Name:Ramya Ajay

Roll No:CB.EN.P2CYS22004 Investigating with ELK 101

Task - 3 ElasticStack Overview

- collection of different open source components linked together to help users take the data from any source and in any format and perform a search, analyze and visualize the data at real-time.

Elasticsearch

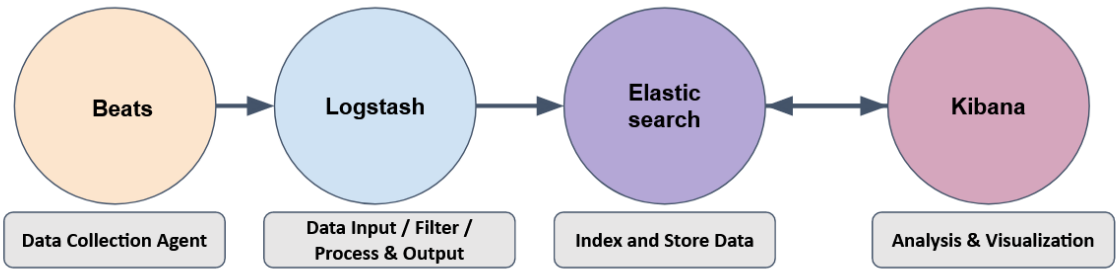
- full-text search and analytics engine used to store JSON-formated documents.
- important component used to store, analyze, perform correlation on the data, etc.

Logstash

- data processing engine used to take the data from different sources, apply the filter on it or normalize it, and then send it to the destination.
- **input part** is where the user defines the source from which the data is being ingested.
- **filter part** is where the user specifies the filter options to normalize the log ingested above.
- **output part** is where the user wants the filtered data to send.

Kibana

- web-based data visualization that works with elasticsearch to analyze, investigate and visualize the data stream in real-time.



a) Logstash is used to visualize the data. (yay / nay)

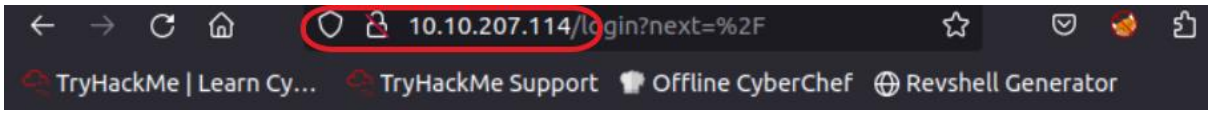
- nay

b) Elasticstash supports all data formats apart from JSON. (yay / nay)

