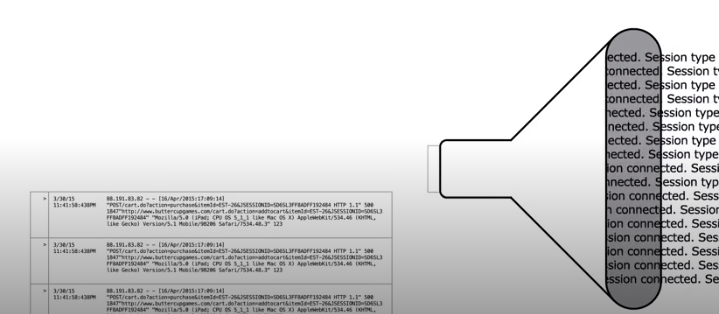
* **Módulo 1:**

Abaixo nós vemos o trabalho do Splunk. Pegando dados de máquina não estruturados e organizando-os em eventos para deixa-los estruturados:



* **Módulo 2:**

Abaixo nós vemos as funções que podemos fazer com o Splunk. Por exemplo, indexar dados, pesquisar e investigar os dados, adicionar conhecimento, visualizar alertas e realizar reportes e analises sobre os dados do sistema. Vale lembrar que basicamente o Splunk é uma fábrica que pega os dados bagunçados e que não estão estruturados e estrutura e organiza tudo certinho para que saiam dados organizados com base em Time Stamps e, com isso, possamos utiliza-los e fazermos analises:



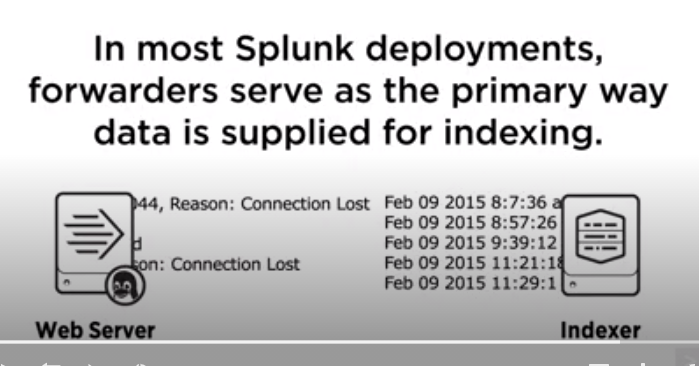
Temos alguns componentes no Splunk que nos ajuda neste trabalho árduo. O primeiro é o Indexer, que basicamente pega os dados não estruturados e coloca de forma estruturada no banco de dados do Splunk, conforme figura abaixo:



Outro componente que temos no Splunk são os Search Head, que servem para utilizarmos a linguagem de busca do Splunk para que possamos buscar nossos dados que estão armazenados nos servidores de indexers (onde ficam os dados após estruturação e organização):



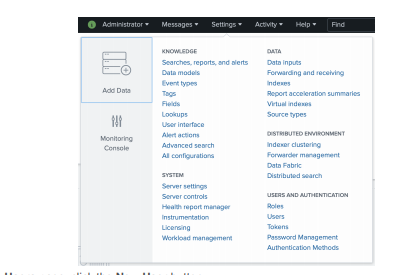
O outro componente do Splunk, o Forwarder serve para que possa ser enviado os dados brutos para o a organização que é feita no Indexer... Normalmente, por exemplo, se quisemos analisar um Web Server, instalamos neste Web Server o Forwarder para que possa enviar as informações que não estão estruturadas para o Indexer e assim para que o Indexer possa estrutura-los:



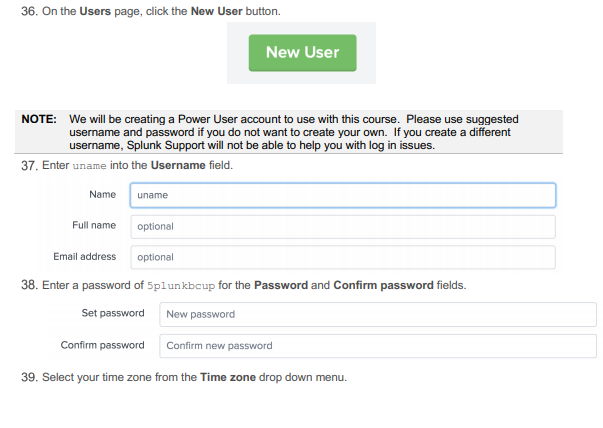
* **Módulo 3:**

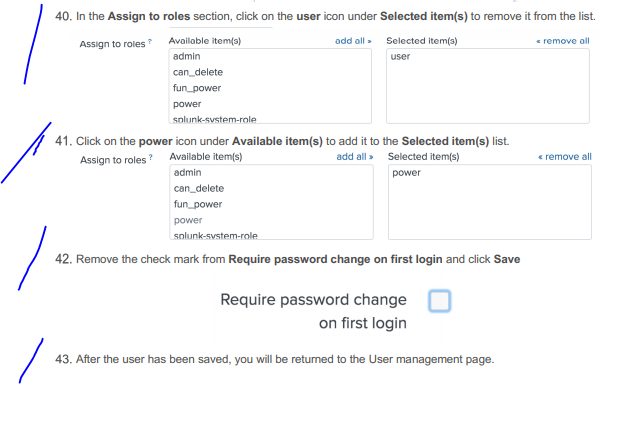
Agora neste módulo vamos fazer algumas tarefas como instalar e criar um usuário de nível Power no Splunk.

