Splunk Dashboard for Web Traffic Logs Project

By Gaurav Ghandat

1. Objective

The objective of this lab is to design and implement a **Splunk Dashboard for Web Traffic Logs** that provides a clear, visual, and actionable summary of web server activity. Using Apache web access logs in JSON format, the dashboard helps analyze:

- Overall web traffic volume
- Success and error responses
- Popular URIs and client IPs
- Geographic distribution of web traffic

This dashboard is useful for **web monitoring, security analysis, troubleshooting, and performance optimization**.

---

2. Lab Environment Setup

2.1 Tools & Platform

- **Splunk Enterprise**
- Web browser (Chrome / Firefox recommended)
- Sample dataset: apache_logs.json

2.2 Data Source

- **Source**: apache_logs.json
- **Host**: webserver
- **Sourcetype**: _json

The dataset contains typical Apache web access fields such as:

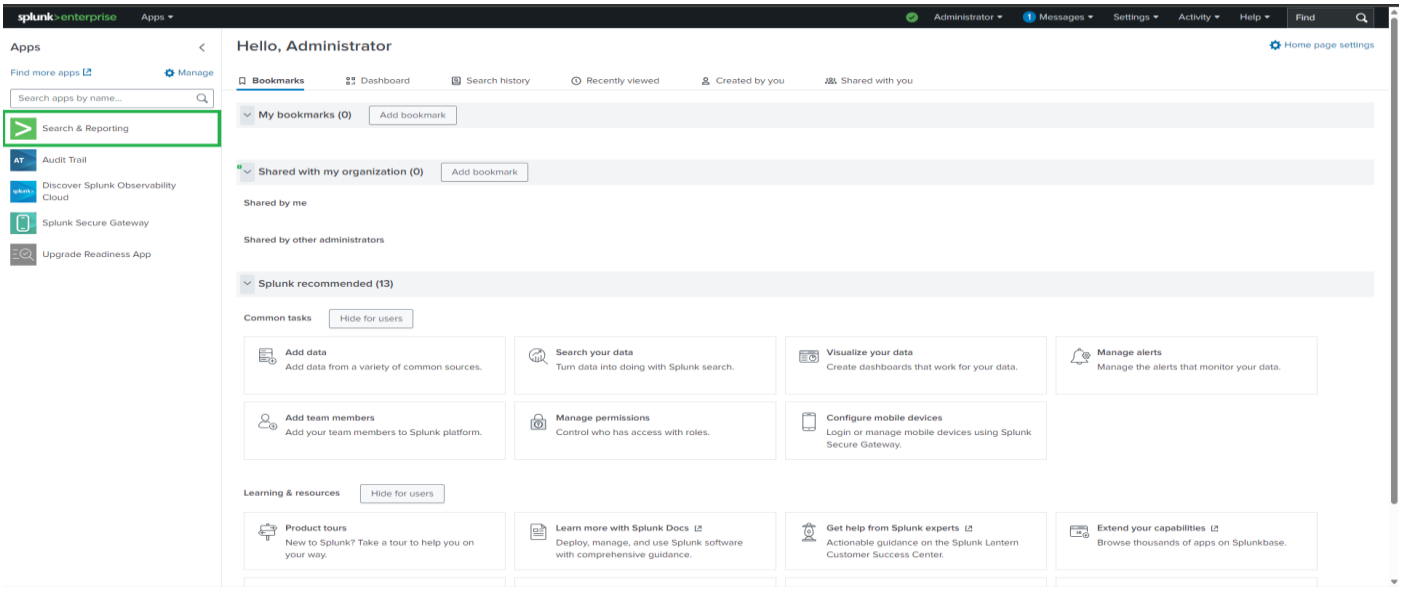
- ip
- method
- uri
- status
- host
- _time

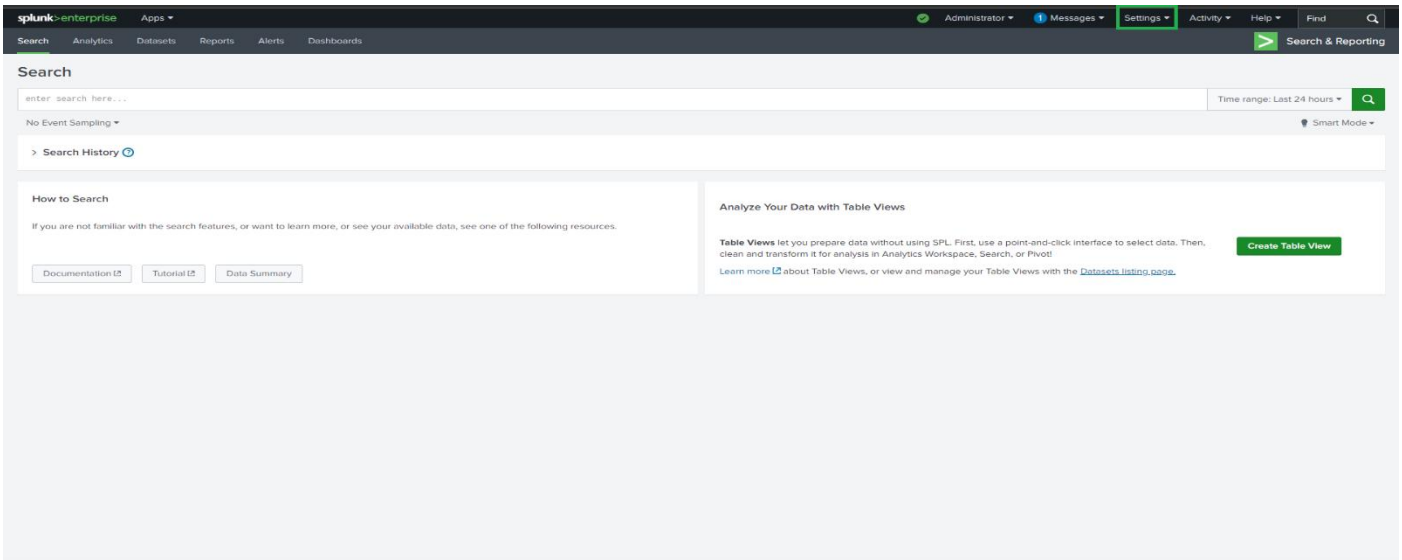
---

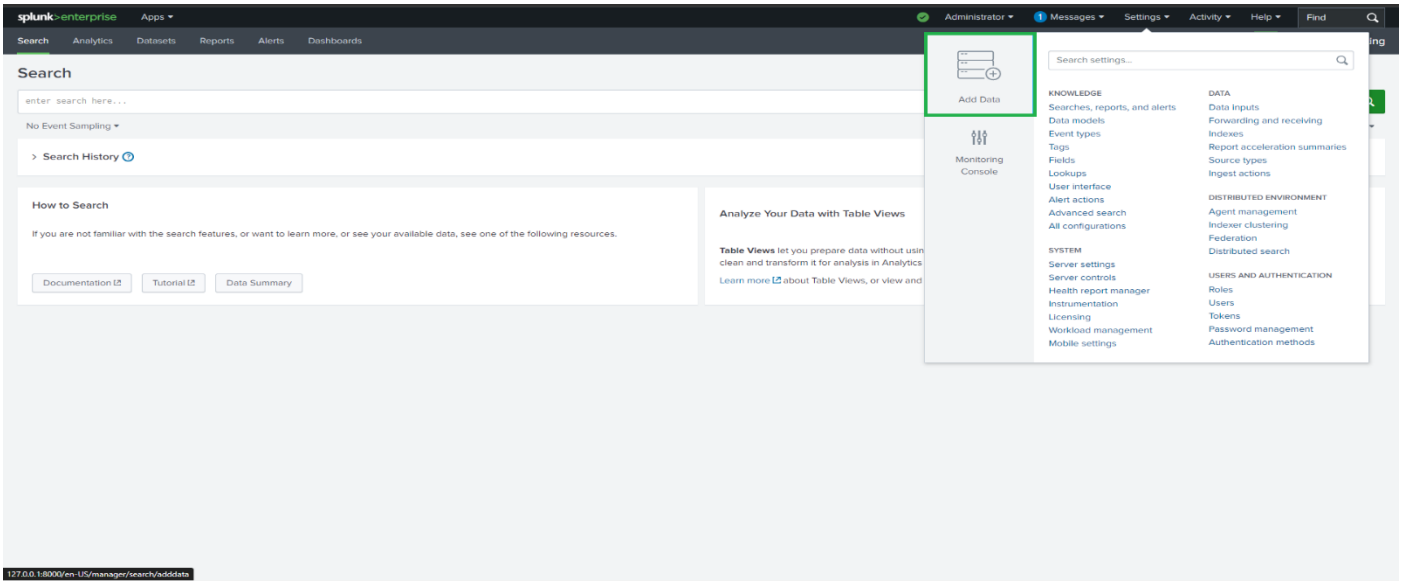
3. Data Ingestion into Splunk

Steps to Upload Data

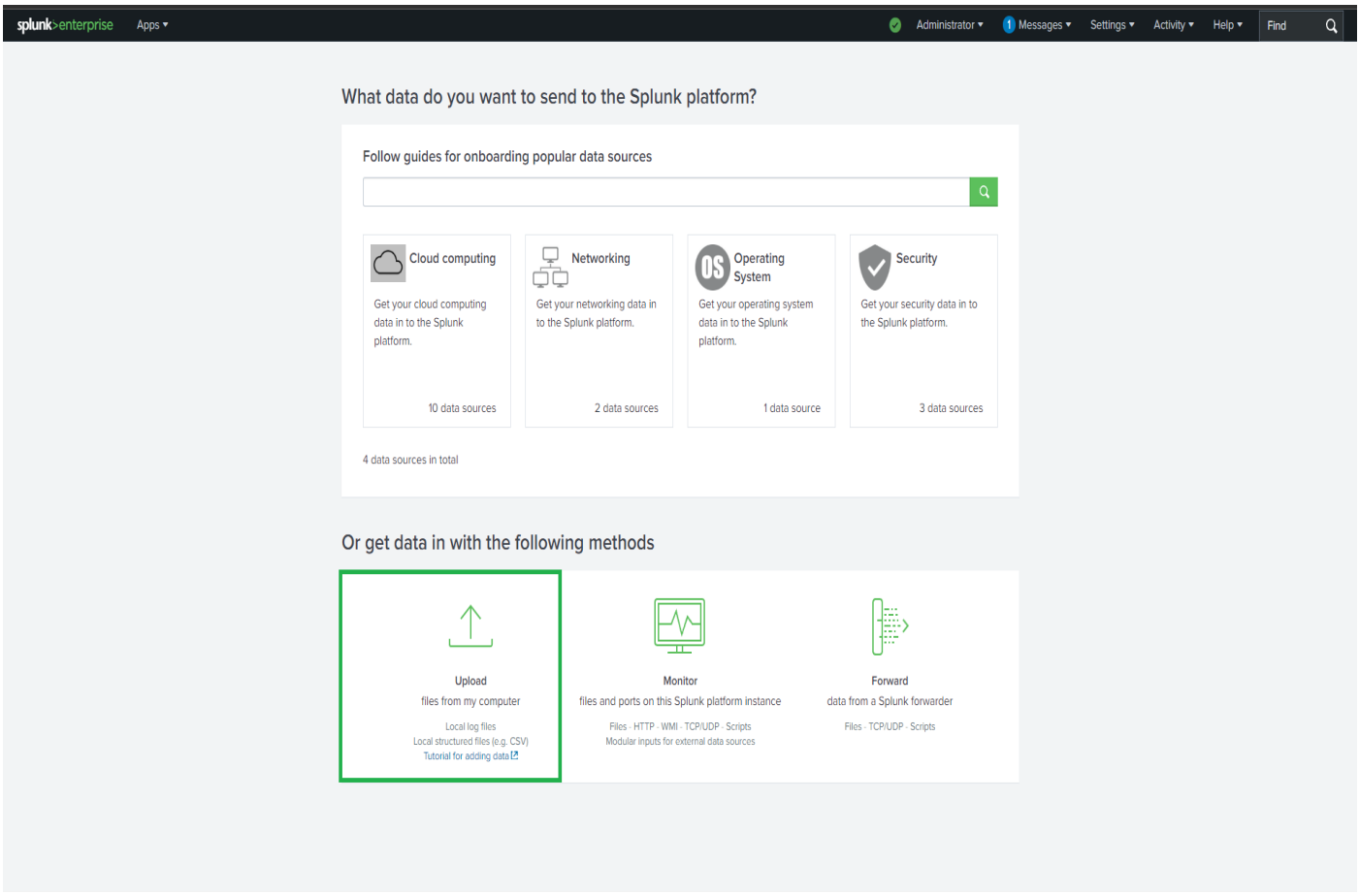
1. Login to Splunk as **Administrator**.
2. Navigate to **Settings → Add Data**.

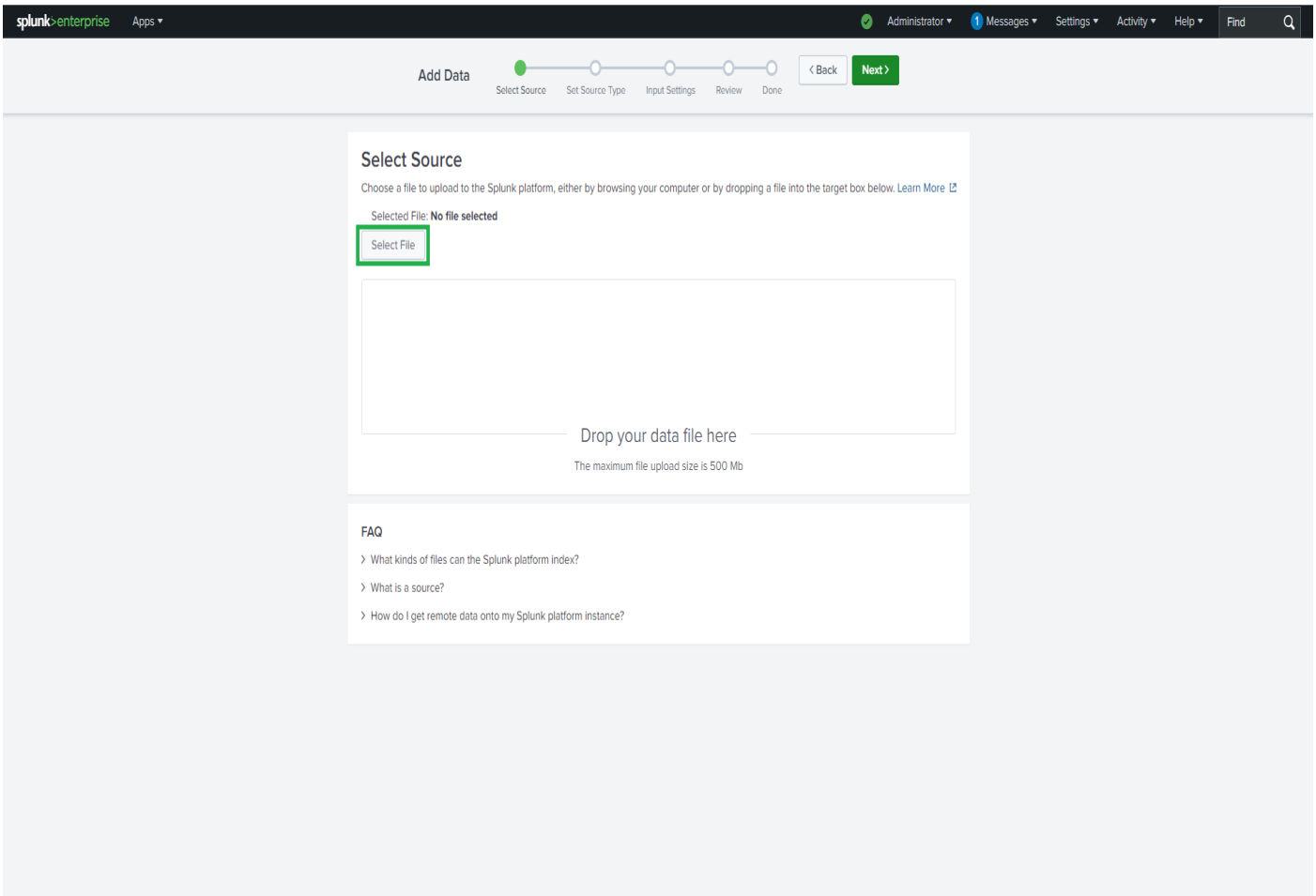




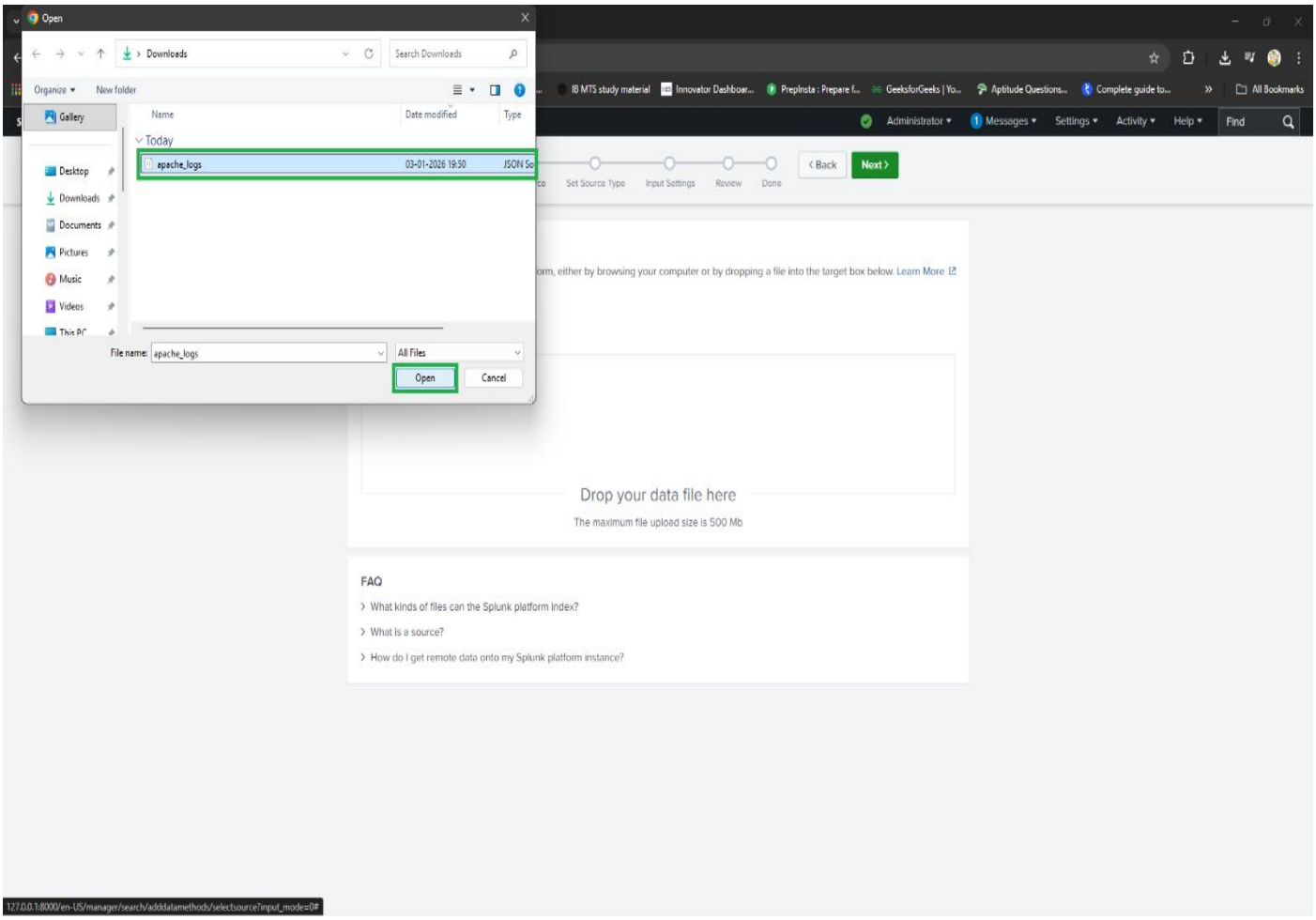


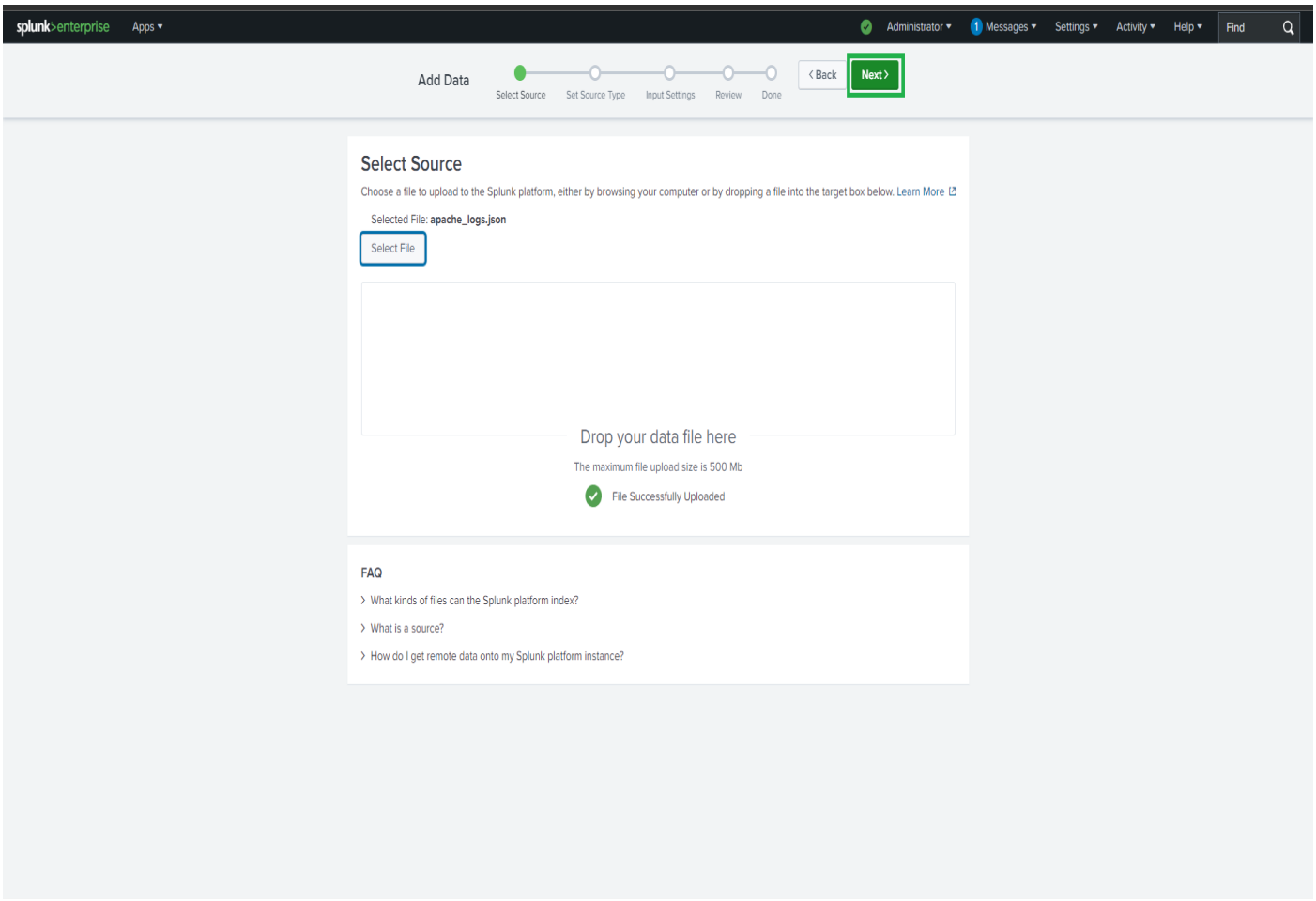
3. Select **Upload** as the data input method.



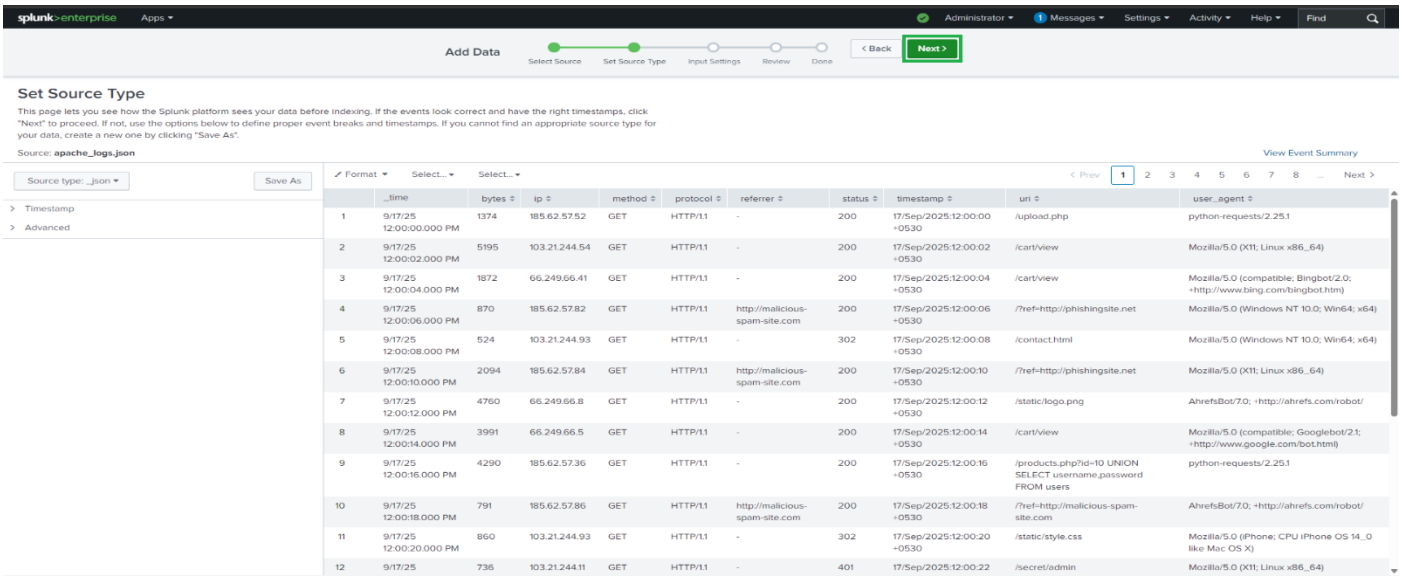


4. Upload the file apache_logs.json.

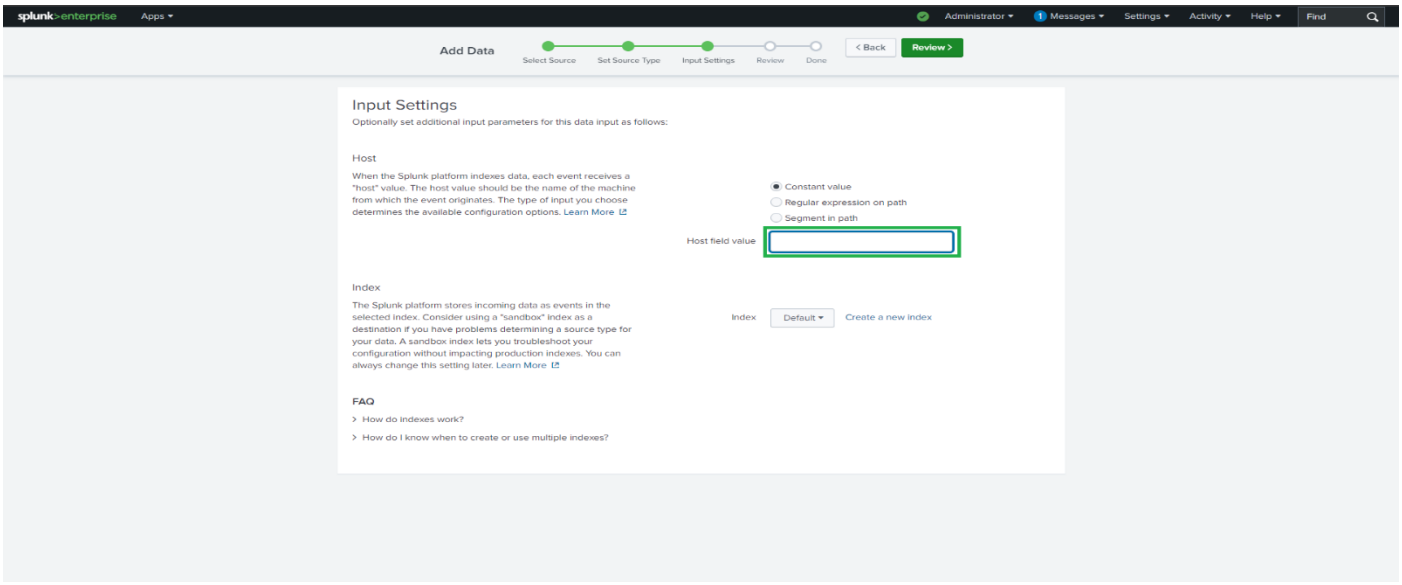


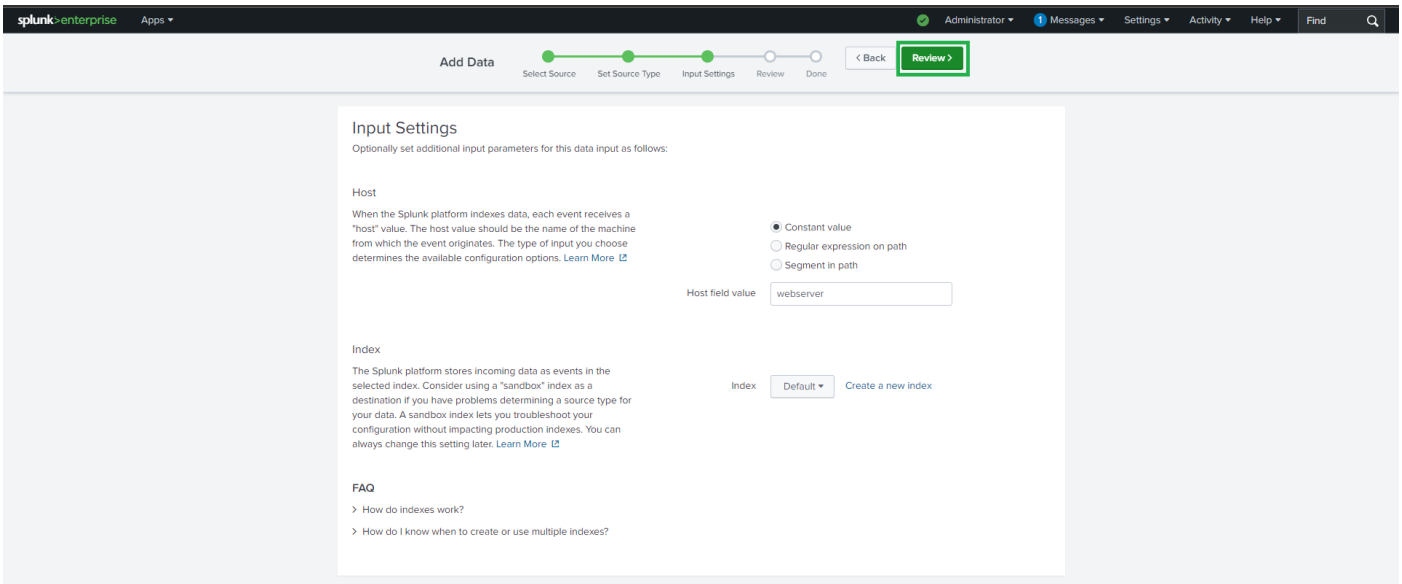


5. Set the **Source Type** to _json.

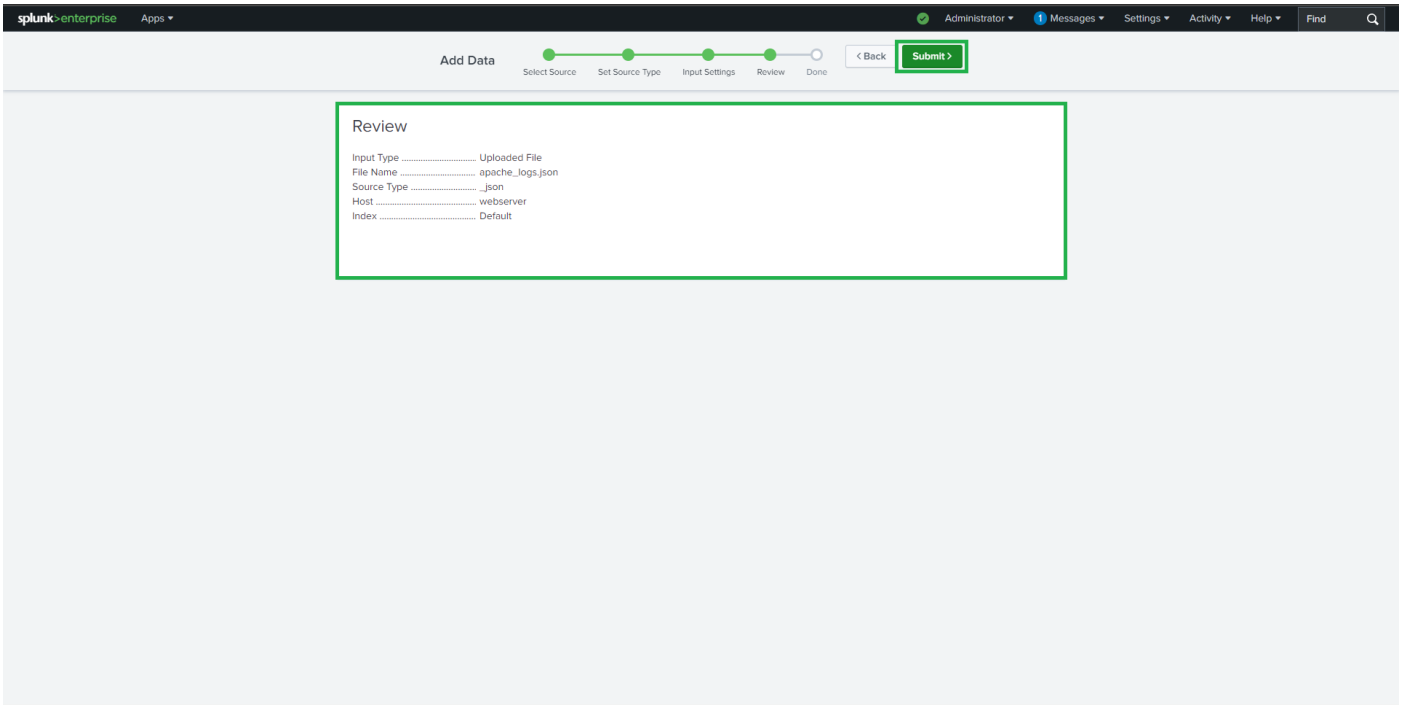


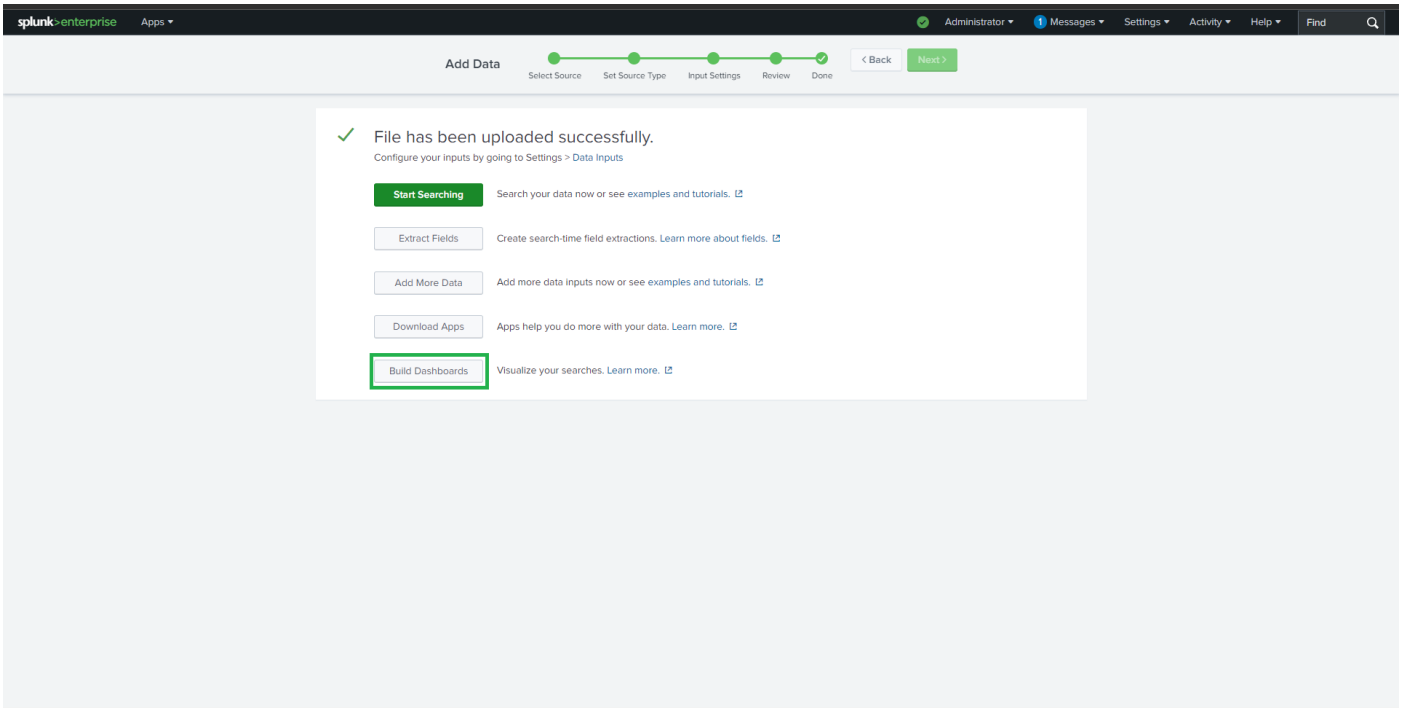
6. Assign **Host = webserver**.





