ELK stack - Problems and (our) solutions

Mladen Čikara - Liferay

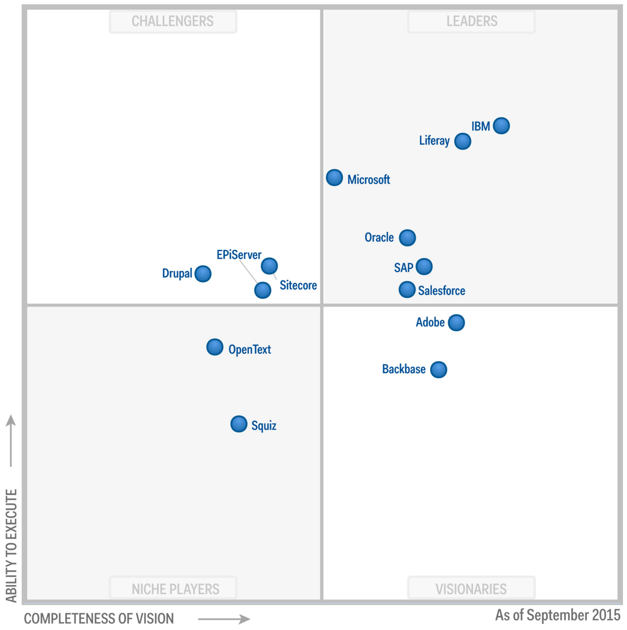
About me

- Worked at IN2, Identalia Consulting, Liferay
- Worked on Financial software, Customer Relation Software, Portals
- Worked with Java EE, RDBMS, MQ Servers
- Interests - Java technologies, Enterprise Integration Patterns, Virtualization and Containers

About Liferay

- Liferay Portal - free and open source enterprise portal
- Java based
- Gartner puts Liferay as leader in Magic Quadrant for last six years
- And we want to stay there, so ….

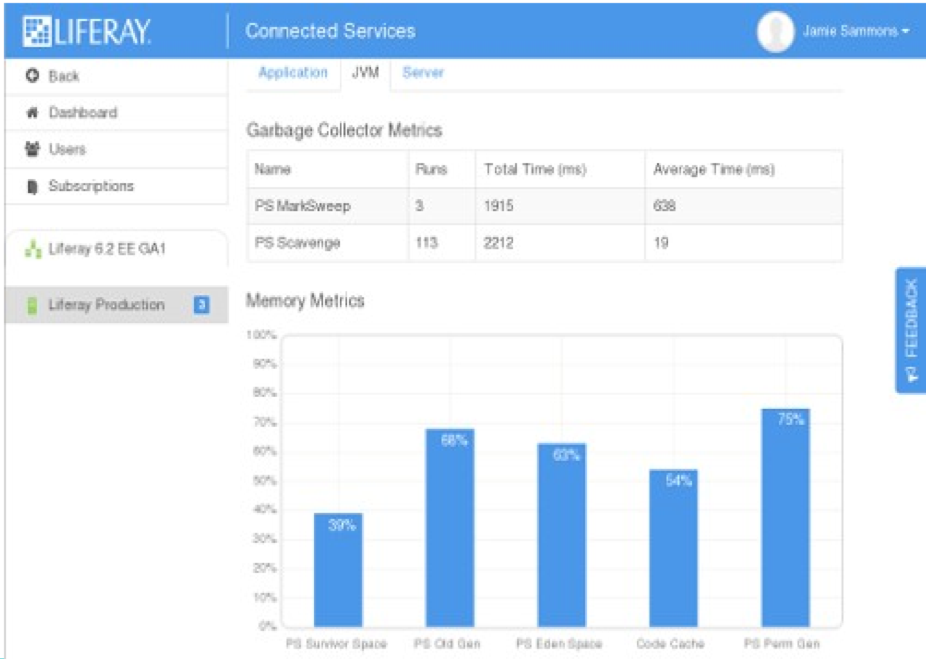
Figure 1. Magic Quadrant for Horizontal Portals



Source: Gartner (September 2015)

About Liferay Connected Services (LCS)

- Portlet that helps with managing and monitoring Liferay portals
- Easy Fix Pack Management
- Monitoring Metrics
- Dashboard for accessing different environments from one place
- Made in Croatia

