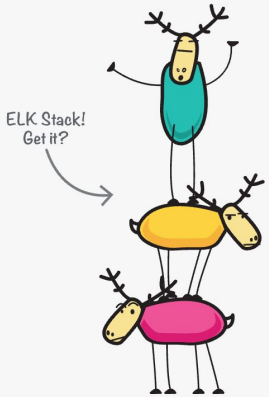


E Elasticsearch

L Logstash

K Kibana

Elastic Stack: Log ve Ötesi

Görsel: https://www.elastic.co/what-is/elk-stack

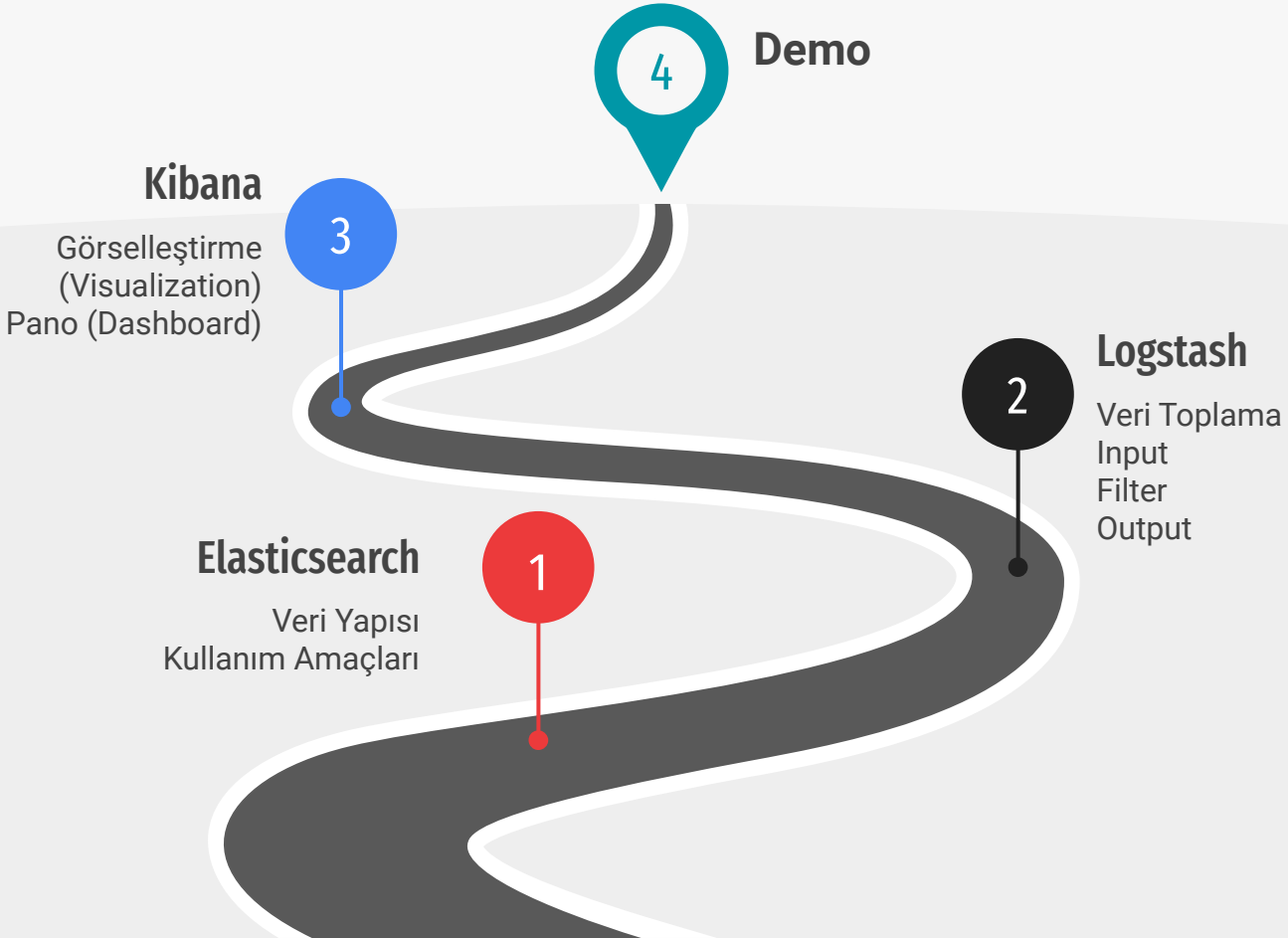
Hoşgeldiniz

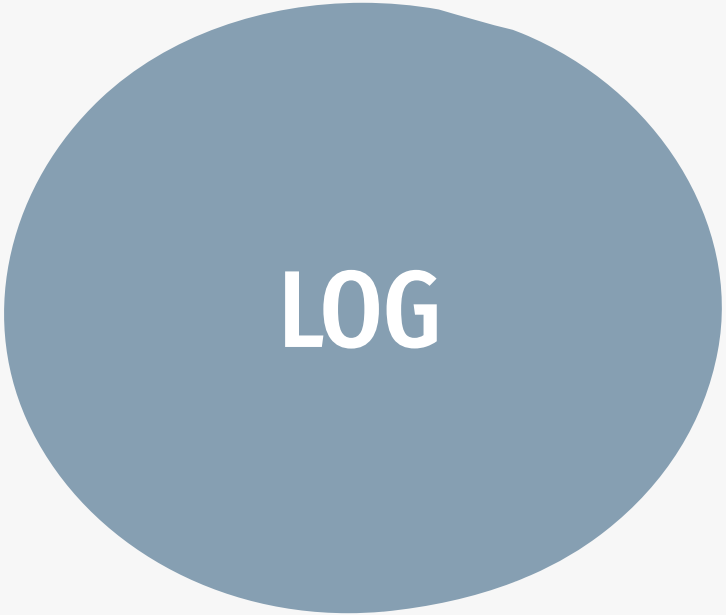
Ahmed Enis ERKAYA

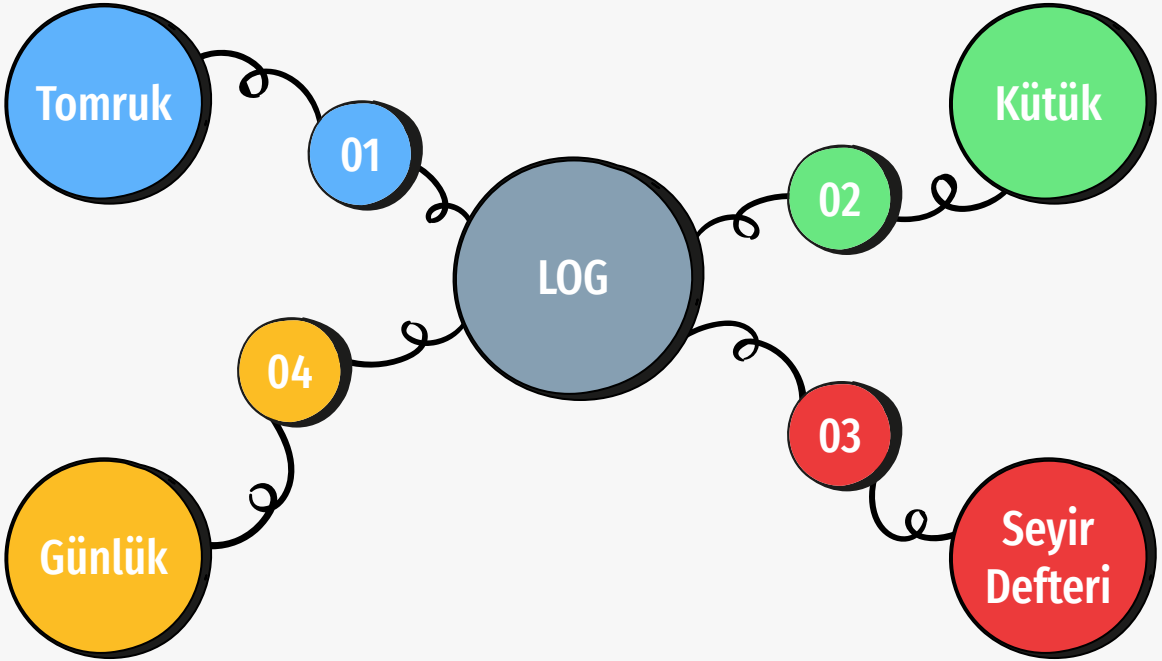
Yazılım Mühendisi, Seyyah, Kahve

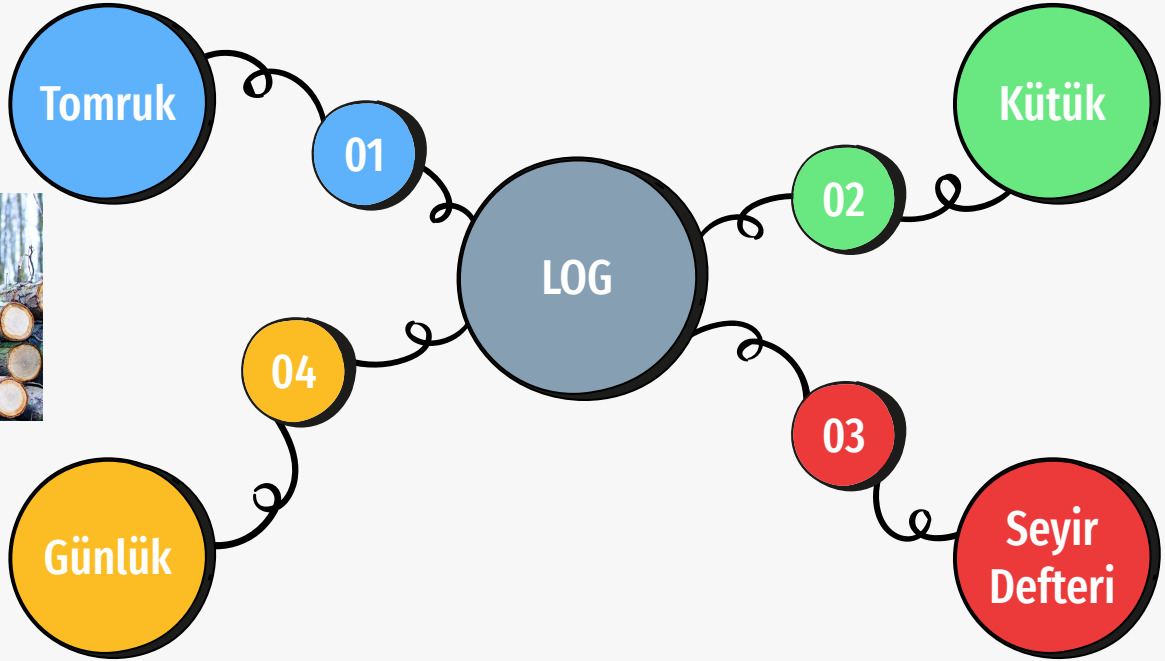
eniserkaya.com

ElasticStack: Log ve Ötesi



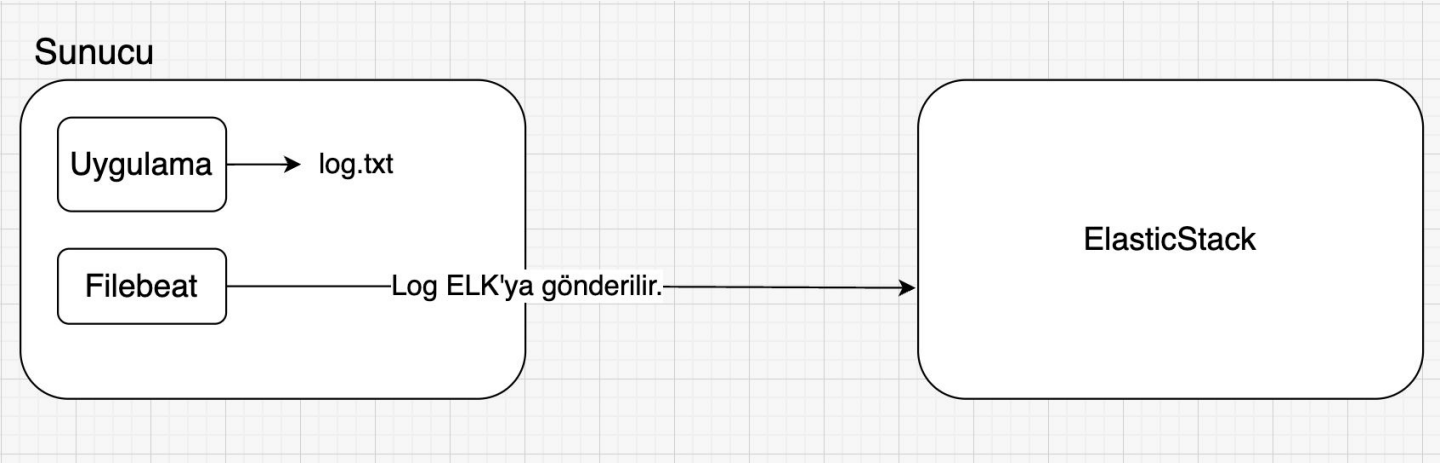