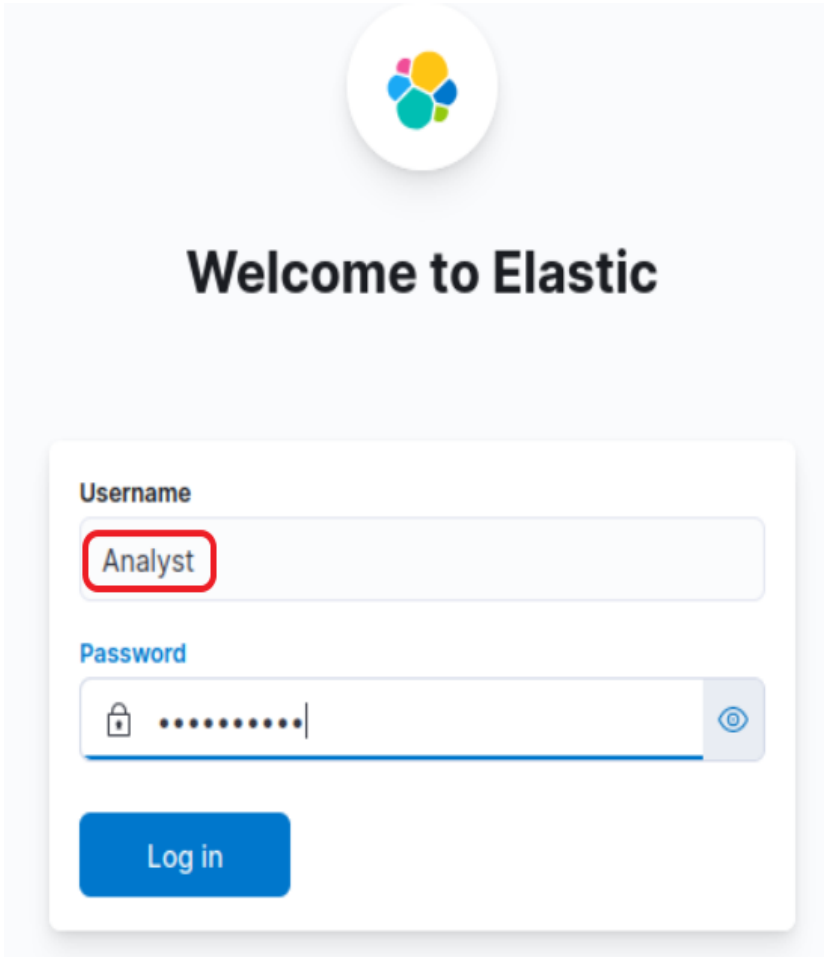
- nay

Task - 5 Discover tab

- First we get into the website of elastic search using the ip provided



- Now we login the wesbsite using the given credentials



- Now we are into the account which has the files for analysis and lets answer the questions

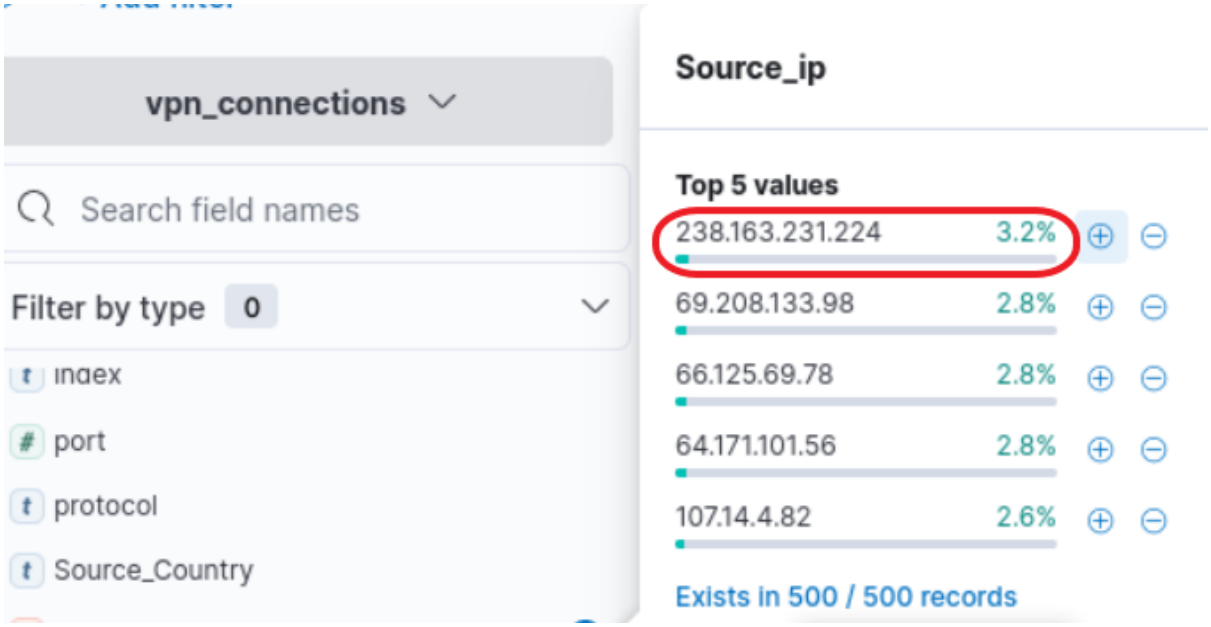
a) Select the index vpn_connections and filter from 31st December 2021 to 2nd Feb 2022. How many hits are returned?

- We first selected the filter vpn_connections and then set the time range from 31st December 2021 to 2nd Feb 2022.

