Table of Contents

Elasticsearch

- https://www.elastic.co

Reliably And Securely Take Data And Search, Analyze, And Visualize It In Real Time.

Elasticsearch, Kibana, Beats, and Logstash (also known as the ELK Stack). Reliably and securely take data from any source, in any format, then search, analyze, and visualize it in real time.

- https://www.elastic.co/products/elastic-stack
- https://www.elastic.co/products/kibana

What is Elasticsearch?

Elasticsearch is a search engine and analytics platform that is used to store, search, and analyze large volumes of data in real time. It is an open-source, distributed search engine based on the Lucene search library. Elasticsearch is designed to be highly scalable and fault-tolerant, and can be used to store and search a wide range of data types, including text, numerical, geospatial, and structured data. It can also be used to perform complex data analytics, such as aggregations and data visualization.

Elasticsearch is often used in conjunction with other technologies, such as Logstash and Kibana, to create what is known as the “ELK stack”. Logstash is used to collect and transform data from a variety of sources, such as logs and databases, and send it to Elasticsearch for indexing and analysis. Kibana is a data visualization tool that allows users to create dashboards and visualizations based on data stored in Elasticsearch.

Some of the key features of Elasticsearch include:

- **Full-text search:** Elasticsearch supports powerful full-text search capabilities, including relevance scoring, stemming, and faceting.
- **Distributed architecture:** Elasticsearch is designed to be highly scalable and fault-tolerant, with support for distributed indexing and search.
- **Near real-time search:** Elasticsearch provides near real-time search capabilities, allowing users to search and analyze data as soon as it is indexed.
- **Document-oriented:** Elasticsearch stores data in a document-oriented format, making it flexible and easy to work with.
- **RESTful API:** Elasticsearch provides a RESTful API for interacting with the search engine, making it easy to integrate with other applications.

Elasticsearch is used in a wide range of applications, including e-commerce, social media, cybersecurity, and data analytics. Its flexibility and scalability make it a popular choice for organizations that need to store and search large volumes of data in real time.

What types of data can be stored in Elasticsearch?

Elasticsearch can store and search a wide range of data types, including text, numerical, geospatial, and structured data. It is designed to be flexible and can be used to index and search almost any type of data.

How is Elasticsearch different from traditional relational databases?

Elasticsearch is a search engine and not a relational database. It is designed to handle unstructured and semi-structured data, whereas traditional databases are designed for structured data. Elasticsearch provides powerful search capabilities and can be used for text search, geospatial search, and more.

Can Elasticsearch handle large volumes of data?

Yes, Elasticsearch is designed to handle large volumes of data. It is a distributed system that can scale horizontally by adding more nodes to the cluster. Elasticsearch is used by organizations to store and search billions of documents.

How does Elasticsearch perform search queries?

Elasticsearch uses a query language called the Elasticsearch Query DSL to perform search queries. The Query DSL is a JSON-based syntax that allows users to specify the search criteria and filters.

What is the ELK stack?

The ELK stack is a combination of Elasticsearch, Logstash, and Kibana. Logstash is used to collect and transform data from various sources, which is then indexed and stored in Elasticsearch. Kibana is used to visualize and analyze the data stored in Elasticsearch.

Is Elasticsearch open source?

Yes, Elasticsearch is open source software that is distributed under the Apache License 2.0. The source code is available on GitHub.

Can Elasticsearch be used for real-time analytics?

Yes, Elasticsearch can be used for real-time analytics. It provides near real-time search capabilities and supports complex data analytics, such as aggregations and data visualization.

How is Elasticsearch different from Solr?

Elasticsearch and Solr are both search engines based on the Lucene search library. However, Elasticsearch is designed to be more scalable and easier to use, whereas Solr is designed to be more customizable. Elasticsearch is also more focused on near real-time search and analytics, whereas Solr is more focused on traditional search applications.

*Snippet from Wikipedia: **Elasticsearch***

> **Elasticsearch** is a search engine based on the Lucene library. It provides a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents. Elasticsearch is developed in Java and is dual-licensed under the source-available Server Side Public License and the Elastic license, while other parts fall under the proprietary (*source-available*) *Elastic License*. Official clients are available in Java, .NET (C#), PHP, Python, Ruby and many other languages. According to the DB-Engines ranking, Elasticsearch is the most popular enterprise search engine.

Related:

- Enterprise Search

tool, architecture, programming, maintenance, search, devopsmonitor

From:
https://www.almbok.com/ - **ALMBoK.com**

Permanent link:
https://www.almbok.com/tools/elasticsearch

Last update: **2023/03/30 15:48**