LOG


Tomruk
01
Kütük
02
LOG
04
03
Günlük
Seyir
Defteri


Tomruk
01
Kütük
02
LOG
04
03
Günlük
Seyir
Defteri

Uygulama Logu

Log Yönetimi

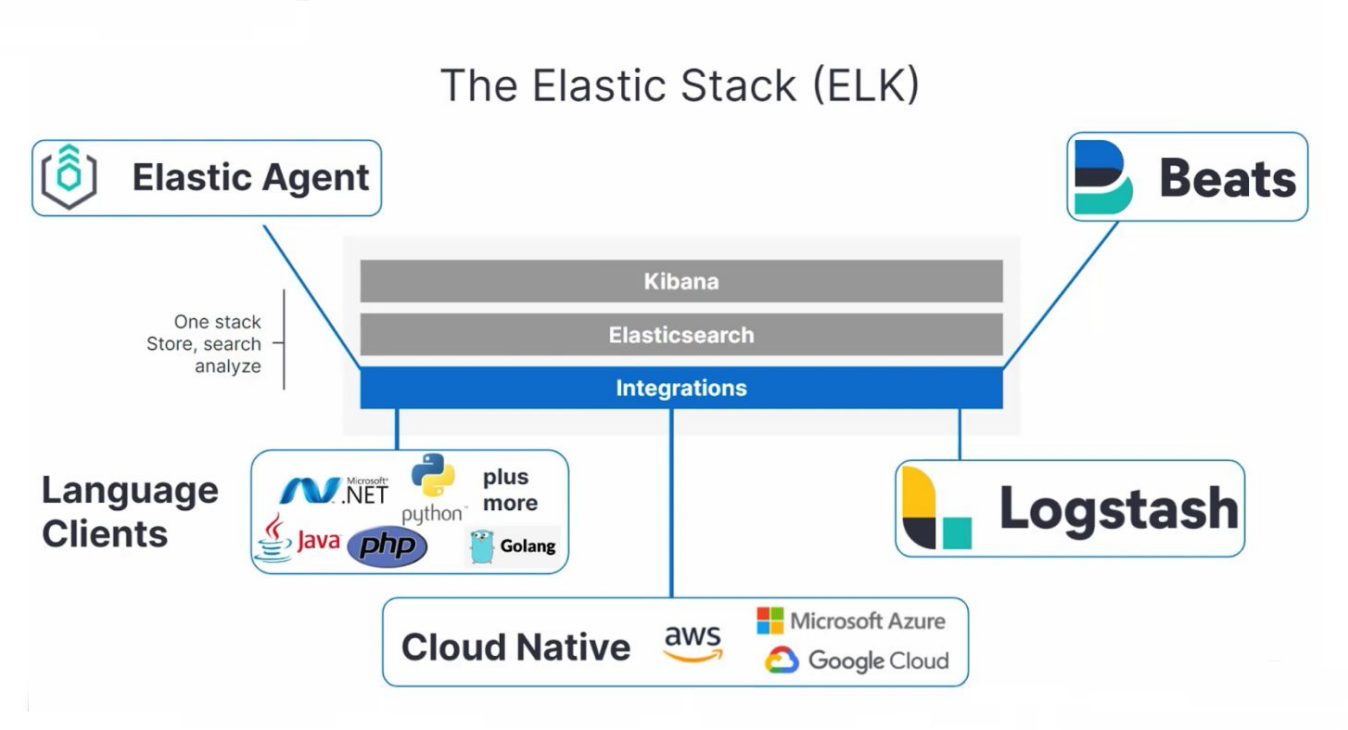


Kubernetes üzerinde çalışan bir uygulamada log dosyası nerede tutulur?

Zamanla büyüyen log verisi nasıl yönetilir?

Binlerce sayfadan oluşan metin içerikleri üzerinde hızlı bir şekilde *arama* nasıl gerçekleştirilir?

ElasticStack (Elasticsearch, Logstash, Kibana)