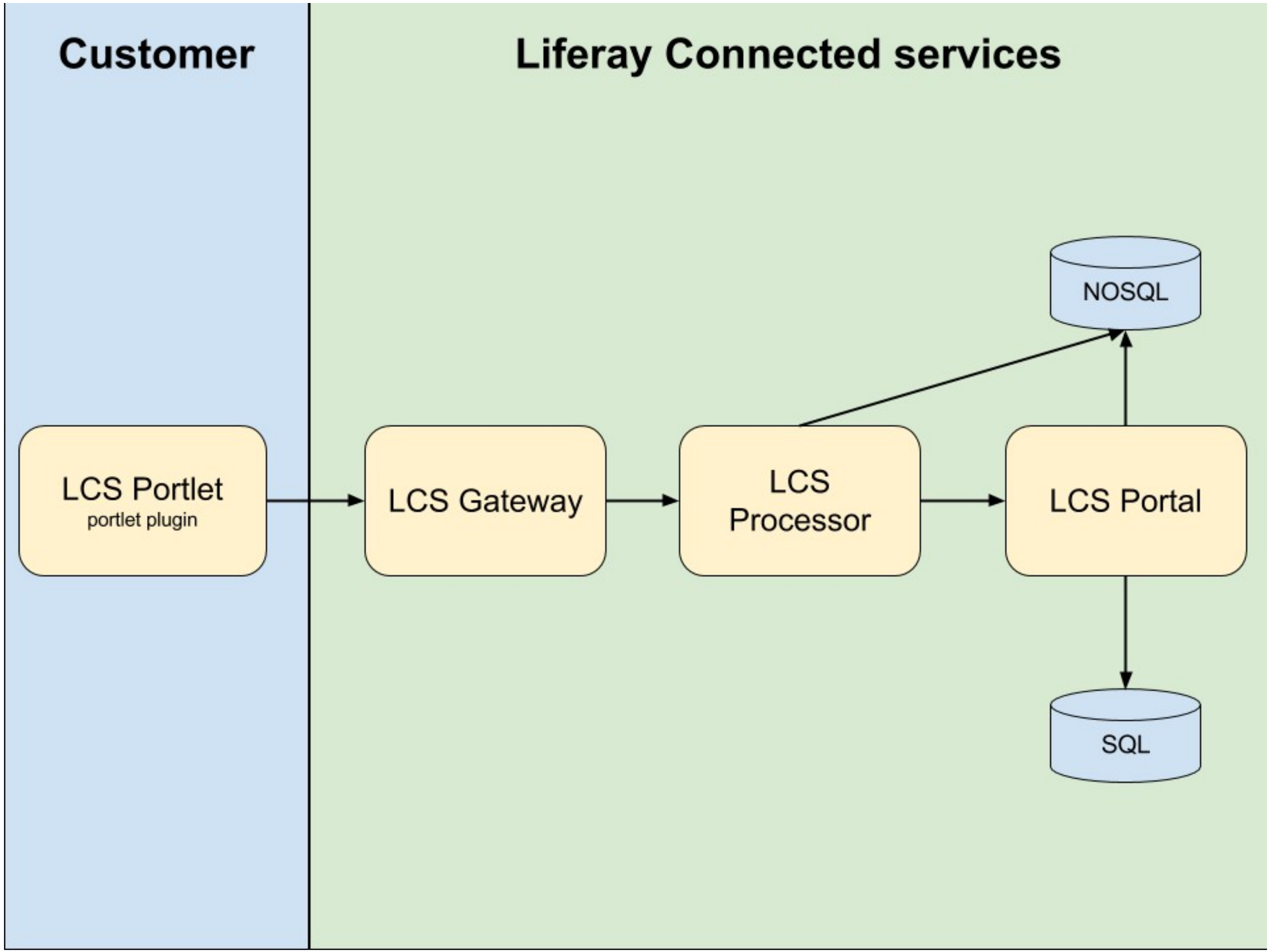


Garbage Collector Metrics

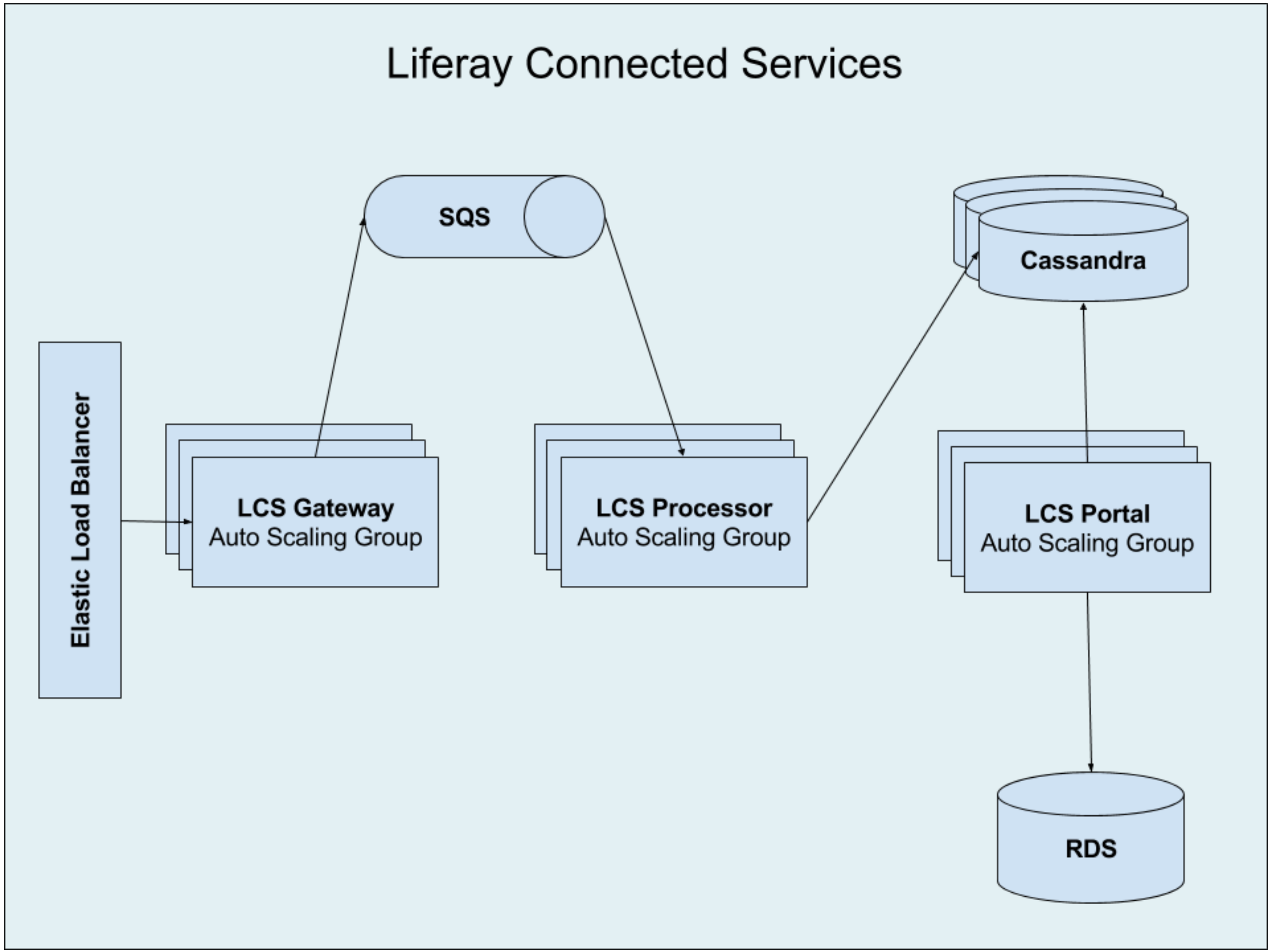
Name	Runs	Total Time (ms)	Average Time (ms)
PS MarkSweep	3	1915	638
PS Scavenge	113	2212	19

Memory Metrics

LCS architecture (I)



LCS architecture (II)



