PROVA TÉCNICA SPLUNK – ACCENTURE

Documentação de APP

Roberto Amorim Jr

Gestor responsável – adalto.s.gomes@accenture.com

Agosto 2021

Primeiros passos (Resumo do executado)

- Última versão do Splunk instalada em ambiente StandAlone local;
- Upload do arquivo de Log do eCommerce realizado com sucesso;
- App eCommerce criado com sucesso;
- Index criado e atribuído ao App eCommerce com sucesso;
- SourceType criado em GSL usando Current Time e devidamente atribuído ao App eCommerce;
- Realizada uma análise das demandas do cliente;
- Contato realizado com o "cliente" (Felipe) para esclarecimento de valores atribuídos a alguns campos do arquivo de Log, como os campos MetododeCompra, Bandeira, entre outros;
- Dashboard criado com sucesso;
- Criados 03 arquivos Lookup para otimizar o tratamento do código;
- Todo o código foi devidamente revisado, respeitando as boas práticas, e zelando pela organização do XML;

Detalhes dos valores específicos de cada campo

Campo **Vendeu**:

0. Venda não realizada
1. Venda realizada

Campo **MetododeCompra**:

0. N/A
1. Débito
2. Crédito

Campo **Bandeira**:

0. N/A
1. Visa
2. Mastercard

Campo **Campanha**:

1. N/A
2. Hotsite
3. E-mail
4. Parceiro

Tratamento das demandas do cliente (Searchs isoladas)

Quantidade de Vendas Bem Sucedidas

```
index="ecommerce" Vendeu=1
| stats count as Qtde
```

- Buscando informações no Index eCommerce onde Vendeu=1 (Venda realizada)
- Geração de estatística em contagem de eventos

Média de Fluxo de Entrada de Caixa por Venda

```
index="ecommerce" Vendeu=1
| stats avg(Valor) as Media
| eval Media=round(Media,2)
```

- Buscando informações no Index eCommerce onde Vendeu=1 (Venda realizada)
- Geração de estatística retornando a média do valor total de vendas
- Arredondamento para duas casas decimais (por se tratar de valor monetário)

Quantidade de clientes (IPs) Únicos

```
index="ecommerce"
| stats dc(IP) as Qtde
```

- Buscando informações no Index eCommerce geral
- Geração de estatística de contagem distinta de IPs únicos (remoção de resultados duplicados)

Compras com Visa

```
index="ecommerce" Vendeu=1
| lookup bandeiras.csv codigo_bandeira as Bandeira output nome_bandeira as Bandeira
| where Bandeira="Visa"
| stats count as Qtde
```

- Buscando informações no Index eCommerce onde Vendeu=1 (Venda realizada)
- Gerado o Lookup bandeiras.csv para o de/para entre código e nome de bandeira
- Limitando o retorno aos resultados Bandeira=”Visa”
- Geração de estatística em contagem de eventos

Compras por Bandeiras

```
index="ecommerce" Vendeu=1
| lookup bandeiras.csv codigo_bandeira as Bandeira output nome_bandeira as Bandeira
| stats count as Qtde by Bandeira
```

- Buscando informações no Index eCommerce onde Vendeu=1 (Venda realizada)
- Gerado o Lookup bandeiras.csv para o de/para entre código e nome de bandeira
- Geração de estatística em contagem de eventos por Bandeira

Compras com MasterCard

```
index="ecommerce" Vendeu=1
| lookup bandeiras.csv codigo_bandeira as Bandeira output nome_bandeira as Bandeira
| where Bandeira="Mastercard"
| stats count as Qtde
```

- Buscando informações no Index eCommerce onde Vendeu=1 (Venda realizada)
- Gerado o Lookup bandeiras.csv para o de/para entre código e nome de bandeira
- Limitando o retorno aos resultados Bandeira=”Mastercard”
- Geração de estatística em contagem de eventos

Métodos de Compra

```
index="ecommerce" Vendeu=1
| lookup metodos.csv codigo_metodo as MetododeCompra output nome_metodo as MetododeCompra
| stats count as Qtde by MetododeCompra
```

- Buscando informações no Index eCommerce onde Vendeu=1 (Venda realizada)
- Gerado o Lookup metodos.csv para o de/para entre código e o método de compra utilizado
- Geração de estatística em contagem de eventos por Método de Compra

Principais Campanhas

```
index="ecommerce"
| lookup campanhas.csv codigo_campanha as Campanha output nome_campanha as Campanha
| stats count as Qtde by Campanha
```

- Buscando informações no Index eCommerce geral
- Gerado o Lookup campanhas.csv para o de/para entre código e o tipo de campanha utilizada
- Geração de estatística em contagem de eventos por Campanha

Quantidade de Vendas Mal Sucedidas

```
index="ecommerce" Vendeu=0
| stats count as Qtde
```

