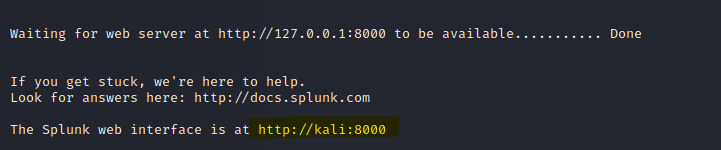
**Splunk**

After installation to start splunk on your system you by following step

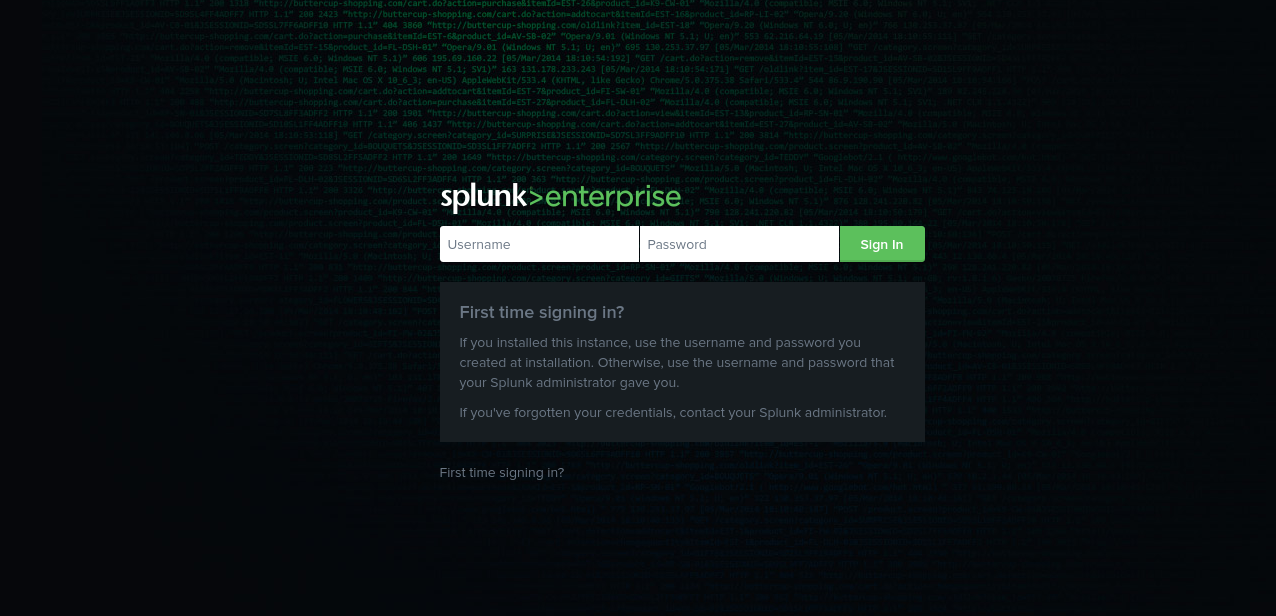
cd /opt/splunk/bin

sudo ./splunk start

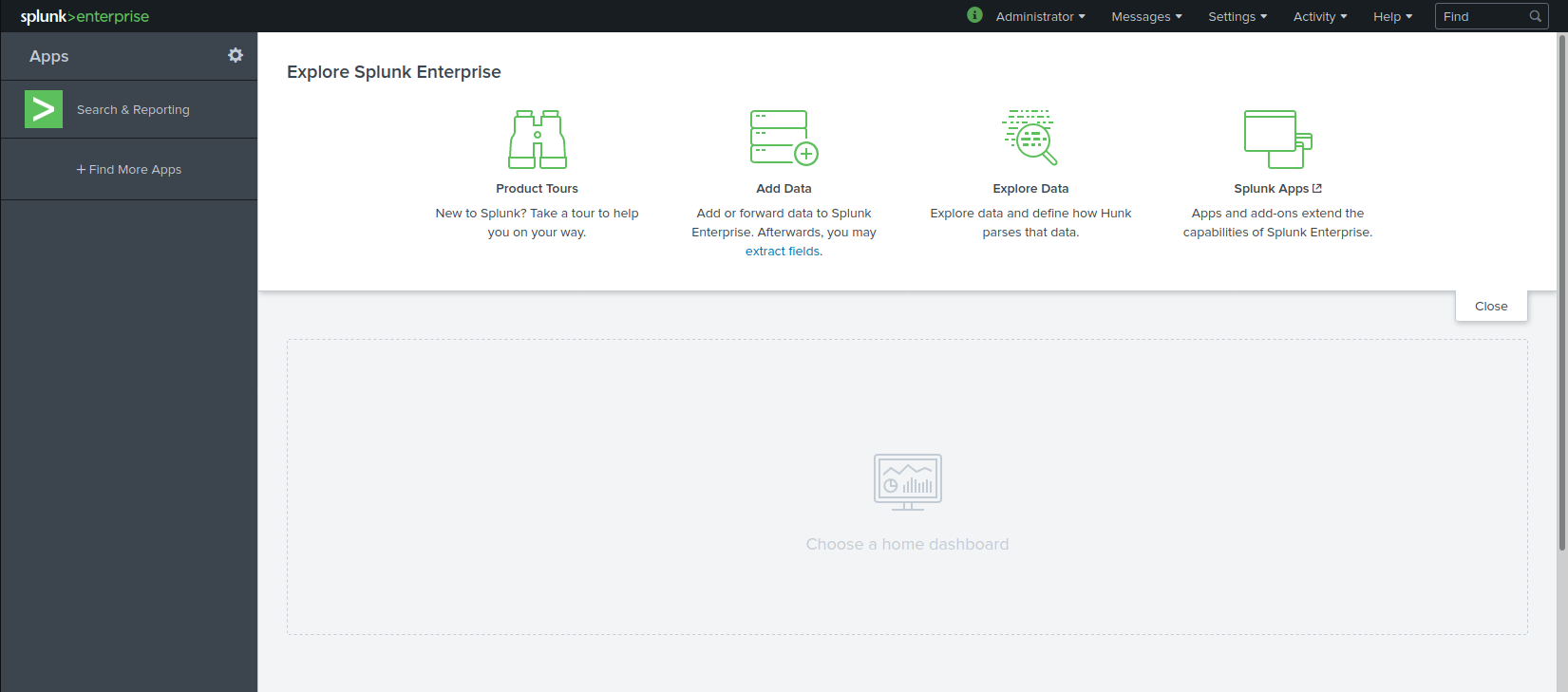
After running this command it will ask you for setting username and password



