Logstash

find happiness in your logs
with Elasticsearch ELK

Open Source

Open Source

Apache 2.0 License

Open Source

Open and Friendly Community

If a new user has a bad time, it's a bug.

Technology

Logstash

Logstash

Processing & Transport

Logstash

Processing & Transport

42

Inputs

51

Filters

54

Outputs

Logstash

Processing & Transport

LAMP Example

Load Balancer
Apache

Mysql
PHP
Syslog

Parse: Latency,
Bandwidth,
and Errors

Nagios

Elasticsearch

Graphite

IRC

Logstash

Example Inputs

Files

Graphite

Email

SNMP

Syslog

RabbitMQ

TCP

Twitter

Example Filters

Grok

Date

GeoIP

Fingerprint

Multiline

Key-Value

User Agent

Logstash

Example Outputs

Elasticsearch

Graphite

Nagios

XMPP

Email

Pagerduty

S3

Elasticsearch

Elasticsearch

Near Real-Time Search & Analysis

Elasticsearch

Scalable

Elasticsearch

REST + JSON API

Kibana

Kibana

Visualization & Exploration

apache

Mar 5, 2014 10:28:30 to Mar 14, 2014 22:27:31

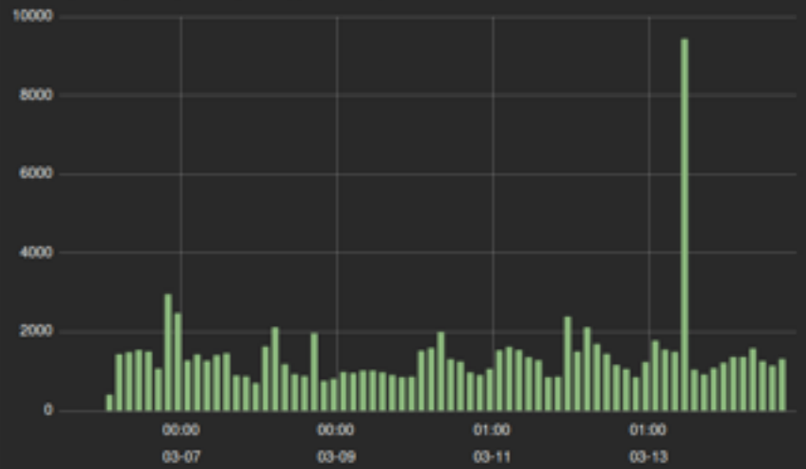
QUERY

*

FILTERING

EVENTS OVER TIME

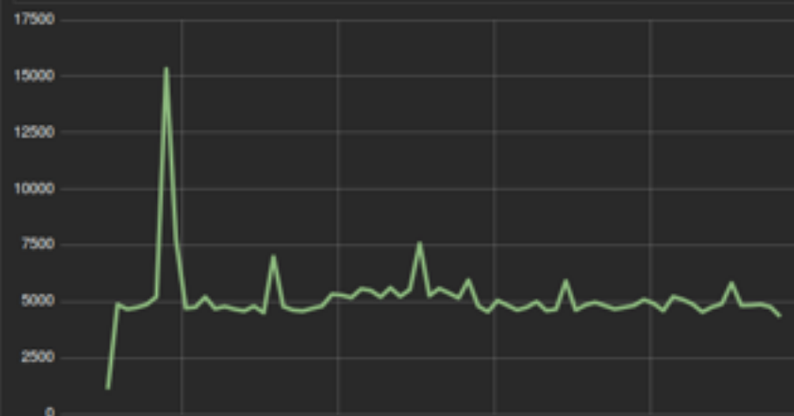
View | * (99468) count per 3h | (99468 hits)



BANDWIDTH (MEGABYTES)

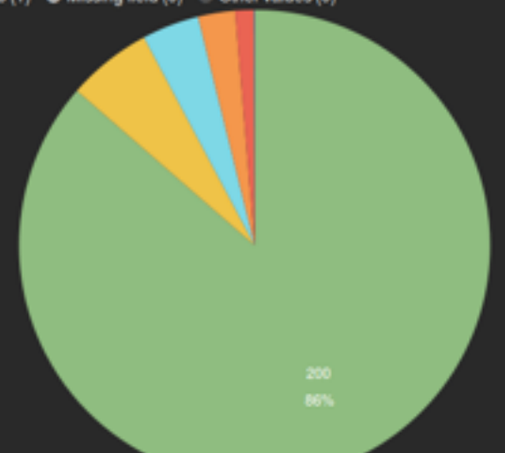
View | * (99468) bytes total per 3h | (99468 hits)

Bars Lines Stack Percent Legend Interval 3h (auto



HTTP STATUS

200 (85935) 404 (5787) 301 (3897) 206 (2532) 304 (1264) 403 (46) 400 (5)
500 (1) 416 (1) Missing field (0) Other values (0)



TOP URLS

Term	Count	Action
/files/logstash/logstash-1.1.0-monolithic.jar	8642	
/favicon.ico	5677	
/style2.css	3981	
/reset.css	3948	
/images/jordan-80.png	3791	
/images/web/2009/banner.png	3726	
/blog/tags/puppet?flav=rss20	3339	
/	1637	
/presentations/fpm-scale12x.pdf	1404	
/?flav=rss20	1027	
Missing field	7	
Other values	62287	