- So it returned a value of '2861 hits'

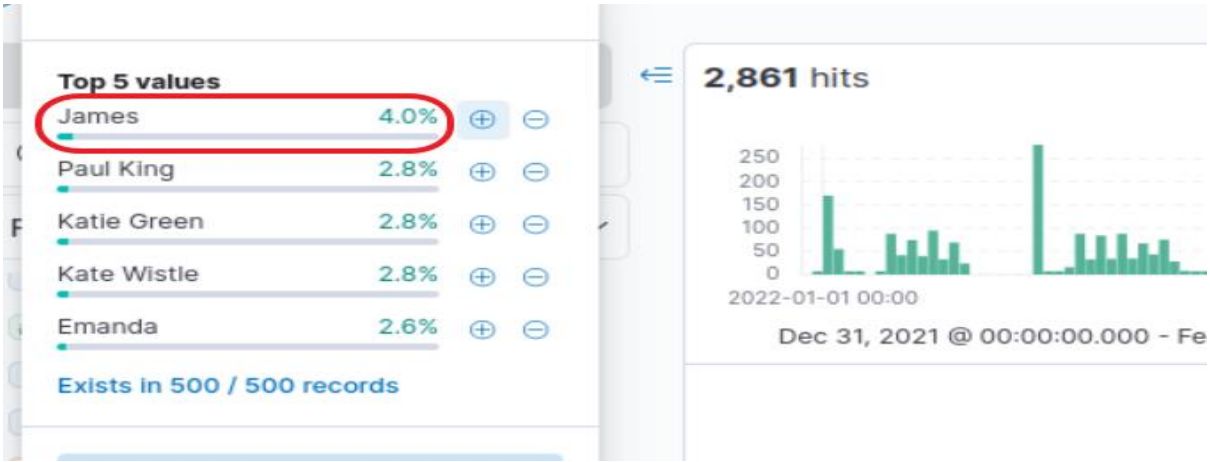
b) Which IP address has the max number of connections?

- When we get into the filters, we see a Source_ip filter present. When we open it we see an ip with maximum number of connection.



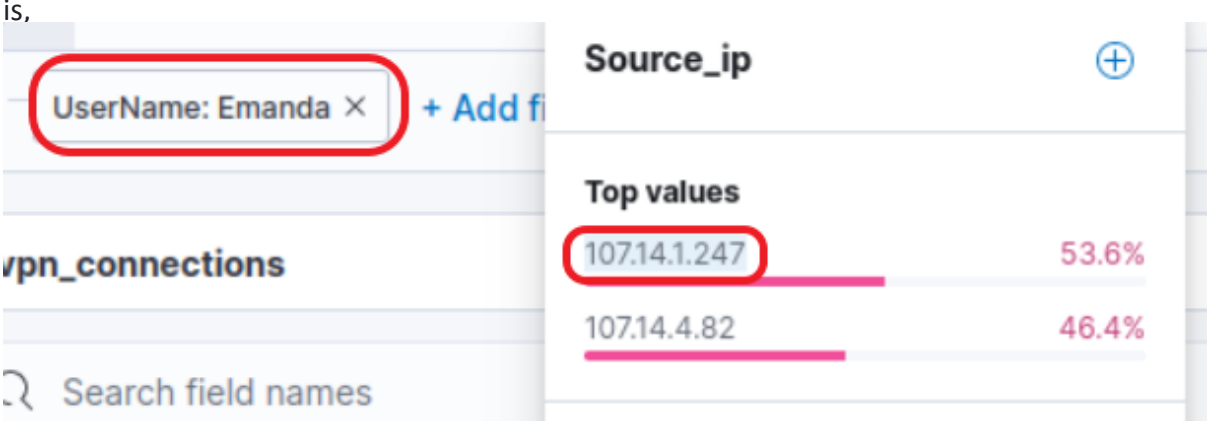
c) Which user is responsible for max traffic?

- Similarly if we select the filter 'Username' we get the user responsible for maximum traffic.



