

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**.

The screenshot shows the Splunk Enterprise home page. At the top, there's a navigation bar with 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. Below the navigation is a 'Hello, Administrator' message and a 'Bookmarks' section. The main focus is the 'Add Data' section under 'Splunk recommended (13)'. It contains six cards: 'Add data' (Add data from a variety of common sources), 'Search your data' (Turn data into doing with Splunk search), 'Visualize your data' (Create dashboards that work for your data), 'Manage alerts' (Manage the alerts that monitor your data), 'Add team members' (Add your team members to Splunk platform), and 'Manage permissions' (Control who has access with roles). Below this is a 'Learning & resources' section with four cards: 'Product tours' (New to Splunk? Take a tour to help you on your way), 'Learn more with Splunk Docs' (Deploy, manage, and use Splunk software with comprehensive guidance), 'Get help from Splunk experts' (Actionable guidance on the Splunk Lantern Customer Success Center), and 'Extend your capabilities' (Browse thousands of apps on Splunkbase).

The screenshot shows the Splunk Enterprise search interface. At the top, there's a navigation bar with 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. The main area is divided into two sections: 'Search' on the left and 'Analyze Your Data with Table Views' on the right. The 'Search' section includes a search bar, a 'How to Search' section with links to 'Documentation', 'Tutorial', and 'Data Summary', and a 'Search History' link. The 'Table Views' section includes a 'Create Table View' button and a 'Table Views' description. A sidebar on the right lists various Splunk components and their sub-options.

The screenshot shows the Splunk Enterprise search interface with a different sidebar. The main sections are the same: 'Search' on the left and 'Analyze Your Data with Table Views' on the right. The 'Search' section includes a search bar, a 'How to Search' section with links to 'Documentation', 'Tutorial', and 'Data Summary', and a 'Search History' link. The 'Table Views' section includes a 'Create Table View' button and a 'Table Views' description. The sidebar on the right is more detailed, listing categories like KNOWLEDGE, DATA, DISTRIBUTED ENVIRONMENT, SYSTEM, and USERS AND AUTHENTICATION, each with sub-options. A URL at the bottom of the page is '127.0.0.1:8000/en-US/manage/search/adddata'.

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

splunk enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

What data do you want to send to the Splunk platform?

Follow guides for onboarding popular data sources

Cloud computing Networking Operating System Security

Get your cloud computing data in to the Splunk platform. Get your networking data in to the Splunk platform. Get your operating system data in to the Splunk platform. Get your security data in to the Splunk platform.

10 data sources 2 data sources 1 data source 3 data sources

4 data sources in total

Or get data in with the following methods

Upload Monitor Forward

files from my computer files and ports on this Splunk platform instance data from a Splunk forwarder

Local log files Modular inputs for external data sources Files - TCP/UDP - Scripts

Local structured files (e.g. CSV) Tutorial for adding data ↗

Add Data

Select Source Set Source Type Input Settings Review Done

Next >

Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More ↗

Selected File: No file selected

Select File

Drop your data file here

The maximum file upload size is 500 Mb

FAQ

What kinds of files can the Splunk platform index?
What is a source?
How do I get remote data onto my Splunk platform instance?

4. Upload the file apache_logs.json.

The screenshot shows the Splunk Add Data interface. At the top, there is a navigation bar with links like 'IB MTS study material', 'Innovator Dashboard...', 'Preplinsta : Prepare I...', 'GeeksforGeeks | You...', 'Aptitude Questions...', 'Complete guide to...', 'All Bookmarks', and user information ('Administrator', 'Messages', 'Settings', 'Activity', 'Help'). Below the navigation bar, a progress bar indicates the current step: 'Add Data' (green dot), 'Select Source' (white circle), 'Set Source Type' (white circle), 'Input Settings' (white circle), 'Review' (white circle), and 'Done' (white circle). The main area is titled 'Select Source' and contains instructions: 'Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below.' A file selection dialog from Windows File Explorer is overlaid on the interface. The dialog shows the file 'apache_logs.json' selected in the 'Downloads' folder. The 'Open' button in the dialog is highlighted with a green box. Below the dialog, there is a large input field labeled 'Drop your data file here' with the instruction 'The maximum file upload size is 500 Mb'. To the right of this input field is a 'FAQ' section with links: 'What kinds of files can the Splunk platform index?', 'What is a source?', and 'How do I get remote data onto my Splunk platform instance?'. At the bottom of the interface, there is a message: 'File Successfully Uploaded' with a checkmark icon. The URL in the browser's address bar is '127.0.0.1:8000/en-US/manage/search/adddata/methods/selectsource/input_mode=0#'. The overall theme of the interface is light gray with blue and green accents for buttons and progress indicators.

5. Set the Source Type to _json.

Source: apache_logs.json

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Format ▾ Select... ▾ Select... ▾

	_time	bytes	ip	method	protocol	referer	status	timestamp	uri	user_agent
1	9/17/25 12:00:00.000 PM	1374	185.62.57.52	GET	HTTP/1.1	-	200	17/Sep/2025:12:00:00 +0530	/upload.php	python-requests/2.25.1
2	9/17/25 12:00:02.000 PM	5195	103.21.244.54	GET	HTTP/1.1	-	200	17/Sep/2025:12:00:02 +0530	/cart/view	Mozilla/5.0 (X11; Linux x86_64)
3	9/17/25 12:00:04.000 PM	1872	66.249.66.41	GET	HTTP/1.1	-	200	17/Sep/2025:12:00:04 +0530	/cart/view	Mozilla/5.0 (compatible; Bingbot/2.0; +http://www.bing.com/bingbot.htm)
4	9/17/25 12:00:06.000 PM	870	185.62.57.82	GET	HTTP/1.1	http://malicious-spam-site.com	200	17/Sep/2025:12:00:06 +0530	/ref=http://phishingsite.net	Mozilla/5.0 (Windows NT 10.0; Win64; x64)
5	9/17/25 12:00:08.000 PM	524	103.21.244.93	GET	HTTP/1.1	-	302	17/Sep/2025:12:00:08 +0530	/contact.html	Mozilla/5.0 (Windows NT 10.0; Win64; x64)
6	9/17/25 12:00:10.000 PM	2094	185.62.57.84	GET	HTTP/1.1	http://malicious-spam-site.com	200	17/Sep/2025:12:00:10 +0530	/ref=http://phishingsite.net	Mozilla/5.0 (X11; Linux x86_64)
7	9/17/25 12:00:12.000 PM	4760	66.249.66.8	GET	HTTP/1.1	-	200	17/Sep/2025:12:00:12 +0530	/static/logo.png	AhrefsBot/7.0; +https://ahrefs.com/robot/
8	9/17/25 12:00:14.000 PM	3991	66.249.66.5	GET	HTTP/1.1	-	200	17/Sep/2025:12:00:14 +0530	/cart/view	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.htm)
9	9/17/25 12:00:16.000 PM	4290	185.62.57.36	GET	HTTP/1.1	-	200	17/Sep/2025:12:00:16 +0530	/products.php?id=10 UNION SELECT username,password FROM users	python-requests/2.25.1
10	9/17/25 12:00:18.000 PM	791	185.62.57.86	GET	HTTP/1.1	http://malicious-spam-site.com	200	17/Sep/2025:12:00:18 +0530	/ref=http://malicious-spam-site.com	AhrefsBot/7.0; +https://ahrefs.com/robot/
11	9/17/25 12:00:20.000 PM	860	103.21.244.93	GET	HTTP/1.1	-	302	17/Sep/2025:12:00:20 +0530	/static/style.css	Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X)
12	9/17/25	736	103.21.244.11	GET	HTTP/1.1	-	401	17/Sep/2025:12:00:22	/secret/admin	Mozilla/5.0 (X11; Linux x86_64)

6. Assign Host = webserver.

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Constant value
 Regular expression on path
 Segment in path

Host field value

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index [Default](#) [Create a new index](#)

FAQ

- How do indexes work?
- How do I know when to create or use multiple indexes?

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Constant value
 Regular expression on path
 Segment in path

Host field value

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index [Default](#) [Create a new index](#)

FAQ

- How do indexes work?
- How do I know when to create or use multiple indexes?

7. Review settings and submit the data.

8. Verify ingestion using a basic search:

9. source="apache_logs.json"

The screenshot shows the Splunk Add Data interface in the Review step. The top navigation bar includes links for Apps, Settings, Activity, Help, and Find. The main header says "Add Data" and the sub-header is "Review". A progress bar at the top shows five steps: Select Source, Set Source Type, Input Settings, Review, and Done. The "Review" step is highlighted with a green circle. Below the progress bar, there is a summary table with the following data:

Input Type	Uploaded File
File Name	apache_logs.json
Source Type	json
Host	webserver
Index	Default

At the bottom right of the review section is a green "Submit" button.

The screenshot shows the Splunk Add Data interface in the Done step. The top navigation bar and progress bar are identical to the previous screenshot. The main content area displays a success message: "✓ File has been uploaded successfully." followed by the instruction "Configure your inputs by going to Settings > Data Inputs". Below this message are several buttons with descriptions:

- Start Searching**: Search your data now or see examples and tutorials.
- Extract Fields**: Create search-time field extractions. Learn more about fields.
- Add More Data**: Add more data inputs now or see examples and tutorials.
- Download Apps**: Apps help you do more with your data. Learn more.
- Build Dashboards**: Visualize your searches. Learn more.

4. Dashboard Creation

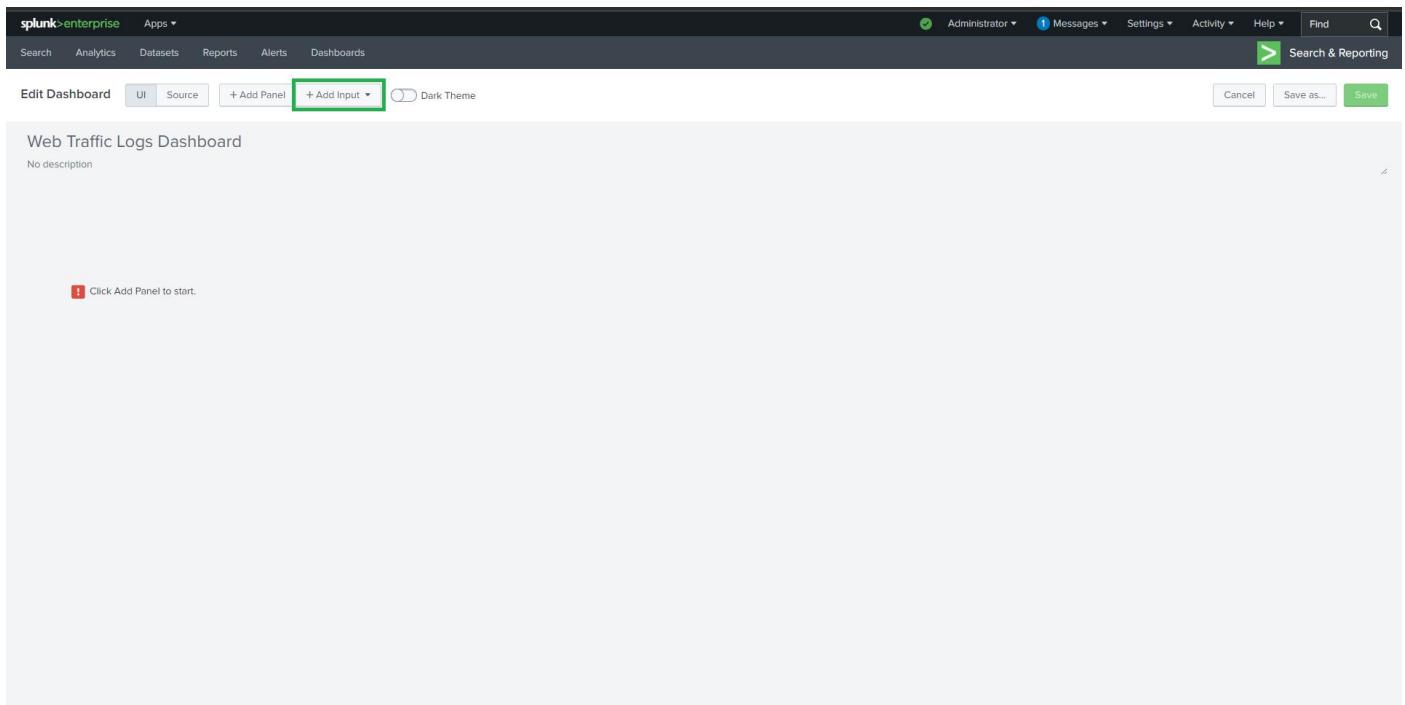
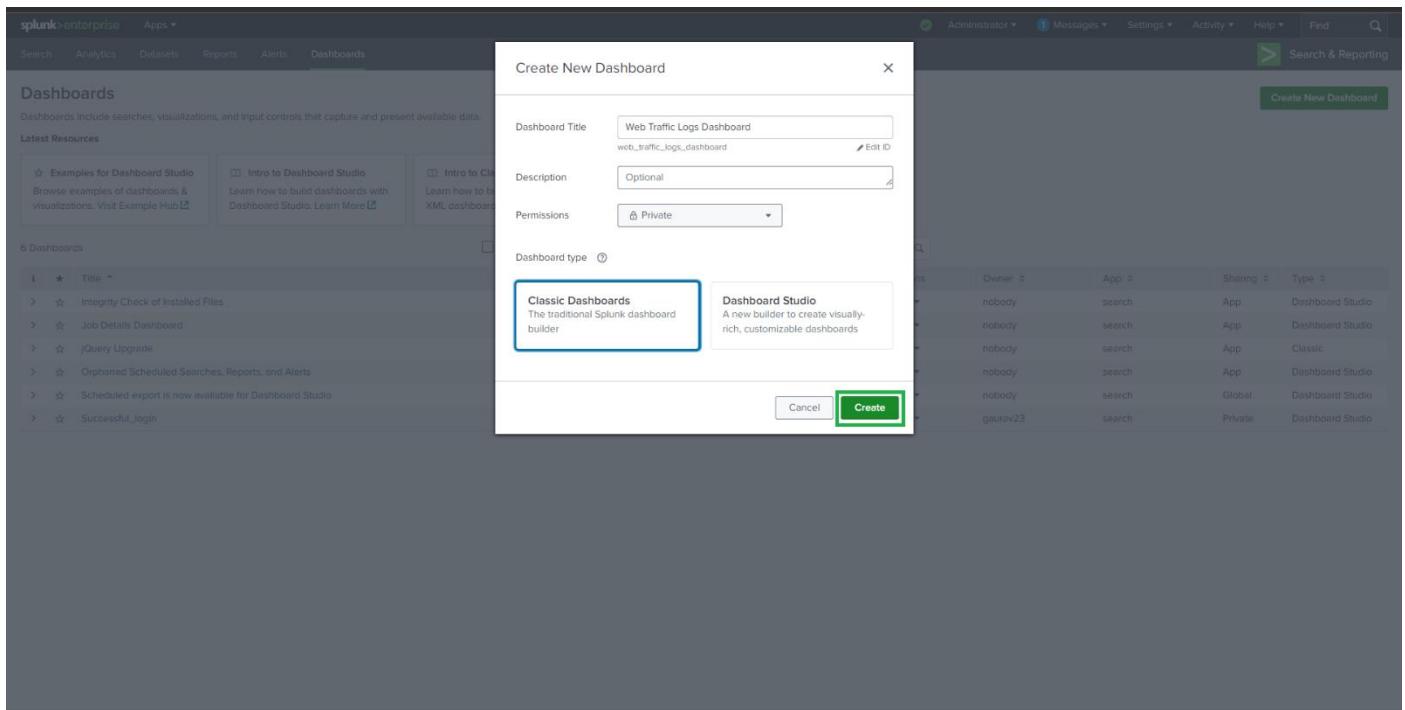
4.1 Create a New Dashboard

