5/29/2025

Splunk Reports and Dashboards: A Practical Guide

RESEARCH REPORT

Balaji Varaprasad
CYBERSAPIENS

SPLUNK REPORTS AND DASHBOARDS

Why Reports and Dashboards Matter in Splunk:

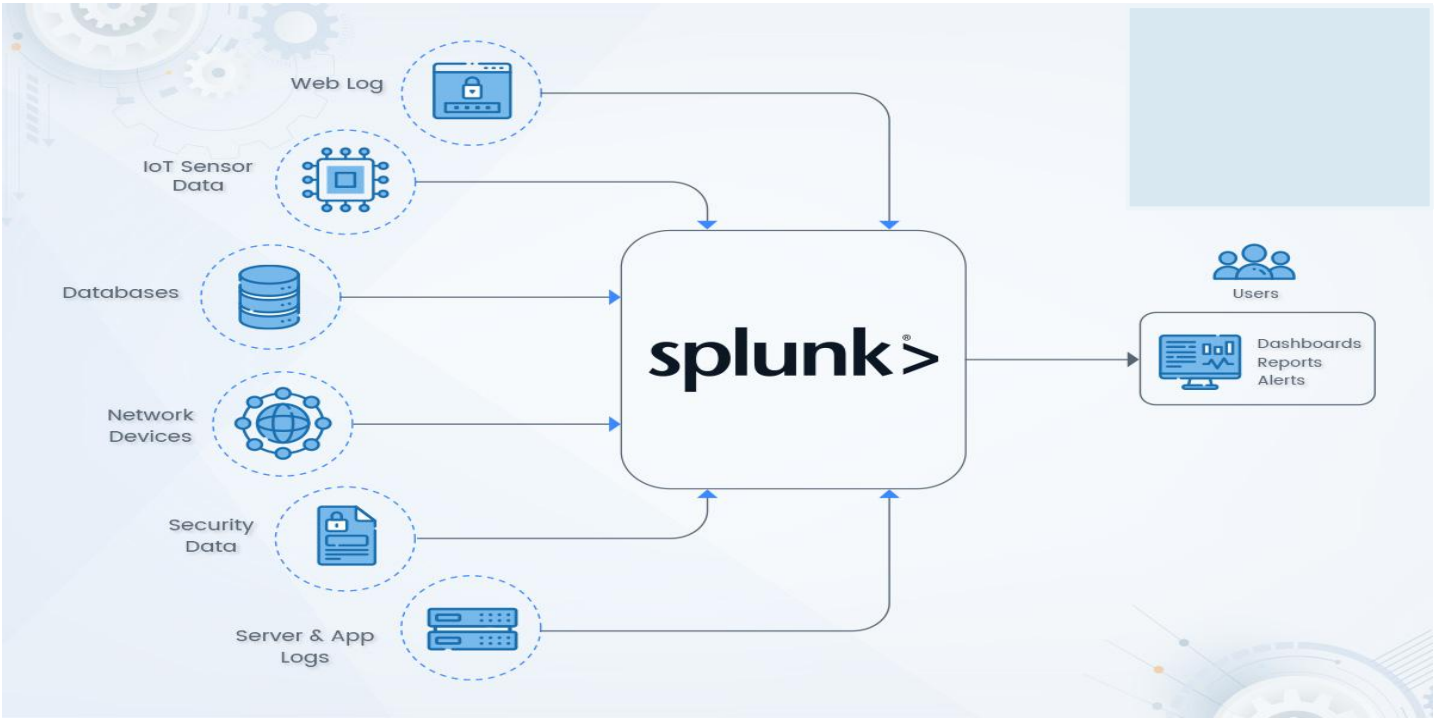
Reports and dashboards in Splunk are vital tools for transforming complex machine-generated data into clear, actionable insights. They provide a structured and visual way to monitor system activities, track security events, and make data-driven decisions. One of their biggest advantages is accessibility even non-technical stakeholders like managers or auditors can easily interpret a well-designed dashboard or summary report without needing to write any queries. Instead of scrolling through raw logs or command-line outputs, users can see trends, patterns, and anomalies through intuitive charts, tables, and visual panels. Reports can also be scheduled and emailed, ensuring the right information is delivered regularly without manual effort. Dashboards offer real-time monitoring, enabling teams to react quickly to issues like failed login attempts, network spikes, or application errors. In essence, reports and dashboards bridge the gap between raw data and business value empowering both technical and non-technical users to understand, act, and collaborate using the same data.

Overview:

In Splunk, reports and dashboards turn raw log data into actionable insights. A report is essentially a saved search that you can run or schedule repeatedly. A dashboard is a visual layout of one or more panels (charts, tables, single-value metrics, etc.) that update as searches run. **Each has advantages:** reports let you reuse queries and offload heavy searches (e.g. by scheduling), while dashboards provide at-a-glance multi-metric views. The table below highlights key differences:

Aspect	Reports	Dashboards
Definition	A saved search (from Search or Pivot) that can be rerun or scheduled.	A collection of visual panels (charts, tables, single-value metrics).
Purpose	Run/share specific searches. Often scheduled to run at intervals.	Display multiple queries or visualizations together for broad insight.
Creation	Run a search, then **Save As > Report** in Splunk Web.	Use the Dashboard Editor to add panels (charts, tables, etc.) or embed saved reports.
Output	Results (table/chart) in a report view, can be exported or emailed.	Interactive panels (line/bar/pie charts, tables, single-value) on a dashboard canvas.
Update	Static until run, can be scheduled to refresh.	Dynamic: panels update automatically (e.g. on load or refresh).
Sharing & Access	Permissions-controlled. Can be private or shared via roles/capabilities.	Permissions-controlled per dashboard. Admins can make it private, app-level or global and grant view/edit to roles.

Data Collection & Indexing in Splunk:



Splunk ingests data from virtually any source (servers, devices, apps) via forwarders or direct inputs. Data is parsed, timestamped, and indexed in real time. During indexing, Splunk extracts fields (like host, source, source type) for fast search. Each index holds events of similar type, for example, the _audit index records Splunk's internal audit events (login attempts, configuration changes, etc.). As Splunk docs note, "When you add data to the Splunk platform the data is indexed" and fields are extracted for searching. In particular, _audit events (e.g. failed logins) are stored locally in index=_audit. By querying this index, we can analyse login activity.

Visualization Options:

Trend

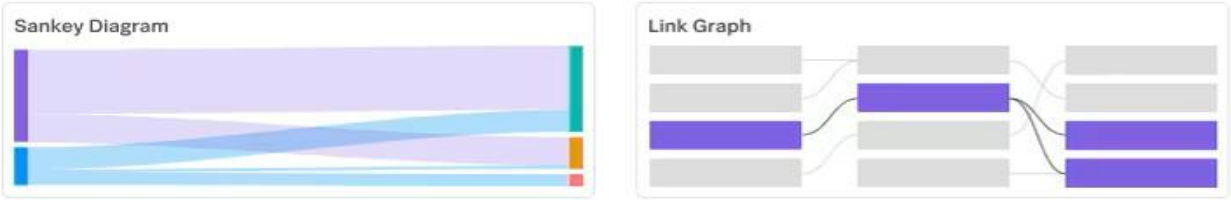
Charts based on the horizontal axis typically display time series data. The visualization represents data over a period of time.

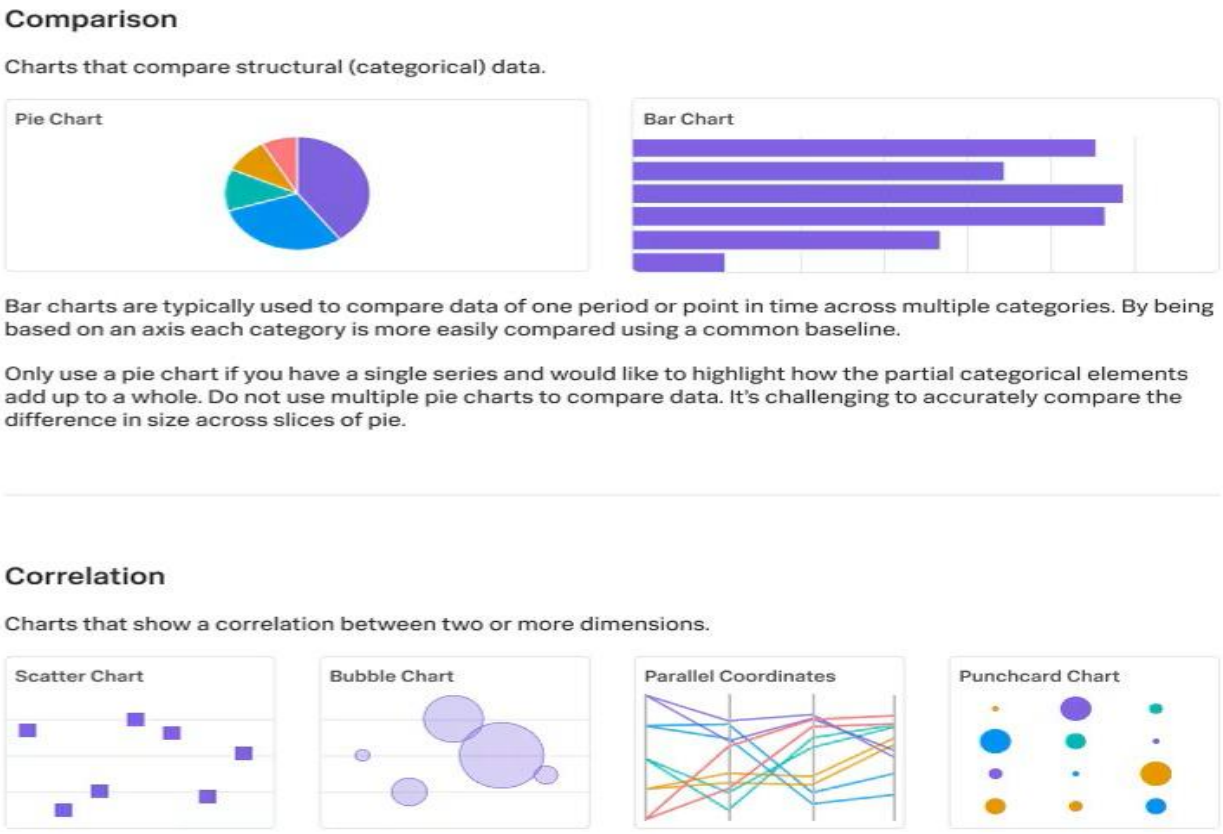
Stacked charts represent the accumulation of more than one data series. Position the data series of central importance directly on the axis in order to best see its development over time.

Use stacked 100% charts if the accumulation of all data series adds to a whole.

Flow

Charts that show movement of data between multiple states.



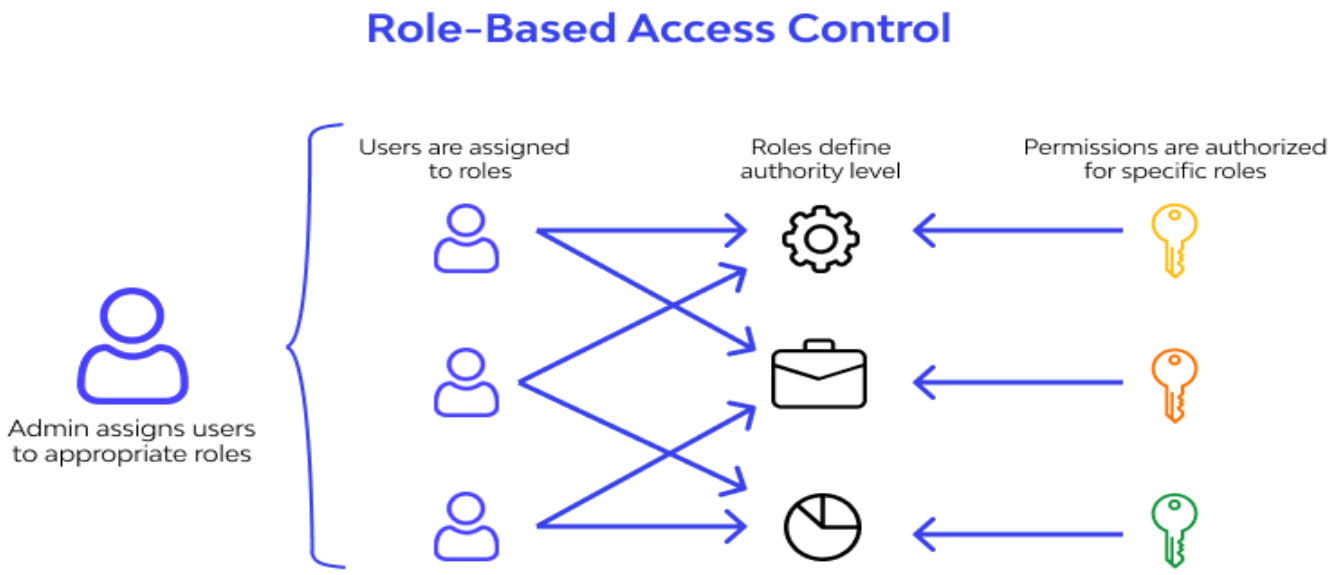


Splunk offers many visualization choices to suit different data patterns. Panels can display charts (line, area, column/bar, pie, scatter, bubble), tables (detailed event or statistic lists), single-value metrics, gauges, and even maps. For example:

- Time series charts (line/area) show trends over time (often created with time chart).
- Bar/column charts compare categories or group counts.
- Pie charts show proportions of a whole.
- Single Value panels highlight a key metric (e.g. Total Failed Logins) prominently.
- Tables list raw events or aggregated stats for drill-down detail.
- Gauges (radial/filler) visualize a metric against a range (e.g. CPU Utilization).
- Maps (choropleth or cluster) plot geo-data by IP or coordinates.

These options are available in Splunk Web's Dashboard Editor or Dashboard Studio. The panels update automatically when the underlying search runs. As Splunk documentation notes, dashboards consist of panels that can contain "charts, tables, and lists" based on search results.

User Access and Permissions:



Splunk enforces **role-based access** control for viewing/editing reports and dashboards. Each user has a role (Admin, Power, User, etc.) with capabilities that determine what they can see or do. By default, only users with read access to an app (like the Search & Reporting app) can see its dashboards and reports.

Reports and dashboards have their own permissions. When you create a report, you can set its sharing (private, app, global) and specify which roles or users can view or edit it. For dashboards, the Dashboard Editor lets an admin set access levels, an admin can make a dashboard private, visible only within its app, or visible to all apps. They can also grant view/edit rights to specific roles (for example, allowing the "user" role to view a dashboard but only "admin" or "power" roles to edit it).

In practice, after building the dashboard, you might share it by setting its permissions so that security analysts (with a certain role) can view it, while only Admins can modify it. This ensures sensitive audit data is only seen by authorized users.

Practical: Performing the failed-login search

Scenario: 1. Create a report and dashboard in Splunk that showcases the top 10 IP addresses with the highest number of failed-login attempts in the last 24 hours. (Index=_audit failed-login).

SPL Query Construction (Failed-Login Use Case):

Splunk's Search Processing Language (SPL) chains commands with pipes. A typical search starts with index=... and filters (keywords or conditions), then uses transforming commands (like stats, top, chart) to aggregate and display results. For our use case, we want the top 10 IP addresses with the most failed logins in the last 24 hours, if the data not available change the time range to 7 days or your desired period of time.

An example SPL might be:

```
index=_audit "failedlogin" earliest=-24h | stats count by clientip | sort – count | head 10
```

(earliest=-24 command is optional, we can also set time range in filters.)

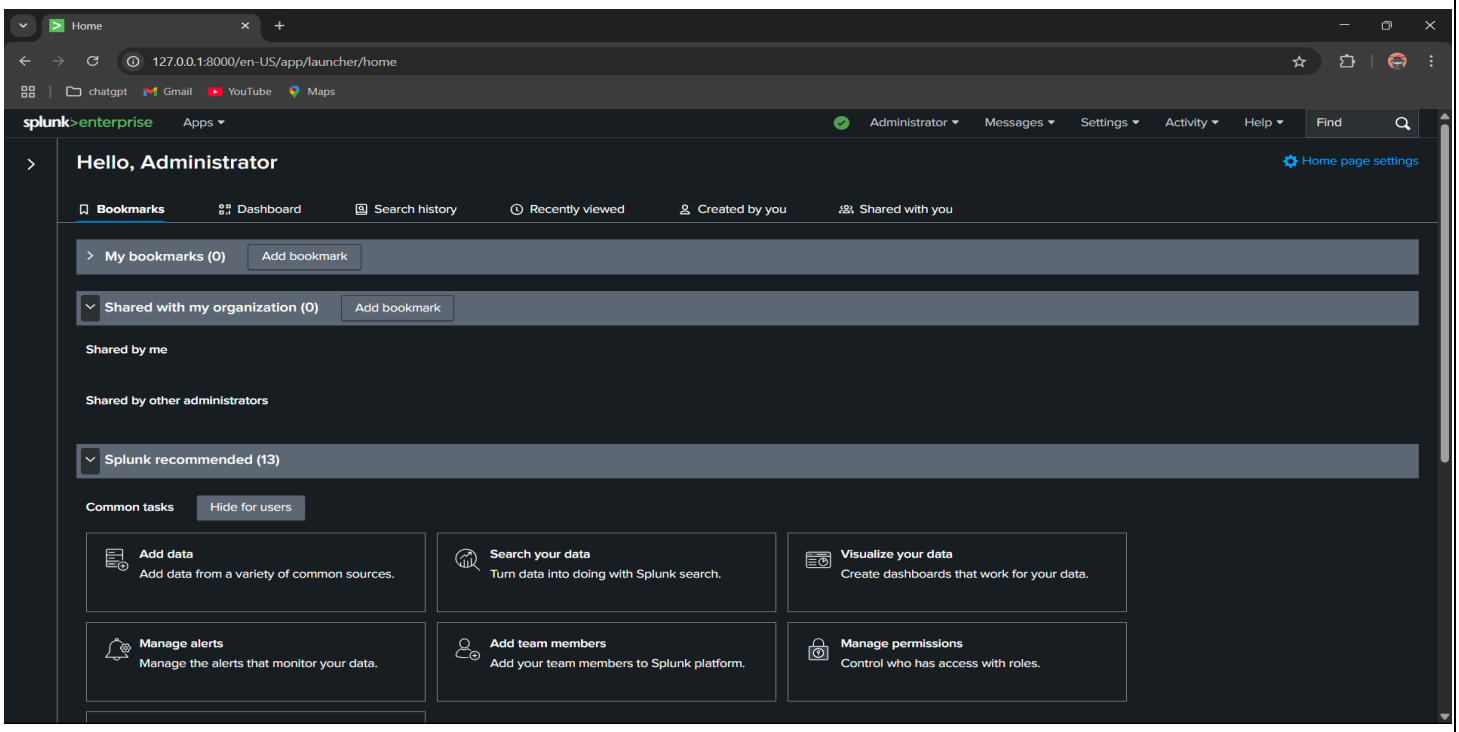
This does the following:

It searches the _audit index for the term failedlogin in the past 24 hours/7days, then uses stats count by clientip to count events per IP, sorts descending by count, and keeps the first 10. (Splunk's docs similarly show using top to get frequent values, e.g. sourcetype=access_* | top limit=20 referer.) We could also use top directly, for example, index=_audit failedlogin | top limit=10 clientip would yield the same result set. In practice, we can run this search in Splunk Web and verify it returns the expected IP list.

