
contasimples

Elastic Stack

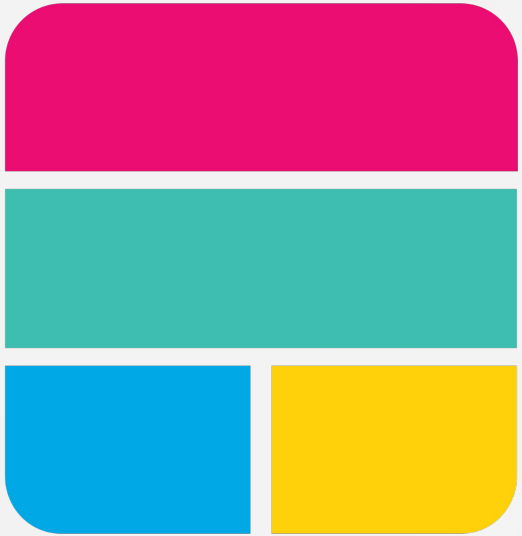
Introdução ElasticSearch, LogStash, Kibana e Beats

Gabriel Prando

Apresentação — 19/11/2021

O que iremos ver?

- Conceitos sobre a stack.
- Funcionamento e arquitetura elasticsearch
- Exemplo.
- Perguntas e dúvidas.



O que é Elastic Stack?

Nasceu de um conjunto de projetos open source chamado “ELK” que era formado pelo **E**lasticsearch, **L**ogstash e **K**ibana

O que é Elastic Stack?

Nasceu de um conjunto de projetos open source chamado “ELK” que era formado pelo **E**lasticsearch, **L**ogstash e **K**ibana

Uma solução bem completa para várias áreas no universo de tecnologia, visando **ingerir, analisar, pesquisar e visualizar todo tipo de dados em escala**. Pode ser utilizada como ferramenta de pesquisa e consulta de dados, monitoramento de aplicações e análise de logs, aprendizagem de máquina

O que é Elastic Stack?

Nasceu de um conjunto de projetos open source chamado “ELK” que era formado pelo **E**lasticsearch, **L**ogstash e **K**ibana

Uma solução bem completa para várias áreas no universo de tecnologia, visando **ingerir, analisar, pesquisar e visualizar todo tipo de dados em escala**. Pode ser utilizada como ferramenta de pesquisa e consulta de dados, monitoramento de aplicações e análise de logs, aprendizagem de máquina

Permite que seja criado dashboards para análise dos dados, alarmes para monitoramento de comportamentos indesejáveis, entre várias outras funcionalidades.

Em resumo

Conjunto ferramental que pode nos ajudar a fazer aplicações mais escaláveis e robustas, bem como acompanhar o desempenho dos nossos produtos e auxiliar em possíveis futuras tomadas de decisões

Composição

Data Collection

Data Aggregation & Processing

Indexing & storage

Analysis & visualization

Beats

- Agentes de dados com a única finalidade de enviar dados de diversas fontes para o Logstash ou o Elasticsearch.
- Ficam nos seus servidores, com os seus containers, ou são implantados como funções.
- Pode enviar os dados diretos ao elasticsearch, mas caso precise processar antes do envio, pode ser enviado ao logstash.

Logstash

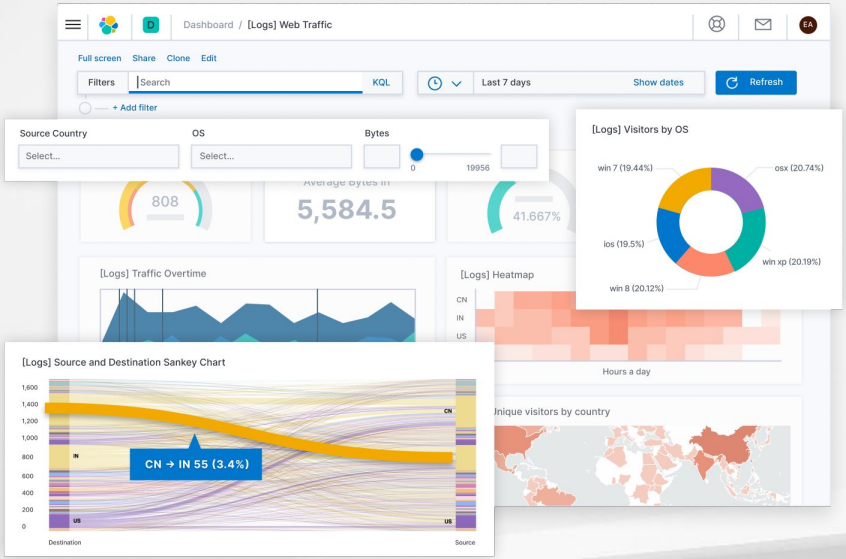
Pipeline de processamento de dados do lado do servidor que faz a ingestão de dados a partir de inúmeras fontes simultaneamente, transforma-os e envia-os para o Elasticsearch

