

# **COMPREHENSIVE DEMONSTRATION: SPLUNK SECURITY INCIDENT AND EVENT MANAGEMENT TOOL (SIEM)**

**By Snehal Borhade**

# INDEX

1) Abstract	....1
2) Purpose	....1
3) Approach	....2
4) Procedure	....2
A) SIEM Overview	
B) Splunk overview	
C) Input data	
D) Search	
E) Event	
F) Report	
G) Dashboard	
H) Lookups	
I) Alerts	
J) Indexes	
K) Log collection	
5) Conclusion	....24

# COMPREHENSIVE DEMONSTRATION: SPLUNK SECURITY INCIDENT AND EVENT MANAGEMENT TOOL (SIEM)

---

## Abstract

This project, titled "A Comprehensive Demonstration of Splunk SIEM," provides an in-depth exploration of Splunk's Security Information and Event Management (SIEM) capabilities. Splunk is a powerful platform for searching, monitoring, and analyzing machine-generated data via a web-style interface. Our demonstration focuses on key functionalities that are essential for effective security management, including events, dashboards, lookups, reports, and alerts. We begin by showcasing how Splunk processes and indexes large volumes of data, transforming raw data into meaningful events. This foundational step enables the extraction of actionable insights from diverse data sources. We then delve into the creation and customization of dashboards, illustrating how Splunk's intuitive interface allows for real-time visualization of critical metrics and trends. Through this comprehensive demonstration, we aim to illustrate the robust features of Splunk SIEM and its application in real-world scenarios. This project serves as a valuable resource for security professionals seeking to leverage Splunk for enhanced visibility and control over their IT environments.

## Purpose

The purpose of the project titled "A Comprehensive Demonstration of Splunk SIEM" is to provide a detailed and practical understanding of Splunk's Security Information and Event Management (SIEM) capabilities. This project helps to understand and explore various aspects of Splunk. This project is a basic overview of how logs are monitored, analyzed and visualized in the cyber-security industry. To demonstrate practical applications of Splunk in a real-world security environment. By showcasing how Splunk can be used to visualize data, enrich event information, and generate actionable insights, the project aims to provide a hands-on learning experience.

## Approach

The approach for the project titled "A Comprehensive Demonstration of Splunk SIEM" involves a systematic and structured methodology to explore and demonstrate the various functionalities of Splunk. Setting up data inputs, explore basic and advanced search commands to filter and extract relevant information from the events, Set up real-time dashboards to monitor critical events and system performance indicators, Demonstrate how to use lookups in searches to enhance the value and meaning of the data.

## Procedure

### Brief overview :

#### **SIEM**

SIEM stands for Security Incident and Event Management. SIEM (Security Information and Event Management) tools are essential for collecting and managing security-relevant data, which is crucial during investigations.

These tools enhance network visibility by providing comprehensive awareness of activities occurring between devices on a network. The insights derived from SIEM tools enable security teams to swiftly investigate and respond to security incidents. With numerous advantages, SIEM tools significantly improve the efficiency and effectiveness of security teams in incident response and management. SIEM (Security Information and Event Management) tools provide comprehensive access to event and activity data across a network, including real-time monitoring. Given that networks can connect to hundreds of different systems and devices, SIEM tools are designed to ingest and centralize this vast amount of data for easy access and analysis. These tools continuously monitor systems and networks in real-time, applying detection rules to identify potential malicious activity.

When an activity matches a rule, an alert is generated and sent to security teams for evaluation. Additionally, SIEM tools serve as data retention systems, offering access to historical data which can be retained or deleted based on the organization's requirements. SIEM tools are primarily used by Security analyst and SOC analyst for monitoring data and access logs.

Security analyst continuously monitor the network for suspicious activity and anomalies. Respond to alerts generated by SIEM tools based on predefined detection rules, to correlate events from various sources to understand the full context of a security incident. SIEM is also used to investigate the root cause of security incidents by analyzing the logs and data collected by the SIEM tool. Maintain audit trails for all activities and access logs to support compliance audits.

SOC analyst is Security Operation Centre analyst who is responsible for monitoring every factor related to security i.e incoming and outgoing data, access to that data, log entries etc. Act as the first responders to security incidents, leveraging SIEM alerts to quickly assess and prioritize threats.

They utilize advanced analytics and threat intelligence integrated into the SIEM to detect sophisticated threats and use insights gained from SIEM data to train and develop the skills of team members, enhancing overall SOC capabilities.

There are many siem tools available such as QRadar, Splunk , Arcsight etc. The one demonstrated in this project is splunk.

## Splunk

Splunk is a leading platform for operational intelligence, providing powerful tools for searching, monitoring, and analyzing machine-generated data from a variety of sources. Designed to handle large volumes of data in real-time, Splunk transforms raw data into valuable insights, enabling organizations to make informed decisions and respond swiftly to security threats and operational issues. Splunk's robust features include data ingestion, indexing, and real-time search capabilities. It supports the creation of detailed dashboards, reports, and alerts, which facilitate proactive monitoring and analysis. With its ability to handle diverse data sources and formats, Splunk is widely used for security information and event management (SIEM), IT operations, business analytics, and more. By leveraging Splunk, organizations can gain comprehensive visibility into their IT infrastructure, enhance security posture, and drive operational efficiency, making it an essential tool for modern enterprises.

There are various features used in Splunk which helps use to categorize,monitor and visualiza data. It provides comprehensive view of the functions going on within the company.Some Features within splunk are events, lookups,dashboard,reports,alerts,logs ,indexes,forward cluster.

## Splunk interface:

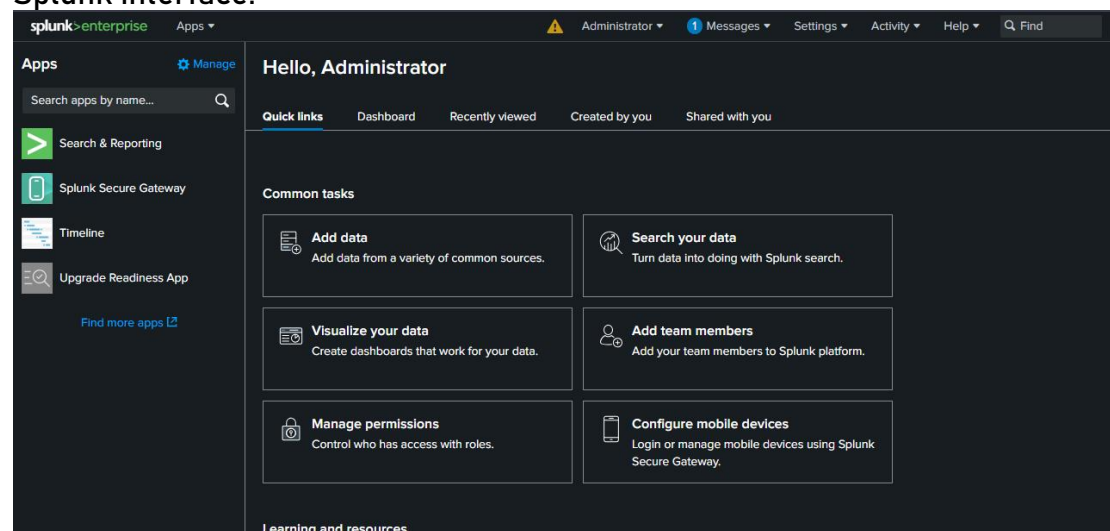


Fig.1 interface

To input data:

We can input data in various way by uploading a file or using by making indexes. If we upload a data file it can be selected by source.