Görsel: https://www.elastic.co/what-is/elk-stack

“Elasticsearch is a **distributed**, **RESTful** search and analytics engine capable of addressing a growing number of use cases. As the **heart of the Elastic Stack**, it centrally stores your data for lightning **fast search**, fine-tuned relevancy, and powerful analytics that scale with ease.”

https://www.elastic.co/elasticsearch/

Elasticsearch

- **Dağıtık**
- **Açık kaynak kodlu**
- **NoSQL, doküman tabanlı**
- **Full Text Search**
- **Veri Tipi**
  - Enlem boylam (geo-point)
  - Int, Float vb.
- **Dev Tools**
- **REST API**

https://www.elastic.co/about/free-and-open

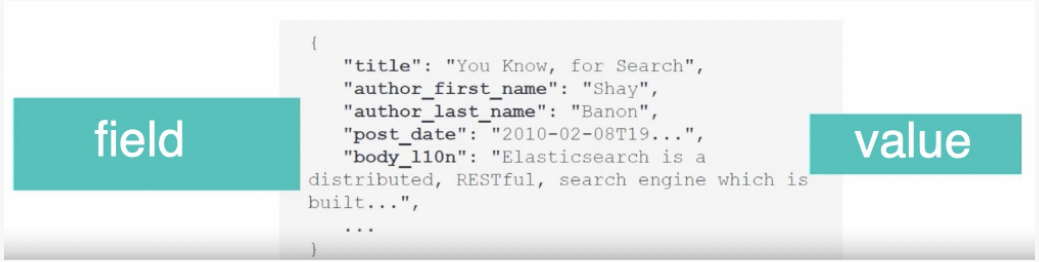
Bir JSON objesi ...

```
{
   "title": "You Know, for Search",
   "author_first_name": "Shay",
   "author_last_name": "Banon",
   "post_date": "2010-02-08T19...",
   "body_l10n": "Elasticsearch is an
open source, distributed, RESTful,
search engine which is built...",
   ...
}
```

