PowMio LAB

Richard Hoepken, 13.03.2025

PowMio

Elastic Stack

Software quality assurance with modern log management

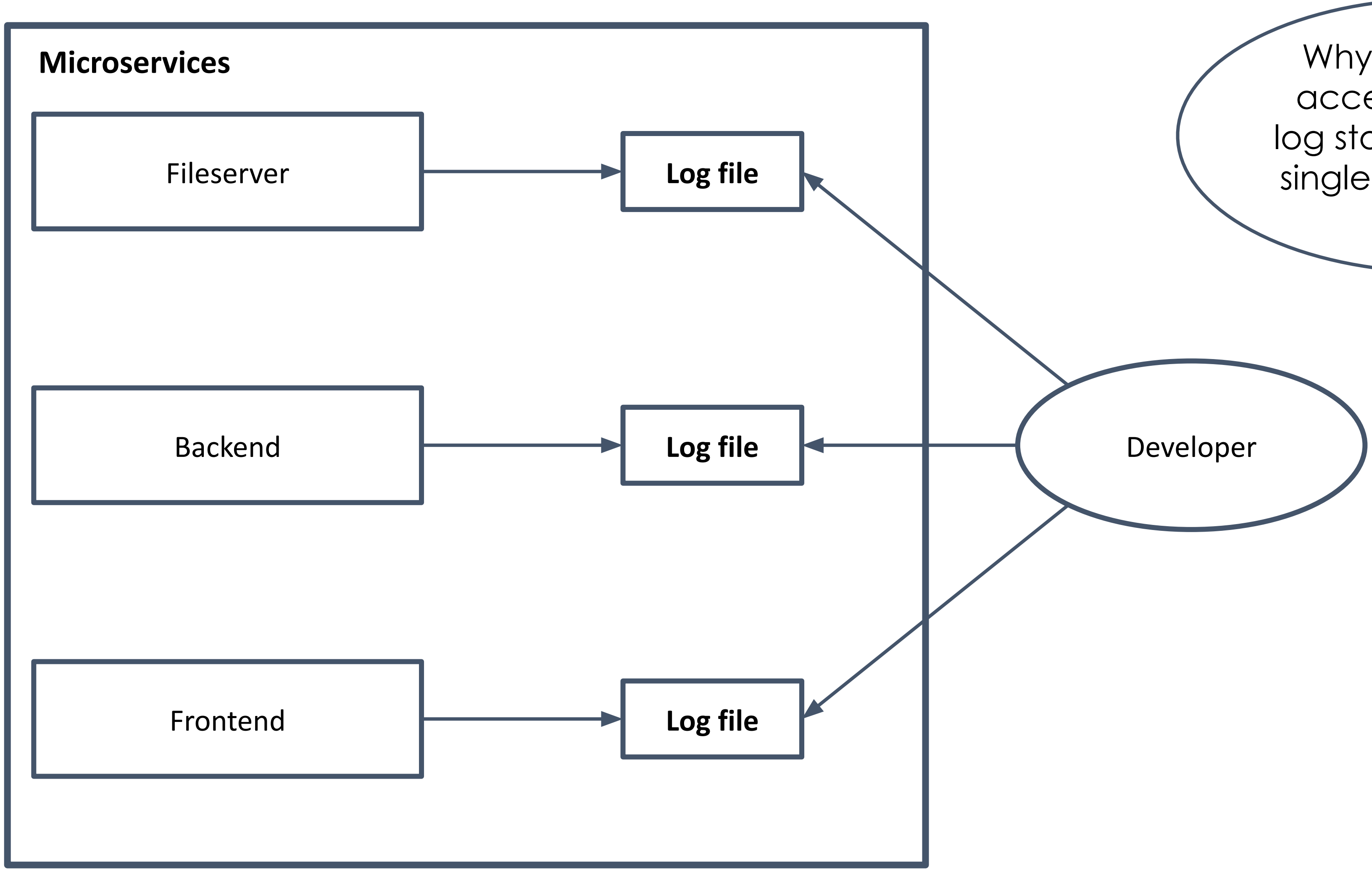
Software is much more than code.

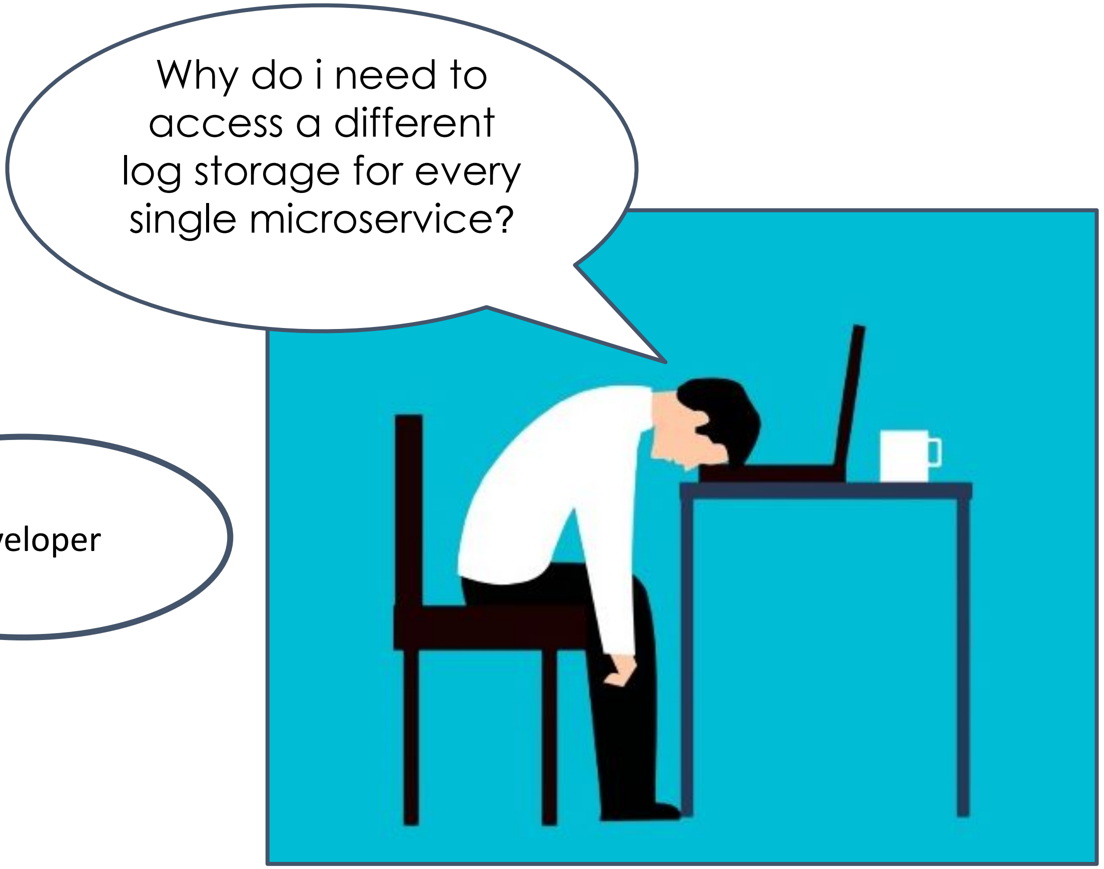
Content

- The problem - Chaotic log data madness
- The solution - Structured log data
- The elastic stack - Gather, structure, analyse
- Alternatives - Grafana stack and more
- Conclusion - Use Cases and Summary