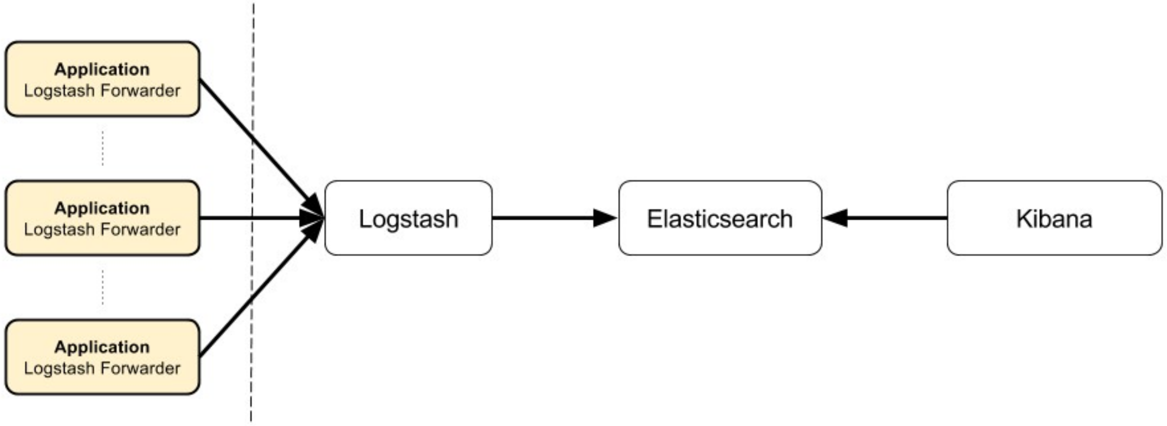
Problem

- How to find and monitor problems in different parts of the system
- Auto scaling group can create and remove instances without user input
- One place to “see” whole system
- Easy searching
- Advanced analytics on gathered data

