

BEYOND GREP

Pragmatic Logging & Metrics

Hynek Schlawack



ПРИВЕТ!

@hynek

https://hynek.me

https://github.com/hynek

NAUMEN 2

NAUMEN

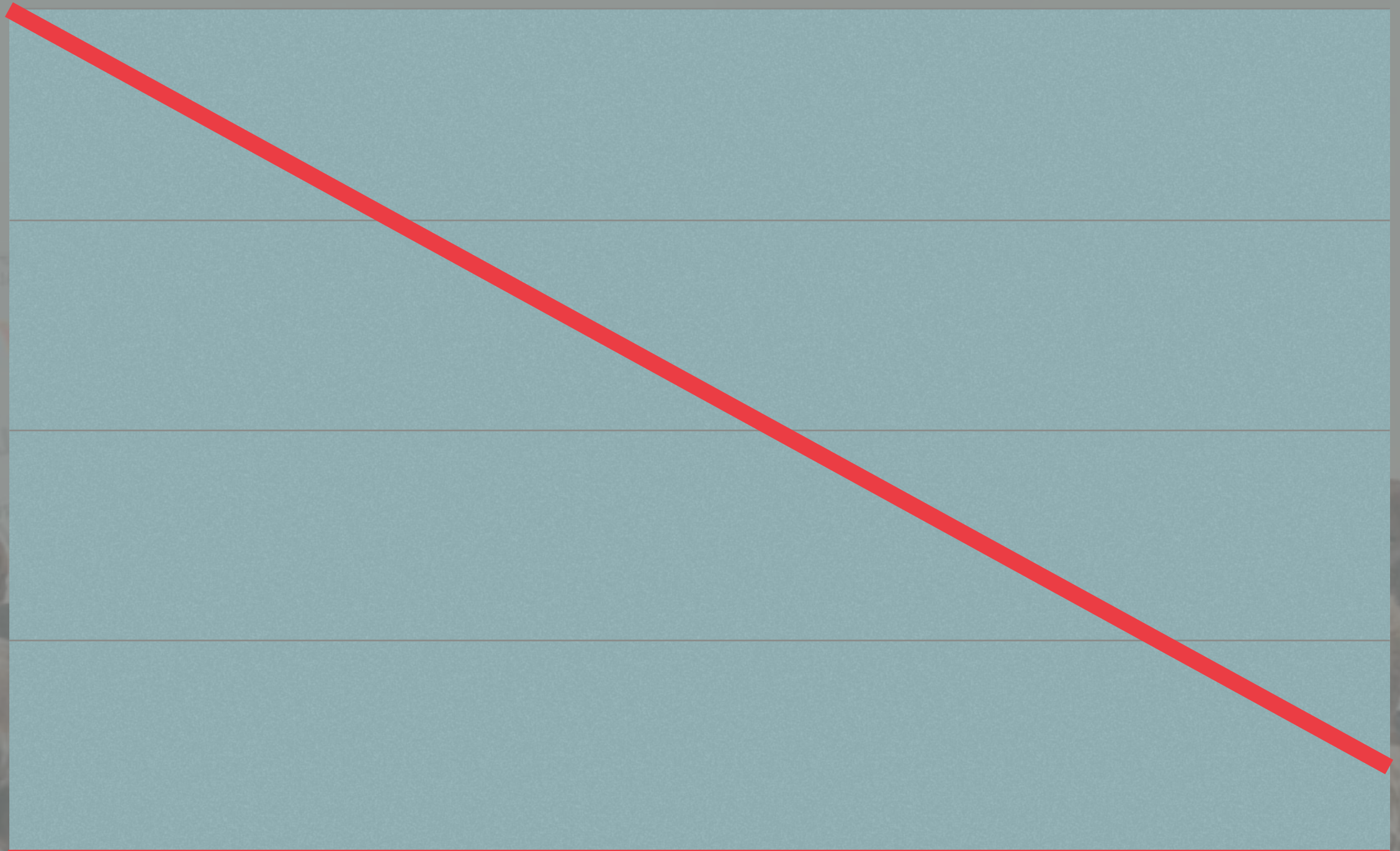
NAUMEN

NAUMEN

NAUMEN



Speaking Speed vs Wi-Fi Speed



Wi-Fi Speed

Speaking Speed



<https://www.variomedia.de>

OX.CX/B

GOALS

GOALS



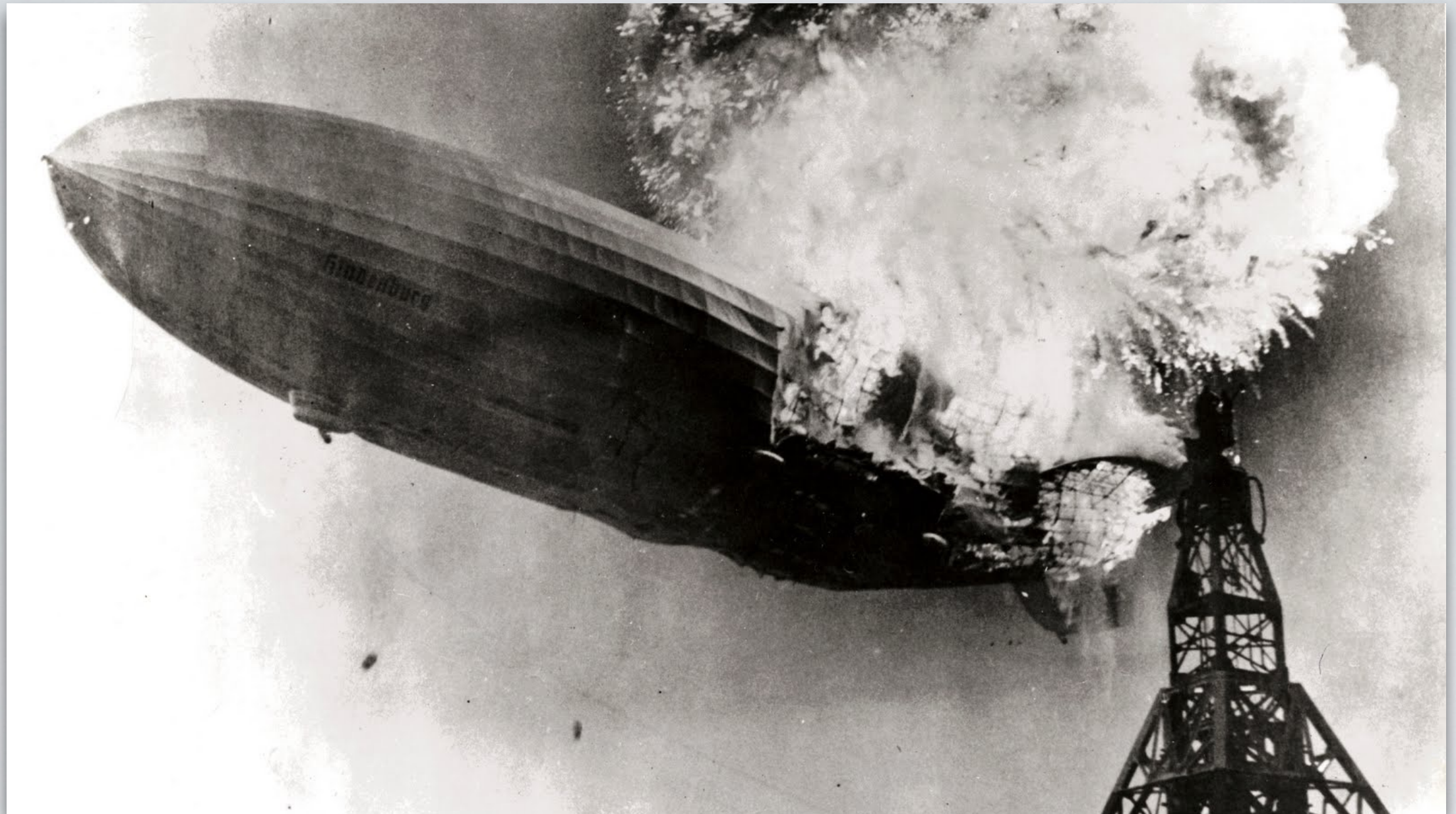
GOALS



GOALS



ERRORS



ERRORS

REQUIREMENTS

REQUIREMENTS

- fast

REQUIREMENTS

- fast
- once

13,678



- fa

- Or

REQUIREMENTS


- fast
- once


REQUIREMENTS

- fast
- once
- context

***** Icinga *****

Notification Type: PROBLEM

Service: HTTPS: domains. 

Host: c-0518. 

Address: 10.6.5.24

State: CRITICAL

Date/Time: Wed Mar 4 06:14:18 CET 2015

Additional Info:

CRITICAL - 2 plugins checked, 1 critical (eu), 1 ok



Sentry
















Sentry is a realtime, platform-agnostic error logging and aggregation platform <https://getsentry.com>

7,393 commits
47 branches
264 releases
200 contributors

branch: master
sentry / +

Simplify/clarify description

 **dcramer** authored 20 hours ago
 latest commit `aff2a28be0`

 <code>.tx</code>	Explicit source file	2 years ago
 <code>bin</code>	Add release to mocks	10 days ago
 <code>docs</code>	Simplify/clarify description	20 hours ago
 <code>hooks</code>	Add js linting to pre-commit	10 months ago
 <code>src/sentry</code>	Add error to example data	2 days ago
 <code>tests</code>	Update tests for safe_urlopen usage	2 days ago
 <code>.bowerrc</code>	JS refactor	2 months ago
 <code>.coveragerc</code>	Better make coverage	2 years ago
 <code>.gitignore</code>	Ignore celerybeat-schedule	a month ago
 <code>.gitmodules</code>	JS refactor	2 months ago
 <code>.jshintignore</code>	Update clean behavior	2 months ago
 <code>.jshintrc</code>	JS refactor	2 months ago
 <code>.travis.yml</code>	Remove coverage reports from Travis	a month ago
 <code>AUTHORS</code>	Move sentry repo	3 years ago
 <code>CHANGES</code>	Changes for 7.3.2	3 days ago

<> Code

 Issues 187


 Pull Requests 12

 Pulse

 Graphs

SSH clone URL

`git@github.com:getsentry/sentry` 

You can clone with [HTTPS](#), [SSH](#), or [Subversion](#). 

 Clone in Desktop

 Download ZIP

All accounts start with a 14-day no-obligation free trial.

\$24_{/mo}

Small

30 day history

25 events per minute
(approx 36.000 per day)

Unlimited members

Unlimited projects

Start free

\$79_{/mo}

Medium

90 day history

50 events per minute
(approx 72.000 per day)

Unlimited members

Unlimited projects

Start free

\$199_{/mo}

Large

90 day history

200 events per minute
(approx 288.000 per day)

Unlimited members

Unlimited projects

Start free

Limited – 7 day history, 250 events per day, no team members

[Sign up for the Limited plan](#)

Individual (\$9/month) – 30 day history, 10 events per min, no team members

[Sign up for the Individual plan](#)

Looking for more? – Tell us what you need.

[Contact us](#)

All accounts start with a 14-day no-obligation free trial.

\$24_{/mo}

Small

30 day history

25 events per minute
(approx 36,000 per day)

Unlimited members

Unlimited projects

Start free

\$79_{/mo}

Medium

Limited – 7 day history, 250 events per day, no team members

[Sign up for the Limited plan](#)

Start free

\$199_{/mo}

Large

30 day history

25 events per minute
(approx 36,000 per day)

Unlimited members

Unlimited projects

Start free

Limited – 7 day history, 250 events per day, no team members

[Sign up for the Limited plan](#)

Individual (\$9/month) – 30 day history, 10 events per min, no team members

[Sign up for the Individual plan](#)

Looking for more? – Tell us what you need.

[Contact us](#)

Sentry

[View on Sentry](#)

New Event on **tech ael**

ValueError: No JSON object could be decoded

Tags

level = **error**

logger = **root**

server_name = **c-0518**

Exception

```
ValueError: No JSON object could be decoded
  File "ael/parser.py", line 20, in parse_next_line
    return tai64n.decode_tai64n(l[1:25]), json.loads(l[26:])
  File "json/__init__.py", line 338, in loads
    return _default_decoder.decode(s)
  File "json/decoder.py", line 366, in decode
    obj, end = self.raw_decode(s, idx=_w(s, 0).end())
  File "json/decoder.py", line 384, in raw_decode
    raise ValueError("No JSON object could be decoded")
```

Sentry

[View on Sentry](#)



New Event on **tech ael**

ValueError: No JSON object could be decoded

Tags

level = **error**

logger = **root**

server_name = **c-0518**

Exception

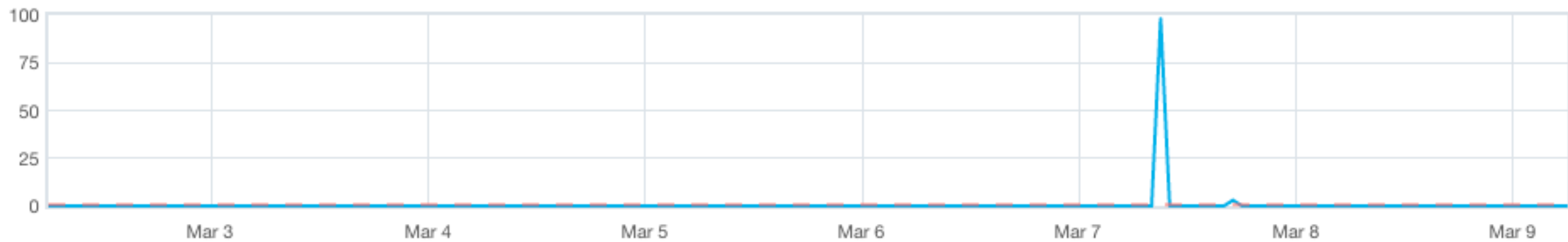
```
ValueError: No JSON object could be decoded
  File "ael/parser.py", line 20, in parse_next_line
    return tai64n.decode_tai64n(l[1:25]), json.loads(l[26:])
  File "json/__init__.py", line 338, in loads
    return _default_decoder.decode(s)
  File "json/decoder.py", line 366, in decode
    obj, end = self.raw_decode(s, idx=_w(s, 0).end())
  File "json/decoder.py", line 384, in raw_decode
    raise ValueError("No JSON object could be decoded")
```




json.decoder in raw_decode

ValueError: No JSON object could be decoded

users 0 2 days ago root



Hynek Schlawack marked this event as resolved — 1 day, 12 hours ago

Add Note

The system marked this event as a regression — 1 day, 12 hours ago

The system first saw this event — 1 day, 21 hours ago

[◀ Newer Sample](#)

