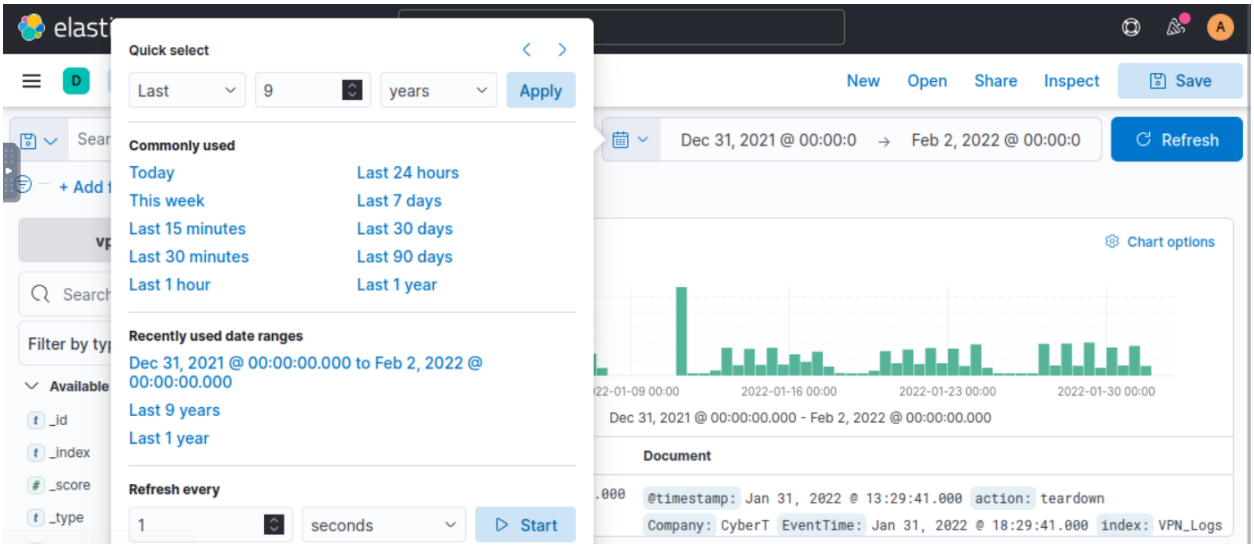
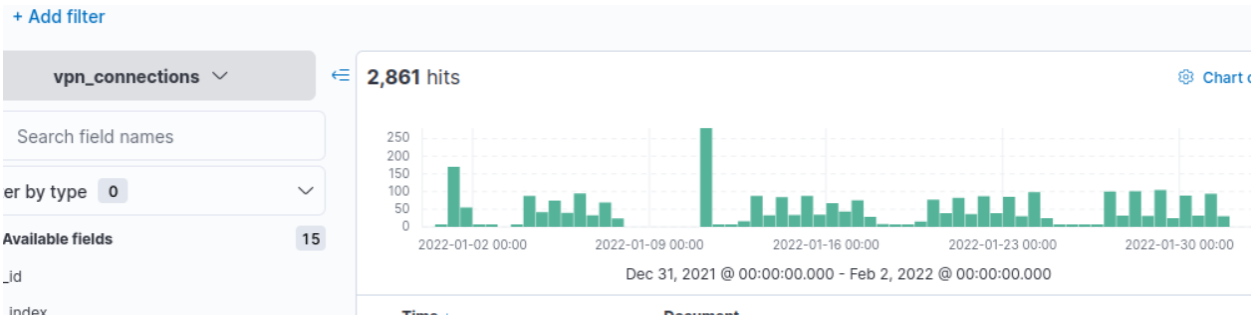
Elastic Stack: The basics 2026/01/05

Objective: Learning the ELK interface and its features from the Discover tab.

Step 1: Select the index **vpn_connections** and filter from 31st December 2021 to 2nd Feb 2022. How many hits are returned?

