



Elasticsearch 101

Finartz Tech Talks
23/11/2020



Content

What is Elasticsearch?

Use Cases

Customers

Supported Programming Language

Features

Terminology

Indexing & Search

Rest API Examples

What is Elasticsearch?



Built-on Apache Lucene



Distributed















Open-source Java project



Most popular search engine

Search Engine Ranking

Rank			DBMS	Database Model	Score		
Nov 2020	Oct 2020	Nov 2019			Nov 2020	Oct 2020	Nov 2019
1.	1.	1.	Elasticsearch 	Search engine, Multi-model 	151.55	-2.29	+3.15
2.	2.	2.	Splunk	Search engine	89.71	+0.30	+0.64
3.	3.	3.	Solr	Search engine	51.82	-0.66	-5.96
4.	4.	4.	MarkLogic 	Multi-model 	11.10	-0.63	-1.72
5.	5.	 8.	Algolia	Search engine	7.38	+0.08	+2.49
6.	6.	6.	Microsoft Azure Search	Search engine	6.80	+0.11	+0.20
7.	7.	 5.	Sphinx	Search engine	6.35	+0.01	-0.69
8.	8.	 7.	ArangoDB 	Multi-model 	5.37	-0.18	+0.36
9.	9.	9.	Amazon CloudSearch	Search engine	2.77	+0.07	-0.40
10.	10.	 11.	Virtuoso 	Multi-model 	2.54	-0.03	-0.10

[db-engines ranking](#)

Use Cases



Search (Application,
Web, Enterprise)



