

Graylog

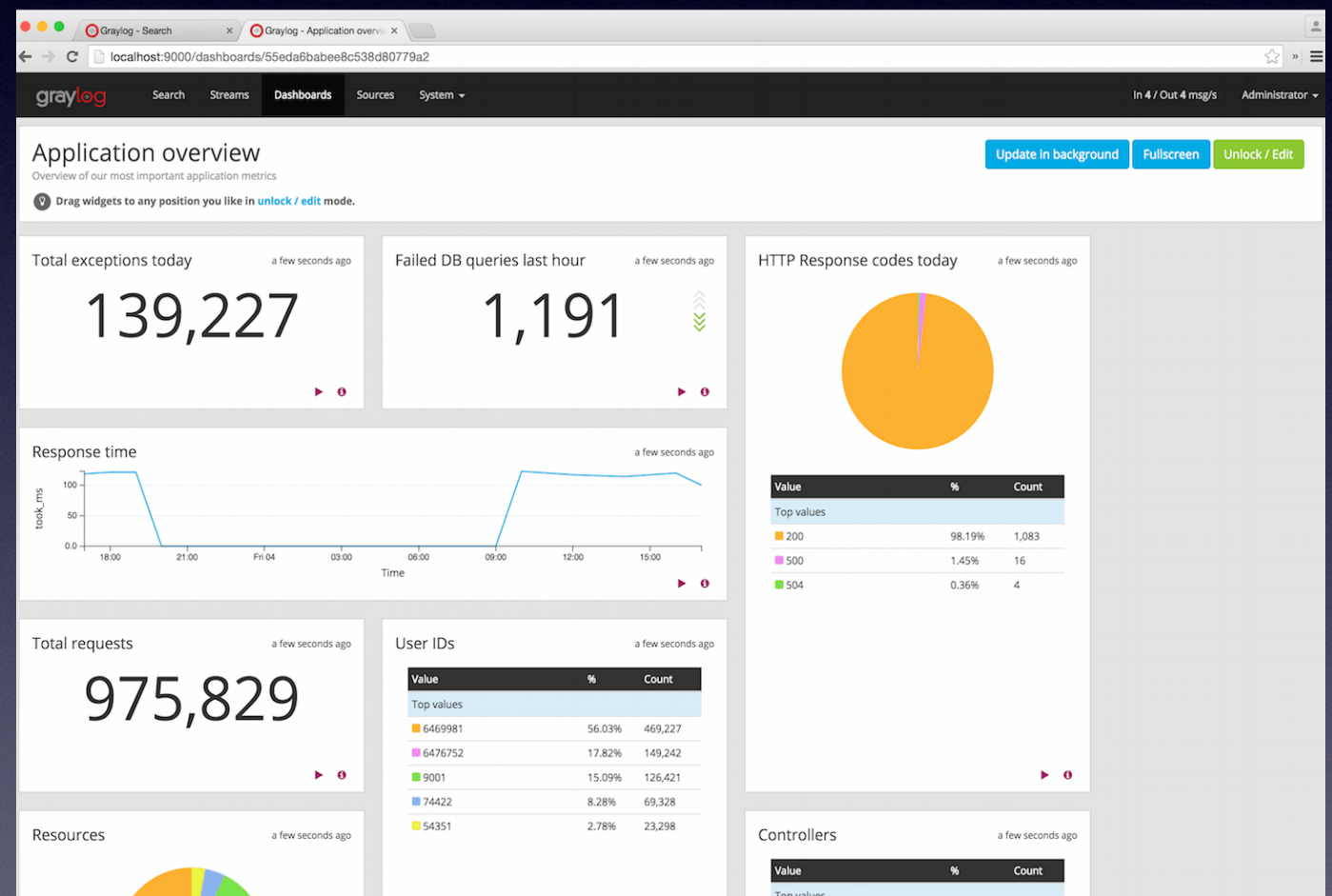
overview and usage

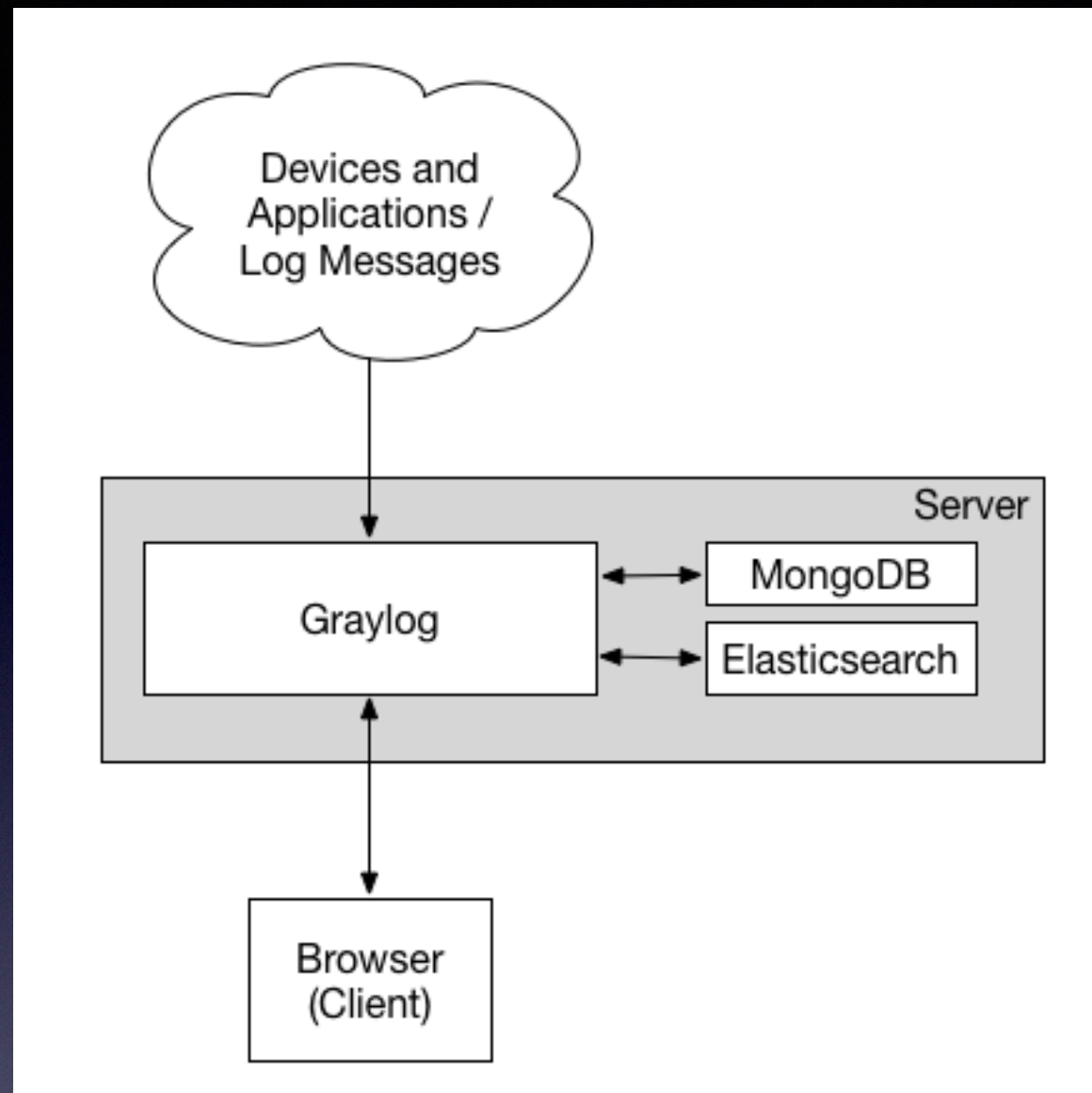
Plan

1. Graylog overview
2. About logging
3. Graylog Inputs
4. Java configuration for Graylog
5. GrayLog Web interface overview
6. Demo

Basic features

- single log entry point
- full-text indexing
- flexible search engine
- dashboards
- analytics abilities
- wide range input types
- REST API
- open source





Graylog architecture



Владимир Красильщик — Что надо знать о логировании прагматичному Java-программисту

<https://youtu.be/j-i3NQiKbcc>

Java logging frameworks

- Java Util logging (JUL/JDK)
- Log4j
- Logback
- Log4j2
- Apache Commons Loggings (JCL) - interface
- Simple Logging Facade For Java (SLF4J) - interface