Practical demonstration:

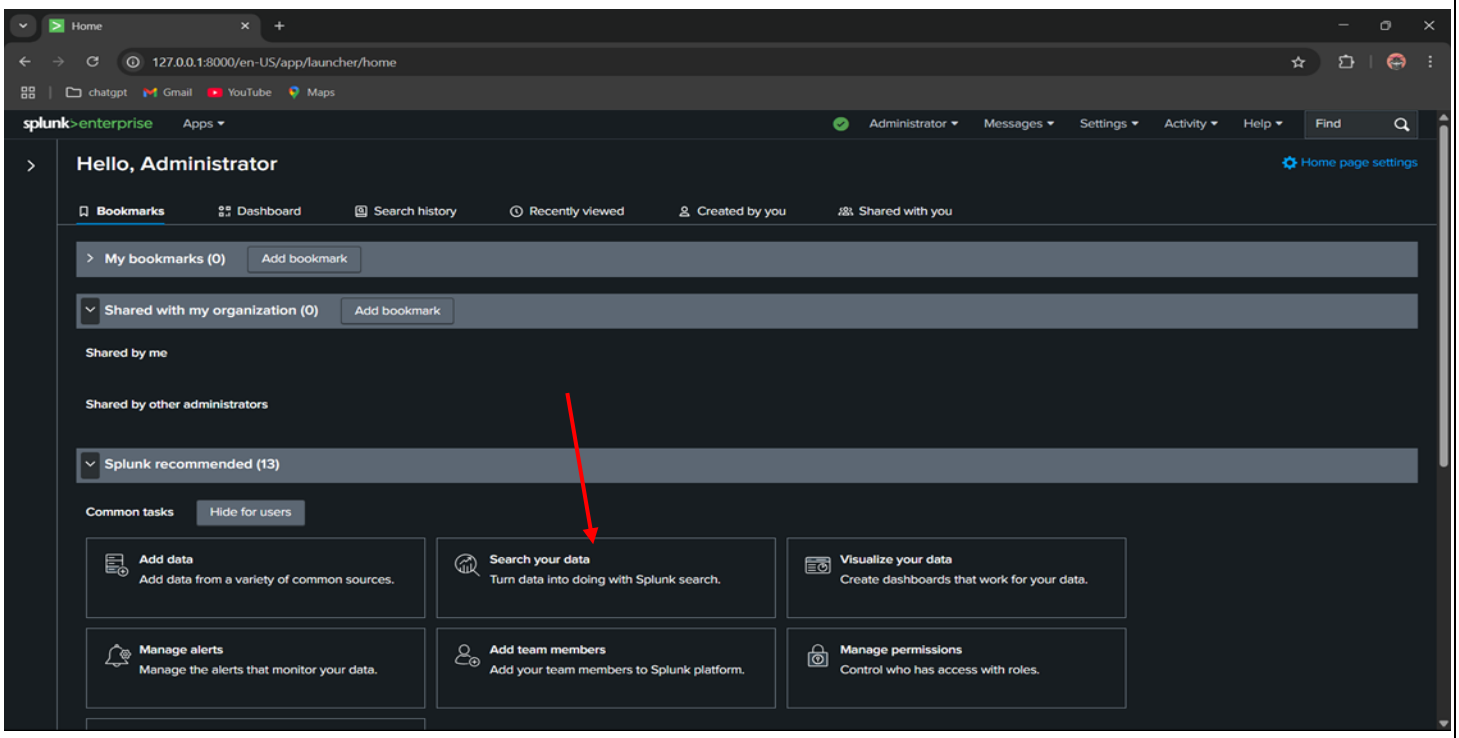
Step 1:

- Open Splunk, log in with your credentials, and navigate to the home page.



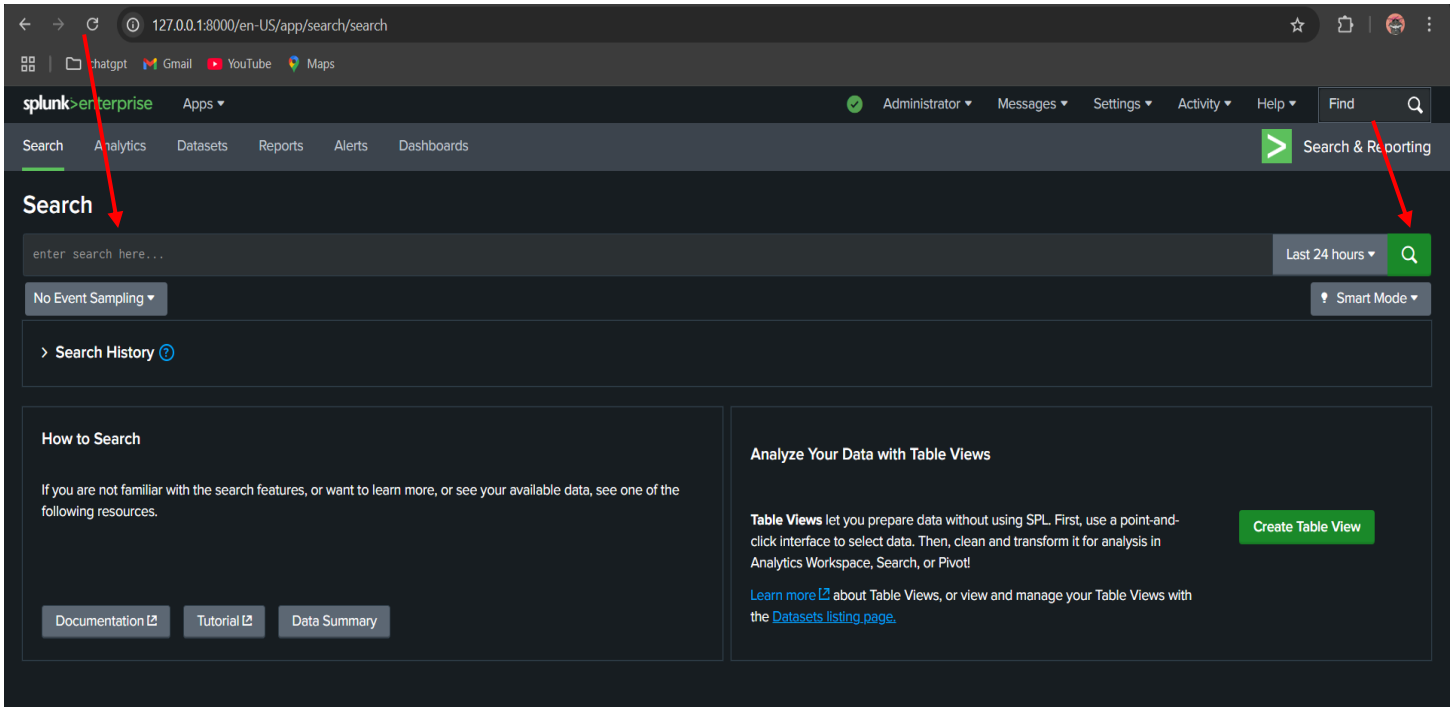
Step 2:

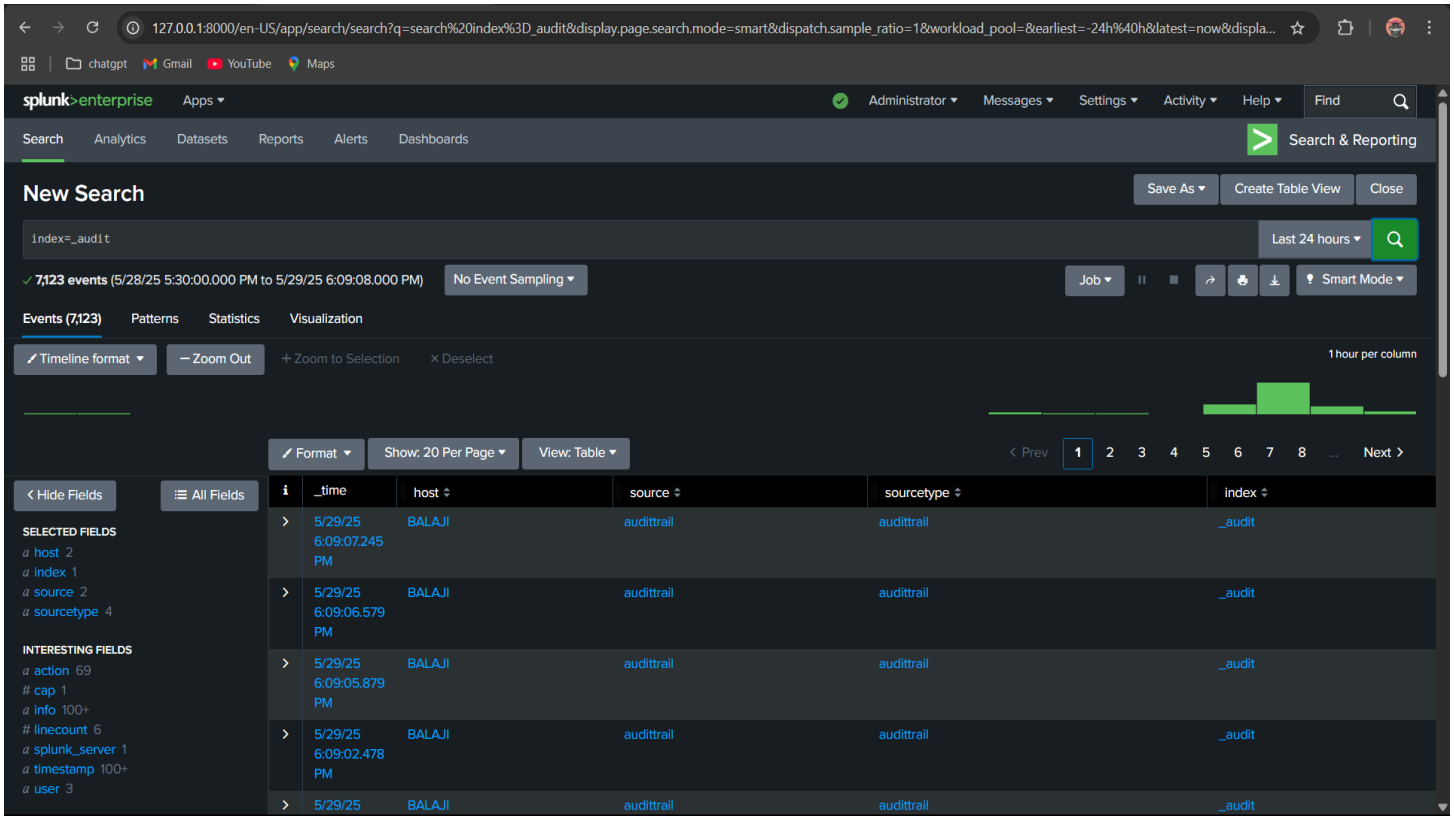
- Click on the Search to access and view your data.



Step 3:

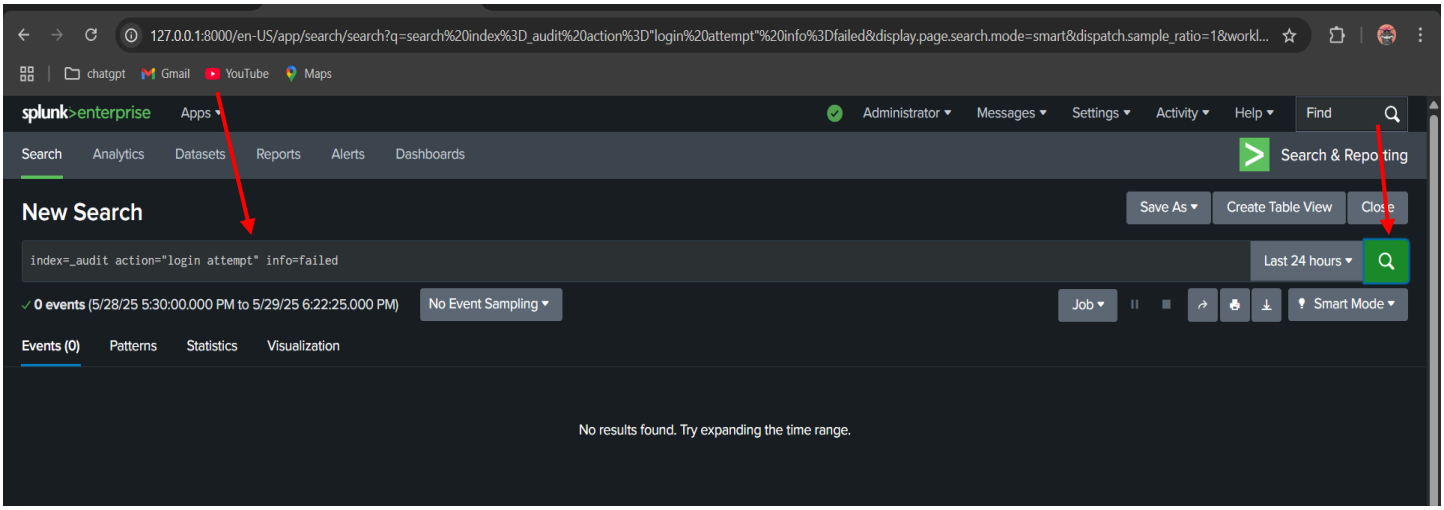
- In the search bar, enter the following command:
- index=_audit



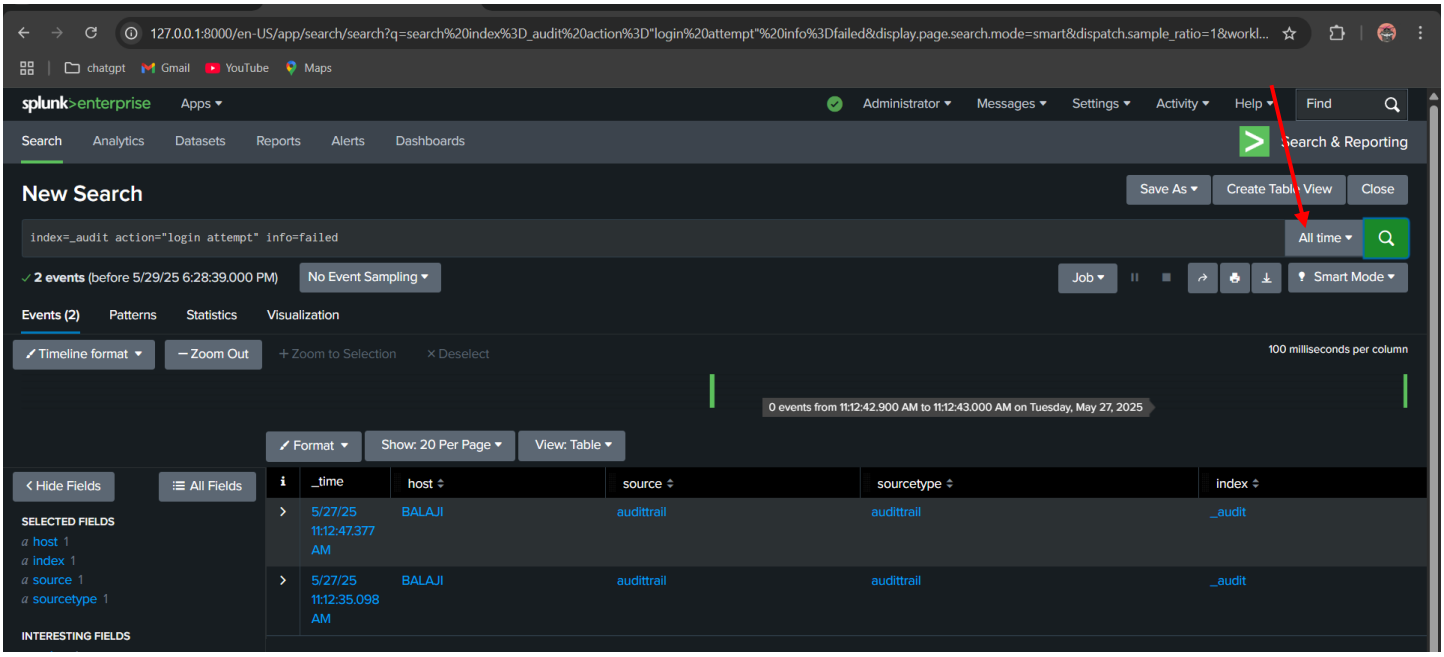


Step 4:

- You will now see some data returned. To filter only the failed login attempts, modify your search command as follows:
- index=_audit action="login attempt" info=failed



- After running the command, you may not see any data if there haven't been any failed login attempts in the last 24 hours. To ensure you capture any past events, expand the time range.
- Change the time range from Last 24 hours to All time before running the search.
- This adjustment increases the chances of retrieving relevant failed login events from the audit index.



