



Instituto Infnet

INSTITUTO INFNET - Centro, Rio de Janeiro

MIT EM BIG DATA

ESTUDO SOBRE SPLUNK

**TRABALHO DE CONCLUSÃO DO SEGUNDO BLOCO DO CURSO DE PÓS
GRADUAÇÃO**

ALLAN DA SILVA ANDRADE

FABIO DOMINGUES

NICOLAS MARCOS

RIO DE JANEIRO
2019

ESTUDO SOBRE AS FUNCIONALIDADES DO SPLUNK

ESTUDO SOBRE O SPLUNK PARA PROJETO
DE BLOCO APRESENTADO COMO
REQUISITO SEMESTRAL PELO INSTITUTO
INFNET.

Sumário

Resumo	3
Abstract.....	3
O que é o Splunk?	4
Instalação	6
Interação.....	8
Integração com soluções programadas	27
Arquitetura SPLUNK	29
Licenciamento.....	30
Conclusão.....	31
Referências Bibliográficas.....	31

Resumo

Este trabalho tem a finalidade de mostrar as funcionalidades da ferramenta de BigData SPLUNK.

Palavras-chave:

SPLUNK, licenciamento, conhecendo, empresas, funciona, armazenamento, relatórios e escalabilidade.

Abstract

This paper aims to show the features of the BigData SPLUNK tool.

Keywords:

SPLUNK, licensing, meeting, enterprise, works, storage, reporting and scalability.

O que é o Splunk?

O Splunk é uma das mais famosas plataformas de análise, agregamento, coleta e reconhecimento automático (de padrões de informação considerada como dado de máquina) em tempo real através de indexações através de alguma fonte.

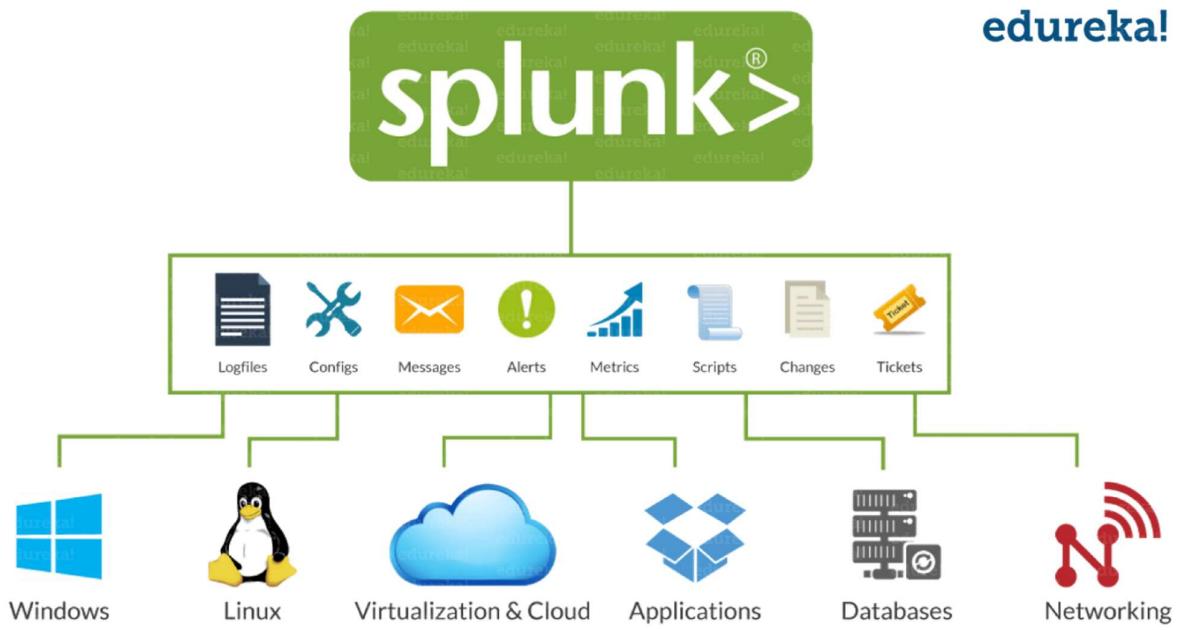
Podemos detalhar fontes como: Computadores, dispositivos de network, máquinas virtuais, dispositivos de internet, dispositivos de comunicação, sensores e databases.

Podemos detalhar dado como: Logs, configurações, mensagens, registros de detalhes da chamada, clickstreams, alerts, métricas, scripts, tickets.

As figuras abaixo ilustram alguns dados e fontes de máquina.

Index ANY data from ANY source





Um diferencial da plataforma Splunk é a não utilização de conectores. Sendo assim o desenvolvedor não precisa se preocupar em criar conectores e indexar em um novo tipo de padrão de informação lançado no mercado. O splunk automaticamente reconhece esse novo padrão e faz sua indexação. Organizando o dado em disco com uma taxa de compressão de até 60% do tamanho original. Os dados são armazenados no formato chave/valor.

Índice é como são chamados os repositórios do Splunk. Por padrão a ferramenta possui três (mas há possibilidade de outros serem criados) Splunk Enterprise armazena dados indexados em buckets, que são diretórios que contêm ambos data e arquivos indexado dentro do dado. Um índice, então, consiste em muitos buckets, organizados por idade dos dados.

O rótulo que irá determinar o tempo em que o dado foi coletado e identificado chama-se timestamp. Será através dele que se torna possível identificar sua idade, recebendo uma das cinco possíveis classificações: hot, warm, cold, frozen e thawed.

Hot: Os eventos com até 89 dias de vida, ou seja, um evento atual, será classificado desta forma onde poderão ter entre 1gb de tamanho ou 10gb em sistemas de 32bits ou 64bits respectivamente.

Warm: Se em até 90 dias não houver alteração ou se exceder o tamanho de arquivo do warm (de 1gb ou 10gb). O bucket do hot será migrado para warm e um novo diretório será criado.

Uma instalação padrão do Splunk poderá contar com até 300 Warm buckets. Quando for criado o Warm bucket número 301, o mais antigo bucket deste estágio será migrado para Cold.

Cold: Armazena os buckets que foram migrados de Warm. Neste estágio quando determinados buckets atingirem seis anos, eles serão migrados para Frozen; Cada bucket armazenado pode chegar até 500gb.

Frozen: Ao ser transferido para o Frozen, por padrão, o Splunk exclui permanentemente todos os buckets aqui presentes, além de terem os dados removidos do índice nesse momento. É possível arquivar os dados que são movidos pra cá, entretanto.

Thawed: Ao ser arquivados os dados permanecem “congelados” (frozen), este estágio, como o nome sugere, trata do “descongelamento”. Uma vez aqui, os buckets podem ficar lá o tempo que for necessário e deverão ser excluídos manualmente ou por script.

As buscas só ocorrerão no Splunk através dos buckets Hot, Warm e Cold (visto que no frozen há a exclusão automática como informado anteriormente).

As buscas ocorrem pelo Search App próprio do Splunk. É nele que será possível serem escritas consultas para extrair informações que terão valor.

Além disso, como o Splunk trabalha com ambos dados estruturados e não estruturados, ele Trabalha com uma linguagem própria de consulta aos dados indexados que é conhecida por Linguagem de Processamento de Busca (SPL, do inglês Search Processing Language). Sua sintaxe foi baseada em processos Unix juntamente com a linguagem SQL.

Através das buscas realizadas pela Search App é possível criar relatórios próprios baseados em diversos gráficos como o Line, Area, Bar, Map e claro, o famoso pie e assim serem salvos em um painel onde poderá não só conter esses gráficos como alertas.

Assim sendo, o Splunk consegue entregar o que tem defendido como sua missão: “tornar os dados de máquina acessíveis, utilizáveis e valorizados por todos”.

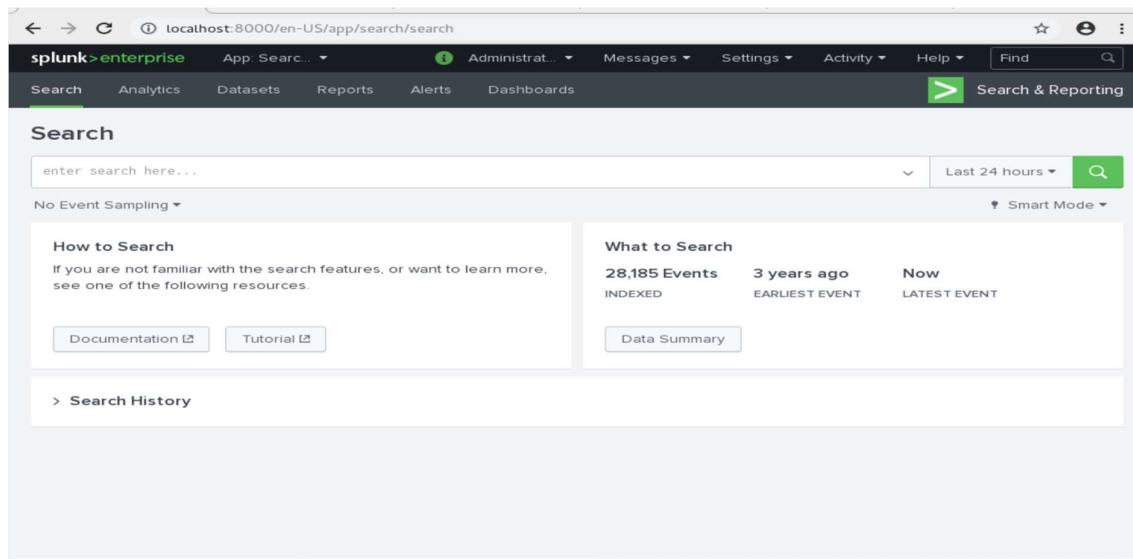
Instalação

A instalação do Splunk pode ocorrer diretamente através do download do software para o sistema operacional desejado. O Splunk possui suporte a sistemas operacionais baseados em Linux, bem como Windows e Mac OS.