The problem

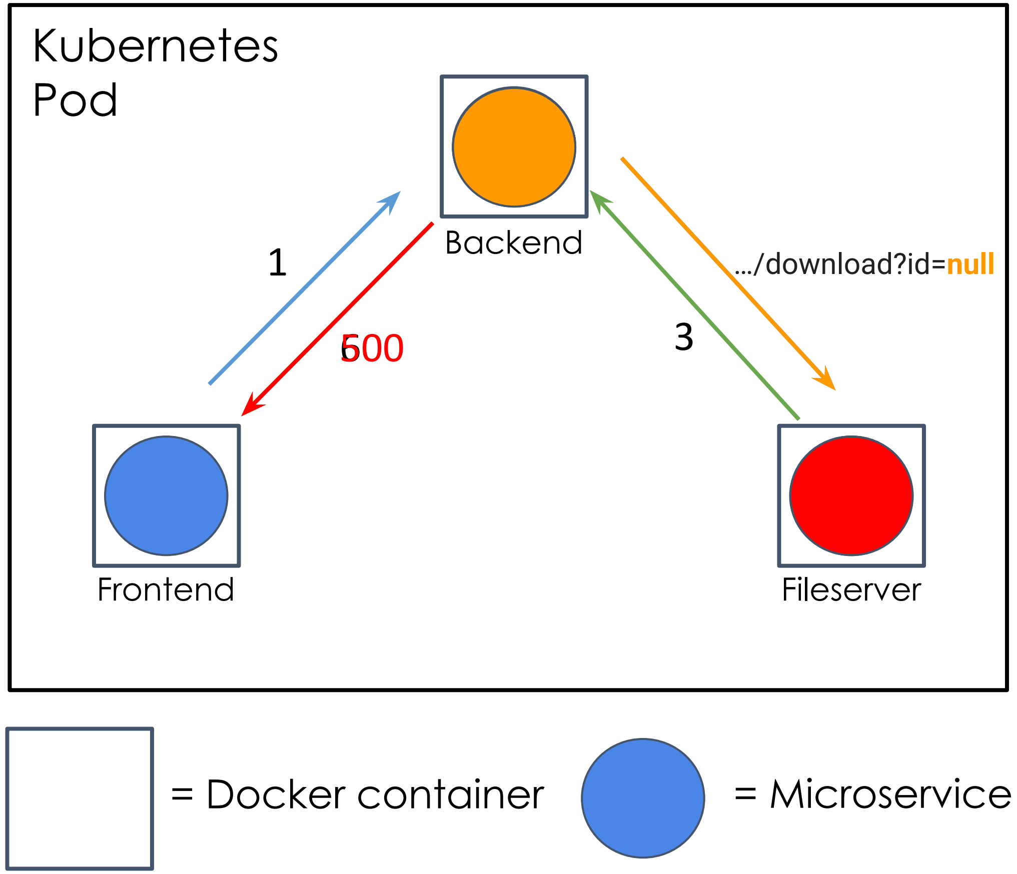
The problem




Why do i need to access a different log storage for every single microservice?

Source:https://pxhere.com/de/photo/1638940?utm_content=shareClip&utm_medium=referral&utm_source=pxhere

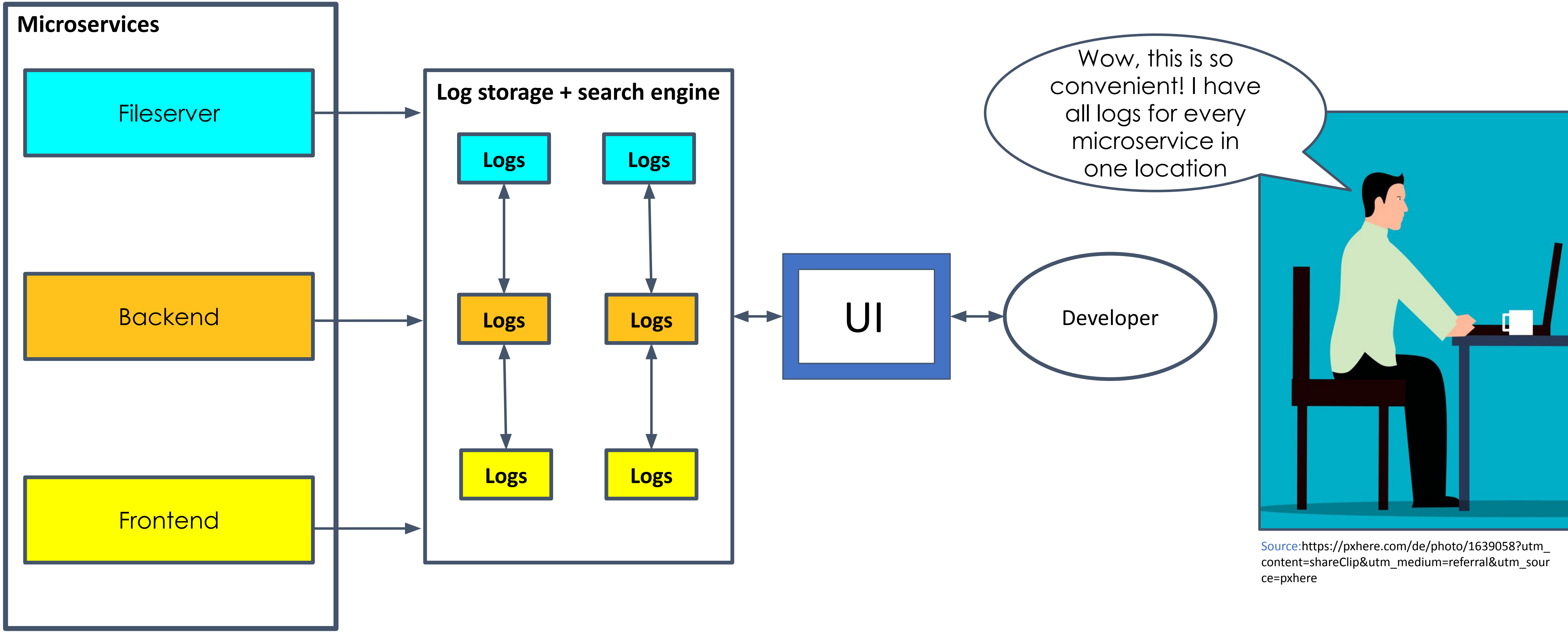
Problem example



- Developers have **no information** about
  - Location where error was thrown
  - Events that are related to the error
- Developers need to **check every Microservice log file** of every Docker container to find the error
- Developers need to **manually reconstruct** to the error related logs

The solution

The solution principle



Microservices

Fileserver

Backend

Frontend

Log storage + search engine

Logs **Logs**

Logs **Logs**

Logs **Logs**

UI

Developer

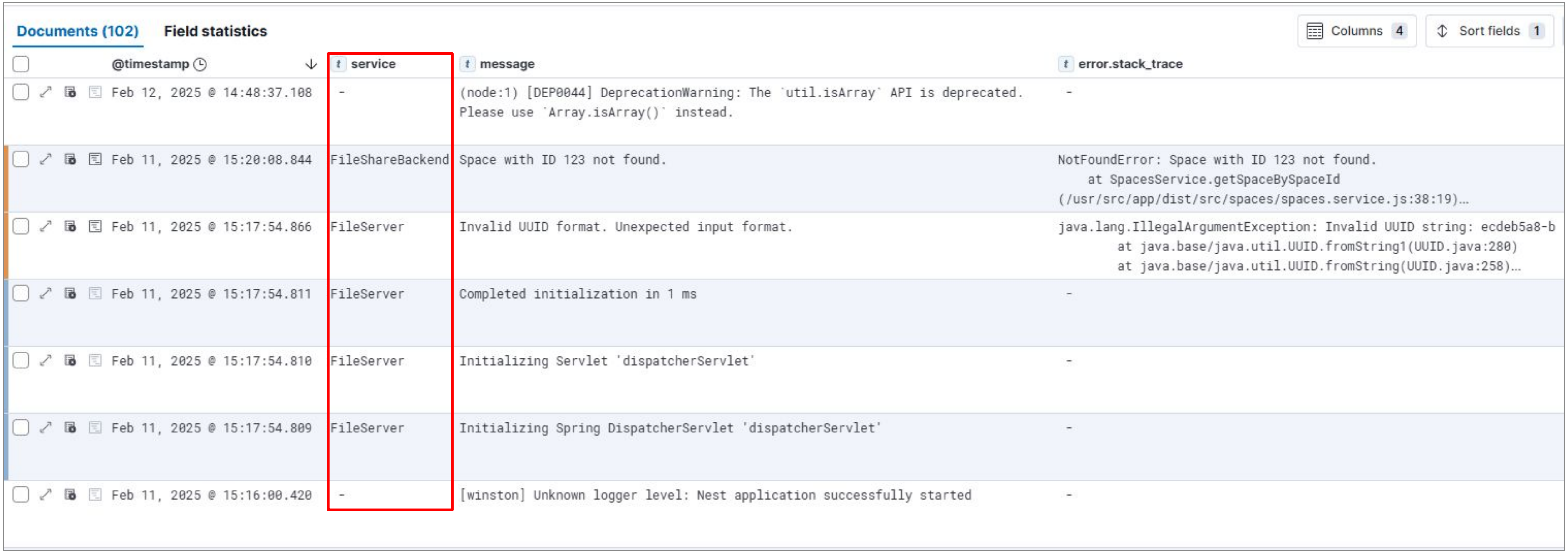
Wow, this is so convenient! I have all logs for every microservice in one location

