The troubles with monitoring your K8s cluster & what to look out for

The importance of monitoring a microservices-based applications

PAYBASE_

Monitoring is important right?

Insert cool monitoring example


“The sun was starting to dip, turning the sky a brilliant orange hue.
Then the ground shook.”
“It felt more powerful than those in recent memory.”

When monitoring is done right

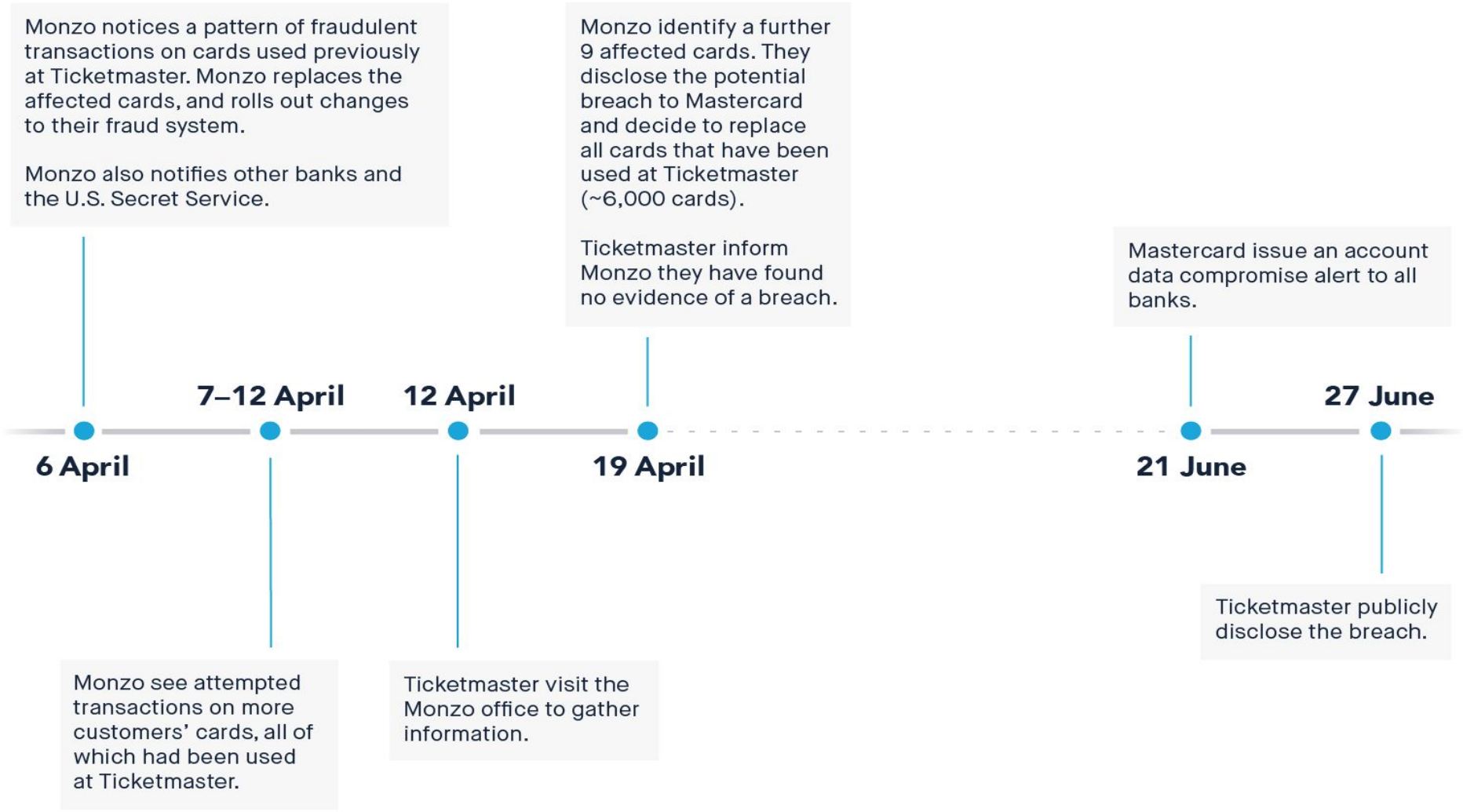


Table of Contents

Monitoring...

“...something we perform against our applications and systems to determine their state. From basic fitness tests and whether they’re up or down, to more proactive performance health checks. We monitor applications to detect problems and anomalies. “

Monitoring ...

- ✓ **“Monitoring”** is used as an umbrella term for operational visibility. You have a set of automated checks that run against systems to ensure none of those things that signify trouble are happening (in any of the ways you predicted).

