

Logging in the era of Microservices

Johannes Unterstein



Software Engineer @mesosphere

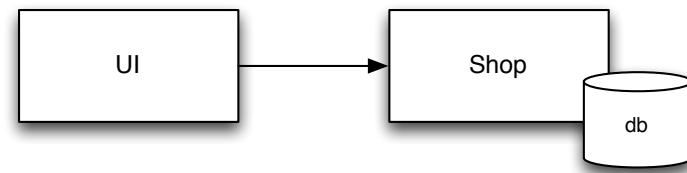
Agenda

- Motivation
- The elastic stack
- Cloud solutions
- DEMO!
- Dashboards
- Conclusion

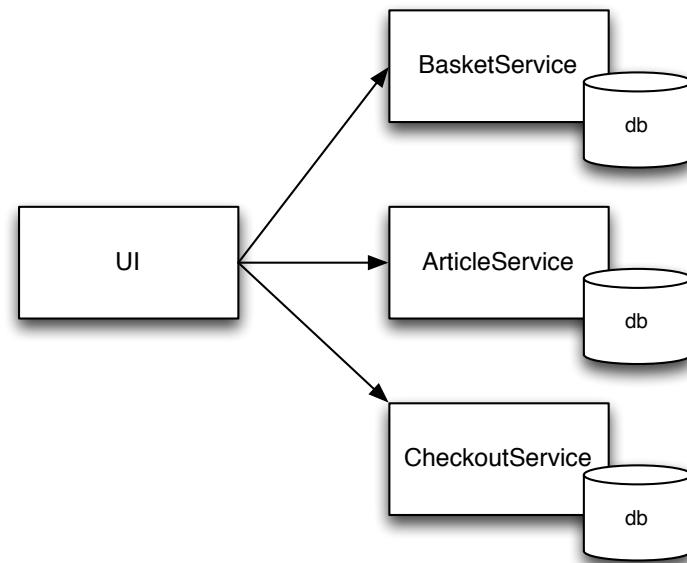
Motivation

- „WTF microservices?“ a.k.a. „vi is not enough“
- Logging is important and even got harder
- Satisfy information needs of different stakeholders
- Not only logging, also monitoring and alerting