Source:https://pxhere.com/de/photo/1639058?utm_content=shareClip&utm_medium=referral&utm_source=pxhere

The objective

- We want…
  - **one location**, where logs can be accessed and **analysed**
  - to see which logs belong to the same API request **(Log Correlation)**
- For log **analysis** we need…
  - to **transform** and **structure** logs
  - to **visualize** and **filter** logs

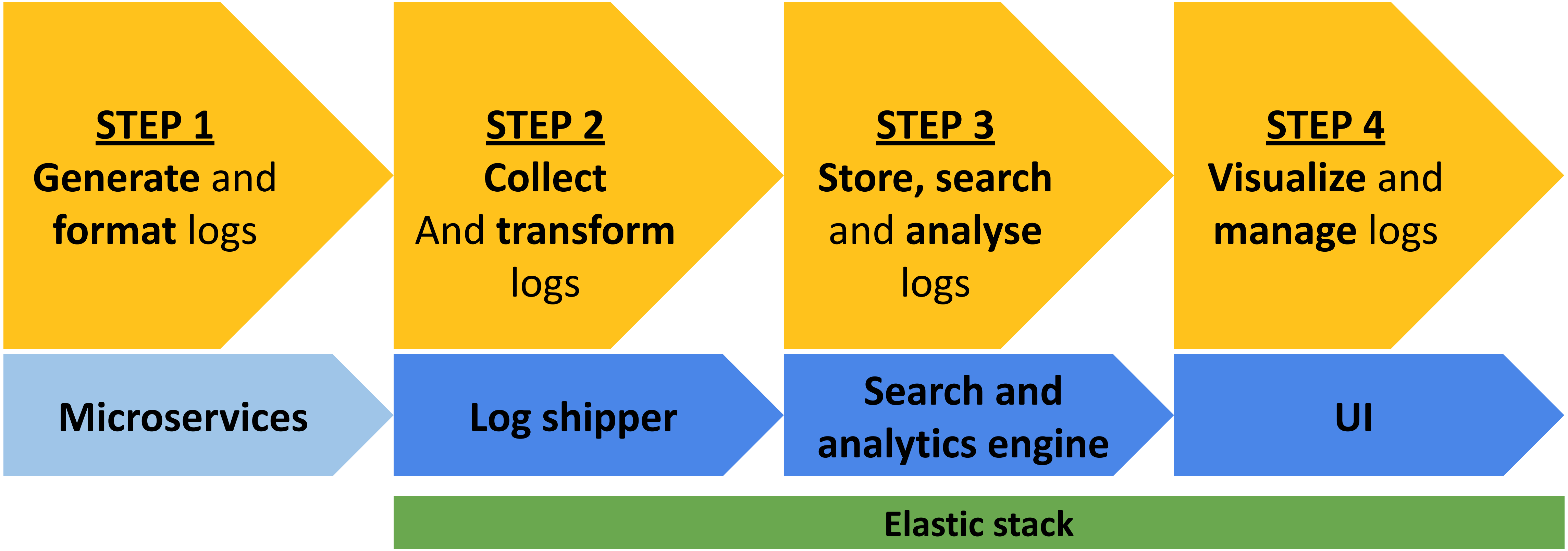
Desired dev experience



@timestamp	service	message	error.stack_trace
Feb 12, 2025 @ 14:48:37.108	-	(node:1) [DEP0044] DeprecationWarning: The `util.isArray` API is deprecated. Please use `Array.isArray()` instead.	-
Feb 11, 2025 @ 15:20:08.844	FileShareBackend	Space with ID 123 not found.	NotFoundError: Space with ID 123 not found. at SpacesService.getSpaceBySpaceId (/usr/src/app/dist/src/spaces/spaces.service.js:38:19)...
Feb 11, 2025 @ 15:17:54.866	FileServer	Invalid UUID format. Unexpected input format.	java.lang.IllegalArgumentException: Invalid UUID string: ecdeb5a8-b at java.base/java.util.UUID.fromString1(UUID.java:280) at java.base/java.util.UUID.fromString(UUID.java:258)...
Feb 11, 2025 @ 15:17:54.811	FileServer	Completed initialization in 1 ms	-
Feb 11, 2025 @ 15:17:54.810	FileServer	Initializing Servlet 'dispatcherServlet'	-
Feb 11, 2025 @ 15:17:54.809	FileServer	Initializing Spring DispatcherServlet 'dispatcherServlet'	-
Feb 11, 2025 @ 15:16:00.420	-	[winston] Unknown logger level: Nest application successfully started	-