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)

The screenshot shows the Splunk Enterprise interface with the 'Dashboards' tab selected. At the top right, there is a green button labeled 'Create New Dashboard'. Below it, a table lists existing dashboards. One dashboard, 'Successful_login', is highlighted with a green border. The table columns include Title, Actions, Owner, App, Sharing, and Type.

Title	Actions	Owner	App	Sharing	Type
Integrity Check of Installed Files	Edit	nobody	search	App	Dashboard Studio
Job Details Dashboard	Edit	nobody	search	App	Dashboard Studio
jQuery Upgrade	Edit	nobody	search	App	Classic
Orphaned Scheduled Searches, Reports, and Alerts	Edit	nobody	search	App	Dashboard Studio
Scheduled export is now available for Dashboard Studio	Edit	nobody	search	Global	Dashboard Studio
Successful_login	Edit	gaurav23	search	Private	Dashboard Studio

The screenshot shows the 'Create New Dashboard' dialog box. The 'Dashboard Title' field is filled with 'Required'. The 'Permissions' dropdown is set to 'Private'. The 'Dashboard type' section shows two options: 'Classic Dashboards' (selected) and 'Dashboard Studio'. A detailed description of 'Classic Dashboards' is provided. At the bottom right of the dialog box are 'Cancel' and 'Create' buttons.



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**.

The screenshot shows the Splunk Enterprise interface for editing a dashboard. The top navigation bar includes links for 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. On the right side of the header are user profile, message center, settings, activity, help, and search functions. Below the header, the main area is titled 'Edit Dashboard' and shows a 'Web Traffic Logs Dashboard' with a note 'No description'. A modal window is open, showing the 'Add Input' dropdown menu. The 'Time' option is highlighted with a green border. Other options listed include 'Text', 'Radio', 'Dropdown', 'Checkbox', 'Multiselect', 'Link List', 'Text', and 'Submit'. At the bottom of the modal, there is a note 'Click Add Panel to start.' and buttons for 'Cancel', 'Save as...', and 'Save'.

splunk-enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾ Search & Reporting

Search Analytics Datasets Reports Alerts Dashboards

Edit Dashboard UI Source + Add Panel + Add Input Dark Theme Cancel Save as... Save

Web Traffic Logs Dashboard

No description

Last 24 hours

Click Add Panel to start.

Autorun dashboard

splunk-enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾ Search & Reporting

Search Analytics Datasets Reports Alerts Dashboards

Edit Dashboard UI Source + Add Panel + Add Input Dark Theme Cancel Save as... Save

Web Traffic Logs Dashboard

No description

General

T Text

Radio

Label

Search on Change

Token Options

Token ? field1

Default ? Last 24 hours

Time

Cancel Apply

Autorun dashboard

splunk-enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾ Search & Reporting

Search Analytics Datasets Reports Alerts Dashboards

Edit Dashboard UI Source + Add Panel + Add Input Dark Theme Cancel Save as... Save

Web Traffic Logs Dashboard

No description

General

T Text

Radio

Label Time Range

Search on Change

Token Options

Token ? time_range

Default ? Last 24 hours

Time

Cancel Apply

Autorun dashboard

splunk enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾

Search Analytics Datasets Reports Alerts Dashboards

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 ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾

Search Analytics Datasets Reports Alerts Dashboards

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.

T Text Radio Dropdown Checkbox Multiselect Link List Time Submit

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 ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾

Search Analytics Datasets Reports Alerts Dashboards

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.

This screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with links for 'splunk>enterprise', 'Apps', 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. On the right side of the header, there are links for 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a search bar. Below the header, the title 'Web Traffic Logs Dashboard' is displayed. Underneath the title, there's a 'Time Range' dropdown set to 'Last 24 hours', a 'Submit' button, and a 'Hide Filters' link. To the right of these controls is a green-bordered 'Edit' button. At the bottom of the dashboard area, there's a message: 'This dashboard has no panels. Start editing to add panels.'

This screenshot shows the 'Edit Dashboard' mode in the Splunk Enterprise interface. The top navigation bar is identical to the previous screenshot. Below it, the title 'Web Traffic Logs Dashboard' is followed by a 'No description' field. Underneath, there are 'Time Range' and 'Submit' buttons, along with a 'Dark Theme' toggle switch. At the top of the main content area, there are tabs for 'UI' (highlighted with a green border), 'Source', '+ Add Panel' (also highlighted with a green border), '+ Add Input', and a 'Dark Theme' switch. In the bottom right corner of the main area, there are 'Cancel', 'Save as...', and 'Save' buttons. A small note at the bottom left says 'Click Add Panel to start.'

splunk>enterprise Apps ▾

Administrator ▾ 1 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 ▾ 1 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 (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 ▾

Administrator ▾ 1 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 (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.

New Panel Find

New (15)

- Events
- Statistics Table
- Line Chart
- Area Chart
- Column Chart
- Bar Chart
- Pie Chart
- Scatter Chart
- Bubble Chart

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 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.

New 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) Content Title optional Search String 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.

New 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) Content Title Total Web Requests Search String source="apache_logs.json" host="webserver" sourcetype="json" | stats count AS "Total Web Requests" Run Search

spunk-enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾ 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

No title

Total Web Requests Chart: 42

0

spunk-enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾ 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

Presets

Real-time	Relative	Last 15 minutes
30 second window	Today	Last 60 minutes
1 minute window	Week to date	Last 4 hours
5 minute window	Business week to date	Last 24 hours
30 minute window	Month to date	Last 7 days
1 hour window	Year to date	Last 30 days
All time (real-time)	Yesterday	
	Previous week	
	Previous business week	
	Previous month	
	Previous year	

> Relative
> Real-time
> Date Range
> Date & Time Range
> Advanced

0

spunk-enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾ Search & Reporting

Edit Dashboard UI Source + Add Panel + Add Input Dark Theme Cancel Save as... Save

Web Traffic Logs Dashboard

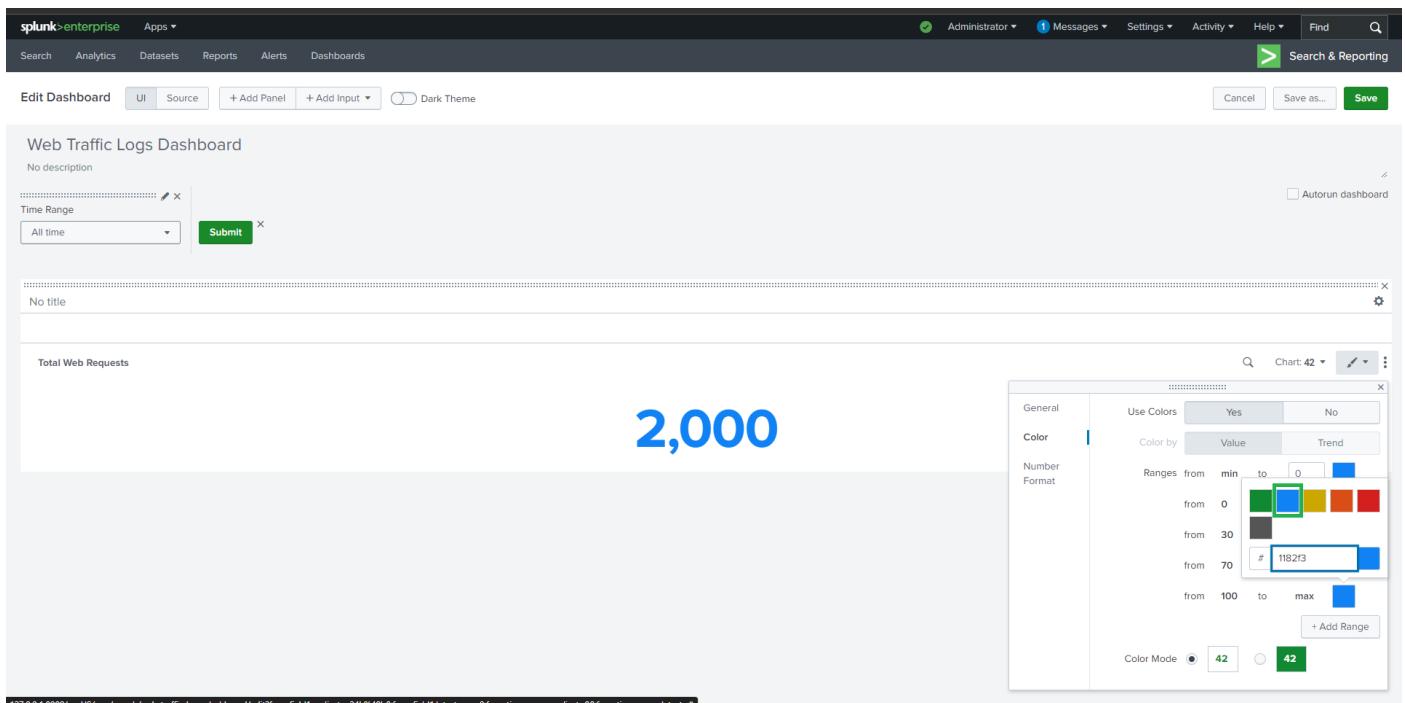
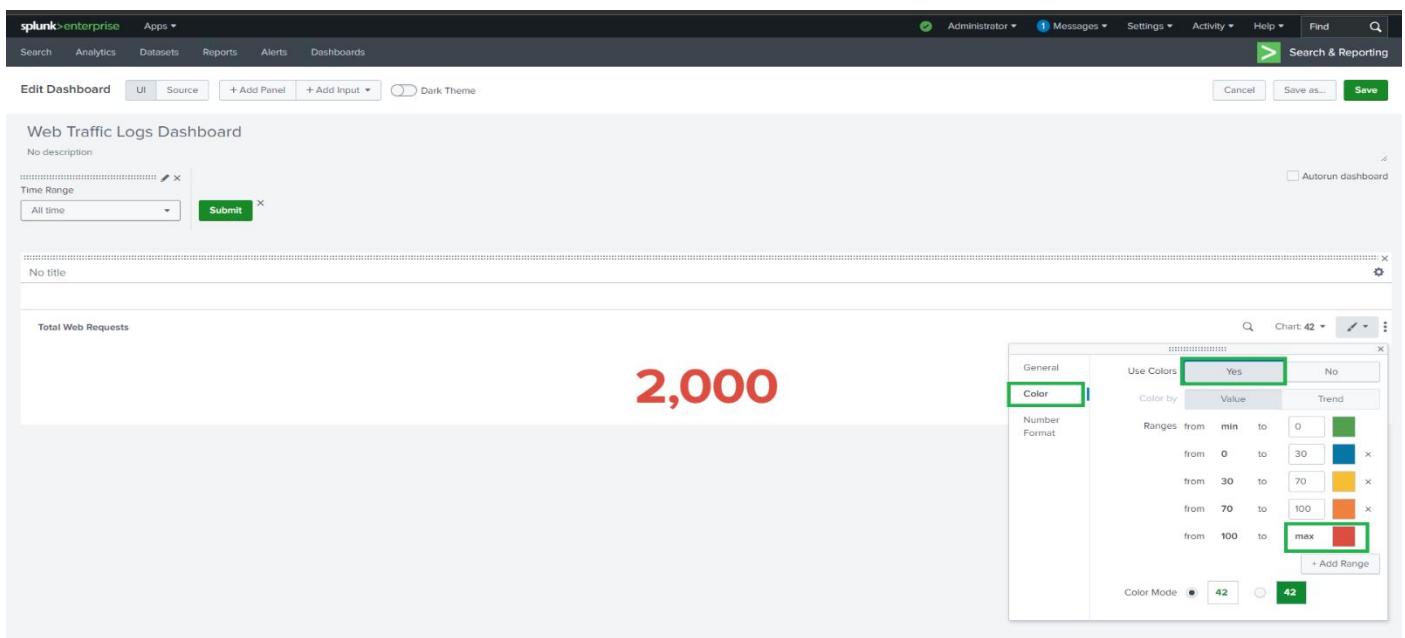
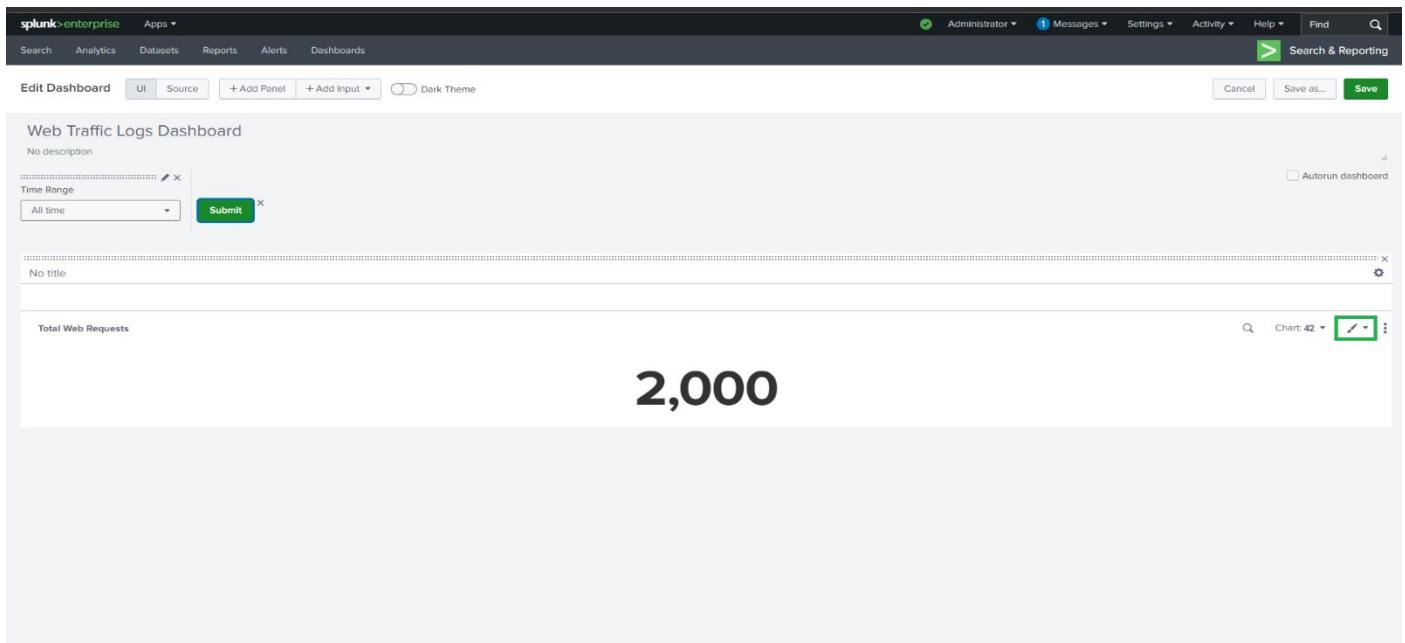
No description