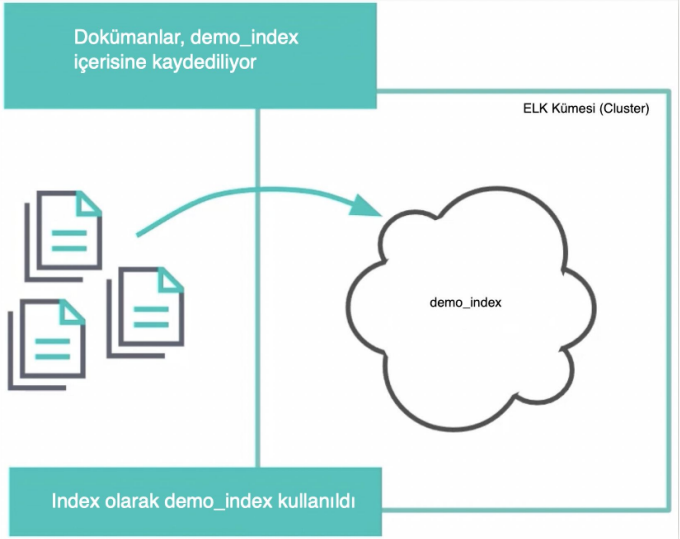
... Elasticsearch için bir dokümandır.

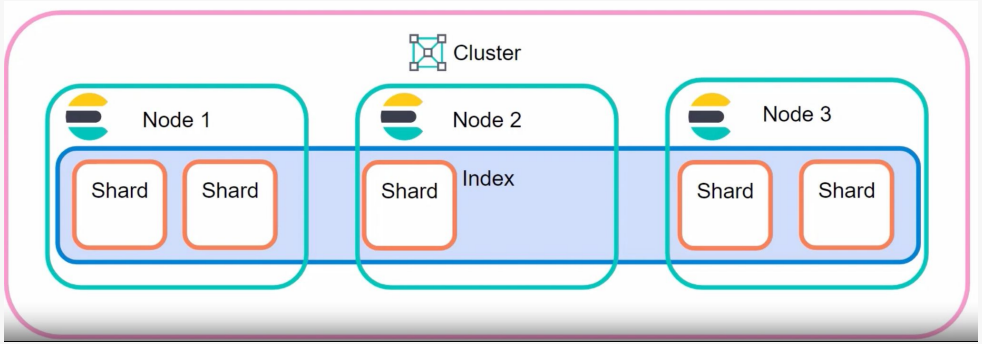
Elasticsearch

title	category	date	author_first_name	author_last_name	author_company	Blog Text
You Know, for Search	Engineering	February 08, 2010	Shay	Banon	Elastic	Elasticsearch is a distributed…
How we saved $100,000/month by keeping our own software up to date	User Stories	April 27, 2022	George	Kobar	Elastic	Let's start with the bottom line…



Elasticsearch Veriyi Nasıl Saklıyor?