Uma vez que o objetivo deste estudo consiste em análise e entendimento da arquitetura e possibilidades da plataforma Splunk, foi utilizada uma imagem docker com instância do Splunk Enterprise, de modo a encapsular as dependências da aplicação de modo independente ao sistema operacional, permitindo à equipe maior dedicação na utilização da ferramenta.

Os comandos abaixo foram testados em uma instância CentOS para instalação do Docker. Em caso de tentativa de instalação em Sistema Operacional diferente, recomenda-se verificar o procedimento de instalação no hospedeiro desejado.

```
--Instala o docker  
yum -y install docker-io  
  
--Verifica o estado do serviço docker  
systemctl status docker  
  
--Starta o docker container  
systemctl start docker  
  
--Lista os containers ativos  
docker ps  
  
--Faremos a instalação de uma imagem docker presente no dockerhub  
--Maiores detalhes podem ser consultados no https://hub.docker.com/r/splunk/splunk/  
docker pull splunk/splunk  
  
--Cria um docker de splunk com 2 volumes: 1 para processos (var) e outro para dados (etc)  
--Para essa abordagem a exclusão o diretório de processos não afetará os dados  
importados no Splunk  
--Onde está MINHA_SENHA, coloque a senha desejada  
docker run --name splunk-mount -v opt-splunk-etc:/opt/splunk/etc -v opt-splunk-  
var:/opt/splunk/var/ -d -p 8000:8000 -e SPLUNK_START_ARGS=--accept-license -e  
SPLUNK_PASSWORD=MINHA_SENHA splunk/splunk:latest  
  
--Lista os volumes  
docker volume ls  
  
--Acessa os volumes no SO  
cd /var/lib/docker/volumes  
ls  
cd opt-splunk-etc/  
ls  
  
--Verificaremos o ID do container docker  
Docker os -a  
  
--No parâmetro CONTAINER_ID, informe o ID da imagem Splunk captado no passo anterior  
Docker start CONTAINER_ID  
  
--Em nosso estudo, o container ID foi 610247a88e6d. Logo, a execução ocorrerá através do  
comando abaixo:  
Docker start 610247a88e6d  
  
--A partir deste momento, você deve estar apto a acessar o Splunk através de seu  
navegador
```



Observação: Em ambientes produtivos, recomenda-se a adoção de modelos que separem em servidores os dados das estruturas de processos. Assim, a estrutura de processos em deve ser mantida em containers separados dos discos das estruturas de dados, de modo a possibilitar independência por equipes de infraestruturas das imagens de processos dos dados consumidos.

Interação

Nesta etapa, abordaremos alguns tutoriais com a utilização da ferramenta Splunk:

1) Criando relatórios de acessos

Objetivo: Criaremos um relatório consumindo um arquivo de log de acessos gerado através de um servidor Linux, aplicando mecanismos de Search da ferramenta.

Nosso objetivo será responder através da ferramenta perguntas como:

Número total de tentativas falhas;

Lista de IPs destas tentativas;

Países que realizaram estas tentativas.

a) Instale o add-on de Linux

Realizaremos a instalação de um add-on comumente usado pelo Splunk, que facilita a leitura de logs Linux, realizando de maneira consistente o “parse” dessas informações e estruturando os dados com base em um source semi-estruturado.

Ao importar um dado no Splunk, é necessária uma expressão regular em linguagem nativa para que os dados sejam tratados de maneira estruturada. Porém, de modo a economizar

esforço, o Splunk possui diversos add-ons que já contém essas expressões, realizar o import dos dados já de maneira estruturada.

Para instalá-los, basta ir na Home do Splunk > Find More Apps e pesquisar pelo App desejado. Em seguida, caso ainda não o tenha instalado, um botão “Install” ficará habilitado. Basta se logar em sua conta Splunk e poderá efetuar o download.

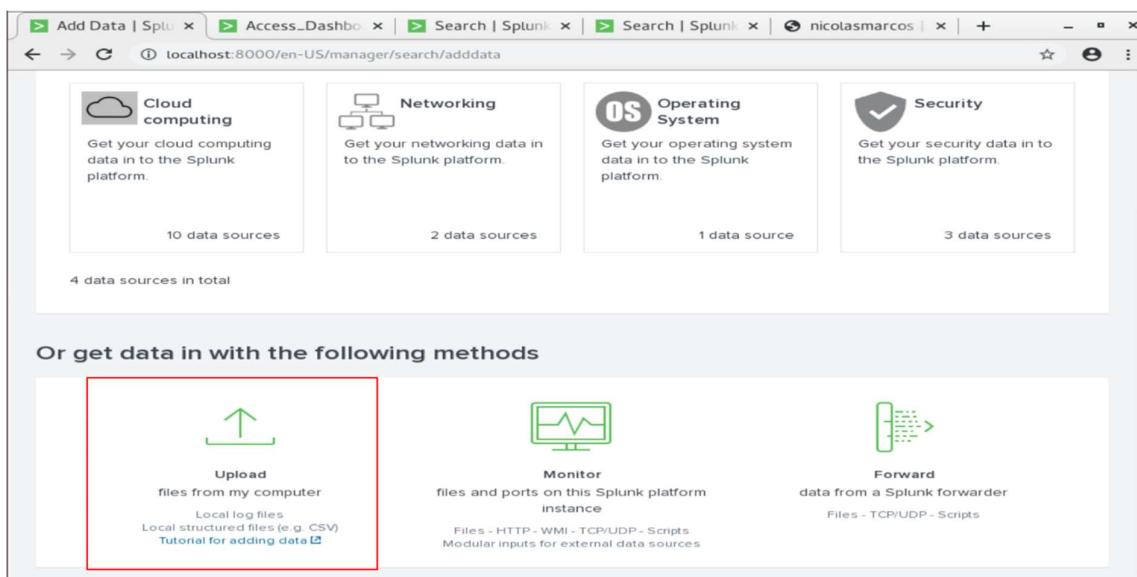
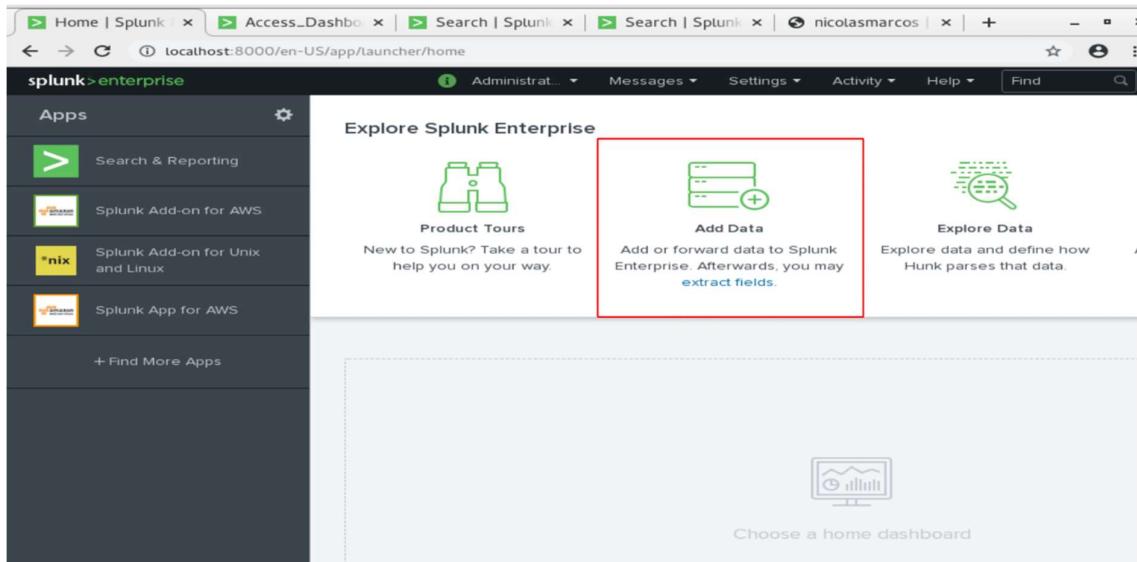
Para nosso exemplo, usaremos o add-on “Splunk add-on for Unix and Linux”

