João Pedro Castro Rachel Bottino

Elastic Stack

Evolução da Ferramenta

Usuários começaram a utilizar o mecanismo para logs e queriam que fosse possível fazer ingestão e visualização de dados. Assim surgem o **Logstash** e **Kibana**.

O ELK Stack passou a se chamar **Elastic Stack**: mesmas ferramentas, mas mais bem integradas e avançadas



mecanismo de busca open source, distribuído, RESTful e baseado em JSON. Novas funcionalidades
começaram a surgir
conforme as
necessidades da
comunidade de usuários

Elasticsearch

Mecanismo de busca e análise de dados.

Kibana

03

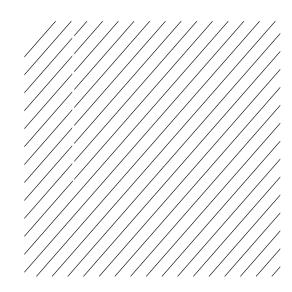
Permite visualização de dados com diagramas e gráficos

Logstash

02

Pipeline de processamento de dados do lado do servidor que faz a ingestão de dados. O Elasticsearch permite o seu usuário realizar e combinar diversos tipos de busca. Suas agregações fazem com que seja possível ver um panorama gera para analisar tendências e padrões dos dados. Ele é considerado o coração do Elastic Stack.

A Ferrament





'antagens

- Velocidade
- Escalabilidade
- Resiliência

Clusters / elasticsearch / Logstash	Pipelines					
module-arcsight Version ac	ive now and first seen 26 min ago	. •				
					This plugin does not have an ID specified. Specifying an ID allow	
					track differences across pipelin You can explicitly specify an ID	
					plugin like so:	
	• tcp			2.65k e/s emitted		
	₩ Queue				elasticsearch { id => "mySpecialId"	
	Queue metrics	not availa	able		}	
	♥ Filters					
	• date	0%	0.02 ms/e	2.64k e/s received	Events	
	• geoip	0%	0.02 ms/e	2.64k e/s received	Latency	0.58 ms/e
	geoip	0%	0 ms/e	2.64k e/s received	Events Emitted Rate	2.6k e/s
	• geoip	0%	0.01 ms/e	2.64k e/s received	Evente	
	⇔ Outputs				Received	77k events
	· outputs				Events	77k events

O Logstash é um pipeline de processamento de dados open source do lado do servidor que faz a ingestão de dados a partir de inúmeras fontes simultaneamente, transforma-os e envia-os para Elasticsearch.



Kibana

O Kibana permite que o usuário visualize os dados do Elasticsearch e navegue pelo Elastic Stack para fazer qualquer coisa, desde rastrear a carga de consultas até entender a maneira como as solicitações fluem pelos aplicativos.



Welcome to Kibana

Your window into the Elastic Stack

De som on a		
Password		



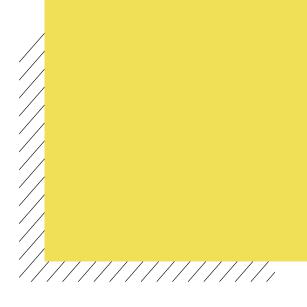
Nesse dataset há registros de todas as corridas completas de táxi na cidade de Nova lorque no ano de 2017. Os campos dos dados coletados incluem:

- Horário de embarque
- Horário de desembarque
- Localização de embarque
- Localização de desembarque
- Distância da viagem
- Taxas
- Tipo de pagamento
- Quantidade de passageiros

113M

Colunds

Demonstração



Perguntas?

João Pedro Castro Rachel Bottino