Sample at March 7, 2015, 6:43 p.m. [5.2 KB]
ID: d69d8d6fa222496babe1dd8420abe6e5

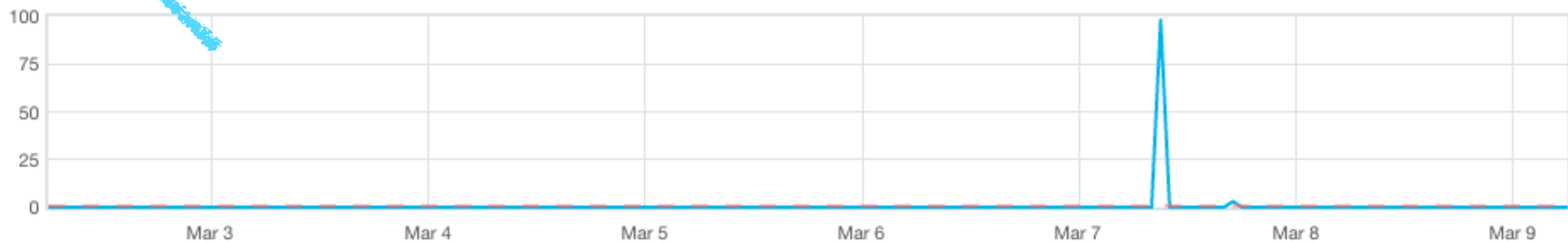
[Older Sample ▶](#)



json.decoder in raw_decode

ValueError: No JSON object could be decoded

users 0 2 days ago root



Hynek Schlawack marked this event as resolved — 1 day, 12 hours ago

Add Note

The system marked this event as a regression — 1 day, 12 hours ago

The system first saw this event — 1 day, 21 hours ago

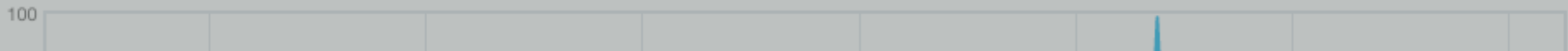
[← Newer Sample](#)

Sample at March 7, 2015, 6:43 p.m. [5.2 KB]
ID: d69d8d6fa222496babe1dd8420abe6e5

[Older Sample ▶](#)



json.decoder in raw_decode
ValueError: No JSON object could be decoded
users 0 2 days ago root





 **Hynek Schlawack** marked this event as resolved — 2015-03-11



 **Hynek Schlawack** marked this event as resolved — 1 day, 12 hours ago

Add Note

 The system marked this event as a regression — 1 day, 12 hours ago

 The system first saw this event — 1 day, 21 hours ago

← Newer Sample

Sample at March 7, 2015, 6:43 p.m. [5.2 KB]
ID: d69d8d6fa222496babe1dd8420abe6e5

Older Sample ►



json.decoder in raw_decode

ValueError: No JSON object could be decoded

users 0 2 days ago root



100



The system marked this event as a regression — 2 days, 6 hours ago

0

Mar 3

Mar 4

Mar 5

Mar 6

Mar 7

Mar 8

Mar 9

Hynek Schlawack marked this event as resolved — 1 day, 12 hours ago

Add Note

The system marked this event as a regression — 1 day, 12 hours ago

The system first saw this event — 1 day, 21 hours ago

◀ Newer Sample

Sample at March 7, 2015, 6:43 p.m. [5.2 KB]

ID: d69d8d6fa222496babe1dd8420abe6e5

Older Sample ▶

Search query or event ID



raven.scripts.runner in main
This is an example Python exception
users 0 3 minutes ago root



The system first saw this event — 2015-02-25 Add Note

Newer Sample Sample at Feb. 25, 2015, 9:56 p.m. [6.2 KB] Older Sample
ID: b994d67e4242448ca985bda4e1602fc1

Tags

Stacktrace Request User Additional Data

Tags

level = error logger = root sentry:release = 4f38b65c62c4565aa94bba391ff8946922a8eed4
browser = Chrome 28.0 device = Other os = Windows 8 url = http://example.com/foo

Stacktrace (most recent call last)

Raw

Aggregate

Tags

Samples

AGGREGATE DETAILS
Status: Unresolved
First Seen: 11 days ago
Last Seen: 3 minutes ago

ACTIONS

- Mute Event
- Share Event
- Raw JSON Data
- Remove Event Data

BROWSER

Chrome 28.0 100%

DEVICE

Other 100%

LEVEL

error 100%

LOGGER

root 100%

Stacktrace (most recent call last)

Raw

raven/base.py ? in build_msg



303. transformer=self.transform)

raven/base.py ? in capture



```

454.         if not self.is_enabled():
455.             return
456.
457.         data = self.build_msg(
458.             event_type, data, date, time_spent, extra, stack, tags=tags,
459.             **kwargs)
460.
461.         self.send(**data)
462.
463.         return (data.get('event_id'),)
464.

```

'data' None

'date' None

'event_type' 'raven.events.Message'

[Expand Context \(6 hidden\)](#)

raven/base.py ? in captureMessage



577. return self.capture('raven.events.Message', message=message, **kwargs)

raven/scripts/runner.py ? in send_test_message



77. 'loadavg': get_loadavg(),

raven/scripts/runner.py ? in main



112. send_test_message(client, extra=dict(

error 100%

LOGGER

root 100%

OS

Windows 8 100%

RELEASE

4f38b65c62c4565aa94bba39... 100%

URL

http://example.com/foo 100%

RAVEN-PYTHON

RAVEN-PYTHON

Transports:

Integrations:

RAVEN-PYTHON

Transports:

- gevent

Integrations:

RAVEN-PYTHON

Transports:

- `gevent`
- `aiohttp`

Integrations:

RAVEN-PYTHON

Transports:

- gevent
- aiohttp
- Twisted

Integrations:

RAVEN-PYTHON

Transports:

- gevent
- aiohttp
- Twisted
- ...8 others

Integrations:

RAVEN-PYTHON

Transports:

- gevent
- aiohttp
- Twisted
- ...8 others

Integrations:

- logging

RAVEN-PYTHON

Transports:

- gevent
- aiohttp
- Twisted
- ...8 others

Integrations:

- logging
- Django

RAVEN-PYTHON

Transports:

- gevent
- aiohttp
- Twisted
- ...8 others

Integrations:

- logging
- Django
- Pyramid

RAVEN-PYTHON

Transports:

- gevent
- aiohttp
- Twisted
- ...8 others

Integrations:

- logging
- Django
- Pyramid
- ...9 others

VANILLA

```
from raven import Client
```

```
client = Client()
```

```
try:
```

```
    1 / 0
```

```
except ZeroDivisionError:
```

```
    client.captureException()
```

VANILLA

```
@client.capture_exceptions  
def foo():  
    raise Exception()
```


DJANGO

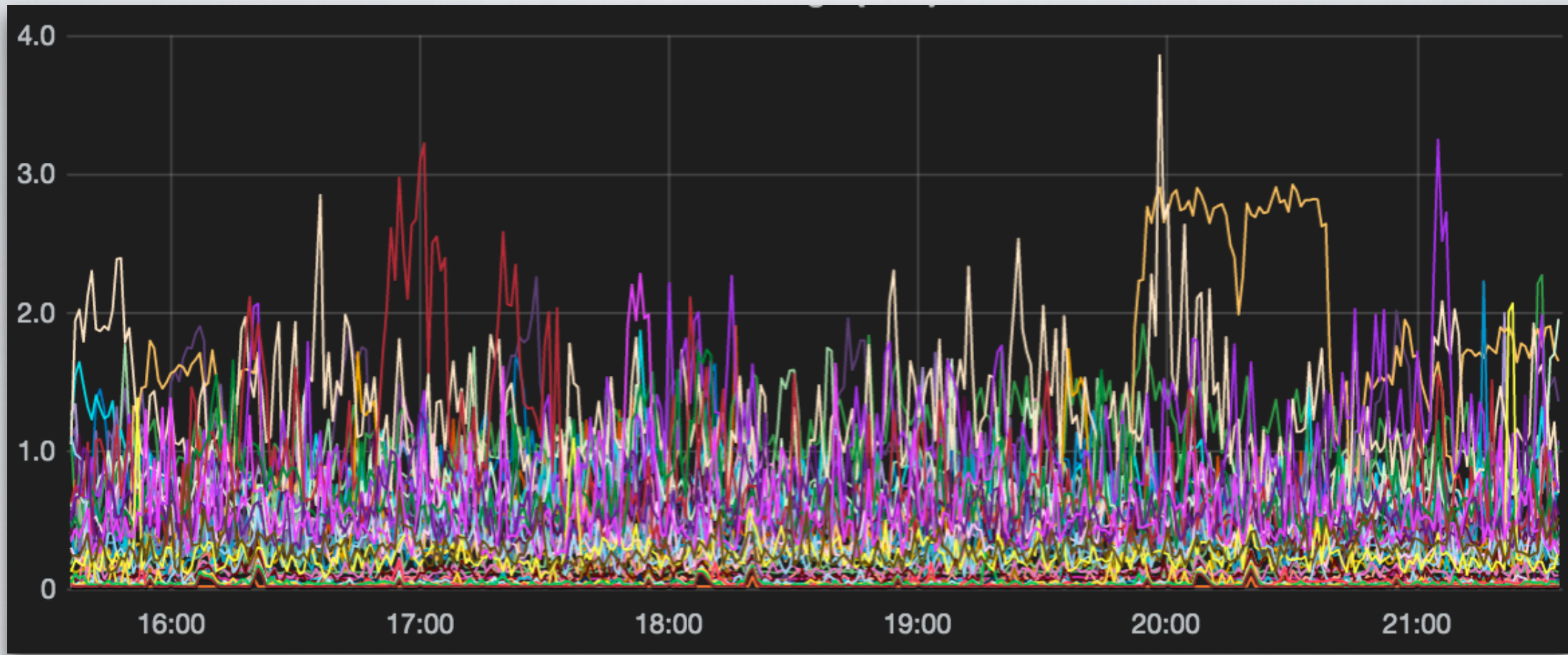
```
INSTALLED_APPS = (  
    ...  
    "raven.contrib.django.raven_compat",  
    ...  
)
```

PROGRESS!



PROGRESS!





METRICS

METRICS?

METRICS?

- numbers in a DB

METRICS?

- numbers in a DB
- difference between guessing & knowing

“Measure. Don’t speculate.”

–D. J. Bernstein

SYSTEM METRICS vs APP METRICS

SYSTEM METRICS vs APP METRICS

- load

SYSTEM METRICS vs APP METRICS

- load
- network traffic

SYSTEM METRICS vs APP METRICS

- load
- network traffic
- I/O

SYSTEM METRICS vs APP METRICS

- load
- network traffic
- I/O
- ...

SYSTEM METRICS vs APP METRICS

- load
- network traffic
- I/O
- ...
- counters

SYSTEM METRICS vs APP METRICS

- load
- network traffic
- I/O
- ...
- counters
- timers

SYSTEM METRICS vs APP METRICS

- load
- network traffic
- I/O
- ...
- counters
- timers
- gauges

SYSTEM METRICS vs APP METRICS

- load
 - network traffic
 - I/O
 - ...
- counters
 - timers
 - gauges
 - ...

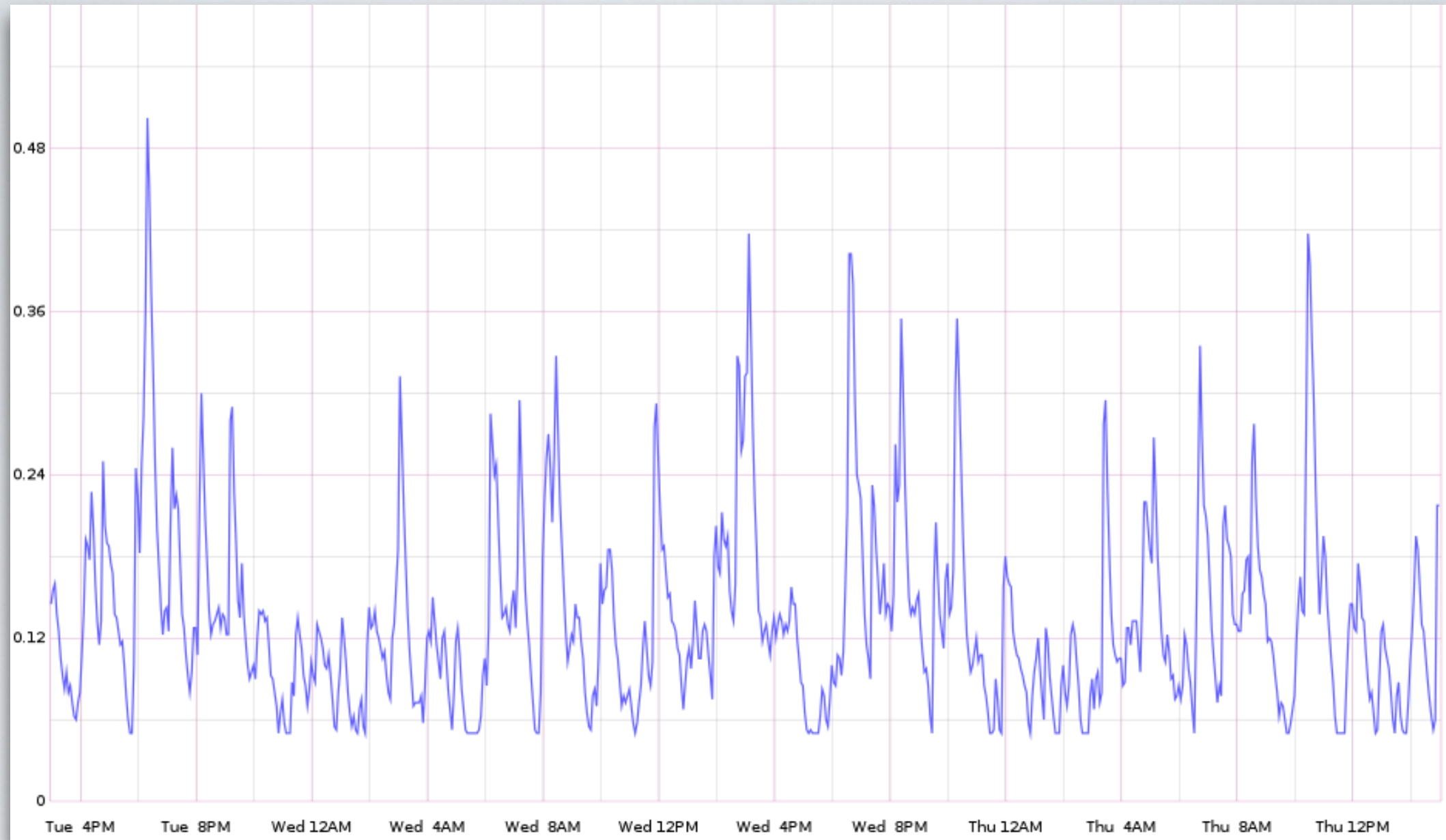
SYSTEM METRICS vs APP METRICS

- load
- network traffic
- I/O
- ...

