Splunk Dashboard for Web Traffic Logs

By GOKUL KRISHNA K

OBJECTIVE

The objective of this project is to analyze and monitor web server traffic using Splunk by visualizing total web requests, successful responses, client errors, top requested URLs, and web traffic by client IP address to improve performance and enhance security visibility.

Tools used

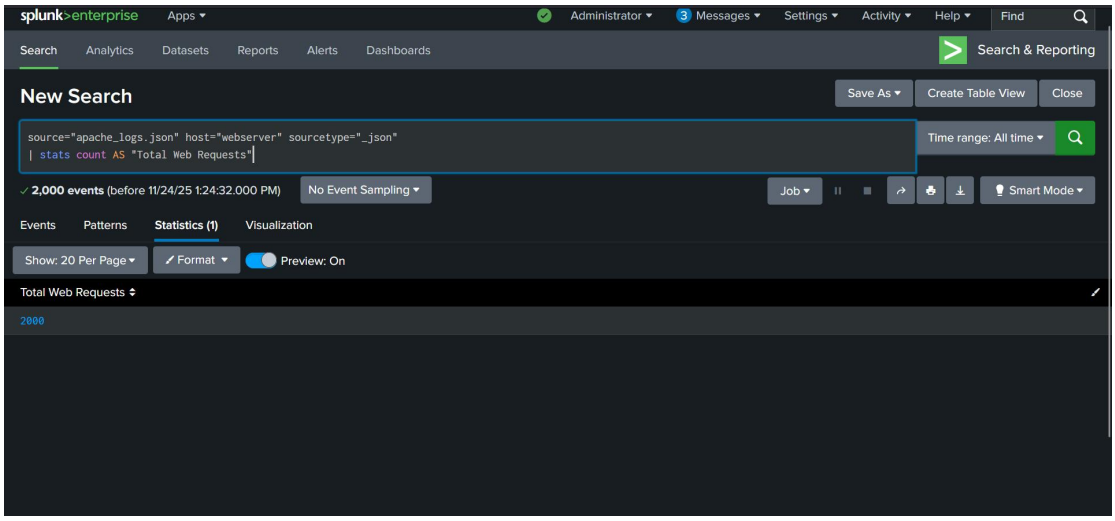
- Splunk
- apache_logs.json file

Task1: Web Activities

To track and analyze user actions and request patterns on the website, helping understand user behavior and detect any suspicious or abnormal activity

1. Total web request

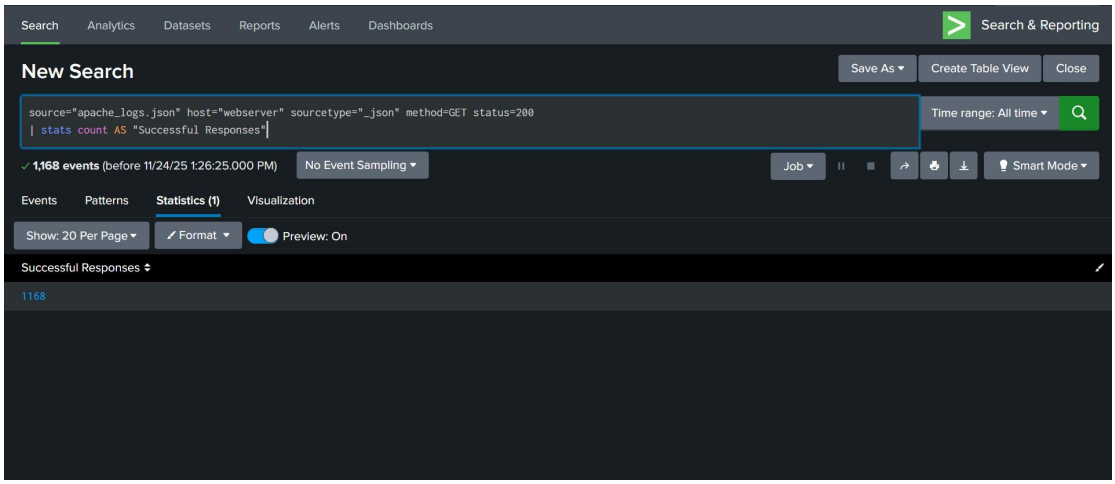
This is for understand how many total requests the web server receives, which helps measure website usage, detect unusual spikes, and monitor overall server performance.



