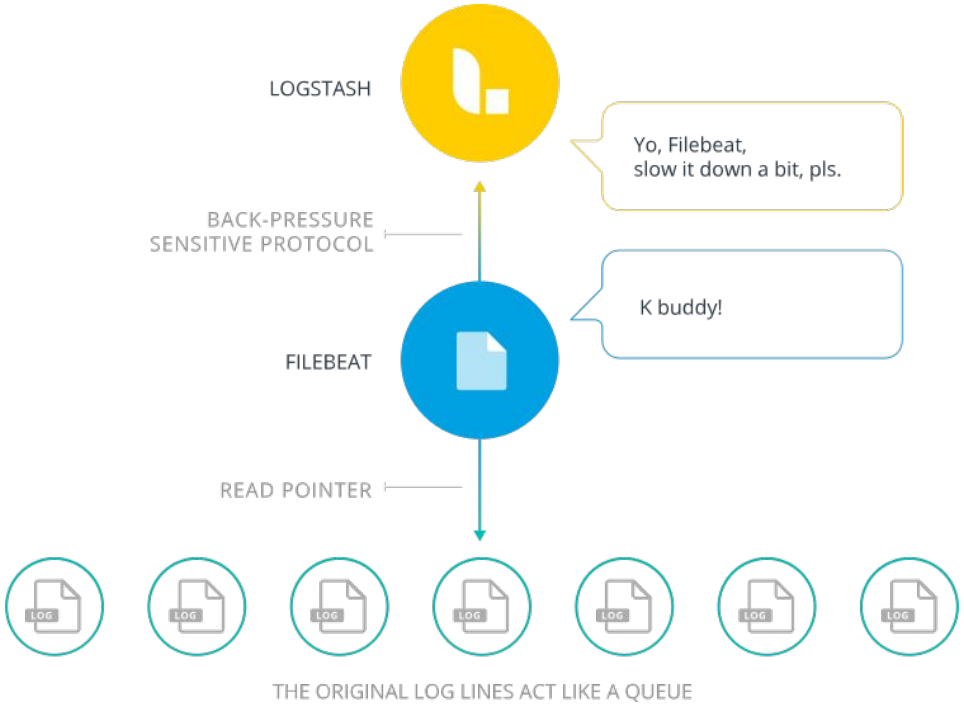


- on-prem & cloud managed/self-managed
- https://www.elastic.co/pricing/

Elastic The Beats Family



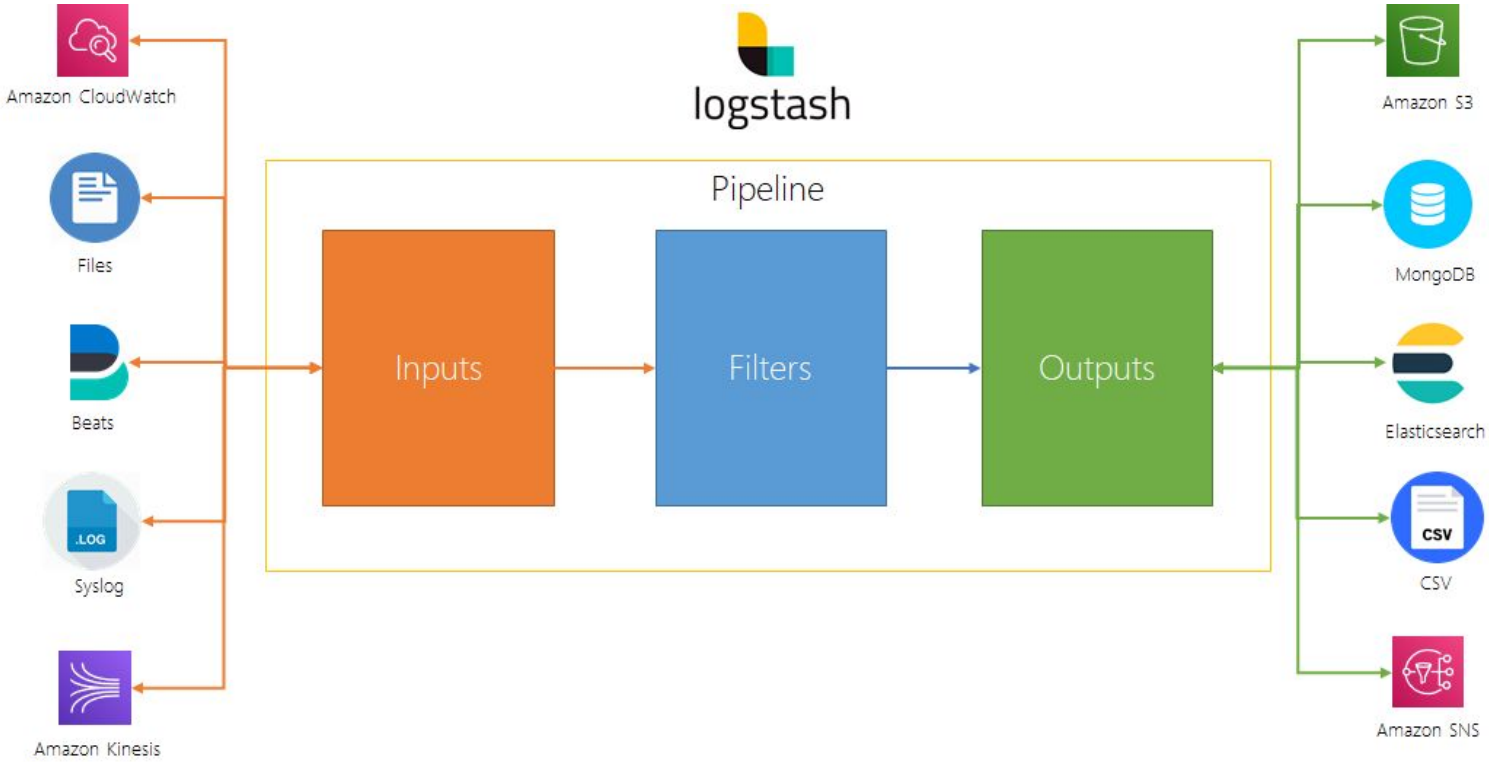
Filebeat


LOGSTASH
Yo, Filebeat,
slow it down a bit, pls.
BACK-PRESSURE
SENSITIVE PROTOCOL
K buddy!
FILEBEAT
READ POINTER
LOG
THE ORIGINAL LOG LINES ACT LIKE A QUEUE

Metricbeat

- system-level CPU usage, memory, file system, disk IO, and network IO statistics
- statystyki/metryki pochodzące z uruchomionych procesów
- dostępne moduły (elastic zachęca do pisania własnych): https://www.elastic.co/guide/en/beats/metricbeat/current/metricbeat-modules.html

Logstash

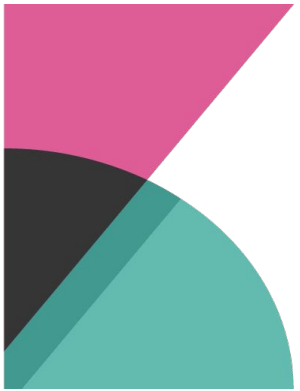

Amazon CloudWatch
Files
Beats
.LOG
Syslog
Amazon Kinesis
logstash
Pipeline
Inputs
Filters
Outputs
Amazon S3
MongoDB
Elasticsearch
CSV
CSV
Amazon SNS

ElasticSearch

- serce ELK
- bazuje na Apache Lucene
- NoSql
- pojęcia:
  - index
  - dokument
  - mapowanie
  - odłamek/kawałek (ang. Shard)
- klaster
- Rollup job

Kibana

- Przeszukiwanie
- Analiza
- Wizualizacja
- Alertowanie*
- Zarządzanie
- Dodatkowe narzędzia



Znalezione w sieci

InfluxDB:

- Ingest performance: 50,000 pts/s;
- Mean query response time: ~1.5s without cache, caching should be handled;
- On-disk storage requirements: 356 MB/project.

Elasticsearch:

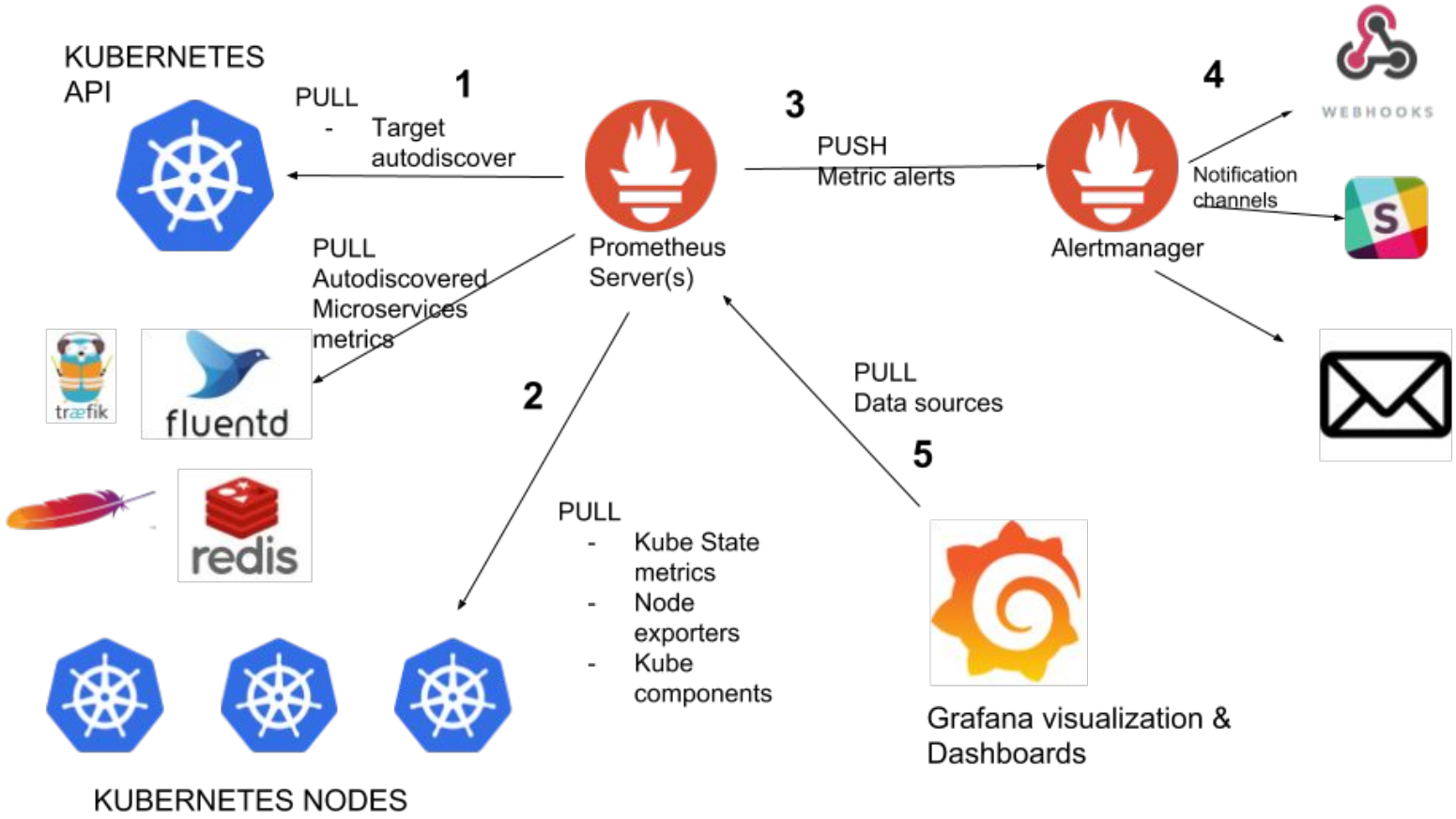
- Ingest performance: 8,800 docs/s;
- Mean query response time: ~130ms without cache, ~15ms with cache;
- On-disk storage requirements: 1.6 GB/project.

https://jolicode.com/blog/influxdb-vs-elasticsearch-for-time-series-and-metrics-data