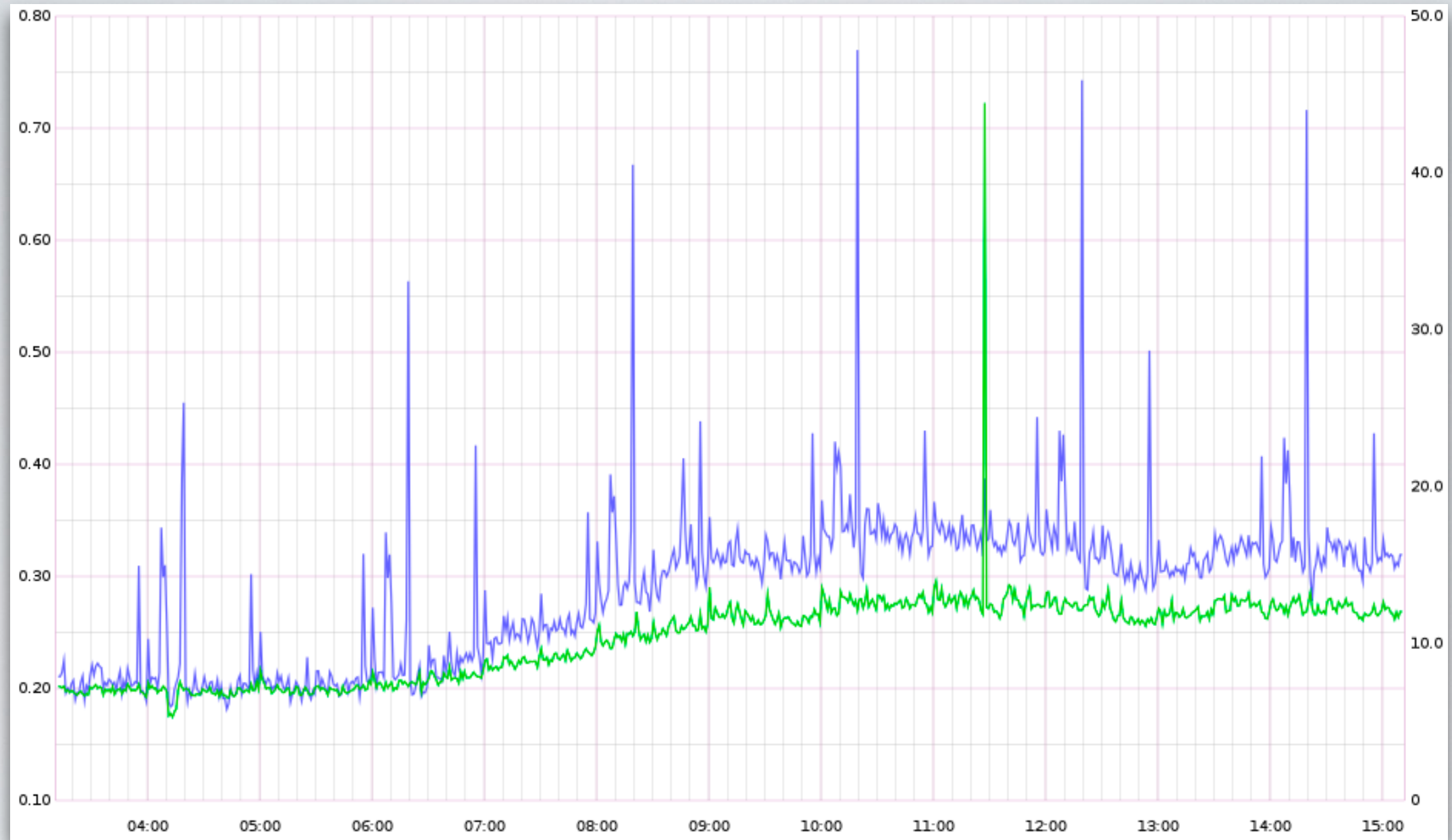
- counters
- timers
- gauges
- ...

load average: 0.18, 0.41, 0.23

AGGREGATION



AGGREGATION



CORRELATION





- # reqs / s?

🪄 MATH 🪄

- # reqs / s?
- worst 0.01% <req time>?

🪄 MATH 🪄

- # reqs / s?
- worst 0.01% <req time>?
- don't try this ~~at home~~ alone!

MONITORING

MONITORING

- latency

MONITORING

- latency
- error rates

MONITORING

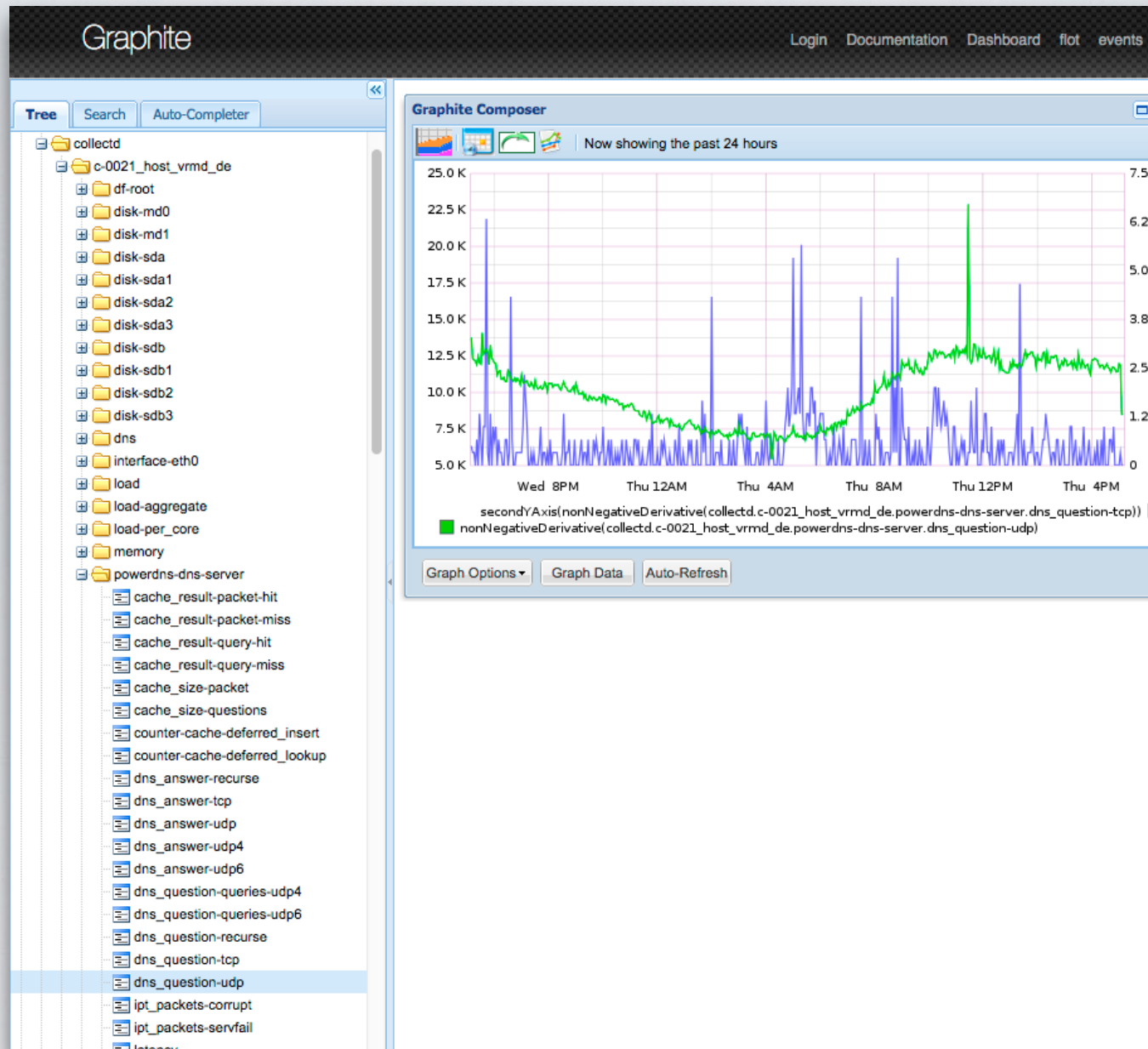
- latency
- error rates
- anomalies

STORAGE

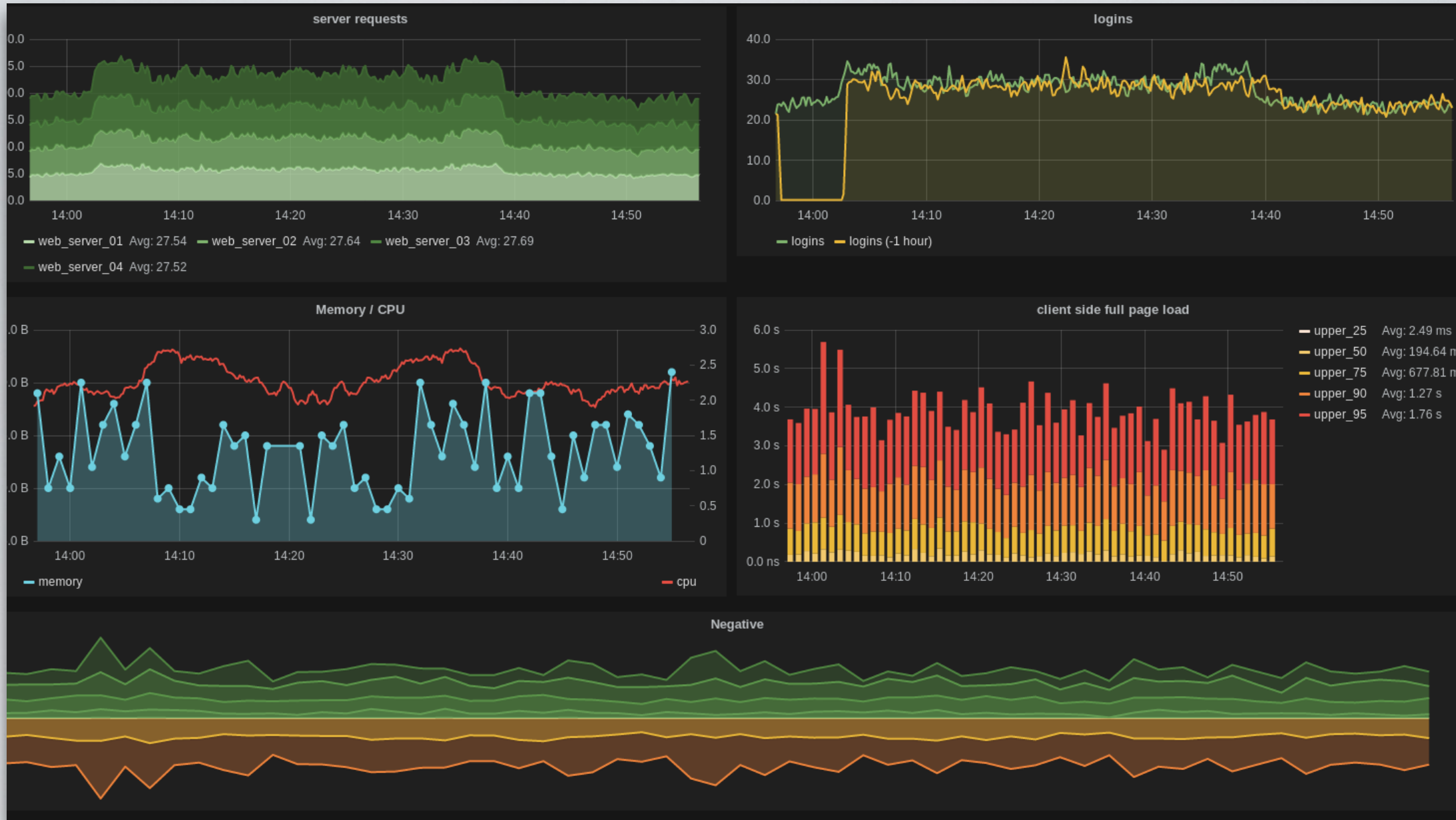


LIBRATO METRICS





GRAPHITE
800 pound gorilla



GRAFANA

InfluxDB Documentation x InfluxDB Administration x

localhost:8083

InfluxDB Databases Cluster Admins Cluster root localhost:8086 Disconnect

Data Interface

Read Points

Query

```
select count(customerId) from customer_events where time > now() - 1d group by time(10m)
```

InfluxDB features a [SQL-like query language](#)

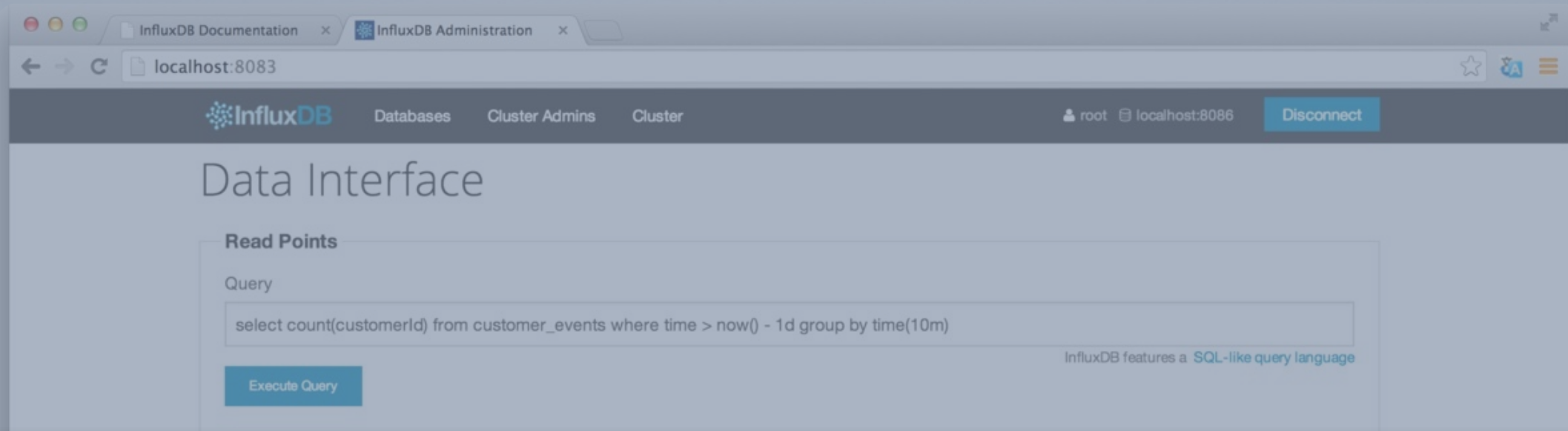
Execute Query

customer_events

time	count
1400365200000	19

INFLUXDB

Graphite++ in Go



Read Points

Query

```
select count(customerId) from customer_events where time > now() - 1d group by time(10m)
```

Execute Query

INFLUXDB

Graphite++ in Go

COLLECTING

APPROACHES

APPROACHES

1. external aggregation: **StatsD**, **Riemann**

APPROACHES

1. external aggregation: **StatsD**, **Riemann**

+ no state, simple

APPROACHES

1. external aggregation: **StatsD**, **Riemann**

+ no state, simple

— no direct introspection

APPROACHES

1. external aggregation: **StatsD**, **Riemann**
 - + no state, simple
 - no direct introspection
2. aggregate in-app, deliver to DB

