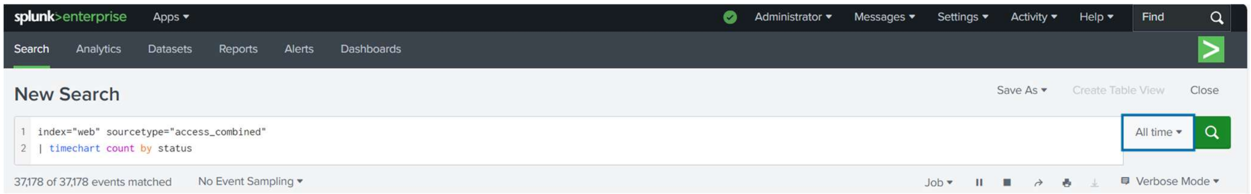
Initial Search Query

- **Description:** This screenshot shows the base Splunk search interface where raw logs are loaded for analysis.
- **Purpose:** Establishes the scope of data and begins the investigation by loading all available events in the selected time frame.
- **Action:** User inputs a time range and launches the first query.
- **Insights:** Sets the initial context for further filtering and aggregation.



New Search

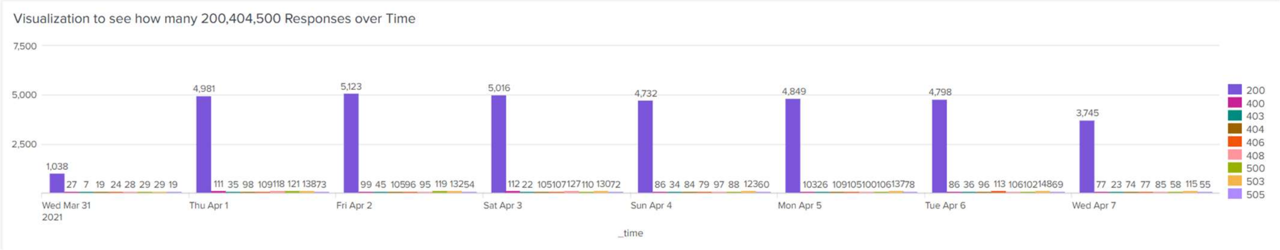
```
index="web" sourcetype="access_combined"
| timechart count by status
```

37,178 of 37,178 events matched

No Event Sampling ▾

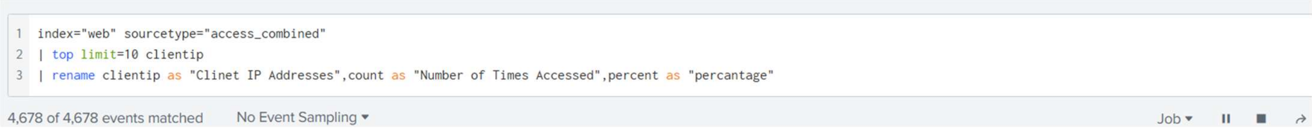
Filtering Log Events

- **Description:** Displays a refined Splunk search where logs are filtered, for example by source or severity.
- **Purpose:** Narrows down the raw data to a manageable subset—such as error events, warnings, or specific hosts.
- **Action:** Utilizes SPL commands (source=xyz, log_level=ERROR) to isolate critical data.
- **Insights:** Allows targeted troubleshooting or incident review.



Aggregation and Statistics

- **Description:** Highlights the statistics panel, showing summarized metrics—such as event counts per error type or user.
- **Purpose:** Aggregates logs to provide numerical summaries.
- **Action:** Uses SPL functions like stats count by event_type for fast assessment.
- **Insights:** Identifies patterns, such as most frequent issues or active users.