Para criarmos o usuário Power, primeiro vamos até o menu de configuração e clicamos em Users:



Agora dentro da página de Users clicamos em “New User” :

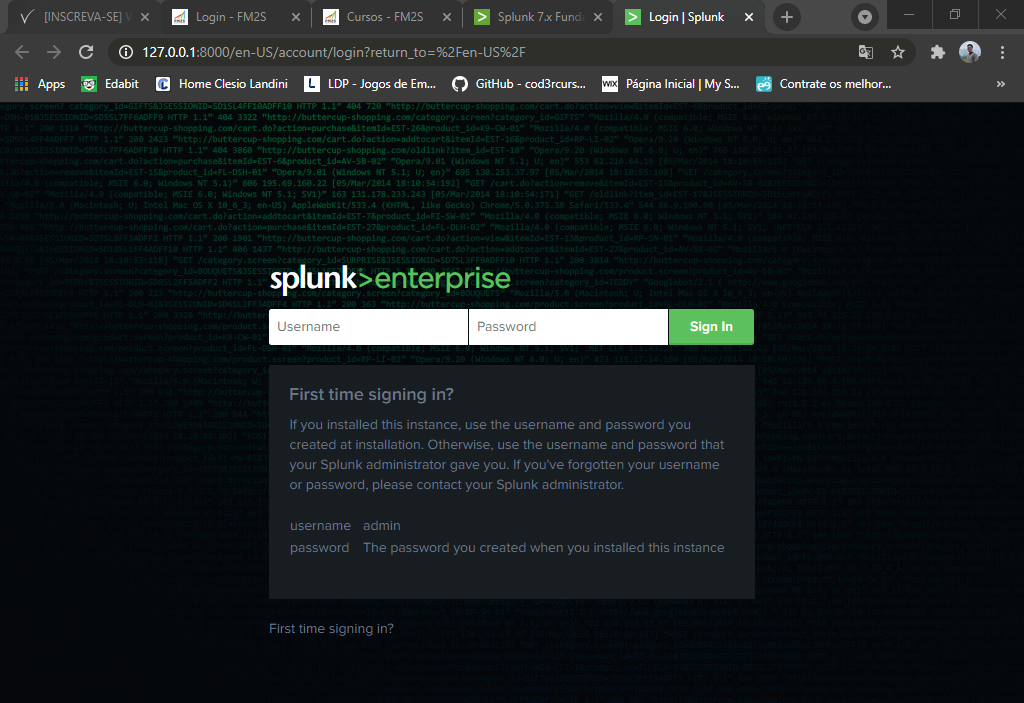




* **Módulo 4:**

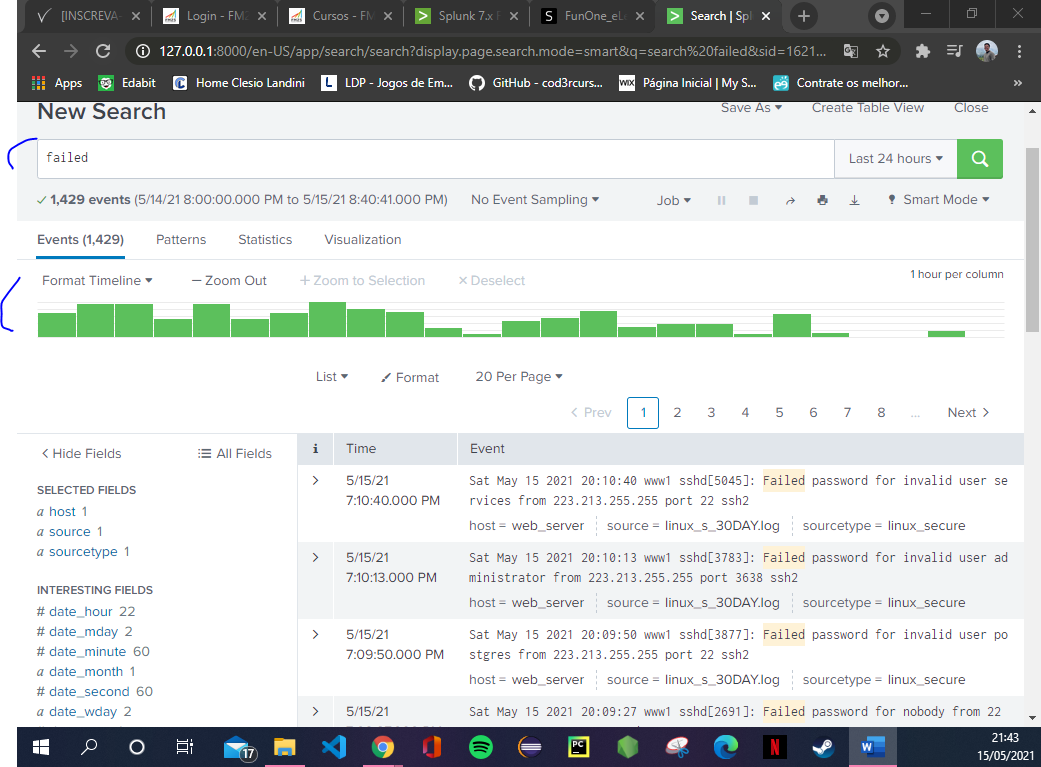
Agora neste módulo vamos Pegar e Inserir Dados dentro do Splunk. É uma boa prática separarmos nossos dados que inputamos em Indexers diferentes, para facilitar na hora da busca. Nós também podemos usar a opção de Monitorar na hora do input. Com isso podemos monitorar um arquivo de log de um servidor, de uma porta, de uma aplicação, de uma requisição HTTP sempre que houver um novo evento sempre atualizando.