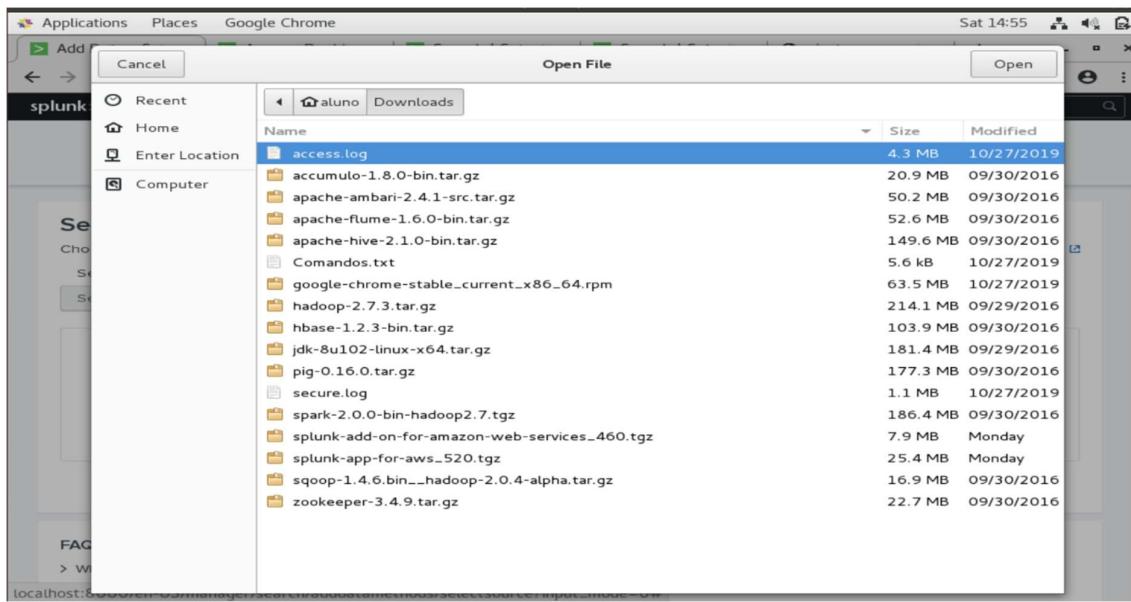
The screenshot shows the Splunk Enterprise home interface. On the left, there's a sidebar titled 'splunk>enterprise' with a 'Apps' section containing icons for 'Search & Reporting', 'Splunk Add-on for AWS', and 'Splunk App for AWS'. Below this is a red box highlighting the 'Find More Apps' button. The main content area is titled 'Explore Splunk Enterprise' and features three sections: 'Product Tours' (with a binoculars icon), 'Add Data' (with a server icon), and 'Explore Data' (with a magnifying glass icon). A large callout at the bottom says 'Choose a home dashboard' with a chart icon.

The screenshot shows the Splunk Apps Browser interface. At the top, there's a search bar with 'linux' typed in. The main area is titled 'Browse More Apps' and shows a list of 58 apps. A red box highlights the 'Splunk Add-on for Unix and Linux' entry, which has a yellow 'nix' category tag. The app details page shows a warning about index changes and upgrade instructions. Below this, another app, 'Linux Auditd', is shown with an 'Install' button.

b) Importe seu data source no Splunk

Uma vez instalado o add-on, ao realizarmos o import de um datasource o Splunk já reconhecerá padrões já utilizados e identificará seus dados de maneira estruturada. Sendo assim, para realizarmos o import de um dado, na Home do Splunk clicaremos em “Add Data”, escolheremos o arquivo “access.log” usado neste tutorial e o importaremos no Splunk.





The screenshot shows the 'Add Data' wizard in the Splunk interface. The title bar includes tabs like 'Add Data - Sele...', 'Access_Dashbo...', 'Search | Splunk...', 'Search | Splunk...', 'nicolasmarcos...', and a '+' button. The main navigation bar has links for 'splunk>enterprise', 'Apps', 'Administrat...', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below the navigation is a progress bar with steps: 'Selected Source' (green dot), 'Set Source Type' (white circle), 'Input Settings' (white circle), 'Review' (white circle), and 'Done' (white circle). Buttons for '< Back' and 'Next >' are at the bottom right.

Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)

Selected File: **access.log**

Select File

Drop your data file here

The maximum file upload size is 500 Mb

Done

FAQ

Na próxima tela, escolheremos importar o arquivo como tipo “access_combined_wcookie” e clicaremos em Next. Posteriormente, “Review” e em seguida “Submit” para realizar a importação de dados. Na próxima tela clicaremos em “Start Searching” para começarmos nossa exploração de dados.

Source: access.log

Source type: access_combined_wcookie

Time	Event
10/18/18 6:22:16 000 PM	209.160.24.63 - - [18/Oct/2018:18:22:16] "GET /product.screen?productId=WC-SH-A02&SESSIONID=SD0SL6FF7ADFF4953 H TTP 1.1" 200 3878 "http://www.google.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 349
2	10/18/18 6:22:16 000 PM

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options.

[Learn More](#)

Constant value
 Regular expression on path
 Segment in path

Host field value: c51d01d9fe90

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later.

[Learn More](#)

Index: Default [Create a new index](#)

Review

Input Type: Uploaded File
File Name: access.log
Source Type: access_combined_wcookie
Host: c51d01d9fe90
Index: Default

Success

✓ File has been uploaded successfully.

Configure your inputs by going to Settings > [Data Inputs](#)

[Start Searching](#) Search your data now or see [examples and tutorials](#).

[Extract Fields](#) Create search-time field extractions. [Learn more about fields](#).

[Add More Data](#) Add more data inputs now or see [examples and tutorials](#).

[Download Apps](#) Apps help you do more with your data. [Learn more](#).

[Build Dashboards](#) Visualize your searches. [Learn more](#).

Perceba que os dados foram devida importados o Splunk identificou itens como ações, dias e horários e outros.

The screenshot shows a Splunk search interface with multiple tabs open. The main search bar contains the query `source="access.log" host=c51d01d9fe90`. The results table has 20 items per page, with the first item selected. The event details show a POST request from 182.236.164.11 at 10/25/18 6:20:55 PM. A modal window is open over the results, titled 'JSESSIONID', showing a table of top 10 JSESSIONID values and their counts.

Top 10 Values	Count	%
SD10SL8FF5ADFF31078	24	0.176%
SD8SL7FF4ADFF20541	23	0.169%
SD9SL6FF7ADFF31619	22	0.161%
SD3SL1FF3ADFF51051	21	0.154%
SD0SL1FF8ADFF11838	21	0.154%
SD10SL5FF2ADFF39953	21	0.154%
SD1SL1FF4ADFF24047	21	0.154%
SD2SL2FF8ADFF26256	21	0.154%

O mesmo processo deverá ser repetido para o arquivo “secure.log”, com a diferença que na etapa de escolha do tipo de arquivo, escolheremos “linux_secure” ao invés de “access_combined_wcookie”. Com ambos arquivos importados, poderemos começar nossas searchs.

c) Crie sua search, aplicando os filtros desejados

Aqui, responderemos às perguntas citadas anteriormente:

i) Número total de tentativas falhas

Aplique a seguinte search e obterá o resultado esperado abaixo:

```
source="secure.log" action=failure | stats count
```

The screenshot shows a Splunk search interface with a search bar containing the query `source="secure.log" action=failure | stats count`. The results table has 20 items per page, with the first item selected. The table shows a single row with the value 8111 under the 'count' column.

count
8111

Neste exemplo, a sintaxe do comando informa que está sendo realizada uma search sob o source "secure.log", filtrando o campo "action" aonde o resultado seja "failure" e realizando um count sob os registros que atendem esse cenário.

- ii) Lista de IPs destas tentativas;

Aplique a seguinte search e obterá o resultado esperado abaixo:

```
source="secure.log" action=failure | stats count by src
```

The screenshot shows the Splunk Enterprise search interface. The search bar contains the command: `source="secure.log" action=failure | stats count by src`. The results table has a header row with columns: src and count. The data below shows 178 entries, with the first few rows being:

src	count
107.3.146.207	98
108.65.113.83	35
109.169.32.135	150
110.138.30.229	45
110.159.208.78	57
111.161.27.20	23
112.111.162.4	22
117.21.246.164	39
118.142.68.222	1

Neste exemplo, a sintaxe do comando informa que está sendo realizada uma search sob o source "secure.log", filtrando o campo "action" aonde o resultado seja "failure" e realizando um count sob os registros, agrupando por IPs que atendem esse cenário.

- iii) Países que realizaram estas tentativas.

Aplique a seguinte search e obterá o resultado esperado abaixo e escolha na opção de visualização a opção "Cluster Map":

```
source="secure.log" action=failure | iplocation src | geostats count by Country
```



Neste exemplo, a sintaxe do comando informa que está sendo realizada uma search sob o source “secure.log”, filtrando o campo “action” aonde o resultado seja “failure” e realizando um count sob os registros e, com base nos IPs, identificando os Internet Service Providers, e por sua vez o país dos mesmos.

