## **Monstache**

Transporter

# What is Monstache

# Monstache is a tool, software that performs data synchronization from MongoDB to Elasticsearch.

# Perform data synchronization in a real time, when there are any data changes on MongoDB (add / edit / delete) it will automatically update to Elasticsearch.

# What is Elasticsearch

# Logstash, Elasticsearch, Kibana

# Logstash: This is a tool used to collect, log processing is written in java. The main task of logstash is log collection and then transfer to Elastichsearch. Each log line of logstash is stored under json.

# Elasticsearch: using NoSQL database. Used to store data and provide interfaces that allow queries to the database.

# Kibana: This is the user interface for users on the web environment. Kibana: Kibana will use Elashtichsearch to search for data with user requirements.

# Operation mechanism of ELK Stack

# First, the log will be taken to Logstash.

# Logstash will read these logs, add information such as time, IP, parse data from the log (server, severity, log content), then write down the database of Elasticsearch.

# When you want to see the log, the user enters Kibana's URL. Kibana will read log information in Elasticsearch, display it to the query user interface and handle

# Elasticsearch is a very powerful search engine.

# The data uploaded by the user will be saved to the database and then synchronized to Elasticsearch.

# When users search, they will search on Elasticsearch, speed is fast, and reduce the load for the database.

* Elasticsearch is document oriented database. It is a search and storage tool. It allows to store, search and analyze with very large data, resulting in real-time results . All documents are displayed in JSON format
* Some cases should use ES:
* Searching text and structured data
* JSON document storage
* Data aggregation

**Advantage of elasticsearch**

* **Lots of search options**: ElasticSearch implements a lot of features. Such as you can find what you are searching for even though you have a spelling mistake. It can be simple suggestions of existing tags, trying to a search based on search history, or just doing a completely new search for every keyword.
* Is open source software, completely free, large development community.
* Elasticsearch executes complex queries quickly and can also save most of the query into the cache to use for filtering results.
* All data saved to Elasticsearch are indexed, which is why Elasticsearch's search performance is very high.
* **Document-oriented:** ElasticSearch stores data as structured JSON with a higher performance result.
* **Speed**: Speaking of performance, ElasticSearch is able to execute complex queries very fast.
* **Easy extend**: providing the ability to extend resources between the nodes in a cluster
* **Data record**: ElasticSearch records any changes made in transactions logs on multiple nodes in the cluster to limit data loss
* **RESTful API**: ElasticSearch is API-driven, so actions can be using a simple RESTful API.

**Basics of Elasticsearch**

* Cluster: A collection of Nodes (servers) contains all the data to ensure reliability and availability
* Node-node: A single server contains some data and participates in cluster’s indexing and querying..
* Index: is a collection of documents that contain similar characteristics.
* **Type**: like concept of collection in MongoDB or table concept in SQL database
* Document: A JSON object with some data. This is the basic information unit in ES(Document concept in MongoDB or concept of row in table of SQL database)