Open this interface on your browser

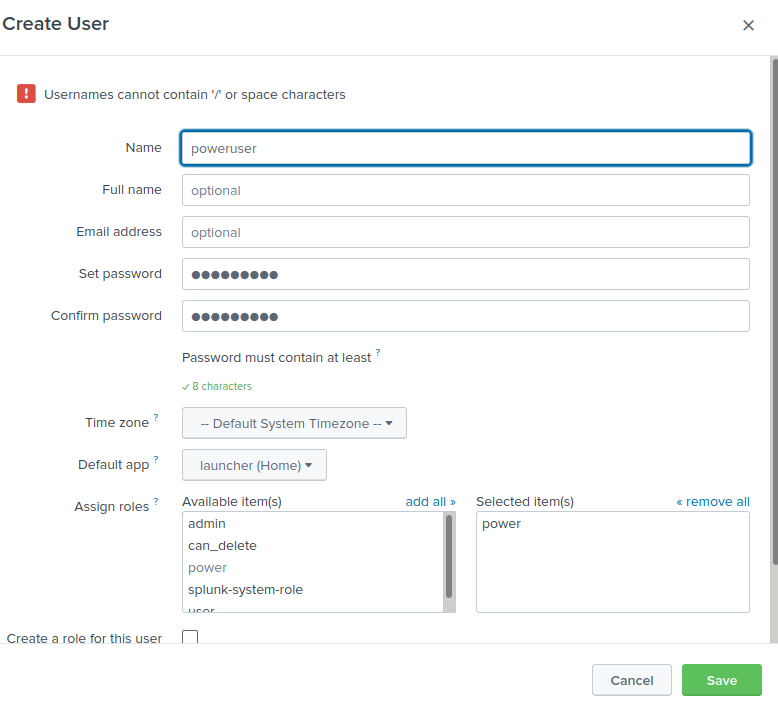


Enter the username and password



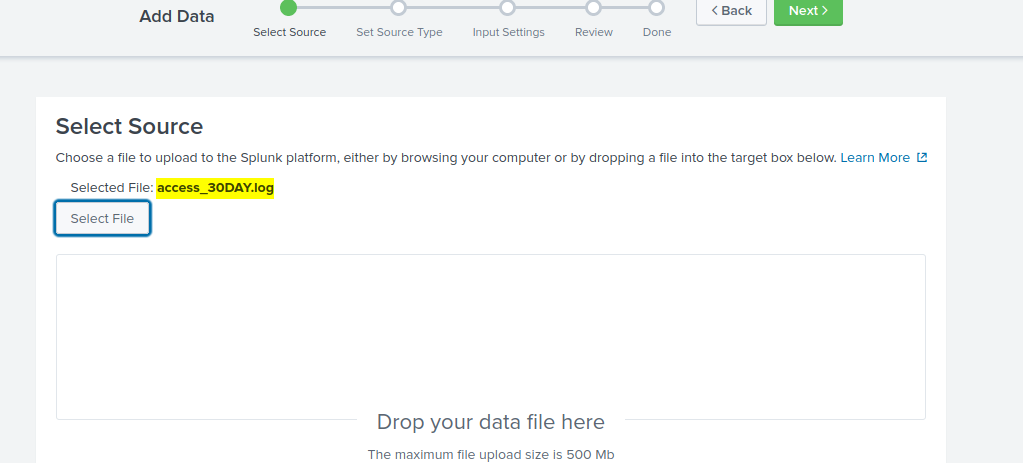
Let create user

Got to Setting->User and authentication->Users->New User. Add a new user and fill the required information and create a Powe user which have less privilege then administrator account

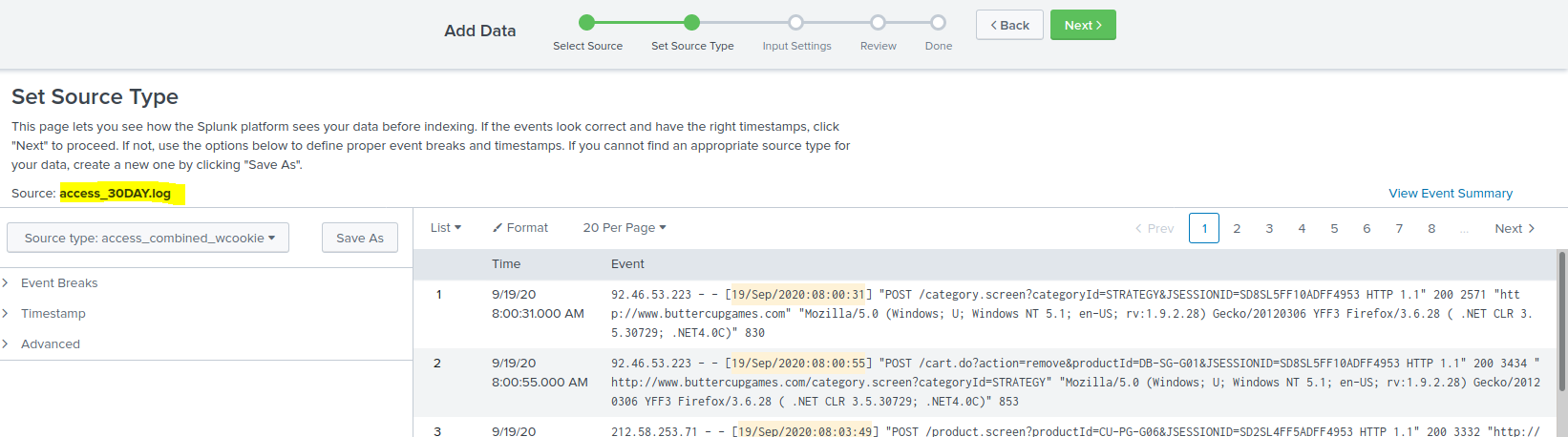


Now let’s proceed for data ingestion so we need some data you can have from [splk.it/f1data](http://splk.it/f1data)