APPROACHES

1. external aggregation: **StatsD**, **Riemann**
 - + no state, simple
 - no direct introspection
2. aggregate in-app, deliver to DB
 - + in-app dashboard, useful in dev

APPROACHES

1. external aggregation: **StatsD**, **Riemann**
 - + no state, simple
 - no direct introspection
2. aggregate in-app, deliver to DB
 - + in-app dashboard, useful in dev
 - state w/i app



(G|PY)?**STATSD**(PY|-CLIENT)?

```
import statsd
```

```
c = statsd.StatsClient("statsd.local", 8125)  
c.incr("foo")  
c.timing("stats.timed", 320)
```


SCALES

```
from greplin import scales
from greplin.scales.meter import MeterStat

STATS = scales.collection(
    "/Resource",
    MeterStat("reqs"),
    scales.PmfStat("request_time")
)
# ...
STATS.reqs.mark()
with STATS.request_time.time():
    do_something_expensive()
```

SCALES

```
from greplin import scales
from greplin.scales.meter import MeterStat

STATS = scales.collection(
    "/Resource",
    MeterStat("reqs"),
    scales.PmfStat("request_time")
)
# ...
STATS.req.mark()
with STATS.request_time.time():
    do_something_expensive()
```

SCALES

```
from greplin import scales
from greplin.scales.meter import MeterStat
```

```
STATS = scales.collection(
    "/Resource",
    MeterStat("reqs"),
    scales.PmfStat("request_time")
)
```

```
#
```

```
STATS.reqs.mark()
with STATS.request_time.time():
    do_something_expensive()
```


Stats

WebAuth

Filter:

Resource

reqs

count 556647316

m1 47.6511883627

m15 50.2568959651

m5 49.6021883021

unit per second

reqs.disabled

count 155594

m1 1.64813883819e-62

m15 5.91172455476e-07

m5 1.39446831144e-14

unit per second

DASHBOARD

Scales

Stats

WebAuth

Filter:

Resource

reqs

count 556647316

m1 47.6511883627

m15 50.2568959651

m5 49.6021883021

unit per second

reqs.disabled

count 155594

m1 1.64813883819e-62

m15 5.91172455476e-07

m5 1.39446831144e-14

unit per second

request_time

75percentile 0.0127675533295

95percentile 0.0261434435844

98percentile 0.0834807777405

999percentile 0.145731252193

99percentile 0.0982514739037

count 556646541

max 30.1348221302

mean 0.0125761426376

median 0.00910007953644

min 0.000244855880737

stddev 0.0149146688535

DASHBOARD

Scales


```
...
  "request_time": {
    "count": 567315293,
    "99percentile": 0.10978688716888428,
    "75percentile": 0.013181567192077637,
    "min": 0.0002448558807373047,
    "max": 30.134822130203247,
    "98percentile": 0.08934824466705339,
    "95percentile": 0.027234303951263434,
    "median": 0.009176492691040039,
    "999percentile": 0.14235656142234793,
    "stddev": 0.01676855570363413,
    "mean": 0.013247184020535955
  },
...
```

DASHBOARD

Scales


```
from greplin.scales import graphite

pusher = graphite.GraphitePeriodicPusher(
    "graphite.host",
    2003,
    period=30,
    prefix="yourapp",
)
pusher.allow("**")
pusher.start()
```



PROGRESS!



PROGRESS!

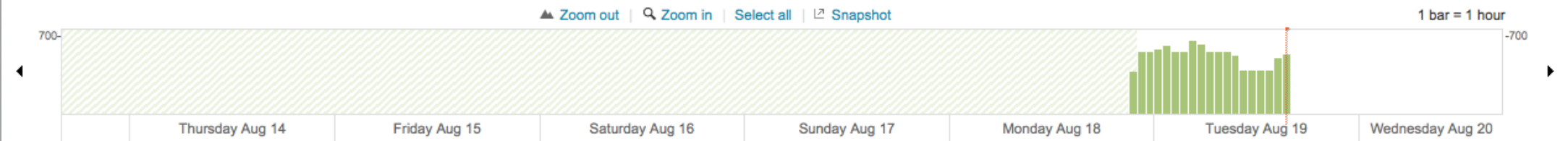




LOGGING

>10,000 results in the past 7 days | Report on results »

Show timeline



Fields | eventtype (≥11) | host (≥2) | name (≥5) | process (≥2) | punct (≥36) | source (≥6) | sourcetype (≥4) | src_ip (≥7) | src_port (≥1,533) | Show fields | Wrap results | Lines per event: 10

08/19/08 15:45:15	Aug 19 15:45:15 virt2 kernel: PASS IN=eth0 OUT= MAC=42:a0:7d:30:03:97:00:15:c5:e0:b4:66:08:00 SRC=8.2.22.121 DST=10.2.1.222 LEN=40 TOS=0x00 PREC=0x00 TTL=41 ID=26214 PROTO=TCP SPT=51699 DPT=80 WINDOW=2048 RES=0x00 ACK URGP=0 eventtypes= firewall-accept communicate firewall host pass success Private-address communicate private source= /home/ram/j2eedata/var/log/messages host= virt2 sourcetype= syslog process= kernel src_ip= 8.2.22.121 src_port= 51699 punct: __:__:__==_=:_____=_...=_...=____=____=
08/19/08 15:45:15	Aug 19 15:45:15 virt2 kernel: PASS IN=eth0 OUT= MAC=42:a0:7d:30:03:97:00:15:c5:e0:b4:66:08:00 SRC=10.2.1.48 DST=10.2.1.222 LEN=40 TOS=0x00 PREC=0x00 TTL=40 ID=61579 PROTO=TCP SPT=51699 DPT=80 WINDOW=1024 RES=0x00 ACK URGP=0 eventtypes= firewall-accept communicate firewall host pass success Private-address communicate private source= /home/ram/j2eedata/var/log/messages host= virt2 sourcetype= syslog process= kernel src_ip= 10.2.1.48 src_port= 51699 punct: __:__:__==_=:_____=_...=_...=____=____=
08/19/08 15:45:06	Insecure Protocol Aug 19 15:45:06 virt2 kernel: BLOCK IN=eth0 OUT= MAC=42:a0:7d:30:03:97:00:15:c5:e0:b4:66:08:00 SRC=212.213.144.88 DST=10.2.1.222 LEN=40 TOS=0x00 PREC=0x00 TTL=51 ID=27363 PROTO=TCP SPT=47184 DPT=110 WINDOW=4096 RES=0x00 SYN URGP=0 eventtypes= Insecure-Ports application communicate insecure service Private-address communicate private source= /home/ram/j2eedata/var/log/messages host= virt2 sourcetype= syslog process= kernel src_ip= 212.213.144.88 src_port= 47184 punct: __:__:__==_=:_____=_...=_...=____=____=
08/19/08 15:45:06	Insecure Protocol Aug 19 15:45:06 virt2 kernel: BLOCK IN=eth0 OUT= MAC=42:a0:7d:30:03:97:00:15:c5:e0:b4:66:08:00 SRC=10.2.1.48 DST=10.2.1.222 LEN=40 TOS=0x00 PREC=0x00 TTL=44 ID=27363 PROTO=TCP SPT=47184 DPT=110 WINDOW=1024 RES=0x00 SYN URGP=0 eventtypes= Insecure-Ports application communicate insecure service Private-address communicate private source= /home/ram/j2eedata/var/log/messages host= virt2 sourcetype= syslog process= kernel src_ip= 10.2.1.48 src_port= 47184 punct: __:__:__==_=:_____=_...=_...=____=____=

SPLUNK



Application Management (123)

Monitor and troubleshoot your development and production applications.



S.o.S - Splunk on Splunk



Splunk Add-on for Unix and Linux



Splunk Support for Active Directory



Splunk 5.x App for Active Directory

Security and Compliance (227)

Improve your security posture, speed incident investigations and meet your compliance mandates.



Cisco Security Suite



Splunk for Palo Alto Networks



Reporting and Management for OSSEC



Cisco Networks

Utilities (217)

Extend visualizations, data integrations, and search and field extraction utils.



Google Maps



Sideview Utils (LGPL)



Splunk DB Connect



PDF Report Server - install on Linux only

IT Operations Management (228)

Provide end-to-end visibility across IT infrastructure including virtualization, servers, storage and network elements



Splunk 5.x App for Microsoft Windows



Splunk App for Unix and Linux



Splunk Add-on for Microsoft Windows



Geo Location Lookup Script (powered by MAXMIND)

Business Analytics (43)

Harness your machine data to gain valuable real-time insight for IT and the business.



Splunk for Excel Export



Splunk ODBC



Sideview Web Analytics



Splunk Hadoop Connect

Cool Stuff (135)

Integrations with popular social media networks, visualizations for interesting data sets, outside of the box uses of Splunk.



Splunk 6.x Dashboard Examples



Web Page Monitor



AfterGlow Visualization



Ocean Theme


```
Mar 24 14:02:50 bigproduct-web1 tomcat.log: 127.0.0.1 - - "GET /secure/Setup!input.jspa?title=Your+Company+ITRA&mode=public HTTP/1.1" 200 24678 4.885
39F9C7F048F7F060A4B9883A7348082D
Mar 24 14:02:50 bigproduct-web1 tomcat.log: 127.0.0.1 - - "GET /styles/global.css HTTP/1.1" 200 548 0.001 39F9C7F048F7F060A4B9883A7348082D
Mar 24 14:02:50 bigproduct-web1 tomcat.log: 127.0.0.1 - - "GET /secure/Setup!input.jspa?title=Your+Company+ITRA&mode=public HTTP/1.1" 200 24678 0.443
39F9C7F048F7F060A4B9883A7348082D
Mar 24 14:02:50 bigproduct-web1 tomcat.log: 127.0.0.1 - - "GET /styles/global.css HTTP/1.1" 200 548 0.001 39F9C7F048F7F060A4B9883A7348082D
Mar 24 14:02:50 bigproduct-web1 tomcat.log: 127.0.0.1 - - "GET /includes/js/combined-javascript.js HTTP/1.1" 200 65508 1.712
39F9C7F048F7F060A4B9883A7348082D
Mar 24 14:02:50 bigproduct-web1 tomcat.log: 127.0.0.1 - - "GET /includes/js/combined-javascript.js HTTP/1.1" 200 65508 4.386
39F9C7F048F7F060A4B9883A7348082D
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 06:54:51 * Server started, Redis version 2.2.1
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 06:54:51 * The server is now ready to accept connections on port 6379
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:07 - 5 clients connected (0 slaves), 78612881 bytes in use
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:12 - DB 0: 6233 keys (0 volatile) in 8749 slots HT.
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:13 - Client closed connection
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:13 - Client closed connection
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:12 - 5 clients connected (0 slaves), 78612181 bytes in use
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:13 - Client closed connection
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:13 - Client closed connection
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:13 - Client closed connection
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:17 - 0 clients connected (0 slaves), 78211238 bytes in use
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:17 - DB 0: 6330 keys (0 volatile) in 8920 slots HT.
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:22 - 0 clients connected (0 slaves), 78211238 bytes in use
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:23 - Accepted 14.136.7.12:49059
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:23 - Accepted 14.136.7.12:49060
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:23 - Accepted 14.136.7.12:49057
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:23 - Accepted 14.136.7.12:49061
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:23 - Accepted 14.136.7.12:49058
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:27 - DB 0: 6337 keys (0 volatile) in 8922 slots HT.
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:27 - 5 clients connected (0 slaves), 78612802 bytes in use
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:32 - DB 0: 6337 keys (0 volatile) in 8922 slots HT.
Mar 24 14:05:18 nyc-redis1 redis.log: [8062] 07:34:32 - 5 clients connected (0 slaves), 78612802 bytes in use
Mar 24 14:11:07 staging-web1 catalina: [info] org.apache.catalina.core.StandardEngine.start:2150: Starting Servlet Engine: org.apache.catalina.core.StandardEngine
Mar 24 14:11:07 staging-web1 catalina: [info] org.apache.catalina.core.StandardEngine.start:2150: Starting Servlet Engine: org.apache.catalina.core.StandardEngine
Mar 24 14:11:07 staging-web1 catalina: [info] org.apache.catalina.core.StandardEngine.start:2150: Starting Servlet Engine: org.apache.catalina.core.StandardEngine
Mar 24 14:11:07 staging-web1 catalina: [info] org.apache.catalina.core.StandardEngine.start:2150: Starting Servlet Engine: org.apache.catalina.core.StandardEngine
Mar 24 14:11:07 staging-web1 catalina: [info] org.apache.catalina.core.StandardEngine.start:2150: Starting Servlet Engine: org.apache.catalina.core.StandardEngine
```

Scroll for older events

Seek to a day & time

Search for anything

3pm yesterday [x] Seek To
See Examples or Hide Sun Jan 29 2012 3:00 PM

Realttime tail

PAPERTRAIL



loggly Dashboards Search Alerts Source Setup sample@loggly.com Help

*Apache + New

All Sources apache.status:404 Last 10 minutes Search

Applied Filters: logtype: apache

Field Explorer Apache

- host
- referer
- remoteAddr
- requestMethod
- requestURI
- status
- userAgent
- XForwardedFor

290 events Jul 9

View: Collapsed Events Sorting: Descending

2014-07-09 16:39:35.476 UTC	107.20.0.0	-	-	[05/Jul/2013:00:04:58 +0000]	"GET /lb.txt HTTP/1.0"	404	16649	"-"	"-"	UdYNqn8AAAAEAADnEYacAAAAQ 33390 X-Forwarded-For= Host=hoover
2014-07-09 16:39:35.476 UTC	107.20.0.0	-	-	[05/Jul/2013:00:04:58 +0000]	"GET /lb.txt HTTP/1.0"	404	16649	"-"	"-"	UdYNqn8AAAAEAAB148QYAAAFG 35855 X-Forwarded-For= Host=hoover
2014-07-09 16:39:35.475 UTC	107.20.0.0	-	-	[05/Jul/2013:00:04:56 +0000]	"GET /lb.txt HTTP/1.0"	404	16649	"-"	"-"	UdYNqH8AAAAEAADnEYaYAAAF 38024 X-Forwarded-For= Host=hoover
2014-07-09 16:39:35.475 UTC	107.20.0.0	-	-	[05/Jul/2013:00:04:56 +0000]	"GET /lb.txt HTTP/1.0"	404	16649	"-"	"-"	UdYNqH8AAAAEAAB148QQAFAFJ 40325 X-Forwarded-For= Host=hoover
2014-07-09 16:39:35.475 UTC	107.20.0.0	-	-	[05/Jul/2013:00:04:54 +0000]	"GET /lb.txt HTTP/1.0"	404	16649	"-"	"-"	UdYNqn8AAAAEAAB148QMAAFA 40073 X-Forwarded-For= Host=hoover
2014-07-09 16:39:35.475 UTC	107.20.0.0	-	-	[05/Jul/2013:00:04:54 +0000]	"GET /lb.txt HTTP/1.0"	404	16649	"-"	"-"	UdYNqn8AAAAEAADnEYaUAAAA 43621 X-Forwarded-For= Host=hoover
2014-07-09 16:39:35.475 UTC	107.20.0.0	-	-	[05/Jul/2013:00:04:52 +0000]	"GET /lb.txt HTTP/1.0"	404	16649	"-"	"-"	UdYNqH8AAAAEAAB148PaAAAFN 35645 X-Forwarded-For= Host=hoover
2014-07-09 16:39:35.475 UTC	107.20.0.0	-	-	[05/Jul/2013:00:04:52 +0000]	"GET /lb.txt HTTP/1.0"	404	16649	"-"	"-"	UdYNqH8AAAAEAADnEYaEAAAAS 39885 X-Forwarded-For= Host=hoover