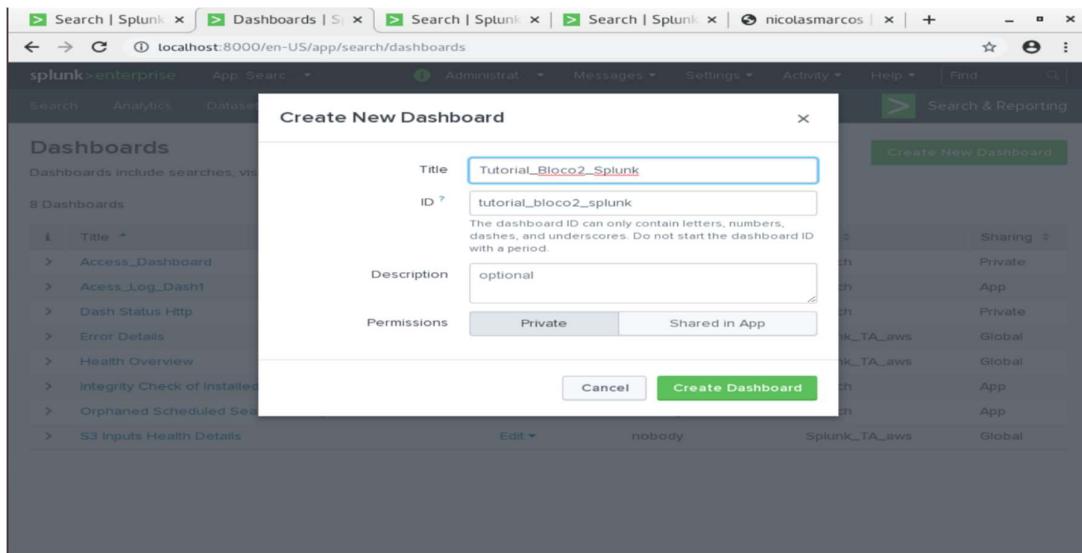
2) Criação de dashboard

Neste tutorial, criaremos um dashboard. Para tal, clique em “Dashboards” > “Create New Dashboard”

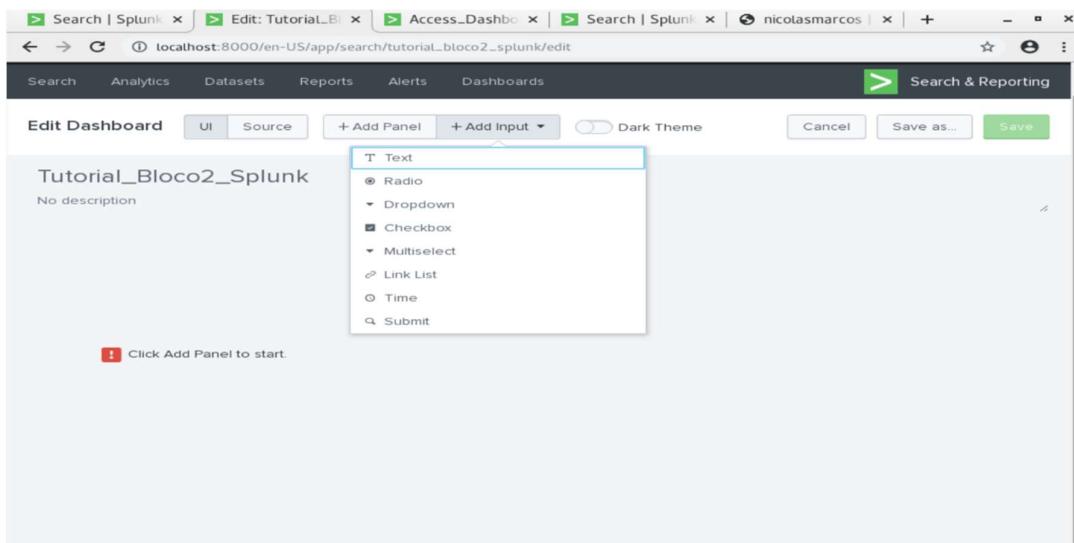
The screenshot shows the Splunk “Dashboards” page. At the top, there is a navigation bar with “splunk>enterprise” and several dropdown menus. Below the navigation is a search bar labeled “Search & Reporting”. The main area is titled “Dashboards” and contains the following text: “Dashboards include searches, visualizations, and input controls that capture and present available data.” A green “Create New Dashboard” button is highlighted with a red box. Below this, there is a table listing 8 Dashboards:

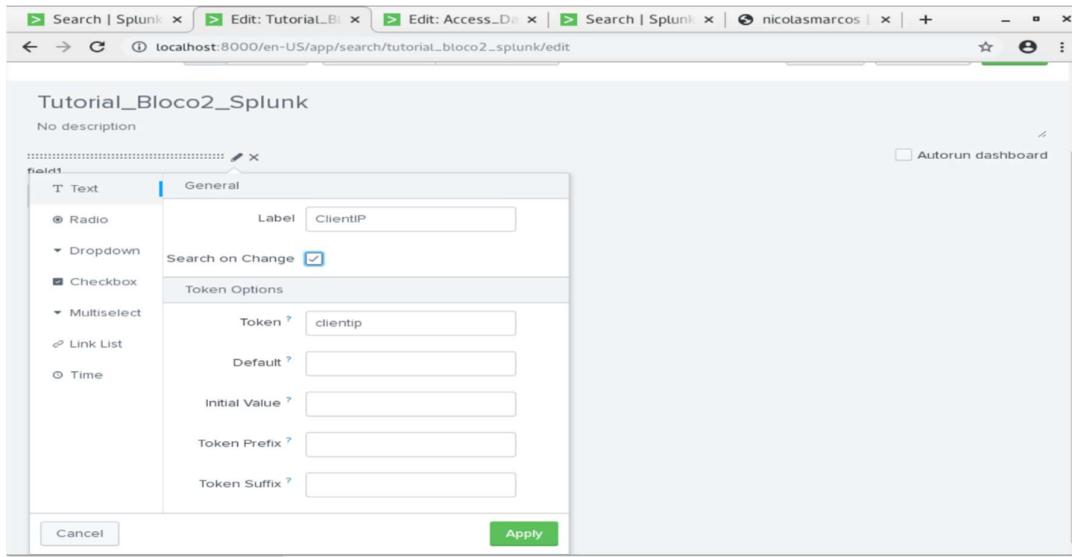
i	Title	Actions	Owner	App	Sharing
>	Access_Dashboard	Edit	admin	search	Private
>	Access_Log_Dash1	Edit	admin	search	App
>	Dash Status Http	Edit	admin	search	Private
>	Error Details	Edit	nobody	Splunk_TA_aws	Global
>	Health Overview	Edit	nobody	Splunk_TA_aws	Global
>	Integrity Check of Installed Files	Edit	nobody	search	App
>	Orphaned Scheduled Searches, Reports, and Alerts	Edit	nobody	search	App
>	S3 Inputs Health Details	Edit	nobody	Splunk_TA_aws	Global

Nomeie seu dashboard e clique em “Create Dashboard”



Na criação do dashboard, criaremos um campo texto de busca pelo IP do cliente. Para tal, clique em Input.