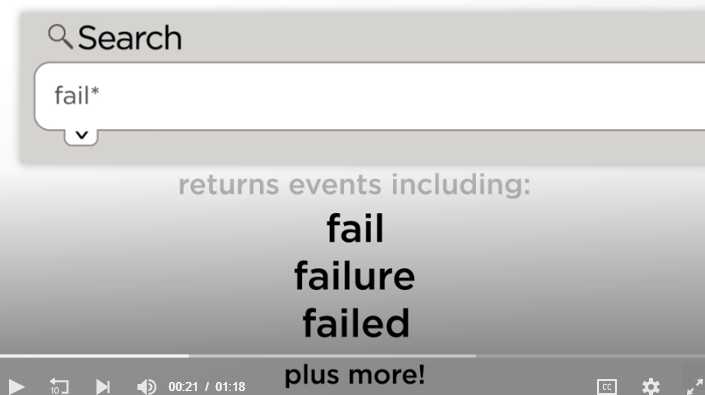
Vale lembrar que quando eu instalo o Splunk, ele abre no meu Browser no servidor local, na porta 8000, como na figura abaixo:



* **Módulo 5:**

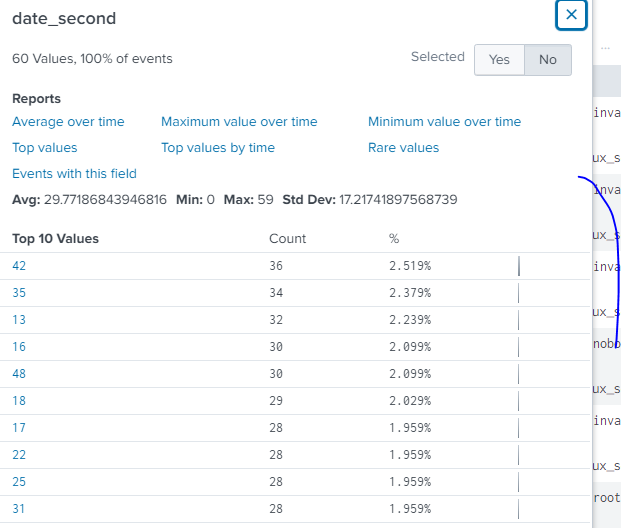
Vamos ver neste modulo agora sobre a linguagem SPL para pesquisa dentro do Splunk. Vamos ver abaixo um exemplo de uma busca por eventos que possuam a palavra Failed:



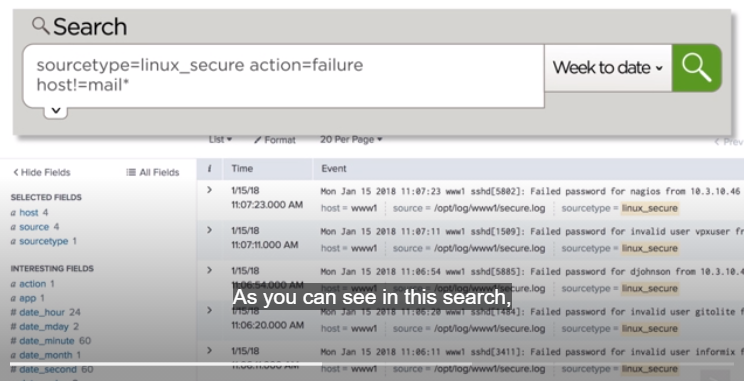


* **Módulo 6:**

Vamos aprender como usarmos os campos no Splunk. Do lado esquerdo temos uma coluna mostrando os campos principais e campos interessantes para usarmos da nossa pesquisa. Clicando em um dos campos, podemos ver os dados estatísticos daquele campo, como contagem de valores daquele campo, porcentagem que um valor aparece em um dos campos, conforme imagem abaixo:



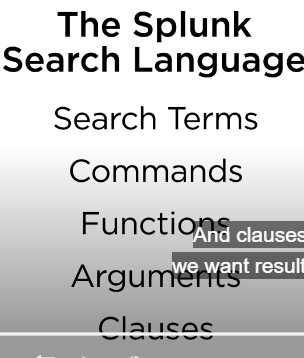
Podemos realizar uma pesquisa utilizando os campos para filtrarmos os valores conforme os campos.

