(( (\_sourceCategory=apache AND !"::1 - -")or(\_source="klj23-03-apache-access")))

| parse "\* \* \* [\*] \"\* \* \*\" \* \* \"\*\" \"\*\"" as src\_ip,client\_id,user\_id,date\_time,Http\_method,uri,http\_version,Response\_Code,size,Referer,User\_Agent  
 **1. Count by source IP and response code. Order by count [panel1]**

(( (\_sourceCategory=apache AND !"::1 - -")or(\_source="klj23-03-apache-access")))

| parse "\* \* \* [\*] \"\* \* \*\" \* \* \"\*\" \"\*\"" as src\_ip,client\_id,user\_id,date\_time,Http\_method,uri,http\_version,Response\_Code,size,Referer,User\_Agent

| count by src\_ip, Response\_Code | order by \_count  
  
**2. Count by city, country name, and IP [panel2]**

(( (\_sourceCategory=apache AND !"::1 - -")or(\_source="klj23-03-apache-access")))

| parse "\* \* \* [\*] \"\* \* \*\" \* \* \"\*\" \"\*\"" as src\_ip,client\_id,user\_id,date\_time,Http\_method,uri,http\_version,Response\_Code,size,Referer,User\_Agent

| lookup latitude, longitude, country\_name, city from geo://location on ip = src\_ip

| fields src\_ip, country\_name, city

| count by country\_name, city, src\_ip

**3. Create a graph (chart) of daily access to the site [panel3]**

(( (\_sourceCategory=apache AND !"::1 - -")or(\_source="klj23-03-apache-access")))

| parse "\* \* \* [\*] \"\* \* \*\" \* \* \"\*\" \"\*\"" as src\_ip,client\_id,user\_id,date\_time,Http\_method,uri,http\_version,Response\_Code,size,Referer,User\_Agent

| timeslice 1d

| count by \_timeslice

**4. Create a pie chart based on the response code (percentage of response codes) [panel4]**

(( (\_sourceCategory=apache AND !"::1 - -")or(\_source="klj23-03-apache-access")))

| parse "\* \* \* [\*] \"\* \* \*\" \* \* \"\*\" \"\*\"" as src\_ip,client\_id,user\_id,date\_time,Http\_method,uri,http\_version,Response\_Code,size,Referer,User\_Agent

| count by Response\_code

**5. Create a map to visualize successful viewer users' (http\_metod="GET") location, based on the source\_ip [panel5]**

(( (\_sourceCategory=apache AND !"::1 - -")or(\_source="klj23-03-apache-access")))

| parse "\* \* \* [\*] \"\* \* \*\" \* \* \"\*\" \"\*\"" as src\_ip,client\_id,user\_id,date\_time,Http\_method,uri,http\_version,Response\_Code,size,Referer,User\_Agent

| where Http\_method = "GET"

| lookup latitude, longitude from geo://location on ip = src\_ip

| count by latitude, longitude,src\_ip

**6. Create a map to visualize users' location that wants to update the Website (http\_metod="POST") based on the source IP [panel6]**