7. Review settings and submit the data.
8. Verify ingestion using a basic search:
9. source="apache_logs.json"

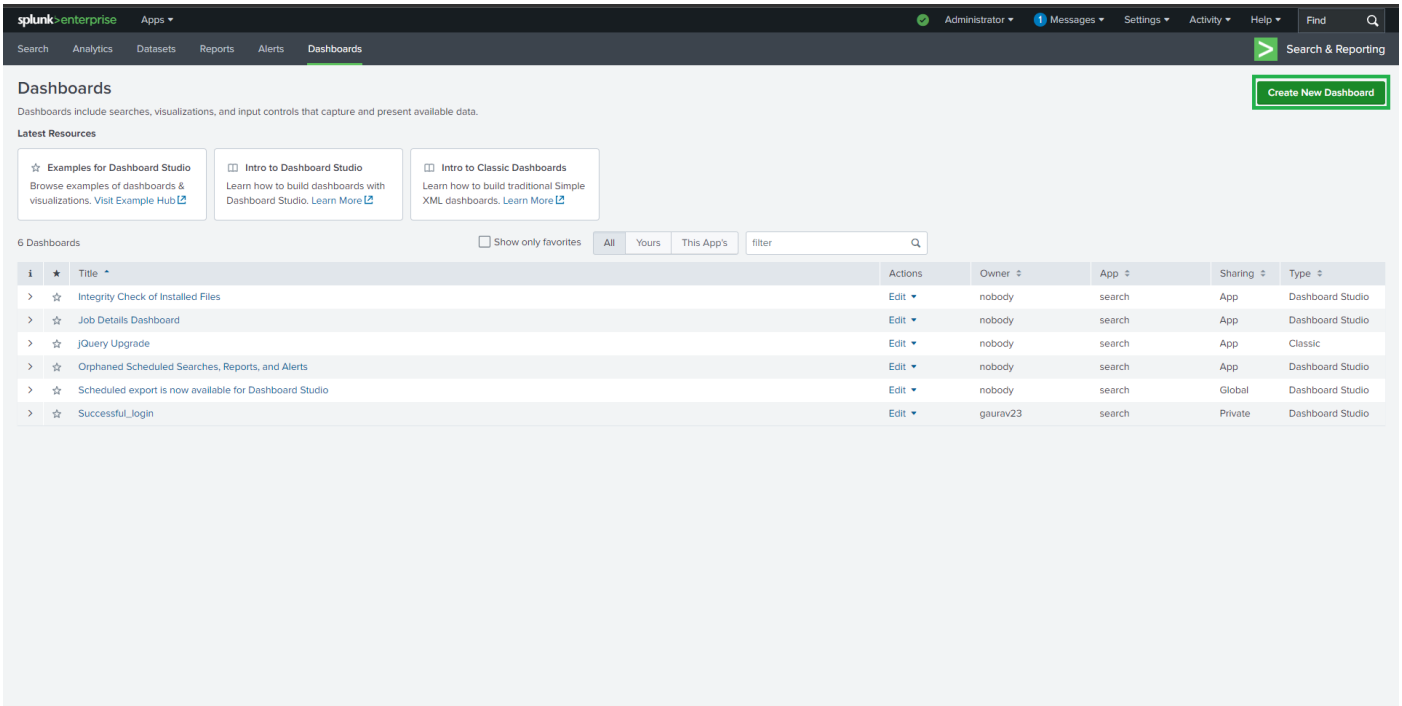


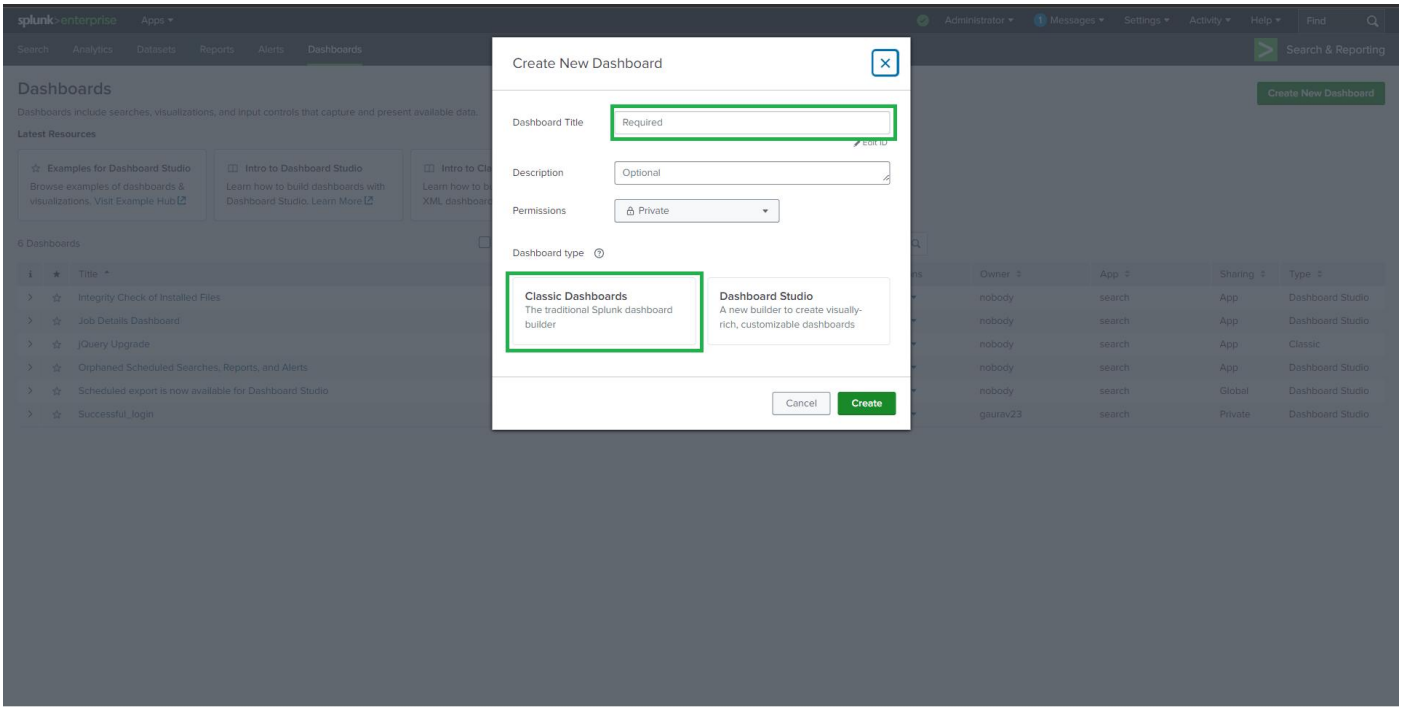


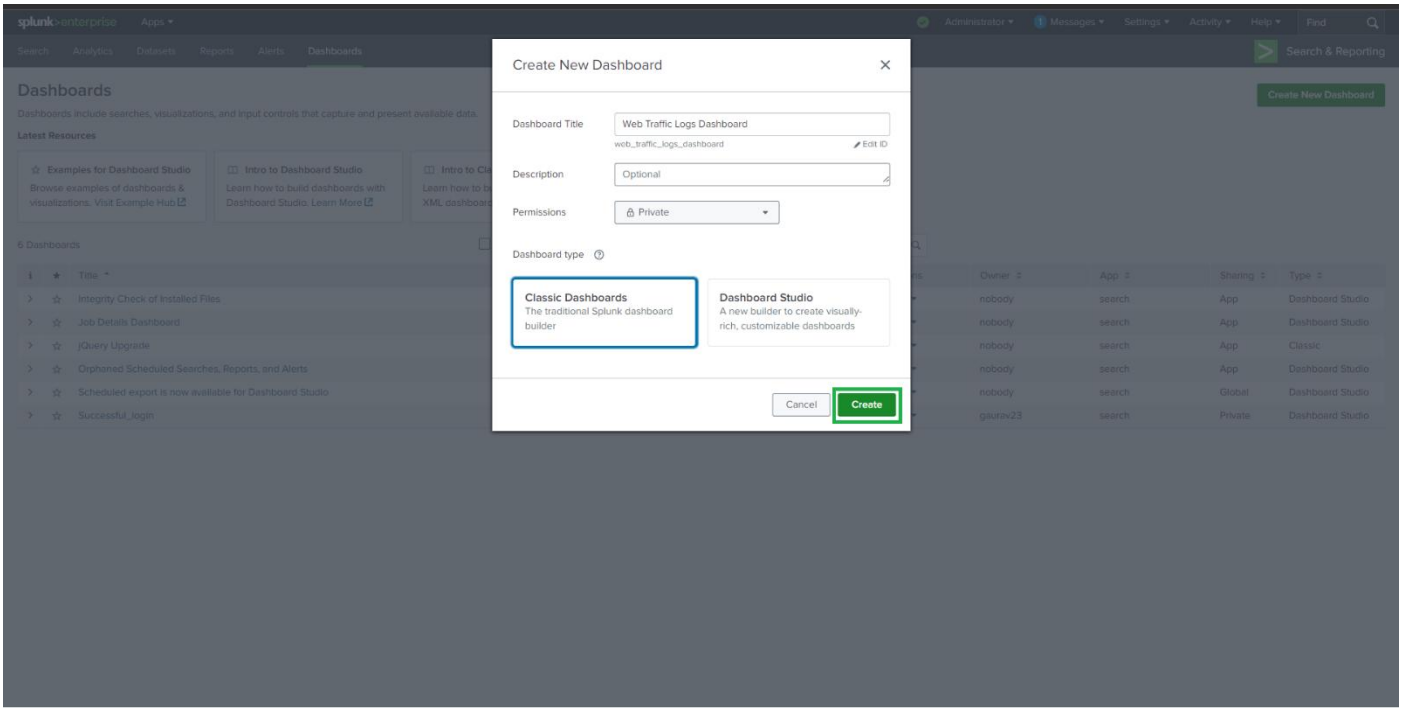
4. Dashboard Creation

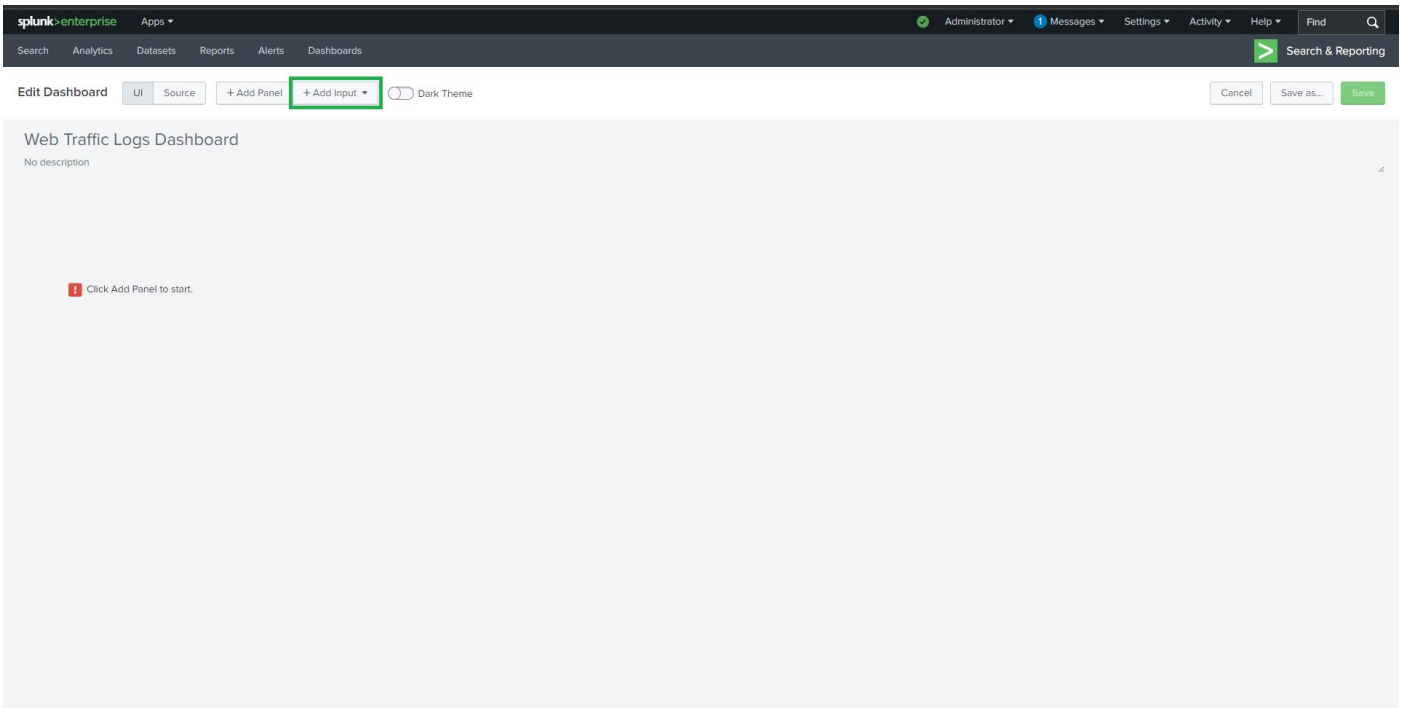
4.1 Create a New Dashboard

1. Go to **Dashboards → Create New Dashboard**.
2. Dashboard Title: **Web Traffic Logs Dashboard**
3. Dashboard Type: **Classic Dashboard**
4. Permissions: Private (can be changed later)






Create New Dashboard
Dashboard Title
Web Traffic Logs Dashboard
web_traffic_logs_dashboard
Edit ID
Description
Optional
Permissions
Private
Dashboard type
Classic Dashboards
The traditional Splunk dashboard builder
Dashboard Studio
A new builder to create visually-rich, customizable dashboards
Cancel
Create


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Click Add Panel to start.

5. Task 0: Setting Up Time Range Input

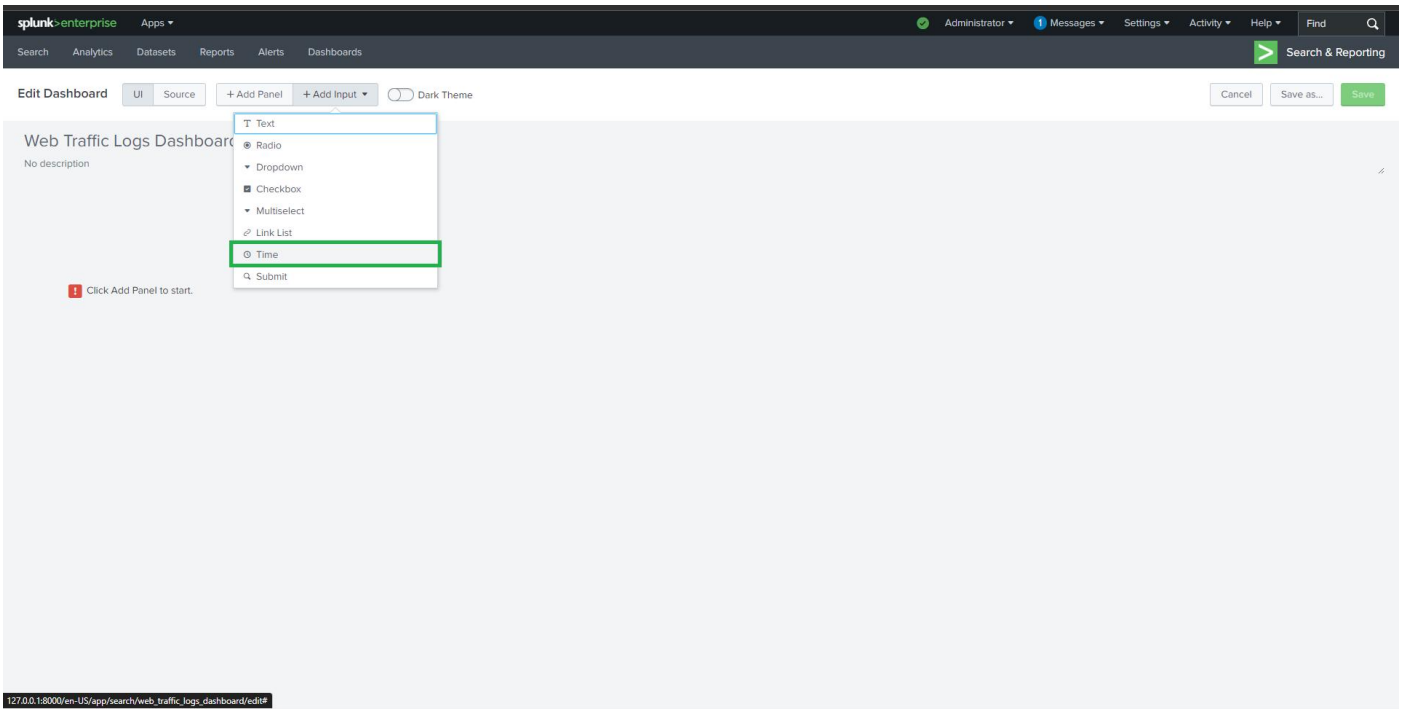
Purpose

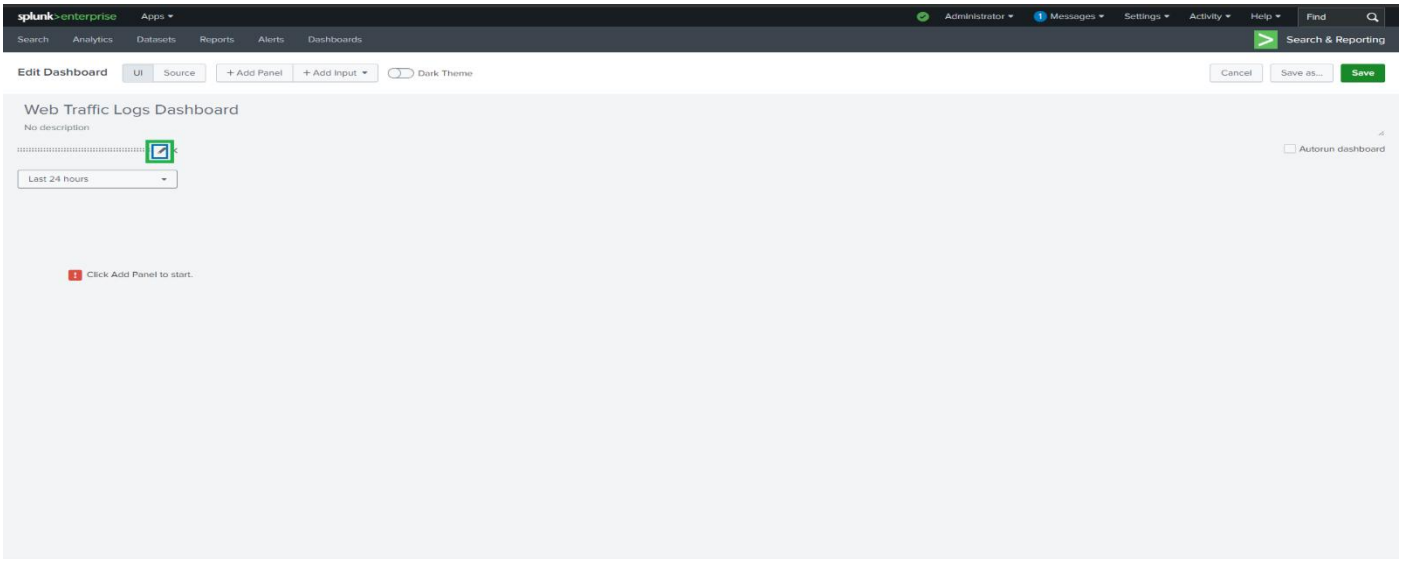
To ensure consistency across all panels by using a **shared time picker**.

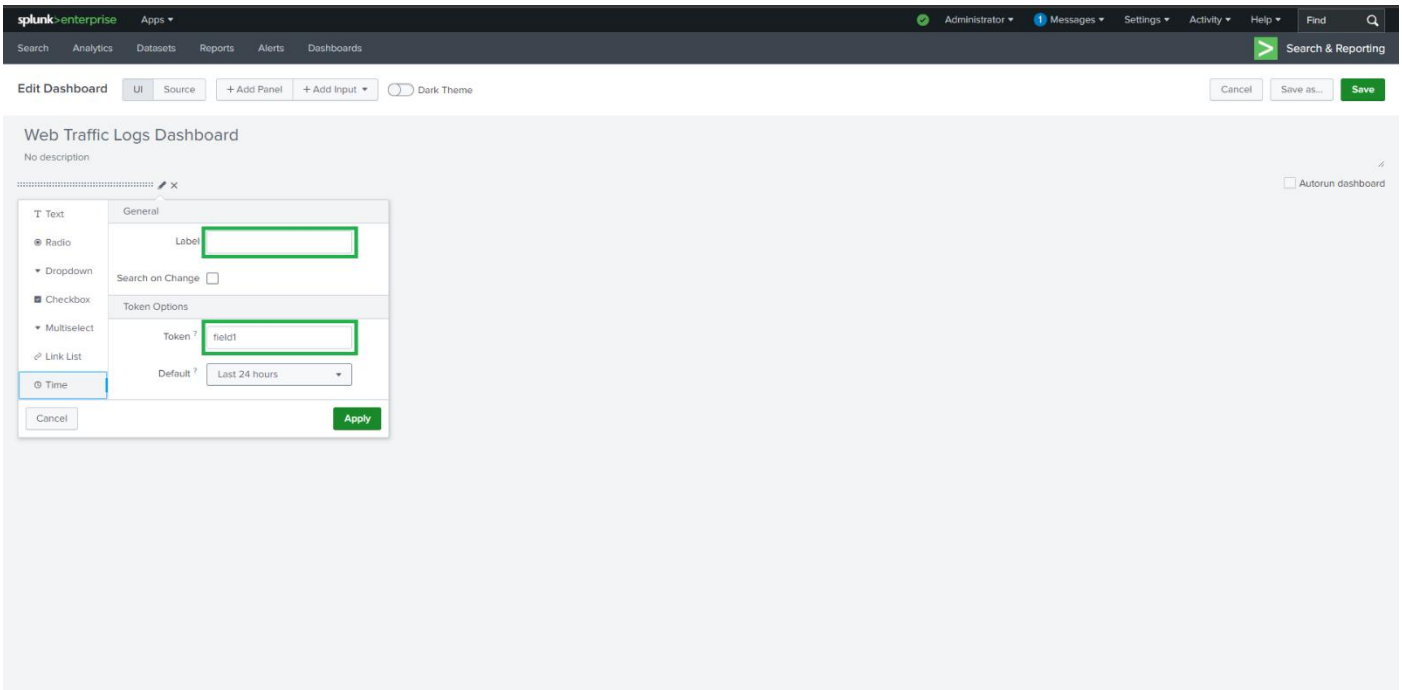
Steps

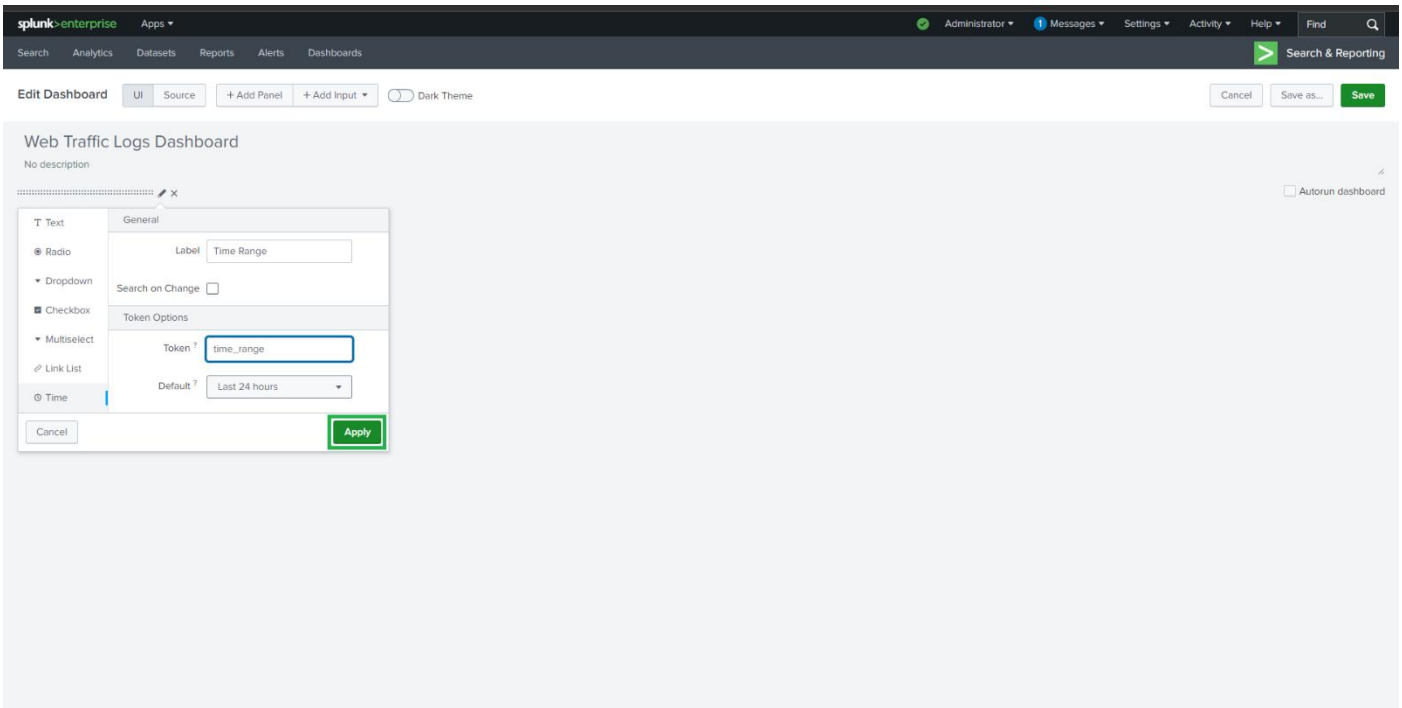
1. Open the dashboard in **Edit Mode**.
2. Click **Add Input → Time**.
3. Click the **pencil icon** to configure.
4. Set:
    - **Label**: Time Range
    - **Token**: time_range
5. Add another input:
    - **Add Input → Submit**

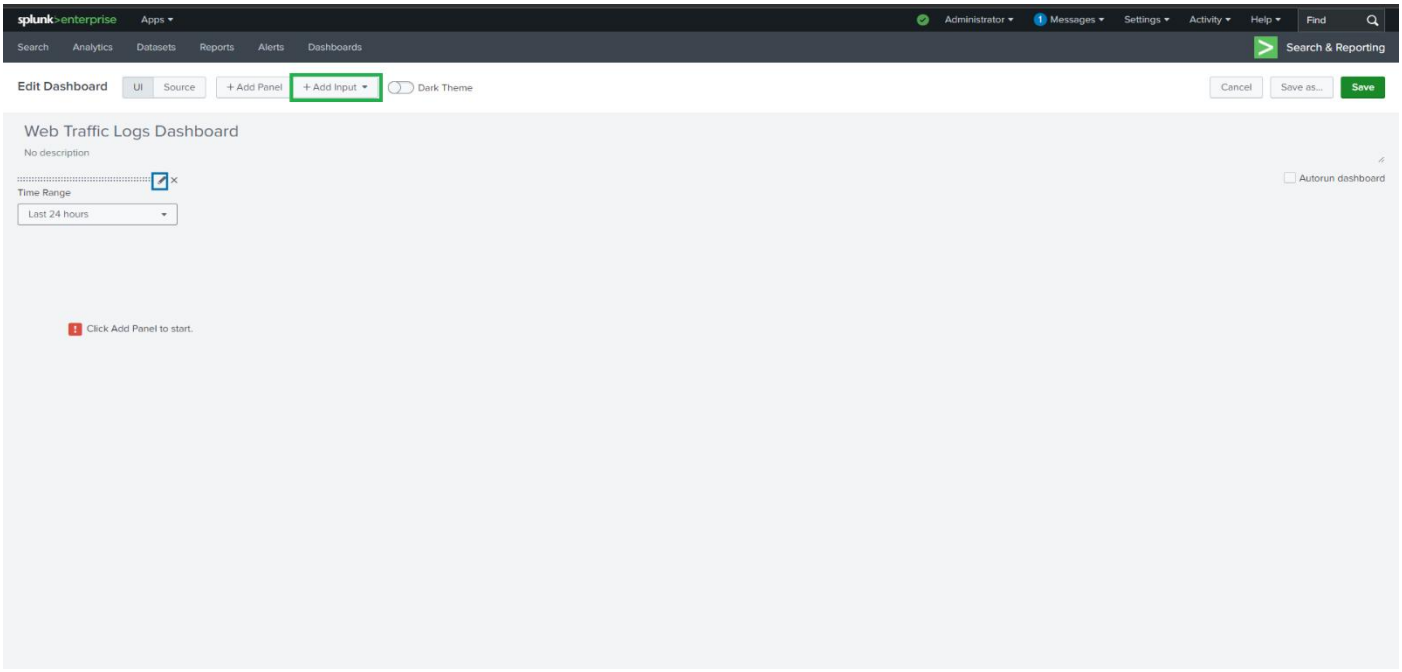
⚠️ Note: For all panels, select **Shared Time Picker → time_range**.

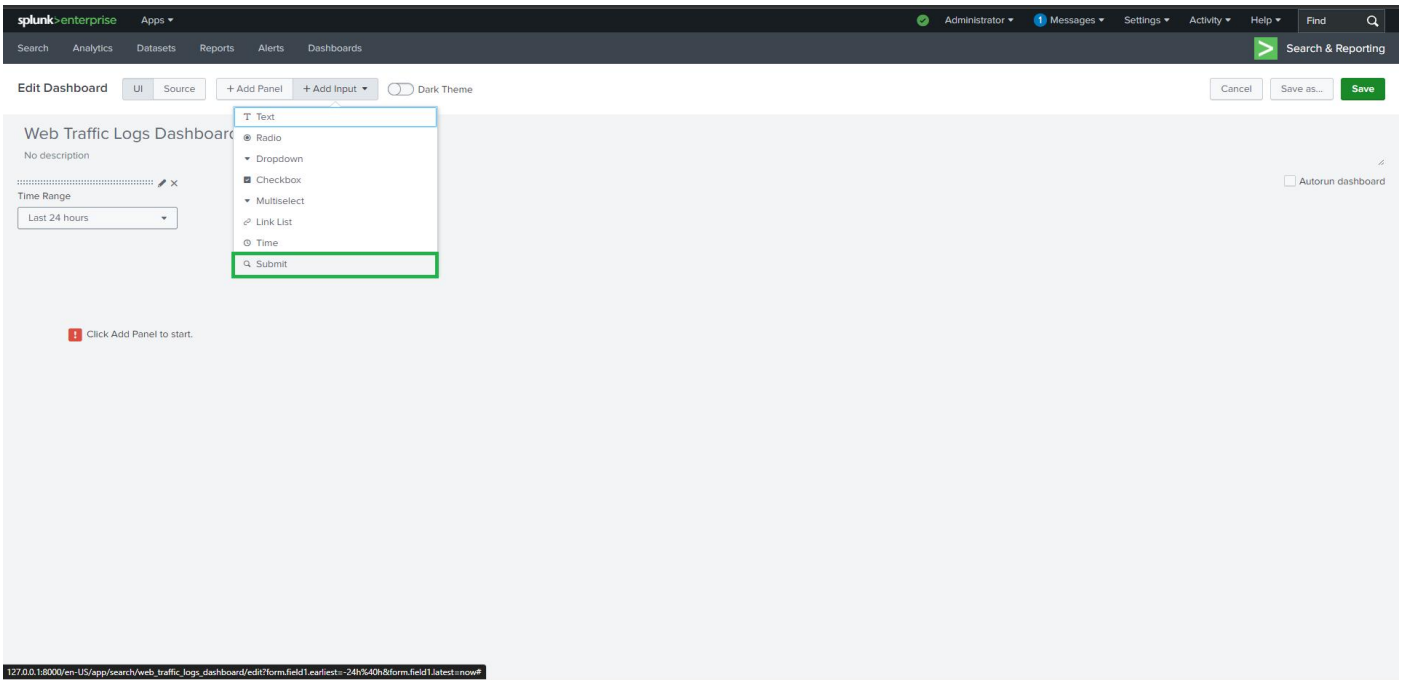


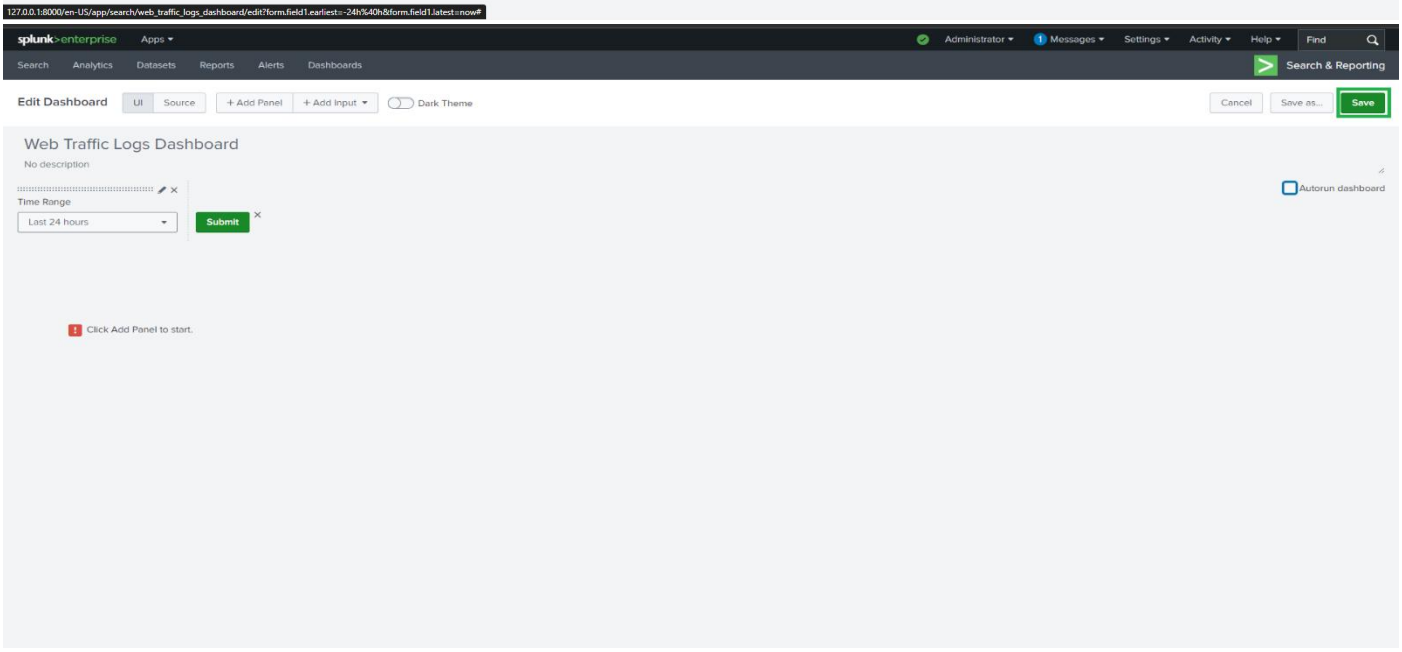

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Last 24 hours
Click Add Panel to start.


