Monitoring

- Marvel
  by Elasticsearch
- Kopf - ES Plugin
  - https://github.com/lmenezes/elasticsearch-kopf
- Monitoring
  - Nagios, Zabbix, Icinga, Munin ....
why redis?

- decoupling for scaling
  - more producer / consumer
- buffer
  - softening spikes
  - downtime of logstash service
one Logstash to rule them all

input {
  redis {} 
}

output{
  elasticsearch_http{}
}
one Logstash to rule them all

input {
  redis { tag => "filtertag123"}
}

output{
  if "filtertag123" in [tags] {
    elasticsearch_http{}
  }
}
Wald
Wald
Wald
cluster optimization

- memory
  - amount
  - tuning for read or write
- refresh interval of lucene index
- disk performance
- shards
  - sizes, amount, distribution
demo time

- keep fingers crossed
- fallback -> whiteboard?
elasticsearch shield

- coming soon ;)
- realized as ES plugin
  - role based access
  - authentication support
  - encrypted communications
  - audit logging
- at least gold subscription
Questions - Alternatives

splunk

Grafana

GRAYLOG2
Open source Log Management

fluentd