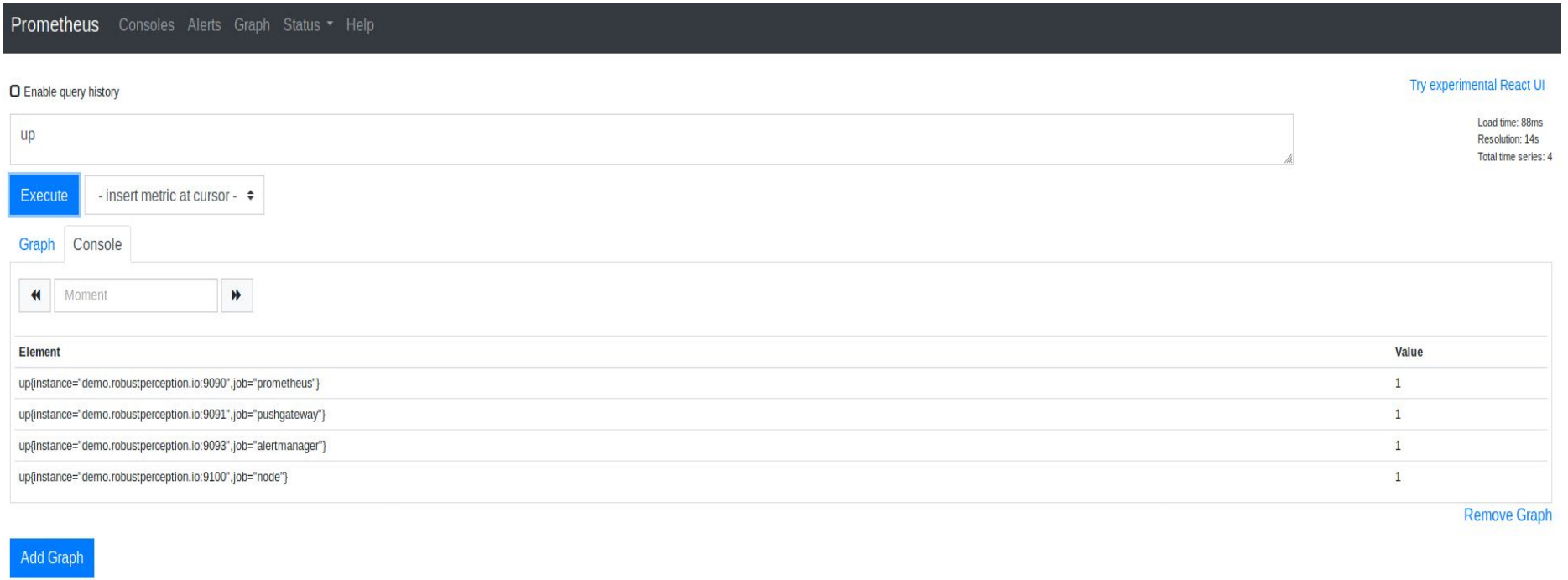
Demo!

- Logi/Metryki
- Wizualizacja
- Dashboard
- Canvas
- APM
- Console
- Machine Learning *

PROMETHEUS

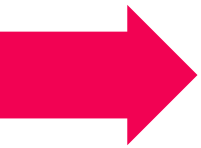

KUBERNETES API
PULL
- Target autodiscover
1
Prometheus Server(s)
3
PUSH
Metric alerts
Alertmanager
4
WEBHOOKS
Notification channels
PULL
Autodiscovered Microservices metrics
træfik
fluentd
2
PULL
Data sources
5
redis
PULL
- Kube State metrics
- Node exporters
- Kube components
Grafana visualization & Dashboards
KUBERNETES NODES

Prometheus


Prometheus
Consoles
Alerts
Graph
Status
Help
Enable query history
Try experimental React UI
up
Load time: 88ms
Resolution: 14s
Total time series: 4
Execute
- insert metric at cursor -
Graph
Console
Moment
Element
Value
up{instance="demo.robustperception.io:9090",job="prometheus"}
1
up{instance="demo.robustperception.io:9091",job="pushgateway"}
1
up{instance="demo.robustperception.io:9093",job="alertmanager"}
1
up{instance="demo.robustperception.io:9100",job="node"}
1
Remove Graph
Add Graph

curl localhost:9100/metrics

```
# HELP node_load1 1m load average.
# TYPE node_load1 gauge
node_load1 0.01
```