Logging and log analytics



Application performance
monitoring



Geospatial data analysis
and visualization



Security analytics



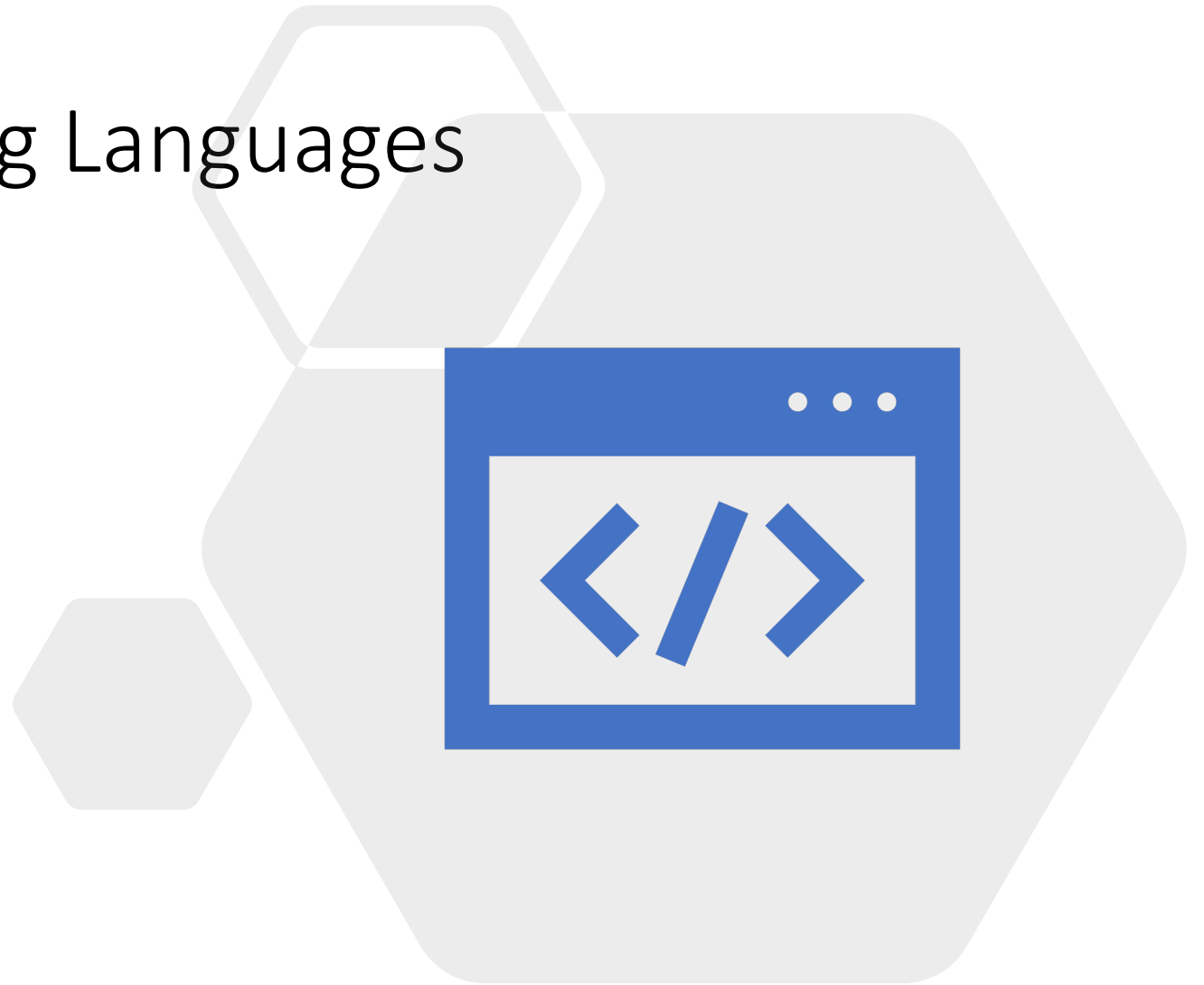
Business analytics

Customers

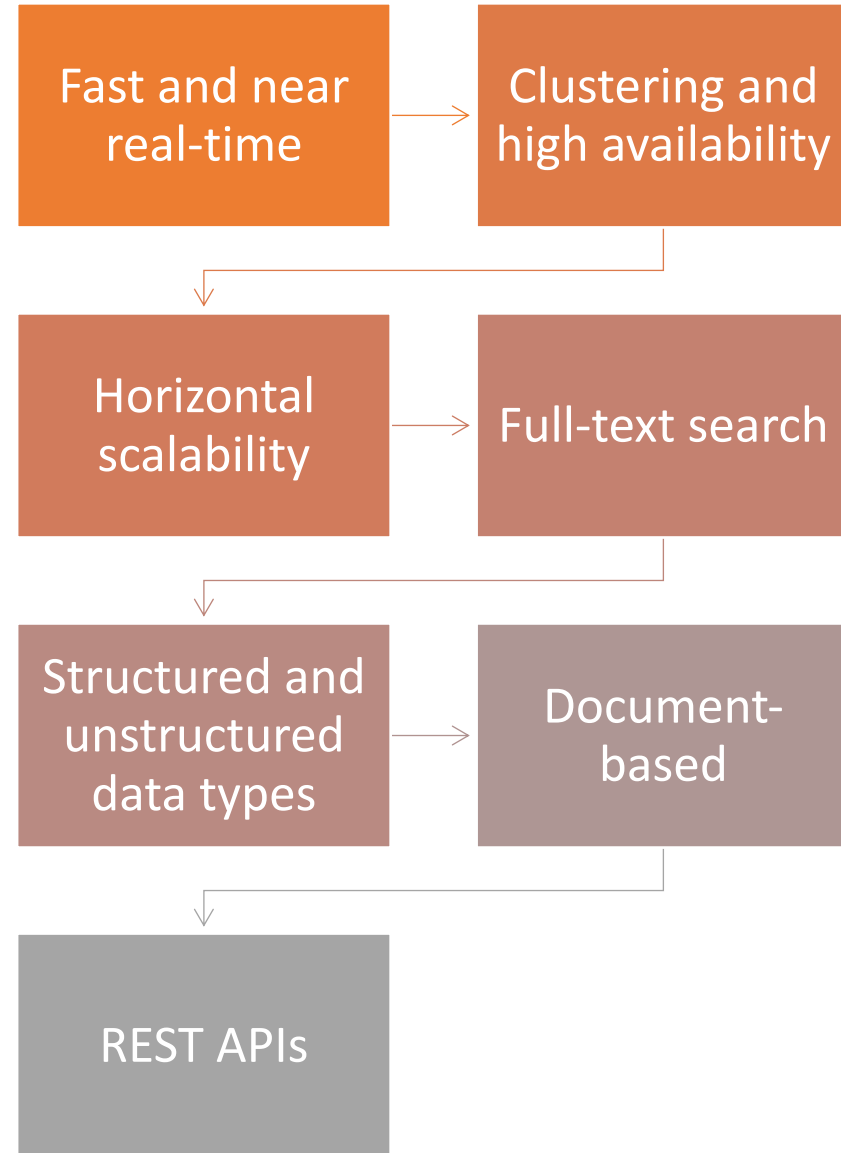


Supported Programing Languages

- Java
- JavaScript (Node.js)
- Go
- .NET (C#)
- PHP
- Perl
- Python
- Ruby



Features



Terminology