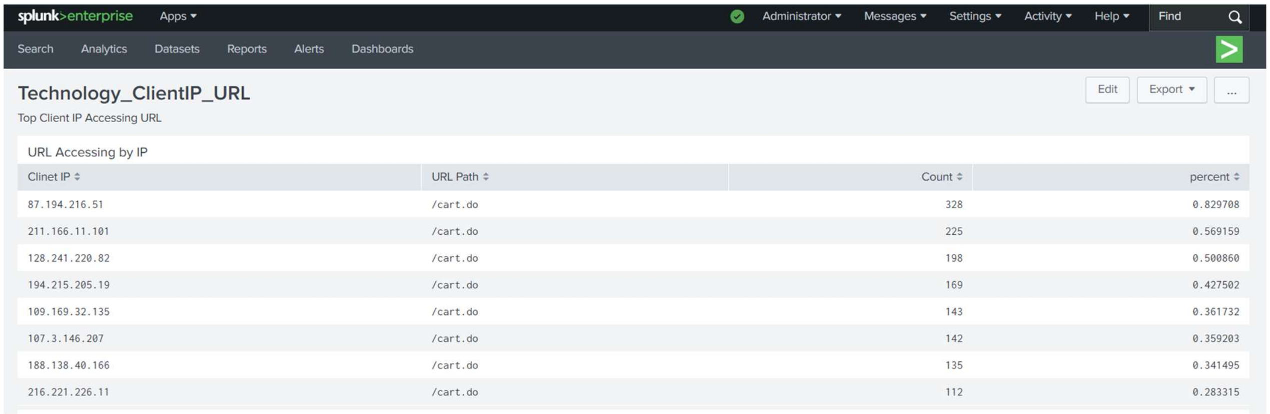


```
index="web" sourcetype="access_combined"
| top limit=10 clientip
| rename clientip as "Clinet IP Addresses",count as "Number of Times Accessed",percent as "percantage"
```

4,678 of 4,678 events matched

Visualization Dashboard

- **Description:** Presents a graphical view (e.g., bar graph or line chart) of the log data for visual analysis.
- **Purpose:** Makes log trends and peaks easy to spot visually.
- **Action:** Selects visualization options within Splunk and customizes fields for meaningful representation.
- **Insights:** Easily notice spikes, drops, or anomalies.



Technology_ClientIP_URL

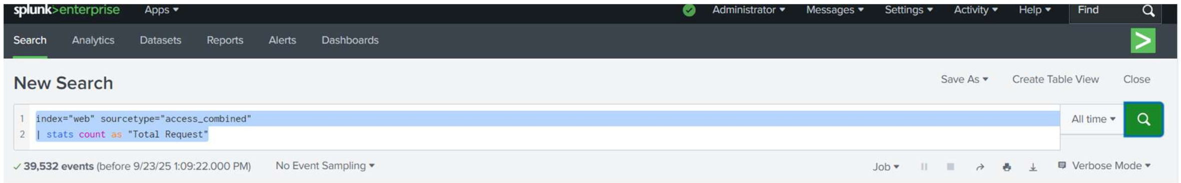
Top Client IP Accessing URL

URL Accessing by IP

Clinet IP	URL Path	Count	percent
87.194.216.51	/cart.do	328	0.829708
211.166.11.101	/cart.do	225	0.569159
128.241.220.82	/cart.do	198	0.500860
194.215.205.19	/cart.do	169	0.427502
109.169.32.135	/cart.do	143	0.361732
107.3.146.207	/cart.do	142	0.359203
188.138.40.166	/cart.do	135	0.341495
216.221.226.11	/cart.do	112	0.283315

Saving Searches and Reports

- **Description:** Shows how to save a search or report for future use, and possibly set up alerts.
- **Purpose:** Ensures reproducibility and continuous monitoring.
- **Action:** Leverages Splunk's save/report features for automation.
- **Insights:** Facilitates regular checks or instant notifications for key events.



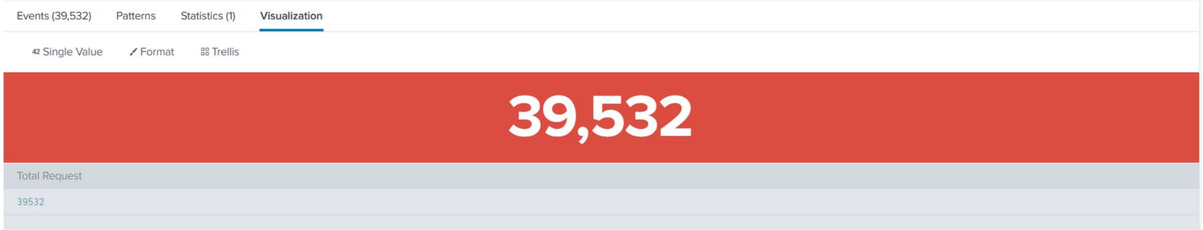
New Search

```
index="web" sourcetype="access_combined"
| stats count as "Total Request"
```

✓ **39,532 events** (before 9/23/25 1:09:22.000 PM)

Full Dashboard Overview

- **Description:** Displays the final dashboard combining multiple panels—each tracking a separate metric or log source.
- **Purpose:** Provides a holistic view for ongoing monitoring or executive reporting.
- **Action:** Customizes dashboard layout for maximum clarity and operational value.
- **Insights:** Centralizes key metrics for efficient oversight.



39,532

Total Request
39532