Time Range All time Submit Autorun dashboard

No title

Total Web Requests Chart: 42

0



splunk-enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾ Search & Reporting

Search Analytics Datasets Reports Alerts Dashboards

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

No title

Total Web Requests

2,000

General Use Colors Yes No

Color Color by Value Trend

Number Format 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

splunk-enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾ Search & Reporting

Search Analytics Datasets Reports Alerts Dashboards

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

No title

Total Web Requests

2,000

Format visualization

splunk-enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾ Search & Reporting

Search Analytics Datasets Reports Alerts Dashboards

Web Traffic Logs Dashboard

Time Range All time Submit Hide Filters

Edit Export ...

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.

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with links for 'splunk>enterprise', 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. On the right side of the header, there are links for 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a 'Find' search bar. Below the header, there are buttons for 'Edit Dashboard', 'UI', 'Source', '+ Add Panel' (which is highlighted with a green box), '+ Add Input', and 'Dark Theme'. To the right of these are 'Cancel', 'Save as...', and 'Save' buttons. The main content area is titled 'Web Traffic Logs Dashboard' with a note 'No description'. It contains a 'Time Range' section with a dropdown set to 'All time' and a 'Submit' button. Below this is a large blue panel with the text 'Total Web Requests' and a large white number '2,000'. In the top right corner of the dashboard area, there's a small note 'Autorun dashboard' with a checkbox. The bottom right of the dashboard has a 'Chart: 42' indicator and a gear icon.

This screenshot shows the same Splunk interface as above, but with the 'Add Panel' sidebar open on the right. The sidebar has a search bar at the top. Below it, there's a list of visualization types under a heading 'New (15)'. The 'Single Value' option is highlighted with a green box. Other items in the list include 'Events', 'Statistics Table', 'Line Chart', 'Area Chart', 'Column Chart', 'Bar Chart', 'Pie Chart', 'Scatter Chart', 'Bubble Chart', 'Radial Gauge', 'Filler Gauge', 'Marker Gauge', 'Cluster Map', and 'Choropleth Map'. At the bottom of the sidebar, there are three more options: 'New from Report (8)', 'Clone from Dashboard (7)', and 'Add Prebuilt Panel (0)'. The URL at the bottom of the page is 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=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 All time Submit

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

Shared Time Picker (time_range)
Use time picker

Run Search

127.0.0.1:8000/en-US/app/search/web_traffic_logs_dashboard/edit?form.field1.earliest=-24h%40s&form.field1.latest=now&form.time_range.earliest=0s&form.time_range.latest=s

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

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

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 ▾

Search Analytics Datasets Reports Alerts Dashboards

Administrator Messages Settings Activity Help Find

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

Total Web Requests

2,000

Autorun dashboard

No title

Successful Response

1,168

spunk-enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 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

No title

Total Web Requests

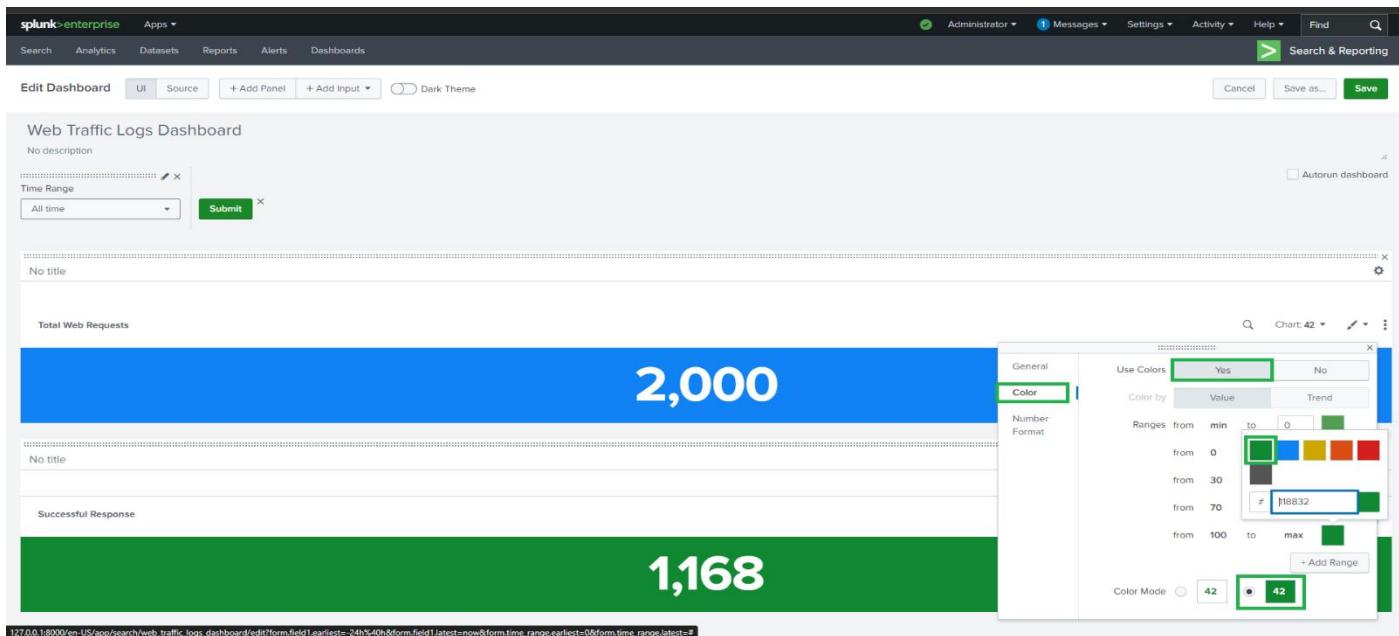
2,000

No title

Successful Response

1,168

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=0



spunk-enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 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

No title

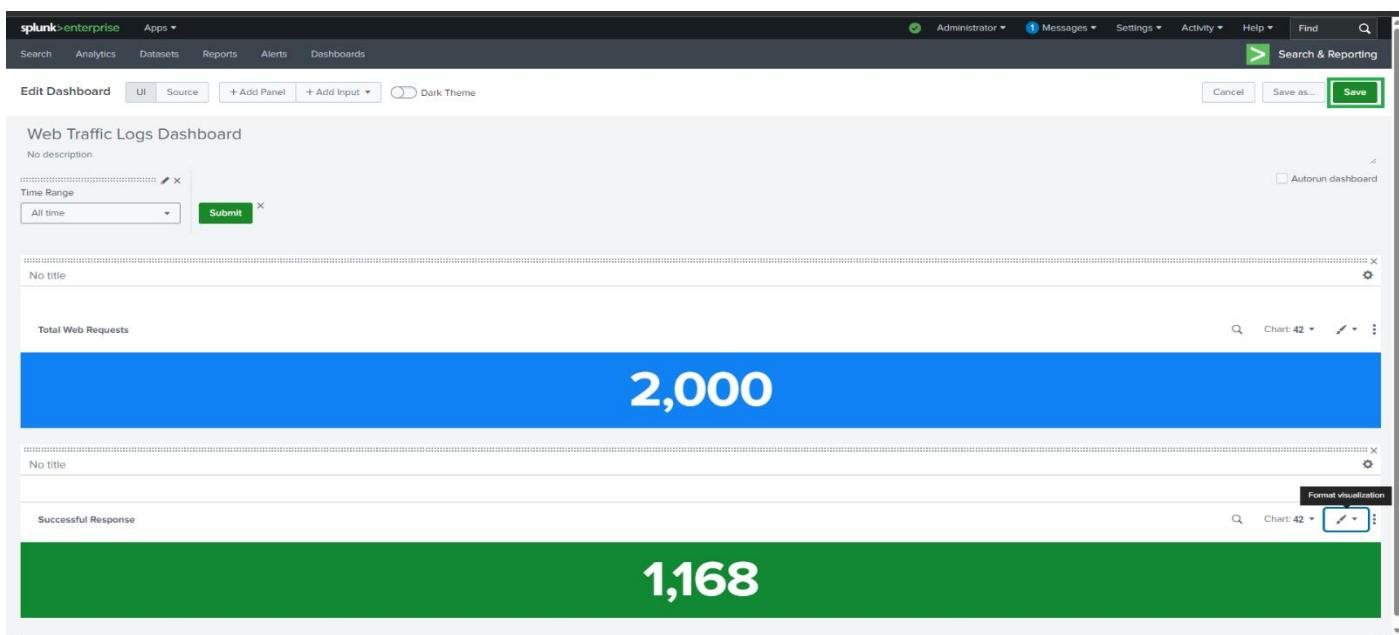
Total Web Requests

2,000

No title

Successful Response

1,168



spunk-enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Search & Reporting

Edit Export ...

Web Traffic Logs Dashboard

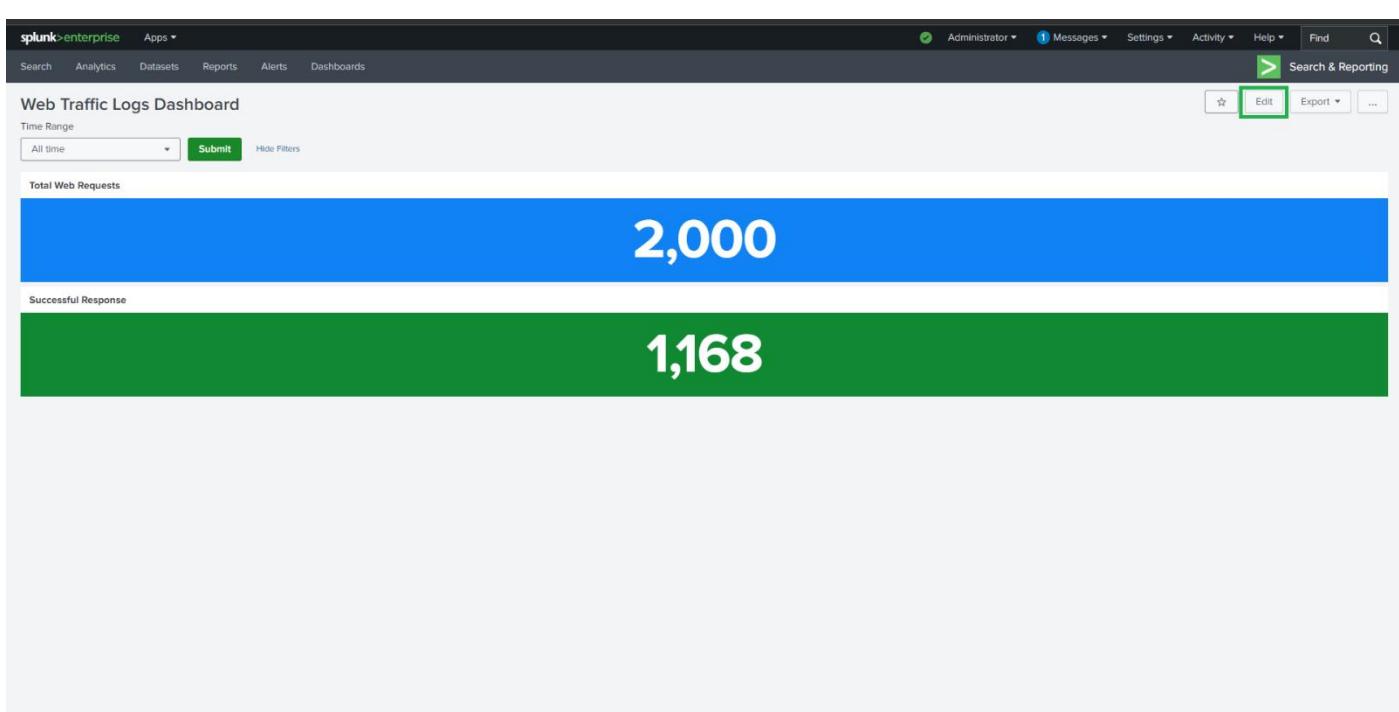
Time Range All time Submit Hide Filters

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.