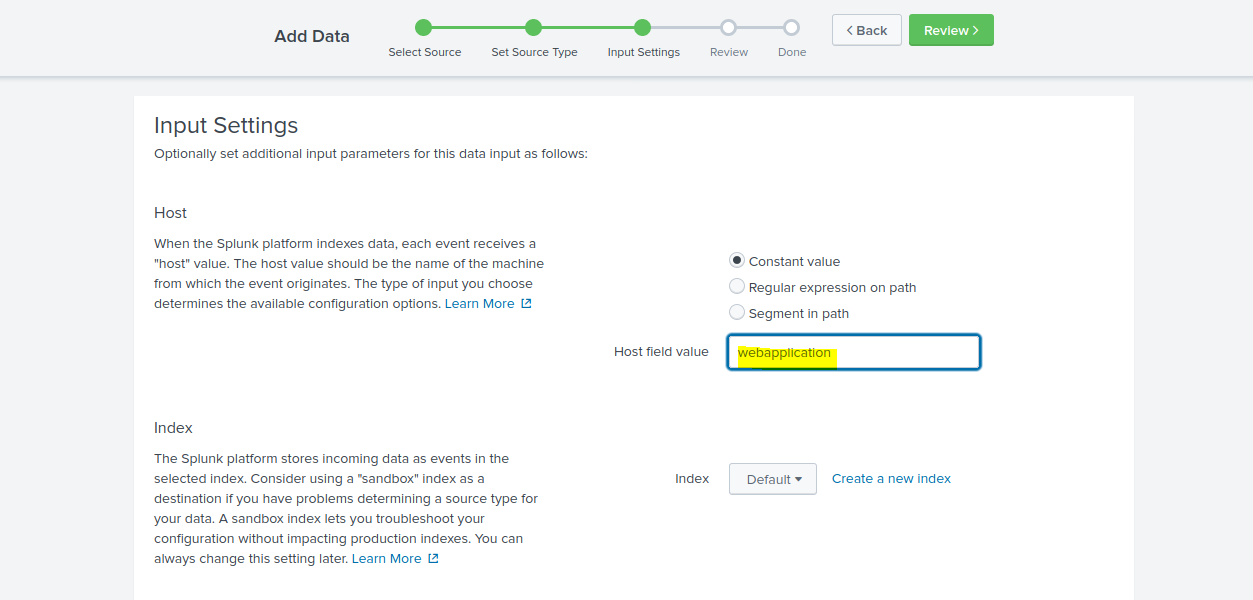
Now go to home page and Click on **add data** now click on upload.And upload the access\_30DAY.log file from tmp folder in zip by clicking on source



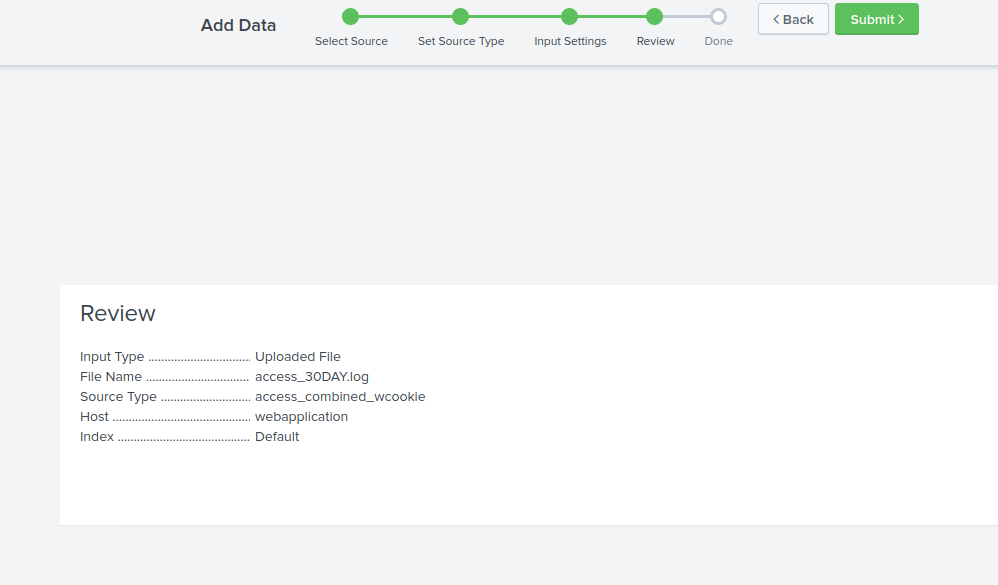
Now click on Next and check your source type



