Mark Hendriks

(M)ELK is goed voor elk

ORDINA

JTECH

/rovingeye

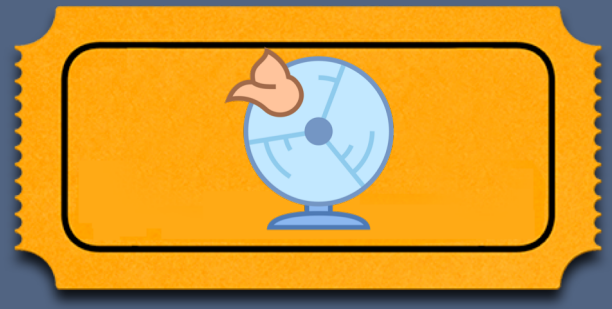
Who am I?

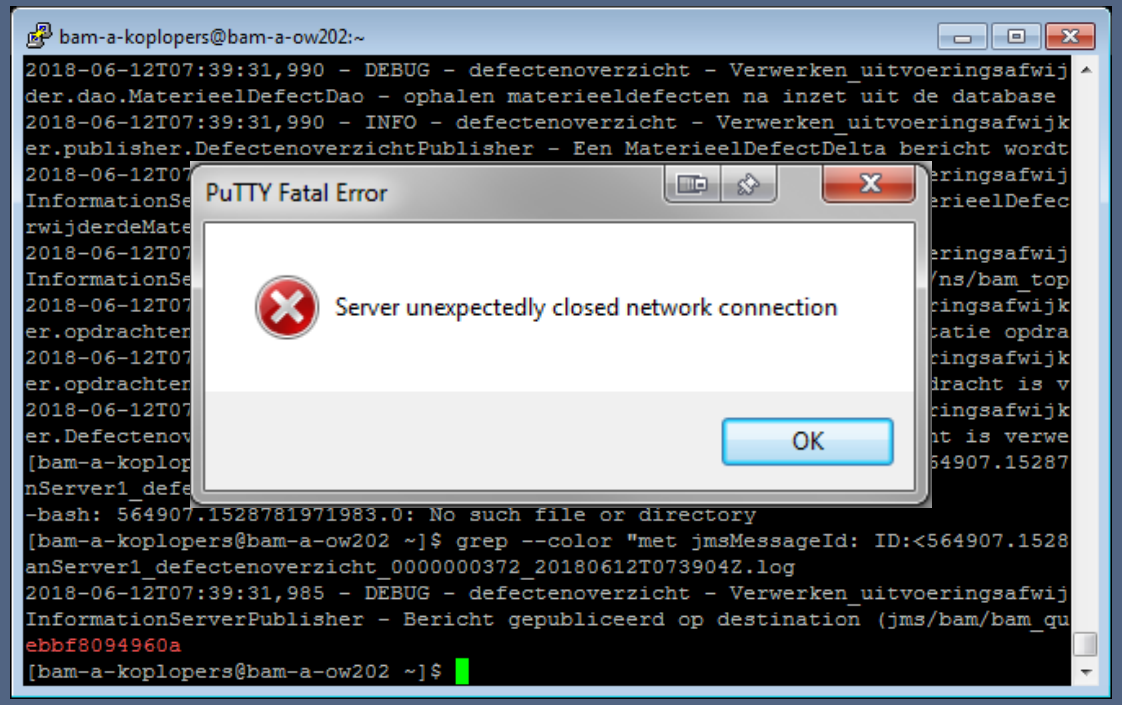
Mark Hendriks