The screenshot shows the Splunk Enterprise interface with the 'Web Traffic Logs Dashboard'. The dashboard contains two large numerical values: '2,000' in a blue box and '1,168' in a green box. A context menu is open on the right side, with the 'Single Value' option highlighted. Other options in the menu include Events, Statistics Table, Line Chart, Area Chart, Column Chart, Bar Chart, Pie Chart, Scatter Chart, Bubble Chart, Radial Gauge, Filler Gauge, Marker Gauge, Cluster Map, Choropleth Map, New from Report (8), Clone from Dashboard (7), and Add Prebuilt Panel (0).

The screenshot shows the Splunk Enterprise interface with the 'Web Traffic Logs Dashboard'. The dashboard contains two large numerical values: '2,000' in a blue box and '1,168' in a green box. A context menu is open on the right side, with the 'Single Value' option highlighted. A new panel titled 'New Single Value' is open, showing a dropdown menu for 'Time Range' with 'Use time picker' selected. Other options in the dropdown include 'Shared Time Picker (time_range)', 'Use time picker', 'Tokens', and 'Global'. The 'Run Search' button is also visible.

The screenshot shows the Splunk Enterprise interface with the following components:

- Header:** Splunk enterprise, Apps ▾, Search, Analytics, Datasets, Reports, Alerts, Dashboards.
- Toolbar:** Edit Dashboard, UI, Source, + Add Panel, + Add Input ▾, Dark Theme.
- Dashboard Area:** Web Traffic Logs Dashboard (No description). It includes a Time Range input (All time) and a Submit button.
- Panel Options:** A modal titled "Add Panel" is open, showing a sidebar with chart types (Events, Statistics Table, Line Chart, etc.) and a main area for "New Single Value". 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"`.
- Panel Preview:** A preview panel titled "Total Web Requests" shows a large blue box with the number "2,000" and a green box labeled "Successful Response".

The screenshot shows the Splunk Enterprise interface with the title bar "splunk>enterprise Apps ▾". The main navigation includes "Search", "Analytics", "Datasets", "Reports", "Alerts", and "Dashboards". On the right, there are links for "Administrator", "Messages", "Settings", "Activity", "Help", and "Find". A green search bar at the top right contains the text "Search & Reporting". Below the title bar, the dashboard is titled "Web Traffic Logs Dashboard" with a "No description" note. It features a "Time Range" section with a dropdown set to "All time" and a "Submit" button. To the right, there is a checkbox labeled "Autorun dashboard". The dashboard itself has three main sections: "Total Web Requests" (blue box, value 2,000), "Successful Response" (green box, value 1,168), and "Client Errors" (light blue box, value 376). Each section includes a search icon, a chart icon labeled "Chart: 42", and a settings icon.

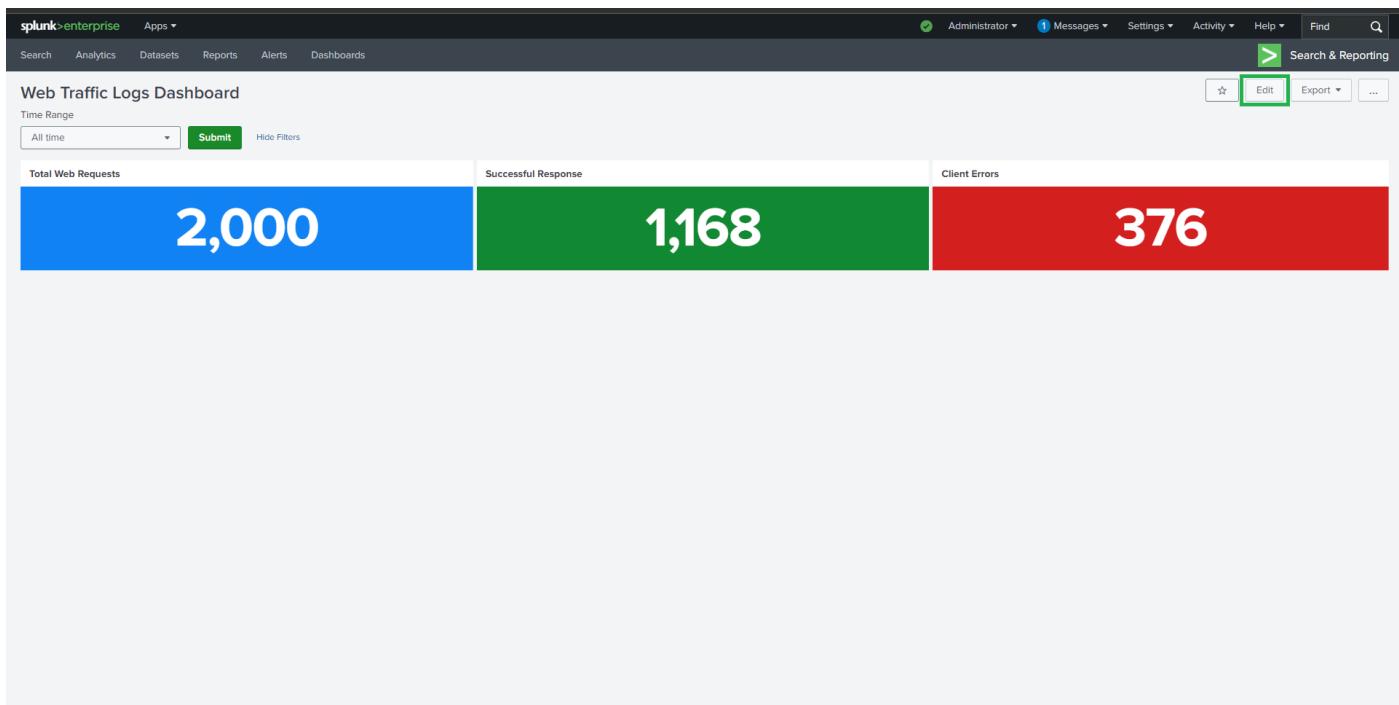
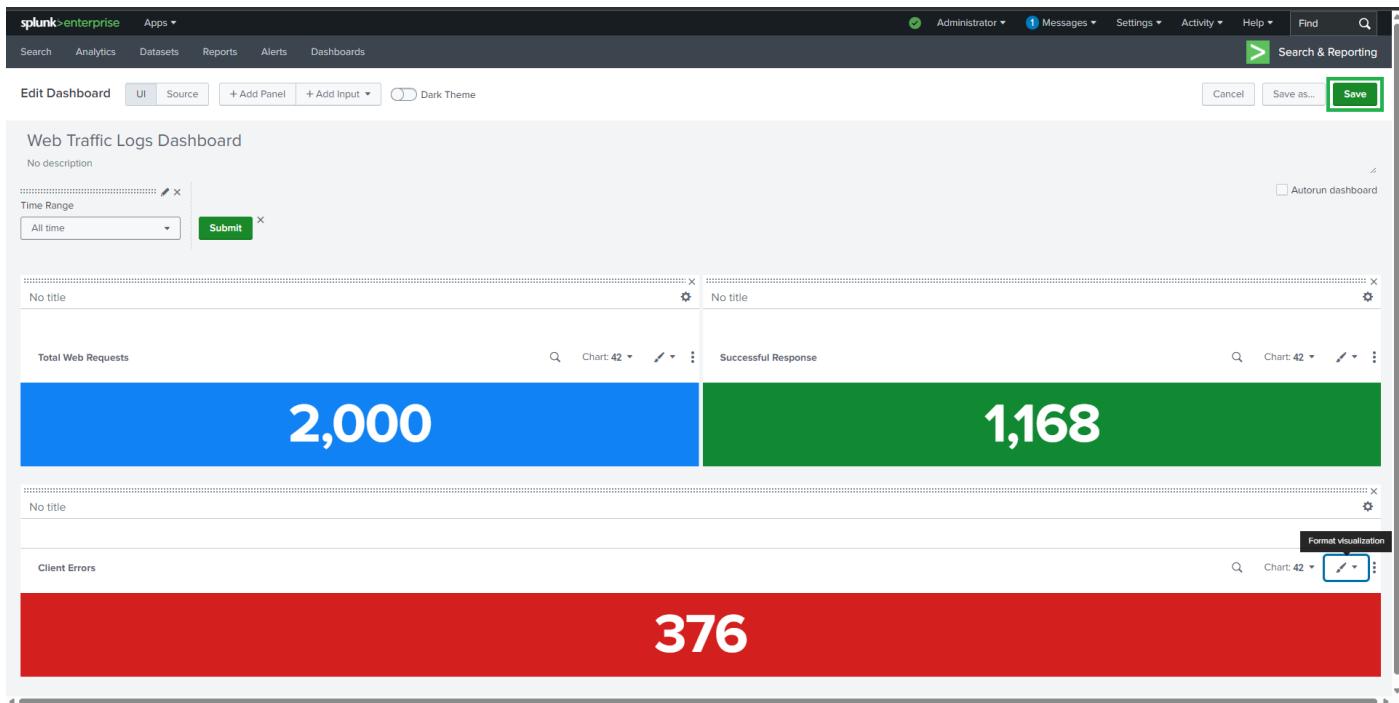
The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with links for 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. On the right side of the header, there are user status indicators ('Administrator'), message notifications ('1 Messages'), and links for 'Settings', 'Activity', 'Help', and 'Find'. Below the header, a search bar labeled 'Search & Reporting' is present.

The main area is titled 'Edit Dashboard' and contains a section for 'Time Range' with a dropdown set to 'All time' and a 'Submit' button. There's also a checkbox for 'Autorun dashboard'.

The dashboard itself has two main cards:

- Total Web Requests:** Displays the value '2,000' in large white text on a blue background. To its right is another card titled 'Successful Response'.
- Client Errors:** Displays the value '376' in large white text on a red background.

A context menu is open over the 'Client Errors' card, specifically on the 'Color' tab. This menu allows for color mapping based on 'Value' or 'Trend', with ranges from 0 to max. It includes a color palette and a preview area showing the current color mapping.



6.4 Server Errors (5xx)

Visualization: Single Value

Title: Server Errors (5xx)

