

FIAP

CHALLENGE SPRINT

95044 - Guilherme Antonio Silva

4º ENTREGA

OBJETIVO: Processar e Analisar grandes conjuntos de dados não estruturados.

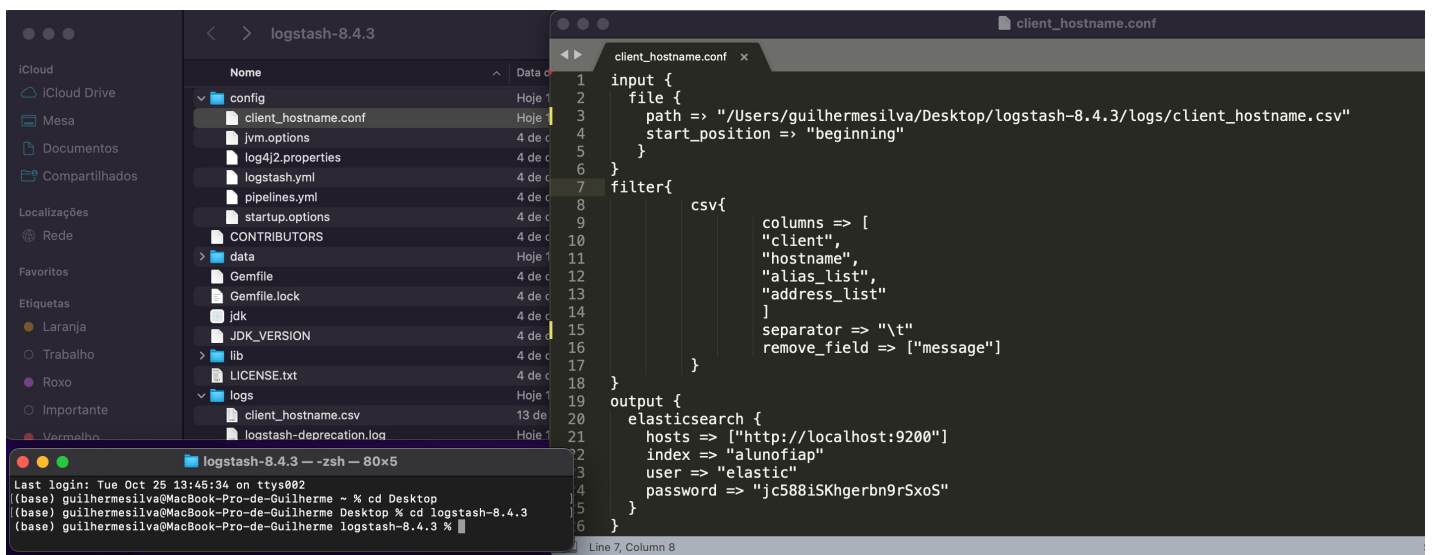
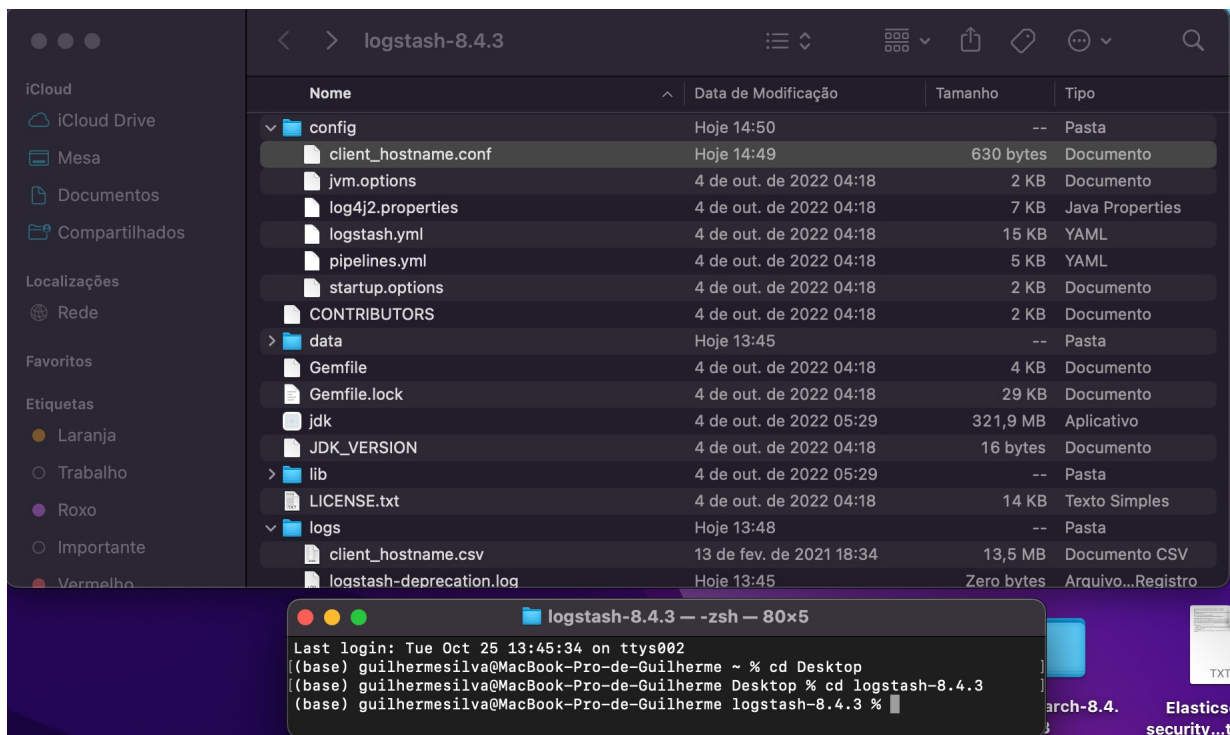
CENÁRIO: Suponha que você trabalha em uma empresa com e-commerce como o da BASF.

