

# **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**

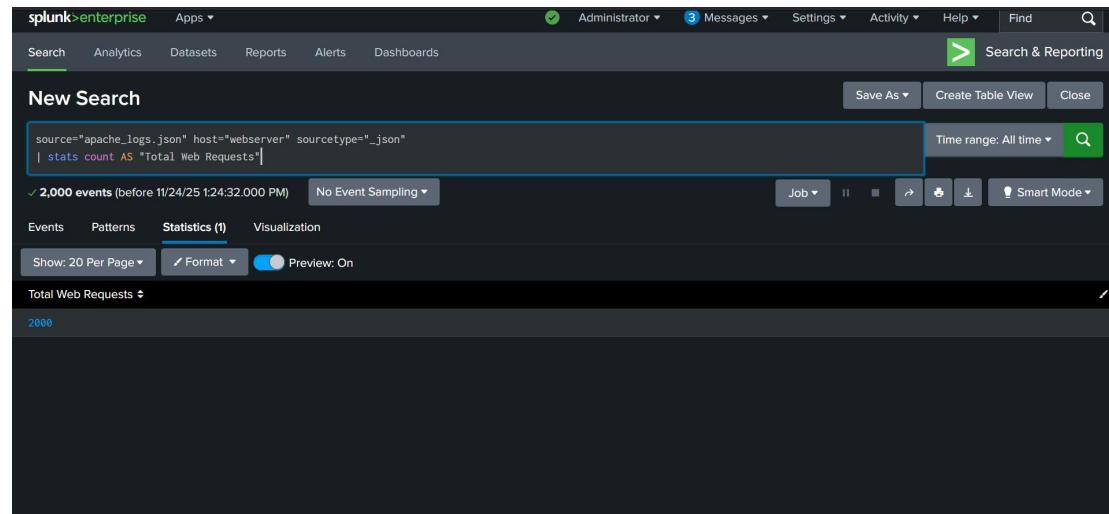
- . Splunk
- . apache\_logs.json file

## 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.

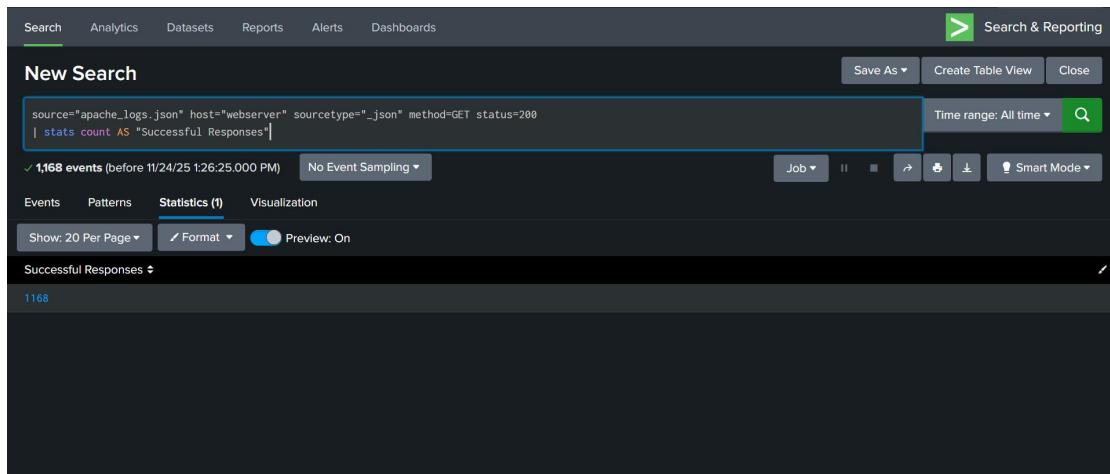


The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `source="apache_logs.json" host="webserver" sourcetype="_json" | stats count AS "Total Web Requests"`. The results pane displays a single row of data with the value '2,000' under the 'Total Web Requests' column. The interface includes standard Splunk navigation and search controls.

