



Kafka, Redis, ELK, Istio





Somkiat Puisungnoen

Somkiat Puisungnoen

Update Info 1 View Activity Log 10+ ...

Timeline About Friends 3,138 Photos More

When did you work at Opendream? X

... 22 Pending Items

Intro

Software Craftsmanship

Software Practitioner at สยามชัมนาภิกิจ พ.ศ. 2556

Agile Practitioner and Technical at SPRINT3r

Post Photo/Video Live Video Life Event

What's on your mind?

Public Post

Somkiat Puisungnoen 15 mins · Bangkok · ⚙️

Java and Bigdata





Page

Messages

Notifications 3

Insights

Publishing Tools

Settings

Help ▾



somkiat.cc

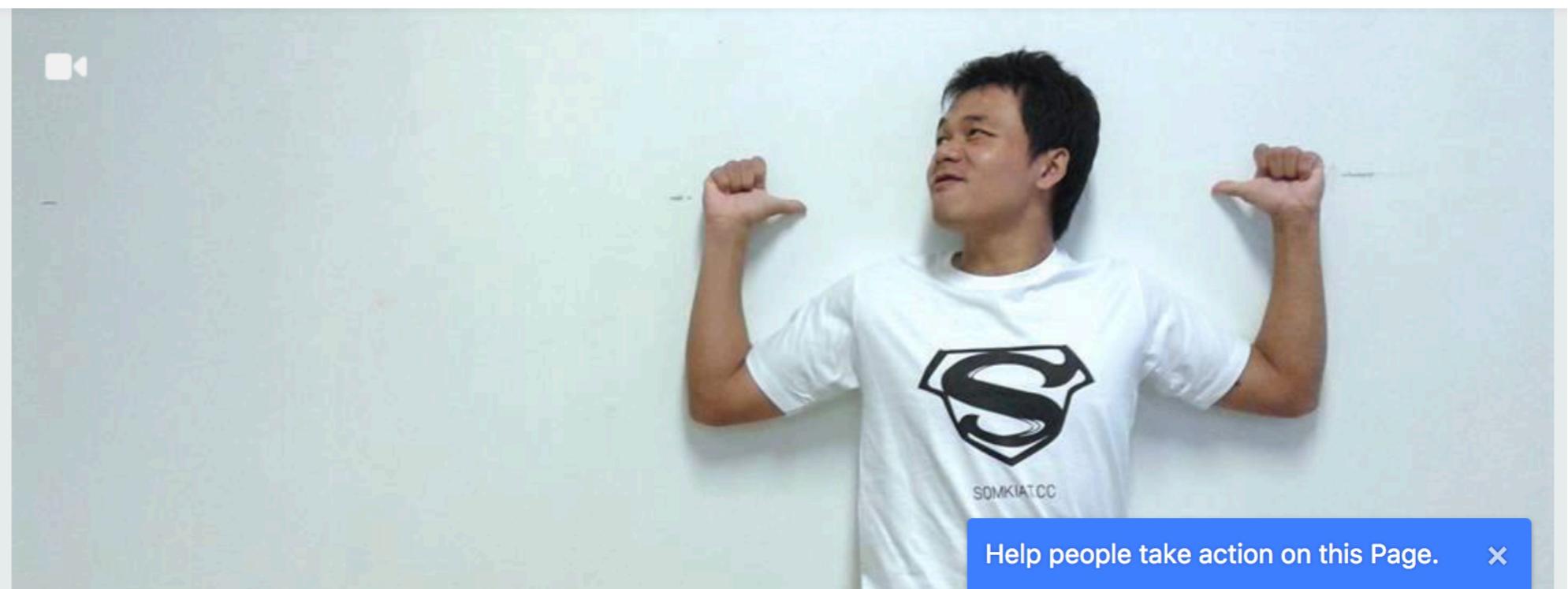
@somkiat.cc

Home

Posts

Videos

Photos



Apache Kafka

- Why Apache Kafka ?
- What is Apache Kafka ?
- Architecture
- Topologies and Tools
- Workshop



Redis

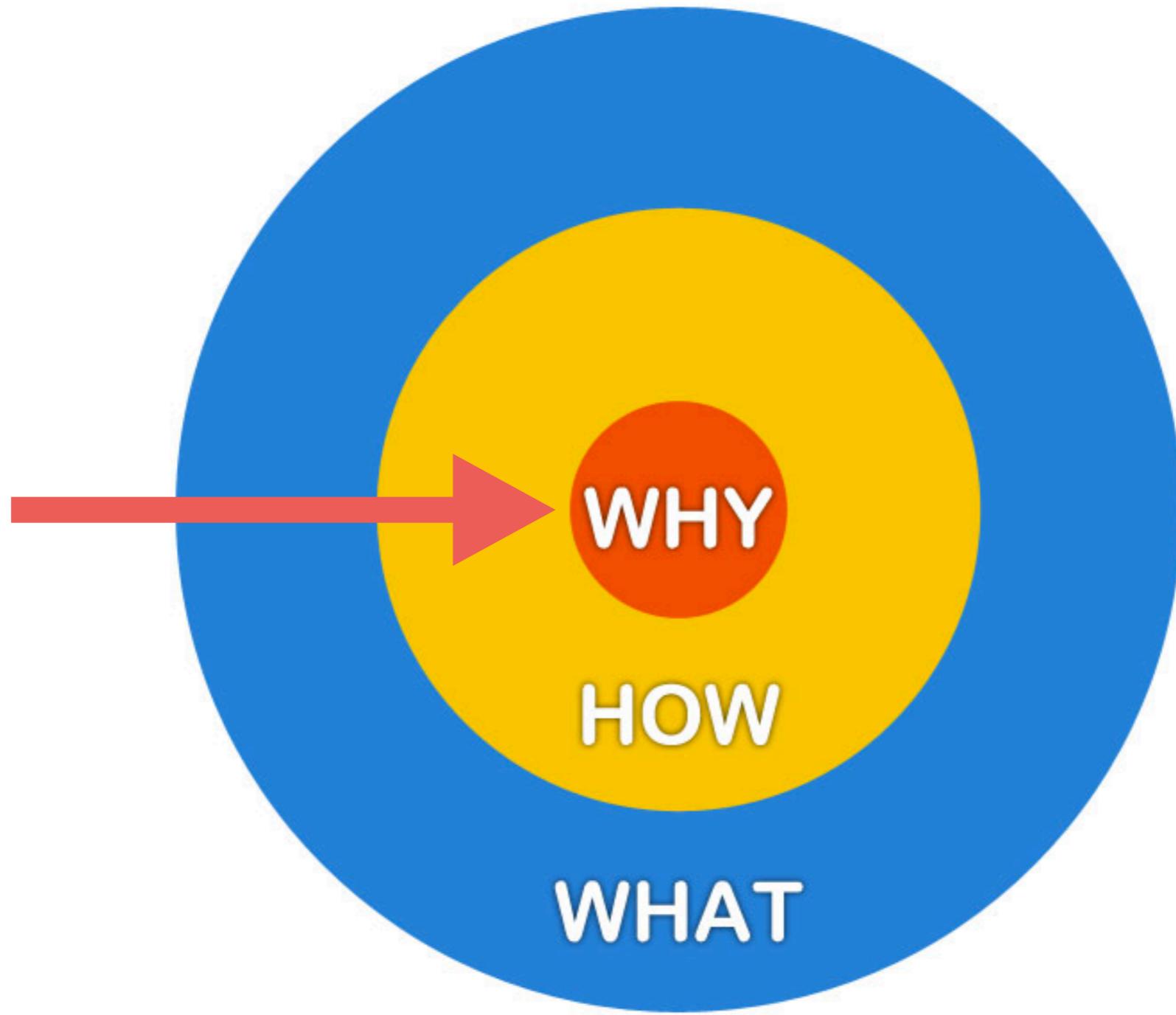
- Why Redis ?
- What is Redis ?
- NoSQL
- Architecture
- Redis command



ELK stack

- ELK stack
- Elasticsearch as data store
- Logstash as data ingestion
- Kibana as data visualization
- How it work ?



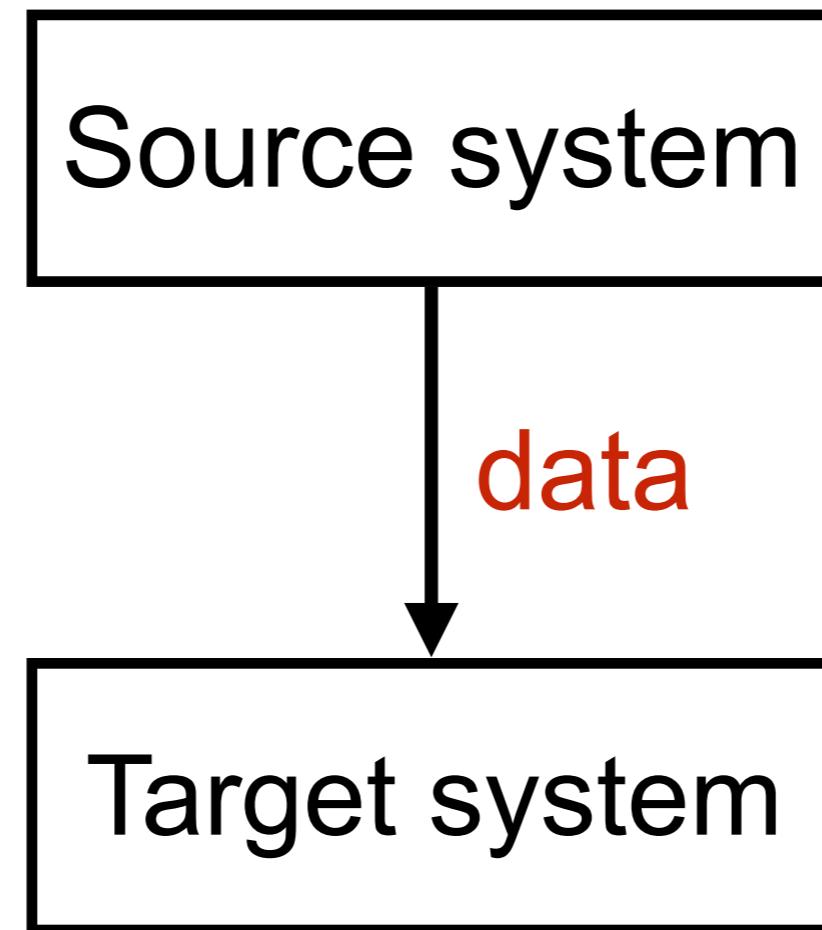


Apache Kafka



Why

Starting with simple



Why

More source systems

More target systems

More protocols

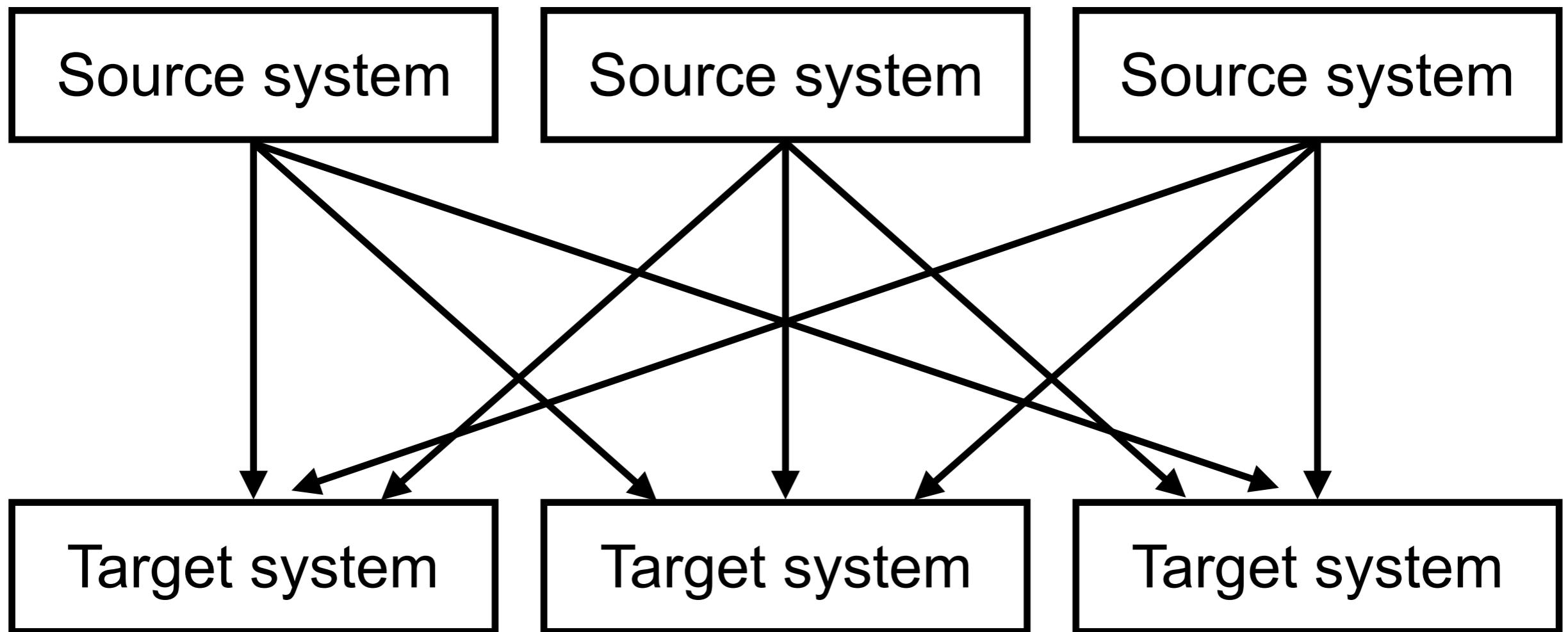
More data formats and schemas

More loads/traffics



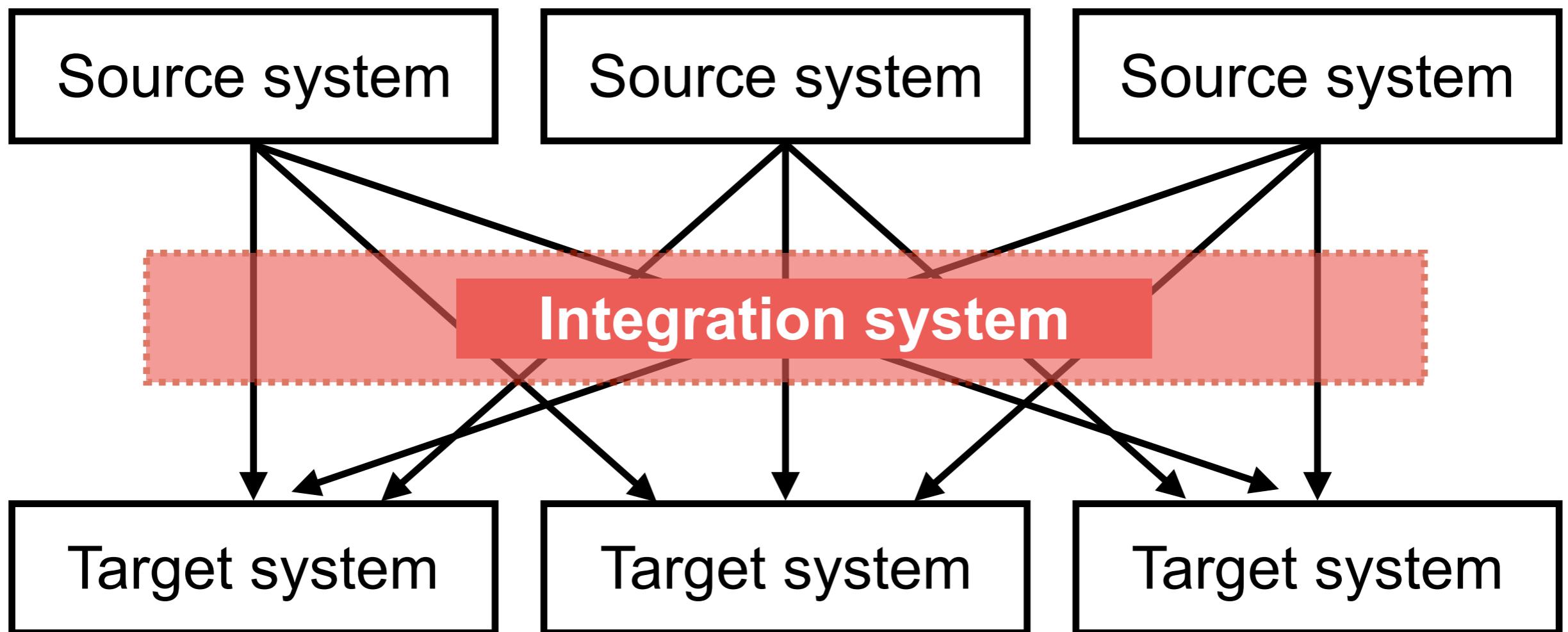
Why

Complex system !!

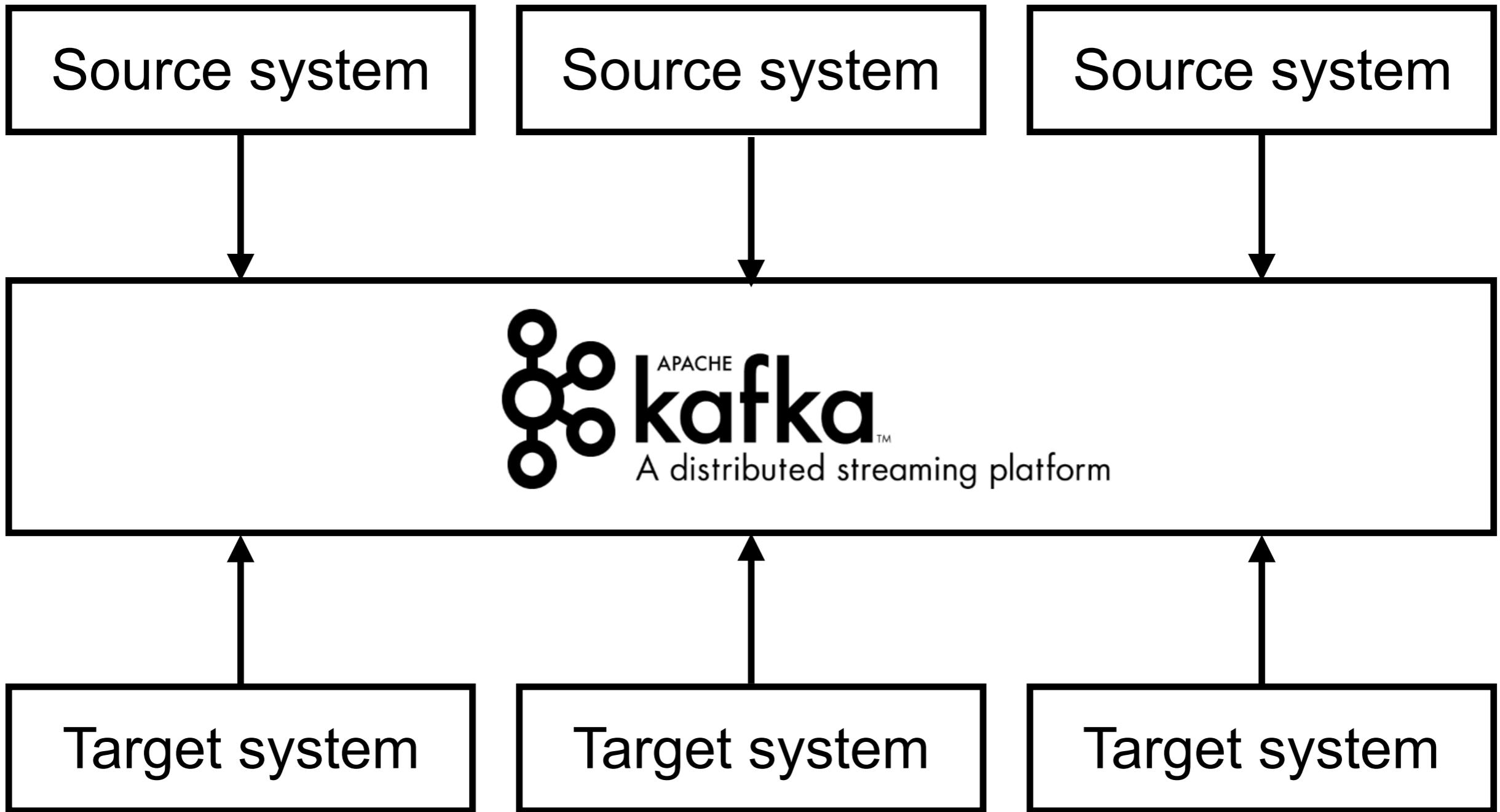


Why

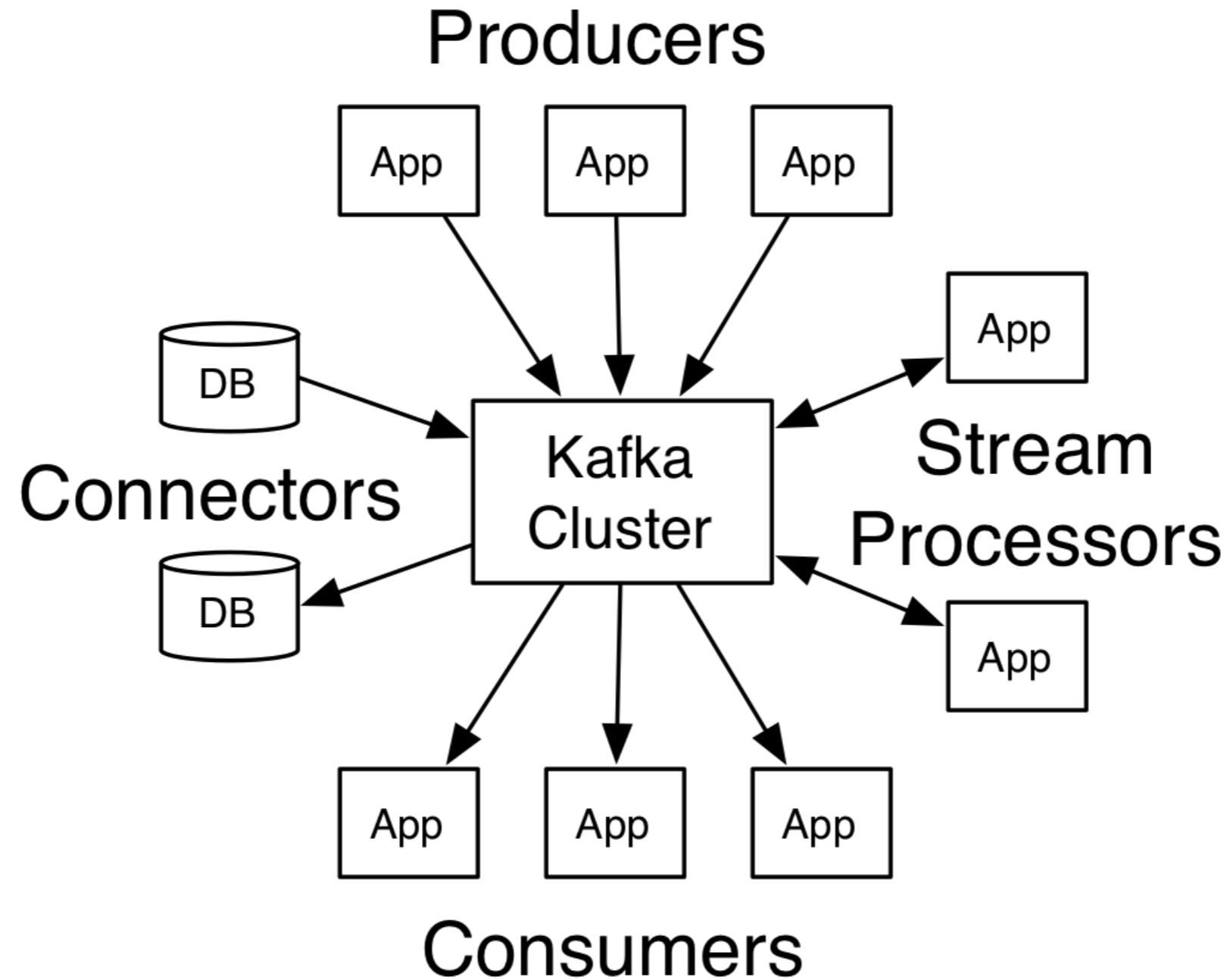
Need integration system



Apache Kafka



Apache Kafka



<https://kafka.apache.org/intro.html>



Why Apache Kafka ?

Created by LinkedIn

Open source project (maintain by Confluent)

Distributed system

Resilient architecture, fault tolerant

Horizontal scalability

High performance/ low latency



Used by



Uber



NETFLIX

<https://cwiki.apache.org/confluence/display/KAFKA/Powered+By>



Use cases

Messaging system

Activity tracking

Gather metric from different locations

Gather application logs

Stream processing

Decoupling of system dependencies

Integration with others system/technologies



Kafka terminologies

Producers

Consumers

Topics

Partitions

Broker

Consumer groups

Cluster/Replicate

Offset



Learning paths

Part 1

Kafka theory

Starting Kafka

Kafka CLI

Kafka with Java

Part 2

Configuration

Producers

Consumers

Monitoring



Kafka theory



Topics, partitions and offsets

Topics

Stream of data

Similar to a table in database

You can have many topics as you want

A topic is identified by **name**

Topic



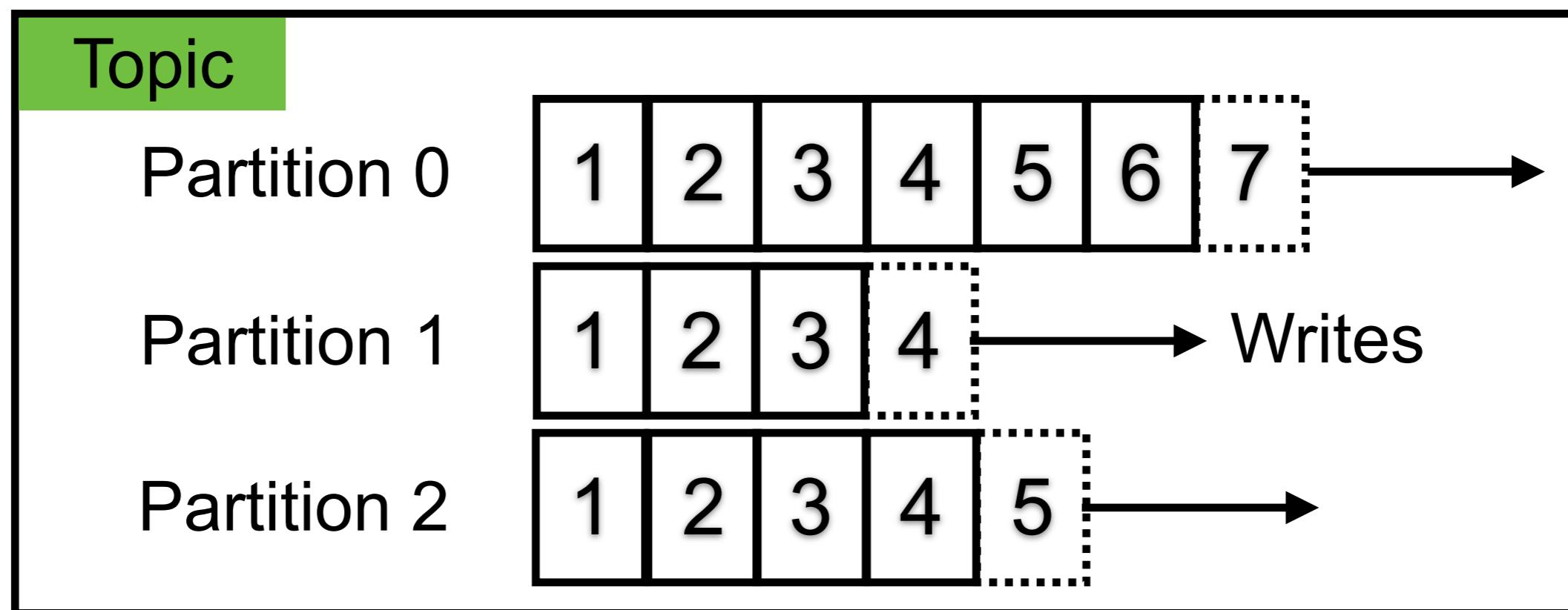
Topics, partitions and offsets

Partitions

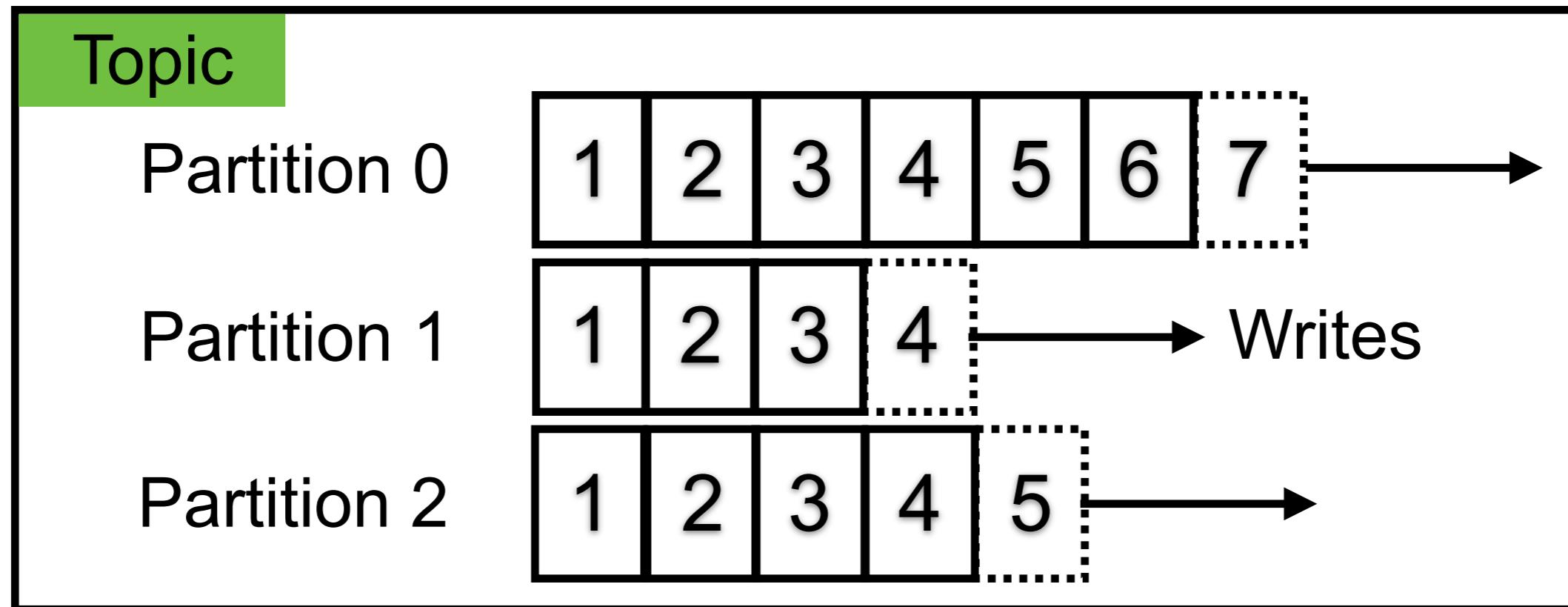
Topics are split in partitions

Each partition is **ordered**

Each message in partition get incremental id (**offset**)



Topics, partitions and offsets



Order is guaranteed only within partition

Data is keep in limited time (**Default = 1 week**)

Data is **immutable** (can't be changed)

Data is assigned **randomly** to a partition



Brokers and topics

Brokers

Kafka cluster is composed of multiple brokers (servers)

Each broker is identified by ID (integer)

Each broker contains certain topic partitions

After connecting any broker (bootstrap broker), you will connected to the entire cluster

Broker 1

Broker 2

Broker 3



Brokers and topics

Brokers

Good number to start id 3 brokers

Broker 1

Broker 2

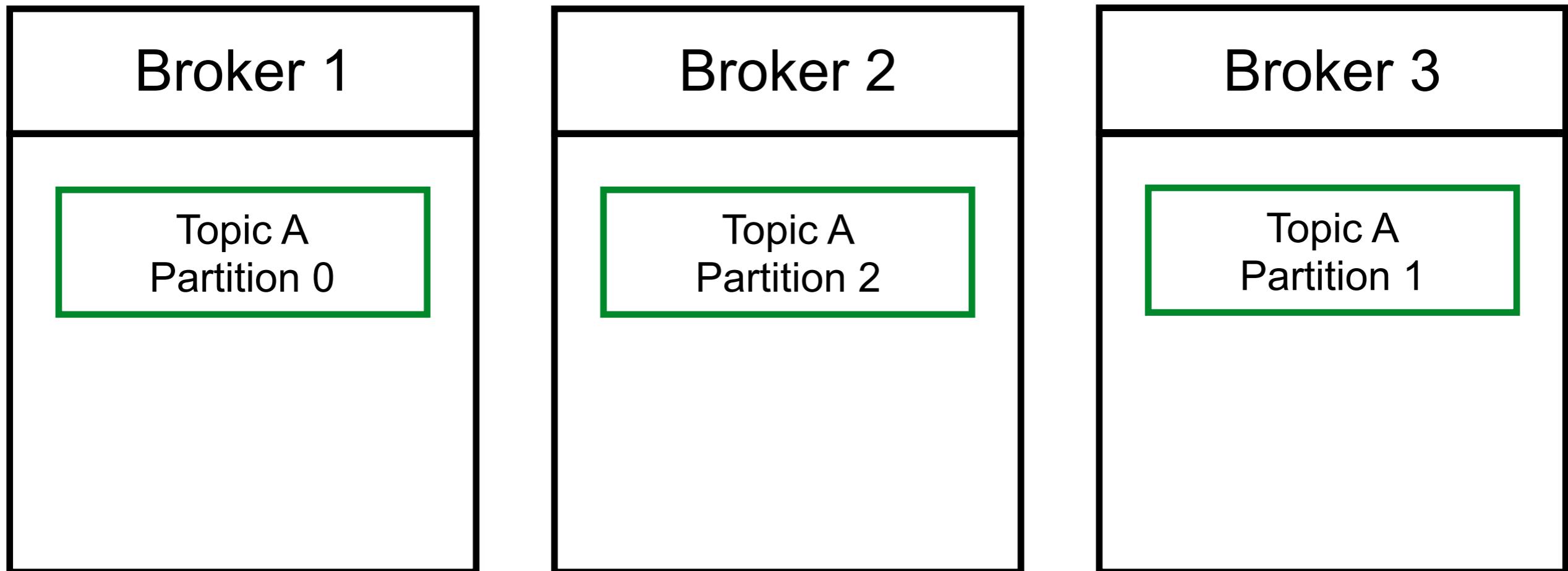
Broker 3



Brokers and topics

Example

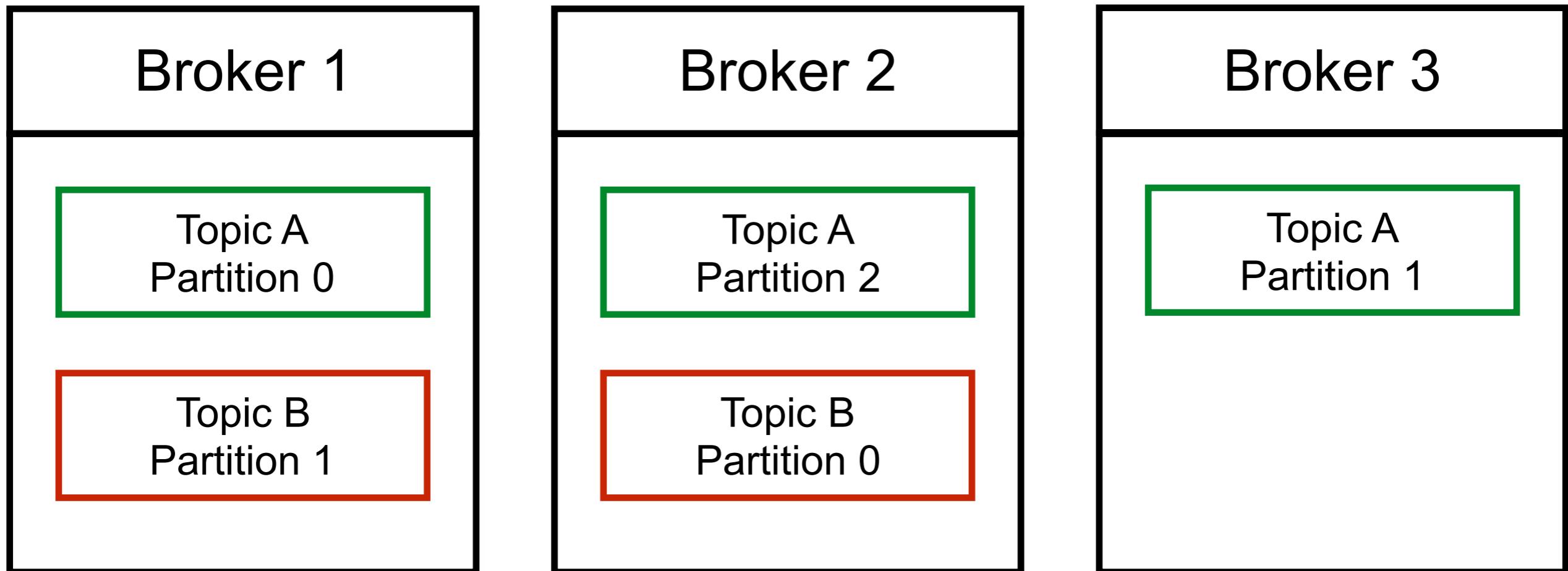
Topic A with 3 partitions



Brokers and topics

Example

Topic B with 2 partitions



Topic with replication factor

Topic should have a replica factor > 1 (2-3)

replica factor $<$ no. of brokers

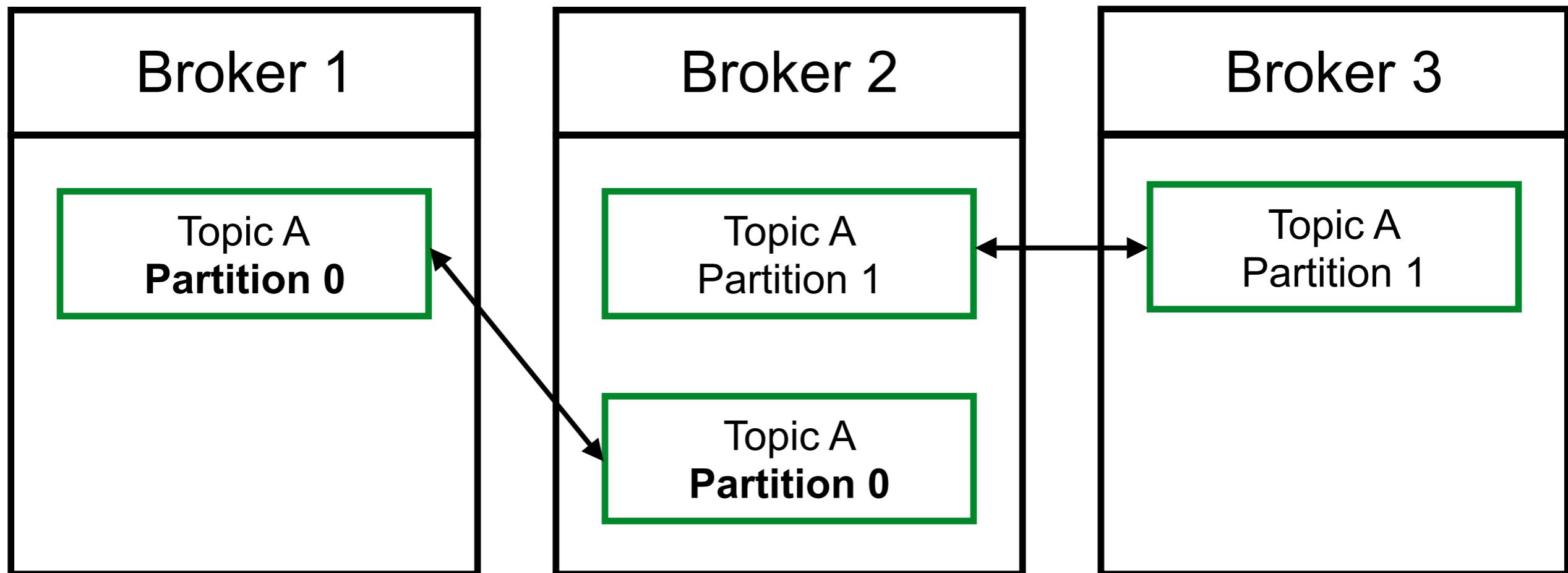
This way if a broker down, another broker can serve the data



