50 shades of ElasticSearch

Denis Ćutić @ Infobip

USE CASE

Event logs

Distributed processing

Multiple events per message

Additional information

Availability?

Retention

Options

Decision

PoC

Hardware rental

CLUSTER #1

16 data nodes
3 master nodes
40 TB

30 days retention

Only message logs

Considerations before starting it up

Network connectivity / throughput

Plan capacity carefully

RAID 0

Mount points

Configuration location

ES version

Java version

Shard allocation

Once it’s started...

Logging

Kopf / Cerebro

Host / ES metrics exporter

Prometheus + Grafana

Slow logs & circuit breakers

Disable automatic index creation

Index / mapping templates

Changes take time to “propagate”

Remove _all field, disable field_data

Use aliases

Avoid custom routing

Security / access logs

Proxy

Throttling

Start filling the data...

Start dealing with challenges...

Rolling restart

Stop indexing
Disable shard allocation
Flush

Recovery not always perfect

“Manually” reallocate shards

Nodes falling down

Recovery slowing down whole cluster

Recovery speedup

Tune up the recovery settings

Stop indexing

Disable replicas

Allocation / task API

CLUSTER #2

Message logs
Billing data

39 data nodes
3 master nodes
50 TB

Traffic and archive data

Joining Kafka streams

Several approaches tried

Painless scripts

GC issues

Result

Indexing: ~50k/s

Searches: ~1k/s

Recovery impact

Still tuning for optimal performance...

Thank you!