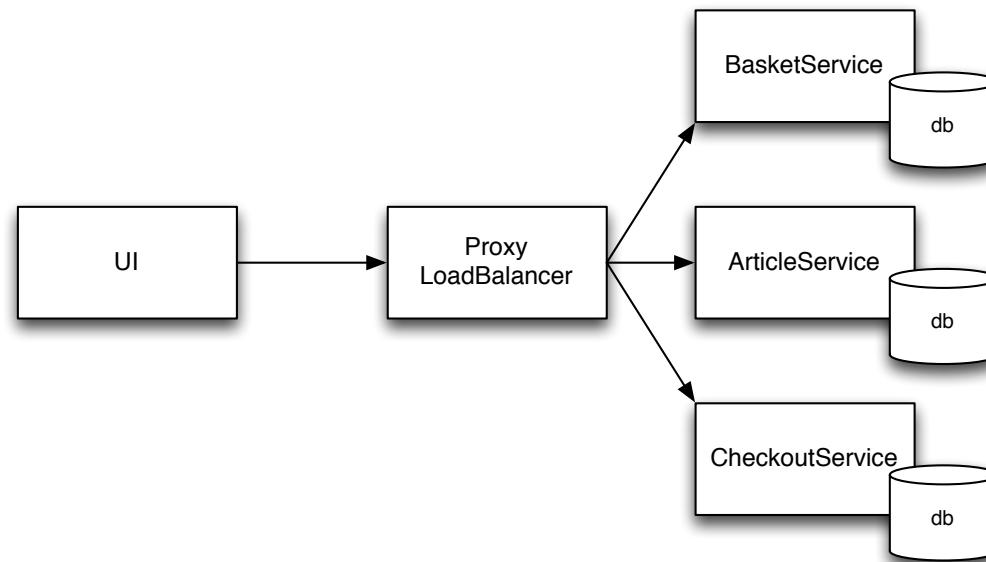
Motivation



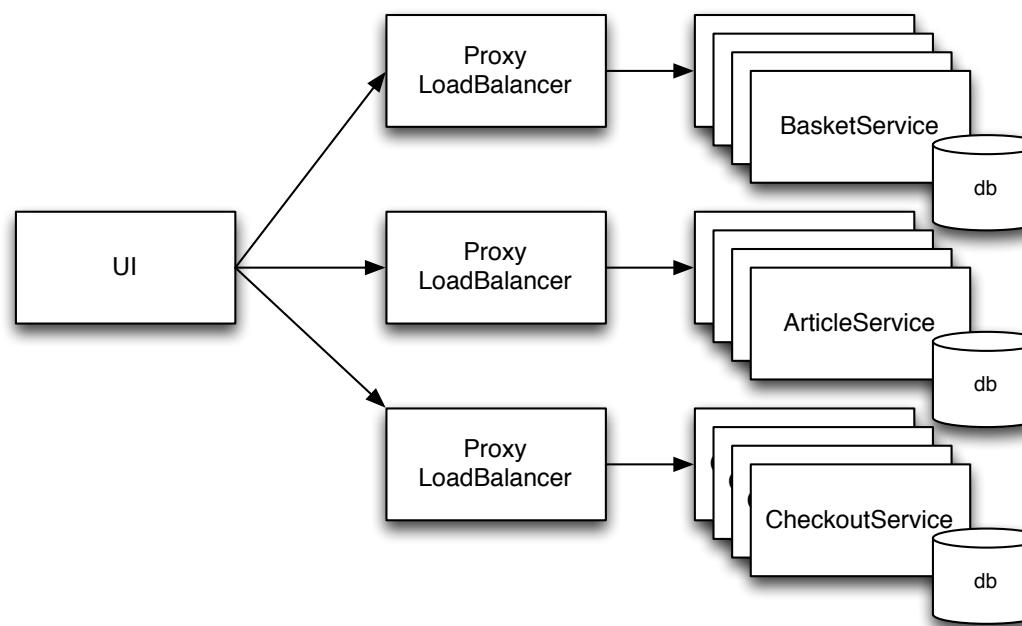
Motivation



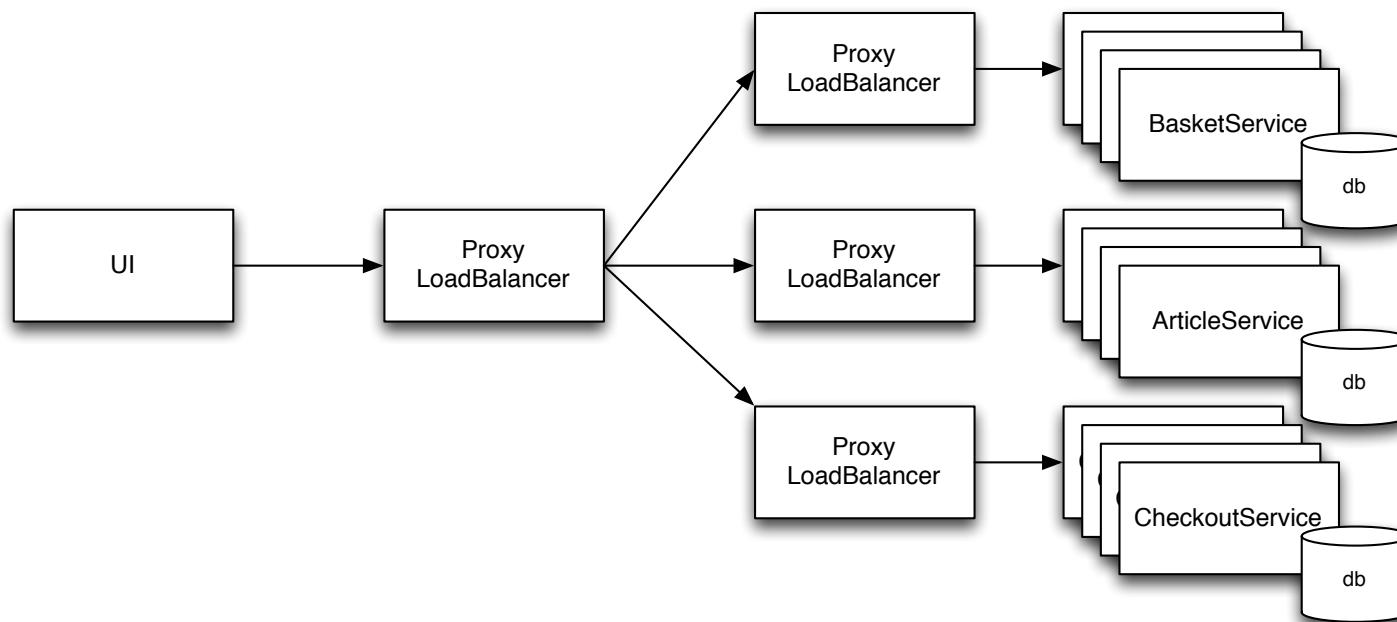
Motivation



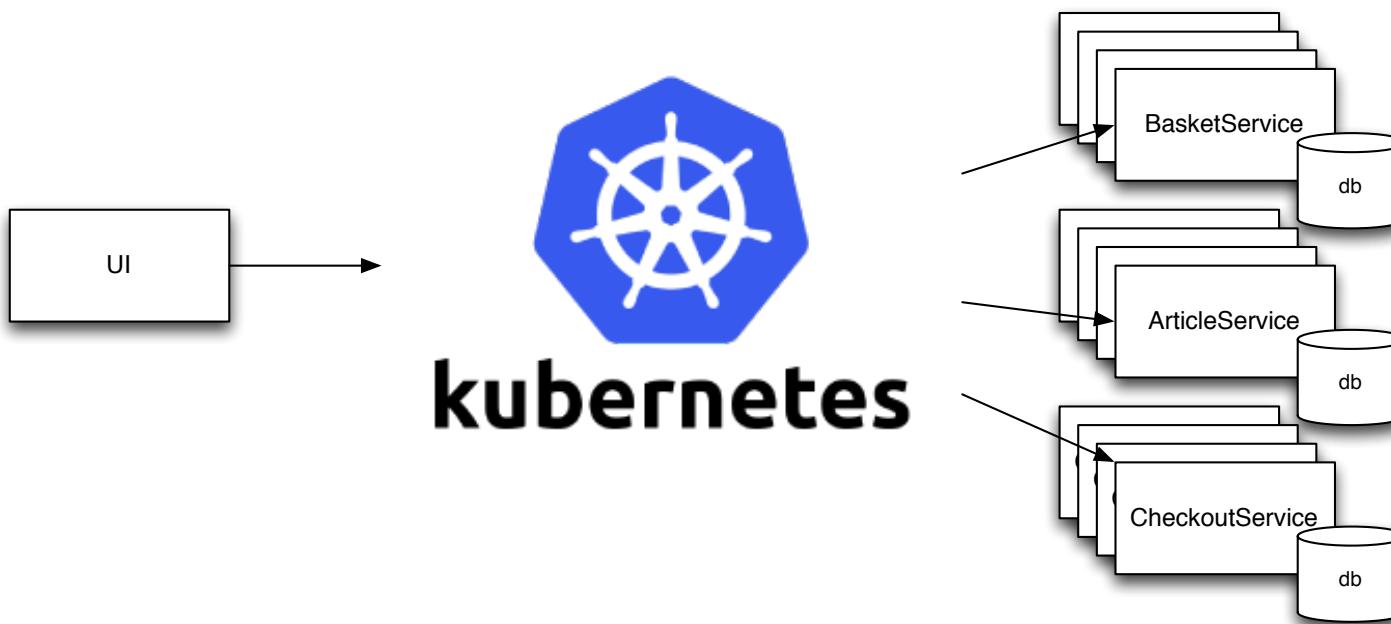