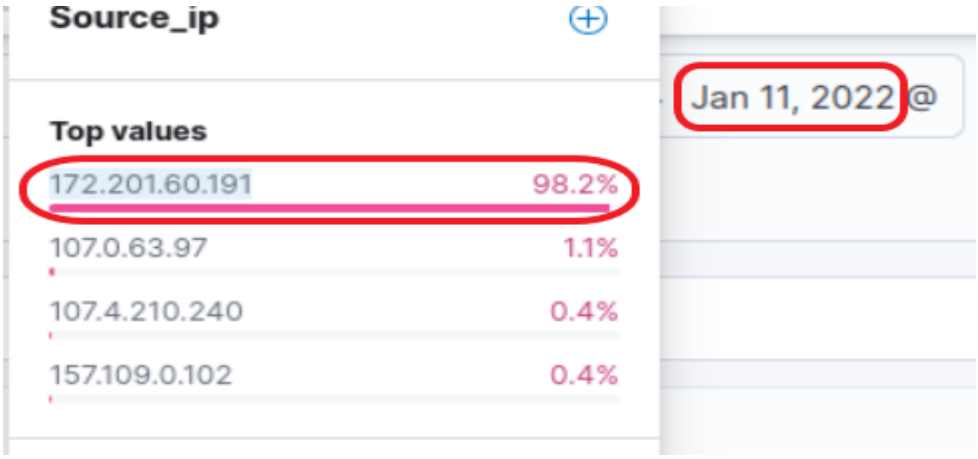
e) Apply Filter on UserName Emanda; which SourceIP has max hits?

- When we filter on UserName Emanda, we get the sourceIp used maximum is,



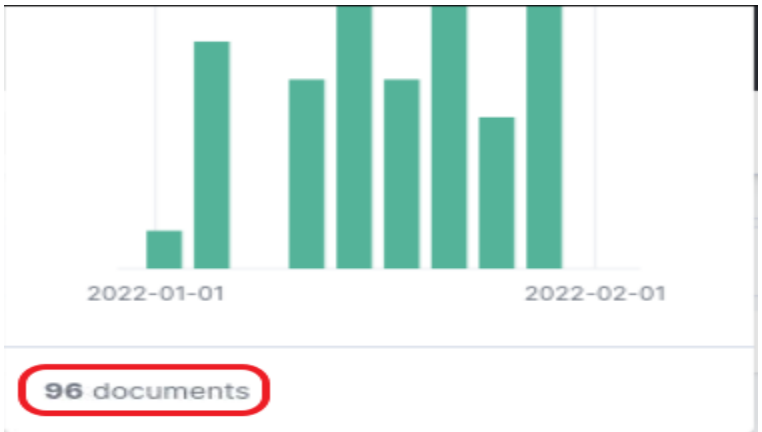
f) On 11th Jan, which IP caused the spike observed in the time chart?

- Now we filter the date to be 11th Jan and select the filter type as Source_ip and observe who has used the maximum traffic.

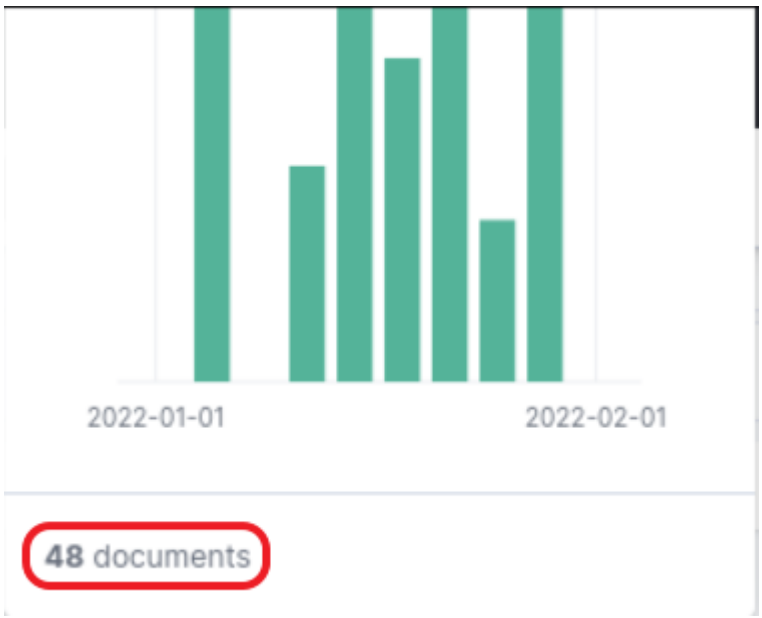


g) How many connections were observed from IP 238.163.231.224, excluding the New York state?