The elastic stack

Elastic stack workflow



STEP 1
Generate and **format** logs

STEP 2
Collect
And **transform** logs

STEP 3
Store, search and **analyse** logs

STEP 4
Visualize and **manage** logs

Microservices

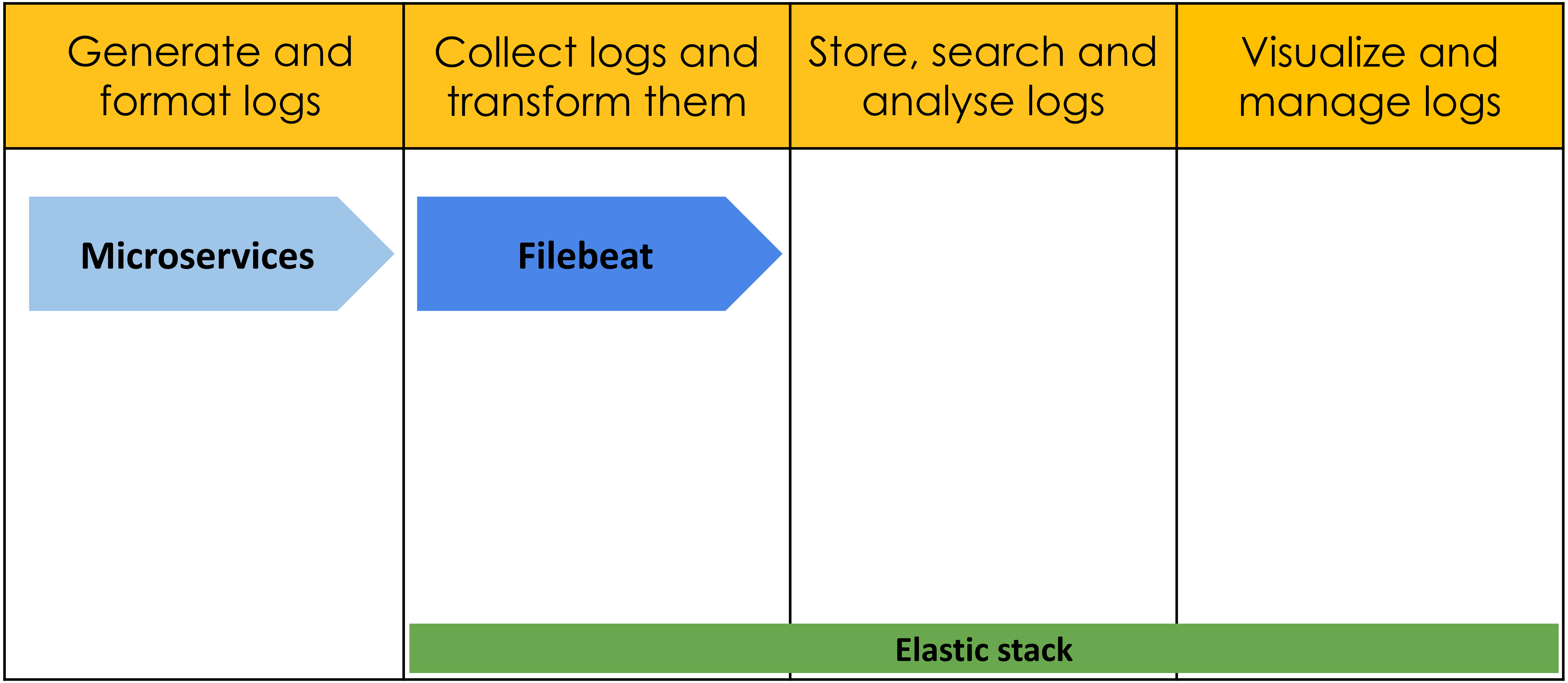
Log shipper

Search and analytics engine

UI

Elastic stack

Elastic stack layers

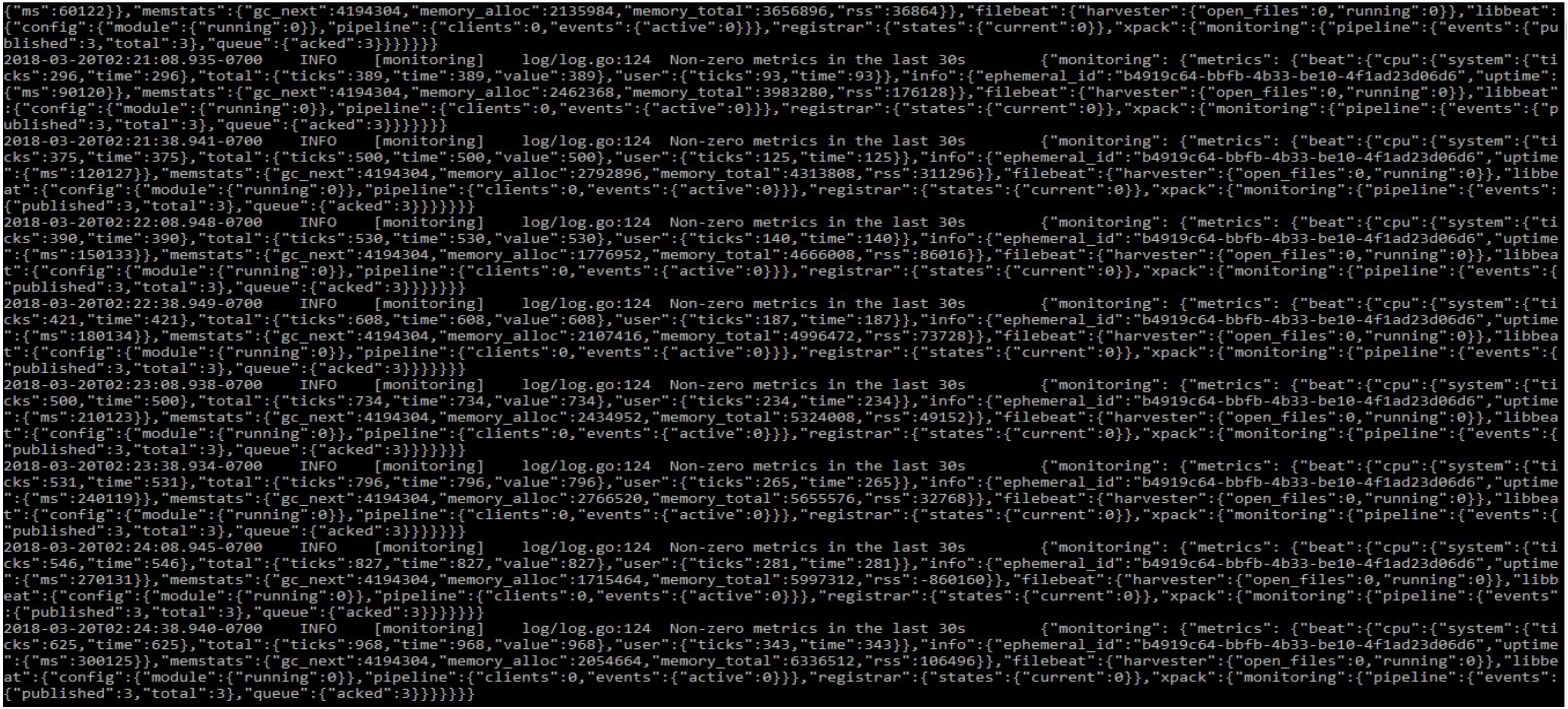


Generate and format logs	Collect logs and transform them	Store, search and analyse logs	Visualize and manage logs
Microservices	**Filebeat**		
	Elastic stack		

Filebeat

- Takes care of **log collection** and **transformation**
- **Log collection**: Filebeat gathers every log from every microservice
- **Transformation**: Filebeat can perform basic transformations like decoding json or basic filtering