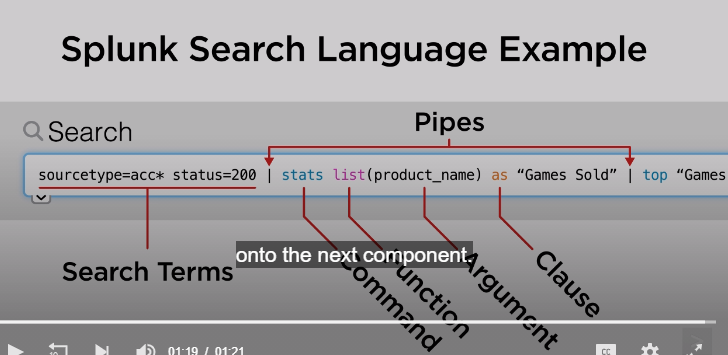


Lembrando que também podemos fazer uma busca dos dados dentro de um index específico.

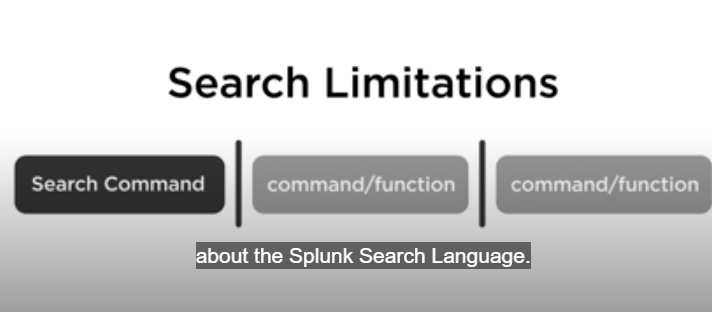
* **Módulo 6:**

Neste módulo vamos ver fundamentos da SPL. Para começar vamos vendo sobre a sintaxe de busca.



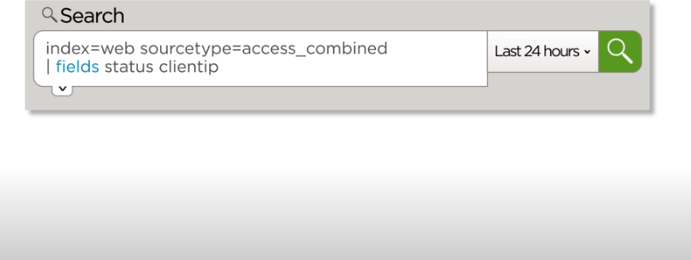


Podemos ver que no primeiro bloco acima pedimos os dados com “acc” e o campos status=200. Depois no segundo bloco de comando aplicamos o comando “stats” que serve para trabalharmos com estatística e usamos a função “list” que serve para listar os resultados do campo “product\_name” do resultado da busca como “Games Sold”.



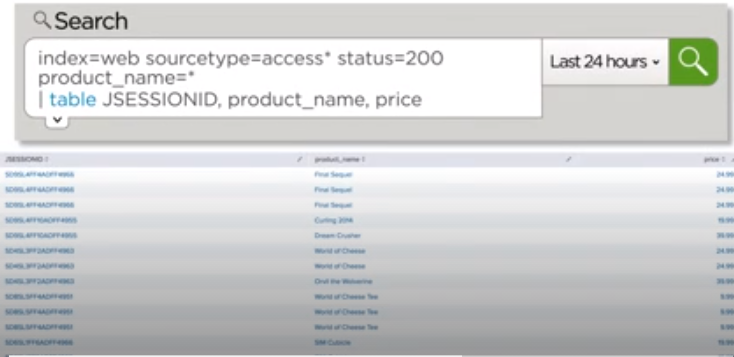
Agora vamos ver sobre os comandos de campos:

Basicamente com os comandos de campos, nós colocamos os campos que queremos mostrar no resultado da busca em vez de mostrar todos os campos da busca nos resultados:



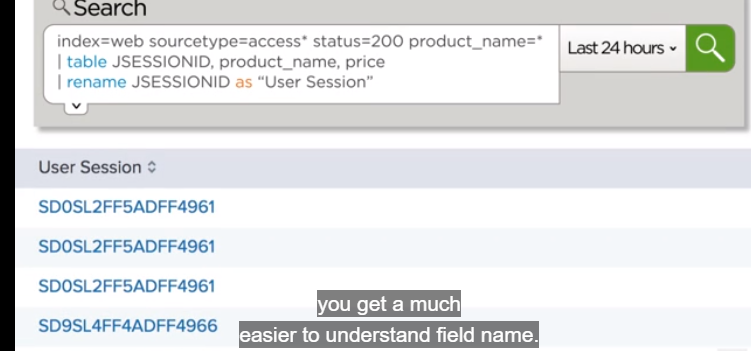
Agora vamos ver os comandos de Tabela:

Com os campos de Tabela a gente faz com que os dados apareçam em formato de tabela, tabulados:



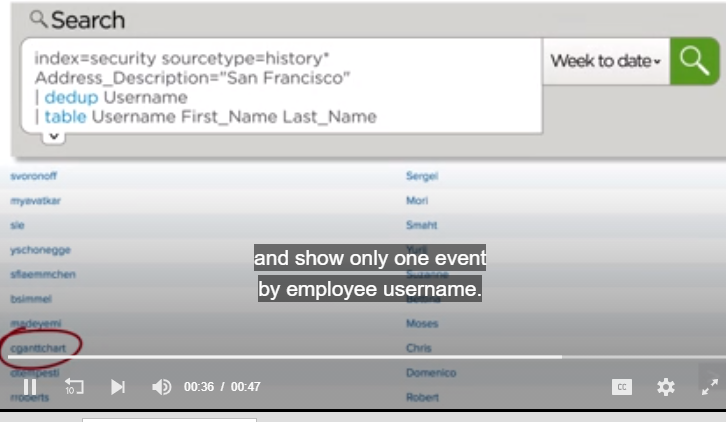
Agora vamos ver os comandos de Rename:

Rename Command serve para renomear os campos da nossa busca:

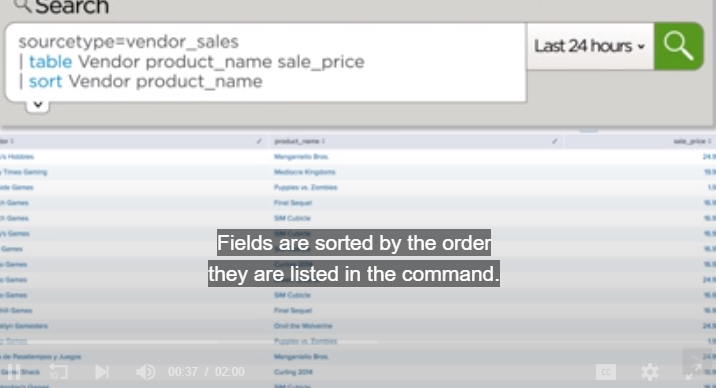


Agora vamos ver os comandos de Dedup:

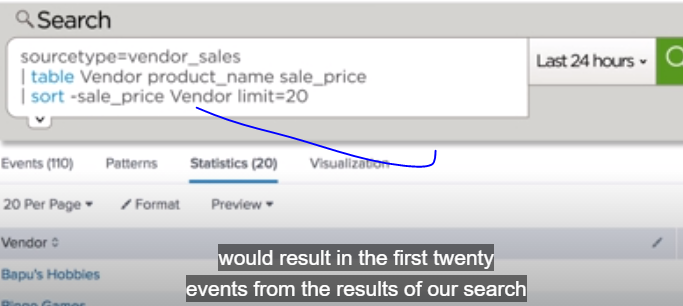
Podemos usar os comandos de Dedup para remover eventos duplicados de nossa busca:



Agora vamos ver os comandos de Sort:



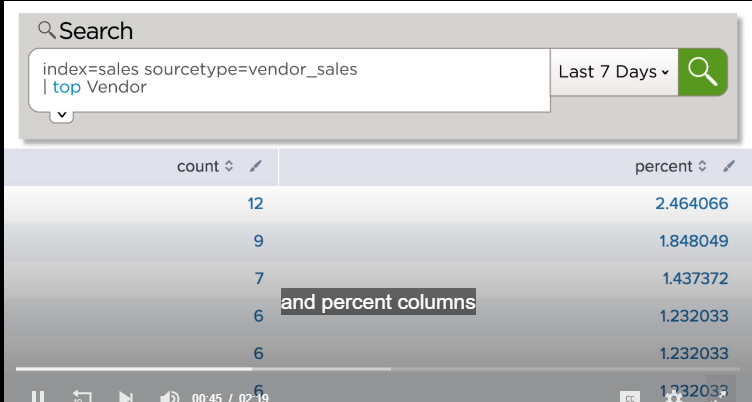
Podemos fazer um limite de resultados da nossa busca usando o comando Sort:

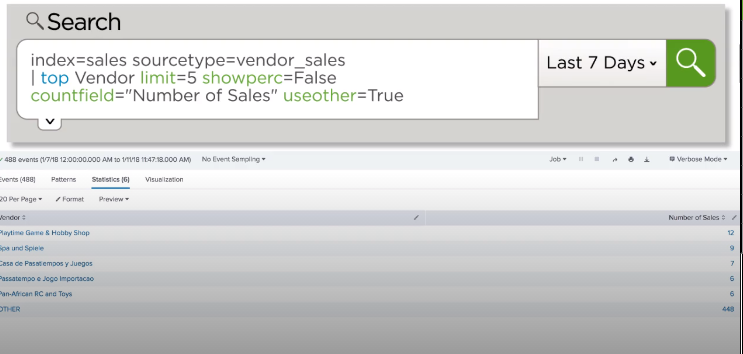


* **Módulo 9:**

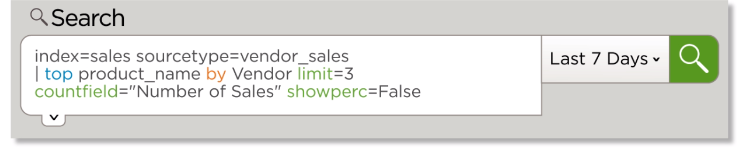
Agora vamos ver os comandos de transformação dos dados.

* + Top:





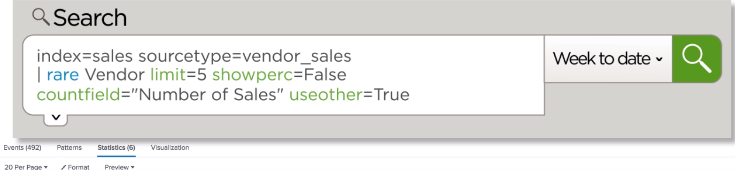
No exemplo abaixo, estamos buscando no index “sales” resultados do tipo “vendor\_sales”. Estamos colocando os tops “product\_names” por Vendedor no máximo 3 resultados. Ou seja, para cada vendedor vai mostrar no máximo 3 produtos que são tops.



* + Rare:

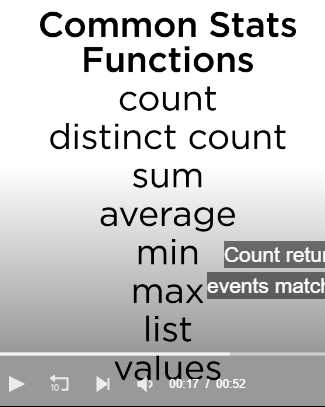
É como o comando de Top, mas ao invés de mostrar os tops resultados, vai mostrar somente os resultados que são menos aparecidos nos resultados.

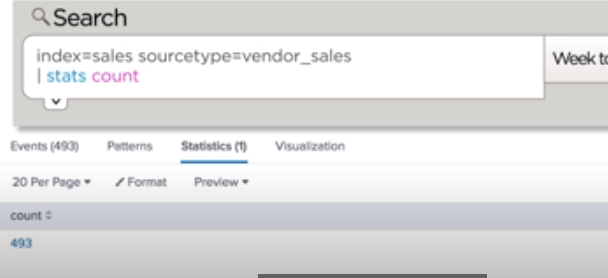
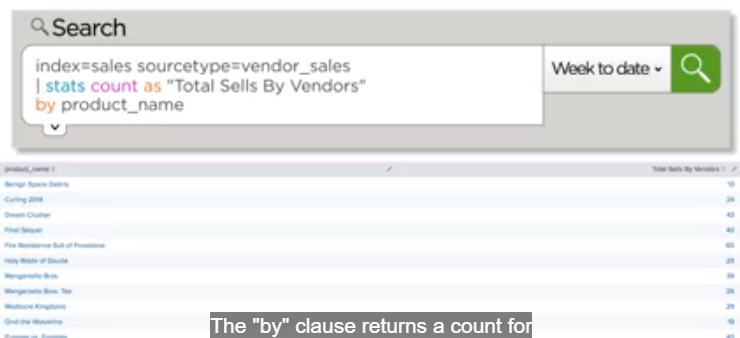
No exemplo abaixo estamos mostrando os resultados mais raros limitados a 5 “Vendor”.



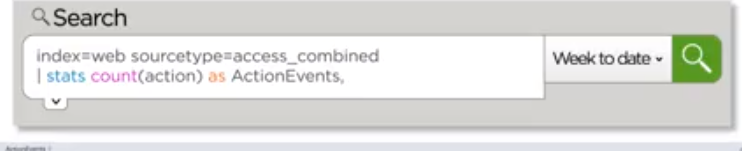
* + Stats:

Usamos o comando Stats para fazermos cálculos estatísticos com nossos resultados. Abaixo estão as funções que podemos fazer para ao usarmos o comando Stats:



Podemos usar a função count para contarmos a quantidade de registros que temos em um campo, neste exemplo abaixo, o campo “action”:



Ou seja, podemos usar essas funções de Stats para nos ajudar a fazermos transformações em nossos dados.