Kibana

Permite que os usuários visualizem os dados com diagramas e gráficos no Elasticsearch

Kibana

“Comece explorando seus dados com visualizações impressionantes no Kibana, desde gráficos de waffle e mapas de calor até análise de séries temporais e muito mais. Use dashboards pré-configurados para suas diversas fontes de dados, crie apresentações ao vivo para destacar KPIs e gerencie a implantação em uma única UI”



Elasticsearch

- Permite armazenar, buscar e analisar com facilidade e em escala.
- Mecanismo de busca e análise
- Desenvolvido em Java sob a biblioteca Apache Lucene
- Solução NoSQL
- Schema less/free (Orientado a documentos)
- API Rest (inclusão, consulta, remoção, atualização)
- Distribuído
- Inteligência para encontrar resultados aproximados com a pesquisa

Termos do elasticsearch

- Node
- Cluster
- Index
- Document
- Shard

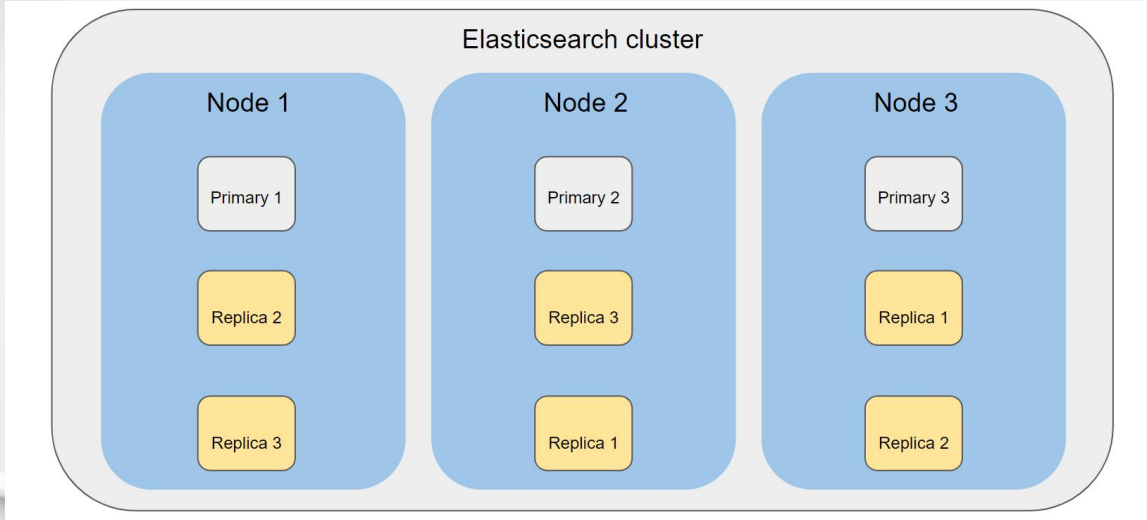
MySQL	ElasticSearch
Database	Index
Table	Type
Row	Document
Column	Field
Schema	Mapping
Partition	Shard

Node

Uma instância de elasticsearch. Ele é criado quando uma instância de elasticsearch começa.

Cluster

Um cluster é uma coleção de Nodes que, juntos, contém dados e fornece recursos de indexação e pesquisa combinados.



Index

- Um índice é uma coleção de documentos com características semelhantes.
- Operações de indexação, pesquisa, atualização e exclusão são feitas em cima de um índice.

Document

- É a unidade básica de informação que pode ser indexada. É expresso no par JSON (chave: valor). '{“Usuário”: “nullcon”}'. Cada documento está associado a um tipo e id único.

Buscas e performance

- O elasticsearch utiliza de índices invertidos para ter mais performance
- Quebra todos os termos de um documento em tokens e os “normaliza” através de um processo de Analyzer

Termo	Frequência	Documentos
afiliado	1	1
brasil	2	3,4
...	...	...

Exemplo

- Processar csv de dados com o logstash usando o plugin logstash-filter-csv
  - Dataset de dados de covid no brasil retirado do brasil.io
  - https://data.brasil.io/dataset/covid19/caso_full.csv.gz
- Importar dados para o elasticsearch
- Visualizar no kibana


contasimples