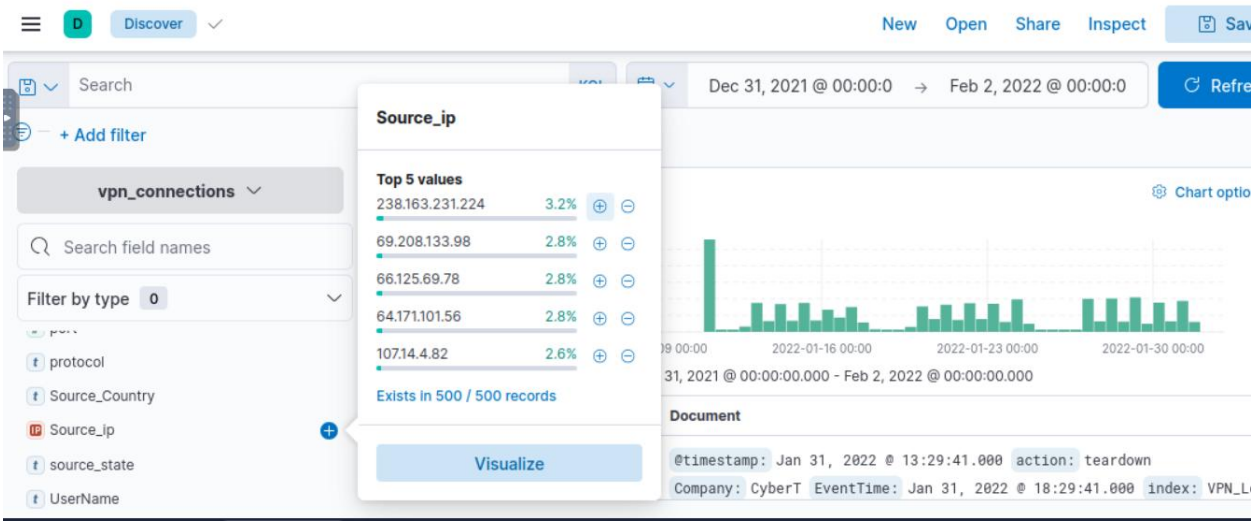


I clicked on the time filter and updated the values. I then clicked the update button which is now refresh button and ran it.



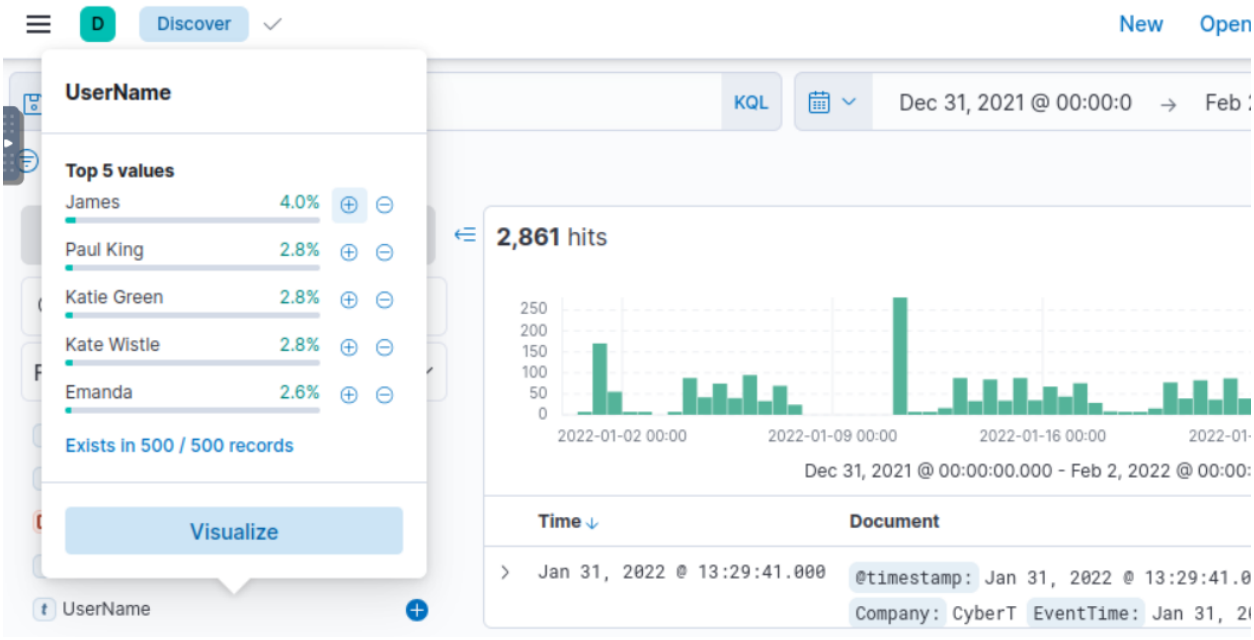
Looking back at the dashboard, we can see that we have **2861** hits.