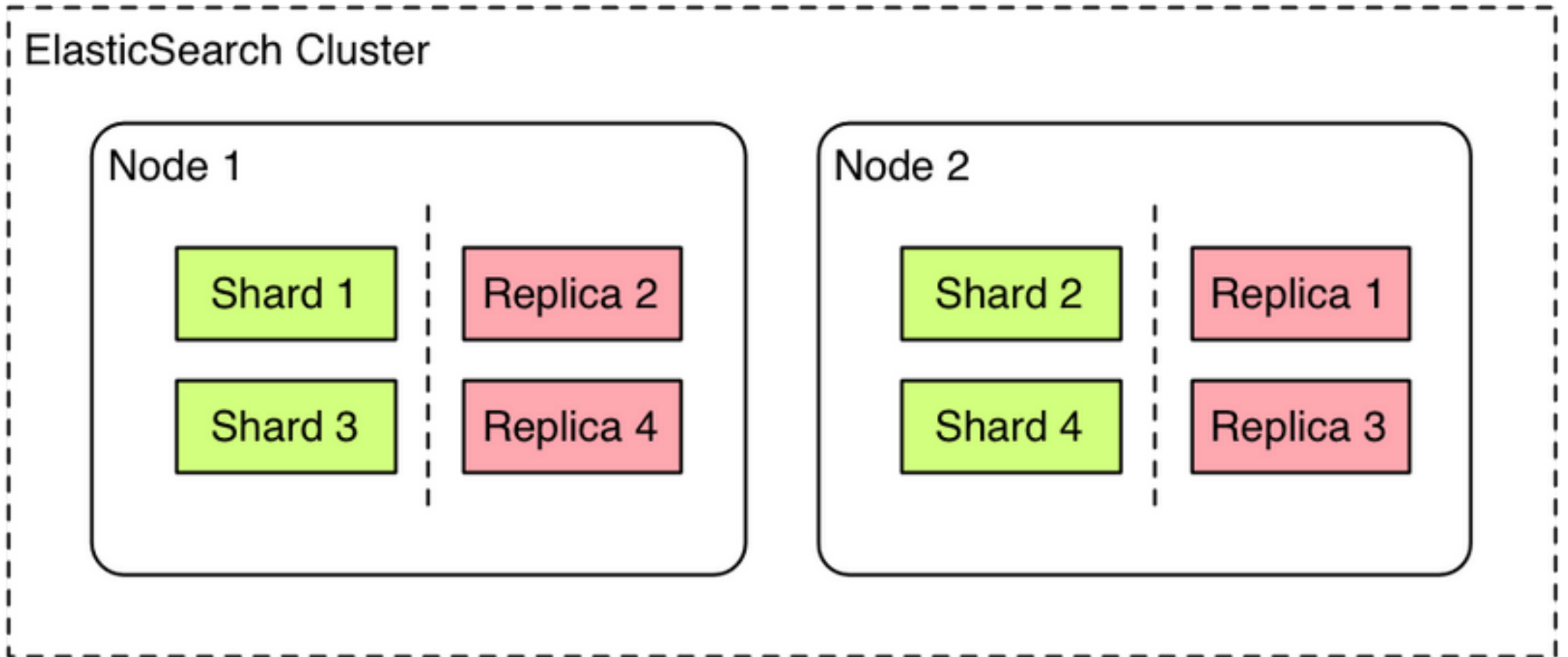
- **Document:** JSON object stored in Elasticsearch
- **Field:** Similar to a column in a table in a relational database
- **Index:** Collection of documents
- **Type:** Represents the type of document
- **Mapping:** Schema definition in a relational database

Relational Database	Elasticsearch
Schema	Mapping
Database	Index
Table	Type
Row	Document
Column	Field

