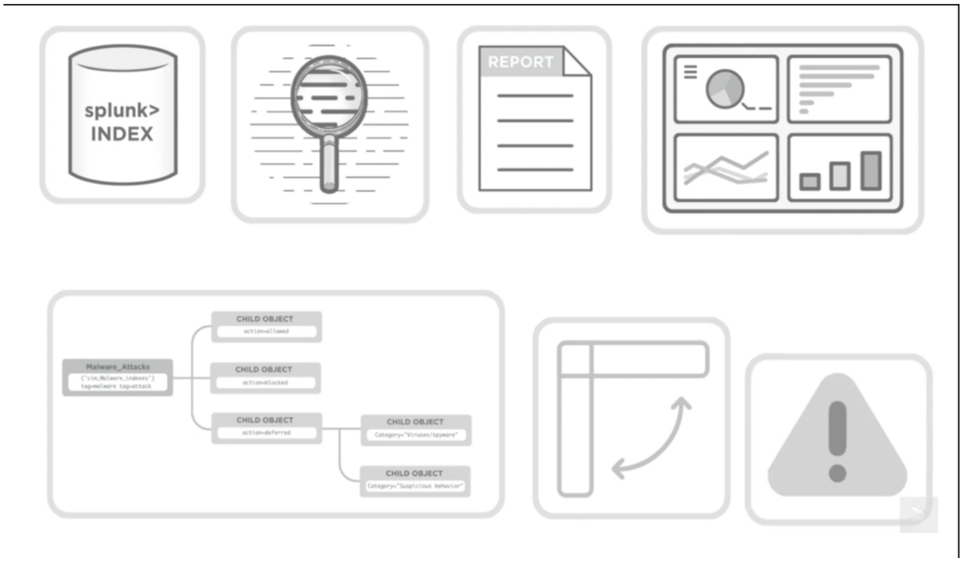
¿Qué es SPLUNK?

Machine Data.- data generated for devices. 90% of data for organizations comes from mobile, also this data coming with different structures and formats making so difficult to process them.

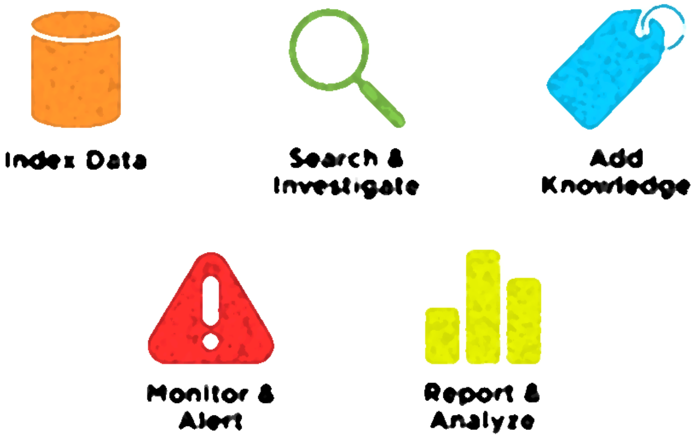
Operational Intelligence.- technology that uses AI to solve how to find and solve problems integrated different kinds of data, for example: Code logs, DB logs, purchase insights, etc. Also, how all this generated data can be corelated using specific data fields or characteristics and try to predict issues of find problems before users break into.

Types of Splunk services:

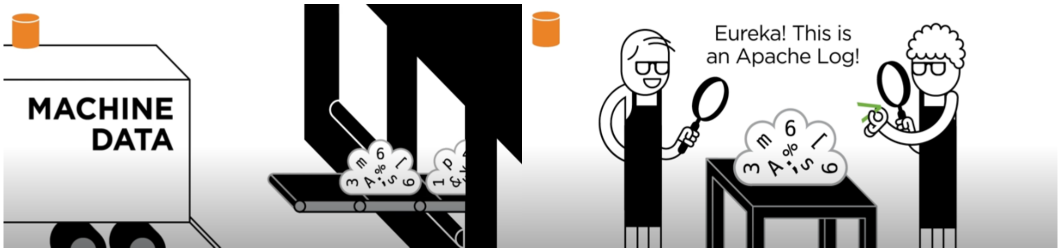
1.- Splunk enterpise (onpremise)
2.- Splunk cloud