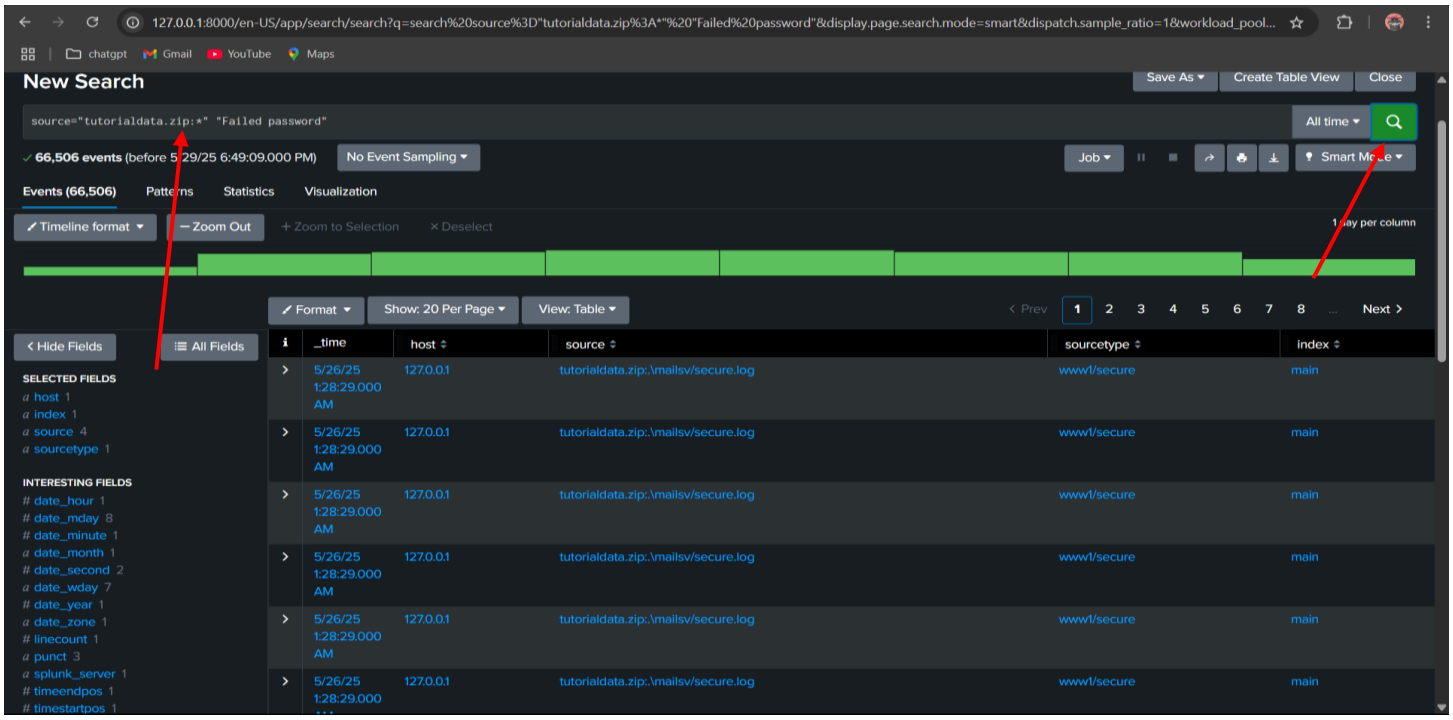
- Even after setting the time range to All time, only a few events (e.g., two) related to our search appear.
- This limited data is not ideal for creating meaningful reports and dashboards, as they rely on sufficient event volume to provide useful insights and visualizations.
- To address the issue of limited data, we will use the **tutorialdata.zip** file, which we previously uploaded during an earlier practical session. This file contains sample event data that is more suitable for creating reports and dashboards.
- Next, we'll write SPL (Search Processing Language) queries based on this tutorial data to generate meaningful insights.

Explanation:

- index=_audit tells Splunk to search within the audit index
- action="login attempt" filters the events to show only login attempts.
- info=failed further narrows it down to only failed login attempts.

Step 5:

- To view and filter failed login attempts from the tutorialdata.zip file, run the following SPL command in the search bar:
- source="tutorialdata.zip:*" "Failed password"

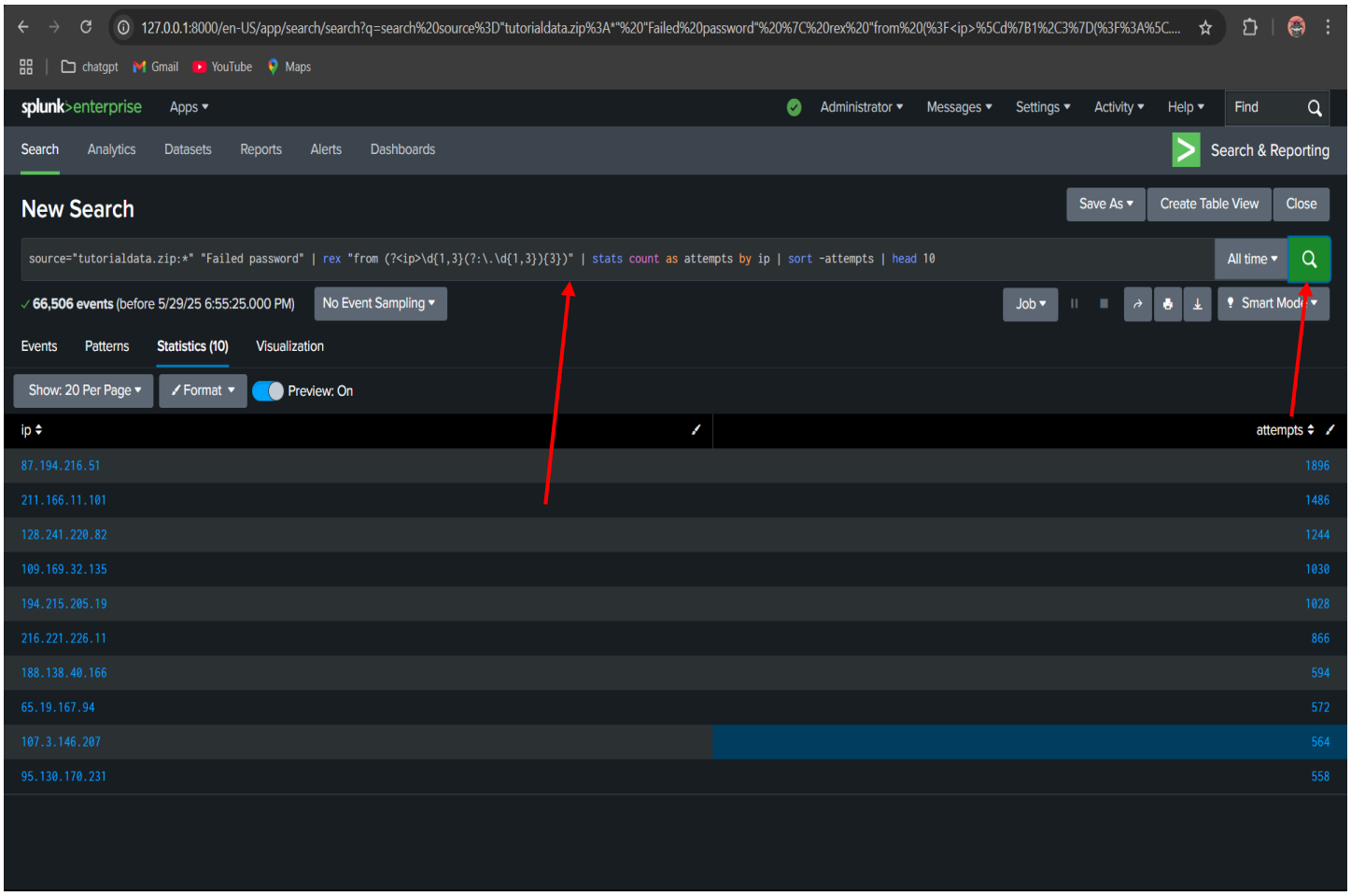


Explanation:

- source="tutorialdata.zip:*" filters events coming specifically from the tutorial data file.
- "Failed password" searches for events that contain the phrase “Failed password,” which indicates failed login attempts.
- This command helps isolate the relevant failed login events from the tutorial dataset.

Step 6:

- To further filter the data and identify the top 10 IP addresses with the most failed login attempts, extend your previous SPL command as follows:
- source="tutorialdata.zip:*" "Failed password"| rex "from (?<ip>\d{1,3}(?:\.\d{1,3}){3})" | stats count as attempts by ip | sort -attempts | head 10



Explanation:

- rex "from (?<ip>\d{1,3}(?:\.\d{1,3}){3})" extracts the IP address from the log message using a regular expression.
- stats count as attempts by ip counts the number of failed attempts per IP address.
- sort -attempts sorts the results in descending order based on the number of attempts.
- head 10 limits the output to the top 10 IP addresses.
- This refined query will give you a clear view of the IPs responsible for the most failed login attempts.

Step 7:

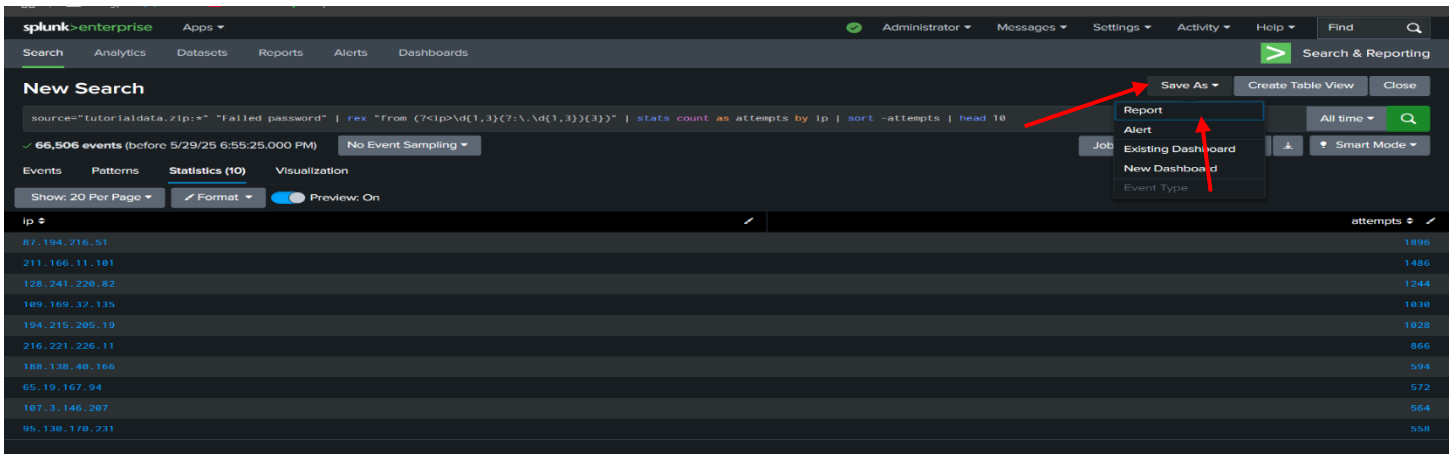
- Now that we have the required data, it's time to create a report based on the results.
- There are two main ways to create a report in Splunk:

1. **Data Report** – Displays the search results in a tabular format.
2. **Visualization Report** – Presents the data using charts or graphs (e.g., bar chart, pie chart) for easier interpretation and insights.

- You can choose the type of report depending on how you want to present and analyze the data.

Step 8:

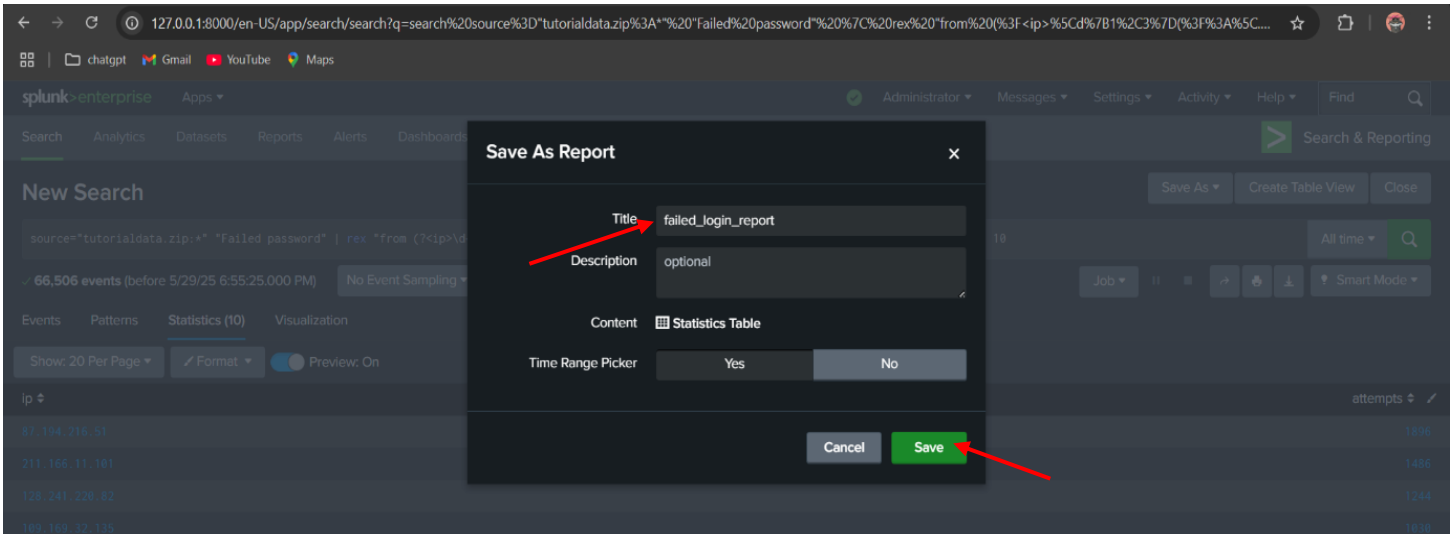
- To create a report from your data, click on the Save As button above the search results and select Report from the dropdown menu.



Step 9:

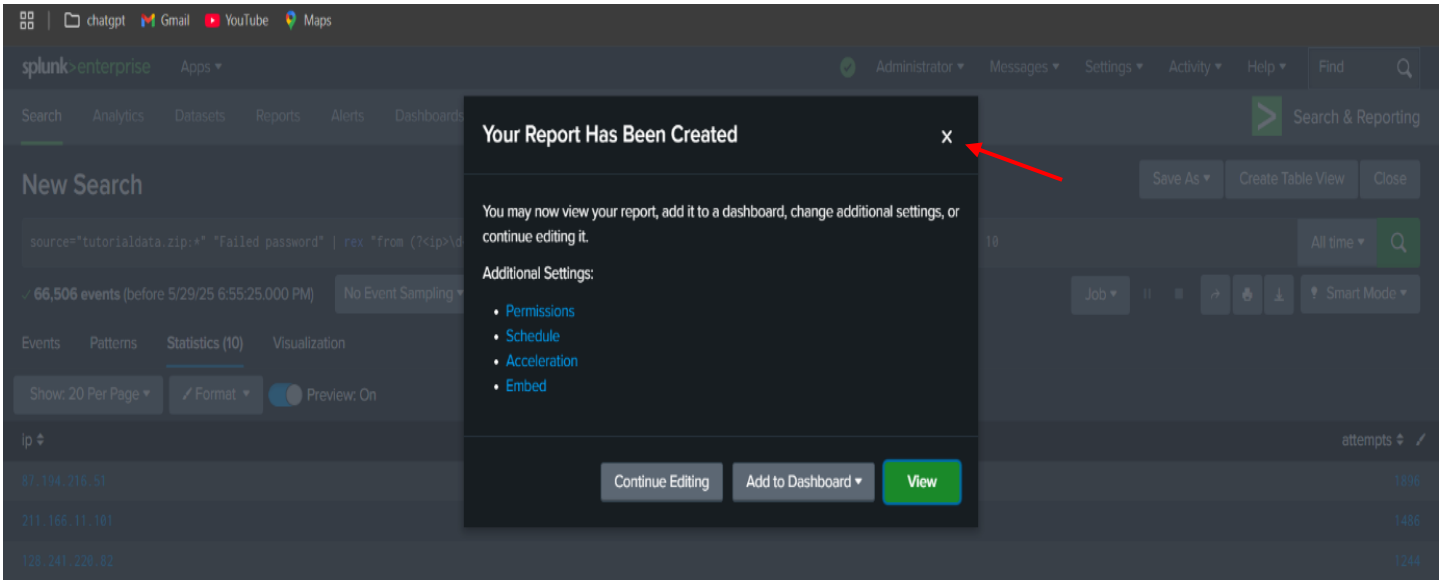
- In the pop-up window, enter a title for your report and click on save.

Note: The title is case-sensitive. Avoid using spaces or special characters to prevent potential errors. Use underscores (_) or hyphens (-) instead of spaces if needed.



Step 10:

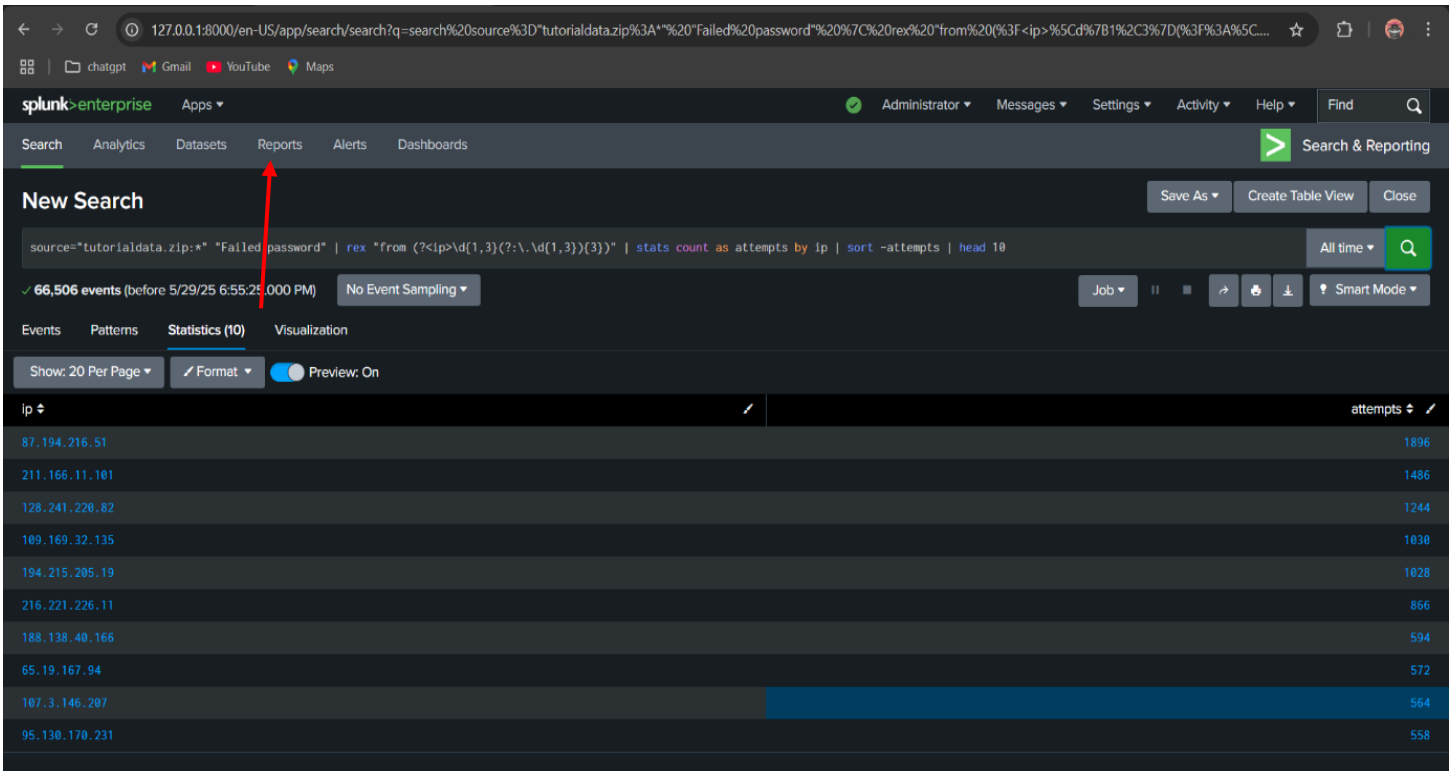
- After saving the report, a confirmation pop-up will appear stating that the report has been successfully created.
- You can either, click "View" to open and review the report immediately, or close the window to return to the search results or continue working.



- Your report is now saved and accessible from the Reports section in Splunk.