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Text
Radio
Dropdown
Checkbox
Multiselect
Link List
Time
General
Label
Search on Change
Token Options
Token
field1
Default
Last 24 hours
Cancel
Apply


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Text
Radio
Dropdown
Checkbox
Multiselect
Link List
Time
General
Label
Time Range
Search on Change
Token Options
Token
time_range
Default
Last 24 hours
Cancel
Apply


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Time Range
Last 24 hours
Autorun dashboard
Click Add Panel to start.


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Text
Radio
Dropdown
Checkbox
Multiselect
Link List
Time
Submit
Web Traffic Logs Dashboard
No description
Time Range
Last 24 hours
Autorun dashboard
Click Add Panel to start.


127.0.0.1:8000/en-US/app/search/web_traffic_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now#
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Time Range
Last 24 hours
Submit
Autorun dashboard
Click Add Panel to start.

6. Task 1: Web Activities Panels

6.1 Total Web Requests

Visualization: Single Value

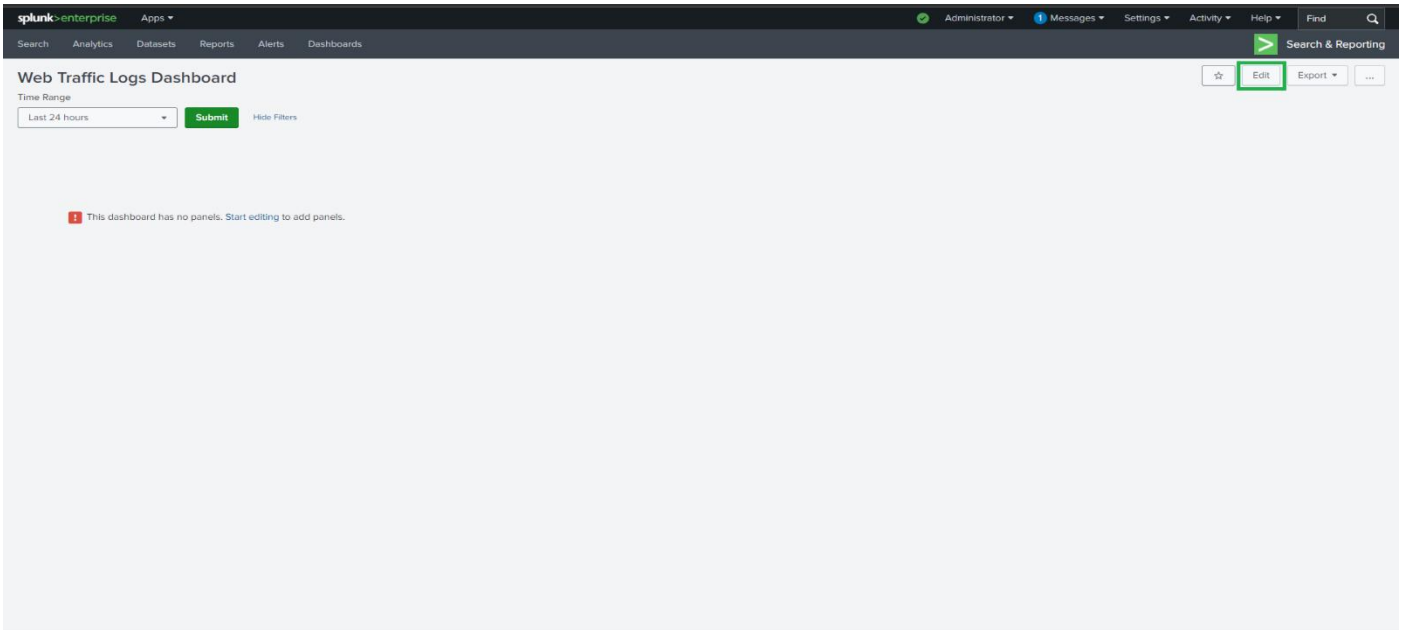
Title: Total Web Requests

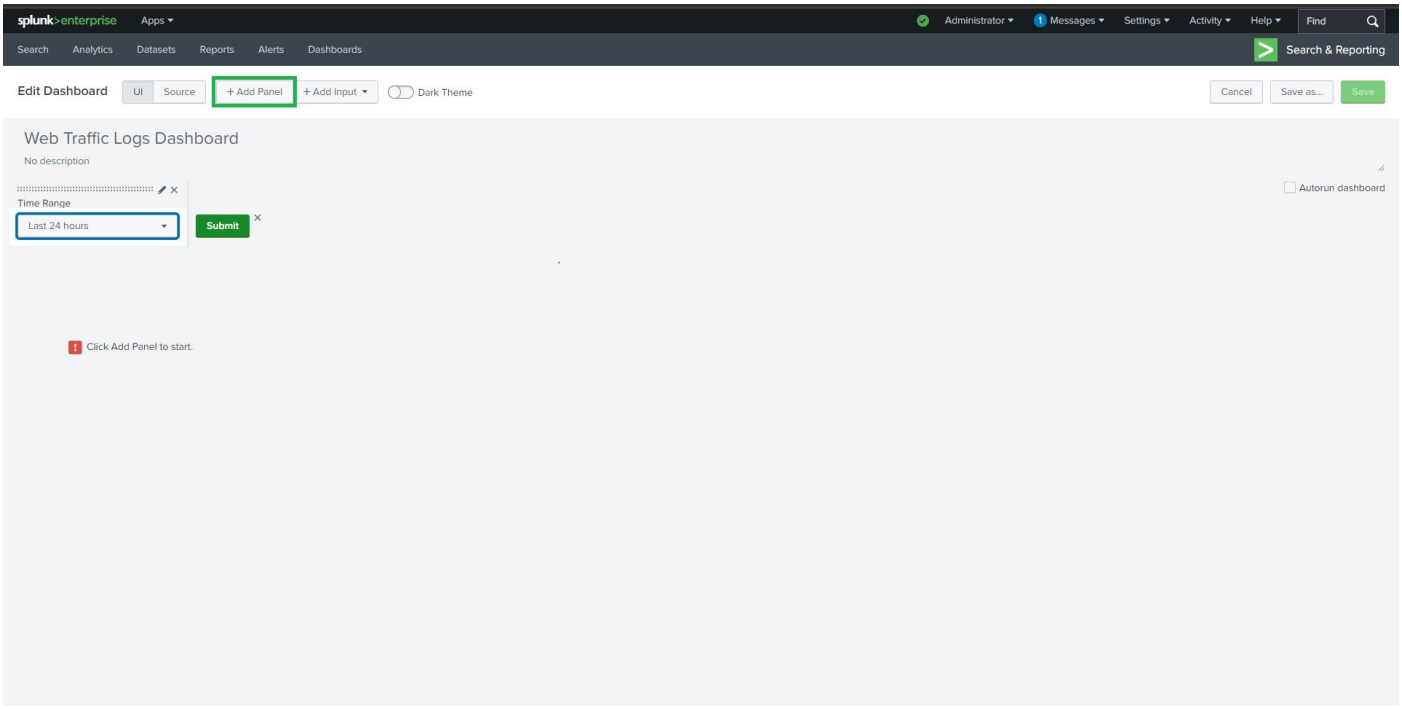
Search Query:

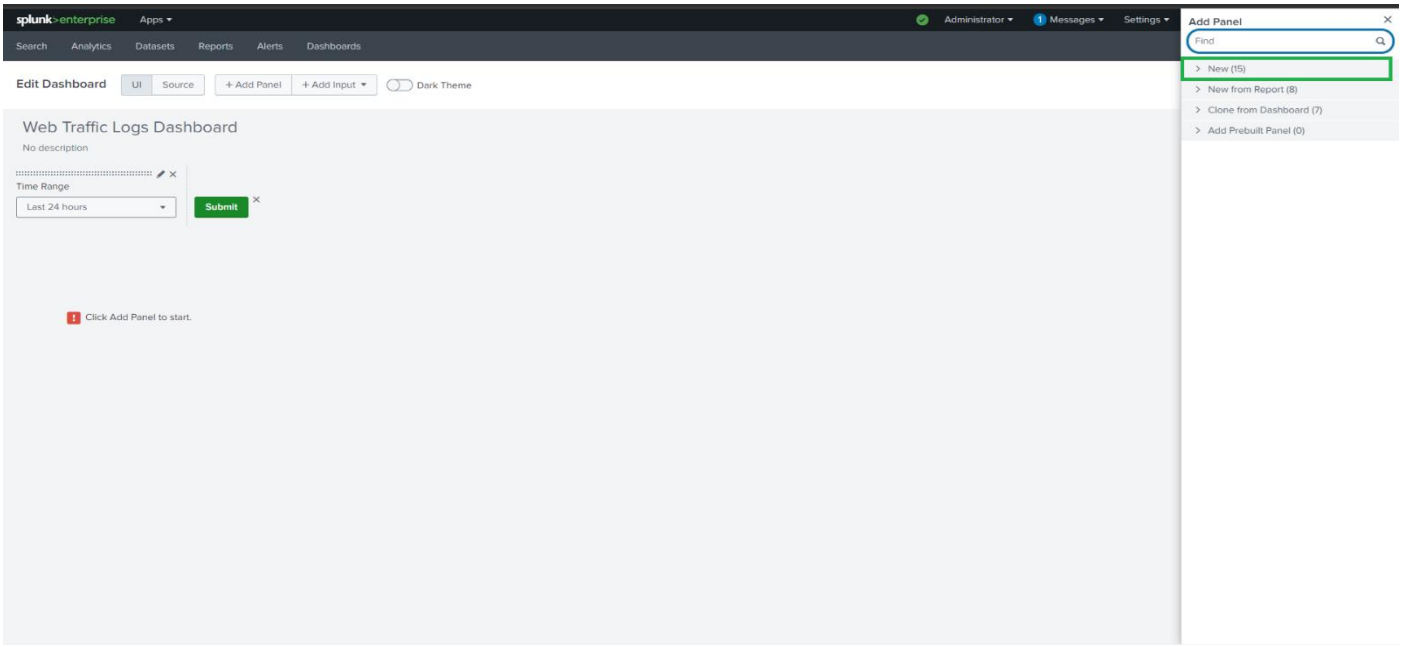
source="apache_logs.json" host="webserver" sourcetype="_json"

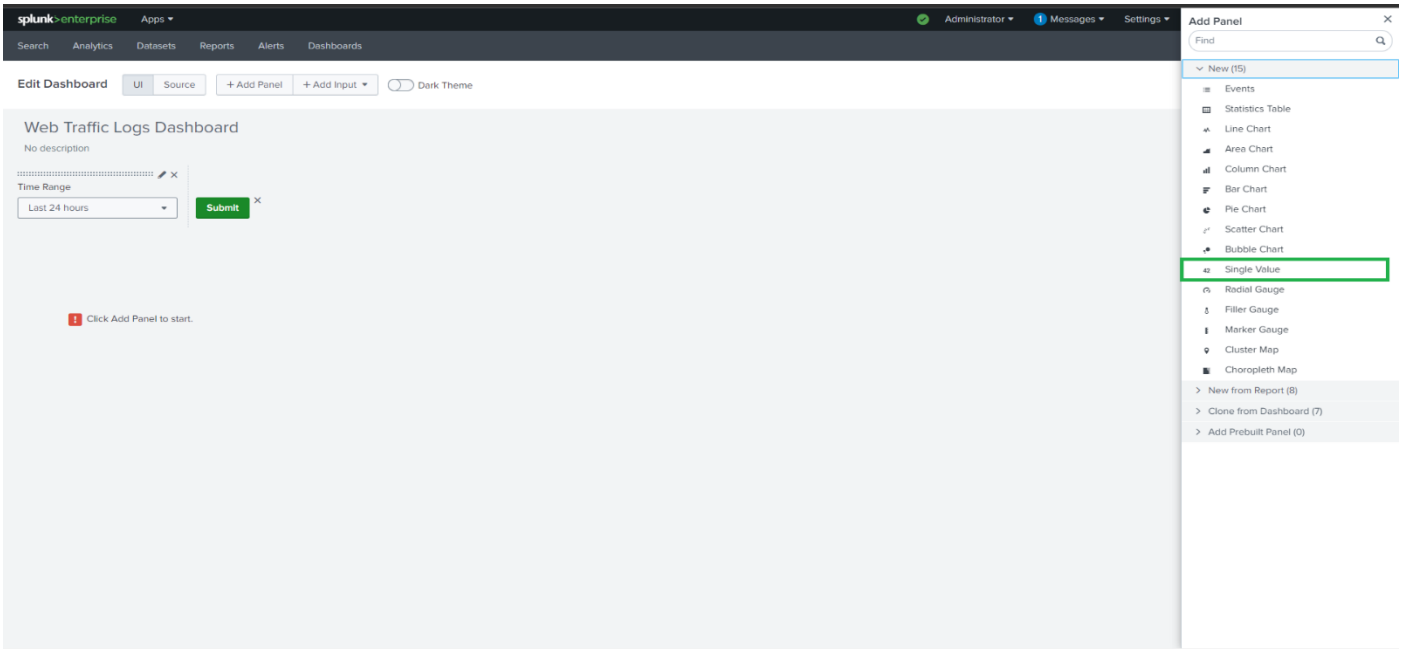
| stats count AS "Total Web Requests"

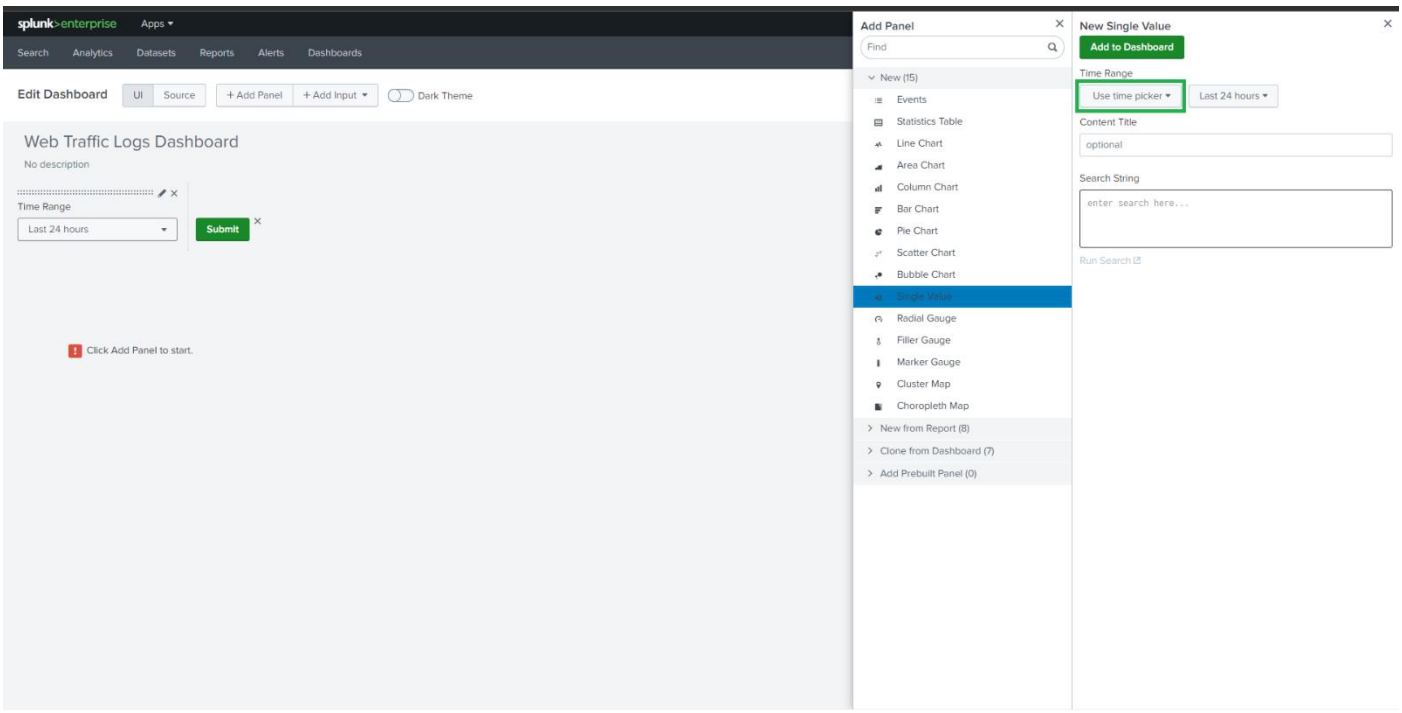
Purpose: Displays the total number of HTTP requests received.

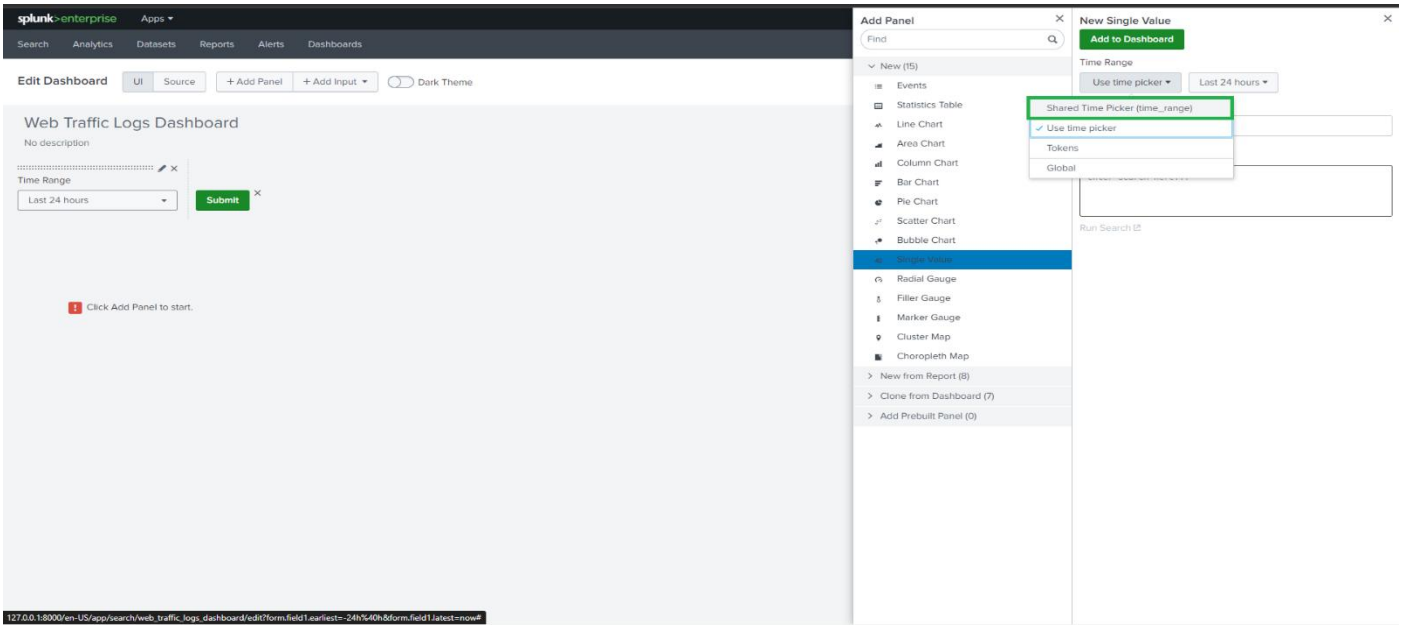


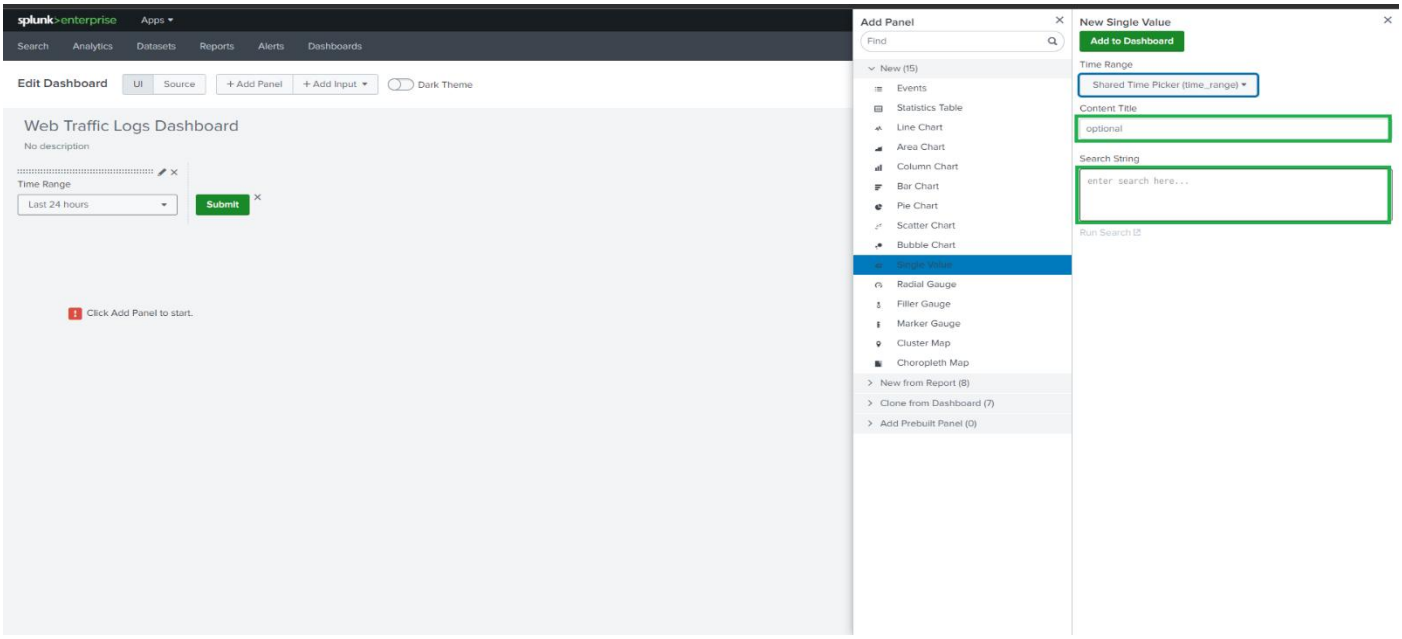


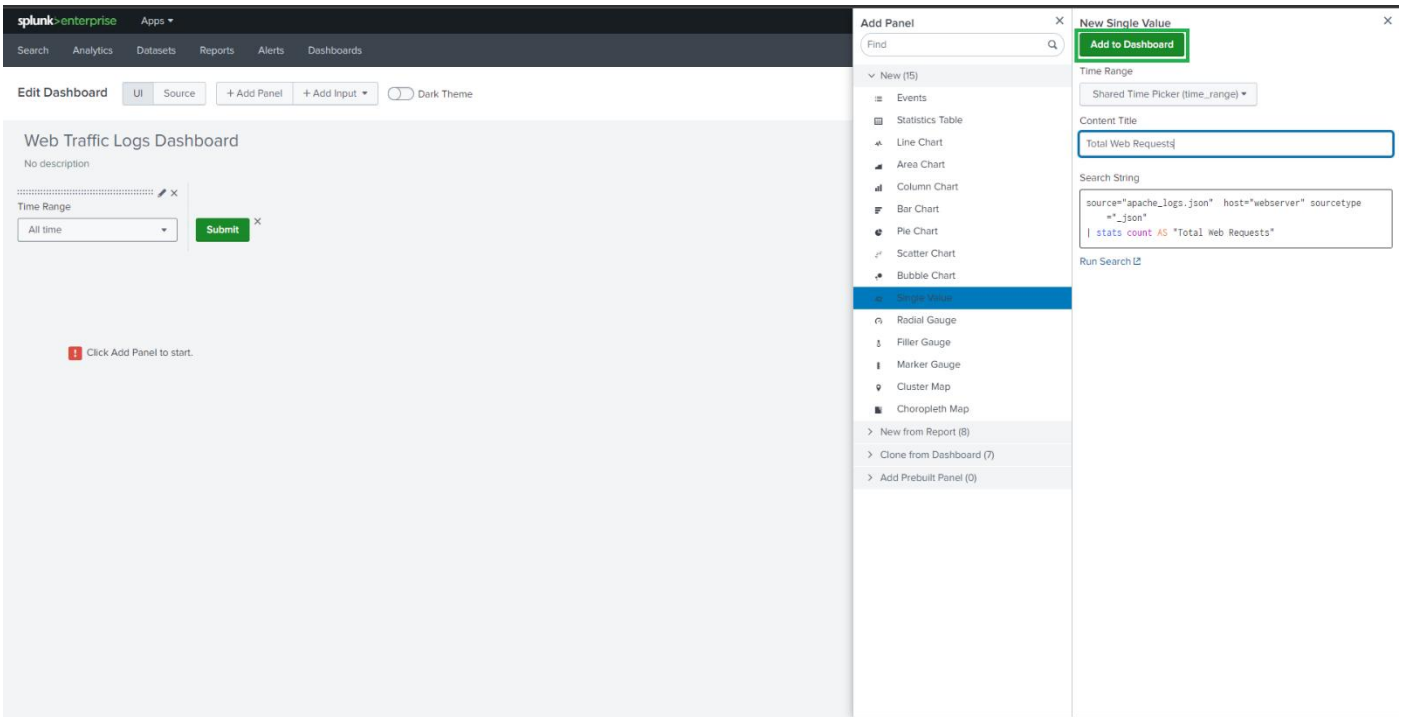

splunk>enterprise
Apps
Administrator
Messages
Settings
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Web Traffic Logs Dashboard
No description
Time Range
Last 24 hours
Submit
Click Add Panel to start.
Add Panel
Find
New (15)
New from Report (8)
Clone from Dashboard (7)
Add Prebuilt Panel (0)

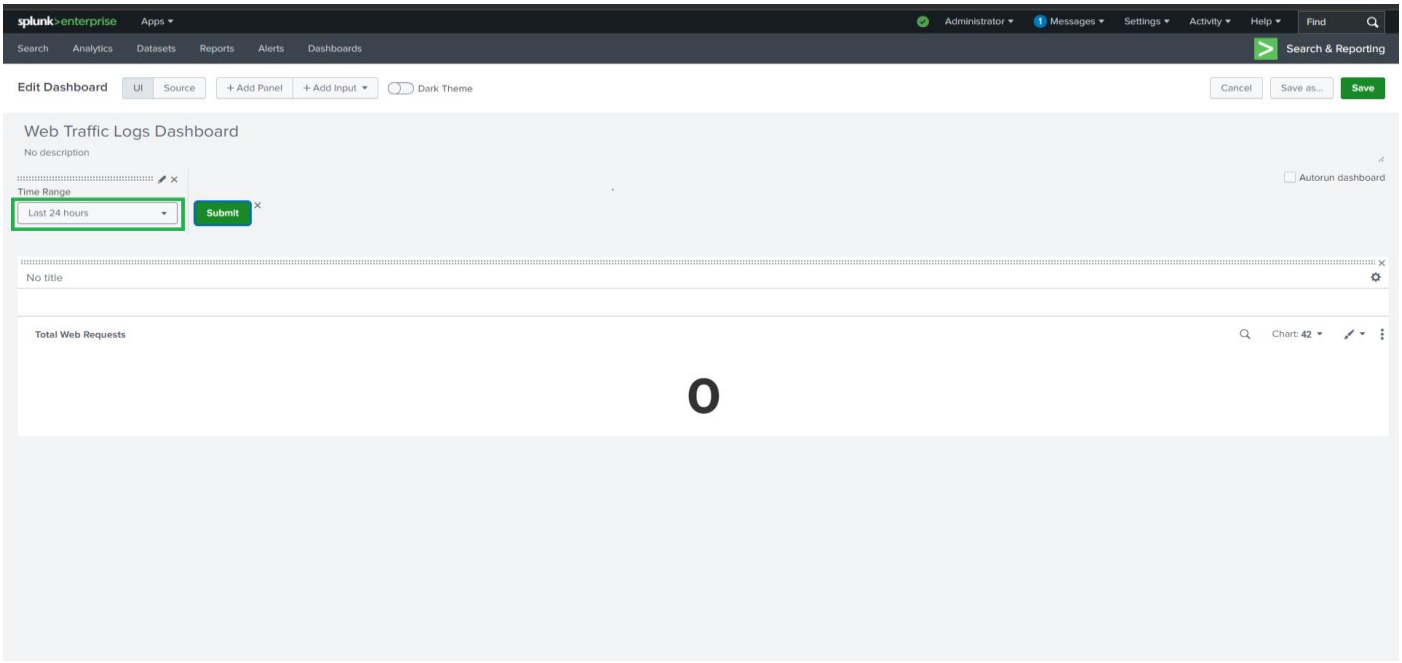

splunk>enterprise
Apps
Administrator
Messages
Settings
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Web Traffic Logs Dashboard
No description
Time Range
Last 24 hours
Submit
Click Add Panel to start.
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (7)
Add Prebuilt Panel (0)

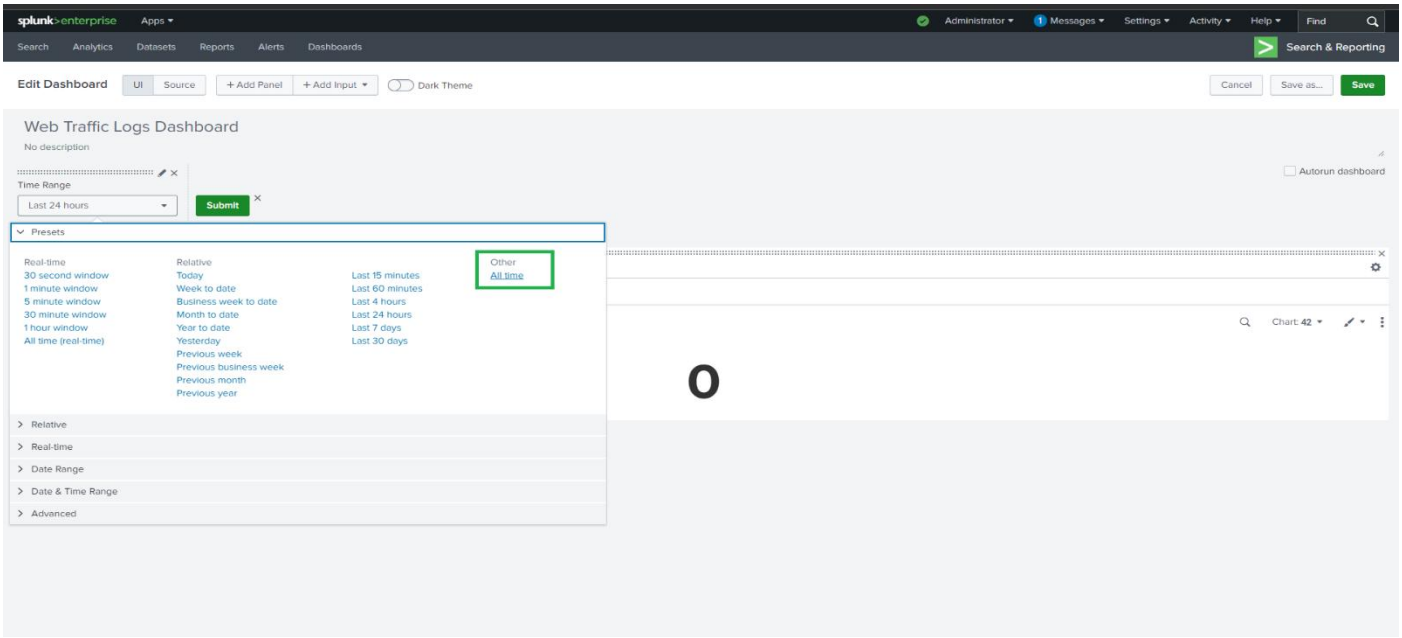

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Web Traffic Logs Dashboard
No description
Time Range
Last 24 hours
Submit
Click Add Panel to start.
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (7)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Use time picker
Last 24 hours
Content Title
optional
Search String
enter search here...
Run Search

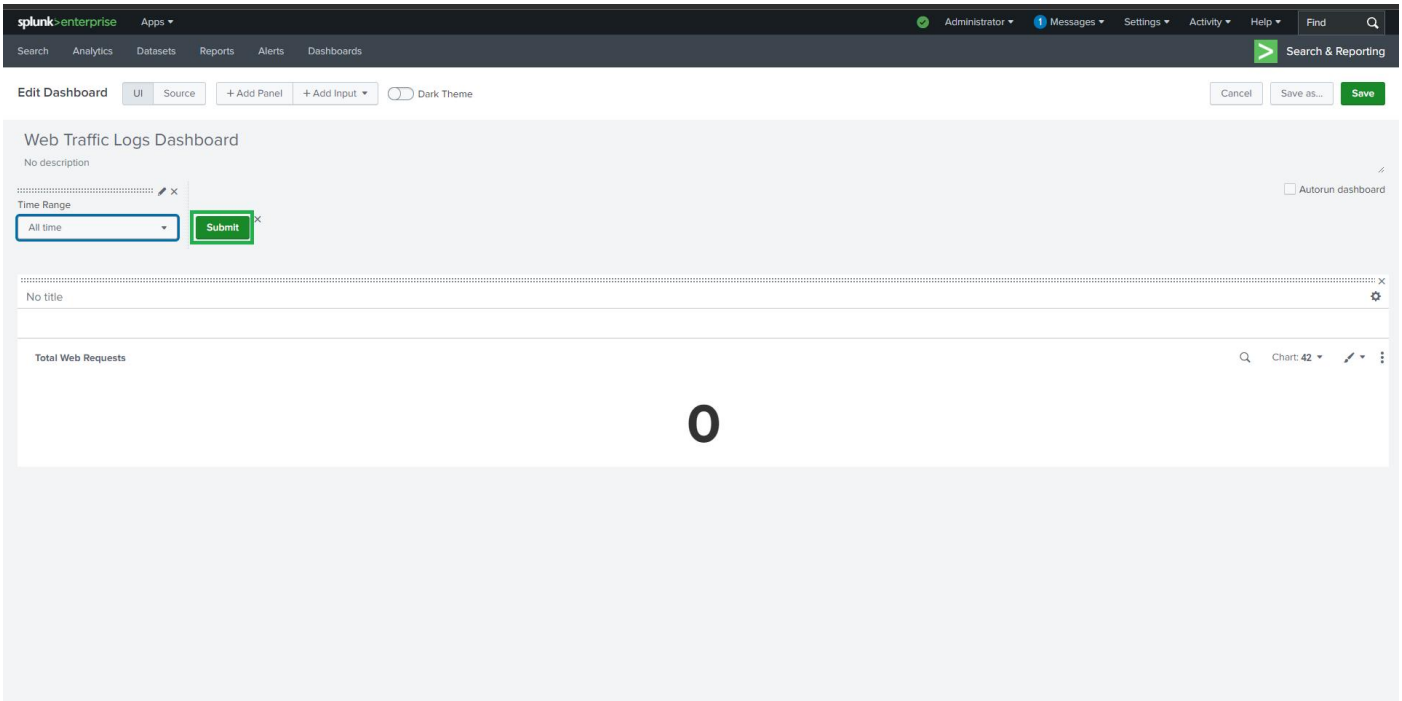

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Web Traffic Logs Dashboard
No description
Time Range
Last 24 hours
Submit
Click Add Panel to start.
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (7)
Add Prebuilt Panel (0)
Shared Time Picker (time_range)
Use time picker
Tokens
Global
New Single Value
Add to Dashboard
Time Range
Use time picker
Last 24 hours
Run Search
127.0.0.1:8000/en-US/app/search/web_traffic_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now#