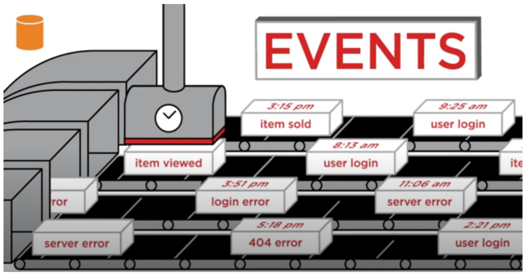


Main Splunk's functions

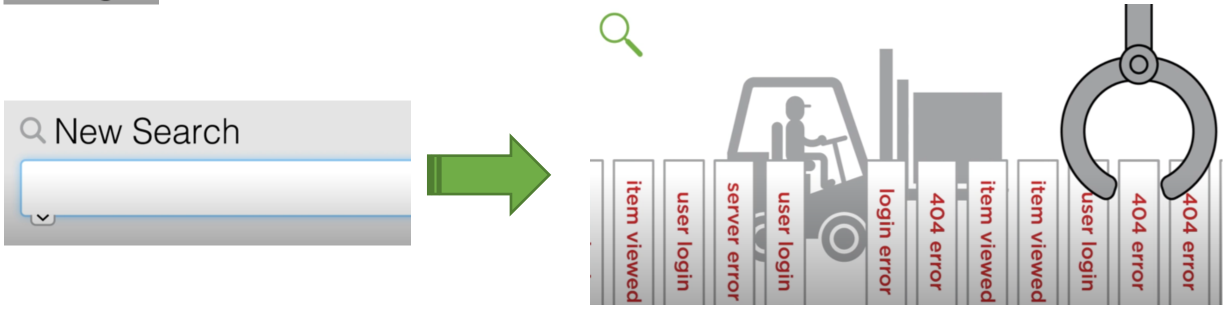


Index Data

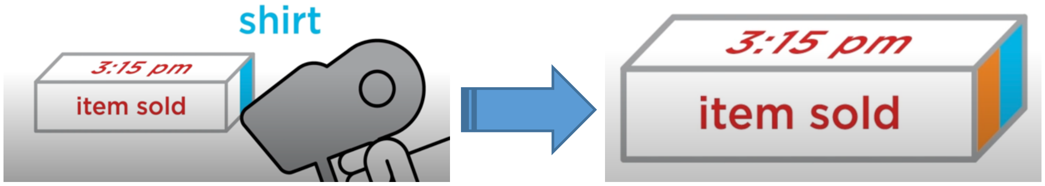




Search &
Investigate


New Search
item viewed
user login
server error
user login
login error
404 error
item viewed
item viewed
user login
404 error
404 error

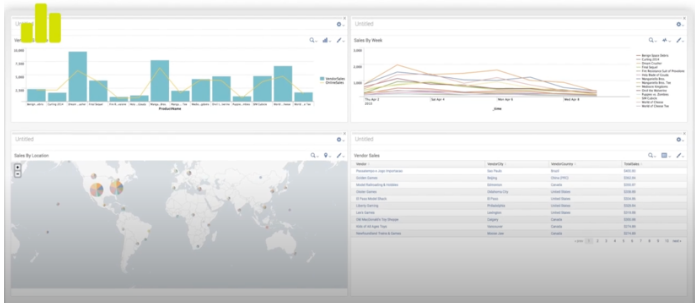
Add
Knowledge


shirt
3:15 pm
item sold
3:15 pm
item sold

Monitor &
Alert

splunk>
item viewed
user login
item sold
user login
item viewed
item sold
user login
item viewed
user login
item sold
item viewed