Topic with replication factor

Example

Topic A with 2 partitions and replication factor = 2



Leader for a partition

At any time only **one Broker** can be leader for partition

Only leader partition can receive and serve data for a partition

Other brokers will synchronize the data

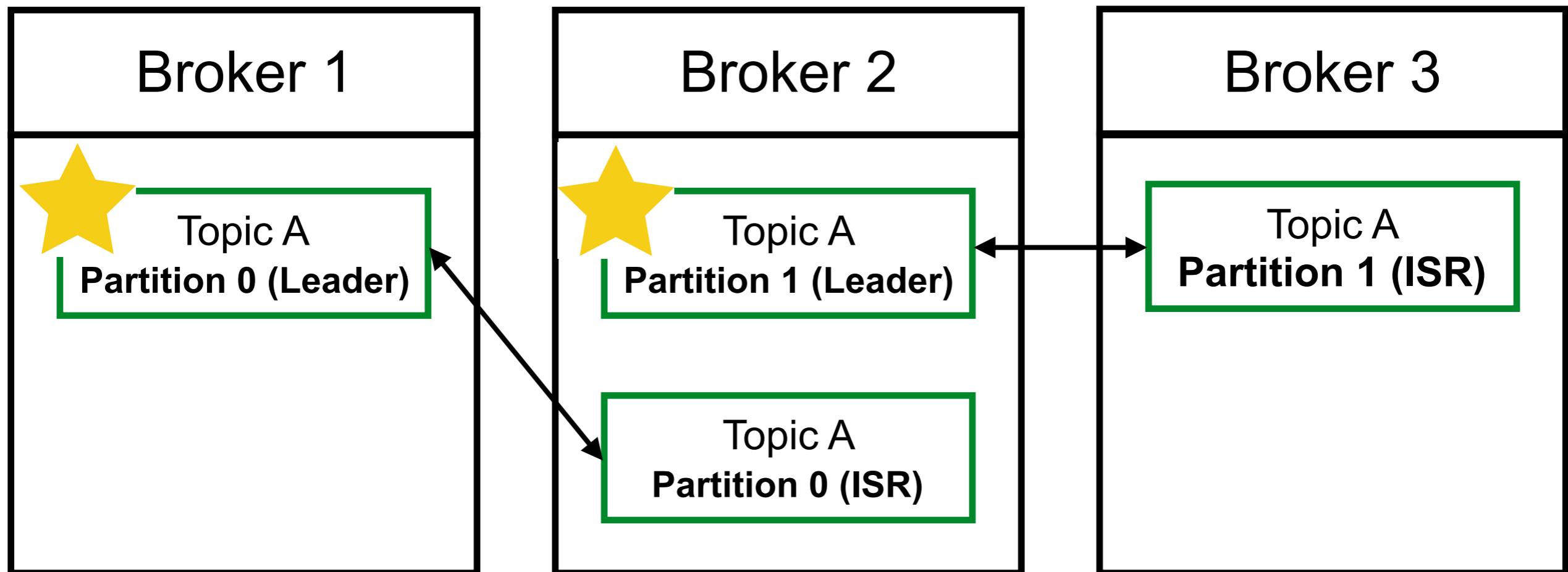
Other partition called **in-sync replica (ISR)**



Leader for a partition

Example

Topic A with 2 partitions and replication factor = 2



Producers

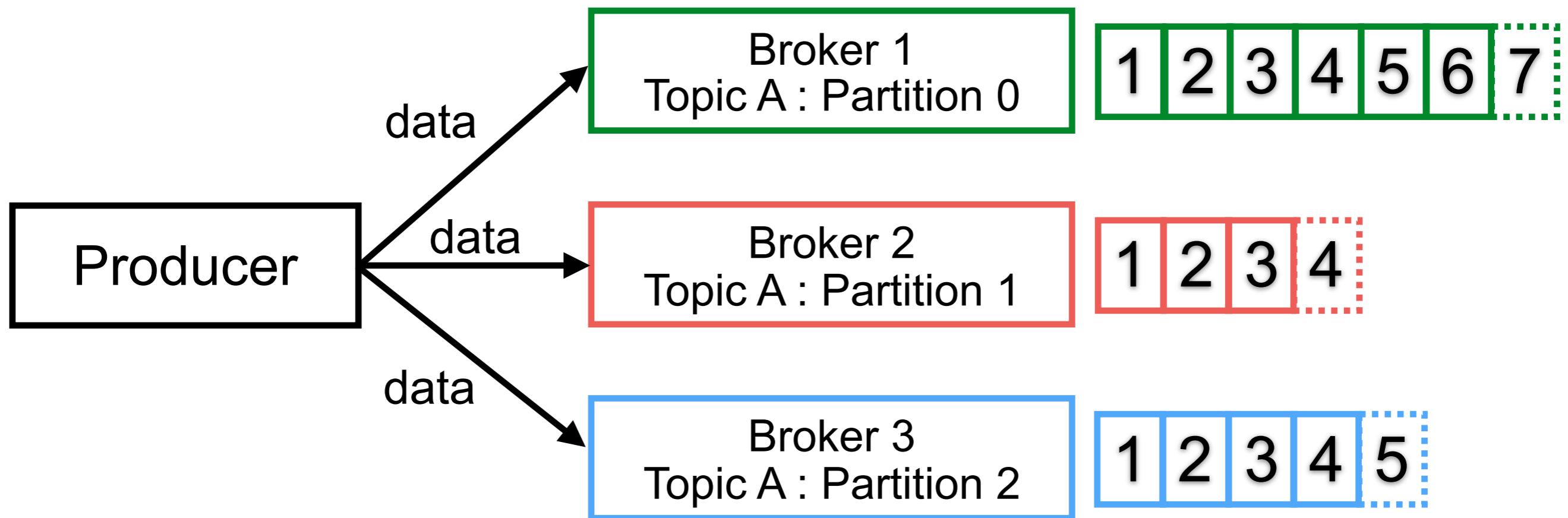
Producers write data to topics

Producers automatically know to broker and partition to write

When broker failures, producers will automatically recover



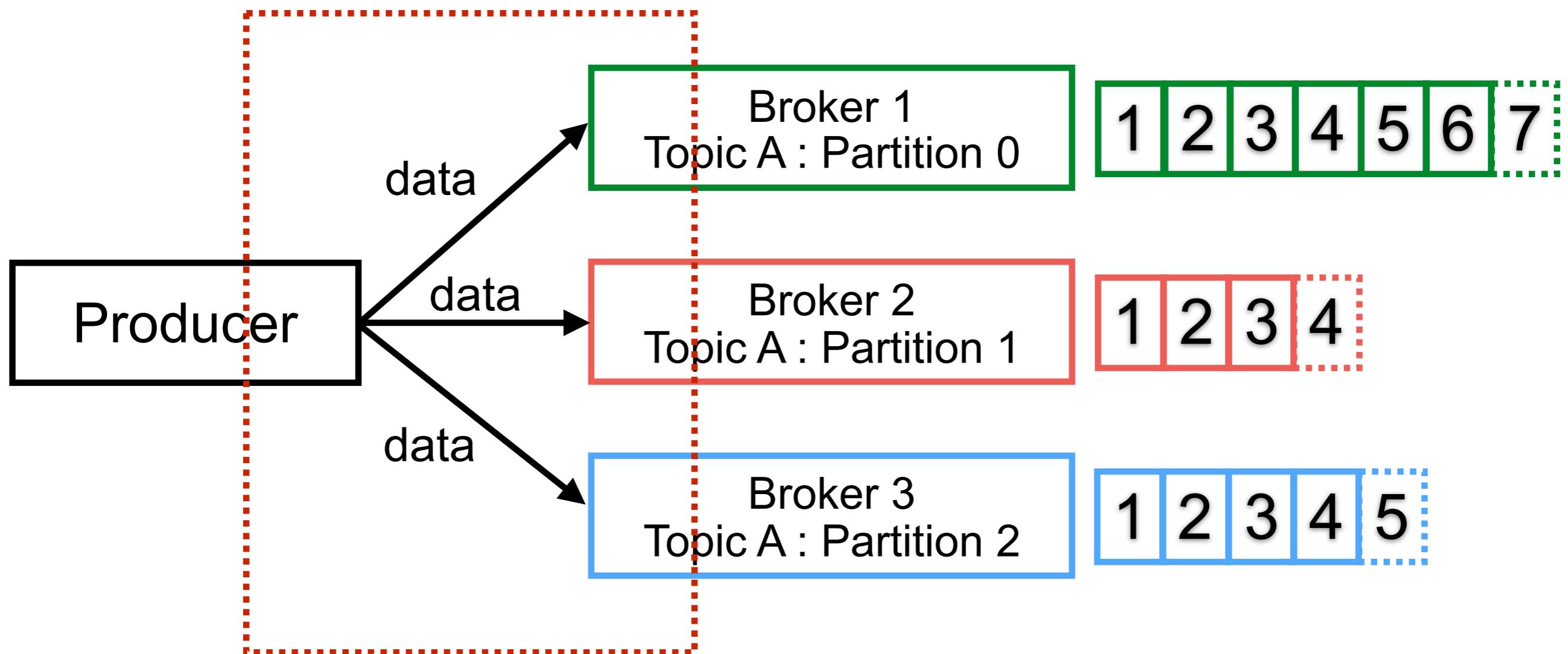
Producers



*** *The load is balanced to many brokers (no. of partitions)* ***



Producers issue to write data !!



Producers with acknowledgment

acks=0

Producer not wait for acknowledgment

Possible data loss

acks=1

Producer will wait for **leader** acknowledgment

Limited data loss

acks=all

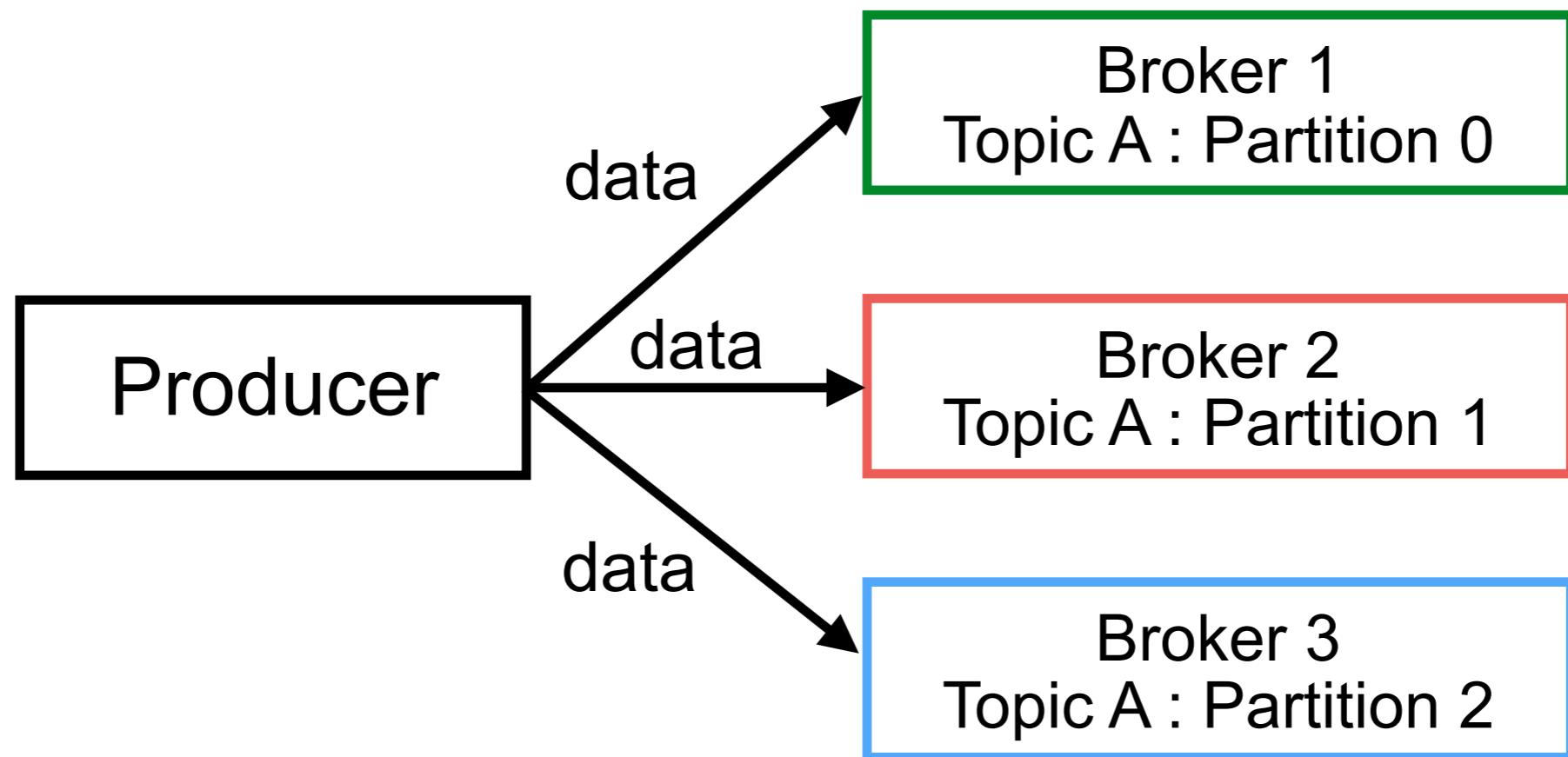
Producer will wait for **leader + ISR** acknowledgment

No data loss



Producers with message keys

Producers can choose to sent a **key** with data
Key = null, data is sent **round-robin**



Producers with message keys

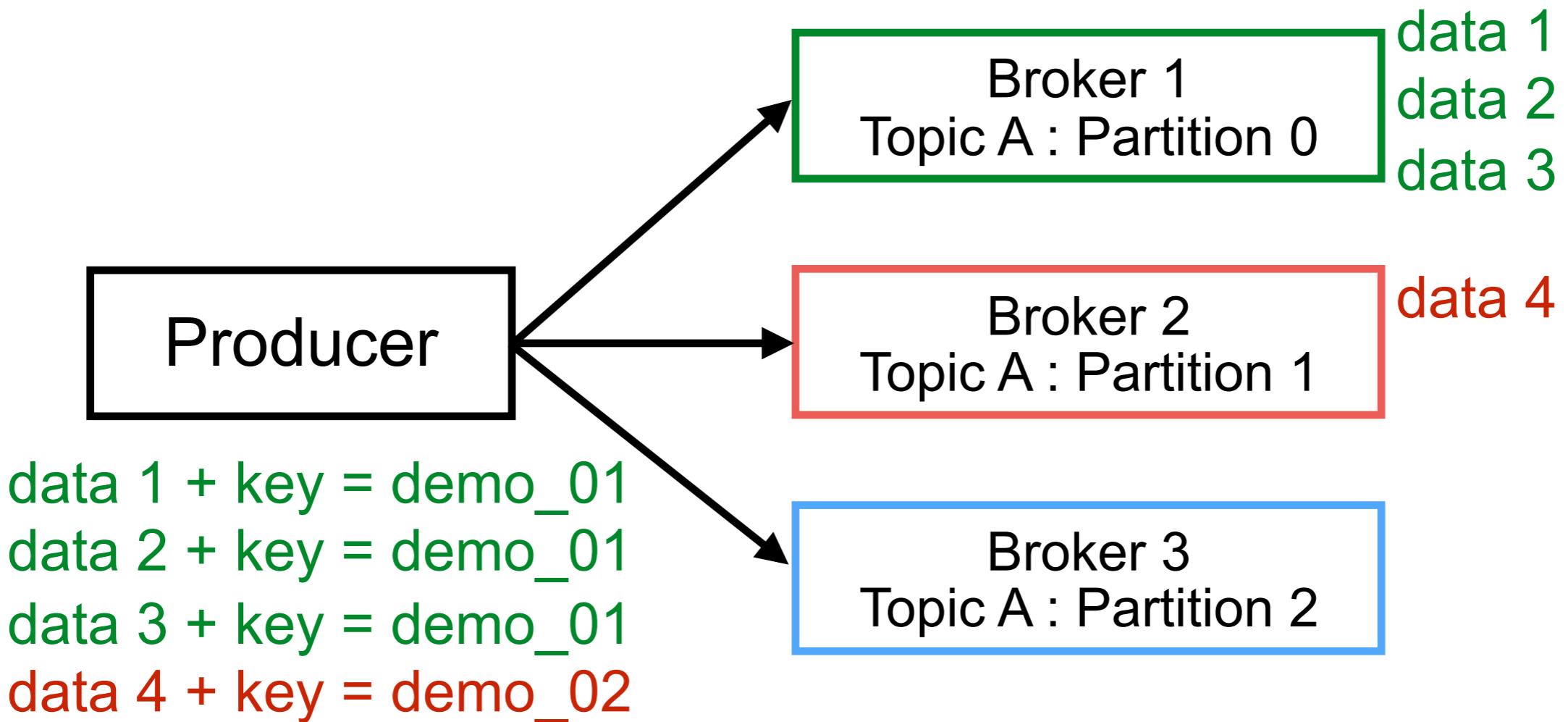
```
public int partition(String topic, Object key, byte[] keyBytes, Object value, byte[]  
... if (keyBytes == null) {  
...     return stickyPartitionCache.partition(topic, cluster);  
... }  
... List<PartitionInfo> partitions = cluster.partitionsForTopic(topic);  
... int numPartitions = partitions.size();  
... // hash the keyBytes to choose a partition  
... return Utils.toPositive(Utils.murmur2(keyBytes)) % numPartitions;  
}
```

<https://github.com/apache/kafka/blob/trunk/clients/src/main/java/org/apache/kafka/clients/producer/internals/DefaultPartitioner.java>



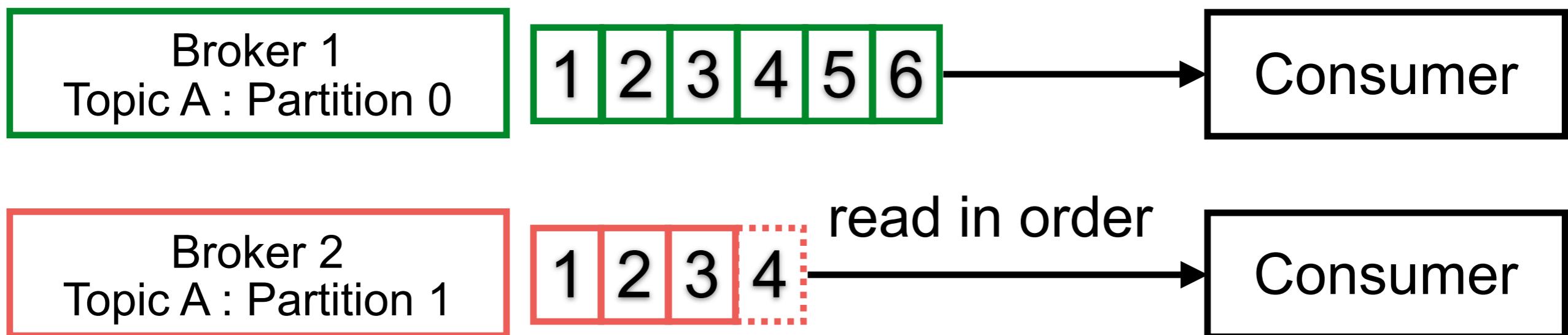
Why use message keys ?

You need message ordering



Consumers

Consumers read data from topic
Consumers know which broker to read from
Data will read in order **within each partition**
When broker **failures**, consumer know how to recover



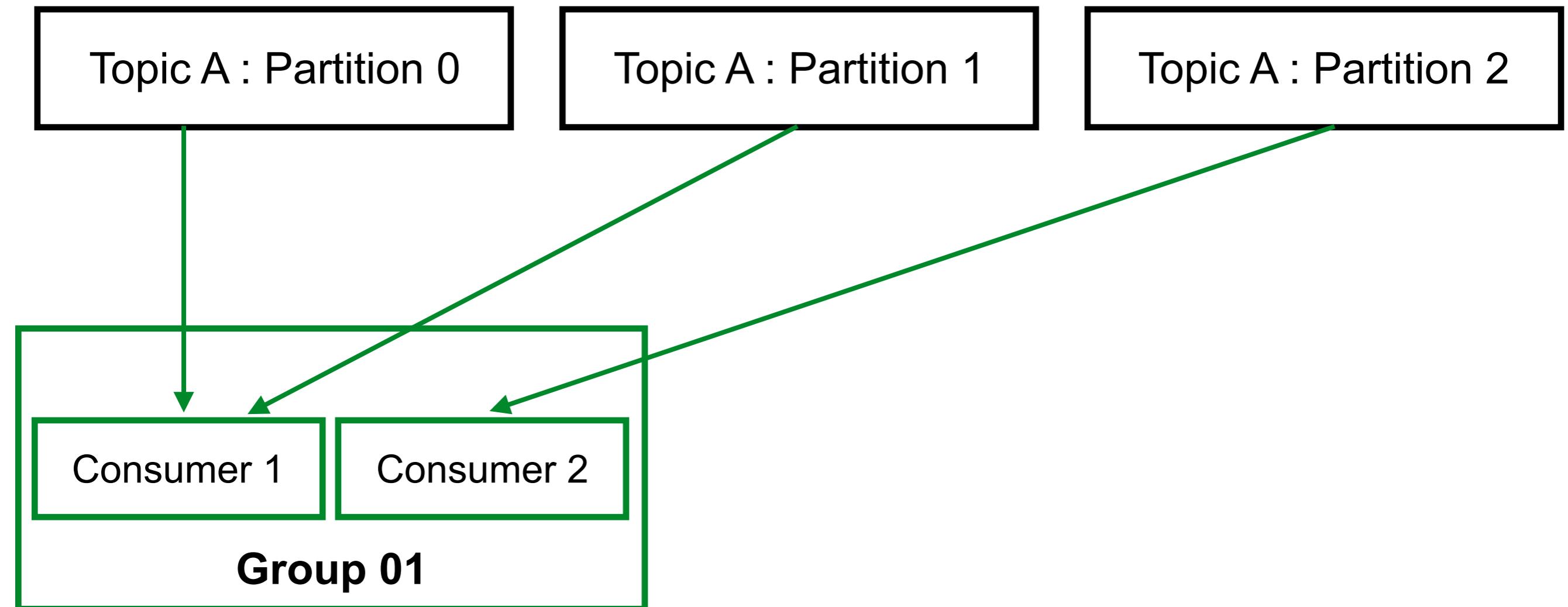
Consumer groups

Consumers read data in consumer groups

Each consumer in a group read from exclusive partitions



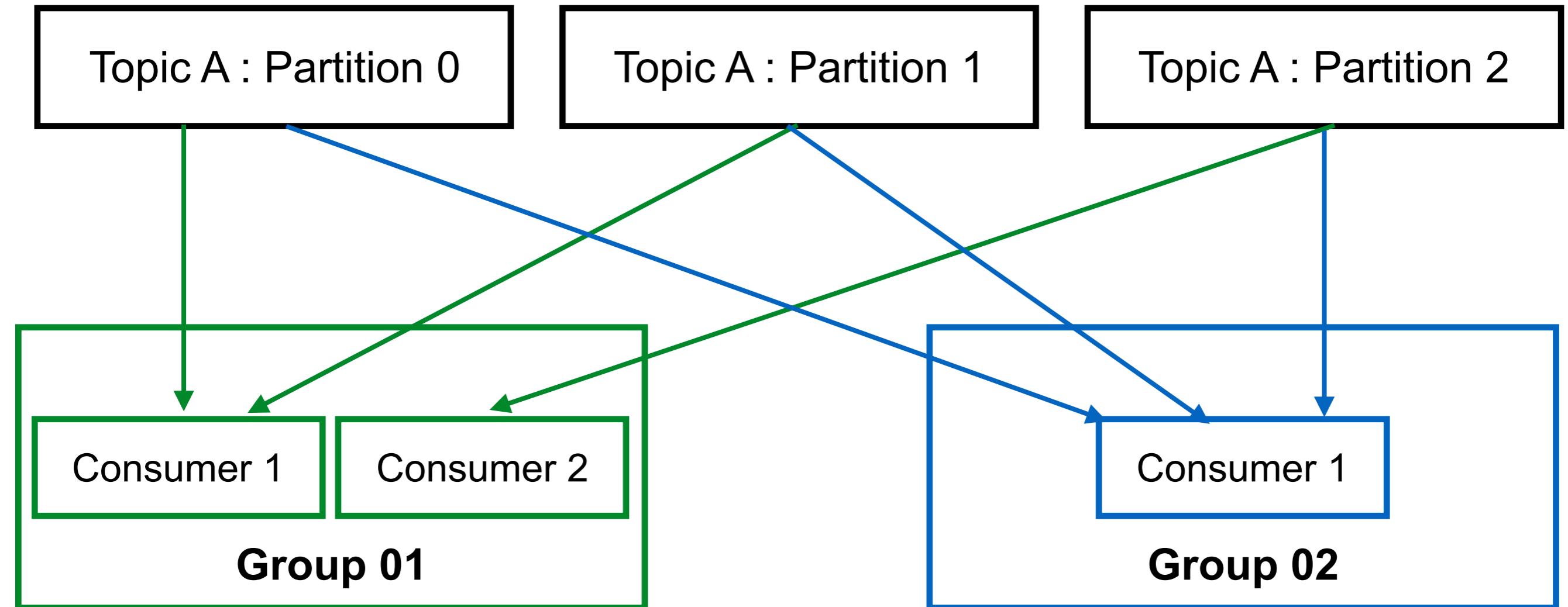
Consumer groups



Consumer will automatically use a GroupCoordinator and ConsumerCoordinator to assign a consumer to a partition.

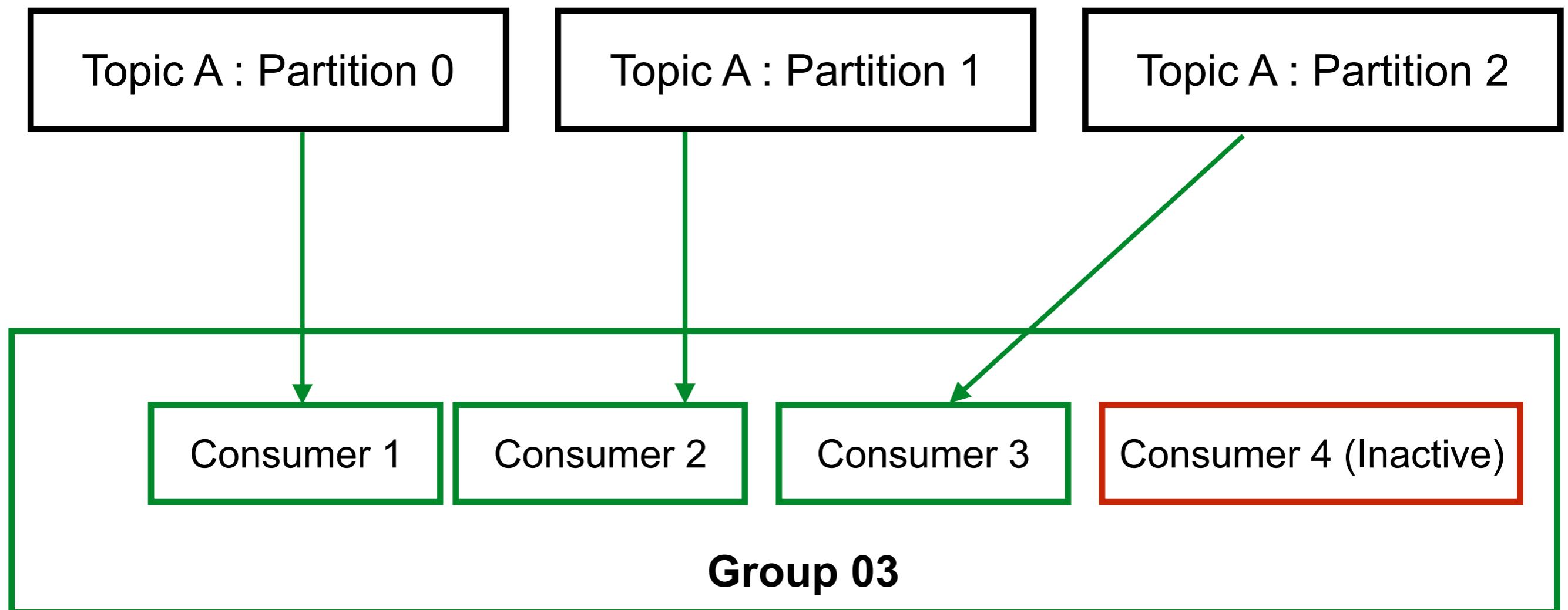


Consumer groups

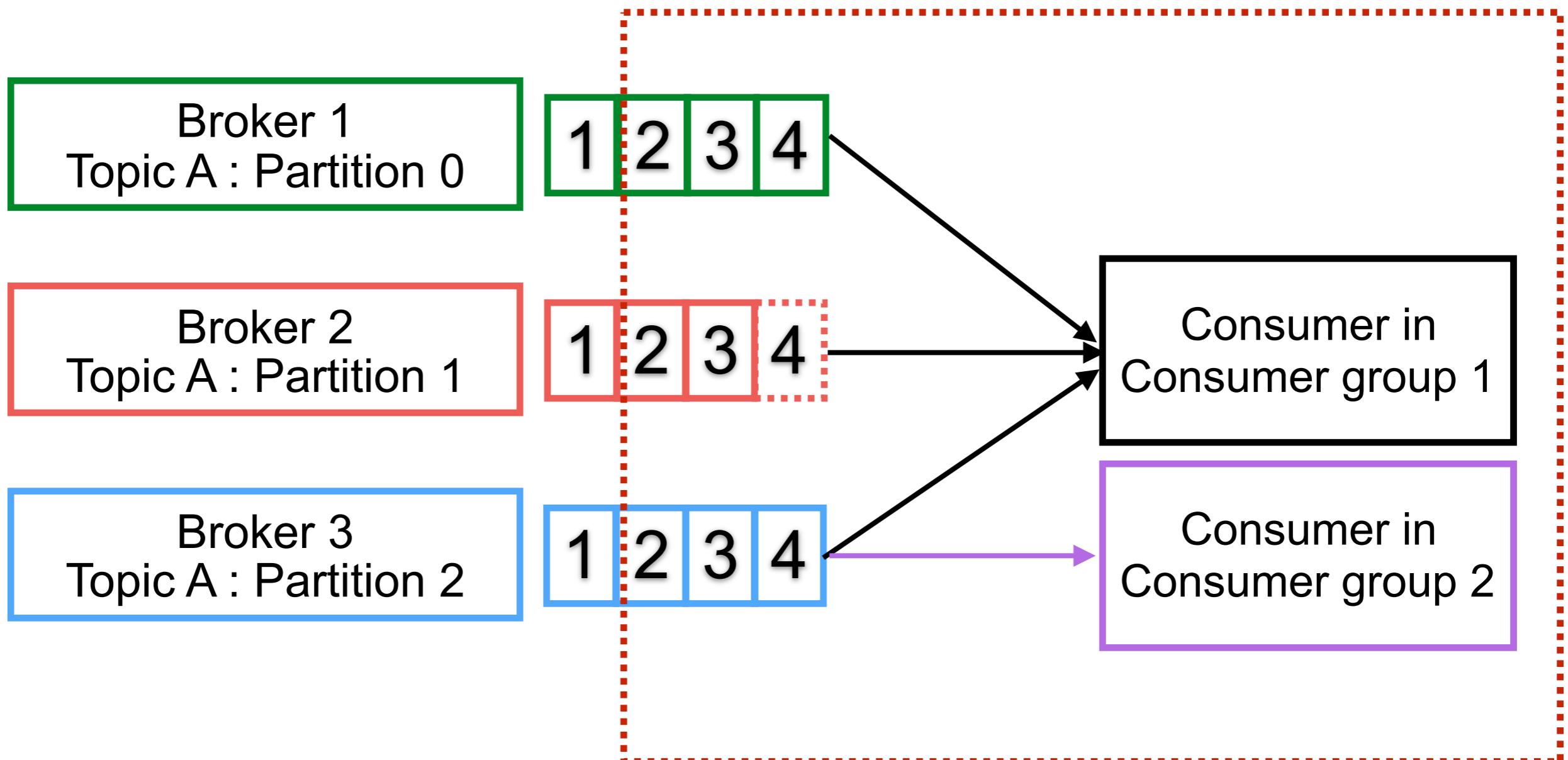


Consumers > partitions ?

Some consumers will **inactive**



Consumers offsets



Consumers offsets

Kafka store the offset at which a consumer group has been reading

The offsets committed live in topic named
“**__consumer_offsets**”

When consumer in a group has processed data received from Kafka,
it should be **committing the offsets**



When to commit the offset ?



Delivery semantics for consumer

At most once

At lease once (preferred)

Exactly once



1. At most once

Offsets are committed as soon as the message is received

If processing go wrong, the message will be loss!!



2. At lease once

Offsets are committed after the message is processed

Messages are never lost but may be **redelivered**

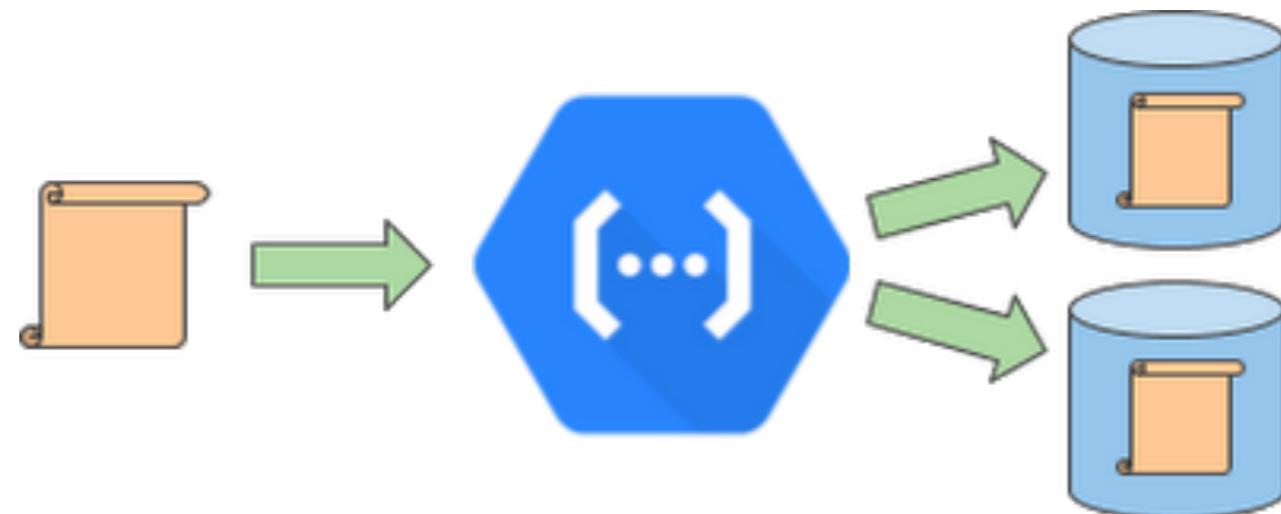
If processing go wrong, the message will be **read again**



2. At lease once

Make sure your processing is **idempotent**

Processing again the message not impact to your system !!



3. Exactly once

Each message is delivered once and only once
Can be achieved for Kafka (Workflow, Stream API)



Kafka broker discovery

Every Kafka broker is called “bootstrap server”
You only need to connect to one broker, and you
will connected to the entire cluster

Broker 1
(bootstrap)

Broker 2
(bootstrap)

Kafka cluster

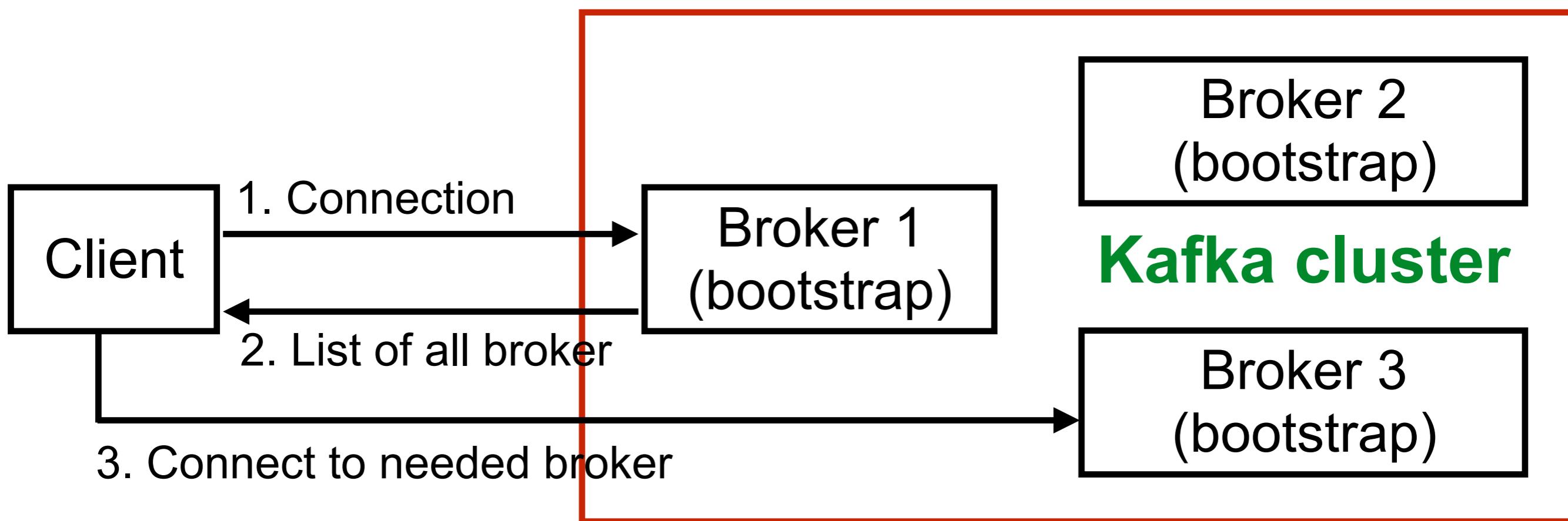
Broker 3
(bootstrap)

Broker 4
(bootstrap)



Kafka broker discovery

Each broker knows about all brokers, topics and partitions (metadata)



Apache Zookeeper

Kafka can not work without Zookeeper !!