Query: `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.



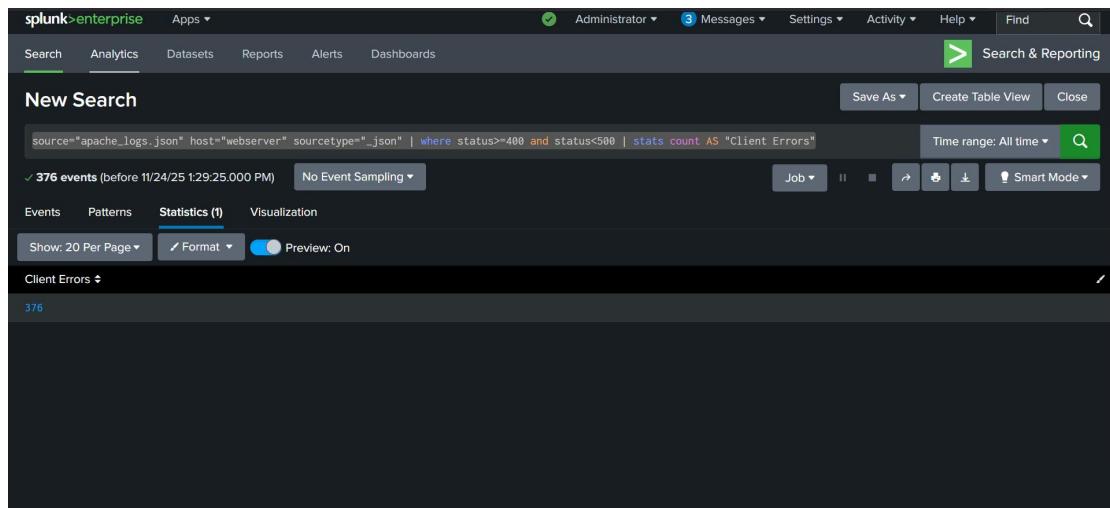
The screenshot shows the Splunk interface with the following details:

- Search Bar:** The search bar contains the command: `source="apache_logs.json" host="webserver" sourcetype="_json" method=GET status=200 | stats count AS "Successful Responses"`.
- Results Summary:** It shows **1,168 events (before 11/24/25 1:26:25.000 PM)** and **No Event Sampling**.
- Statistics View:** The Statistics tab is selected, showing one result: **Successful Responses** with a value of **1168**.
- Navigation and Tools:** The interface includes tabs for Events, Patterns, Visualization, and Statistics. It also features a search bar, time range selector, and various dashboard controls.

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

A screenshot of the Splunk Enterprise search interface. The search bar contains the query: "source='apache\_logs.json' host='webserver' sourcetype='json' | where status>=400 and status<500 | stats count AS 'Client Errors'". The results section shows a single row with the value "376". The interface includes standard Splunk navigation and search controls.

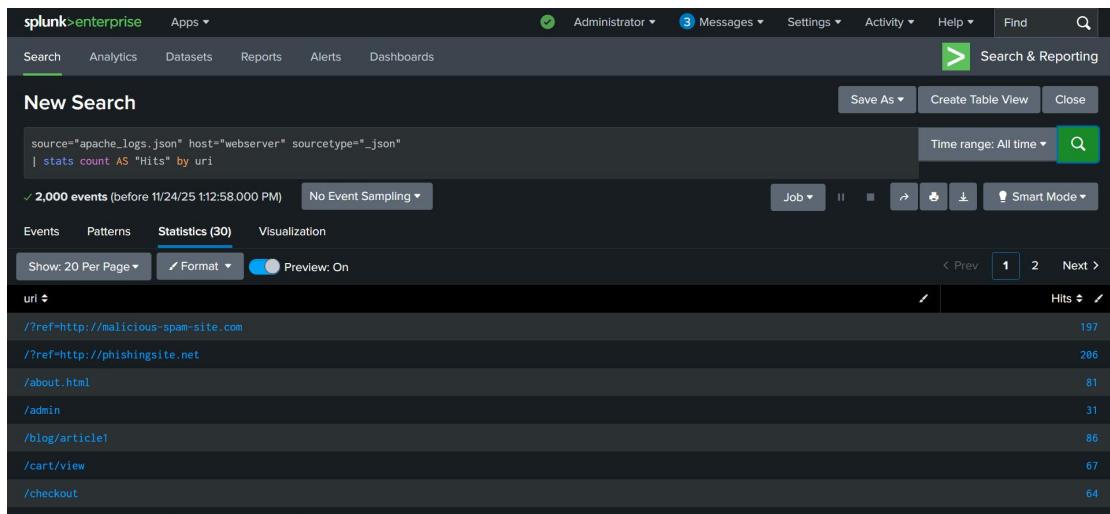
Query: source="apache\_logs.json" host="webserver" sourcetype="json" | where status>=400 and status<500 | stats count AS "Client Errors"

