Realtime Log aggregation for Apache Storm

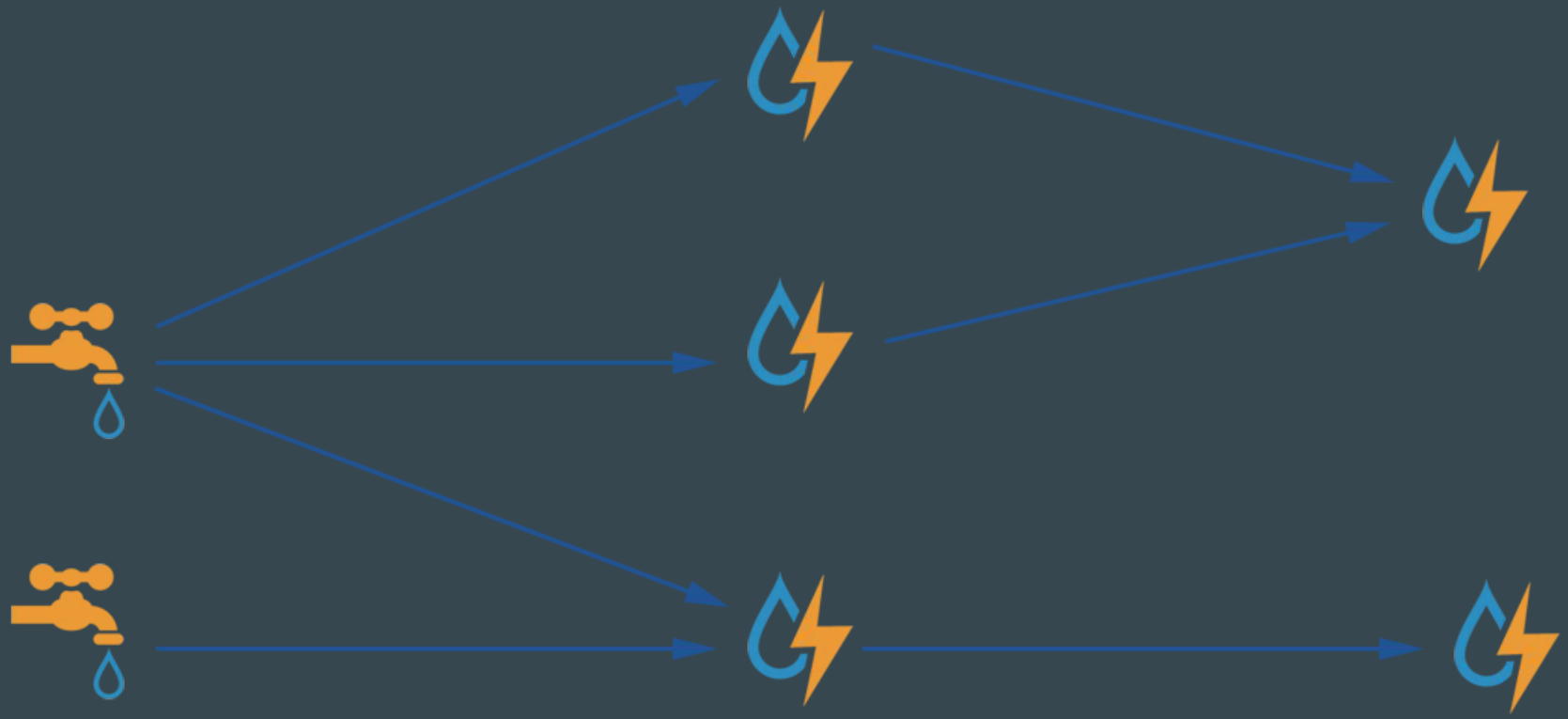
...