Report & Analyze

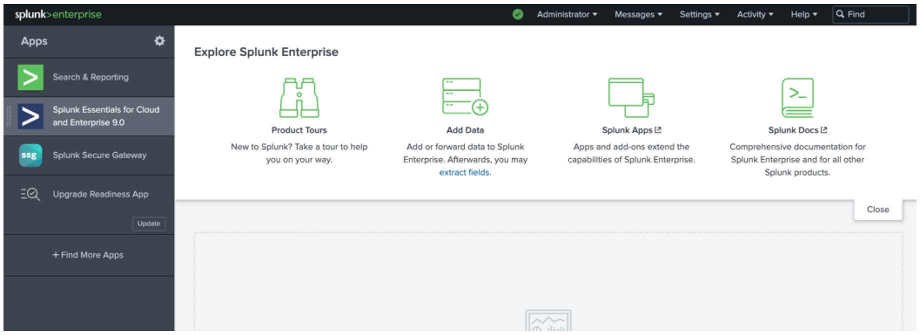


Install Splunk Enterprise:

1. Install splunk Enterprise edition: https://www.splunk.com/en_us/download/splunk-enterprise.html?locale=en_us

2. Introduce an user admin and password (jcagarcia@up.edu.mx, Esposa212100)

3. Launch Splunk Enterprise console and introduce your previous admin user and password



Explore Splunk Enterprise

Product Tours
New to Splunk? Take a tour to help you on your way.

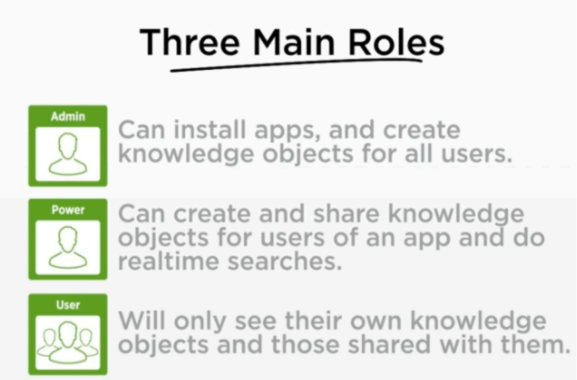
Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Splunk Apps
Apps and add-ons extend the capabilities of Splunk Enterprise.

Splunk Docs
Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

Command that creat statatiscs and/or visualizations are called**: transforming commands**

If you want to run command programmatically, you must configure Jobs. Jobs are available for execution after 10 minutes and for 7 days.



Three Main Roles

Admin
Can install apps, and create knowledge objects for all users.

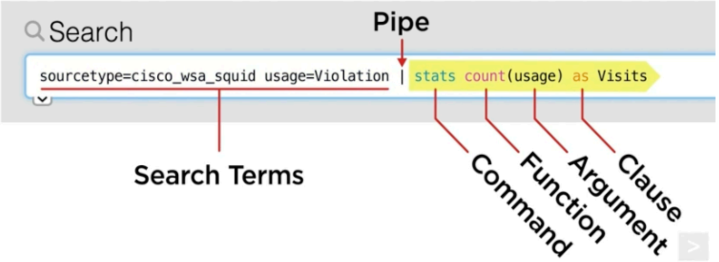
Power
Can create and share knowledge objects for users of an app and do realtime searches.

User
Will only see their own knowledge objects and those shared with them.

- Execution mode:

- Boolean operator for Queries: NOT, OR, AND . Parenthesis are available to priorize
- Use “ ” for string criteria

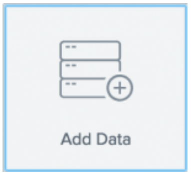
Splunk Search Language Example



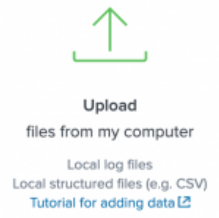
```
sourcetype=cisco_wsa_squid usage=Violation | stats count(usage) as Visits
```

Use the Add Data wizard

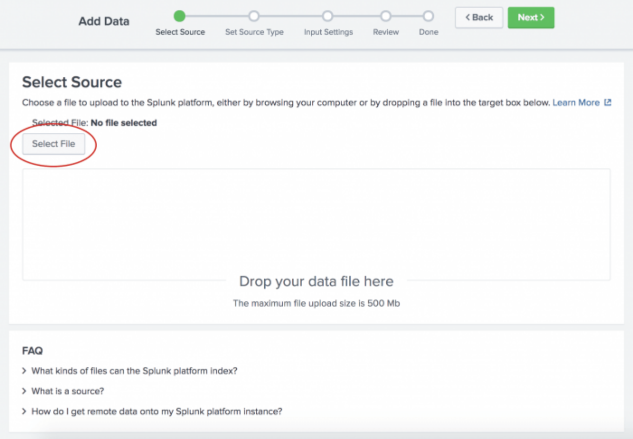
1. If there is a **Welcome** window displayed, close that window.
2. Click **Settings > Add Data**.