And click on next again and window you will add host field name

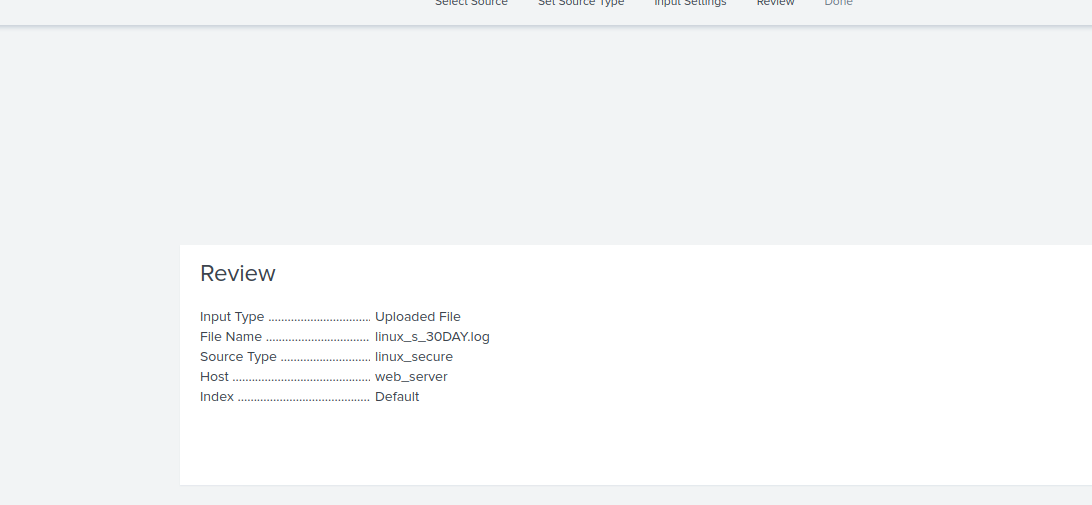


Click on **review** and review tab will appear



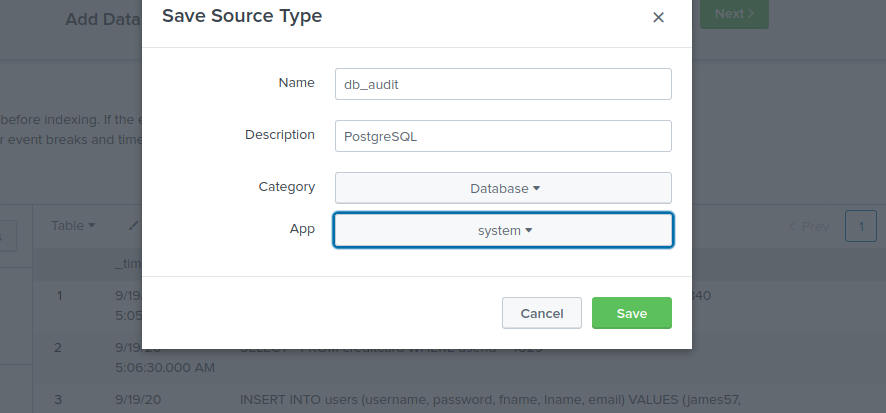
Now click on submit and the file processing will start

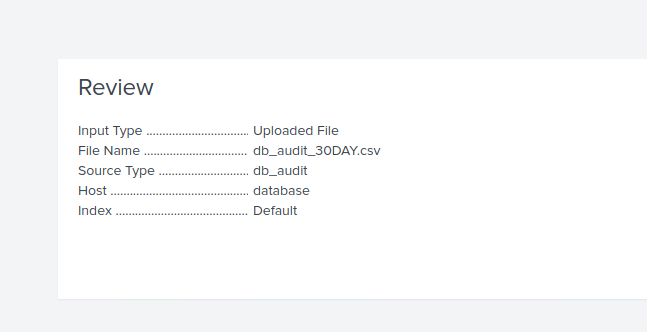
Now add linux\_s\_30DAY.log for this select **source type -> Operating system->linux->secure\_type**



Now click on submit

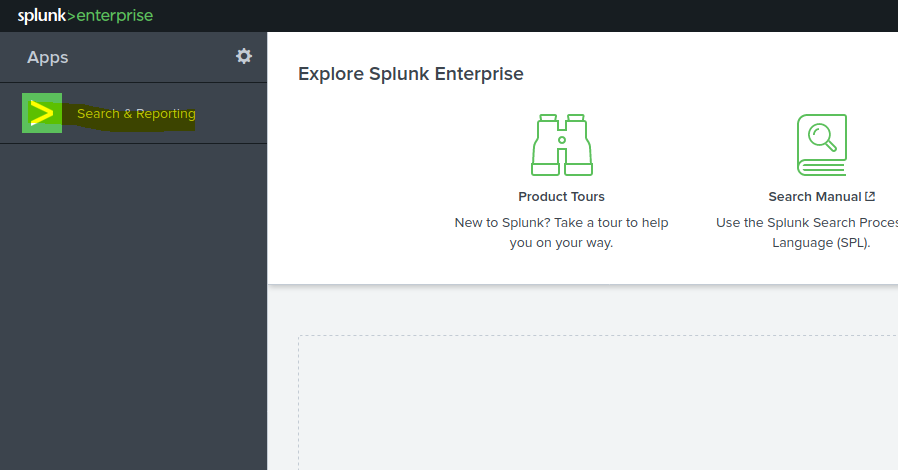
Now upload **db\_audit\_30DAY.csv** and click on **Save as** and fill the details as given below