Graylog inputs

GELF

- GELF AMQP
- GELF HTTP
- GELF Kafka
- GELF TCP
- GELF UDP

Raw/Plaintext

- Raw/Plaintext AMQP
- Raw/Plaintext Kafka
- Raw/Plaintext TCP
- Raw/Plaintext UDP

Syslog

- Syslog AMQP
- Syslog Kafka
- Syslog TCP
- Syslog UDP

Others

- JSON path from HTTP API
- Random HTTP message generator

Graylog Java Config

- Logback config file (logback.xml or logback-spring.xml):

```
<appender name="GRAYLOG_TCP" class="de.appelgriepsch.logback.GelfAppender">
  <server>127.0.0.1</server>
  <port>12201</port>
  <hostName>my-app-name</hostName>
  <protocol>TCP</protocol>
</appender>

<root level="INFO">
  <appender-ref ref="GRAYLOG_TCP" />
</root>
```

- Logback GELF appender library (build.gradle):

```
compile('de.appelgriepsch.logback:logback-gelf-appender:1.2.3')
```


Graylog web interface components

- Search
- Streams
- Dashboards

graylog

SearchStreamsDashboardsSourcesSystem

In 3 / Out 3 msg/sHelpAdministrator

Search in the last 1 day

▶ Not updating

Saved searches

🔍

source:macbook AND _exists_:request-id AND status-code:503

📌

Search result

Found **382 messages** in 67 ms, searched in 1 index.
Results retrieved at 2017-01-20 16:25:49.

Add count to dashboard

Save search criteriaMore actions

FieldsDecorators

DefaultAllNoneFilter fields

▶ ☐ cat

▶ ☐ cow

▶ ☐ execution-time-ms

▶ ☐ headers_Connection

▶ ☐ headers_Content-Length

▶ ☐ headers_Content-Type

▶ ☐ headers_Date

▶ ☐ level

▶ ☐ loggerName

▶ ☒ message

▶ ☐ request-id

List fields of **current page** or **all fields**.

☒ Highlight results

Histogram

Add to dashboard

🕒 Year, Quarter, Month, Week, Day, **Hour**, Minute

Messages

Previous123Next

Timestamp🔍source

2017-01-20 16:25:33.601macbook

```
{ "response-name": "client-incoming-response", "uri": "http://localhost:8080/service2/status", "request-id": 50, "status-code": "503", "status-text": null, "headers": { "Content-Type": "text/plain; charset=UTF-8", "Content-Length": 17, "Date": "Fri, 20 Jan 2017 13:25:33 GMT", "Connection": "close" }, "response-body": "Service2 is alive", "execution-time-ms": 3 }
```


2017-01-20 16:25:28.596macbook

```
{ "response-name": "client-incoming-response", "uri": "http://localhost:8080/service2/status", "request-id": 48, "status-code": "503", "status-text": null, "headers": { "Content-Type": "text/plain; charset=UTF-8", "Content-Length": 17, "Date": "Fri, 20 Jan 2017 13:25:28 GMT", "Connection": "close" }, "response-body": "Service2 is alive", "execution-time-ms": 4 }
```

2017-01-20 16:25:23.588macbook


```
{ "response-name": "client-incoming-response", "uri": "http://localhost:8080/service2/status", "request-id": 46, "status-code": "503", "status-text": null, "headers": { "Content-Type": "text/plain; charset=UTF-8", "Content-Length": 17, "Date": "Fri, 20 Jan 2017 13:25:23 GMT", "Connection": "close" }, "response-body": "Service2 is alive", "execution-time-ms": 2 }
```

Search

SearchStreamsDashboardsSourcesSystem ▾In 3 / Out 3 msg/sHelp ▾Administrator ▾

Streams

You can route incoming messages into streams by applying rules against them. If a message matches all rules of a stream it is routed into it. A message can be routed into multiple streams. You can for example create a stream that contains all SSH logins and configure to be alerted whenever there are more logins than usual. Read more about streams in the [documentation](#).

 Take a look at the [Graylog stream dashboards](#) for wall-mounted displays or other integrations.



