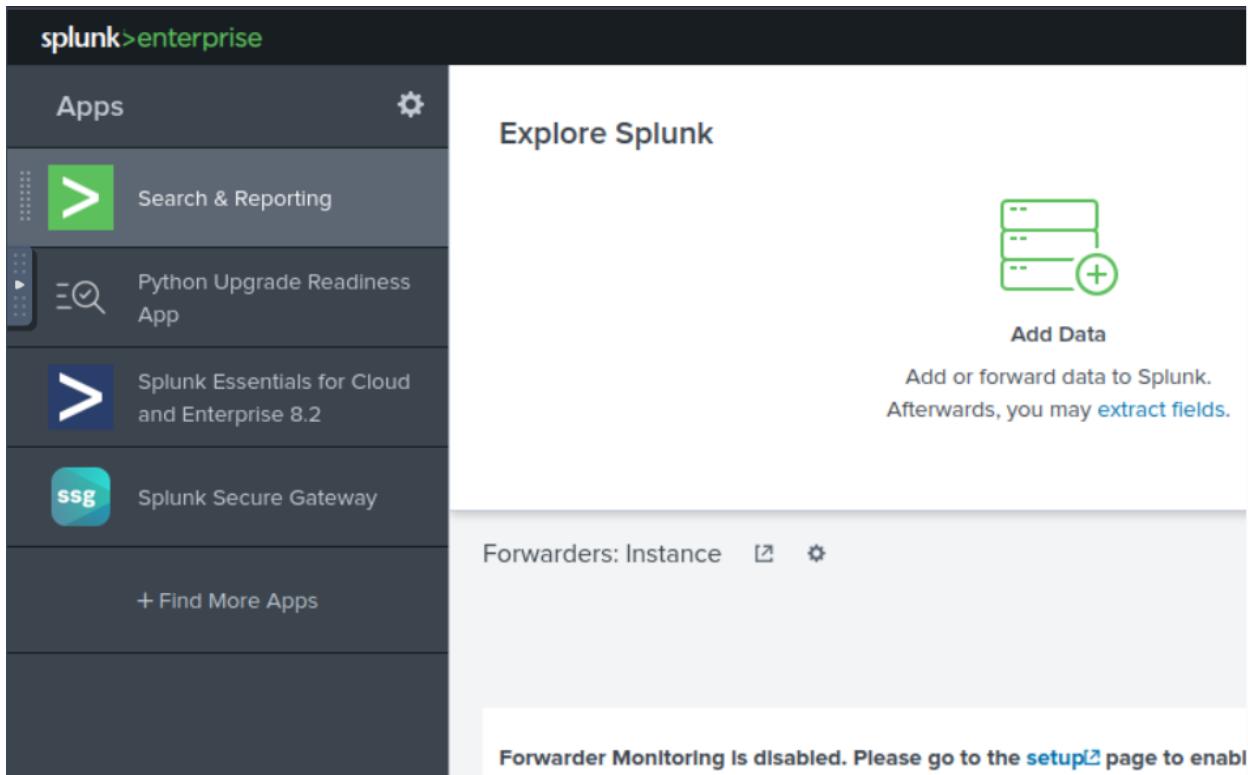


SPLUNK BASIC Report

2025/12/08

Objective: Ingesting log data into splunk and performing a log analysis.

STEP 1: Loading splunk as a web application and ingesting data.



I clicked in 'Add Data' in the 'Explore Splunk' section.

