



ORDINA



Mark Hendriks

(M)ELK is goed
voor elk



/rovingeye

Who am I?

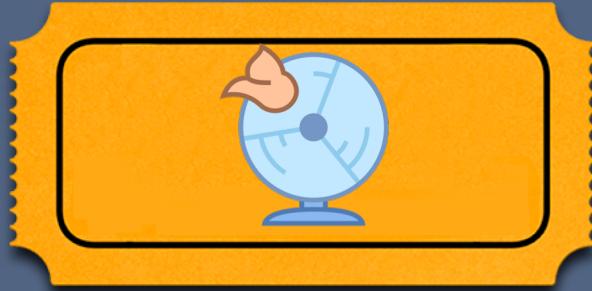
Mark Hendriks

Chapter lead @ Ordina JTech

Ordina Academy Trainer

Dutch Railways

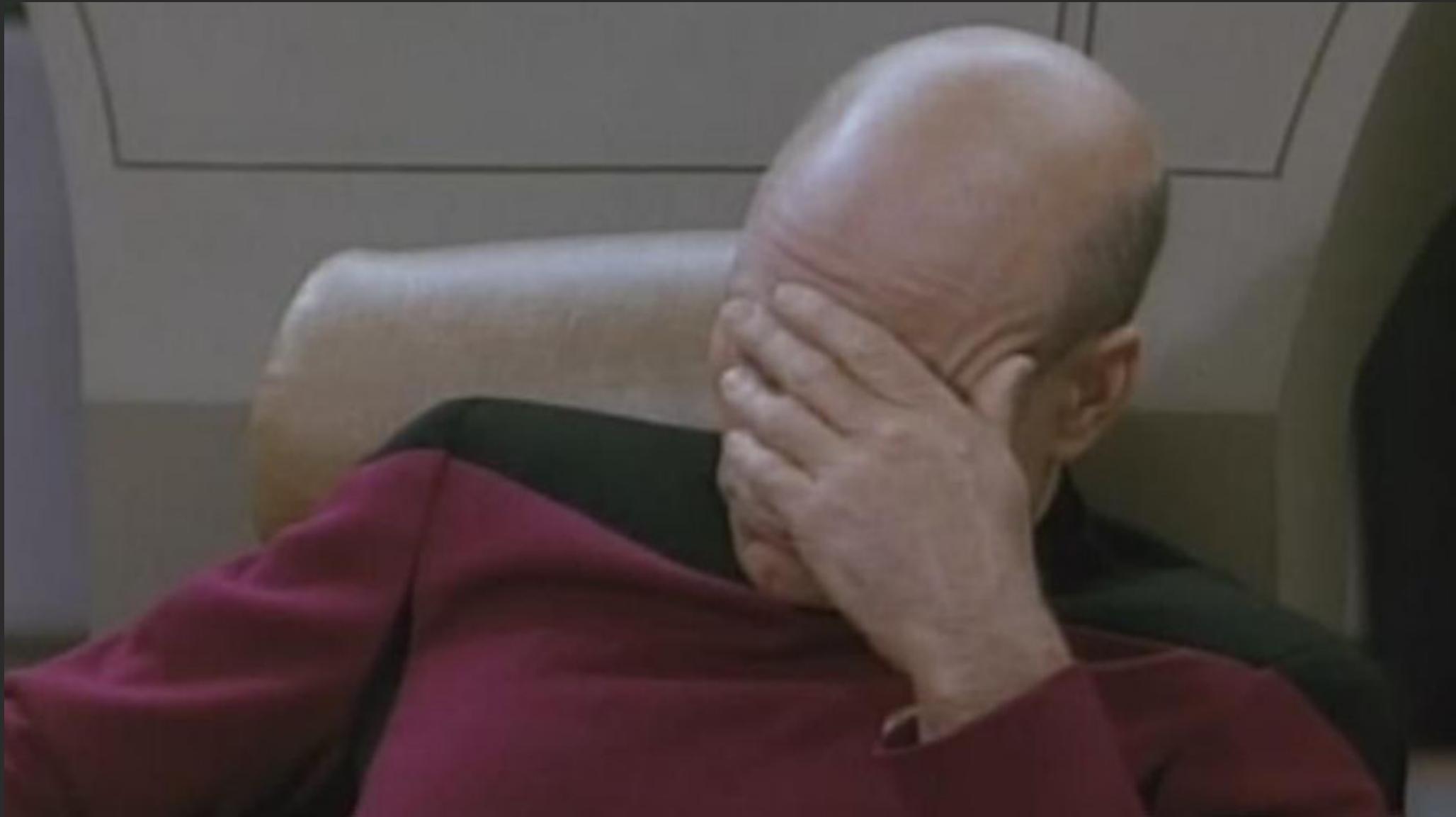




A screenshot of a PuTTY session window. The terminal output shows several lines of log messages from a Java application, including DEBUG and INFO levels. A modal dialog box titled "PuTTY Fatal Error" is displayed in the center of the screen, showing the message "Server unexpectedly closed network connection". An "OK" button is visible at the bottom right of the dialog. The background terminal window has a blue scroll bar.

```
bam-a-koplopers@bam-a-ow202:~  
2018-06-12T07:39:31,990 - DEBUG - defectenoverzicht - Verwerken_uitvoeringsafwij  
der.dao.MaterieelDefectDao - ophalen materieeldefecten na inzet uit de database  
2018-06-12T07:39:31,990 - INFO - defectenoverzicht - Verwerken_uitvoeringsafwij  
ker.publisher.DefectenoverzichtPublisher - Een MaterieelDefectDelta bericht wordt  
2018-06-12T07:  
InformationSe  
rwijlderdeMate  
2018-06-12T07:  
InformationSe  
2018-06-12T07:  
er.opdrachter  
2018-06-12T07:  
er.opdrachter  
2018-06-12T07:  
er.Defectenov  
[bam-a-koplop  
nServer1_defe  
-bash: 564907.1528781971983.0: No such file or directory  
[bam-a-koplopers@bam-a-ow202 ~]$ grep --color "met jmsMessageId: ID:<564907.1528  
anServer1_defectenoverzicht_0000000372_20180612T073904Z.log  
2018-06-12T07:39:31,985 - DEBUG - defectenoverzicht - Verwerken_uitvoeringsafwij  
InformationServerPublisher - Bericht gepubliceerd op destination (jms/bam/bam_qu  
ebbf8094960a  
[bam-a-koplopers@bam-a-ow202 ~]$
```

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



Could there be an easier way?