Motivation



Motivation



Motivation



Motivation



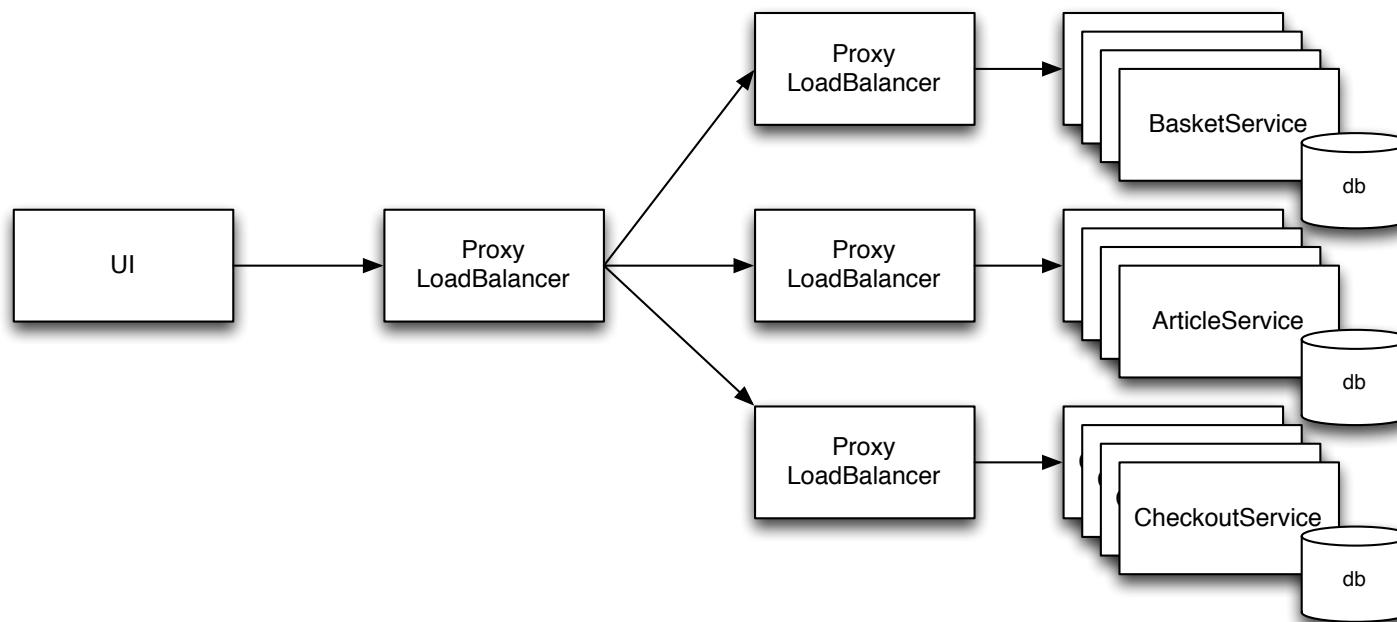
Motivation



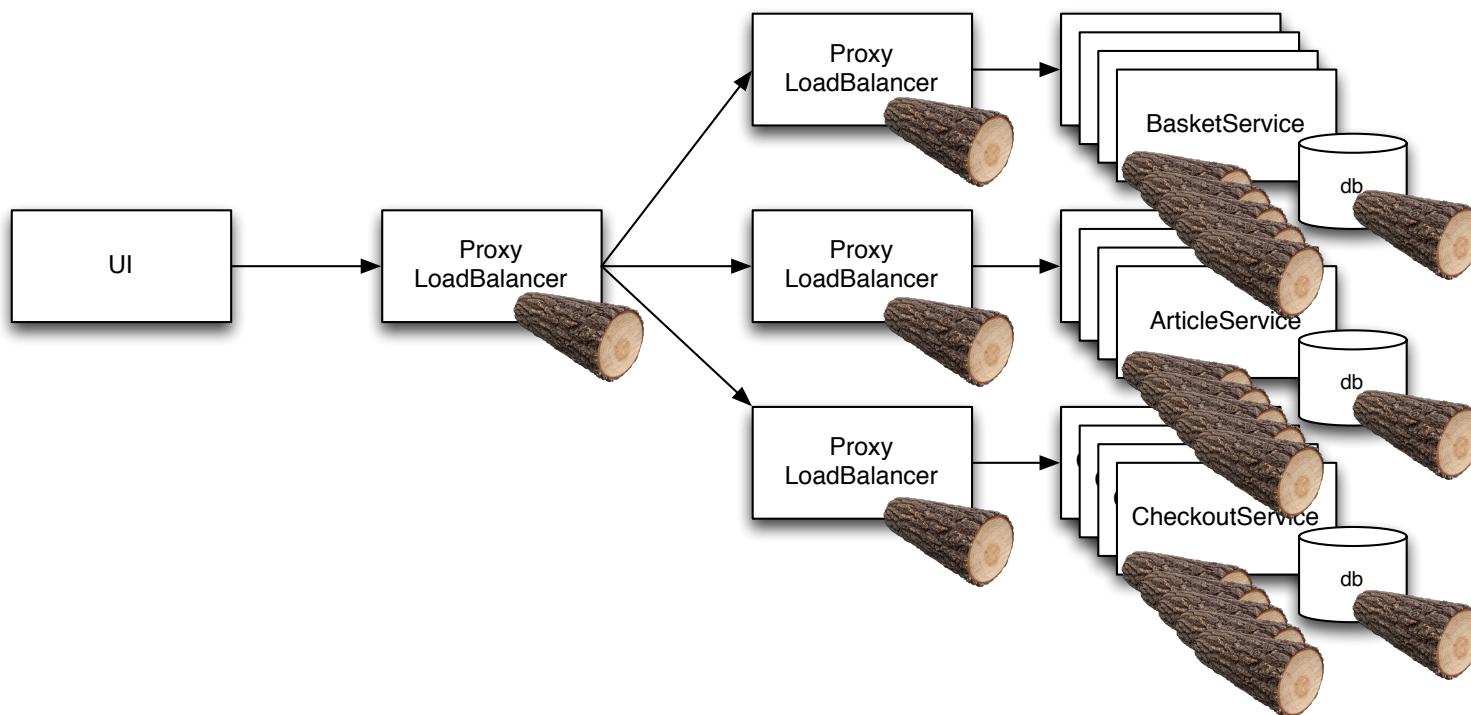
Motivation

WTF?