Step 2: Which IP address has the maximum number of connections?



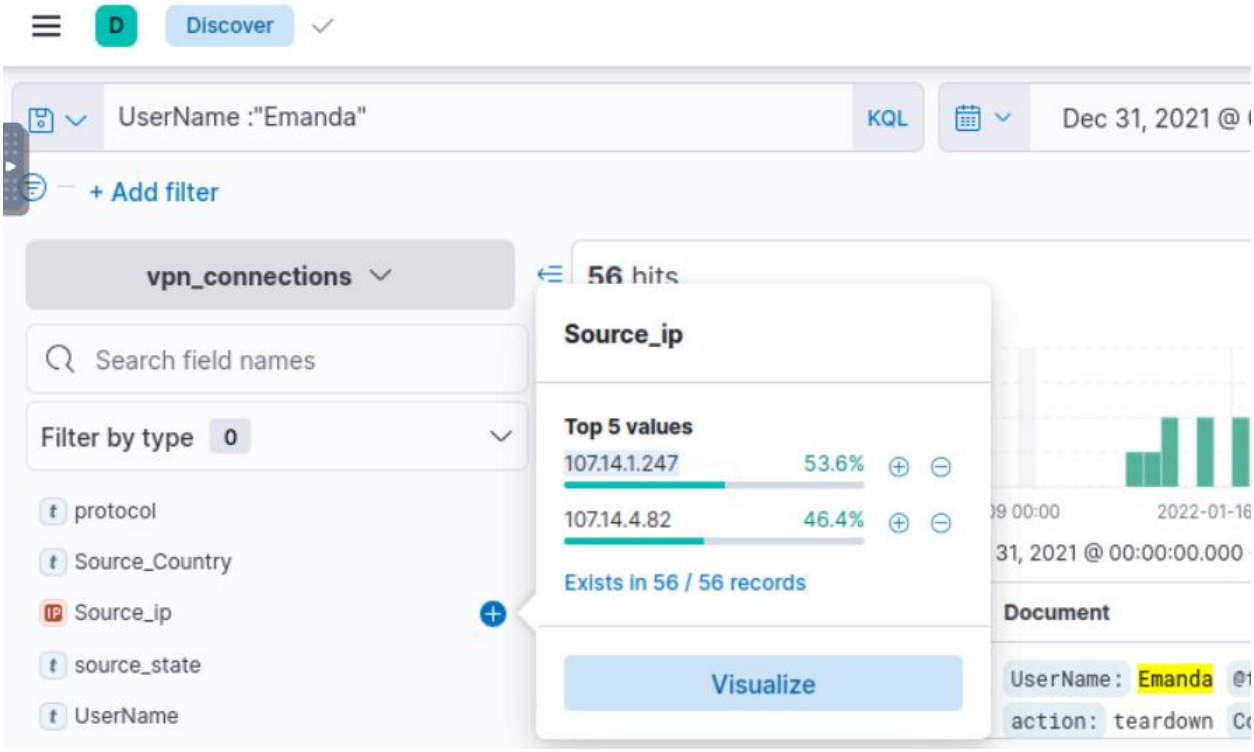
For this I went over to the fields pane on the left side and scrolled down to '**source_ip**'. The IP with the most number of connections was – 238.163.231.224.

