KubeCon | CloudNativeCon
Europe 2022

Autoscaling Elasticsearch for Logs on Kubernetes

Radu Gheorghe, Sematext

Ciprian Hacman, polypoly

Hello world!

Radu Gheorghe, Sematext Group

Elasticsearch and Solr
⇒ Consultant
⇒ Trainer

Engineering for Sematext Cloud
⇒ Observability SaaS
⇒ Logs and metrics from Elasticsearch, Solr, Kubernetes, etc

Ciprian Hacman, polypoly Enterprise

Kubernetes and Automation
⇒ Consultant
⇒ Software Engineer
⇒ Open Source Maintainer

Agenda

Why? Use-case

Agenda

Why? Use-case

How? What should happen on scale up/down

Agenda

Why? Use-case

How? What should happen on scale up/down

What? Available options

Agenda

Why? Use-case

How? What should happen on scale up/down

What? Available options

Demo of (enhanced) es-operator

Why?

Small cluster → zero maintenance

Why?

Small cluster → zero maintenance

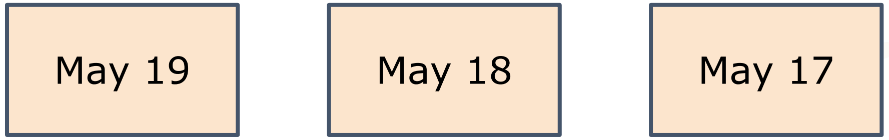
Big problems, big knowledge, big team

Easier to manage access

Big/multi-tenant cluster → N small clusters

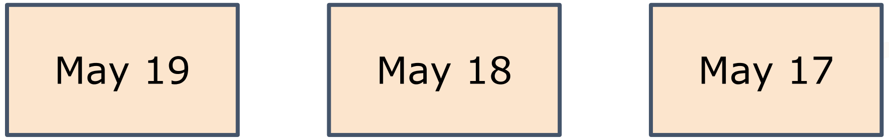
How?

Use time-based indices



How?

Use time-based indices


May 19

May 18

May 17

Rotate indices by size (and time)

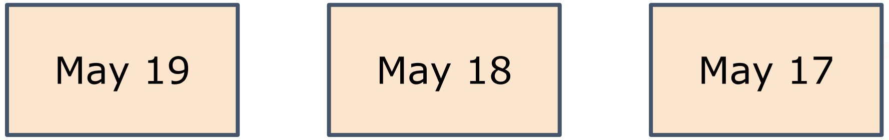
10GB

10GB

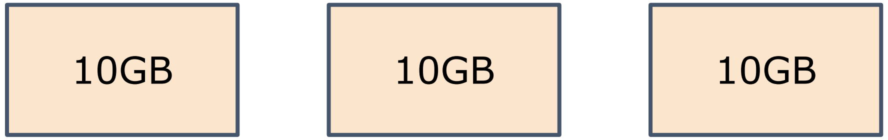
10GB

How?