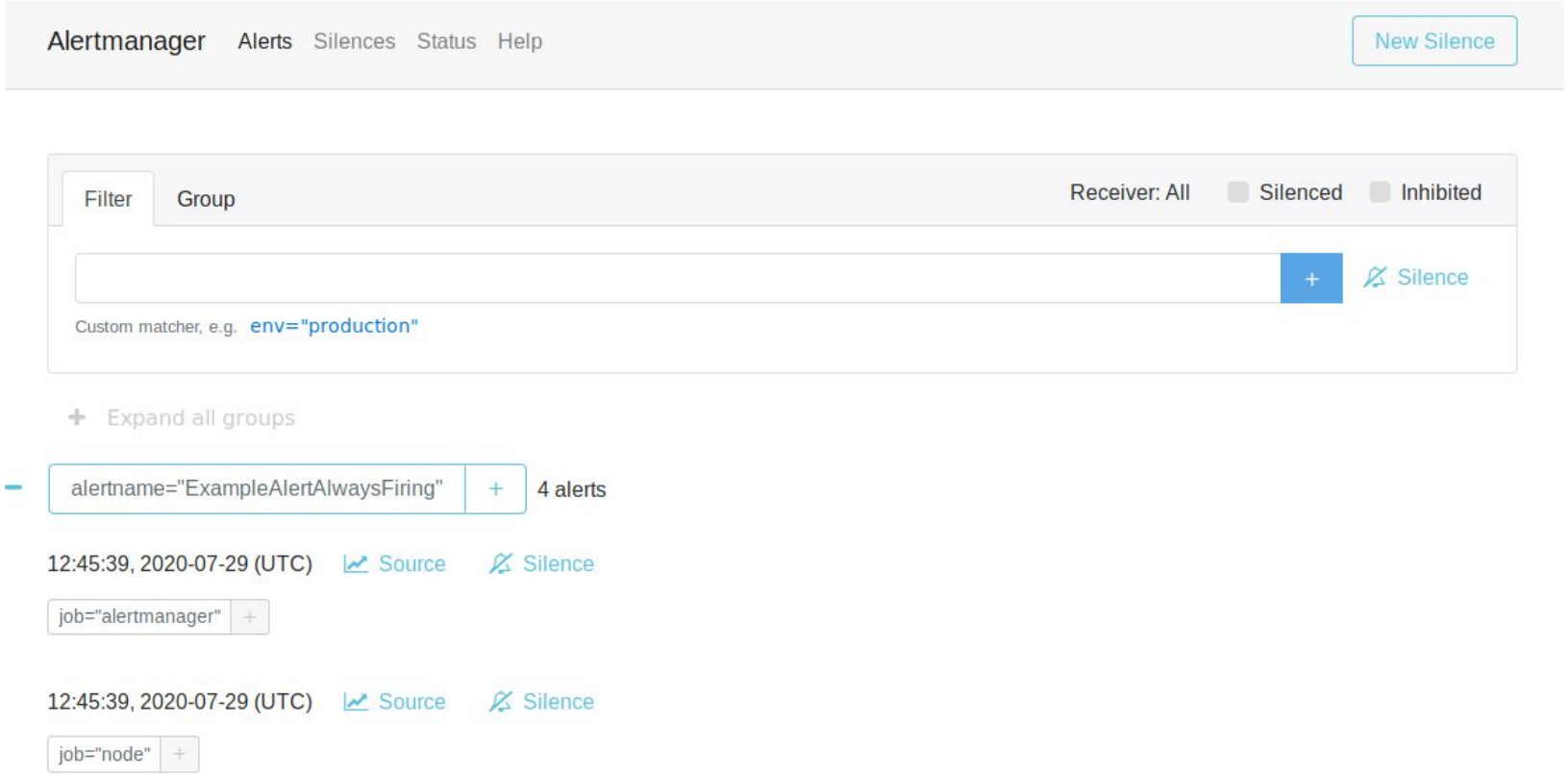
223 exporters

PromQL

```
up{job="prometheus"}
```

```
min(node_filesystem_free_bytes{fqdn=~"$cluster.*",fstype!~"rootfs|selinuxfs|autofs|rpc_pipefs|tmpfs", mountpoint=~"^/data|/$", tenant=~"$tenant"}
 / on (fqdn,mountpoint)
node_filesystem_size_bytes{fqdn=~"$cluster.*", fstype!~"rootfs|selinuxfs|autofs|rpc_pipefs|tmpfs", mountpoint=~"^/data|/$", tenant=~"$tenant"})*100
```