Step 3: Which user is responsible for the overall maximum traffic?



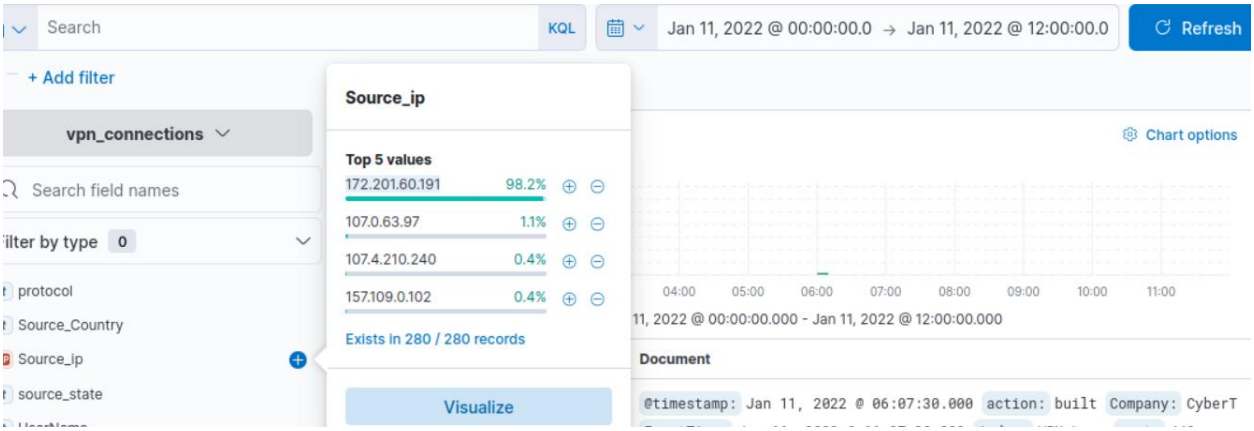
For this I scrolled further down the pane right up to the '**UserName**' field. The name responsible for the overall maximum traffic is – **James**.

Step 4: Apply Filter on UserName **Emanda;** which SourceIP has max hits?



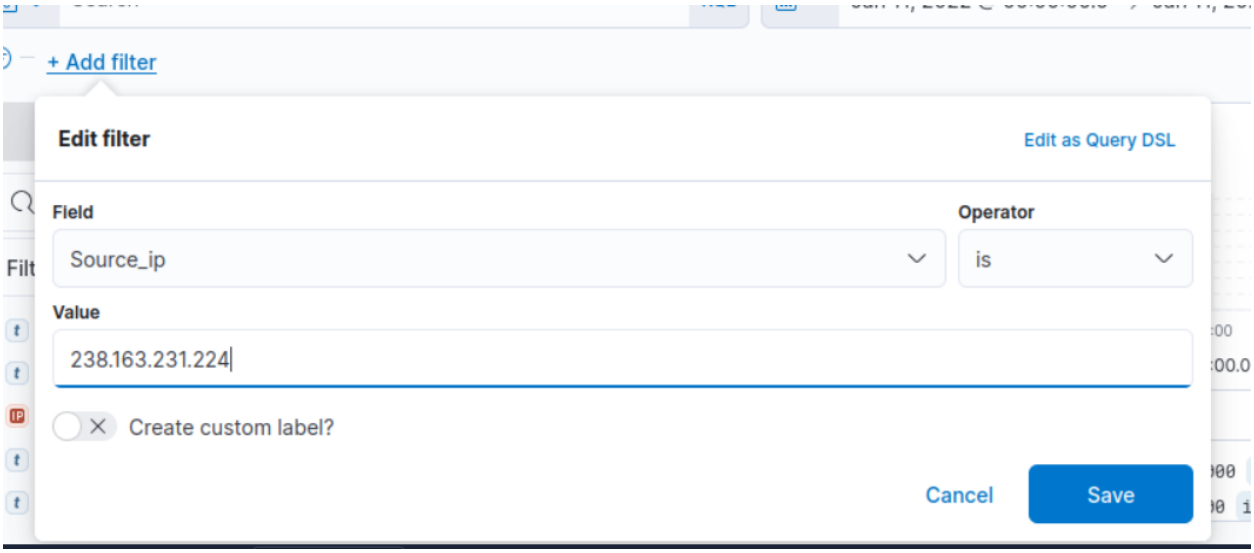
For this I applied the filter '**UserName :"Emanda"**', went to the left pane to scroll through the fields again and clicked on '**source_ip**'. The IP address that appeared with the most hits was - **107.14.1.247**.