elasticsearch



logstash



kibana



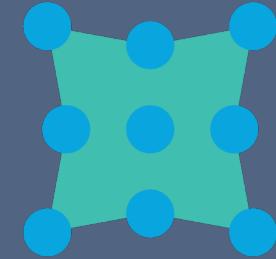
Beats



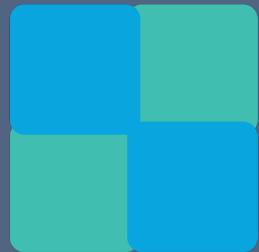
Filebeat



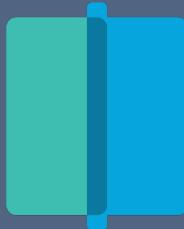
Metricbeat



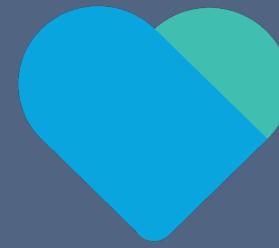
Packetbeat



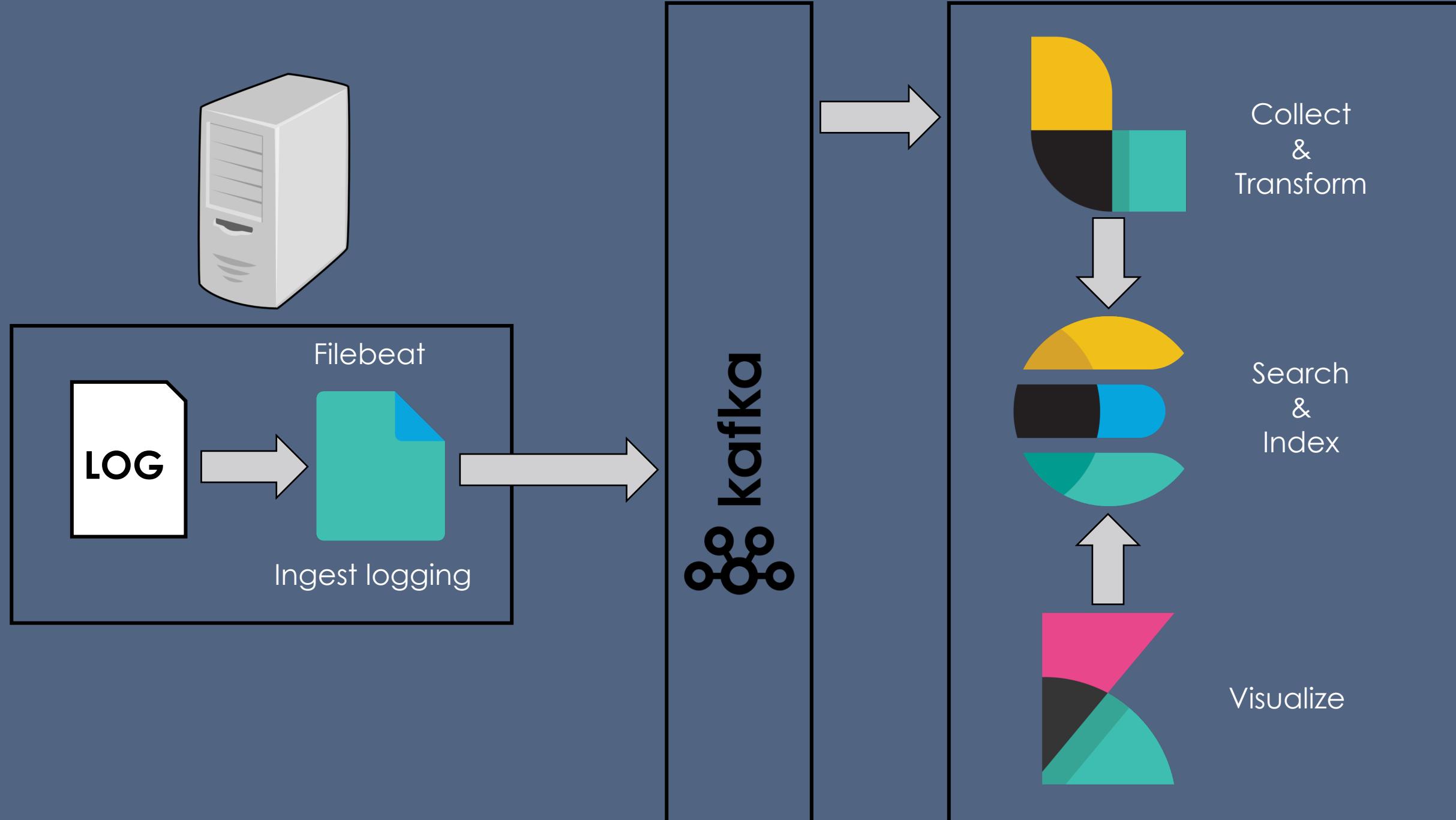
Winlogbeat

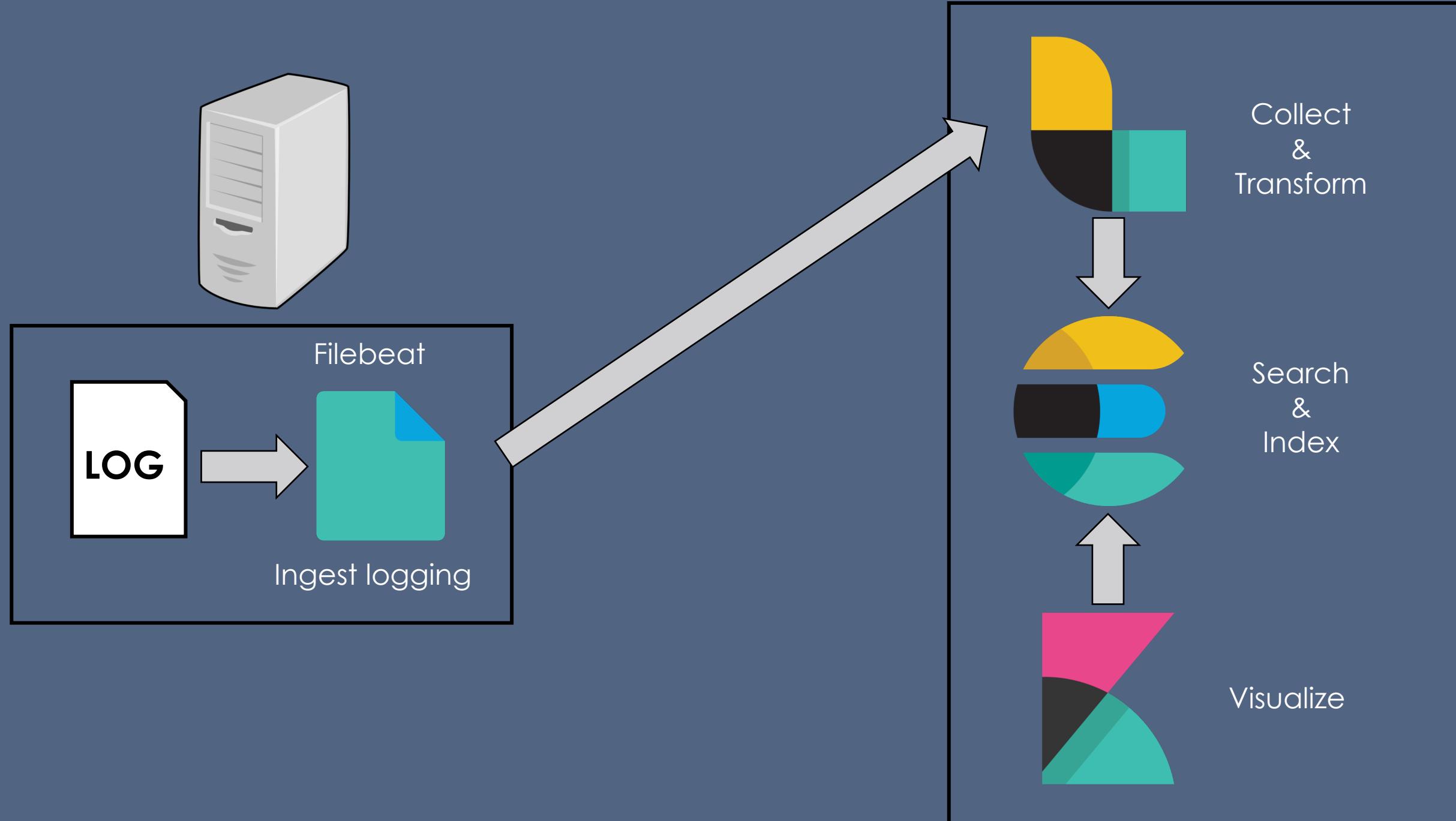


Auditbeat



Heartbeat





DEMO

Grok filter plugin

Discover - Kibana x logstash/grok-patterns at v1.4.2 +/-

GitHub, Inc. [US] | github.com/elastic/logstash/blob/v1.4.2/patterns/grok-patterns