Karri

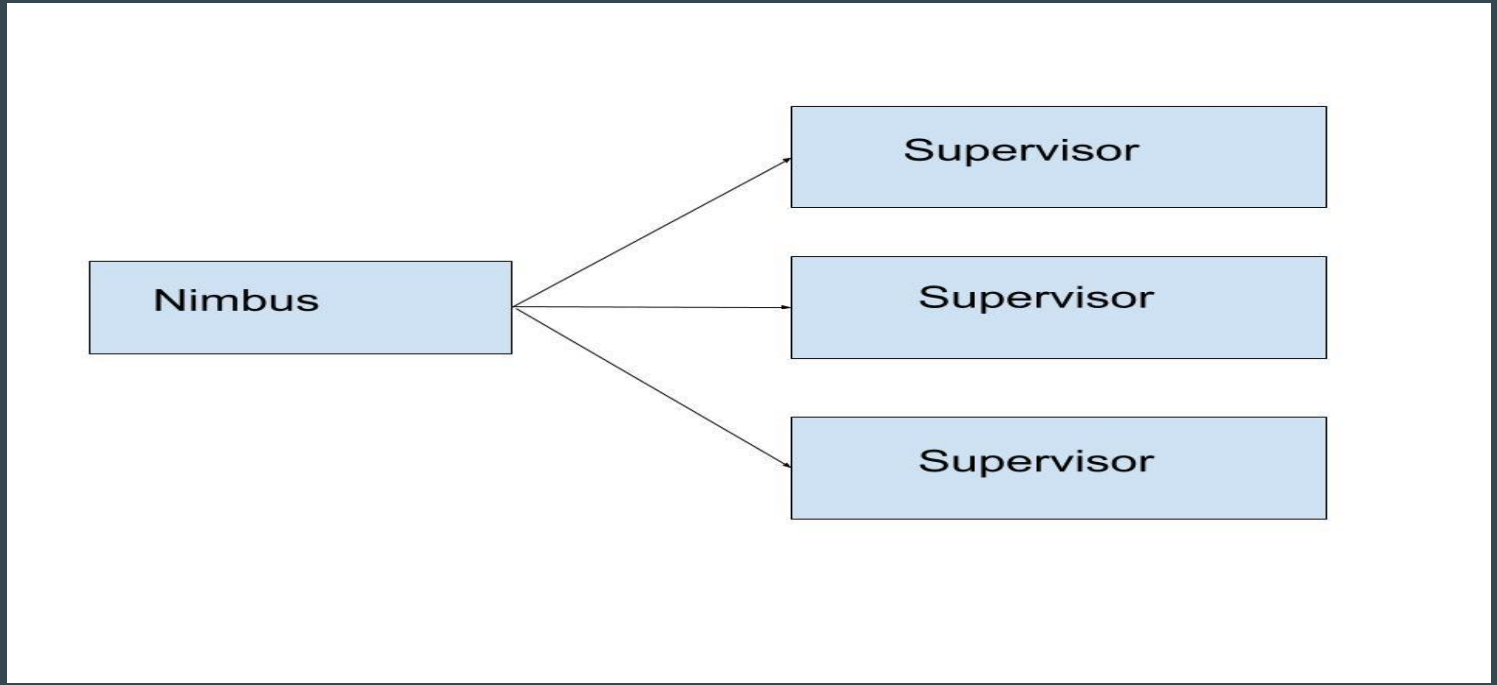
Apache Storm

- Free and opensource (Apache 2.0)
- Distributed realtime computation system
- Reliably process unbounded streams of data