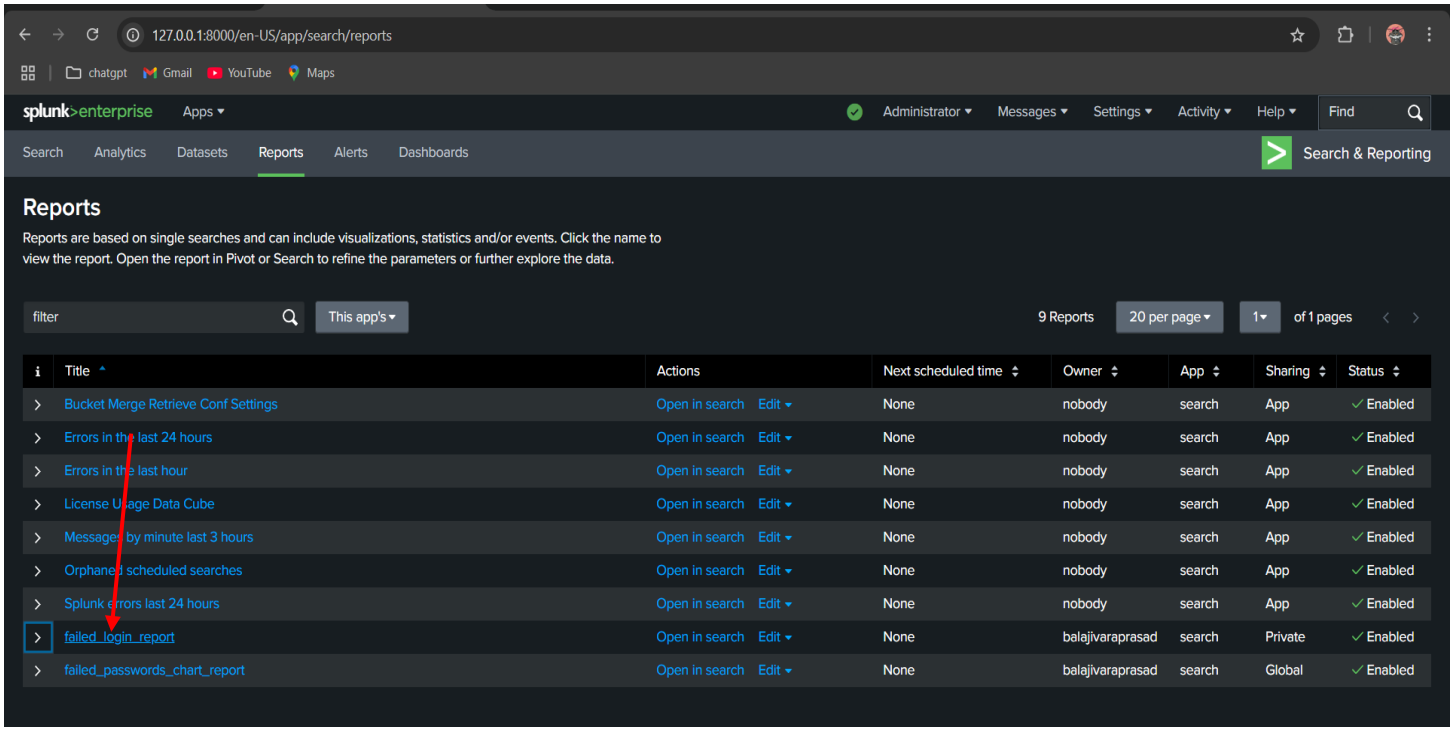
Step 11:

- To view your saved reports, navigate to the Reports section in Splunk by clicking on Reports from the navigation menu.
- Here, you will find a list of all your saved reports, including the one you just created. You can open, edit, or schedule reports from this section.



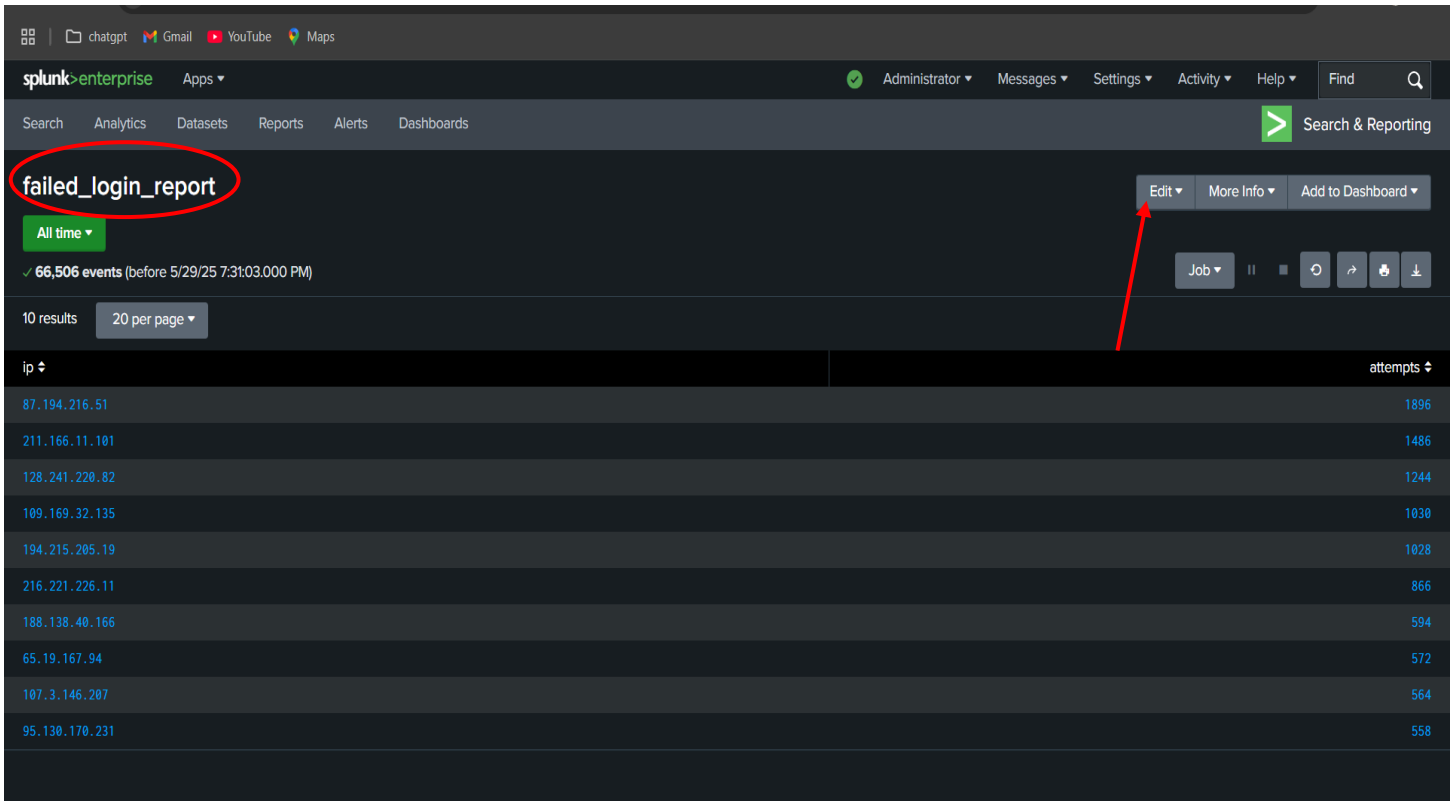
Step 12:

- Your saved reports will now be displayed in a list.
- Locate and click on the report you just created to open and view its contents.
- You can choose to edit the report to update its title, description, permissions, or visualization type.
- You also have the option to export the report in various formats (e.g., CSV, PDF) or schedule it to run automatically at specified intervals.



Step 13:

Once you open the saved report, it will display the failed login data based on your search query. To make changes to the report, click on the Edit option. This allows you to modify the report.

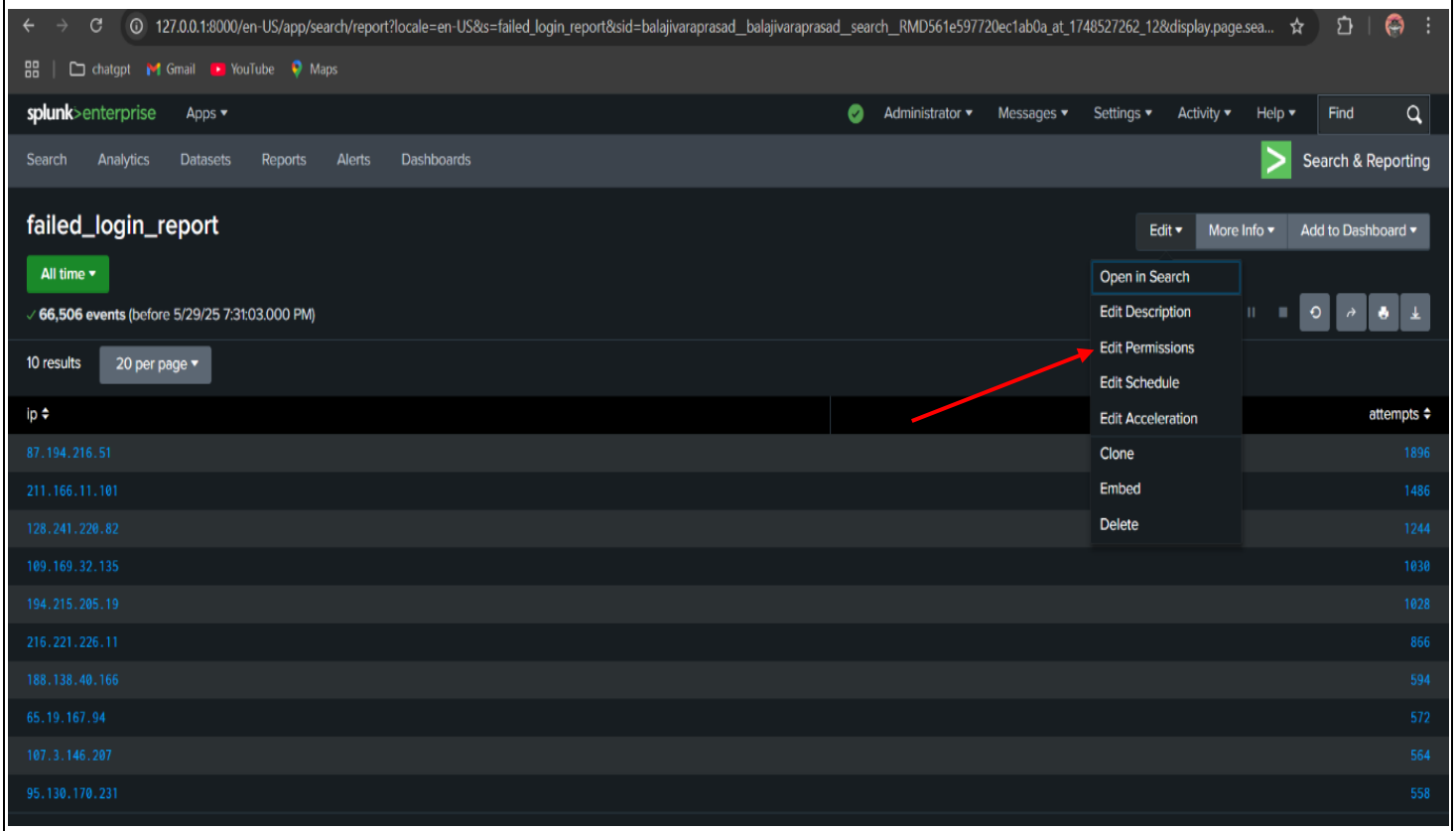


Step 14:

After clicking on Edit, a dropdown menu appears with several options for modifying the report:

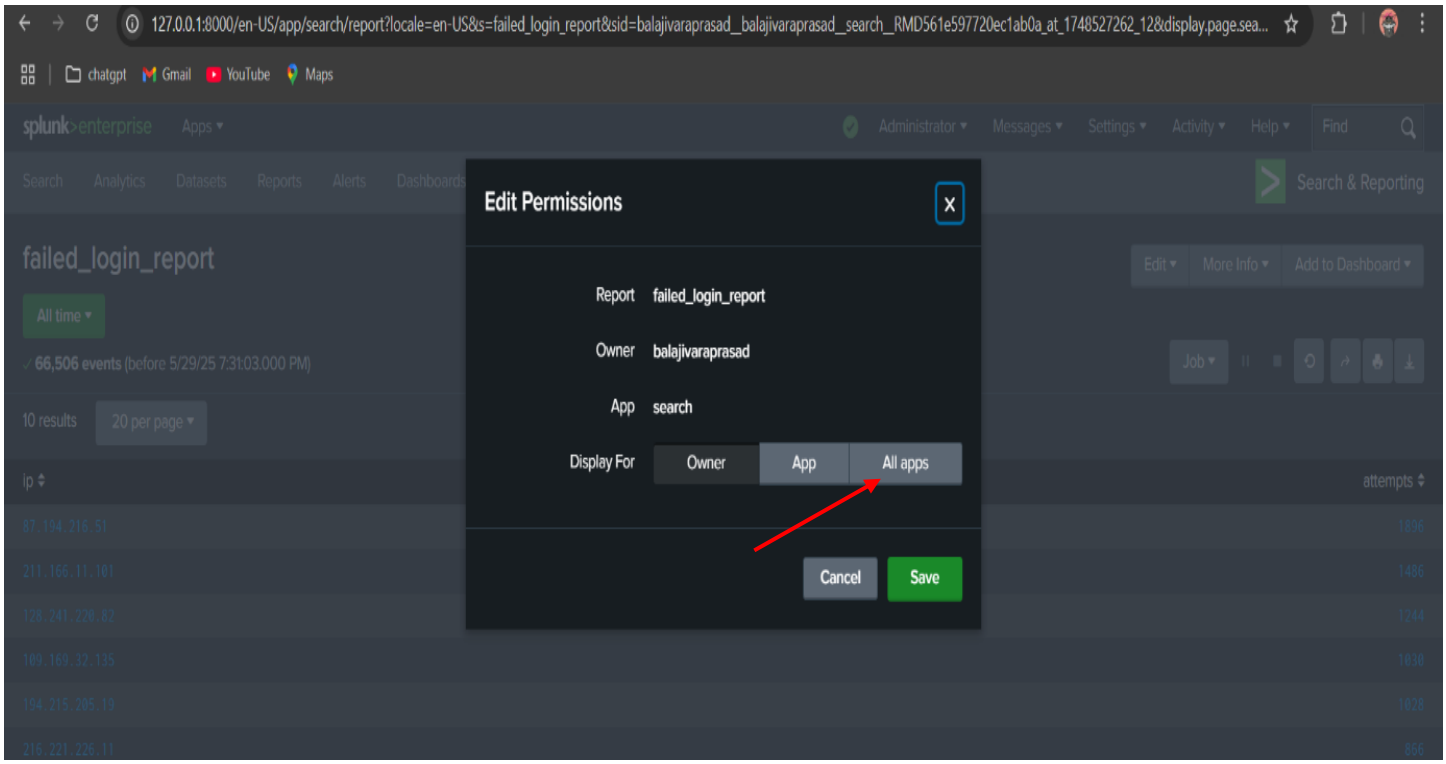
- **Open in Search** – Opens the underlying search query for further editing.
- **Edit Description** – Add or update the report's description.
- **Edit Permissions** – Manage who can view or modify the report.
- **Edit Schedule** – Set up automated scheduling for the report.
- **Edit Acceleration** – Enable or configure report acceleration for performance.
- **Clone** – Create a duplicate of the report.
- **Embed** – Generate an embed link to use the report externally.
- **Delete** – Remove the report permanently.

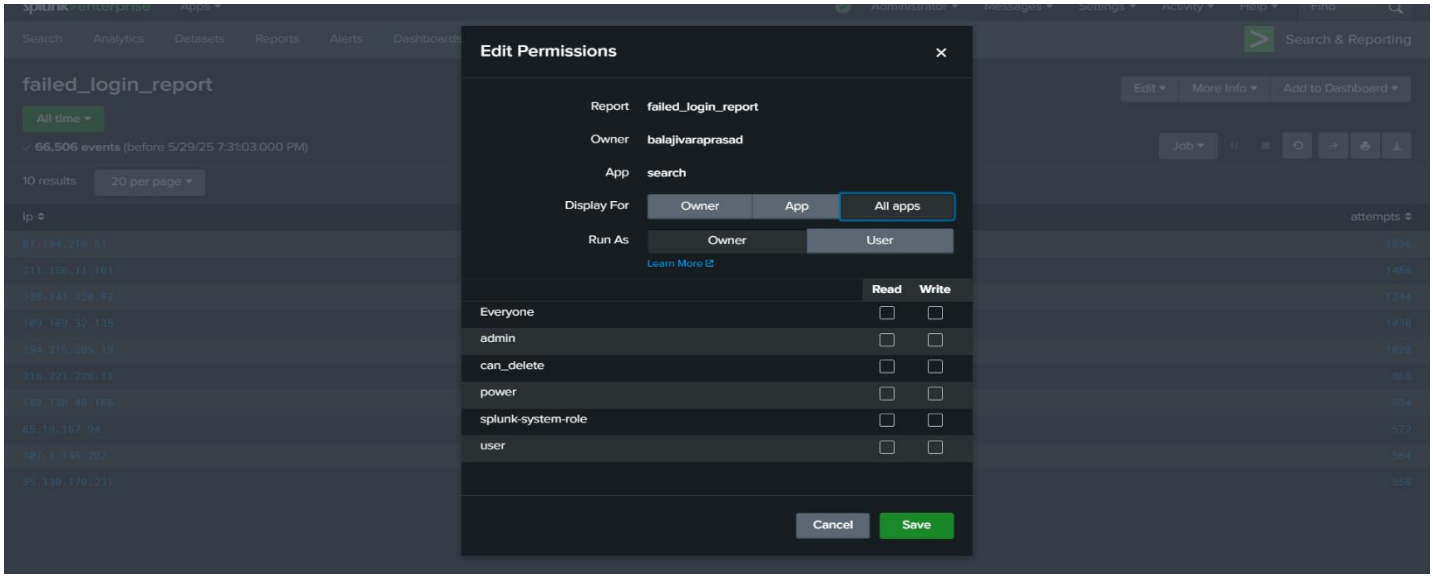
For this step, we'll focus on Edit Permissions, which is crucial for controlling access and ensuring security. This allows you to define who can view or edit the report, an essential step for managing sensitive data visibility.



