ELASTICSEARCH

Elasticsearch is a distributed, free and open search and analytics engine for all types of data, including textual, numerical, geospatial, structured, and unstructured.

How does Elasticsearch work?

Raw data flows into Elasticsearch from a variety of sources, including logs, system metrics, and web applications. *Data ingestion* is the process by which this raw data is parsed, normalized, and enriched before it is *indexed* in Elasticsearch. Once indexed in Elasticsearch, users can run complex queries against their data and use aggregations to retrieve complex summaries of their data. From Kibana, users can create powerful visualizations of their data, share dashboards, and manage the Elastic Stack.

What is an Elasticsearch index?

An Elasticsearch *index* is a collection of documents that are related to each other. Elasticsearch stores data as JSON documents. Each document correlates a set of *keys* (names of fields or properties) with their corresponding values (strings, numbers, Booleans, dates, arrays of *values*, geolocations, or other types of data).

Elasticsearch uses a data structure called an *inverted index*, which is designed to allow very fast full-text searches.

What is Logstash used for?

Logstash, one of the core products of the Elastic Stack, is used to aggregate and process data and send it to Elasticsearch. Logstash is an open source, server-side data processing pipeline that enables you to ingest data from multiple sources simultaneously and enrich and transform it before it is indexed into Elasticsearch.

What is Kibana used for?

Kibana is a data visualization and management tool for Elasticsearch that provides real-time histograms, line graphs, pie charts, and maps. Kibana also includes advanced applications such as Canvas, which allows users to create custom dynamic infographics based on their data, and Elastic Maps for visualizing geospatial data.

Why use Elasticsearch?

Elasticsearch is fast.

Elasticsearch is distributed by nature.

Elasticsearch comes with a wide set of features. Elasticsearch has a number of powerful built-in features that make storing and searching data even more efficient, such as data rollups and index lifecycle management.

The Elastic Stack simplifies data ingest, visualization, and reporting.