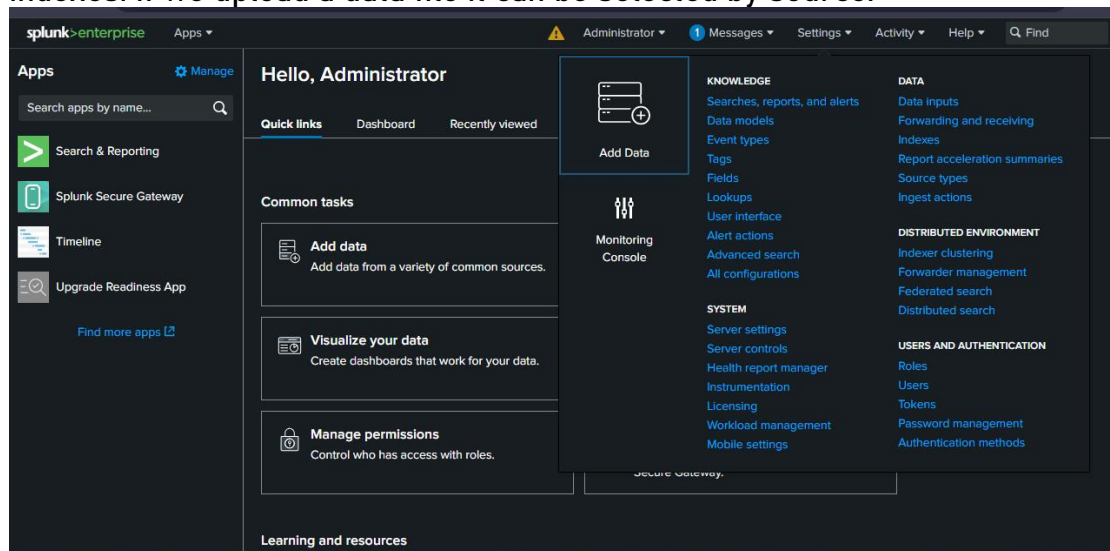


Fig.2 input data 1

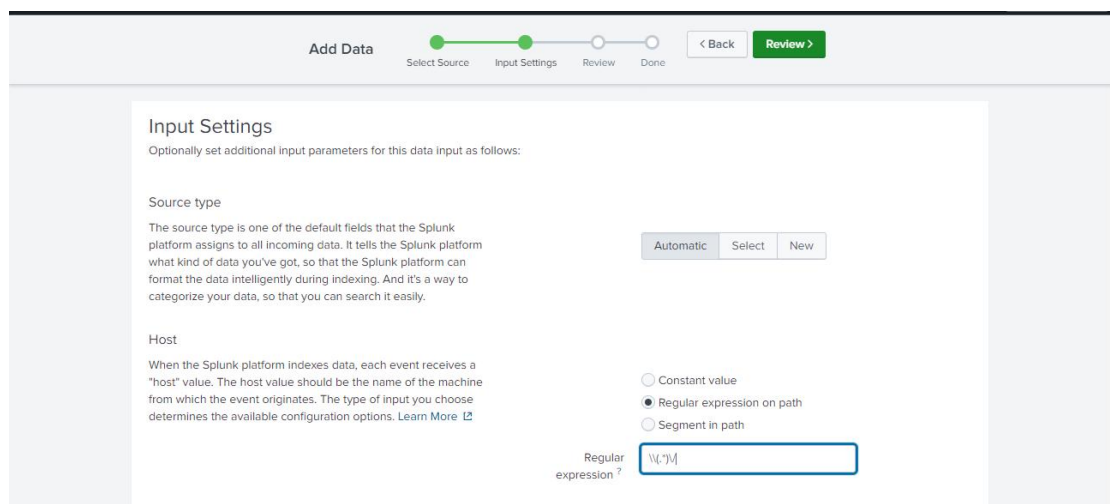


Fig.3 input data 2

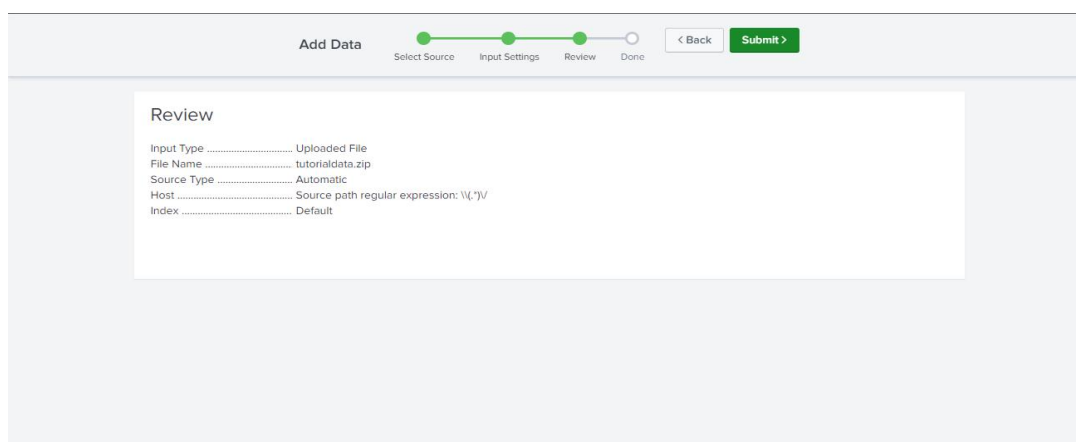


Fig.4 input data 3

Once the data is uploaded it can be searched by its source:

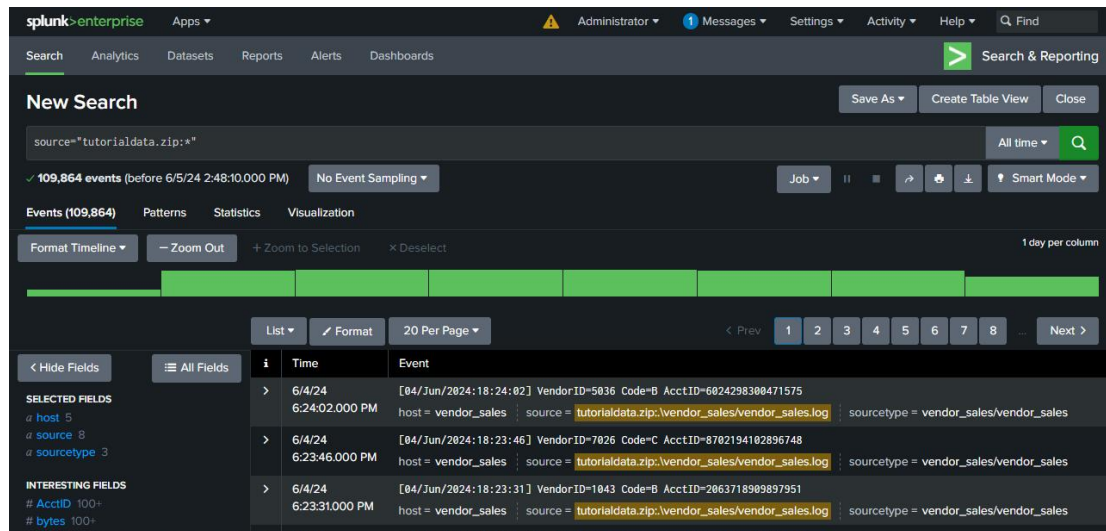


Fig5.Search

Search feature is used to search through the data and get results for our specific keyword. In Splunk, the search feature is the core functionality that allows users to query and analyze large volumes of machine-generated data. It enables users to search for specific events, patterns, or trends within their data sets. The search feature supports a powerful query language that enables complex searches and filtering based on various criteria such as time, source, and event type. Users can utilize search commands to manipulate and analyze their data, performing functions like aggregation, filtering, and visualization. Splunk's search feature also supports real-time searching, allowing users to monitor data as it streams in, and historical searching, enabling analysis of past events. Overall, the search feature in Splunk provides users with the ability to extract valuable insights from their data, facilitating proactive monitoring, troubleshooting, and decision-making.

## To create event:

In Splunk, events represent individual occurrences or entries in the data being analyzed. Each event typically contains timestamped information about a specific action, event, or log entry. Splunk's event feature organizes and indexes these events, making them searchable and analyzable. When we create an event we highlight the fields we want to be noticing more. For eg. We can create an event or highlight the areas which has failed password entry. We further can also make another event that will show failed entry or login for valid user and invalid user.

The screenshot shows the Splunk Enterprise interface with a search for "password fail\* for invalid user". The search results show 24,011 events. The results table lists several failed password attempts for various users, including 'appserver', 'testuser', 'mongodb', 'desktop', 'cyrus', 'guest', 'itnadmin', and 'root'.

Time	Event
6/4/24 4:13:04.000 AM	Thu Jun 04 2024 04:13:04 mailsvl ssh[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2
6/4/24 4:13:04.000 AM	Thu Jun 04 2024 04:13:04 mailsvl ssh[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2
6/4/24 4:13:04.000 AM	Thu Jun 04 2024 04:13:04 mailsvl ssh[3760]: Failed password for invalid user mongodb from 194.8.74.23 port 2472 ssh2
6/4/24 4:13:04.000 AM	Thu Jun 04 2024 04:13:04 mailsvl ssh[5801]: Failed password for invalid user desktop from 194.8.74.23 port 2285 ssh2
6/4/24 4:13:04.000 AM	Thu Jun 04 2024 04:13:04 mailsvl ssh[5979]: Failed password for invalid user cyrus from 194.8.74.23 port 3417 ssh2
6/4/24 4:13:04.000 AM	Thu Jun 04 2024 04:13:04 mailsvl ssh[4984]: Failed password for invalid user guest from 194.8.74.23 port 2294 ssh2
6/4/24 4:13:04.000 AM	Thu Jun 04 2024 04:13:04 mailsvl ssh[2605]: Failed password for invalid user itnadmin from 194.8.74.23 port 4692 ssh2
6/4/24 4:13:04.000 AM	Thu Jun 04 2024 04:13:04 mailsvl ssh[53331]: Failed password for invalid user root from 194.8.74.23 port 6564 ssh2

Fig6 event 1

The screenshot shows the Splunk Enterprise interface with a search for "password fail\* NOT invalid". The search results show 9,242 events. A modal dialog titled "Your Event Type Has Been Created" is displayed over the search results, indicating that a new event type has been created. The dialog also includes a "Done" button and a message: "You can edit this event type via Event Types in the Settings menu."

Time	Event
6/4/24 4:13:04.000 AM	Thu Jun 04 2024 04:13:04 mailsvl ssh[1839]: Failed password for root from 194.8.74.23 port 3768 ssh2
6/4/24 4:13:04.000 AM	Thu Jun 04 2024 04:13:04 mailsvl ssh[1165]: Failed password for apache from 194.8.74.23 port 4894 ssh2
6/4/24 4:13:04.000 AM	Thu Jun 04 2024 04:13:04 mailsvl ssh[4988]: Failed password for mail from 194.8.74.23 port 1552 ssh2
6/4/24 4:13:04.000 AM	Thu Jun 04 2024 04:13:04 mailsvl ssh[1530]: Failed password for games from 194.8.74.23 port 3867 ssh2
6/4/24 4:13:04.000 AM	Thu Jun 04 2024 04:13:04 mailsvl ssh[3750]: Failed password for nagios from 194.8.74.23 port 3703 ssh2
6/4/24 4:13:04.000 AM	Thu Jun 04 2024 04:13:04 mailsvl ssh[4583]: Failed password for ftp from 283.45.206.135 port 3866 ssh2
6/4/24 4:13:04.000 AM	Thu Jun 04 2024 04:13:04 mailsvl ssh[4782]: Failed password for nagios from 283.45.206.135 port 1851 ssh2

Fig7 event 2



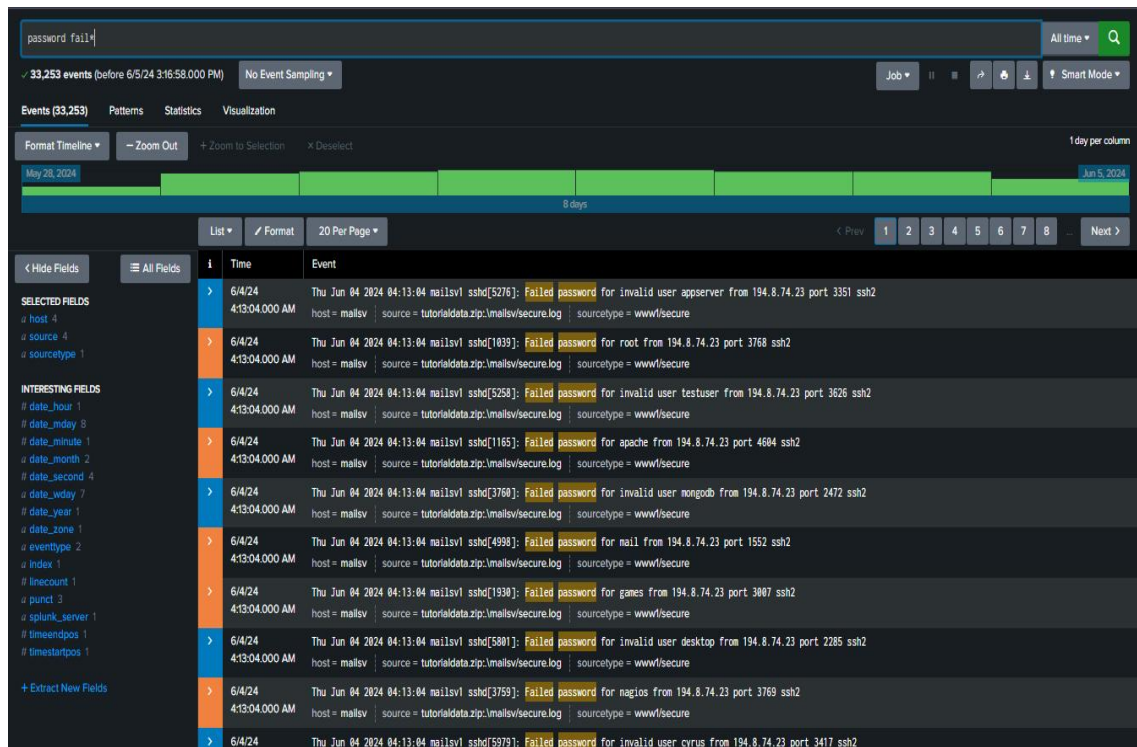


Fig8. event 3

Here password fail by invalid user is shown by orange and by valid user in blue. We can set color, name, description and value for how critical it is. We can also set permissions for event type. Permission is giving rights to other users or apps to write or read our event.

