What’s going on with your logs?

Fran Álvarez

REINVENT YOUR CONTENT

A Strategic Alfresco Partner

Working with Alfresco since Alfresco v0.6

Over 140 Alfresco implementations

Alfresco & WCM Architecture Design Patterns

First worldwide implementation of the first Alfresco WCM product in 2007

Excellent Alfresco knowledge and highly trained and experienced staff

Alfresco Certified Engineers and Alfresco Certified Administrators

Authoring of leading Alfresco books

Alfresco Technical blogs http://www.ixxus.com/blog/

Multiple speaking engagements at the Alfresco Conferences (2011-2014), Alfresco Days and BeeCon 2016

Alfresco Million $ Club (May 2012) – Only 2 companies awarded

Alfresco Solution Partner of the Year 2013 and 2014

Alfresco Best Solution 2015 and Partner of the Year 2015 (Northern Europe)

Agenda

- Troubleshooting’s troubles
- Centralised logging with Graylog
- Demo

Troubleshooting troubles

Details

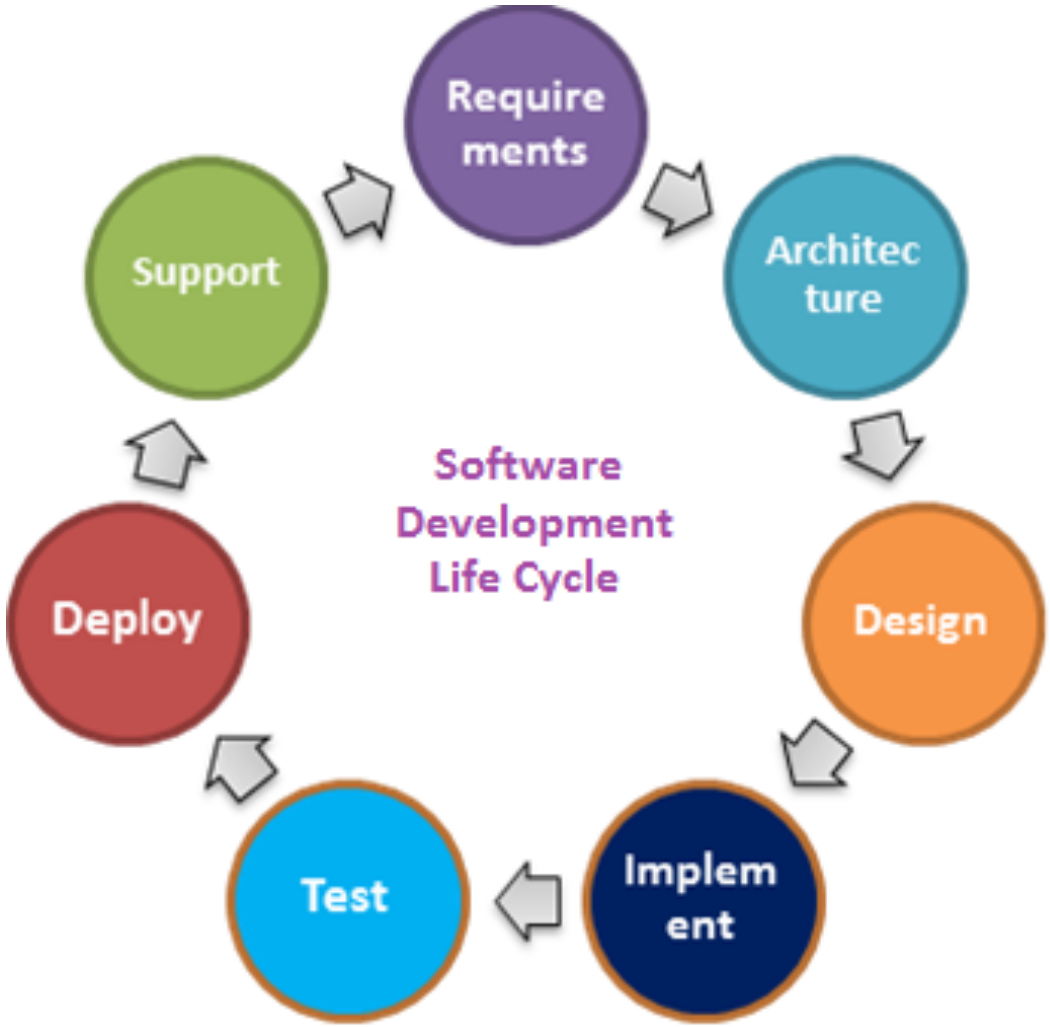
A typical agile SDLC

Requirements

- User stories

- Improvements

- Bugs



http://theintrovertmusings.blogspot.com.es/2015/02/software-process-models.html