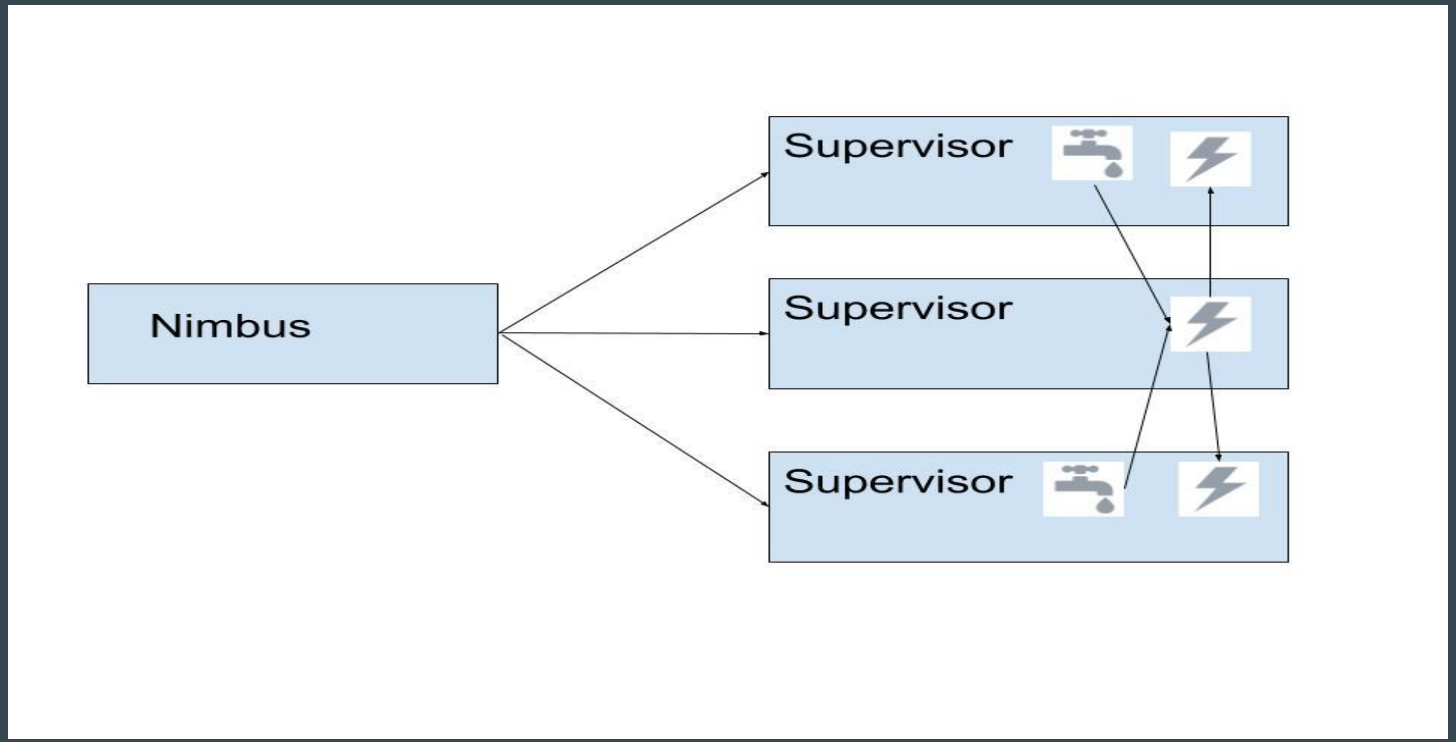
Apache Storm - Processing Logical Layout



Apache Storm - Cluster Layout



Apache Storm - Overlapped view



What are we trying to solve ?

- Application logs scattered across multiple nodes
- Logs are stored locally = Loss
- Not easy to see old log data
- Troubles while troubleshooting
- Visualization