AlertManager



Promtail

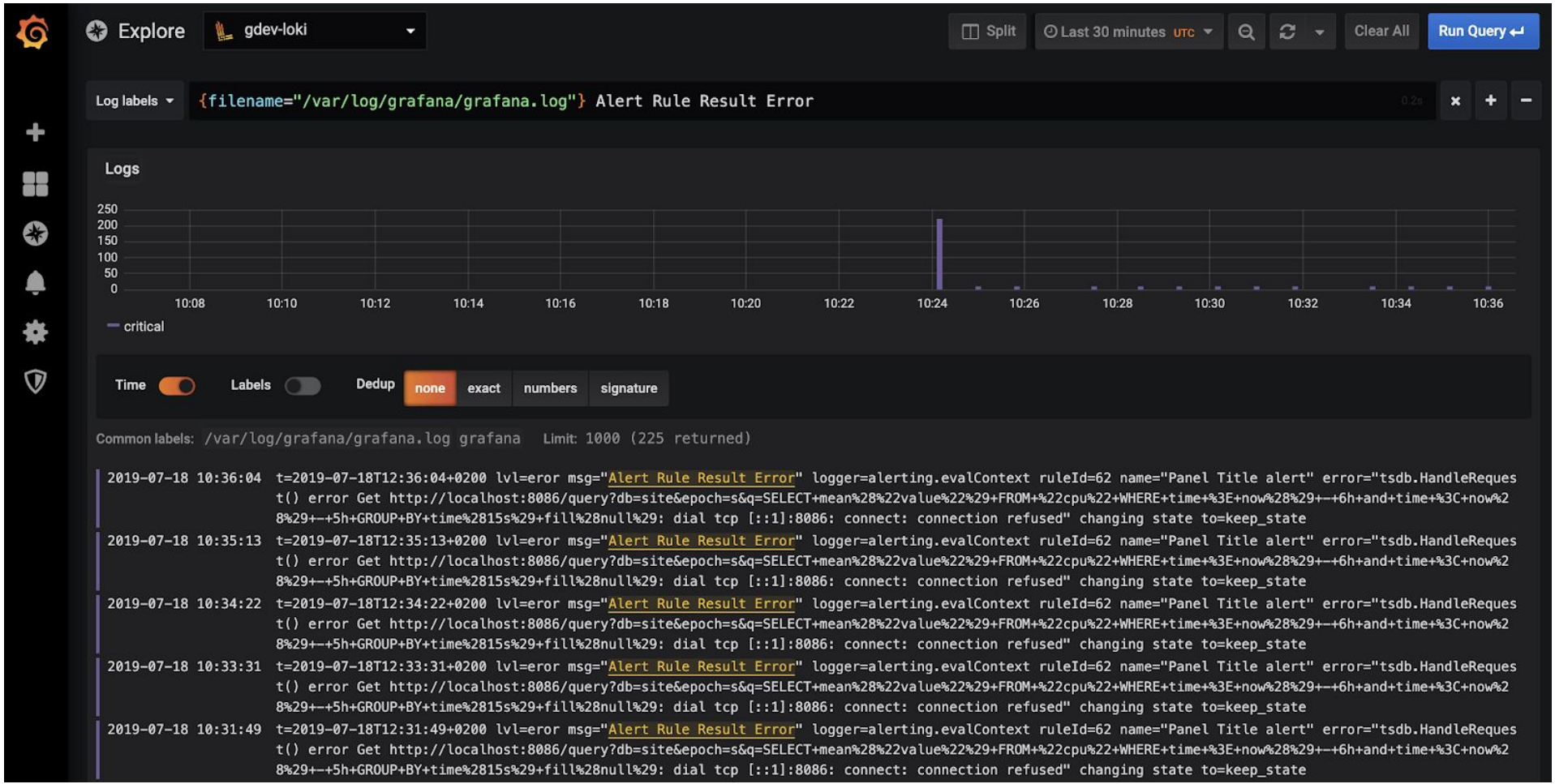
- is the agent, responsible for gathering logs and sending them to Loki.

Loki

- is the main server, responsible for storing logs and processing queries.

Grafana

- for querying and displaying the logs.


