Centralised Logging....

without the blood, sweat and tears

Paul Stack
http://twitter.com/stack72
mail: paul@paulstack.co.uk

Paul Stack

@stack72

Why Centralised logging?

“ANYTHING THAT CAN GO WRONG
WILL GO WRONG”

MURPHY'S LAW

What happens if you lose a server and the logs were only on that server?

logz.io

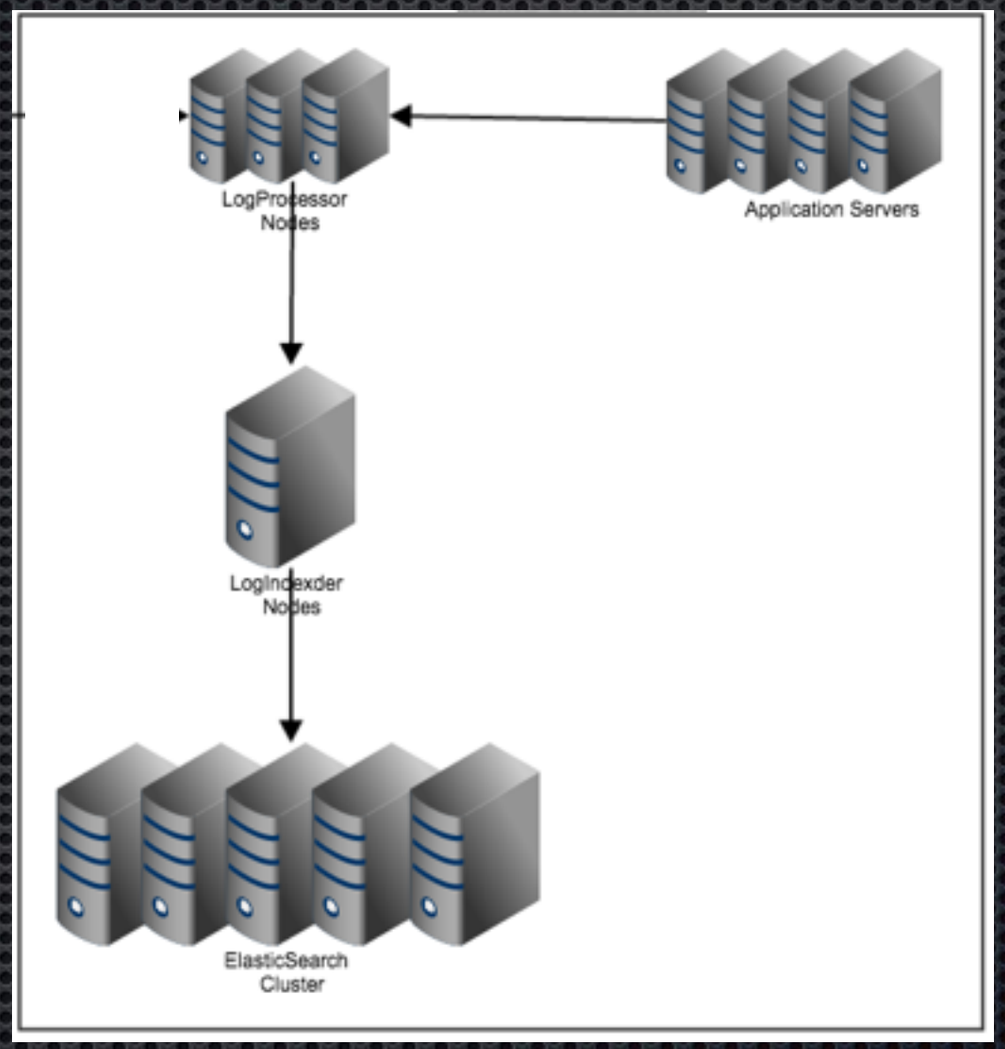