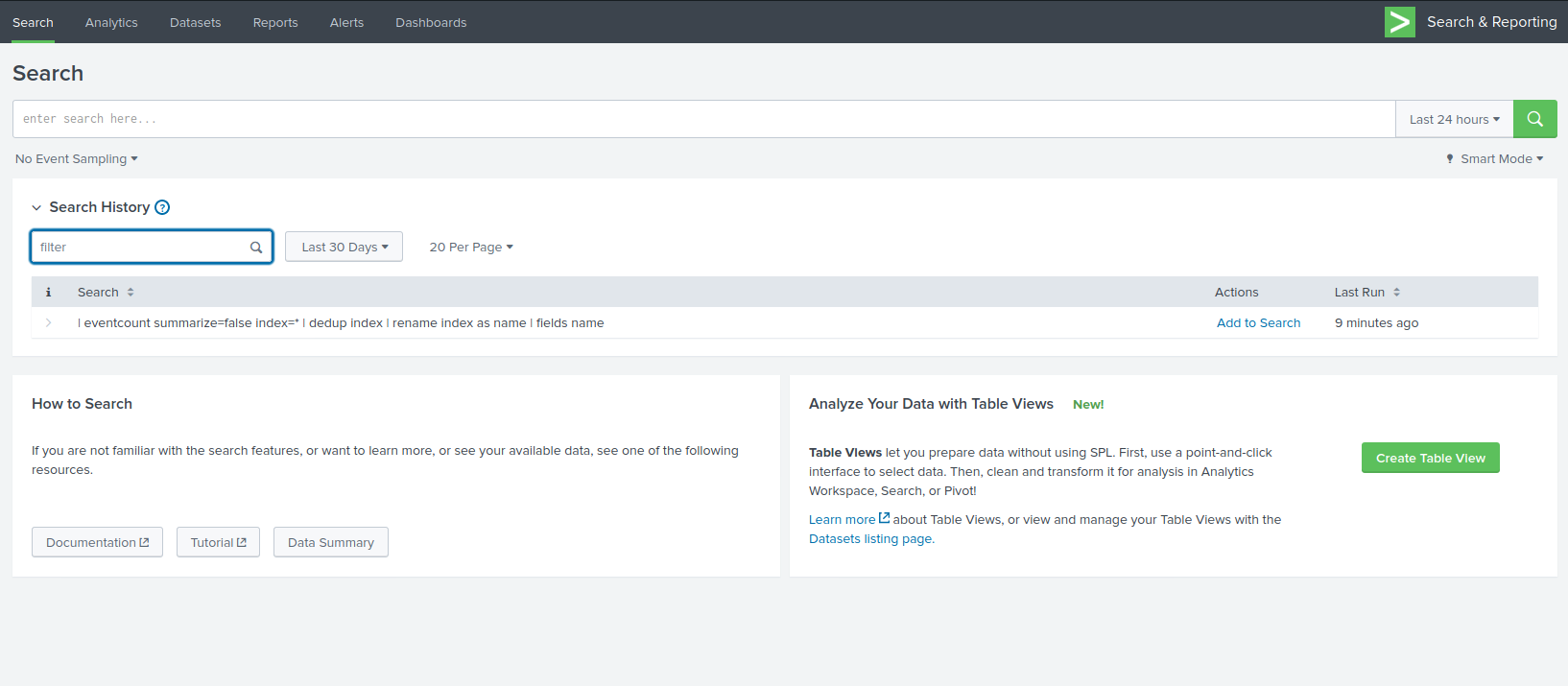




Now logout from Adminstrator and lo in as Power user

Click on searching and reporting





index=main sourcetype=access\_combined\_wcookie action=purchase status=200 file=success.do | fields action, JSESSIONID, status

index=main sourcetype=access\_combined\_wcookie action=purchase status=200 file=success.do | table action, JSESSIONID, status

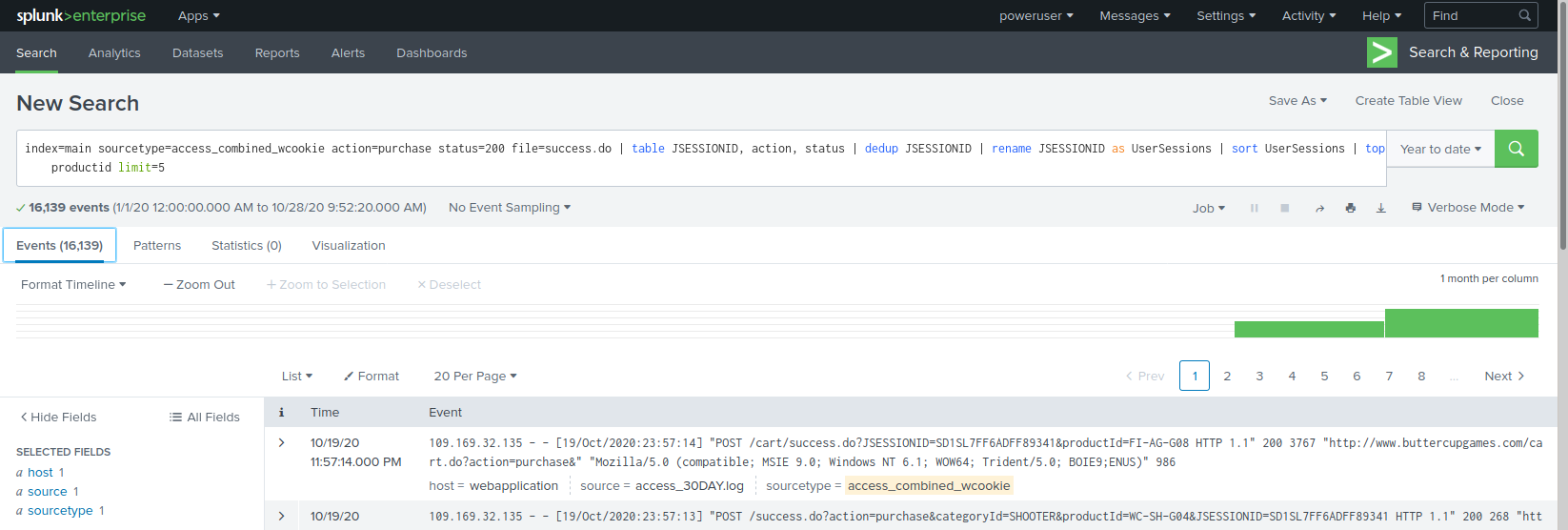
index=main sourcetype=access\_combined\_wcookie action=purchase status=200 file=success.do | table JSESSIONID, action, status | sort UserSessions