Cost of fixing a bug by stages

Production

Understand

Reproduce

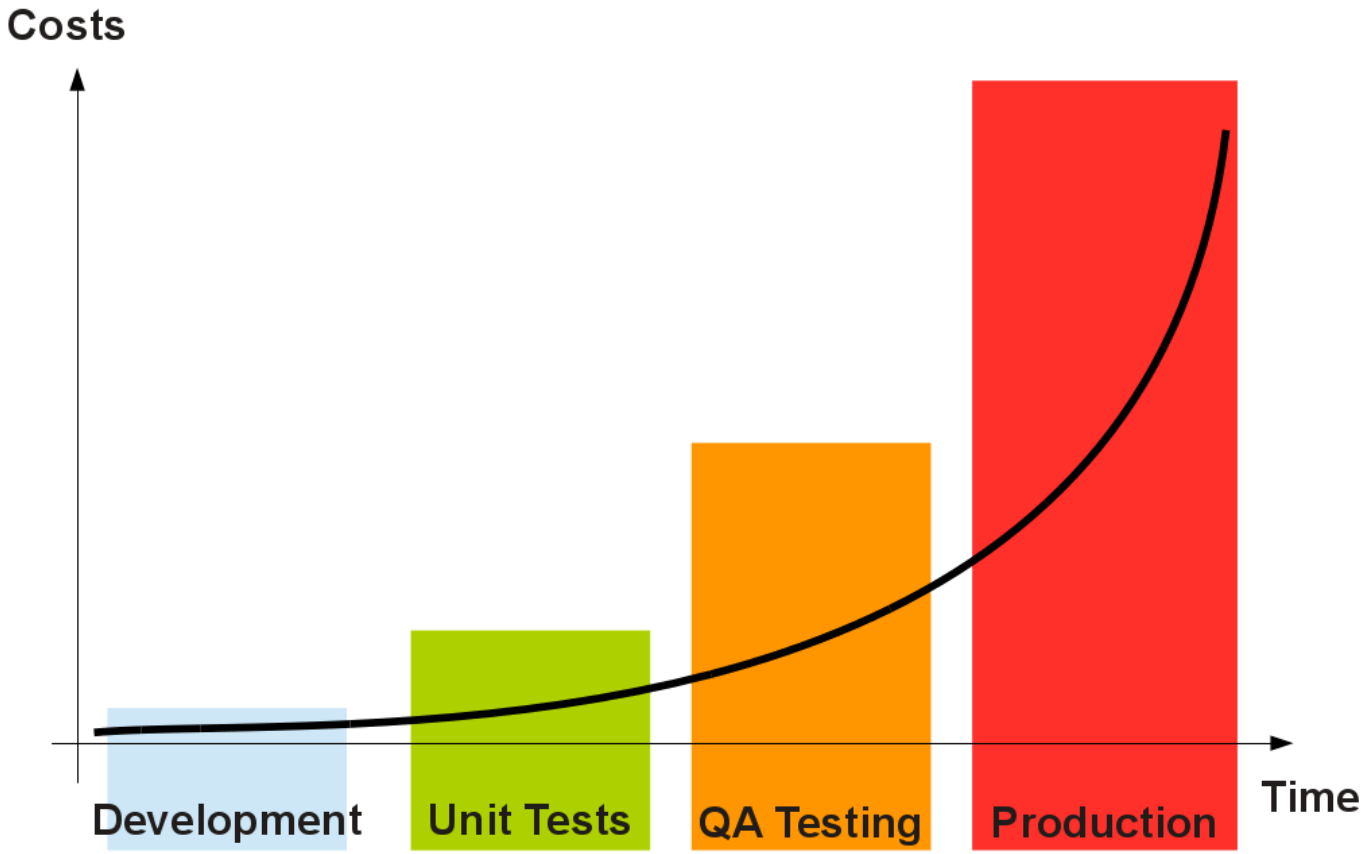
Replicate

Fix

Test

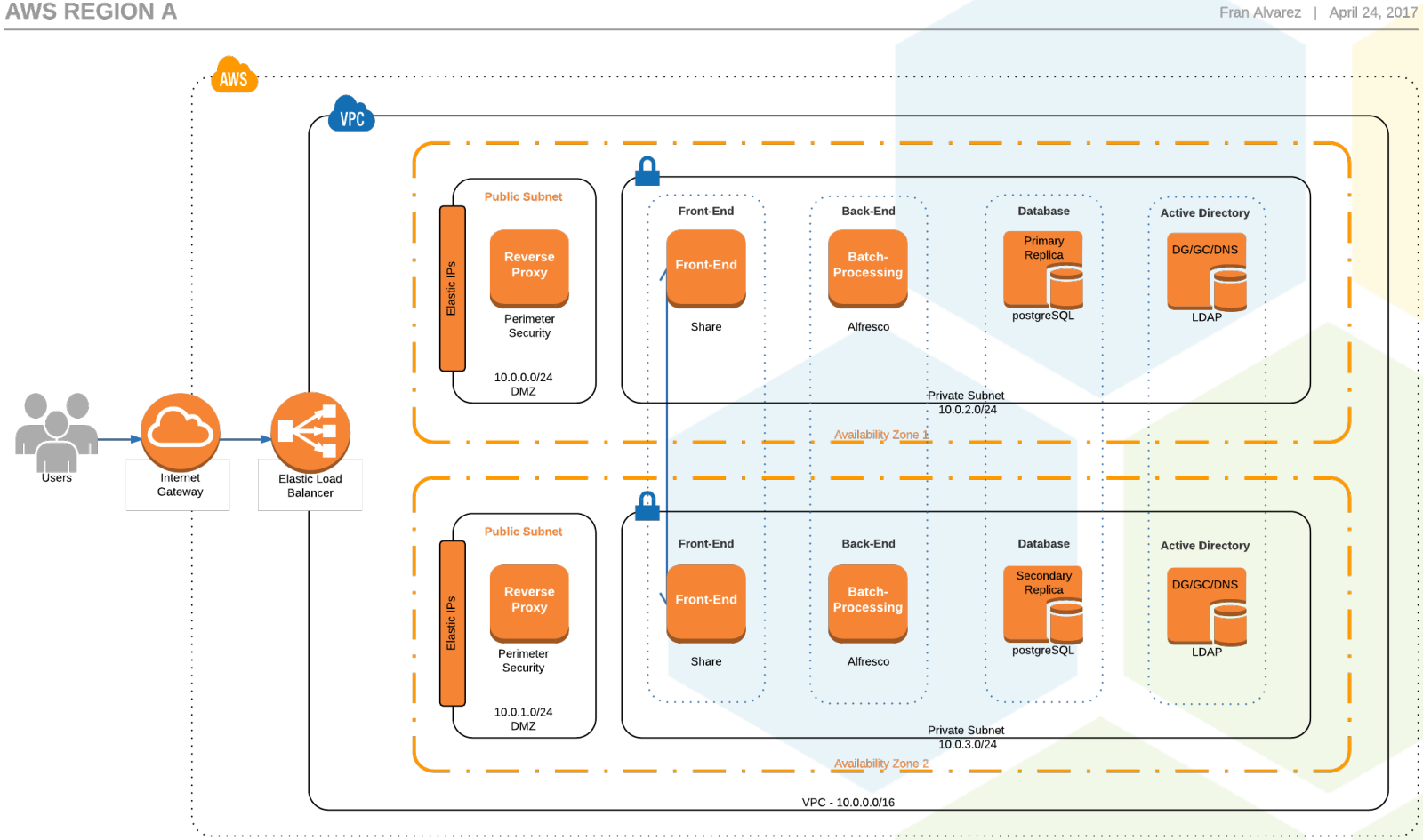
Regression

Deploy

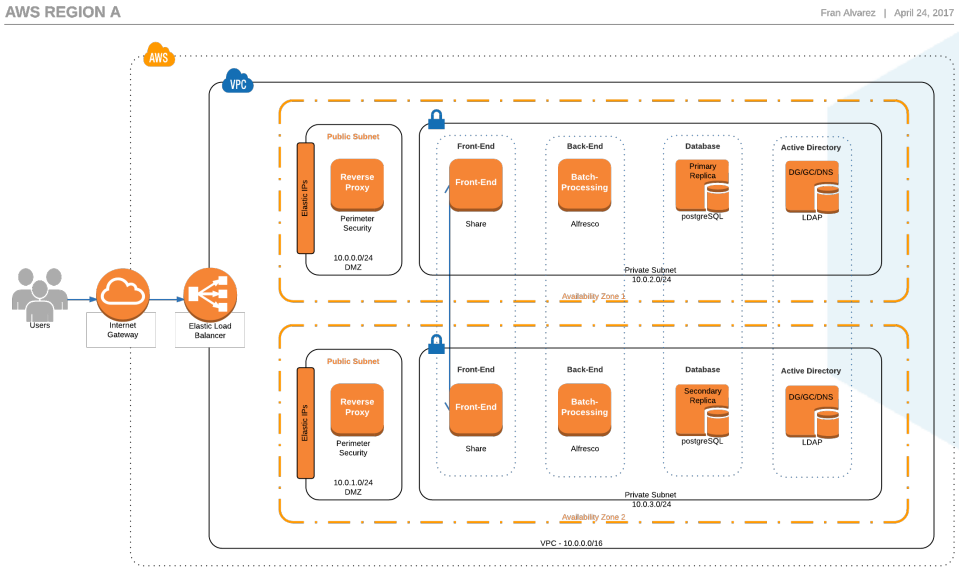


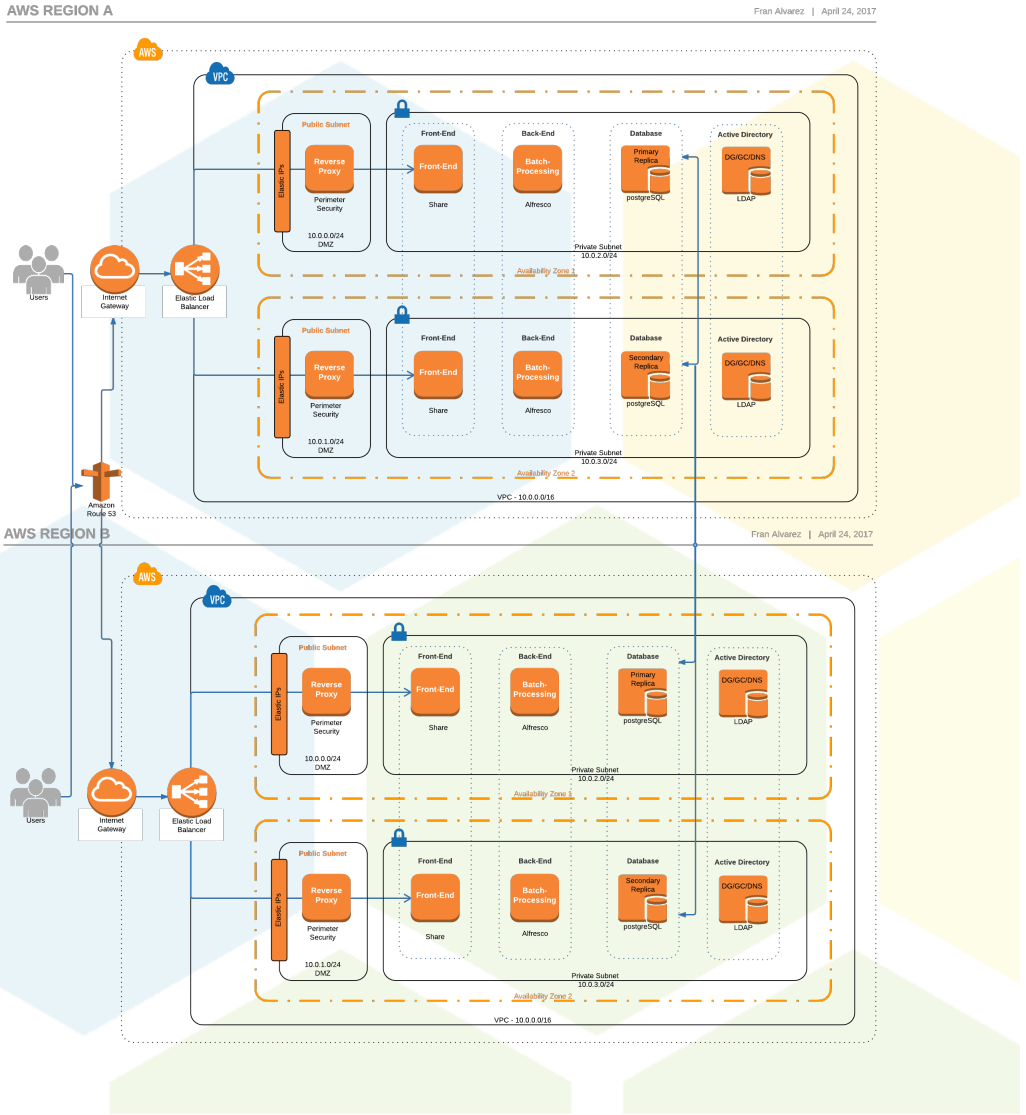
https://blog.pdark.de/2012/07/21/software-development-costs-bugfixing/