Chapter lead @ Ordina JTech

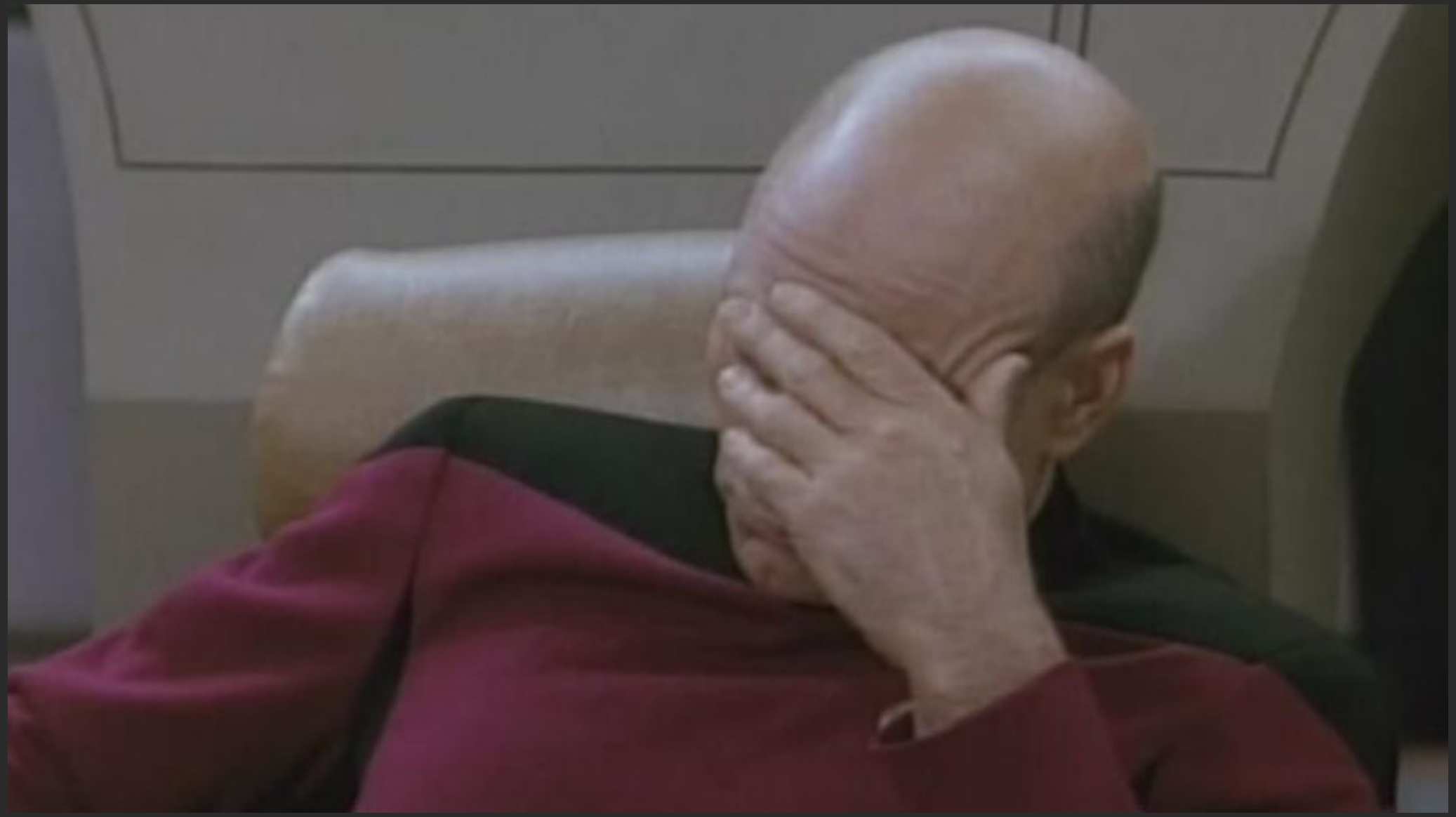
Ordina Academy Trainer

Dutch Railways





$ grep --color debug.log “find my error”



Could there be an easier way?