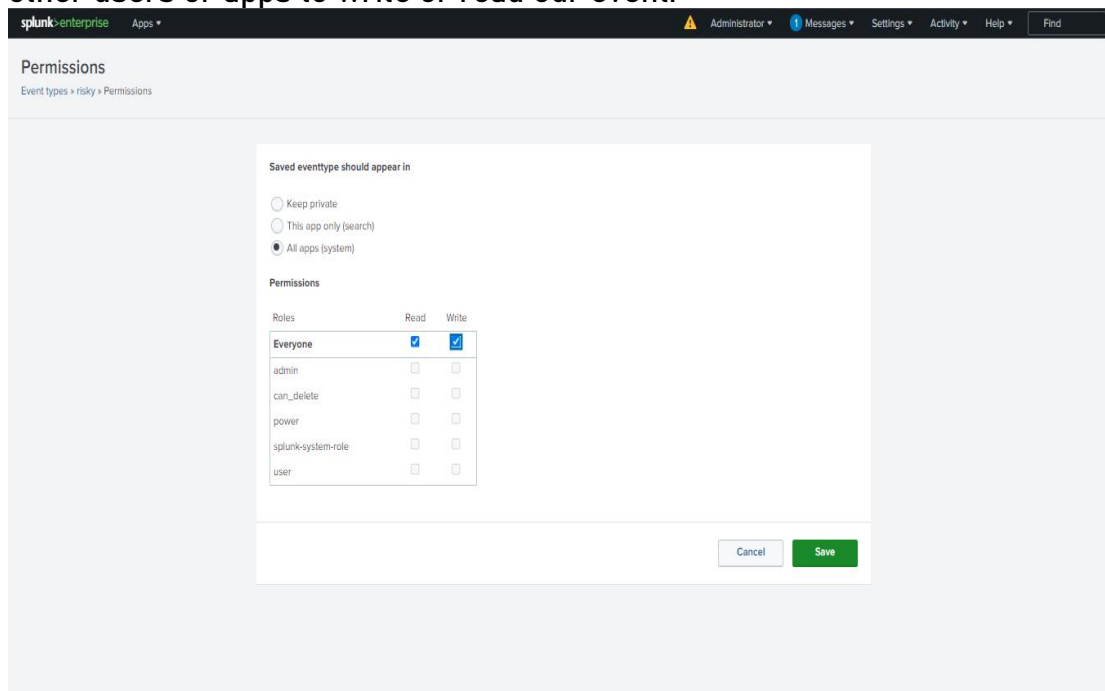


Fig9. event permissions

## Count by event type :

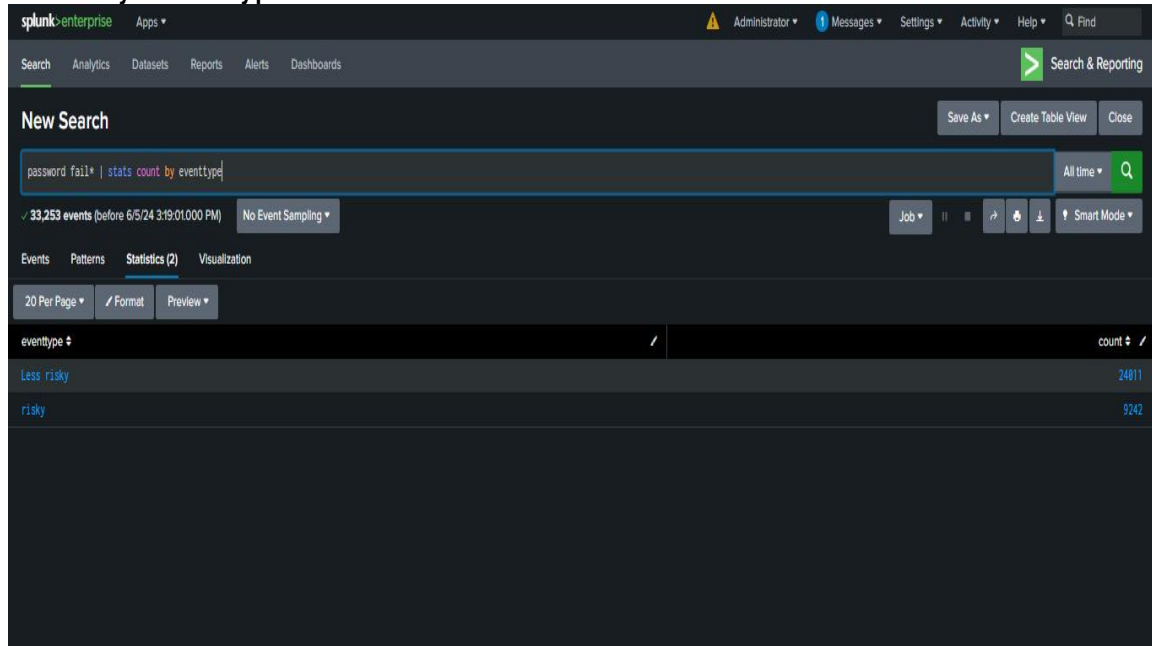


Fig10. event count

We can also create tables and visualisation using command table and then specifying columns we want. :

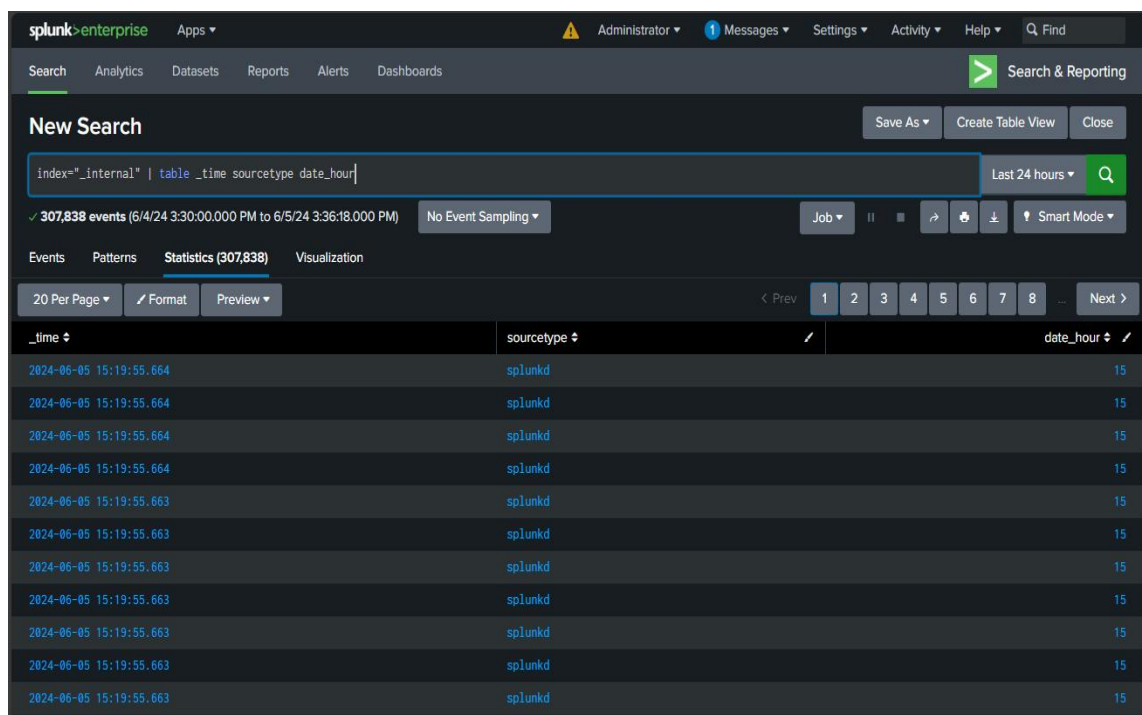


Fig11. table

Here we have used table command to get table of time,source-type and date.

To visualize this data we can simply choose visualize:

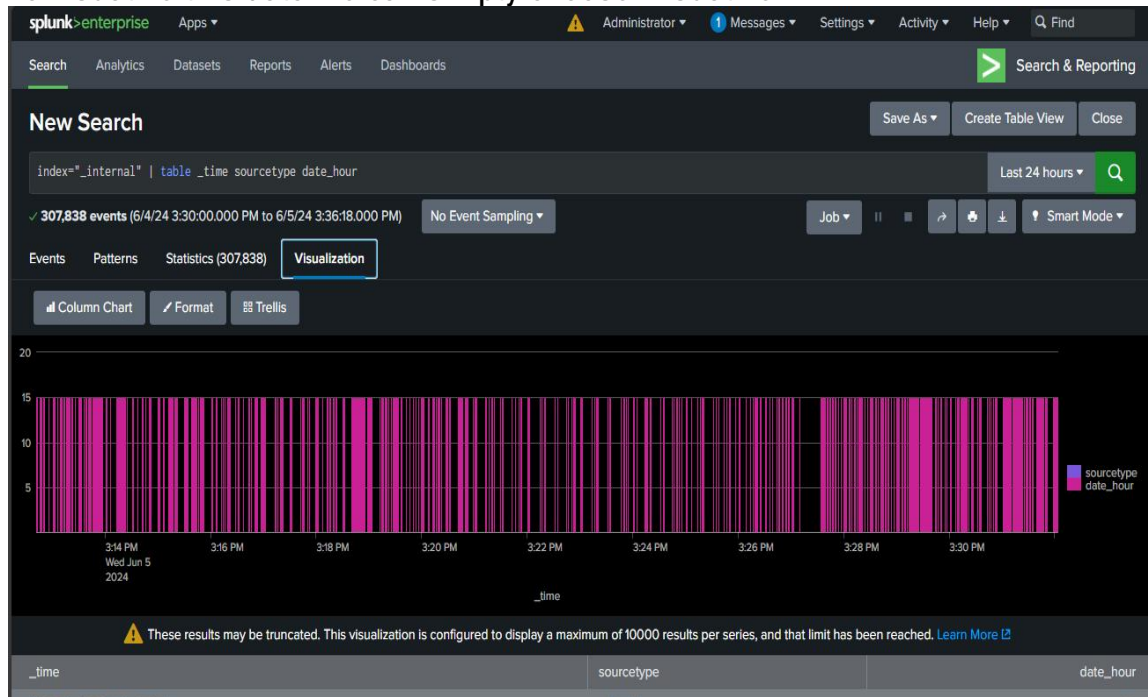


Fig12. table\_visualize

Visualization provide various pattern options such as bar chart , line chart , pie chart , bubble , geographical etc.