To remove duplicate values

index=main sourcetype=access\_combined\_wcookie action=purchase status=200 file=success.do | table JSESSIONID, action, status | dedup JSESSIONID | rename JSESSIONID as UserSessions | sort UserSessions

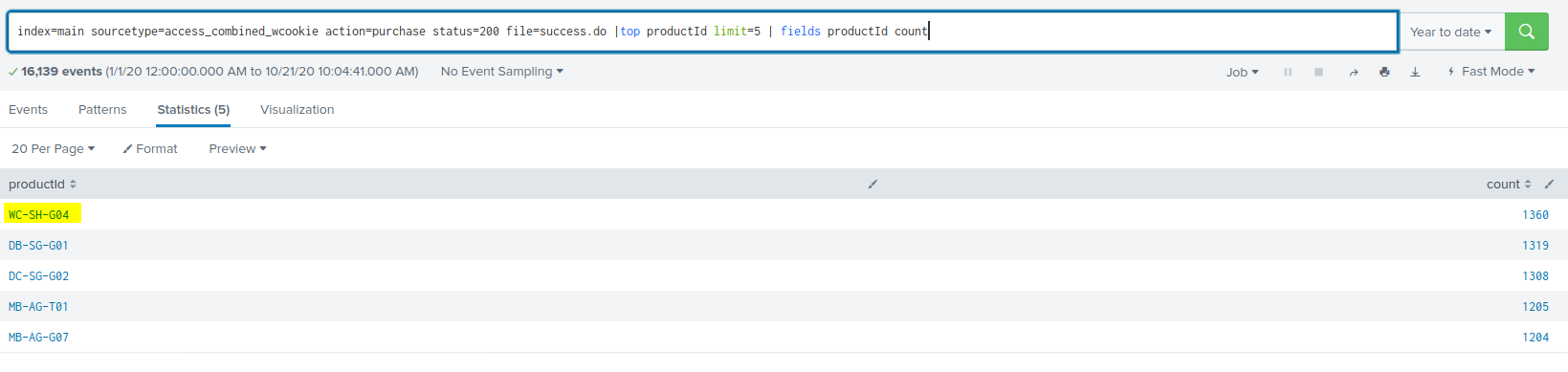
6

index=main sourcetype=access\_combined\_wcookie action=purchase status=200 file=success.do | table JSESSIONID, action, status | dedup JSESSIONID | rename JSESSIONID as UserSessions | sort UserSessions | top productid limit=5



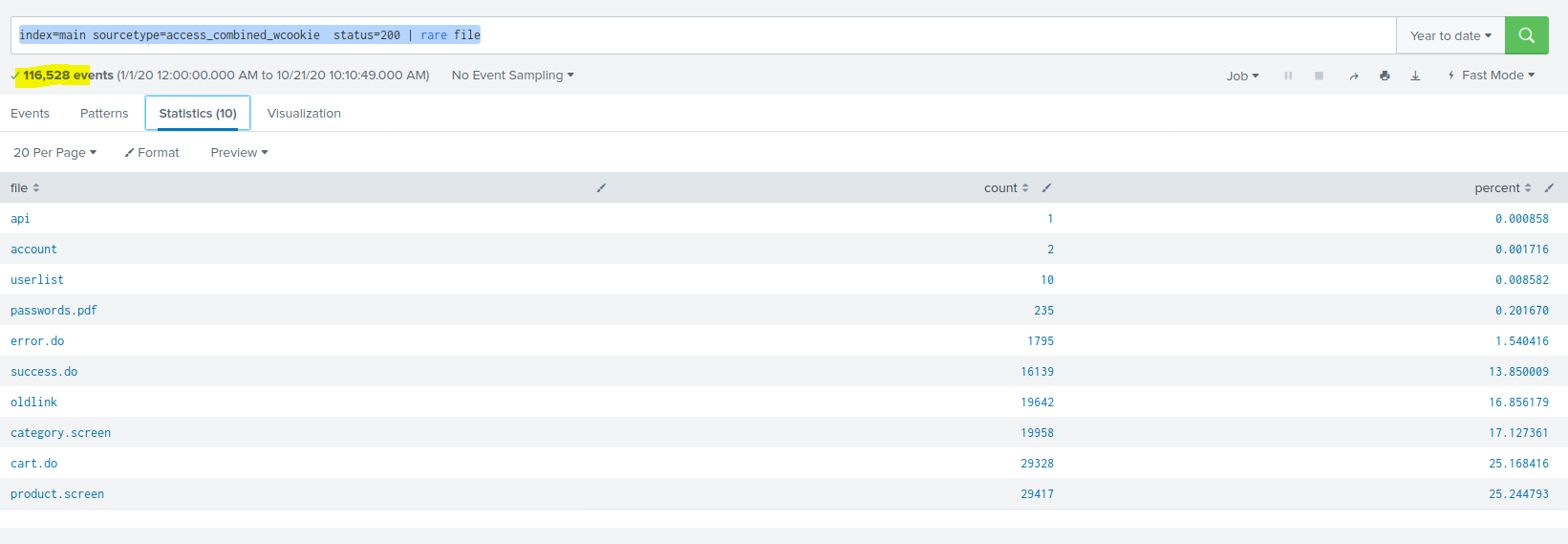
to get a famous product

index=main sourcetype=access\_combined\_wcookie action=purchase status=200 file=[success.do](http://success.do/) |top productId limit=5 | fields productId countv