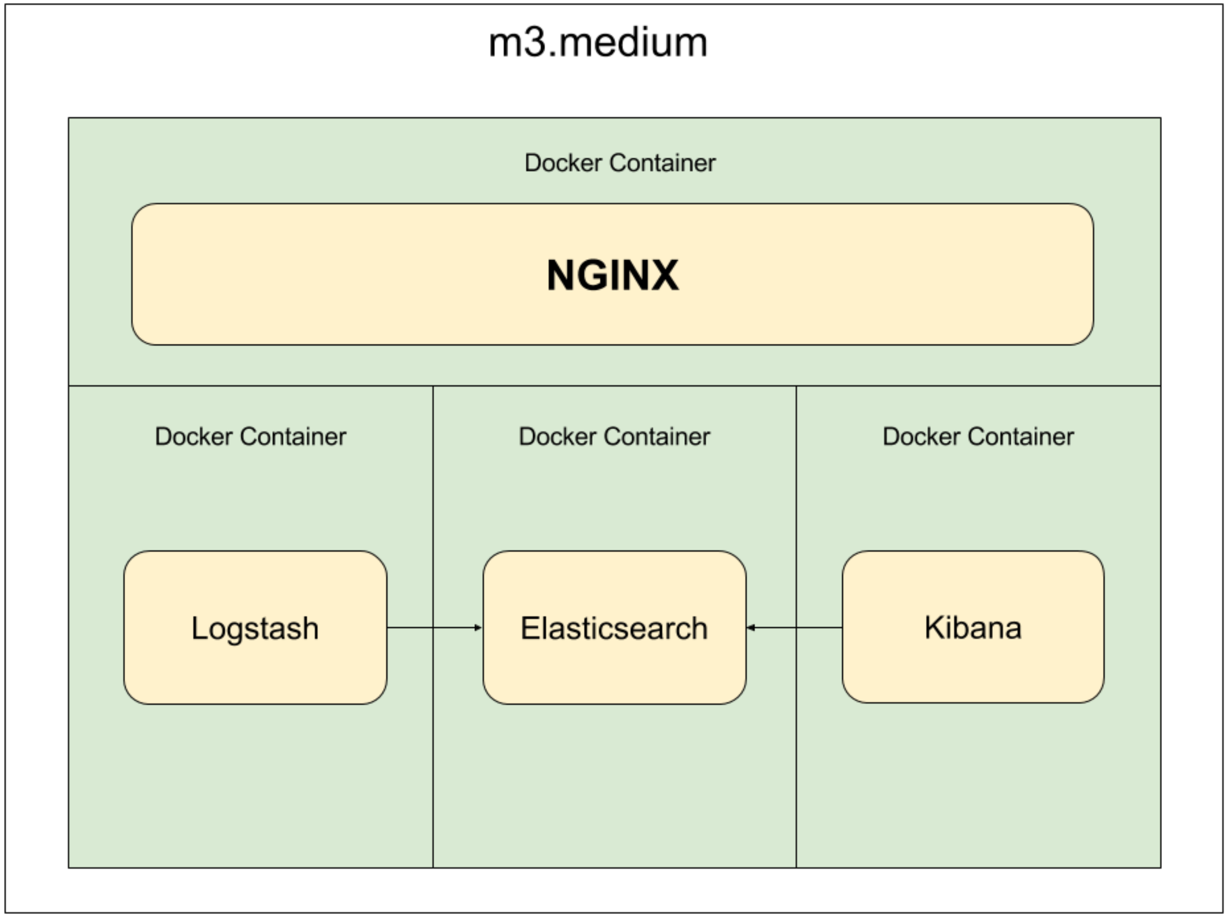
About ELK stack

- Elasticsearch - Search server based on Lucene
- Logstash - Tool for gathering and managing events and logs
- Kibana - Open source data visualisation platform
- ELK - Collecting, processing, storing, searching and displaying event data
- Very Active Community - Logstash has over 150 plugins

ELK architecture (I)



ELK architecture (II)



Problem 1

- Clients stopped sending logs to logstash
- Error message

```
Failed to tls handshake with <ip> x509: certificate has expired or is not yet valid
```

- Inspecting certificate

```
openssl x509 -in logstash-forwarder.crt -noout -text
```