Filebeat logs



```
{"ms":60122}},"memstats":{"gc_next":4194304,"memory_alloc":2135984,"memory_total":3656896,"rss":36864}},"filebeat":{"harvester":{"open_files":0,"running":0}},"libbeat":
{"config":{"module":{"running":0}},"pipeline":{"clients":0,"events":{"active":0}}},"registrar":{"states":{"current":0}},"xpack":{"monitoring":{"pipeline":{"events":{"pu
blished":3,"total":3},"queue":{"acked":3}}}}}}}
2018-03-20T02:21:08.935-0700    INFO    [monitoring]    log/log.go:124  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ti
cks":296,"time":296},"total":{"ticks":389,"time":389,"value":389},"user":{"ticks":93,"time":93}},"info":{"ephemeral_id":"b4919c64-bbfb-4b33-be10-4f1ad23d06d6","uptime":
{"ms":90120}},"memstats":{"gc_next":4194304,"memory_alloc":2462368,"memory_total":3983280,"rss":176128}},"filebeat":{"harvester":{"open_files":0,"running":0}},"libbeat"
:{"config":{"module":{"running":0}},"pipeline":{"clients":0,"events":{"active":0}}},"registrar":{"states":{"current":0}},"xpack":{"monitoring":{"pipeline":{"events":{"p
ublished":3,"total":3},"queue":{"acked":3}}}}}}}
2018-03-20T02:21:38.941-0700    INFO    [monitoring]    log/log.go:124  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ti
cks":375,"time":375},"total":{"ticks":500,"time":500,"value":500},"user":{"ticks":125,"time":125}},"info":{"ephemeral_id":"b4919c64-bbfb-4b33-be10-4f1ad23d06d6","uptime
":{"ms":120127}},"memstats":{"gc_next":4194304,"memory_alloc":2792896,"memory_total":4313808,"rss":311296}},"filebeat":{"harvester":{"open_files":0,"running":0}},"libbe
at":{"config":{"module":{"running":0}},"pipeline":{"clients":0,"events":{"active":0}}},"registrar":{"states":{"current":0}},"xpack":{"monitoring":{"pipeline":{"events":
{"published":3,"total":3},"queue":{"acked":3}}}}}}}
2018-03-20T02:22:08.948-0700    INFO    [monitoring]    log/log.go:124  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ti
cks":390,"time":390},"total":{"ticks":530,"time":530,"value":530},"user":{"ticks":140,"time":140}},"info":{"ephemeral_id":"b4919c64-bbfb-4b33-be10-4f1ad23d06d6","uptime
":{"ms":150133}},"memstats":{"gc_next":4194304,"memory_alloc":1776952,"memory_total":4666008,"rss":86016}},"filebeat":{"harvester":{"open_files":0,"running":0}},"libbea
t":{"config":{"module":{"running":0}},"pipeline":{"clients":0,"events":{"active":0}}},"registrar":{"states":{"current":0}},"xpack":{"monitoring":{"pipeline":{"events":{
"published":3,"total":3},"queue":{"acked":3}}}}}}}
2018-03-20T02:22:38.949-0700    INFO    [monitoring]    log/log.go:124  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ti
cks":421,"time":421},"total":{"ticks":608,"time":608,"value":608},"user":{"ticks":187,"time":187}},"info":{"ephemeral_id":"b4919c64-bbfb-4b33-be10-4f1ad23d06d6","uptime
":{"ms":180134}},"memstats":{"gc_next":4194304,"memory_alloc":2107416,"memory_total":4996472,"rss":73728}},"filebeat":{"harvester":{"open_files":0,"running":0}},"libbea
t":{"config":{"module":{"running":0}},"pipeline":{"clients":0,"events":{"active":0}}},"registrar":{"states":{"current":0}},"xpack":{"monitoring":{"pipeline":{"events":{
"published":3,"total":3},"queue":{"acked":3}}}}}}}
2018-03-20T02:23:08.938-0700    INFO    [monitoring]    log/log.go:124  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ti
cks":500,"time":500},"total":{"ticks":734,"time":734,"value":734},"user":{"ticks":234,"time":234}},"info":{"ephemeral_id":"b4919c64-bbfb-4b33-be10-4f1ad23d06d6","uptime
":{"ms":210123}},"memstats":{"gc_next":4194304,"memory_alloc":2434952,"memory_total":5324008,"rss":49152}},"filebeat":{"harvester":{"open_files":0,"running":0}},"libbea
t":{"config":{"module":{"running":0}},"pipeline":{"clients":0,"events":{"active":0}}},"registrar":{"states":{"current":0}},"xpack":{"monitoring":{"pipeline":{"events":{
"published":3,"total":3},"queue":{"acked":3}}}}}}}
2018-03-20T02:23:38.934-0700    INFO    [monitoring]    log/log.go:124  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ti
cks":531,"time":531},"total":{"ticks":796,"time":796,"value":796},"user":{"ticks":265,"time":265}},"info":{"ephemeral_id":"b4919c64-bbfb-4b33-be10-4f1ad23d06d6","uptime
":{"ms":240119}},"memstats":{"gc_next":4194304,"memory_alloc":2766520,"memory_total":5655576,"rss":32768}},"filebeat":{"harvester":{"open_files":0,"running":0}},"libbea
t":{"config":{"module":{"running":0}},"pipeline":{"clients":0,"events":{"active":0}}},"registrar":{"states":{"current":0}},"xpack":{"monitoring":{"pipeline":{"events":{
"published":3,"total":3},"queue":{"acked":3}}}}}}}
2018-03-20T02:24:08.945-0700    INFO    [monitoring]    log/log.go:124  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ti
cks":546,"time":546},"total":{"ticks":827,"time":827,"value":827},"user":{"ticks":281,"time":281}},"info":{"ephemeral_id":"b4919c64-bbfb-4b33-be10-4f1ad23d06d6","uptime
":{"ms":270131}},"memstats":{"gc_next":4194304,"memory_alloc":1715464,"memory_total":5997312,"rss":-860160}},"filebeat":{"harvester":{"open_files":0,"running":0}},"libb
eat":{"config":{"module":{"running":0}},"pipeline":{"clients":0,"events":{"active":0}}},"registrar":{"states":{"current":0}},"xpack":{"monitoring":{"pipeline":{"events"
:{"published":3,"total":3},"queue":{"acked":3}}}}}}}
2018-03-20T02:24:38.940-0700    INFO    [monitoring]    log/log.go:124  Non-zero metrics in the last 30s        {"monitoring": {"metrics": {"beat":{"cpu":{"system":{"ti
cks":625,"time":625},"total":{"ticks":968,"time":968,"value":968},"user":{"ticks":343,"time":343}},"info":{"ephemeral_id":"b4919c64-bbfb-4b33-be10-4f1ad23d06d6","uptime
":{"ms":300125}},"memstats":{"gc_next":4194304,"memory_alloc":2054664,"memory_total":6336512,"rss":106496}},"filebeat":{"harvester":{"open_files":0,"running":0}},"libbe
at":{"config":{"module":{"running":0}},"pipeline":{"clients":0,"events":{"active":0}}},"registrar":{"states":{"current":0}},"xpack":{"monitoring":{"pipeline":{"events":
{"published":3,"total":3},"queue":{"acked":3}}}}}}}
```

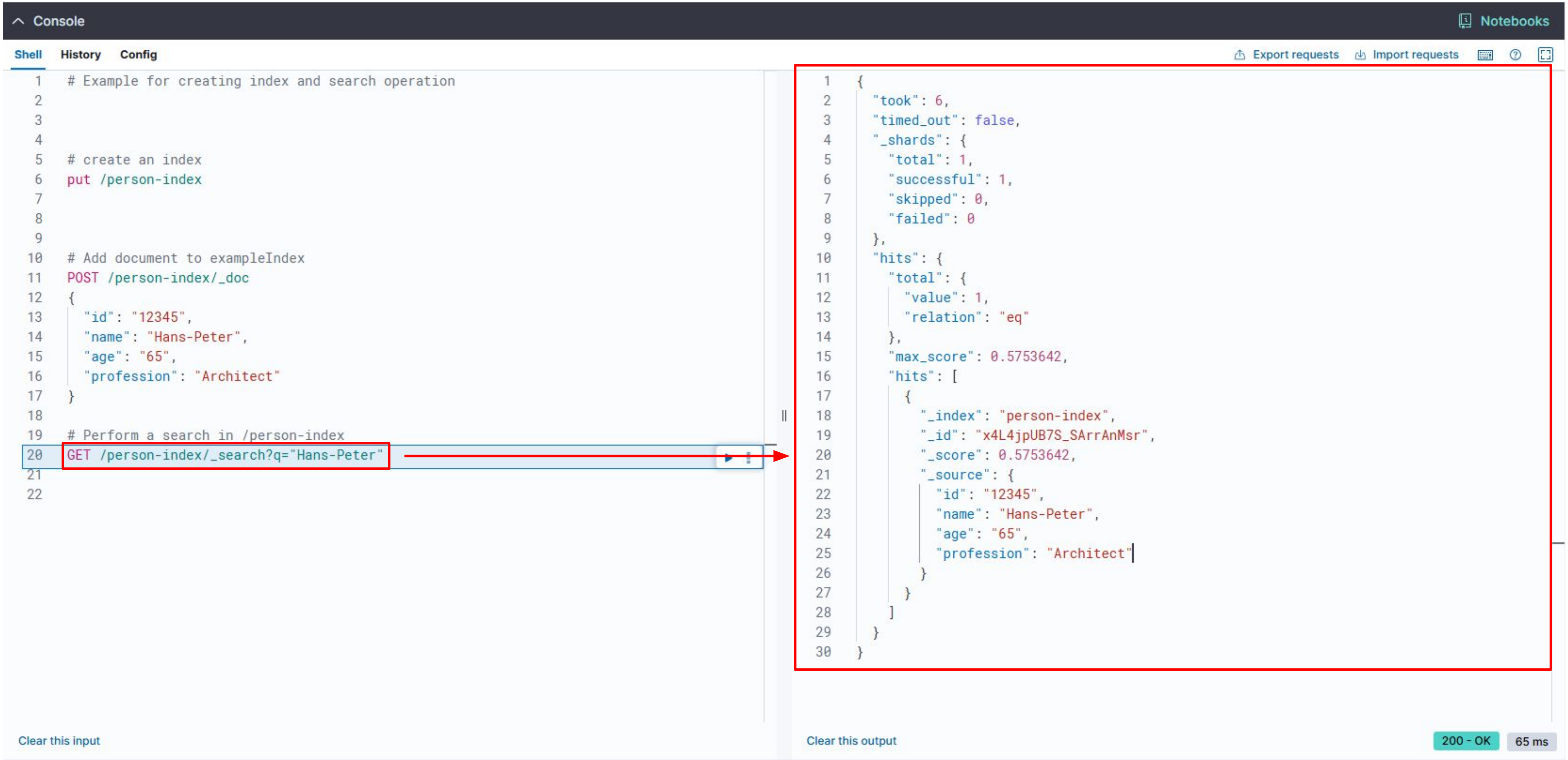
Elastic stack layers

<table>
<tr><th>Generate and format logs</th><th>Collect logs and transform them</th><th>Store, search and analyse logs</th><th>Visualize and manage logs</th></tr>
<tr><td><b>Microservices</b></td><td><b>Filebeat</b></td><td><b>Elasticsearch</b></td><td></td></tr>
<tr><td></td><td colspan="3"><b>Elastic stack</b></td></tr>
</table>