Monitoring a microservices application

Microservices-based applications have different, and more intensive, monitoring requirements.

- ✓ a process is distributed between many separate services
- ✓ all systems fail
- ✓ reliability and availability - in other words SLAs
- ✓ monitoring systems can alert operators to degraded states before failures happen
- ✓ failure of a dependency will result in upstream effects on overall throughput

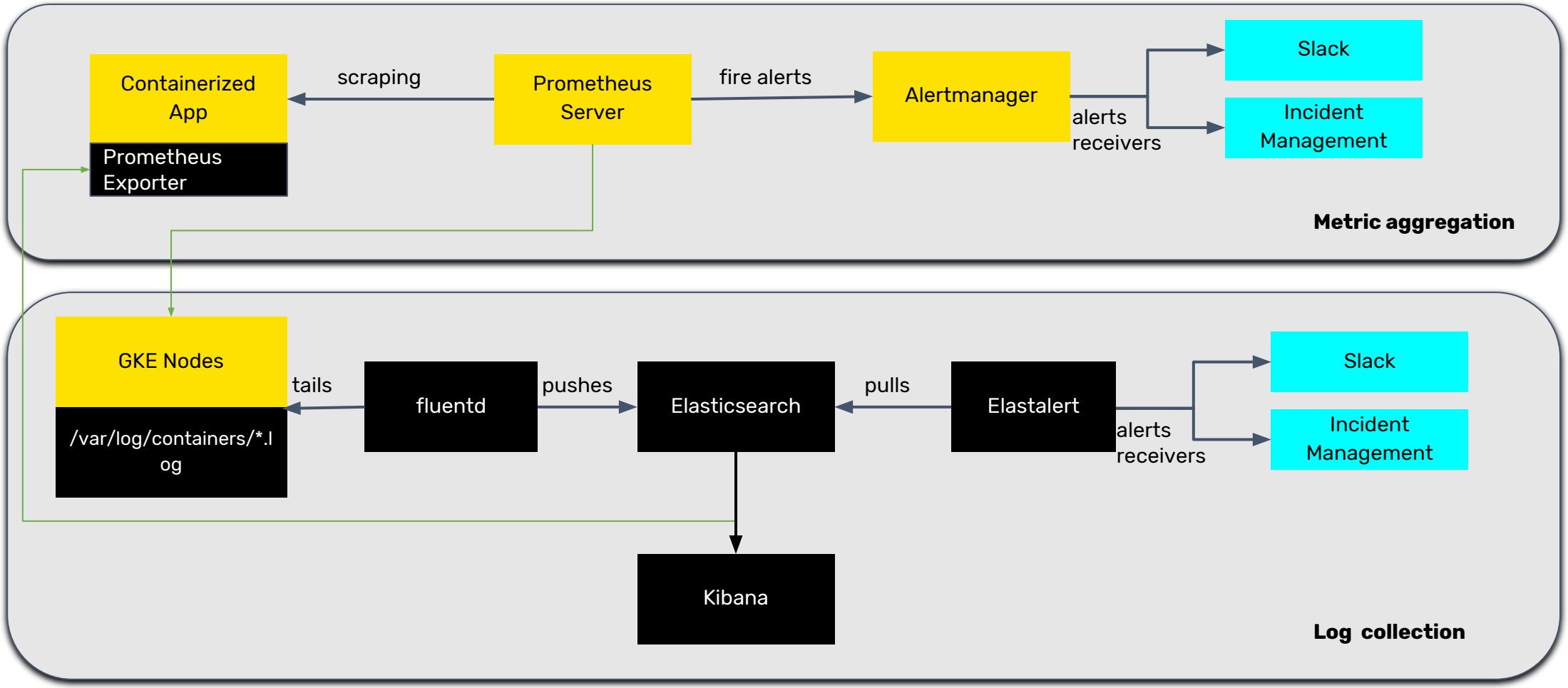
Types of monitoring in modern systems:

- ✓ Metric Aggregation
- ✓ Log collection
- ✓ Anomaly detection
- ✓ Tracing

Logging vs metric collection

- ✓ A *log message* is a system generated set of data that provides details when an event happens
- ✓ Metrics are time series (measured over intervals of time)
- ✓ Metrics are optimized for storage and enable longer retention of data
- ✓ Logs and metrics are complementary