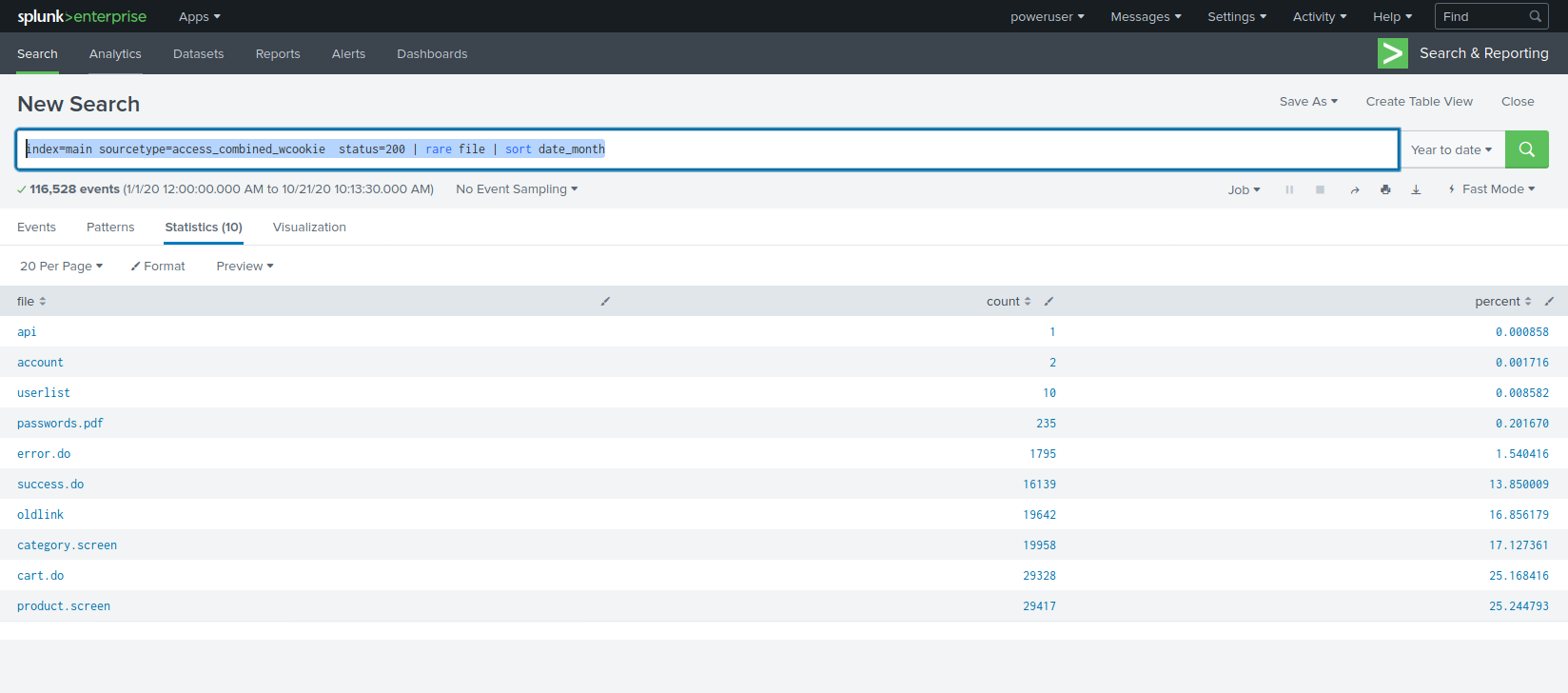
7

index=main sourcetype=access\_combined\_wcookie status=200 | rare file



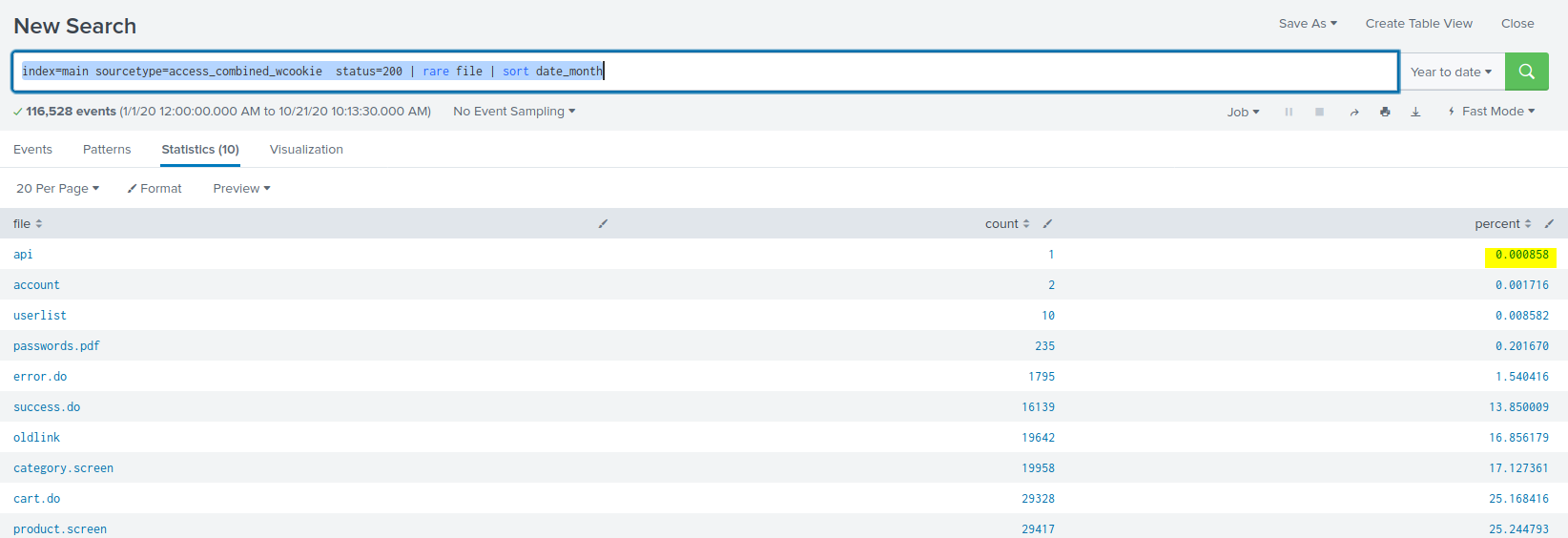
Sorting by date\_month

index=main sourcetype=access\_combined\_wcookie status=200 | rare file | sort date\_month