elasticsearch

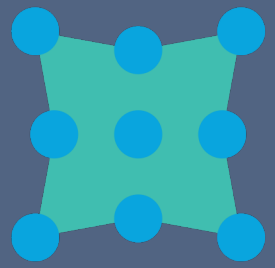
logstash

kibana

Beats

Filebeat

Metricbeat

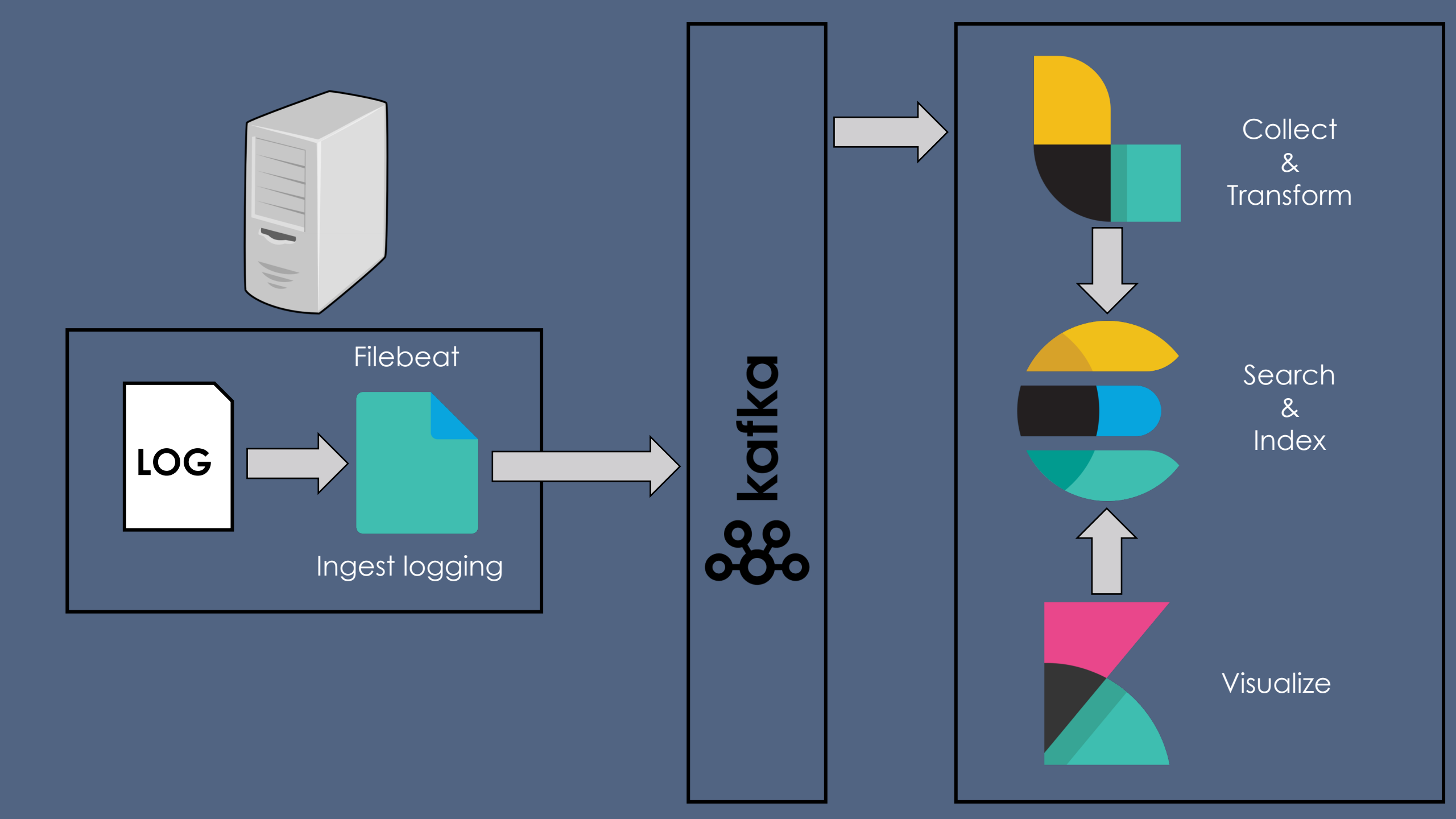


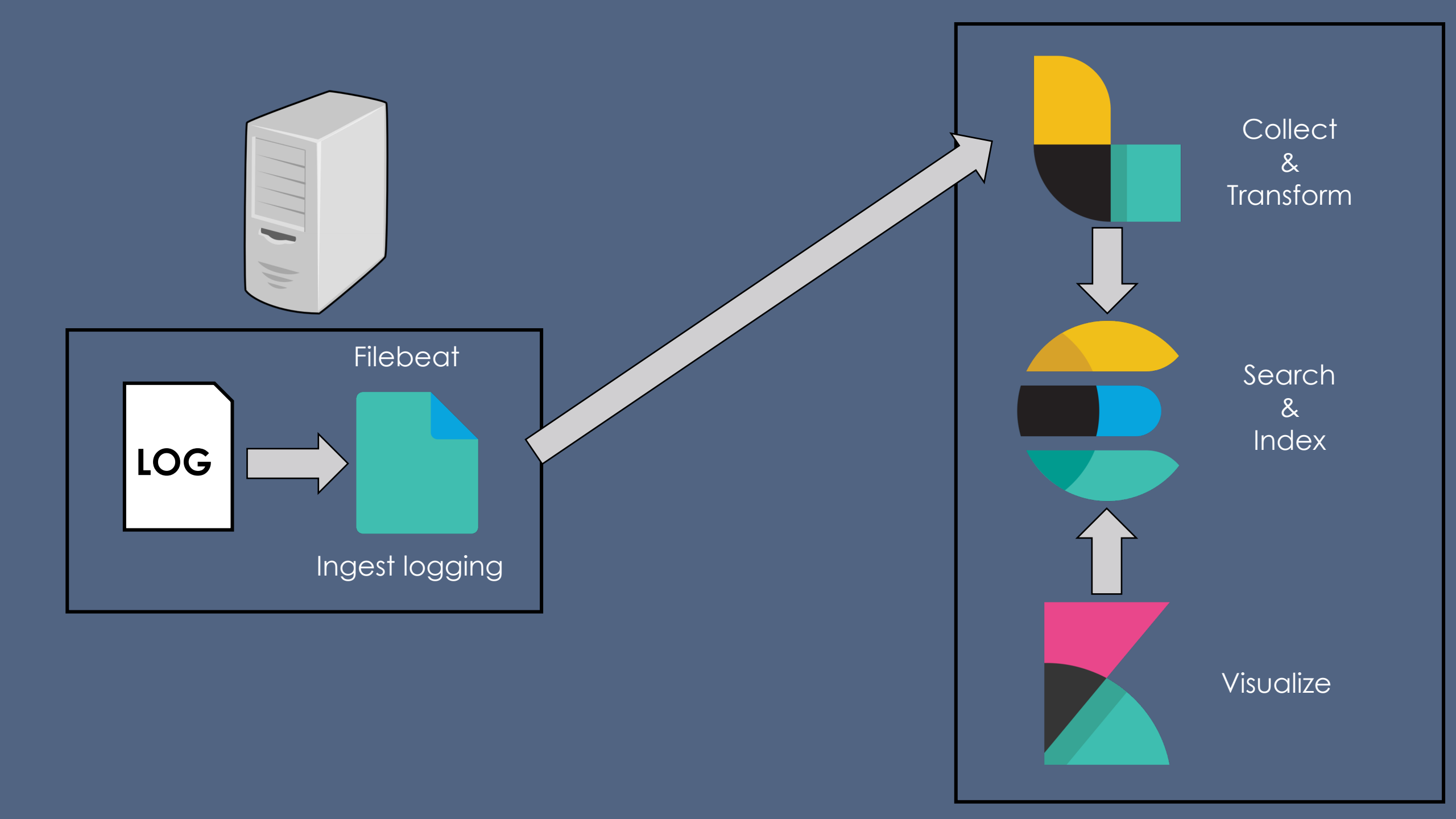
Packetbeat

Winlogbeat

Auditbeat

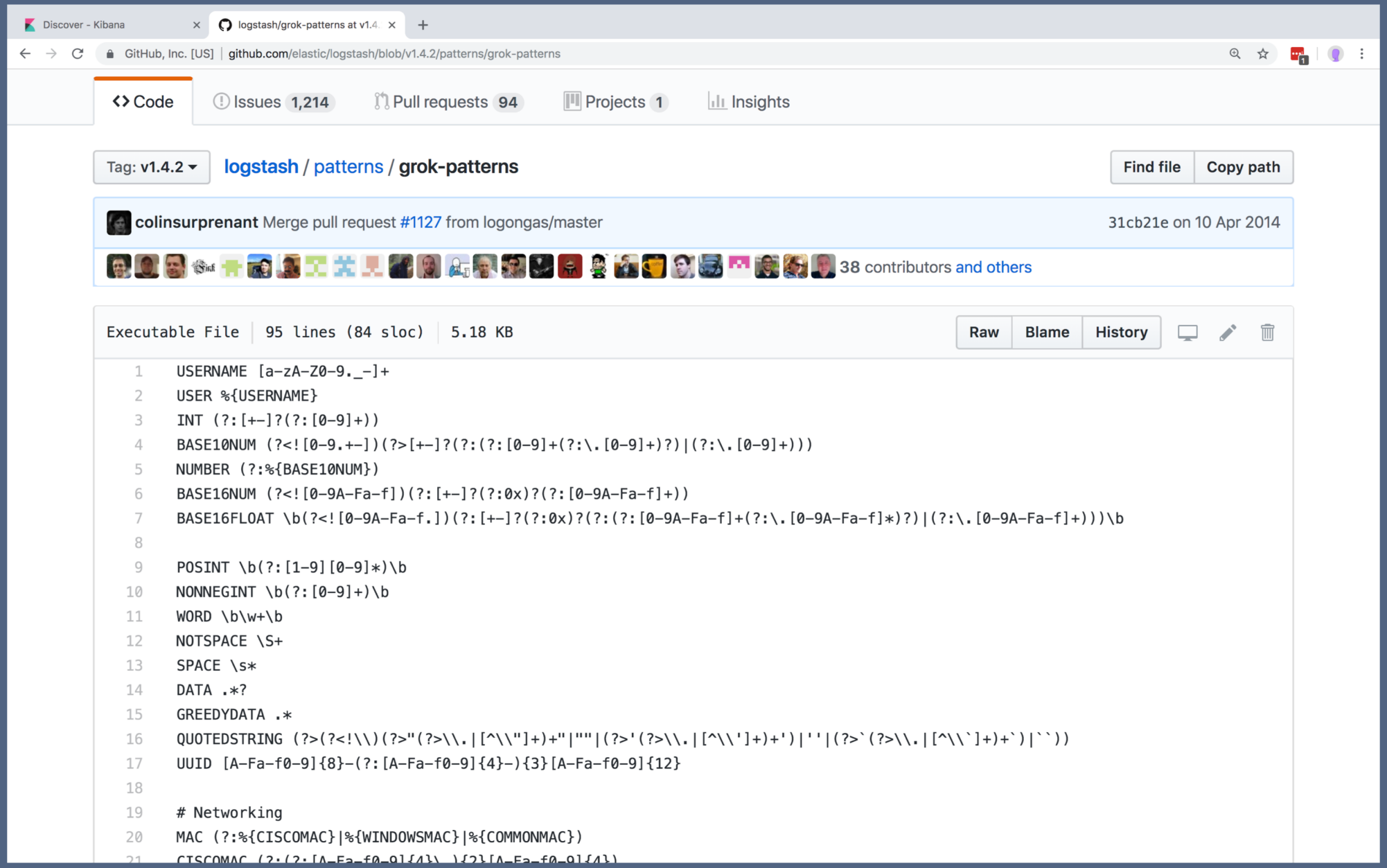
Heartbeat


Filebeat
LOG
Ingest logging
kafka
Collect
&
Transform
Search
&
Index
Visualize


Filebeat
LOG
Ingest logging
Collect
&
Transform
Search
&
Index
Visualize

DEMO

Grok filter plugin


Discover - Kibana
logstash/grok-patterns at v1.4
GitHub, Inc. [US] | github.com/elastic/logstash/blob/v1.4.2/patterns/grok-patterns
Code
Issues 1,214
Pull requests 94
Projects 1
Insights
Tag: v1.4.2
logstash / patterns / grok-patterns
Find file
Copy path