## Jobs:

It keeps record of all the searches we have done. The search can be deleted,stored, scheduled, paused and restart from here. This option can be found in activity section.

The screenshot shows the Splunk Enterprise Jobs page. It displays a list of search jobs with columns for Owner, Application, Events, Size, Created at, Expires, Runtime, Status, and Actions. The jobs are listed in a table with pagination controls. The first job is owned by 'snehal\_splunk24' and has 307,838 events. The second job has 307,775 events. The third job has 12,992 events. The fourth job has 12,992 events. The fifth job has 0 events. The sixth job has 0 events. The seventh job has 0 events. The eighth job has 0 events. The ninth job has 0 events. The tenth job has 0 events. The jobs are listed in a table with pagination controls. The first job is owned by 'snehal\_splunk24' and has 307,838 events. The second job has 307,775 events. The third job has 12,992 events. The fourth job has 12,992 events. The fifth job has 0 events. The sixth job has 0 events. The seventh job has 0 events. The eighth job has 0 events. The ninth job has 0 events. The tenth job has 0 events.

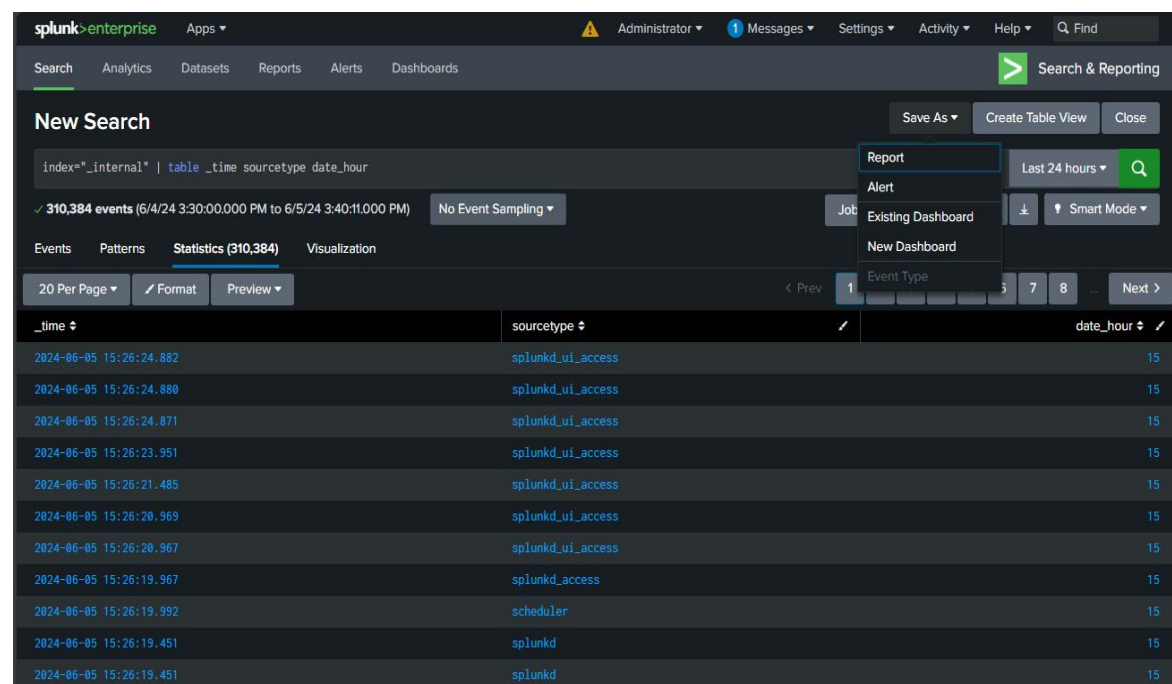
i	Owner	Application	Events	Size	Created at	Expires	Runtime	Status	Actions
>	snehal_splunk24	search	307,838	980 KB	Jun 5, 2024 3:36:18 PM	Jun 5, 2024 3:46:52 PM	00:00:03	Done	Job ▾    ■ ↗ ⬇
index="_internal"   table _time sourcetype date_hour [6/4/24 3:30:00.000 PM to 6/5/24 3:36:18.000 PM]									
>	snehal_splunk24	search	307,775	2.96 MB	Jun 5, 2024 3:36:03 PM	Jun 5, 2024 3:46:08 PM	00:00:05	Done	Job ▾    ■ ↗ ⬇
index="_internal" [6/4/24 3:30:00.000 PM to 6/5/24 3:36:03.000 PM]									
>	snehal_splunk24	search	12,992	128 KB	Jun 5, 2024 3:33:01 PM	Jun 5, 2024 3:44:04 PM	00:00:01	Done	Job ▾    ■ ↗ ⬇
source="tutorialdata.zip:\\www3\\access.log"   table _time sourcetype source [before 6/5/24 3:33:01.000 PM]									
>	snehal_splunk24	search	12,992	7.47 MB	Jun 5, 2024 3:32:22 PM	Jun 5, 2024 3:42:55 PM	00:00:03	Done	Job ▾    ■ ↗ ⬇
source="tutorialdata.zip:\\www3\\access.log" [before 6/5/24 3:32:22.000 PM]									
>	snehal_splunk24	search	0	92 KB	Jun 5, 2024 3:32:03 PM	Jun 5, 2024 3:42:18 PM	00:00:01	Done	Job ▾    ■ ↗ ⬇
mstats _metrics [before 6/5/24 3:32:03.000 PM]									
>	snehal_splunk24	search	0	92 KB	Jun 5, 2024 3:31:43 PM	Jun 5, 2024 3:41:58 PM	00:00:01	Done	Job ▾    ■ ↗ ⬇

Fig13. Jobs

## Report :

In Splunk, the report feature allows users to create structured summaries of data analysis and insights for further review or distribution. Reports in Splunk are customizable and can be tailored to specific needs and requirements. Reports in Splunk enable users to summarize data findings from searches, dashboards, or saved events. Users can aggregate data using various statistical functions, such as count, sum, average, and more. Reports can include visualizations such as charts, graphs, and tables to present data in a clear and understandable format. Users can customize the appearance and layout of visualizations to suit their preferences. Splunk allows users to schedule the generation and distribution of reports at predefined intervals. Users can schedule reports to be sent via email or saved to a shared location, ensuring stakeholders receive timely updates and insights. Splunk reports offer flexibility in terms of customization. Users can customize report parameters, data filters, and time ranges to focus on specific aspects of the data. Additionally, users can add annotations, comments, and descriptions to provide context and insights into the data presented in the report.

We can save our search as report to create a report.



The screenshot displays the Splunk Enterprise web interface. At the top, there's a navigation bar with 'splunk>enterprise' and various user options. Below this, a 'Search & Reporting' section is visible. The main area shows a 'New Search' header with a search bar containing the query 'index="\_internal" | table \_time sourcetype date\_hour'. Below the search bar, it indicates '310,384 events' and provides a time range filter. A dropdown menu is open, showing options: 'Report', 'Alert', 'Job', 'Existing Dashboard', and 'New Dashboard'. The 'Report' option is highlighted. Below the menu, there's a table with columns '\_time', 'sourcetype', and 'date\_hour'. The table contains several rows of data, including timestamps and sourcetypes like 'splunkd\_ui\_access' and 'scheduler'.

_time	sourcetype	date_hour
2024-06-05 15:26:24.882	splunkd_ui_access	15
2024-06-05 15:26:24.880	splunkd_ui_access	15
2024-06-05 15:26:24.871	splunkd_ui_access	15
2024-06-05 15:26:23.951	splunkd_ui_access	15
2024-06-05 15:26:21.485	splunkd_ui_access	15
2024-06-05 15:26:20.969	splunkd_ui_access	15
2024-06-05 15:26:20.967	splunkd_ui_access	15
2024-06-05 15:26:19.967	splunkd_access	15
2024-06-05 15:26:19.992	scheduler	15
2024-06-05 15:26:19.451	splunkd	15
2024-06-05 15:26:19.451	splunkd	15

Fig14. Reports

**internal\_report\_1**  
Last 24 hours  
✓ 310,384 events (6/4/24 3:30:00.000 PM to 6/5/24 3:40:11.000 PM)

310,384 results 20 per page

_time	sourcetype	date_hour
2024-06-05 15:26:24.882	splunkd_ui_access	15
2024-06-05 15:26:24.880	splunkd_ui_access	15
2024-06-05 15:26:24.871	splunkd_ui_access	15
2024-06-05 15:26:23.951	splunkd_ui_access	15
2024-06-05 15:26:21.485	splunkd_ui_access	15
2024-06-05 15:26:20.969	splunkd_ui_access	15
2024-06-05 15:26:20.967	splunkd_ui_access	15
2024-06-05 15:26:19.967	splunkd_access	15
2024-06-05 15:26:19.992	scheduler	15
2024-06-05 15:26:19.451	splunkd	15
2024-06-05 15:26:19.451	splunkd	15
2024-06-05 15:26:19.451	splunkd	15

Fig15. Reports

**Reports**  
Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

11 Reports

i	Title ^	Actions	Next Scheduled Time	Owner	App	Sharing
>	Bucket Merge Retrieve Conf Settings	Open in Search Edit	None	nobody	search	App
>	Errors in the last 24 hours	Open in Search Edit	None	nobody	search	App
>	Errors in the last hour	Open in Search Edit	None	nobody	search	App
>	License Usage Data Cube	Open in Search Edit	None	nobody	search	App
>	Messages by minute last 3 hours	Open in Search Edit	None	nobody	search	App
>	Orphaned scheduled searches	Open in Search Edit	None	nobody	search	App
>	Splunk errors last 24 hours	Open in Search Edit	None	nobody	search	App
>	dash_demo	Open in Search Edit	None	snehal_splunk24	search	Private
>	intenal_scheduled_report	Open in Search Edit	None	snehal_splunk24	search	Private
>	Internal_report_1	Open in Search Edit	None	snehal_splunk24	search	Private
>	Internal_trial	Open in Search Edit	None	snehal_splunk24	search	Global

Fig16. Reports

All reports can be seen in the reports section. We can edit , give permissions and delete our report from here. We can schedule report so as to obtain it weekly ,daily monthly as so on.

**Edit Schedule**

⚠ Scheduling this report results in removal of the time picker from the report display.

Report: access\_log

Schedule Report ☒ [Learn More](#)

Schedule: Run every week

On: Monday at 6:00

Time Range: Last 24 hours

Schedule Priority: Higher

Schedule Window: 8 hours

Trigger Actions

+ Add Actions

When triggered: Send email

Cancel Save

Fig. Reports schedule



## Dashboard :

The dashboard feature in Splunk offers users a comprehensive and interactive platform to visualize and monitor key metrics and trends within their data. Users can create customized dashboards with various visualizations such as charts, graphs, maps, and tables to present data in a visually appealing and intuitive format. Dashboards can be tailored to specific use cases, allowing users to focus on relevant information and insights. With real-time data updates and the ability to drill down into specific details, Splunk dashboards empower users to quickly identify patterns, anomalies, and opportunities for optimization. Whether used for operational monitoring, security analysis, or business intelligence, Splunk dashboards provide a centralized hub for data-driven decision-making and actionable insights.