- Buscando informações no Index eCommerce onde vendeu=0 (Venda não realizada)
- Geração de estatística em contagem de eventos

Top 10 Produtos abandonados no carrinho

```
index="ecommerce" Vendeu=0
| top 10 Produto
| rename count as Qtde
```

- Buscando informações no Index eCommerce onde vendeu=0 (Venda não realizada)
- Comando estatístico retornando os 10 resultados com maior quantidade de eventos
- Renomeando a variável “count” para “Qtde”

Categorias mais Populares

```
index="ecommerce"
| top 5 Categoria
| rename count as Qtde
```

- Buscando informações no Index eCommerce geral
- Comando estatístico retornando os 5 resultados com maior quantidade de eventos
- Renomeando a variável “count” para “Qtde”

Produtos mais Procurados

```
index="ecommerce"
| top 10 Produto
| rename count as Qtde
```

- Buscando informações no Index eCommerce geral
- Comando estatístico retornando os 10 resultados com maior quantidade de eventos
- Renomeando a variável “count” para “Qtde”

Mapa com categorias por região

```
index="ecommerce"
| iplocation IP
| geostats count by Categoria latfield=lat longfield=lon
```

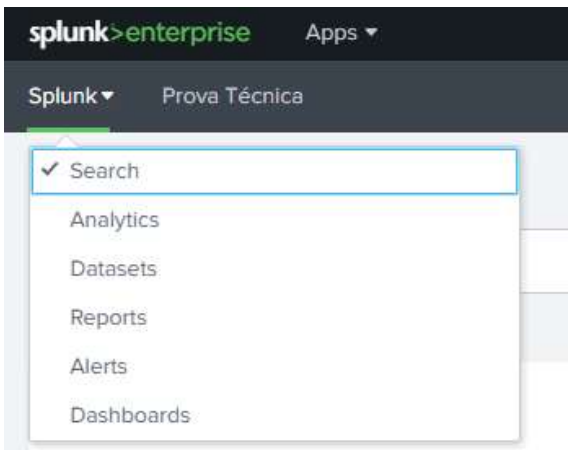
- Buscando informações no Index eCommerce geral
- Levantamento de informações de latitude e longitude, baseado na variável IP
- Geração de estatísticas por geolocalização em contagem de eventos por Categoria

APP exclusiva para o projeto

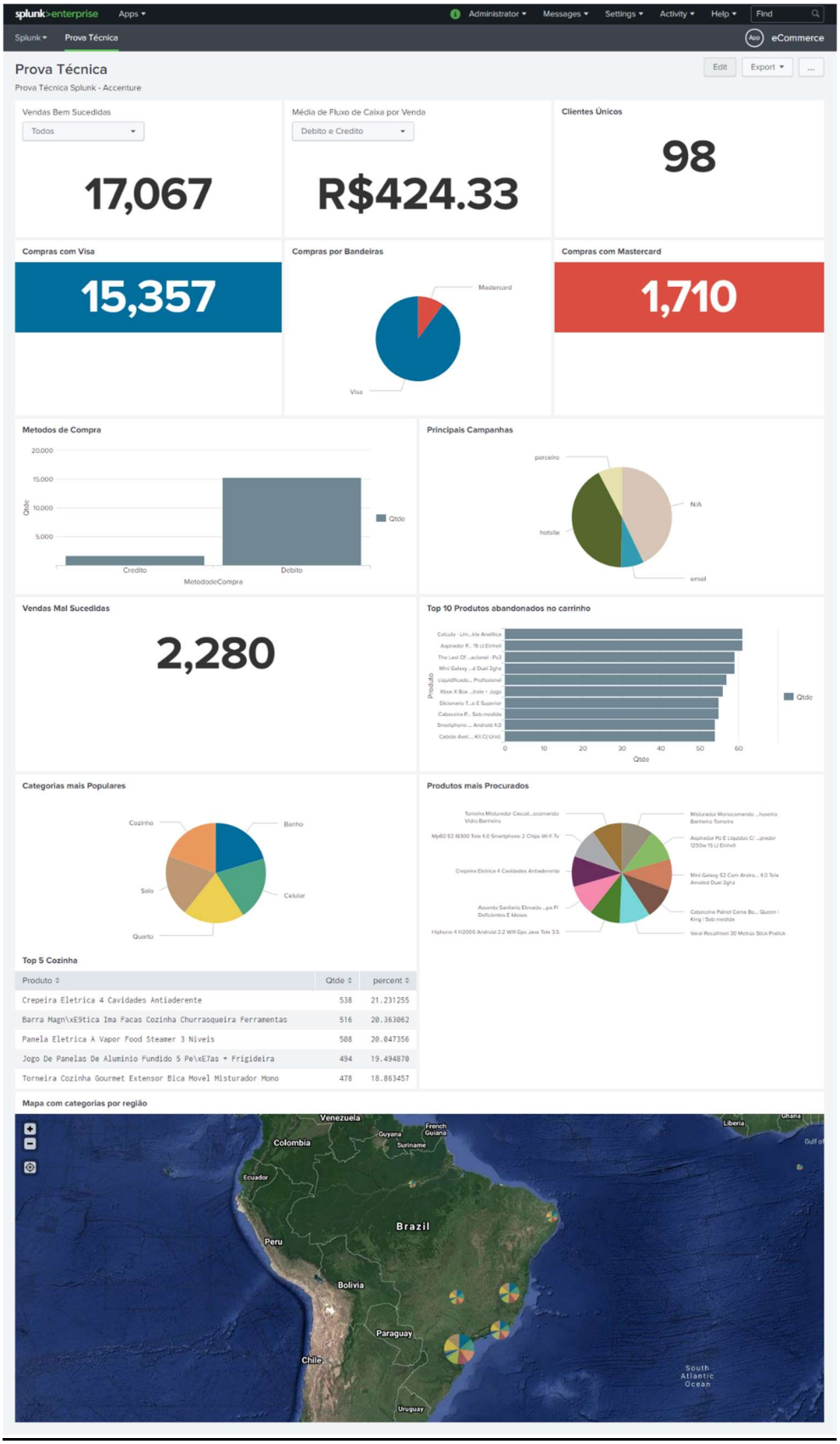
Com base nas **Boas Práticas**, decidi criar uma App exclusiva para o projeto (**App-eCommerce**), contendo **Index**, **SourceType**, **Lookups**, **Dashboard** e um sistema de menu facilitando a navegação.