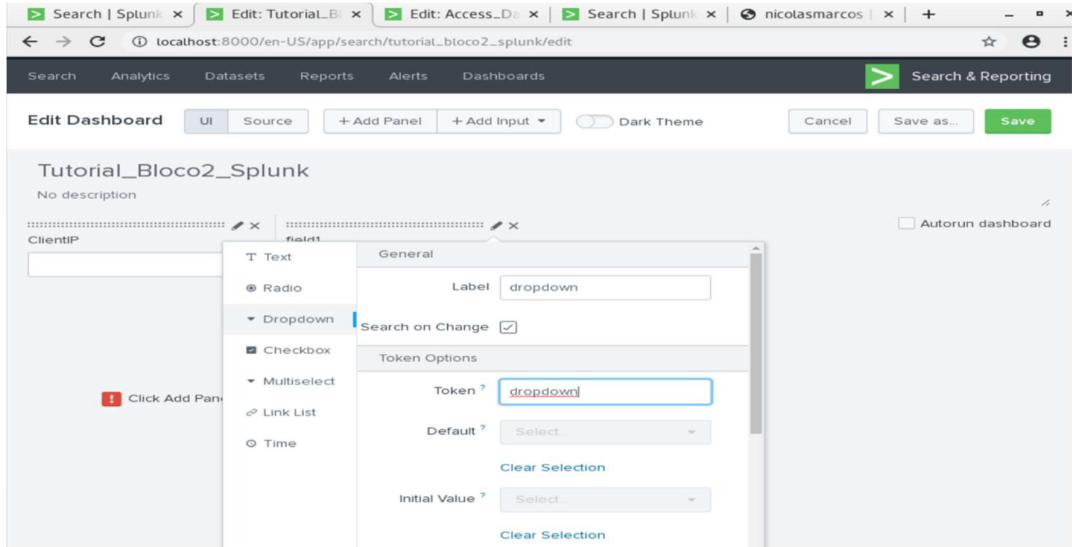


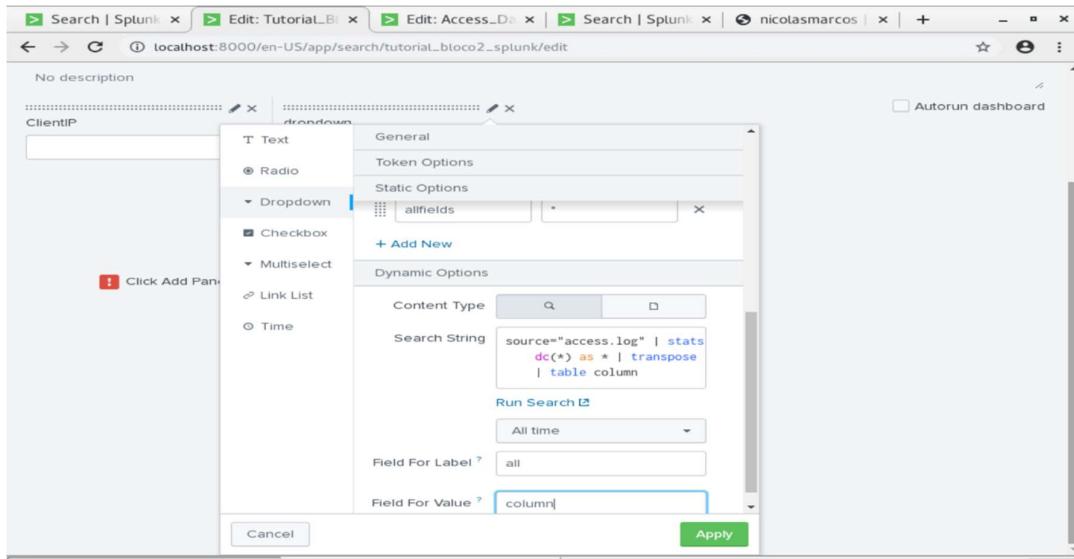


Abaixo de nosso dashboard, deixaremos uma tabela que apresente uma listagem das informações daquele IP que estamos consultando. Porém, pode ser que não seja necessário ao usuário do dashboard visualizar todas as informações. Portanto, criaremos um menu dropdown que permitirá ao usuário escolher ver todas as colunas ou apenas uma.

Clique em “Add Input” > Dropdown e preencha conforme abaixo, utilizando a seguinte search:

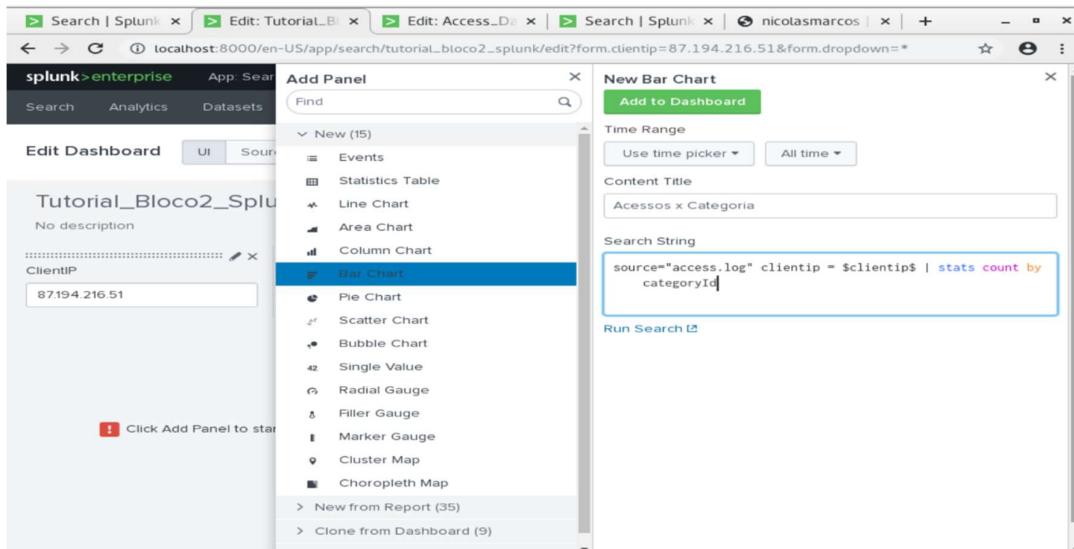
```
source="access.log" | stats dc(*) as * | transpose | table column
```

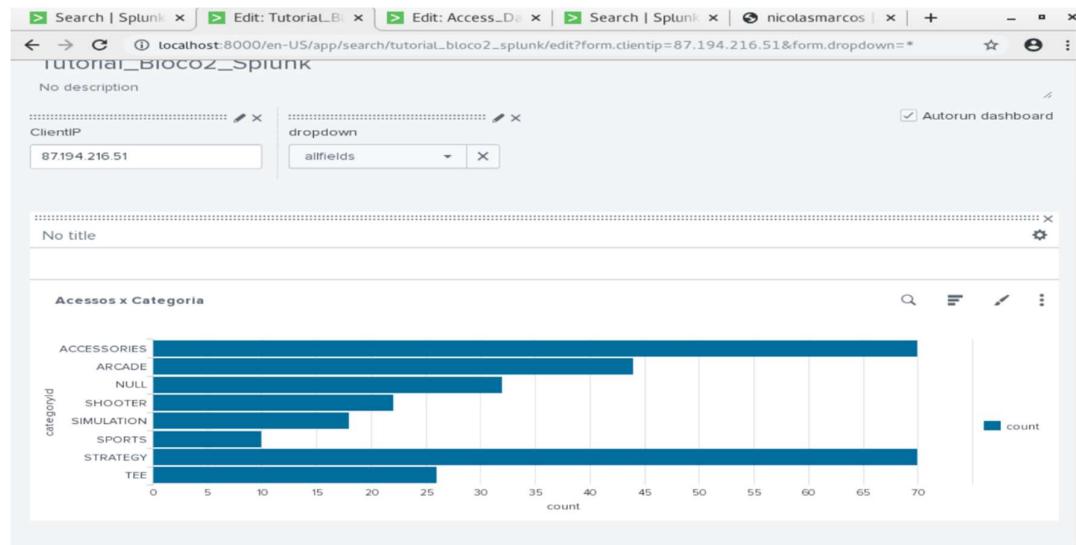




O próximo passo será criar o primeiro painel do dashboard. Criaremos um painel que apresente, com base no IP filtrado, os acessos x categoria de produtos. Clique em “Add Panel” > “New” > “Bar Chart”. Escolha a opção “All Time” no seletor de tempo por evento, nomeie seu painel e utilize a search abaixo. Após, clique em “Add to Dashboard”:

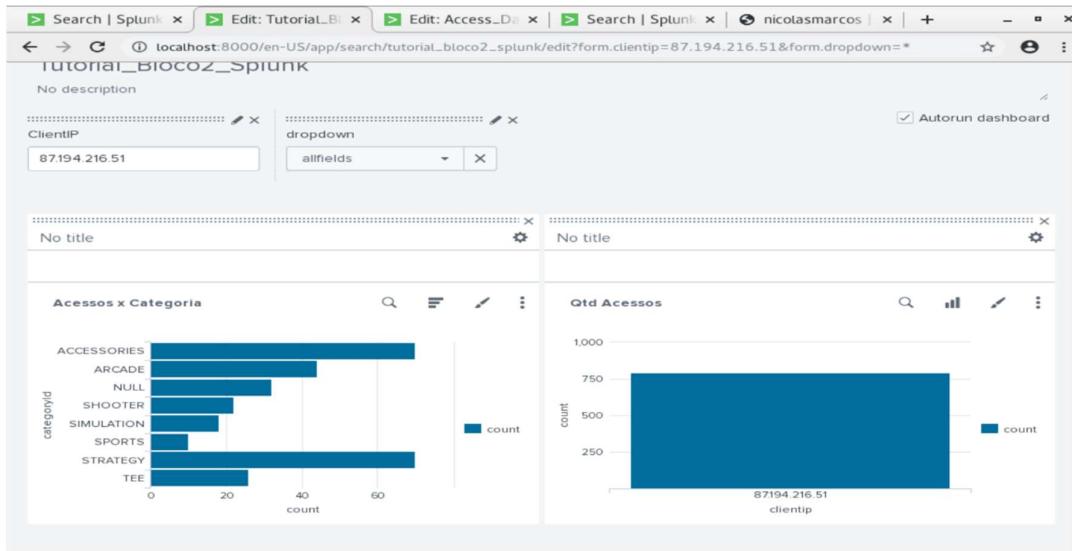
`source="access.log" clientip = $clientip$ | stats count by categoryId`