Step 5: On 11th Jan, which IP caused the spike observed in the time chart?

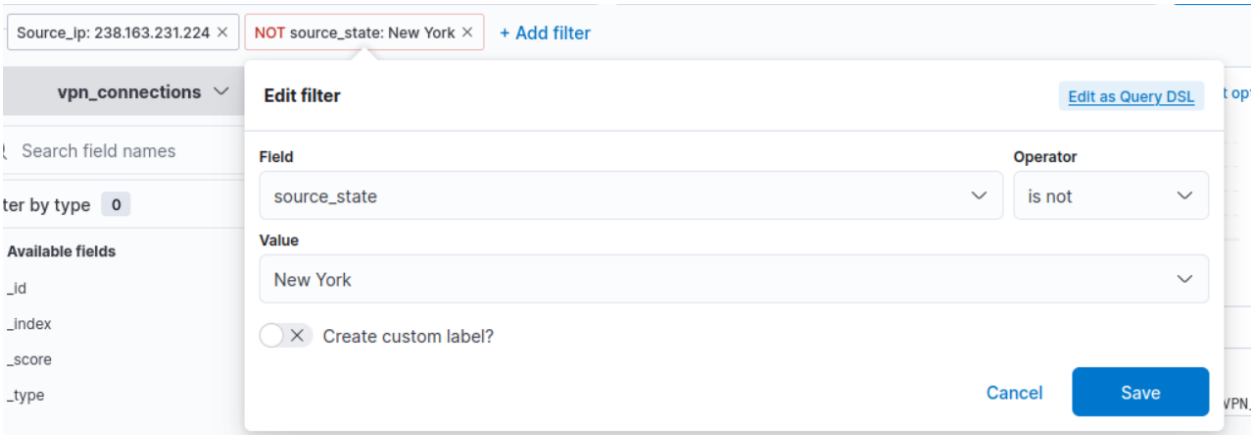


I went ahead and removed the filters, updated the page, then looked at the chart. I clicked on the 11th of January 2022, went to the fields pane then scrolled down to '**source_ip**' and clicked on it where I found the IP that caused the spike - **172.201.60.191**.

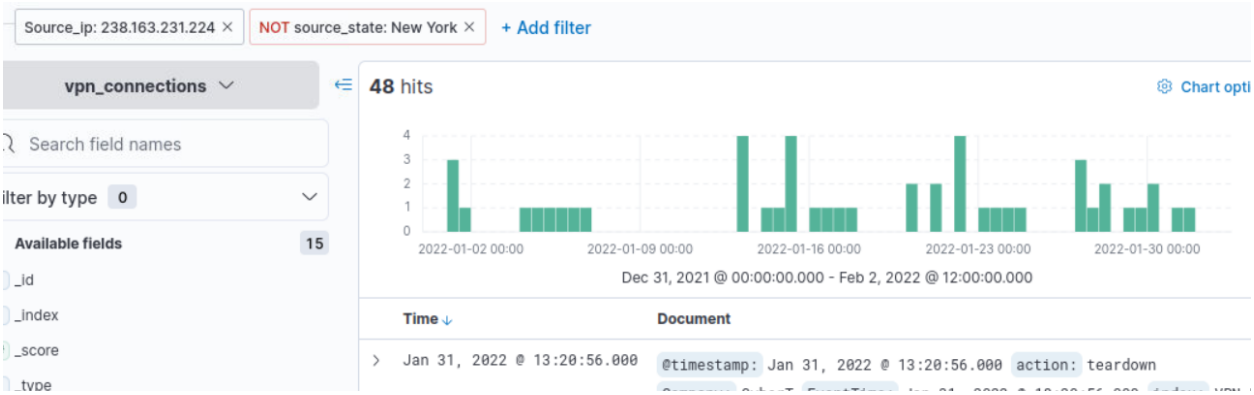
Step 6: How many connections were observed from IP **238.163.231.224**, excluding the **New York** state?