LOGGLY



kibana Discover Visualize Dashboard Settings June 1st 2011, 00:16:26.010 to May 7th 2013, 14:29:14.931

+article 700,316 hits

Selected Fields: _source

Fields: agent, # bytes, † geo.city, † geo.coordinates, † geo.country_code, † @timestamp, † _id, † _index, † _type, † creation_time, † destination, † geo.region, † referrer, † request, † timezone, † user

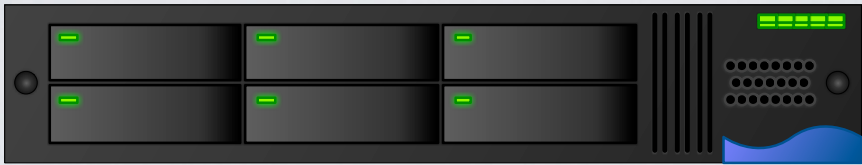
Time	_source
▶ May 7th 2013, 14:29:02.000	referrer: http://www.spk.usace.army.mil/Media/NewsReleases/tabid/1034/Article/13480/corps-releases-inspection-rating-sacramento-river-west-bank-levees.aspx @timestamp: May 7th 2013, 14:29:02.000 creation_time: May 7th 2012, 14:15:25.000 agent: Mozilla/5.0 (windows NT 6.1; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0 bytes: 379990 geo.country_code: US geo.city: Fort Huachuca geo.region: AZ geo.coordinates: {"lat":31.5273,"lon":-110.360703} timezone: America/Phoenix request: http://bit.ly/JMGCUW destination: http://www.spk.usace.army.mil/M
▼ May 7th 2013, 14:28:50.000	destination: http://www.spk.usace.army.mil/Media/NewsReleases/tabid/1034/Article/13480/corps-releases-inspection-rating-sacramento-river-west-bank-levees.aspx @timestamp: May 7th 2013, 14:28:50.000 creation_time: May 3rd 2013, 12:01:44.000 agent: Mozilla/5.0 (windows NT 6.1; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0 bytes: geo.country_code: US geo.city: Fort Huachuca geo.region: AZ geo.coordinates: {"lat":31.5273,"lon":-110.360703} timezone: America/Phoenix request: http://1.usa.gov/18ikFnb user: usacesacramento referrer: direct

Table JSON [Link to /usagov/log/AUuEF4d3npiyxElinDkv](#)