Filter streams

FilterReset

rest

REST messages

2 messages/second, Must match all of the 1 configured stream rule(s). [Hide stream rules](#)

  request-id must be present (REST marker)

Manage Rules

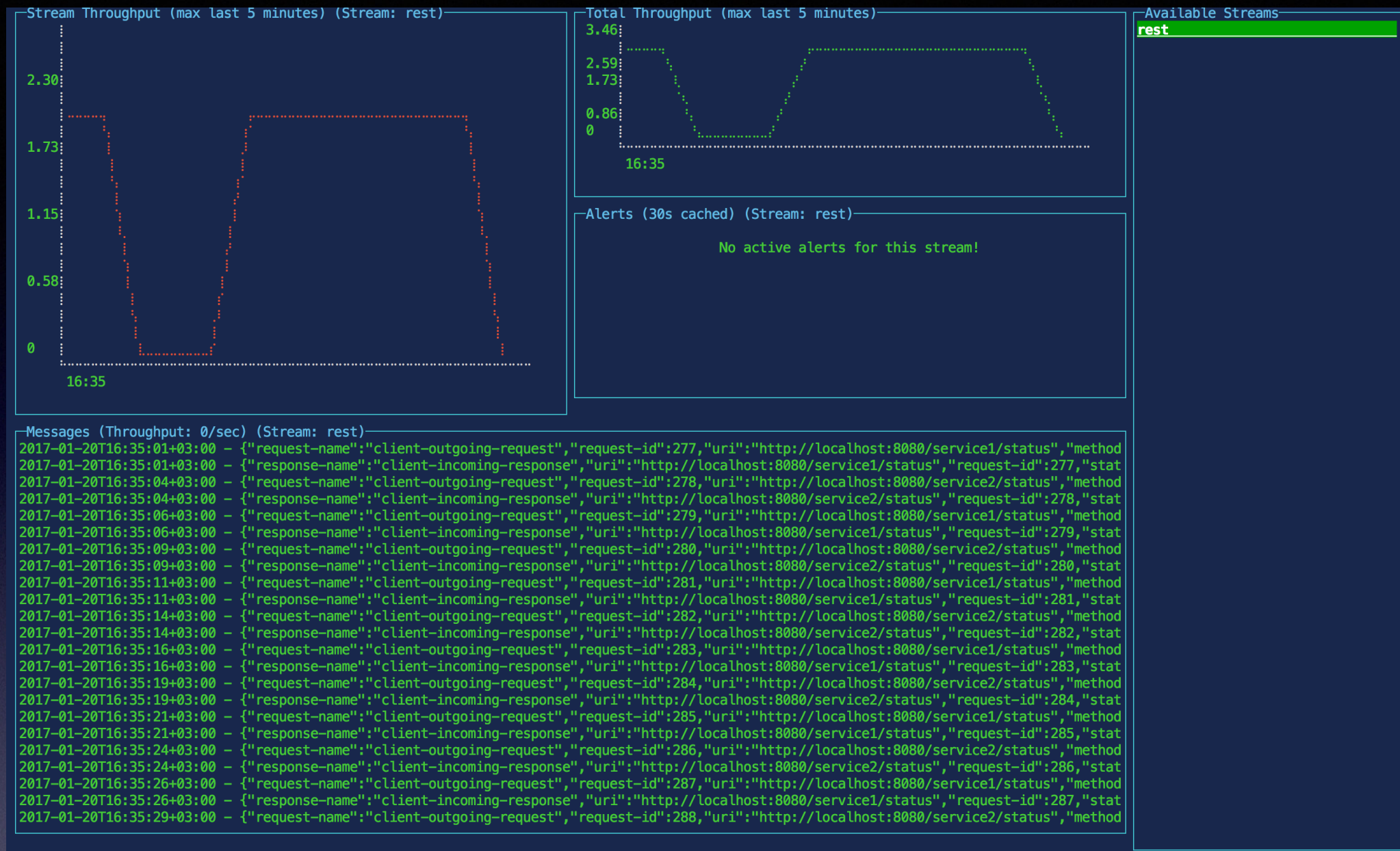
Manage Outputs

Manage Alerts

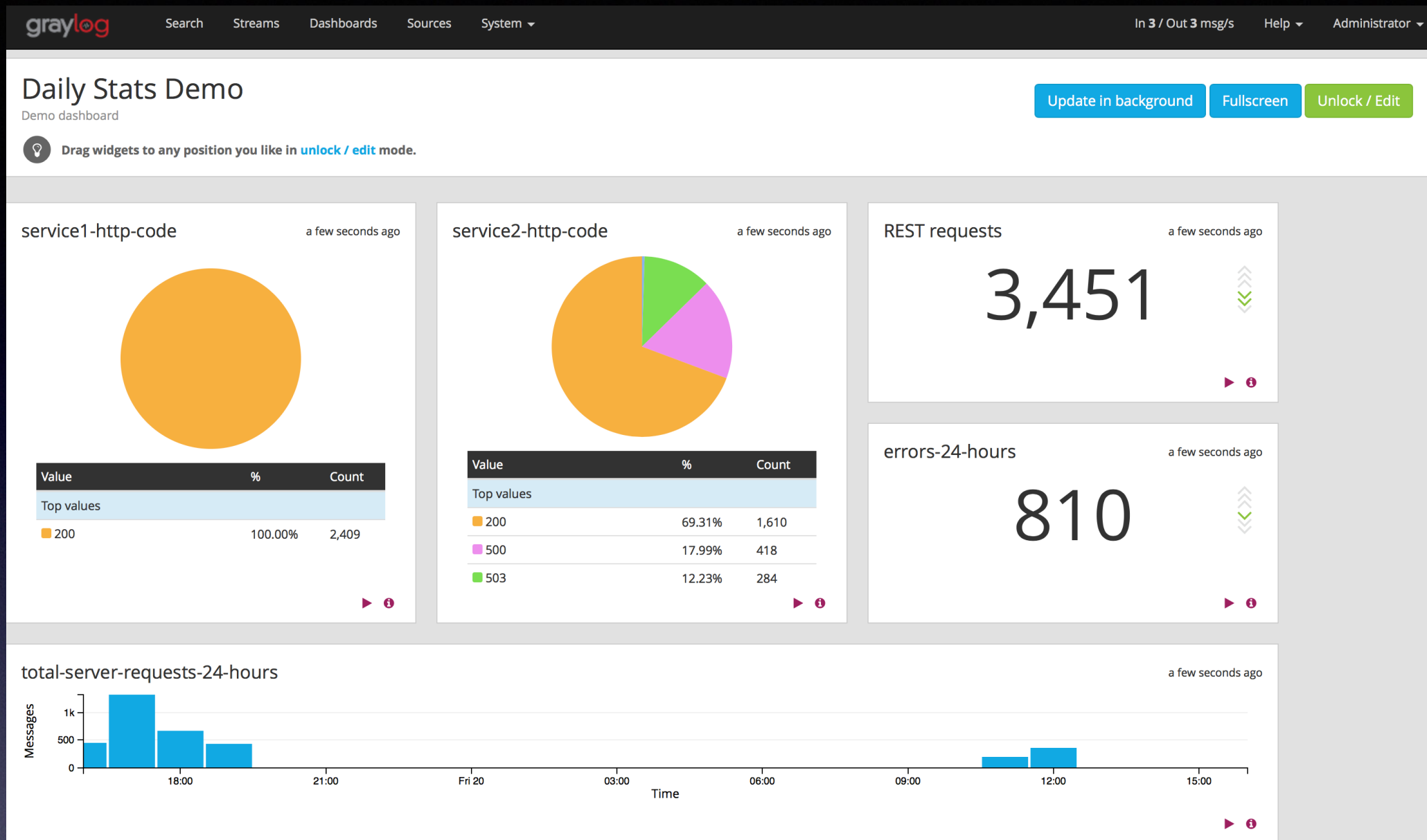
Pause Stream

More Actions ▾

Streams (web)



Streams (terminal)



Dashboards

Links

- Graylog search queries: <http://docs.graylog.org/en/2.1/pages/queries.html>
- Graylog dashboard tutorial: <http://docs.graylog.org/en/2.1/pages/dashboards.html>
- Graylog GELF format: <http://docs.graylog.org/en/2.1/pages/gelf.html>
- Graylog CLI dashboard: <https://github.com/Graylog2/cli-dashboard>
- Logback manual: <http://logback.qos.ch/manual/index.html>
- Spring boot logging: <https://docs.spring.io/spring-boot/docs/current-SNAPSHOT/reference/htmlsingle/#boot-features-logging>

Demo

Thanks for watching