Elasticsearch

- Takes care of **log storage**, **search** and **analysation**
- **Log storage**: Elasticsearch stores logs for performance reasons and log persistence
- **Search**: Elasticsearch uses a specific data model called indices, which optimizes log filtering and searching
- **Analysation**: Faster filtering and aggregation of logs enables a faster analysation of logs

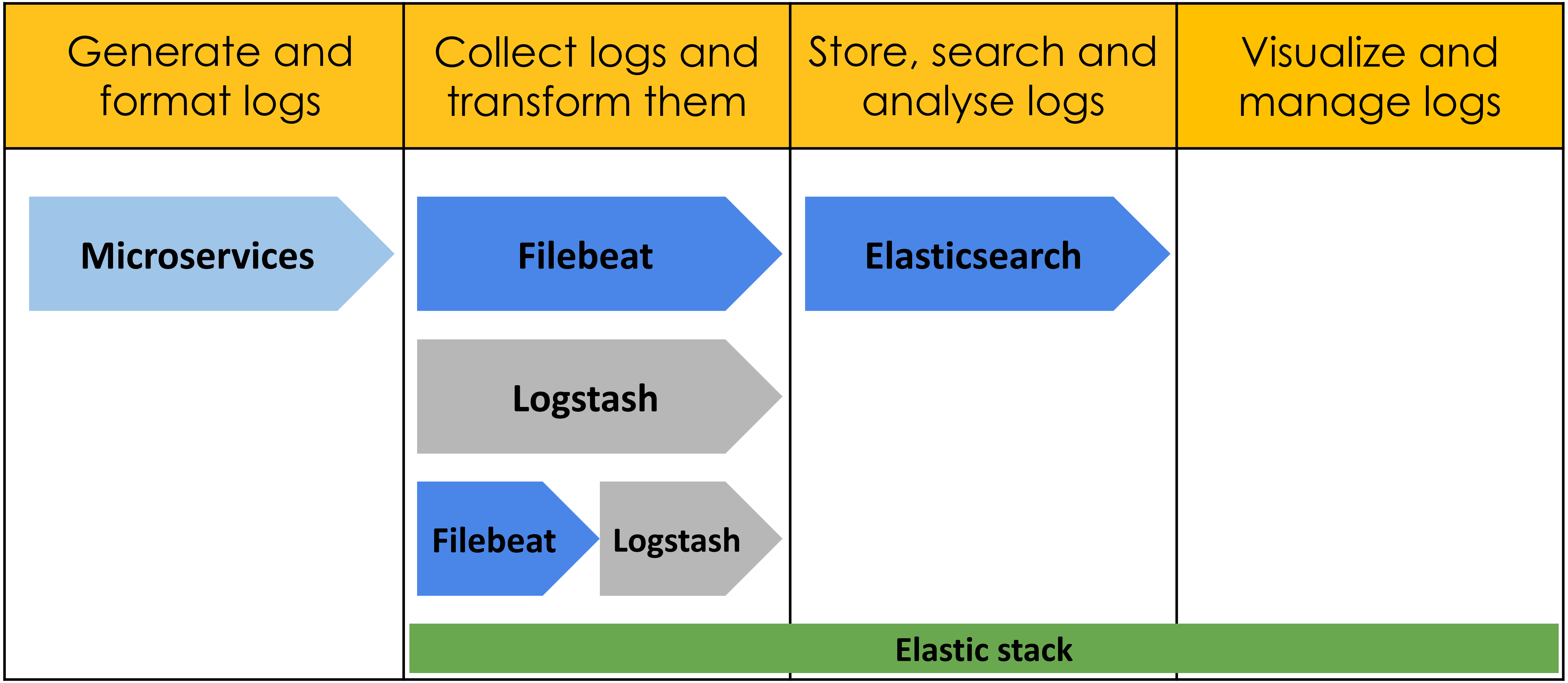
Elasticsearch logs



```
# Example for creating index and search operation



# create an index
put /person-index



# Add document to exampleIndex
POST /person-index/_doc
{
  "id": "12345",
  "name": "Hans-Peter",
  "age": "65",
  "profession": "Architect"
}

# Perform a search in /person-index
GET /person-index/_search?q="Hans-Peter"
```

```
{
  "took": 6,
  "timed_out": false,
  "_shards": {
    "total": 1,
    "successful": 1,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": {
      "value": 1,
      "relation": "eq"
    },
    "max_score": 0.5753642,
    "hits": [
      {
        "_index": "person-index",
        "_id": "x4L4jpUB7S_SArrAnMsr",
        "_score": 0.5753642,
        "_source": {
          "id": "12345",
          "name": "Hans-Peter",
          "age": "65",
          "profession": "Architect"
        }
      }
    ]
  }
}
```

Elastic stack layers



Generate and format logs	Collect logs and transform them	Store, search and analyse logs	Visualize and manage logs
Microservices	Filebeat	Elasticsearch	
	Logstash		
	Filebeat Logstash		
	Elastic stack		