APACHE
ZooKeeperTM

<https://zookeeper.apache.org/>



Apache Zookeeper

Zookeeper **manages** brokers

Zookeeper help in performing **leading election** for partitions

Zookeeper sends **notifications** to Kafka in case of changes (new topic, broker die)

Zookeeper by design operates with a odd number of servers (3, 5, 7)

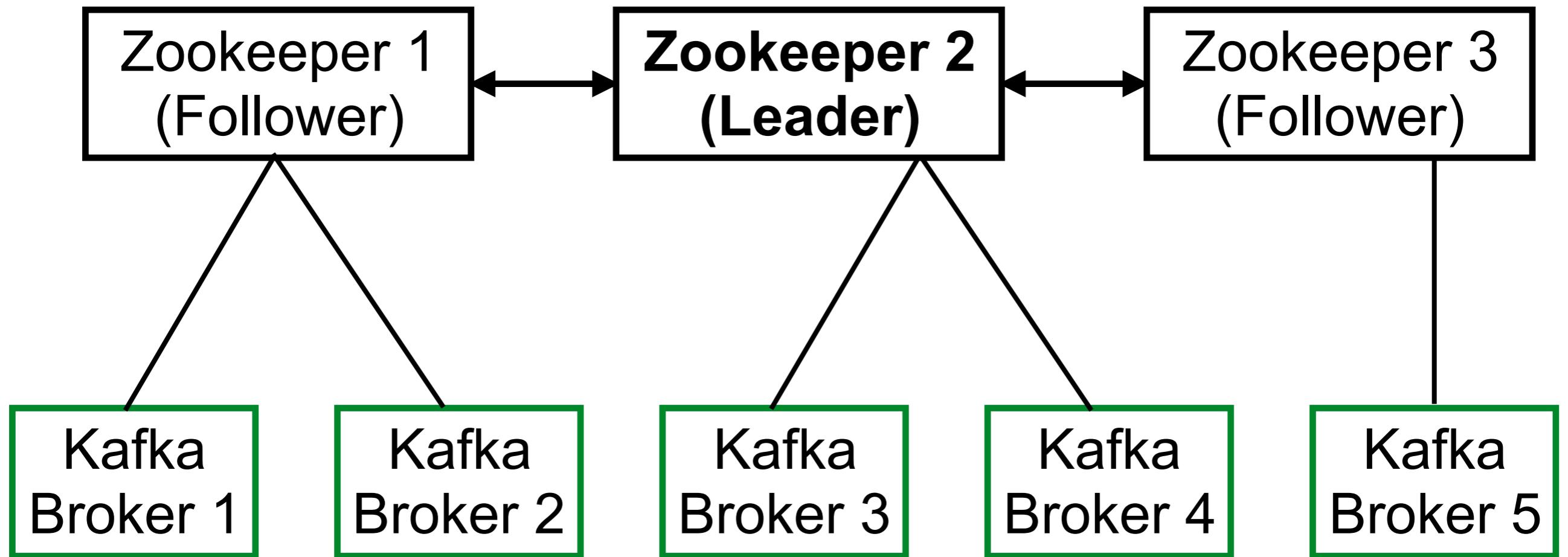


Zookeeper architecture

Leader for write
Follows for read



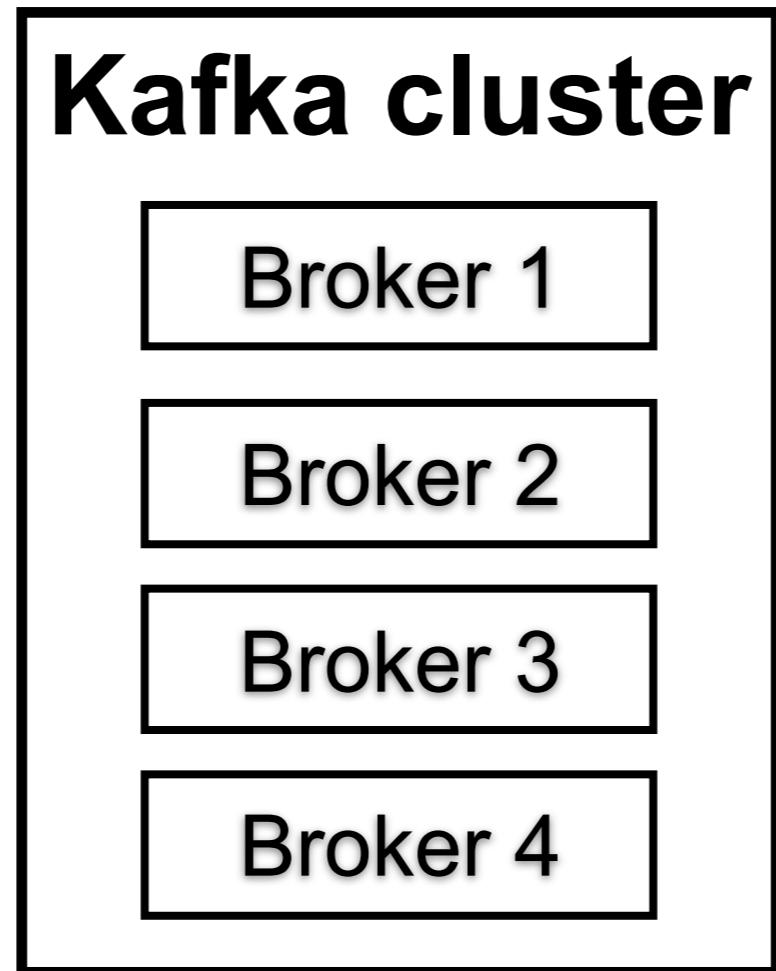
Zookeeper architecture



Summary of Kafka



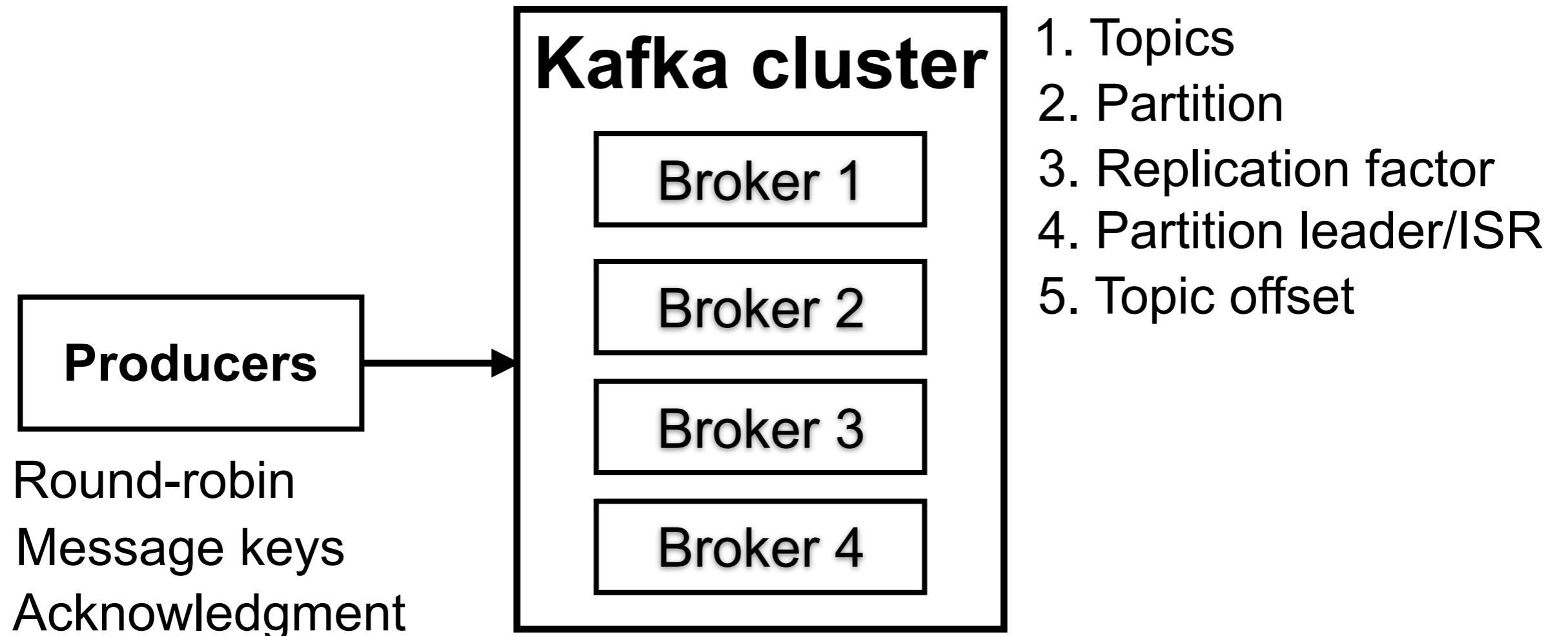
Kafka concepts



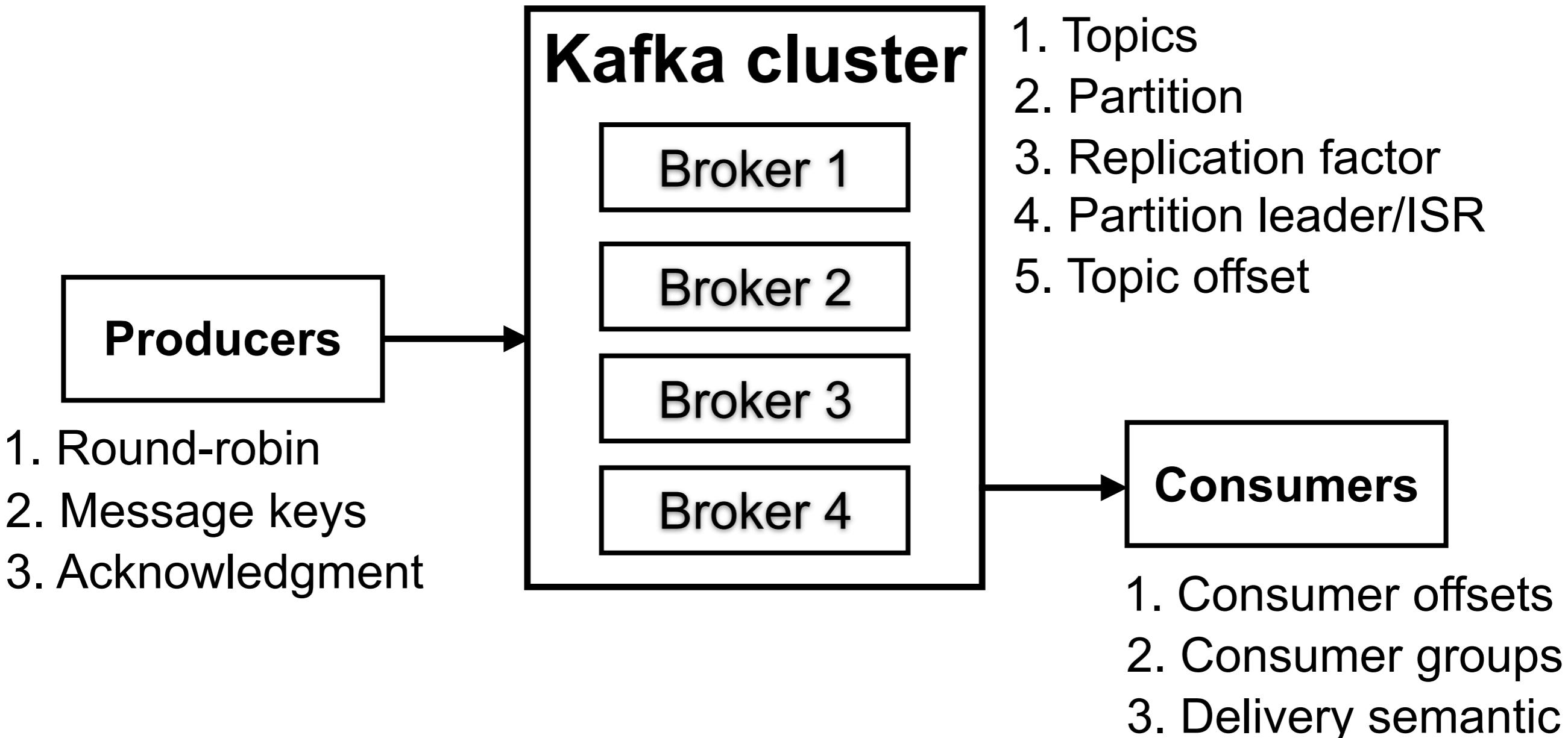
1. Topics
2. Partition
3. Replication factor
4. Partition leader/ISR
5. Topic offset



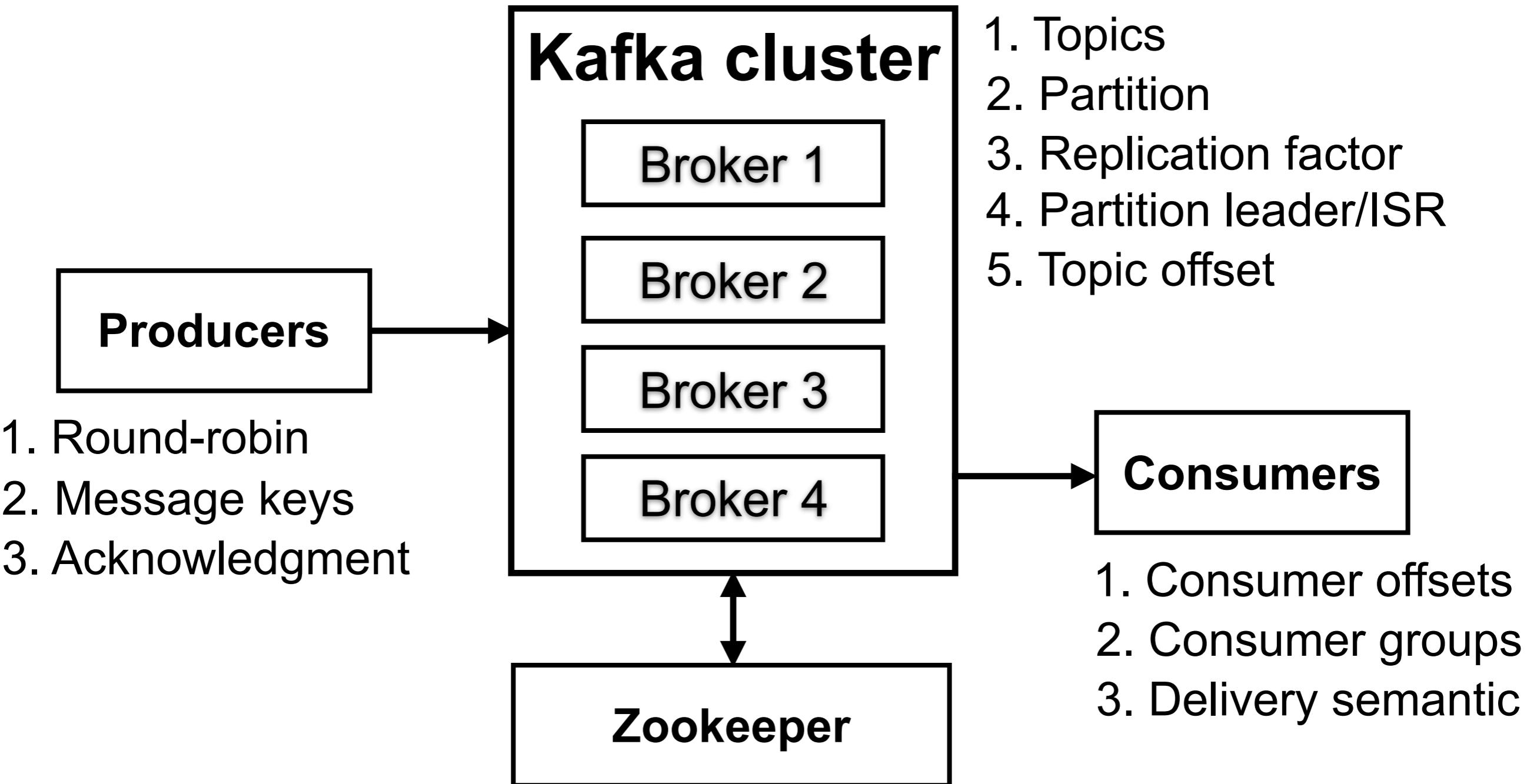
Kafka concepts



Kafka concepts



Kafka concepts



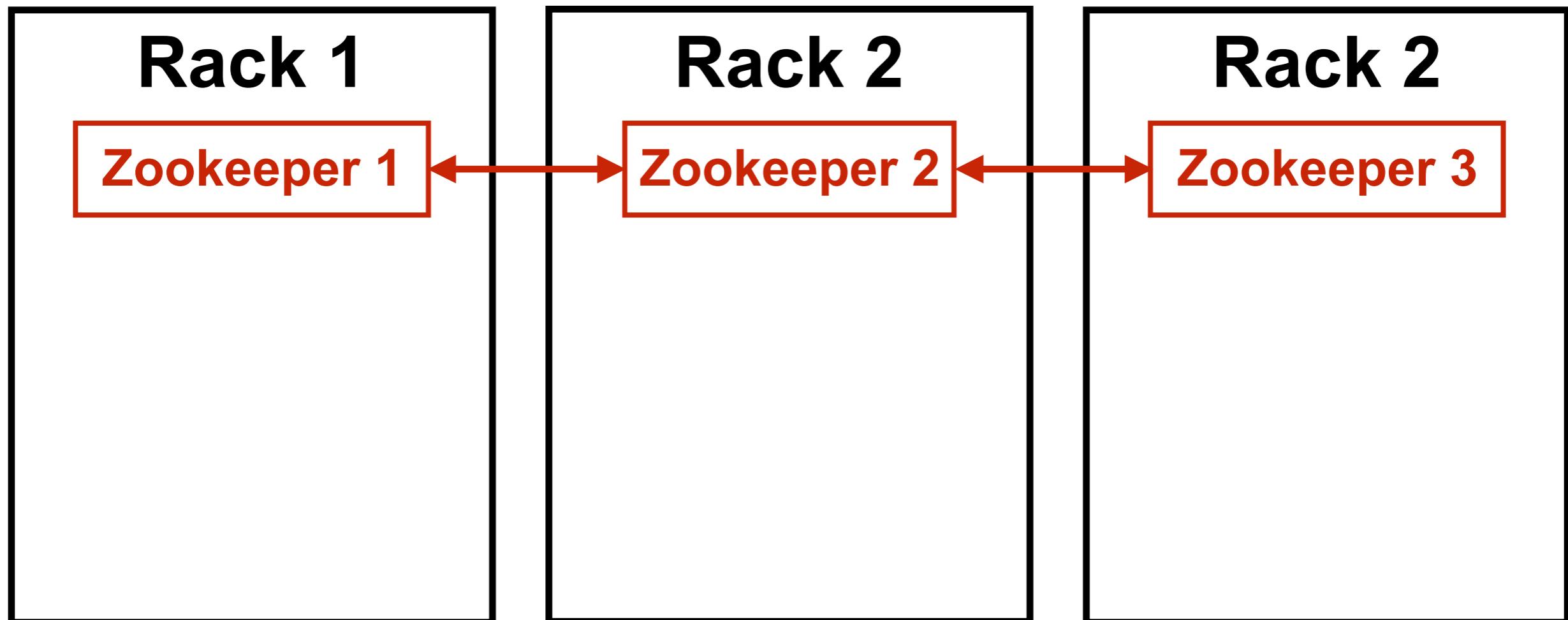
Kafka workshop



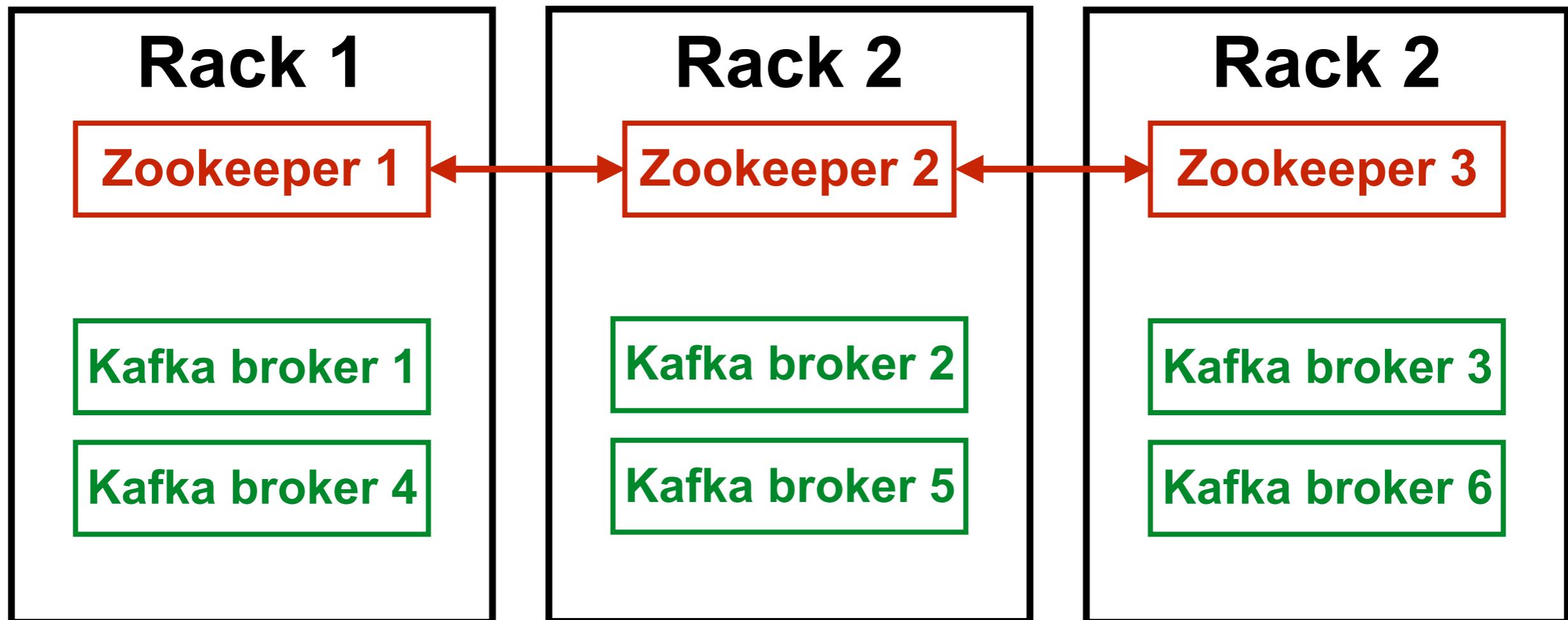
Monitoring Kafka



Kafka cluster



Kafka cluster



Kafka cluster

It's not easy to setup a cluster

Need to isolate each Zookeeper and broker on separate servers

Need to implement a **Monitoring system**

Need skill of **operation teams**

Need a good **Kafka Admin**



Kafka monitoring



Tips #1

Please monitor Your Kafka !!



Monitoring ?

Broker health
Message delivery
Performance
Capacity



Kafka monitoring

Kafka exposes **metrics** through JMX

These metrics are very important for monitoring



Kafka monitoring

JConsole
JMX/Metrics integration
Burrow



Keep Kafka metrics ?

ELK stack
Prometheus
Confluent control center
Datadog
NewRelic
etc...



Important metrics

Under replicated partitions

of partitions are have problem with the **ISR**

May indicate a high load on the system

Request handlers

Utilization of threads for I/O, network

Utilization of Kafka broker



Important metrics

Request timing

How long it takes to reply to requests

Low is better, latency will improved

<https://kafka.apache.org/documentation/#monitoring>

<https://docs.confluent.io/current/kafka/monitoring.html>

<https://www.datadoghq.com/blog/monitoring-kafka-performance-metrics/>

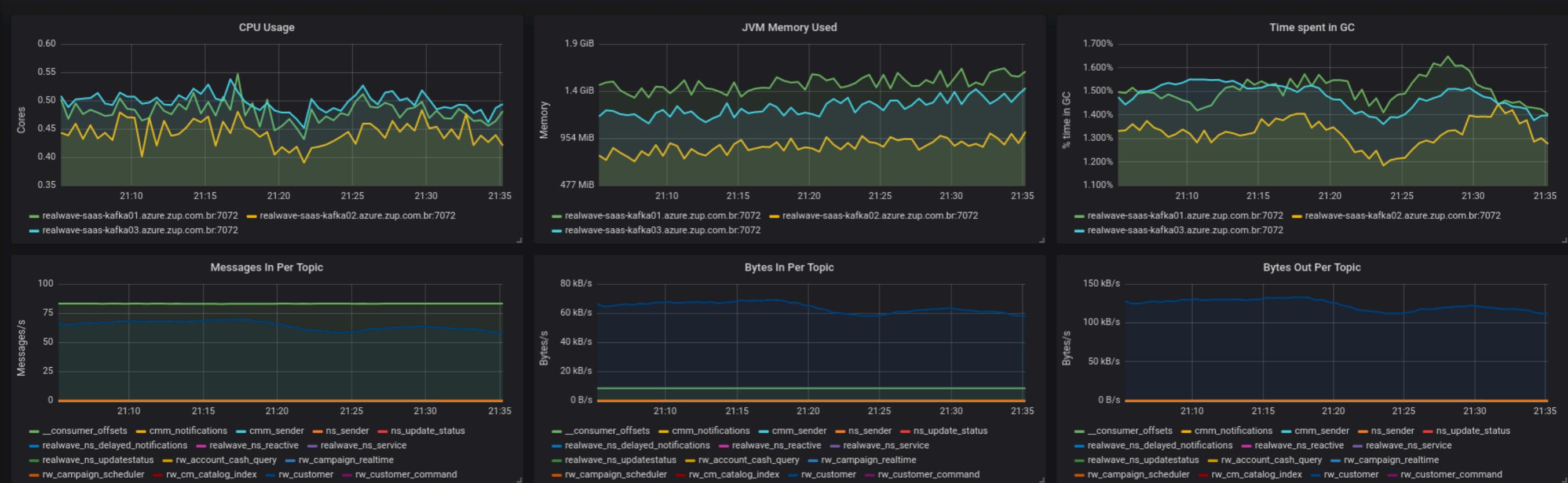


Tips #2

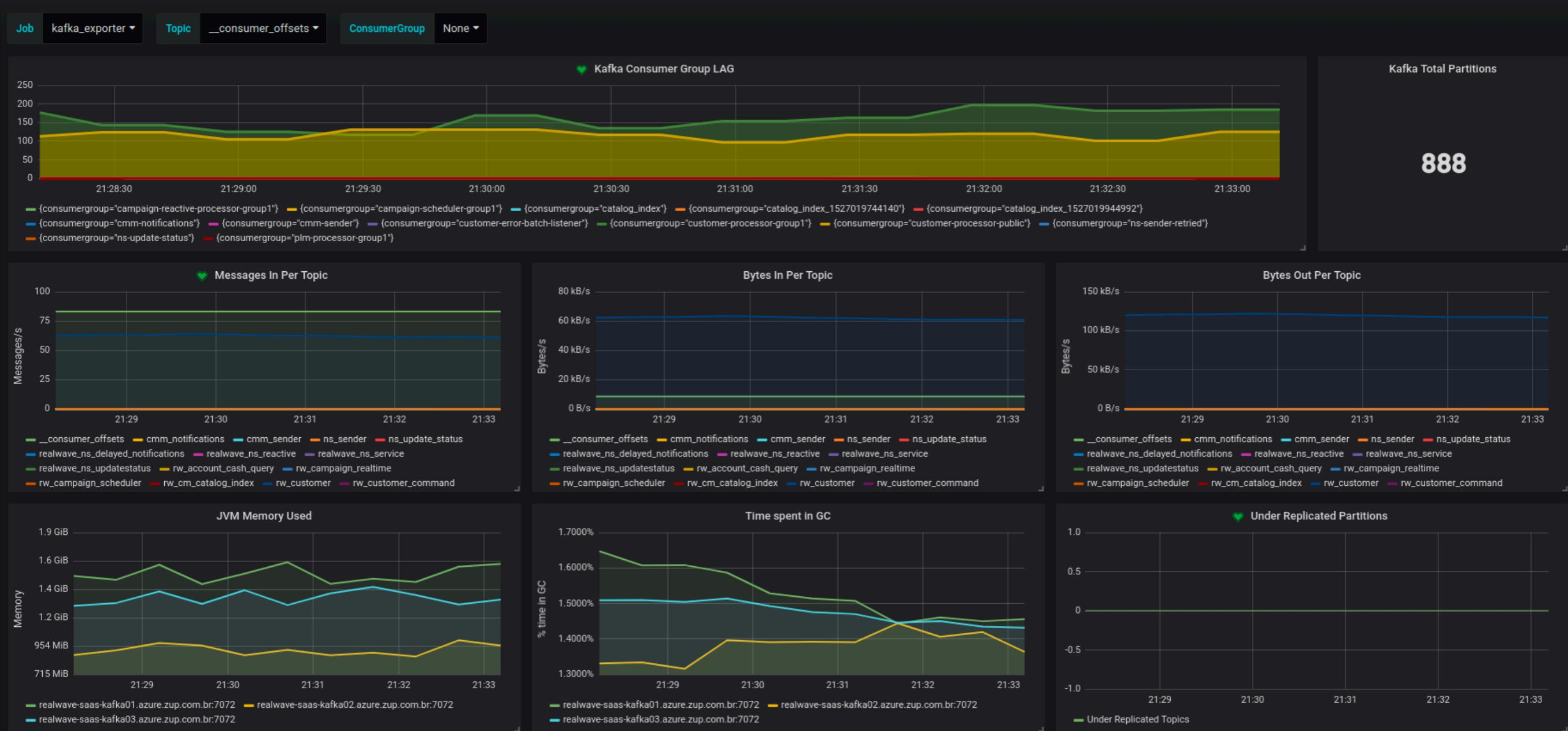
Have a dashboard that lets you know
“Everything is OK ?”
(in one look)



Dashboard



Dashboard



Tips #3

Don't watch the dashboard
Alert on what is important

Only restart if you know why this will fix the issue !!



Capacity planning

CPU

Network and thread pool usages

Request latency

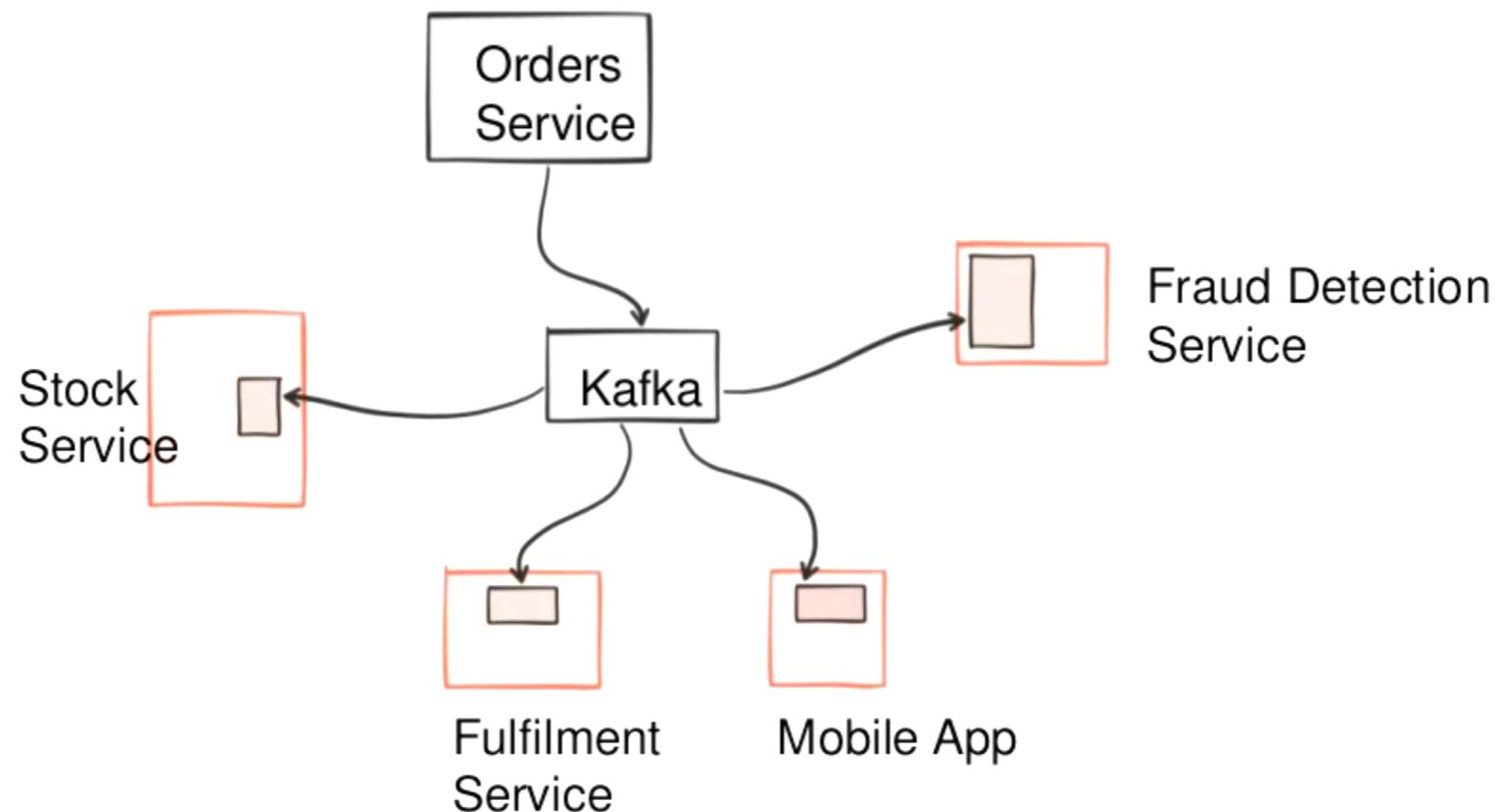
Network utilization

Disk utilization



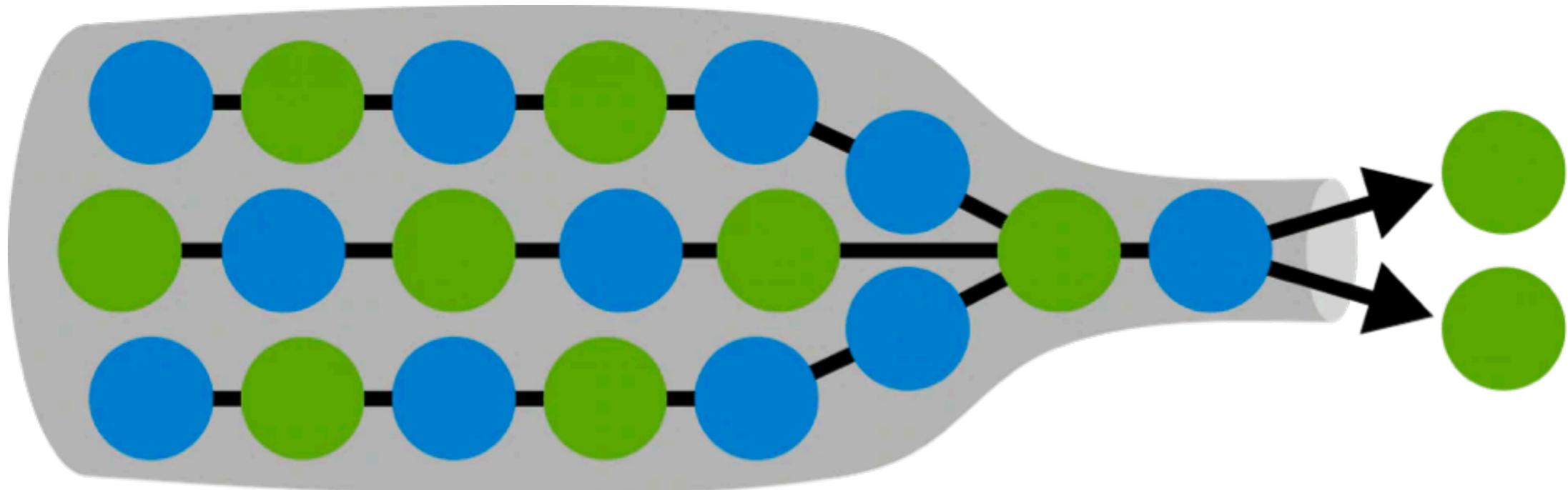
Tips #4

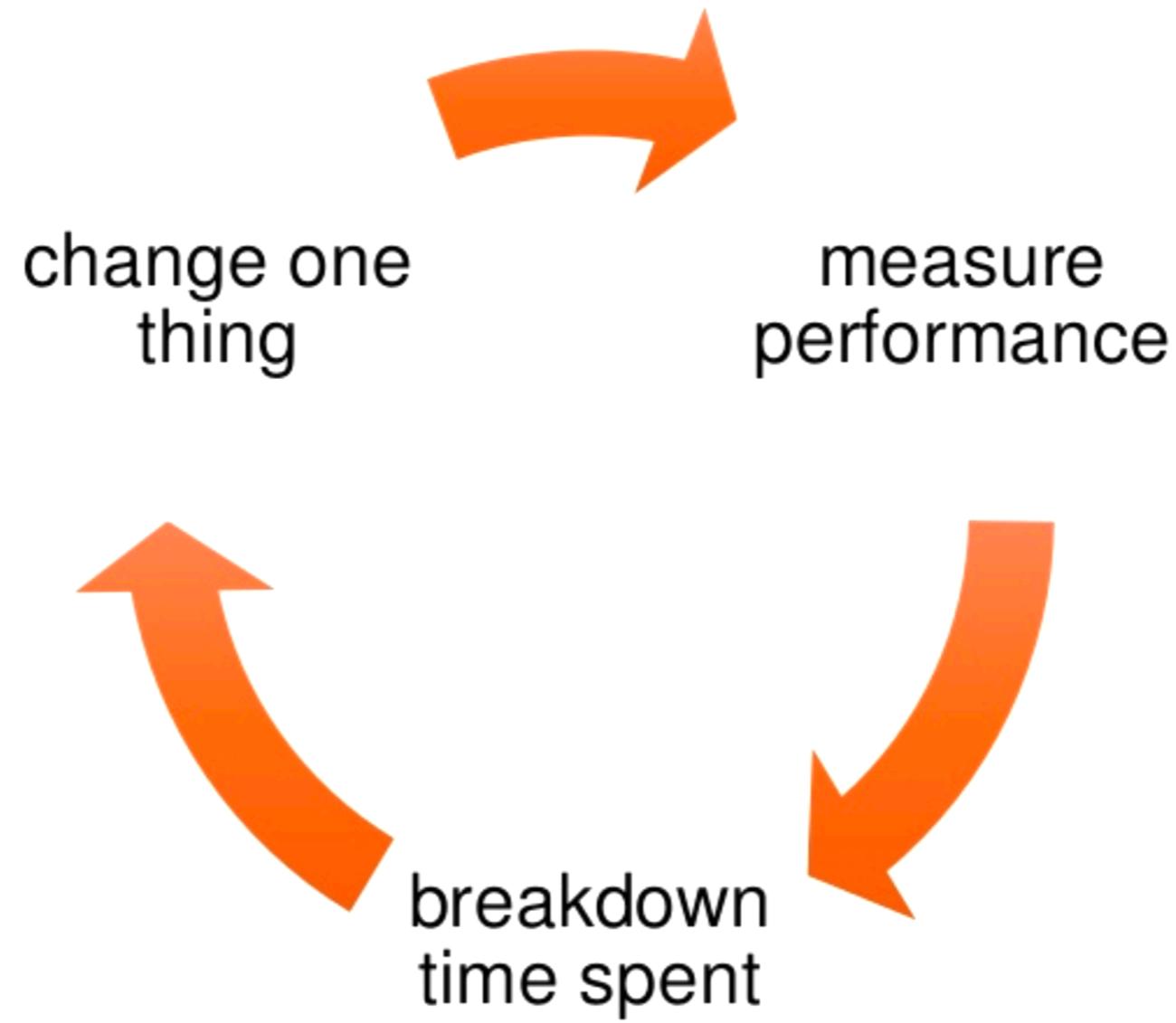
Monitoring brokers isn't enough
Need to monitor events



Tips #4

Tuning the bottlenecks





Life cycle of request

Client send request to broker

Network thread get request and put on queue

I/O thread/handler pick up request and process

(Read and write from/to disk)

Waiting for other brokers to ack messages

Put response on queue

Network thread send response to client



Kafka for operation



Kafka operations

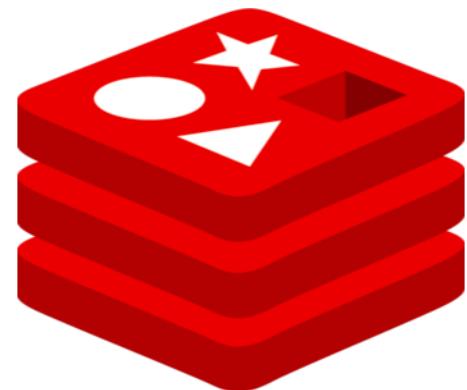
- Rolling restart of brokers
- Update configurations
- Rebalancing partitions
- Increase replication factor
- Add/replace/remove a broker
- Upgrade a Kafka cluster with zero downtime



Kafka workshop

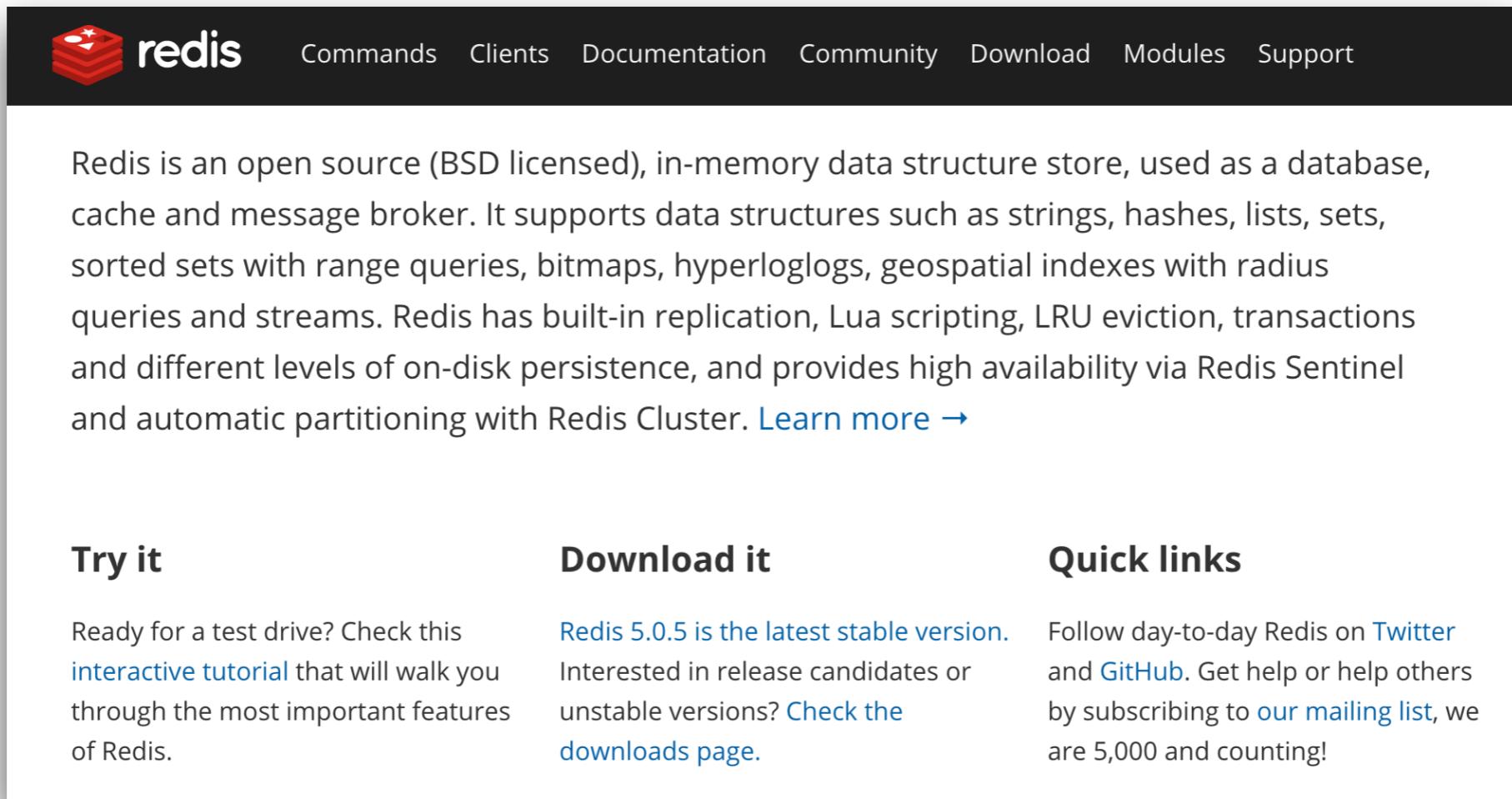


Redis



Redis

In-memory data structure store Using for database cache and message broker



The screenshot shows the Redis homepage with a dark header bar containing the Redis logo and navigation links: Commands, Clients, Documentation, Community, Download, Modules, and Support. The main content area contains a brief introduction to Redis, followed by three sections: Try it, Download it, and Quick links.

Redis is an open source (BSD licensed), in-memory data structure store, used as a database, cache and message broker. It supports data structures such as strings, hashes, lists, sets, sorted sets with range queries, bitmaps, hyperloglogs, geospatial indexes with radius queries and streams. Redis has built-in replication, Lua scripting, LRU eviction, transactions and different levels of on-disk persistence, and provides high availability via Redis Sentinel and automatic partitioning with Redis Cluster. [Learn more →](#)

Try it	Download it	Quick links
Ready for a test drive? Check this interactive tutorial that will walk you through the most important features of Redis.	Redis 5.0.5 is the latest stable version. Interested in release candidates or unstable versions? Check the downloads page.	Follow day-to-day Redis on Twitter and GitHub . Get help or help others by subscribing to our mailing list , we are 5,000 and counting!