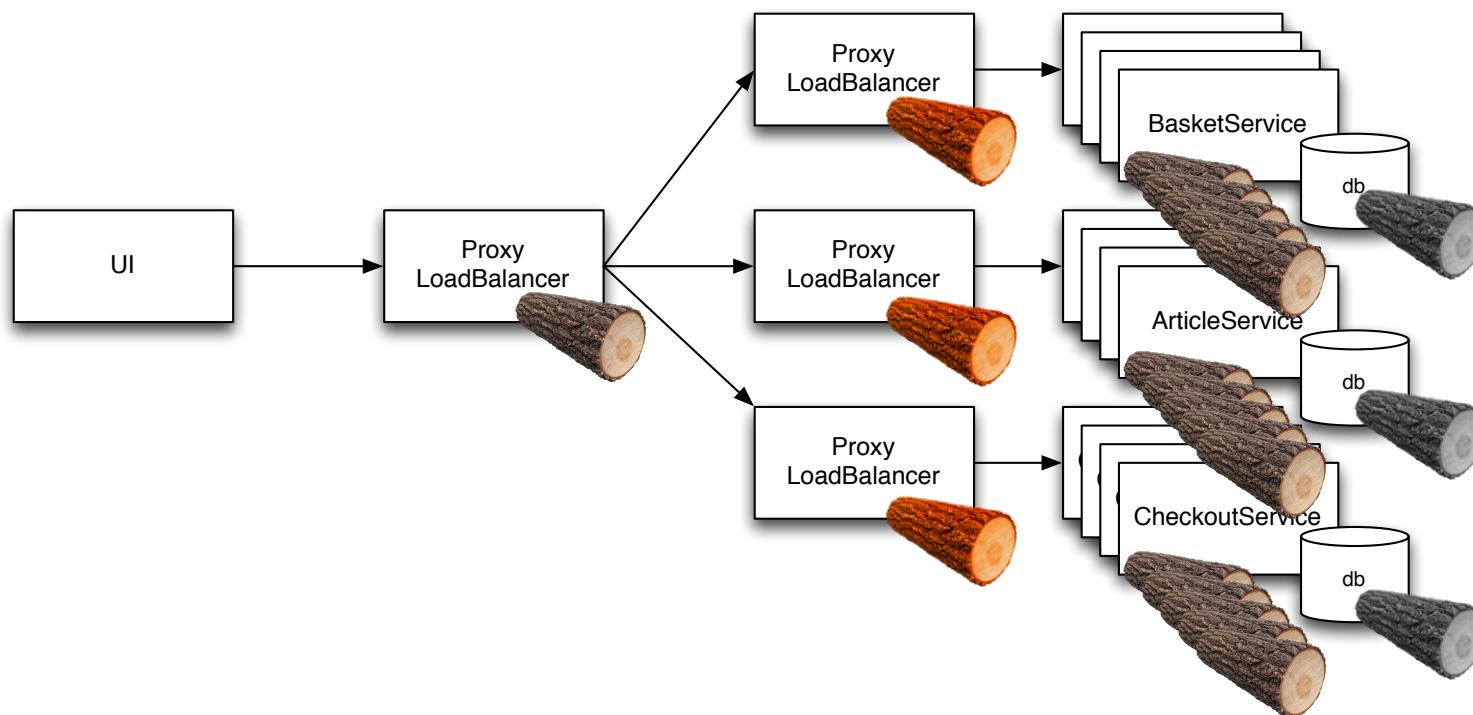
Motivation



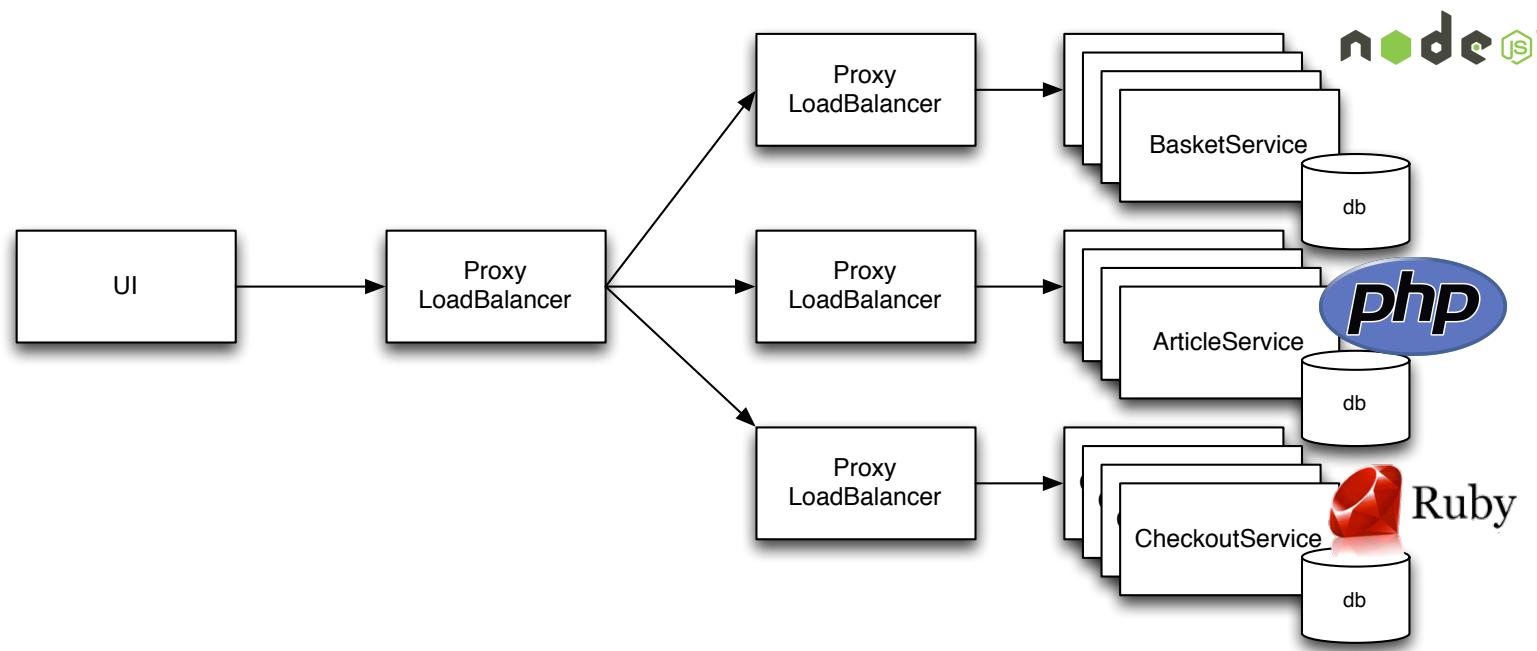
Motivation



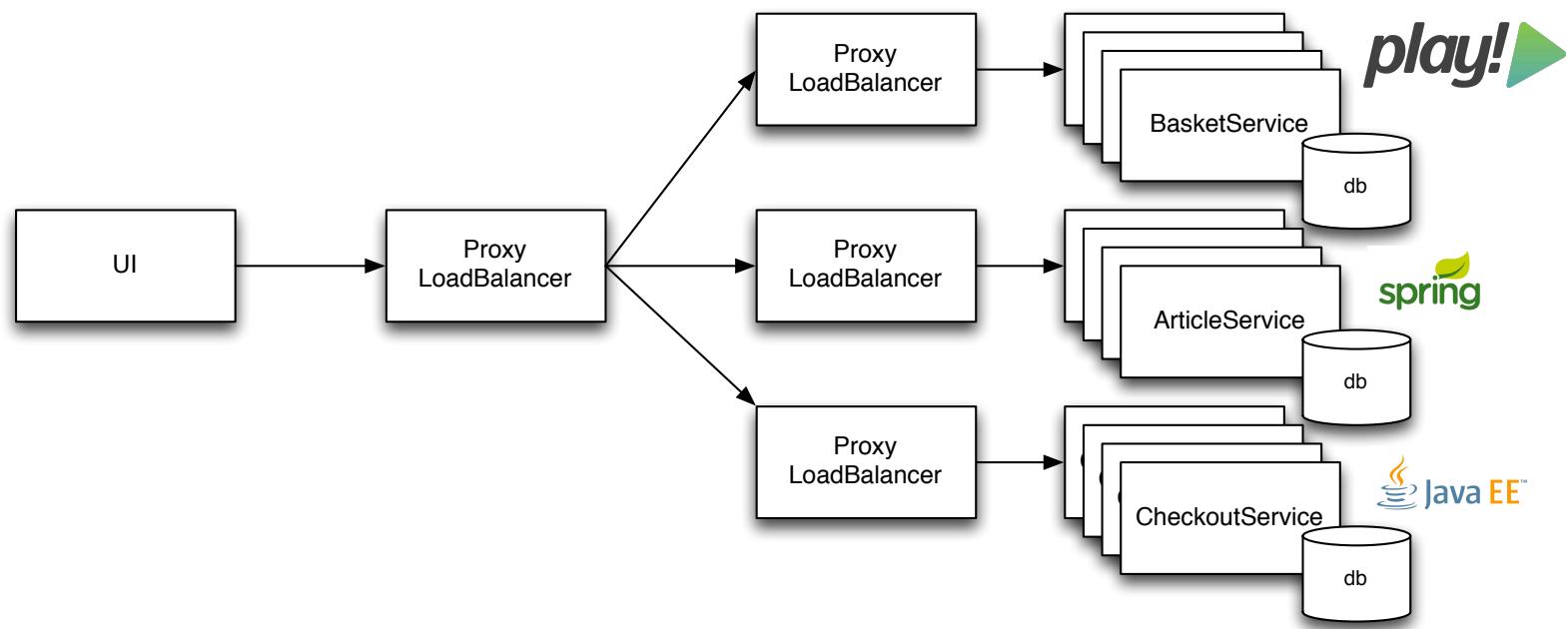
Motivation



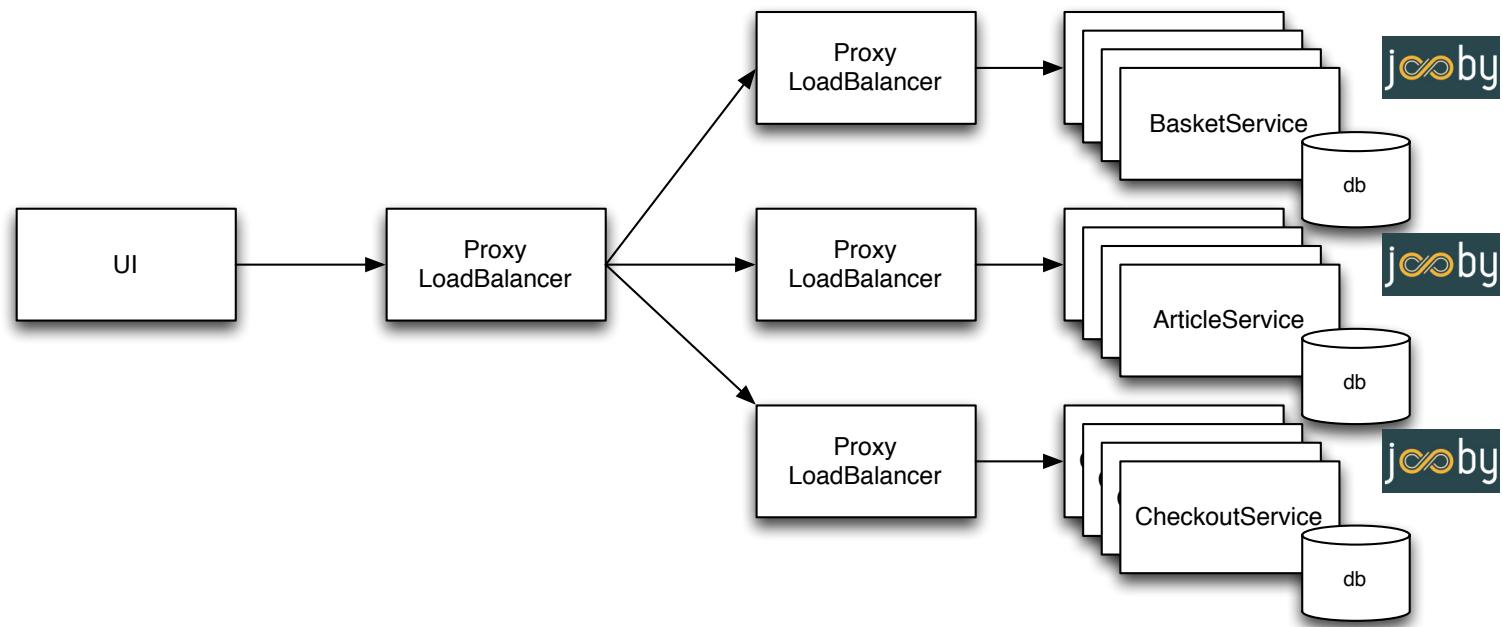
Motivation



Motivation



Motivation



The elastic stack

-  elasticsearch
-  logstash
-  kibana
-  beats
- (Watcher)

The elastic stack

- Elasticsearch
 - Distributed database
 - Search engine based on Lucene
 - Scaleable
 - Replicated
 - REST & JSON