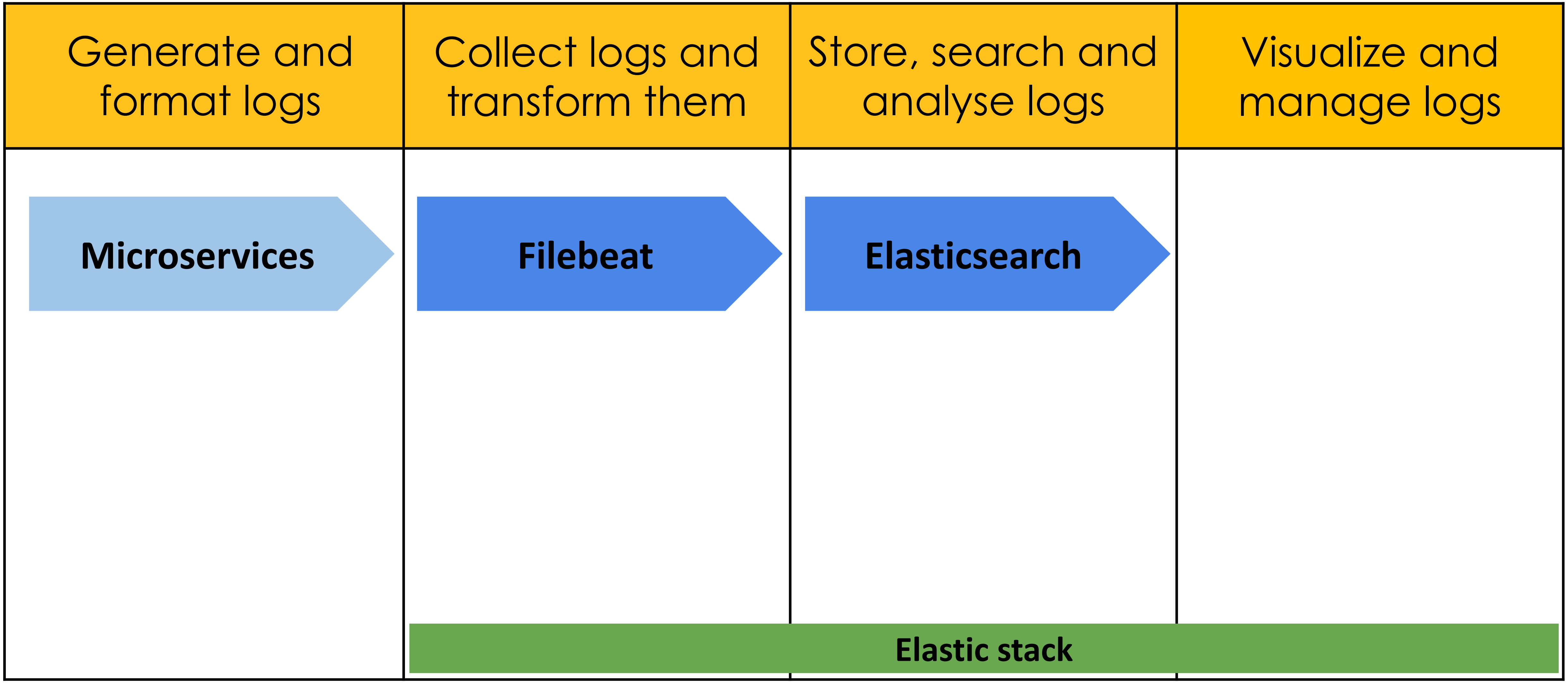
Logstash

- Can be used **instead** or **together** with filebeat
  - Instead: Takes care of log **collection** and **transformation**
  - Together: **Filebeat** takes care of **log collection**, **logstash** takes care of **log transformation**
- **More options** than filebeat but needs **more resources** as well
- Use logstash for **complexity**, use filebeat for **performance**
- Use them together if you need a lightweight log collector but more complex log transformations

Filebeat vs Logstash

Feature	Filebeat	Logstash
Type	Lightweight log shipper	Heavyweight data pipeline
Resource Consumption	Very low	Higher (CPU and RAM intensive)
Data Sources (Collecting)	Reads logs from files, JournalD, Syslog, Docker	Supports more sources: Databases, APIs, Beats, TCP, UDP
Data Processing (Transforming)	Simple (JSON decoding, basic filtering)	Advanced (Mutations, GeoIP, DNS resolution, aggregations)

Elastic stack layers



Generate and format logs	Collect logs and transform them	Store, search and analyse logs	Visualize and manage logs
Microservices	Filebeat	Elasticsearch	
	Elastic stack		

Not using a log collector

- You can send logs directly to elasticsearch (e.g logger configuration)
- Simpler architecture → easier maintenance and setup
- Better performance
- Own implementations for collecting and transforming logs
- No log caching in case of connection issues with Elasticsearch

Elastic stack layers

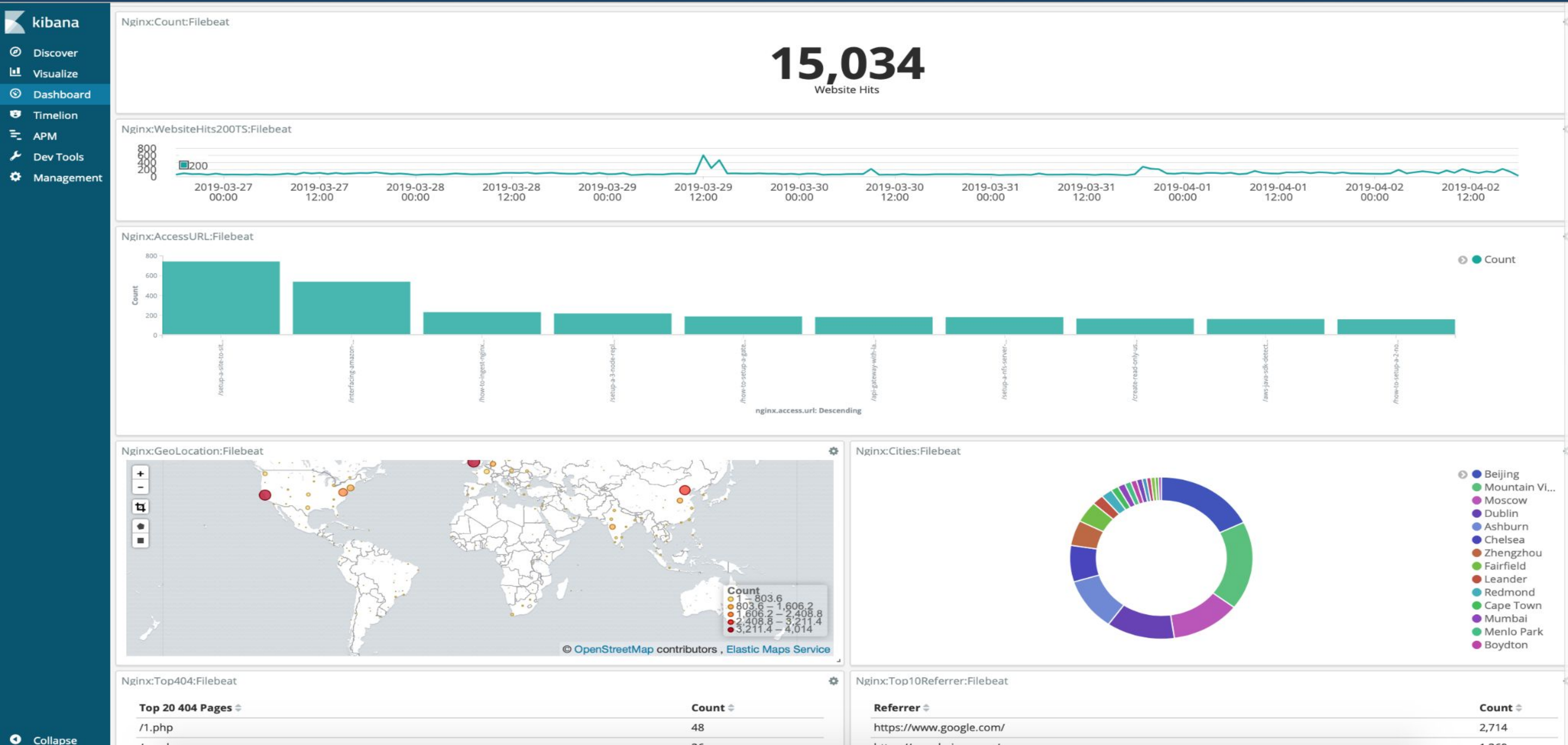
Generate and format logs	Collect logs and transform them	Store, search and analyse logs	Visualize and manage logs
Microservices	Filebeat	Elasticsearch	Kibana
	Elastic stack		

Kibana

- Powerful UI, which takes care of log **visualisation** and **management**
- **Visualisation**: Kibana dashboard provides multiple visualisation options from charts over maps and more
- **Management**: Because kibana works as UI for elasticsearch, it has many log managing functionalities like index management or index lifecycle management