<https://redis.io/>

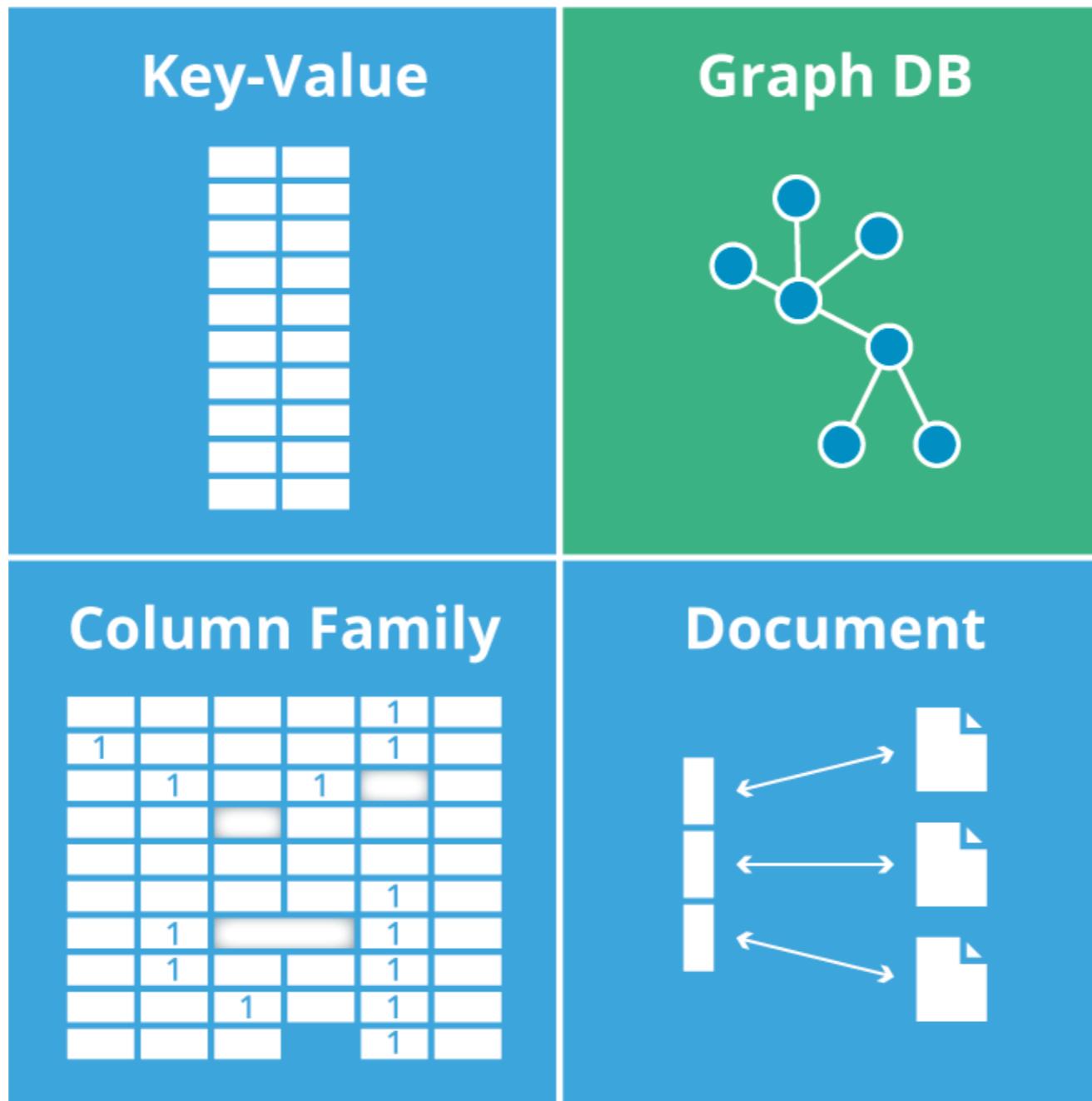


Learning path

Install and connect to Redis
Data storage and retrieval
Basic Redis data structures
Redis pub/sub functionality



NoSQL



Database ranking

351 systems in ranking, August 2019

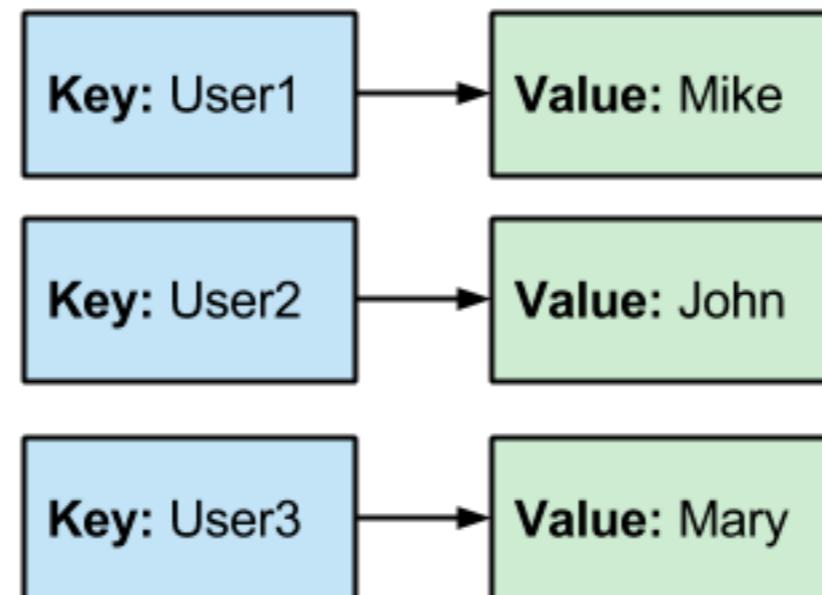
Rank			DBMS	Database Model	Score		
Aug 2019	Jul 2019	Aug 2018			Aug 2019	Jul 2019	Aug 2018
1.	1.	1.	Oracle 	Relational, Multi-model 	1339.48	+18.22	+27.45
2.	2.	2.	MySQL 	Relational, Multi-model 	1253.68	+24.16	+46.87
3.	3.	3.	Microsoft SQL Server 	Relational, Multi-model 	1093.18	+2.35	+20.53
4.	4.	4.	PostgreSQL 	Relational, Multi-model 	481.33	-1.94	+63.83
5.	5.	5.	MongoDB 	Document	404.57	-5.36	+53.59
6.	6.	6.	IBM Db2 	Relational, Multi-model 	172.95	-1.19	-8.89
7.	7.	8.	Elasticsearch 	Search engine, Multi-model 	149.08	+0.27	+10.97
8.	8.	7.	Redis 	Key-value, Multi-model 	144.08	-0.18	+5.51
9.	9.	9.	Microsoft Access	Relational	135.33	-1.98	+6.24
10.	10.	10.	Cassandra 	Wide column	125.21	-1.80	+5.63

<https://db-engines.com/en/ranking>



What is Redis ?

In-memory key-value store
Focus on performance and simplicity
All data keep in memory



What is Redis ?

REmote DIctionary Server

Data structure server

String, list, set, hash, sorted set

No index

No query language



Networking

Local or distributed access
Replication
Clustering



Durability options

Memory only
Snapshot (RDB)
Append-only file (AOF)
Master-slave replication



Use cases

Caching data

Session storage

Queue

Notifications

Leaderboards



Redis workshop



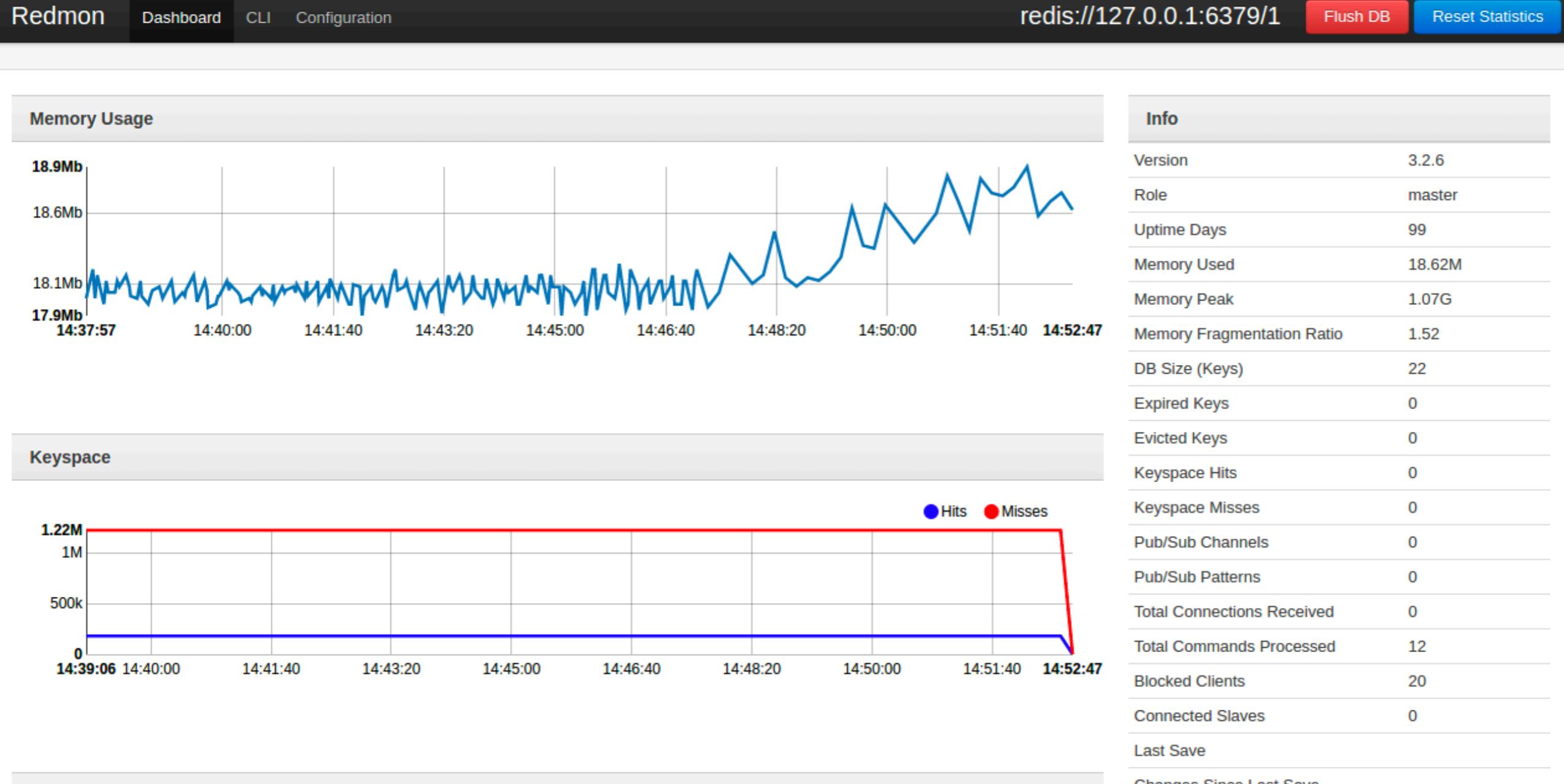
Monitoring Redis

Redis-cli info Redis-cli monitor

```
127.0.0.1:6379> info commandstats
# Commandstats
cmdstat_get:calls=797,usec=4041,usec_per_call=5.07
cmdstat_append:calls=797,usec=4480,usec_per_call=5.62
cmdstat_expire:calls=797,usec=5471,usec_per_call=6.86
cmdstat_auth:calls=147,usec=288,usec_per_call=1.96
cmdstat_info:calls=46,usec=902,usec_per_call=19.61
cmdstat_config:calls=2,usec=130,usec_per_call=65.00
cmdstat_eval:calls=796,usec=36950,usec_per_call=46.42
cmdstat_command:calls=796,usec=8578,usec_per_call=10.78
```



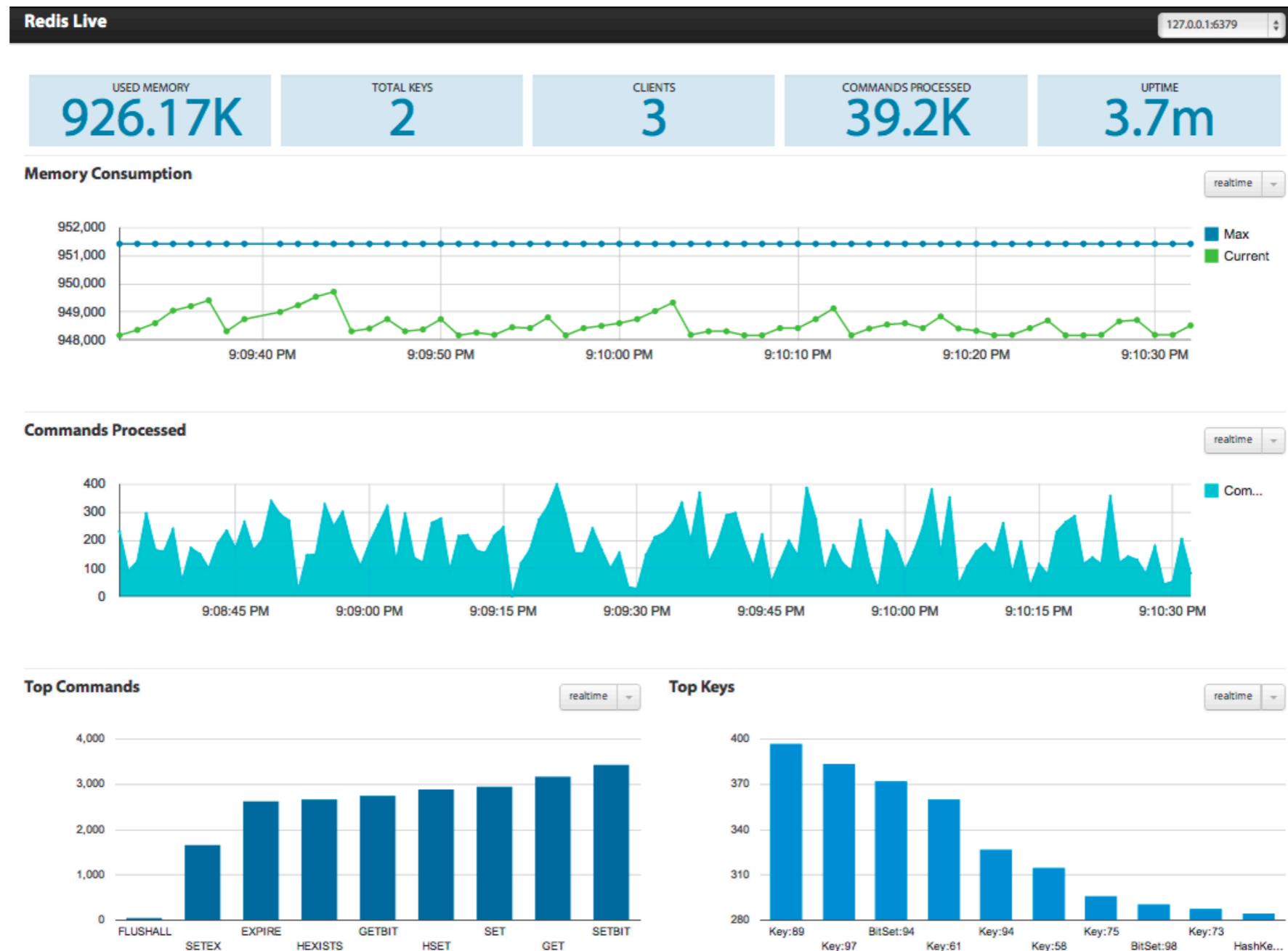
Redmon



<https://github.com/steelThread/redmon>



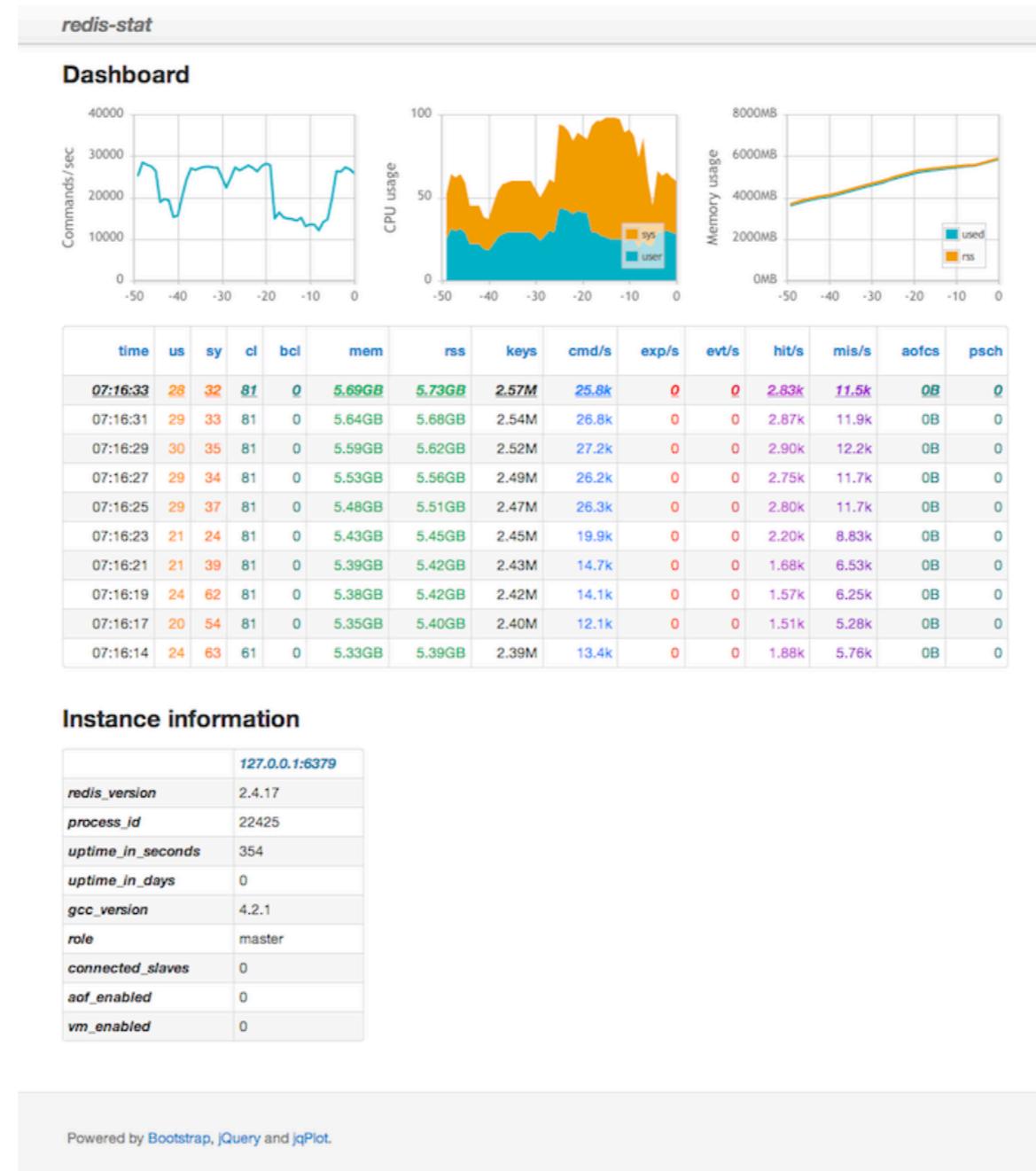
Redis Live



<https://github.com/nkrode/RedisLive>



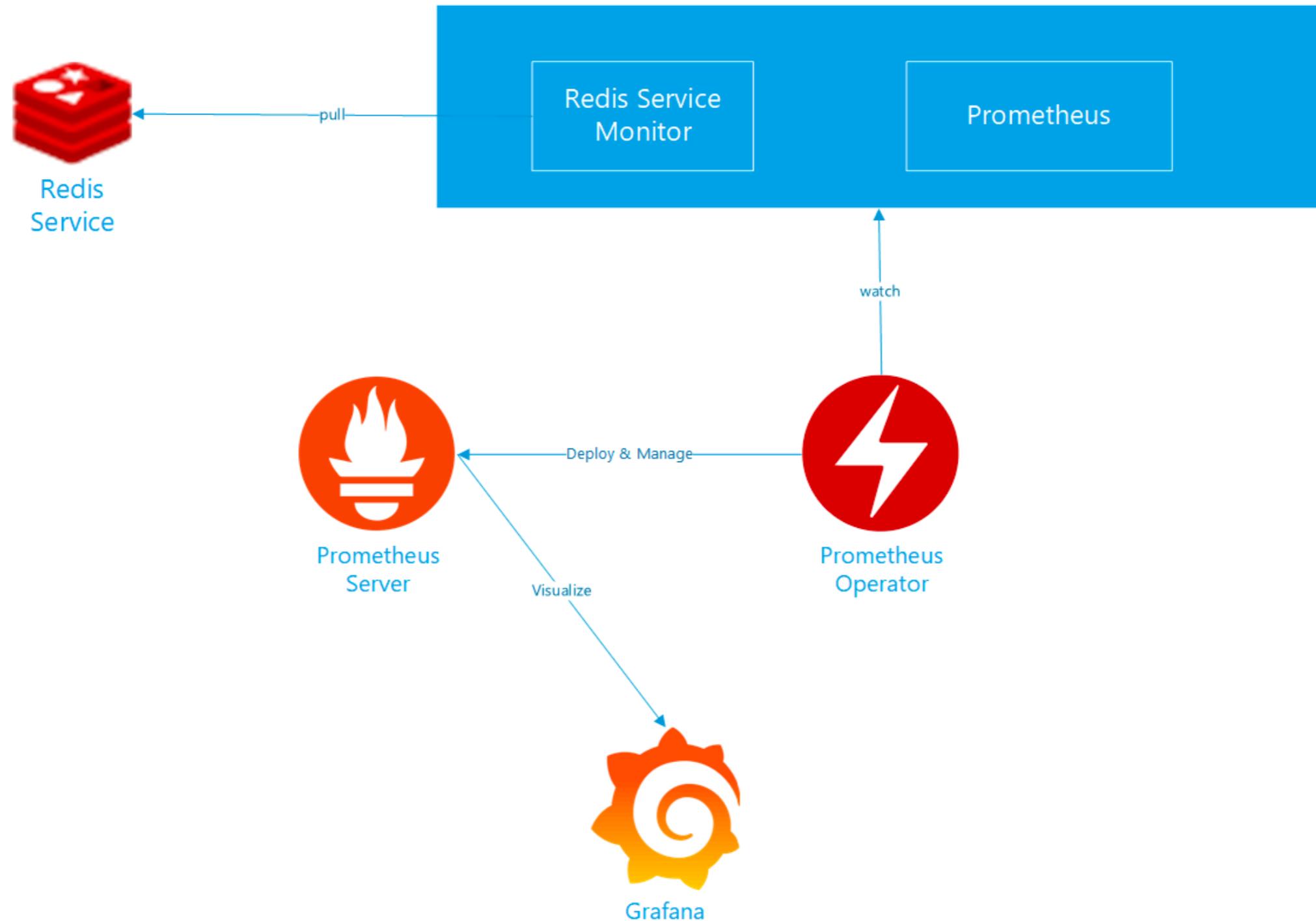
Redis-stat



<https://github.com/junegunn/redis-stat>



Workshop Redis Monitoring

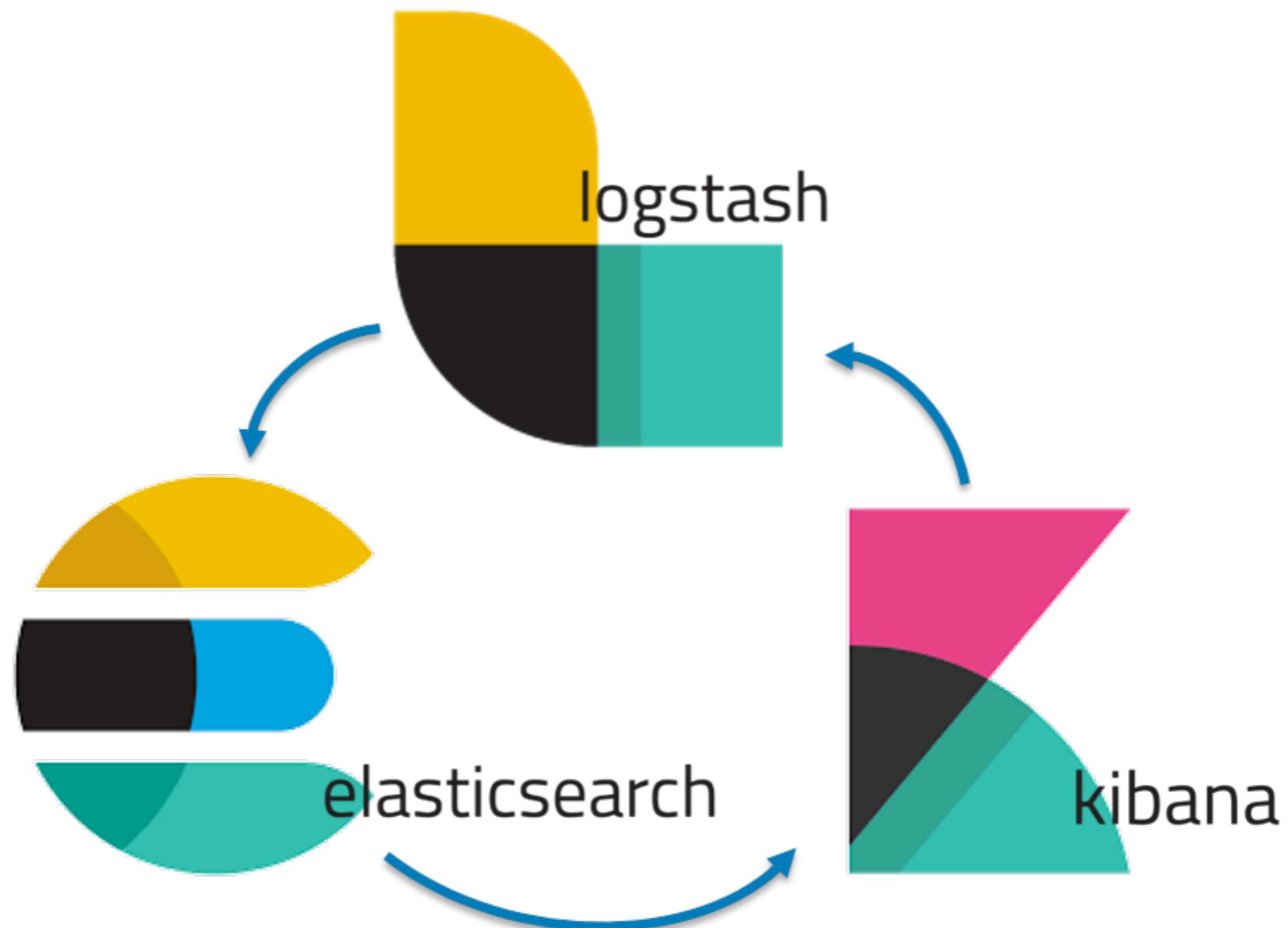


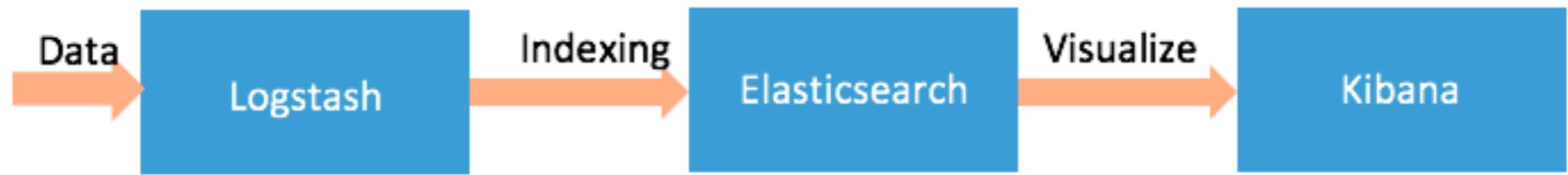
Workshop Redis Monitoring



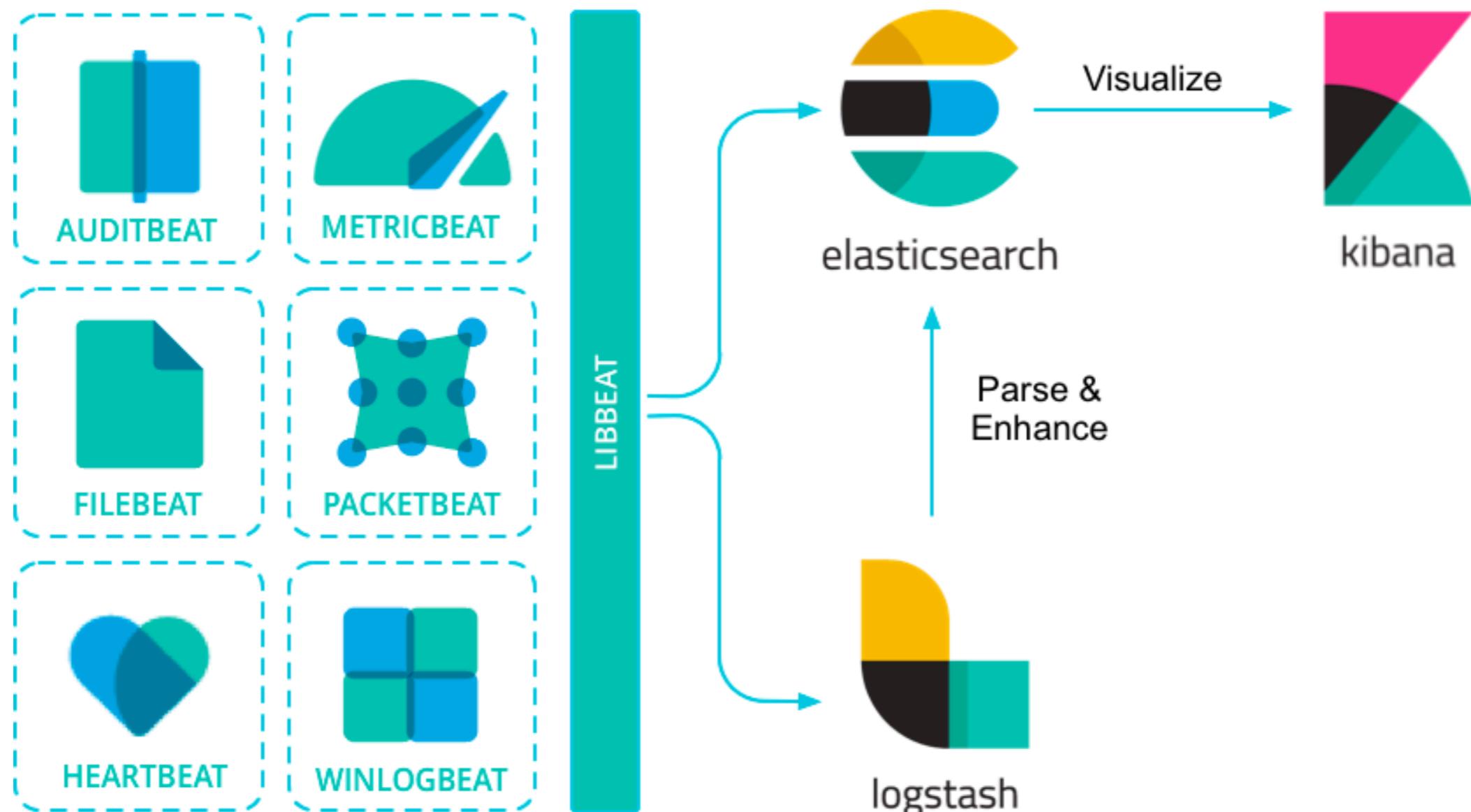
ELK stack







Beat



<https://www.elastic.co/guide/en/beats/libbeat/current/index.html>

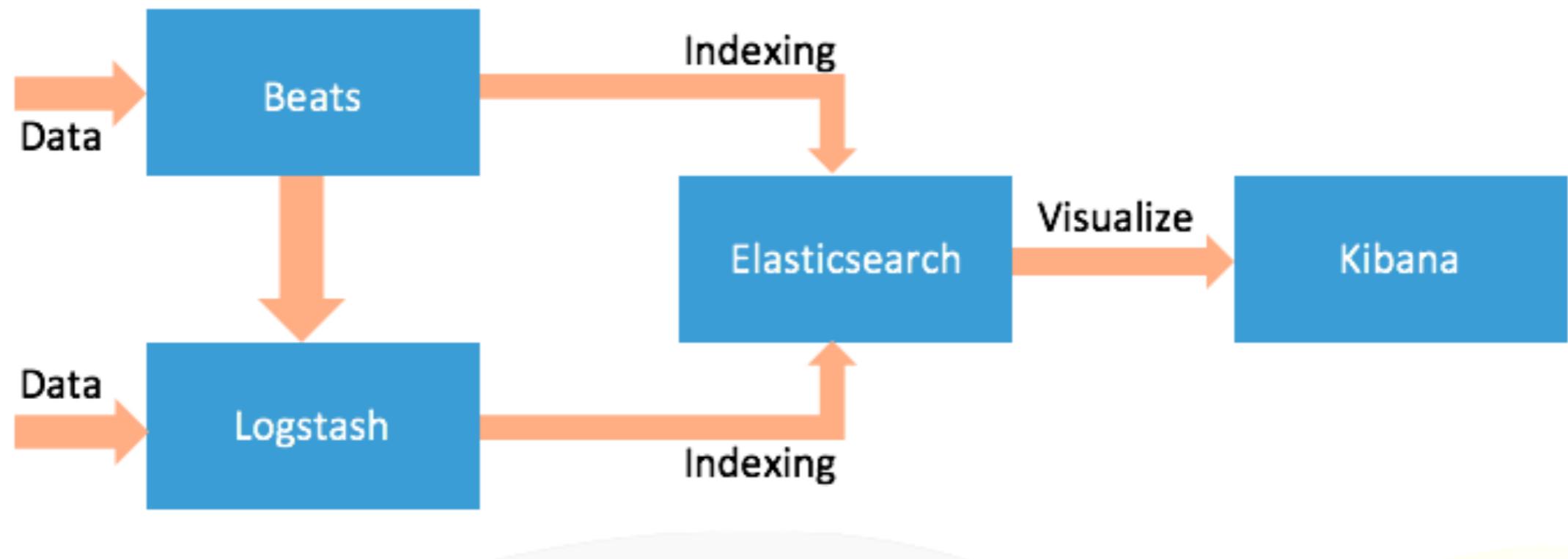


Beat

Purpose	Library
Audit data	Auditbeat
Log files	Filebeat
Cloud data	Functionbeat
Availability	Heartbeat
Metrics	Metricbeat
Network traffic	Packetbeat
Windows event logs	Winlogbeat



ELK stack



Elasticsearch ?



Elasticsearch

Search
Analytic
Real-time
Distributed



Distributed Search Engine

Open Source
Document-based
Based on Apache Lucene
JSON over HTTP



Document based

JSON (JavaScript Object Notation)

Dynamic Schema

Some relationship (nested, parent/child)



StackOverflow Question

```
{  
  "items": [  
    {  
      "owner": {  
        "reputation": 13,  
        "user_id": 9796344,  
        "user_type": "registered",  
        "profile_image": "",  
        "display_name": "Cherry",  
        "link": "https://stackoverflow.com/users/9796344/cherry"  
      },  
      "score": 0,  
      "last_activity_date": 1528986761,  
      "creation_date": 1528986761,  
      "post_type": "question",  
      "post_id": 50859951,  
      "link": "https://stackoverflow.com/q/50859951"  
    }  
  ],  
  "has_more": false,  
  "quota_max": 10000,  
  "quota_remaining": 9986  
}
```

<https://api.stackexchange.com/docs/posts-by-ids>



Database ranking

351 systems in ranking, August 2019

Rank			DBMS	Database Model	Score		
Aug 2019	Jul 2019	Aug 2018			Aug 2019	Jul 2019	Aug 2018
1.	1.	1.	Oracle 	Relational, Multi-model 	1339.48	+18.22	+27.45
2.	2.	2.	MySQL 	Relational, Multi-model 	1253.68	+24.16	+46.87
3.	3.	3.	Microsoft SQL Server 	Relational, Multi-model 	1093.18	+2.35	+20.53
4.	4.	4.	PostgreSQL 	Relational, Multi-model 	481.33	-1.94	+63.83
5.	5.	5.	MongoDB 	Document	404.57	-5.36	+53.59
6.	6.	6.	IBM Db2 	Relational, Multi-model 	172.95	-1.19	-8.89
7.	7.	8.	Elasticsearch 	Search engine, Multi-model 	149.08	+0.27	+10.97
8.	8.	7.	Redis 	Key-value, Multi-model 	144.08	-0.18	+5.51
9.	9.	9.	Microsoft Access	Relational	135.33	-1.98	+6.24
10.	10.	10.	Cassandra 	Wide column	125.21	-1.80	+5.63

<https://db-engines.com/en/ranking>



Installation

Elasticsearch
Kibana



Elasticsearch

Required Java 8

JDK 1.8.0_131+

Need \$JAVA_HOME



Start Elasticsearch

./bin/elasticsearch

```
[0g8-71W] loaded module [reindex]
[0g8-71W] loaded module [repository-url]
[0g8-71W] loaded module [transport-netty4]
[0g8-71W] loaded module [tribe]
[0g8-71W] no plugins loaded
[0g8-71W] using discovery type [zen]
initialized
[0g8-71W] starting ...
[0g8-71W] publish_address {127.0.0.1:9300},
[0g8-71W] recovered [0] indices into cluster_state
transport] [0g8-71W] publish_address {127.0.0.1:9200},
```



Default of Memory

1 GB !!! (Java need more memory)

```
 ] [DW5j42N] JVM arguments [-Xms1g, -Xmx1g, -  
ction=75, -XX:+UseCMSInitiatingOccupancyOnly, -XX:  
Dfile.encoding=UTF-8, -Djna.nosys=true, -XX:-Omit  
.netty.noKeySetOptimization=true, -Dio.netty.recy  
led=false, -Dlog4j2.disable.jmx=true, -Djava.io.t  
T/elasticsearch.G4kbTLZn, -XX:+HeapDumpOnOutOfMem  
s_err_pid%p.log, -Xlog:gc*,gc+age=trace,safepoint  
ize=64m, -Djava.locale.providers=COMPAT, -XX:UseA
```



Config of JVM

`$ES_HOME/config/jvm.options`

```
# Xms represents the initial size of total heap space  
# Xmx represents the maximum size of total heap space  
  
-Xms1g  
-Xmx1g
```



Default plugins

```
[o.e.p.PluginsService      ] [DW5j42N] loaded module [aggs-matrix-stats]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [analysis-common]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [ingest-common]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [lang-expression]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [lang-mustache]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [lang-painless]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [mapper-extras]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [parent-join]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [percolator]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [rank-eval]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [reindex]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [repository-url]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [transport-netty4]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [tribe]
```



Install X-Pack by default

```
[o.e.p.PluginsService      ] [DW5j42N] loaded module [x-pack-core]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [x-pack-deprecation]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [x-pack-graph]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [x-pack-logstash]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [x-pack-ml]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [x-pack-monitoring]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [x-pack-rollup]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [x-pack-security]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [x-pack-sql]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [x-pack-upgrade]
[o.e.p.PluginsService      ] [DW5j42N] loaded module [x-pack-watcher]
[o.e.p.PluginsService      ] [DW5j42N] no plugins loaded
```

<https://www.elastic.co/guide/en/elasticsearch/reference/current/installing-xpack-es.html>



X-Pack ?

Elastic Stack Extension
Security
Monitoring
Alerting
Reporting
Machine Learning



Hello Elasticsearch

<http://localhost:9200/>

```
{  
  "name": "DW5j42N",  
  "cluster_name": "elasticsearch",  
  "cluster_uuid": "boIZeF6MSHyxZ2owIG66rg",  
  "version": {  
    "number": "6.4.2",  
    "build_flavor": "default",  
    "build_type": "tar",  
    "build_hash": "04711c2",  
    "build_date": "2018-09-26T13:34:09.098244Z",  
    "build_snapshot": false,  
    "lucene_version": "7.4.0",  
    "minimum_wire_compatibility_version": "5.6.0",  
    "minimum_index_compatibility_version": "5.0.0"  
  },  
  "tagline": "You Know, for Search"  
}
```



```
{  
  name: "19f9aJW",  
  cluster_name: "elasticsearch",  
  cluster_uuid: "jGPzn4phQOWck81uuGDUNQ",  
  - version: {  
      number: "6.5.4",  
      build_flavor: "default",  
      build_type: "tar",  
      build_hash: "d2ef93d",  
      build_date: "2018-12-17T21:17:40.758843Z",  
      build_snapshot: false,  
      lucene_version: "7.5.0",  
      minimum_wire_compatibility_version: "5.6.0",  
      minimum_index_compatibility_version: "5.0.0"  
    },  
  tagline: "You Know, for Search"  
}
```



Name of node and cluster

```
{  
  name: "19f9aJW",  
  cluster_name: "elasticsearch",  
  cluster_uuid: "jGPzn4phQOWck81uuGDUNQ",  
  - version: {  
      number: "6.5.4",  
      build_flavor: "default",  
      build_type: "tar",  
      build_hash: "d2ef93d",  
      build_date: "2018-12-17T21:17:40.758843Z",  
      build_snapshot: false,  
      lucene_version: "7.5.0",  
      minimum_wire_compatibility_version: "5.6.0",  
      minimum_index_compatibility_version: "5.0.0"  
    },  
  tagline: "You Know, for Search"  
}
```



Name of node and cluster

\$ES_HOME/config/elasticsearch.yml

```
# ----- Cluster -----  
#  
# Use a descriptive name for your cluster:  
#  
cluster.name: my-application  
#  
# ----- Node -----  
#  
# Use a descriptive name for the node:  
#  
node.name: node-1  
#  
# Add custom attributes to the node:  
#  
#node.attr.rack: r1  
#
```



Change in Elasticsearch 7.x

Default name = Hostname

<https://www.elastic.co/guide/en/elasticsearch/reference/master/breaking-changes-7.0.html>



Try to change and restart !!!



```
{  
  name: "19f9aJW",  
  cluster_name: "elasticsearch",  
  cluster_uuid: "jGPzn4phQOWck81uuGDUNQ",  
  - version: {  
      number: "6.5.4",  
      build_flavor: "default",  
      build_type: "tar",  
      build_hash: "d2ef93d",  
      build_date: "2018-12-17T21:17:40.758843Z",  
      build_snapshot: false,  
      lucene_version: "7.5.0",  
      minimum_wire_compatibility_version: "5.6.0",  
      minimum_index_compatibility_version: "5.0.0"  
    },  
  tagline: "You Know, for Search"  
}
```



Apache Lucene

The screenshot shows the official Apache Lucene website. At the top, there's a navigation bar with a search bar containing "Search with Apache So" and a dropdown menu "select provider". Below the search bar are three tabs: "CORE (JAVA)", "SOLR", and "PYLUCENE". The main content area features the Apache Lucene logo (a green feather) on the left and the Solr logo (a red sunburst icon next to the word "Solr") on the right. A large green banner in the center reads "Ultra-fast Search Library and Server". Below this banner, a dark grey box contains the text "Apache Lucene and Solr set the standard for search and indexing performance". In the middle section, there's a heading "Welcome to Apache Lucene" followed by a paragraph about the project's goals and a list of sub-projects. To the right of this text are two large download buttons: a green one for "Apache Lucene 7.5.0" and an orange one for "Apache Solr 7.5.0". At the bottom right of this section is a link labeled "Projects".