Ouery: source="apache_logs.json" host="webserver" sourcetype="_json"
| stats count AS "Total Web Requests"

2. Successful web response

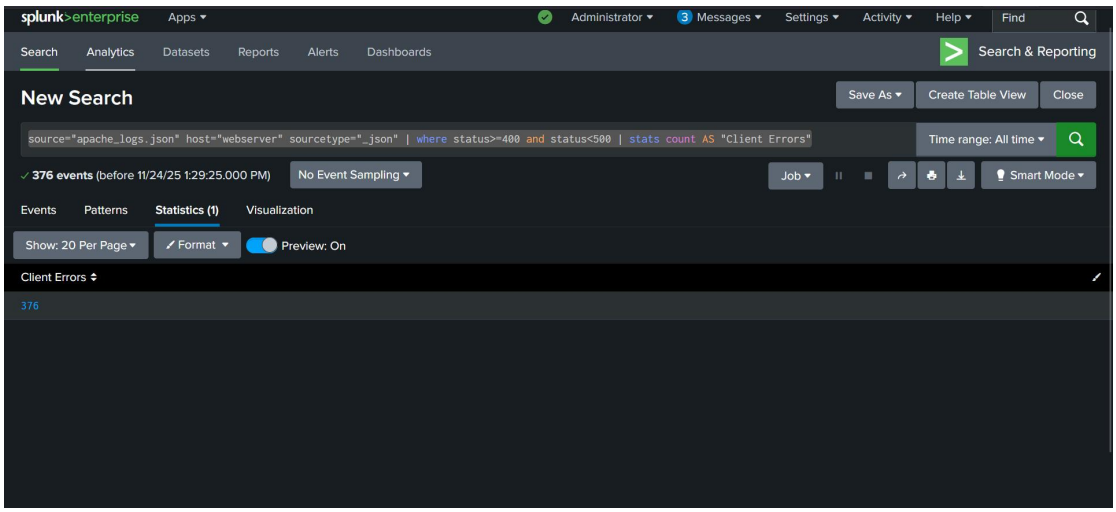
To track how many requests were successfully handled by the webserver (HTTP 2xx), so we can confirm the server is healthy and responding correctly to users.



Query : source="apache_logs.json" host="webserver" sourcetype="_json" method=GET status=200
| stats count AS "Successful Responses"

3. Client Error

To identify how many requests failed due to client-side issues (HTTP 4xx), helping detect broken links, bad requests, or user-side problems



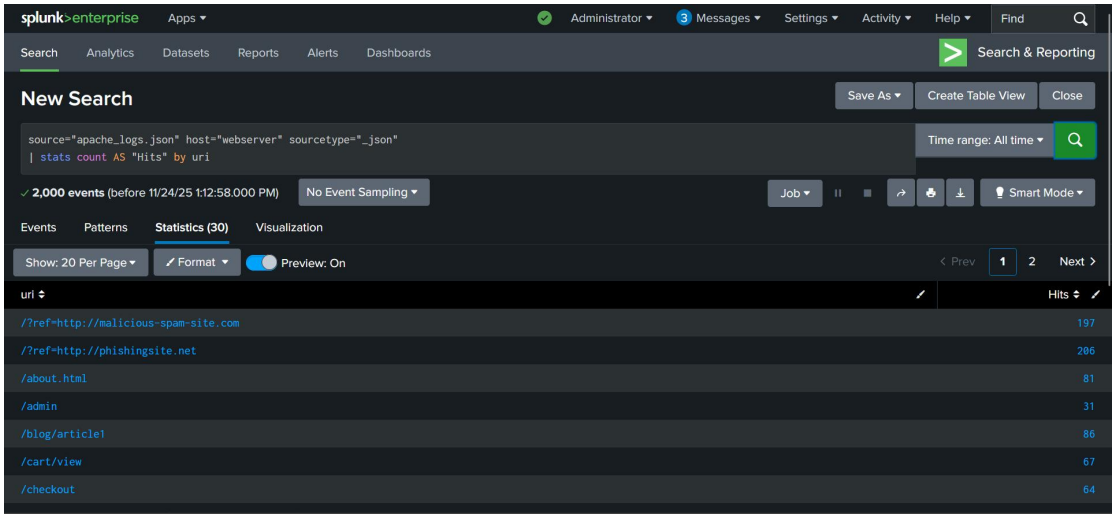
Query: source="apache_logs.json" host="webserver" sourcetype="_json" | where status>=400 and status<500 | stats count AS "Client Errors"

Task2: Web Stats

To analyze overall website activity such as hits, unique users, response types, and traffic patterns to understand how the webserver is being used and to detect any unusual behavior