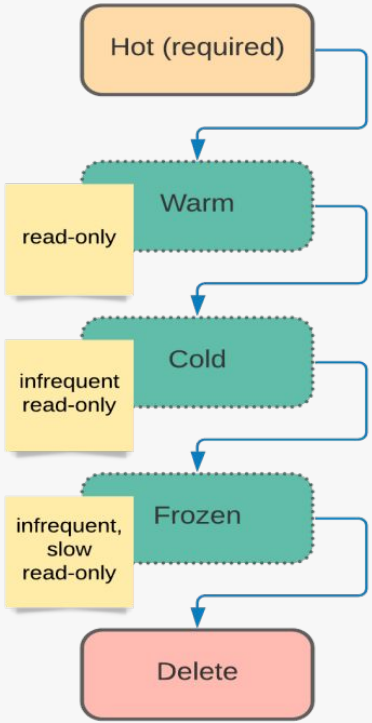




Elasticsearch Temel Kavramlar

1. Cluster
2. Node
3. Index
4. Document
5. Shard

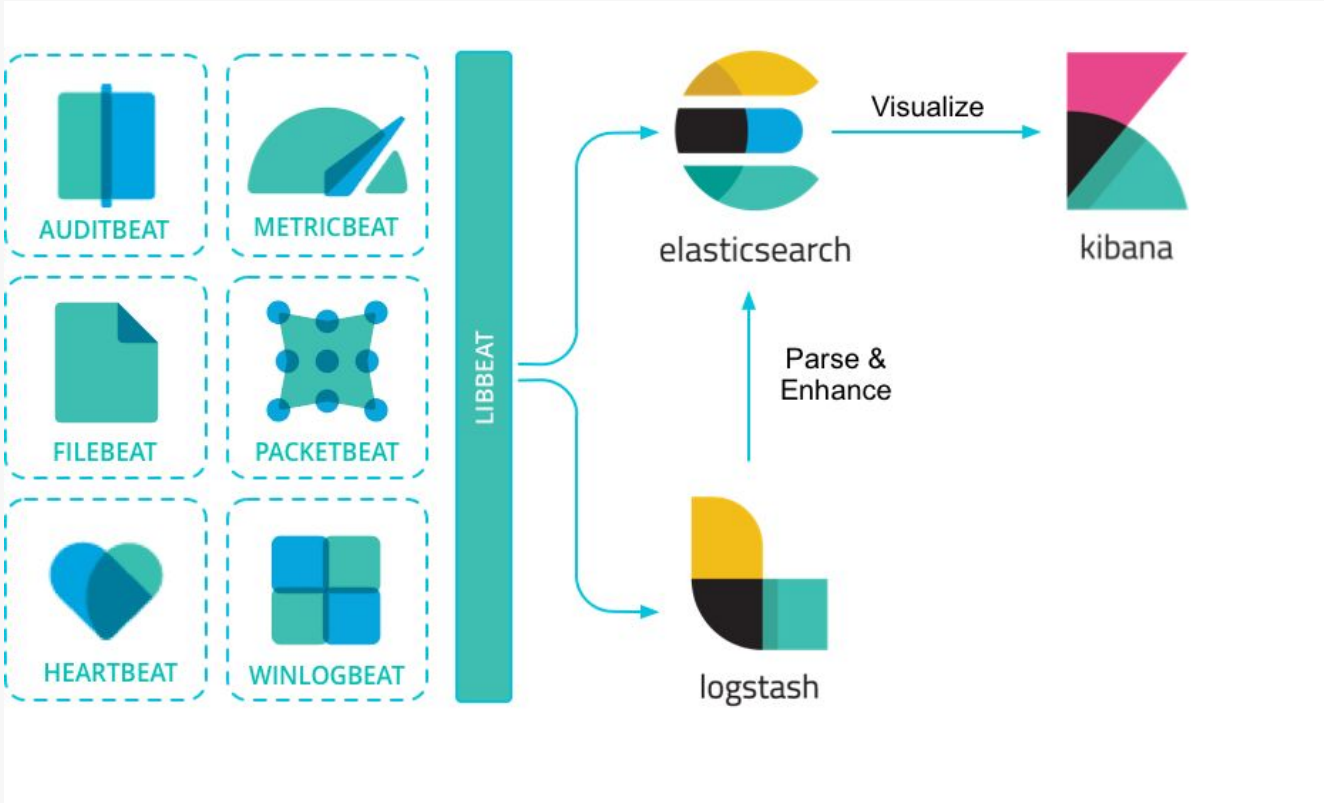
Index Lifecycle Management




```
PUT _ilm/policy/ilm_aken
{
  "policy": {
    "phases": {
      "hot": {
        "min_age": "0ms",
        "actions": {
          "rollover": {
            "max_size": "50gb",
            "max_age": "1m"
          },
          "set_priority": {
            "priority": 100
          }
        }
      },
      "warm": {
        "actions": {}
      },
      "cold": {
        "min_age": "2m",
        "actions": {}
      },
      "delete": {
        "min_age": "3m",
        "actions": {}
      }
    }
  }
}
```

Görsel: https://medium.com/knowledgelens/an-introduction-to-index-life-cycle-management-in-elasticsearch-da6b0ff579c3