Apache Lucene™ is a Java-based search library and server.

Apache Lucene and Solr set the standard for search and indexing performance.

Welcome to Apache Lucene

The Apache Lucene™ project develops open-source search software, including:

- [Lucene Core](#), our flagship sub-project, provides Java-based indexing and search technology, as well as spellchecking, hit highlighting and advanced analysis/tokenization capabilities.
- [Solr™](#) is a high performance search server built using Lucene Core, with XML/HTTP and JSON/Python/Ruby APIs, hit highlighting, faceted search, caching, replication, and a web admin interface.
- [PyLucene](#) is a Python port of the Core project.

[DOWNLOAD](#)

Apache Lucene 7.5.0

[DOWNLOAD](#)

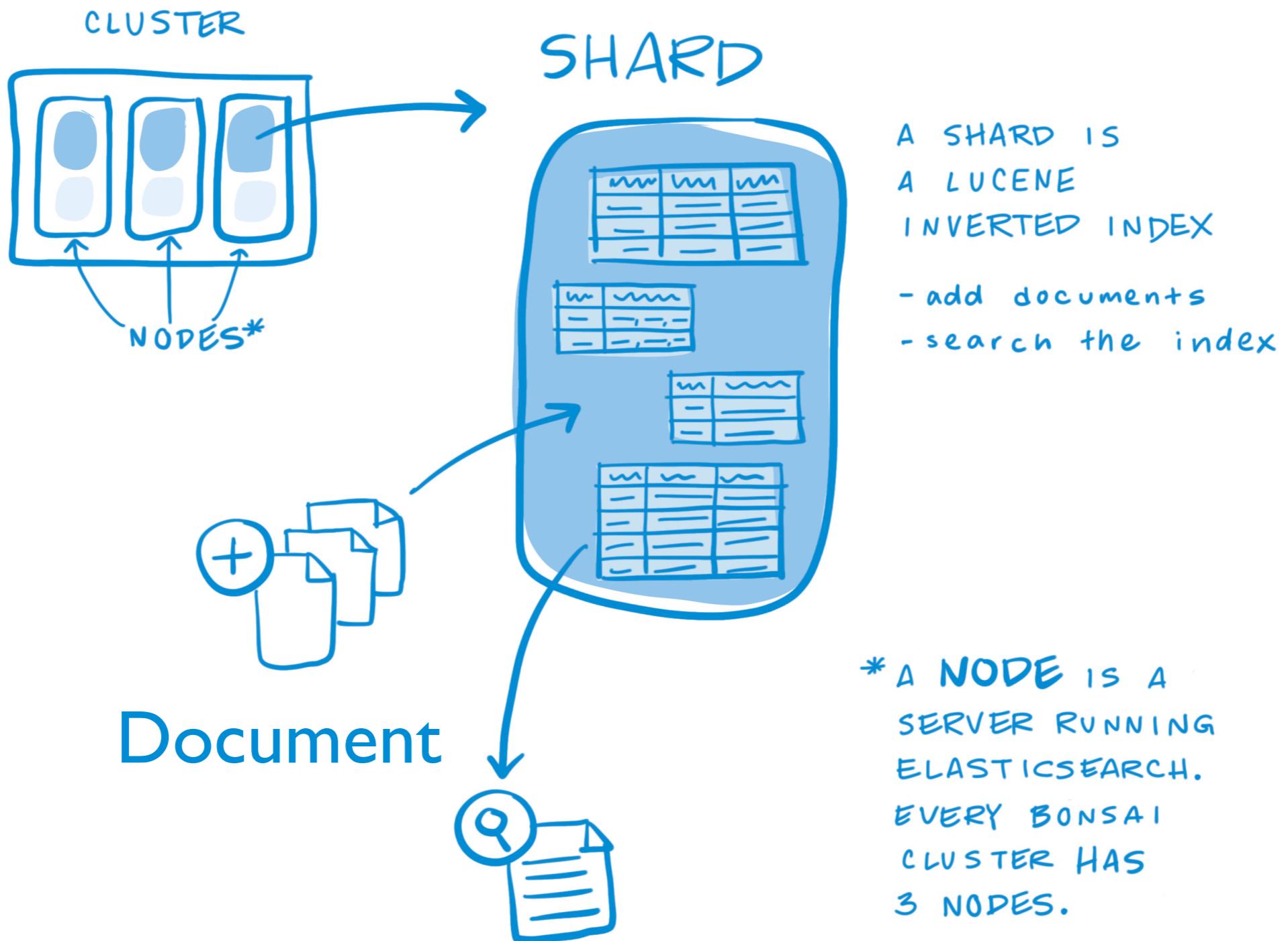
Apache Solr 7.5.0

[Projects](#)

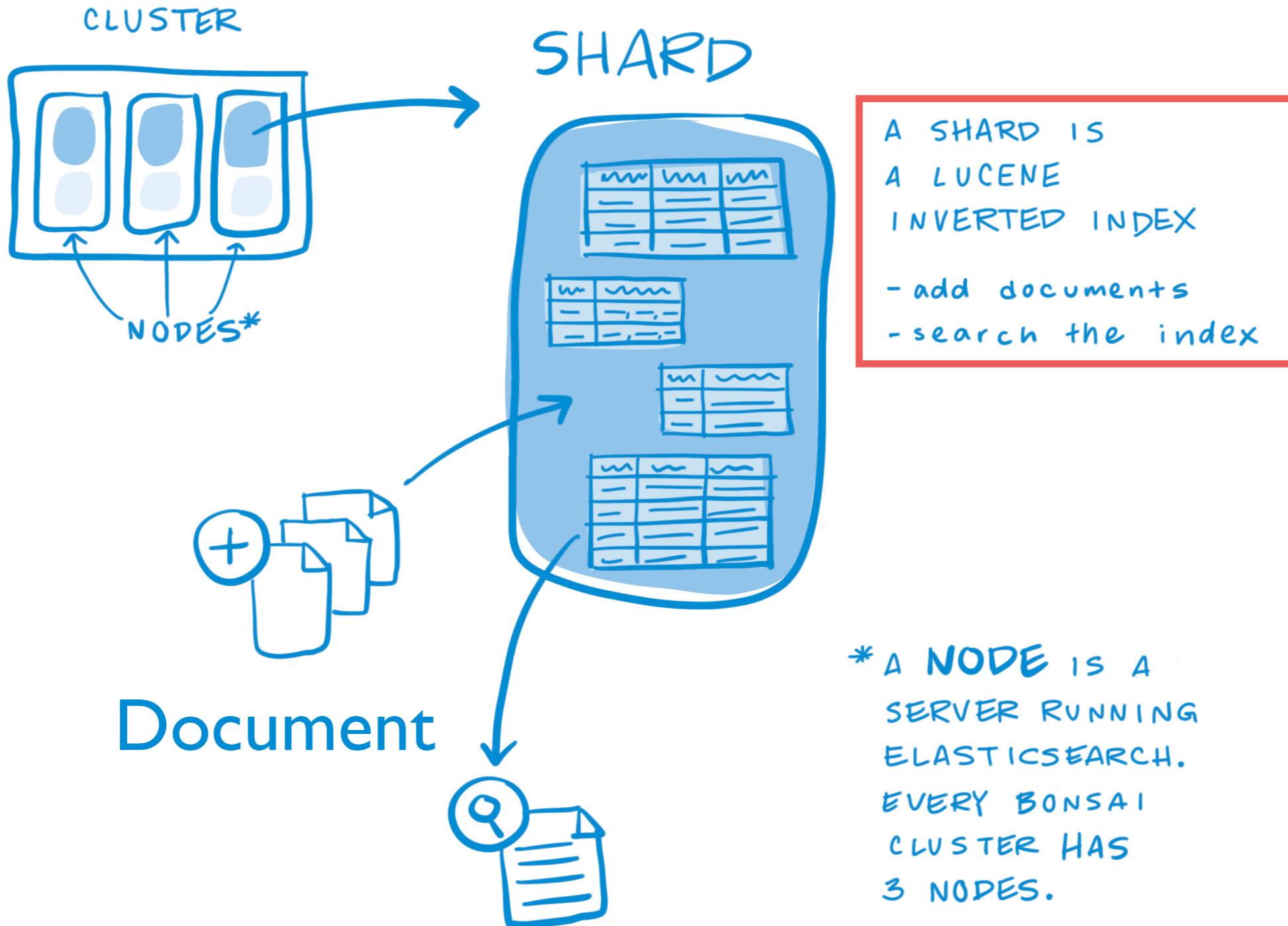
<http://lucene.apache.org/>



Basic concepts

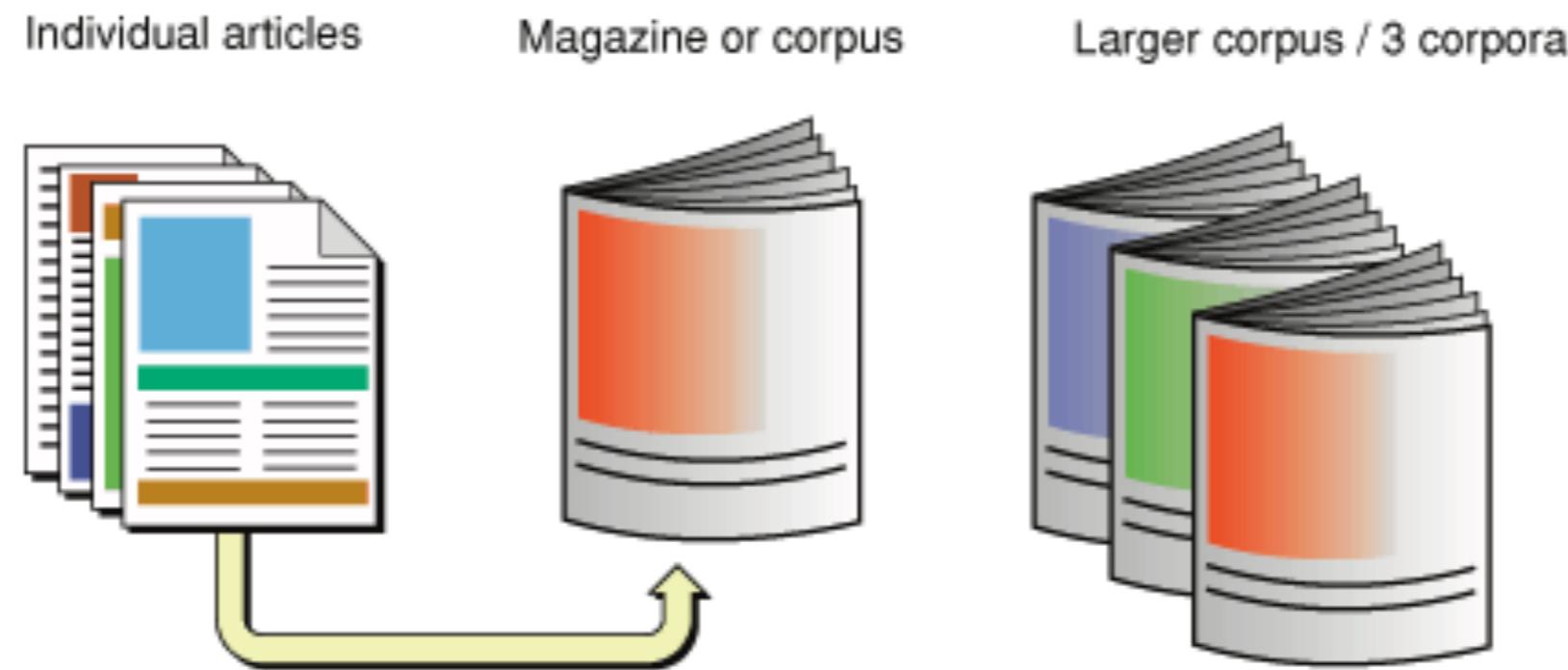


Basic concepts



Inverted Index

Corpus is a collection of documents

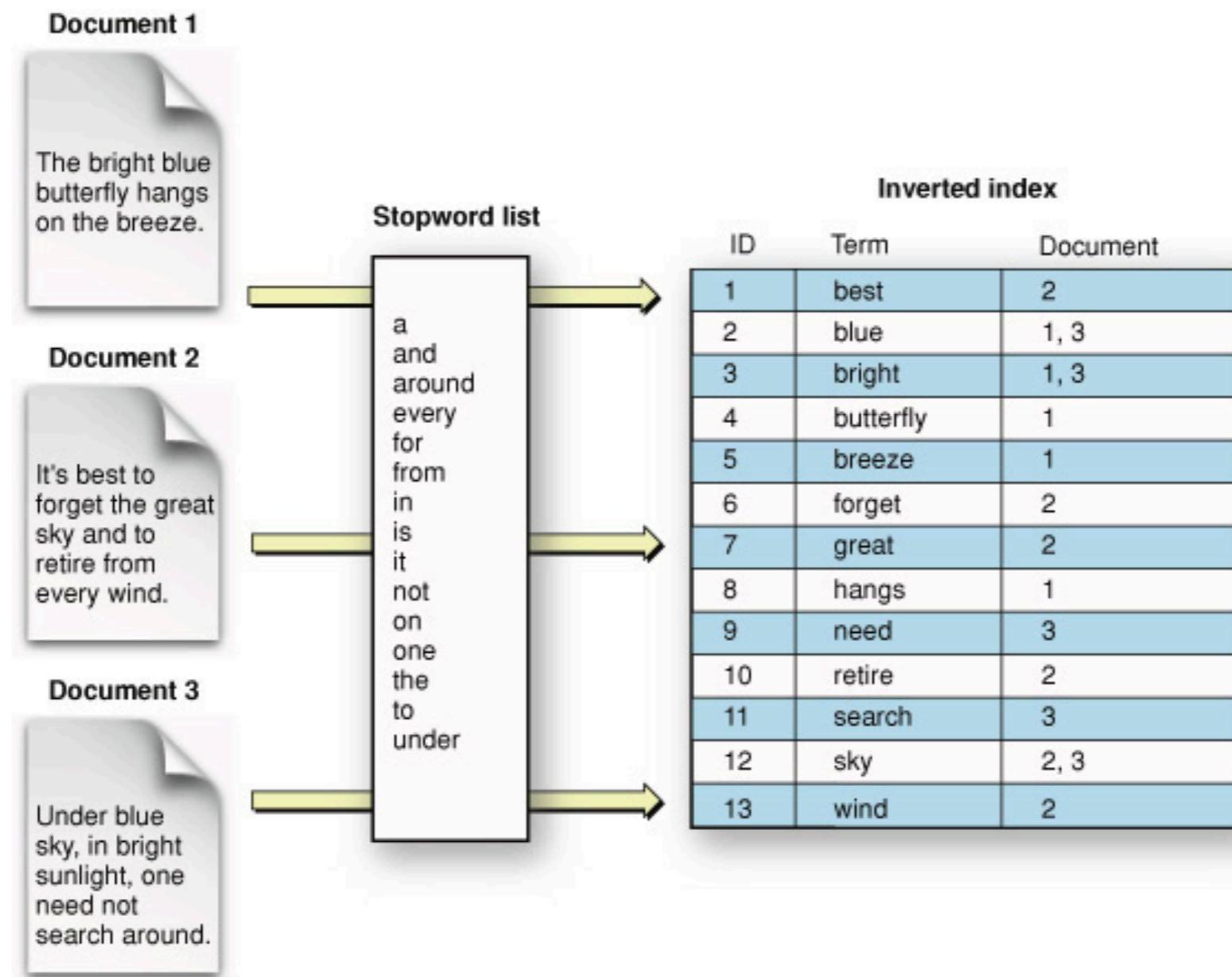


https://developer.apple.com/library/archive/documentation/UserExperience/Conceptual/SearchKitConcepts/searchKit_basics/searchKit_basics.html#/apple_ref/doc/uid/TP40002843-TPXREF101

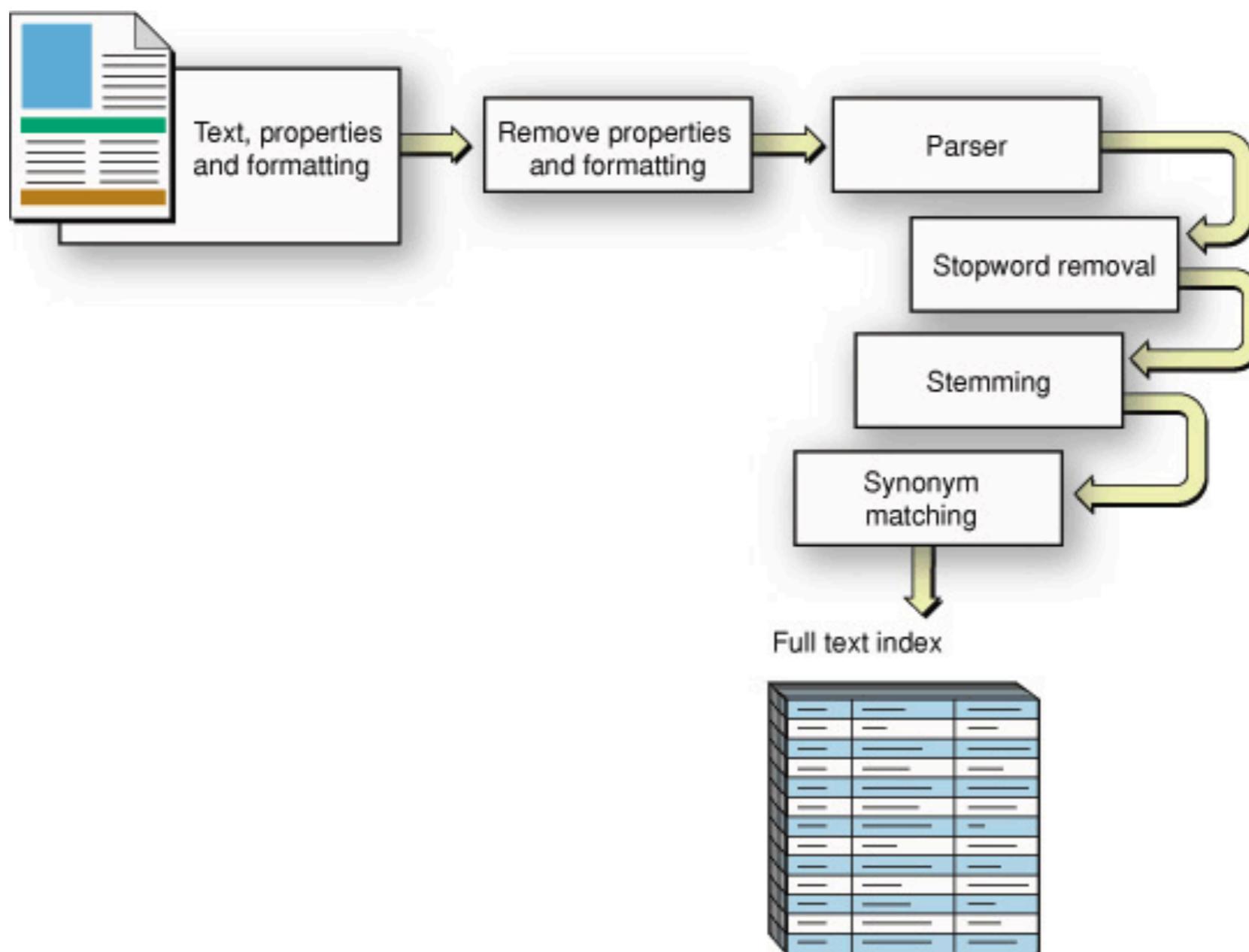


Inverted Index

Try to construct index



Text extraction



```
{  
  name: "19f9aJW",  
  cluster_name: "elasticsearch",  
  cluster_uuid: "jGPzn4phQOWck81uuGDUNQ",  
  - version: {  
      number: "6.5.4",  
      build_flavor: "default",  
      build_type: "tar",  
      build_hash: "d2ef93d",  
      build_date: "2018-12-17T21:17:40.758843Z",  
      build_snapshot: false,  
      lucene_version: "7.5.0", DSL version  
      minimum_wire_compatibility_version: "5.6.0",  
      minimum_index_compatibility_version: "5.0.0"  
    },  
  tagline: "You Know, for Search" Index version  
}
```

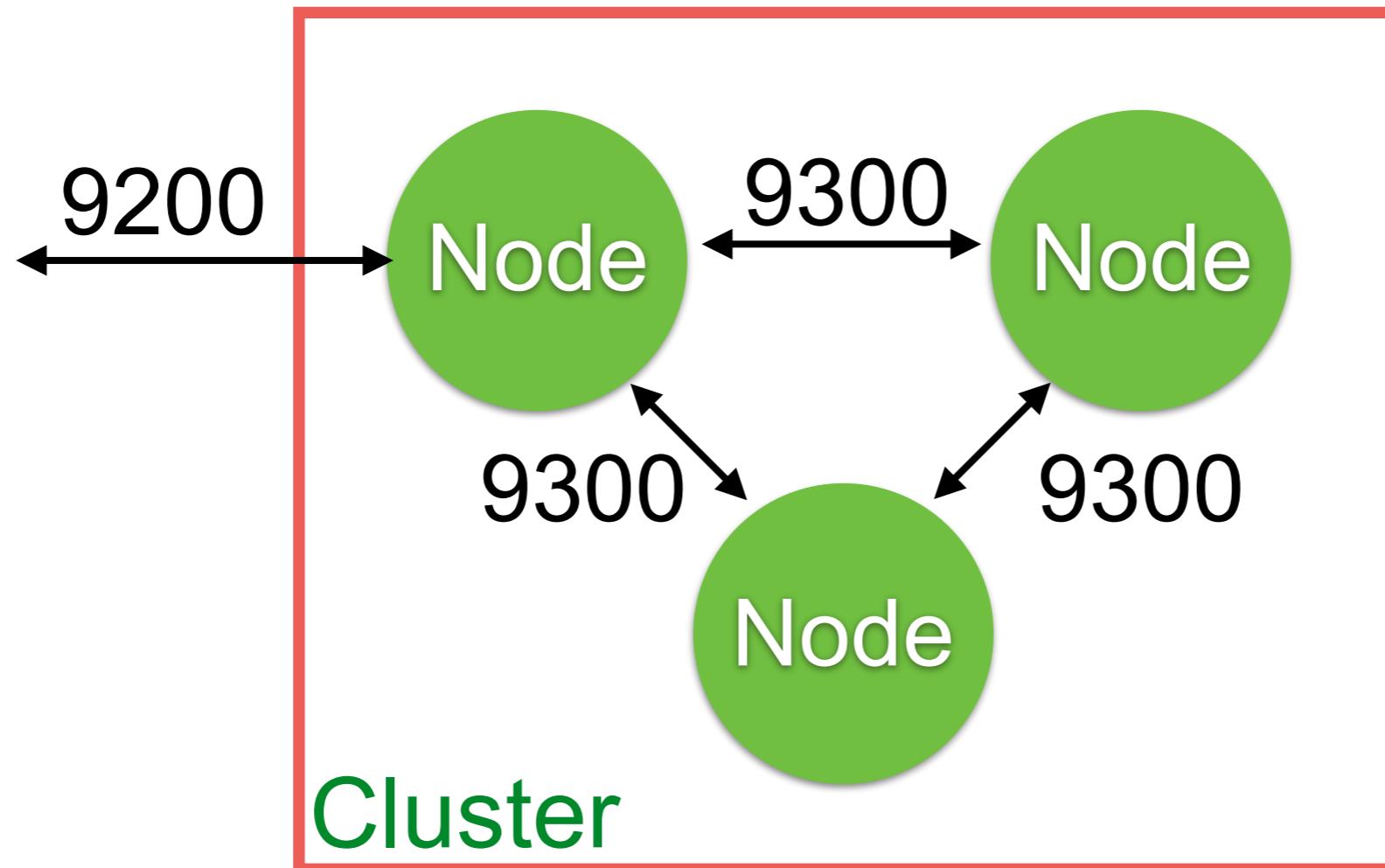


```
{  
  name: "19f9aJW",  
  cluster_name: "elasticsearch",  
  cluster_uuid: "jGPzn4phQOWck81uuGDUNQ",  
  - version: {  
      number: "6.5.4",  
      build_flavor: "default",  
      build_type: "tar",  
      build_hash: "d2ef93d",  
      build_date: "2018-12-17T21:17:40.758843Z",  
      build_snapshot: false,  
      lucene_version: "7.5.0",  
      minimum_wire_compatibility_version: "5.6.0",  
      minimum_index_compatibility_version: "5.0.0"  
    },  
  tagline: "You Know, for Search" Index version  
}
```



Ports of Elasticsearch

RESTful API with JSON Over HTTP (9200)
Java API (9300)



Health of cluster

http://localhost:9200/_cluster/health

```
{  
  "cluster_name": "elasticsearch",  
  "status": "green",  
  "timed_out": false,  
  "number_of_nodes": 1,  
  "number_of_data_nodes": 1,  
  "active_primary_shards": 0,  
  "active_shards": 0,  
  "relocating_shards": 0,  
  "initializing_shards": 0,  
  "unassigned_shards": 0,  
  "delayed_unassigned_shards": 0,  
  "number_of_pending_tasks": 0,  
  "number_of_in_flight_fetch": 0,  
  "task_max_waiting_in_queue_millis": 0,  
  "active_shards_percent_as_number": 100.0  
}
```



Health of cluster

Status	Meaning
Green	All shards are allocated
Yellow	Primary shard is allocated, but replicas are not
Red	Shard not allocated in the cluster



cat APIs

`http://localhost:9200/_cat`

```
=^.^=
/_cat/allocation
/_cat/shards
/_cat/shards/{index}
/_cat/master
/_cat/nodes
/_cat/tasks
/_cat/indices
/_cat/indices/{index}
/_cat/segments
/_cat/segments/{index}
/_cat/count
/_cat/count/{index}
/_cat/recovery
/_cat/recovery/{index}
/_cat/health
/_cat/pending_tasks
/_cat/aliases
/_cat/aliases/{alias}
```

<https://www.elastic.co/guide/en/elasticsearch/reference/current/cat.html>



cat APIs

`http://localhost:9200/_cat/nodes?v`

ip	heap.percent	ram.percent	cpu	load_1m	load_5m	load_15m	node.role	master	name
127.0.0.1	20	100	7	1.98			mdi	*	DW5j42N



Start Kibana

```
[status][plugin:xpack_main@6.4.2] Status changed from yellow to green - Ready
[status][plugin:searchprofiler@6.4.2] Status changed from yellow to green - Ready
[status][plugin:ml@6.4.2] Status changed from yellow to green - Ready
[status][plugin:tilemap@6.4.2] Status changed from yellow to green - Ready
[status][plugin:watcher@6.4.2] Status changed from yellow to green - Ready
[status][plugin:index_management@6.4.2] Status changed from yellow to green - Ready

[status][plugin:graph@6.4.2] Status changed from yellow to green - Ready
[status][plugin:grokdebugger@6.4.2] Status changed from yellow to green - Ready
[status][plugin:logstash@6.4.2] Status changed from yellow to green - Ready
[status][plugin:reporting@6.4.2] Status changed from yellow to green - Ready
[kibana-monitoring][monitoring-ui] Starting monitoring stats collection
[status][plugin:security@6.4.2] Status changed from yellow to green - Ready
[license][xpack] Imported license information from Elasticsearch for the [monitor]
tatus: active
[listening][server][http] Server running at http://localhost:5601
```



Hello Kibana

<http://localhost:5601/>

The image shows the Kibana landing page. On the left is a vertical sidebar with icons for Kibana, APM, Metrics, Security, Visualize, Discover, and Admin. The main content area has two main sections: "Add Data to Kibana" and "Visualize and Explore Data".

Add Data to Kibana:

- APM:** APM automatically collects in-depth performance metrics and errors from inside your applications. [Add APM](#)
- Logging:** Ingest logs from popular data sources and easily visualize in preconfigured dashboards. [Add log data](#)
- Metrics:** Collect metrics from the operating system and services running on your servers. [Add metric data](#)
- Security analytics:** Centralize security events for interactive investigation in ready-to-go visualizations. [Add security events](#)

Data already in Elasticsearch? [Set up index patterns](#)

Visualize and Explore Data:

- Dashboard:** Display and share a collection of visualizations and saved searches.
- Timelion:** Use an expression language to analyze time series data.
- Discover:** Interactively explore your data by querying and filtering raw documents.
- Visualize:** Create visualizations and aggregate data stores in your

Manage and Administer the Elastic Stack:

- Console:** Skip cURL and use this JSON interface to work with your data directly.
- Index Patterns:** Manage the index patterns that help retrieve your data from Elasticsearch.
- Saved Objects:** Import, export, and manage your saved searches,



Using Dev Tools

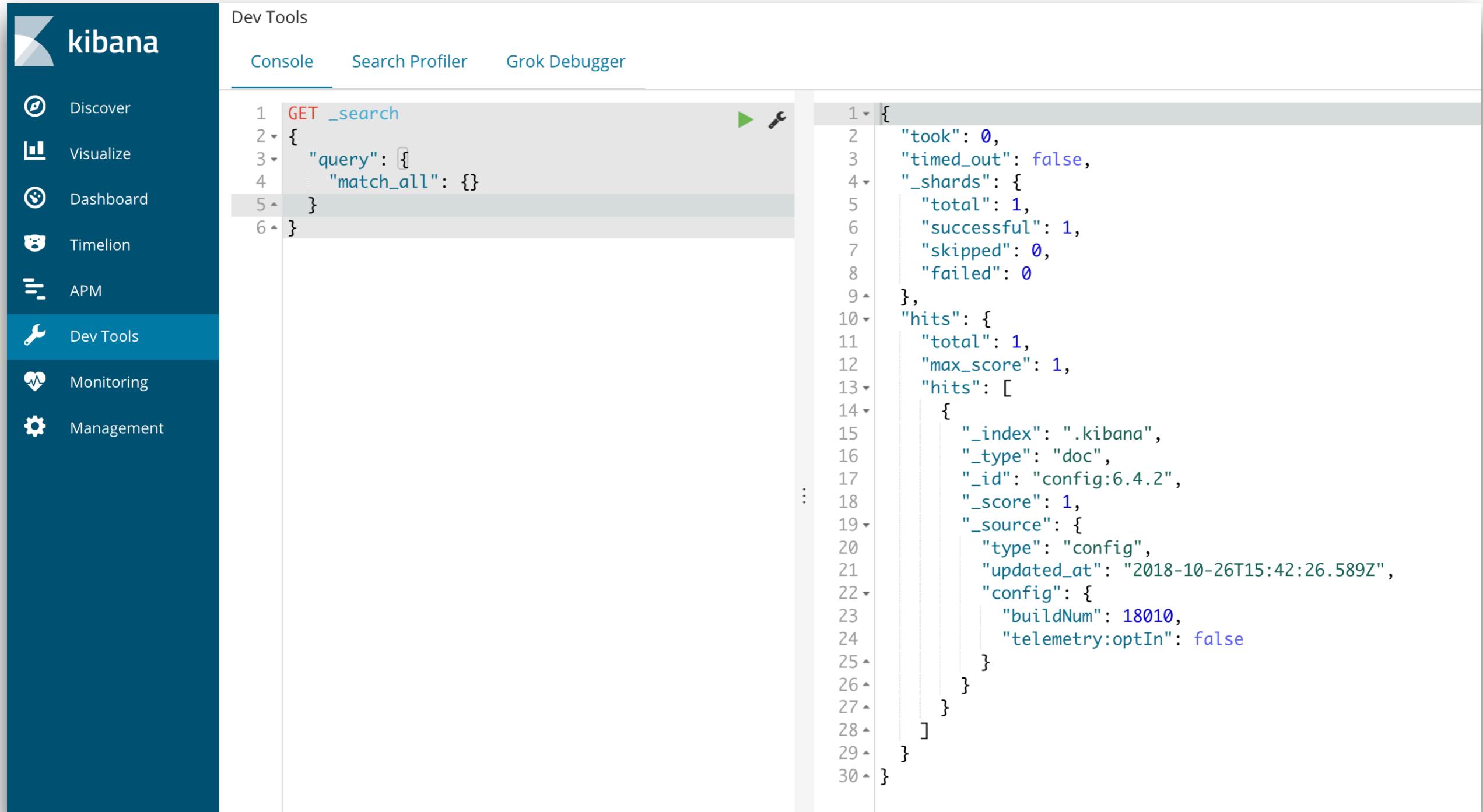
The screenshot shows the Kibana interface with a sidebar on the left containing various navigation items: Discover, Visualize, Dashboard, Timelion, APM, Dev Tools (which is highlighted with a red box), Monitoring, and Management. The main content area is titled "Dev Tools" and "Welcome to Console". It includes a "Quick intro to the UI" section with text about the split editor and response panes, and a code editor pane showing a cURL request example:

```
1 # index a doc
2 PUT index/type/1
3 {
4   "body": "here"
5 }
6
7 # and get it ...
8 GET index/type/1
```

Below the code editor, there is a note about request suggestions and a section titled "A few quick tips, while I have your attention" with a bulleted list of tips. At the bottom of the content area is a blue button labeled "Get to work".



Ready to start



The screenshot shows the Kibana Dev Tools interface. On the left is a sidebar with icons for Discover, Visualize, Dashboard, Timelion, APM, Dev Tools (which is selected), Monitoring, and Management. The main area is titled "Dev Tools" and contains three tabs: Console, Search Profiler, and Grok Debugger. The "Console" tab is active, displaying a code editor with a GET _search request and its JSON response. The request is as follows:

```
1 GET _search
2 {
3   "query": {
4     "match_all": {}
5   }
6 }
```

The response is as follows:

```
1 {
2   "took": 0,
3   "timed_out": false,
4   "_shards": {
5     "total": 1,
6     "successful": 1,
7     "skipped": 0,
8     "failed": 0
9   },
10  "hits": {
11    "total": 1,
12    "max_score": 1,
13    "hits": [
14      {
15        "_index": ".kibana",
16        "_type": "doc",
17        "_id": "config:6.4.2",
18        "_score": 1,
19        "_source": {
20          "type": "config",
21          "updated_at": "2018-10-26T15:42:26.589Z",
22          "config": {
23            "buildNum": 18010,
24            "telemetry:optIn": false
25          }
26        }
27      }
28    ]
29  }
30 }
```



CRUD with Elasticsearch

02-crud/book_document.json



CRUD with Elasticsearch

Create document

Read document

Update document

Delete document



Create a document

PUT /store/book/1

```
{  
  "title": "Elasticsearch: The Definitive Guide",  
  "author_name": [  
    "Clinton Gormley",  
    "Zachary Tong"  
,  
  "tag": [  
    "search",  
    "computer"  
,  
  "isbn-13": "978-1449358549",  
  "isbn-10": "1449358543",  
  "price": 44.3,  
  "page": 724,  
}
```



Create document

PUT **/store/book/1**

Index name

Type name

Document ID



Compare with RDBMS

Database

Table

Row

Column

Index

Type*

Document

Field

* Only 1 type per index



Change in Elasticsearch 7.x

of shard of index change from 5 to 1

#! Deprecation: the default number of shards will change from [5] to [1] in 7.0.0; if you wish to continue using the default of [5] shards, you must manage this on the create index request or with an index template

```
{  
  "_index": "store1",  
  "_type": "book",  
  "_id": "2",  
  "_version": 1,  
  "result": "created",  
  "_shards": {  
    "index": "store1",  
    "status": "CREATED",  
    "shards": 1,  
    "primary": true  
  }  
}
```



Read document

GET /store/book/1

```
{  
  "_index": "store",  
  "_type": "book",  
  "_id": "1",  
  "_version": 1,  
  "found": true,  
  "_source": {  
    "title": "Elasticsearch: The Definitive Guide",  
    "author_name": [  
      "Clinton Gormley",  
      "Zachary Tong"  
    ],  
    "tag": [  
      "search",  
      "computer"  
    ]  
  }  
}
```

Information of document



Update document

Whole document
Partial document



Update whole document

PUT /store/book/123

```
{  
  "title": "Update",  
  "author_name": [  
    "user1",  
    "user2"  
  ],  
  "tag": [  
    "update",  
    "book"  
  ]  
}
```



Update partial document

POST /store/book/123/_update

```
{  
  "doc": {  
    "title": "partial update",  
    "tag": [  
      "test",  
      "computer"  
    ],  
    "views": 0  
  }  
}
```



Delete document

DELETE /store/book/1

```
{  
  "_index": "store",  
  "_type": "book",  
  "_id": "1",  
  "_version": 2,  
  "result": "deleted",  
  "_shards": {  
    "total": 2,  
    "successful": 1,  
    "failed": 0  
  },  
  "_seq_no": 1,  
  "_primary_term": 1  
}
```



More features

Update by query

Delete by query

Partial update document



Bulk API

<https://www.elastic.co/guide/en/elasticsearch/reference/current/docs-bulk.html>



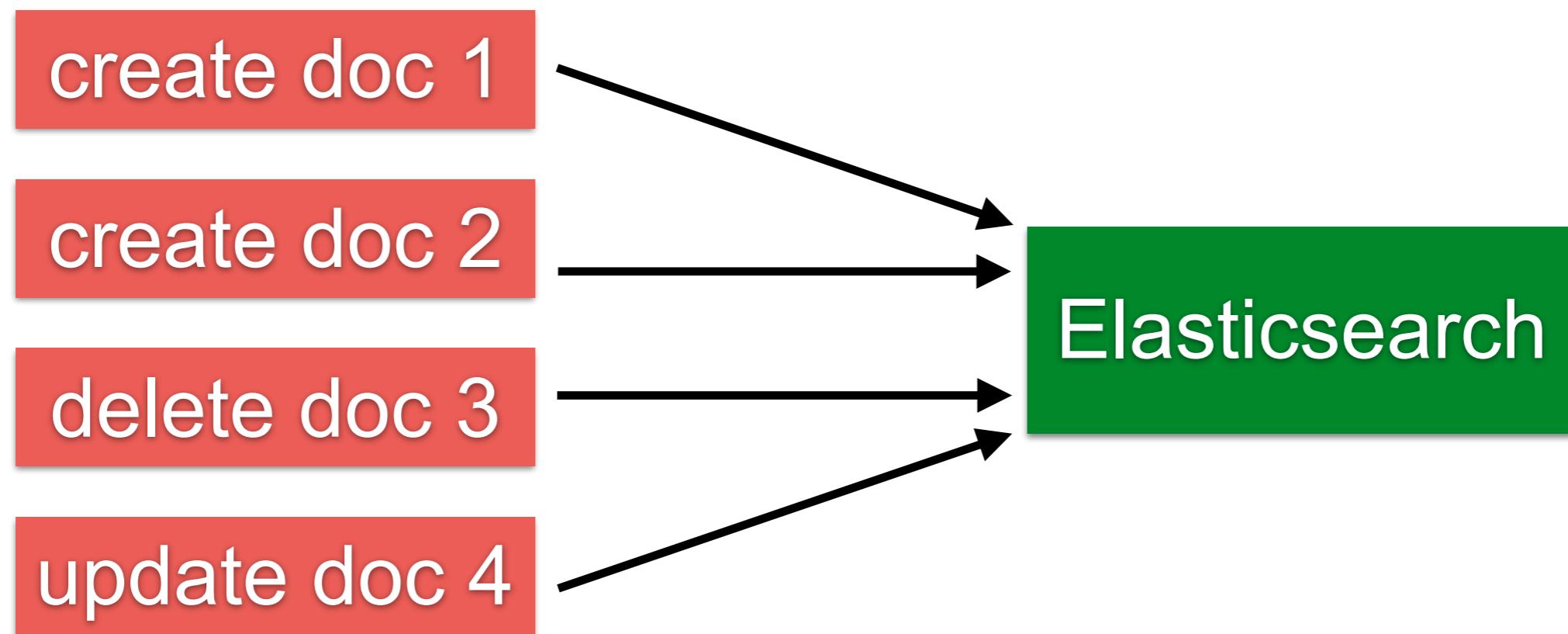
Bulk API

Perform many index/delete operation in single API call

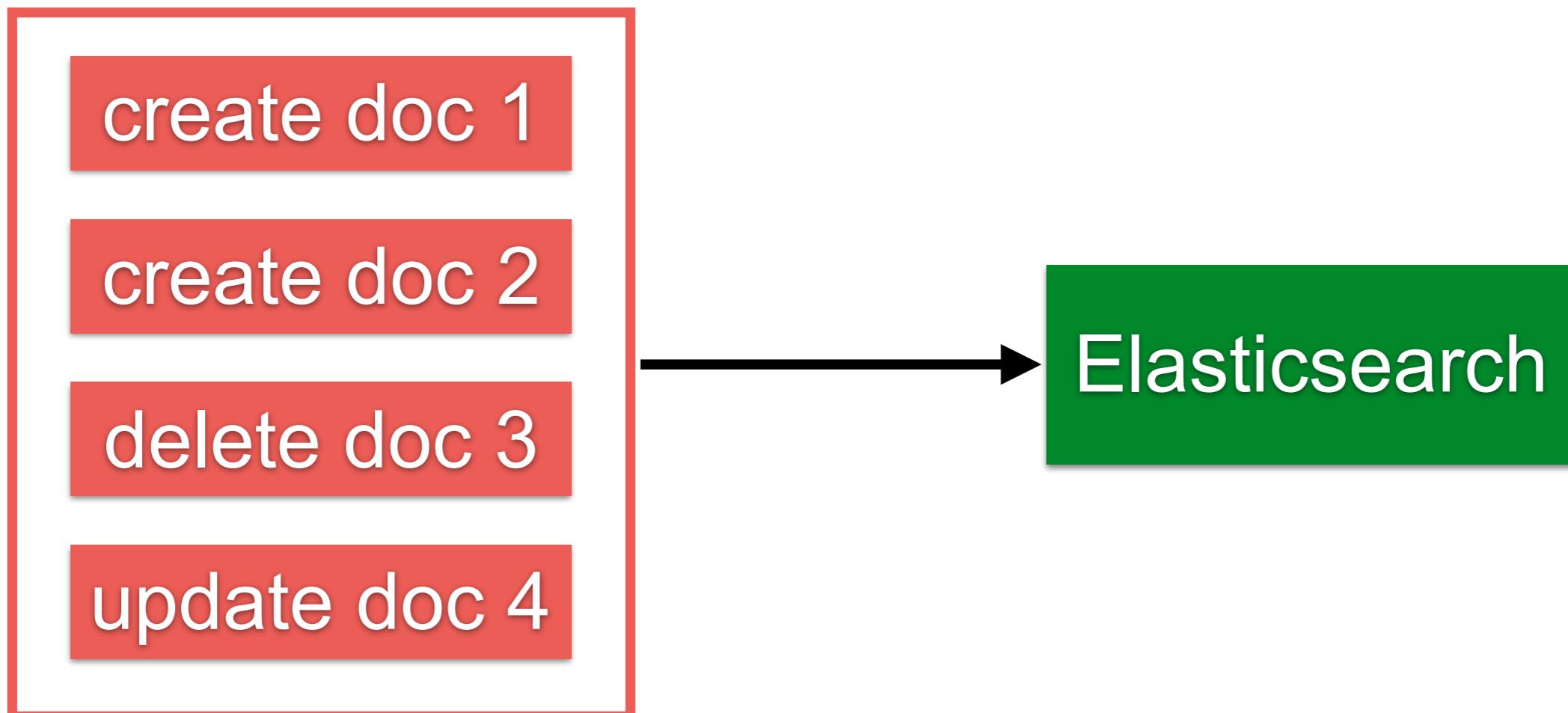
Increase indexing speed



Without Bulk API



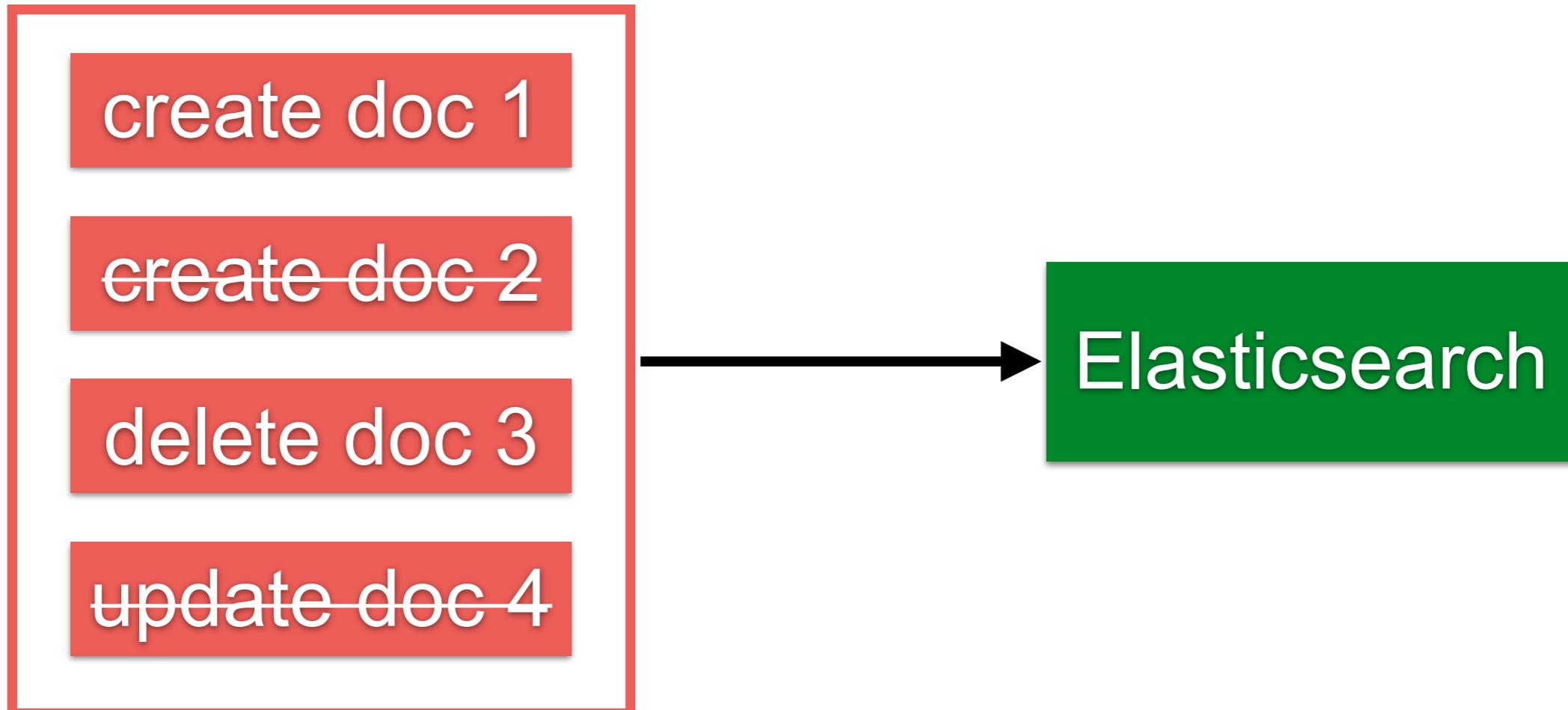
With Bulk API



Store in memory 5-15 MB



No transaction in bulk api



Create a document

POST /store/book/_bulk

```
{"create": {"_id": "1001"}  
{"title": "new book 1000", "description": "my new book"}}
```