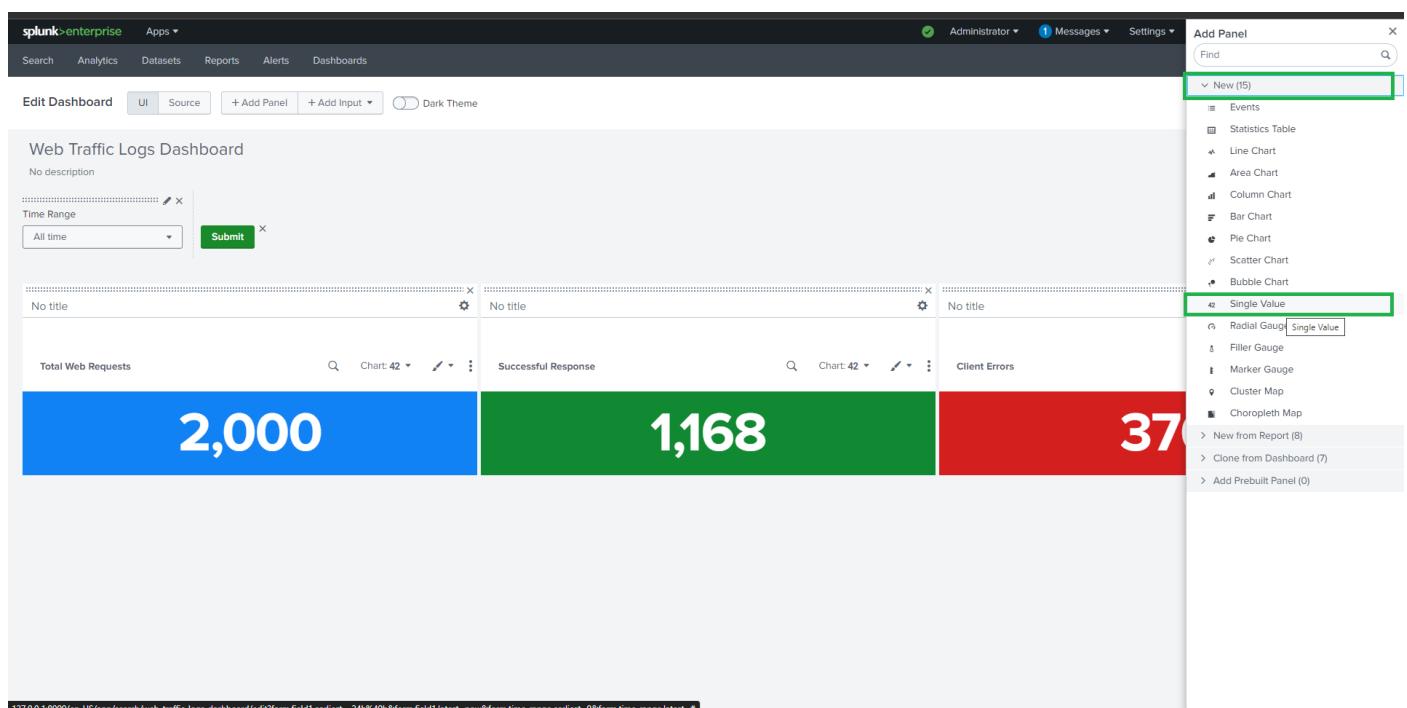
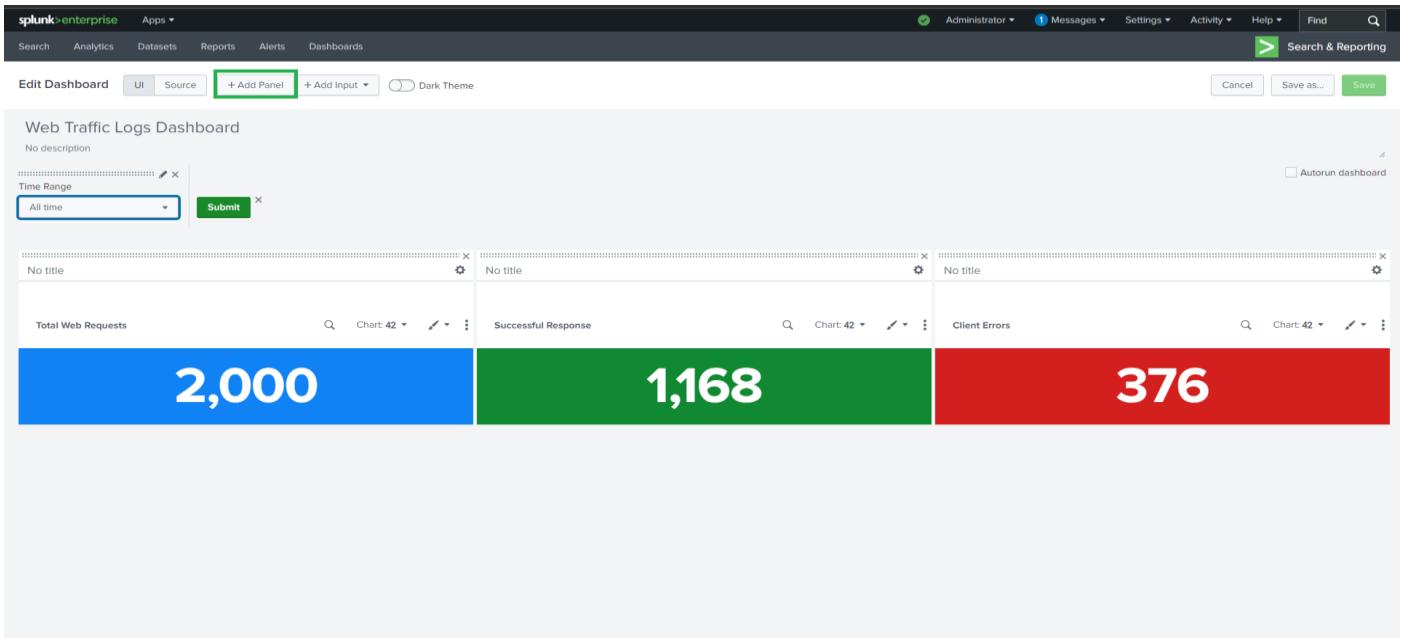
Search Query:

```
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 No title

Total Web Requests Chart: 42 Successful Response Chart: 42

2,000 **1,168**

Add Panel Find New (15)

- Events
- Statistics Table
- Line Chart
- Area Chart
- Column Chart
- Bar Chart
- Pie Chart
- Scatter Chart
- Bubble Chart
- Radial Gauge
- Filler Gauge
- Marker Gauge
- Cluster Map
- Choropleth Map

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=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 All time Submit

No title No title

Total Web Requests Chart: 42 Successful Response Chart: 42

2,000 **1,168**

Add Panel Find New (15)

- Events
- Statistics Table
- Line Chart
- Area Chart
- Column Chart
- Bar Chart
- Pie Chart
- Scatter Chart
- Bubble Chart
- Radial Gauge
- Filler Gauge
- Marker Gauge
- Cluster Map
- Choropleth Map

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 ▾

Search Analytics Datasets Reports Alerts Dashboards

Administrator Messages Settings Activity Help Find 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

No title No title No title

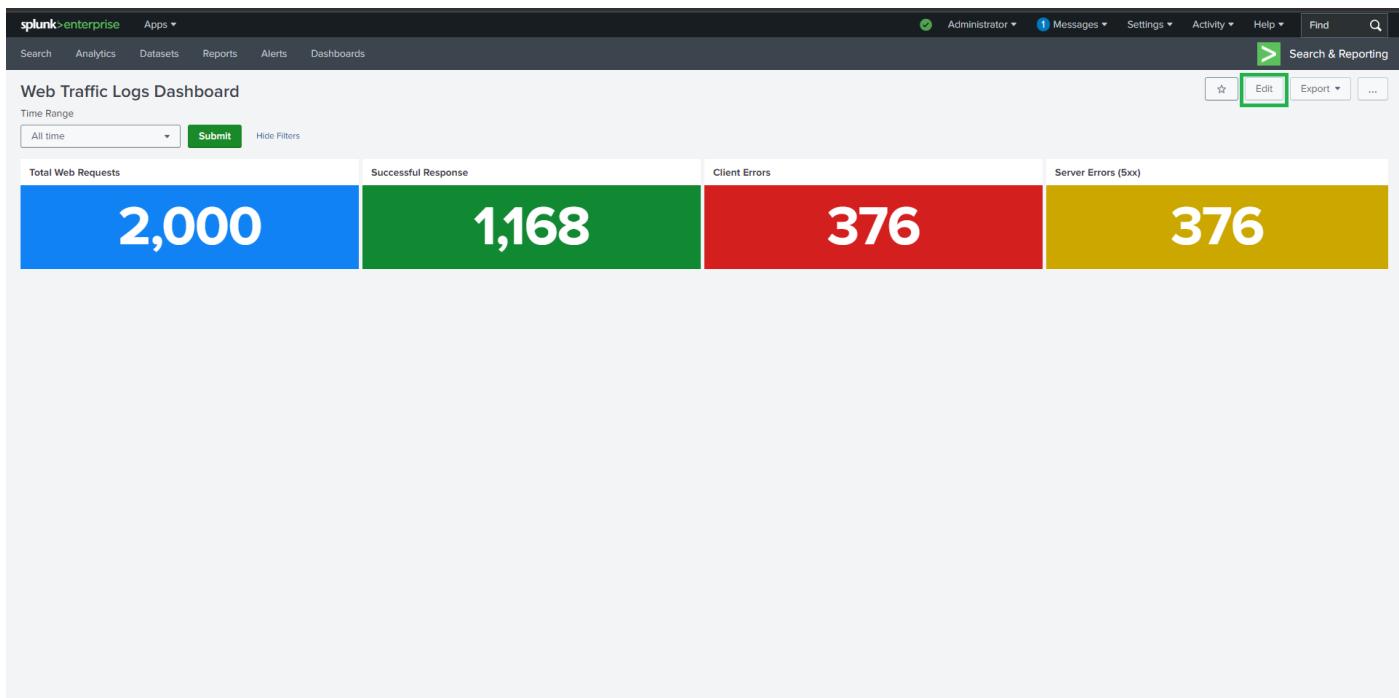
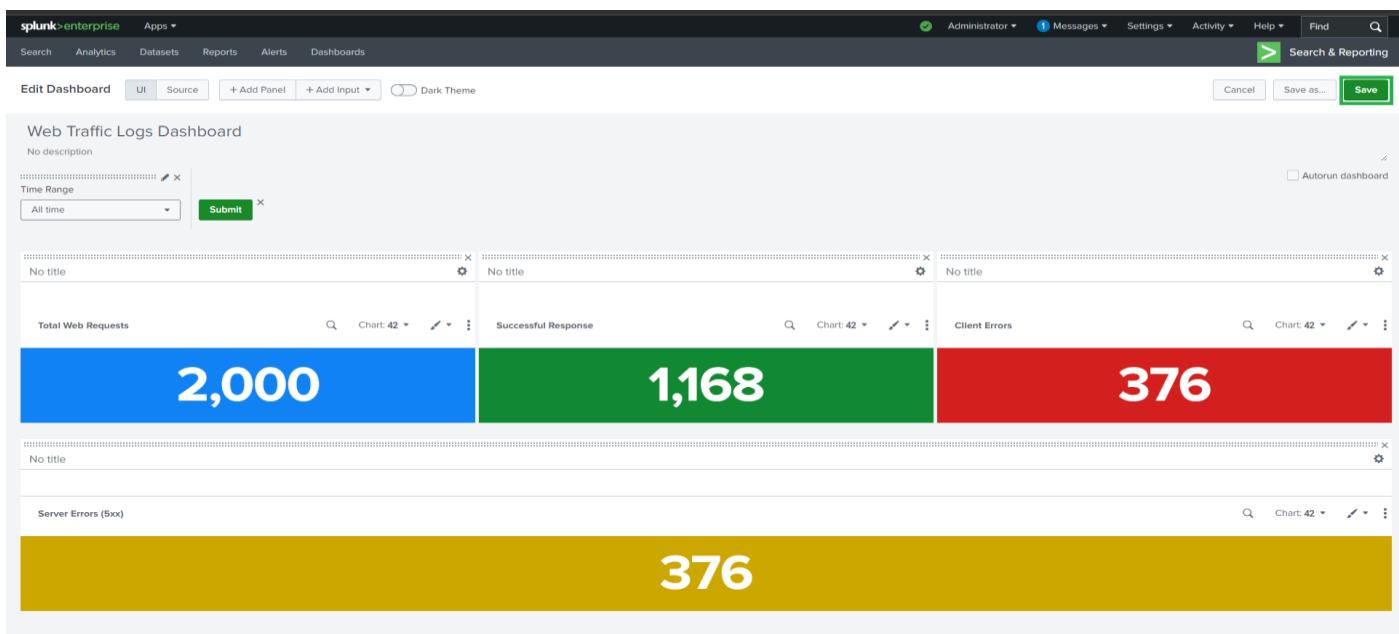
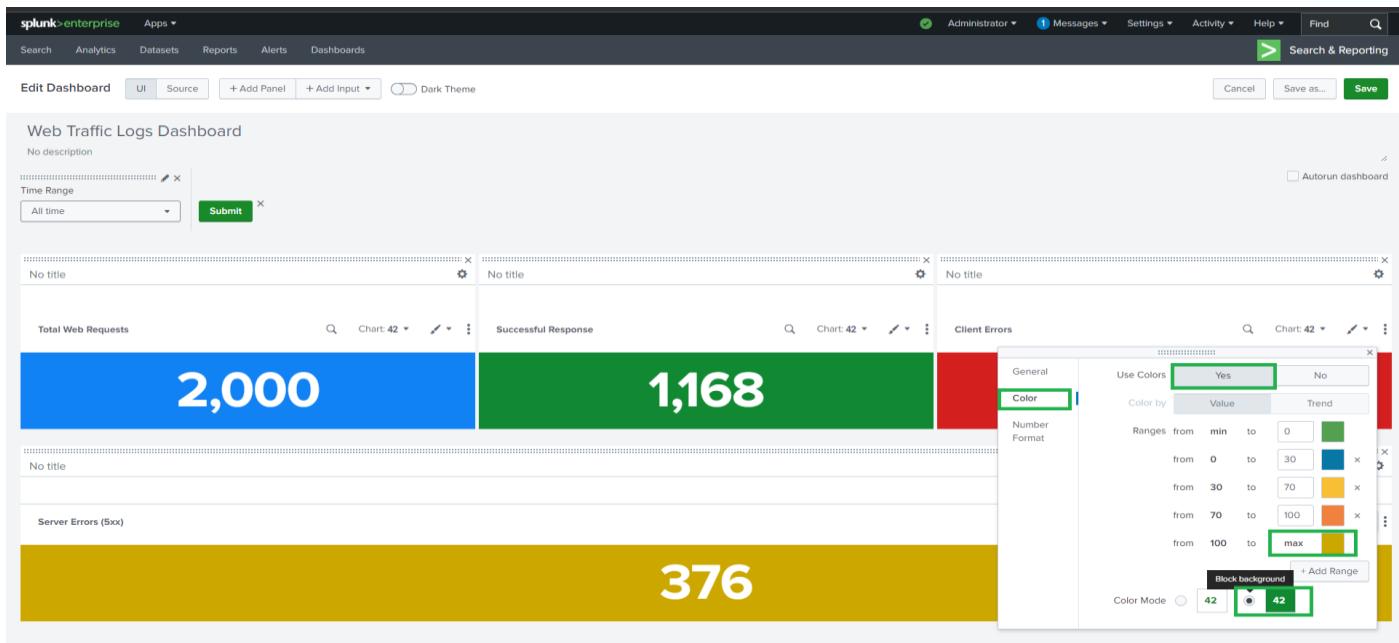
Total Web Requests Chart: 42 Successful Response Chart: 42 Client Errors Chart: 42

2,000 **1,168** **376**

Autorun dashboard

Server Errors (5xx) Chart: 42

376



7. Task 2: Web Statistics Panels

7.1 Top Requested URIs

Visualization: Bar Chart

Title: Top Requested URIs

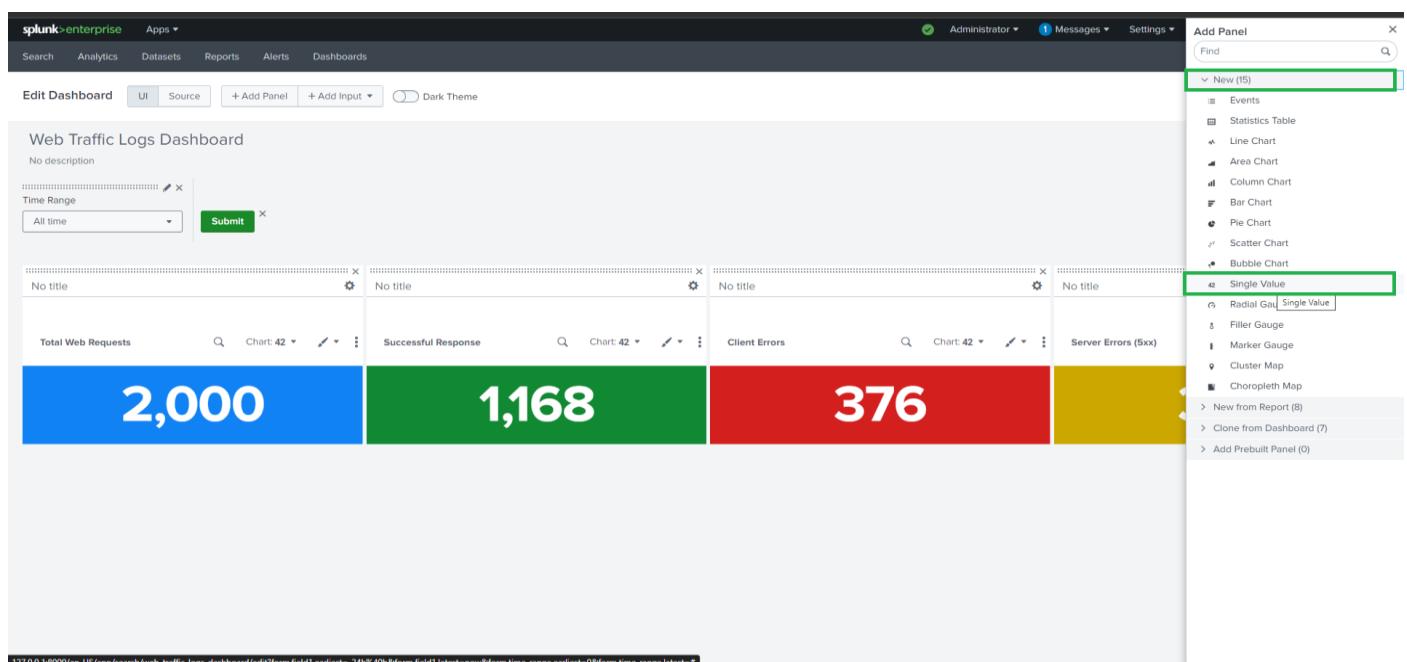
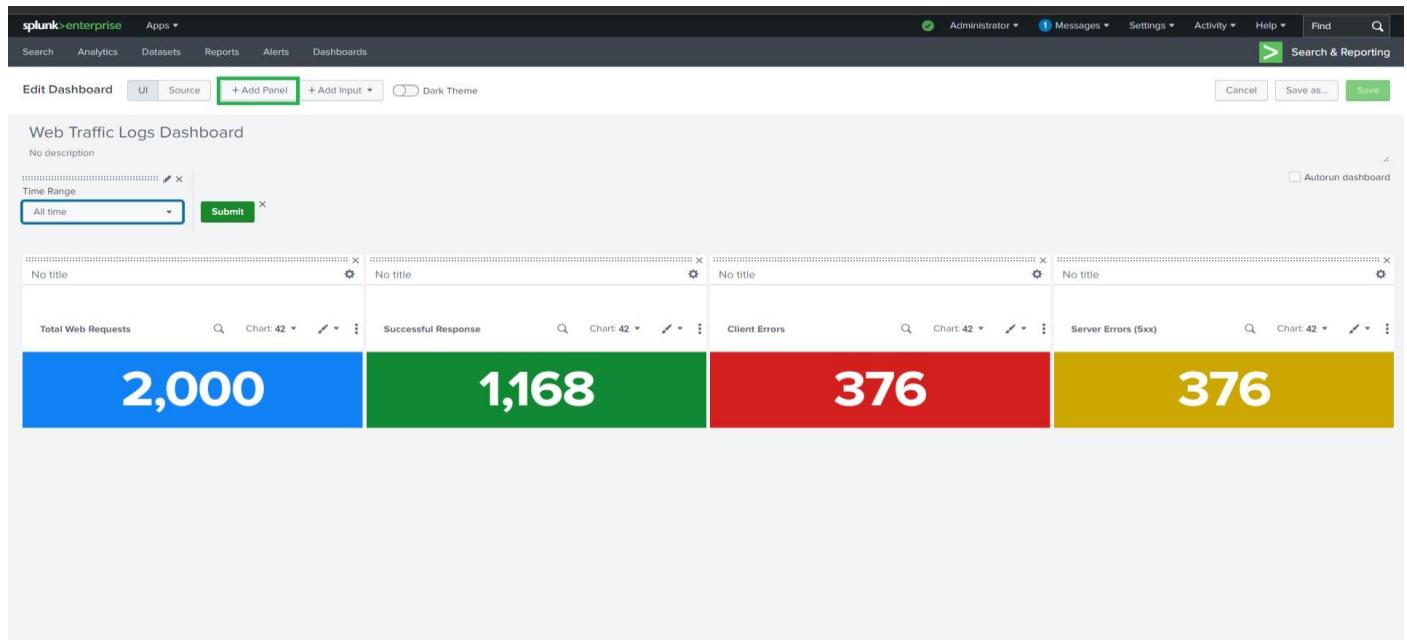
Search Query:

```
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 No title No title

Total Web Requests Chart: 42 Successful Response Chart: 42 Client Errors

2,000 **1,168** **376**

Add Panel Find New (15)

- Events
- Statistics Table
- Line Chart
- Area Chart
- Column Chart
- Bar Chart
- Pie Chart
- Scatter Chart
- Bubble Chart
- Shared Time Picker
- Tokens
- Global

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=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 All time Submit

No title No title No title

Total Web Requests Chart: 42 Successful Response Chart: 42 Client Errors

2,000 **1,168** **376**

Add Panel Find New (15)

- Events
- Statistics Table
- Line Chart
- Area Chart
- Column Chart
- Bar Chart
- Pie Chart
- Scatter Chart
- Bubble Chart
- Shared 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

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=0

Splunk Enterprise Apps

Search Analytics Datasets Reports Alerts Dashboards

Edit Dashboard UI Source + Add Panel + Add Input Dark Theme Administrator Messages Settings Activity Help Find Search

Web Traffic Logs Dashboard No description

Time Range All time Submit

No title No title No title No title

Total Web Requests Chart: 42 Successful Response Chart: 42 Client Errors Chart: 42 Server Errors (5xx) Chart: 42

2,000 **1,168** **376** **376**

Autorun dashboard

Top Requested URIs Chart: 42

/?ref=http://malicious-spam-site.com

splunk enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾ Search & Reporting

Search Analytics Datasets Reports Alerts Dashboards

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

No title No title No title No title

Total Web Requests Chart: 42 Successful Response Chart: 42 Client Errors Chart: 42 Server Errors (5xx) Chart: 42

2,000 1,168 376 376

No title

Top Requested URIs

/?ref=http://malicious-spam-site.com

127.0.0.1:8000/en-US/app/search/web_traffic_logs_dashboard/field?form.field1.earliest=-24h%40h&form.field1.latest=now&form.time_range.earliest=0s&form.time_range.latest=0s

Web Traffic Logs Dashboard
No description

Time Range All time Submit

No title No title No title No title

Total Web Requests Chart: 42 Successful Response Chart: 42 Client Errors Chart: 42 Server Errors (5xx) Chart: 42

2,000 1,168 376 376

No title

Top Requested URIs

Chart: 42 Hits

splunk enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾ Search & Reporting

Search Analytics Datasets Reports Alerts Dashboards

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

No title No title No title No title

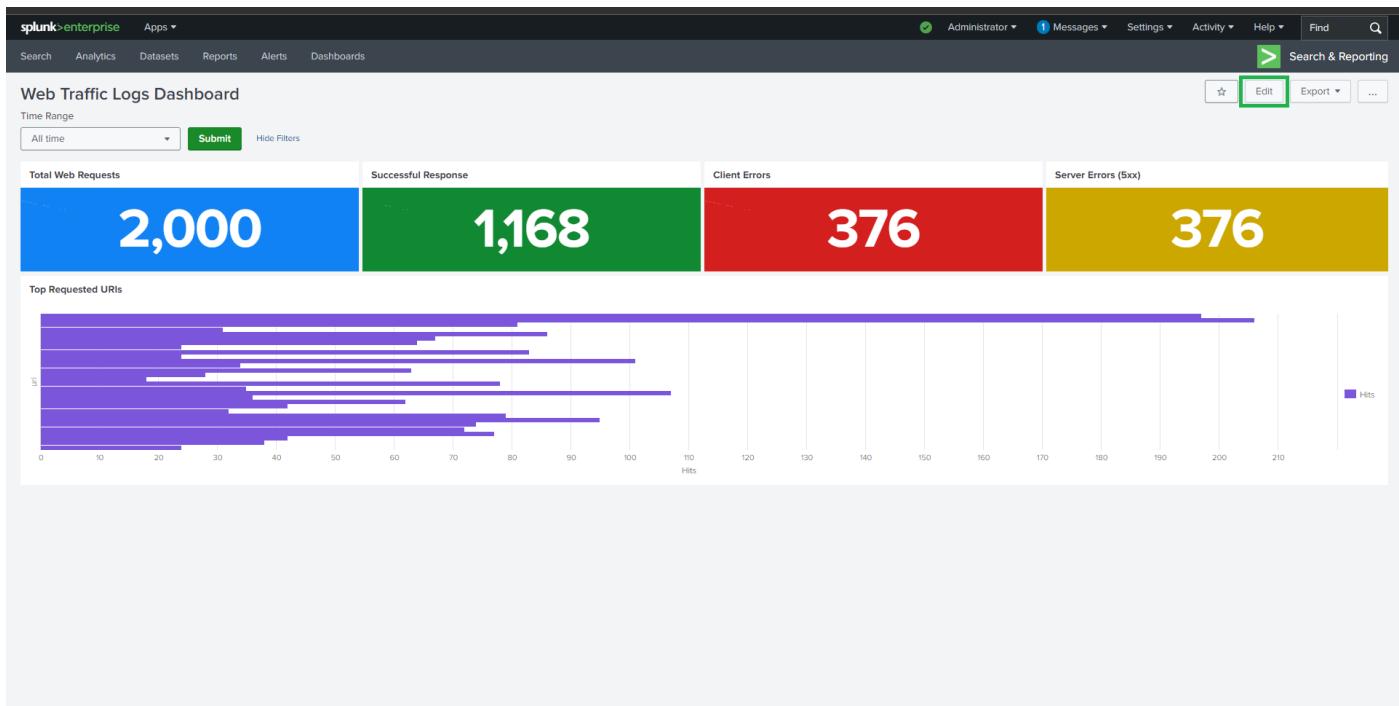
Total Web Requests Chart: 42 Successful Response Chart: 42 Client Errors Chart: 42 Server Errors (5xx) Chart: 42