## 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.



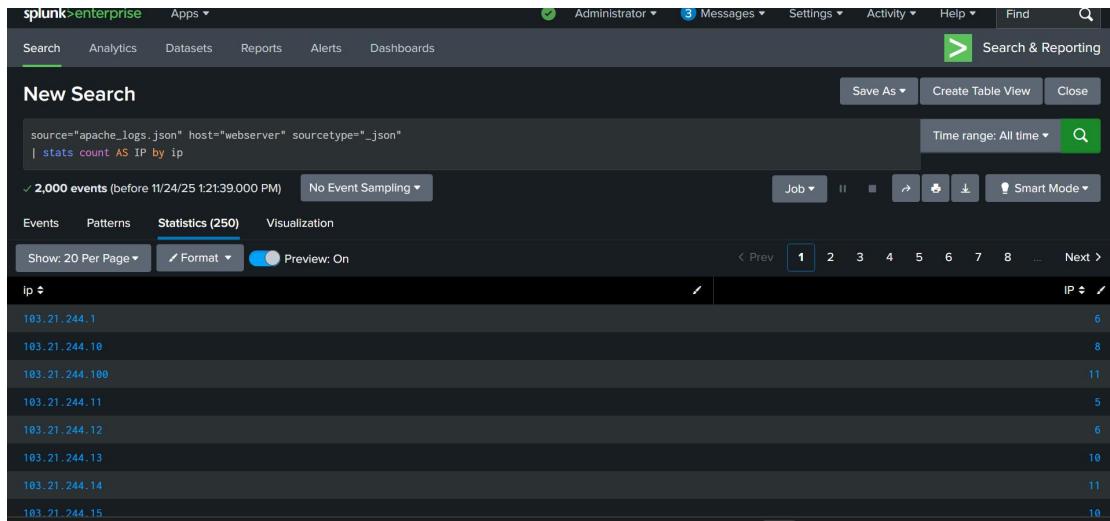
The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `source="apache_logs.json" host="webserver" sourcetype="_json" | stats count AS "Hits" by uri`. The results section displays 2,000 events from the time range 'All time'. The 'Statistics' tab is selected, showing a table of URLs and their hit counts. The table is sorted by hits in descending order. The top entries are:

url	Hits
?ref=http://malicious-spam-site.com	197
?ref=http://phishingsite.net	286
/about.html	81
/admin	31
/blog/article1	86
/cart/view	67
/checkout	64

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.

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** source="apache\_logs.json" host="webserver" sourcetype="\_json" method=GET
- Time Range:** All time
- Event Count:** 2,000 events (before 11/24/25 1:40:12:00 PM)
- Sampling:** No Event Sampling
- Job Buttons:** Job, II, ■, ↗, ↘, Smart Mode
- Statistics (3) Tab:** Selected.
- Visualization:** Not selected.
- Table Headers:** Country, count, featureCollection, geom.
- Data Rows:** One row for Canada, showing 805 events. The 'geom' column contains a complex JSON object representing a MultiPolygon geometry for Canada's borders.

## Query:

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