splunk>

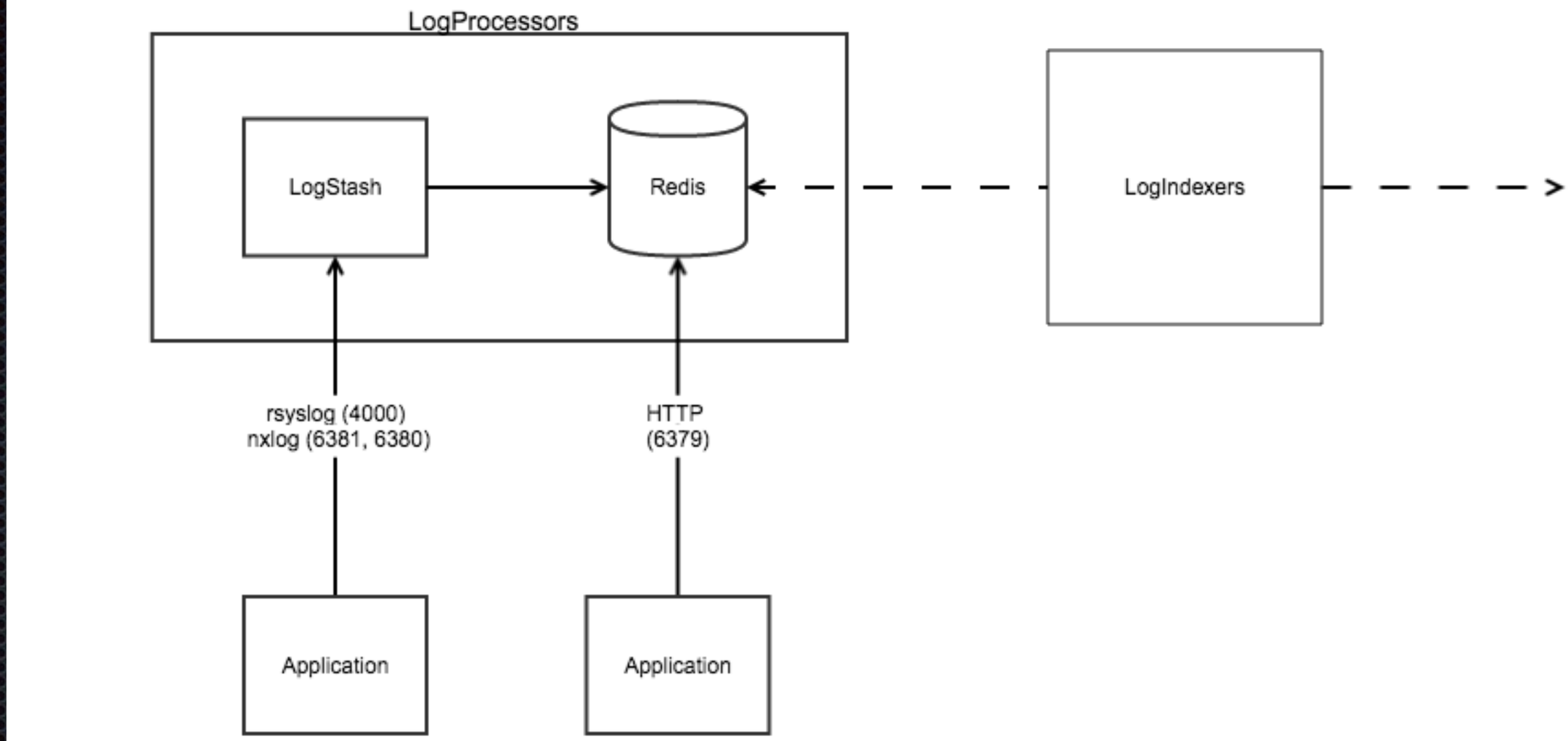
{GRAYLOG2

Open source Log Management

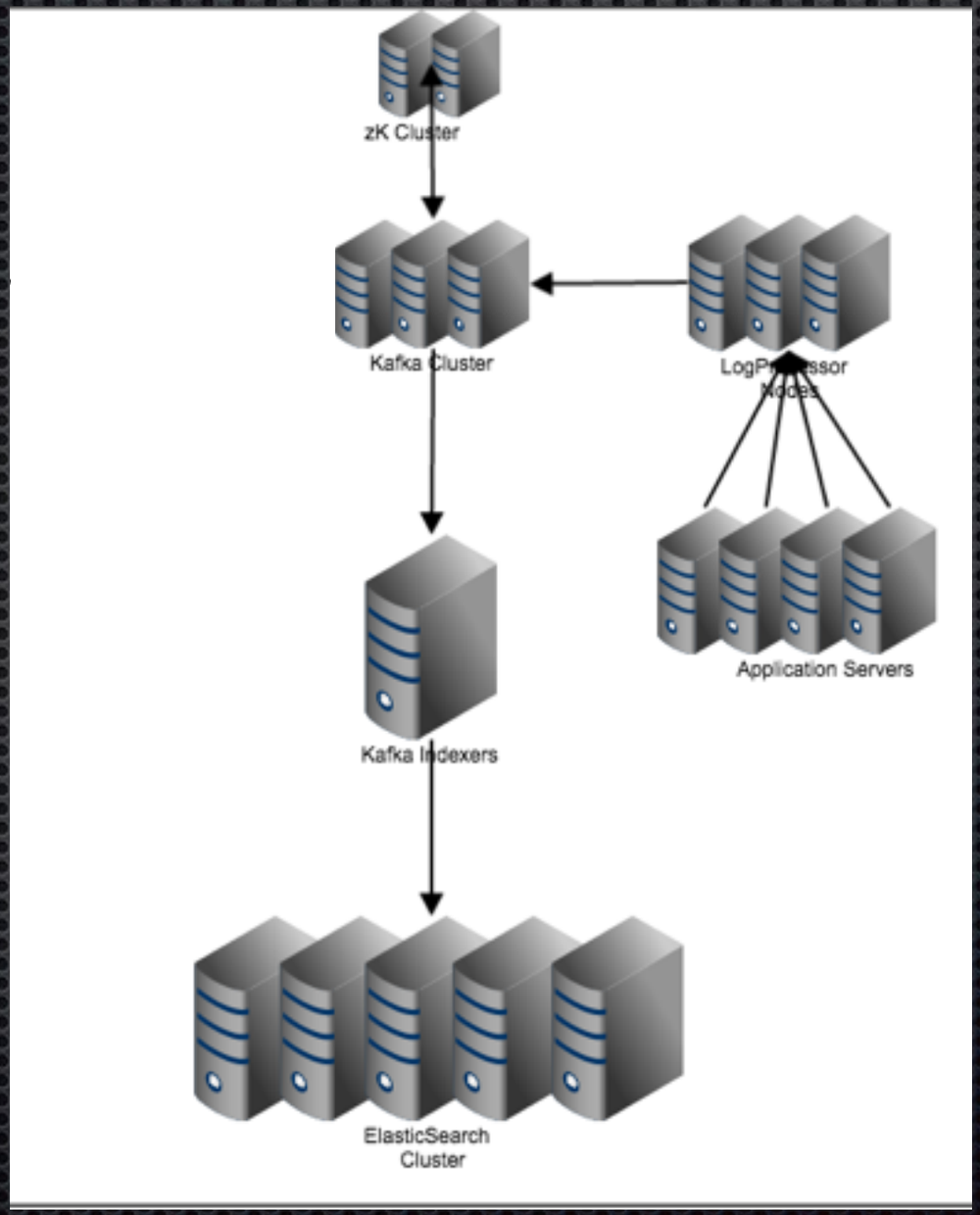
elastic