A typical architecture



Can be more complex





Support Challenges

More diagnostic logging

‘Debug build’, follow trace Vs follow code

view all logs at the same point-in-time (sequence) for correlation events across those services

Provide/Collect information/insight

Some data/report enquiries might be asked *(how many assets were moved yesterday?)*

Anticipate or Prevent a problem

Reduce the time to narrow the problem

Graylog

Details

Graylog

Application to manage log data from a one central location

- Parse and enrich logs
- Allows to search and filter messages along with their properties
- User friendly charts and dashboards
- Alerts and Triggers
- Community and Enterprise
- Open Source

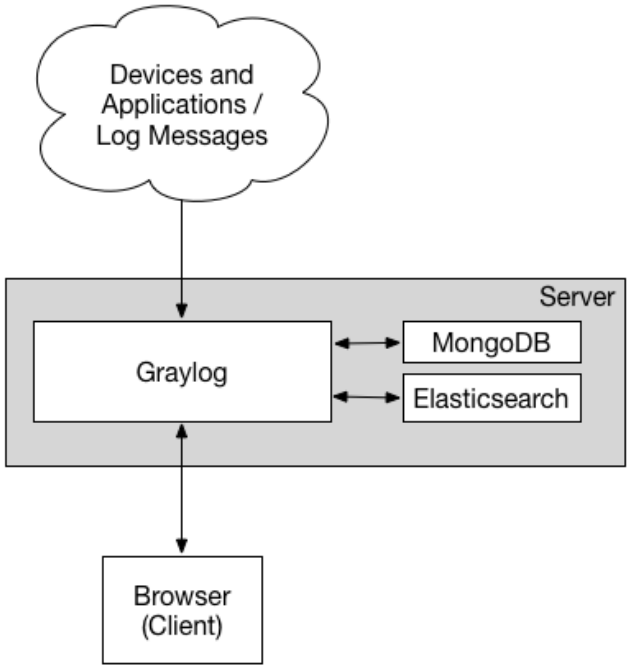
Graylog - Architecture

Graylog Web as browser based UI

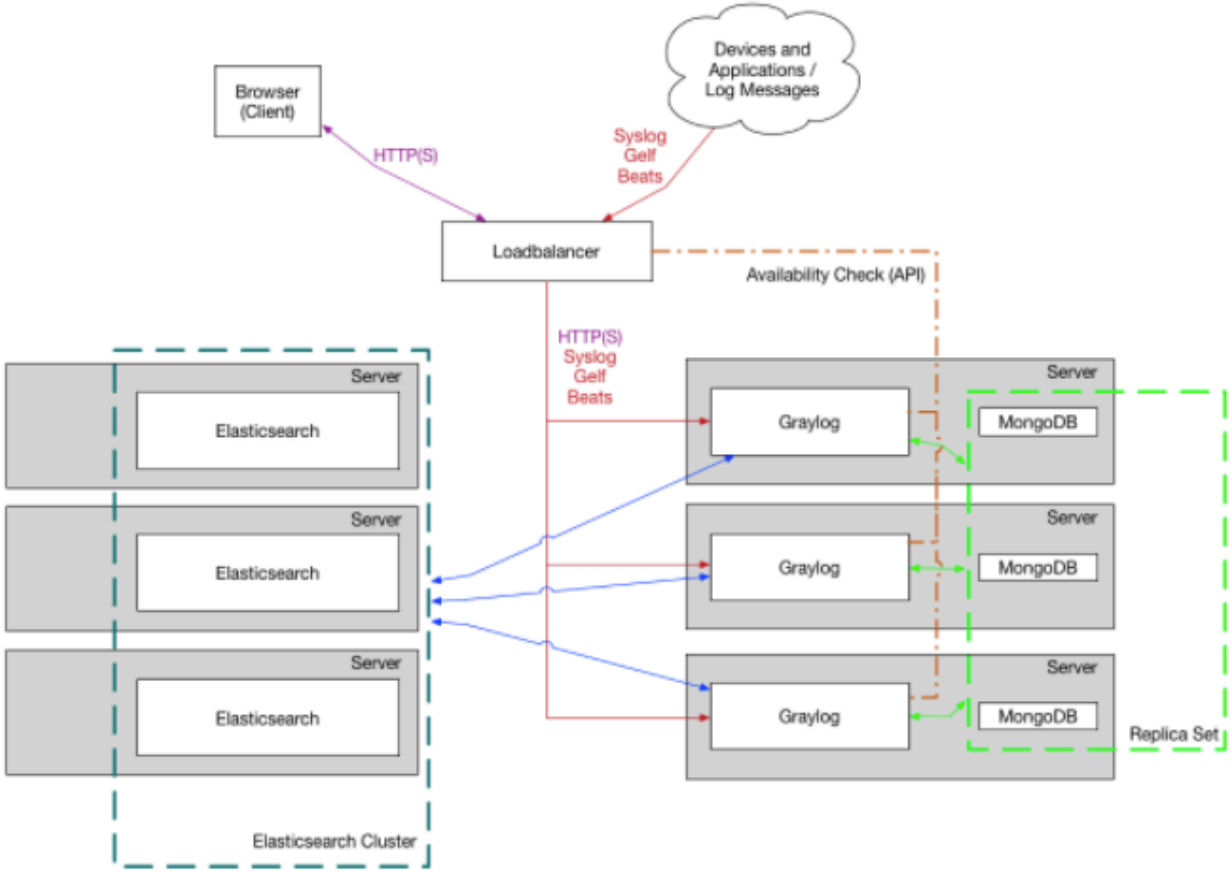
Graylog server: logic and configuration

It also includes mongoDB storing meta info and config

Elastic Search server: Storing log data information to be consumed

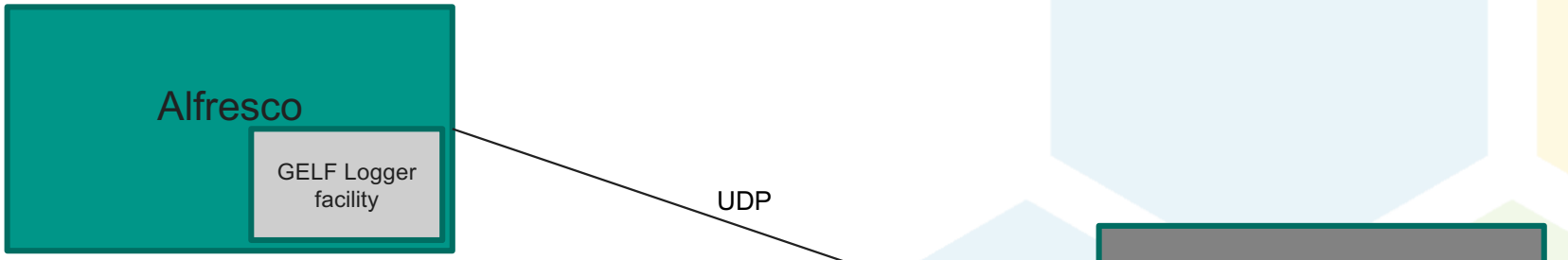


Graylog - Architecture



…and it's very scalable!