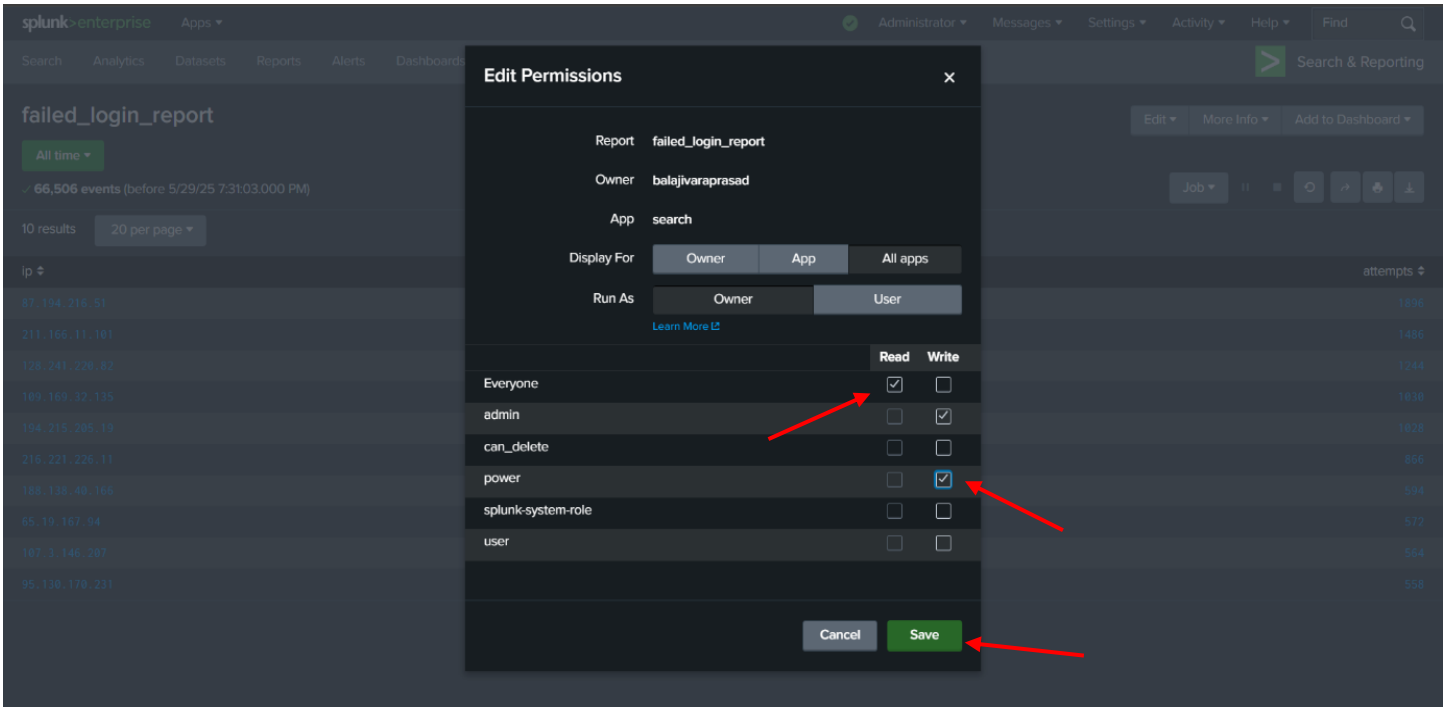
Step 15:

- After selecting Edit Permissions, a dialog box will appear where you can configure access settings for your report.
- First, review the report details.
- Set the visibility by selecting All apps under the "Display For" section. This allows the report to be accessed from any app within Splunk.





- Under the Permissions section, you'll see a list of user roles including:
    - Everyone
    - admin
    - can_delete
    - power
    - splunk-system-role
    - user
- You can assign **Read** and **Write** permissions to each role.



- In this example: The Everyone role has been granted Read access, meaning all users can view the report. The power role has been given Write access, allowing users with this role to edit the report.
- After making the necessary changes, click Save to apply the new permissions**.**

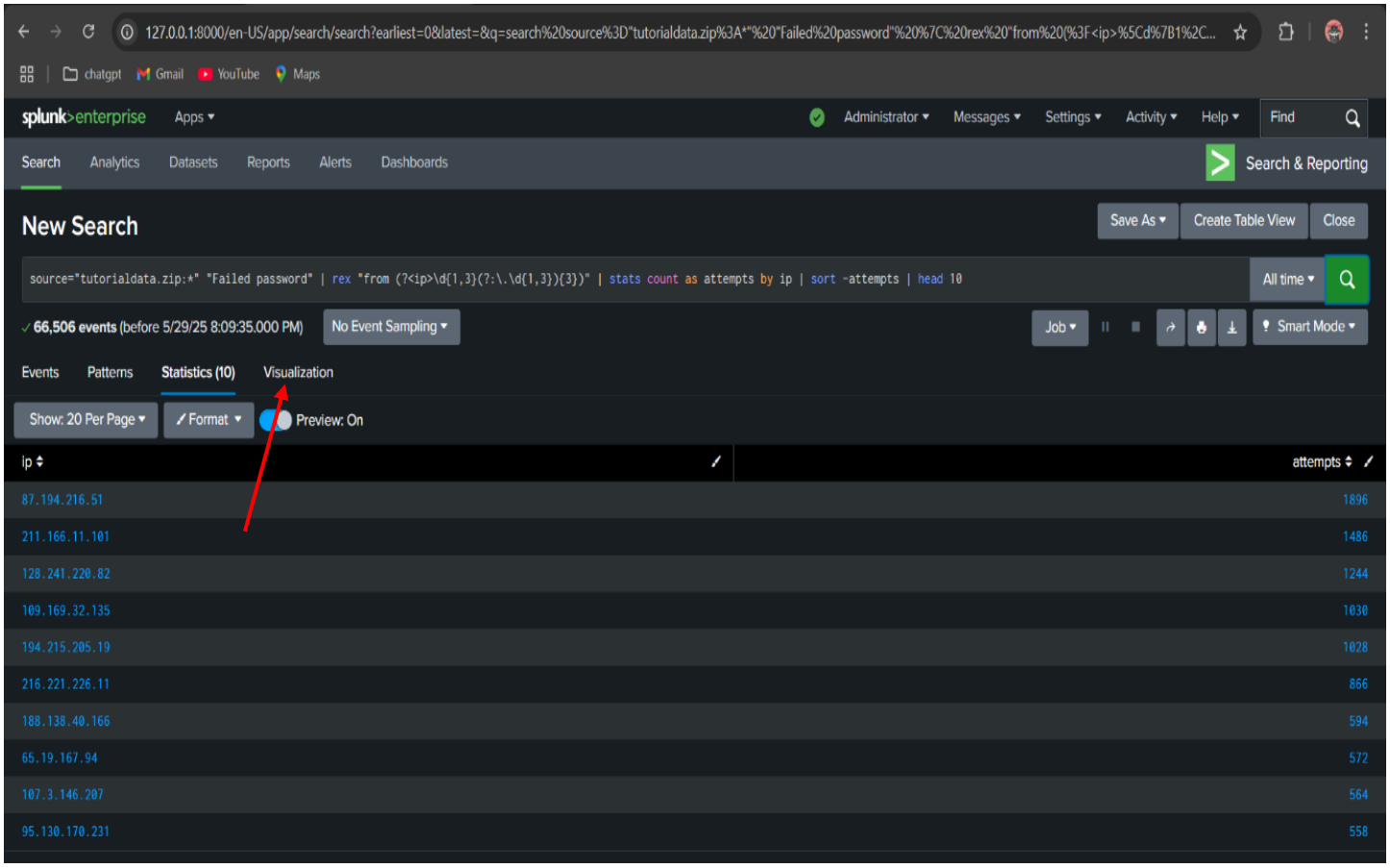
Step 16:

- Now, we will generate a visual report by representing the data using various chart and graph types available in Splunk. This helps in better understanding and interpretation of the data trends and patterns.

- To create the visual report, we will use the same dataset as in the previous data report.
- Navigate to a new search window in Splunk and enter the same SPL (Search Processing Language) command used earlier.
- Set the time filter to "All Time" to ensure we extract the complete dataset for accurate visualization.

Step 17:

Once the results are displayed, click on the "Visualization" tab to view the graphical representation of the data. Splunk provides various visualization options such as bar charts, pie charts, and line graphs, which help in understanding trends and patterns more effectively.



Step 18:

At this stage, the data is displayed using a column chart. In this visualization, the X-axis represents the IP addresses, while the Y-axis indicates the number of

attempts associated with each IP. This graphical format provides a clear and concise way to analyze which IPs have the highest or lowest number of attempts, making it easier to identify patterns or anomalies.

Step 19:

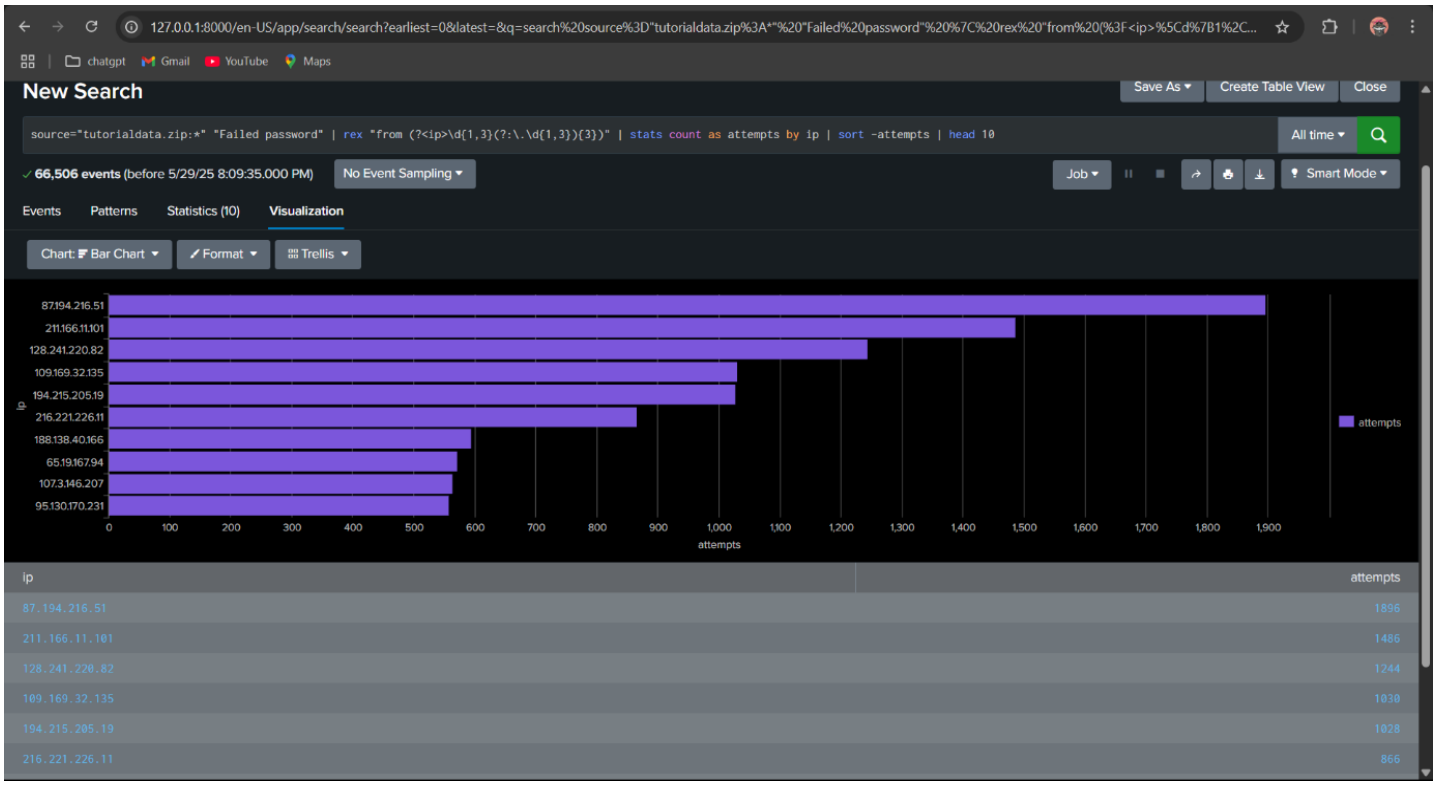
To modify the type of chart used for visualization, click on the chart type dropdown menu located within the "Visualization" tab. A list of available chart types such as line charts, pie charts, area charts, and more will appear. You can select any of these options to display your data in the format that best suits your analysis needs.

Note:

Not all data types are suitable for every chart format. It is important to choose a chart type that accurately represents the structure and nature of your data for clear and meaningful visualization.

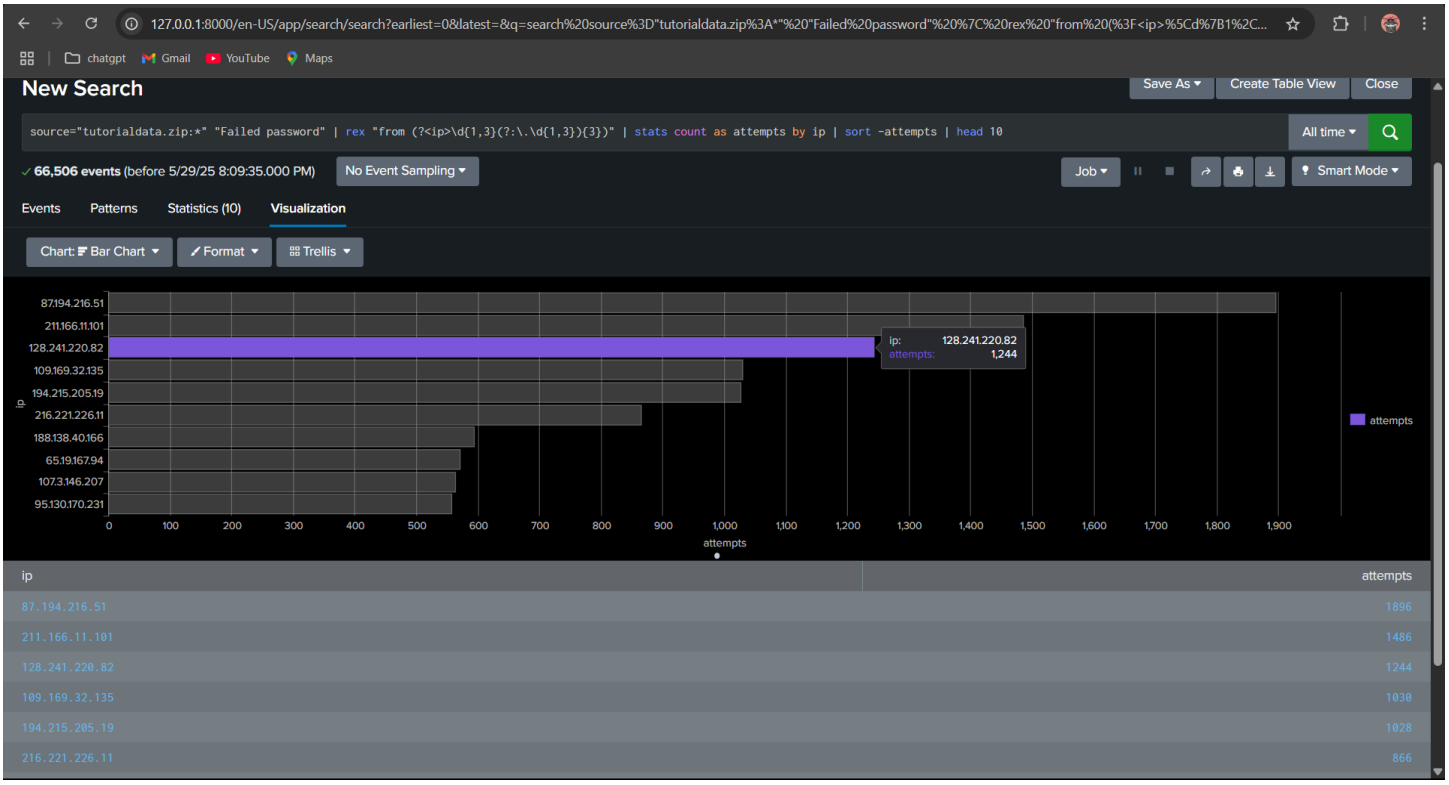
Step 20:

For my visualization, the Bar Chart has been selected to represent the data. In this format, the Y-axis displays the IP addresses, while the X-axis shows the number of attempts associated with each IP.



Step 21:

To view more details about a specific data point, hover your cursor over any individual bar this will display additional information related to that particular IP address.



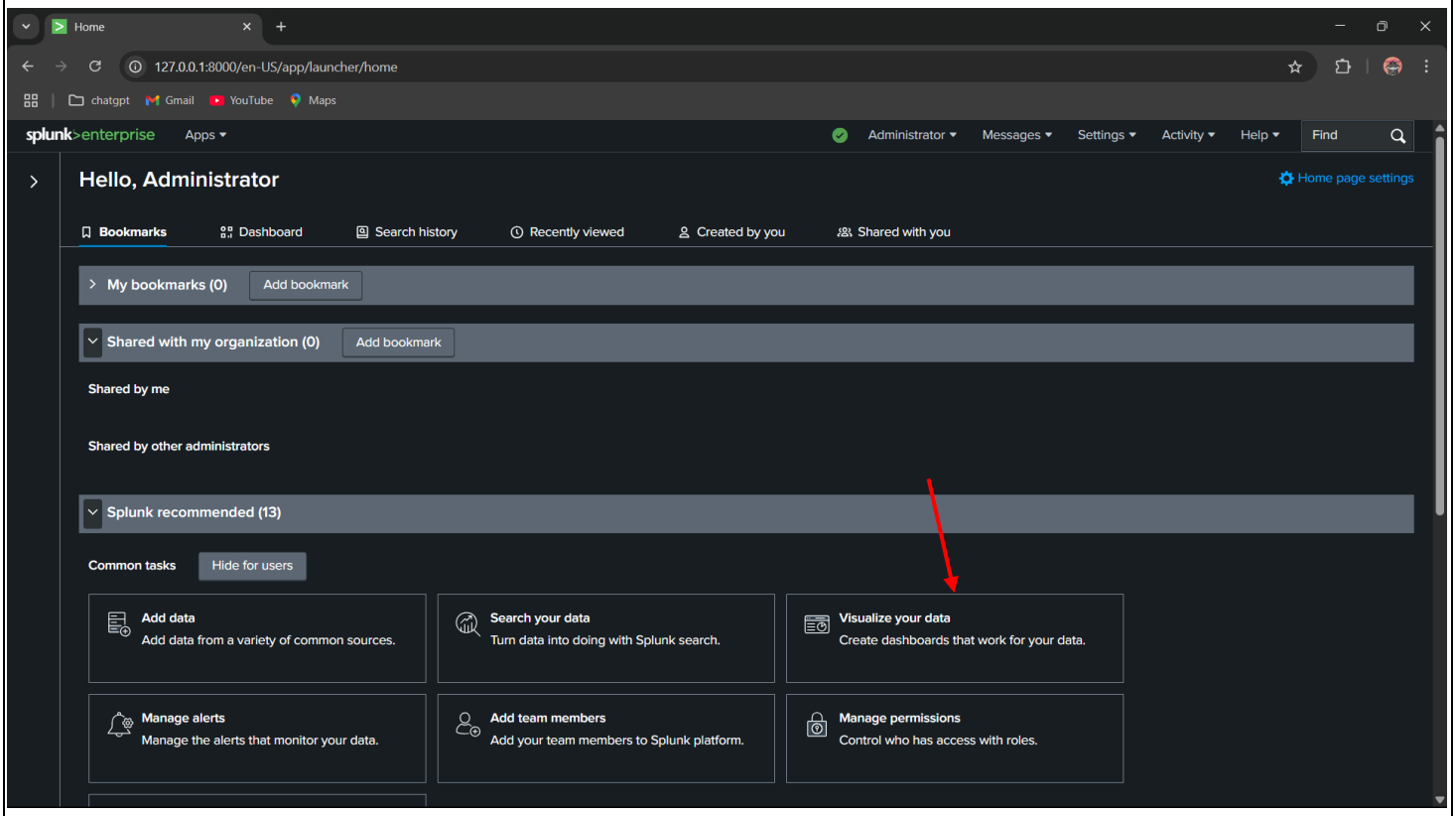
Now that the data visualization is complete, Now you can save this graph data report , by using the same proccess before, which we used to save raw report data. it's time to create a dashboard. Dashboards in Splunk allow you to combine multiple visualizations and reports into a single, interactive view, making it easier to monitor, analyze, and share insights from your data.