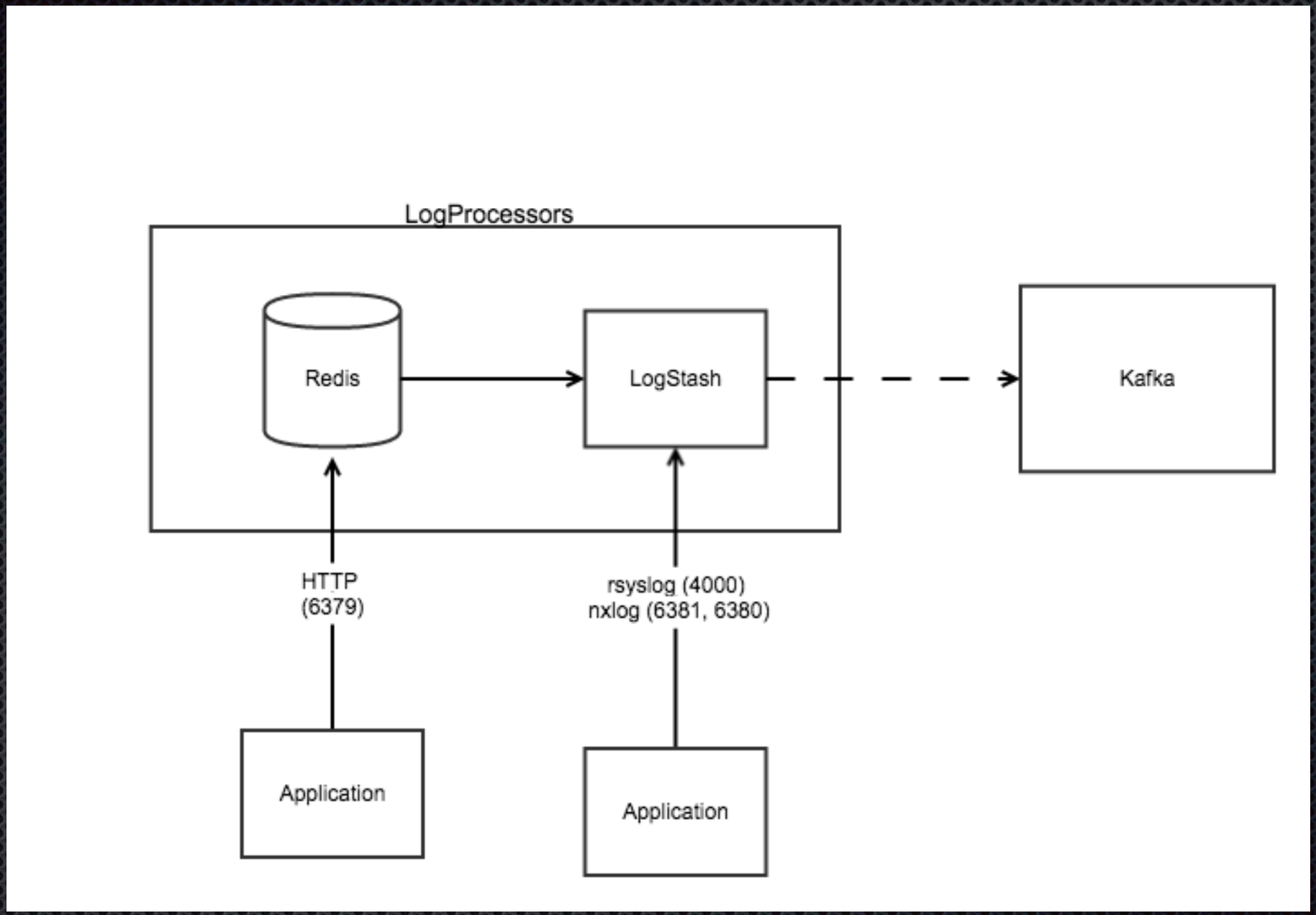
Simple Logging Architecture




LogProcessors
LogStash
Redis
LogIndexers
rsyslog (4000)
nxlog (6381, 6380)
HTTP
(6379)
Application
Application