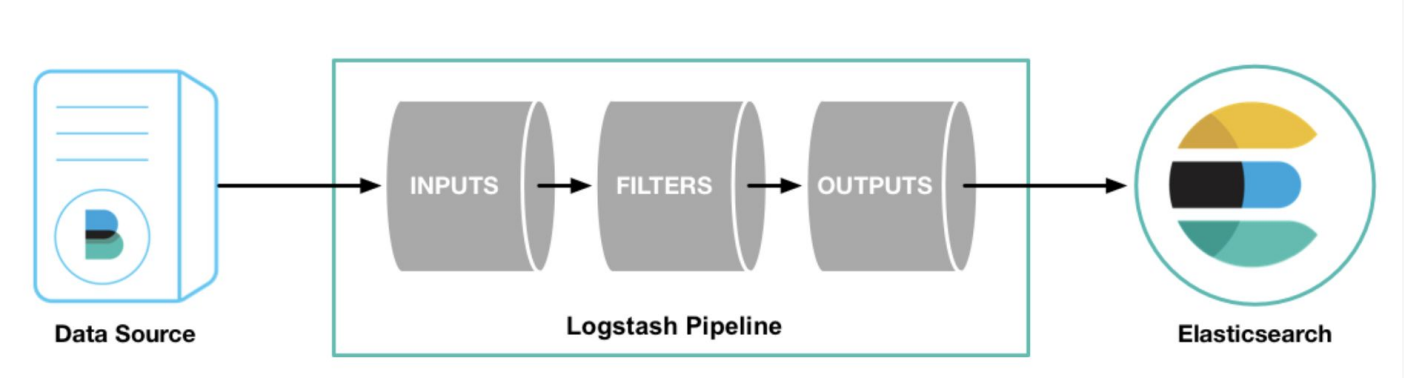
Beats



Görsel: https://www.elastic.co/guide/en/beats/libbeat/current/beats-reference.html

Logstash

- **Açık kaynak veri toplama motorudur.**



Logstash

```
# This is a comment. You should use comments to describe
# parts of your configuration.
input {
  ...
}

filter {
  ...
}

output {
  ...
}
```

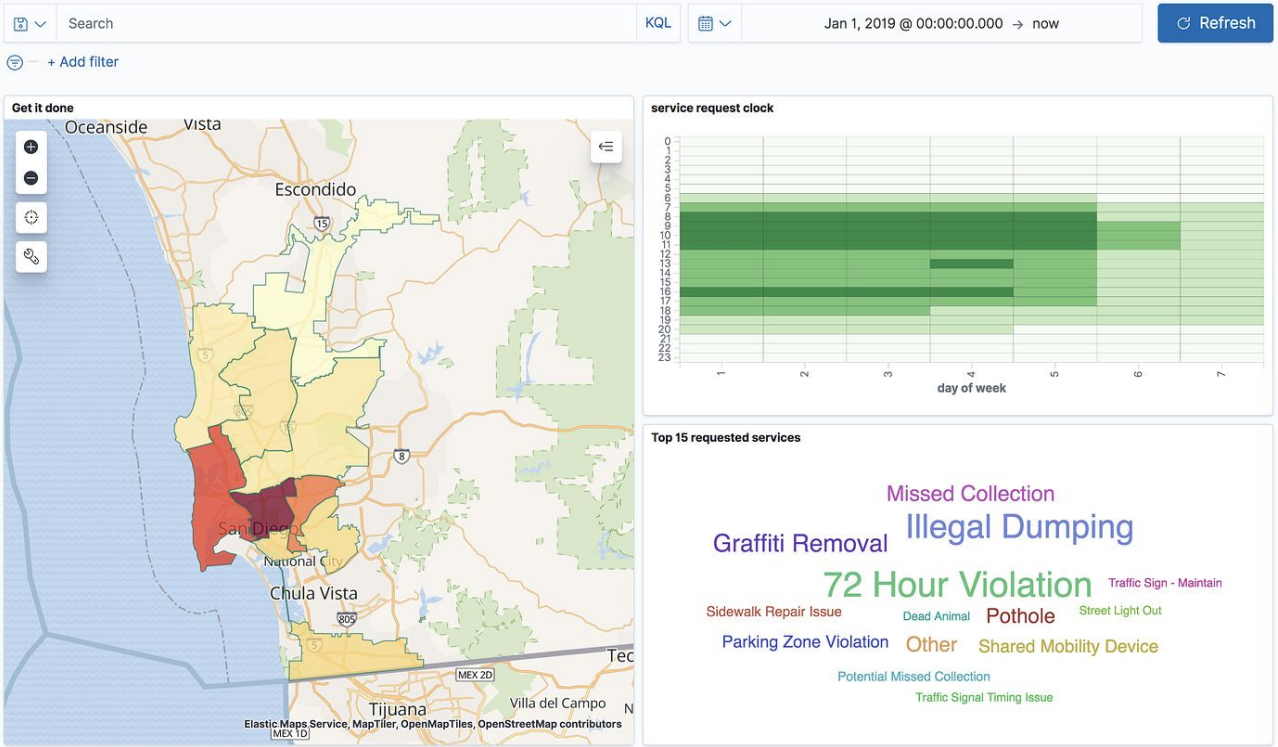
```
input {
    twitter {
        consumer_key => "enter_your_consumer_key_here"
        consumer_secret => "enter_your_secret_here"
        keywords => ["cloud"]
        oauth_token => "enter_your_access_token_here"
        oauth_token_secret => "enter_your_access_token_secret_here"
    }
    beats {
        port => "5044"
    }
}
output {
    elasticsearch {
        hosts => ["IP Address 1:port1", "IP Address 2:port2", "IP Address 3"]
    }
    file {
        path => "/path/to/target/file"
    }
}
```

https://www.elastic.co/guide/en/logstash/8.10/pipeline.html
https://www.elastic.co/guide/en/logstash/8.10/configuration.html