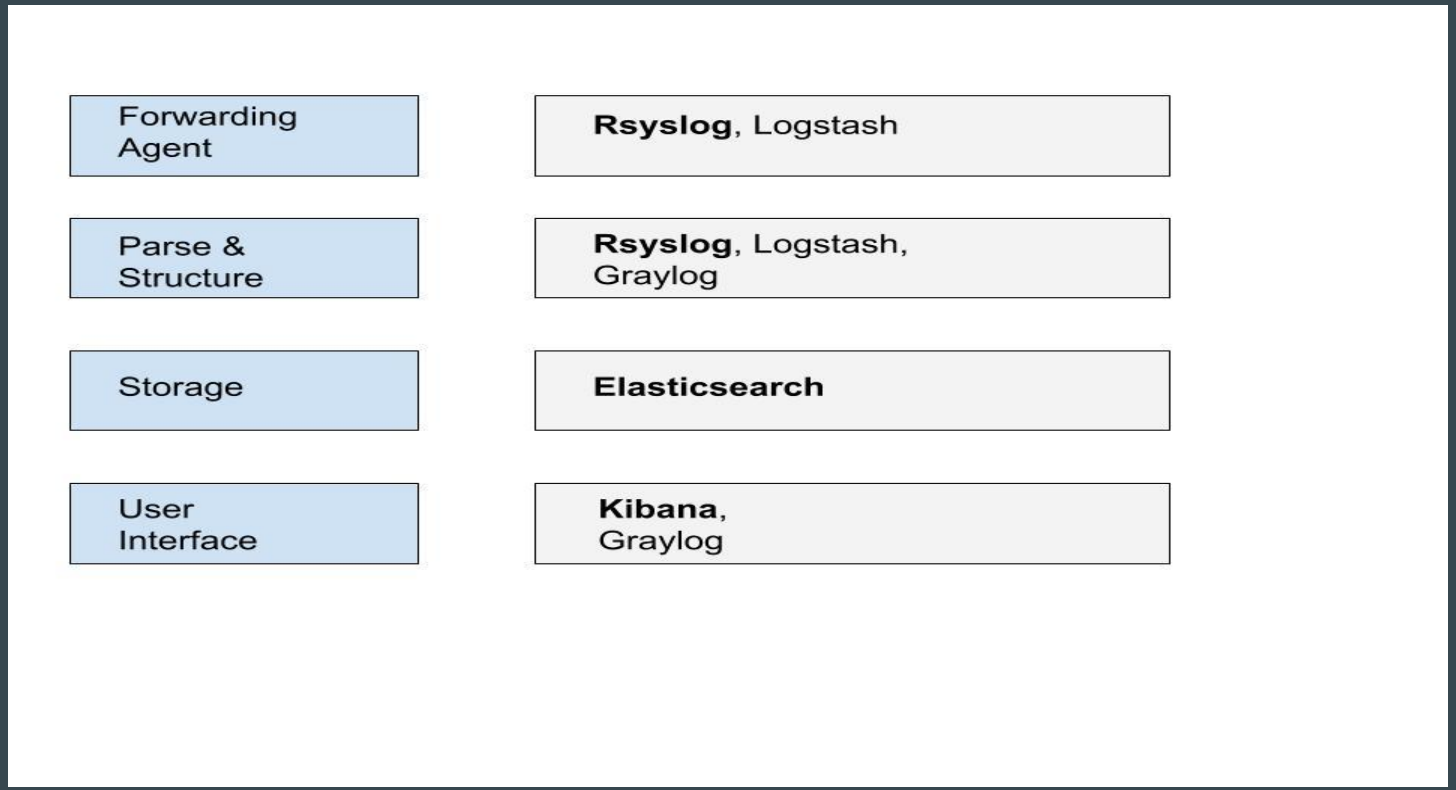
Requirements

- No Storm Code changes
- Real time
  - Aggregation
  - Indexing
- Atleast 2 billion events per day
- Distributed
- Linearly Scalable
- Fault tolerant
- Commodity hardware

Choices

- Splunk - Could not justify cost
- Graylog + Elasticsearch
- ELK
- ERK

Choices


Forwarding Agent
Rsyslog, Logstash
Parse & Structure
Rsyslog, Logstash, Graylog
Storage
Elasticsearch
User Interface
Kibana, Graylog