TOP IPS

Term	Count	Action
177.135.170.179	7862	
202.43.182.16	2599	
46.105.14.53	2490	
81.144.138.34	2325	
66.249.73.135	1712	
128.30.28.58	1235	
115.100.62.170	1215	
5.9.112.68	1001	
208.115.113.88	763	
208.115.111.72	729	
Missing field	0	
Other values	77537	

TOP REFERRERS

Term	Count	Action
"-"	57974	
"http://semicomplete.com/presentations/logstash-puppetconf-2012/"	5890	
"http://www.semicomplete.com/projects/xdotool/"	3582	
"http://semicomplete.com/presentations/logstash-scale11x/"	2998	
"http://www.semicomplete.com/articles/dynamic-dns-with-dhcp/"	2420	
"http://www.semicomplete.com/"	2158	
"http://semicomplete.com/presentations/logstash-monitorama-2013/"	1483	
"http://www.semicomplete.com/style2.css"	1138	
"http://www.semicomplete.com/blog/geekery/ssl-latency.html"	1003	
"http://semicomplete.com/"	925	
Missing field	705	
Other values	19192	

ADD A ROW

Use Cases

Use Cases

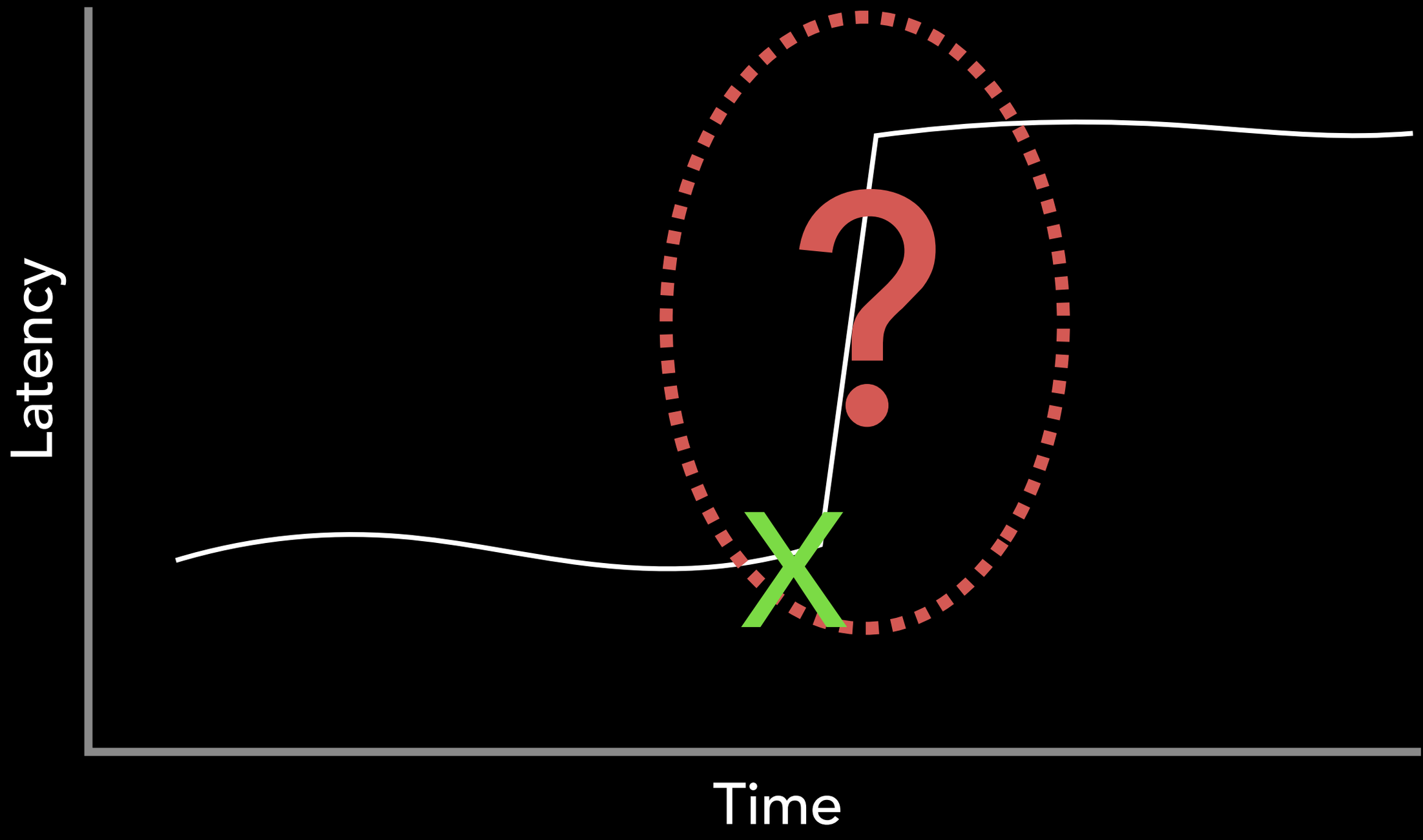
Share Logs with Your Tech Support Team

Graph all things!

Use Cases

Exploration by Non-Technical Users

Troubleshooting Latency



Use Cases

Movie Releases Demo

Apache Logs Demo