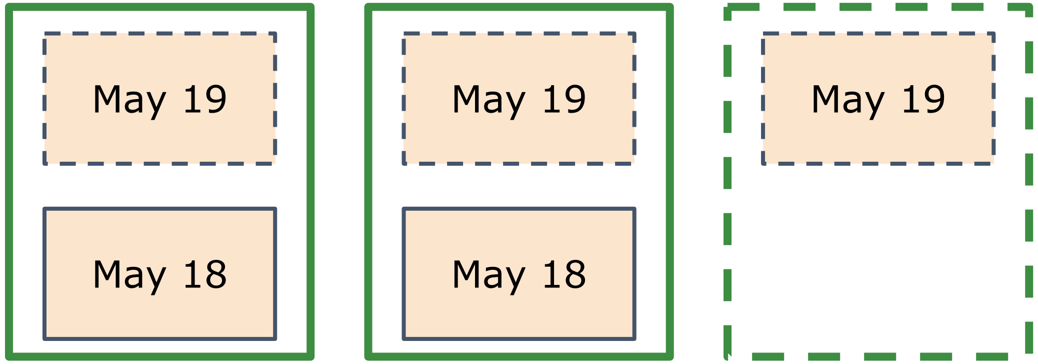
Use time-based indices



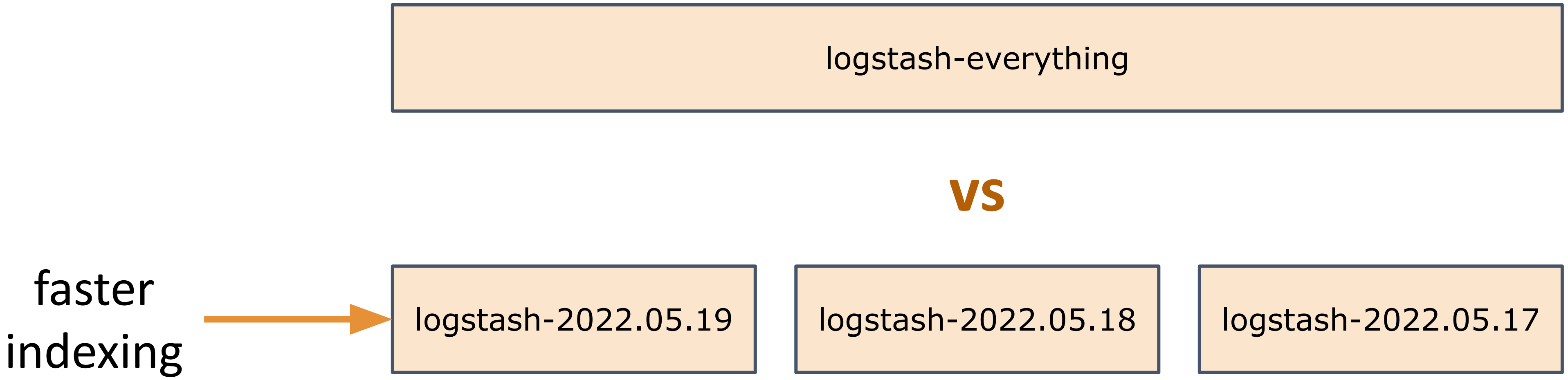
Rotate indices by size (and time)