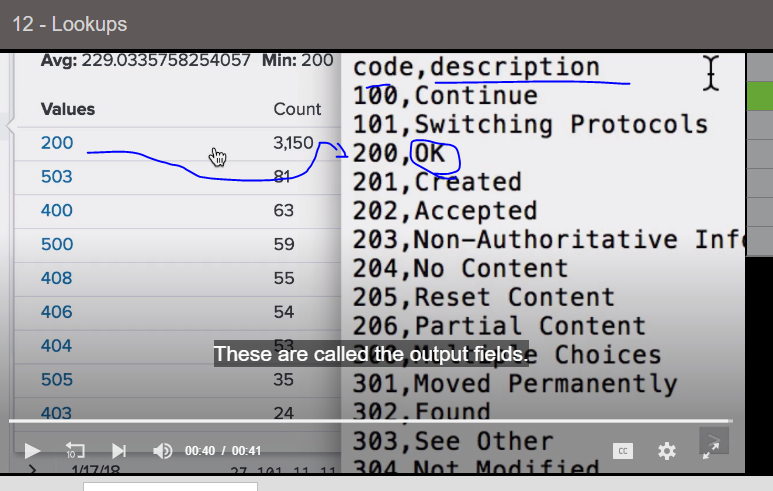
* **Módulo 10:**

Agora vamos aprender de como trabalhomos com Pivot no Splunk. O Pivot são dados já pré estruturados e organizados pelo próprio Splunk para nos ajudar a construir tabelas, gráficos e dashboards de forma rápida e de uma forma que fique fácil para quem não tem tanto conhecimento com a SPL.

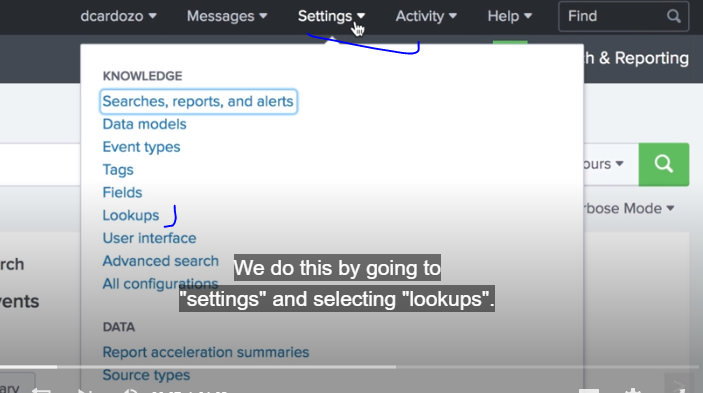
* **Módulo 11:**

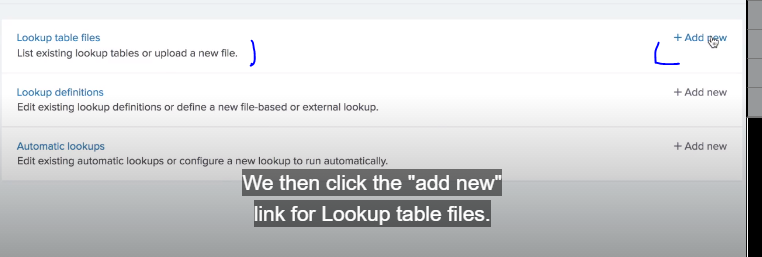
Agora vamos aprender a usarmos os Lookups (semelhante ao VLOOKUP – PROCV do Excel).

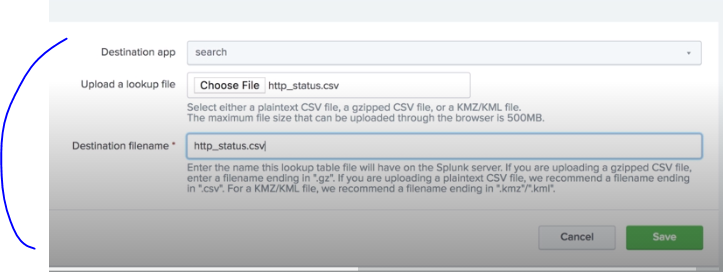
Para entendermos, vamos ter um exemplo onde nos meus dados indexados tenho uma coluna com os códigos de retorno da requisição HTTP. Porém, precisaríamos de uma coluna com a descrição do código para entendermos melhor. Para isso, temos um arquivo externo que tem essa descrição. Para adicionar essa descrição aos meus dados indexados, basta eu definir um Lookup para realizar o trabalho de varredura no meu arquivo externo que tem as descrições e adiciona-las a uma coluna nos meus dados indexados no Splunk.