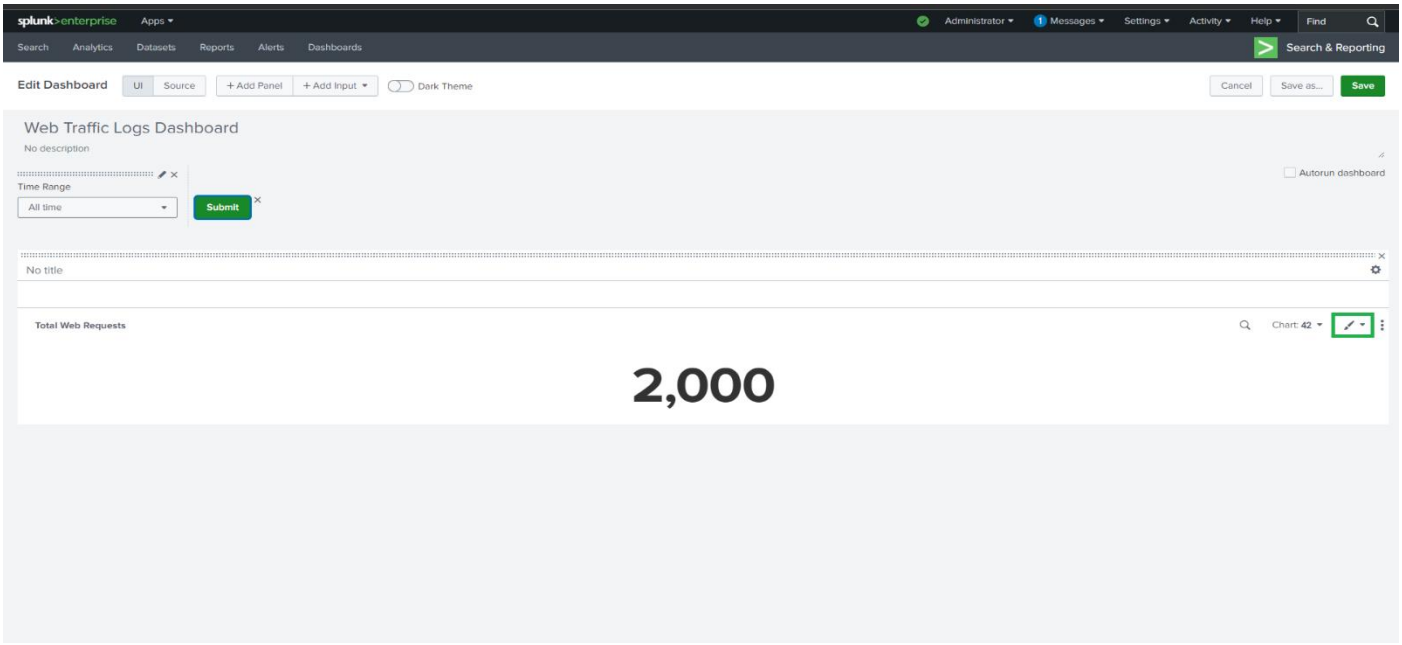

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Web Traffic Logs Dashboard
No description
Time Range
Last 24 hours
Submit
Click Add Panel to start.
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (7)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
optional
Search String
enter search here...
Run Search

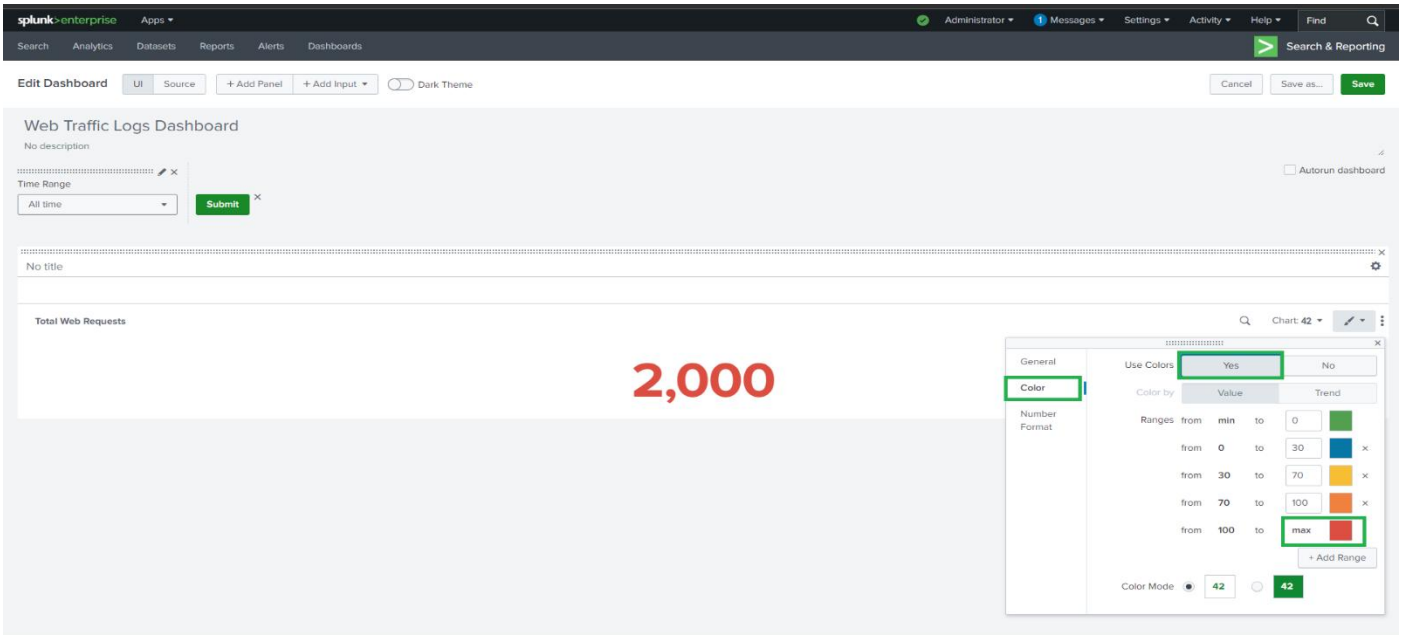

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Web Traffic Logs Dashboard
No description
Time Range
All time
Submit
Click Add Panel to start.
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (7)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
Total Web Requests
Search String
source="apache_logs.json" host="webserver" sourcetype="_json"
| stats count AS "Total Web Requests"
Run Search

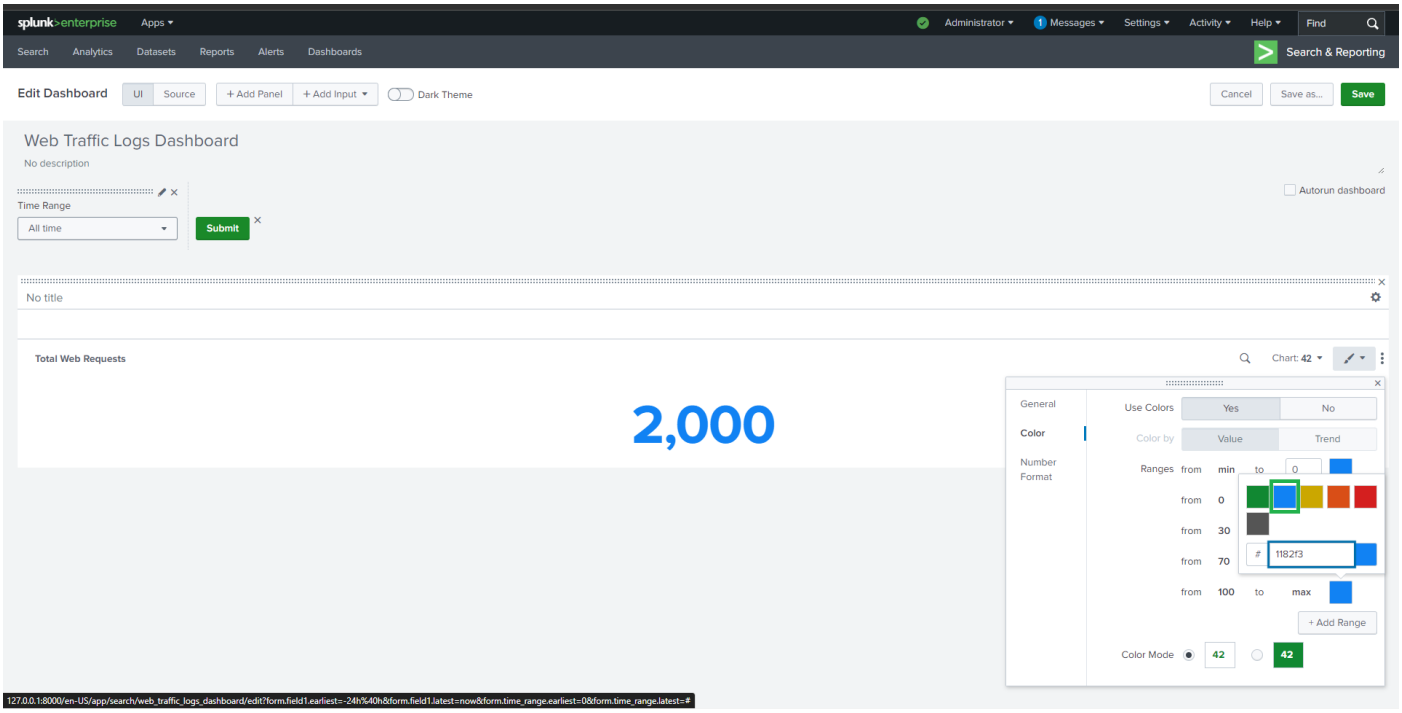

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Time Range
Last 24 hours
Submit
No title
Total Web Requests
Chart: 42
0

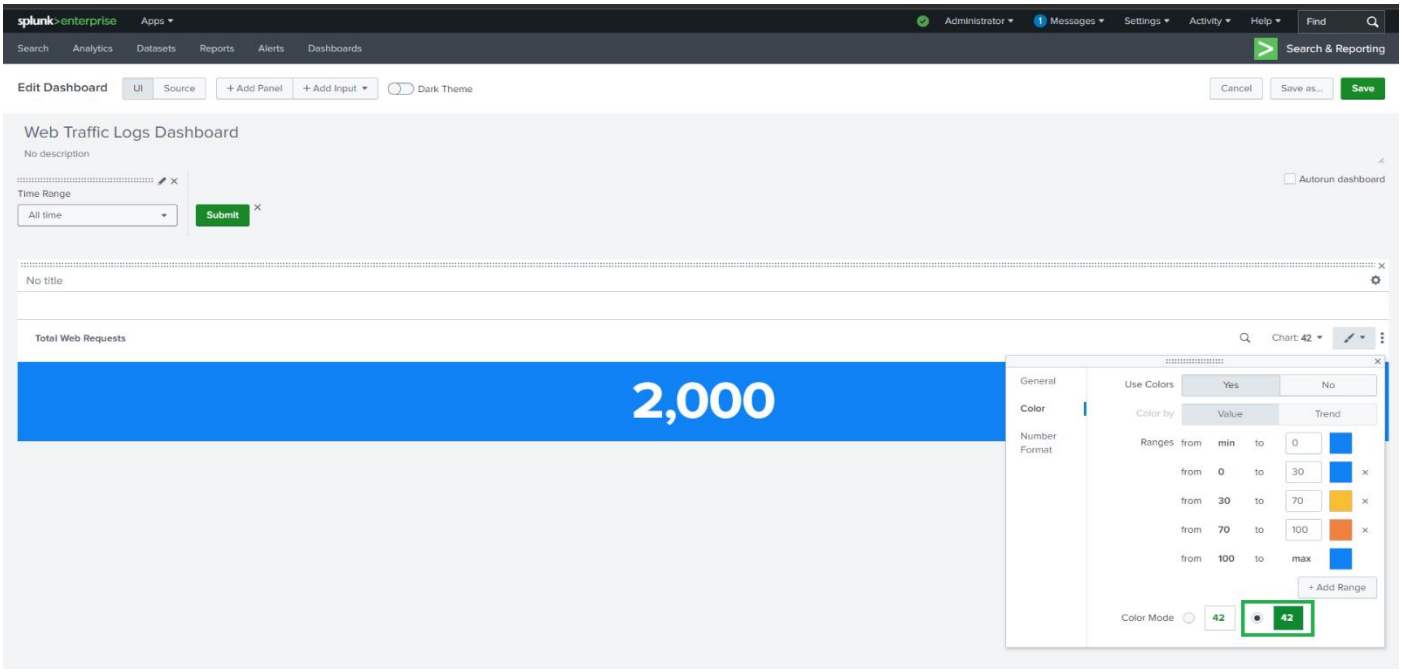

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Time Range
Last 24 hours
Submit
Presets
Real-time
30 second window
1 minute window
5 minute window
30 minute window
1 hour window
All time (real-time)
Relative
Today
Week to date
Business week to date
Month to date
Year to date
Yesterday
Previous week
Previous business week
Previous month
Previous year
Last 15 minutes
Last 60 minutes
Last 4 hours
Last 24 hours
Last 7 days
Last 30 days
Other
All time
Relative
Real-time
Date Range
Date & Time Range
Advanced
Chart: 42
0

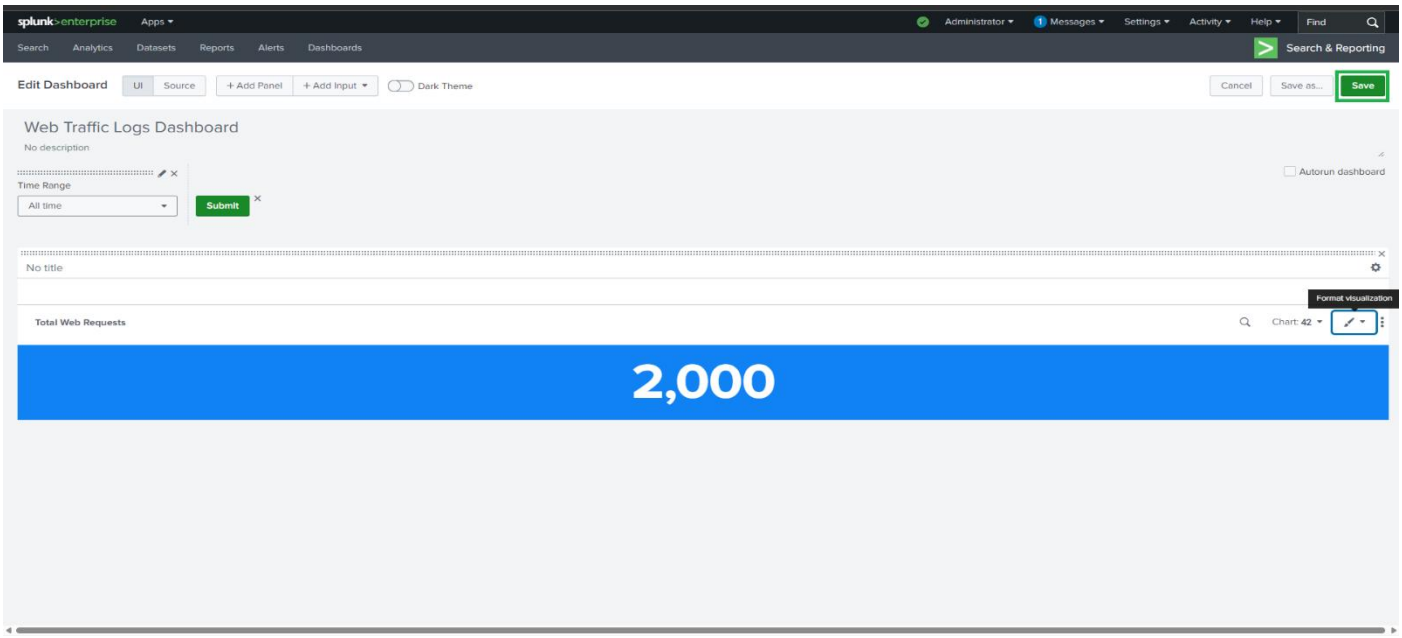

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
0

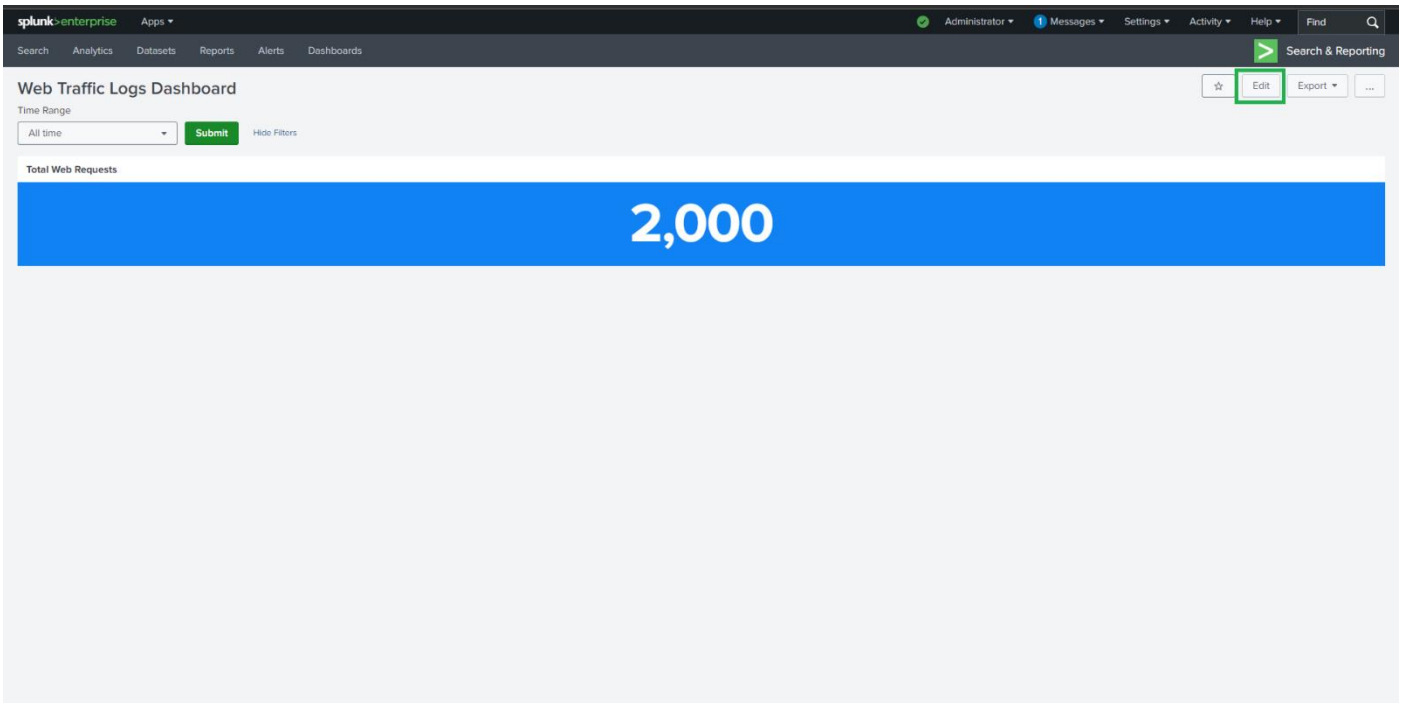

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000
General
Color
Number Format
Use Colors
Yes
No
Color by
Value
Trend
Ranges
from min to 0
from 0 to 30
from 30 to 70
from 70 to 100
from 100 to max
+ Add Range
Color Mode
42
42


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000
General
Color
Number Format
Use Colors
Yes
No
Color by
Value
Trend
Ranges
from min to 0
from 0
from 30
from 70
from 100 to max
1182f3
+ Add Range
Color Mode
42
42
127.0.0.1:8000/en-US/app/search/web_traffic_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&form.time_range.earliest=0&form.time_range.latest=#


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000
General
Color
Number Format
Use Colors
Yes
No
Color by
Value
Trend
Ranges
from min to 0
from 0 to 30
from 30 to 70
from 70 to 100
from 100 to max
+ Add Range
Color Mode
42
42


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Format visualization
Total Web Requests
Chart: 42
2,000


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Web Traffic Logs Dashboard
Edit
Export
Time Range
All time
Submit
Hide Filters
Total Web Requests
2,000

6.2 Successful Responses (200 OK)

Visualization: Single Value

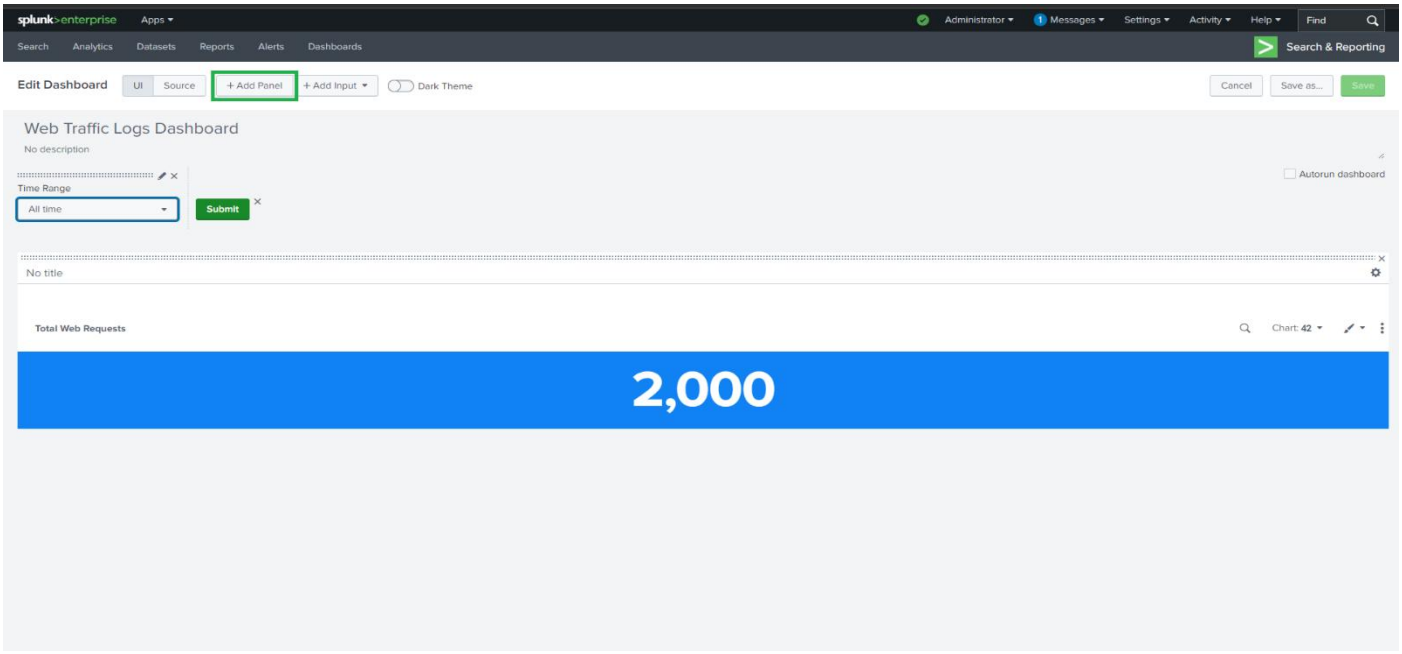
Title: Successful Response

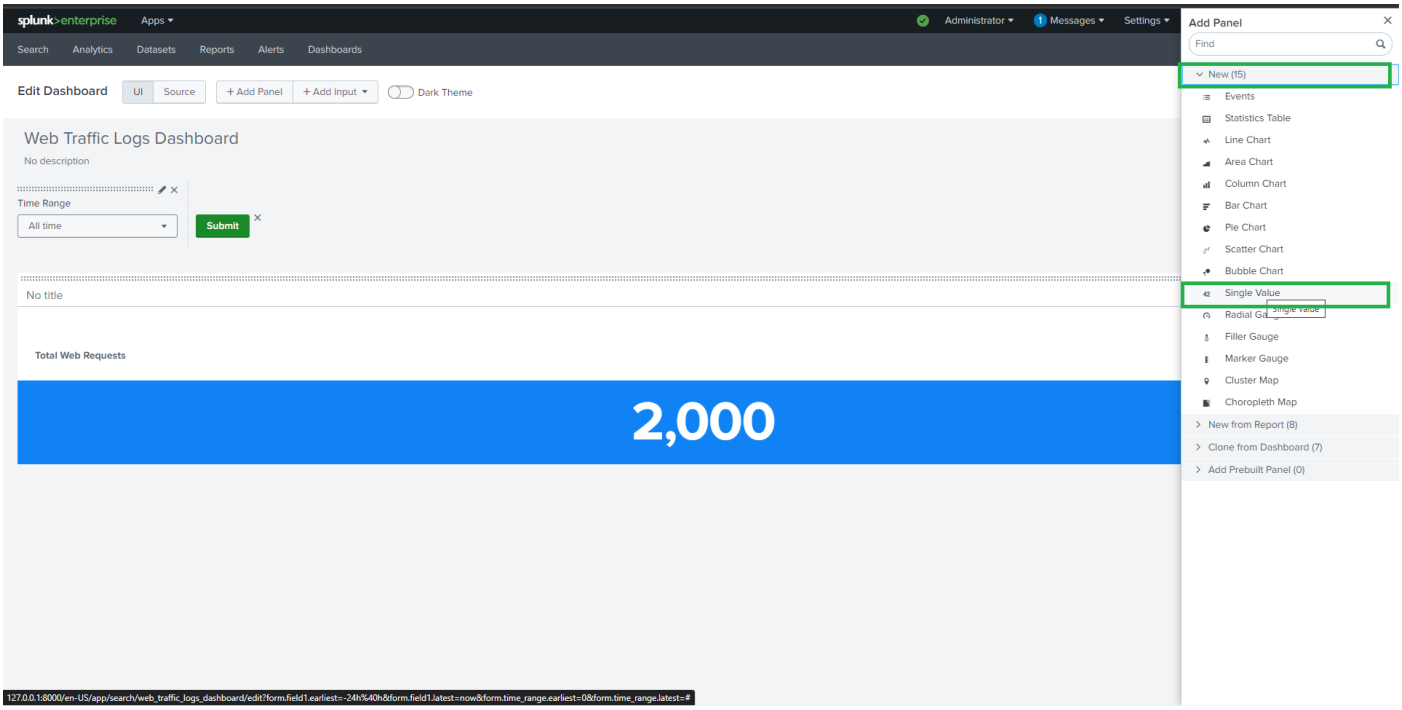
Search Query:

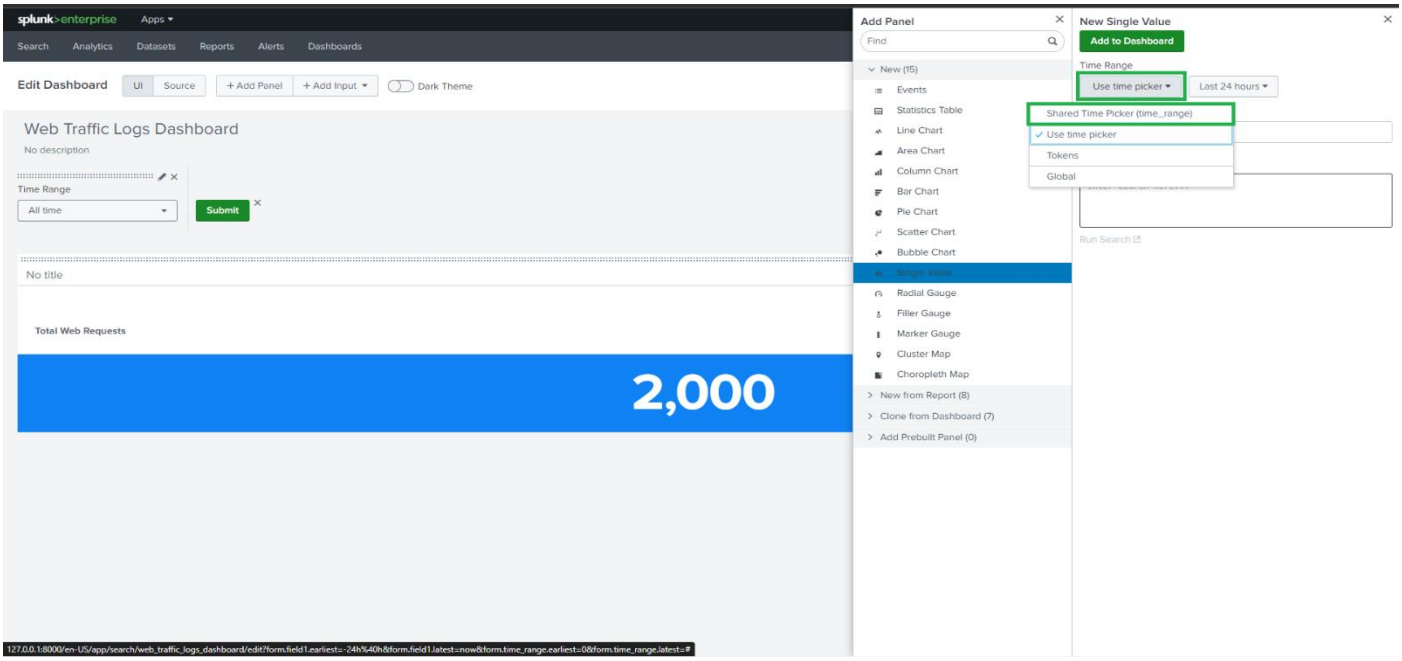
source="apache_logs.json" host="webserver" sourcetype="_json" method=GET status=200

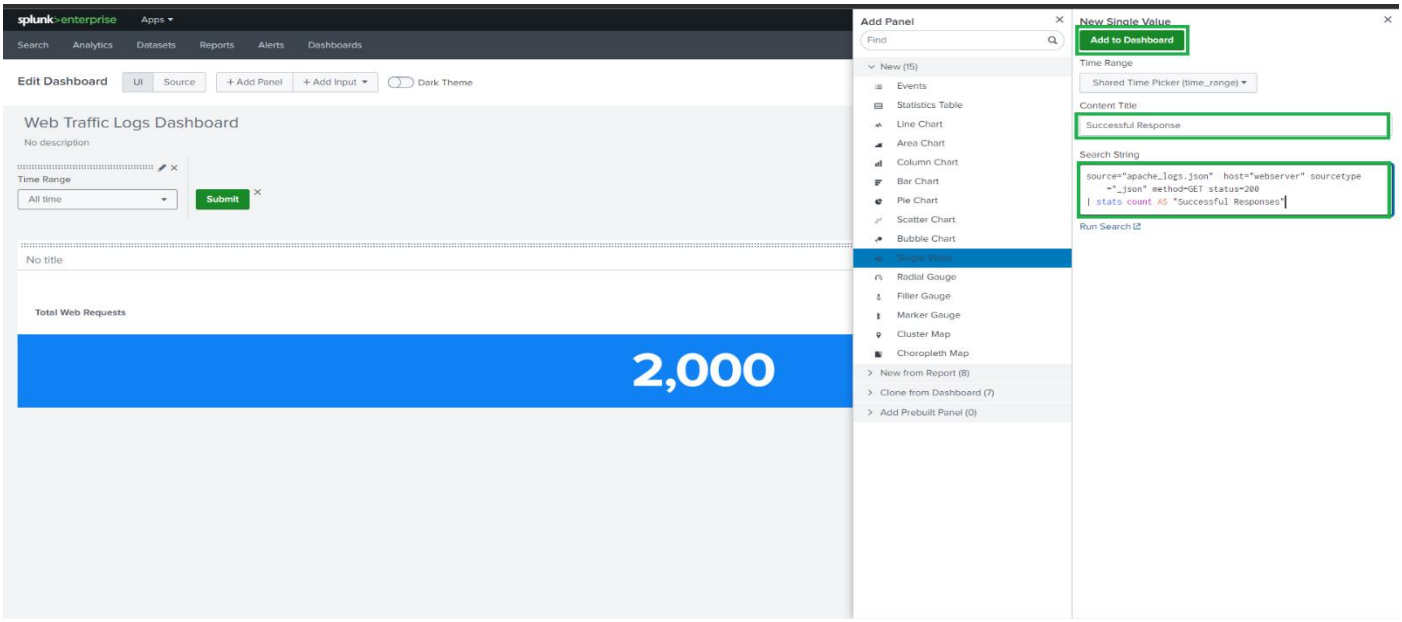
| stats count AS "Successful Responses"

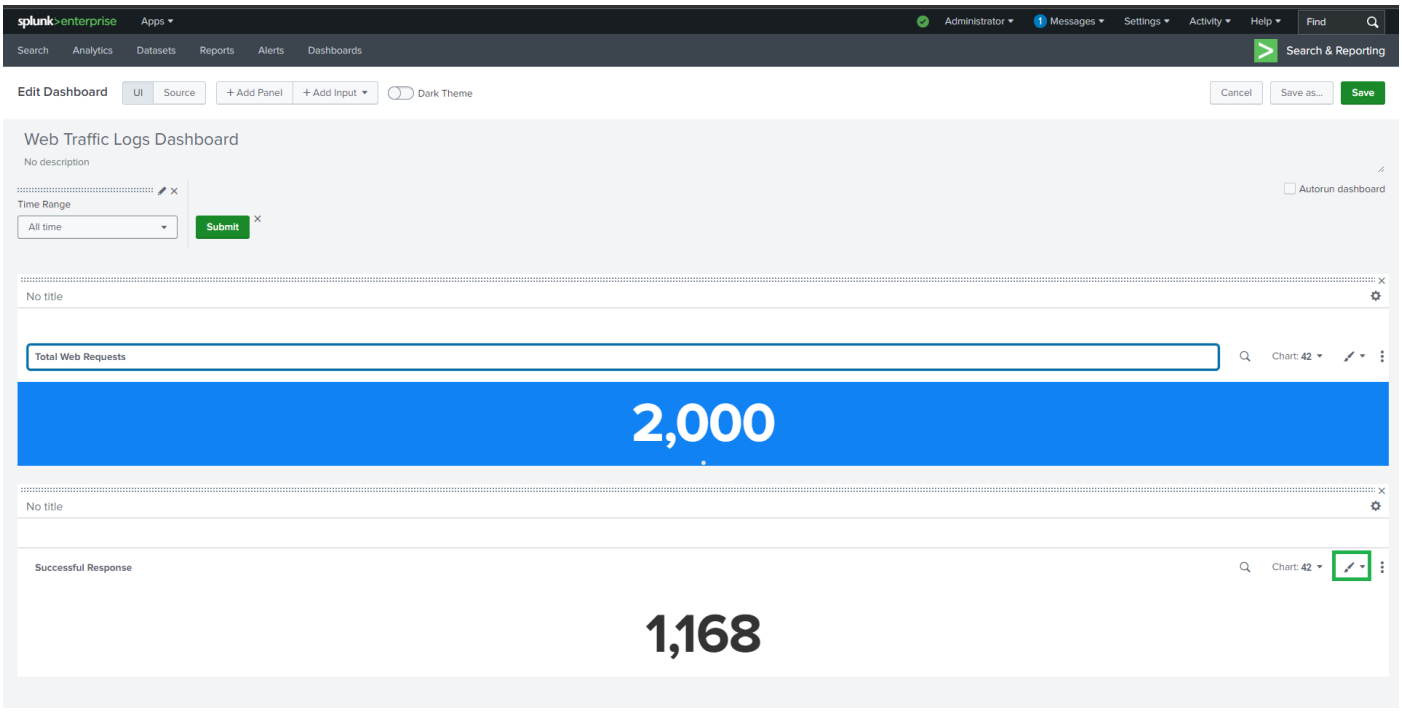
Purpose: Measures successful GET requests indicating normal operation.