I clicked on add filter, added the necessary values in the Field, Operator, and Value sections and clicked save.



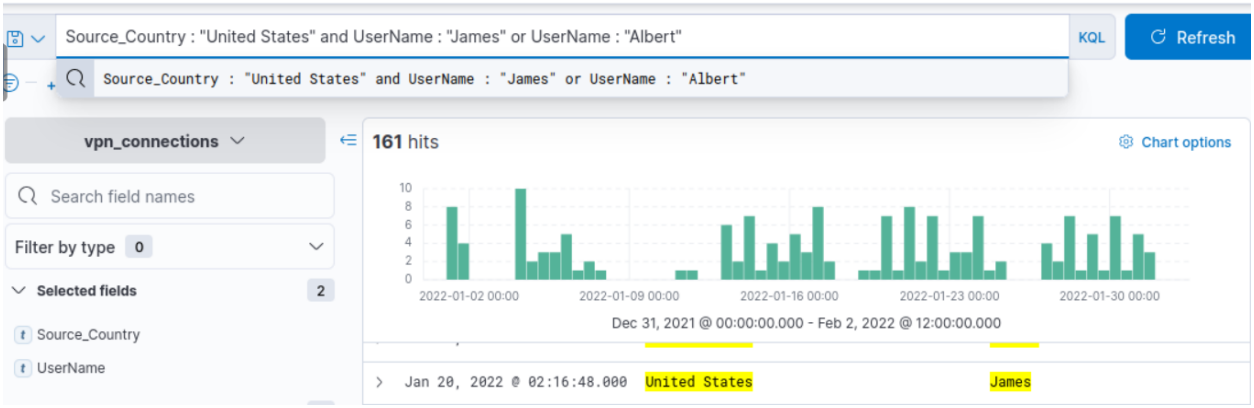
I clicked on add another filter, added the necessary values in the Field, Operator, and Value sections again and clicked save.



The IP had **48** hits.