Graylog – Alfresco integration



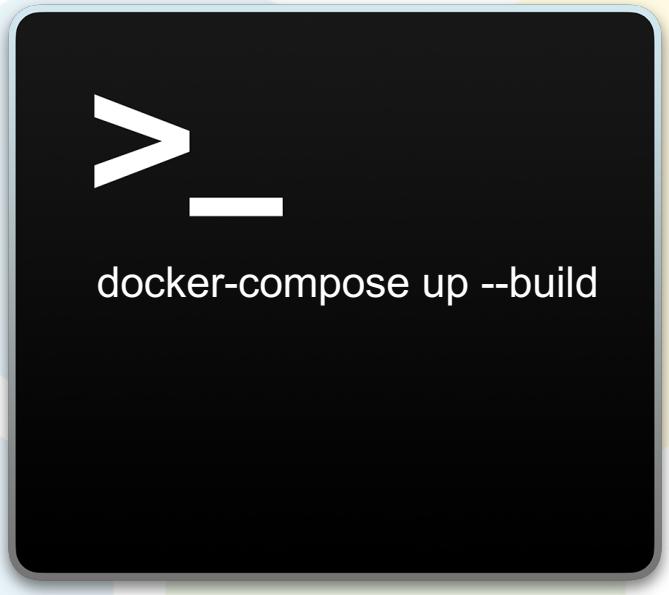
Graylog – Alfresco integration

What we need

- GrayLog
- Alfresco
- A Graylog log appender library
- Some configurations in log4j properties file

GrayLog

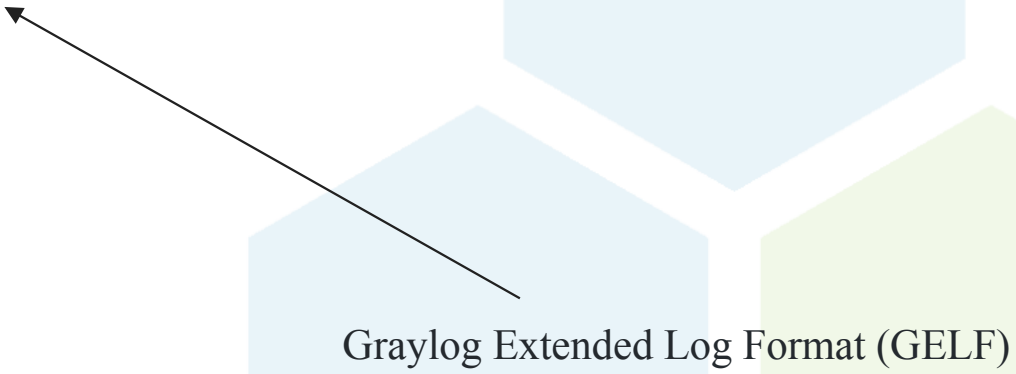
```yaml
version: '2'
services:
  mongo:
    image: "mongo:3"
  elasticsearch:
    image: "elasticsearch:2.3"
    command: "elasticsearch -Des.cluster.name='graylog'"
  graylog:
    image: graylog2/server:2.0.3-2
    environment:
      GRAYLOG_PASSWORD_SECRET: putyourpasswordhere
      GRAYLOG_ROOT_PASSWORD_SHA2: 00AABB.....
      GRAYLOG_REST_TRANSPORT_URI: http://127.0.0.1:12900
    depends_on:
      - mongo
      - elasticsearch
    ports:
      - "9999:9000"
      - "12900:12900"
      - "12201/udp:12201/udp"
      - "1514/udp:1514/udp"
```



Alfresco

GrayLog log appender library

```
<dependency>
<groupId>org.graylog2</groupId>
<artifactId>gelfj</artifactId>
<version>1.1.14</version>
</dependency>
```



GrayLog log appender library

A GELF payload:

```
{
  "version": "1.1",
  "host": "example.org",
  "short_message": "A short message that helps you identify what is going on",
  "full_message": "Backtrace here\n\nmore stuff",
  "timestamp": 1385053862.3072,
  "level": 1,
  "_user_id": 9001,
  "_some_info": "foo",
  "_some_env_var": "bar"
}
```