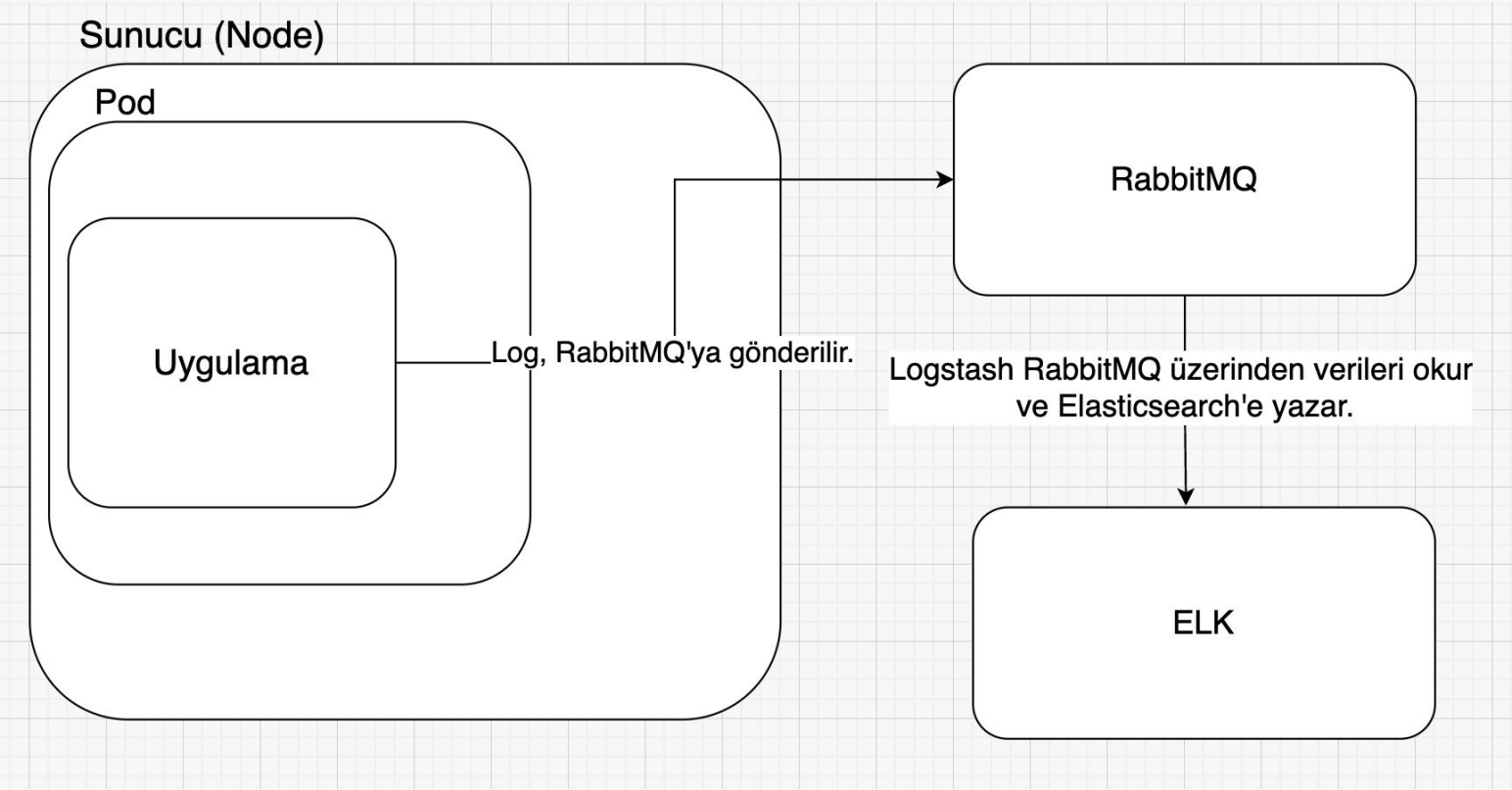
Kibana

- **Elastic Stack içerisine açılan bir penceredir.**
- **Discover**
- **Visualizations, Lens, Dashboards**
- **Maps**

Kibana



Görsel: https://www.elastic.co/guide/en/kibana/current/maps.html


Sunucu (Node)
Pod
Uygulama
Log, RabbitMQ'ya gönderilir.
RabbitMQ
Logstash RabbitMQ üzerinden verileri okur
ve Elasticsearch'e yazar.
ELK

Demo Zamanı

Teşekkürler, sorular? :)