The elastic stack

```
# nginx default access log
127.0.0.1 -- [02/Nov/2015:12:41:47 +0100] "GET / HTTP/1.1" 200 612 "http://localhost:8080/"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/46.0.2490.80 Safari/537.36"

# example adapted nginx access log
localdock:8080 192.168.99.1 [02/May/2016:21:58:23 +0000] "GET /articleservice/articles
HTTP/1.1" 200 318 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.36 (
KHTML, like Gecko) Chrome/50.0.2661.86 Safari/537.36" 2.398 2.398 request-9-1462226301.
048-192.168.99.1-548 sess9-1462223552.986-501

# example tomcat log
Nov 13, 2014 2:11:09 PM org.apache.catalina.startup.Catalina start

# example jooby log (logback)
[2016-05-02 21:58:13,645]-[main]-[]-[INFO ]-[info.unterstein.BasketService]-[[dev@netty]:
Server started in 10128ms

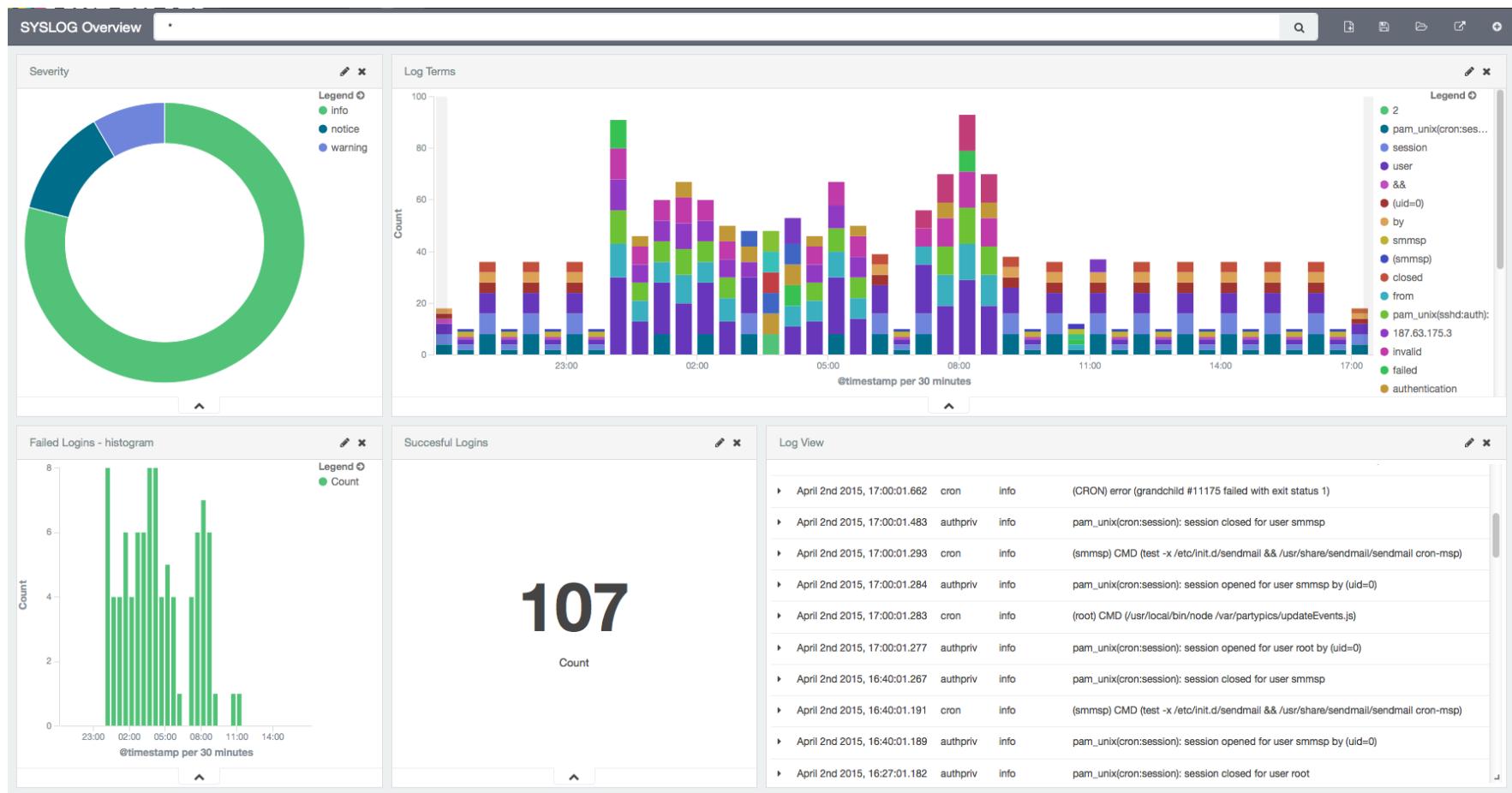
# example nodejs log
info: Hello world! timestamp=1402286804314, pid=80481
```

The elastic stack

- Logstash
 - Sync logs from host to elasticsearch
 - Own operation system process
 - Unify logs with grok patterns
 - <https://github.com/logstash-plugins/logstash-patterns-core/tree/master/patterns>
 - <http://grokdebug.herokuapp.com/>

The elastic stack

- Kibana



The elastic stack

- Beats
 - Analyzes protocols HTTP, SQL, Files, ...
 - Analyzes own and third party services
 - Syncs to Elasticsearch
 - Filebeat, Metricbeat, Dockbeat, SpringBeat,...

The elastic stack

- Watcher
 - Premium plugin
 - Alerting based on Elasticsearch queries
 - „More than 10 errors in 1 minute -> SMS all Ops“
 - „More than \$X in sales -> Mail sales manager“