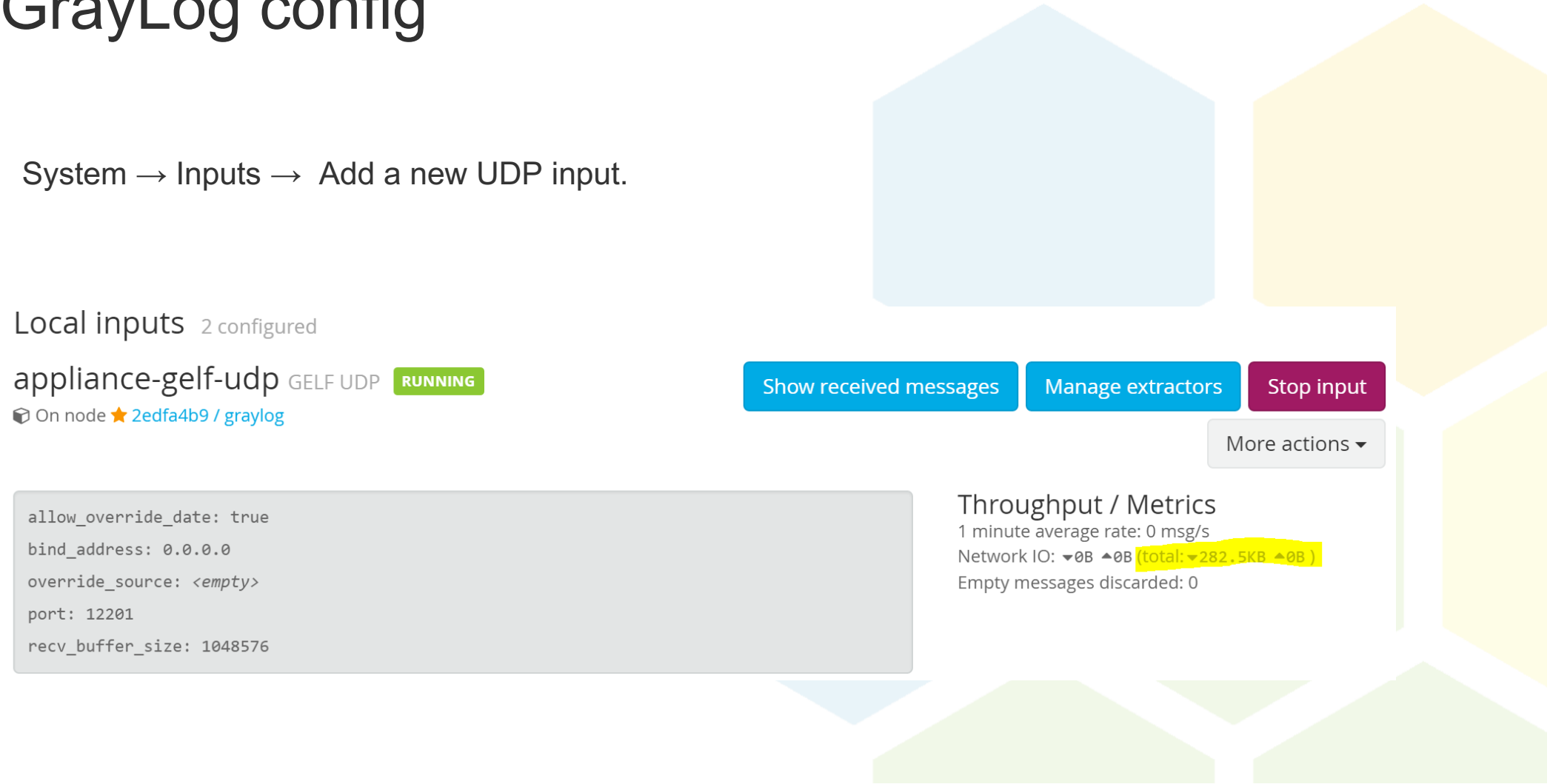
custom-log4j.properties

```
log4j.rootLogger=INFO, graylog2

log4j.appender.graylog2=org.graylog2.log.GelfAppender
log4j.appender.graylog2.graylogHost=localhost
log4j.appender.graylog2.graylogPort=12201
log4j.appender.graylog2.facility=gelf-java
log4j.appender.graylog2.layout=org.apache.log4j.PatternLayout
log4j.appender.graylog2.extractStacktrace=true
log4j.appender.graylog2.addExtendedInformation=true
log4j.appender.graylog2.additionalFields={'environment': 'localdev', 'application': 'YOUR-APPLICATION-NAME'}
```

GrayLog config

System → Inputs → Add a new UDP input.



Demo

Details

GrayLog Vs ELK

- ELK = Elastic Search + Logstash + Kibana
- They both solve a similar problem with similar technologies
- GrayLog solves a specific problem whereas ELK is more generic
- GrayLog interface easier and simpler than Kibana

It’s your choice actually ☺

GrayLog

- Simple, scalable, user friendly tool for centralized logging
- Search, reports, alerts
- Suitable for new architectural trends

- It’s part of your architecture, don’t let it become a bottleneck!

Fran Alvarez
Ixxus

fran.alvarez@ixxus.com