3. At the bottom of the window, click **Upload**. There are other options for adding data, but for this tutorial you will upload the data files.



4. Under **Select Source**, click **Select File**..



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: **No file selected**

Drop your data file here

The maximum file upload size is 500 Mb

- What kinds of files can the Splunk platform index?
- What is a source?
- How do I get remote data onto my Splunk platform instance?

5. In your download directory, select the `tutorialdata.zip` file and click **Open**.

Because you specified a compressed file, the Splunk software recognizes that type of data source. The **Set Source Type** step in the Add Data wizard is skipped. When you load data that is not in a compressed file, you will be asked to set the data source type.

6. Click **Next** to continue to **Input Settings**.

7. Under **Input Settings**, you can override the default settings for Host, Source type, and Index.

Because this tutorial uses a ZIP file, you are going to modify the **Host** setting to assign the host values by using a portion of the path name for the files included in the ZIP file. The setting that you specify depends whether you are using Splunk Cloud Platform or Splunk Enterprise, and on the operating system that you are using.

Splunk Cloud Platform

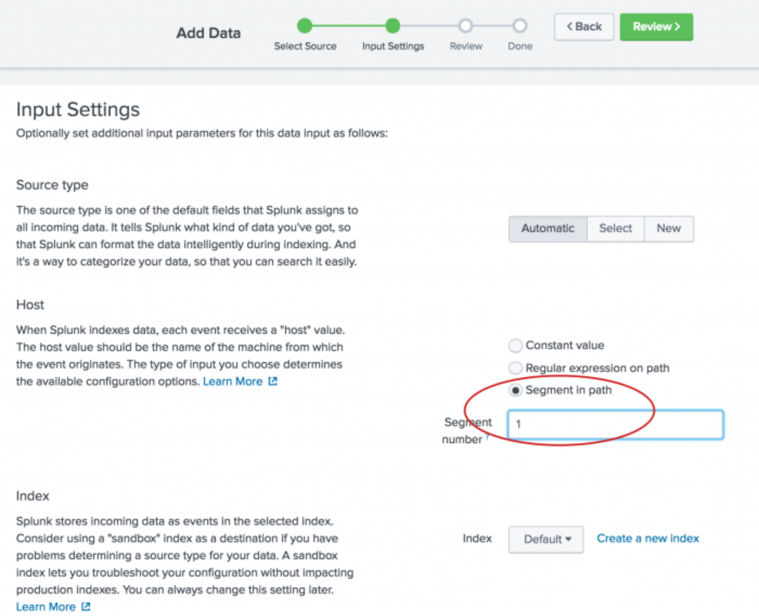
a. Select **Segment in path**.

b. Type **1** for the segment number.

Splunk Enterprise for Linux or Mac OS X

a. Select **Segment in path**.

b. Type **1** for the segment number.



Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that Splunk assigns to all incoming data. It tells Splunk what kind of data you've got, so that Splunk can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Automatic | Select | New

Host

When Splunk 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

Segment number: 1

Index

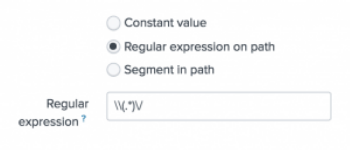
Splunk stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting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

Index: Default ▾ Create a new index

Splunk Enterprise for Windows

a. Select **Regular expression on path**.

b. Type **\\(.*)\/** for the regex to extract the host values from the path.