Response from Bulk API

```
{  
  "took": 89,  
  "errors": false,  
  "items": [  
    {  
      "create": {  
        "_index": "store",  
        "_type": "book",  
        "_id": "1001",  
        "_version": 1,  
        "result": "created",  
        "_shards": {  
          "total": 2,  
          "successful": 1,  
          "failed": 0  
        },  
        "_seq_no": 0,  
        "_primary_term": 1,  
        "status": 201  
      }  
    }  
  ]  
}
```

Time in milliseconds

HTTP Status 201 = Created



Query DSL



Query DSL

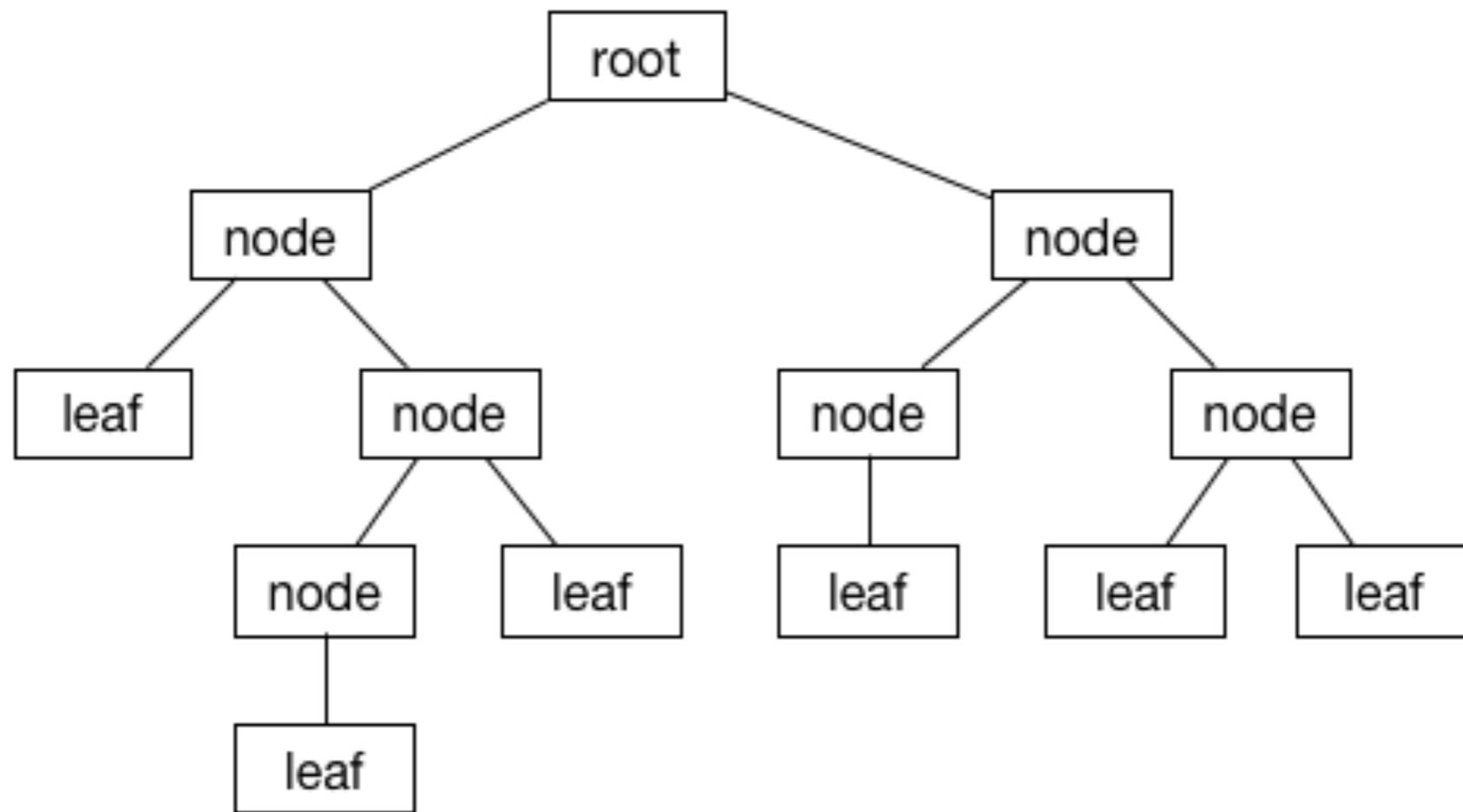
Domain Specific Language for query data
Flexible query language
Based on JSON format

<https://www.elastic.co/guide/en/elasticsearch/reference/current/query-dsl.html>



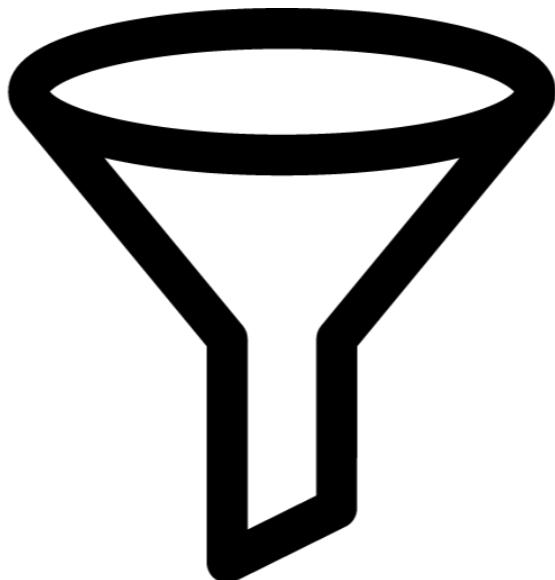
Query DSL

1. Leaf query clause
2. Compound query clause



Query DSL

Query (unstructured data)
Filter (structured data)



Query



Query DSL

Query	Filter
Relevance	Boolean, yes/no
Full text search	Exact values
Not cached	Cached
Slower	Faster

Filter first, then query remaining documents



Query DSL

Full text query
Term level query
Compound query
Joining query
Geo query
Specialized query
Span query



Leaf query clause

GET /store/book/_search

```
{  
  "query": {  
    "match_all": {}  
  }  
}
```



Compound query clause

GET /store/book/_search

```
{  
  "query": {  
    "bool": {  
      "must": [{}],  
      "should": [{}],  
      "must_not": [{}]  
    }  
  }  
}
```



Use case

amazon

All ▾ elasticsearch

New to Amazon? Click here to learn more

Deliver to Thailand

Departments ▾ Your Amazon.com Today's Deals Gift Cards Sell

EN ▾ Hello. Sign in Account & Lists ▾ Orders Cart 0

1-16 of 119 results for "elasticsearch"

Show results for

Books

- Computers & Technology
- Data Processing
- Web Development & Design
- Online Internet Searching
- Databases & Big Data
- ▼ See more

Kindle Store

- Computers & Technology
- Business Software
- Search Engines
- Application Development
- Computer Databases
- ▼ See more
- ▼ See All 8 Departments

Refine by

Book Language

- English

Book Format

- Paperback

Packt

SPONSORED BY PACKT PUBLISHING

Complete Database Solutions with PostgreSQL

Shop now ▾

SQL Server 2017 Administrator's Guide

By Waheed Ahmad and Imanuele Pollicino

PostgreSQL 9.6 High Performance

By Waheed Ahmad, Gregory Smith

SQL Server 2017 Administrators Guide

3 ★★★★★ prime

PostgreSQL 9.6 High Performance: Optimize your...

1 ★★★★★ prime

Advertisement

Sponsored ⓘ

Learning Elastic Stack 6.0: A beginner's guide to distributed search, analytics, and visualization using Elasticsearch, Logstash and Kibana

Dec 22, 2017

by Pranav Shukla and Sharath Kumar M N

Eligible for Shipping to Thailand

Get to grips with the new features introduced in Elastic Stack 6.0, and deliver end-to-end real-time distributed data processing solutions.

Paperback

\$34⁹⁹

In Stock

★★★★★ 7

Previous Page 1 2 3 ... 8 Next Page



Query

amazon

All ▾ elasticsearch 

Departments ▾ Your Amazon.com Today's Deals Gift Cards Sell

New to Amazon? EN Hello, Sign In Account Lists Orders Cart

Sort by Featured

1-16 of 119 results for "elasticsearch"

Filter

Books

- Computers & Technology
- Data Processing
- Web Development & Design
- Online Internet Searching
- Databases & Big Data
- ▼ See more

Kindle Store

- Computers & Technology
- Business Software
- Search Engines
- Application Development
- Computer Databases
- ▼ See more
- ▼ See All 8 Departments

Refine by

Book Language

- English

Book Format

- Paperback

Packt

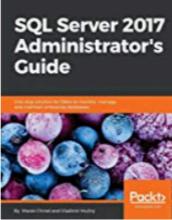
SPONSORED BY PACKT PUBLISHING

Complete Database Solutions with PostgreSQL

Shop now ›

SQL Server 2017 Administrator's Guide

By Waheed Ahmad and Imanuele Pollicino



SQL Server 2017 Administrators Guide

★★★★★ 3
prime

PostgreSQL 9.6 High Performance

By Waheed Ahmad, Gregory Smith



PostgreSQL 9.6 High Performance: Optimize your PostgreSQL database

★★★★★ 1
prime

Sponsored ⓘ

Learning Elastic Stack 6.0: A beginner's guide to distributed search, analytics, and visualization using Elasticsearch, Logstash and Kibana

Dec 22, 2017

by Pranav Shukla and Sharath Kumar M N

Eligible for Shipping to Thailand

Get to grips with the new features introduced in Elastic Stack 6.0, and deliver end-to-end real-time distributed data processing solutions.

Paperback

Paging

Previous Page 1 2 3 ... 8 Next Page



Aggregation API

<https://www.elastic.co/guide/en/elasticsearch/reference/current/search-aggregations.html>



```
SELECT count(1), sum(price)  
FROM some_table  
GROUP BY some_column
```



Aggregation Types

Bucketing
Metric
Matrix
Pipeline



Structure

```
"aggregations" : {  
    "<aggregation_name>" : {  
        "<aggregation_type>" : {  
            <aggregation_body>  
        }  
        [ , "meta" : { [ <meta_data_body> ] } ] ?  
        [ , "aggregations" : { [ <sub_aggregation> ]+ } ] ?  
    }  
    [ , "<aggregation_name_2>" : { ... } ] *  
}
```



Count by category

GET /store/book/_search

```
{  
  "aggs": {  
    "all_book_title": {  
      "terms": {  
        "field": "category.keyword"  
      }  
    }  
  }  
}
```



Count by category

GET /store/book/_search

```
{  
  "aggs": {  
    "all_book_title": {  
      "terms": {  
        "field": "category.keyword"  
      }  
    }  
  }  
}
```



Count by category

GET /store/book/_search

```
{  
  "aggs": {  
    "all_book_title": {  
      "terms": { Aggregation type  
        "field": "category.keyword"  
      }  
    }  
  }  
}
```



Result of aggregation

```
{  
  "hits": {  
    "total": 5,  
    "max_score": 1,  
    "hits": [  
      {  
        "_source": {  
          "title": "The Logstash Book"  
        }  
      },  
      {  
        "_source": {  
          "title": "Elasticsearch Server: Second Edition"  
        }  
      }  
    ]  
  }  
}
```

Search result



Result of aggregation

```
"aggregations": {  
    "all_book_title": {  
        "doc_count_error_upper_bound": 0,  
        "sum_other_doc_count": 0,  
        "buckets": [          Aggregation result  
            {  
                "key": "Computer & Technology",  
                "doc_count": 5  
            },  
            {  
                "key": "Online Searching",  
                "doc_count": 3  
            },  
            {  
                "key": "Java Programming",  
                "doc_count": 2  
            }  
        ]  
    }  
}
```



Show only aggregation result

GET /store/book/_search

```
{  
  "size": 0, Set search result size = 0  
  "aggs": {  
    "all_book_title": {  
      "terms": {  
        "field": "category.keyword"  
      }  
    }  
  }  
}
```



Range of price

GET /store/book/_search

```
{  
  "size": 0,  
  "aggs": {  
    "price_range": {  
      "range": {  
        "field": "price",  
        "ranges": [  
          { "from": 0,"to": 10 },  
          { "from": 11,"to": 20 },  
          { "from": 21,"to": 50 }  
        ]  
      }  
    }  
  }  
}
```



Result of aggregation

```
"buckets": [
  {
    "key": "0.0-10.0",
    "from": 0,
    "to": 10,
    "doc_count": 1
  },
  {
    "key": "11.0-20.0",
    "from": 11,
    "to": 20,
    "doc_count": 0
  },
  {
    "key": "21.0-50.0",
    "from": 21,
    "to": 50,
    "doc_count": 3
  }
]
```



Range of price and ordering

GET /store/book/_search

```
{  
  "size": 0,  
  "aggs": {  
    "price_range": {  
      "range": {  
        "field": "price",  
        "ranges": [  
          { "from": 0, "to": 10 },  
          { "from": 11, "to": 20 },  
          { "from": 21, "to": 50 }  
        ]  
      }  
    }  
  }  
}
```



Mapping

<https://www.elastic.co/guide/en/elasticsearch/reference/current/mapping.html>



Mapping type

Meta-fields

Field or properties



Meta-field

Metadata of document
`_index, _type, _id, _source`



Field or properties

List of fields or properties of document



Mapping/Schema of document

GET /store/_mapping/book

```
"mappings": {  
    "book": {  
        "properties": {  
            "author name": {  
                "type": "text",  
                "fields": {  
                    "keyword": {  
                        "type": "keyword",  
                        "ignore_above": 256  
                    }  
                }  
            }  
        }  
    }  
}
```



Mapping/Schema of document

GET /store/_mapping/book

```
"mappings": {  
    "book": {  
        "page": {  
            "type": "long"  
        },  
        "price": {  
            "type": "float"  
        },  
        "published_date": {  
            "type": "date"  
        }  
    }  
}
```



Field Datatypes

text	date
keyword	ip
long	boolean
double	completion
geo_point	geo_shape
array	object
nested	binary

<https://www.elastic.co/guide/en/elasticsearch/reference/current/mapping-types.html>



Field Datatypes

text	date
keyword	ip
long	boolean
double	completion
geo_point	geo_shape
array	object
nested	binary

<https://www.elastic.co/guide/en/elasticsearch/reference/current/mapping-types.html>



Array

No data type **array** in Elasticsearch

["name", "title"]	array of string
[1, 2, 3]	array of integer
[{"name": "up1", "age": 30}]	array of object



Mapping configuration

Maximum number of fields = 1,000

Maximum depth of fields = 20

Maximum depth of nested fields = 50



Dynamic mapping

Fields and mapping types not need to defined before being used



Analyzer

<https://www.elastic.co/guide/en/elasticsearch/reference/current/analysis.html>



More tools



Elasticsearch Head

 **ElasticSearch Head**
offered by travistx

★★★★★ (75) | [Developer Tools](#) | 45,312 users

[OVERVIEW](#) | [REVIEWS](#) | [SUPPORT](#) | [RELATED](#)

ElasticSearch http://192.168.7.8:9200/ Connect Rick cluster health: yellow (6, 18)

Overview Browser Structured Query Any Request Info Status Nodes Stats Cluster Nodes Cluster State Cluster Health

Cluster Overview New Index

	cu_docs	bnvil	cu_msg	anvil
Leon	size: 180Gb (540Gb) docs: 995131 (995131)	size: 80kb (480kb) docs: 90 (90)	size: 313Gb (1.56Tb) docs: 10047450 (10140915)	index: close
Pris	Info Actions	Info Actions	Info Actions	Info Actions
Rick	0 1	0 1	0 1 2 3 4	0 1 2 3 4
Rachel	1 2	0 1	0 1 2 3 4	0 1 2 3 4
Zhora	1 2	0 1	0 1 2 3 4	0 1 2 3 4
Roy	0 2	0 1	0 1 2 3 4	0 1 2 3 4
Unassigned	0 0	0 1	0 1 2 3 4	0 1 2 3 4

Compatible with your device

ElasticSearch Head
Chrome Extension containing the excellent Elasticsearch Head application.

[Website](#) | [Report Abuse](#)

Additional Information
Version: 0.1.3
Updated: December 4, 2017
Size: 434KiB
Language: English (United States)



<https://github.com/mobz/elasticsearch-head>



Elasticsearch Dump



<https://github.com/taskrabbit/elasticsearch-dump>



Kibana



Explain and Profiling your query



2 ways

Explain API
Profile API



Explain API

GET /my_map/_search

```
{  
  "explain": true,  
  "query": {  
    "bool": {
```

<https://www.elastic.co/guide/en/elasticsearch/reference/6.3/search-explain.html>



Profile API

Debugging tool

Add overhead to search execution

Output is verbose and depend on internal operation

<https://www.elastic.co/guide/en/elasticsearch/reference/6.3/search-profile.html>



Profile API

GET /my_map/_search

```
{  
  "profile": true,  
  "query": {  
    "bool": {
```



Working with Logstash

<https://www.elastic.co/guide/en/logstash/current/index.html>



Logstash



Input
Filter
Output



Design your input first !!

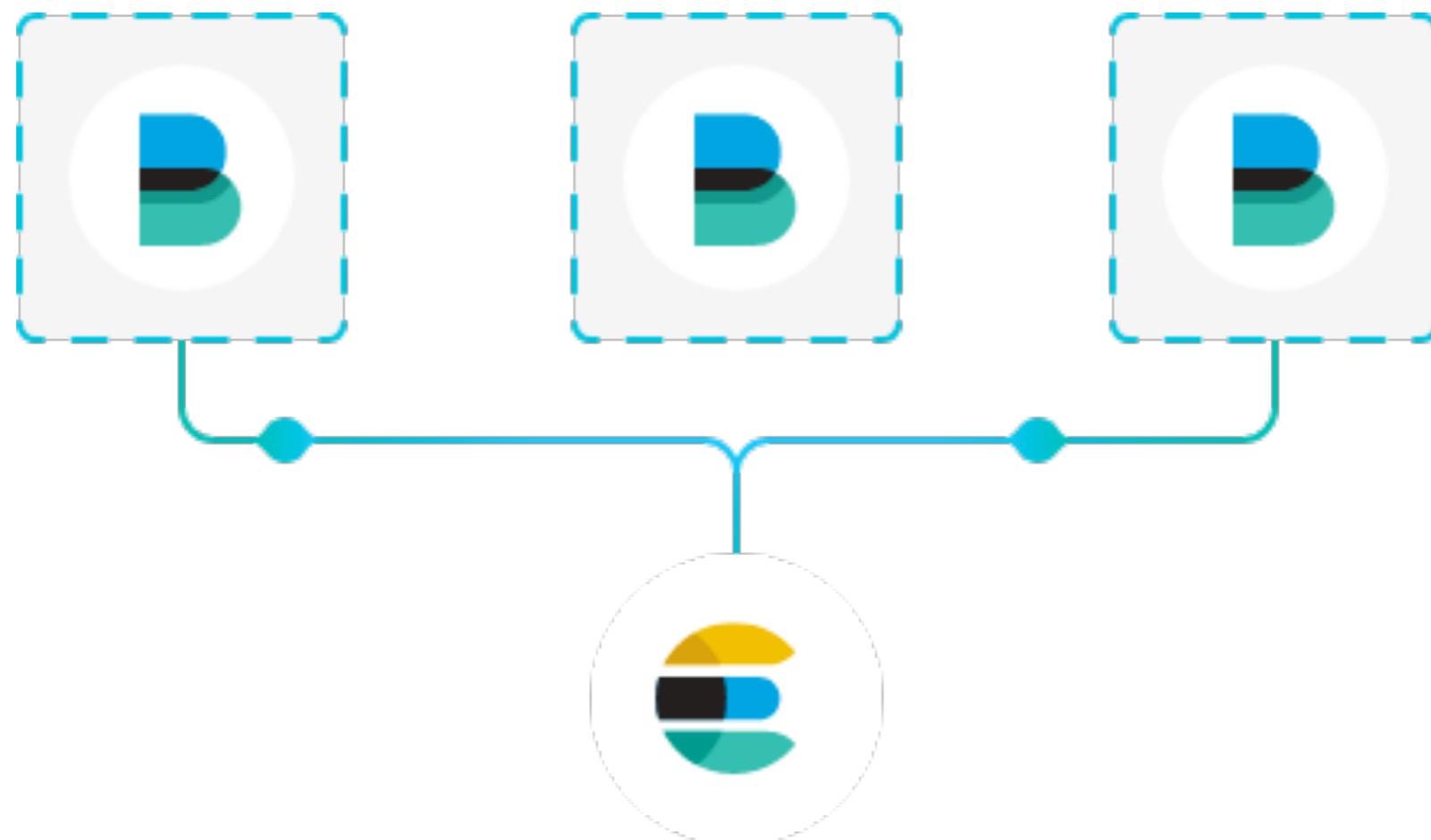


Use beats is better

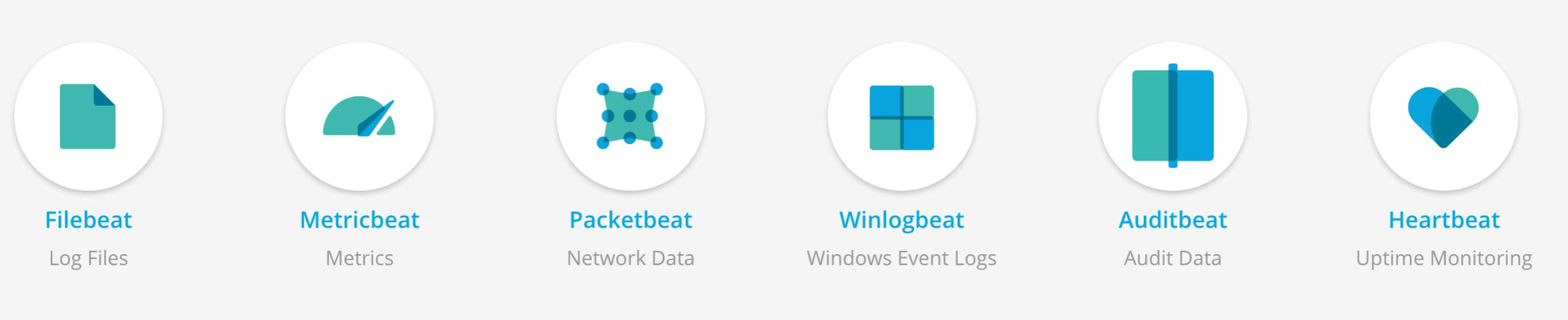
<https://www.elastic.co/products/beats>



Beat



Beat



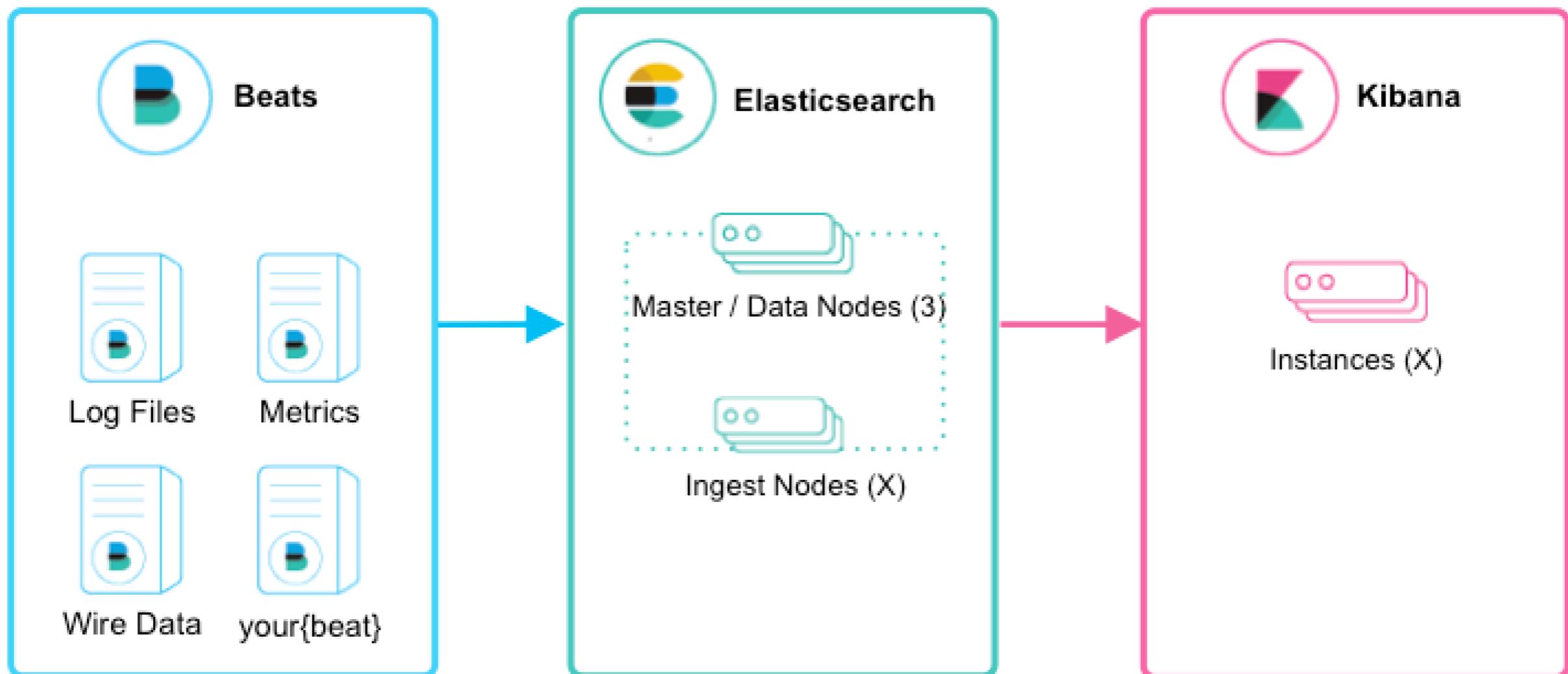
Example

```
$filebeat -e -c beat.yml -d "publish"
```

<https://www.elastic.co/guide/en/beats/filebeat/current/index.html>



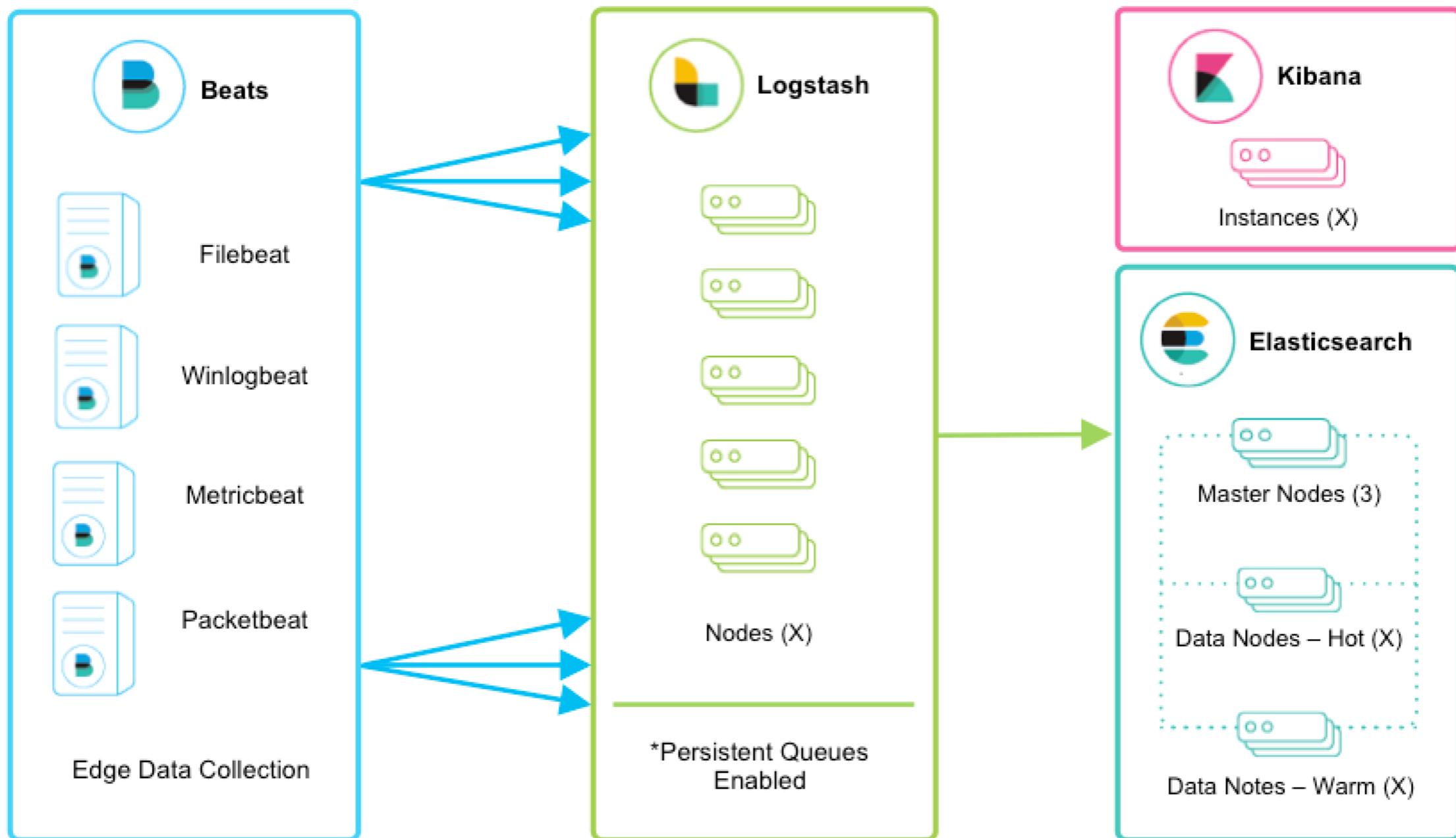
Beat and Logstash



<https://www.elastic.co/guide/en/logstash/current/deploying-and-scaling.html>



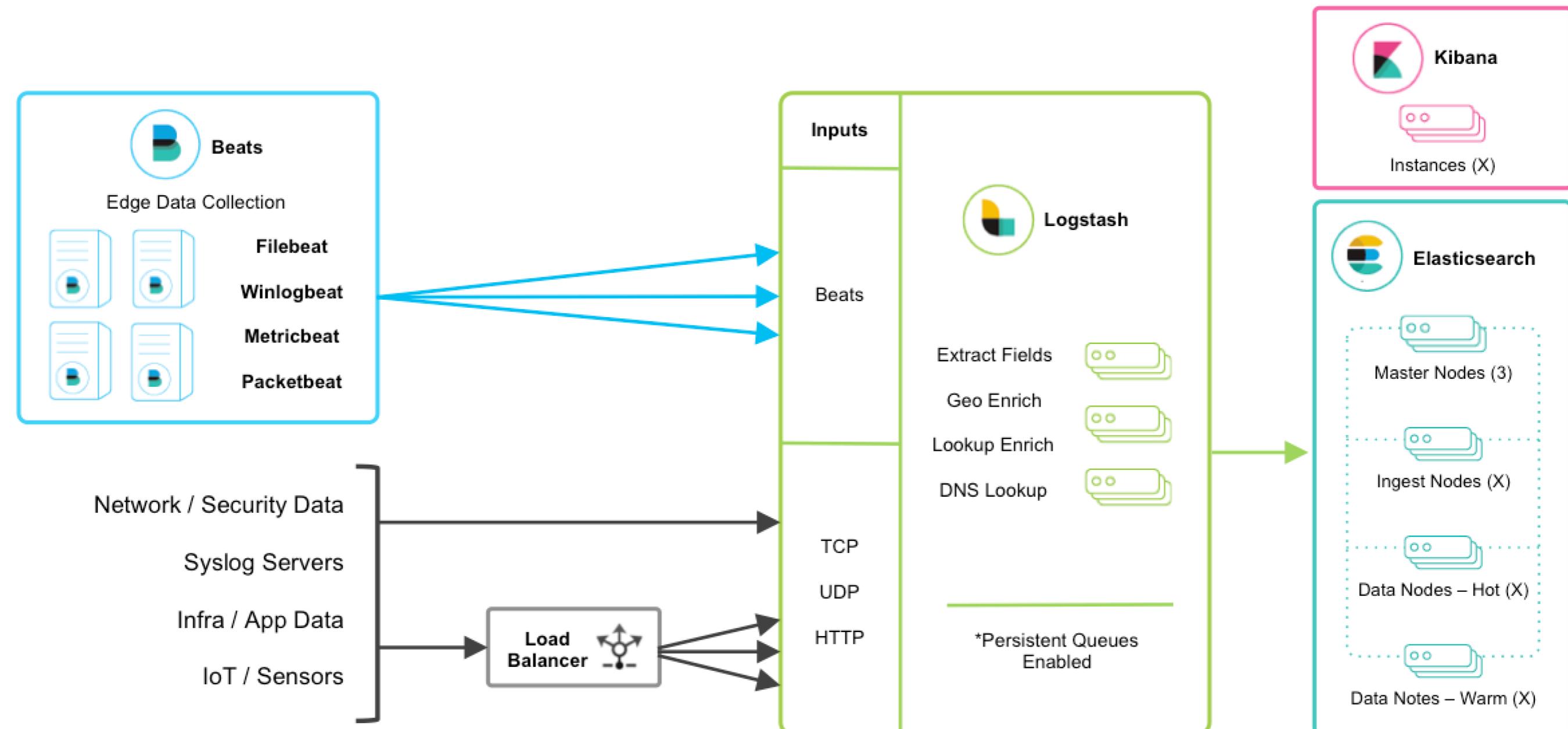
Scaling



<https://www.elastic.co/guide/en/logstash/current/deploying-and-scaling.html>



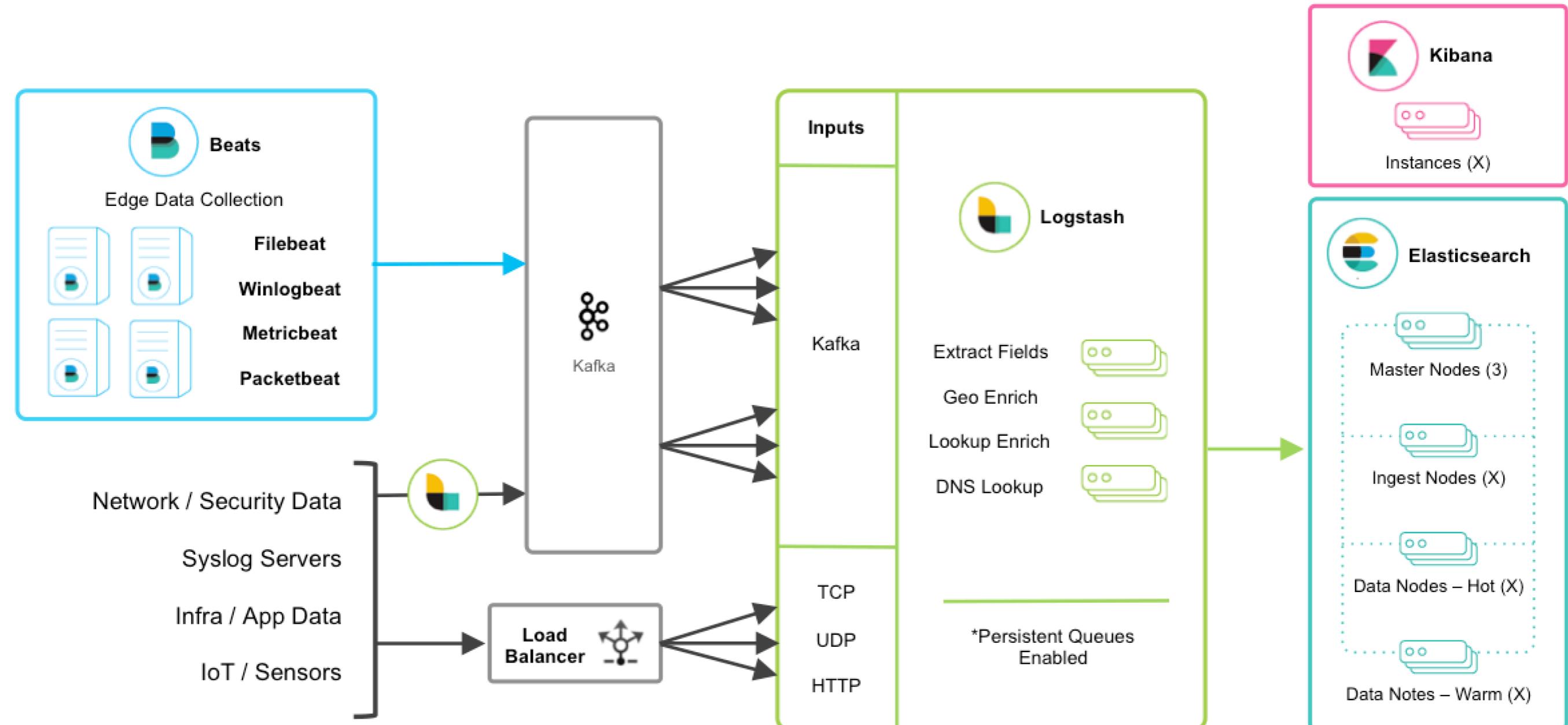
More data sources



<https://www.elastic.co/guide/en/logstash/current/deploying-and-scaling.html>



Use messaging Queue



<https://www.elastic.co/blog/logstash-persistent-queue>



Design for Failure

09-cluster



Elasticsearch Nodes

Node Type	Description
Master	Control the cluster
Data	Keep/store data
HTTP/Query	Run your query
Coordinating	Smart Load Balancer
Ingest	Pre-processing documents before indexing