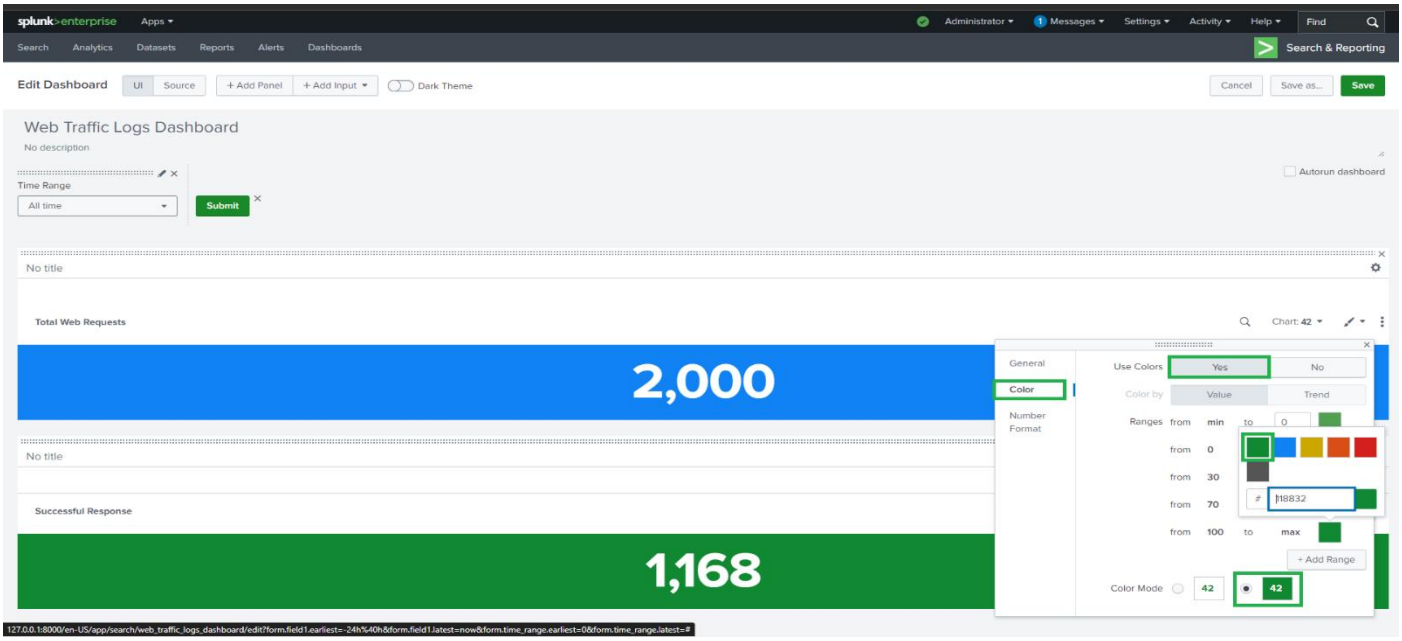


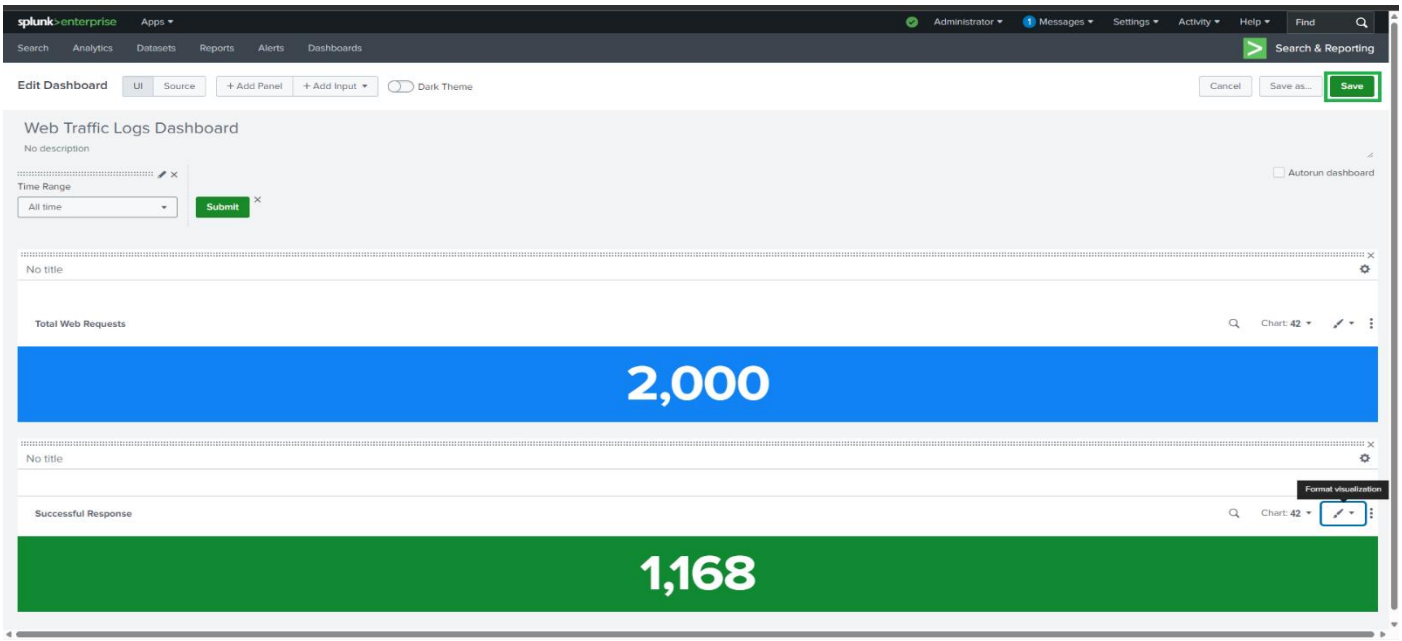


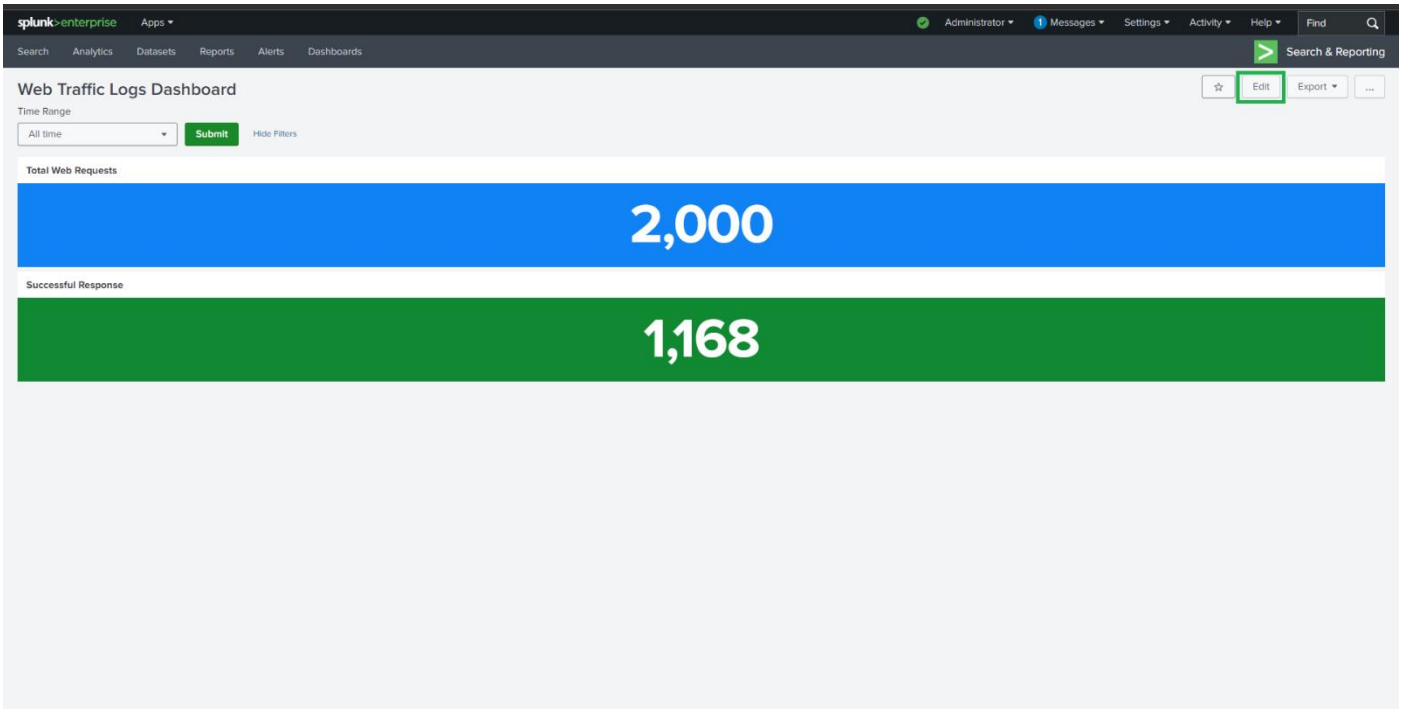

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Web Traffic Logs Dashboard
No description
Time Range
All time
Submit
No title
Total Web Requests
2,000
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (7)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Use time picker
Last 24 hours
Shared Time Picker (time_range)
Use time picker
Tokens
Global
Run Search
127.0.0.1:8000/en-US/app/search/web_traffic_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&form.time_range.earliest=0&form.time_range.latest=#


splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Web Traffic Logs Dashboard
No description
Time Range
All time
Submit
No title
Total Web Requests
2,000
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (7)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
Successful Response
Search String
source="apache_logs.json" host="webserver" sourcetype
="_json" method=GET status=200
| stats count AS "Successful Responses"
Run Search


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000
No title
Successful Response
Chart: 42
1,168


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Time Range
All time
Submit
Autorun dashboard
No title
Total Web Requests
Chart: 42
2,000
No title
Successful Response
1,168
General
Color
Number Format
Use Colors
Yes
No
Color by
Value
Trend
Ranges
from min to 0
from 0
from 30
from 70
from 100 to max
#18832
+ Add Range
Color Mode
42
42
127.0.0.1:8000/en-US/app/search/web_traffic_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&form.time_range.earliest=0&form.time_range.latest=#


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Time Range
All time
Submit
Autorun dashboard
No title
Total Web Requests
Chart: 42
2,000
No title
Format visualization
Successful Response
Chart: 42
1,168


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Web Traffic Logs Dashboard
Edit
Export
Time Range
All time
Submit
Hide Filters
Total Web Requests
2,000
Successful Response
1,168

6.3 Client Errors (4xx)

Visualization: Single Value

Title: Client Errors

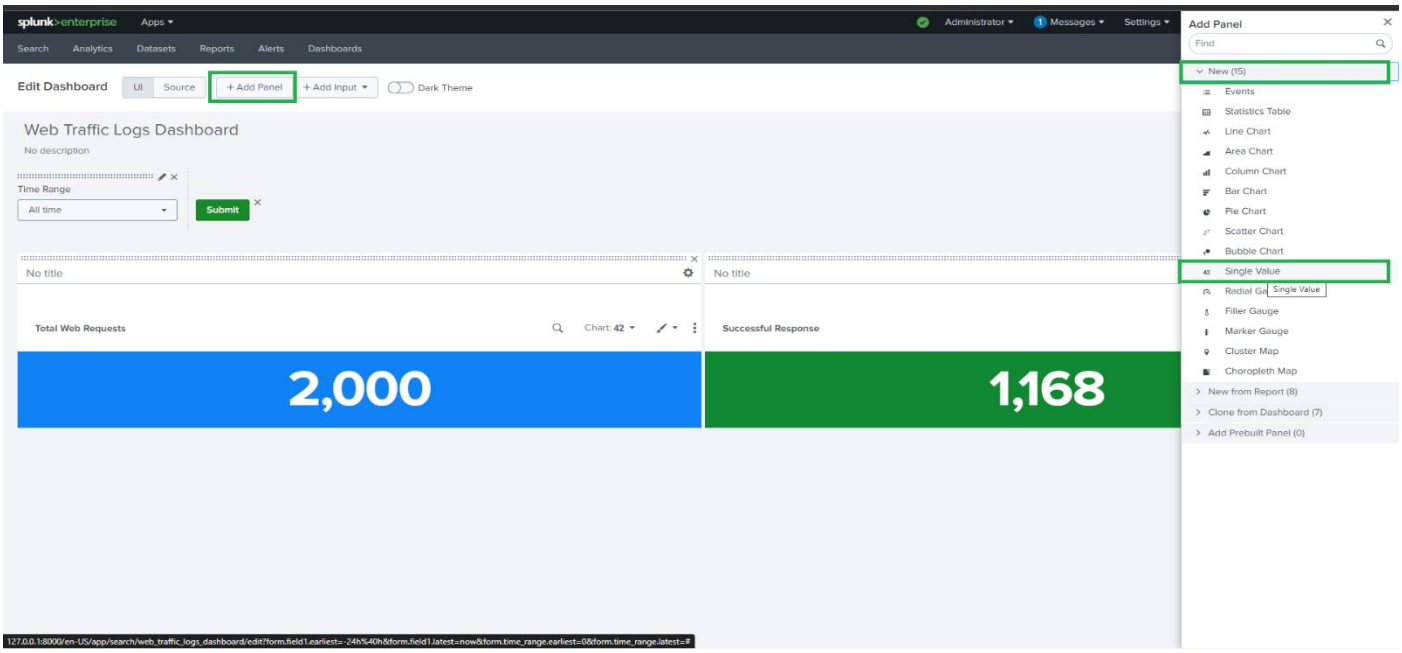
Search Query:

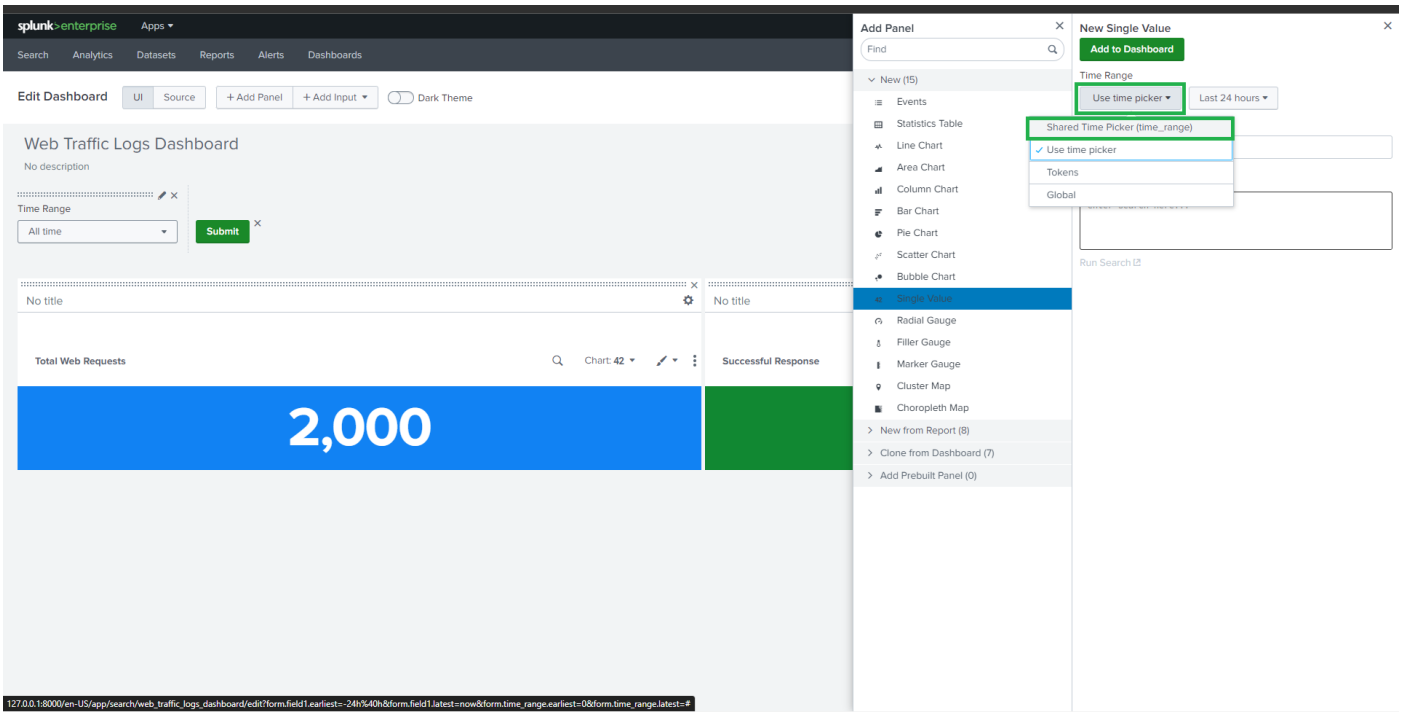
source="apache_logs.json" host="webserver" sourcetype="_json"

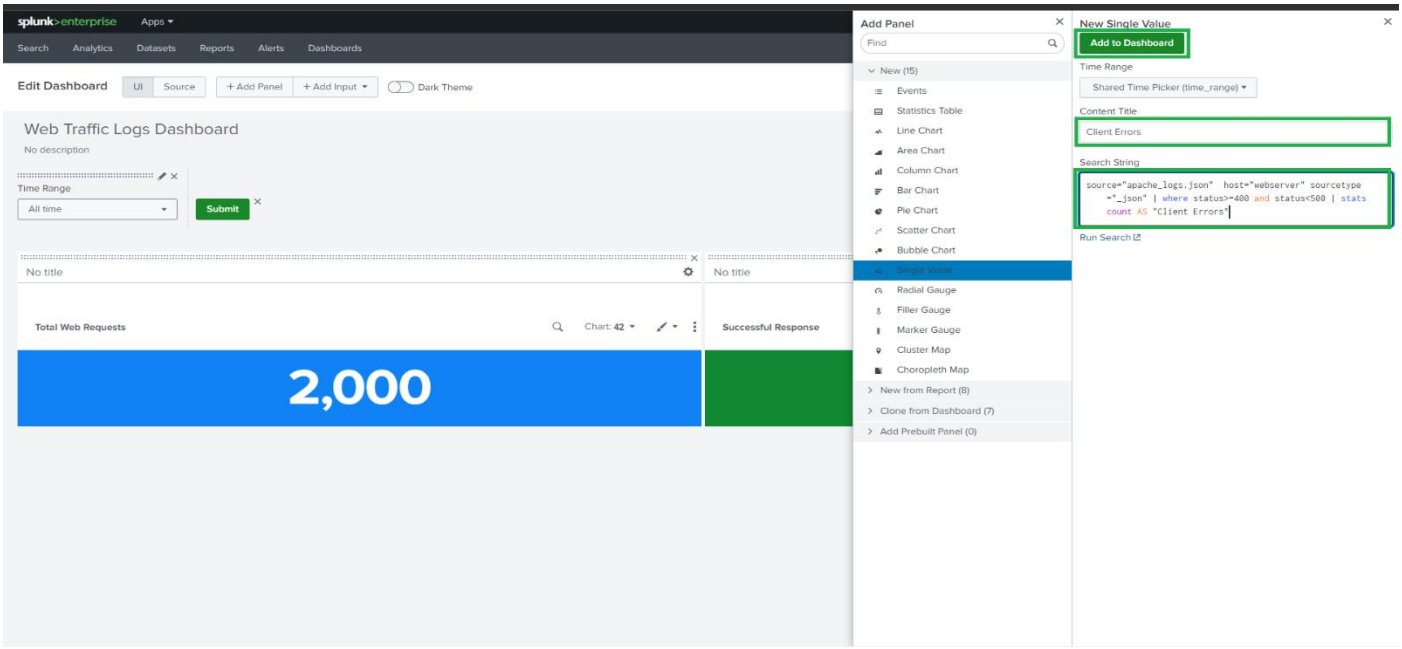
| where status>=400 AND status<500

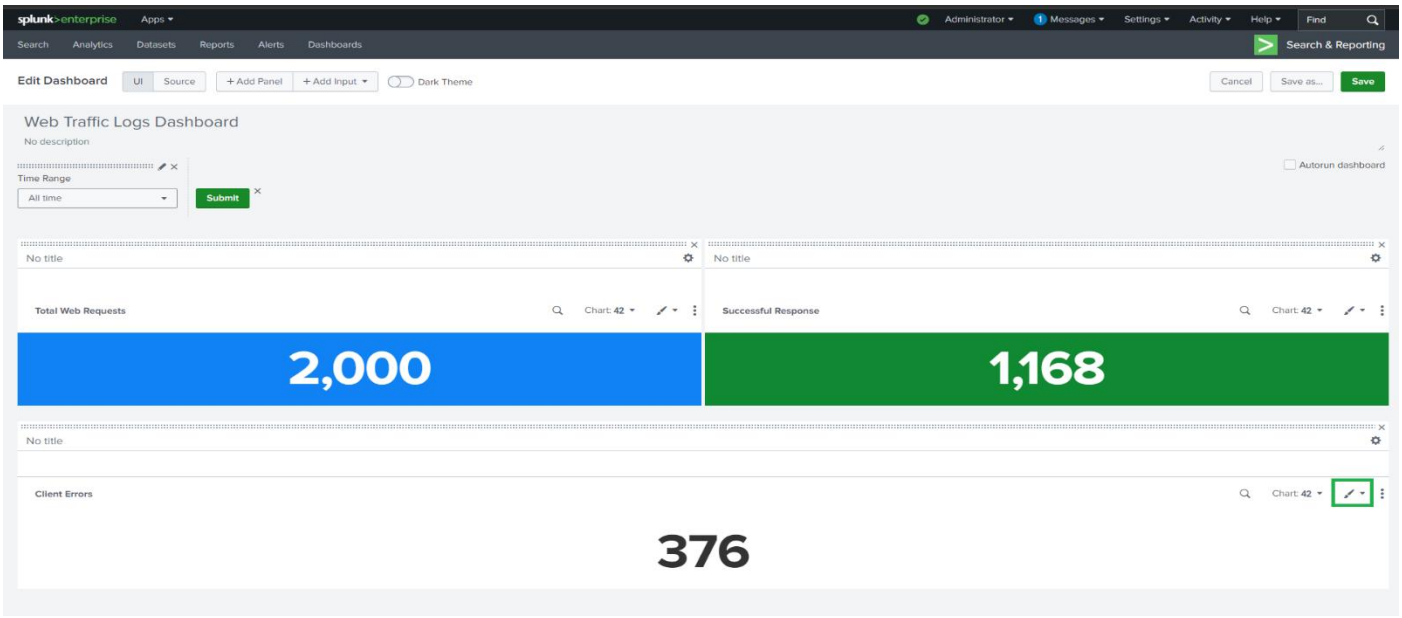
| stats count AS "Client Errors"

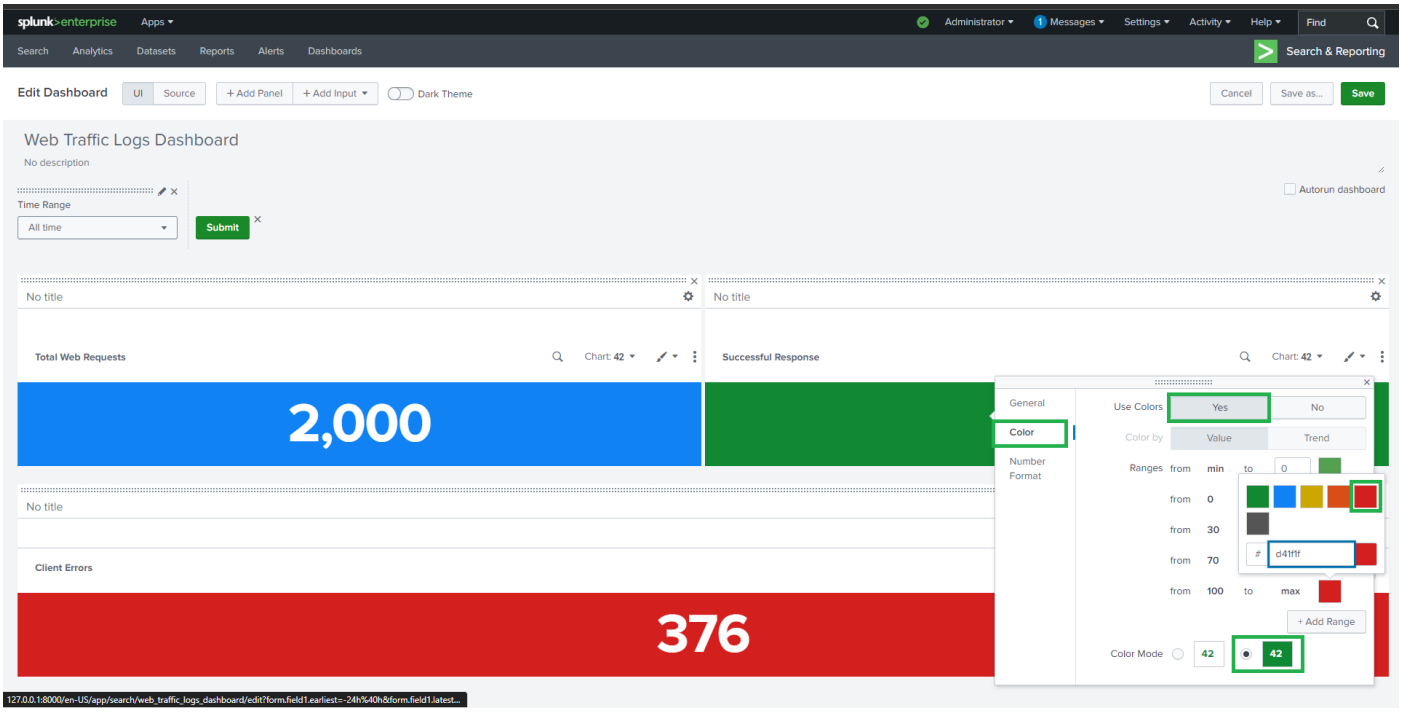
Purpose: Identifies issues caused by incorrect client requests.

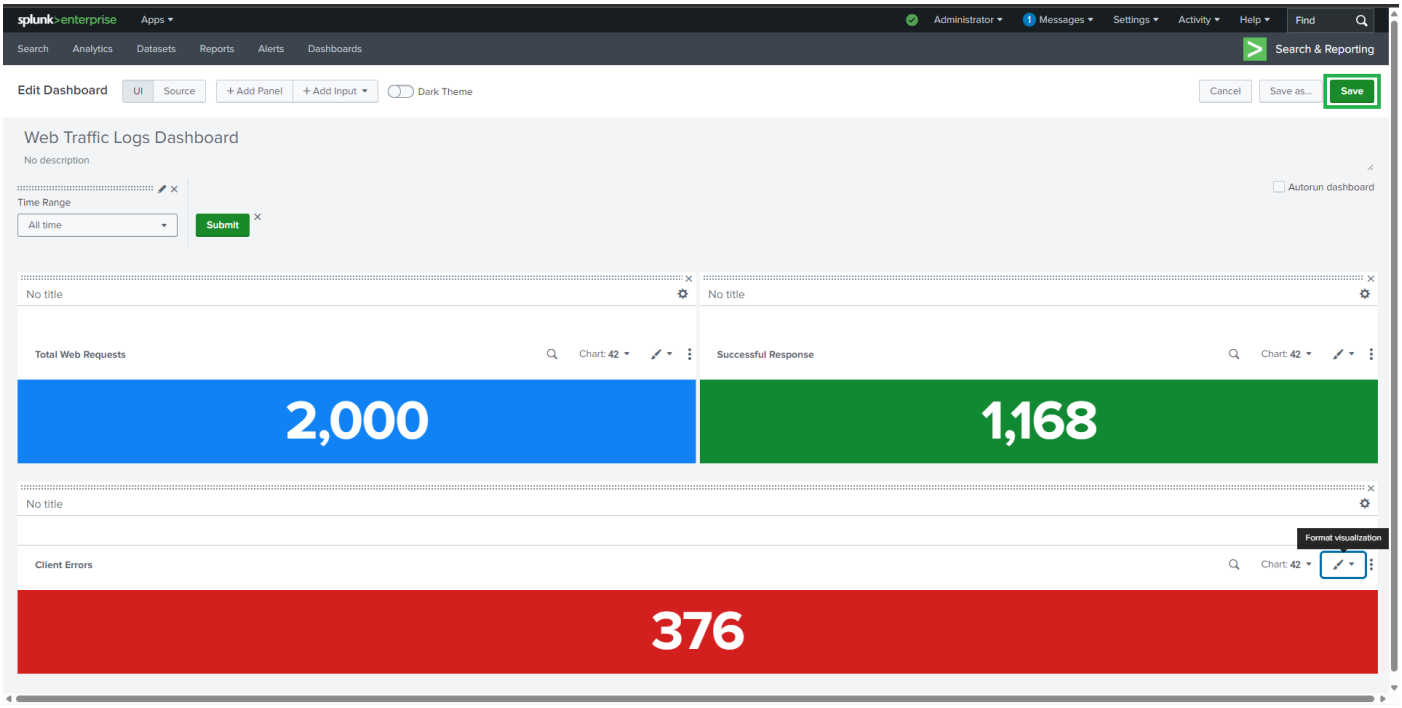


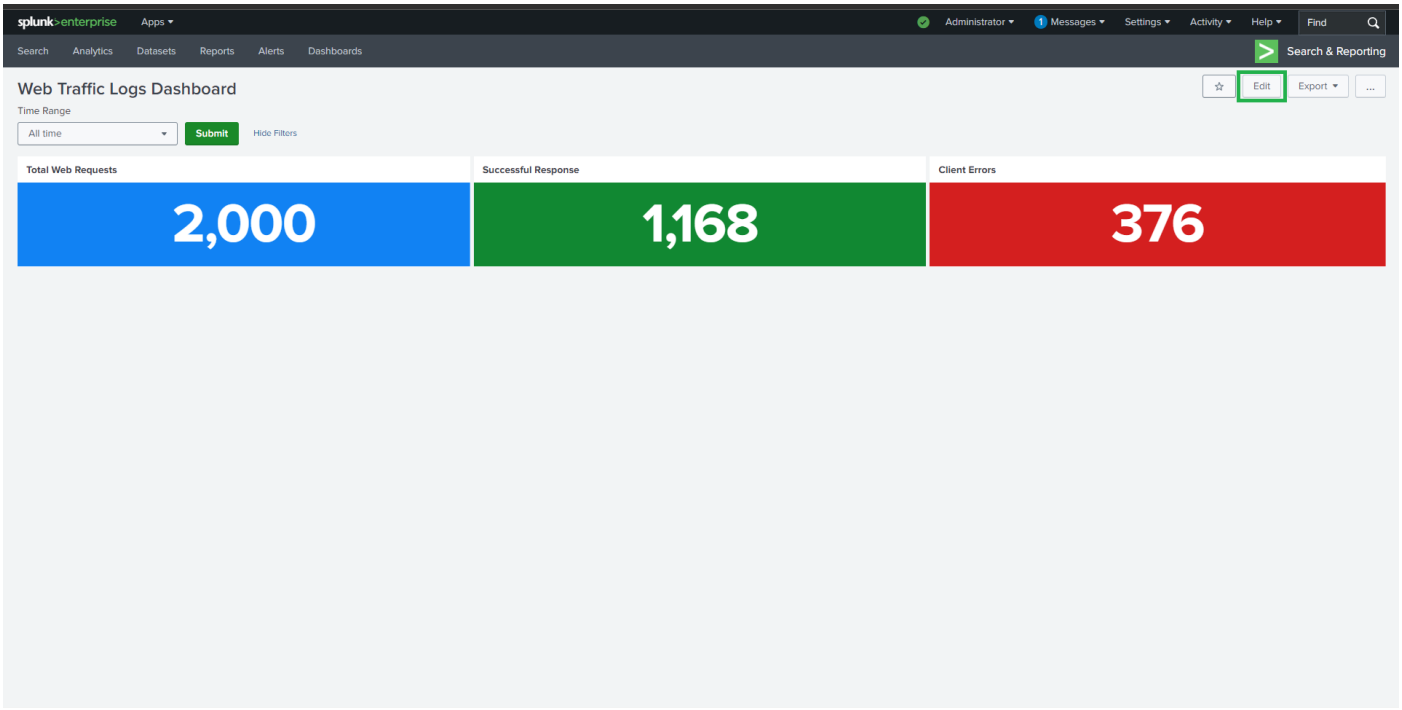



splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Web Traffic Logs Dashboard
No description
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (7)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
Client Errors
Search String
source="apache_logs.json" host="webserver" sourcetype="_json" | where status>=400 and status<500 | stats count AS "Client Errors"
Run Search


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search & Reporting
Edit Dashboard
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total Web Requests
2,000
Successful Response
1,168
Client Errors
376


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search & Reporting
Edit Dashboard
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total Web Requests
2,000
Successful Response
Client Errors
376
General
Color
Number Format
Use Colors
Yes
No
Color by
Value
Trend
Ranges
from min to 0
from 0
from 30
from 70
from 100 to max
d41f1f
+ Add Range
Color Mode
42
42
127.0.0.1:8000/en-US/app/search/web_traffic_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest...