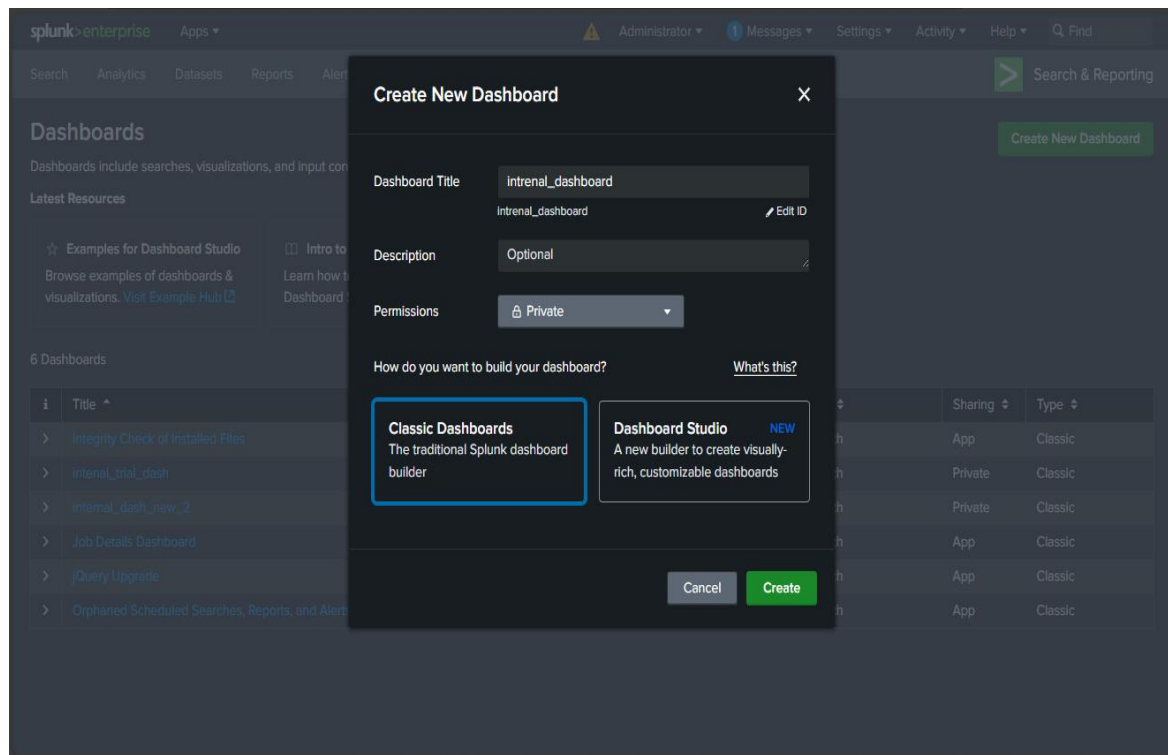


Fig17. Dashboards

We can set title , description , permissions and choose how we want to build your dashboard

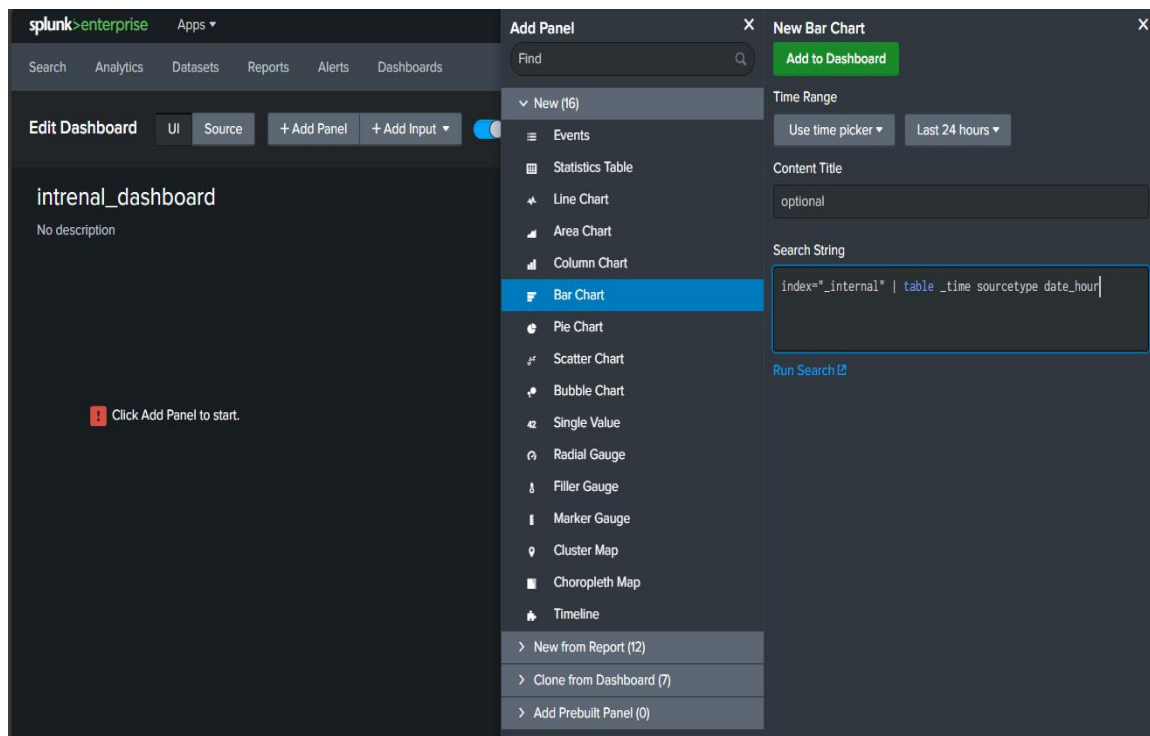


Fig18. Dashboards\_panels

We need to add panel in dashboard once it is created. The panels ia panel is a visual component or element within a dashboard that displays specific data or information. Panels are used to present data in a visual format, such as charts, graphs, tables, maps, or single value visualizations, allowing users to quickly interpret and analyze the data.

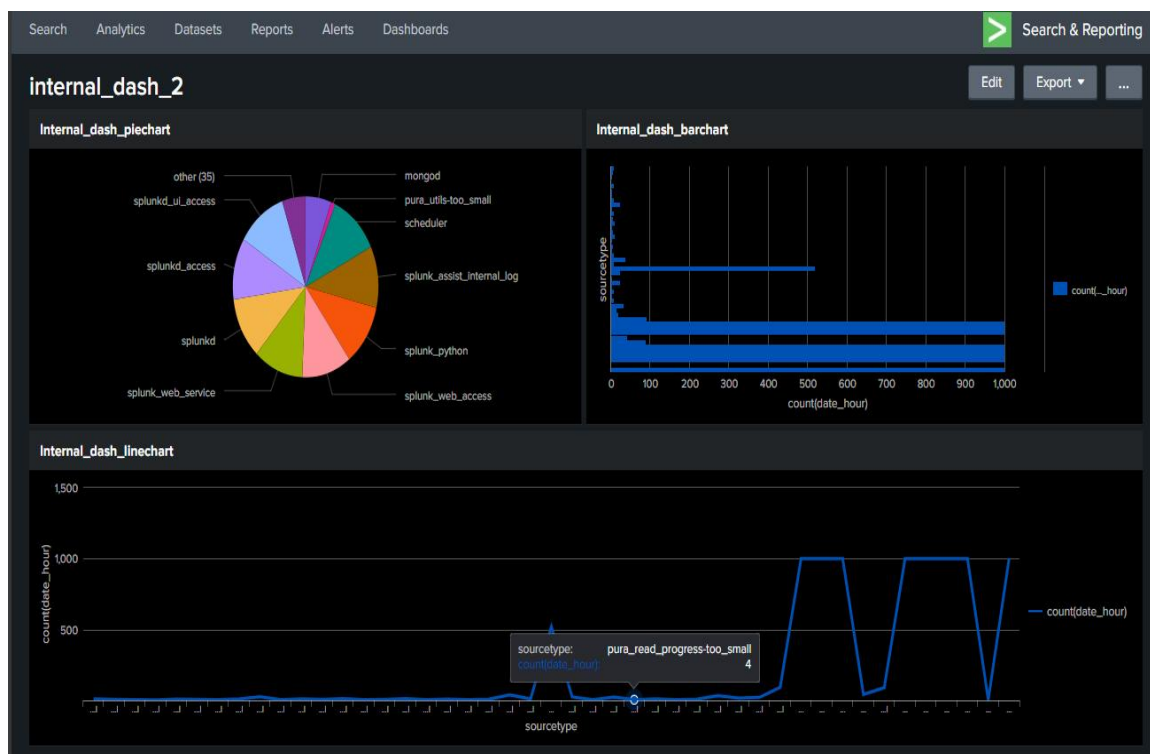


Fig19. Dashboards\_visualisation

Here we have added 3 panels and visualized them.

## Lookup

A lookup is a feature in which we take data from 2 different datasets to represent desired data output. The lookup feature in Splunk allows users to enrich and augment their data by integrating external reference datasets into their analysis. With lookups, users can enhance the context and relevance of their data by cross-referencing it with supplementary information from external sources such as CSV files, databases, or custom tables. This capability enables users to correlate and analyze data more comprehensively, leading to deeper insights and more informed decision-making. Lookups in Splunk can be used for various purposes, including adding geographical information to IP addresses, enriching user activity logs with additional attributes, or performing entity resolution across different data sets. By leveraging the lookup feature, users can unlock the full potential of their data and gain valuable insights that would otherwise be inaccessible.

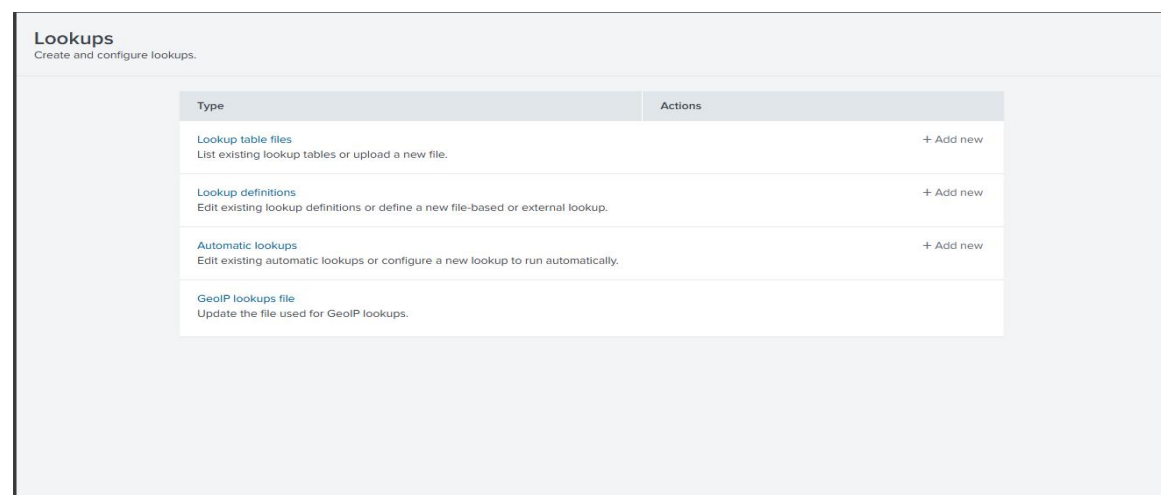


Fig20. Lookups

To create a lookup first we will select lookup table files and then create a lookup by adding external csv data file.