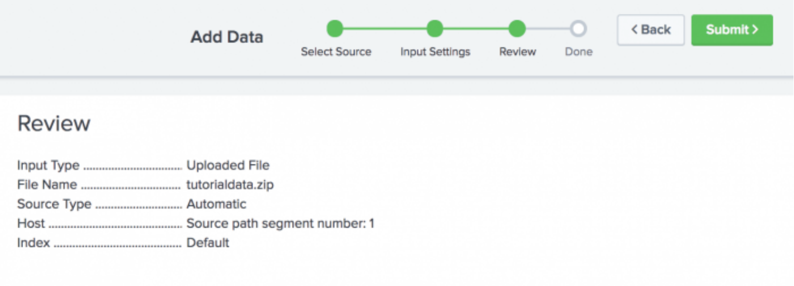
○ Constant value

● Regular expression on path

○ Segment in path

Regular expression: \\(.*)\/

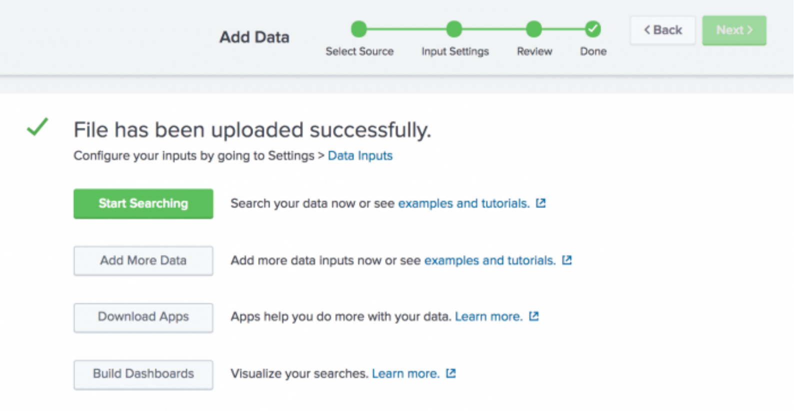
8. Click **Review**. The following screen appears where you can review your input settings.



Review

Input Type .... Uploaded File
File Name .... tutorialdata.zip
Source Type .... Automatic
Host .... Source path segment number: 1
Index .... Default

9. Click **Submit** to add the data.



✓ File has been uploaded successfully.

Configure your inputs by going to Settings > Data Inputs

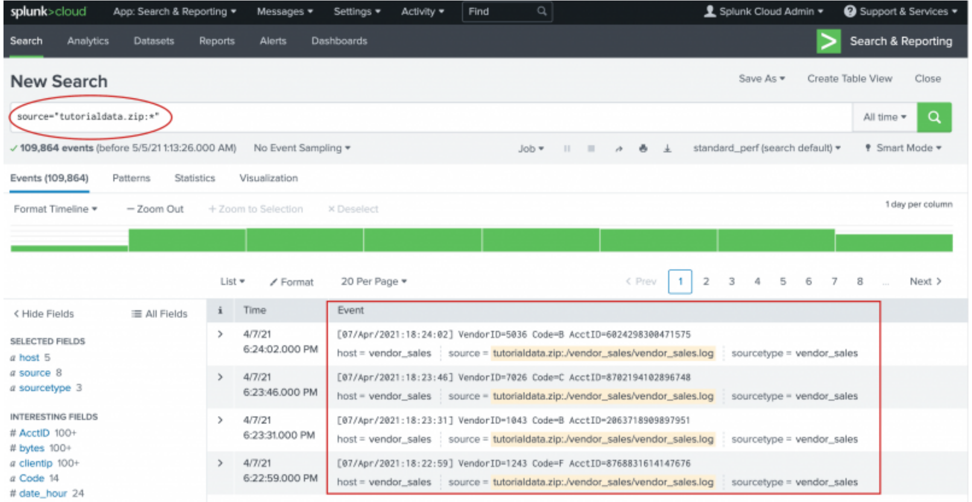
Start Searching — Search your data now or see examples and tutorials.

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.

10. To see the data in the Search app, click **Start Searching**.
You might see a screen asking if you want to take a tour. You can take the tour or click **Skip**.
The Search app opens and a search is automatically run on the tutorial data source.