Update number of shards as you scale



How? Time-based indices



logstash-everything

vs

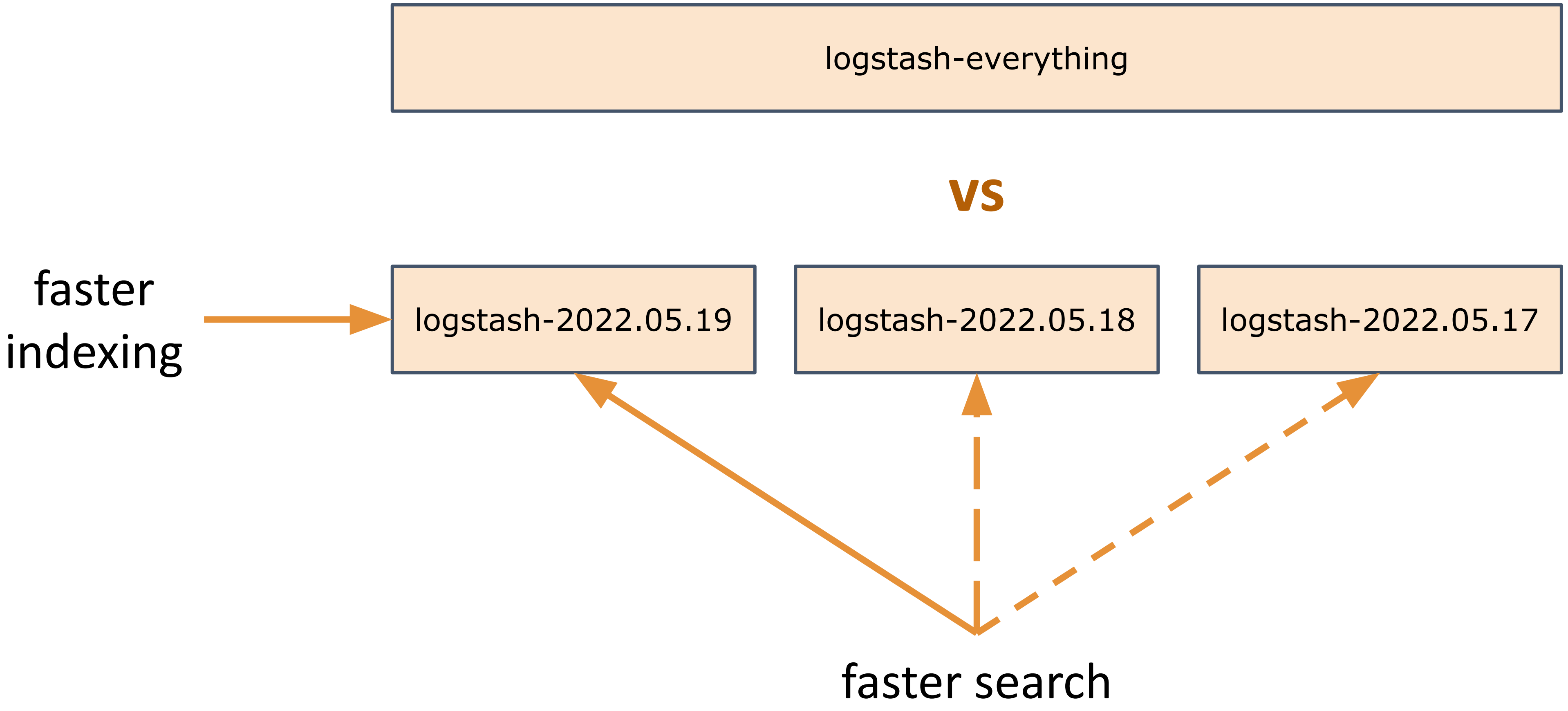
faster indexing

logstash-2022.05.19

logstash-2022.05.18

logstash-2022.05.17

How? Time-based indices



logstash-everything

vs

faster indexing

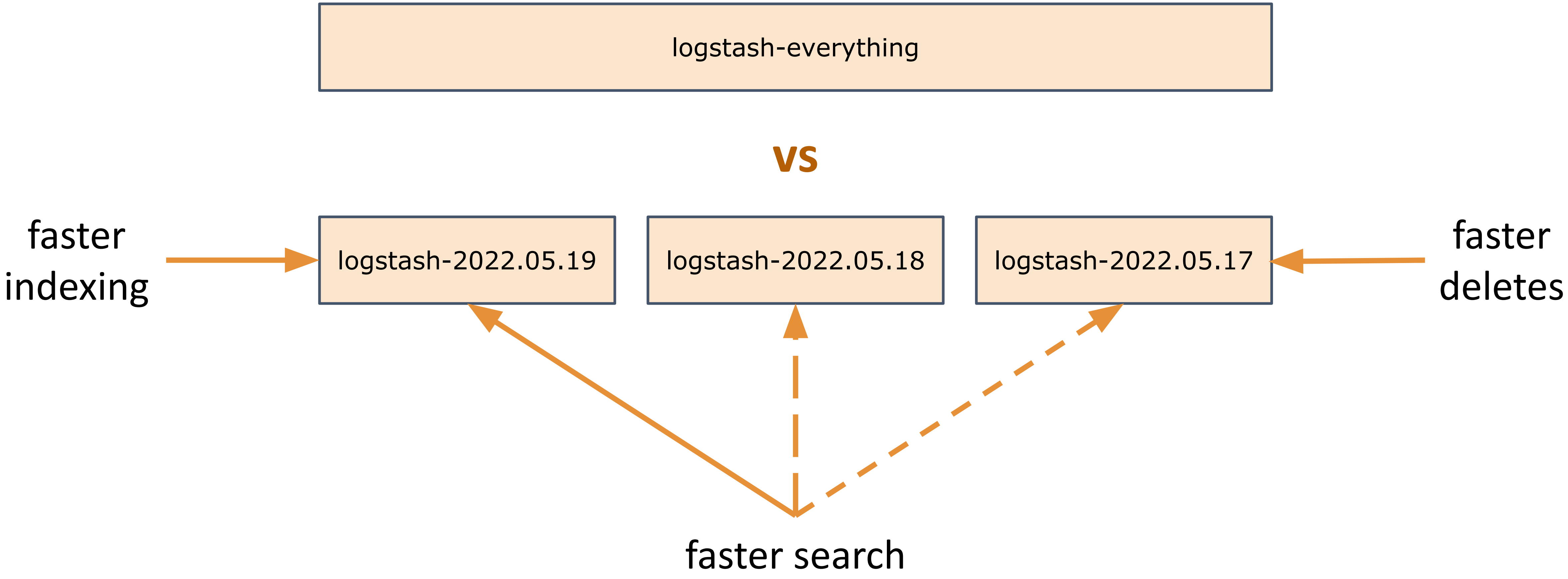
logstash-2022.05.19

logstash-2022.05.18

logstash-2022.05.17

faster search

How? Time-based indices



logstash-everything

vs

faster indexing