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000
No title
Successful Response
Chart: 42
1,168
No title
Client Errors
Chart: 42
Format visualization
376


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Web Traffic Logs Dashboard
Edit
Export
Time Range
All time
Submit
Hide Filters
Total Web Requests
2,000
Successful Response
1,168
Client Errors
376

6.4 Server Errors (5xx)

Visualization: Single Value

Title: Server Errors (5xx)

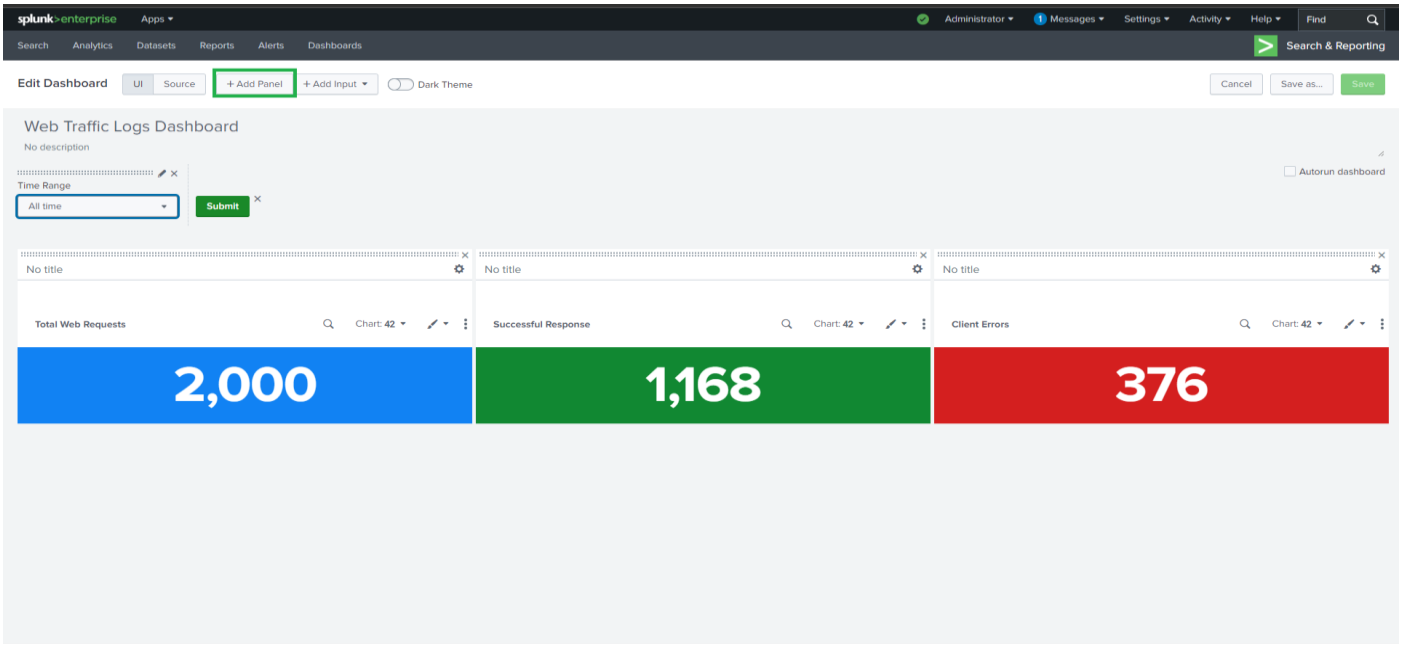
Search Query:

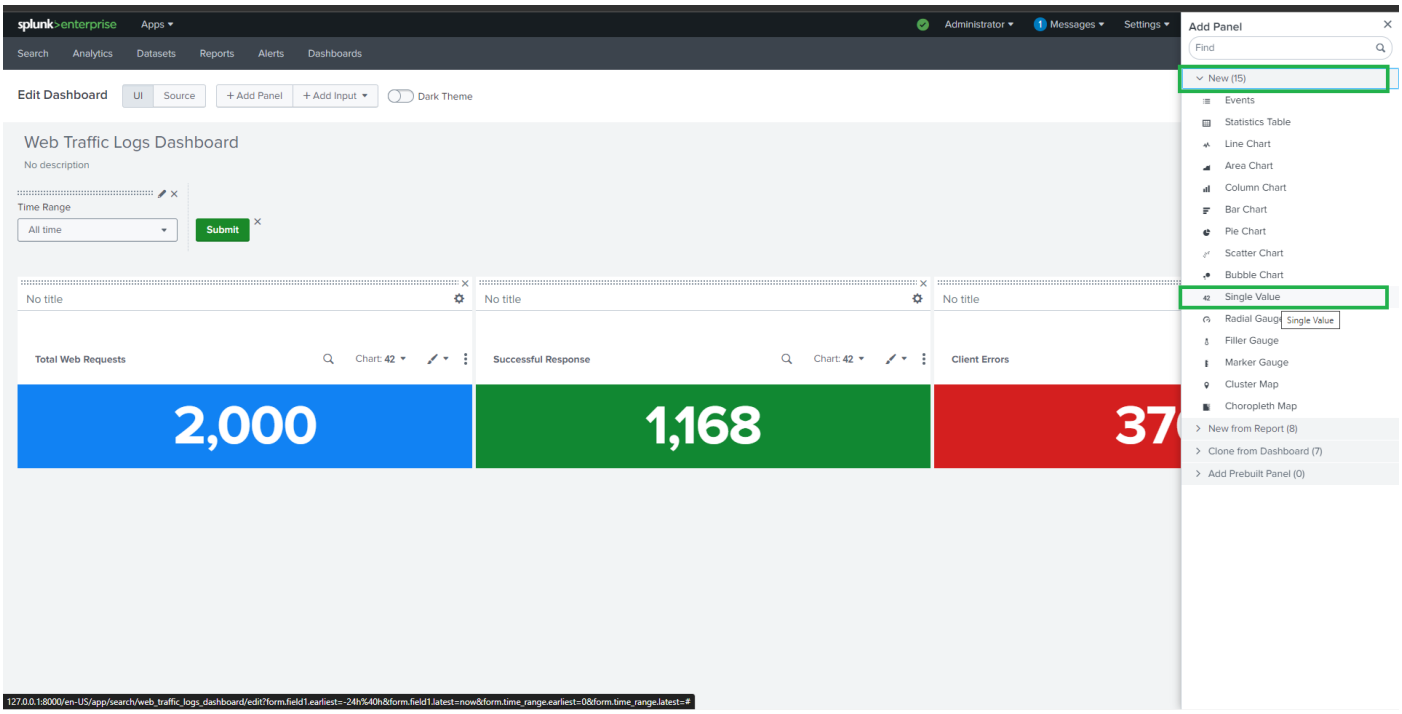
source="apache_logs.json" host="webserver" sourcetype="_json"

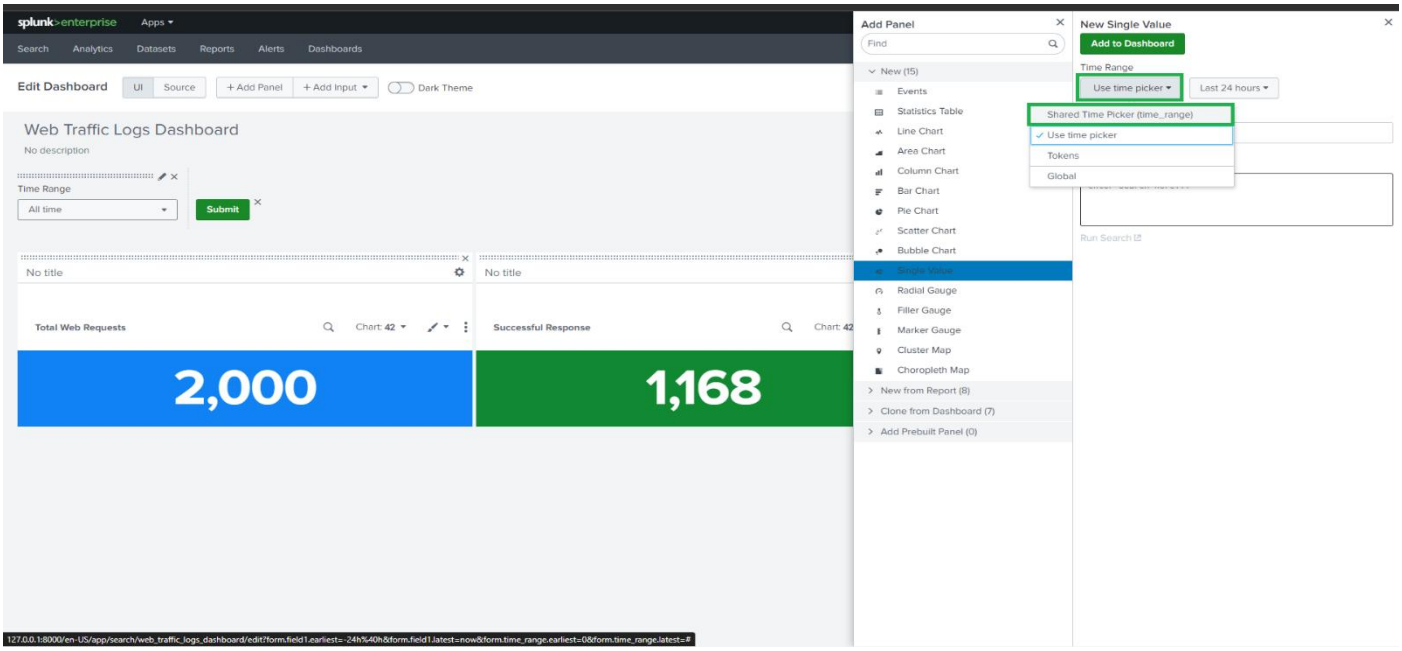
| where status>=500 AND status<600

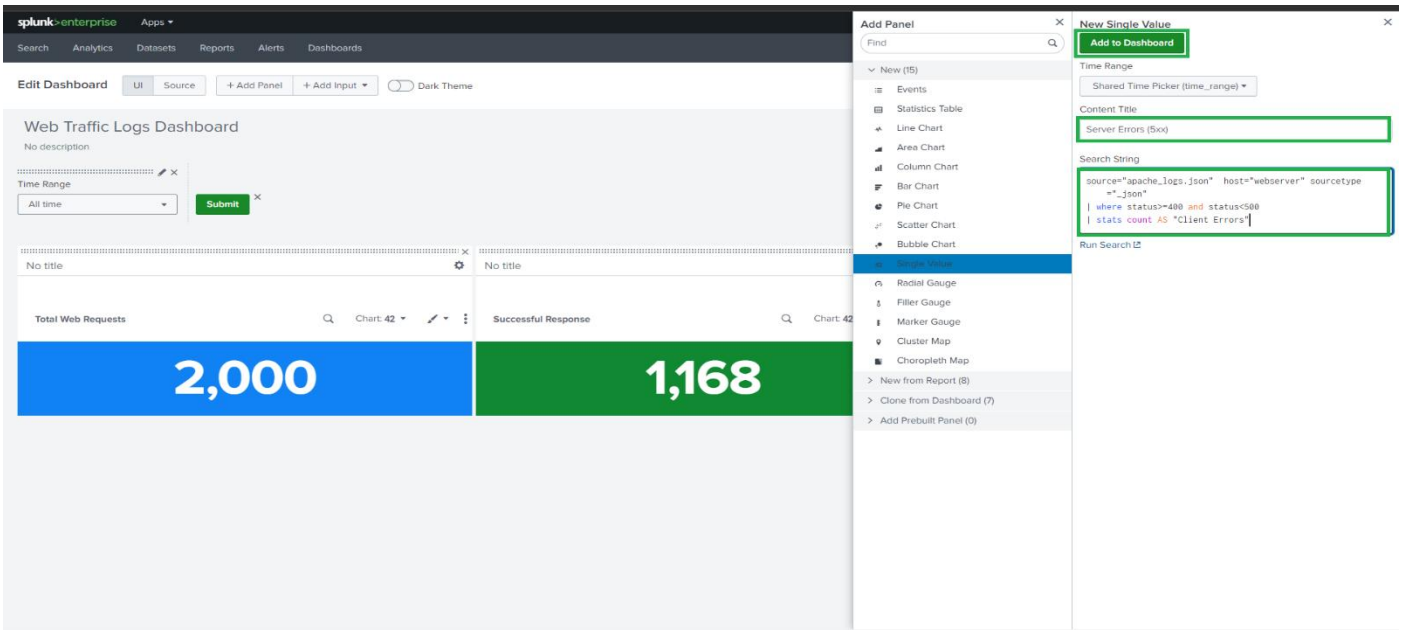
| stats count AS "Server Errors"

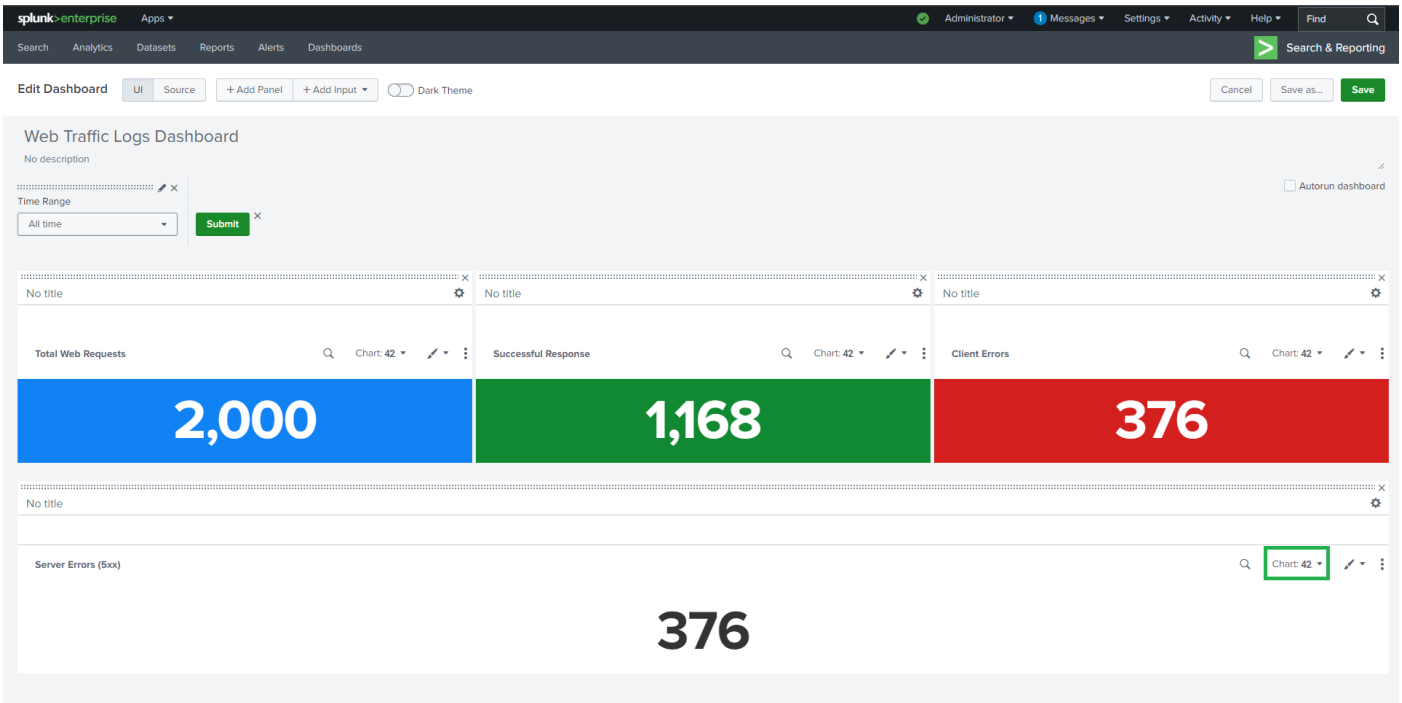
Purpose: Highlights server-side failures that require immediate attention.

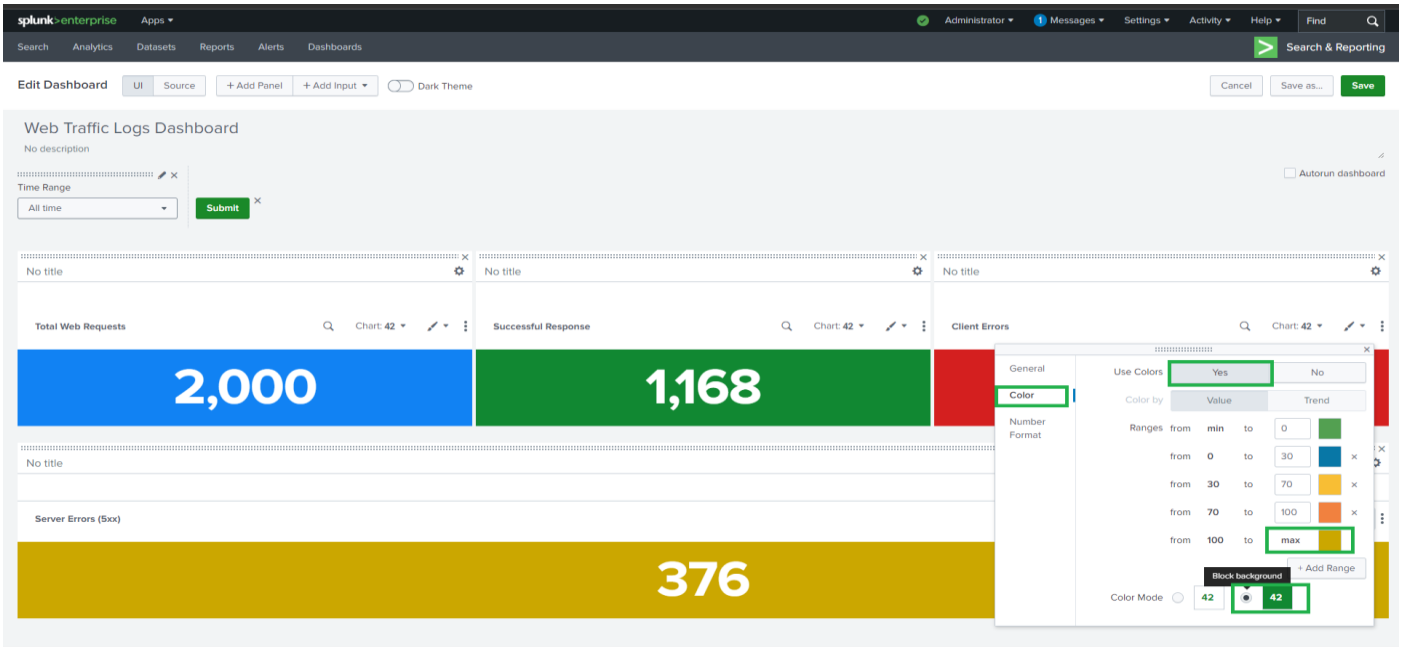


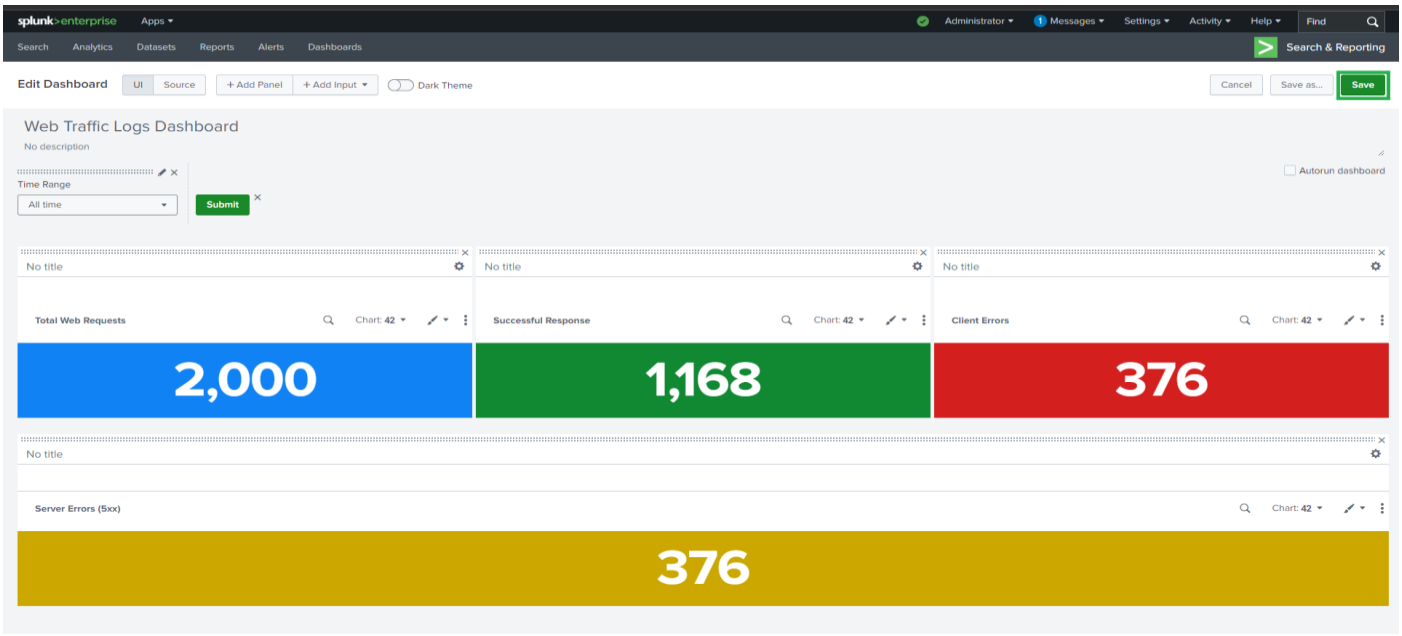


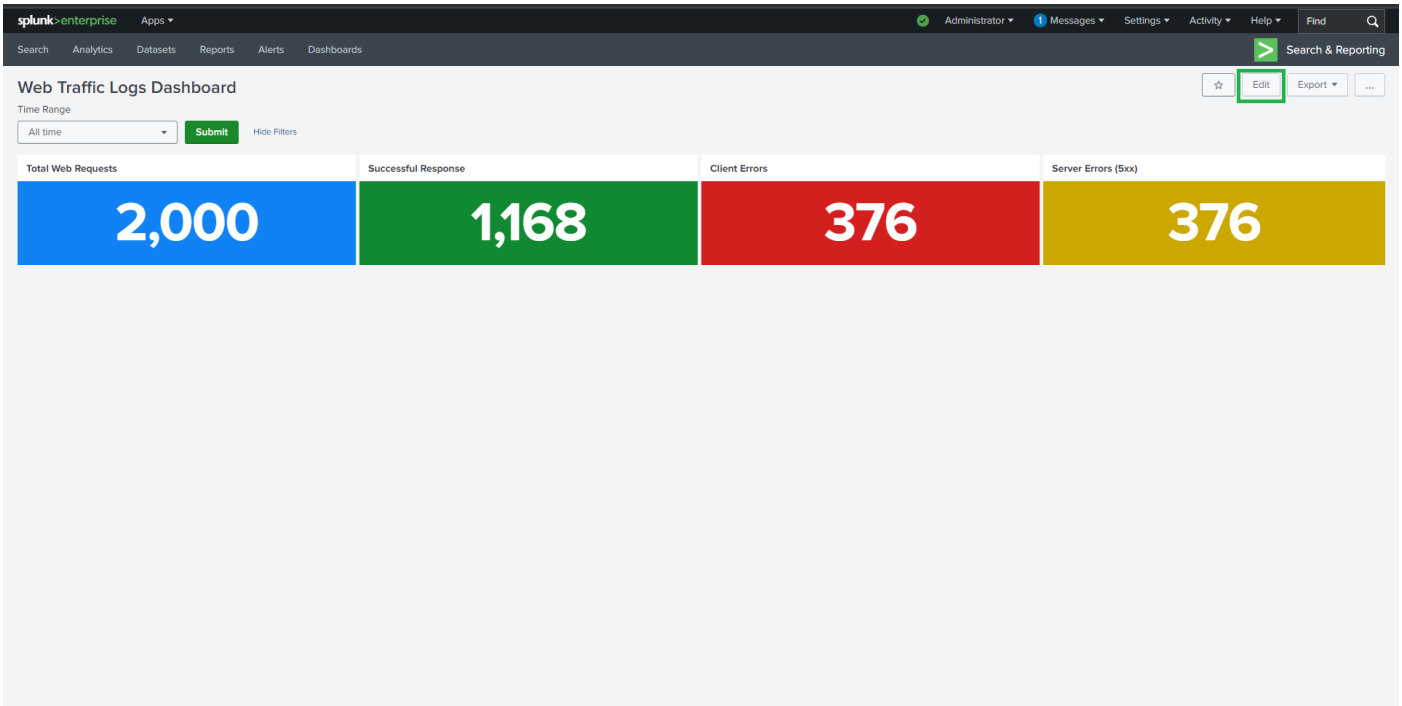

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Web Traffic Logs Dashboard
No description
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000
Successful Response
1,168
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (7)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Use time picker
Last 24 hours
Shared Time Picker (time_range)
Use time picker
Tokens
Global
Run Search
127.0.0.1:8000/en-US/app/search/web_traffic_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&form.time_range.earliest=0&form.time_range.latest=#


splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Web Traffic Logs Dashboard
No description
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000
Successful Response
1,168
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (7)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
Server Errors (5xx)
Search String
source="apache_logs.json" host="webserver" sourcetype="_json"
| where status>=400 and status<500
| stats count AS "Client Errors"
Run Search


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Time Range
All time
Submit
Autorun dashboard
No title
Total Web Requests
Chart: 42
2,000
Successful Response
1,168
Client Errors
376
Server Errors (5xx)
376


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000
Successful Response
1,168
Client Errors
General
Color
Number Format
Use Colors
Yes
No
Color by
Value
Trend
Ranges
from min to 0
from 0 to 30
from 30 to 70
from 70 to 100
from 100 to max
+ Add Range
Block background
Color Mode
42
Server Errors (5xx)
376


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000
Successful Response
1,168
Client Errors
376
Server Errors (5xx)
376


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Web Traffic Logs Dashboard
Edit
Export
Time Range
All time
Submit
Hide Filters
Total Web Requests
2,000
Successful Response
1,168
Client Errors
376
Server Errors (5xx)
376

7. Task 2: Web Statistics Panels

7.1 Top Requested URIs

Visualization: Bar Chart

Title: Top Requested URIs

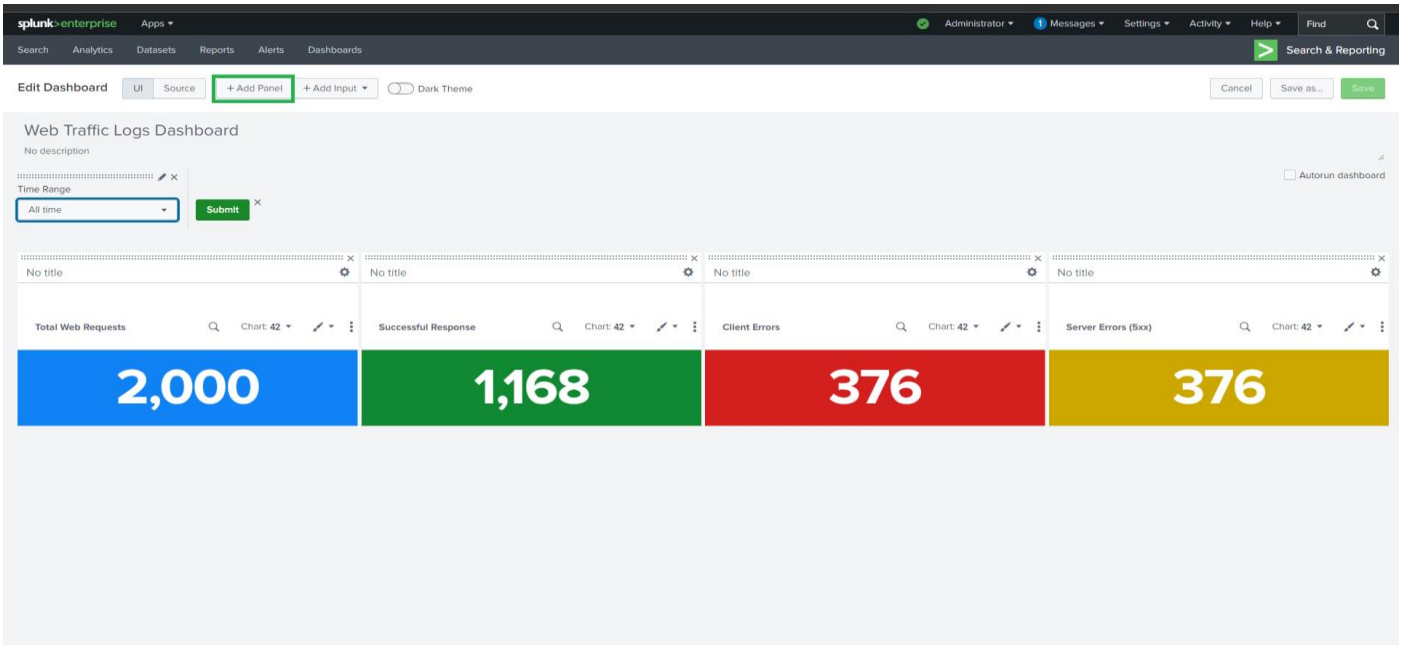
Search Query:

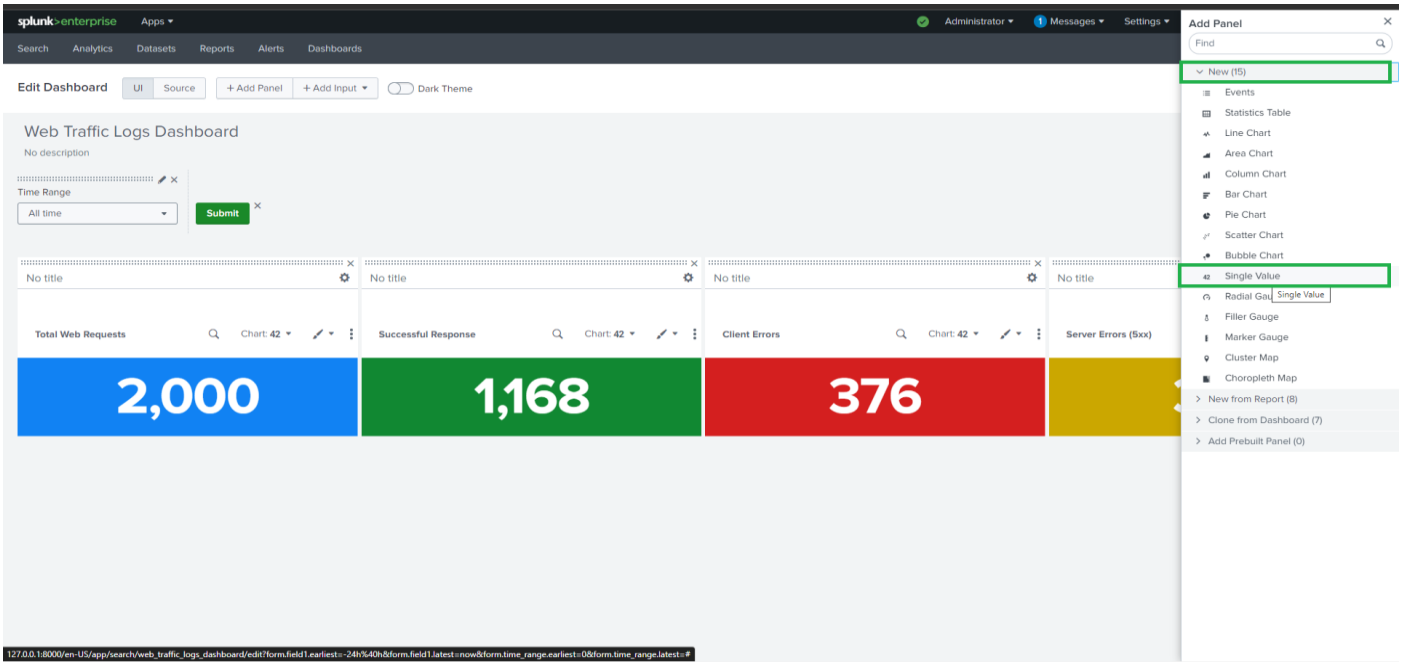
source="apache_logs.json" host="webserver" sourcetype="_json"

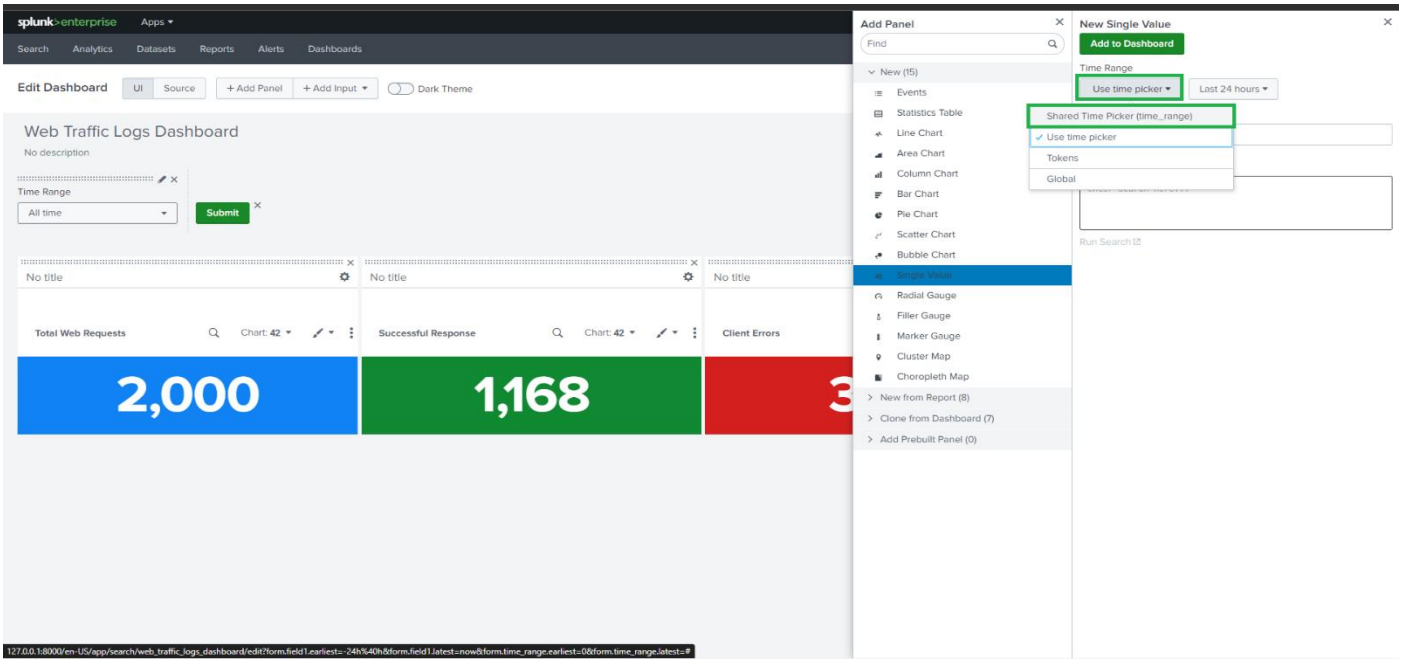
| stats count AS "Hits" by uri

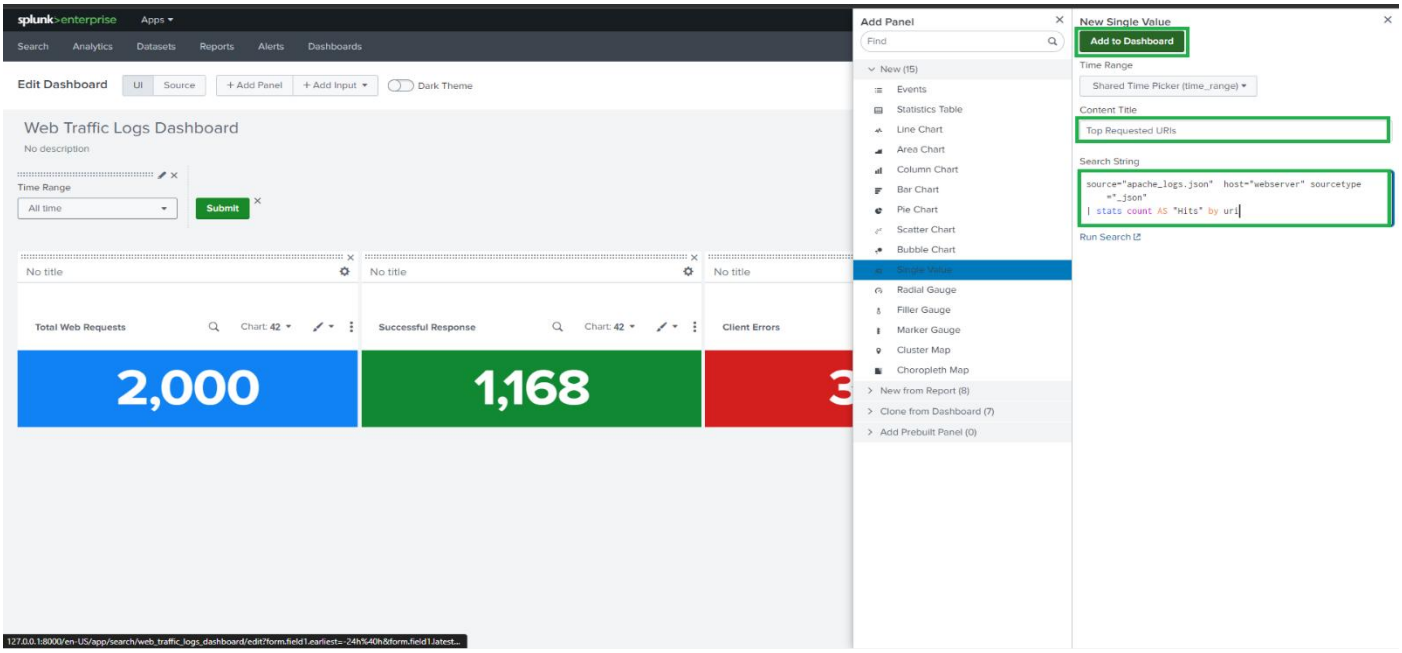
| sort - Hits

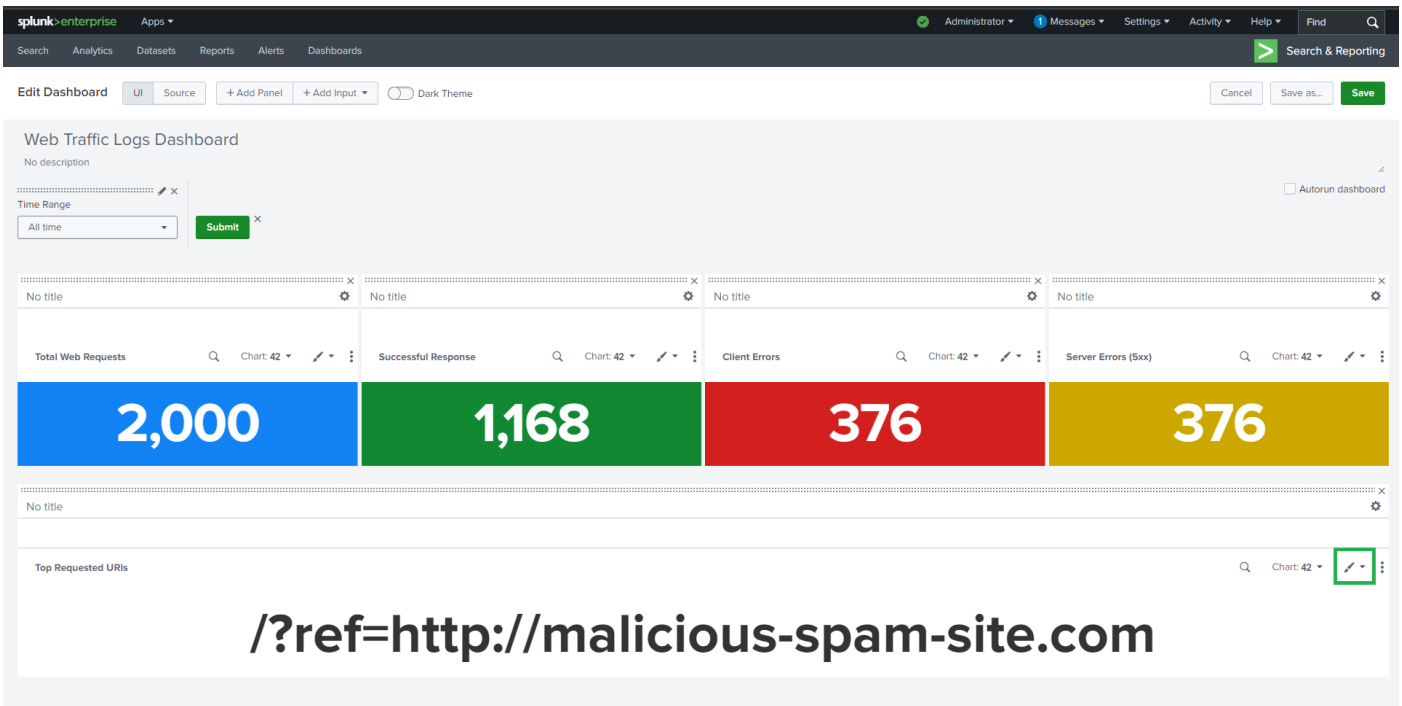
Purpose: Identifies the most frequently accessed web resources.