Menu de navegação

```
<nav search_view="search">
  <collection label="Splunk">
    <view name="search" default='true' />
    <view name="analytics_workspace" />
    <view name="datasets" />
    <view name="reports" />
    <view name="alerts" />
    <view name="dashboards" />
  </collection>
  <view name="prova_tecnica" />
</nav>
```



Desenvolvimento da Dashboard



Boa Prática – Search Flutuante

Devido a dashboard estar executando 13 **searchs** simultâneas, foi possível reduzir as mesmas a apenas 1 **search**, através da **Boa Prática de Search Flutuante**.

```
<search id="query_flutuante">
   <query>
      index="ecommerce"
      | table Vendeu Valor IP Bandeira MetododeCompra Campanha Categoria Produto
   </query>
   <earliest>0</earliest>
   <latest></latest>
</search>
```

E utilizando nos painéis da seguinte maneira:

```
<search base="query_flutuante">
   <query>
         | search Vendeu=1 Categoria="$categoria_selecionada$"
         | stats count as Qtde
   </query>
</search>
```

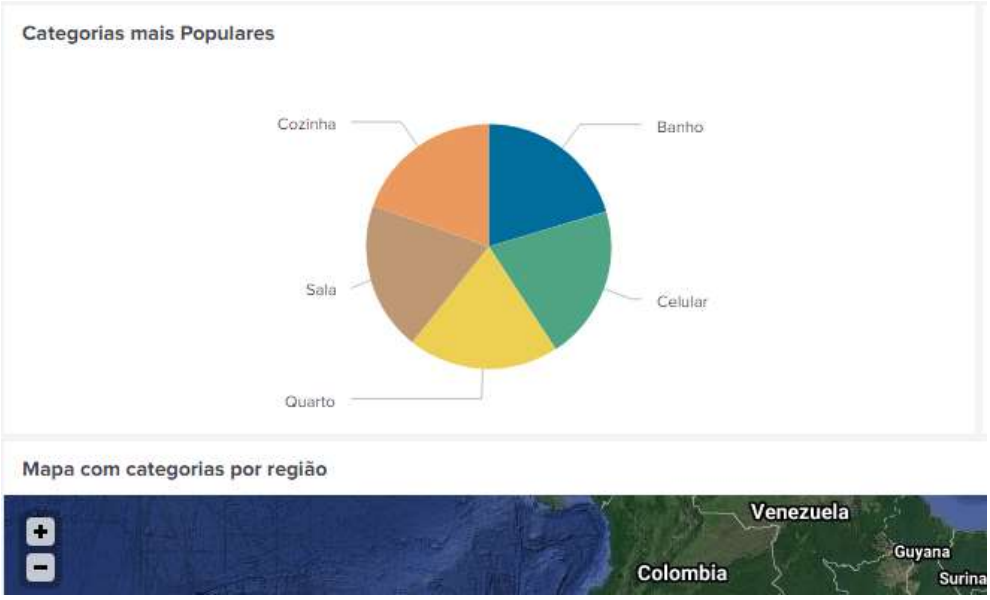
Filtros / Inputs exclusivos em painel

Observando que cada painel já atendia a sua Search de uma forma específica, optei por criar Inputs exclusivos para determinados painéis, com o objetivo de refinar seus insights.