Streaming Architecture

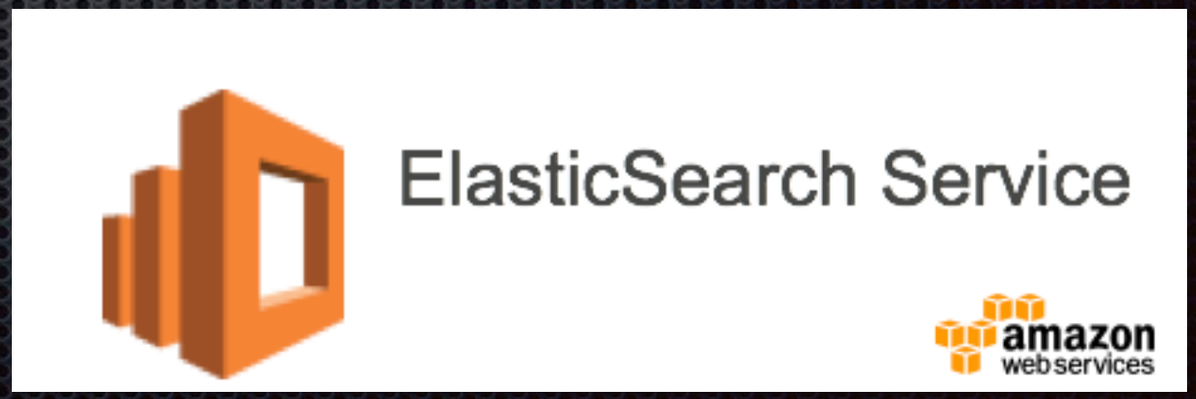


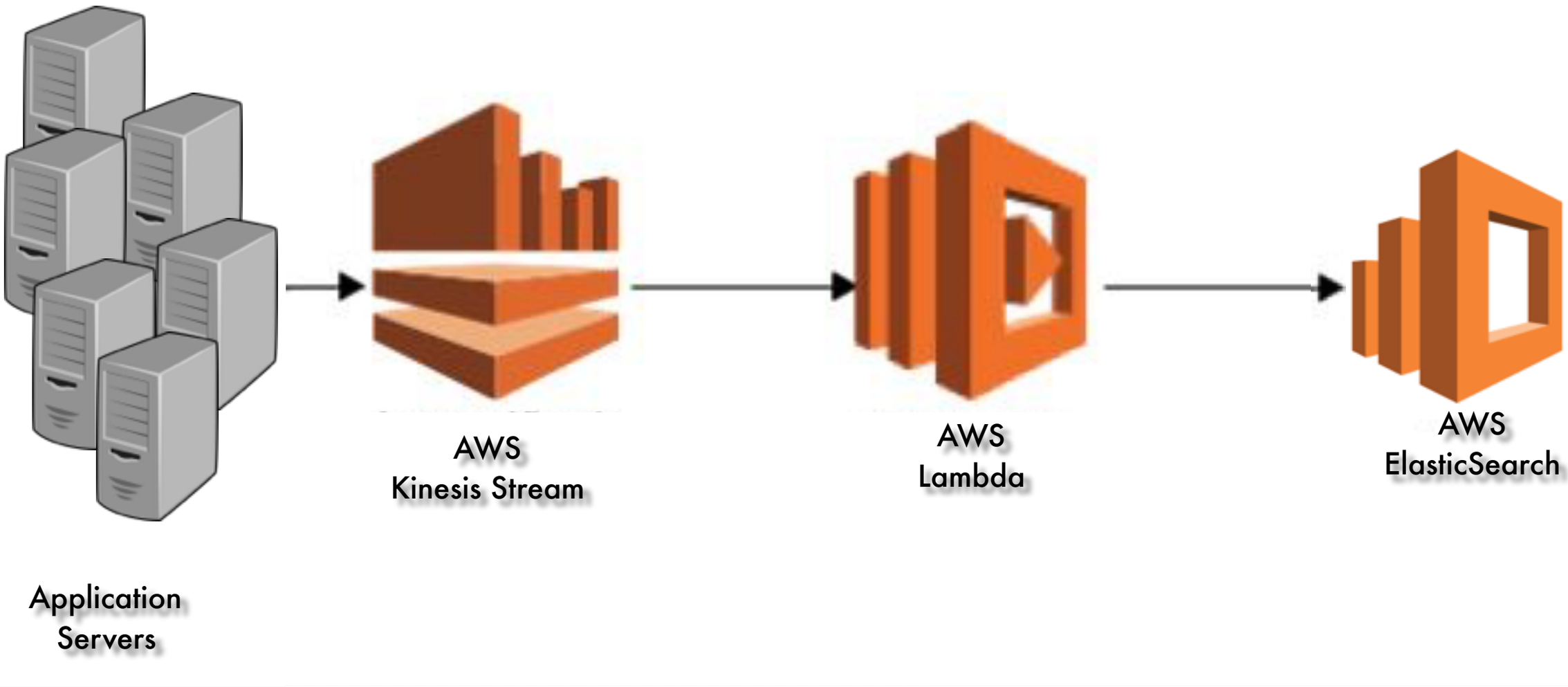

LogProcessors
Redis
LogStash
Kafka
HTTP
(6379)
rsyslog (4000)
nxlog (6381, 6380)
Application
Application

There has to be another way....


AWS Lambda


Kinesis


ElasticSearch Service
amazon
web services


Application
Servers
AWS
Kinesis Stream
AWS
Lambda
AWS
ElasticSearch

Code Time...

How do I send logs to Kinesis?

```
https://github.com/samcday/logstash-output-kinesis


output {
  kinesis {
    kinesis_stream_name => "my_stream_name"
    region => "us-west-2"
    codec => json { }
  }
}
```

Costs of running this...

- Kinesis Streams - $0.015 for every million PUT
- Kinesis Streams - Extended Data $0.02
- Lambda - $0.22 for every million queries
- ElasticSearch - $0.09 per hour per node
- ElasticSearch - $0.135 per GB / per month

$ 144.87 per month

Questions?

Paul Stack

@stack72