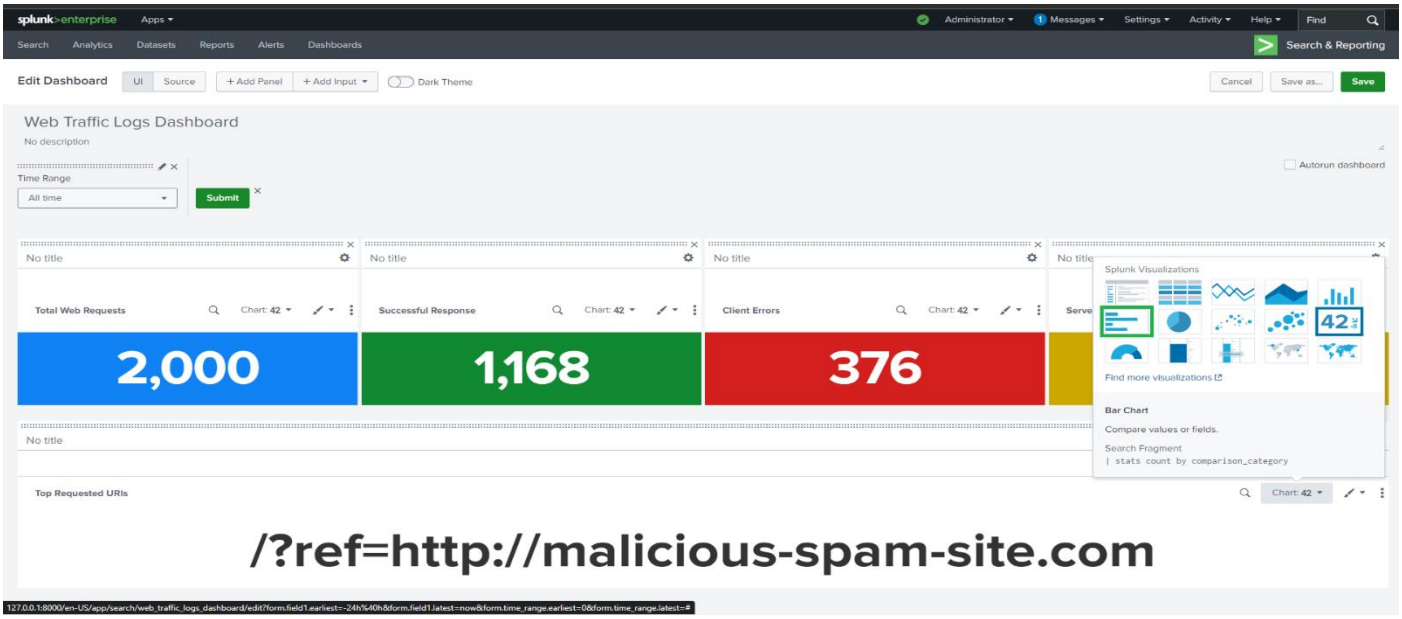


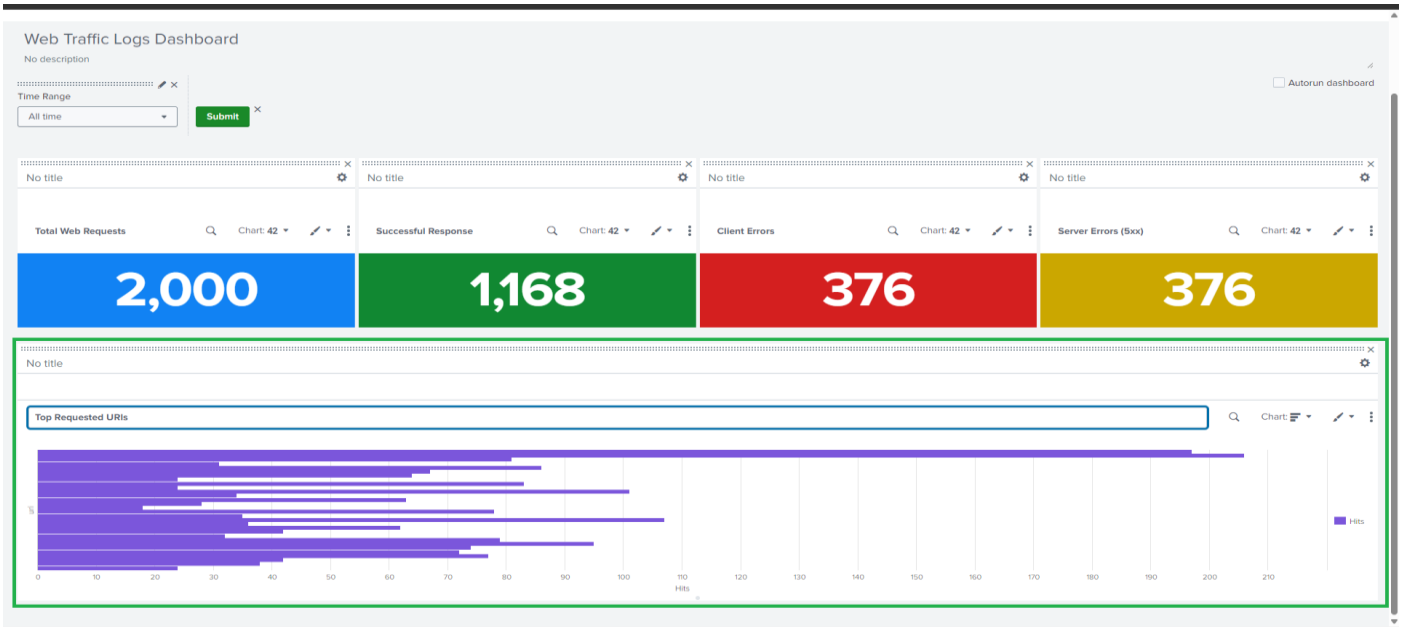


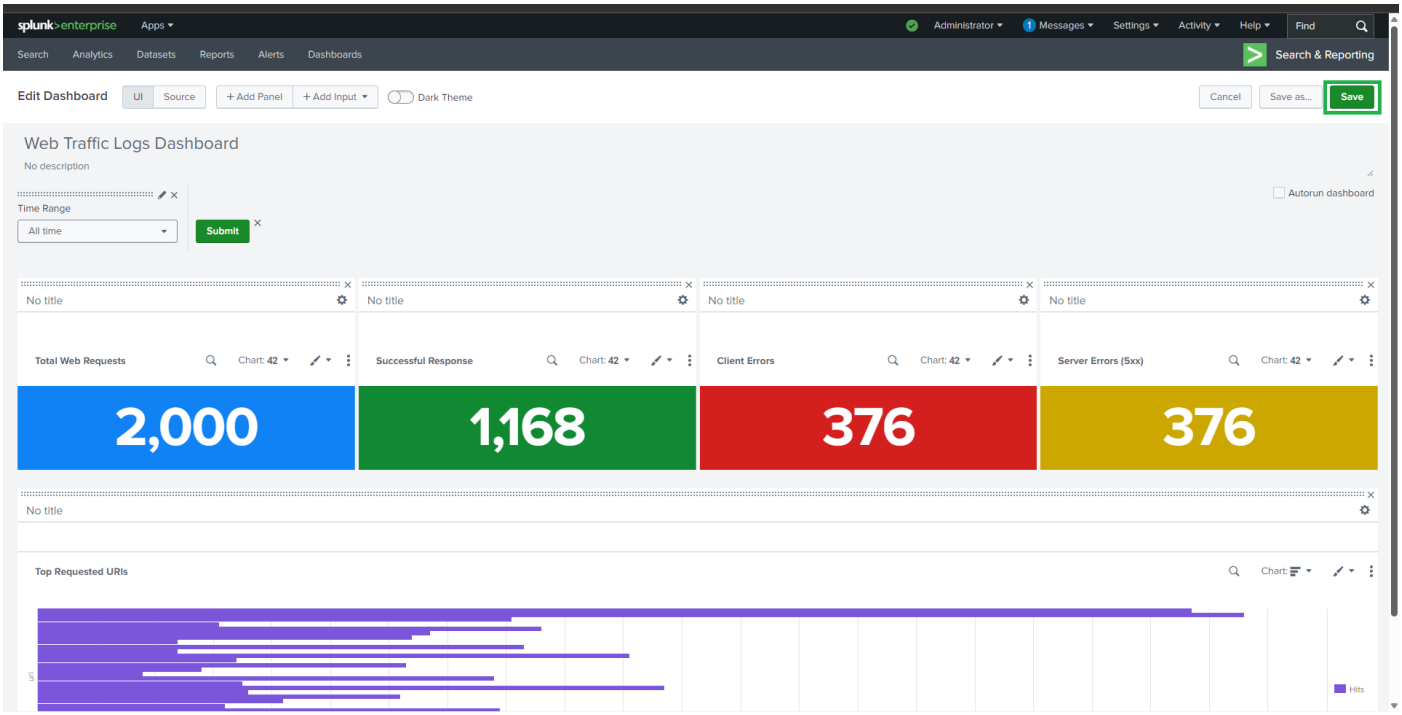

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Web Traffic Logs Dashboard
No description
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000
Successful Response
1,168
Client Errors
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (7)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Use time picker
Last 24 hours
Shared Time Picker (time_range)
Use time picker
Tokens
Global
Run Search

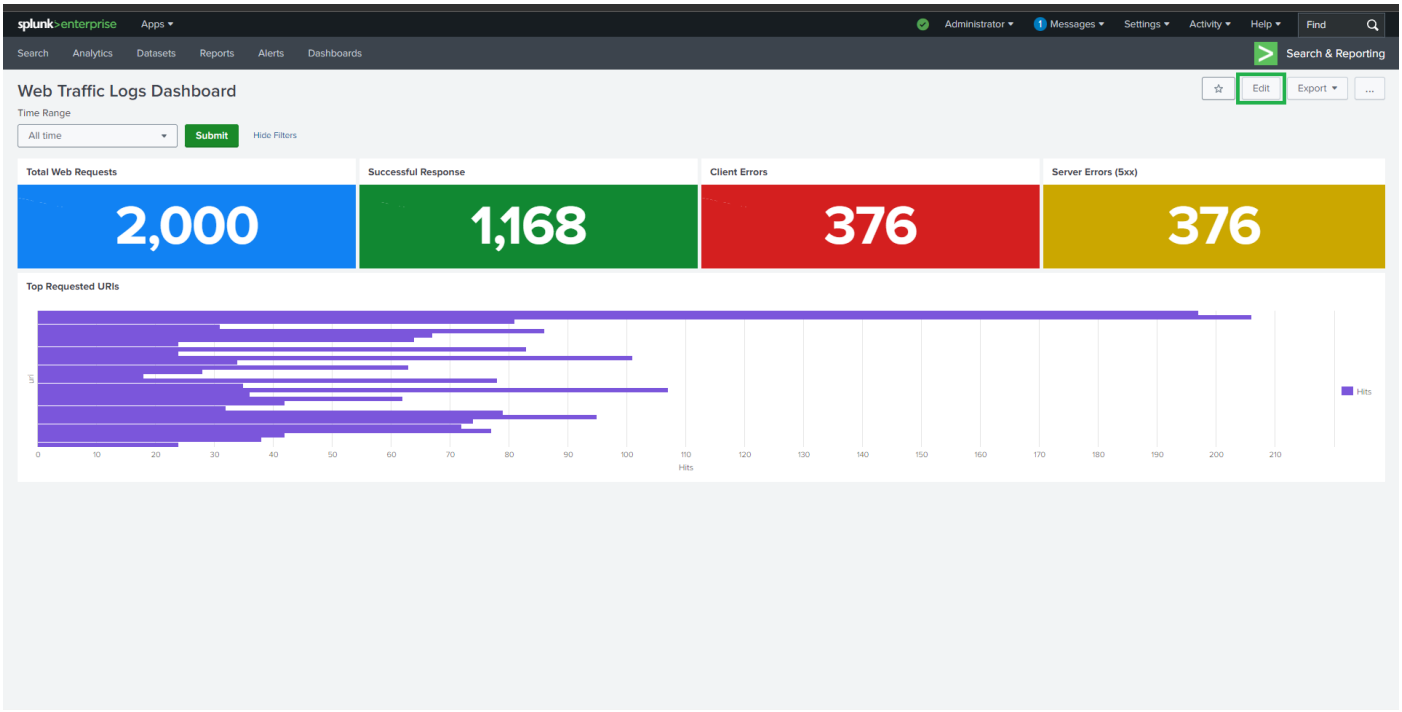

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Web Traffic Logs Dashboard
No description
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000
Successful Response
1,168
Client Errors
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (7)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
Top Requested URIs
Search String
source="apache_logs.json" host="webserver" sourcetype="_json"
| stats count AS "Hits" by uri
Run Search


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000
Successful Response
1,168
Client Errors
376
Server Errors (5xx)
376
Top Requested URIs
/?ref=http://malicious-spam-site.com


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Time Range
All time
Submit
Autorun dashboard
No title
Total Web Requests
Chart: 42
Successful Response
Client Errors
Splunk Visualizations
Find more visualizations
Bar Chart
Compare values or fields.
Search Fragment
| stats count by comparison_category
2,000
1,168
376
Top Requested URIs
/?ref=http://malicious-spam-site.com
127.0.0.1:8000/en-US/app/search/web_traffic_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&form.time_range.earliest=0&form.time_range.latest=#


Web Traffic Logs Dashboard
No description
Time Range
All time
Submit
Autorun dashboard
No title
Total Web Requests
Chart: 42
Successful Response
Client Errors
Server Errors (5xx)
2,000
1,168
376
376
Top Requested URIs
Hits


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Time Range
All time
Submit
Autorun dashboard
No title
Total Web Requests
Chart: 42
Successful Response
Client Errors
Server Errors (5xx)
2,000
1,168
376
376
Top Requested URIs
Hits


splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Web Traffic Logs Dashboard
Edit
Export
Time Range
All time
Submit
Hide Filters
Total Web Requests
2,000
Successful Response
1,168
Client Errors
376
Server Errors (5xx)
376
Top Requested URIs
Hits
0
10
20
30
40
50
60
70
80
90
100
110
120
130
140
150
160
170
180
190
200
210

7.2 Top Users by IP Address

Visualization: Bar Chart

Title: Top Users by IP Address

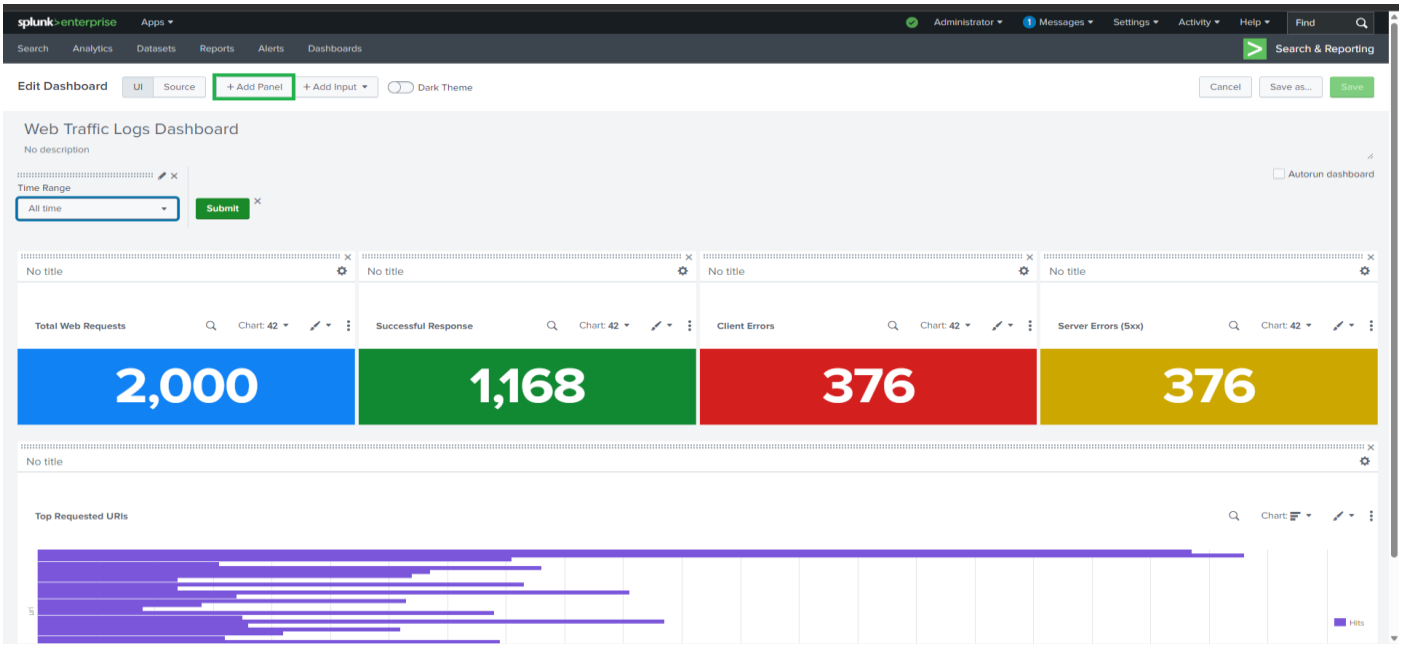
Search Query:

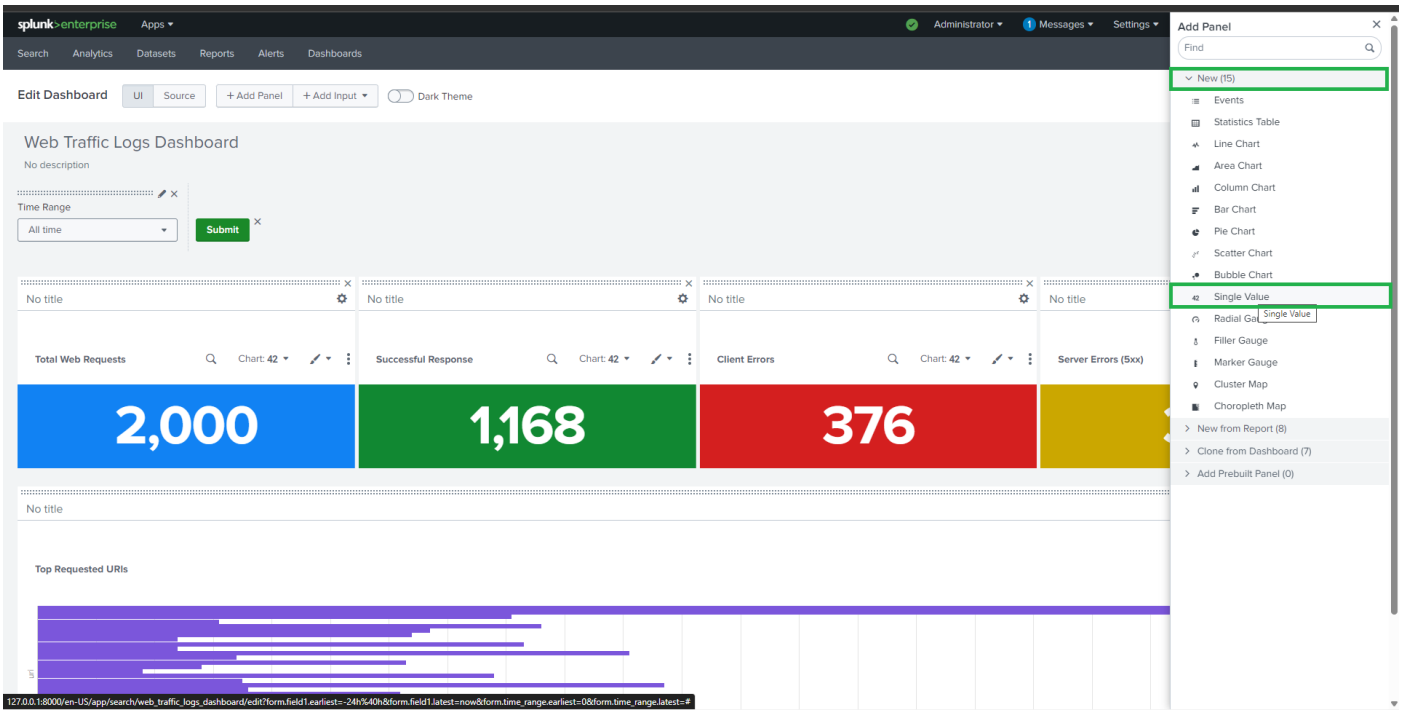
source="apache_logs.json" host="webserver" sourcetype="_json"

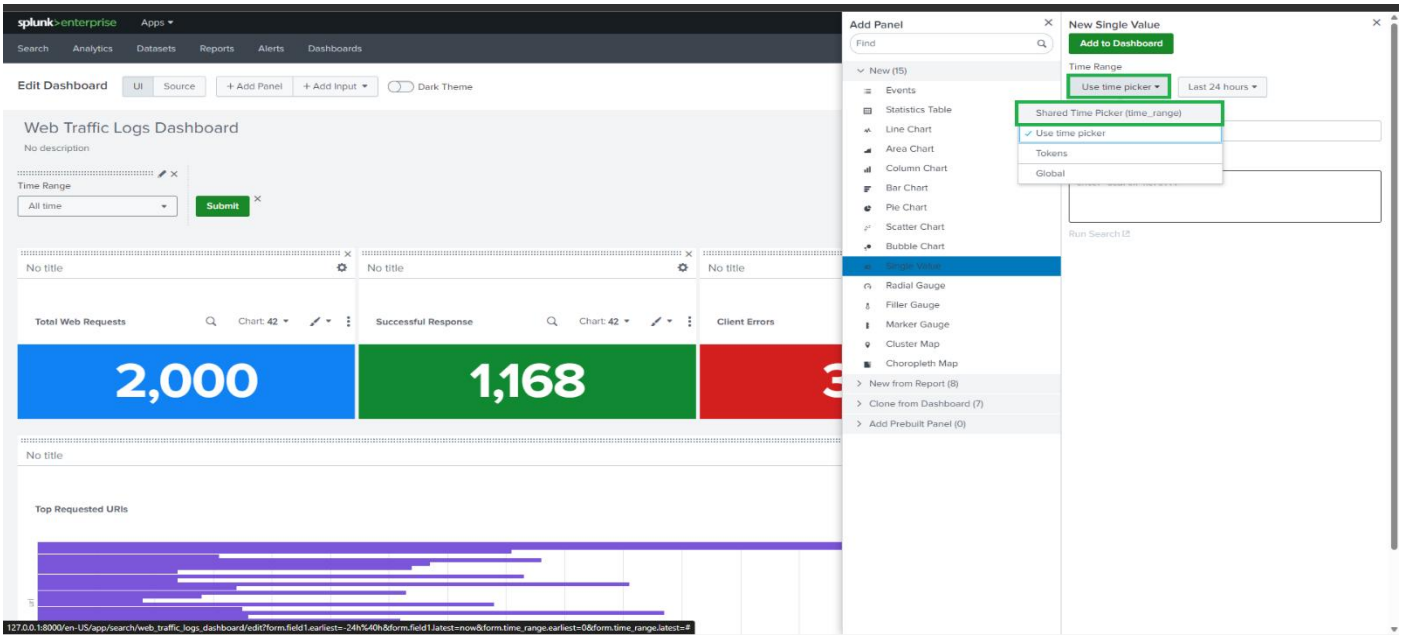
| stats count AS "Requests" by ip

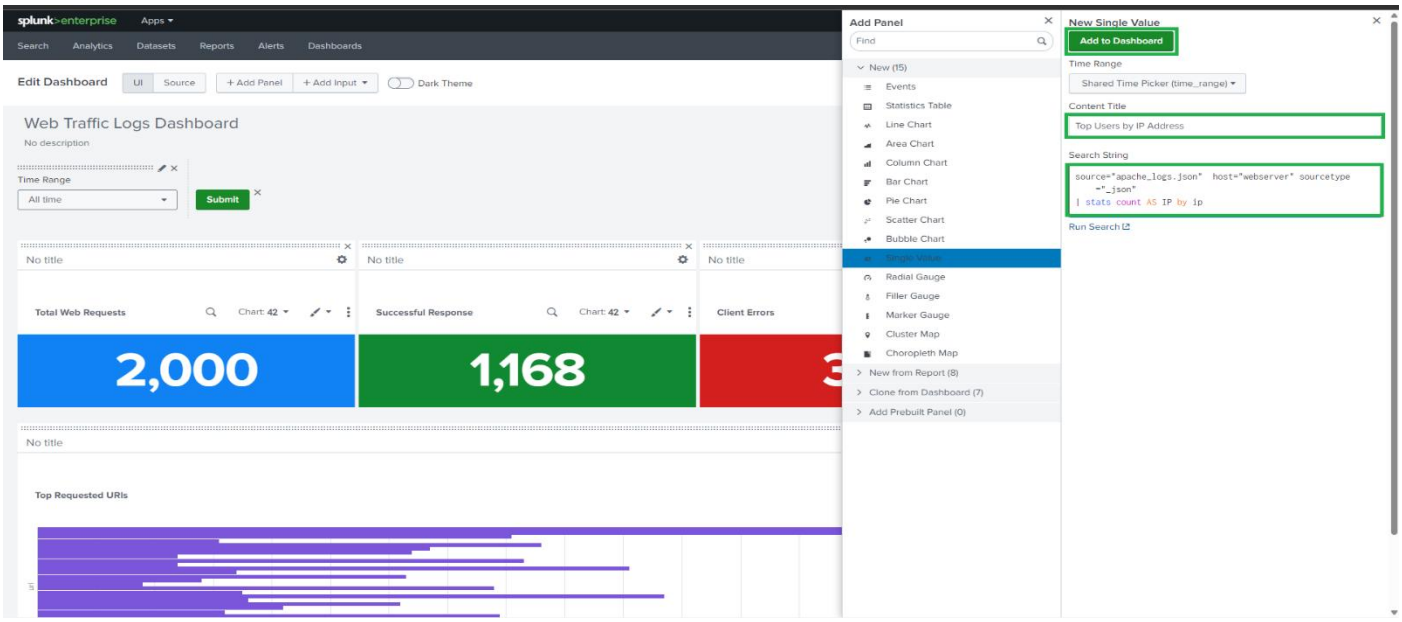
| sort - Requests

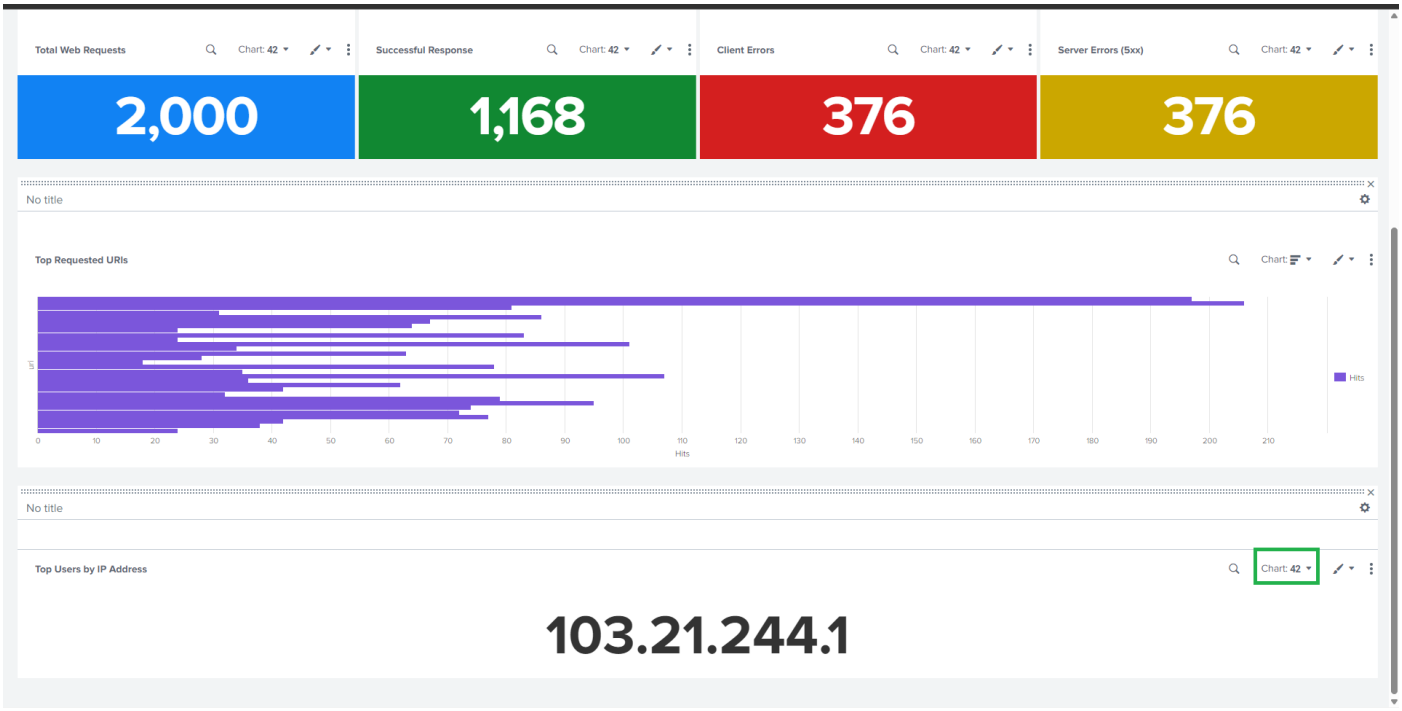
Purpose: Detects high-traffic IP addresses and potential abuse patterns.