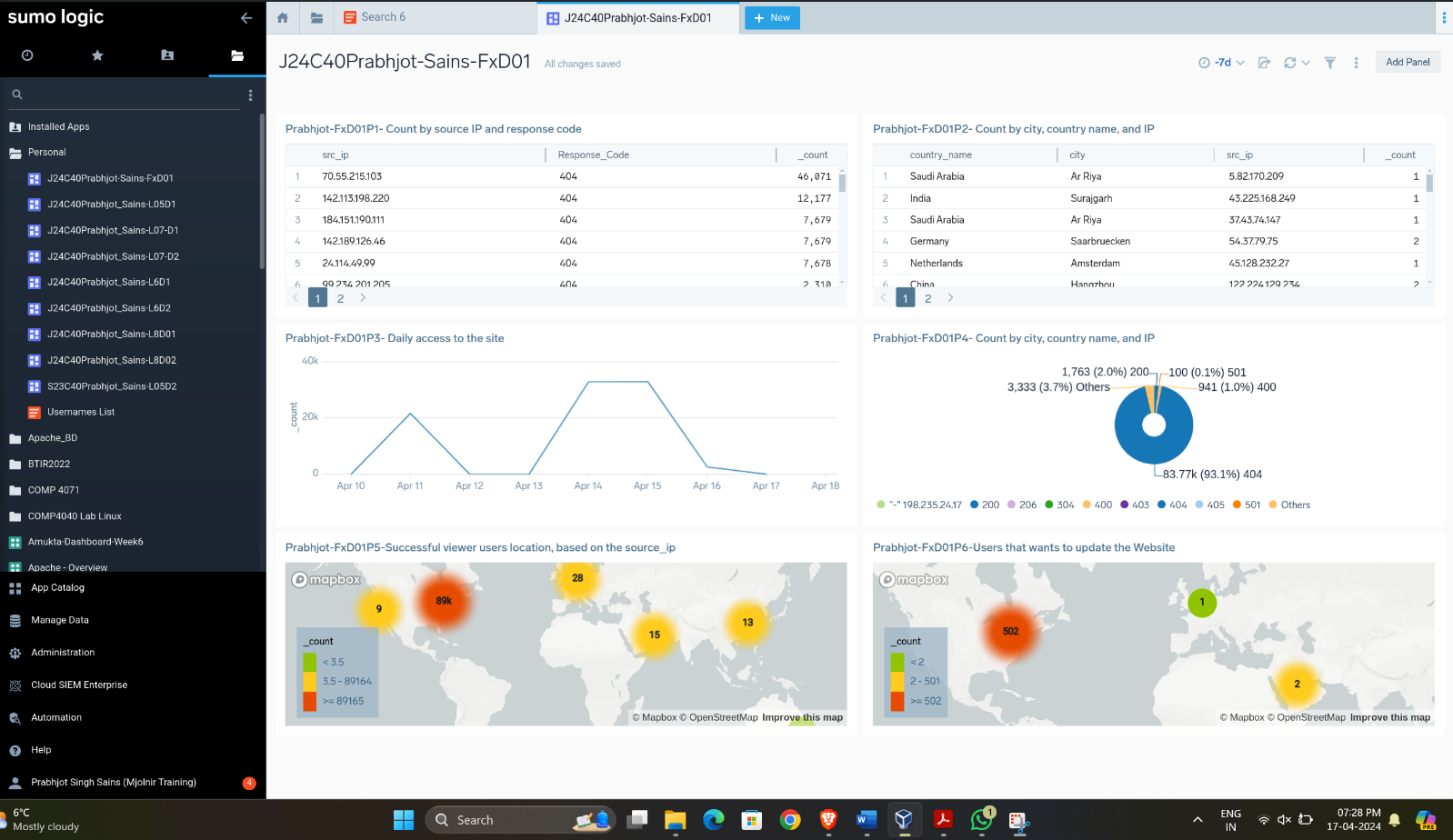
(( (\_sourceCategory=apache AND !"::1 - -")or(\_source="klj23-03-apache-access")))

| parse "\* \* \* [\*] \"\* \* \*\" \* \* \"\*\" \"\*\"" as src\_ip,client\_id,user\_id,date\_time,Http\_method,uri,http\_version,Response\_Code,size,Referer,User\_Agent

| where Http\_method = "POST"

| lookup latitude, longitude from geo://location on ip = src\_ip

| count by latitude, longitude,src\_ip



1. Panel 1: This table is used for analyzing web traffic, specifically tracking the frequency of 404 errors encountered by different source IPs. The high counts suggest repeated attempts to access unavailable content.
2. Panel 2: It shows the traffic count on the website from the country name and city based on the source ID. Each row represents a unique combination of country name, city, and source IP with their count
3. Panel 3: It shows the graph of daily access to the website by the users. The graph provides a visual representation of site traffic, highlighting a significant spike in accesses on April 14, followed by a steep drop-off.
4. Panel 4: It shows the percentage of response code. The pie chart provides a visual breakdown of the frequency of HTTP status codes for a particular dataset, with a significant majority being the 404 error code.
5. Panel 5: It shows the successful user location on the website based on source IP. The map provides a clear visual representation of where the users are located globally, with the largest concentration in Europe.
6. Panel 6: It shows the user location based on the source IP that wants to update the website. The map provides a visual representation of user distribution and their desire to update a website, with a significant number of users concentrated in North America.