2,000 1,168 376 376

No title

Top Requested URIs

Chart: 42 Hits



7.2 Top Users by IP Address

Visualization: Bar Chart

Title: Top Users by IP Address

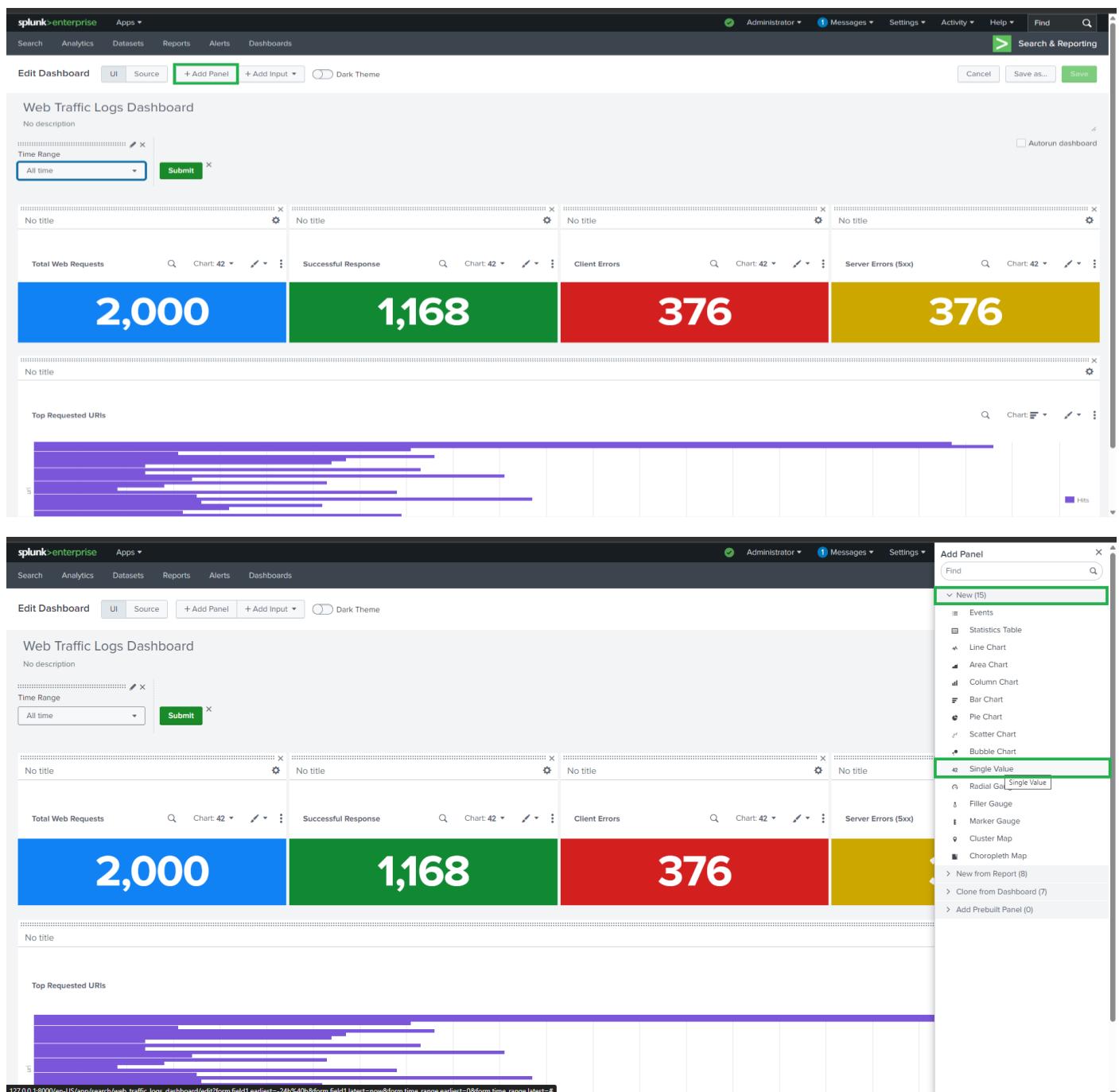
Search Query:

```
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.



spunk-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 No title No title

Total Web Requests Chart: 42 Successful Response Chart: 42 Client Errors Chart: 42

2,000 **1,168** **376**

Top Requested URIs

127.0.0.1:8000/en-US/app/search/web_traffic_logs_dashboard/edit?form.field1.earliest=-24h%50h&form.field1.latest=now&form.time_range.earliest=0&form.time_range.latest=now

Add Panel Find New (15) Time Range Shared Time Picker (time_range) Use time picker Use time picker Last 24 hours Run Search

New Single Value Add to Dashboard

Events Statistics Table Line Chart Area Chart Column Chart Bar Chart Pie Chart Scatter Chart Bubble Chart

Shared Time Picker (time_range)

Use time picker Tokens Global

Run Search

spunk-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 No title No title

Total Web Requests Chart: 42 Successful Response Chart: 42 Client Errors Chart: 42

2,000 **1,168** **376**

Top Requested URIs

Add Panel Find New (15) Time Range Shared Time Picker (time_range) Content Title Top Users by IP Address

New Single Value Add to Dashboard

Events Statistics Table Line Chart Area Chart Column Chart Bar Chart Pie Chart Scatter Chart Bubble Chart

Search String source="apache_logs.json" host="webserver" sourcetype=".json" | stats count AS IP by ip

Run Search

spunk-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 No title No title

Total Web Requests Chart: 42 Successful Response Chart: 42 Client Errors Chart: 42 Server Errors (5xx) Chart: 42

2,000 **1,168** **376** **376**

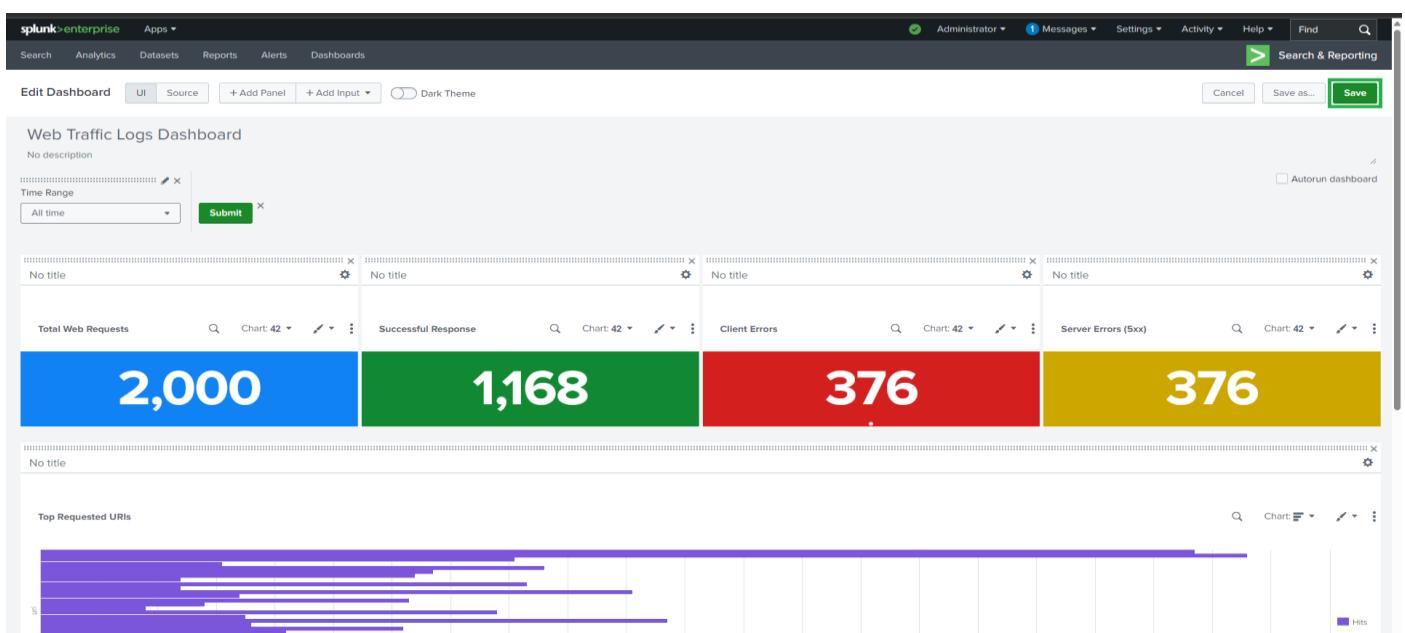
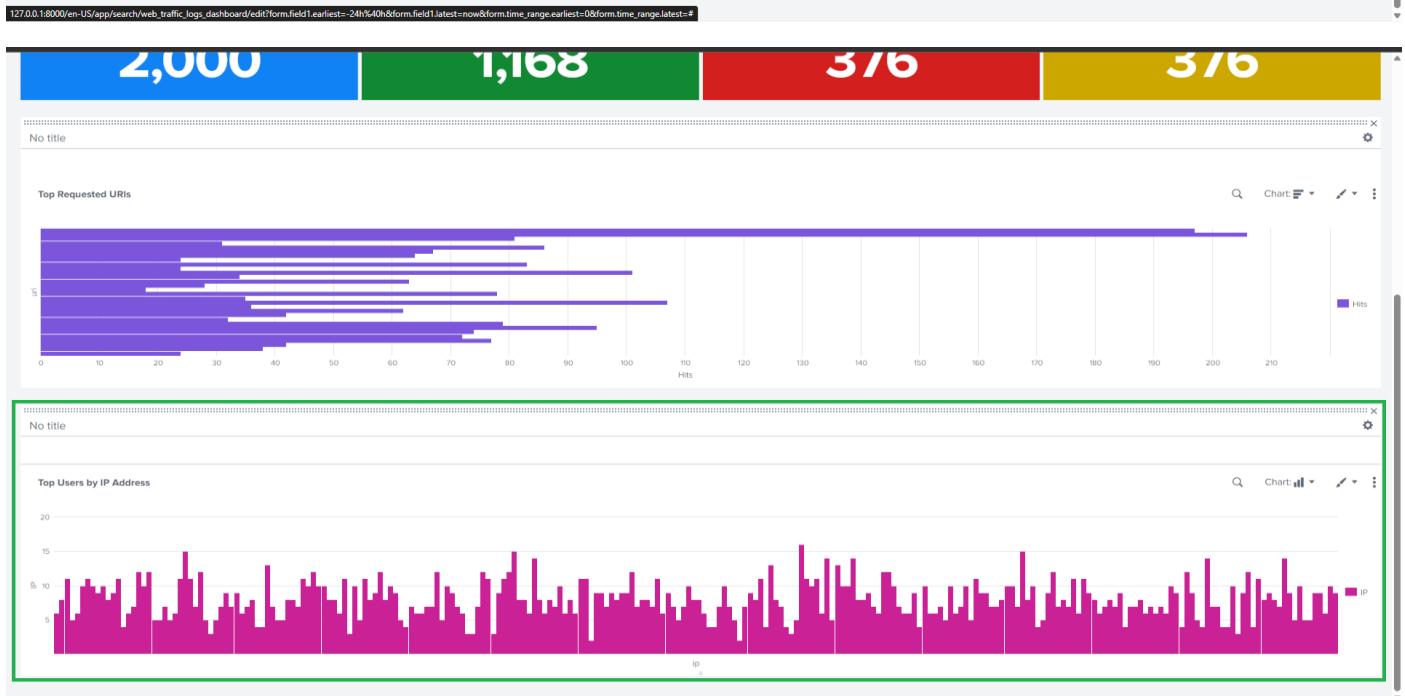
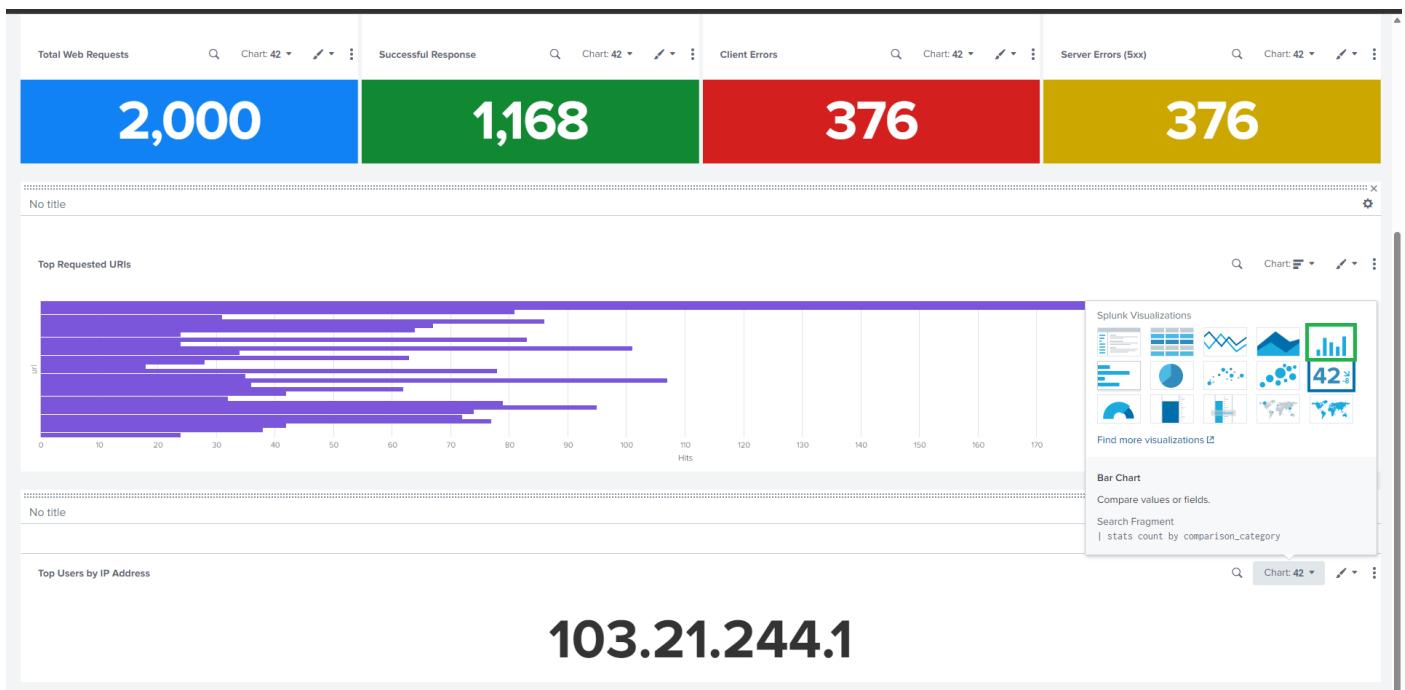
Top Requested URIs

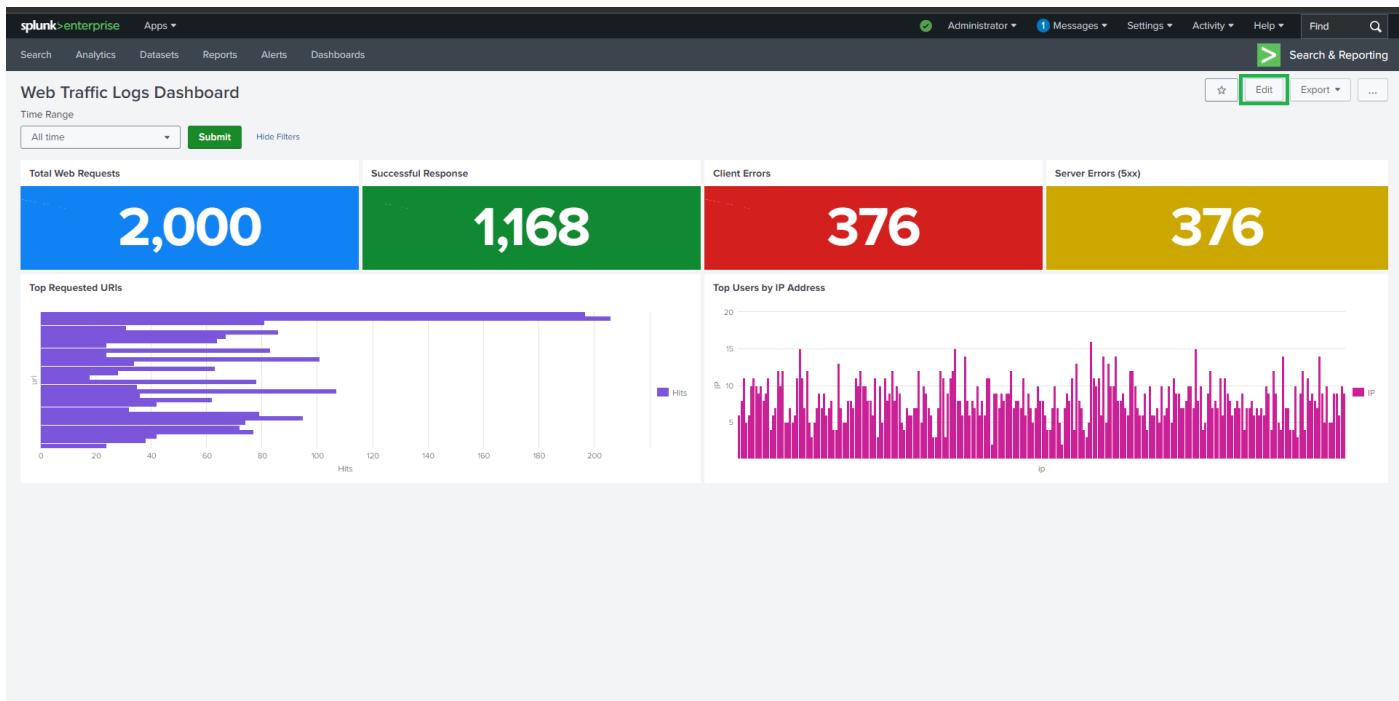
No title

Top Users by IP Address

103.21.244.1

Chart: 42





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

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with 'splunk>enterprise' and various links like 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. Below the navigation is a toolbar with 'Edit Dashboard', 'UI', 'Source', '+ Add Panel' (which is highlighted with a green box), '+ Add Input', and a 'Dark Theme' switch.

The main area displays a dashboard titled 'Web Traffic Logs Dashboard' with no description. It contains several panels: 'Total Web Requests' (blue box with '2,000'), 'Successful Response' (green box with '1,168'), 'Client Errors' (red box with '3'), 'Top Requested URIs' (a horizontal bar chart), and 'Top Users by IP Address' (a bar chart).

A context menu is open over the 'Client Errors' panel, specifically over the red box. The menu is titled 'Add Panel' and includes sections for 'Time Range' (with 'Last 24 hours' selected) and 'Panel Type'. Under 'Panel Type', 'Choropleth Map' is highlighted with a blue box. Other options in this section include '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', and 'New from Report' (8). There are also links for 'Clone from Dashboard' (7), 'Add Prebuilt Panel' (0), and 'Run Search'.

Web Traffic Logs Dashboard

No description

Time Range: All time | Submit

Total Web Requests: 2,000 | Successful Response: 1,168 | Client Errors: 376 | Server Errors (5xx): 376

Top Requested URIs

Top Users by IP Address

Web Traffic by Client IP Addresses

Canada

Add Panel

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
| location ip
| stats count by Country
| geom geo_countries featureIdField="Country"
```