Least access file

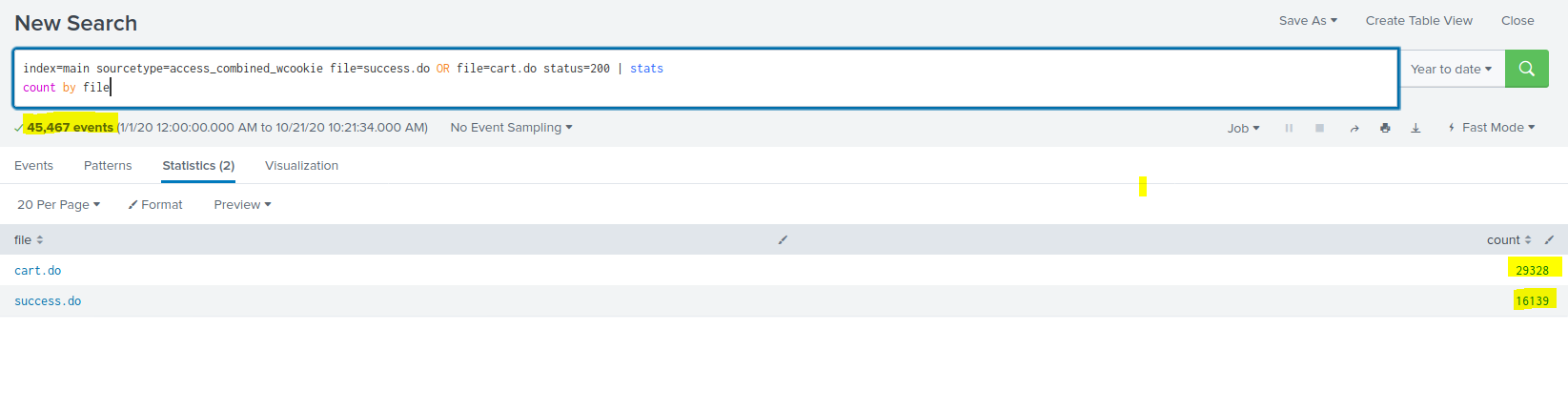
index=main sourcetype=access\_combined\_wcookie status=200 | rare file | sort date\_month



8

index=main sourcetype=access\_combined\_wcookie file=success.do OR file=cart.do status=200 | stats

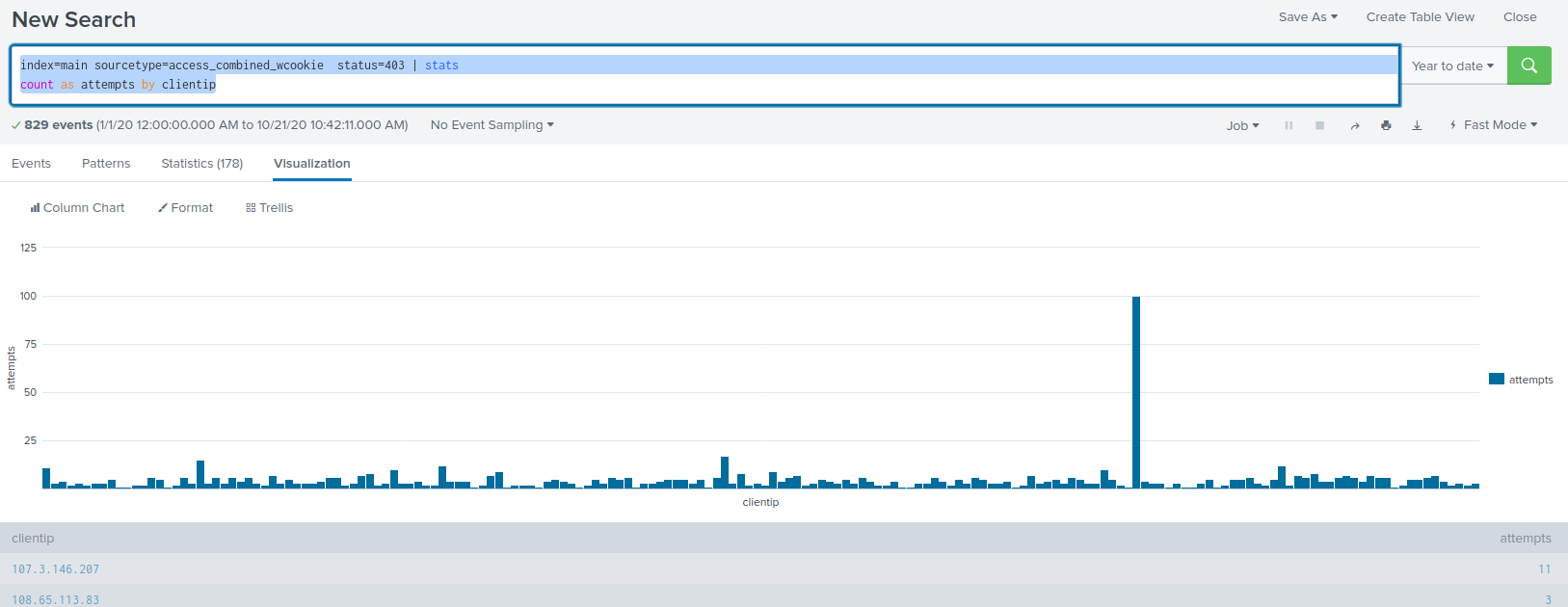
count by file



Module VII: CREATING REPORTS AND DASHBOARDS

index=main sourcetype=access\_combined\_wcookie status=403 | stats

count as attempts by clientip



index=main sourcetype=access\_combined\_wcookie status=200 file=success.do | stats

count as productId

