Monitoring with syslog-ng, Riemann and Kibana

@algernoone

@balabit

OSDC.de

OPEN SOURCE DATA CENTER CONFERENCE

syslog-ng

syslog-ng

- Open source event processor and swiss army knife

syslog-ng

- Open source event processor and swiss army knife
- Developed since 1998, LGPL + GPL

syslog-ng

- Open source event processor and swiss army knife
- Developed since 1998, LGPL + GPL
  - (Commercial offering since 2007)

syslog-ng

- Open source event processor and swiss army knife
- Developed since 1998, LGPL + GPL
  - (Commercial offering since 2007)
- Collects, parses, filters, transforms, transfers events

syslog-ng

- Open source event processor and swiss army knife
- Developed since 1998, LGPL + GPL
  - (Commercial offering since 2007)
- Collects, parses, filters, transforms, transfers events
- Wide variety of plugins

syslog-ng

- Open source event processor and swiss army knife
- Developed since 1998, LGPL + GPL
  - (Commercial offering since 2007)
- Collects, parses, filters, transforms, transfers events
- Wide variety of plugins
- A sizable, helpful and very inclusive community

Riemann

Riemann

- Riemann monitors distributed systems

Riemann

- Riemann monitors distributed systems
- Event aggregator with a powerful stream processing language

Riemann

- Riemann monitors distributed systems
- Event aggregator with a powerful stream processing language
- Provides a low-latency, transient shared state