logstash-2022.05.19

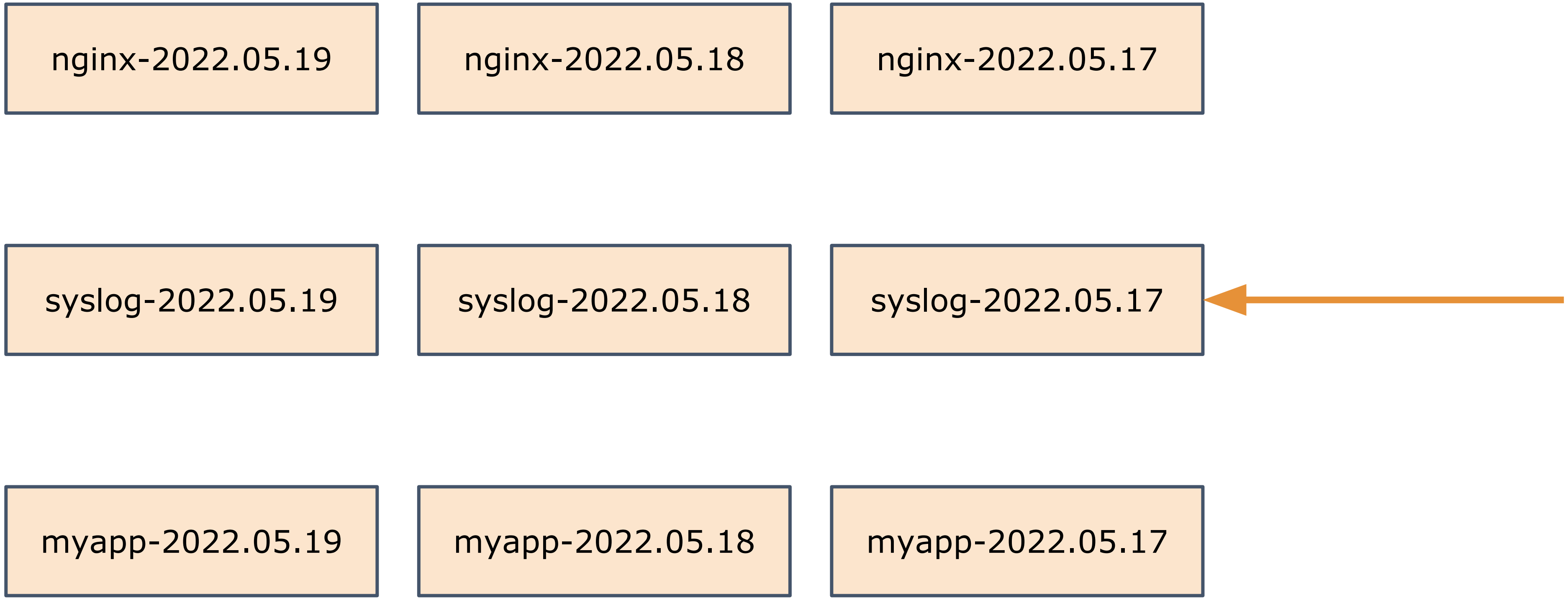
logstash-2022.05.18

logstash-2022.05.17

faster deletes

faster search

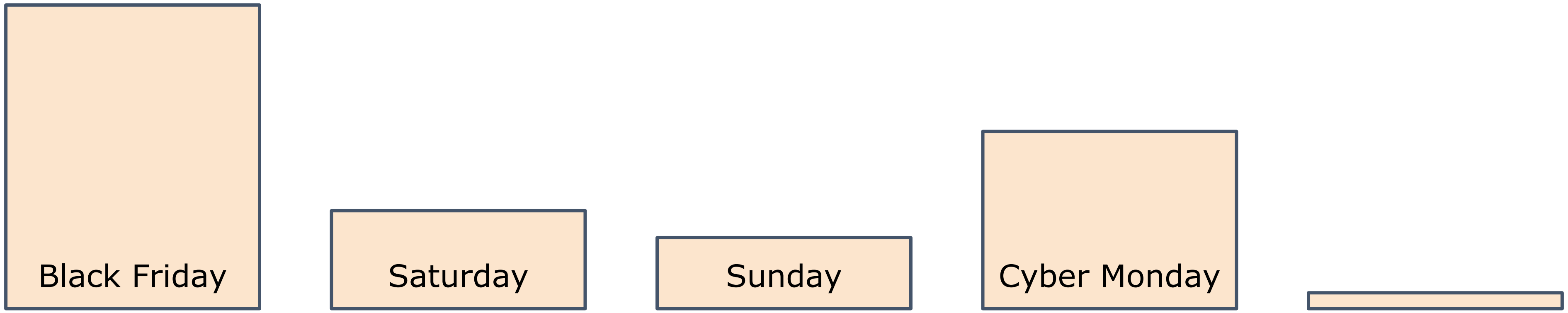
How? Time-based indices per use-case



nginx-2022.05.19	nginx-2022.05.18	nginx-2022.05.17
syslog-2022.05.19	syslog-2022.05.18	syslog-2022.05.17
myapp-2022.05.19	myapp-2022.05.18	myapp-2022.05.17

Often searched separately

How? Rotate indices by size (typically via ISM/ILM)