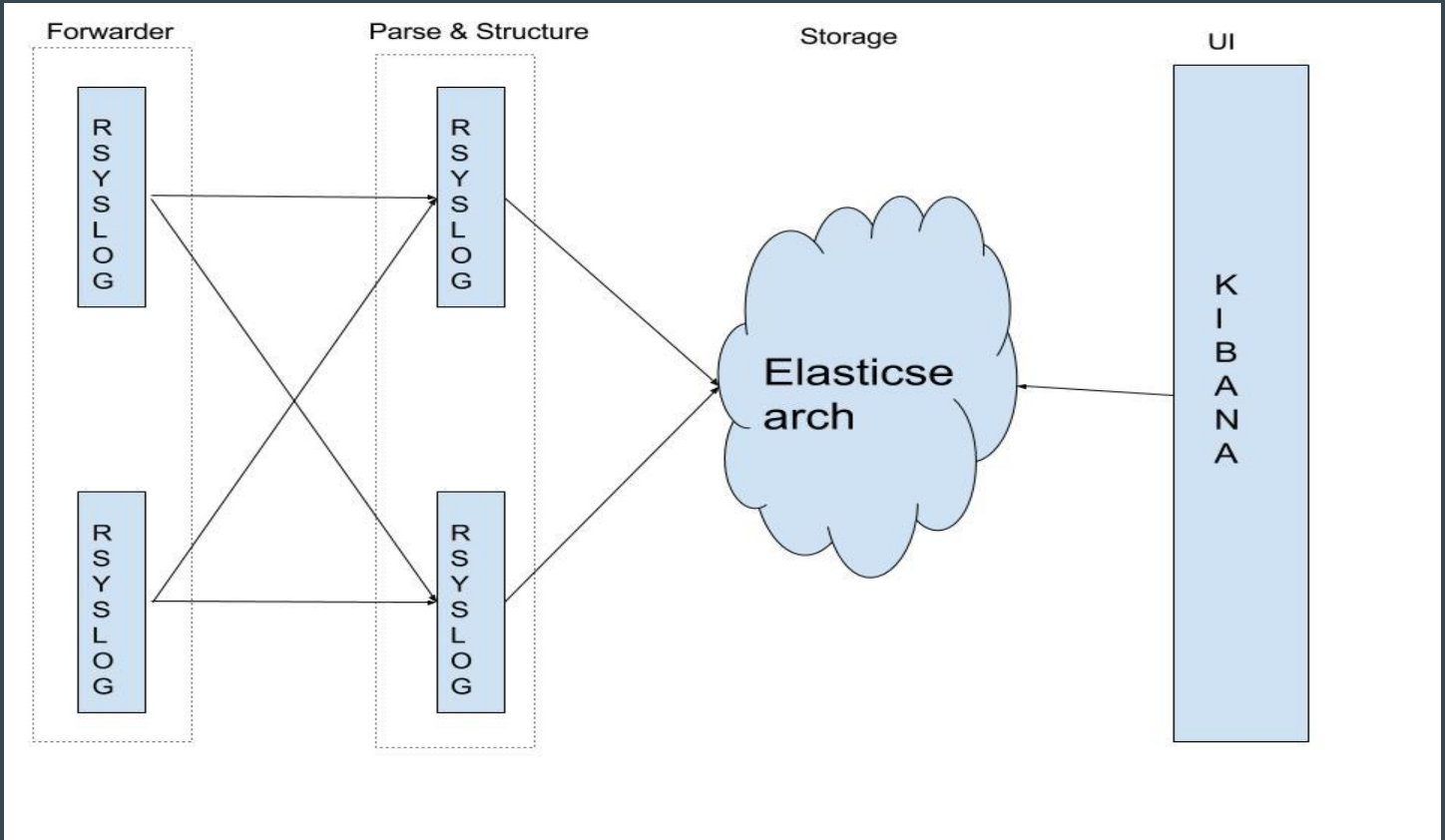
Issues

- Storm uses logback for logging
- Logback does not support RFC5424
- STORM-833

Changes - Storm end

- Add Syslog Appender to Log4J2
- Send to local rsyslog
- UDP
- Embed Metadata into RFC5424 SD