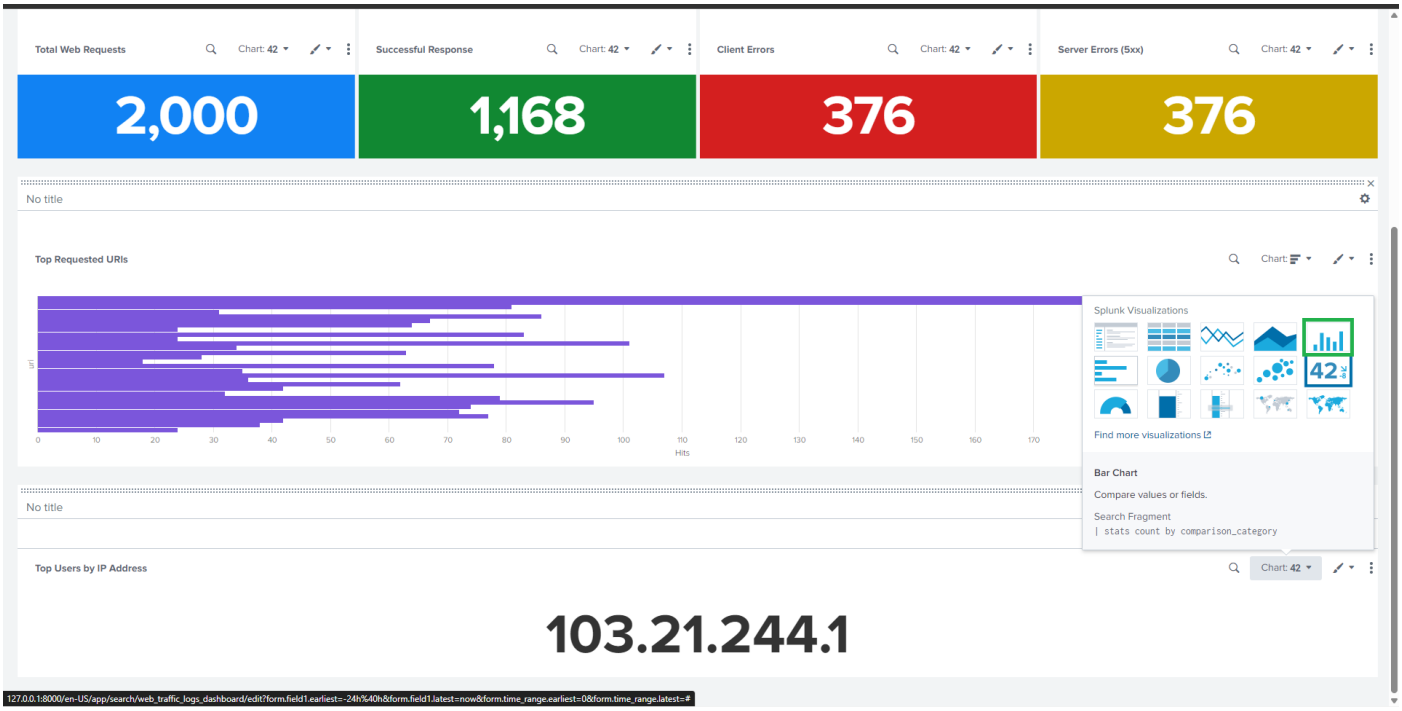


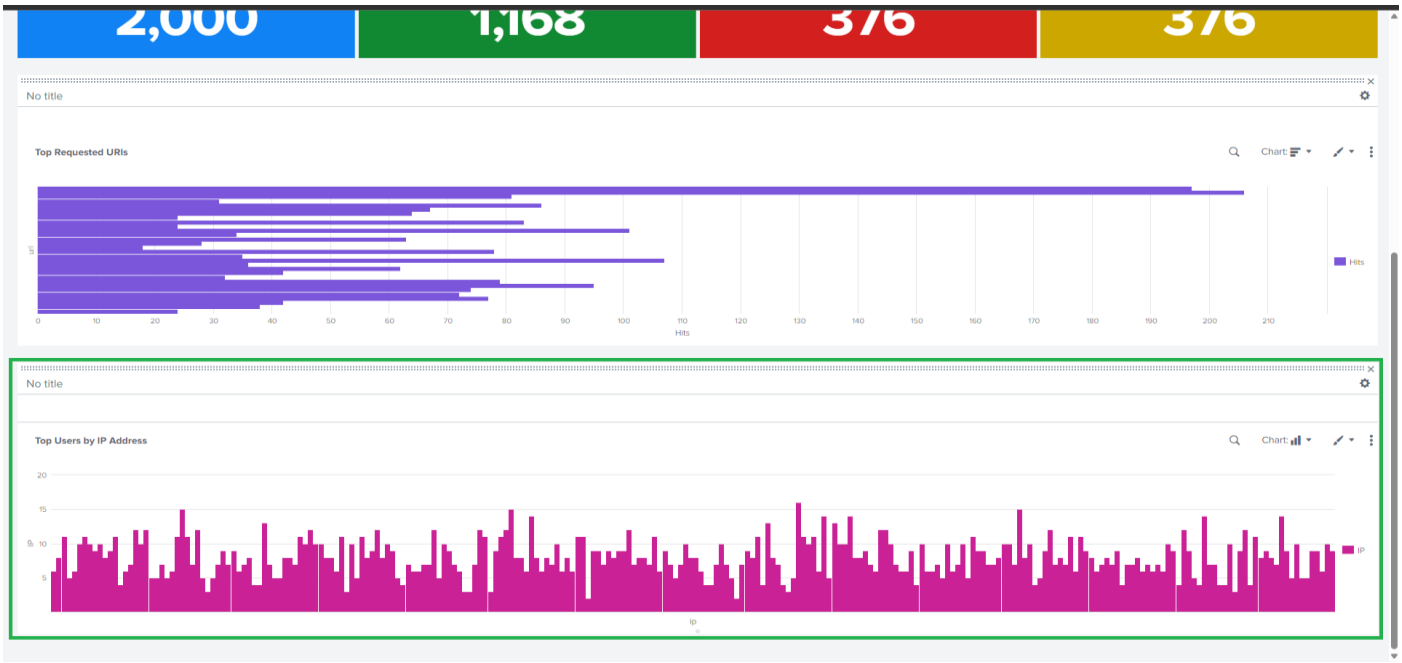


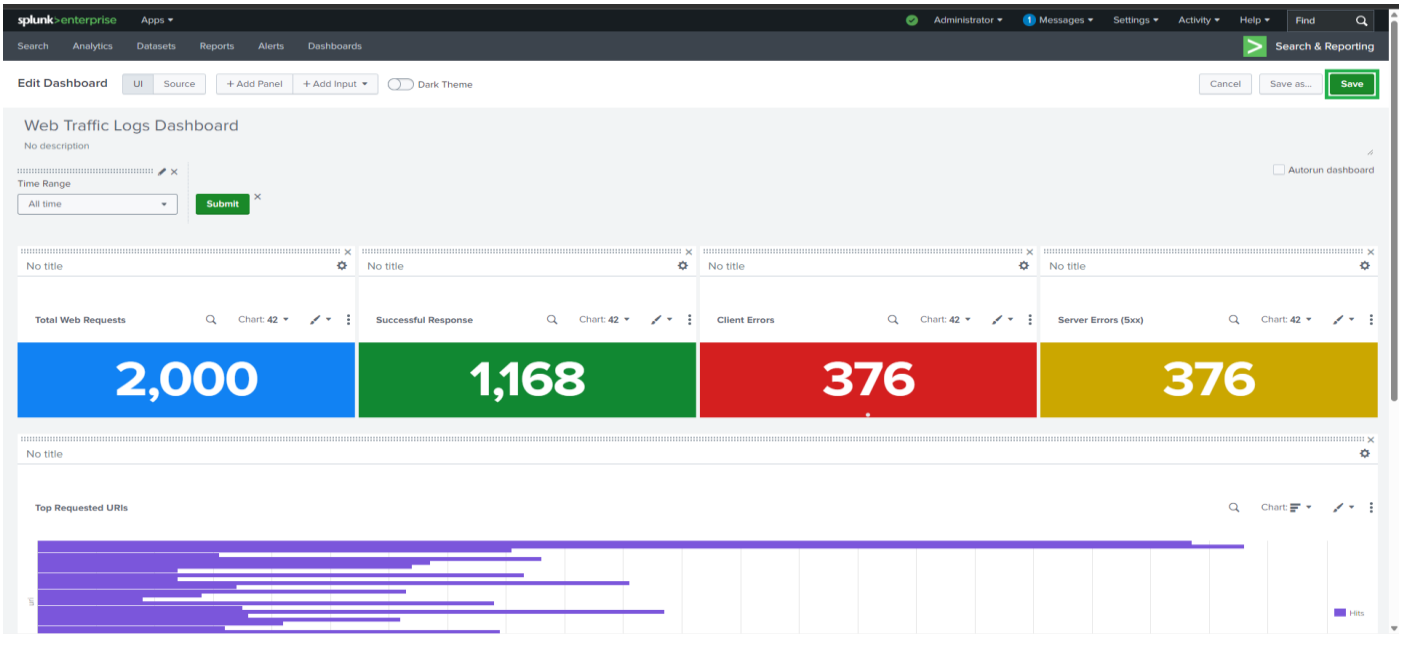

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Web Traffic Logs Dashboard
No description
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000
Successful Response
1,168
Client Errors
Top Requested URIs
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (7)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Use time picker
Last 24 hours
Shared Time Picker (time_range)
Use time picker
Tokens
Global
Run Search
127.0.0.1:8000/en-US/app/search/web_traffic_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&form.time_range.earliest=0&form.time_range.latest=#

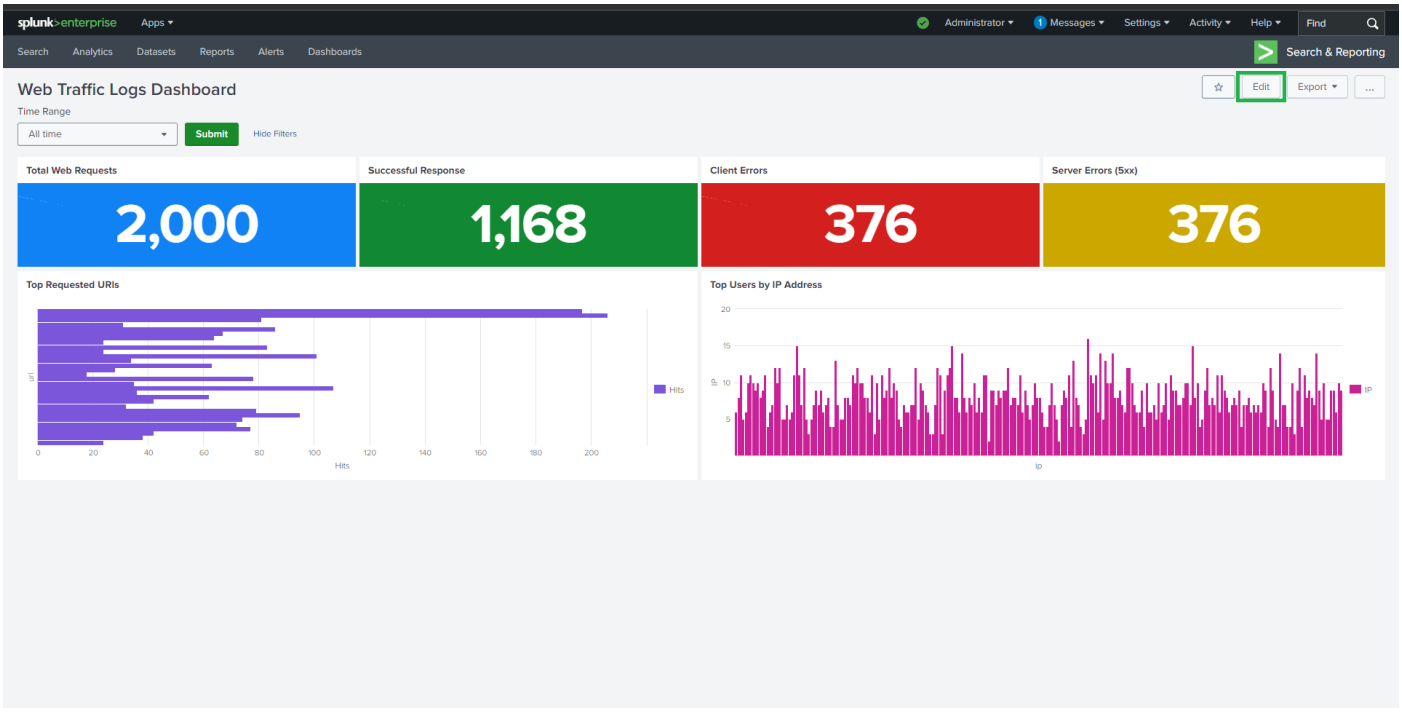

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Web Traffic Logs Dashboard
No description
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000
Successful Response
1,168
Client Errors
Top Requested URIs
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (7)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
Top Users by IP Address
Search String
source="apache_logs.json" host="webserver" sourcetype="_json"
| stats count AS IP by ip
Run Search


Total Web Requests
Chart: 42
2,000
Successful Response
1,168
Client Errors
376
Server Errors (5xx)
376
No title
Top Requested URIs
Chart:
Hits
0
10
20
30
40
50
60
70
80
90
100
110
120
130
140
150
160
170
180
190
200
210
No title
Top Users by IP Address
Chart: 42
103.21.244.1


Total Web Requests
Chart: 42
2,000
Successful Response
Chart: 42
1,168
Client Errors
Chart: 42
376
Server Errors (5xx)
Chart: 42
376
No title
Top Requested URIs
Chart:
Splunk Visualizations
Find more visualizations
Bar Chart
Compare values or fields.
Search Fragment
| stats count by comparison_category
No title
Top Users by IP Address
Chart: 42
103.21.244.1
127.0.0.1:8000/en-US/app/search/web_traffic_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&form.time_range.earliest=0&form.time_range.latest=#


No title
Top Requested URIs
Chart:
Hits
No title
Top Users by IP Address
Chart:
IP


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000
Successful Response
Chart: 42
1,168
Client Errors
Chart: 42
376
Server Errors (5xx)
Chart: 42
376
No title
Top Requested URIs
Chart:
Hits


splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Web Traffic Logs Dashboard
Edit
Export
Time Range
All time
Submit
Hide Filters
Total Web Requests
2,000
Successful Response
1,168
Client Errors
376
Server Errors (5xx)
376
Top Requested URIs
Hits
Top Users by IP Address
IP

8. Task 3: Web Traffic by Client IP (Geographic View)

Choropleth Map Panel

Visualization: Choropleth Map

Title: Web Traffic by Client IP Addresses

Search Query:

source="apache_logs.json" host="webserver" sourcetype="_json" method=GET

| table ip

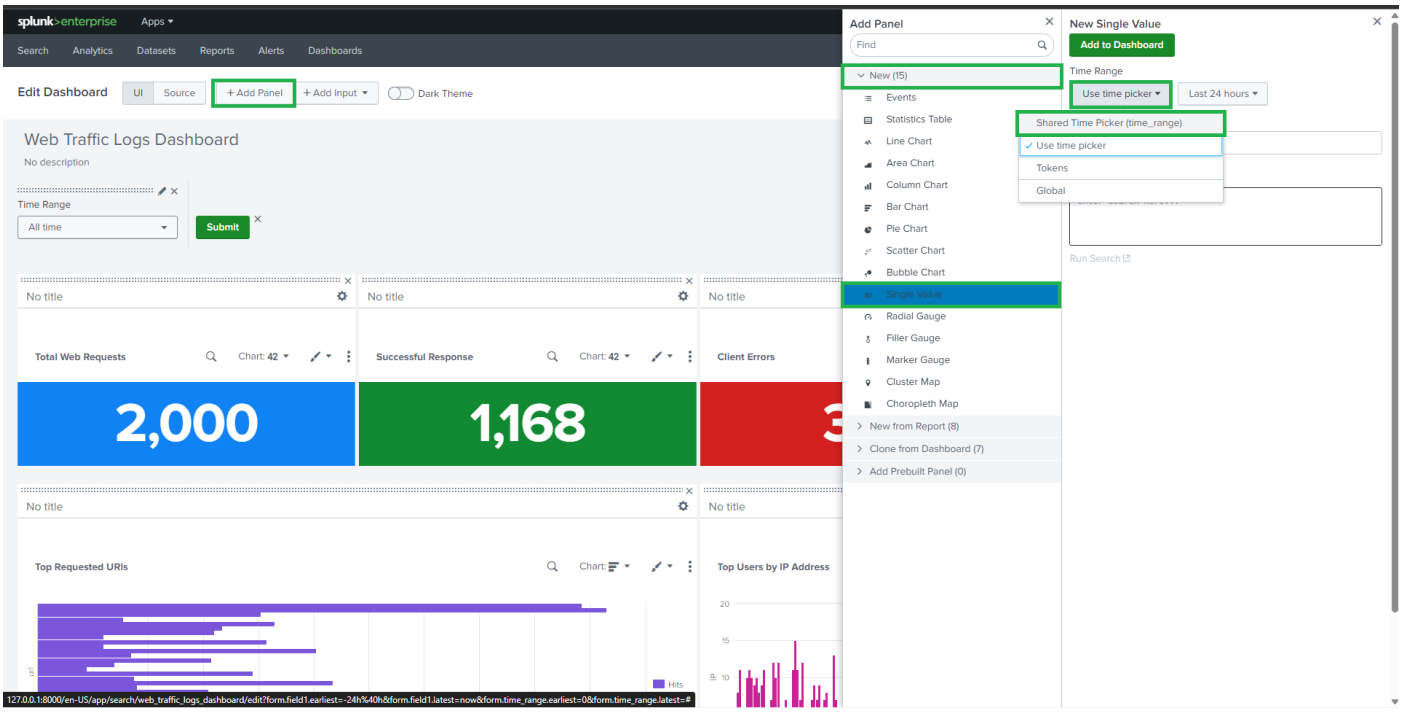
| iplocation ip

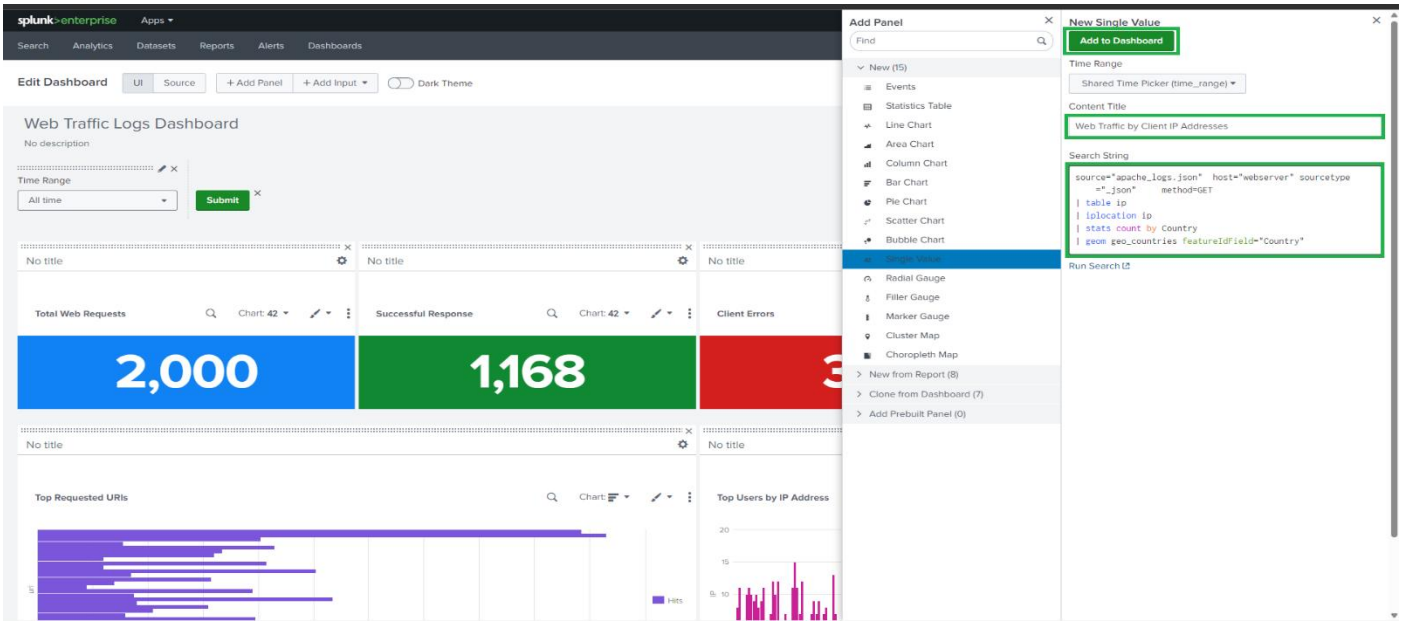
| stats count by Country

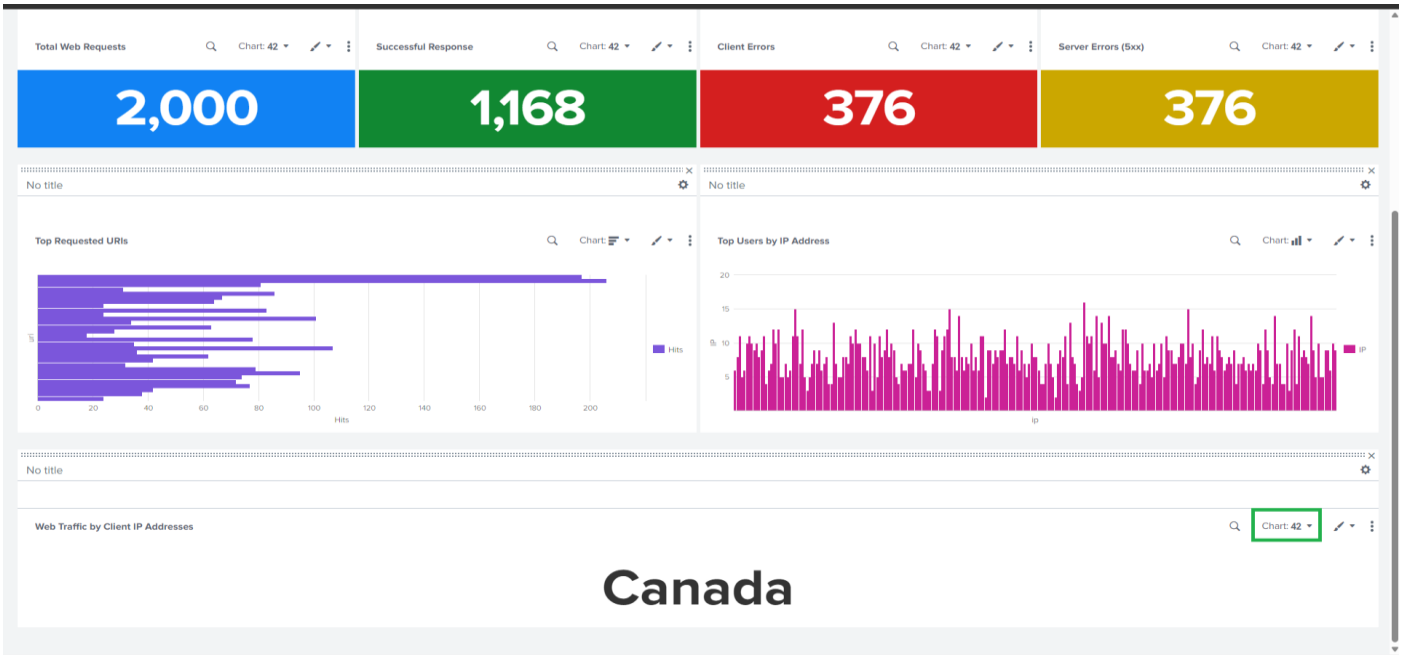
| geom geo_countries featureIdField="Country"

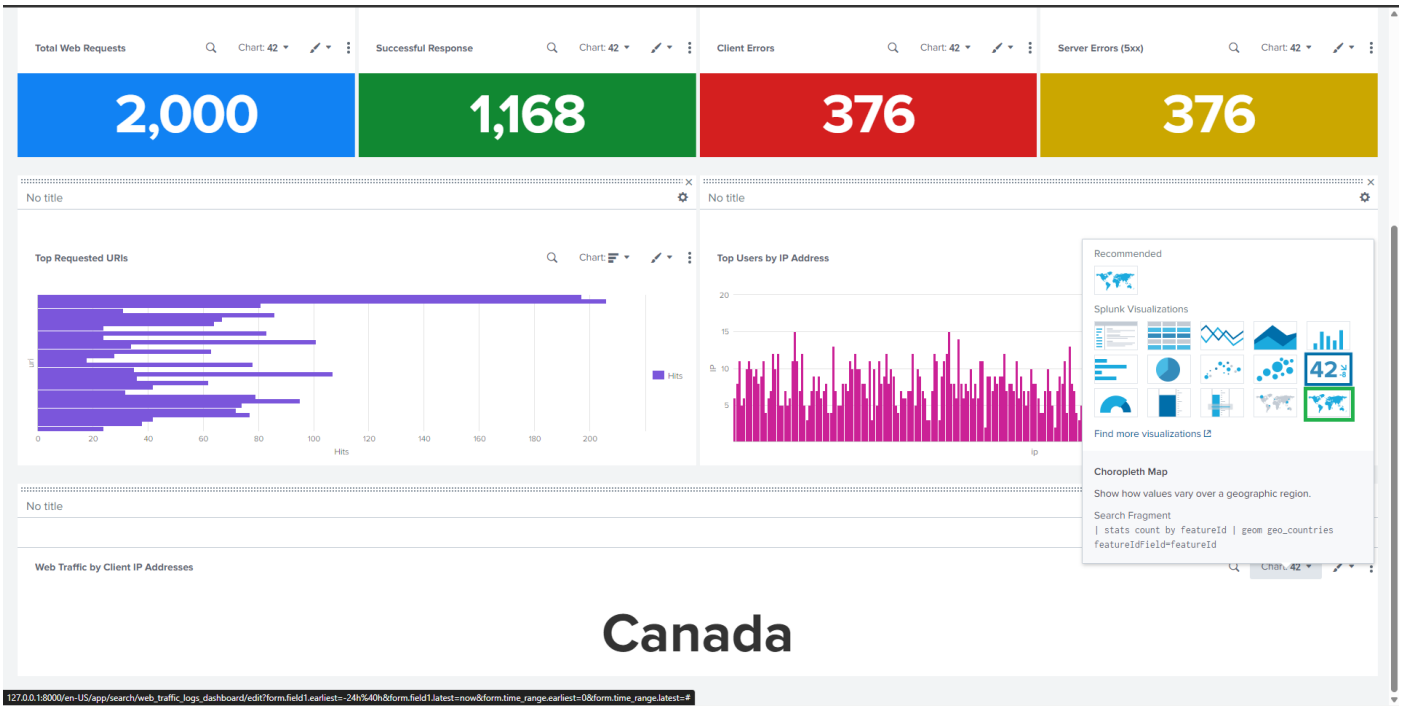
Purpose:

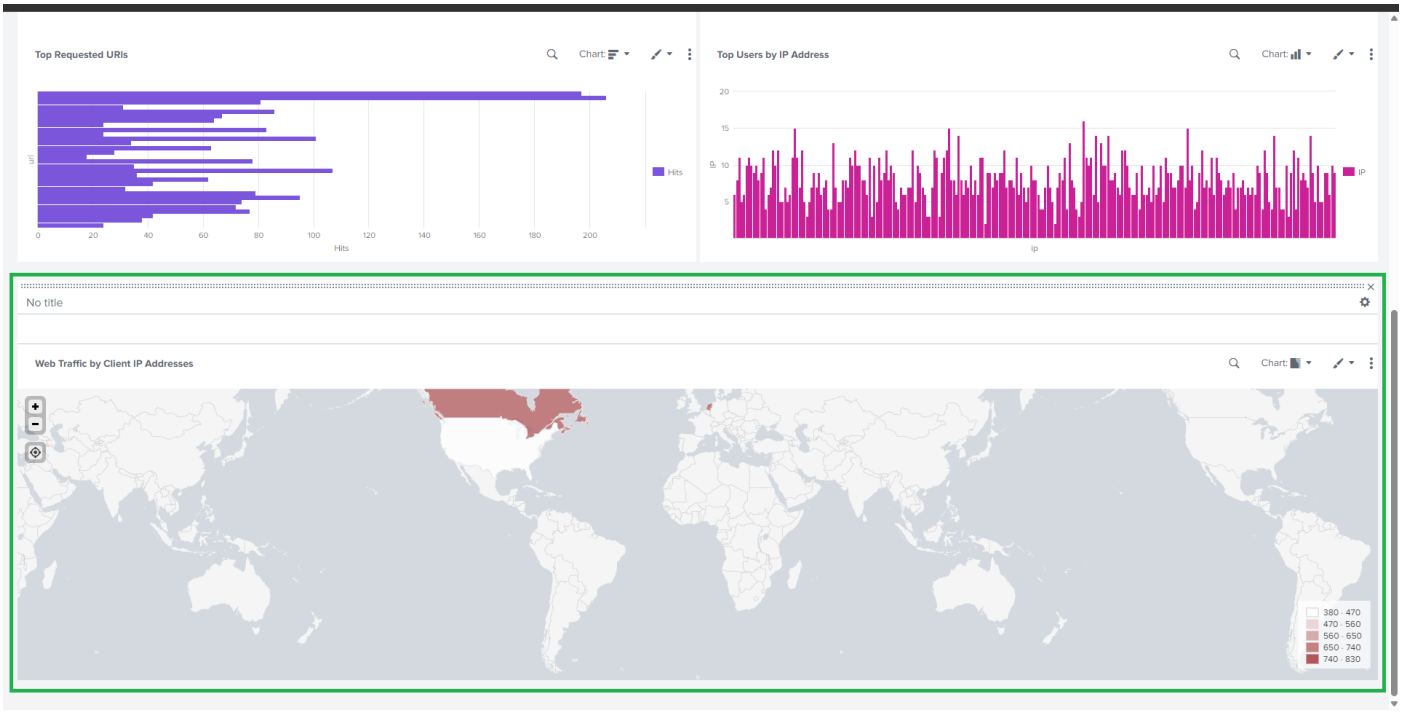
- Converts IP addresses into geographic locations
- Visualizes traffic distribution by country
- Useful for detecting suspicious geographic traffic



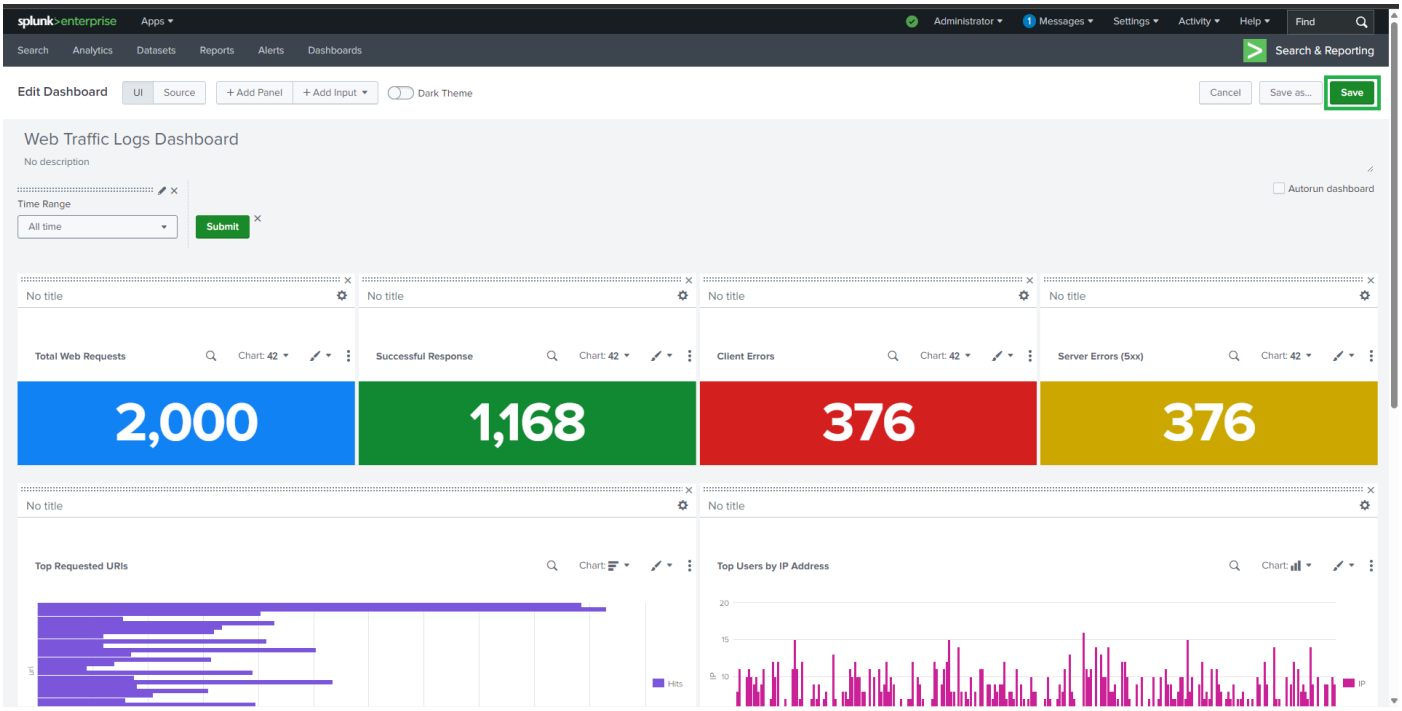

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Web Traffic Logs Dashboard
No description
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000
Successful Response
1,168
Client Errors
Top Requested URIs
Top Users by IP Address
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (7)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
Web Traffic by Client IP Addresses
Search String
source="apache_logs.json" host="webserver" sourcetype="_json" method=GET
| table ip
| iplocation ip
| stats count by Country
| geom geo_countries featureIdField="Country"
Run Search


Total Web Requests
Chart: 42
2,000
Successful Response
1,168
Client Errors
376
Server Errors (5xx)
376
No title
Top Requested URIs
Hits
Top Users by IP Address
ip
Web Traffic by Client IP Addresses
Canada


Total Web Requests
Chart: 42
2,000
Successful Response
1,168
Client Errors
376
Server Errors (5xx)
376
No title
Top Requested URIs
Hits
Top Users by IP Address
ip
Recommended
Splunk Visualizations
Find more visualizations
Choropleth Map
Show how values vary over a geographic region.
Search Fragment
| stats count by featureId | geom geo_countries featureIdField=featureId
Web Traffic by Client IP Addresses
Canada
127.0.0.1:8000/en-US/app/search/web_traffic_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&form.time_range.earliest=0&form.time_range.latest=#

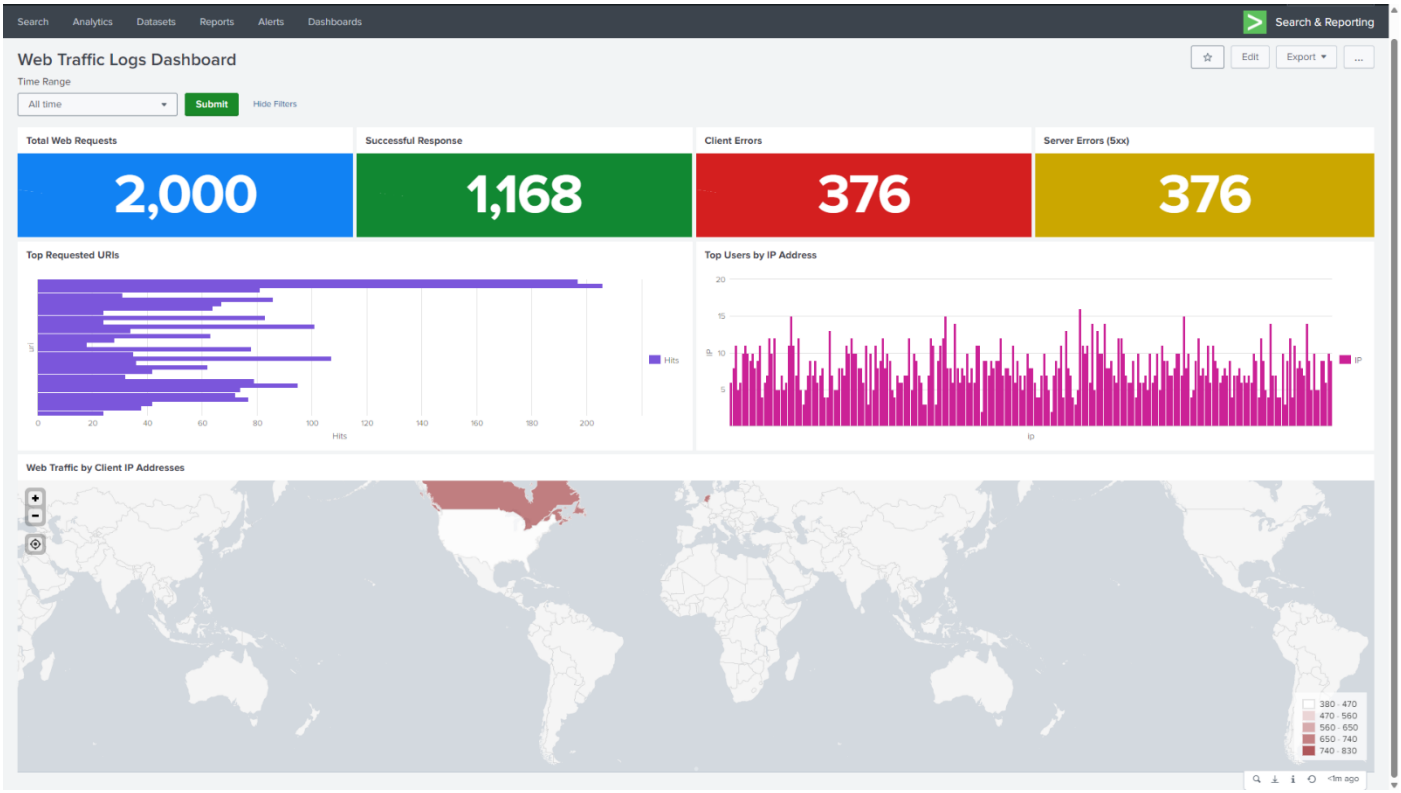

Top Requested URIs
Chart:
uri
Hits
0
20
40
60
80
100
120
140
160
180
200
Top Users by IP Address
Chart:
ip
IP
20
15
10
5
ip

No title
Web Traffic by Client IP Addresses
Chart:
380 - 470
470 - 560
560 - 650
650 - 740
740 - 830


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Web Traffic Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total Web Requests
Chart: 42
2,000
Successful Response
1,168
Client Errors
376
Server Errors (5xx)
376
Top Requested URIs
Hits
Top Users by IP Address
IP

9. Dashboard Benefits

- 📊 Centralized visibility of web activity
- 🌍 Geographic awareness of client traffic
- 🚨 Quick identification of errors and anomalies
- 🔍 Better troubleshooting and monitoring
- 🔐 Supports security analysis and threat detection



10. Conclusion

This Splunk dashboard provides a **comprehensive and interactive view of web traffic logs**. By combining statistical panels, charts, and geographic mapping, it enables administrators and security analysts to monitor system health, detect issues early, and make data-driven decisions.

The dashboard can be further enhanced by:

- Adding alerts for high error rates
- Including time-series trends
- Integrating security use cases (e.g., brute-force detection)