⊙ @timestamp 🔍 May 7th 2013, 14:28:50.000

ELK

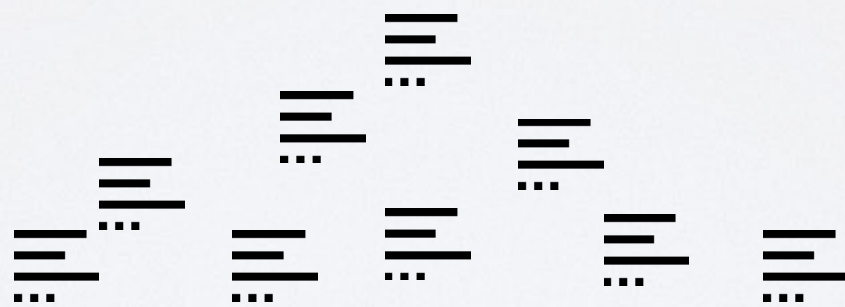
Elasticsearch + Logstash + Kibana





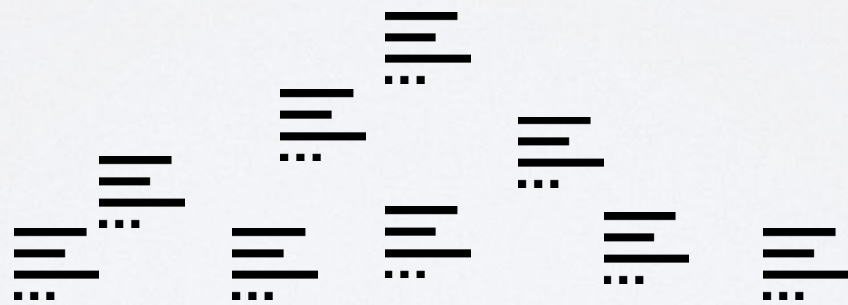


Logstash





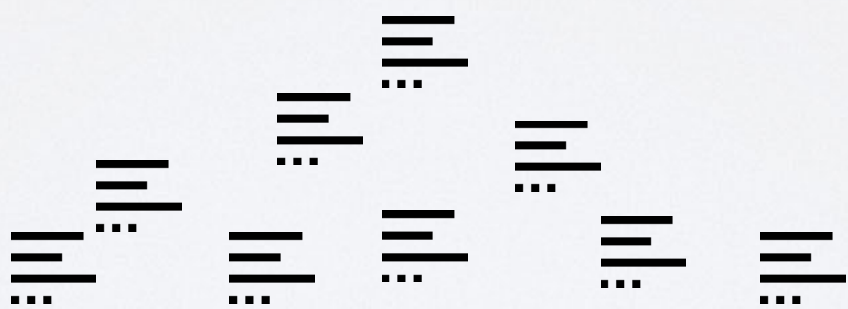
Logstash



Elasticsearch



Logstash

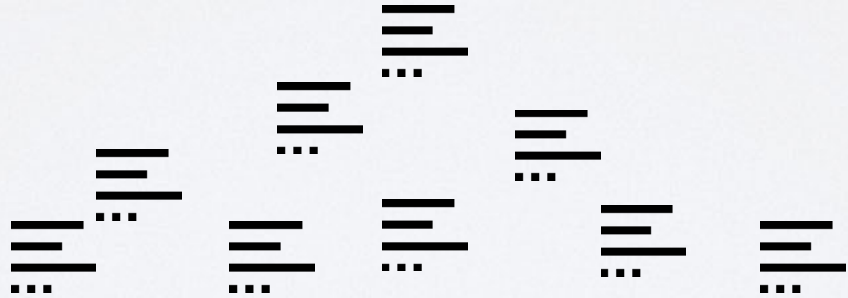


Elasticsearch

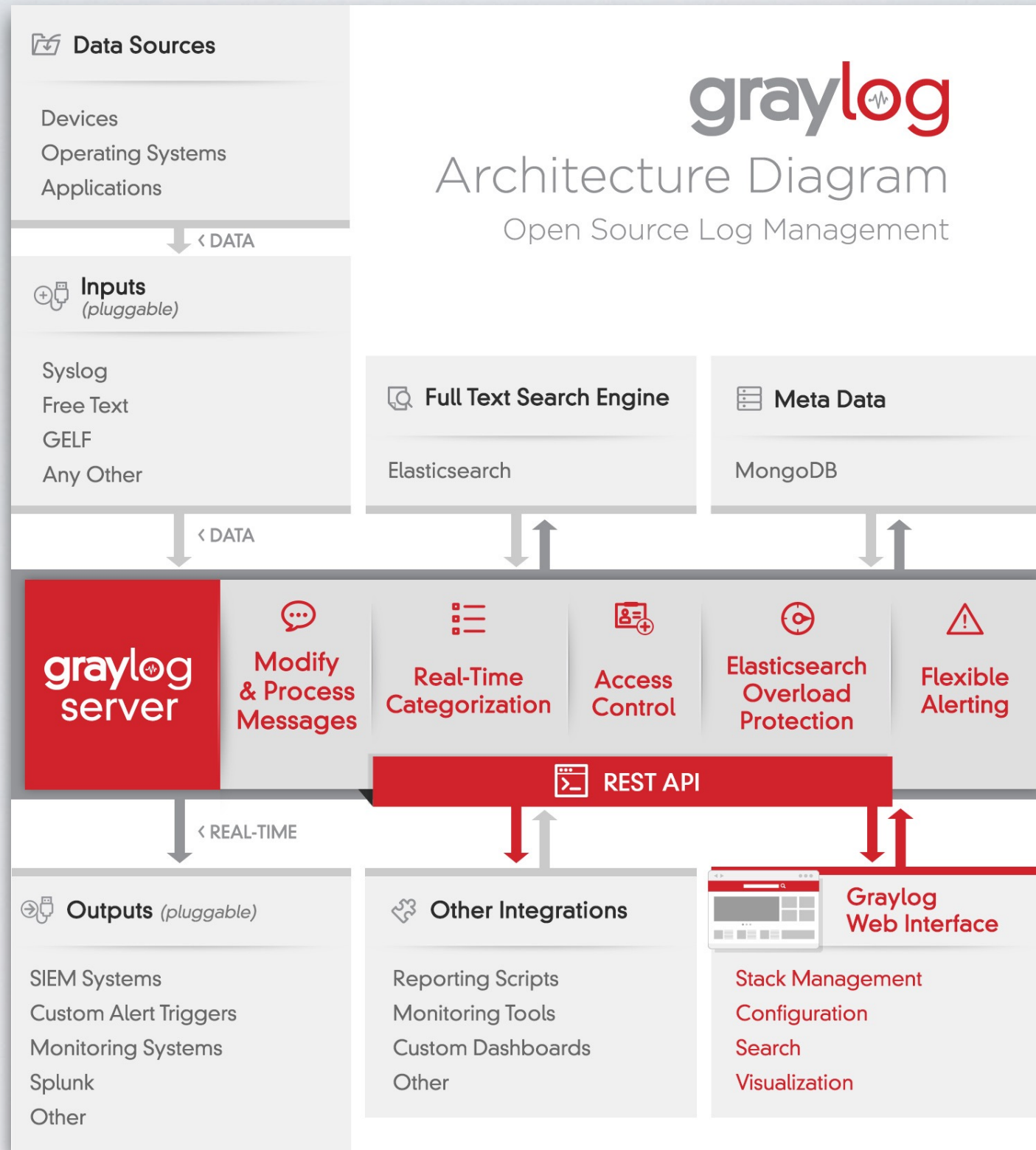


Logstash

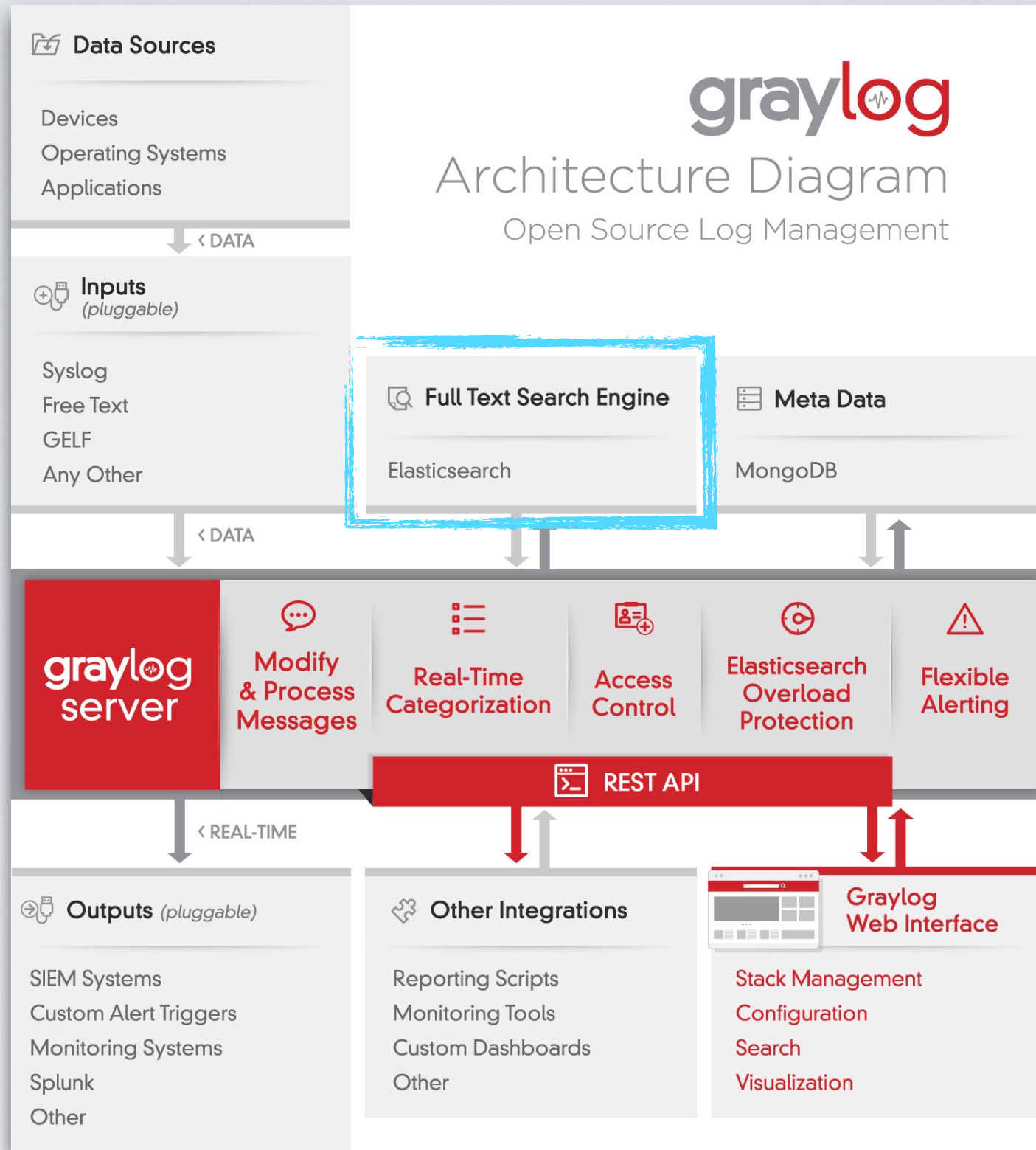
Kibana



Elasticsearch



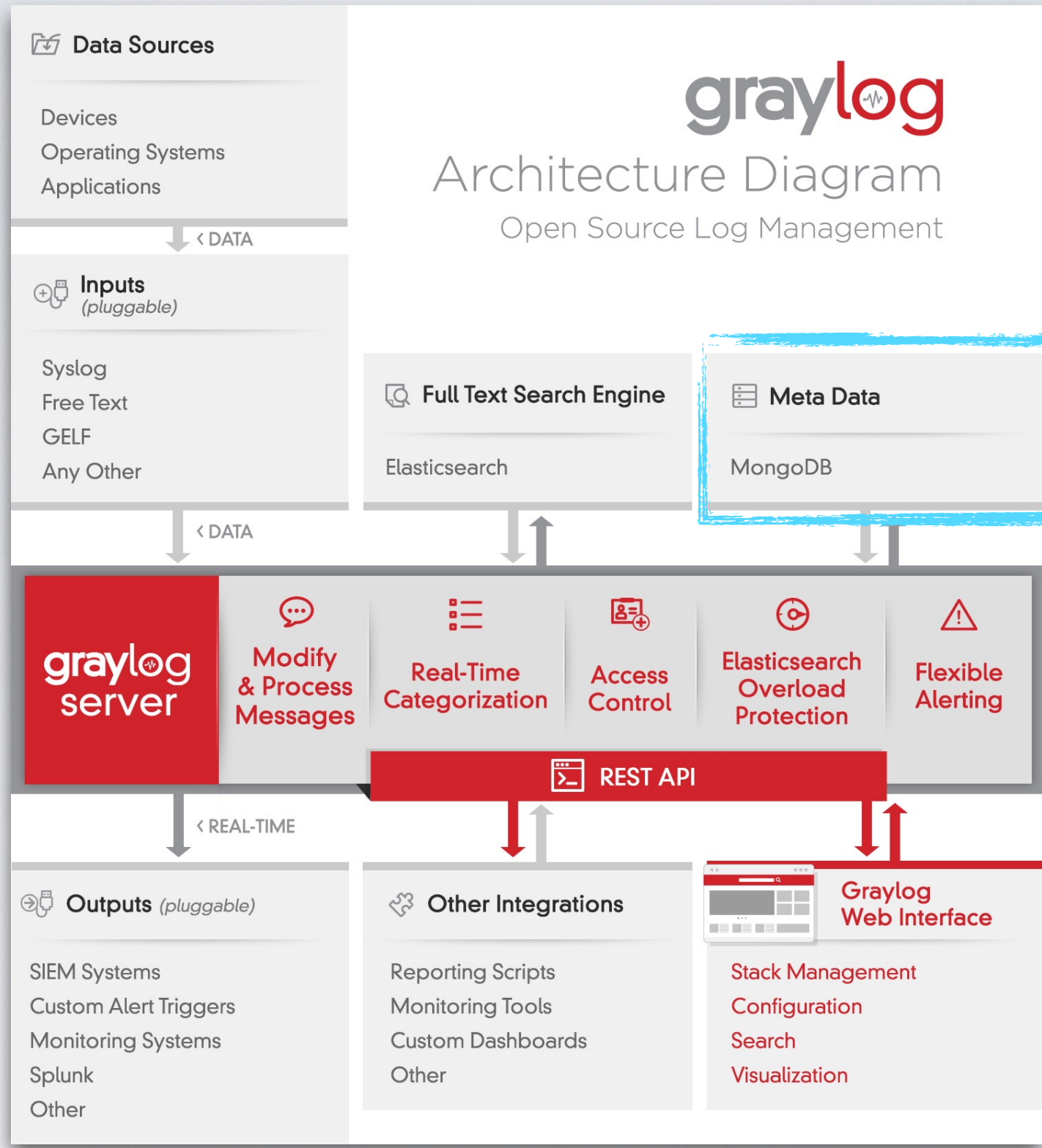
GRAYLOG



GRAYLOG

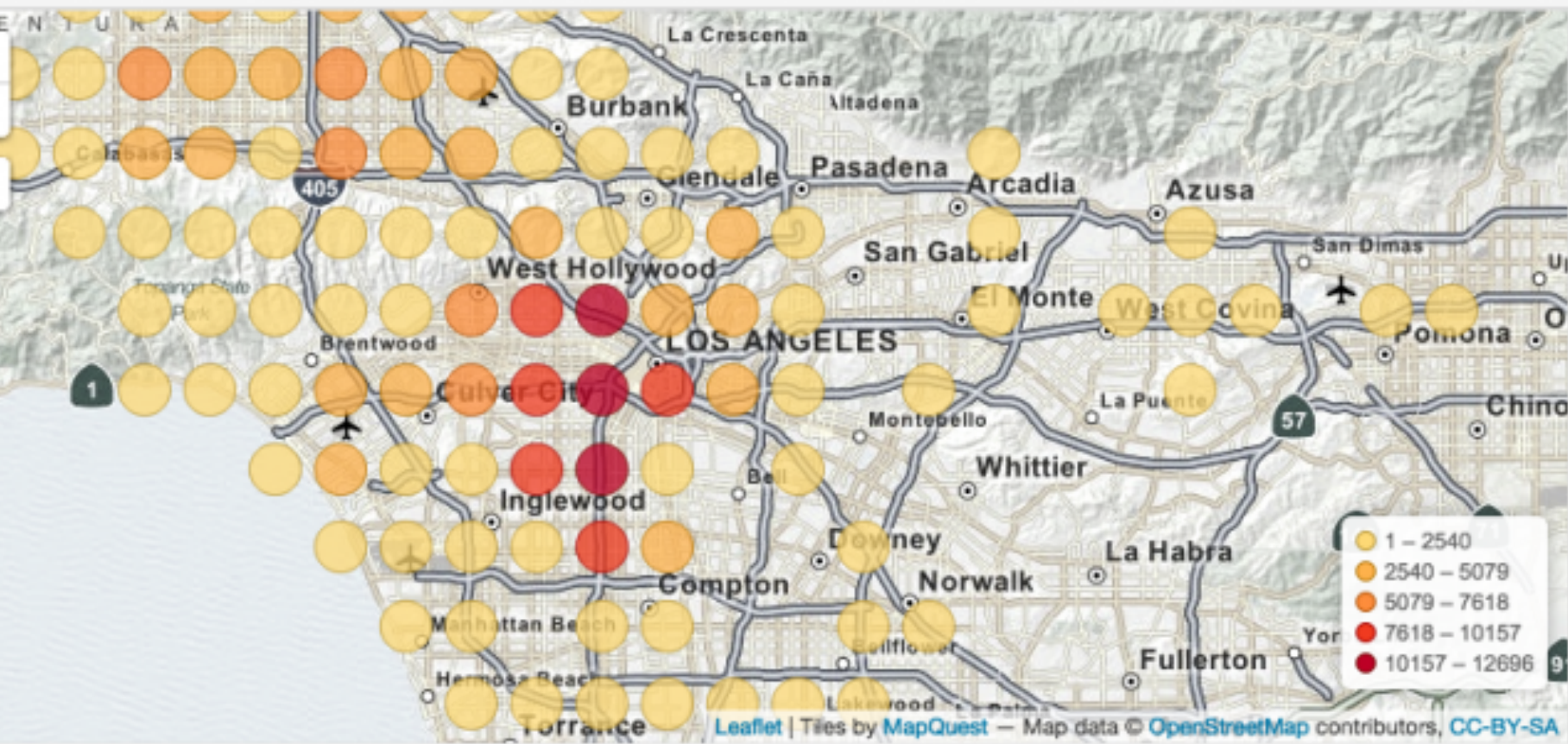


GRAYLOG

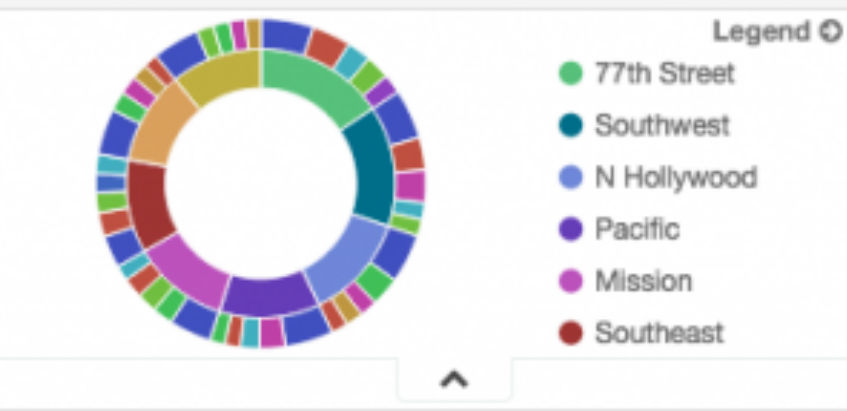


GRAYLOG

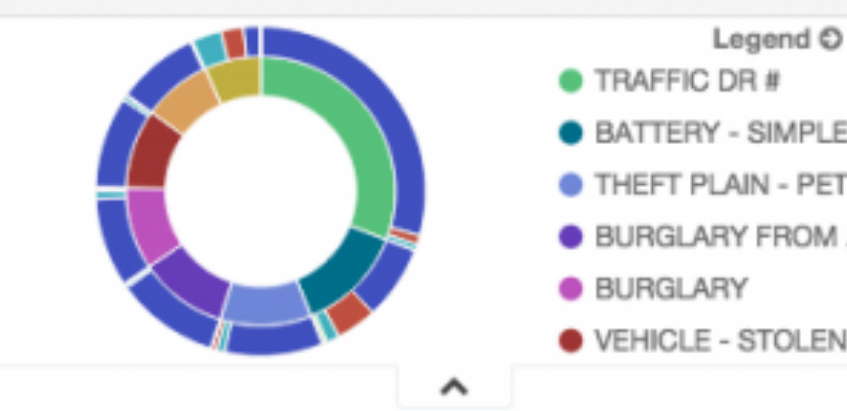
Dashboard: Tile map



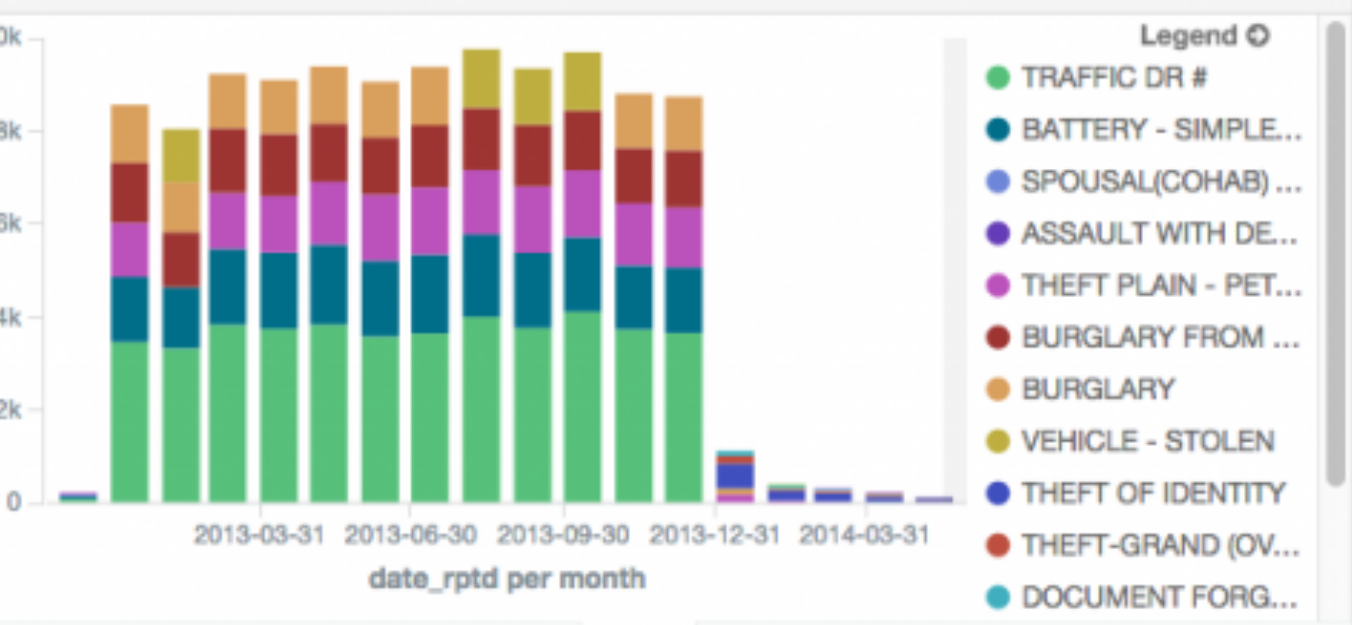
LAPD: Crime Type by Area



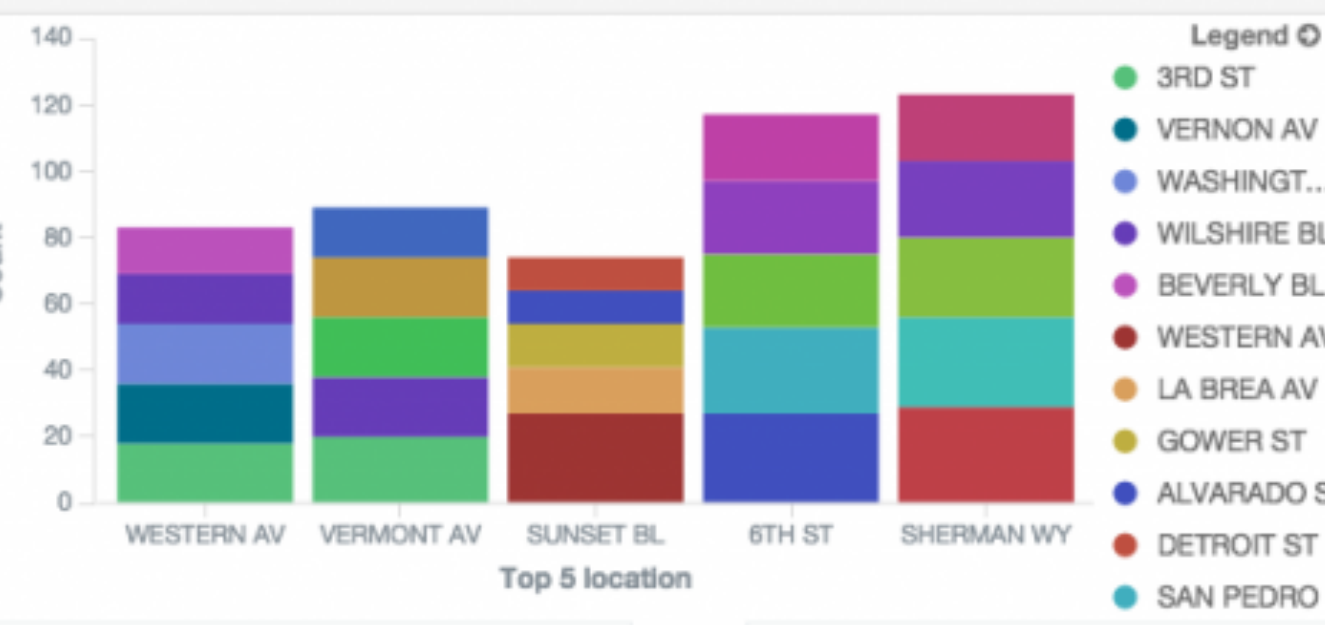
LAPD: Crime Status by Crime Type



Dashboard: Monthly histogram by Crime Type



LAPD: Intersections





GOAL

```
@40000005270e0d604afce64 {  
  "event": "logged_in",  
  "user": "guido",  
  "ip": "8.8.8.8",  
  "referrer": "http://google.com"  
}
```