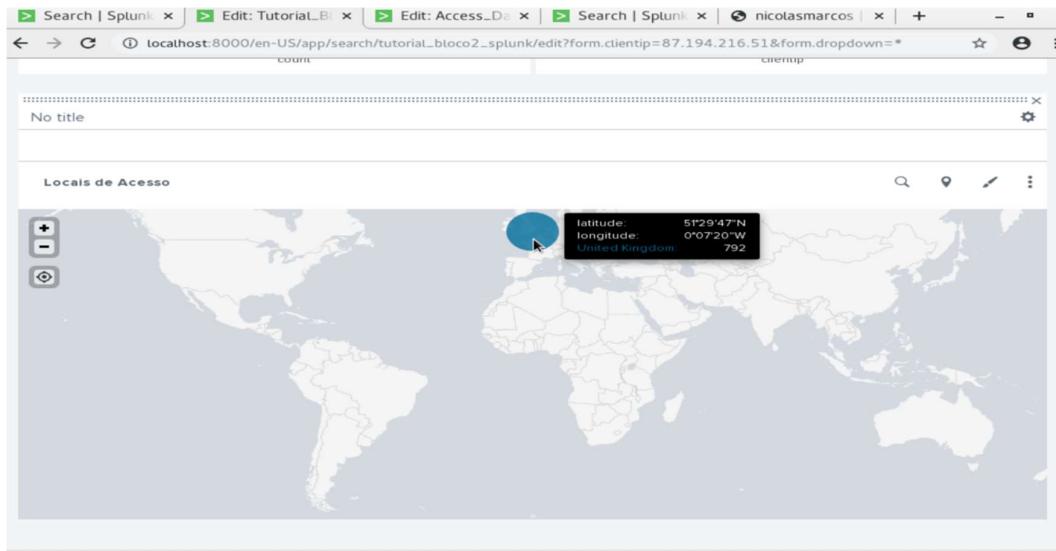
Criaremos agora um painel ao lado do anterior que apresente a quantidade de acessos do IP filtrado. Clique em “Add Panel” > “New” > “Column Chart”. Escolha a opção “All Time” no seletor de tempo por evento, nomeie seu painel e utilize a search abaixo. Após, clique em “Add to Dashboard”. Arraste o novo painel e o posicione ao lado do anterior:

```
source="access.log" clientip = $clientip$ | stats count by clientip
```



Criaremos um painel de mapa que apresente os acessos por país daquele IP. Clique em “Add Panel” > “New” > “Cluster Map”. Escolha a opção “All Time” no seletor de tempo por evento, nomeie seu painel e utilize a search abaixo. Após, clique em “Add to Dashboard”. Arraste o novo painel abaixo dos anteriores:

```
source="access.log" clientip = $clientip$ | iplocation clientip | geostats count by Country
```

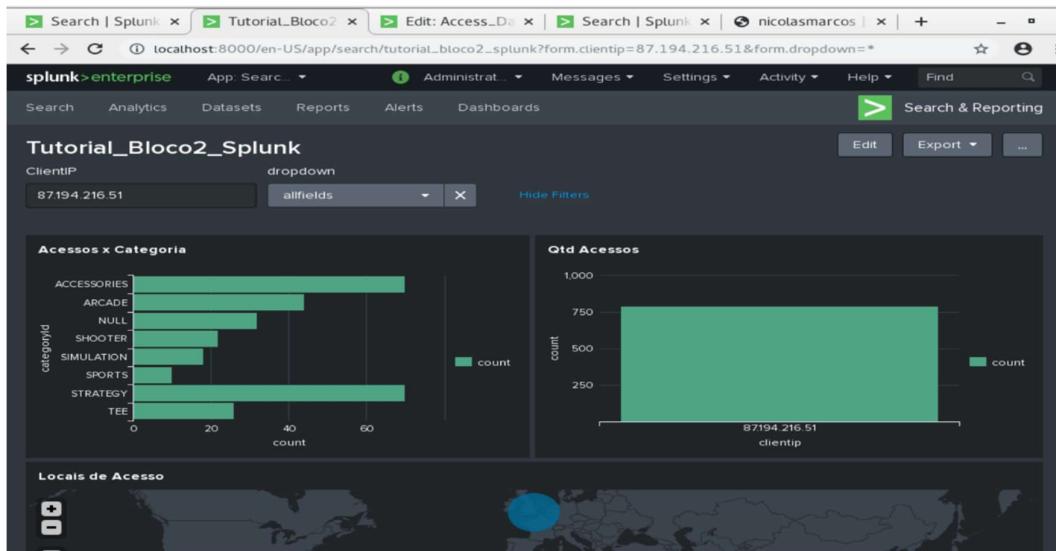


Para finalizar, criaremos a tabela com colunas em acordo aos inputs definidos anteriormente. Sendo no menu dropdown escolhida uma coluna, apenas esta ficará visível na listagem. Clique em “Add Panel” > “New” > “Statistics Table”. Escolha a opção “All Time” no seletor de tempo por evento, nomeie seu painel e utilize a search abaixo. Após, clique em “Add to Dashboard”. Arraste o novo painel abaixo dos anteriores:

```
source="access.log" | table $clientip$, $dropdown$
```

ClientIP	JSESSIONID	action	bytes	categoryid	clientip	cookie	date_hour	date_mday	date_minute
87.194.216.51	SD9SL8FF3ADFF20350	addtocart	1748		86.212.199.60		23	20	11
					1363	TEE			
					3265	SIMULATION	86.212.199.60	23	20

Se desejar, ao salvar seu dashboard, clique no seletor “Dark Theme” e salve. A aparência do seu dashboard mudará para uma visão mais escura que pode facilitar o foco nas informações.



3) Configuração de alertas e reports

Outra funcionalidade de relevância do Splunk é sua capacidade de se integrar com servidores de e-mail para gerar reports com base em eventos. Abordaremos neste tutorial como realizar a configuração de um report que periodicamente gere e-mails com base em uma consulta desejada. Não chegará a ser abordada a completa configuração de um servidor de e-mail com o ambiente, limitando-se apenas à criação e configuração da geração dos reports e alertas.

Em search, crie a consulta desejada sobre seus dados. Neste exemplo, serão consultadas as tentativas falhas de acessos. Para repetir esse processo, realize a search que segue:

```
source="secure.log" action="failure" | iplocation src | table src, Country | uniq
```

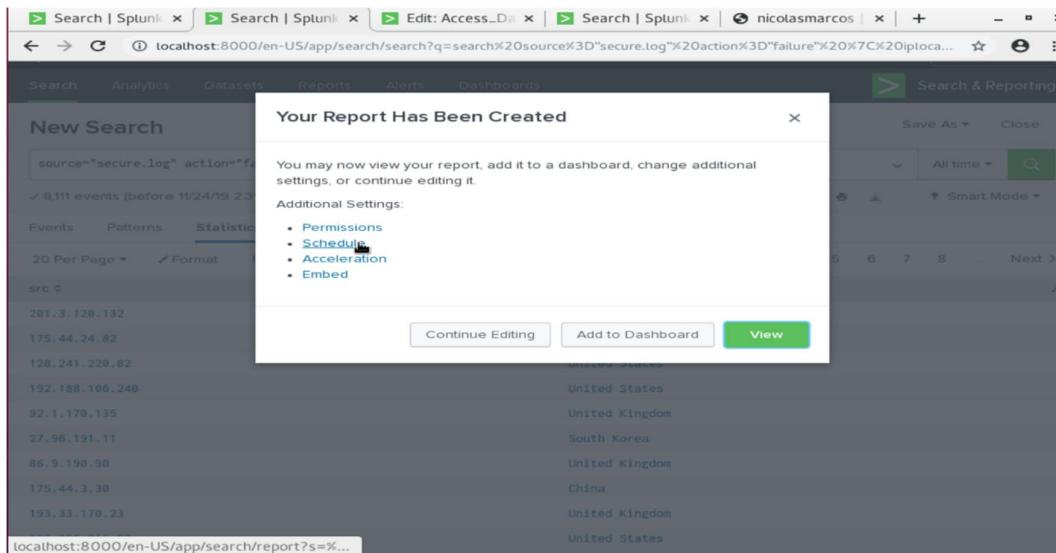
Após realizar a search, clique em “Save As” > “Report”. Configuraremos a partir deste ponto o report. Nomeie o report e clique em “Save”. Na tela seguinte, clique em “Schedule” para que possamos parametrizar a execução do report e definir ações ou triggers sob eles.