Solution 1

- Recreate certificate with longer validity

```
sudo openssl req -config /etc/pki/tls/openssl.cnf -x509 -days 3650 -batch -nodes -newkey rsa:2048 \

-keyout private/logstash-forwarder.key -out certs/logstash-forwarder.crt
```

- Redistribute certificate to all clients
- You should understand every part of your configuration
- Disable copy-paste at OS level :-)

Problem 2

- Our ELB is logging event in S3 bucket
- ELB was working long before ELK stack
- 65 MB per day of logs
- S3 input plugin for logstash would not start collecting logs
- No error message

Solution 2

- Not really a problem
- Tried S3 plugin on bucket with less data and it worked
- Started collecting logs after two hours
- Lesson learned - Try things out on lesser scale

Problem 3

- Elasticsearch crashes after disk partition fills
- Whole system is down
- 3 GB of logs every day
- DEBUG log level can really fill in elasticsearch

Solution 3

- Add more space to Elasticsearch partition
- Crontab job to delete old logs and all DEBUG logs older than two hours
- Move to hosted Elasticsearch

Problem 4

- Logstash crashes with Out Of Memory Error
- After recovering of filled disk failure
- All logstash forwarders sending backed up logs at the same time

Solution 4

- Start logstash forwarders one by one and waiting to send all backed up logs
- Move Logstash to separate instance
- Create Auto Scaling Group for Logstash instances
- Separate Logstash gateway and Logstash processor

Problem 5

- Some consumers report connection refused for short period
- Starts working without interventions

Solution 5

- Same as previous solution
- Auto scaling group and separating gateway and processor

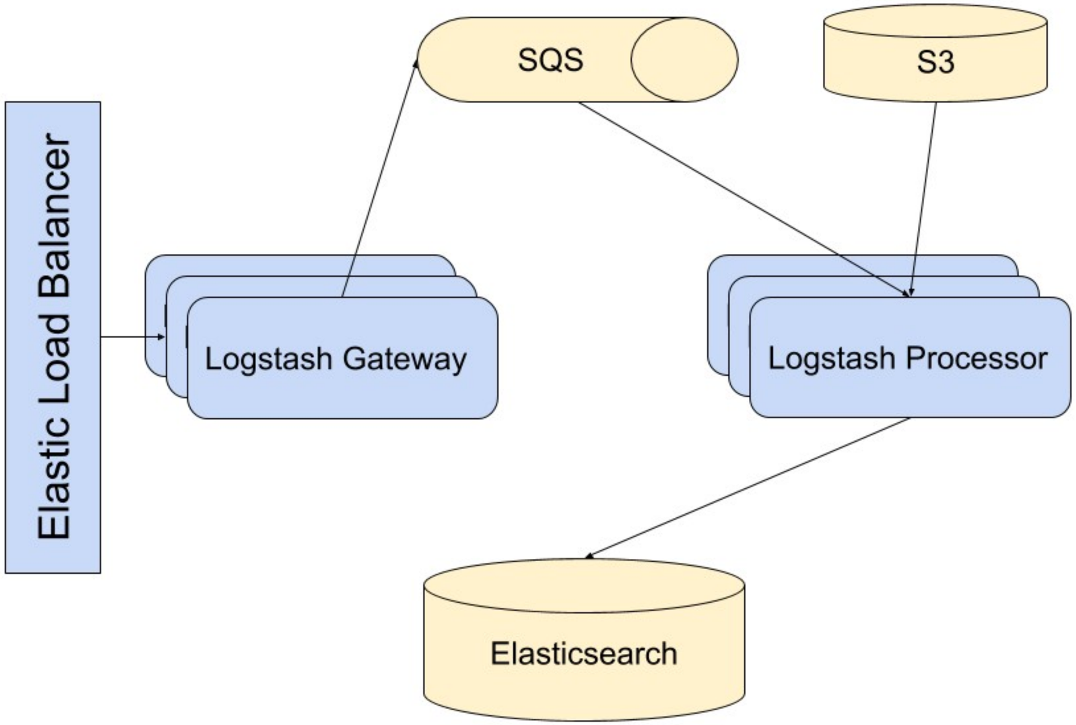
Problem 6

- Securing access to Elasticsearch and Kibana

Solution 6

- Installing Nginx
- Create user and password in /etc/nginx/.htpasswd

ELK architecture - finish



Conclusion

- Delivers what it promises
- Easy to scale part by part
- Takes some time to be adopted by team
- Dynamic development
  - Logstash-Forwarder → filebeat
  - Logstash versions
    May 2015 (v1.4.4) → May 2016(v2.3.2)

Questions?

We are hiring! igor.beslic@liferay.com