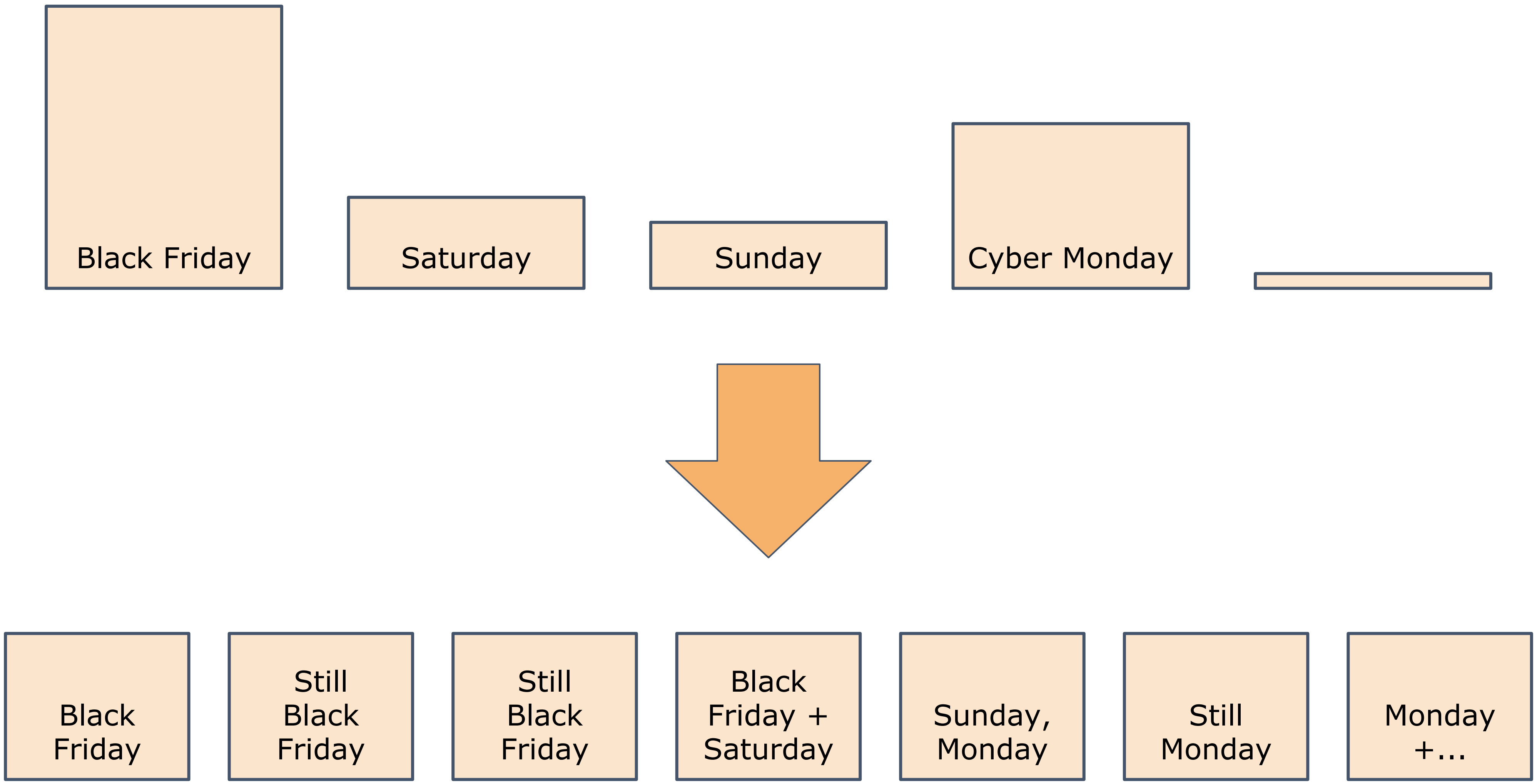
Black Friday

Saturday

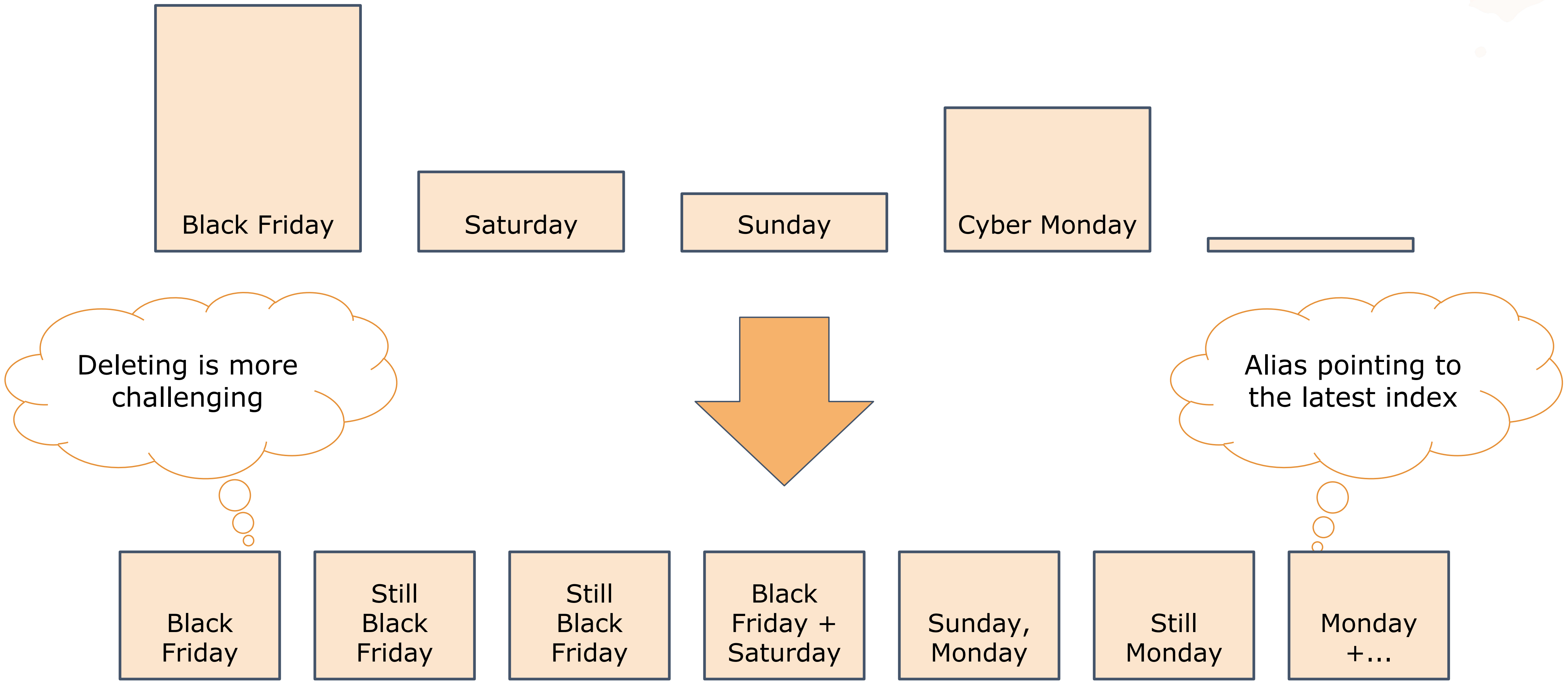
Sunday