Cloud solutions



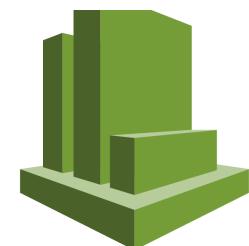
AppDynamics



papertrail

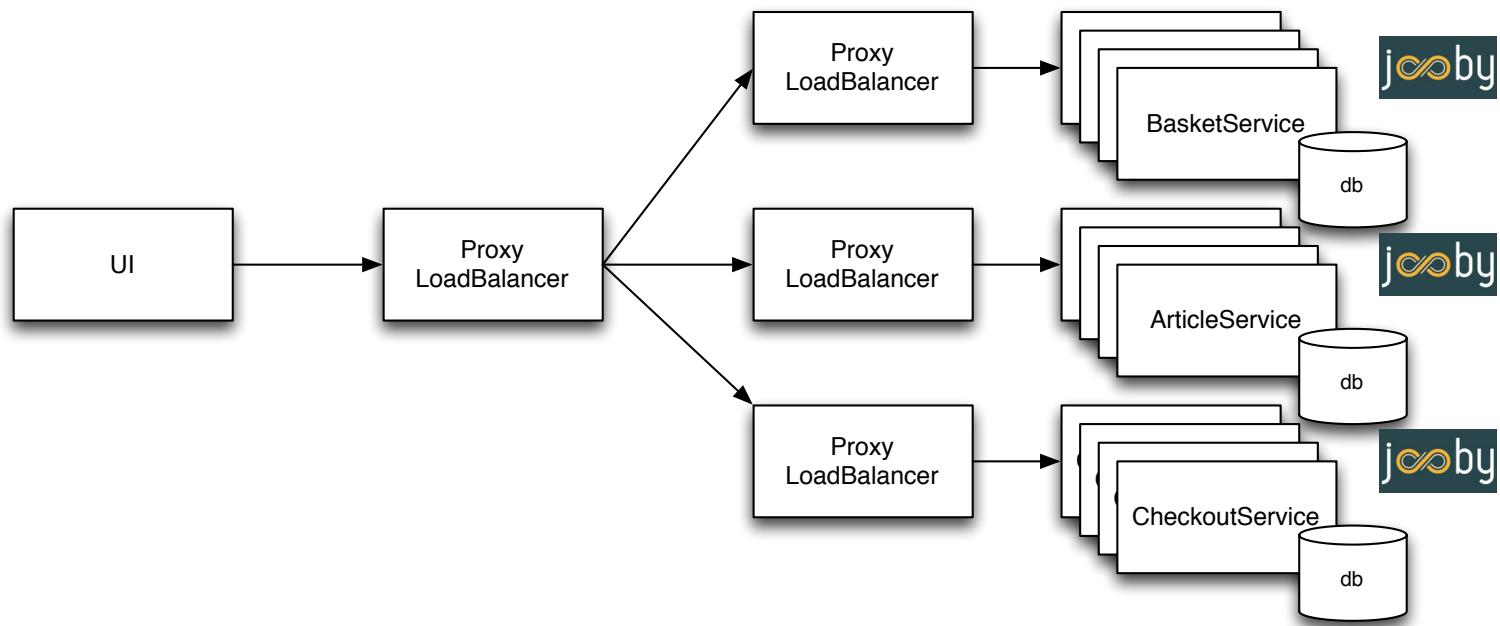


ploggr

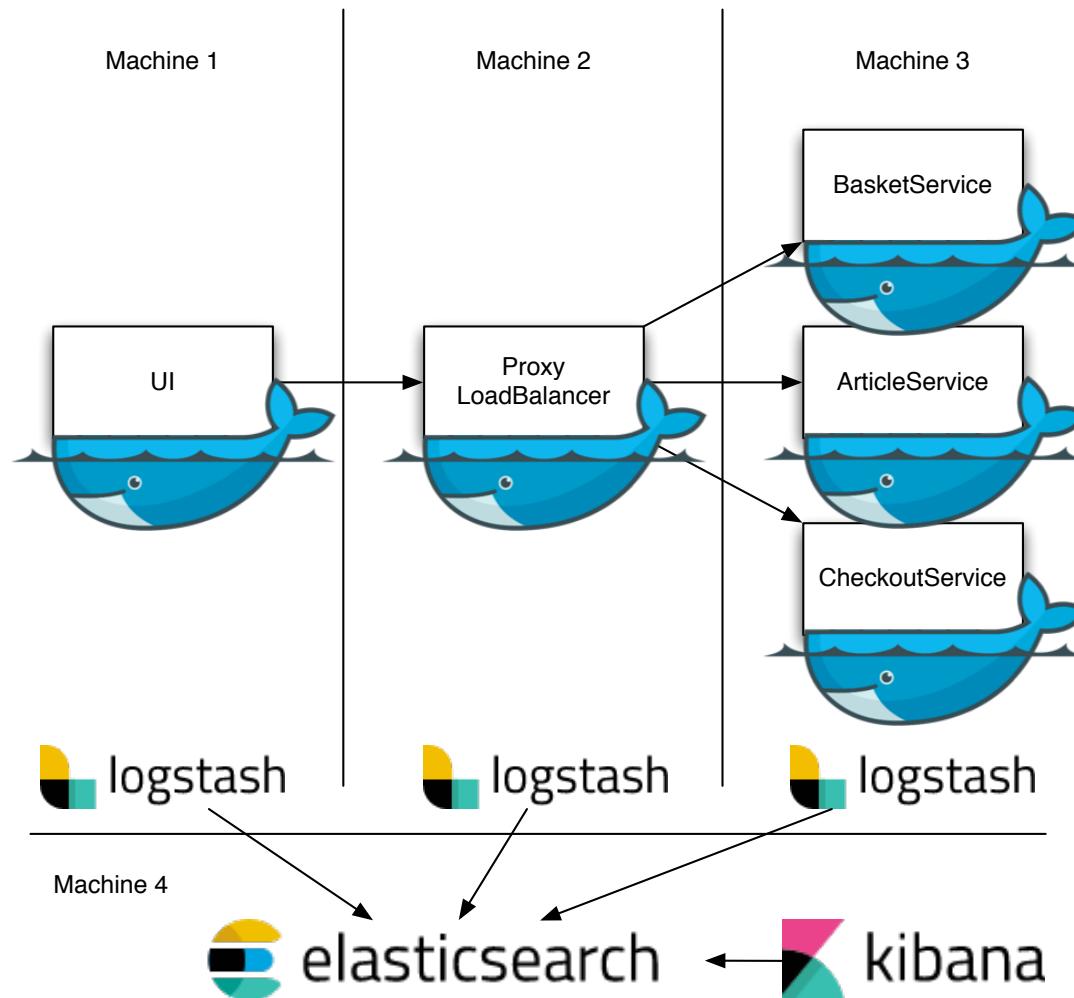


AWS CloudWatch

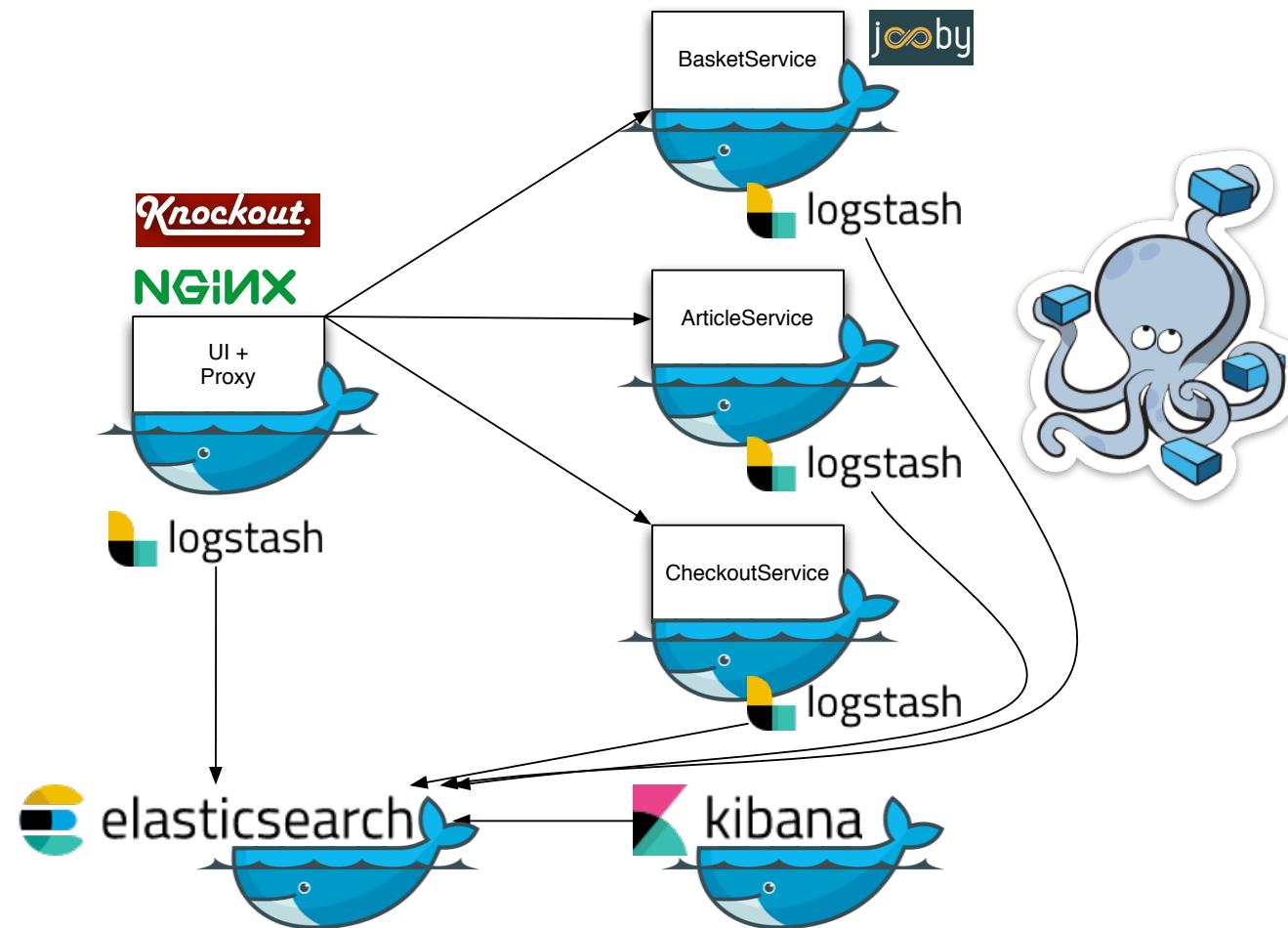
DEMO!