Explore
gdev-loki
Split
Last 30 minutes UTC
Clear All
Run Query
Log labels
{filename="/var/log/grafana/grafana.log"} Alert Rule Result Error
Logs
250
200
150
100
50
0
10:08
10:10
10:12
10:14
10:16
10:18
10:20
10:22
10:24
10:26
10:28
10:30
10:32
10:34
10:36
critical
Time
Labels
Dedup
none
exact
numbers
signature
Common labels: /var/log/grafana/grafana.log grafana
Limit: 1000 (225 returned)
2019-07-18 10:36:04 t=2019-07-18T12:36:04+0200 lvl=eror msg="Alert Rule Result Error" logger=alerting.evalContext ruleId=62 name="Panel Title alert" error="tsdb.HandleRequest() error Get http://localhost:8086/query?db=site&epoch=s&q=SELECT+mean%28%22value%22%29+FROM+%22cpu%22+WHERE+time+%3E+now%28%29+-+6h+and+time+%3C+now%28%29+-+5h+GROUP+BY+time%2815s%29+fill%28null%29: dial tcp [::1]:8086: connect: connection refused" changing state to=keep_state
2019-07-18 10:35:13 t=2019-07-18T12:35:13+0200 lvl=eror msg="Alert Rule Result Error" logger=alerting.evalContext ruleId=62 name="Panel Title alert" error="tsdb.HandleRequest() error Get http://localhost:8086/query?db=site&epoch=s&q=SELECT+mean%28%22value%22%29+FROM+%22cpu%22+WHERE+time+%3E+now%28%29+-+6h+and+time+%3C+now%28%29+-+5h+GROUP+BY+time%2815s%29+fill%28null%29: dial tcp [::1]:8086: connect: connection refused" changing state to=keep_state
2019-07-18 10:34:22 t=2019-07-18T12:34:22+0200 lvl=eror msg="Alert Rule Result Error" logger=alerting.evalContext ruleId=62 name="Panel Title alert" error="tsdb.HandleRequest() error Get http://localhost:8086/query?db=site&epoch=s&q=SELECT+mean%28%22value%22%29+FROM+%22cpu%22+WHERE+time+%3E+now%28%29+-+6h+and+time+%3C+now%28%29+-+5h+GROUP+BY+time%2815s%29+fill%28null%29: dial tcp [::1]:8086: connect: connection refused" changing state to=keep_state
2019-07-18 10:33:31 t=2019-07-18T12:33:31+0200 lvl=eror msg="Alert Rule Result Error" logger=alerting.evalContext ruleId=62 name="Panel Title alert" error="tsdb.HandleRequest() error Get http://localhost:8086/query?db=site&epoch=s&q=SELECT+mean%28%22value%22%29+FROM+%22cpu%22+WHERE+time+%3E+now%28%29+-+6h+and+time+%3C+now%28%29+-+5h+GROUP+BY+time%2815s%29+fill%28null%29: dial tcp [::1]:8086: connect: connection refused" changing state to=keep_state
2019-07-18 10:31:49 t=2019-07-18T12:31:49+0200 lvl=eror msg="Alert Rule Result Error" logger=alerting.evalContext ruleId=62 name="Panel Title alert" error="tsdb.HandleRequest() error Get http://localhost:8086/query?db=site&epoch=s&q=SELECT+mean%28%22value%22%29+FROM+%22cpu%22+WHERE+time+%3E+now%28%29+-+6h+and+time+%3C+now%28%29+-+5h+GROUP+BY+time%2815s%29+fill%28null%29: dial tcp [::1]:8086: connect: connection refused" changing state to=keep_state