Cyber Monday

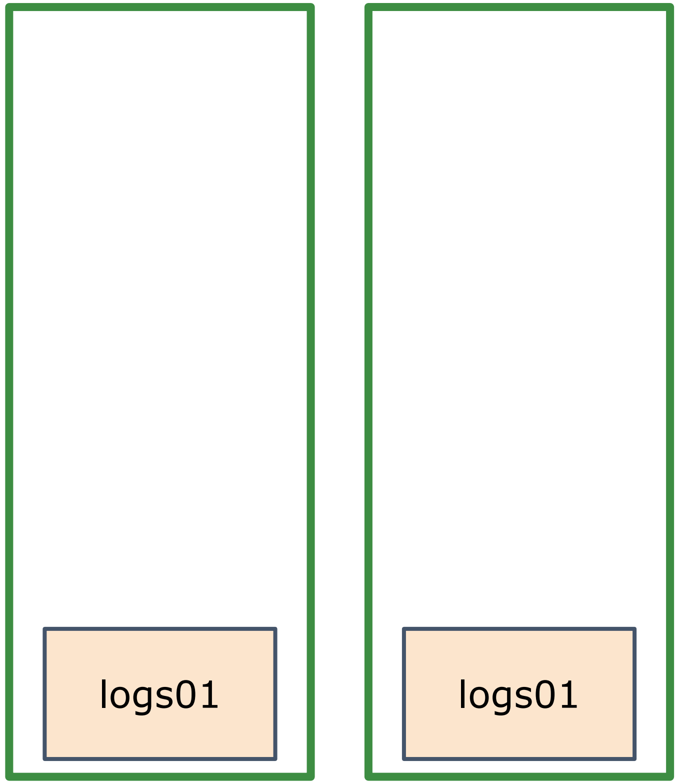
How? Rotate indices by size (typically via ISM/ILM)