CONTEXT

&

FORMAT

structlog

structLog

BoundLogger

structLog

e.g.
logging.Logger

BoundLogger

Original
Logger

structlog

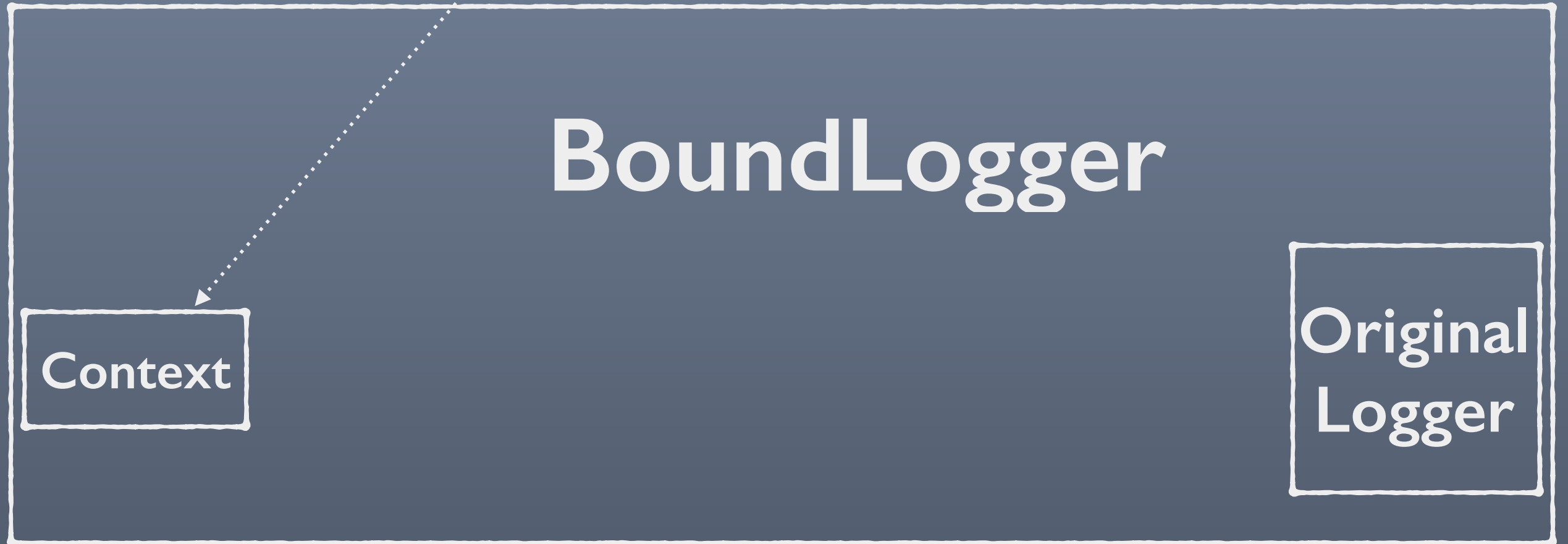
bind values

```
log.bind(key=value)
```

BoundLogger

Context

**Original
Logger**

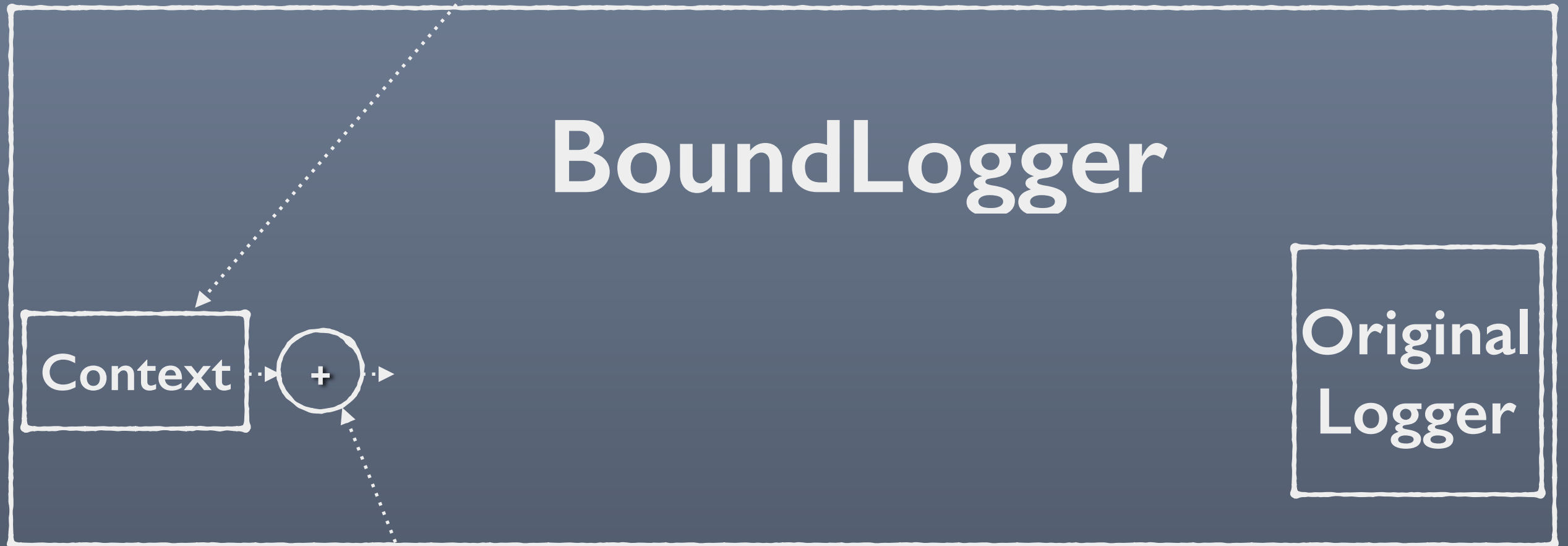


structlog

bind values

```
log.bind(key=value)
```

BoundLogger



log events

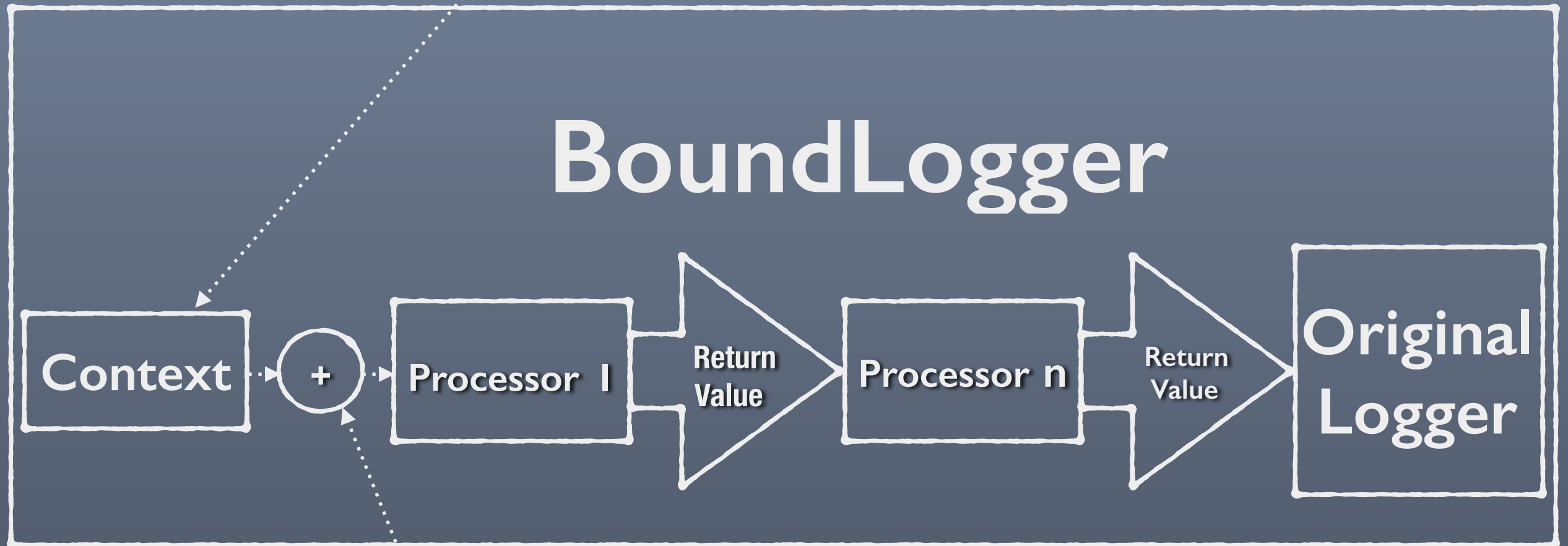
```
log.info(event, another_key=another_value)
```

structlog

bind values

```
log.bind(key=value)
```

BoundLogger



log events

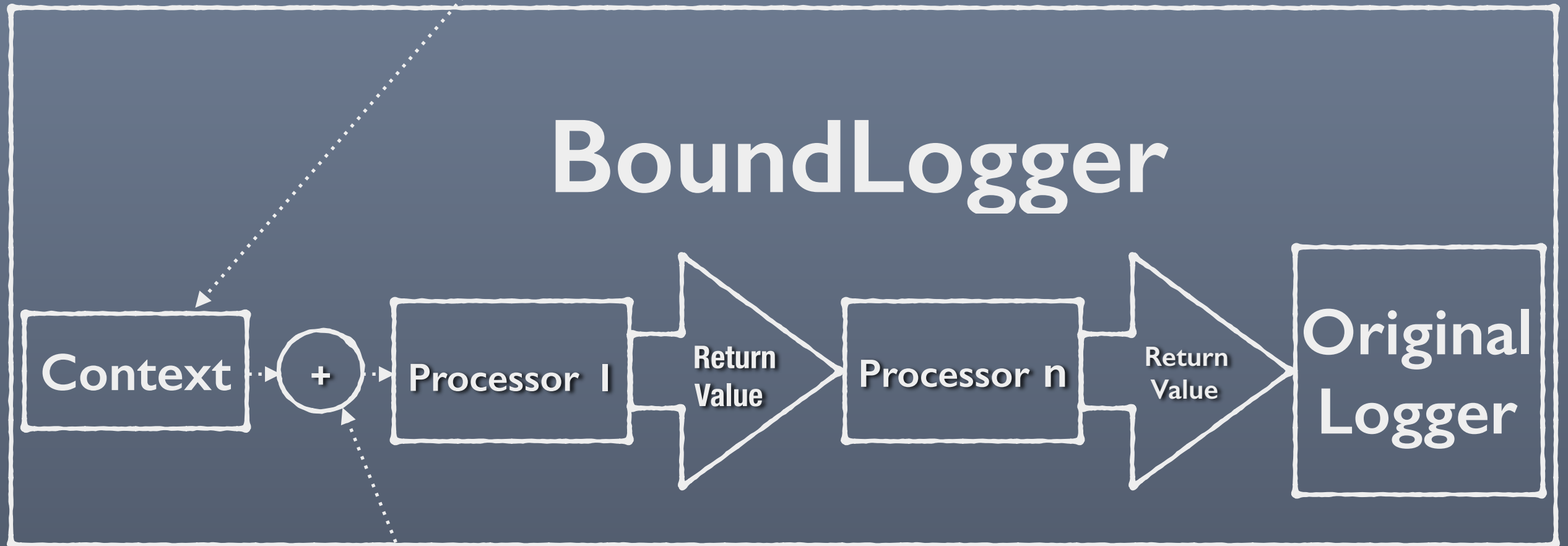
```
log.info(event, another_key=another_value)
```

structlog

bind values

```
log.bind(key=value)
```

BoundLogger



log events

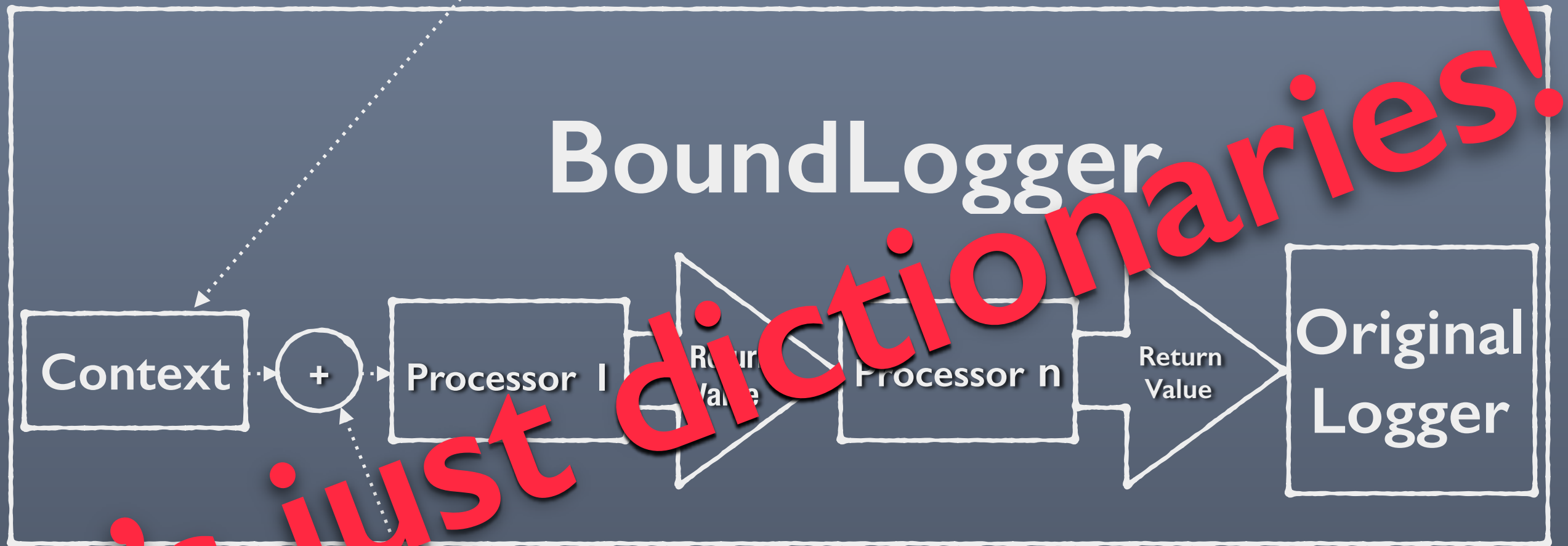
```
log.info(event, another_key=another_value)
```


structlog

bind values

```
log.bind(key=value)
```

BoundLogger



log events

```
log.info(event, another_key=another_value)
```

```
>>> from structlog import get_logger
>>> log = get_logger()
>>> log = log.bind(user='anonymous', some_key=23)
>>> log = log.bind(user='hynek', another_key=42)
>>> log.info('user.logged_in', happy=True)
```

```
some_key=23 user='hynek' another_key=42
happy=True event='user.logged_in'
```

```
>>> from structlog import get_logger
>>> log = get_logger()
>>> log = log.bind(user='anonymous', some_key=23)
>>> log = log.bind(user='hynek', another_key=42)
>>> log.info('user.logged_in', happy=True)
```

```
some_key=23 user='hynek' another_key=42
happy=True event='user.logged_in'
```



```
>>> from structlog import get_logger
>>> log = get_logger()
>>> log = log.bind(user='anonymous', some_key=23)
>>> log = log.bind(user='hynek', another_key=42)
>>> log.info('user.logged_in', happy=True)
```

```
some_key=23 user='hynek' another_key=42
happy=True event='user.logged_in'
```

```
>>> from structlog import get_logger
>>> log = get_logger()
>>> log = log.bind(user='anonymous', some_key=23)
>>> log = log.bind(user='hynek', another_key=42)
>>> log.info('user.logged_in', happy=True)
```

```
some_key=23 user='hynek' another_key=42
happy=True event='user.logged_in'
```

```
>>> from structlog import get_logger
>>> log = get_logger()
>>> log = log.bind(user='anonymous', some_key=23)
>>> log = log.bind(user='hynek', another_key=42)
>>> log.info('user.logged_in', happy=True)
```

```
some_key=23 user='hynek' another_key=42
happy=True event='user.logged_in'
```