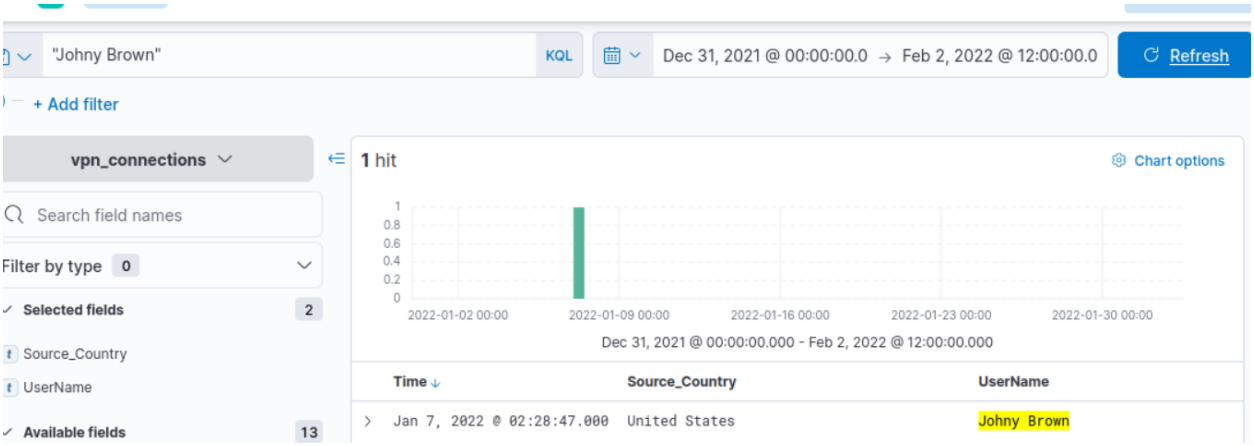
KQL Overview

Step 7: Create a search query to filter the logs where **Source_Country** is the **United States** and show logs from User **James** or **Albert**. How many records were returned?



I ended with a KQL query of – '**Source_Country : "United States" and UserName : "James" or UserName : "Albert"**'. The number of hits it had was – **161**.

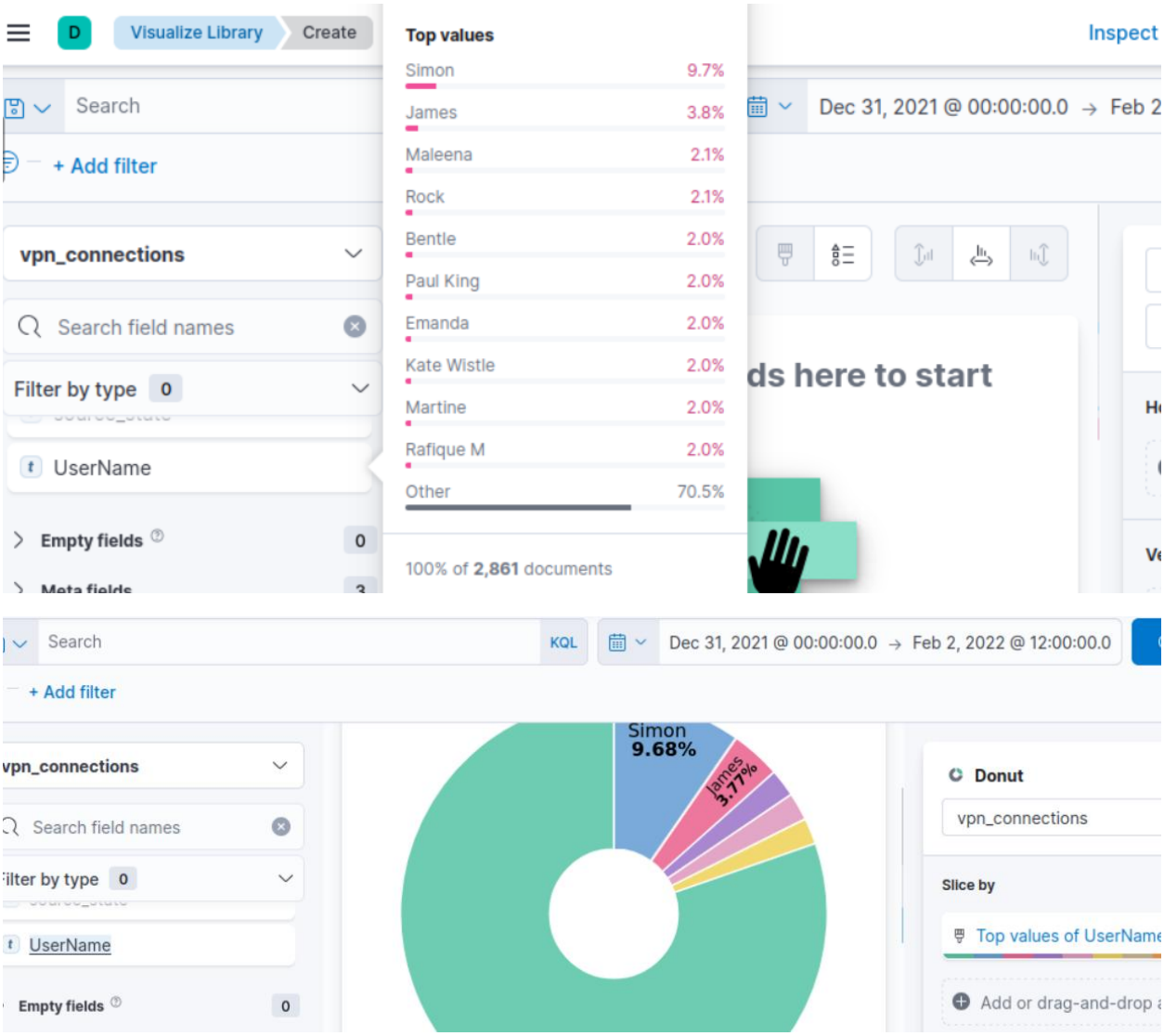
Step 8: A user **Johny Brown** was terminated on the 1st of January, 2022. Create a search query to determine how many times a VPN connection was observed after his termination.