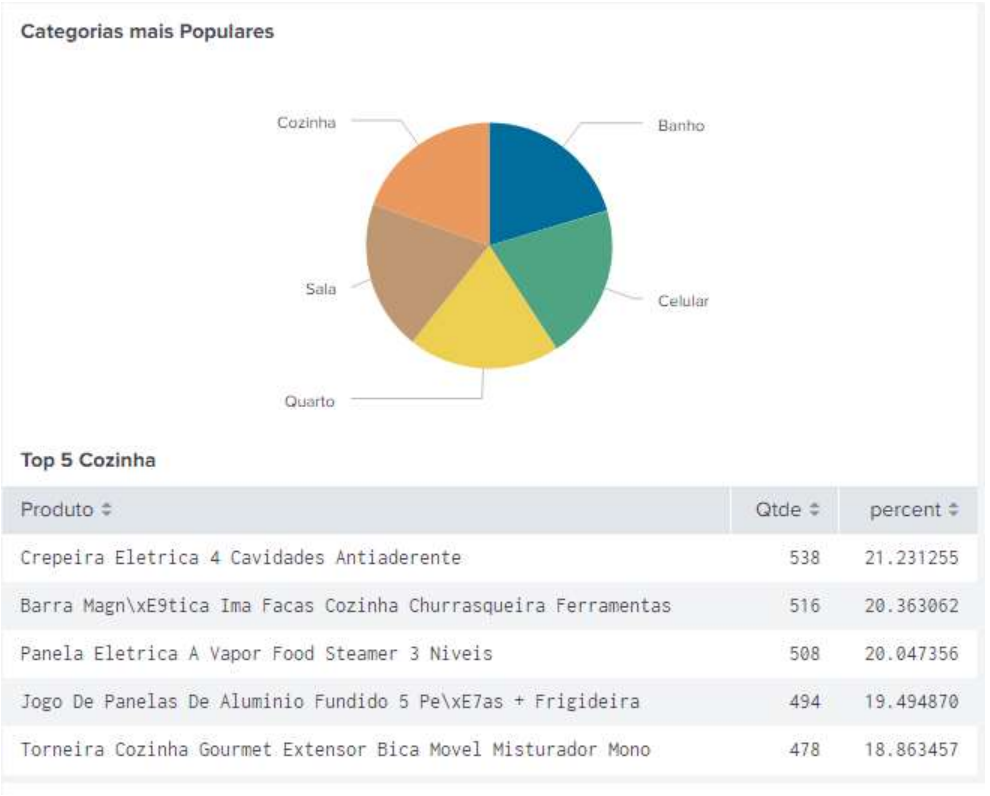

```
<input type="dropdown" token="categoria_selecionada" searchWhenChanged="true">
    <label>Vendas Bem Sucedidas</label>
    <fieldForLabel>Categoria</fieldForLabel>
    <fieldForValue>Categoria</fieldForValue>
    <search base="query_flutuante">
        <query>
            | dedup Categoria
            | table Categoria</query>
    </search>
    <choice value="*">Todos</choice>
    <default>*</default>
    <initialValue>*</initialValue>
</input>
```

Drilldown

Optei por criar um **drilldown** no painel **Categorias mais Populares**, apresentando um ranking com os 5 produtos mais vendidos da categoria selecionada.



O mesmo permanece oculto até que o usuário clique na categoria de seu interesse.



Produto	Qtde	percent
Crepeira Eletrica 4 Cavidades Antiaderente	538	21.231255
Barra Magn\xE9tica Ima Facas Cozinha Churrasqueira Ferramentas	516	20.363062
Panela Eletrica A Vapor Food Steamer 3 Niveis	508	20.047356
Jogo De Panelas De Aluminio Fundido 5 Pe\xE7as + Frigideira	494	19.494870
Torneira Cozinha Gourmet Extensor Bica Movel Misturador Mono	478	18.863457

```
<panel>
    <chart>
        <title>Categorias mais Populares</title>
        <search base="query_flutuante">
            <query>
                | top 5 Categoria
                | rename count as Qtde</query>
        </search>
        <option name="charting.chart">pie</option>
        <option name="charting.drilldown">all</option>
        <drilldown>
            <set token="categoria_popular">$click.value$</set>
        </drilldown>
    </chart>
    <table depends="$categoria_popular$">
        <title>Top 5 $categoria_popular$</title>
        <search base="query_flutuante">
          <query>
            | where Categoria="$categoria_popular$"
            | top 5 Produto
            | rename count as Qtde Percent as Porcentagem
          </query>
        </search>
        <option name="drilldown">none</option>
    </table>
</panel>
```