New Search

```
source="tutorialdata.zip:*"
```

✓ 109,864 events (before 5/5/21 1:13:26.000 AM)   No Event Sampling ▾   standard_perf (search default) ▾

Events (109,864)

SELECTED FIELDS
a host 5
a source 8
a sourcetype 3

INTERESTING FIELDS
AcctID 100+
# bytes 100+
a clientip 100+
a Code 14
# date_hour 24

i	Time	Event
>	4/7/21 6:24:02.000 PM	[07/Apr/2021:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575 host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log sourcetype = vendor_sales
>	4/7/21 6:23:46.000 PM	[07/Apr/2021:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748 host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log sourcetype = vendor_sales
>	4/7/21 6:23:31.000 PM	[07/Apr/2021:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951 host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log sourcetype = vendor_sales
>	4/7/21 6:22:59.000 PM	[07/Apr/2021:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676 host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log sourcetype = vendor_sales

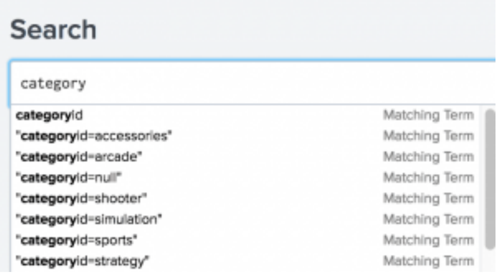
Success! The results confirm that the data in the `tutorialdata.zip` file was indexed and that events were created.

11. Click the **Splunk** logo to return to Splunk Home.

Using the Search Assistant

The Search Assistant is a feature in the Search app that appears as you type your search criteria. The Search Assistant is like autocomplete, but so much more.

1. Click **Search** in the App bar to start a new search.
2. Type `buttercup` in the Search bar.
   When you type a few letters into the Search bar, the Search Assistant shows you terms in your data that match the letters that you type in.
3. Click **Search** in the App bar to start a new search.
4. Type `category` in the Search bar. The terms that you see are in the tutorial data.

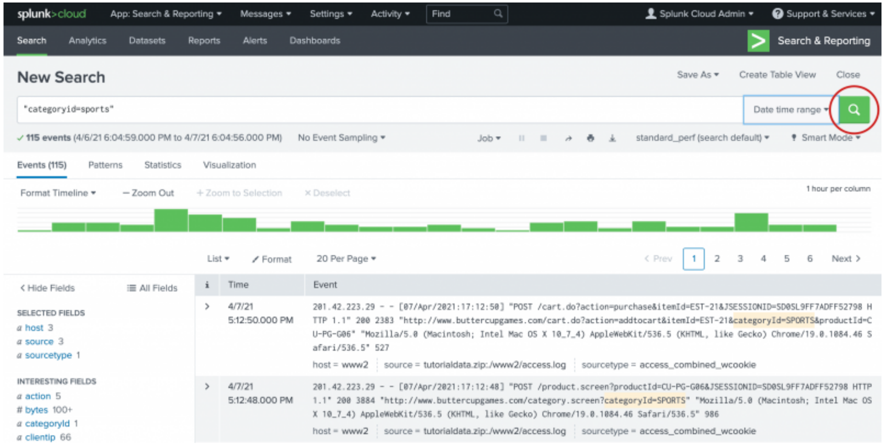


Search

category

categoryid	Matching Term
"**category**id=accessories"	Matching Term
"**category**id=arcade"	Matching Term
"**category**id=null"	Matching Term
"**category**id=shooter"	Matching Term
"**category**id=simulation"	Matching Term
"**category**id=sports"	Matching Term
"**category**id=strategy"	Matching Term

5. Select **"categoryid=sports"** from the Search Assistant list.
6. Press **Enter**, or click the **Search icon** on the right side of the Search bar, to run the search.



New Search

"categoryid=sports"

✓ 115 events (4/6/21 6:04:59.000 PM to 4/7/21 6:04:56.000 PM) No Event Sampling ▾

SELECTED FIELDS
a host 3
a source 3
a sourcetype 1

INTERESTING FIELDS
a action 5
# bytes 100+
a categoryId 1
a clientip 66

i	Time	Event
>	4/7/21 5:12:50.000 PM	201.42.223.29 - - [07/Apr/2021:17:12:50] "POST /cart.do?action=purchase&itemId=EST-21&JSESSIONID=SD0SL9FF7ADFF52798 HTTP 1.1" 200 2383 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-21&categoryId=SPORTS&productId=CU-PG-G06" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 527 host = www2 source = tutorialdata.zip:./www2/access.log sourcetype = access_combined_wcookie
>	4/7/21 5:12:48.000 PM	201.42.223.29 - - [07/Apr/2021:17:12:48] "POST /product.screen?productId=CU-PG-G06&JSESSIONID=SD0SL9FF7ADFF52798 HTTP 1.1" 200 3884 "http://www.buttercupgames.com/category.screen?categoryId=SPORTS" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 986 host = www2 source = tutorialdata.zip:./www2/access.log sourcetype = access_combined_wcookie