Kibana

Kibana

- Visualize logs and time-stamped data

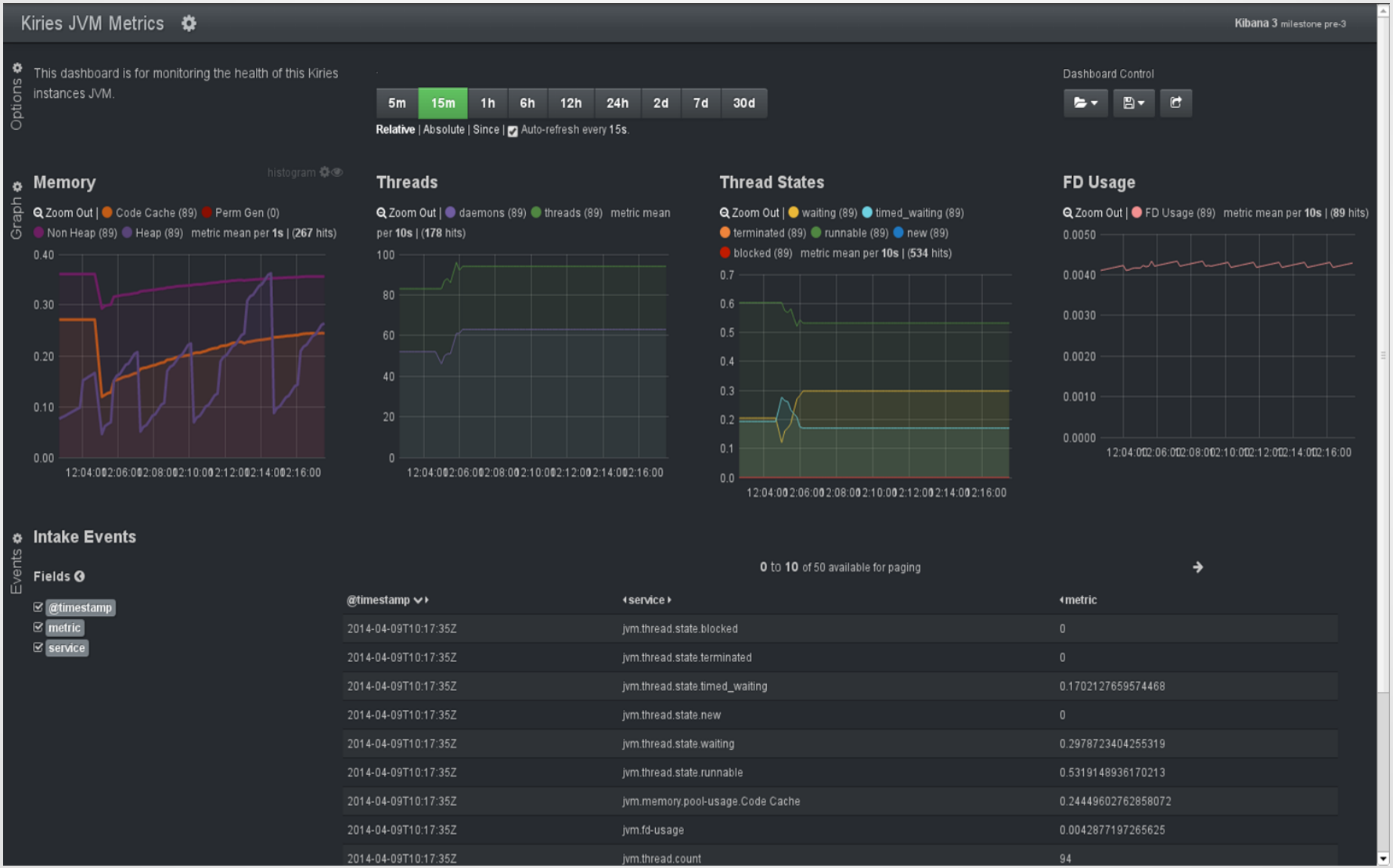
Kibana

- Visualize logs and time-stamped data
- Powerful search syntax

Kibana

- Visualize logs and time-stamped data
- Powerful search syntax
- Flexible, powerful, yet intuitive interface

Kibana


Kiries JVM Metrics
Kibana 3 milestone pre-3
Options
This dashboard is for monitoring the health of this Kiries instances JVM.
5m 15m 1h 6h 12h 24h 2d 7d 30d
Relative | Absolute | Since | Auto-refresh every 15s.
Dashboard Control
Graph
Memory
histogram
Zoom Out | Code Cache (89) Perm Gen (0) Non Heap (89) Heap (89) metric mean per 1s | (267 hits)
Threads
Zoom Out | daemons (89) threads (89) metric mean per 10s | (178 hits)
Thread States
Zoom Out | waiting (89) timed_waiting (89) terminated (89) runnable (89) new (89) blocked (89) metric mean per 10s | (534 hits)
FD Usage
Zoom Out | FD Usage (89) metric mean per 10s | (89 hits)
Events
Intake Events
Fields
@timestamp
metric
service
0 to 10 of 50 available for paging
@timestamp
service
metric
2014-04-09T10:17:35Z jvm.thread.state.blocked 0
2014-04-09T10:17:35Z jvm.thread.state.terminated 0
2014-04-09T10:17:35Z jvm.thread.state.timed_waiting 0.1702127659574468
2014-04-09T10:17:35Z jvm.thread.state.new 0
2014-04-09T10:17:35Z jvm.thread.state.waiting 0.2978723404255319
2014-04-09T10:17:35Z jvm.thread.state.runnable 0.5319148936170213
2014-04-09T10:17:35Z jvm.memory.pool-usage.Code Cache 0.2444960276285807
2014-04-09T10:17:35Z jvm.fd-usage 0.0042877197265625
2014-04-09T10:17:35Z jvm.thread.count 94

Monitoring

Monitoring

What

Monitoring

What

- System state

Monitoring

What

- System state
- Application state

Monitoring

What

- System state
- Application state
- Exceptions

Monitoring

What

- System state
- Application state
- Exceptions
- Activity

Monitoring

Tools

Monitoring

Tools

- Nagios
- Collectd
- Munin

Monitoring

Tools

- Nagios
- Collectd
- Munin

- Riemann

Logging

Logging

Logging

- Persisting application state

Logging

- Persisting application state
- Format is usually application specific

Logging

- Persisting application state
- Format is usually application specific
- Structured vs unstructured

Logging

- Persisting application state
- Format is usually application specific
- Structured vs unstructured
- Great source for monitoring too!

Monitoring + Logging

Monitoring + Logging

- What do we already have?

Monitoring + Logging

- What do we already have?
- What can we add?

Monitoring + Logging

- What do we already have?
- What can we add?
- How will we benefit from all of this?

Q & A

Thanks!

- http://www.syslog-ng.org/
- https://github.com/balabit/syslog-ng-incubator
- https://talien.blogs.balabit.com/
- https://algernon.blogs.balabit.com/