<https://www.elastic.co/guide/en/elasticsearch/reference/current/modules-node.html>



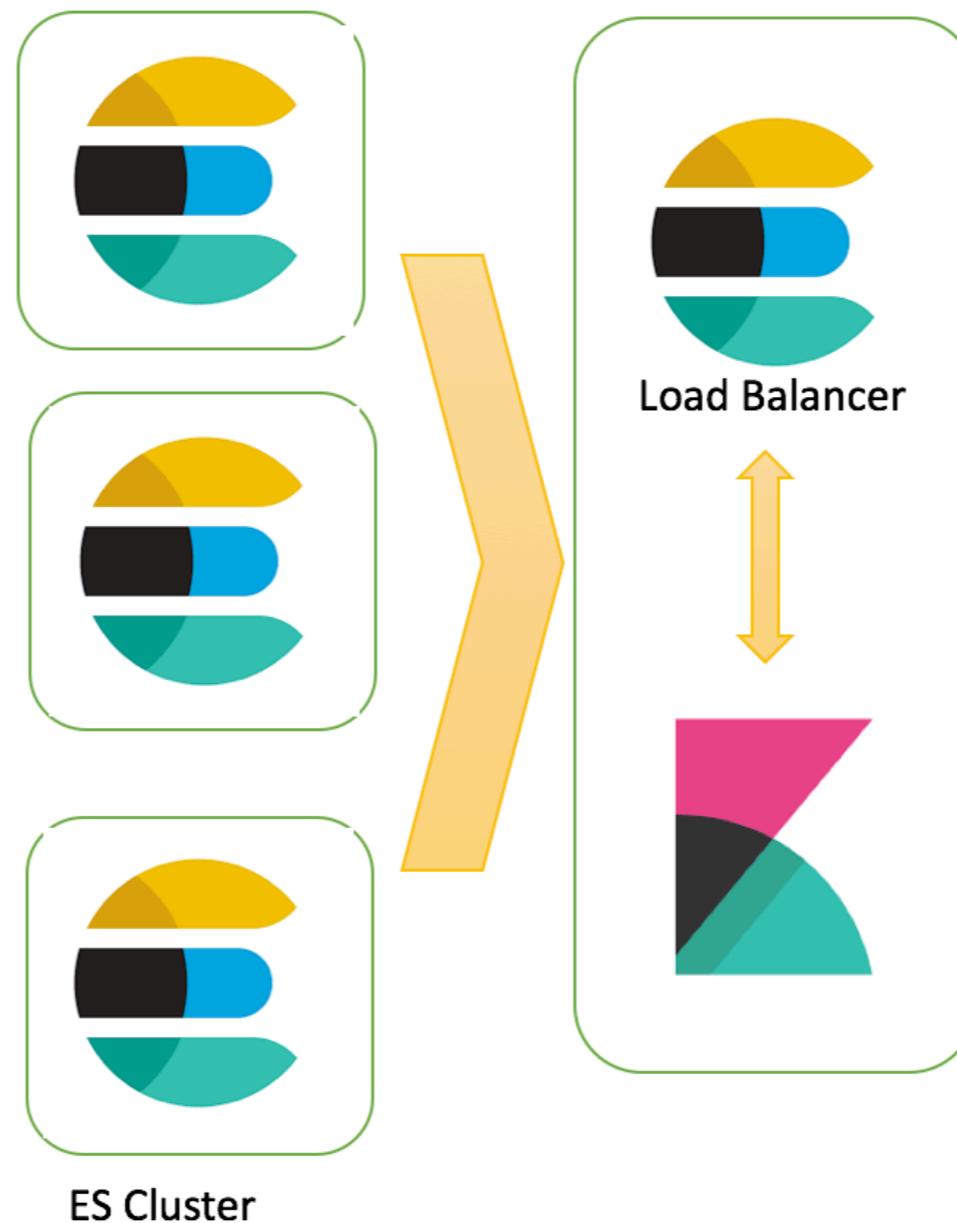
Elasticsearch Nodes

← → ⌂ ⓘ Not Secure | 35.240.161.188:9200/_cat/nodes?v&h=ip,name,node.role,master,heap.percent,ram.percent

ip	name	node.role	master	heap.percent	ram.percent
10.148.0.2	master	m	*	17	33
10.148.0.4	query	-	-	10	63
10.148.0.5	coordinator	-	-	9	78
10.148.0.3	data	d	-	13	63



Elasticsearch Nodes



<https://www.elastic.co/guide/en/kibana/current/production.html#load-balancing>



Elasticsearch Nodes

Master

Data

Query

Master

Data

Query

Ingest

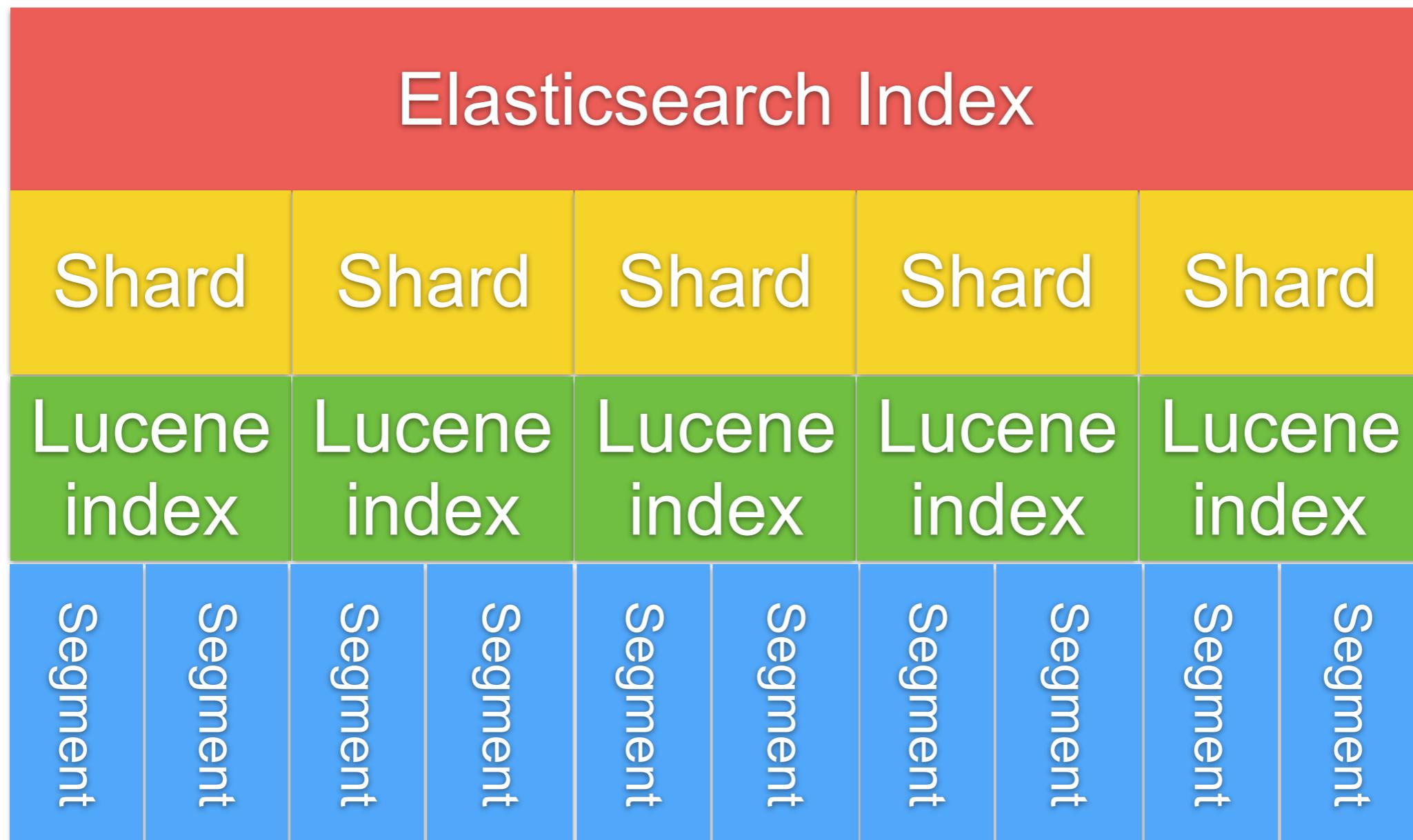


Apache Lucene

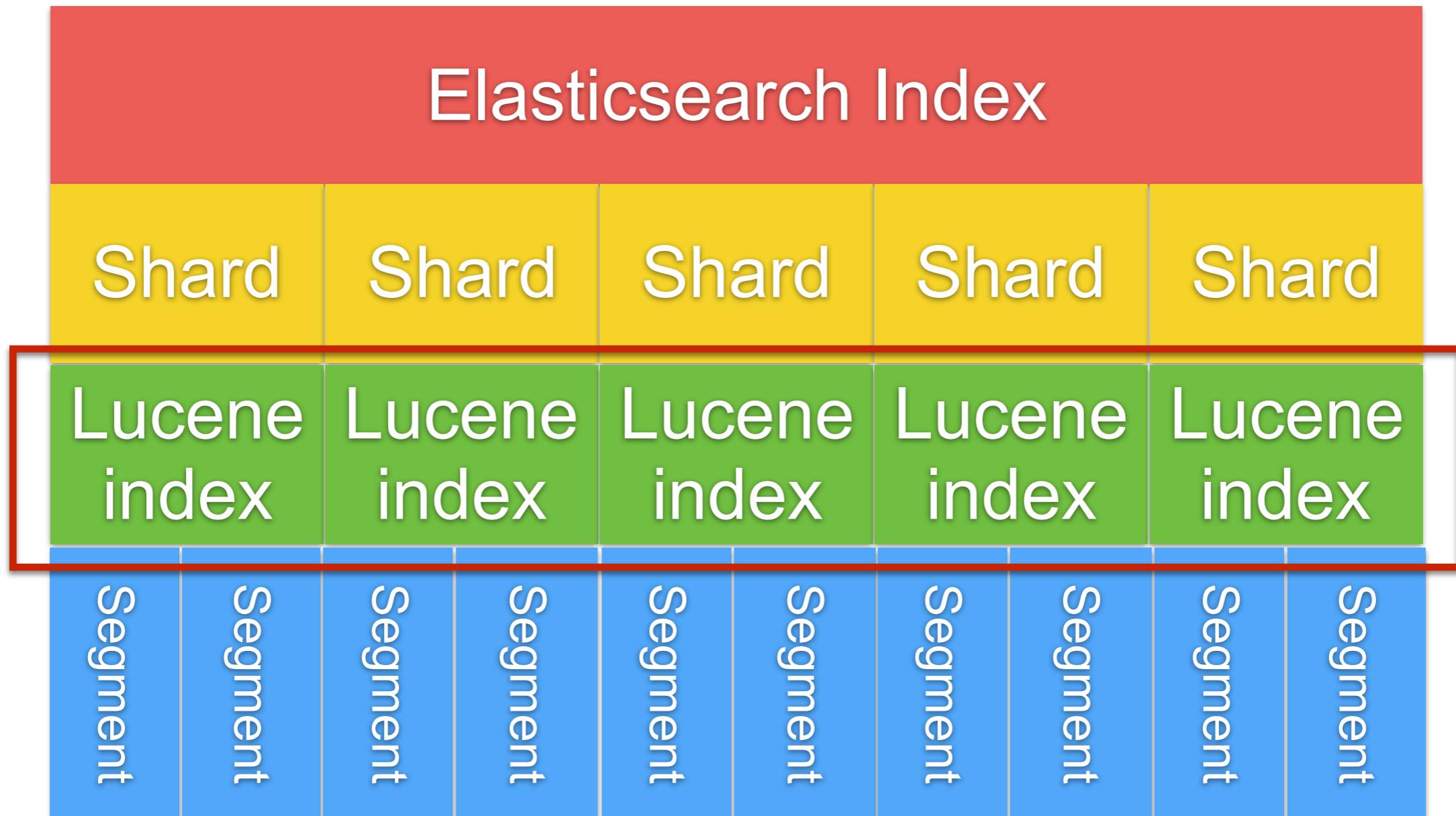
<http://lucene.apache.org/>



Apache Lucene



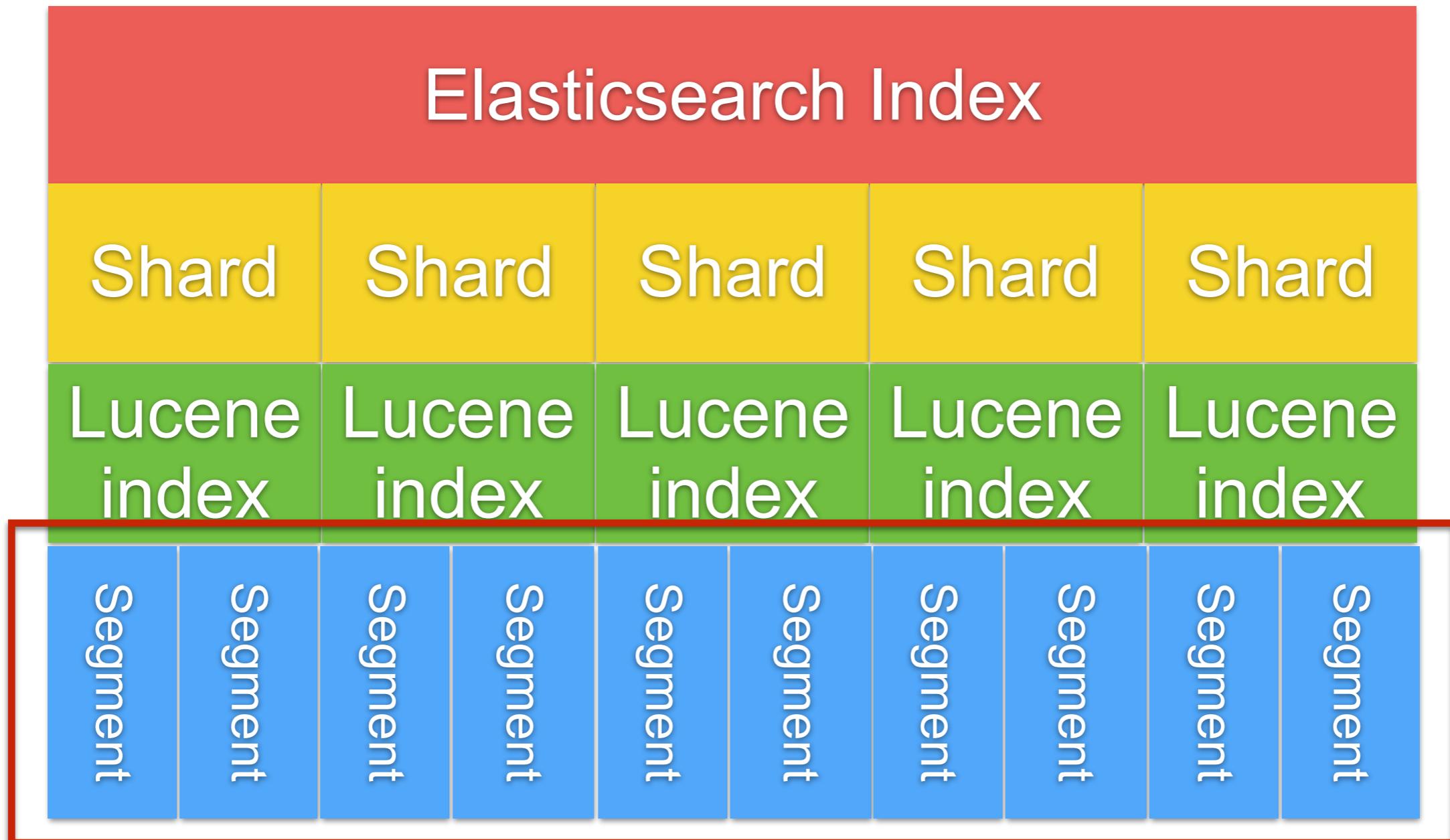
Apache Lucene



Max # of document of Lucene index = 2,147,483,519



Apache Lucene



Segments are immutable

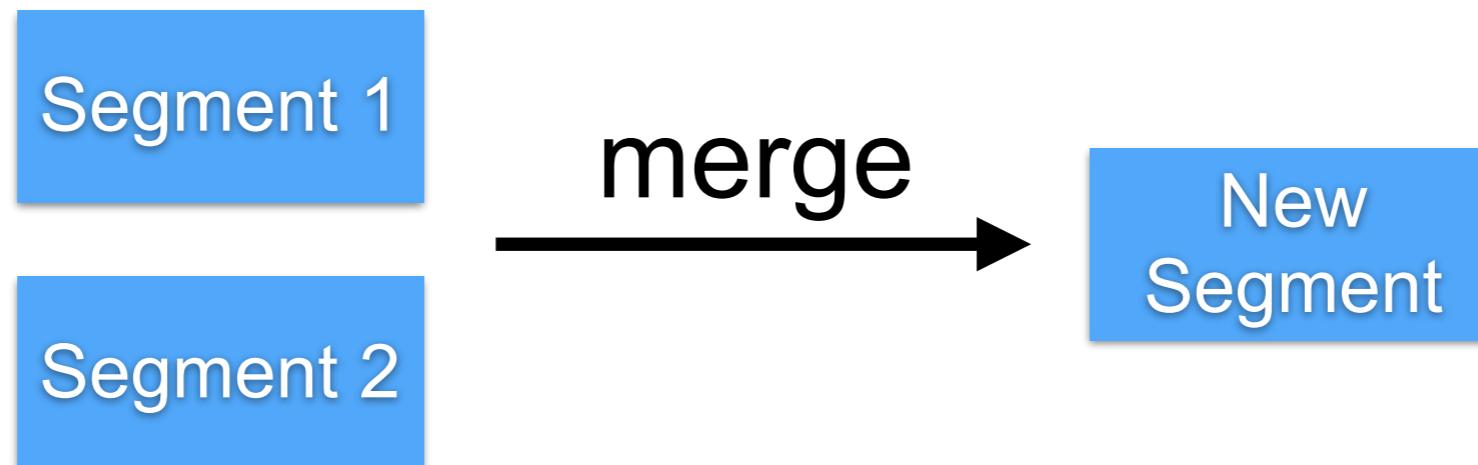


Segment

More shards, more segments

Documents are never delete !!

Lucene segment **merge** use more CPU/IO
Segments are immutable



Hardware



Hardware

CPU
Memory
Network
Storage



Memory

Enable bootstrap.memorylock

Disable all swap files

Change `ES_HEAP_SIZE` (default 1G)

<https://www.elastic.co/guide/en/elasticsearch/reference/current/setup-configuration-memory.html>



Design your index



Design your index

Sharding
Replication



Sharding

Elasticsearch divides the data in **logical** parts
of sharding is define when index created



How many shard ?



Need to know your size of data

Data Size	# of shard
< 3M	1
>3M <5M	2
>5M	(# of document / 5M) + 1



Sharding

Small shards on multiple nodes make the cluster recovery faster

Small shards on a lot of nodes solve memory mgt problem when query on large data



More shard, more Segment !!

Elasticsearch Index				
Shard	Shard	Shard	Shard	Shard
Lucene index	Lucene index	Lucene index	Lucene index	Lucene index
Segment	Segment	Segment	Segment	Segment

Need to config file descriptor

<https://www.elastic.co/guide/en/elasticsearch/reference/current/system-config.html>



Don't create more shard than you need !!



Replication

Prevent data loss

Default = 1

```
# nodes = [(primary + # replication) /2 ] + 1
```



Problems with scaling

CPU consumption
Load average
Request rate
Search latency



Slow log

```
PUT /myindex/_settings
```

```
{  
  "index.search.slowlog.threshold.query.warn: 1s",  
  "index.search.slowlog.threshold.query.info: 500ms",  
  "index.search.slowlog.threshold.query.debug: 1500ms",  
  "index.search.slowlog.threshold.query.trace: 300ms",  
  "index.search.slowlog.threshold.fetch.warn: 500ms",  
  "index.search.slowlog.threshold.fetch.info: 400ms",  
  "index.search.slowlog.threshold.fetch.debug: 300ms",  
  "index.search.slowlog.threshold.fetch.trace: 200ms"  
}
```

If can't optimize then add more resources or rewrite

<https://www.elastic.co/guide/en/elasticsearch/reference/current/index-modules-slowlog.html>



Indexing Data



Indexing data

Must be define data schema for your need
Default mapping == more cost (Memory/Disk)
Default for data is “text” + “keyword”
Understand analyzer and tokenizer
Use auto generated IDs if possible



Indexing data

Prefer bulk indexing

Change refresh interval

Time based index for log data

<https://www.elastic.co/guide/en/elasticsearch/reference/current/indices-update-settings.html>



For Large data

Increase refresh interval
Decrease replica number

```
PUT /logstash-2015.05.20/_settings
{
  "index" : {
    "refresh_interval" : "-1",
    "number_of_replicas" : 0
  }
}
```

<https://www.elastic.co/guide/en/elasticsearch/reference/current/indices-update-settings.html>



Query Data



Query data

Use filters as much as possible

Use scan and scroll for dumping large data

Node query cache

Shard query cache

Retrieve only necessary fields

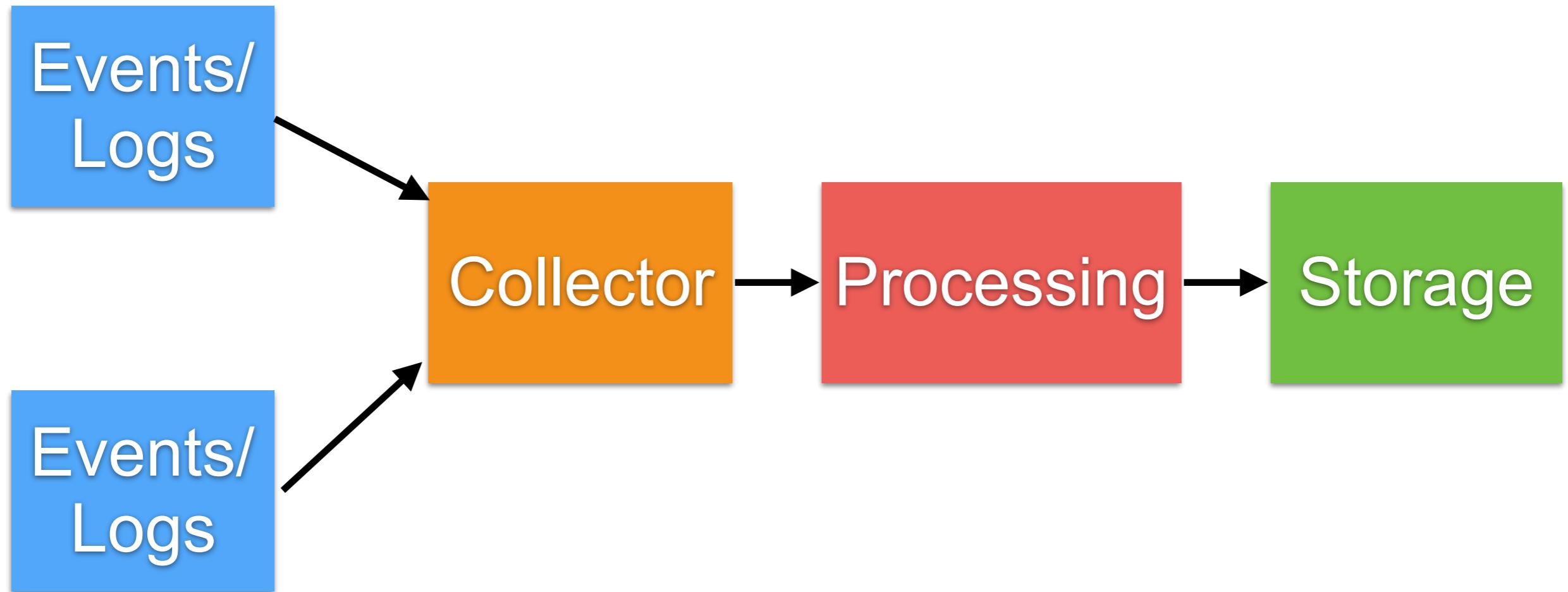
<https://www.elastic.co/guide/en/elasticsearch/reference/current/query-cache.html>



Use cases



Event or Logging from Servers



Event or Logging from Servers



Data
Collection

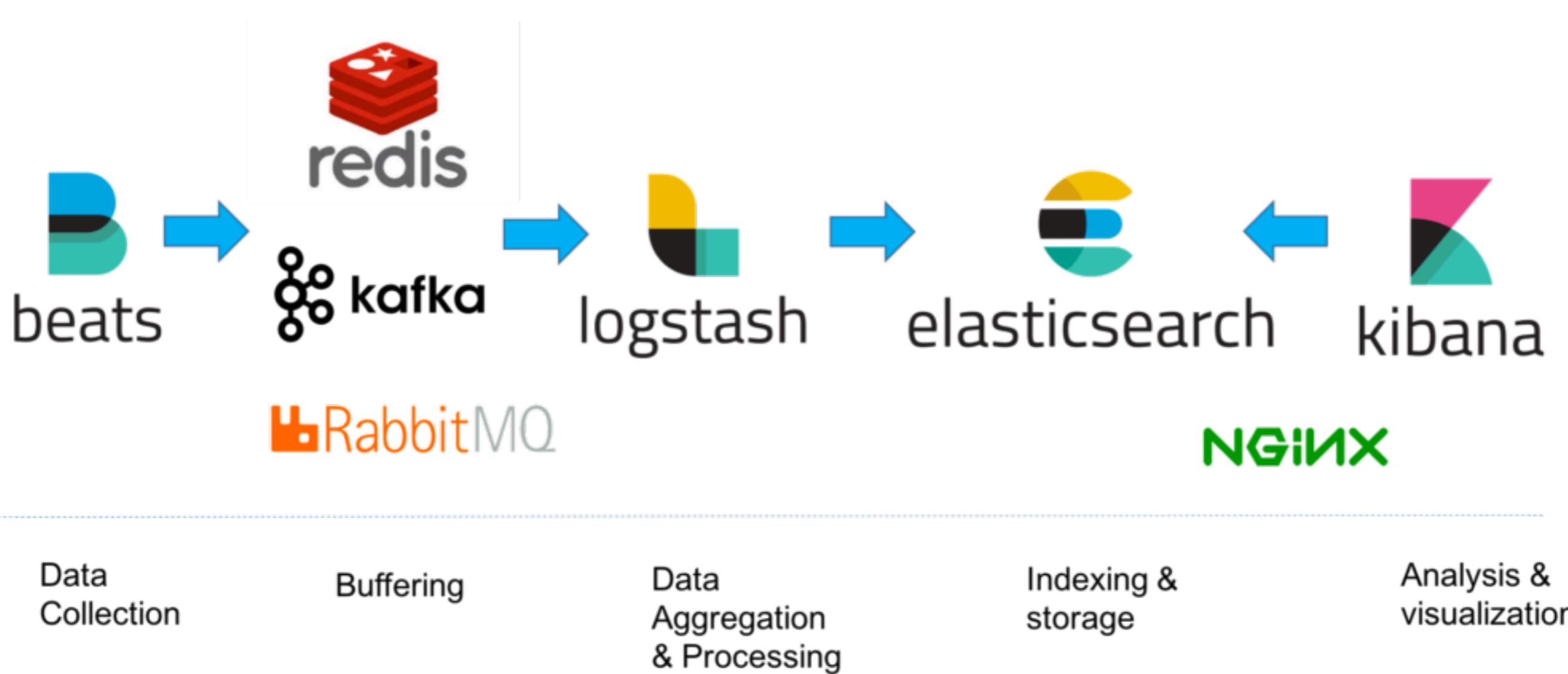
Data
Aggregation
& Processing

Indexing &
storage

Analysis &
visualization



Event or Logging from Servers



Istio



Microservices

Distributed system



Distributed system

Deployment
Resiliency
Networking
Security



Distributed system



kubernetes



Services have to deal with

- Client-side load balancing
- Fault tolerance (timeout/retry)
- Observability
- Monitoring and tracing
- Circuit breaking



Popular tools/library

Client-side load balancing = **Ribbon**

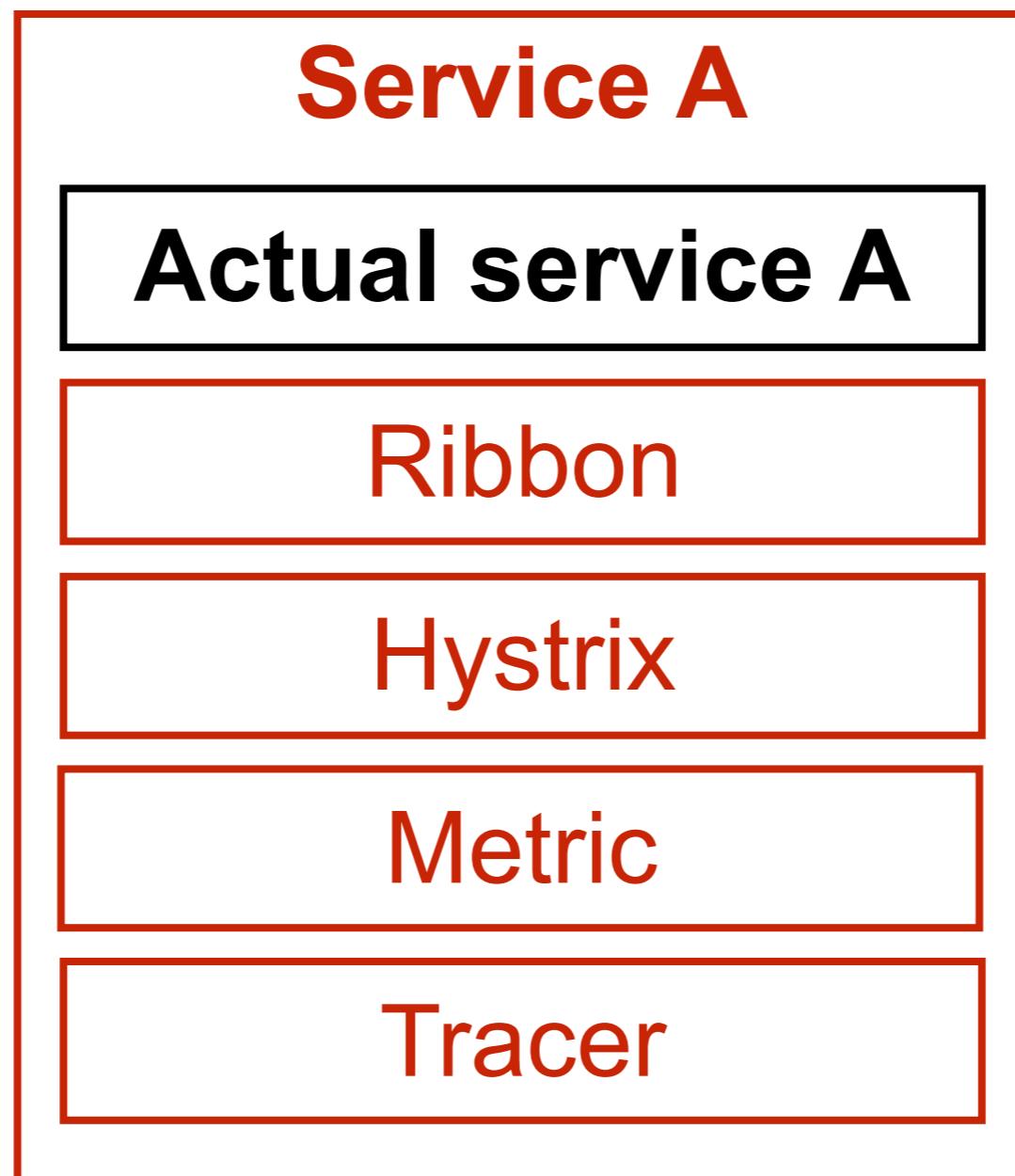
Service registry = **Eureka**

Circuit breaking = **Hystrix**

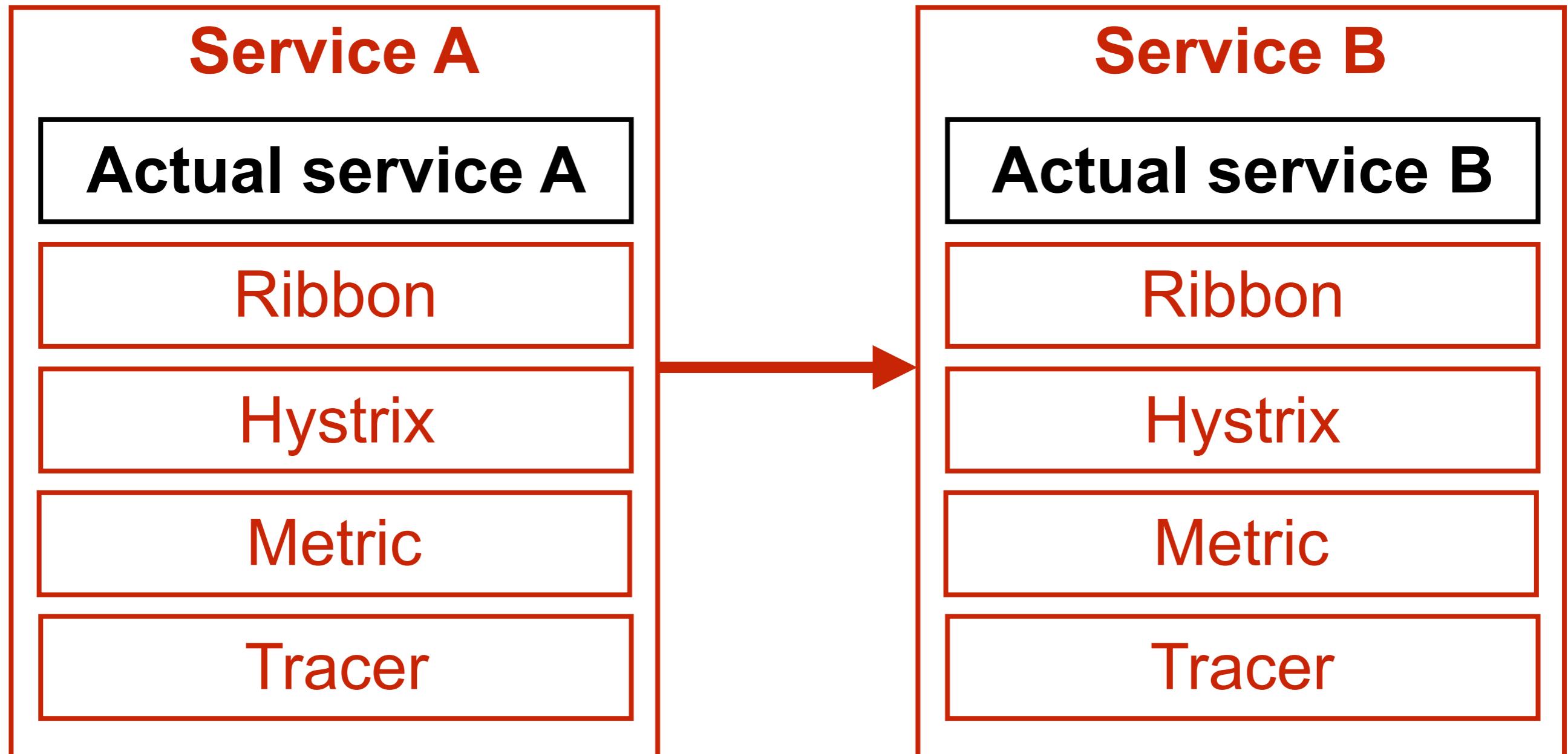
Distributed tracing = **Zipkin**



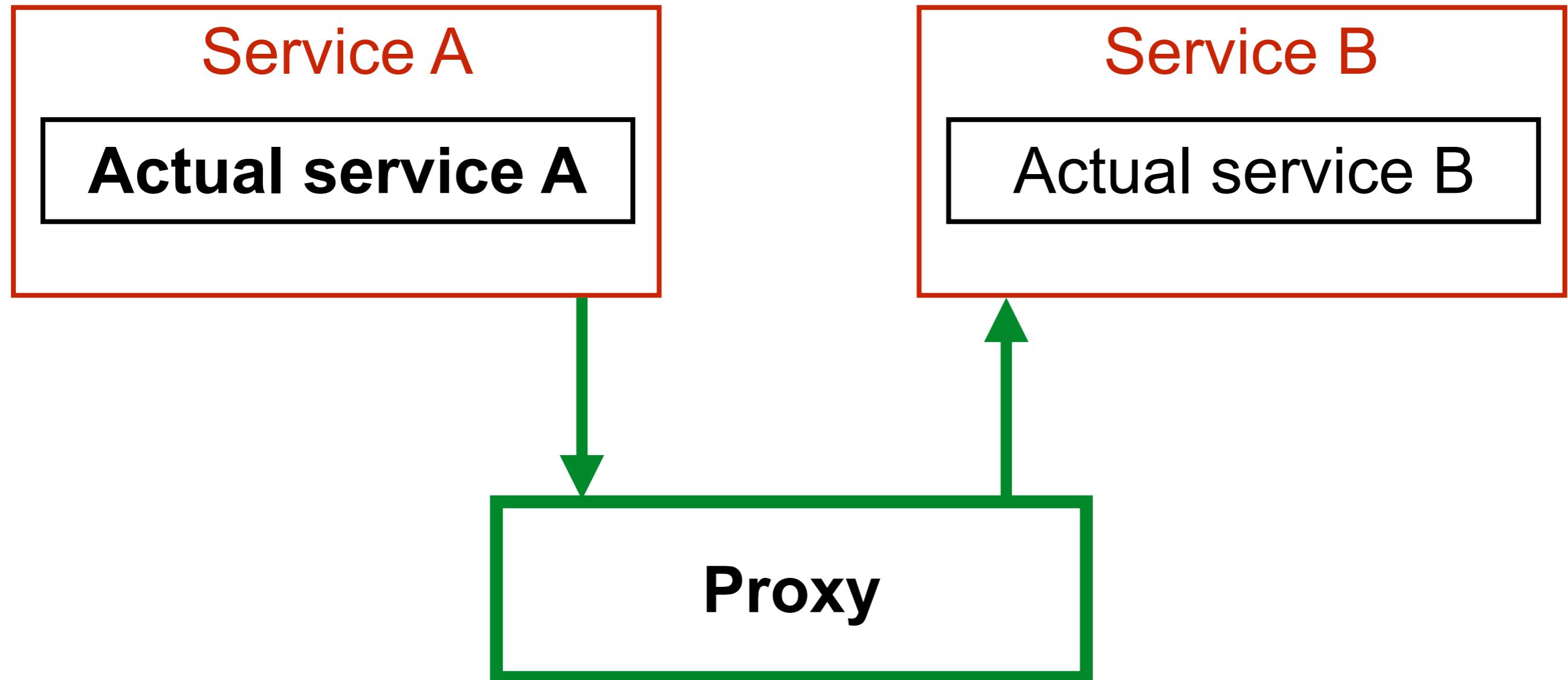
Microservice ?



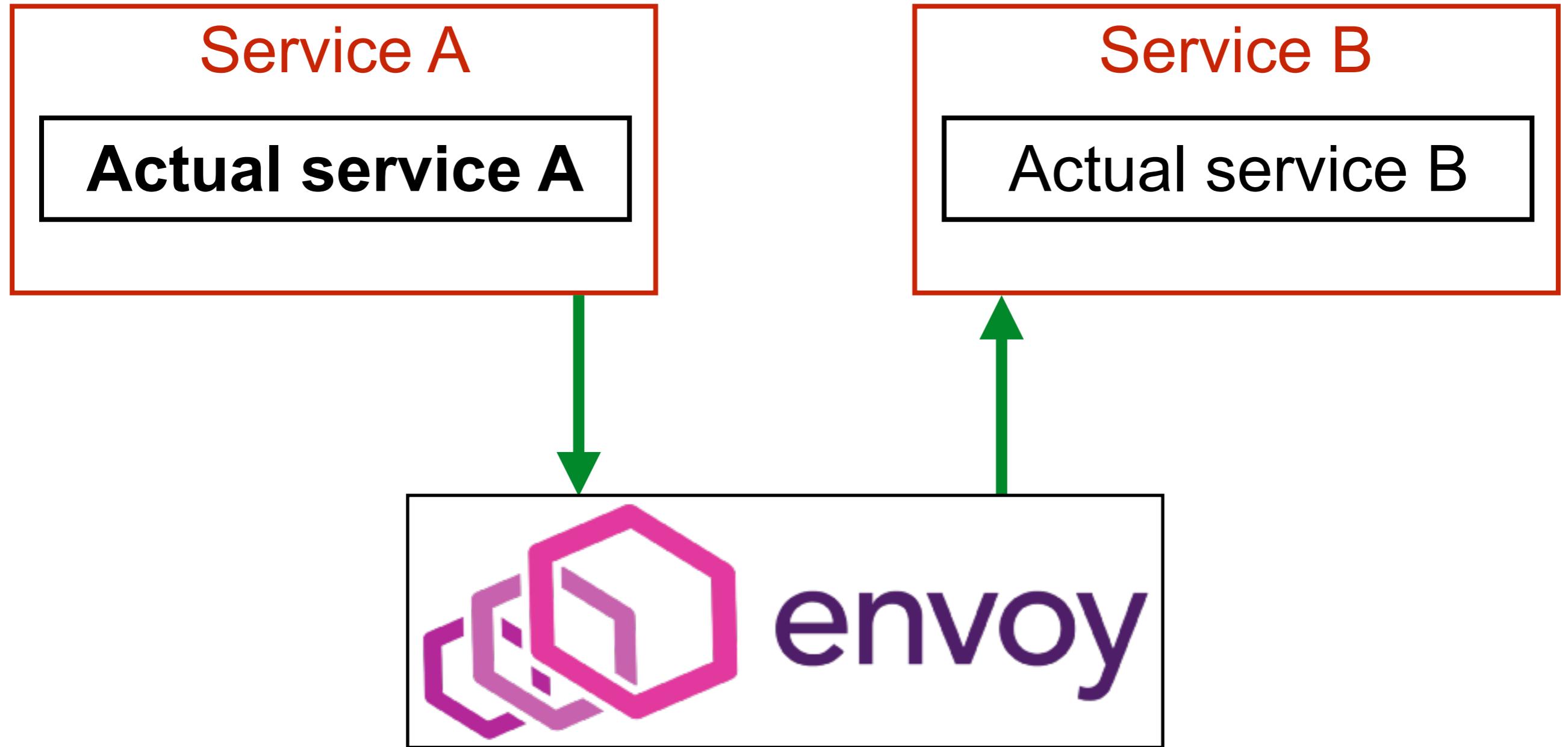
Microservice ?