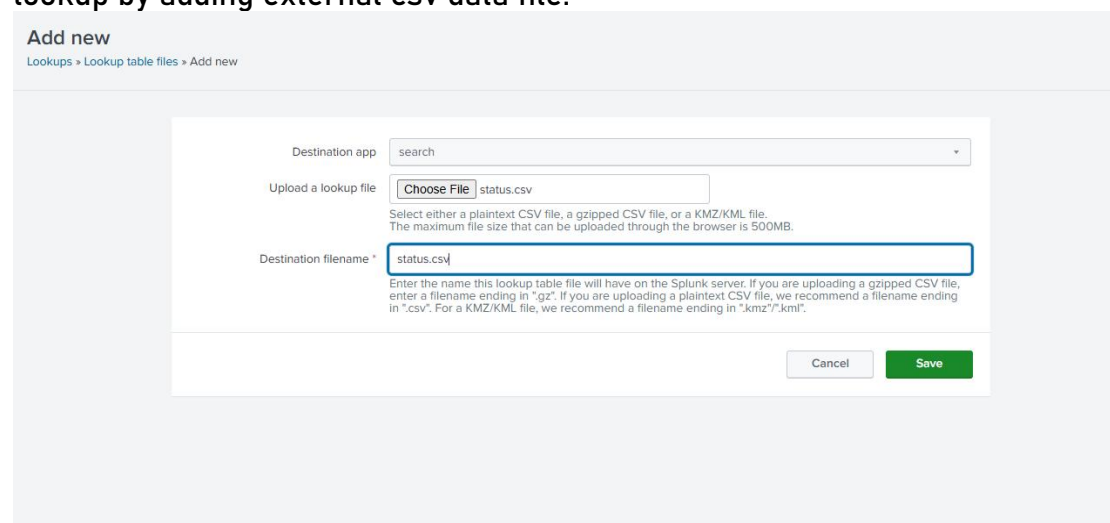
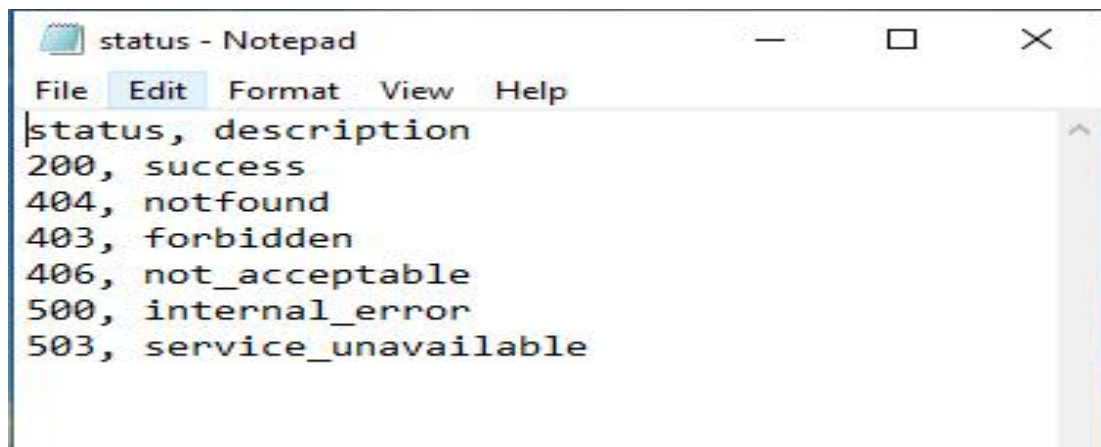


Fig21. new Lookups



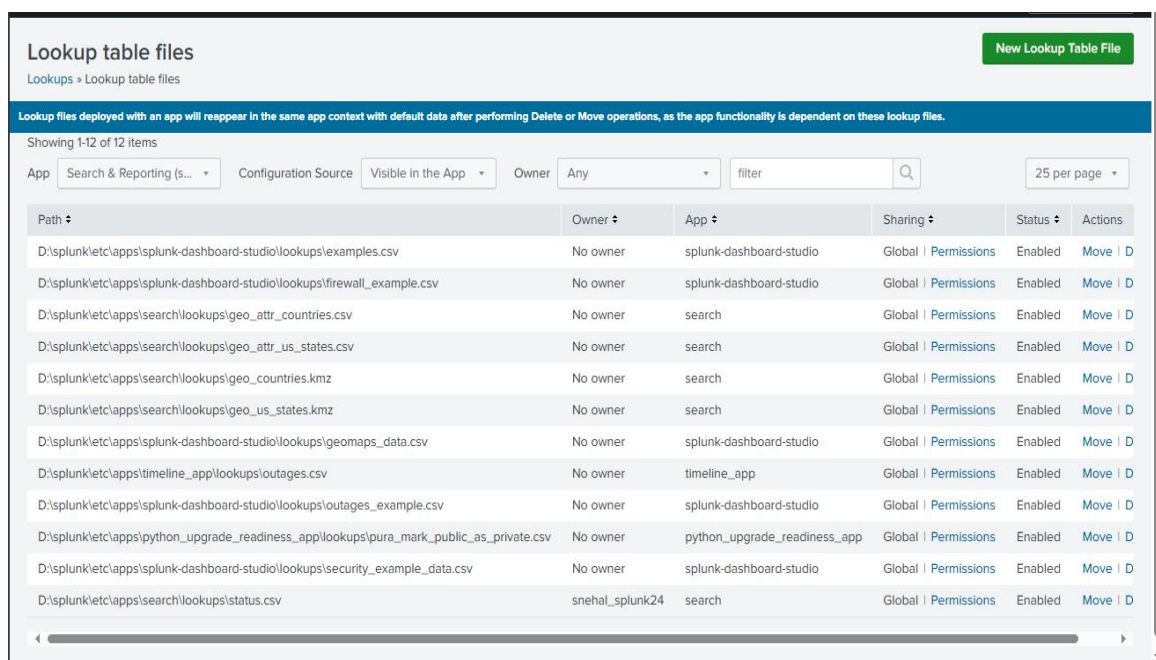
Added csv file has few status codes and description separated by comma.



```
status, description
200, success
404, notfound
403, forbidden
406, not_acceptable
500, internal_error
503, service_unavailable
```

Fig22. csv file

Created lookups can be seen in the lookup table files.



Lookup table files

Lookups > Lookup table files

Lookup files deployed with an app will reappear in the same app context with default data after performing Delete or Move operations, as the app functionality is dependent on these lookup files.

Showing 1-12 of 12 items

App: Search & Reporting (s...) Configuration Source: Visible in the App Owner: Any filter 25 per page

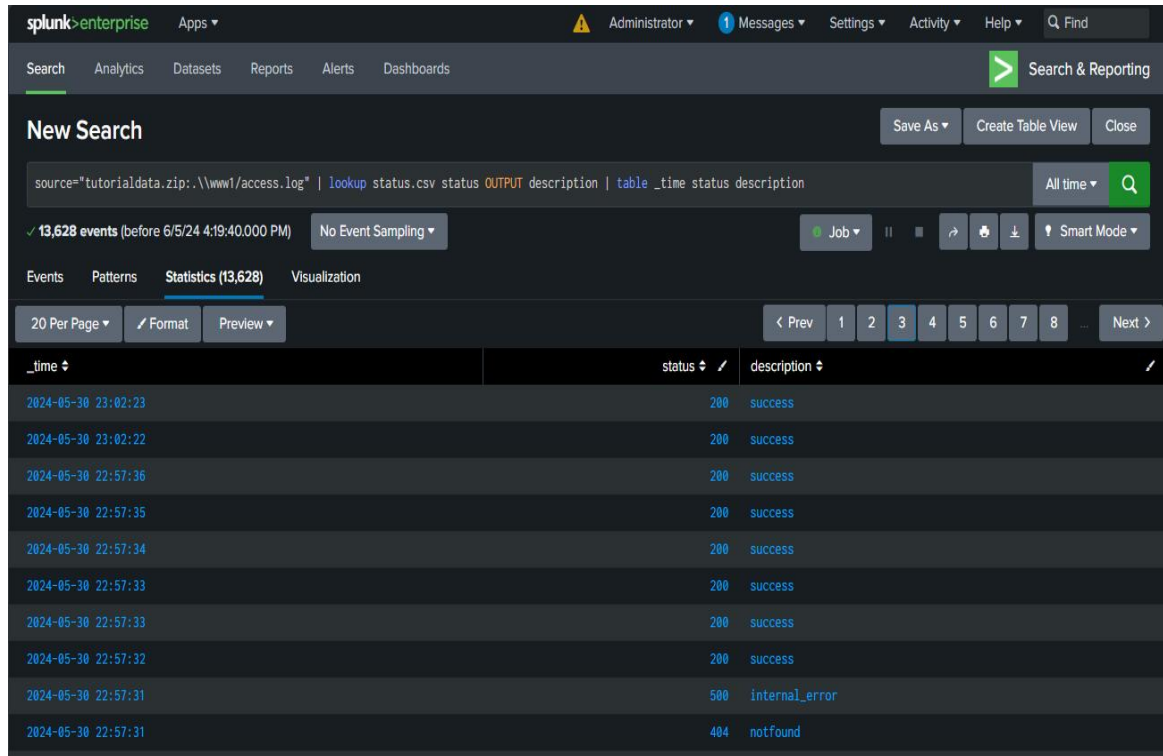
Path	Owner	App	Sharing	Status	Actions
D:\splunk\etc\apps\splunk-dashboard-studio\lookups\examples.csv	No owner	splunk-dashboard-studio	Global   Permissions	Enabled	Move   D
D:\splunk\etc\apps\splunk-dashboard-studio\lookups\firewall_example.csv	No owner	splunk-dashboard-studio	Global   Permissions	Enabled	Move   D
D:\splunk\etc\apps\search\lookups\geo_attr_countries.csv	No owner	search	Global   Permissions	Enabled	Move   D
D:\splunk\etc\apps\search\lookups\geo_attr_us_states.csv	No owner	search	Global   Permissions	Enabled	Move   D
D:\splunk\etc\apps\search\lookups\geo_countries.kmz	No owner	search	Global   Permissions	Enabled	Move   D
D:\splunk\etc\apps\search\lookups\geo_us_states.kmz	No owner	search	Global   Permissions	Enabled	Move   D
D:\splunk\etc\apps\splunk-dashboard-studio\lookups\geomaps_data.csv	No owner	splunk-dashboard-studio	Global   Permissions	Enabled	Move   D
D:\splunk\etc\apps\timeline_app\lookups\outages.csv	No owner	timeline_app	Global   Permissions	Enabled	Move   D
D:\splunk\etc\apps\splunk-dashboard-studio\lookups\outages_example.csv	No owner	splunk-dashboard-studio	Global   Permissions	Enabled	Move   D
D:\splunk\etc\apps\python_upgrade_readiness_app\lookups\pura_mark_public_as_private.csv	No owner	python_upgrade_readiness_app	Global   Permissions	Enabled	Move   D
D:\splunk\etc\apps\splunk-dashboard-studio\lookups\security_example_data.csv	No owner	splunk-dashboard-studio	Global   Permissions	Enabled	Move   D
D:\splunk\etc\apps\search\lookups\status.csv	snehal_splunk24	search	Global   Permissions	Enabled	Move   D

Fig23. table\_file

A lookup command is used to invoke field value lookups.