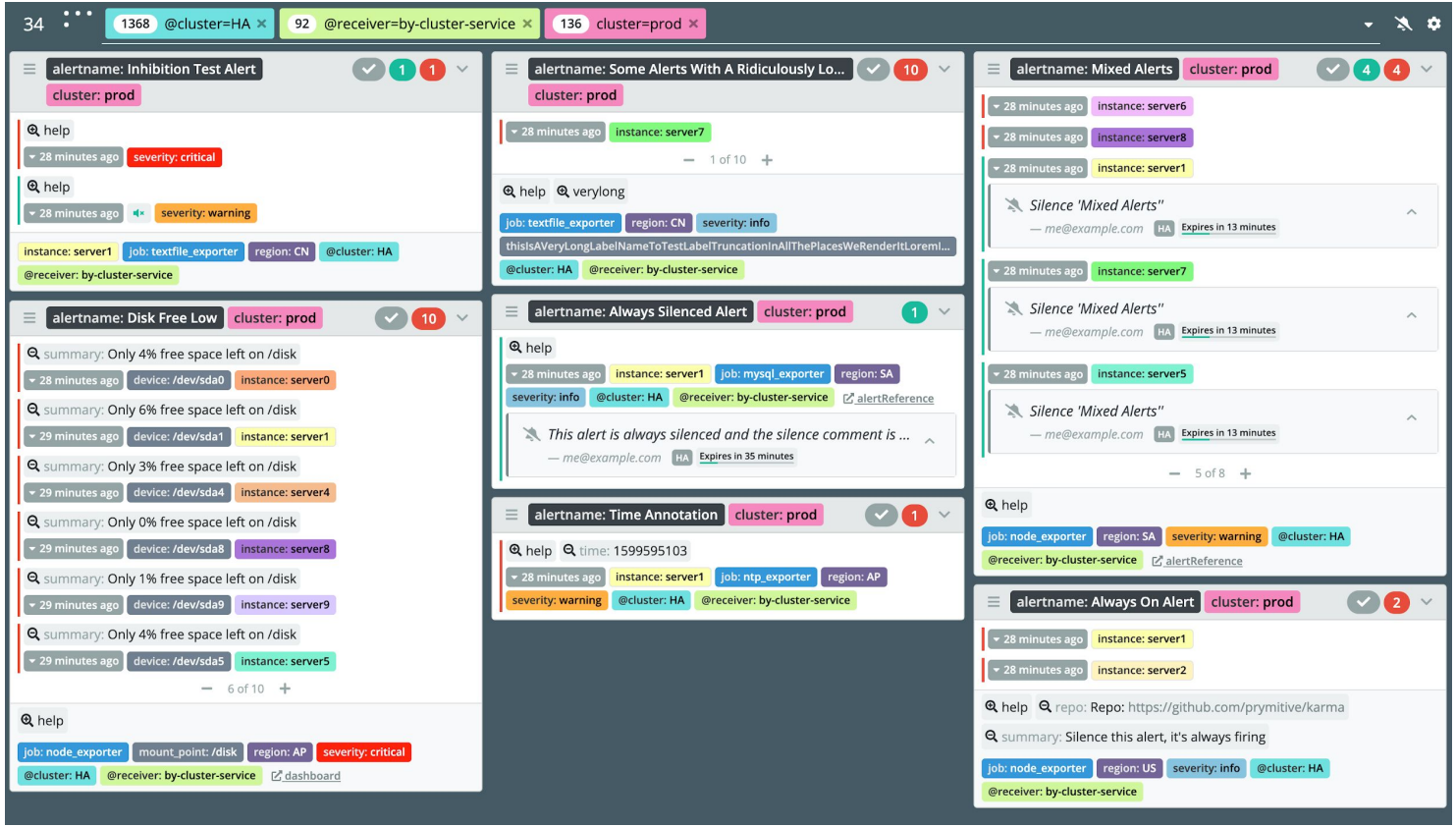
Grafana


Grafana Play Home
Last 1 hour
Feature showcases
Alerting
Demo
Annotations
Demo
Bar Gauge
Demo
Grafana Dashboard
Demo
Graph Gradient Area Fills
Data source demos
Elasticsearch Metrics
Elastic
Elasticsearch Templated
Elastic
Graphite Templated Nested
Graphite
InfluxDB Templated
Influx DB
Prometheus - Demo Dashboard
What's New
1 - New Features in v7.0
Demo
2 - New Features in v6.6
What's new
3 - New Features in v6.3
What's new
4 - New Features in v6.2
What's new
server requests
150
100
50
0
11:20
11:25
11:30
11:35
11:40
11:45
11:50
11:55
12:00
12:05
12:10
12:15
web_server_01
web_server_02
web_server_03
web_server_04
Memory / CPU
60 B
40 B
20 B
0 B
20%
15%
10%
5%
0%
11:20
11:30
11:40
11:50
12:00
12:10
memory
cpu
client side full page load
5 s
4 s
3 s
2 s
1 s
0 ms
avg
upper_25 2 ms
upper_50 192 ms
upper_75 650 ms
upper_90 1.246 s
upper_95 1.816 s
logins
80
60
40
20
0
11:20
11:30
11:40
11:50
12:00
12:10
logins
logins (-1 hour)

Grafana


ELEKTRON
GREEN 13 24807 1 3 1 0 16 67% 31% 87%
GREEN 10 8354 0 0 0 0 0 16% 50% 82%
GREEN 10 25300 0 0 0 0 0 28% 55% 73%
OK 944 19.18% 56%
OK 677 31.52% 91%
9 No Data 2.46% 90%

Karma dashboard



Demo!

- Exporter
- Prometheus
- AlertManager
- Grafana

Pull (Push)
TSDB
Grafana
Exporter
Loki
AlertManager/Grafana
Metryki + logi

Push
ElasticSearch
Kibana
MetricBeat
File Beat
Kibana/ElasticSearch
Logi + metryki

“Plus i Minus to jedyne co widzę” ~ Kaliber 44

- Wsparcie CNCF
- K8S/Cloud
- Duży wybór już istniejących eksporterów
- Open Source
- Service Discovery
- Popularność

- Bardzo szeroki zakres narzędzi i możliwości
- Wydajny silnik wyszukiwania
- Duży wybór już istniejących modułów i pluginów (zawsze możesz dopisać coś własnego)
- Open Source
- Popularnosć ELK Stack
- Java
- Dokumentacja

“Plus i Minus to jedyne co widzę” ~ Kaliber 44

- PromQL
- Ilość komponentów
- PULL Limits
- Long Term Storage (Thanos)
- Filtrowanie logów
- Skalowalność
- APM
- AIOps/ML

- Konfiguracja
- Zarządzanie
- Java
- Optymalizacja
- Zasoby (RAM, dysk, $$$)
- Dokumentacja
- Relatywnie długi czas zapisu
- https://www.elastic.co/pricing/

Dziękujemy!

Czas na pytania.

Tomasz Gintowt
https://www.linkedin.com/in/tomasz-gintowt/

Karol Cienkosz
https://www.linkedin.com/in/karol-cienkosz-56997a165/