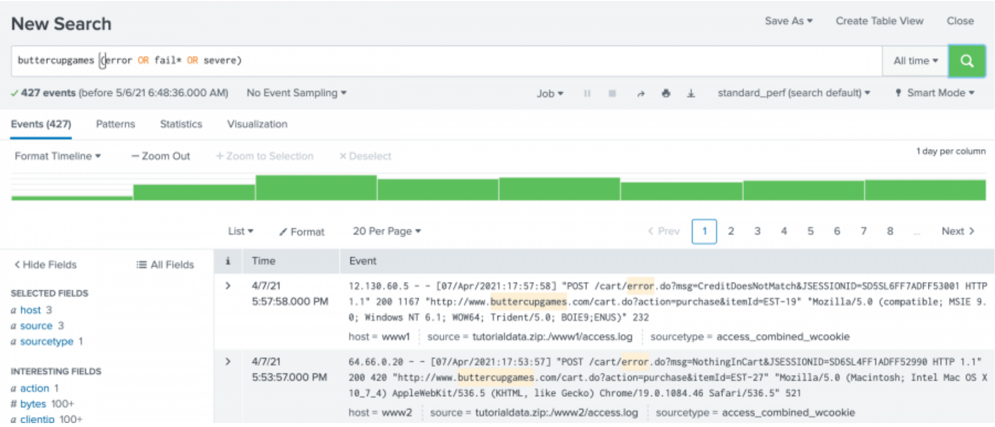
Retrieve events from the index

1. Start a new search.
2. Change the time range to **All time**.
3. To search for the terms error, fail, failure, failed, or severe, in the events that also mention buttercupgames, run the following search.
   `buttercupgames (error OR fail* OR severe)`
   Tip: Instead of typing the search string, you can copy and paste the search from this tutorial directly into the Search bar.

4. Click the Search icon to the right of the time range picker to run the search.

Notice that you must capitalize Boolean operators. The asterisk (*) character is used as a wildcard character to match `fail`, `failure`, `failed`, `failing`, and so forth.

When evaluating Boolean expressions, precedence is given to terms inside parentheses. NOT clauses are evaluated before OR clauses. AND clauses have the lowest precedence.



```
buttercupgames (error OR fail* OR severe)
```

✓ 427 events (before 5/6/21 6:48:36.000 AM)

i	Time	Event

>	4/7/21
	5:57:58.000 PM
		`12.130.60.5 - - [07/Apr/2021:17:57:58] "POST /cart/error.do?msg=CreditDoesNotMatch&JSESSIONID=SD5SL6FF7ADFF53001 HTTP 1.1" 200 1167 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-19" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 232`
		host = www1 source = tutorialdata.zip:./www1/access.log sourcetype = access_combined_wcookie

>	4/7/21
	5:53:57.000 PM
		`64.66.0.20 - - [07/Apr/2021:17:53:57] "POST /cart/error.do?msg=NothingInCart&JSESSIONID=SD6SL4FF1ADFF52990 HTTP 1.1" 200 420 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-27" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 521`
		host = www2 source = tutorialdata.zip:./www2/access.log sourcetype = access_combined_wcookie

Patterns, Statistics, and Visualizations

The **Patterns** tab displays a list of the most common patterns among the set of events returned by your search. Each of these patterns represents events that share a similar structure.

The **Statistics** tab populates when you run a search with transforming commands such as `stats`, `top`, `chart`, and so on. The keyword search for "buttercupgames" does not show results in this tab because the search does not include any transforming commands.

Searches with transforming commands also populate the **Visualization** tab. The results area of the **Visualizations** tab includes a chart and the statistics table that is used to generate the chart.