Run Search

Total Web Requests: 2,000 | Successful Response: 1,168 | Client Errors: 376 | Server Errors (5xx): 376

Top Requested URIs

Top Users by IP Address

Web Traffic by Client IP Addresses

Canada

Recommended Visualizations:

- Choropleth Map
- Search Fragment
- 42

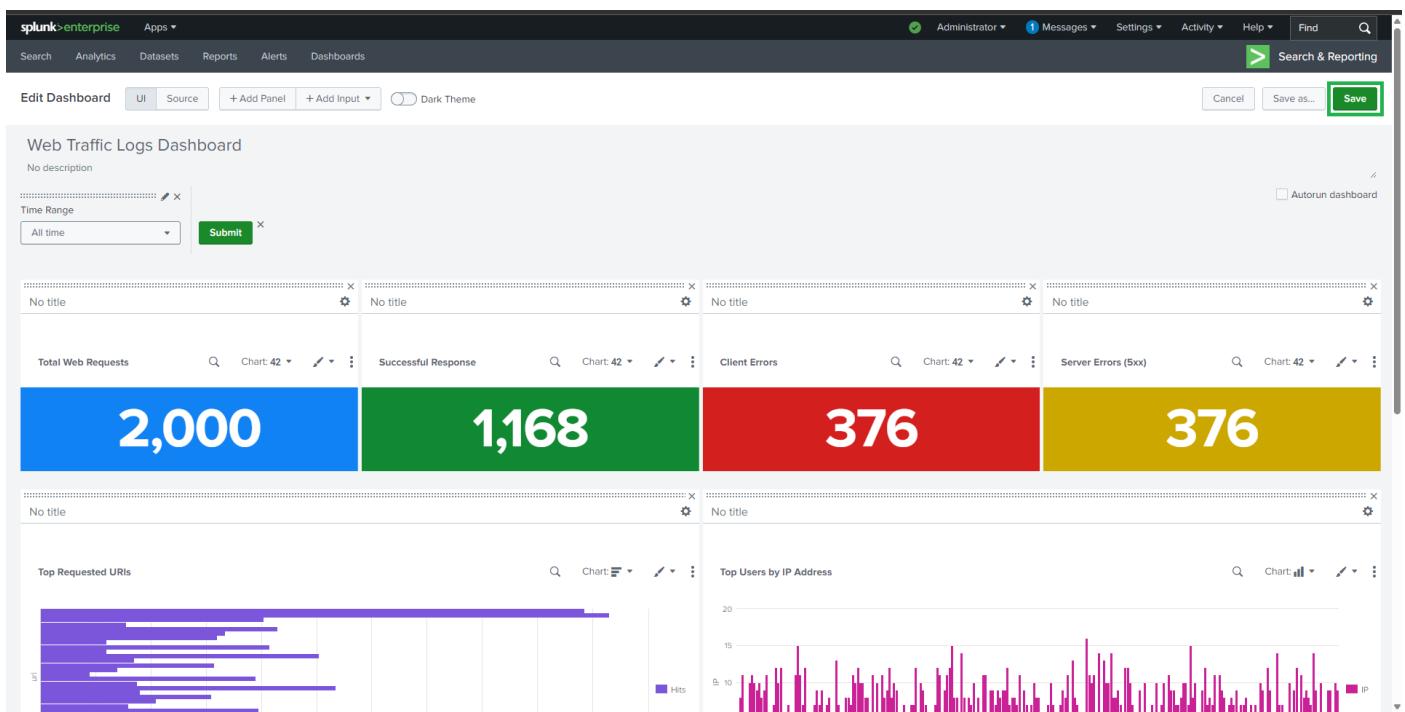
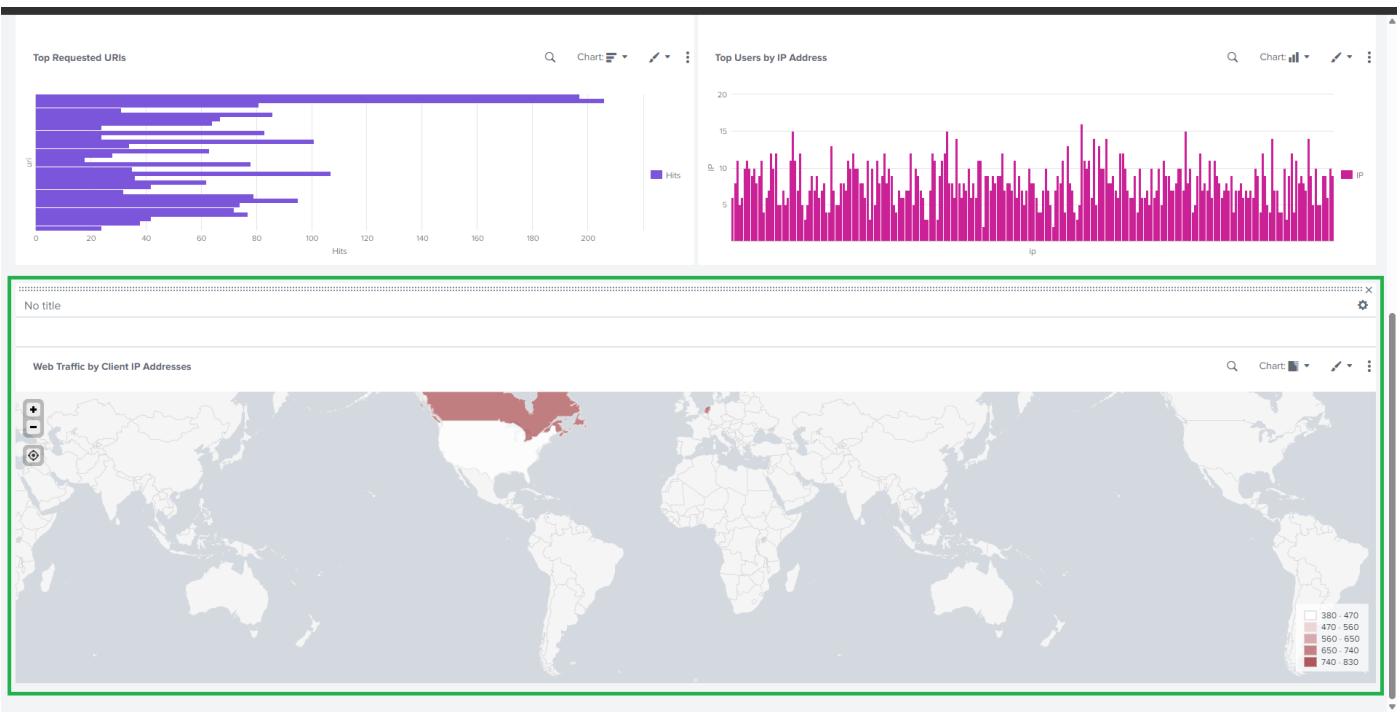
Find more visualizations

Choropleth Map

Show how values vary over a geographic region.

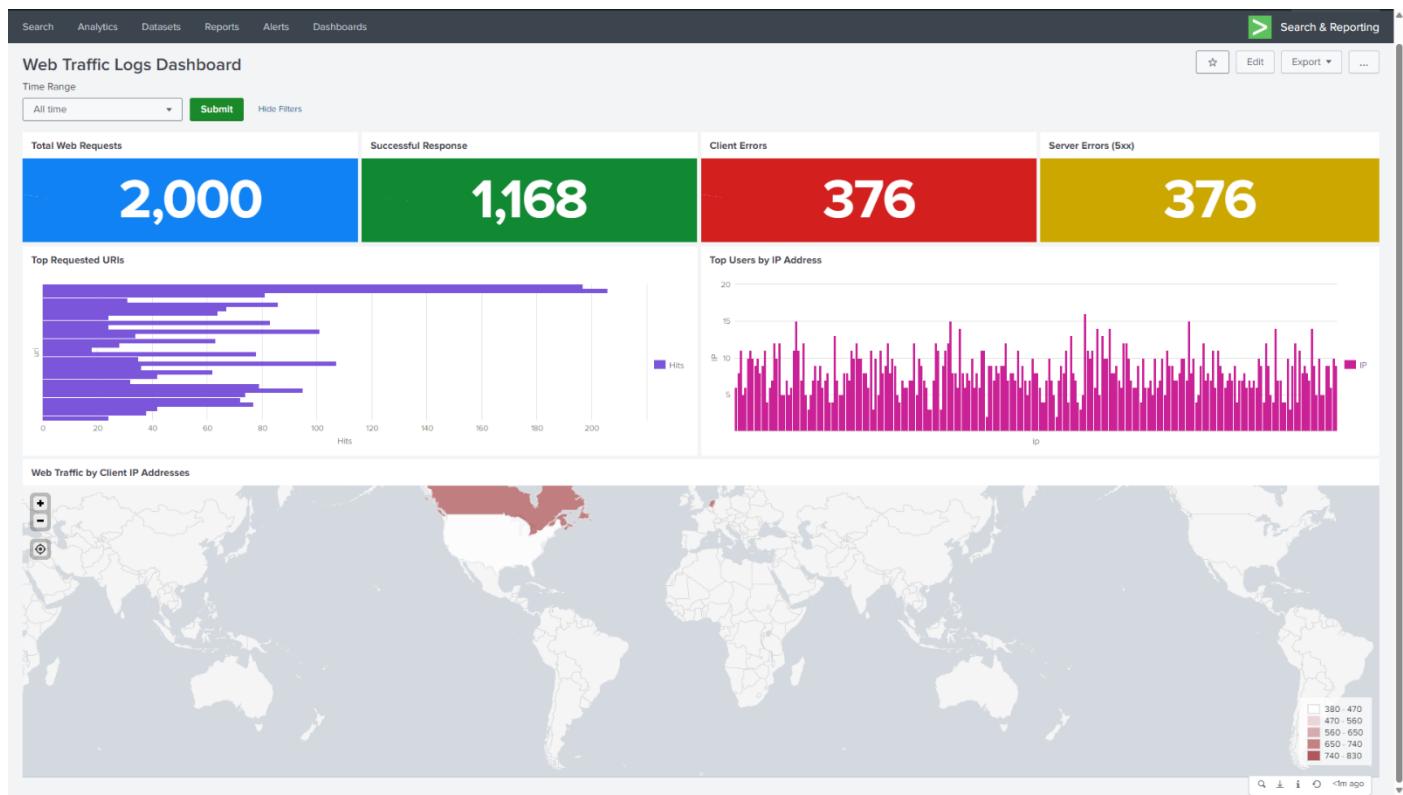
Search Fragment

| stats count by featureId | geom geo_countries featureIdField=featureId



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)