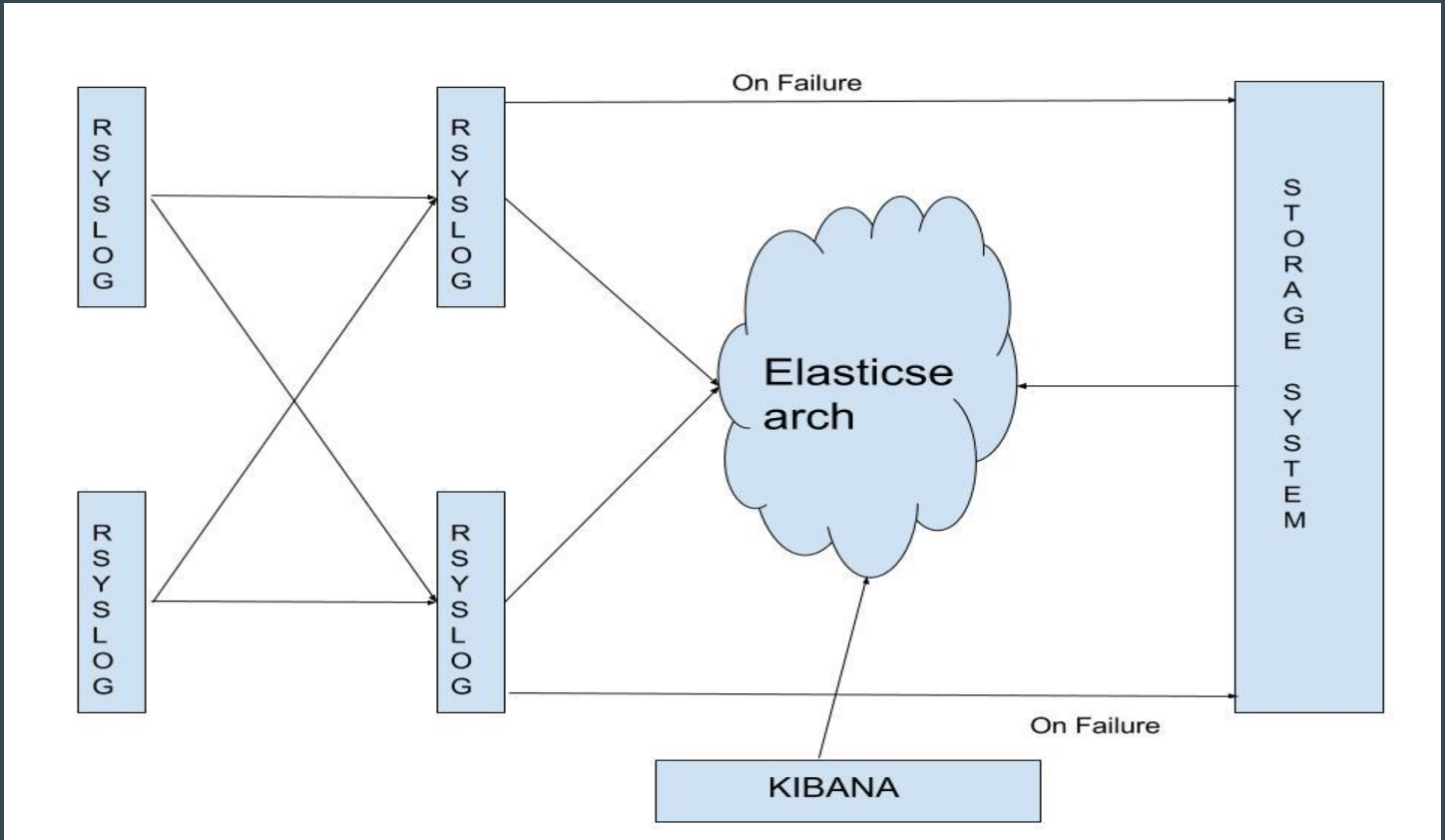
Setup


Forwarder
Parse & Structure
Storage
UI
RSYSLOG
RSYSLOG
RSYSLOG
RSYSLOG
Elasticsearch
KIBANA

No message broker ?

- It is a choice
- Everything has a cost
- Logs need not be shipped immediately
- Local filesystem as buffer
- Explicitly targeting failure cases ?

Setup


RSYSLOG
RSYSLOG
RSYSLOG
RSYSLOG
On Failure
Elasticsearch
STORAGE SYSTEM
On Failure
KIBANA

How about spikes ?

- Antipatterns
- DA queues in rsyslog
  - At forwarder
  - At parser
- Rsyslog Failover
  - ActionExecOnlyWhenPreviousIsSuspended

Lessons : Elasticsearch

- Dedicated Master nodes
- Use Bulk load
- Fixed thread pool
- **Circuit Breakers**
- **refresh_interval**

Lessons

- Rsyslog
  - Impstats is your friend
  - Name your actions
  - Keep an eye on Capacity
  - Should not impact local daemons
- Reduce Centralized Overhead
- Operational overhead vs requirements