- When we give a filter of 238.163.231.224 in Source_ip, we get



- Now we give with filter 'New York'



- So we do the calculation of Total - Newyork(hits)
- 96 - 48 = 48

Task - 6 KQL Overview

KQL(Kibana Query Language)

- search query language used to search the ingested logs/documents in the elasticsearch.

With KQL, we can search for the logs in two different ways.

a) Free text Search

- allows users to search for the logs based on the text-only.

i)Wild Card

- KQL allows the wild card * to match parts of the term/word.

ii) Logical Operators (AND | OR | NOT)

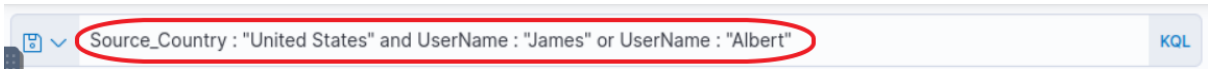
- 1- OR Operator
- 2- AND Operator
- 3- NOT Operator

b) Field-based search

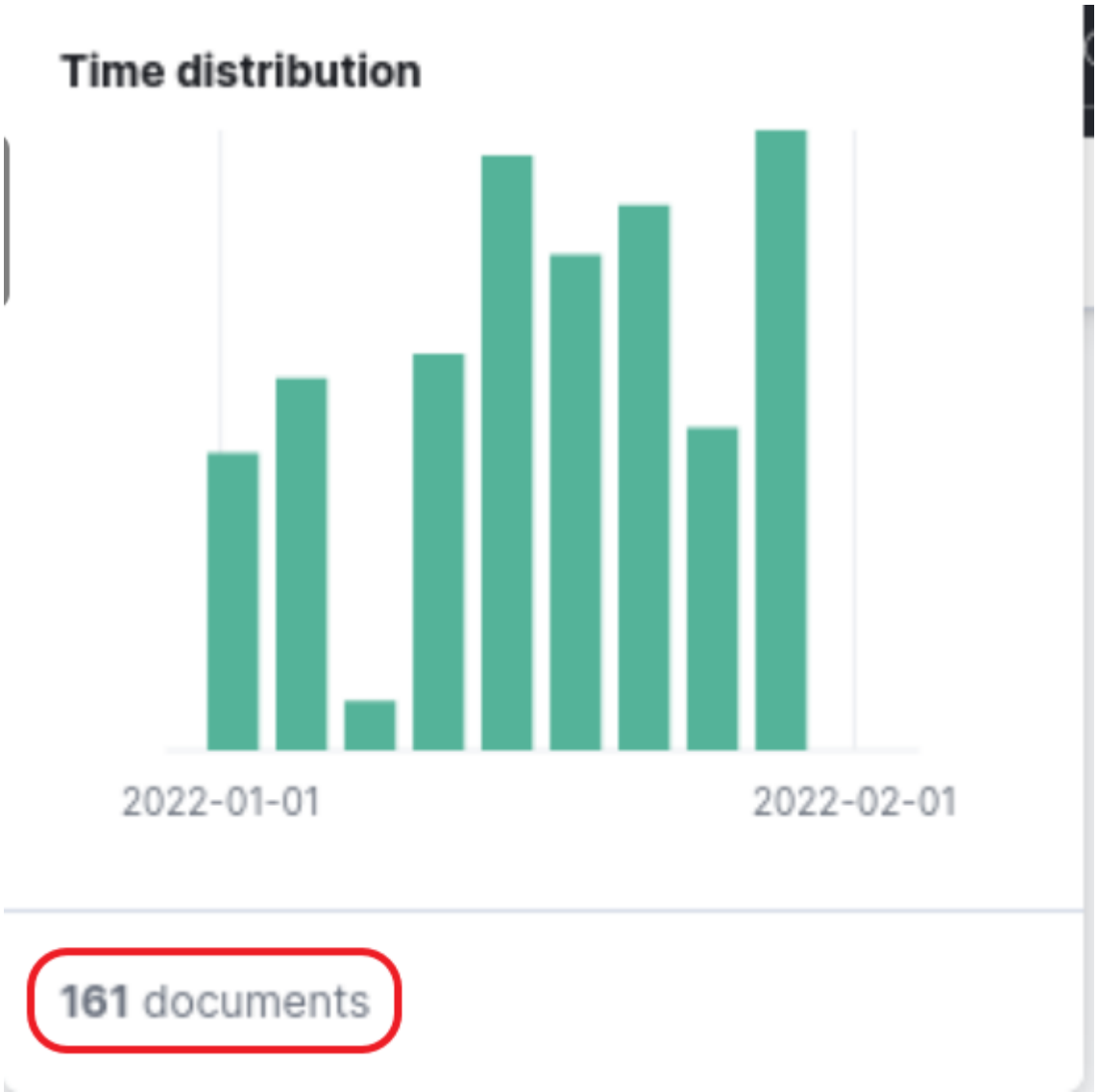
- we will provide the field name and the value we are looking for in the logs.