Step 22:

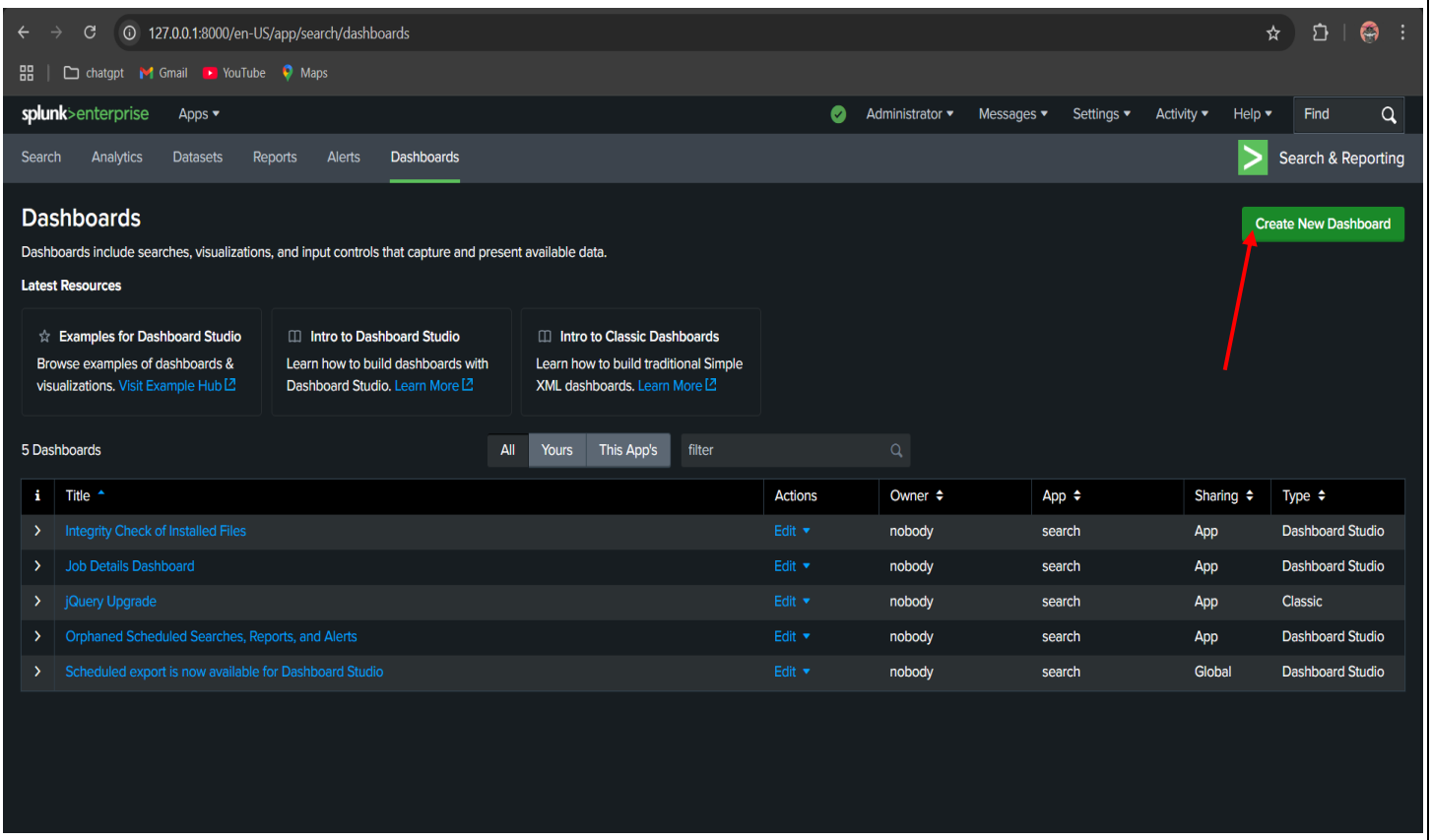
To begin creating the dashboard, first return to the Splunk Home Page. This can be done by clicking on the Splunk logo or selecting “Home” from the navigation menu. From there, you will have access to the dashboard creation options.

Step 23:

Once on the home page, click on "Visualize your data" to begin the process of creating a new dashboard. This section provides tools to design and organize visual reports in a consolidated and interactive format.

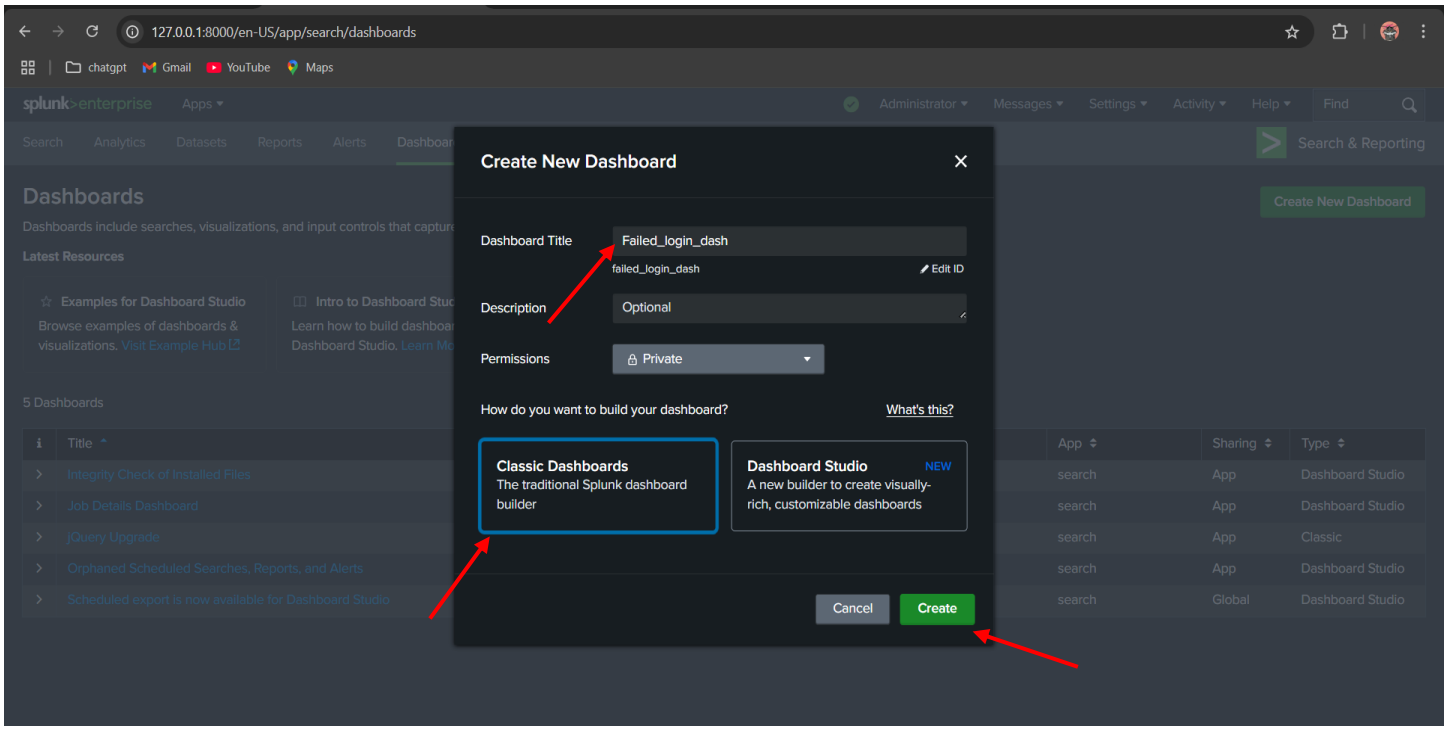


Step 24: After clicking on "Visualize your data", you will be directed to the dashboard creation interface. Click on "Create New Dashboard" to begin.



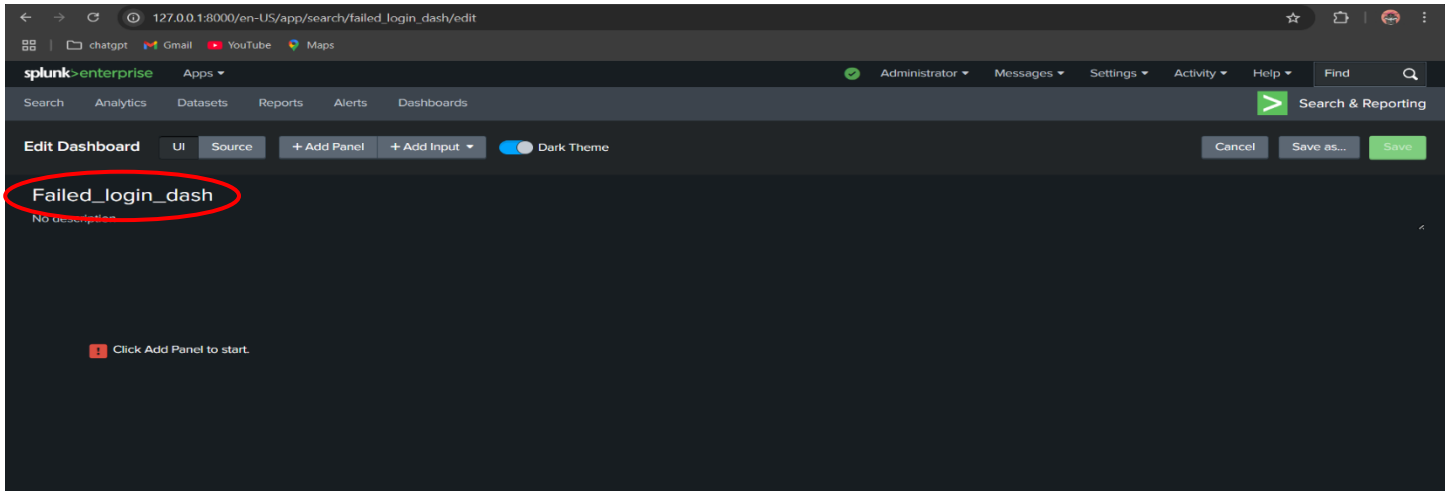
Step 25:

You will be prompted to enter details such as the dashboard title, description, and permissions (private or shared). Fill in the required information and click "Create" to proceed.



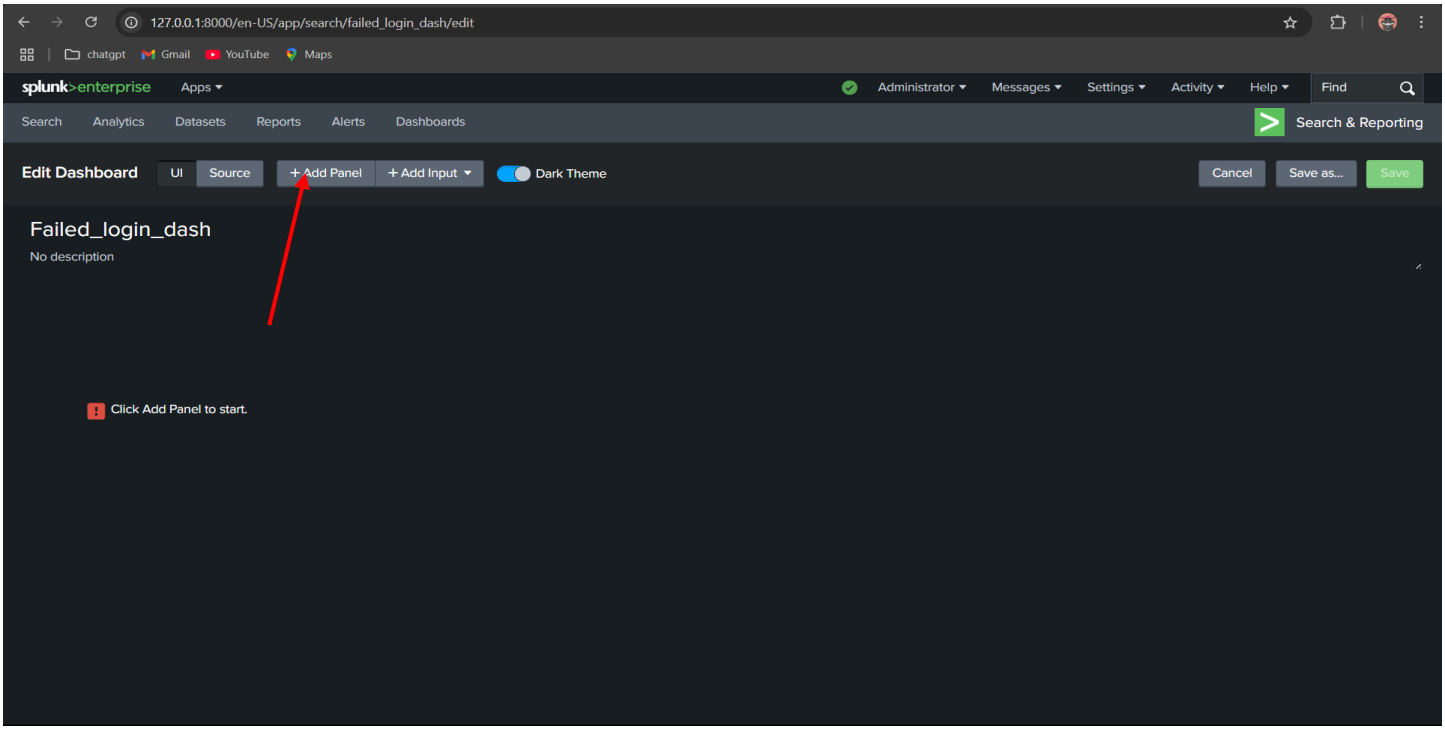
Step 26:

After creating the dashboard, you will be automatically redirected to the newly created dashboard interface. At this point, the dashboard will be empty, with no visualizations or data panels added yet. You can now begin adding content to build your customized dashboard view.



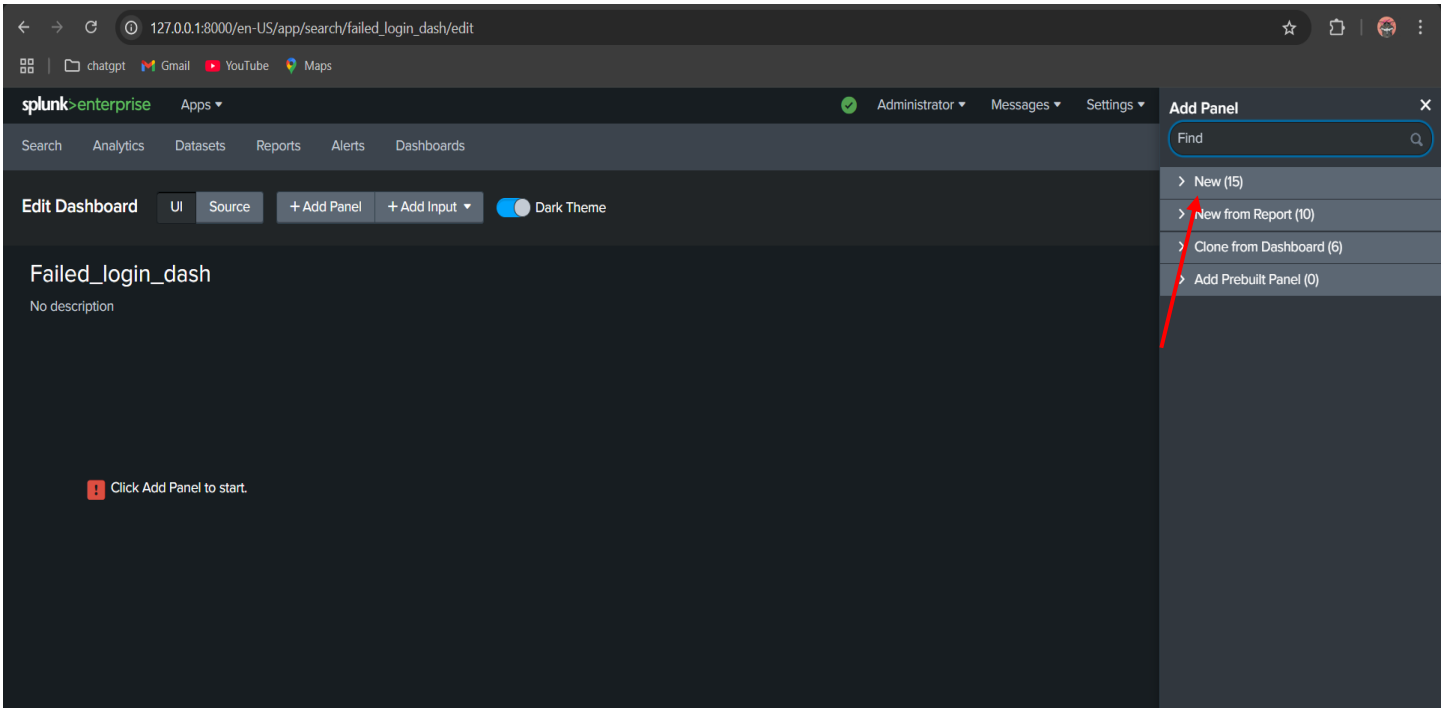
Step 27:

Click on the “Add Panel” button.