Code Issues Pull requests Projects 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

```
1 USERNAME [a-zA-Z0-9._-]+
2 USER %{USERNAME}
3 INT (?:[+-]?(?:[0-9]+))
4 BASE10NUM (?<! [0-9.+-])(?>[+-]?(?:(:[0-9]+(?:\.[0-9]+)?))|(?:\.\.[0-9]+)))
5 NUMBER (?%{BASE10NUM})
6 BASE16NUM (?<! [0-9A-Fa-f])(?:[+-]?(?:0x)?(?:[0-9A-Fa-f]+))
7 BASE16FLOAT \b(?<! [0-9A-Fa-f.])(?:[+-]?(?:0x)?(?:(:[0-9A-Fa-f]+(?:\.[0-9A-Fa-f]*))|(?:\.\.[0-9A-Fa-f]+)))\b
8
9 POSINT \b(?:[1-9][0-9]*)\b
10 NONNEGINT \b(?:[0-9]+)\b
11 WORD \b\w+\b
12 NOTSPACE \s+
13 SPACE \s*
14 DATA .*?
15 GREEDYDATA .*
16 QUOTEDSTRING (?>(?<!\\)(?>"(?>\\.|[^\"])+"+|"||(?>'(?>\\.|[^\'])+')+)|''|(?>`(?>\\.|[^\`])+`)|``))
17 UUID [A-Fa-f0-9]{8}-(?:[A-Fa-f0-9]{4}-){3}[A-Fa-f0-9]{12}
18
19 # Networking
20 MAC (?%{CISCOMAC}|%{WINDOWS_MAC}|%{COMMON_MAC})
21 CISCOMAC (?:(?:(A-Fa-f0-9){2}\.){3}(A-Fa-f0-9){4})
```

```
> 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





ORDINA



Mark Hendriks

(M)ELK is goed
voor elk



/rovingeye



TACTICAL FACEPALM

Sometimes a regular facepalm just doesn't cut it