a) Create a search query to filter out the logs from Source_Country as the United States and show logs from User James or Albert. How many records were returned?

- The search query to filter the souce_country, username includes the following

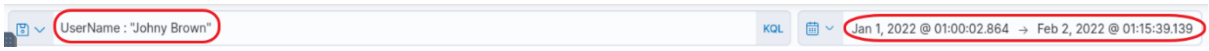


- When we select these filters we get output as
-



b) As User Johny Brown was terminated on 1st January 2022, create a search query to determine how many times a VPN connection was observed after his termination.

- In this we give the username filter as johny brown and the time to be from 1st January 2022

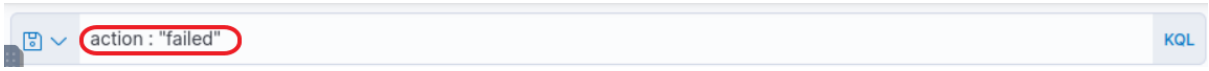


- This gives the result

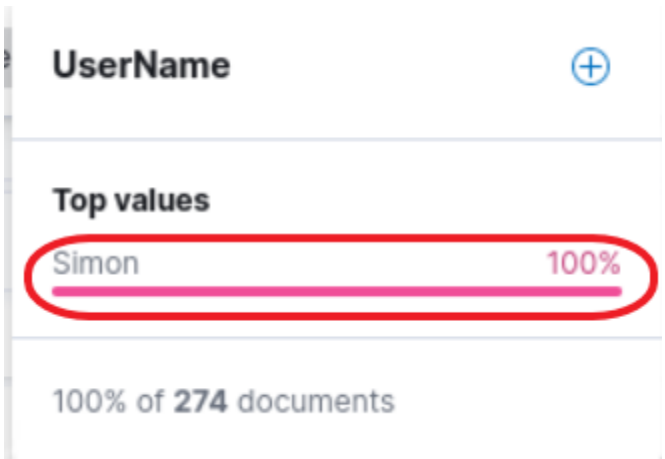
Task - 7 Create Visualizations

a) Which user was observed with the greatest number of failed attempts?

- In the filter search field, we give a filter action whose value is to be 'failed'

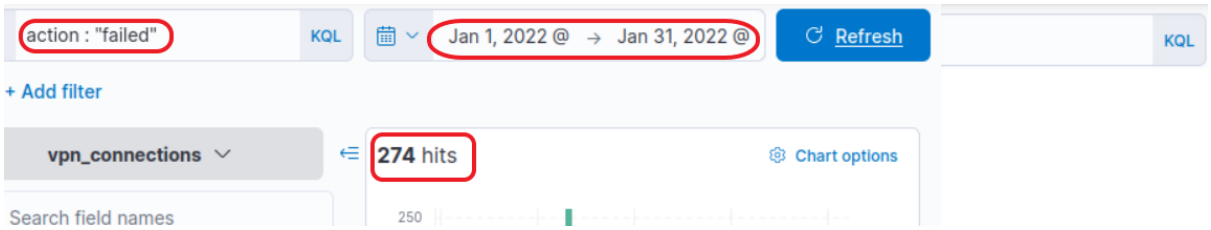


- Now we go the filter by type and set it as Username to get the result



b) How many wrong VPN connection attempts were observed in January?

- In this we proceed with the filter action with a value true and set the time from Jan 1st to Jan 31st which the number of hits.



Task - 8 Creating Dashboards

a) Create the dashboard containing the available visualizations.