Syntax:

Lookup <lookup-table-name><lookup-field1>AS<event-field1>, <lookup-field2>AS<event-field2>OUTPUTNEW<lookup-destfield1>AS<event-destfield>



The screenshot displays the Splunk Enterprise web interface. At the top, the navigation bar includes 'splunk>enterprise', 'Apps', and various user and system links. Below this, the 'Search' tab is active, showing a 'New Search' page. The search query is: `source="tutorialdata.zip:\\www1\\access.log" | lookup status.csv status OUTPUT description | table _time status description`. The results show 13,628 events. The 'Statistics' tab is selected, displaying a table with three columns: '\_time', 'status', and 'description'. The table contains 11 rows of data, showing timestamps, status codes (200, 500, 404), and descriptions ('success', 'internal\_error', 'notfound').

_time	status	description
2024-05-30 23:02:23	200	success
2024-05-30 23:02:22	200	success
2024-05-30 22:57:36	200	success
2024-05-30 22:57:35	200	success
2024-05-30 22:57:34	200	success
2024-05-30 22:57:33	200	success
2024-05-30 22:57:33	200	success
2024-05-30 22:57:32	200	success
2024-05-30 22:57:31	500	internal_error
2024-05-30 22:57:31	404	notfound

Fig24. lookup command

## Lookup definition

A lookup definition provides a lookup name and a path to find the lookup table. Lookup definitions can include extra settings such as matching rules, or restrictions on the fields that the lookup is allowed to match. One lookup table can have multiple lookup definitions.

All lookup types require a lookup definition. After you create a lookup definition you can invoke the lookup in a search with the `lookup` command.

**Lookup definitions**

Showing 1-25 of 31 items

App: Search & Reporting (s...) Configuration Source: Visible in the App Owner: Any filter 25 per page

Name	Type	Supported fields	Lookup file	Owner	App	Sharing
dnslookup	external	clienthost,clientip		No owner	system	Global   Pe
era_email_notification_switch	kvstore	is_era_email_enabled, is_updated		No owner	python_upgrade_readiness_app	Global   Pe
era_email_receivers_list	kvstore	name, email, roles, selected		No owner	python_upgrade_readiness_app	Global   Pe
era_page_visits	kvstore	user, time_stamp		No owner	python_upgrade_readiness_app	Global   Pe
era_remote_dismiss_app	kvstore	app, app_path, dismissed_by, dismiss_app_date		No owner	python_upgrade_readiness_app	Global   Pe
era_remote_dismiss_file	kvstore	app, check, file_path, app_path, instance, dismissed_by, dismiss_file_date		No owner	python_upgrade_readiness_app	Global   Pe
era_remote_dismiss_system_check	kvstore	check_name, dismiss_check_date		No owner	python_upgrade_readiness_app	Global   Pe
era_remote_export_report	kvstore	app, exported_by, export_report_date		No owner	python_upgrade_readiness_app	Global   Pe

Fig25. lookup definition

## Add new

Lookups > Lookup definitions > Add new

Destination app
search

Name \*
status\_code\_lookup

Type
File-based

Lookup file \*
status.csv

Create and manage lookup table files.

☐ Configure time-based lookup
☐ Advanced options

Cancel
Save

Fig26. lookup definition

splunk>enterprise

Apps

⚠ Administrator

1 Messages

Settings

Activity

Help

Find

## Lookup definitions

Lookups > Lookup definitions

New Lookup Definition

Showing 1-1 of 1 item

App

Search & Reporting (s...

Configuration Source

Visible in the App

Owner

Any

status

25 per page

Name	Type	Supported fields	Lookup file	Owner	App	Sharing	Status	Actions
status_code_lookup	file	status,description	status.csv	snehal_splunk24	search	Global   Permissions	Enabled   Disable	Clone   Move   Delete

Fig27. lookup definition

## Automatic lookup

Use automatic lookups to apply a lookup to all searches at search time. After you define an automatic lookup for a lookup definition, you do not need to manually invoke it in searches with the `lookup` command.

**Add new**  
Lookups > Automatic lookups > Add new

Destination app: search

Name \*: status\_automatic\_lookup

Lookup table \*: status\_code\_lookup

Apply to: sourcetype | named \*:

Lookup input fields: status = status | Delete  
+ Add another field

Lookup output fields: description = description | Delete  
+ Add another field

☐ Overwrite field values

Cancel Save

Fig28. Automatic lookup1

**Automatic lookups**  
Lookups > Automatic lookups

Showing 1-1 of 1 item

App: Search & Reporting (s...) | Configuration Source: Visible in the App | Owner: Any | filter: | 25 per page

Name	Lookup	Owner	App	Sharing	Status	Actions
access_combined_wcookie : LOOKUP-status_automatic_lookup	status_code_lookup status AS status OUTPUTNEW description AS description	snehal_splunk24	search	Global   Permissions	Enabled	Clone   Move   Delete

New Automatic Lookup

Fig29. Automatic lookup2

**New Search** Save As Create Table View Close

source="tutorialdata.zip:\\www1/access.log" sourcetype="access\_combined\_wcookie" | table \_time status description Last 24 hours Q

✓ 240 events (6/4/24 4:30:00.000 PM to 6/5/24 4:31:31.000 PM) No Event Sampling Job II ■ ↻ ⬇ ⬆ Smart Mode

Events Patterns Statistics (240) Visualization

20 Per Page Format Preview < Prev 1 ... 3 4 5 6 7 8 9 ... Next >

_time	status	description
2024-06-04 18:18:58	406	not_acceptable
2024-06-04 18:18:58	200	success
2024-06-04 18:18:57	200	success
2024-06-04 18:18:56	200	success
2024-06-04 18:18:59	200	success
2024-06-04 18:18:58	200	success
2024-06-04 18:18:58	200	success
2024-06-04 18:18:56	200	success
2024-06-04 18:18:55	500	internal_error
2024-06-04 18:18:55	200	success
2024-06-04 18:18:57	200	success

Fig30. Automatic lookup3

Here , no lookup command was used ,but still the data from external file was used to display status and description.

### To create an alert:

We can save our search as alert to create an alert. The alert feature in Splunk empowers users to proactively monitor their data for specific conditions or events and receive notifications when these conditions are met. Users can create alerts based on predefined criteria, such as threshold values, patterns, or anomalies detected in their data. When an alert condition is triggered, Splunk can automatically send notifications via email, SMS, or other channels, alerting users and stakeholders to potential issues or opportunities in real-time. Alerts can be customized with various parameters, including severity levels, suppression conditions, and escalation actions, ensuring that users receive timely and relevant notifications tailored to their specific needs. By leveraging the alert feature in Splunk, users can stay informed, respond quickly to critical events, and take proactive measures to address emerging challenges or capitalize on opportunities in their data. We can write our query in search bar and save it as alert.

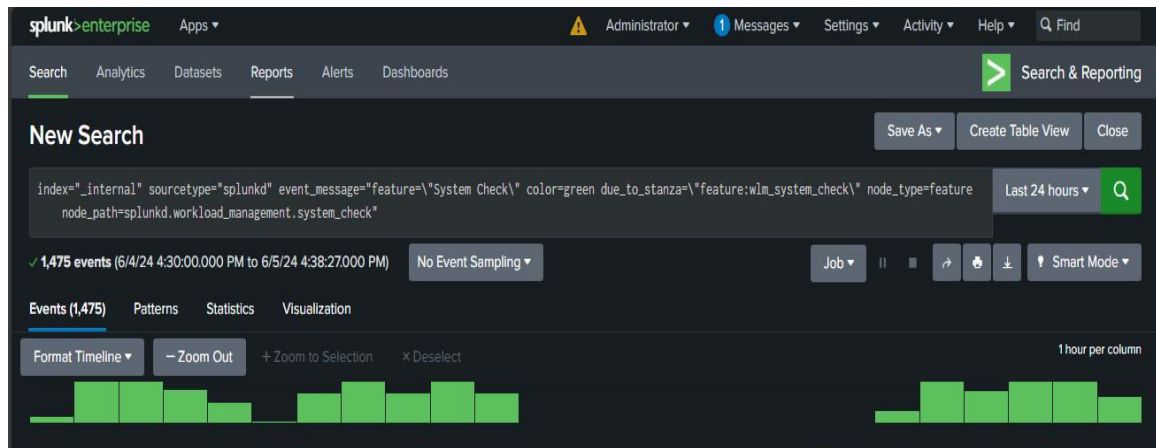


Fig31. Alert\_definition

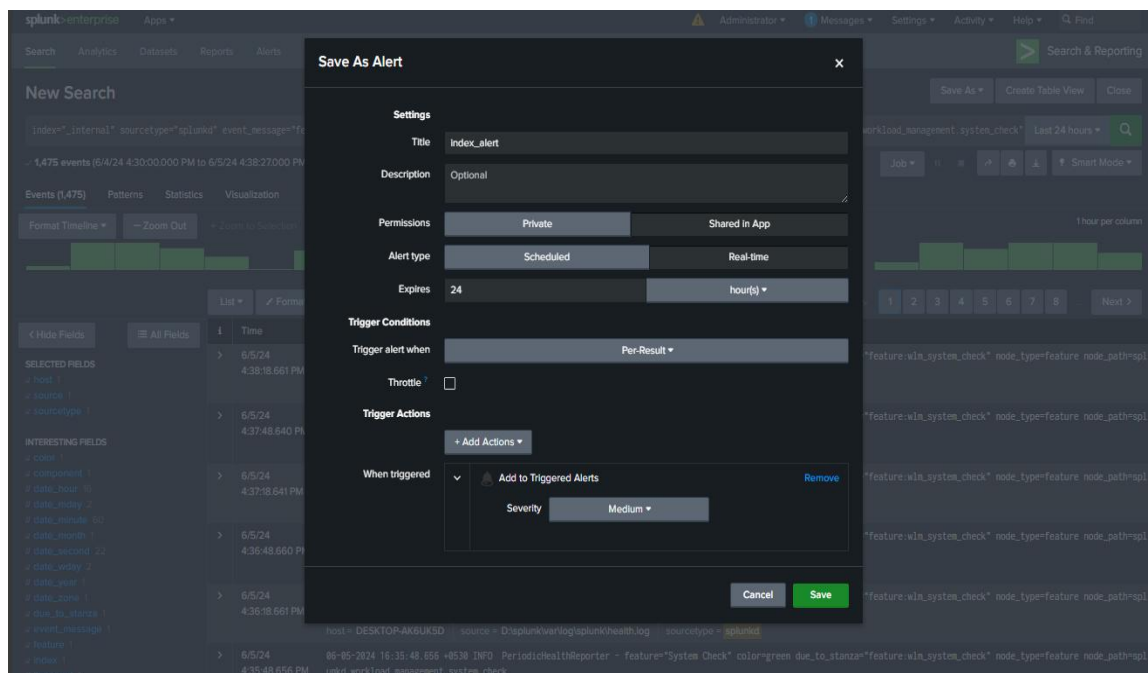


Fig32. Alert\_definition

**Searches, Reports, and Alerts**

Searches, reports, and alerts are saved searches created from pivot or the search page. [Learn more](#)