The screenshots show the Splunk web interface. The top screenshot displays a search results page with the following search query:
source="secure.log" action="failure" | iplocation src | table src, Country | uniq

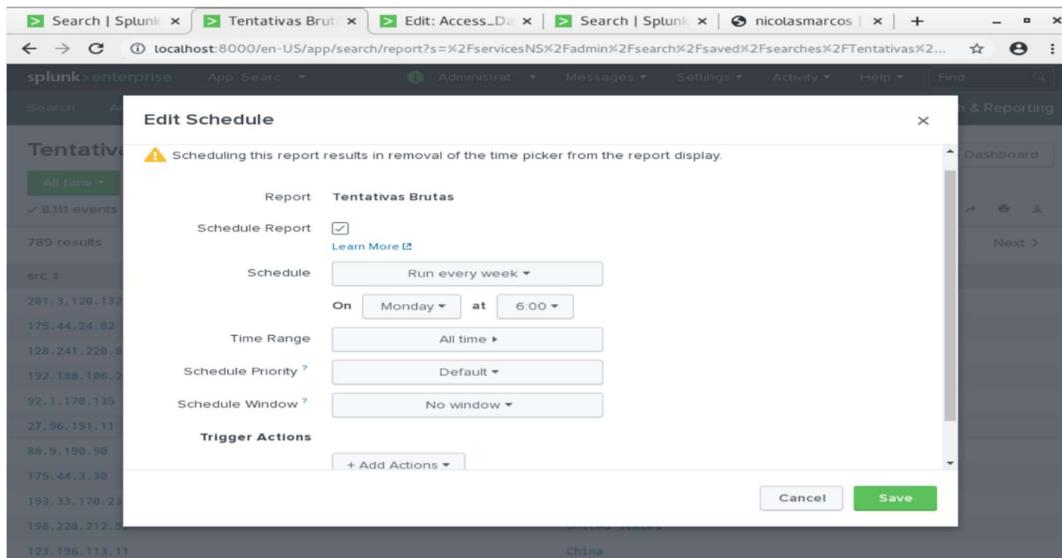
The results table shows 8,111 events from November 24, 2019, at 2:36:44.000 AM. The table lists IP addresses (src) and their countries (Country). The data includes:

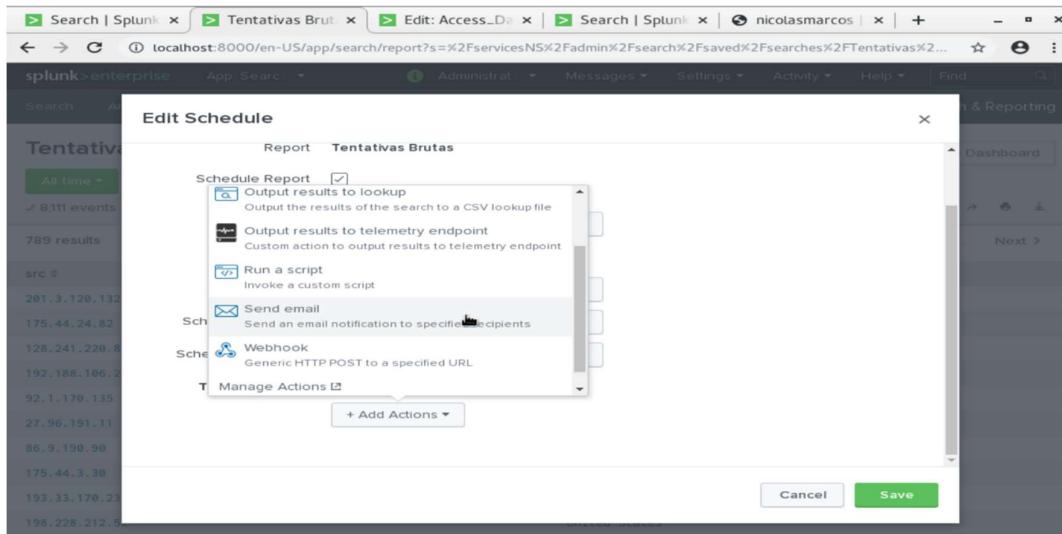
src	Country
201.3.120.132	Brazil
175.44.24.82	China
128.241.220.82	United States
192.188.106.240	United States
92.1.170.135	United Kingdom
27.96.191.11	South Korea
86.9.190.90	United Kingdom
175.44.3.30	China
193.33.170.23	United Kingdom

The bottom screenshot shows the 'Save As Report' dialog box. The title field is filled with 'Tentativas Brutas'. The content is set to 'Statistics Table'. The time range picker is set to 'All time'. There are 'Yes' and 'No' buttons for a time range picker setting. At the bottom right are 'Cancel' and 'Save' buttons.

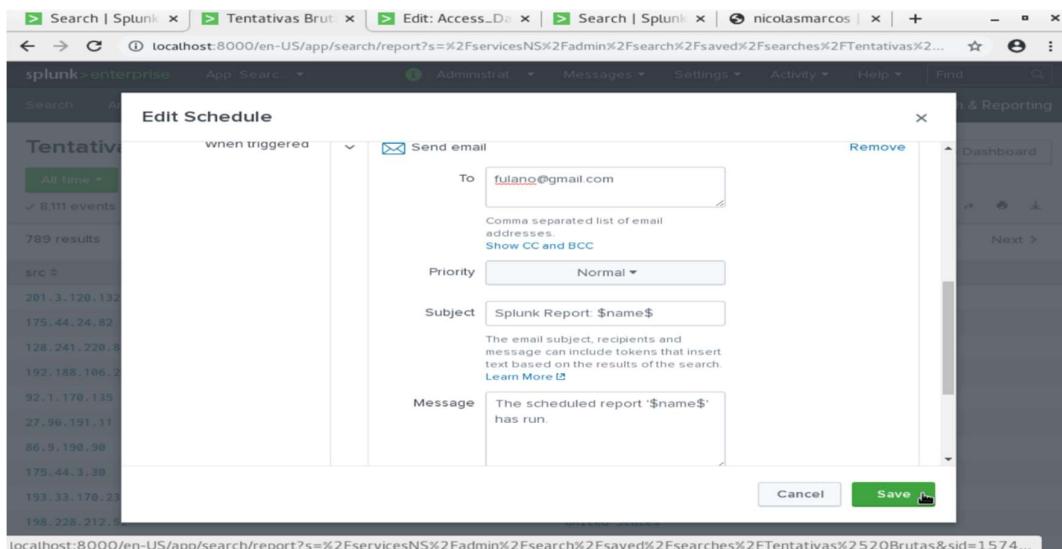


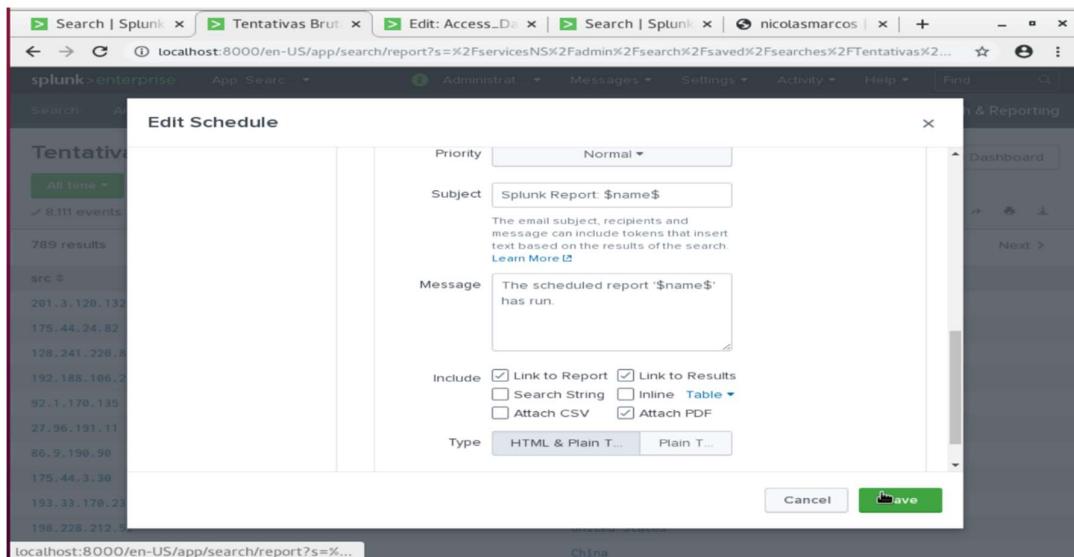
Na edição do schedule que se abrirá, poderemos configurar frequência de execução, dia da semana, hora, tempo de eventos que serão considerados, prioridades, entre outros. Em “Trigger Actions”, poderemos configurar ações a serem tomadas quando o schedule for executado. Configuraremos então o envio de um e-mail, clicando em “Add Actions” e escolhendo a opção “Send email”.





Nas configurações de e-mail, poderemos configurar lista de destinatários, assunto, conteúdo do e-mail, forma de envio de report (HTML ou PDF em anexo), entre outros. Ao finalizar as configurações, clique em “Save”. Uma tela sem o report aparecerá, isso ocorrerá porque ainda não há instâncias de execução do schedule. Uma vez que se dê momento (dia/data/hora) configuradas, o sistema gerará o report e realizará seu envio por e-mail.





Integração com soluções programadas

Conforme demonstrado ao longo dos exercícios, o Splunk possui plugins em seu esquema de add-ons que permitem integrações com diferentes tecnologias e fornecedores. Todavia, é necessário compreender na arquitetura Splunk um conceito chave que é a diferença entre add-ons e apps.

No Splunk, os add-ons atuam como plugins, normalmente destinados à ingestão e tratativa de dados, enriquecimento de dados, lookups, entre outros. Por sua vez, ao instalar no Splunk um app, este contém dentro de si uma gama de recursos específicos, como dashboards, searches específicas, reports, entre outros.

Utilizando um exemplo da integração com a plataforma AWS, caso fosse utilizado um add-on do Splunk com a AWS, este add-on se conectaría à plataforma AWS (uma vez que com as devidas configurações) e ingeriria os dados disponíveis no ambiente. Porém, não seria capaz de sozinho criar dashboards, reports e demais. Todavia, realizando a instalação de um app Splunk para AWS, este traria consigo uma série de dashboards e reports preparados com necessidades normalmente requisitadas.