1. Top Requested URIs

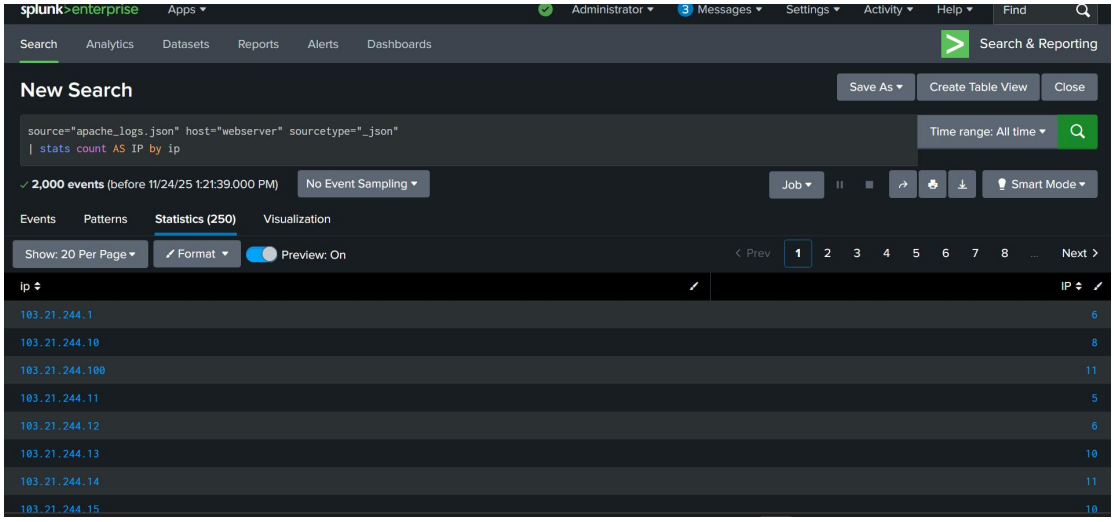
To identify the most frequently accessed pages or endpoints, helping understand user interest, traffic hotspots, and detect unusual or suspicious access patterns.



Query: source="apache_logs.json" host="webserver" sourcetype="_json"
| stats count AS "Hits" by uri

2. Top users by ip address

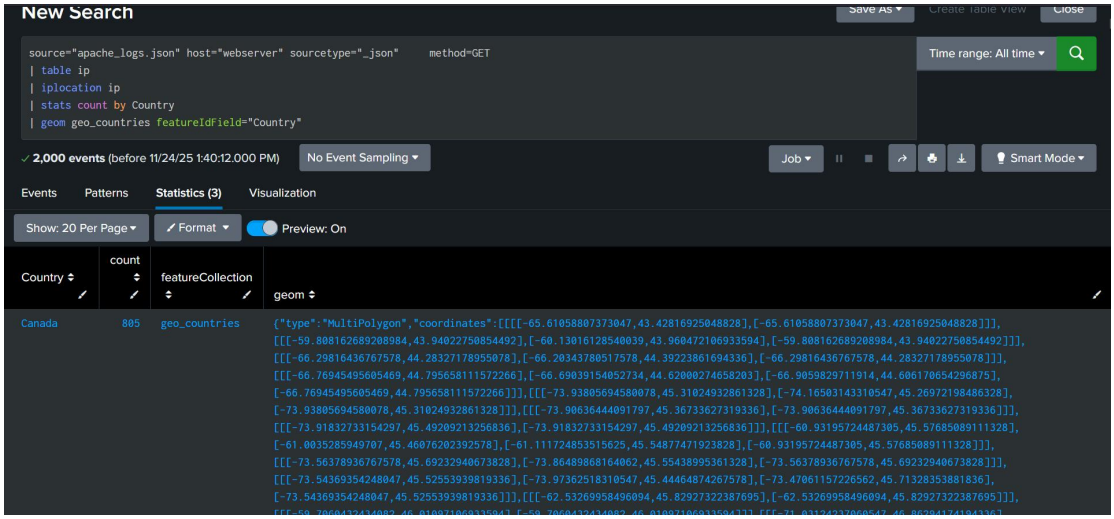
To identify which IP addresses generate the most requests, helping track heavy users, analyze traffic sources, and detect potential malicious or abnormal activity



Query:
source="apache_logs.json" host="webserver" sourcetype="_json"
| stats count AS IP by ip

Task3: Web Traffic by Client IP Addresses

To analyze how much traffic each client IP generates, helping identify active users, detect abnormal spikes, and spot potential malicious IPs.



Query:
source="apache_logs.json" host="webserver" sourcetype="_json"
method=GET
| table ip
| iplocation ip
| stats count by Country
| geom geo_countries featureIdField="Country"