Analise os logs do servidor web para extrair alguns insights sobre o comportamento dos usuários e do site.

ENTREGA: Entregar o resultado em um único arquivo PDF.

a) Faça a carga do arquivo de log de um website de compras online (fonte abaixo) usando o logstash. Crie um index pattern. Exiba as evidências (4 pontos)

Fonte: <https://www.kaggle.com/datasets/eliasdabbas/web-server-access-logs>



elastic

Find apps, content, and more. Ex: Discover

Discover

test3

NOT response : 200

Search field names

Filter by type 0

Available fields 13

Popular

- request
- response

Fields:

- _id
- _index
- _score
- @timestamp
- agent
- auth
- bytes
- clientip
- httpversion
- ident
- message
- referrer

Add a field

1,895 hits

Documents

Field statistics BETA

Jan 26, 2019 @ 14:08:37.000 - Jan 26, 2019 @ 14:16:30.000 (Interval: Auto - 10 seconds)

1 field sorted

@timestamp

Document

Jan 26, 2019 @ 14:16:30.000	@timestamp Jan 26, 2019 @ 14:16:30.000 agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 message 104.222.32.91 - - [26/Jan/2019:19:46:30 +0330] "GET /rapidGrails/jsonList?maxColumns=16&domainClass=esh [{op:inSession,%20field:id,%20val:orderList53a5b4401a1244b492124d718e6c27bd)]&columns=[(name:trackingCode,width:
Jan 26, 2019 @ 14:16:30.000	@timestamp Jan 26, 2019 @ 14:16:30.000 agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 message 104.222.32.91 - - [26/Jan/2019:19:46:30 +0330] "GET /rapidGrails/jsonList?maxColumns=16&domainClass=esh [{op:inSession,%20field:id,%20val:orderList3f65f9d93fdc4f0d9f2f6ec1ea42cb6f)]&columns=[(name:trackingCode,width:
Jan 26, 2019 @ 14:16:30.000	@timestamp Jan 26, 2019 @ 14:16:30.000 agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 message 104.222.32.91 - - [26/Jan/2019:19:46:30 +0330] "GET /rapidGrails/jsonList?maxColumns=16&domainClass=esh [{op:inSession,%20field:id,%20val:orderListf9985d74edb04ddf14dba7540e1c7d)]&columns=[(name:trackingCode,width:
Jan 26, 2019 @ 14:16:30.000	@timestamp Jan 26, 2019 @ 14:16:30.000 agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 message 104.222.32.91 - - [26/Jan/2019:19:46:30 +0330] "GET /rapidGrails/jsonList?maxColumns=16&domainClass=esh [{op:inSession,%20field:id,%20val:orderList1985e2c5d27496b8bc205bd5bf559d6)]&columns=[(name:trackingCode,width:
Jan 26, 2019 @ 14:16:29.000	@timestamp Jan 26, 2019 @ 14:16:29.000 agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 message 104.222.32.91 - - [26/Jan/2019:19:46:29 +0330] "GET /rapidGrails/jsonList?maxColumns=16&domainClass=esh [{op:inSession,%20field:id,%20val:orderList5143bf08e8e54ecba8c8f67a3f99974c)]&columns=[(name:trackingCode,width:

Rows per page: 100

Mostrar tudo

b) Filtre pelo DevTools do Kibana as requisições HTTP diferentes de 200. Exiba as evidências (3 pontos)

elastic

Find apps, content, and more. Ex: Discover

Discover

test3

NOT response : 200

Search field names

Filter by type 0

Available fields 13

Popular

- request
- response

Fields:

- _id
- _index
- _score
- @timestamp
- agent
- auth
- bytes
- clientip
- httpversion
- ident
- message
- referrer

Add a field

1,895 hits

Documents

Field statistics BETA

Jan 26, 2019 @ 14:08:37.000 - Jan 26, 2019 @ 14:16:30.000 (Interval: Auto - 10 seconds)

1 field sorted

@timestamp

Document

Jan 26, 2019 @ 14:16:30.000	@timestamp Jan 26, 2019 @ 14:16:30.000 agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 message 104.222.32.91 - - [26/Jan/2019:19:46:30 +0330] "GET /rapidGrails/jsonList?maxColumns=16&domainClass=esh [{op:inSession,%20field:id,%20val:orderList53a5b4401a1244b492124d718e6c27bd)]&columns=[(name:trackingCode,width:
Jan 26, 2019 @ 14:16:30.000	@timestamp Jan 26, 2019 @ 14:16:30.000 agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 message 104.222.32.91 - - [26/Jan/2019:19:46:30 +0330] "GET /rapidGrails/jsonList?maxColumns=16&domainClass=esh [{op:inSession,%20field:id,%20val:orderList3f65f9d93fdc4f0d9f2f6ec1ea42cb6f)]&columns=[(name:trackingCode,width:
Jan 26, 2019 @ 14:16:30.000	@timestamp Jan 26, 2019 @ 14:16:30.000 agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 message 104.222.32.91 - - [26/Jan/2019:19:46:30 +0330] "GET /rapidGrails/jsonList?maxColumns=16&domainClass=esh [{op:inSession,%20field:id,%20val:orderListf9985d74edb04ddf14dba7540e1c7d)]&columns=[(name:trackingCode,width:
Jan 26, 2019 @ 14:16:30.000	@timestamp Jan 26, 2019 @ 14:16:30.000 agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 message 104.222.32.91 - - [26/Jan/2019:19:46:30 +0330] "GET /rapidGrails/jsonList?maxColumns=16&domainClass=esh [{op:inSession,%20field:id,%20val:orderList1985e2c5d27496b8bc205bd5bf559d6)]&columns=[(name:trackingCode,width:
Jan 26, 2019 @ 14:16:29.000	@timestamp Jan 26, 2019 @ 14:16:29.000 agent "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 message 104.222.32.91 - - [26/Jan/2019:19:46:29 +0330] "GET /rapidGrails/jsonList?maxColumns=16&domainClass=esh [{op:inSession,%20field:id,%20val:orderList5143bf08e8e54ecba8c8f67a3f99974c)]&columns=[(name:trackingCode,width:

Rows per page: 100

c) Crie um Dashboard para exibir os diferentes status de requisição HTTP e suas respectivas contagens. (3 pontos)