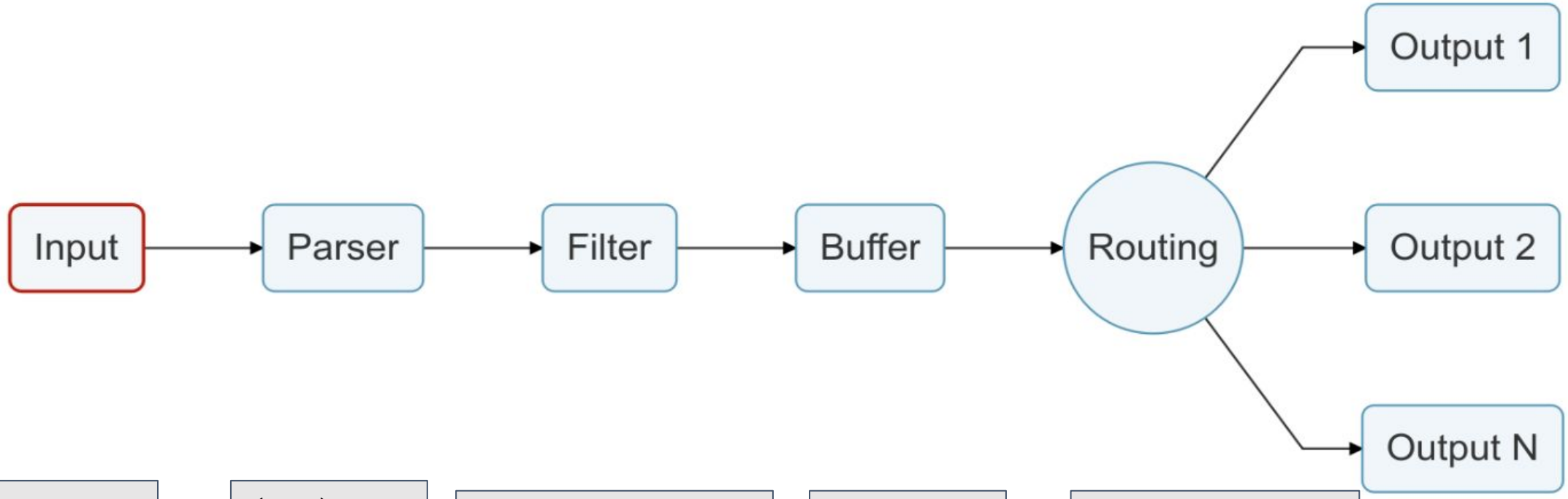
The whole system



Points of failure with log aggregation systems

- Garbage collection issues
- logs are rejected
- log content is not searchable
- Fluentd makes logs unreadable
- buffer overflow
- indexing issues

The life of a Fluentd event




```
<source>
    @type tail
        .
        .
        .
  </source>
```

```
<parse>
  @type regexp
  expression /.../
        .
        .
        .
</parse>
```

```
<filter kubernetes.**>
   @type kubernetes_metadata
   @id filter_kube_metadata
 </filter>
```

```
<buffer>
    @type file
    path /var/log/
 </buffer>
```

```
<match **>
      @type elasticsearch
      @id out_es
      host elasticsearch
      port 9200
</match>
```

Demo time

Super cool demo coming up

Structured vs Unstructured logs

- By default when you set `logstash_format` to true - a dynamic index is created in elasticsearch
- new log:

```
{
    "avengers": [{
        "name": "Antman",
        "rank": "Bestofthemall"
    }]
}
```

192.168.1.105/json/heroes.php

```
// 20170208210437
// http://192.168.1.105/json/heroes.php

{
  "avengers": [
    {
      "name": "Captain America",
      "rank": 1
    },
    {
      "name": "Iron Man",
      "rank": 2
    },
    {
      "name": "Hulk",
      "rank": 3
    },
    {
      "name": "Thor",
      "rank": 4
    },
    {
      "name": "Spiderman",
      "rank": 5
    }
  ]
}
```

JVM Options - A heap of trouble

- Java objects reside heap memory. When the heap fills up, objects that are no longer referenced by the application (garbage) are automatically released from memory.
- The maximum size of heap is specified at application startup and cannot be changed; the size impacts allocation speed, GC frequency and duration
- Elasticsearch advises for the heap to not be set too small or too large (under 32GB RAM)

To recap

- Having visibility of your system is very important
- Managing an EFK cluster is difficult
- Managing an Elasticsearch cluster is difficult
- …but without a monitoring system it’s hard to know what happens in you cluster

Resources

- efk-demo: https://github.com/calinah/efk-demo
- A heap of trouble:

  https://www.elastic.co/blog/a-heap-of-trouble

whoami

Ana Calin
Systems Engineer @Paybase
Twitter: @AnaMariaCalin

Thank you

<call to action here>

PAYBASE_