PowMio

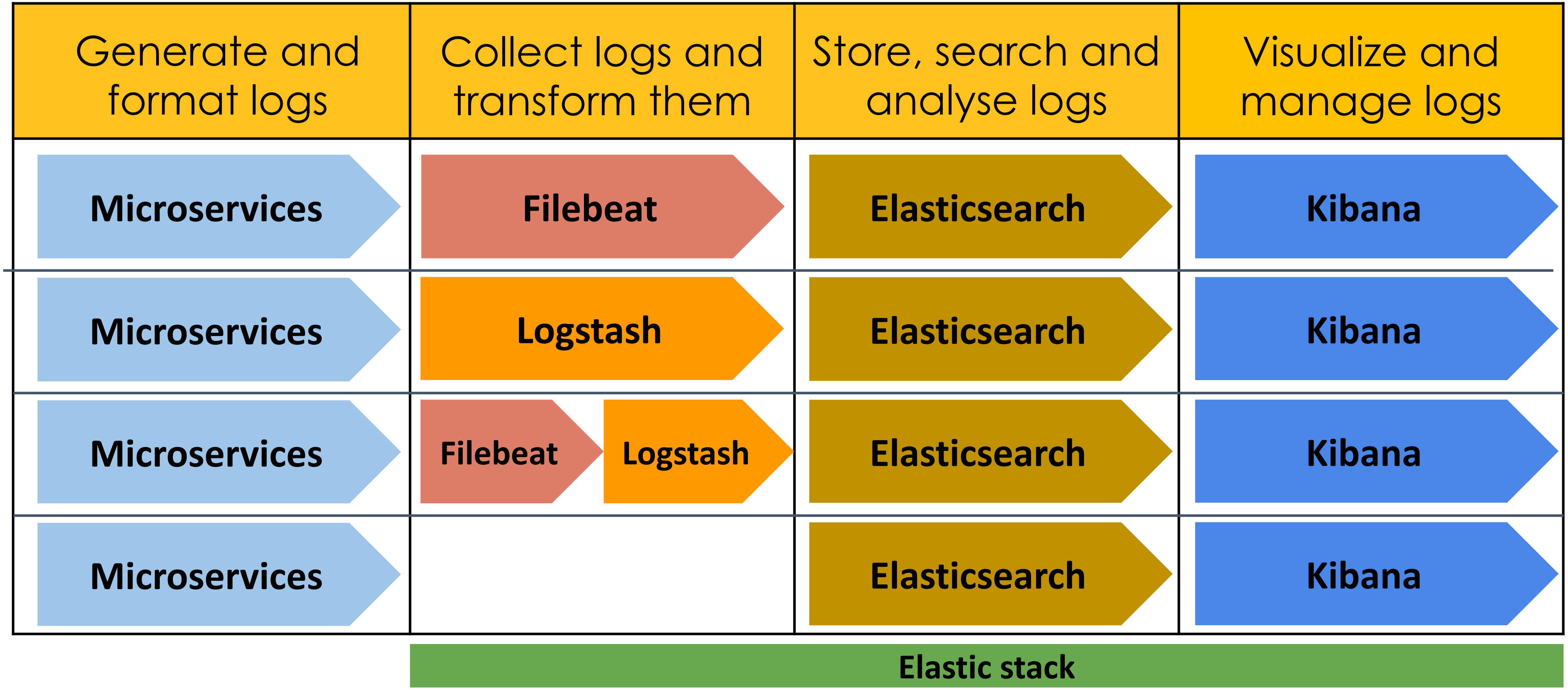
Kibana dashboards



Top 20 404 Pages	Count
/1.php	48

Referrer	Count
https://www.google.com/	2,714

Elastic stack layer options



Generate and format logs	Collect logs and transform them	Store, search and analyse logs	Visualize and manage logs
Microservices	Filebeat	Elasticsearch	Kibana
Microservices	Logstash	Elasticsearch	Kibana
Microservices	Filebeat Logstash	Elasticsearch	Kibana
Microservices		Elasticsearch	Kibana

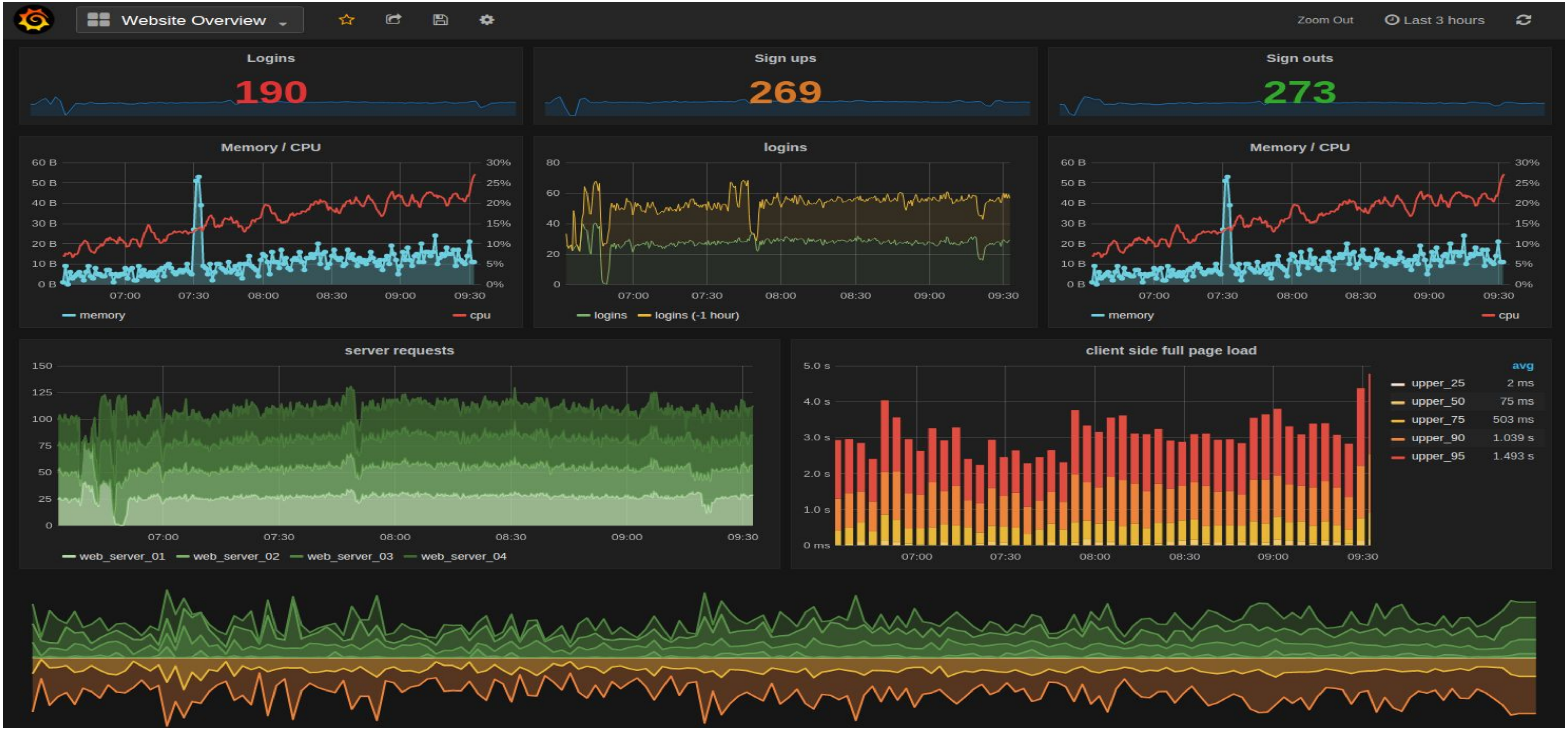
Elastic stack

Alternatives

Alternatives

- FluentD/Promtail ⇒ Loki ⇒ Grafana
  - Lightweight version of the elastic stack
  - Uses less resources
  - Easier to implement and run
  - Less powerful
- Cloud based alternatives
  - Datadog
  - New Relic
  - Azure Monitor
- Database based alternatives
  - Redash
  - Metabase

Grafana Example



Source: https://commons.wikimedia.org/wiki/File:Grafana_dashboard.png

Conclusion

When to use elastic stack

- **Elastic stack checklist:**
  - Complex systems/applications
  - High log flow
  - Many microservices or complex Microservice architecture
  - Demand for log visualisation and/or management
  - High demand on system stability and reliability
- There is **no need** for elastic stack if…
  - Server resources are scarce
  - Not a single point on the **elastic stack checklist** is fulfilled

Summary

- **The Problem:** Logs are scattered over multiple locations and do not possess a clean structure
- **The Solution:** Collect and structure logs so they are easier to access and read
- **Elastic Stack:** Consisting of three components
  - Filebeat/Logstash: Collects and Transforms logs
  - Elasticsearch: stores, searches and analyses logs
  - Kibana: Visualizes and manages logs
- **Alternatives:**
  - Grafana stack
  - Cloud based, database based

Thank you!

PowMio

Alter Schlachthof 33
76131 Karlsruhe

www.powmio.com

contact@powmio.com