10 data sources

2 data sources

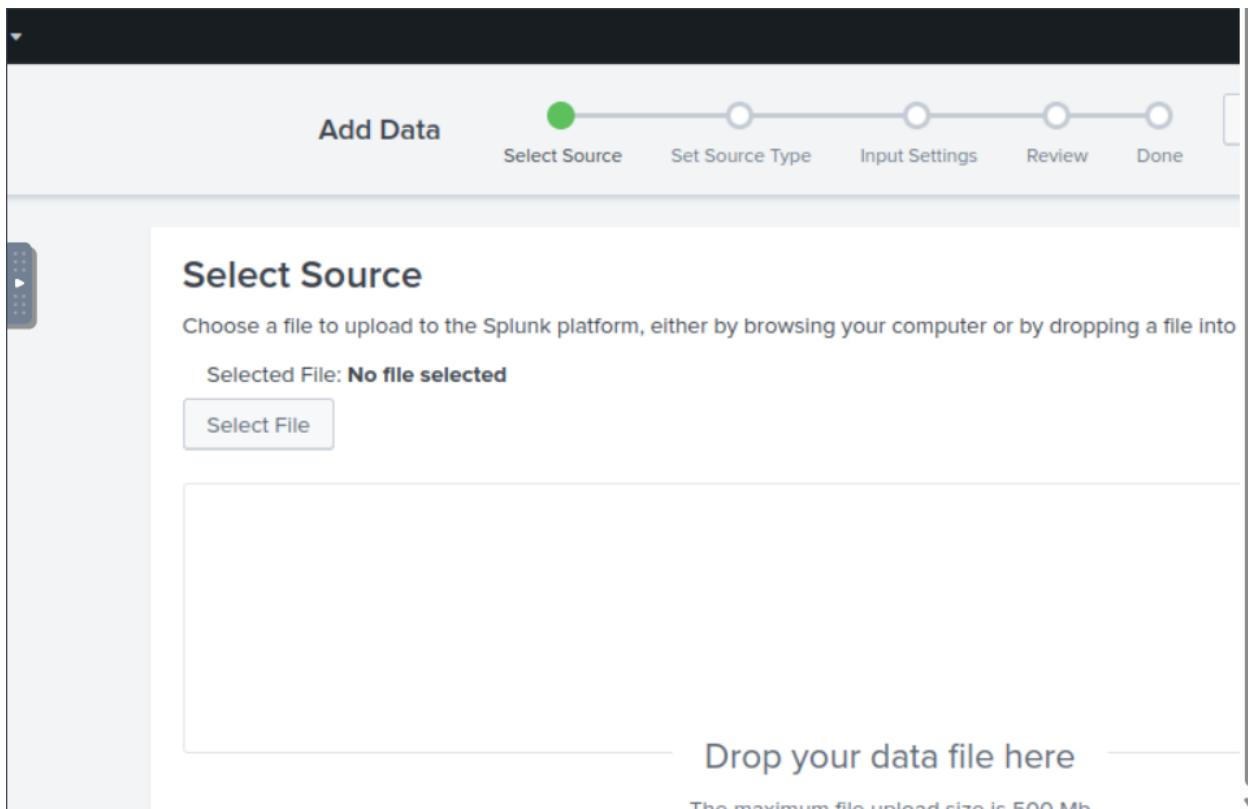
4 data sources in total

Or get data in with the following methods

 **Upload**
files from my computer
Local log files
Local structured files (e.g. CSV)
[Tutorial for adding data ↗](#)

 **Monitor**
files and ports on this Splunk p
Files - HTTP - WMI - TCP/UD
Modular inputs for external d

I then scrolled down just a bit and clicked on 'Upload', navigated my way to the correct directory then into the correct folders to upload the relevant files from my computer.



I was then faced with the 'Select Source' page and chose the log file as well as the data source.

The screenshot shows the Splunk interface for setting source types. At the top, there's a navigation bar with 'Add Data' and a progress bar indicating the process is at 'Select Source'. Below this is a section titled 'Set Source Type' with a play button icon.

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

Source: **VPNlogs.Json**

Source type: `_json` ▾ Save As

Table ▾ ✓ Format 20 Per Page ▾

	<code>_time</code>	<code>action</code> ▾	Code
1	1/1/22 7:58:42.000 AM	built	Cyber
2	1/1/22 5:26:59.000 PM	teardown	Cyber
3	1/1/22 7:10:01.000 AM	built	Cyber

Next was the 'Set Source Type' where I had to select the type of logs being ingested but, in this case, all I had to do was verify that it was in the intended format.

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](#)