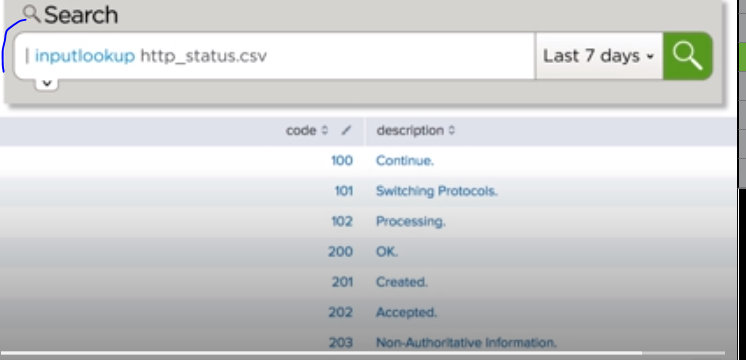
Para isso, primeiro vamos criar uma Tabela Lookup no Splunk, seguindo os passos abaixo:



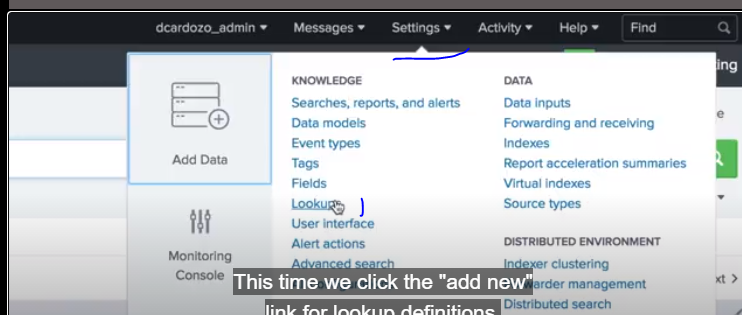


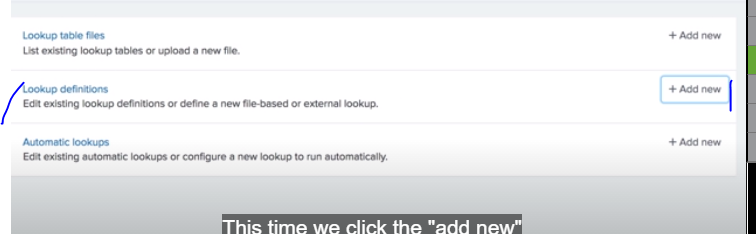


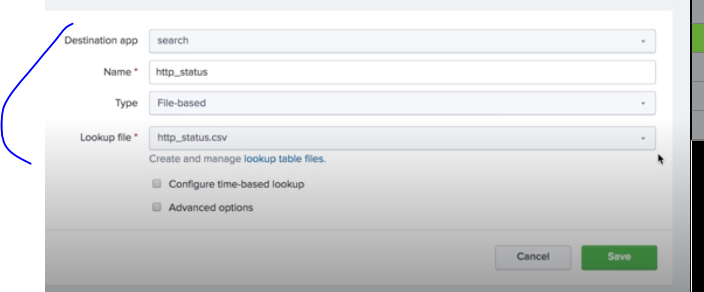
Após definir e criar a tabela de lookup no Splunk, eu posso verificar se esta tudo ok digitando o comando abaixo na barra de pesquisa:



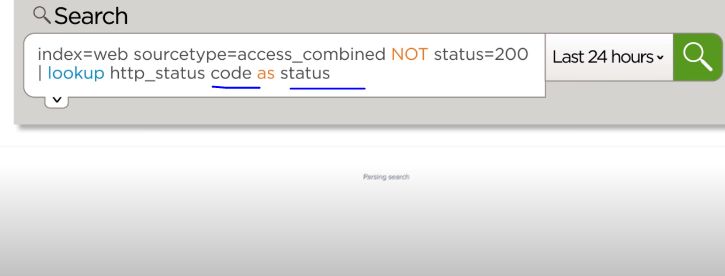
Agora que temos já o nosso arquivo de Lookup dentro do Splunk, temos que definir o Lookup:







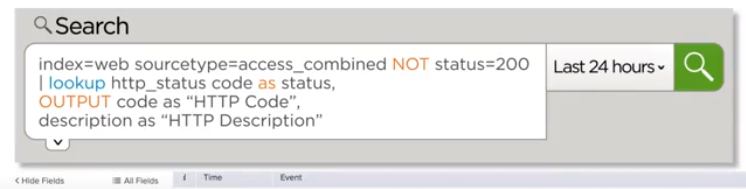
Agora que já temos a tabela de Lookup no Splunk e que já a definimos como um LookUp, podemos usar os comandos de Lookup na nossa barra de busca:



Então basicamente acima fizemos nossa busca e depois da busca usamos o comando de lookup. Abrimos o arquivo de Lookup com o nome que definimos “http\_status”. Depois colocamos a coluna dos nossos dados “code” que queremos que seja dado o match no arquivo de lookup “status”.

Mas ainda não mostramos o campo com os Lookups de descrição.

Para mostrar, utilizamos o comando abaixo “OUTPUT”:



Se quisermos criar Lookups de forma mais fácil, podemos utilizar em configurações de Lookup o Lookup Automático.