7 Searches, Reports, and Alerts Type: All App: Search & Reporting (search) Owner: Administrator (snehal\_splunk24) filter 10 per page

Name	Actions	Type	Next Scheduled Time	Display View	Owner	App	Alerts	Sharing	Status
access_log	Edit Run	Report	none	none	snehal_splunk24	search	0	Private	Enabled
dash_demo	Edit Run	Report	none	none	snehal_splunk24	search	0	Private	Enabled
index_alert	Edit Run	Alert	none	none	snehal_splunk24	search	0	App	Enabled
index_opt_alert	Edit Run View Recent	Alert	2024-06-05 16:42:00 India Standard Time	none	snehal_splunk24	search	1266	App	Enabled
internal_scheduled_report	Edit Run	Report	none	none	snehal_splunk24	search	0	Private	Enabled
internal_report_1	Edit Run	Report	none	none	snehal_splunk24	search	0	Private	Enabled
internal_trial	Edit Run	Report	none	none	snehal_splunk24	search	0	Global	Enabled

Fig33. Alert



## Indexes:

Indexes in Splunk serve as repositories for storing and organizing data ingested into the platform. They provide a structured and efficient way to store and retrieve data, enabling users to quickly search, analyze, and visualize large volumes of machine-generated data. Splunk indexes can be configured to accommodate diverse data types and sources, including logs, metrics, and event data. Users can define index settings such as retention periods, access controls, and data segmentation to optimize storage and performance according to their specific requirements. Indexes play a critical role in enabling fast and reliable data retrieval, supporting various use cases such as security monitoring, IT operations, and business analytics. By effectively managing indexes, users can efficiently leverage the full capabilities of Splunk to derive actionable insights and drive informed decision-making from their data.

The screenshot shows the 'New Index' configuration window in Splunk Enterprise. The window is titled 'New Index' and has a close button (X) in the top right corner. The 'General Settings' section includes the following fields:

- Index Name:** Set to 'System\_index'. A tooltip indicates: 'Set index name (e.g., INDEX\_NAME). Search using index=INDEX\_NAME.'
- Index Data Type:** Set to 'Events'. A tooltip indicates: 'The type of data to store (event-based or metrics).'
- Home Path:** Set to 'optional'. A tooltip indicates: 'Hot/warm db path. Leave blank for default (\$SPLUNK\_DB/INDEX\_NAME/db).'
- Cold Path:** Set to 'optional'. A tooltip indicates: 'Cold db path. Leave blank for default (\$SPLUNK\_DB/INDEX\_NAME/colddb).'
- Thawed Path:** Set to 'optional'. A tooltip indicates: 'Thawed/resurrected db path. Leave blank for default (\$SPLUNK\_DB/INDEX\_NAME/thaweddb).'
- Data Integrity Check:** Set to 'Enable'. A tooltip indicates: 'Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.'
- Max Size of Entire Index:** Set to '500 GB'. A tooltip indicates: 'Maximum target size of entire index.'
- Max Size of Hot/Warm/Cold Bucket:** Set to 'auto GB'. A tooltip indicates: 'Maximum target size of buckets. Enter "auto\_high\_volume" for high-volume indexes.'
- Frozen Path:** Set to 'optional'. A tooltip indicates: 'Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.'
- App:** Set to 'Search & Reporting'.

The 'Storage Optimization' section is expanded, showing the following information:

- 14 MB
- 488.28 GB
- 10K
- 9 days ago
- 1 day ago
- \$SPLUNK\_DB/defaultdb

The 'Save' button is highlighted in green, and the 'Cancel' button is in grey.

Fig34. Create Indexes



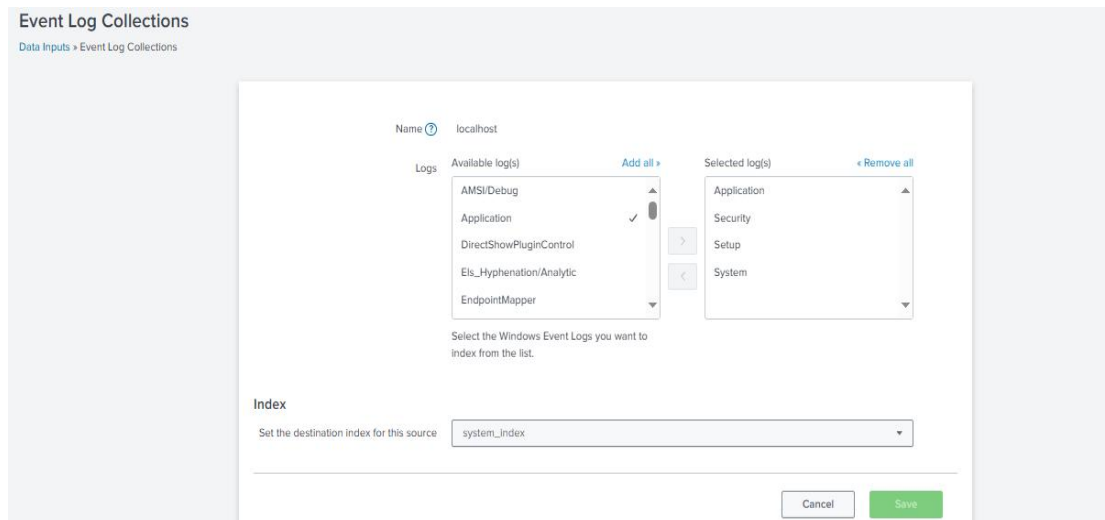


Fig35. event\_log\_collection

The log collection feature in Splunk enables users to gather, aggregate, and index log data from diverse sources across their IT infrastructure. Splunk provides a versatile platform for collecting logs from applications, servers, network devices, and other systems, allowing users to centralize their log data in one location for easy access and analysis. With support for various log formats and protocols, including syslog, Windows Event Logs, and APIs, Splunk offers flexibility in capturing log data from virtually any source. Users can configure log collection settings to specify which logs to collect, how frequently to collect them, and where to store them within Splunk indexes. By leveraging Splunk's log collection capabilities, organizations can gain comprehensive visibility into their IT environment, streamline troubleshooting and monitoring processes, and extract valuable insights from their log data to support business objectives and security initiatives.

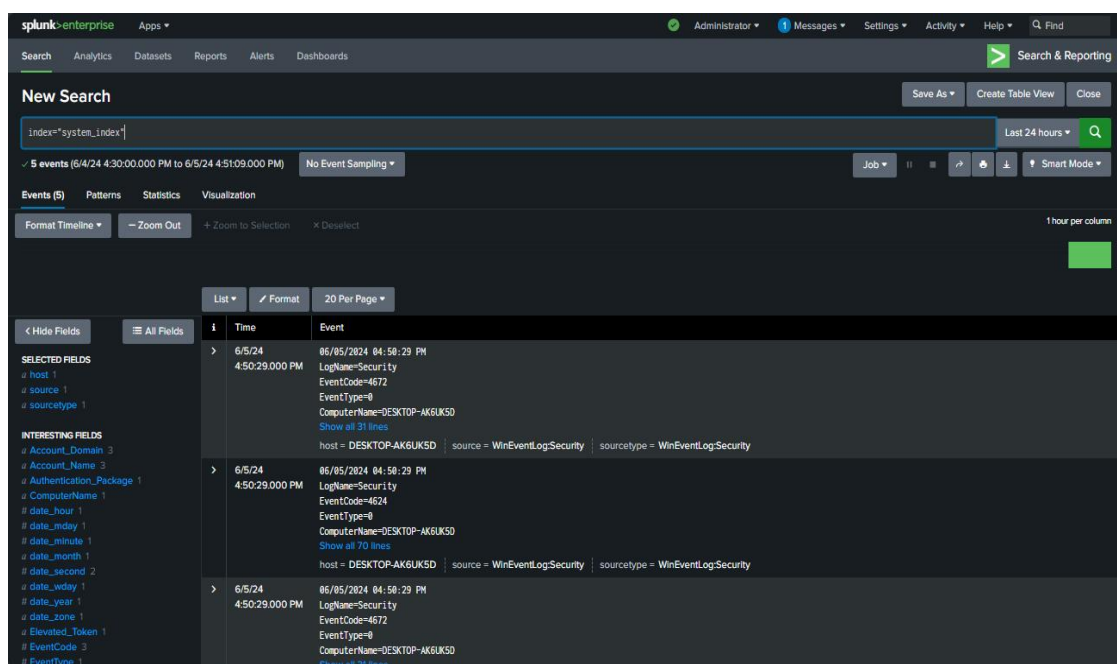


Fig35. windows\_log

## Conclusion

In conclusion, the project "A Comprehensive Demonstration of Splunk SIEM" has provided an extensive exploration of Splunk's diverse functionalities, including event management, dashboard creation, lookup integration, report generation, and alert configuration. Through this comprehensive demonstration, we have showcased how Splunk serves as a powerful platform for security information and event management, empowering organizations to effectively monitor, analyze, and respond to security threats and operational challenges. By leveraging Splunk's capabilities, users can gain deep insights into their data, visualize key metrics and trends, enrich data analysis with external references, generate actionable reports, and proactively detect and mitigate security incidents through automated alerts. Overall, this project underscores the significance of Splunk as a leading solution for operational intelligence and security management, enabling organizations to enhance their security posture, optimize operational efficiency, and make informed decisions based on data-driven insights.