FAQ

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

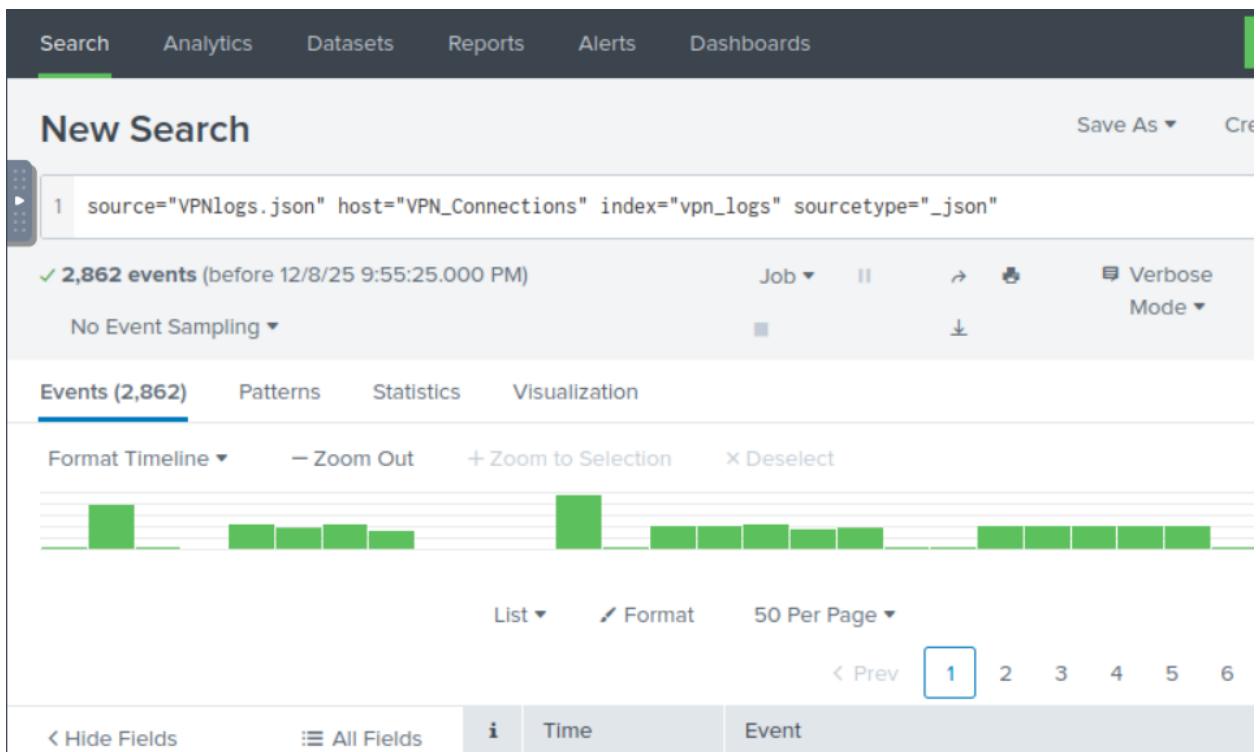
After that I landed on 'Input Settings' where I created the Index and selected it as the default index where the logs would then be dumped and associated it with the HOSTNAME of my choice.

The screenshot shows the Splunk Enterprise interface with the title bar "splunk>enterprise". Below it is a navigation bar with "Messages" (3 notifications), "Settings", "Activity", and "Help". The main content area has a header "Add Data" and a progress bar with five steps: "Select Source" (green dot), "Set Source Type" (green dot), "Input Settings" (green dot), "Review" (green dot), and "Done" (white dot). A "Back" button is located to the right of the progress bar. The "Review" section contains the following configuration details:

Input Type	Uploaded File
File Name	VPNlogs.json
Source Type	_json
Host	VPN_Connections
Index	vpn_logs

Before landing on the 'Done' page and wrapping up the ingestion phase and loading the data, I was faced with the preceding 'Review' page where I had a chance to double check the choices I had made and was happy so I proceeded onto the next step.

STEP 2: Finding how many events are present in the file.



I skimmed through the page where the data loaded manifests itself and identified the number of events (2862).

STEP 2: Discovering the number of log events by the user Maleena.

The screenshot shows a user interface for analyzing log events. At the top, there's a header with a 'Hide field' button, a 'UserName' field, a blue 'X' button, and a 'Next >' button. Below this, it says '51 Values, 100% of events'. There are three buttons: 'Selected' (highlighted with a blue border), 'Yes', and 'No'. A sidebar on the left has a 'Reports' section with 'Top values', 'Top values by time', and 'Rare values' links, and a 'Events with this field' link. A 'Top 10 Values' table follows, with columns for 'Top 10 Values', 'Count', and '%'. The table data is as follows:

Top 10 Values	Count	%
Simon	278	9.713%
James	108	3.774%
Maleena	60	2.096%
Rock	60	2.096%
Bentle	58	2.026%
Paul King	58	2.026%
Emanda	56	1.957%
Kate Wistle	56	1.957%
Martine	56	1.957%
Rafique M	56	1.957%

A yellow 'Json' button is located at the bottom right of the table area.