Step 28:

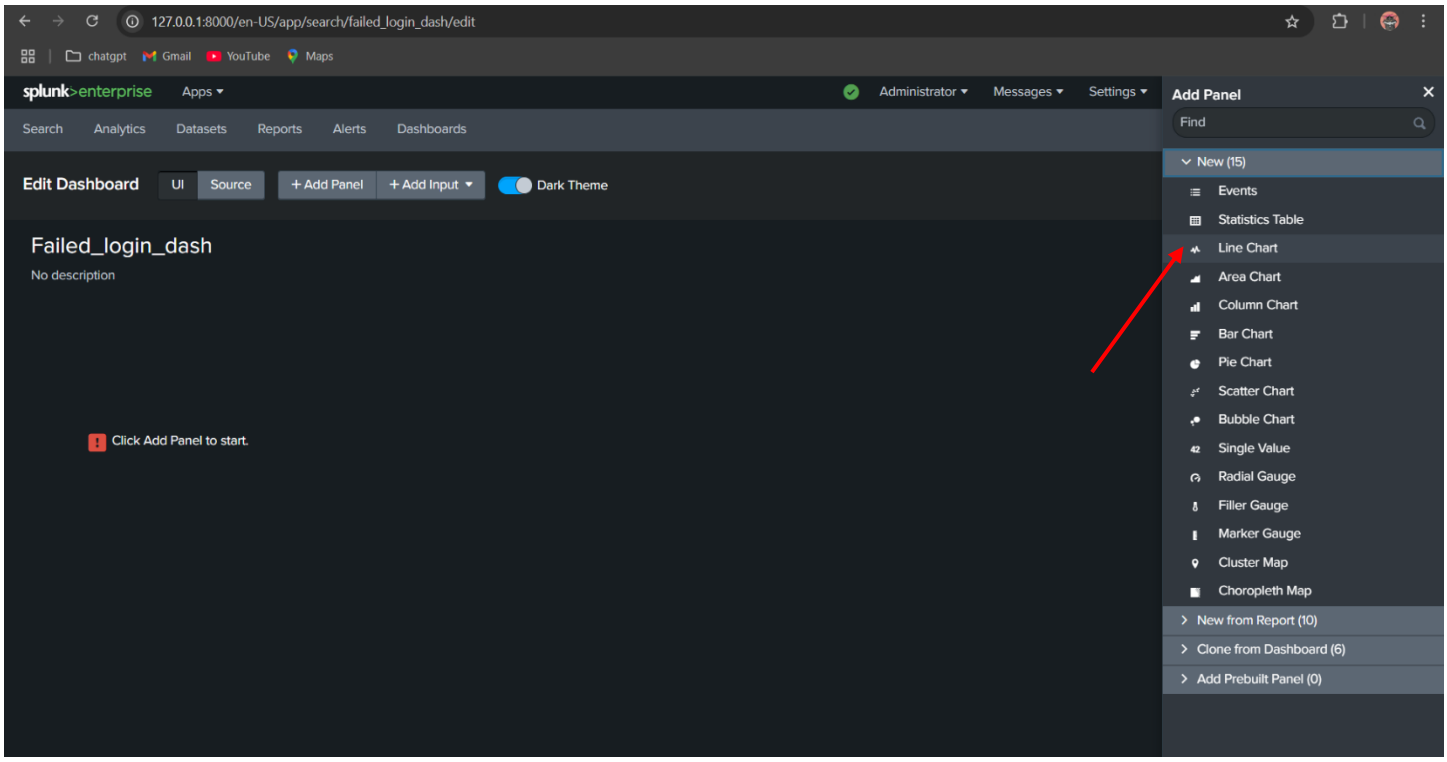
After clicking on “Add Panel”, a pop-up window will appear with multiple options: New, New from Report, Clone from Dashboard, and Add Prebuilt Panel.



Since we are creating a new dashboard from scratch, click on the “New” option. A dropdown menu will appear, allowing you to define the type of panel you want to create.

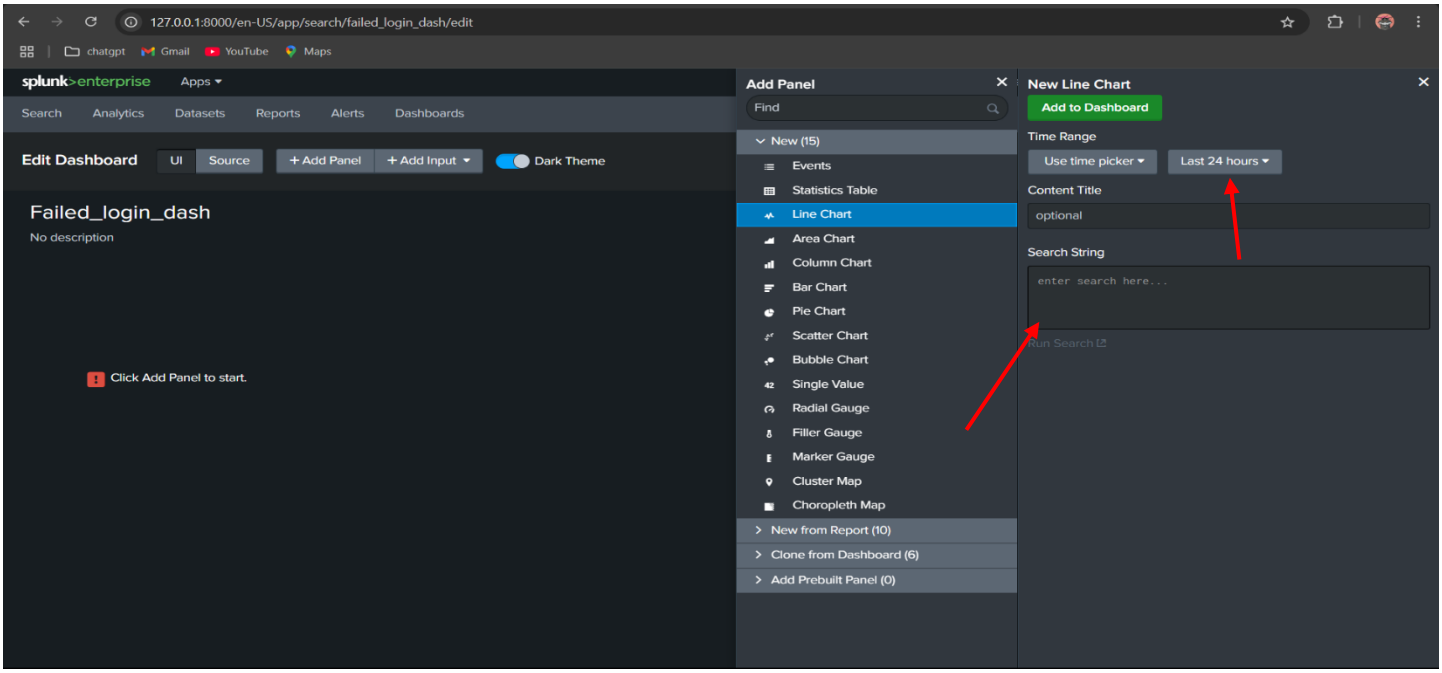
Step 29:

In the dropdown menu under the “New” option, you will see a variety of chart types available for selection, such as line charts, bar charts, pie charts, and more. Choose the chart type that best represents your data. For this example, a Line Chart has been selected as the initial visualization to display our data**.**



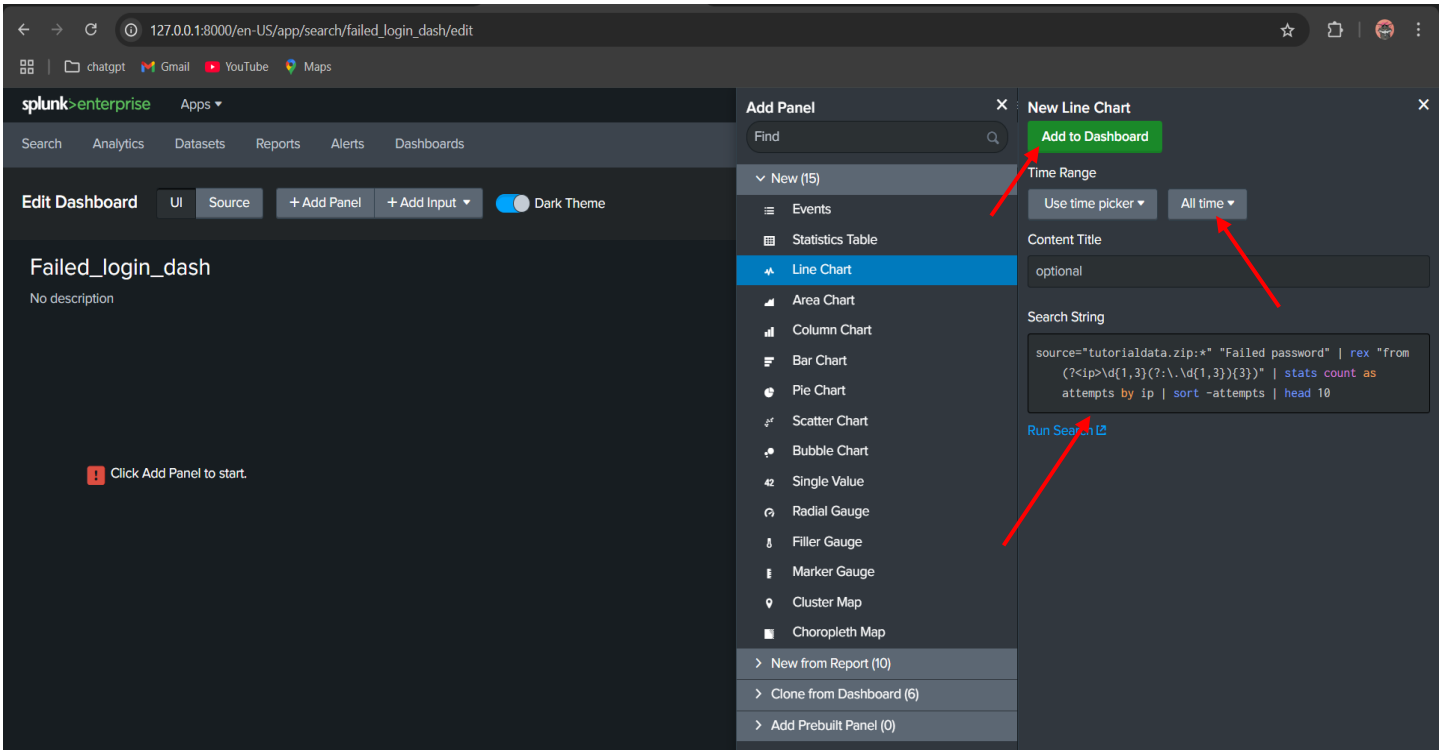
Step 30:

After selecting the line chart, a new dialog box appears prompting you to specify the time range and the data string you want to add to the dashboard.



Step 31:

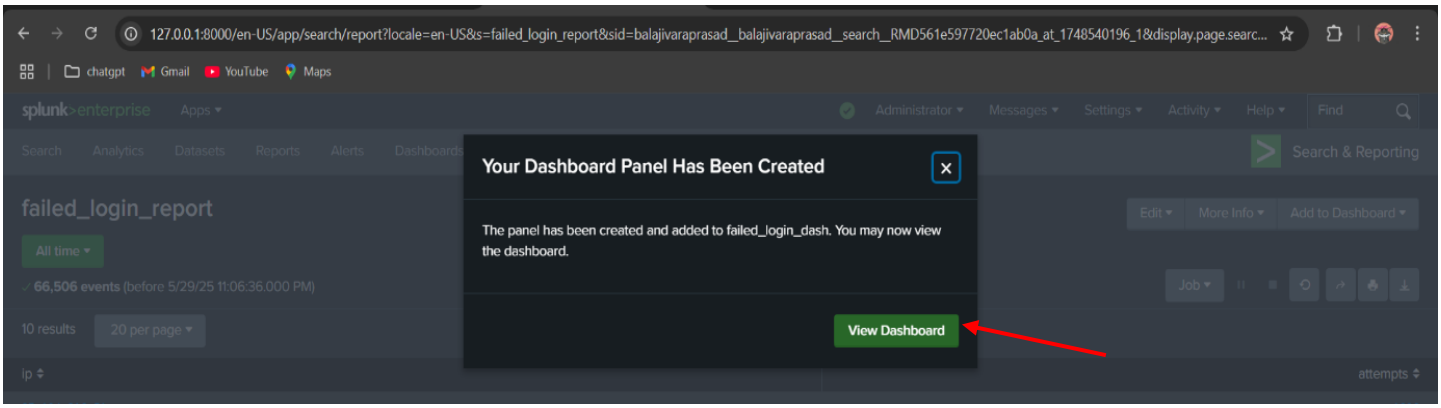
In the search string, enter the SPL (Search Processing Language) command used to retrieve the desired data. For consistency and easier understanding, use the same SPL command that was previously used in the search bar to fetch failed login data and also set the time filter to “all time” as we used same filter before



and click add to dashboard. This allows you to analyze the same data in the dashboard.

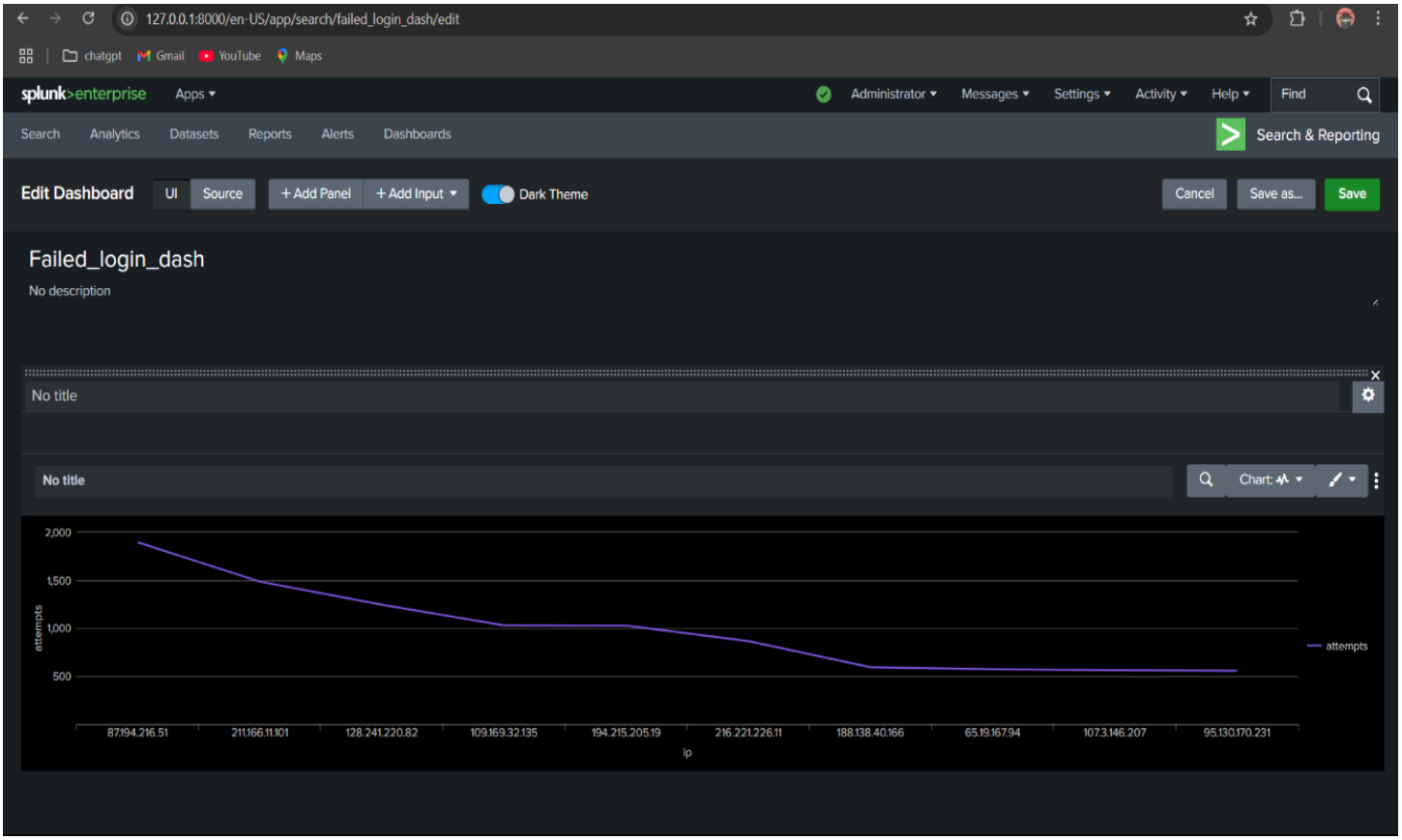
Step 32:

We can see our new dashboard has been created and click on view dashboard.



Step 33:

The data is now displayed as a line graph on the dashboard.



Step 34:

In a Splunk dashboard, you can view multiple types of data visualizations simultaneously. Now, we will add another type of graph to this same dashboard using the same failed login data.

Step 35:

To add another graph to the same dashboard, repeat the process described in steps 27 to 32. But select the different type of chart to represent your data. Here I selected bar chart to visualize the data.

Note: Don't create new dashboard, countine same procces from step 27 which we done before to add the new graph in that failed login dashboard.

Step 36:

After adding the new graph, both graphs displaying the same data will be visible on the dashboard.

Step 37:

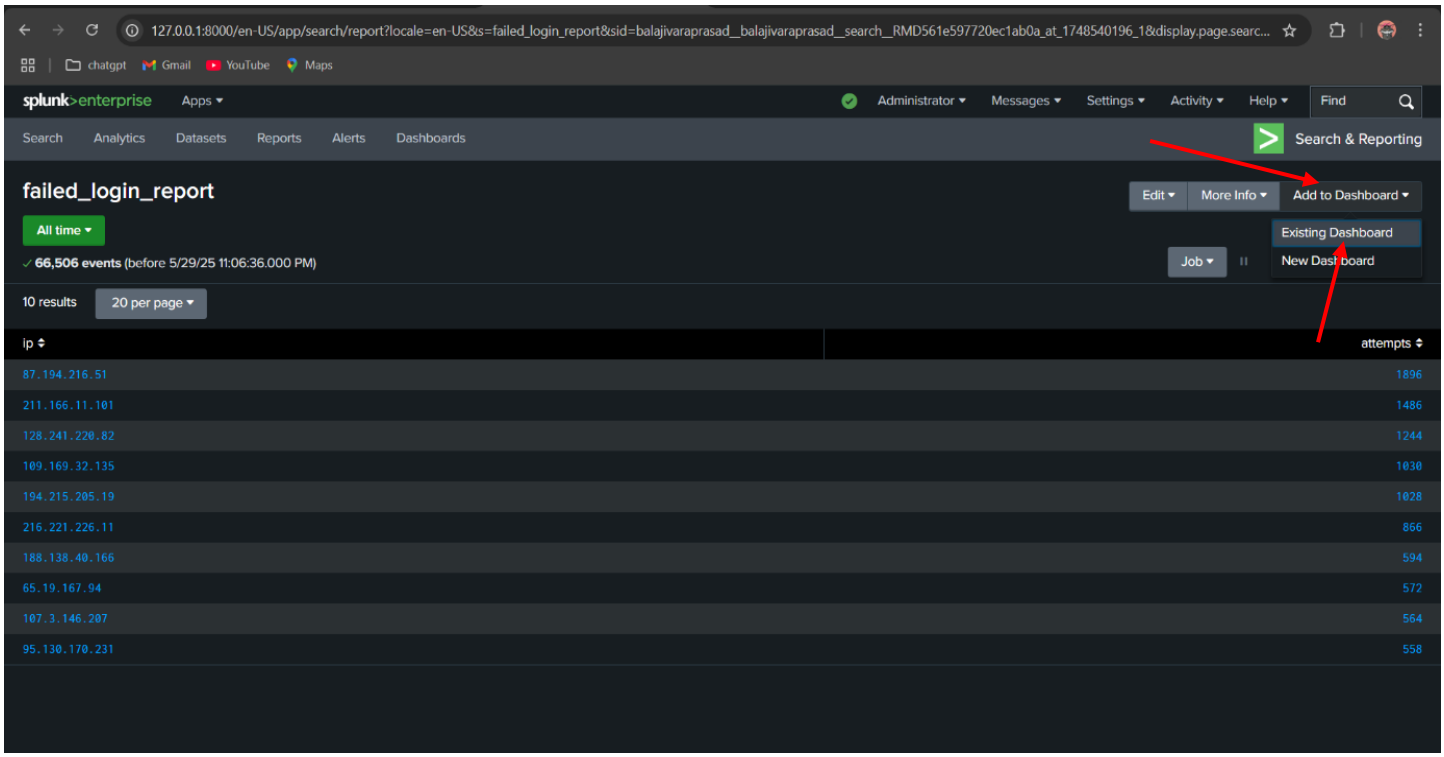
After arranging both graphs in the dashboard, we can also enhance the dashboard by importing raw data from previously created reports. For this step, let's import the raw data from the "Failed Logins" report we created earlier. This allows us to display both visual insights and detailed log data in a single view for better analysis.