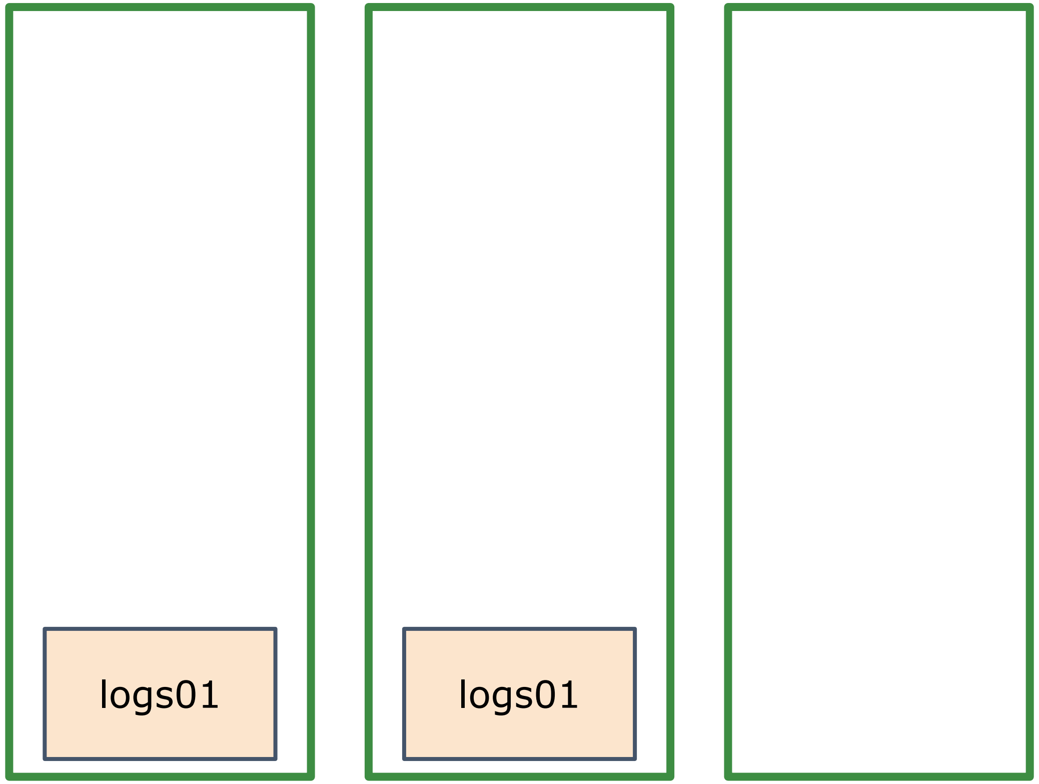
How? Rotate indices by size (typically via ISM/ILM)



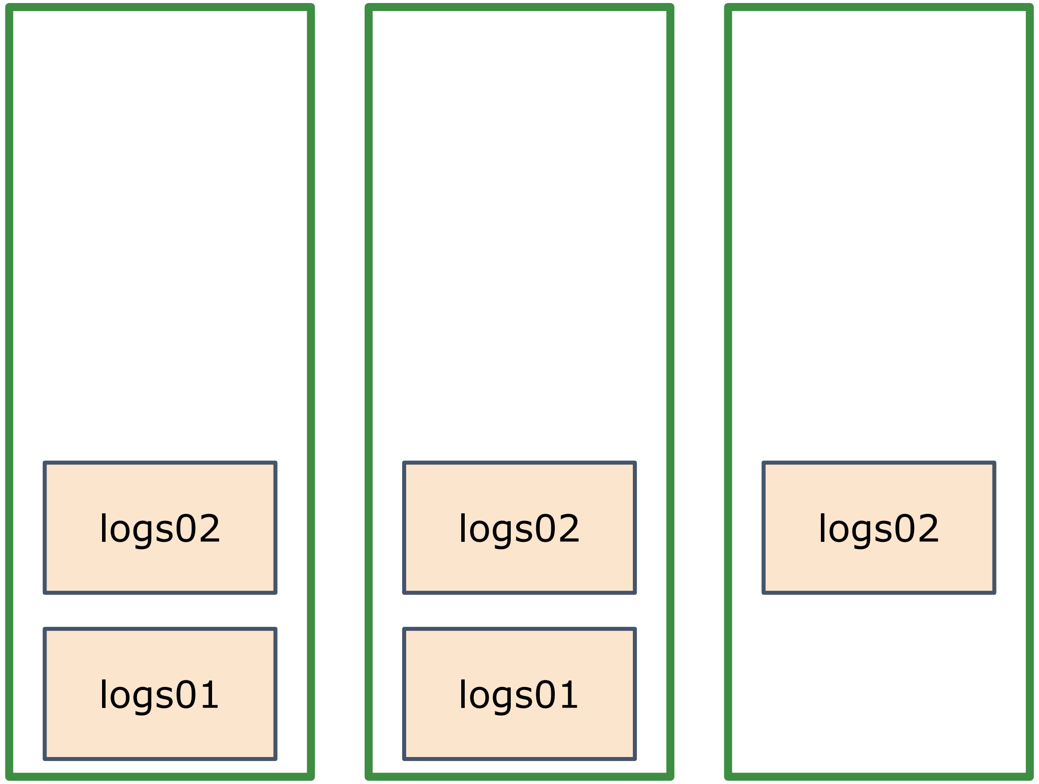
How? Update number of shards as you scale