I looked to the left side of the page and scrolled down to find the target name in the 'UserName' filter and clicked on it. I looked through the section and spotted the target name as well as the Count of events associated with the name – 60.

STEP 3: Locating the name associated with username associated with IP 107.14.182.38.

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

- Query Bar:** host="VPN_Connections" index="vpn_logs" sourcetype="_json" source_ip="107.14.182.38" (The entire query is highlighted with a blue border).
- Time Range:** All time
- Search Buttons:** Save As, Create Table View, Close, and a green Search button.
- Job Controls:** Job dropdown, play/pause, stop, and a Verbose Mode checkbox.
- Statistics and Visualization:** Statistics and Visualization tabs are present.
- Zoom Options:** Zoom Out, + Zoom to Selection, and X Deselect.
- Results:** A message "No results found." is displayed.
- Time Scale:** 1 day per column.

I entered the following query (source_ip="107.14.182.38") and nothing showed up. I took a few steps back and took a breather prior to me second attempt.

The screenshot shows a Splunk search interface. The search bar at the top contains the query: " host='VPN_Connections' index='vpn_logs' sourcetype='json' 107.14.182.38". To the right of the search bar are buttons for "All time" and a magnifying glass icon. Below the search bar is a toolbar with icons for Job, Verbose Mode, and a dropdown menu. The main area displays a histogram followed by a table of search results.

Below the histogram, there are buttons for "Statistics" and "Visualization". Under the visualization section, there are buttons for "Zoom Out", "+ Zoom to Selection", and "Deselect", along with a setting for "1 day per column".

The table has columns for "All Fields", "Time", and "Event". A row in the table shows the following details:

All Fields	Time	Event
	> 1/31/22 6:22:08.000 PM	{ [-] Company: CyberT EventTime: 2022-01-31T18:22:08 Source_Country: United States Source_ip: 107.14.182.38 UserName: Smith action: teardown

A URL "https://tryhackme.com" is visible at the bottom of the table row.

I then removed the filter and pasted only the desired IP and voila! UserName identified – Smith.

STEP 4: What is the number of events that originated from all countries except France?

The screenshot shows a data visualization interface with a table titled "Source_Country". The table lists seven countries with their respective event counts and percentages. The "Selected" button is set to "Yes".

Values	Count	%
United States	2,304	80.503%
Canada	278	9.713%
England	117	4.088%
Israel	66	2.306%
France	48	1.677%
Singapore	48	1.677%
China	1	0.035%

Below the table, there are two lines of code:

```
protocol: tcp
source_state: Maine
```

There were a total of 2862 events from the countries and I looked at France and saw 48. I took the 48 and differenced it from the total and got the answer – 2814.

STEP 5: How many VPN events were associated with the IP 107.3.206.58

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

- Search Bar:** The search bar contains the query: `source="VPNlogs.json" host="VPN_Connections" index="vpn_logs" sourcetype="_json" 107.3.206.58`.
- Results Summary:** It displays **14 events** (before 12/8/25 10:18:18.000 PM).
- Event Sampling:** Set to "No Event Sampling".
- Job Control:** Includes buttons for Job, Refresh, Stop, and Verbose Mode.
- Event Types:** Events (14) is selected, followed by Patterns, Statistics, and Visualization.
- Timeline:** Format Timeline dropdown with options: Zoom Out, Zoom to Selection, Deselect.
- List View:** Shows a list of 14 events, with the first few visible.
- Fields:** Filter bar includes Hide Fields, All Fields, Time, and Event.

I pasted the IP address in the filter/search section and got the number of events associated with it - 14.

Summary Conclusion

This exercise demonstrated the complete process of ingesting and analysing log data in Splunk. I successfully uploaded data, verified the source type, configured input settings, and created a custom index for log storage. Once ingested, I carried out several analysis tasks, including identifying total events, filtering events by specific users, locating usernames linked to IP addresses, and calculating event counts based on geographic sources. Through targeted searches and filters, I identified user activity patterns, IP-associated behaviours, and event counts across different criteria. Overall, this exercise strengthened my understanding of Splunk's workflow, search capabilities, and practical log analysis techniques essential for cybersecurity monitoring.