DEMO!!



DEMO!!!



<https://git.io/vwV6S>

Logging 101

- Create RequestId/SessionId in first load balancer and pass to following systems
- Enrich logging statements with markers
- Add currently logging app, node, instanceId, ...
- Long static part of log message
- Use different log messages

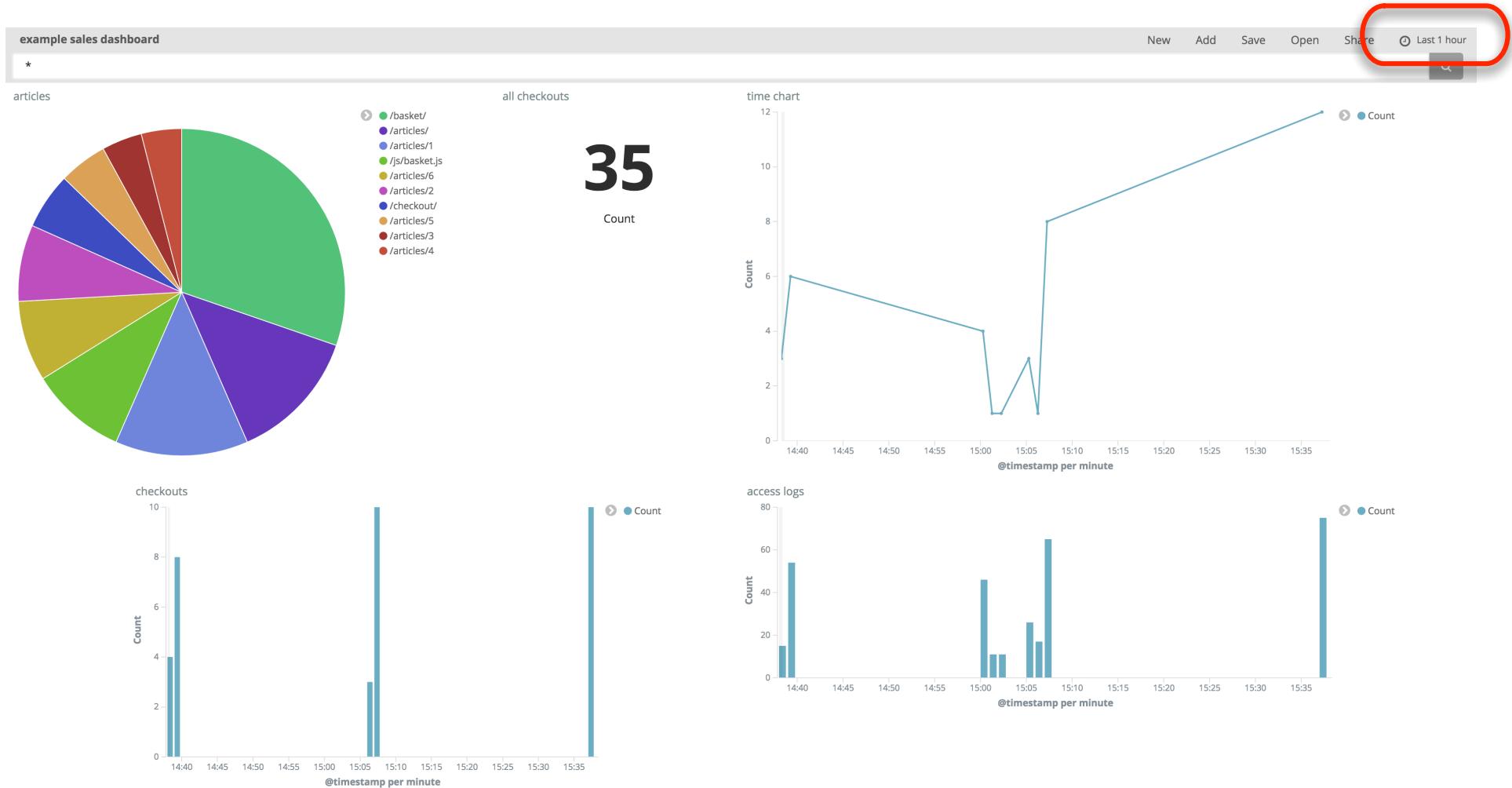
Dashboards

- Different stakeholders, different questions
- Different views on same data
- „.... just another Kibana configuration!“
- Import and export with elasticdump

Dashboards

- Sales
 - How many sales this week?
 - How many conversions by form A, B, C ?
 - How many traffic from channel X, Y, Z?

Dashboards



Dashboards

- Marketing
 - How successful was campaign A, B, C?
 - Was mailing X, Y, Z accepted?
 - Was button relocate/restyling successful?

Dashboards

- Dev
 - F*@k! Something crashed - what happened?
 - Was my performance enhancement successful?
 - Did someone hit my new button? :-)

Dashboards

- Ops
 - Why is service A, B, C slow?
 - How healthy is my system?
 - Do I run out of resources?
 - When do I have traffic peaks?

Conclusion

- Just a quick demo - imagine the possibilities!
- Services do not know about ELK
- Logging is awesome (again) and you will love it!
- Enjoy the conference :-)

<https://git.io/vwV6S>

More about x-pack

- ELK introduction webinar by Jordan Sissel
 - <https://www.elastic.co/webinars/introduction-elk-stack>
- „Awesome logging infrastructure“ talk by Alex Reelsen
 - <https://speakerdeck.com/elastic/awesome-logging-infrastructure-using-the-elastic-stack>
- X-Pack overview
 - <https://www.elastic.co/de/blog/heya-elastic-stack-and-x-pack>