I added the name as a free text search and **1** hit popped up after clicking update for **vpn_connections**.

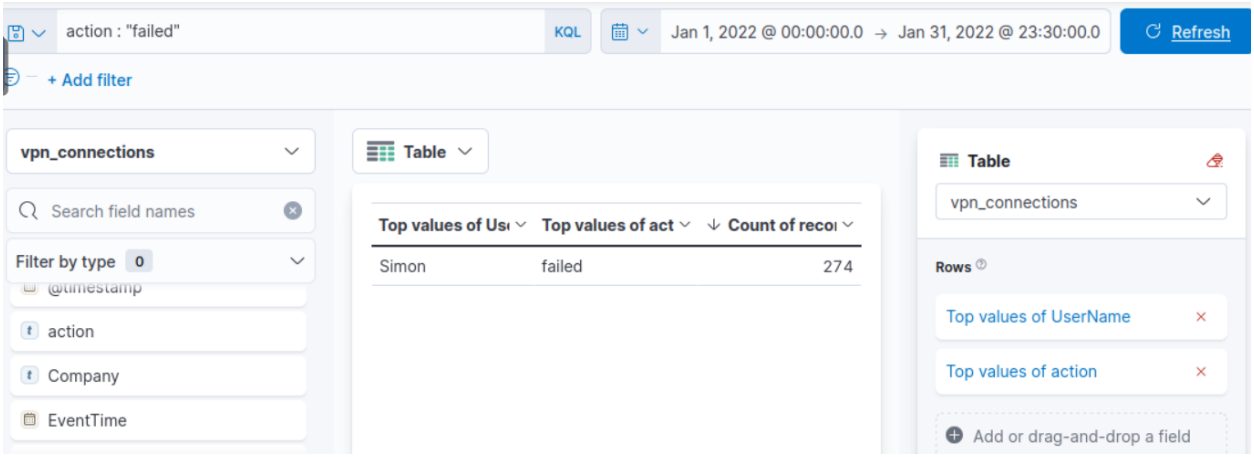
Visualization library

Step 9: Which user was observed with the greatest number of failed attempts?



After creating a lens on visual library, I clicked on the UserName field in the left pane and dragged it to the middle and then got the name – **Simon**.

Step 10: How many wrong VPN connection attempts were observed in January?



I changed the donut chart to a table and used 2 fields – **action** and **UserName**. I then added the query - **action : "failed"** and clicked update. I then got the number of failed vpn attempts – **274**.

Conclusion Summary

This lab provided hands-on exposure to the Elastic Stack interface, focusing on log exploration, filtering, and visualization through the Discover tab and KQL. By analysing VPN connection data, I identified traffic patterns, high-volume users, suspicious IP activity, and failed authentication attempts across specific timeframes. The exercise strengthened my ability to query, filter, and visualise log data effectively, reinforcing core SOC skills such as traffic analysis, user behaviour monitoring, and data-driven investigation using ELK.