A fonte de consulta para analisar melhor apps e add-ons é a Splunk Base (<https://splunkbase.splunk.com/>). Nela, é possível pesquisar e identificar apps e add-ons organizados por categorias, fornecedores, entre outros. Ainda, é possível verificar o tipo de sustentação adotado sob aquele app ou add-ons. São eles:

- Splunk supported: Apps e add-ons mantidos pela própria Splunk.
- Developer supported: Apps e add-ons mantidos pela própria entidade que o desenvolveu.
- Community supported: Apps mantidos pela comunidade Splunk.

De modo a corroborar o entendimento sobre a diferença entre apps e add-ons dentro da arquitetura Splunk, vide de exemplo as descrições fornecidas na Splunk Base sobre o add-on AWS (<https://splunkbase.splunk.com/app/1876/#/overview>) e o app de integração com a AWS (<https://splunkbase.splunk.com/app/1274/>)

O Splunk tem promovido novas aplicações focadas em áreas específicas, como segurança da informação e gerenciamento de eventos, inteligência de serviços de TI e comportamento de usuários.

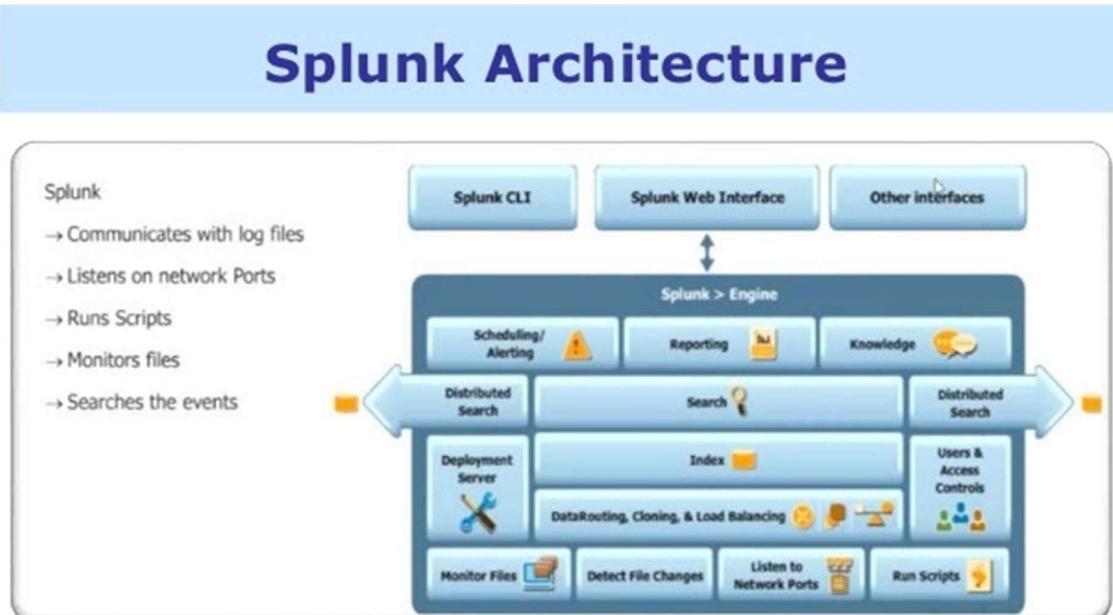
- Enterprise Security: https://www.splunk.com/en_us/software/enterprise-security.html
- IT Service: [splunk.com/en_us/software/it-service-intelligence.html](https://www.splunk.com/en_us/software/it-service-intelligence.html)
- User Behavior: https://www.splunk.com/en_us/software/user-behavior-analytics.html

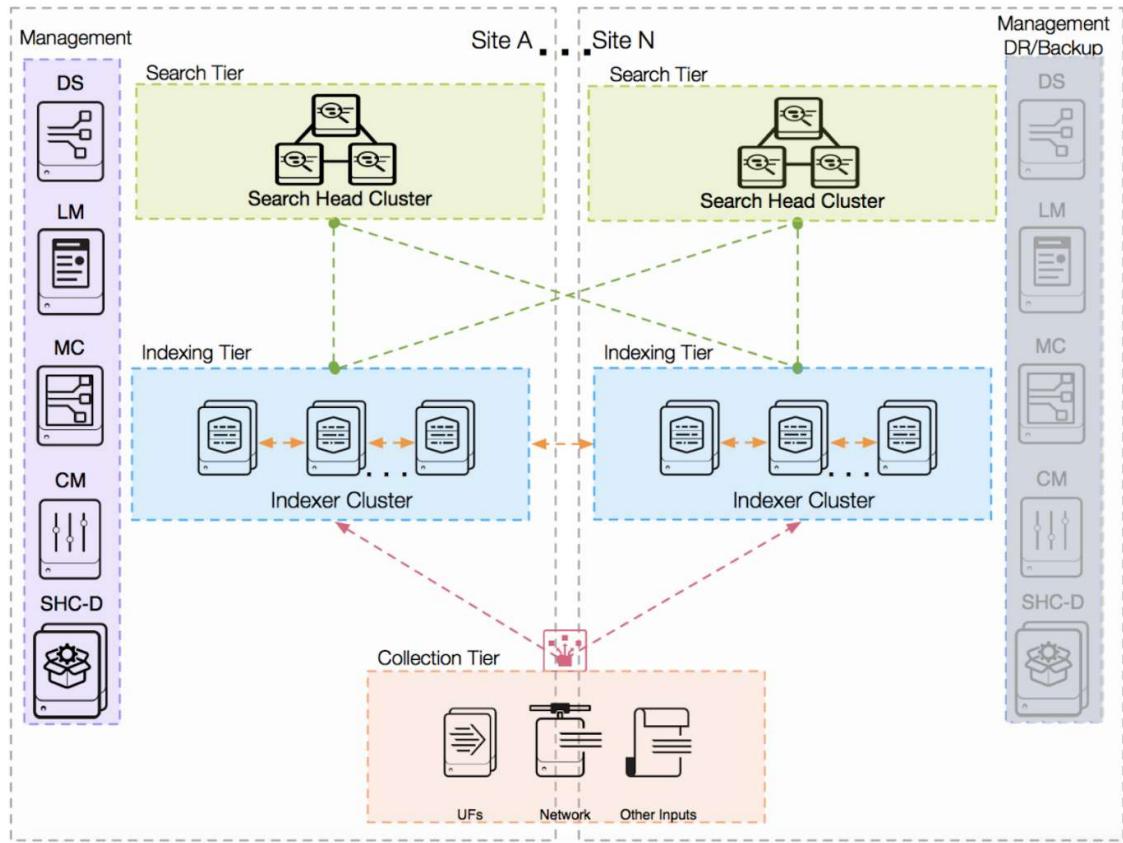
Em mercado, o Splunk tem sido líder no segmento de ferramentas de monitoramento de ambientes em segurança da informação e gerenciamento de eventos, permitindo em sua plataforma toda a arquitetura necessária, desde a ingestão de dados até a tratativa e criação de dashboards e reports.

Figure 1. Magic Quadrant for Security Information and Event Management



Arquitetura SPLUNK





Licenciamento

O Splunk possui alguns modelos principais de licenciamento. Sendo eles:

- Standard Splunk Enterprise License - On Premise: Oferece suporte a usuários ilimitados, escalabilidade, visualização real-time, dashboards, reports e demais recursos da ferramenta, consumindo infraestrutura local.
- Standard Splunk Enterprise License - Cloud: Oferece suporte a usuários ilimitados, escalabilidade, visualização real-time, dashboards e reports e demais recursos da ferramenta, consumindo infraestrutura cloud cedida pelo Splunk.
- Enterprise Trial License e Sales Trial License: Oferece os mesmos recursos que Enterprise License, por tempo limitado.
- Dev/Test License: Oferece os mesmos recursos da Enterprise License, pelo prazo de 6 meses e com limitação de processamento de 10GB/dia.

- Free License: Oferece suporte para um usuário, processamento de 500mb por dia, visualização em tempo real e mais alguns recursos da ferramenta.

Conclusão

O Splunk é uma plataforma universal de dados de máquina que possibilita que a organização aprenda com os dados que já possui assim como com os dados que são gerados diariamente em suas operações.

Os dados são coletados e o Splunk os armazena em disco nos chamados “buckets”, e usa mecanismos de indexação para que informações estejam sempre disponíveis com muita rapidez. Utilizando o Search App para gerar relatórios e gráficos para os membros dos diferentes departamentos possibilitando acompanhar a operação em tempo real.

Referências Bibliográficas

Sobre Splunk: <https://www.devmedia.com.br/splunk-monitorando-o-ambiente-de-ti-parte-1-revista-infra-magazine-10/27418>

Enterprise Security: https://www.splunk.com/en_us/software/enterprise-security.html

IT Service: https://www.splunk.com/en_us/software/it-service-intelligence.html

User Behavior: https://www.splunk.com/en_us/software/user-behavior-analytics.html

Zeal Vora - Curso Splunk 2019 - Beginner to Architect:

<https://www.udemy.com/course/splunk-beginner-to-architect/>