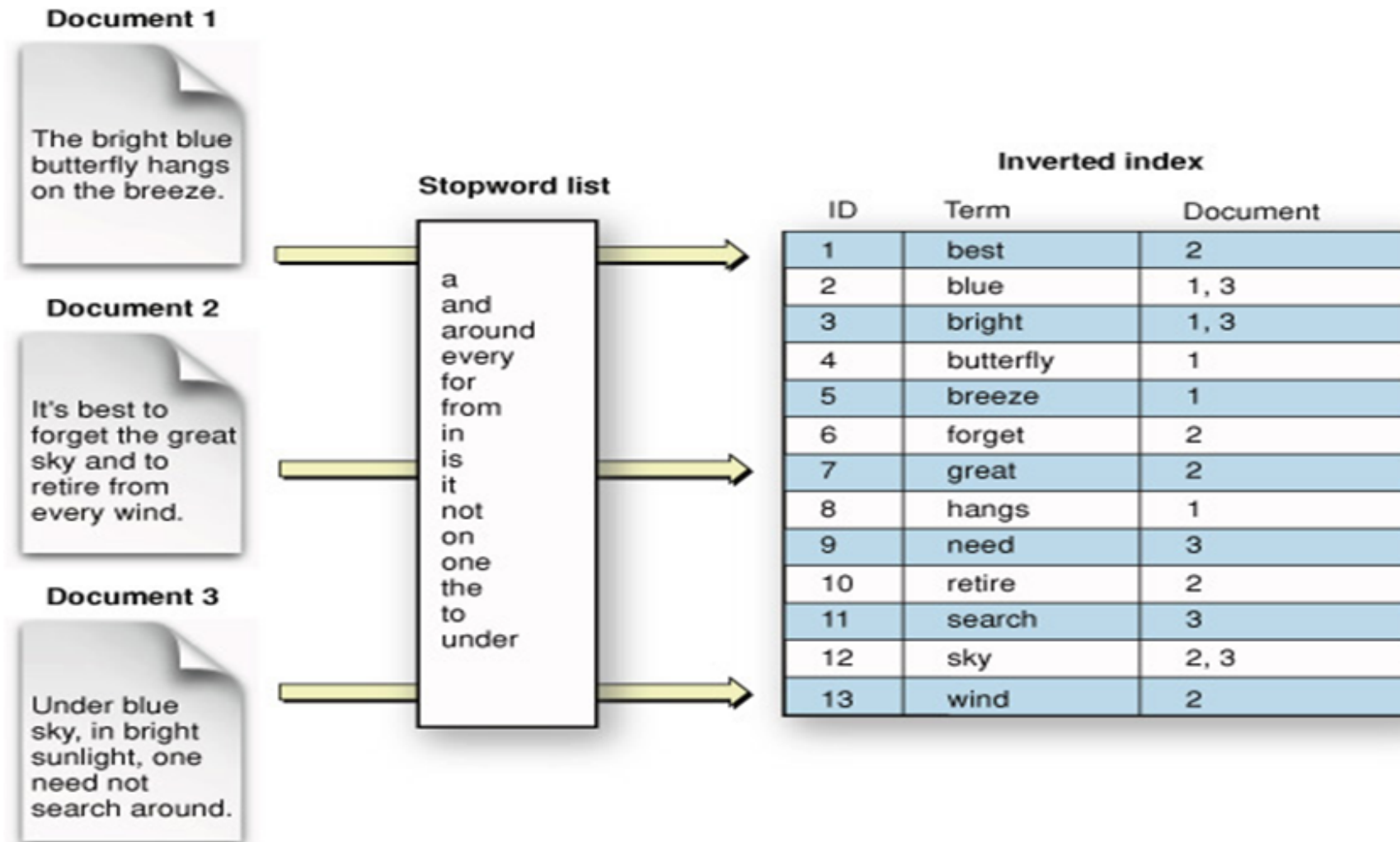
Terminology

- **Cluster:** Contains nodes
- **Node:** A running instance of Elasticsearch
- **Shard:** A single Lucene instance
- **Replica:** A copy of primary shard

Elasticsearch Cluster



Indexing & Search





REST APIs

- **Cat API:** User-friendly information service
- **Cluster API:** Cluster informations
- **Index API:** Responsible for Index operations
- **Document API:** Responsible for Document operations
- **Search API:** Responsible for Search operations



Thank you...