Moving common functionality !!



Moving common functionality !!



<https://www.envoyproxy.io/>



What is Envoy ?

Service proxy

Developed by Lyft

Written in C++, non-blocking, highly parallel
HTTP 2, including gRPC

Service discovery/registry and health check

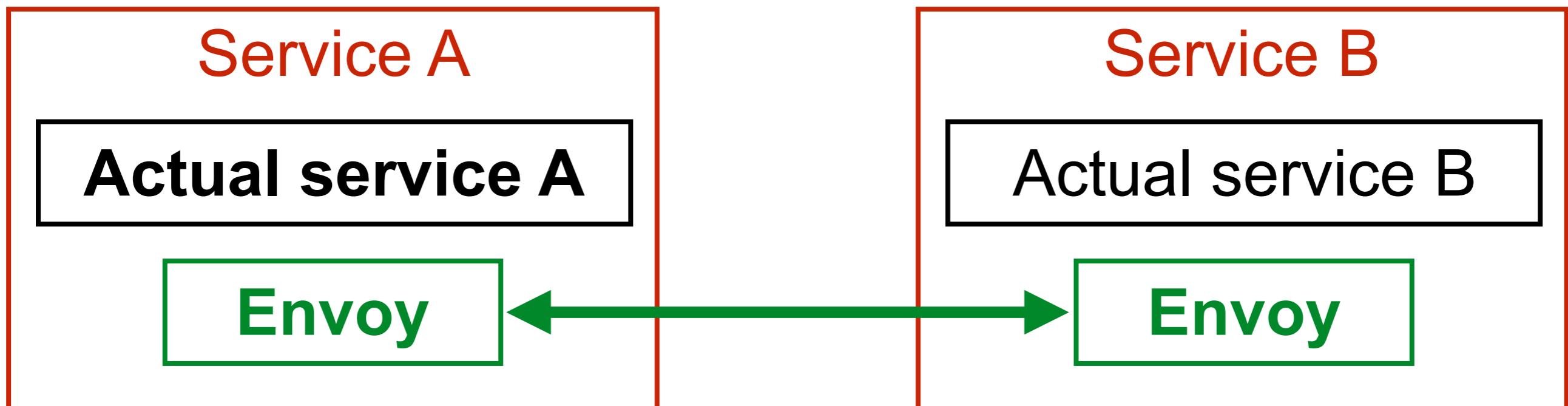
Advance load balancing

Stat, metrics and tracing

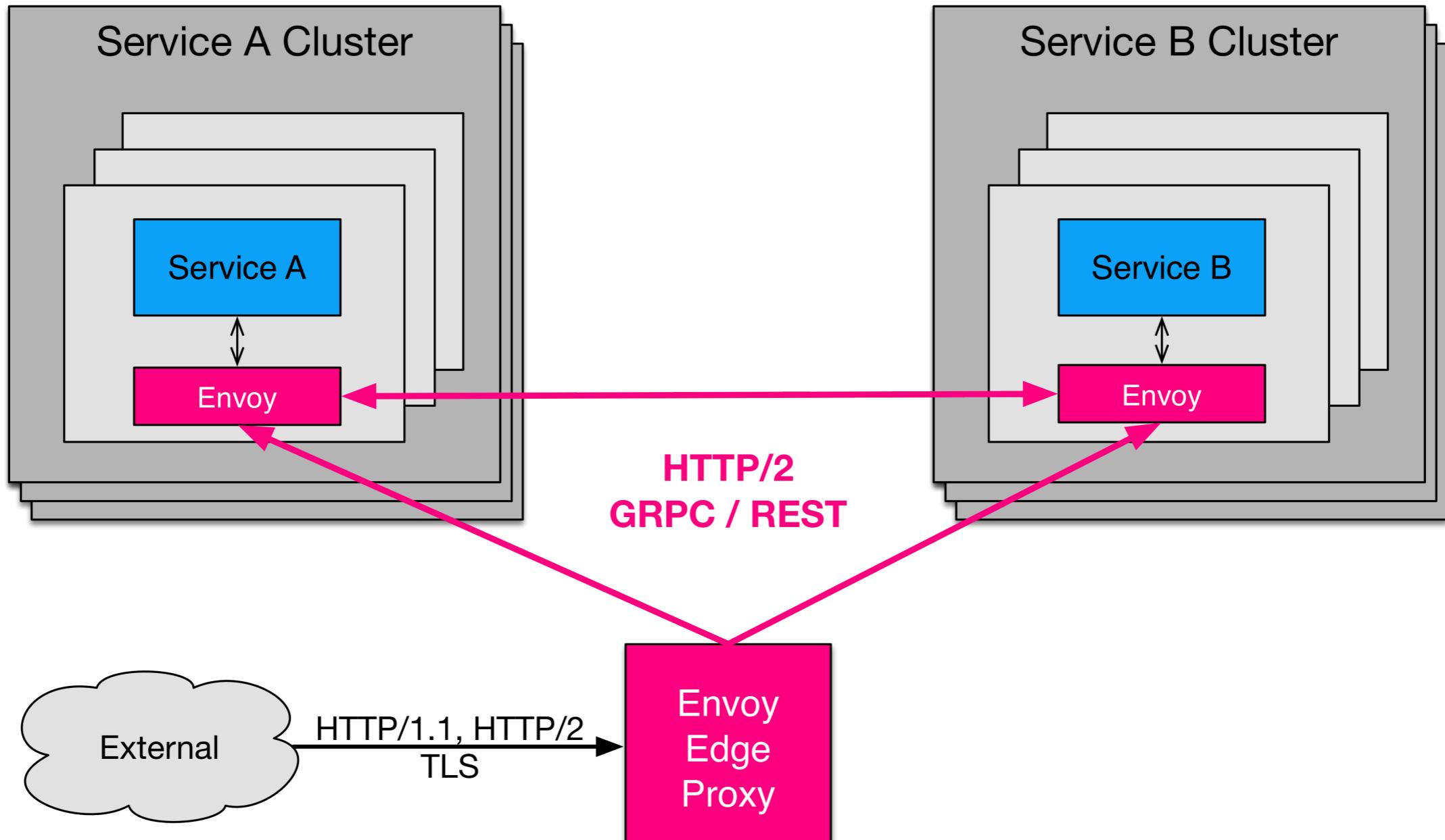


Deployment with Kubernetes

Using sidecar model



Envoy

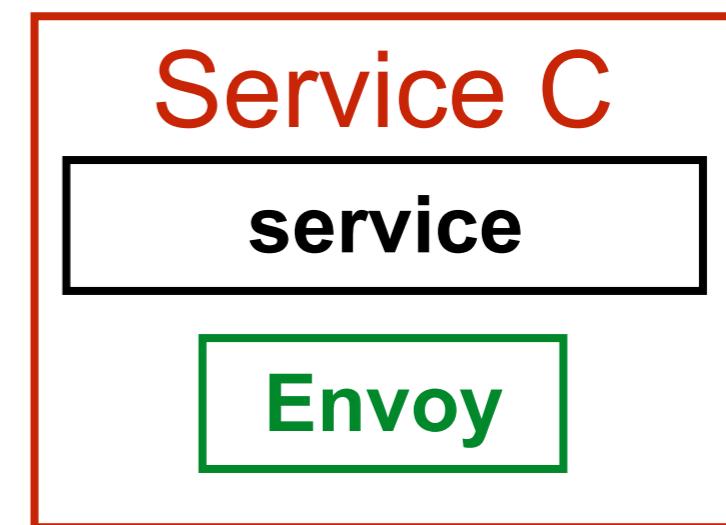
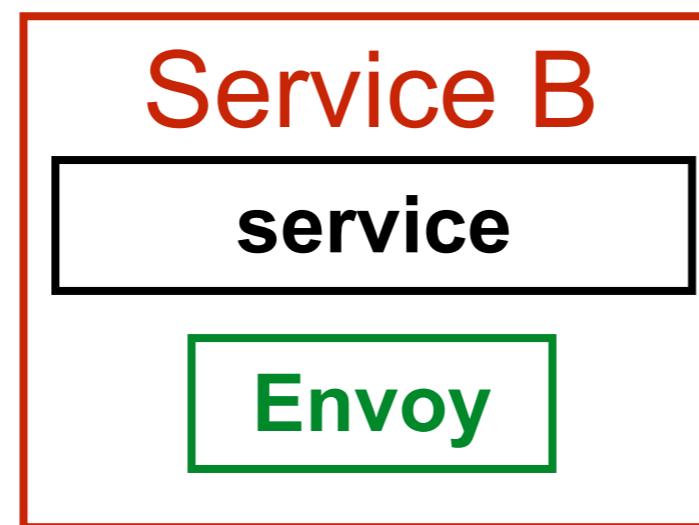
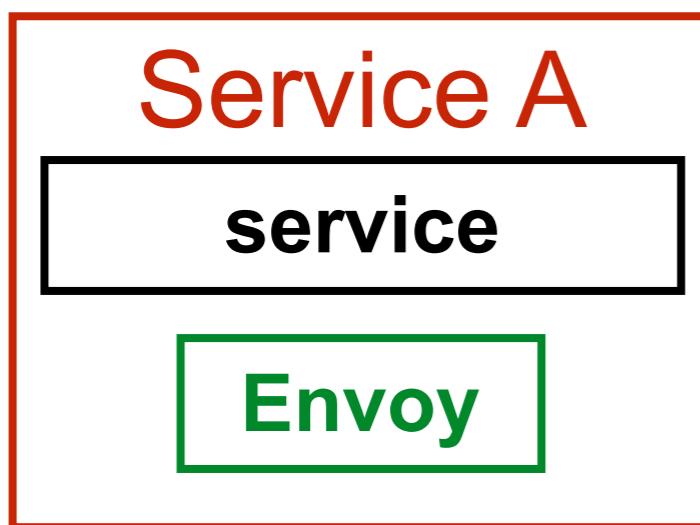


<https://www.envoyproxy.io/>

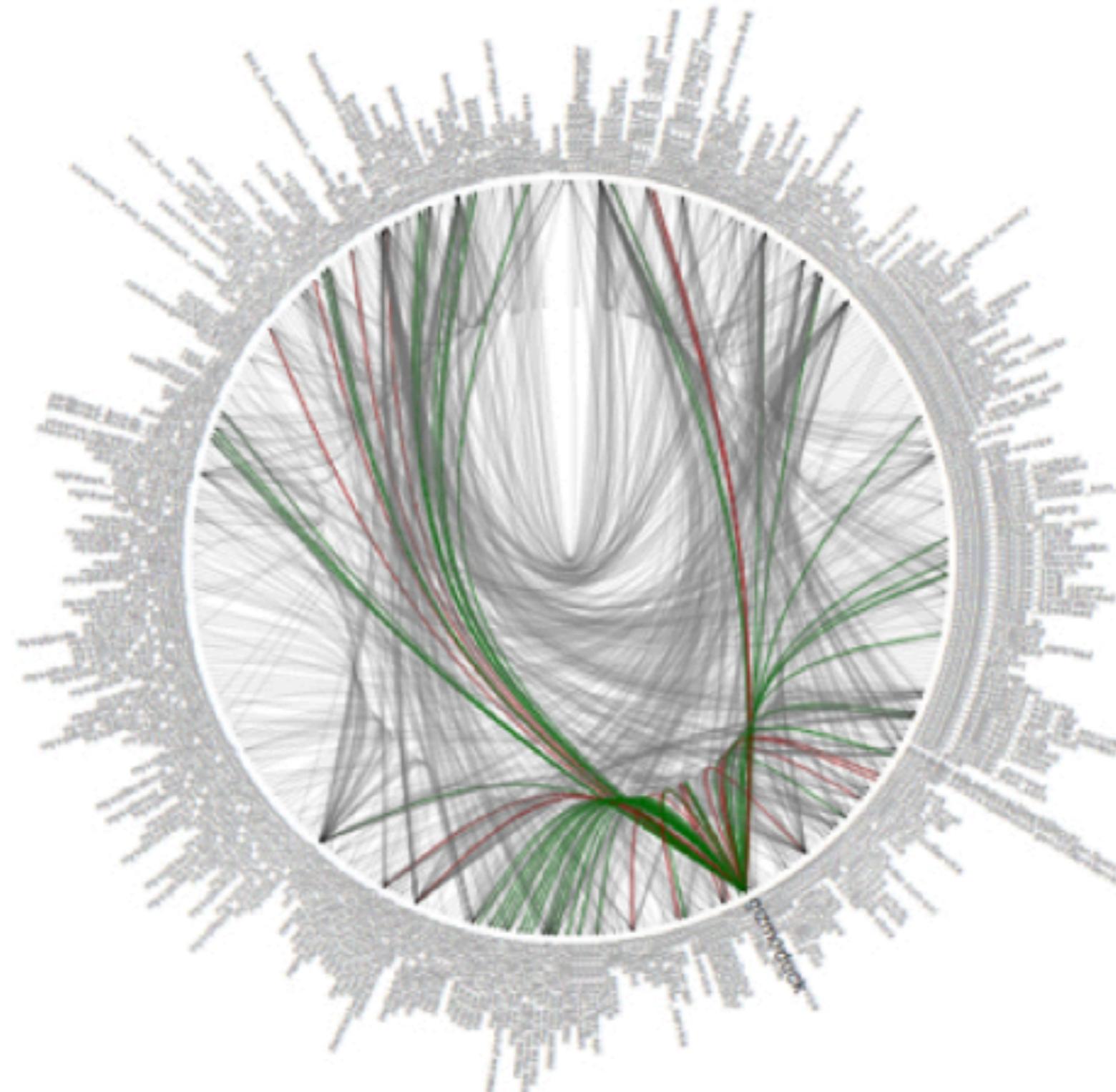


More services !!

Configure can be verbose and error prone !!



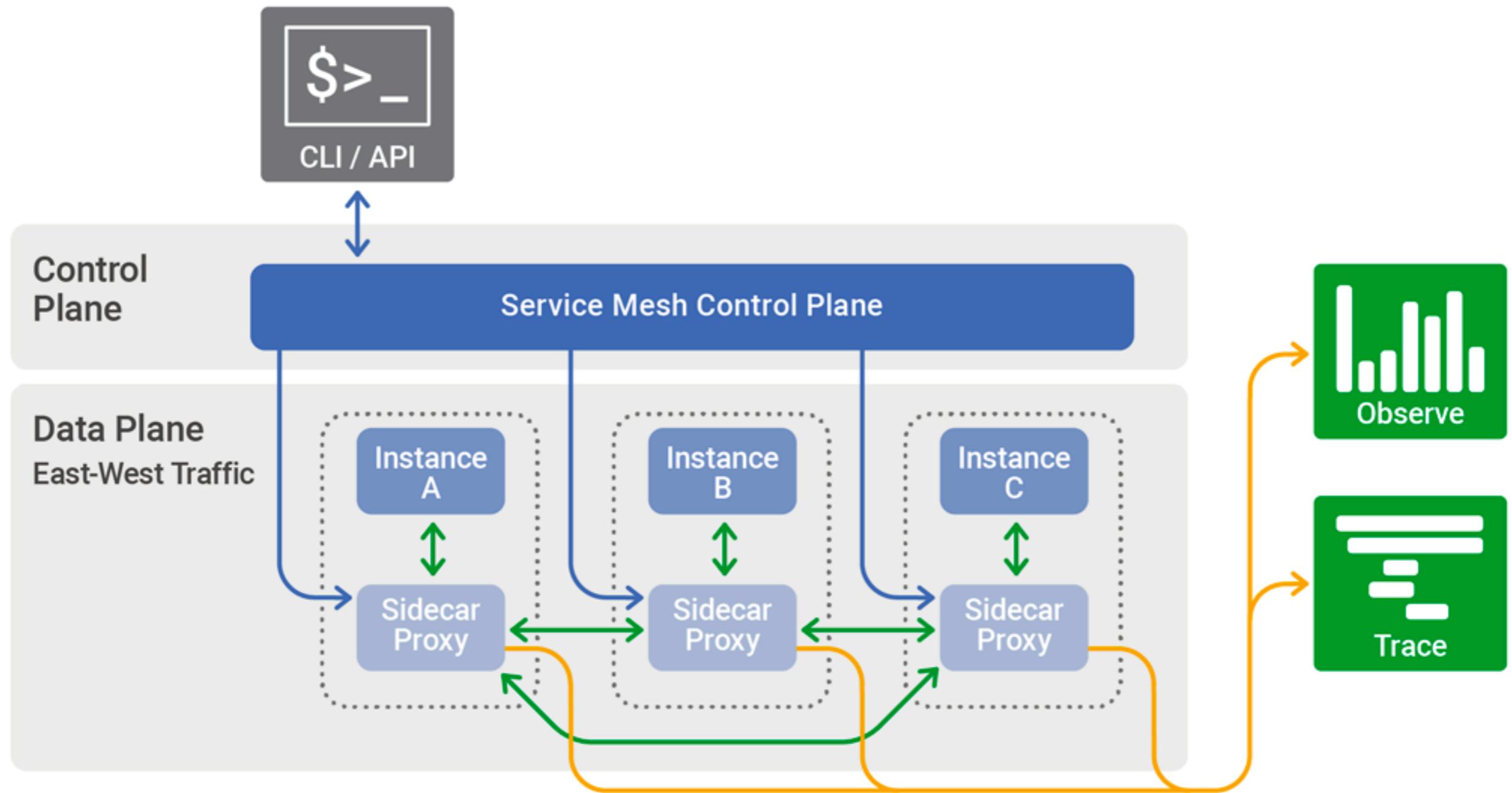
Service mesh



We need control plane



Control plane

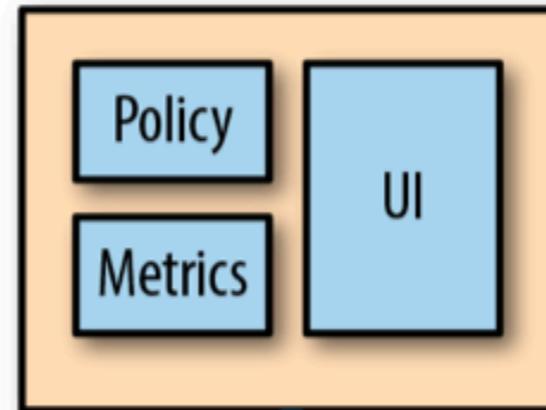


<https://www.nginx.com/blog/what-is-a-service-mesh/>

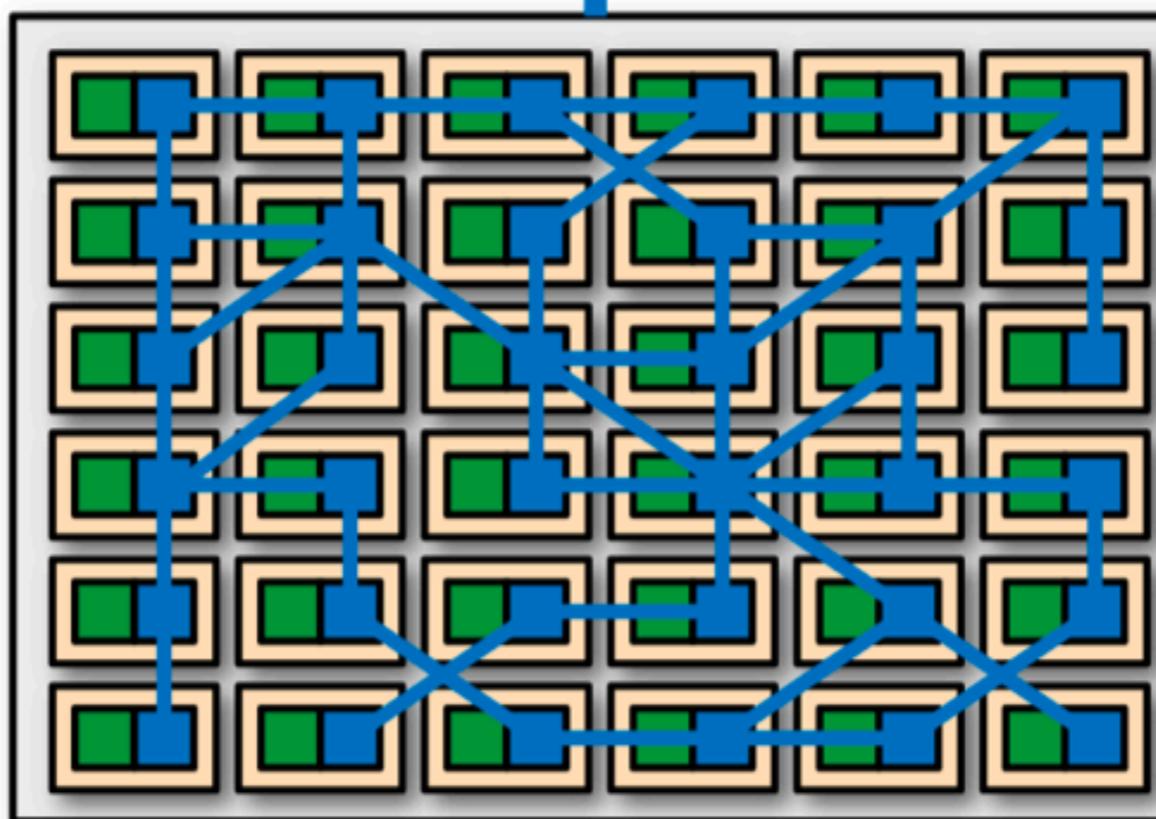


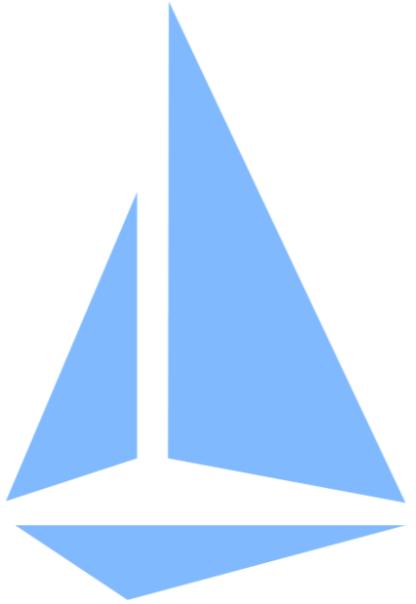
Control and data plane

Control plane



Data plane

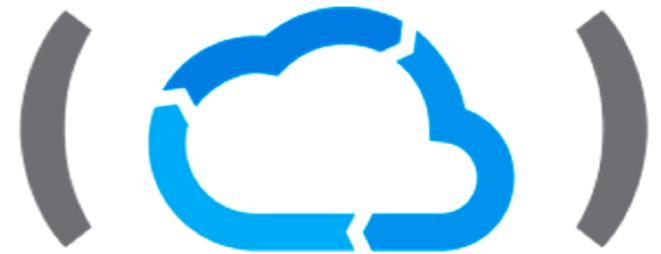




Istio



linkerd



OPENCONTRAIL



Welcome to Istio



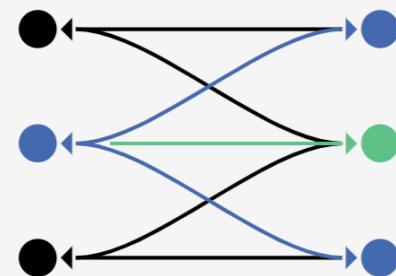
Istio

Docs Blog FAQ About



Istio

Connect, secure, control, and observe services.



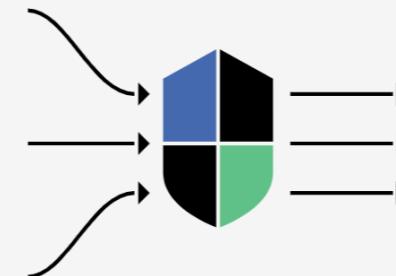
Connect

Intelligently control the flow of traffic and API calls between services, conduct a range of tests, and upgrade gradually with red/black deployments.



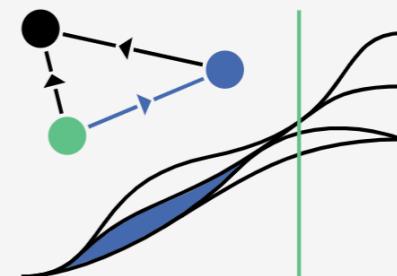
Secure

Automatically secure your services through managed authentication, authorization, and encryption of communication between



Control

Apply policies and ensure that they're enforced, and that resources are fairly distributed among consumers.



Observe

See what's happening with rich automatic tracing, monitoring, and logging of all your services.

<https://istio.io/>



© 2017 - 2018 Siam Chamnankit Company Limited. All rights reserved.

Kafka, Redis, ELK

277

Welcome to Istio

Control plane for service mesh

Abstracts Envoy's concepts and configurations

Easy to operate (kubectl and istioctl)

HTTP 2, including gRPC

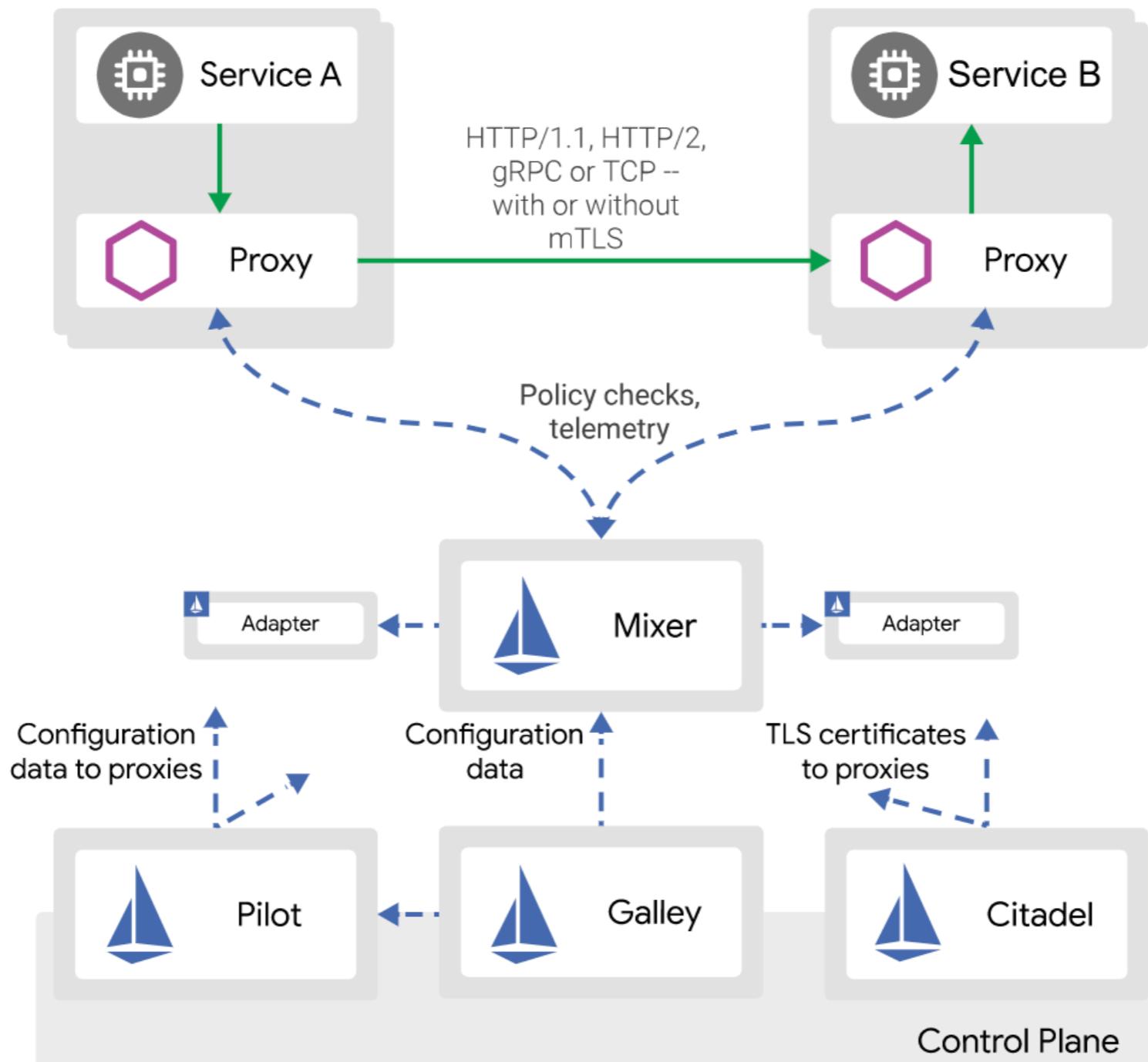
Service discovery/registry and health check

Advanced load balancing

Stat, metrics and tracing



Istio Architecture

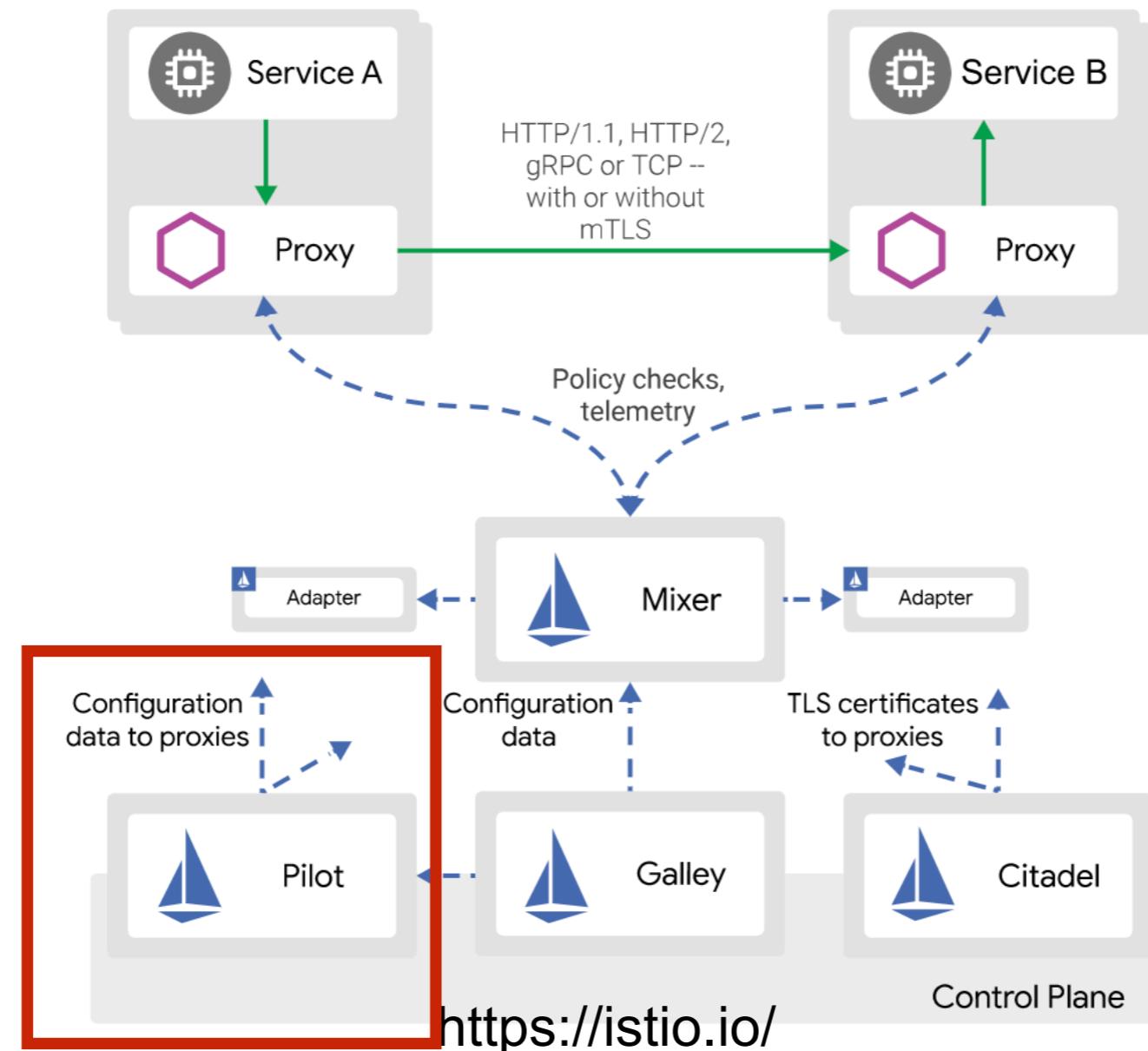


<https://istio.io/>



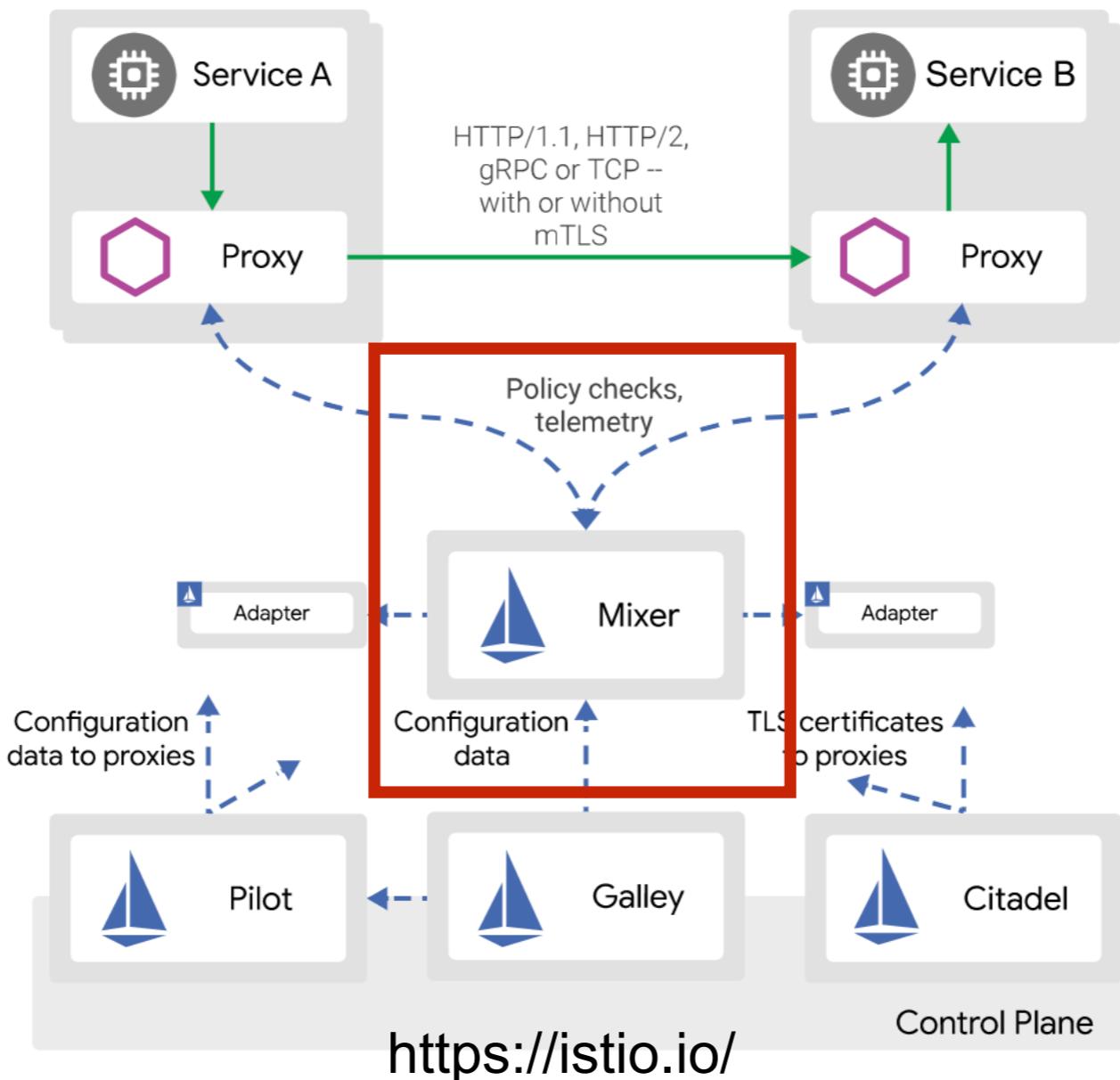
Pilot

Traffic control (route rules and policies)
Resiliency (circuit breaker, timeout and retry)



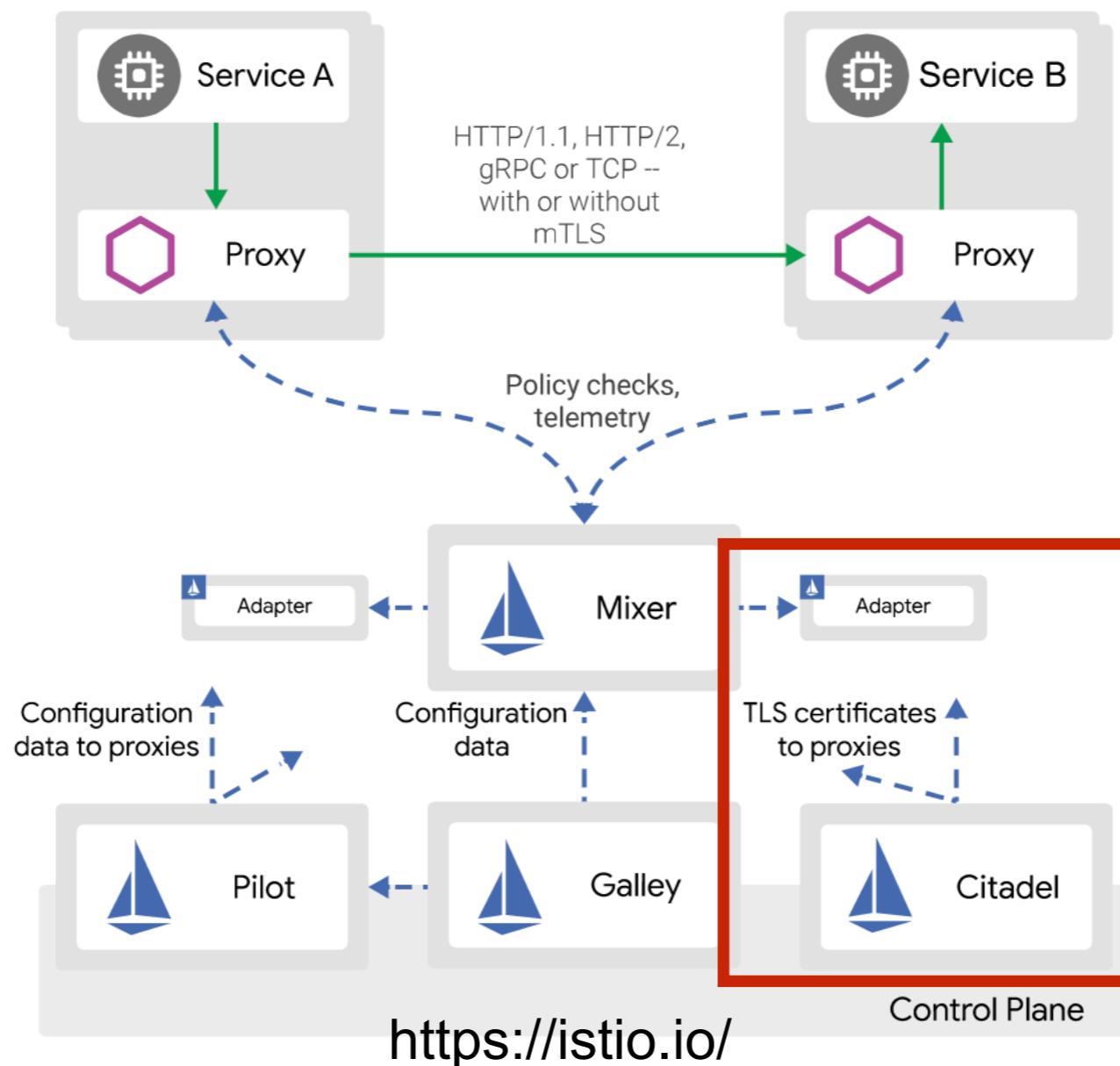
Mixer

API management
Telemetry, tracing and integration with others



Citadel

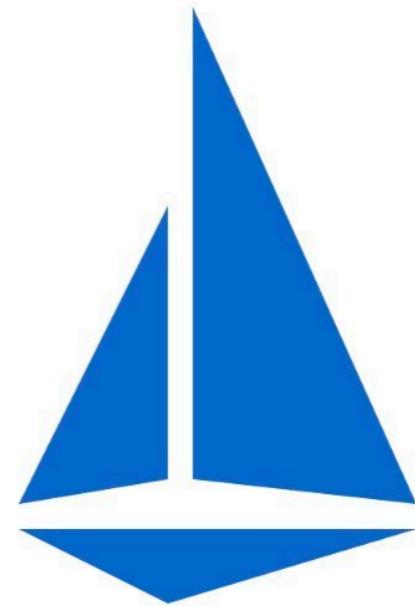
Enforce mTLS between services
Along with mixer and pilot allows authorization & audit



Istio workshop



kubernetes



ISTIO