Step 38:

To import data from an existing report, navigate to the Reports section in Splunk. Locate and open the report named "failed_login_report", which we created earlier. This report contains the raw data related to failed login attempts that we will add to the dashboard.(Follow step 11 and 12 to open "failed_login_report" reports data.)

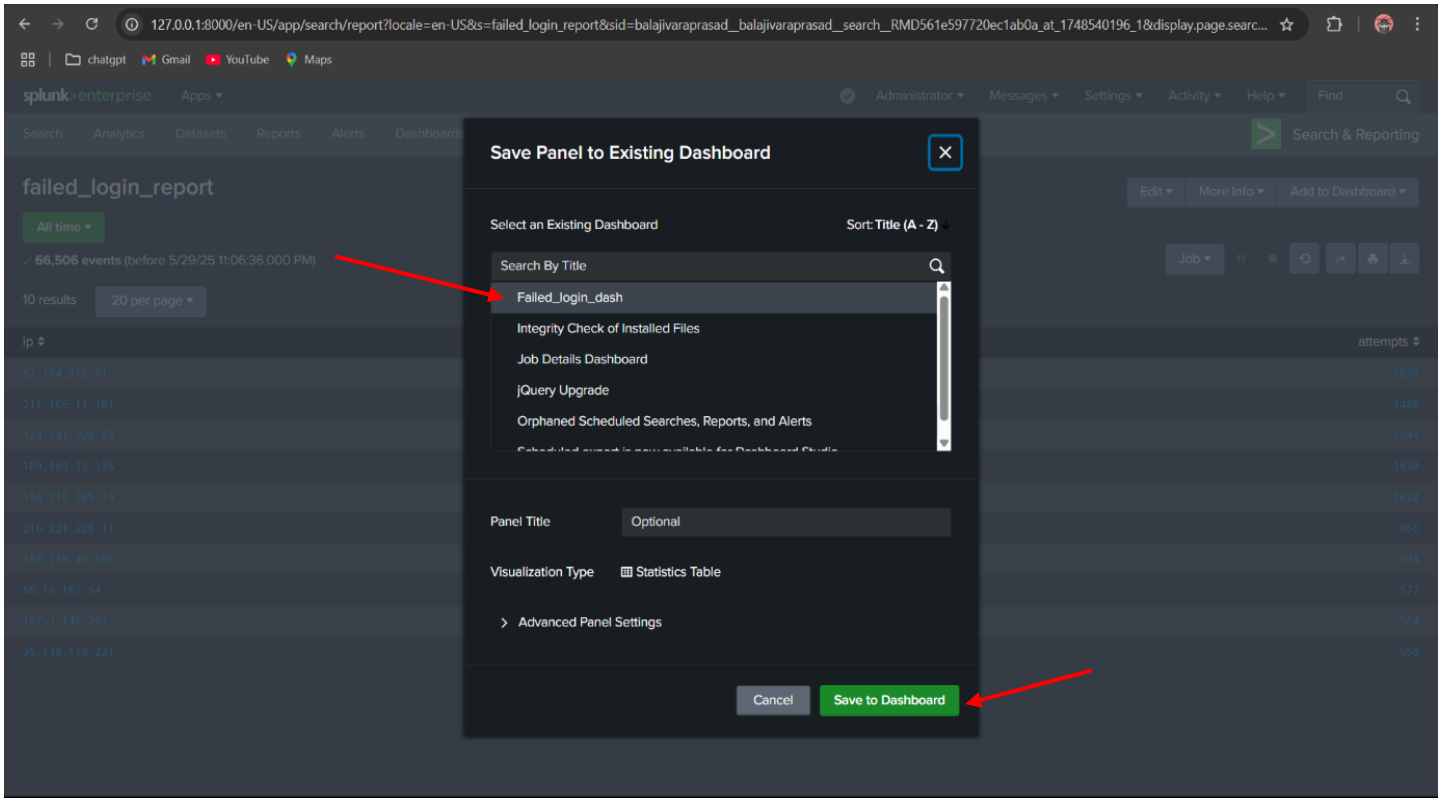
Step 39:

Once the report is open, click on the "Add to Dashboard" option. From the available choices, select "Existing Dashboard" to add the failed login report to the dashboard you've already created.



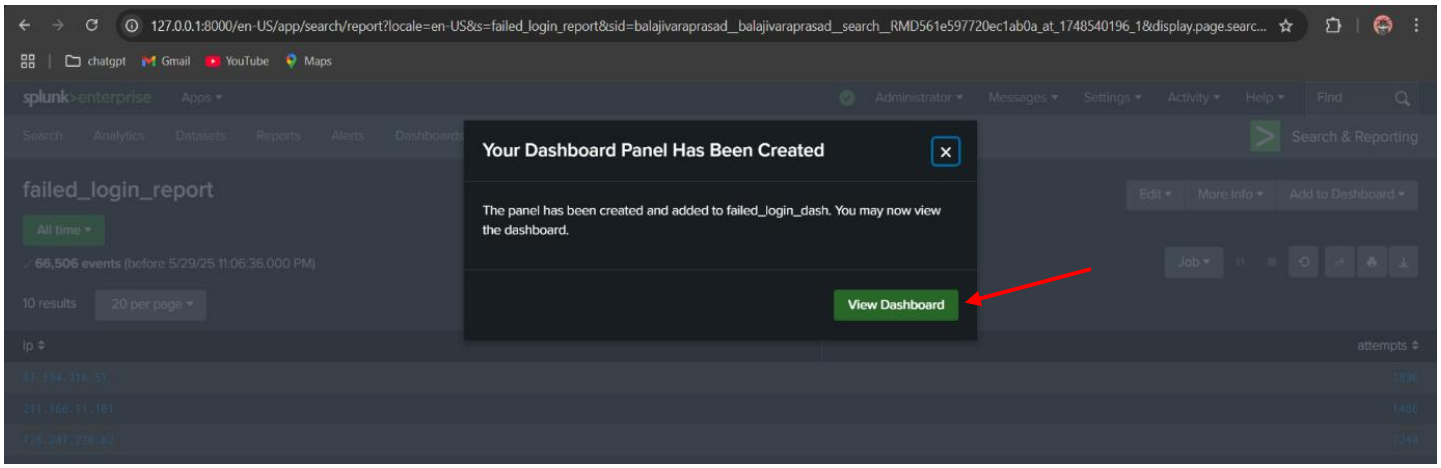
Step 40:

A pop-up window will appear displaying a list of existing dashboards. From this list, select the "Failed Login Dashboard" that we created earlier. This ensures the report is added to the correct dashboard for centralized monitoring.



Step 41:

After adding the report to the selected dashboard, a pop-up message will appear stating "Your dashboard panel has been created." This confirms that the report has been successfully added as a new panel in the dashboard layout.

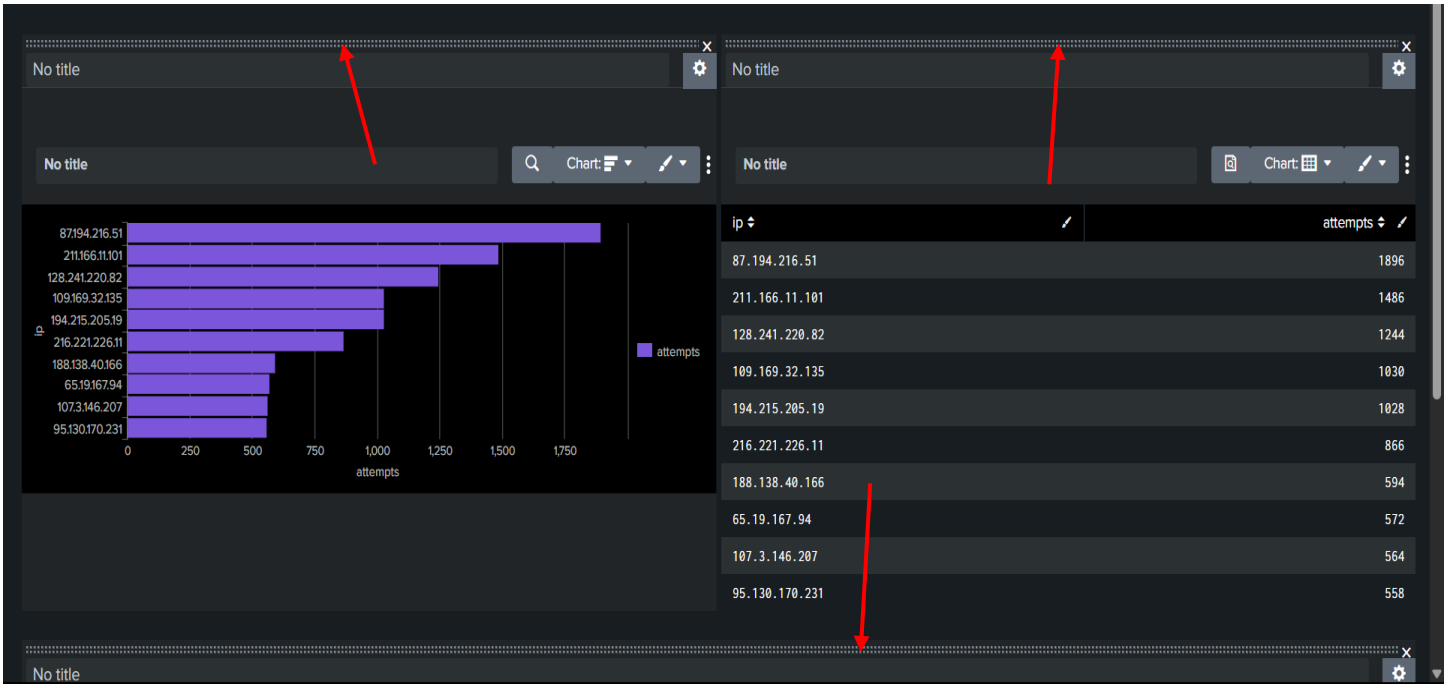


Step 42:

Now, open the dashboard to verify the contents. You should see all the previously added elements, including the two chart visualizations and the raw data panel imported from the "Failed Login" report. This combination provides both graphical and detailed data insights in a single view.

Step 43:

Although the data has been successfully imported and visualized, displaying large datasets and multiple charts stacked vertically can make analysis difficult. To improve readability and space utilization, click and drag the panels by placing your cursor on the dotted borders of each graph or table. Rearranging the panels according to your preference allows you to view more content efficiently within the dashboard space.(if the dotted lines are not visible, click on the edit button to replace the graphs and tables)

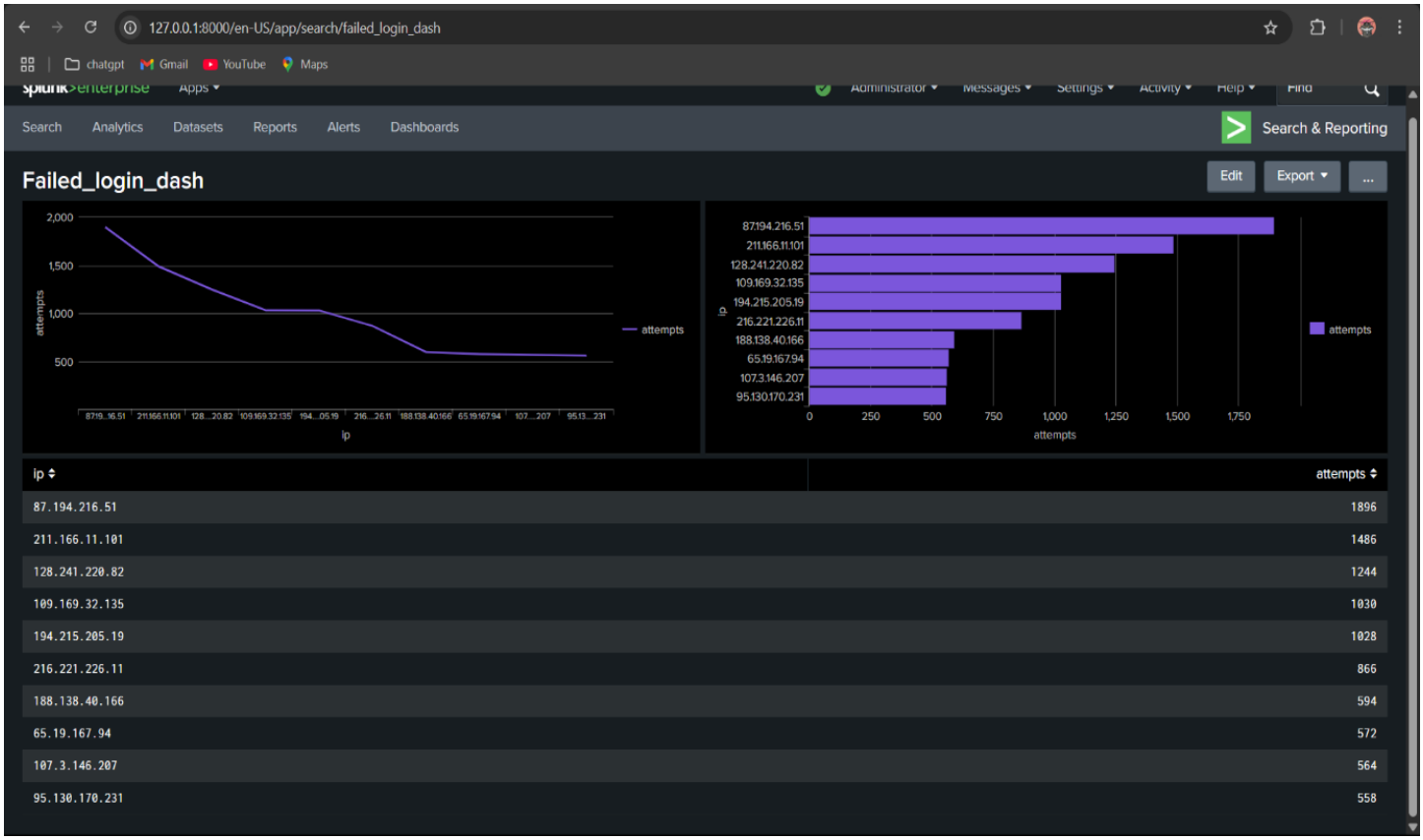


Step 44:

After rearranging the visual elements and raw data in the dashboard, we achieve a clear and well organized view of failed login attempts. As seen in the image, the dashboard includes:

- A line chart showing the trend of failed login attempts per IP address.
- A bar chart representing the same data for easy comparison of attempts.
- A raw data table which we imported from reports, listing IP addresses along with the number of failed login attempts.

This layout allows quick identification of suspicious IPs with high failure rates and provides both visual and detailed data for analysis. By optimizing the panel arrangement, we enhance readability and make efficient use of screen space, which is especially helpful when monitoring large datasets.



Summary:

In summary, Splunk reports (saved searches) and dashboards (panel layouts) work hand-in-hand to surface insights. We collect data into, build a saved search to count failed logins by IP, and then visualize the top results on a dashboard panel. Splunk's rich SPL syntax and visualization library allow us to craft precise queries (as shown above) and display them in charts or tables. With scheduling and role-based sharing, the solution can run continuously and deliver timely alerts or views to the right team members.

Conclusion:

This research comprehensively explored the practical applications of Splunk reports and dashboards, highlighting their pivotal role in transforming raw machine data into meaningful insights. Through hands on implementation using failed login attempt data, the project demonstrated how SPL queries can be used to extract critical security metrics, visualize trends, and present data in a structured, user friendly format. The use of various visualizations, such as line and bar charts, combined with raw data panels within a single dashboard, showcased how Splunk can support real time monitoring and forensic analysis in security-focused environments.

Furthermore, the study emphasized the importance of customization, access control, and scheduling in the creation of reports and dashboards. By integrating saved searches, visual representations, and permission based sharing, Splunk ensures that valuable information reaches the right stakeholders efficiently. This research not only strengthens the understanding of Splunk's core functionalities but also reinforces its value as a vital tool in modern security operations and data analysis workflows.

References:

https://www.scribd.com/document/782318508/001-Now-You-Know-Splunk-FreeCourseWeb-com#:~:text=A%20report%20is%20a%20saved,search

https://docs.splunk.com/Documentation/Splunk/9.4.2/SearchTutorial/Aboutdashboards#:~:text=Dashboards%20are%20views%20that%20are,are%20usually%20connected%20to%20reports

https://www.splunk.com/en_us/blog/tips-and-tricks/dashboard-design-visualization-choices-and-configurations-part-1.html#:~:text=Visualization%20Types

https://vyshak-hari.medium.com/splunk-dashboards-and-reports-by-tryhackme-41f1ba6ed859#:~:text=Reports%20can%20also%20help%20reduce,they%20will%20accomplish%20two%20tasks

https://docs.splunk.com/Documentation/Splunk/9.4.2/Report/Createandeditreports#:~:text=1,9%2C%20or

https://kinneygroup.com/blog/splunk-reports-and-dashboards-for-beginners/#:~:text=A%20dashboard%20is%20a%20collection,report%20visualization%20to%20a%20dashboard

https://docs.splunk.com/Documentation/Splunk/9.4.2/Report/Createandeditreports#:~:text=,95

https://docs.splunk.com/Documentation/Splunk/9.4.2/SearchTutorial/Aboutdashboards#:~:text=Change%20dashboard%20permissions

https://docs.splunk.com/Documentation/Splunk/9.4.2/Security/AuditSplunkactivity#:~:text=The%20Splunk%20platform%20stores%20audit,SPLUNK_HOME%2Fvar%2Flog%2Fsplunk%2Faudit.log

https://docs.splunk.com/Documentation/Splunk/9.4.2/Report/Createandeditreports#:~:text=reports%2C%20%20in%20this%20manual,in%20the%20Dashboard%20Studio%20manual

THANK YOU