colinsurprenant Merge pull request #1127 from logongas/master
31cb21e on 10 Apr 2014
38 contributors and others
Executable File | 95 lines (84 sloc) | 5.18 KB
Raw
Blame
History
USERNAME [a-zA-Z0-9._-]+
USER %{USERNAME}
INT (?:[+-]?(?:[0-9]+))
BASE10NUM (?<![0-9.+-])(?>[+-]?(?:(?:[0-9]+(?:\.[0-9]+)?)|(?:\.[0-9]+)))
NUMBER (?:%{BASE10NUM})
BASE16NUM (?<![0-9A-Fa-f])(?:[+-]?(?:0x)?(?:[0-9A-Fa-f]+))
BASE16FLOAT \b(?<![0-9A-Fa-f.])(?:[+-]?(?:0x)?(?:(?:[0-9A-Fa-f]+(?:\.[0-9A-Fa-f]*)?)|(?:\.[0-9A-Fa-f]+)))\b
POSINT \b(?:[1-9][0-9]*)\b
NONNEGINT \b(?:[0-9]+)\b
WORD \b\w+\b
NOTSPACE \S+
SPACE \s*
DATA .*?
GREEDYDATA .*
QUOTEDSTRING (?>(?<!\\)(?>"(?>\\.|[^\\"]+)+"|""|(?>'(?>\\.|[^\\']+)+')|''|(?>`(?>\\.|[^\\`]+)+`)|``))
UUID [A-Fa-f0-9]{8}-(?:[A-Fa-f0-9]{4}-){3}[A-Fa-f0-9]{12}
Networking
MAC (?:%{CISCOMAC}|%{WINDOWSMAC}|%{COMMONMAC})

```
> logstash-plugin install logstash-patterns-core

> logstash-plugin install logstash-filter-grok
```

```
%{SYNTAX:SEMANTIC}
%{DATA:log_timestamp}

.*?
```

2018-09-08T17:04:08,690 - INFO - transadapter

%{DATA:log_timestamp} %{DATA:component}

%{DATA:loglevel}

What about the dashes (-)?

Custom patterns

DELIM \s-\s

```
2018-09-08T17:04:08,690 - INFO - transadapter
```

```
%{DATA:log_timestamp}%{DELIM}%{DATA:loglevel}
%{DELIM}%{DATA:component}
```

DEMO

Mark Hendriks

(M)ELK is goed voor elk

ORDINA

JTECH

/rovingeye

TACTICAL FACEPALM

Sometimes a regular facepalm just doesn't cut it