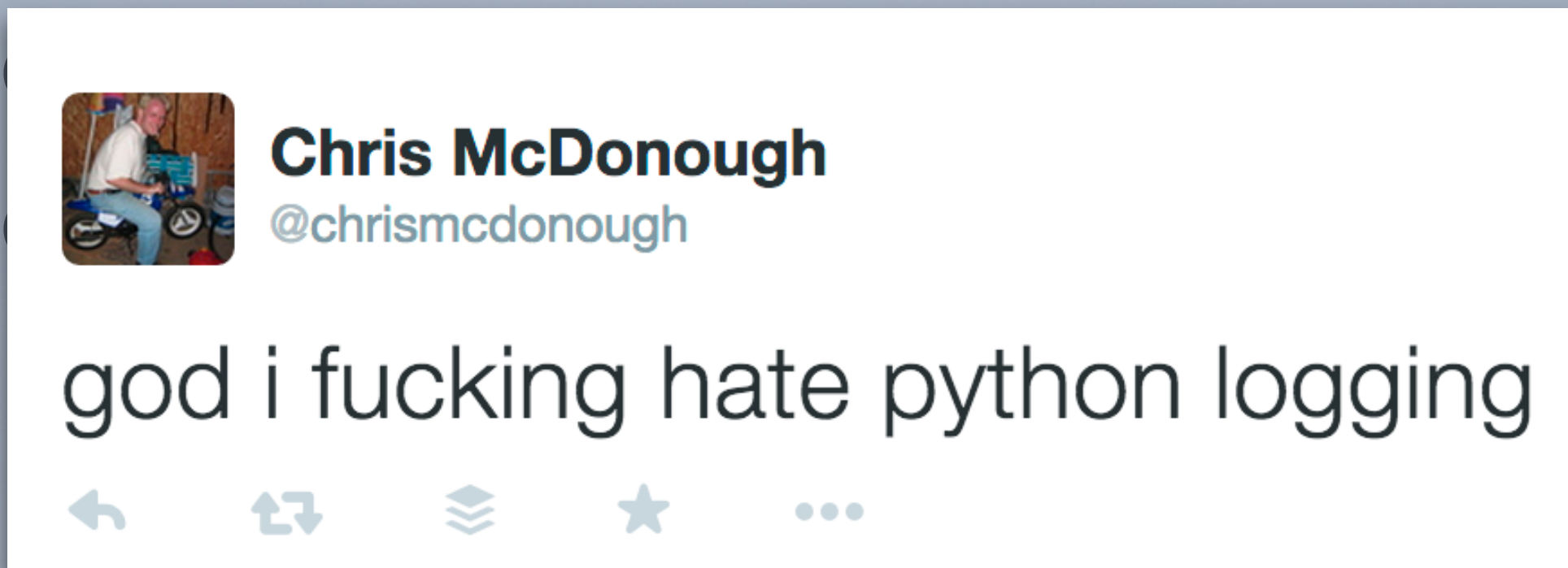


```
import logging, sys
```


```
logger = logging.getLogger()  
logger.addHandler(  
    logging.StreamHandler(  
        sys.stdout  
    )  
)
```

```
import logging, sys
```






```
logging  
logging
```



A screenshot of a tweet from Chris McDonough (@chrismcdonough). The tweet text reads "god i fucking hate python logging". The tweet interface shows the user's profile picture, name, and handle, followed by the text and interaction icons (reply, retweet, quote, favorite, and more options).

 **Chris McDonough**
@chrismcdonough

god i fucking hate python logging

```
er()
```

```
r(
```

```
)
```

```
)
```

CAPTURE

CAPTURE

- into files

CAPTURE

- into files
- to syslog / a queue

CAPTURE

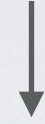
- into files
- to *syslog* / a queue
- pipe into a logging agent



```
log = log.bind(user="guido")  
log.info("user.login")
```



```
log = log.bind(user="guido")  
log.info("user.login")
```

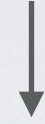


structlog

```
{"event": "user.login", "user": "guido"}
```

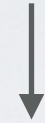


```
log = log.bind(user="guido")  
log.info("user.login")
```



structlog

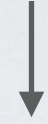
```
{"event": "user.login", "user": "guido"}
```



logging

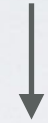
stdout

```
log = log.bind(user="guido")
log.info("user.login")
```



structlog

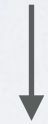
```
{"event": "user.login", "user": "guido"}
```



logging

stdout

(adds TAI64 timestamp)



runit's svlogd

`/var/log/app/current`

```
log = log.bind(user="guido")
log.info("user.login")
```

↓ **structlog**

```
{"event": "user.login", "user": "guido"}
```

↓ **logging**

stdout

(adds TAI64 timestamp)

↓ **runit's svlogd**

```
/var/log/app/current
```

↓ **logstash-forwarder**

logstash


```
log = log.bind(user="guido")
log.info("user.login")
```

↓ **structlog**

```
{"event": "user.login", "user": "guido"}
```

↓ **logging**

stdout

(adds TAI64 timestamp)

↓ **runit's svlogd**

`/var/log/app/current`

↓ **logstash-forwarder**

logstash

↓

`1010001101`

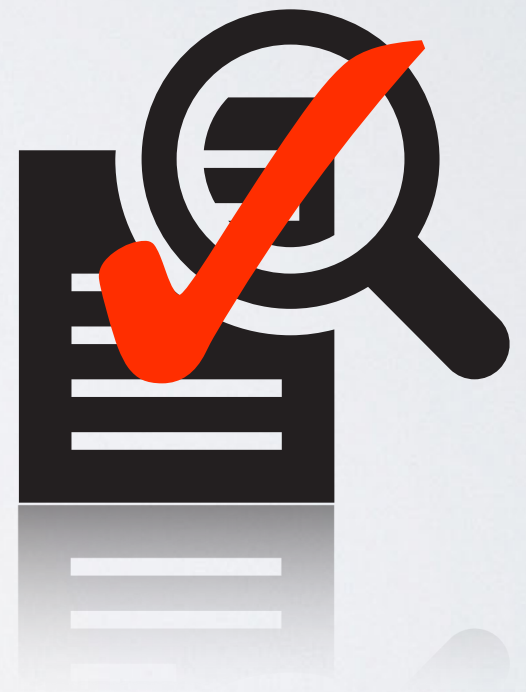
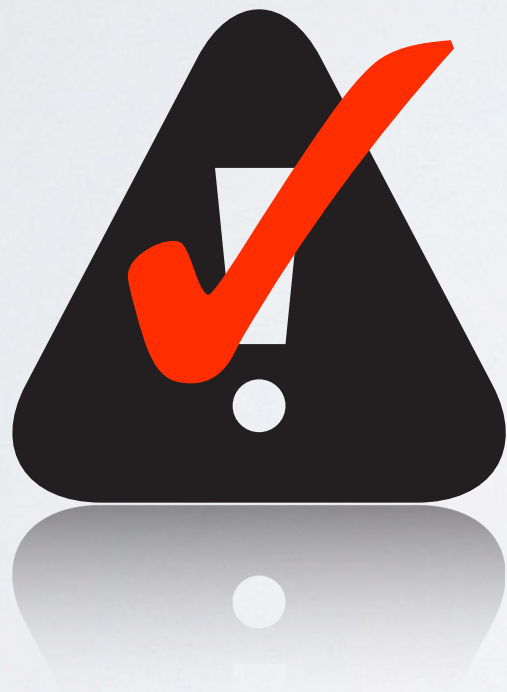
↓

Elasticsearch

PROGRESS!



PROGRESS!



WAIT A MINUTE...

UGH

```
try:
```

```
    STATS.time.timing():  
        something()
```

```
except Exception as e:
```

```
    log.error("omg", exc_info=e)  
    raven_client.captureError()  
    STATS.errors.mark()
```

UGH

```
try:
```

```
    STATS.time.timing():
```

```
        something()
```

```
except Exception as e:
```

```
    log.error("omg", exc_info=e)
```

```
    raven_client.captureError()
```

```
    STATS.errors.mark()
```


UGH

```
try:  
    something()  
except Exception as e:  
    log.error("omg", exc_info=e)
```

ERRORS

ERRORS

- Logging integration

ERRORS

- logging
- structlog

ERRORS

- logging
- structlog
- web apps: error views

PYRAMID ERROR VIEW

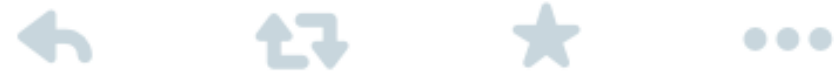
```
@view_config(context=Exception)
def err(exc, request):
    return Response("oops: " + raven_client.captureException())
```




Armin Ronacher

@mitsuhiko

The future: see a guy playing your game encounter an error condition on twitch, find the corresponding record in sentry and act on it.



Armin Ronacher

@mitsuhiko

Proper error logging is awesome :)



3:37 PM - 8 Jan 2015

METRICS

measure from *outside*

WSGI SERVERS

WSGI SERVERS

- `gunicorn`: `--statsd-host <host>`

WSGI SERVERS

- `gunicorn`: `--statsd-host <host>`
- `uWSGI`:

WSGI SERVERS

- `gunicorn`: `--statsd-host <host>`
- `uWSGI`:
 - `--stats-push statsd:<host>`

WSGI SERVERS

- **gunicorn**: `--statsd-host <host>`
- **uWSGI**:
 - `--stats-push statsd:<host>`
 - `--carbon <host>`

WSGI SERVERS

- **gunicorn**: `--statsd-host <host>`
- **uWSGI**:
 - `--stats-push statsd:<host>`
 - `--carbon <host>`
 - SNMP...

MIDDLEWARE

```
def timing_tween_factory(handler, registry):  
    def timing_tween(request):  
        with STATS.request_time.time():  
            return handler(request)  
  
    return timing_tween
```


MIDDLEWARE

```
def timing_tween_factory(handler, registry):  
    def timing_tween(request):  
        with STATS.request_time.time():  
            return handler(request)  
  
    return timing_tween
```

EXTRACT FROM LOGS

EXTRACT FROM LOGS

logstash

EXTRACT FROM LOGS

logstash

- StatsD

EXTRACT FROM LOGS

logstash

- StatsD
- Graphite

EXTRACT FROM LOGS

logstash

- StatsD
- Graphite
- librato

EXTRACT FROM LOGS

logstash

- StatsD
- Graphite
- librato
- Riemann

EXTRACT FROM LOGS

logstash

- StatsD
- Graphite
- librato
- Riemann
- ...

EXTRACT FROM LOGS

logstash

- StatsD
- Graphite
- librato
- Riemann
- ...

or `structlog`

LEVERAGE MONITORING

REMAINING

REMAINING

1. measure code paths

REMAINING

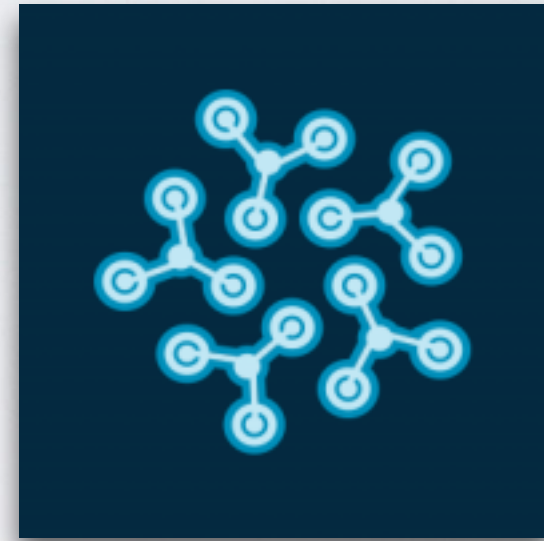
1. measure code paths
2. expose gauges

SUMMARY

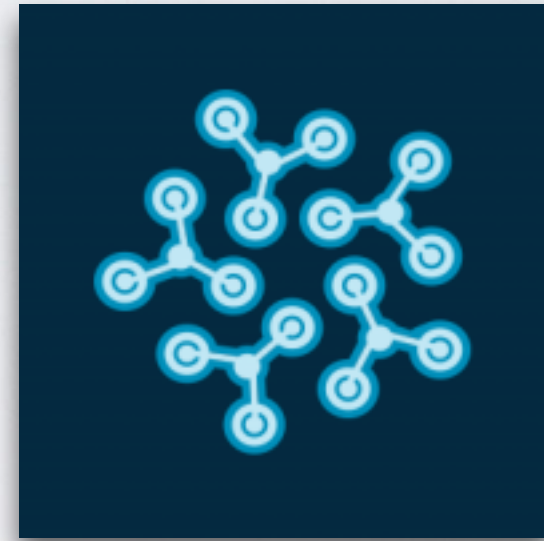
SUMMARY



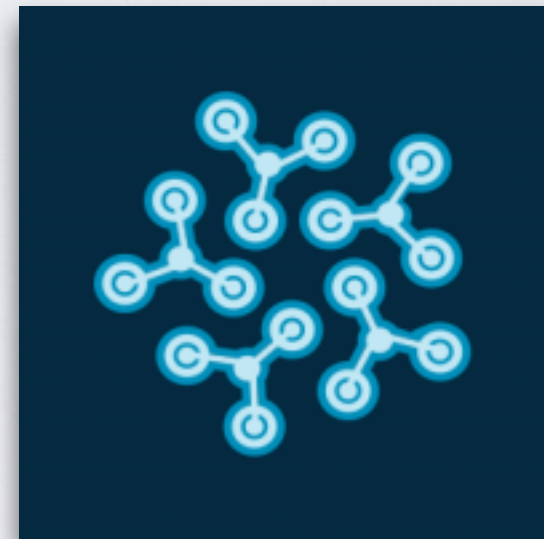
SUMMARY



SUMMARY



SUMMARY



OX.CX/b

@hynek

vrmd.de