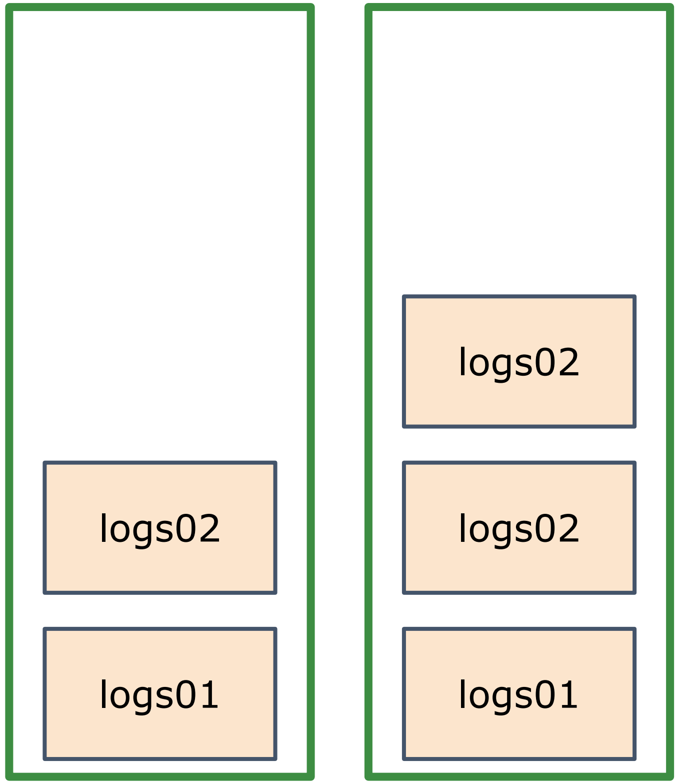
How? Update number of shards as you scale



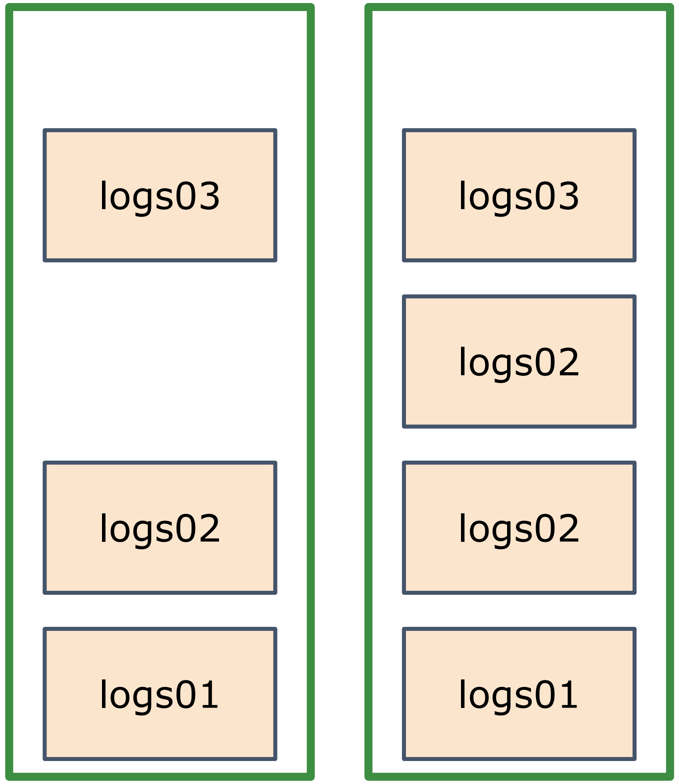
How? Update number of shards as you scale



How? Update number of shards as you scale



How? Update number of shards as you scale



How? Local storage and other optimizations

Indexing takes more CPU, but search latency dictates capacity

How? Local storage and other optimizations

Indexing takes more CPU, but search latency dictates capacity

Searches do lots of random IO

⇒ local SSDs give good latency

=> use replicas and backups

How? Local storage and other optimizations

Indexing takes more CPU, but search latency dictates capacity

Searches do lots of random IO

⇒ local SSDs give good latency

=> use replicas and backups

Tiered setup (e.g. hot-cold) rarely helps

What?

Elastic Cloud on Kubernetes

- ❏ Elastic license
- ❏ Autoscaling requires Enterprise license

What?

Elastic Cloud on Kubernetes

- ❑ Elastic license
- ❑ Autoscaling requires Enterprise license

es-operator: https://github.com/zalando-incubator/es-operator/

- ❑ Apache2/MIT license
- ❑ Autoscaling that drains pods, adjusts replicas. See their KubeCon+CloudNativeCon EU 2019 presentation

⇒ works for independent indices (e.g. E-commerce)

⇒ let’s make it work for logs :)

Demo

https://en.wikipedia.org/wiki/Twelve_Grapes

Thank you!

Radu Gheorghe, Sematext Group

@radu0gheorghe

@sematext

Ciprian Hacman, polypoly Enterprise

@hakman0