

**SPLUNK ENTERPRISE IN DATA DOMINATION**

**By**

**Isha Singh Malik Ma’am**

**Log Analysis & Threat Detection Using Splunk: Data Ingestion on Dashboarding.**

**On**

**Cyber Security Project Report : Splunk Enterprise Platform**

Submitted in partial fulfillment of the requirements for the Boot camp Certification

**Bachelor of Technology**

**In**

**Computer Science and Engineering – Data Science**

**Of**

**Garden City University**

By

Gangothri Devi M

**Under the guidance of Isha Singh Malik Ma’am.**

**1. Introduction**

This project demonstrates how to use **Splunk’s Search & Reporting app** for log analysis and threat detection.  
It covers **data ingestion**, **SPL queries**, and **dashboard creation** to monitor login events, identify anomalies, and visualize authentication trends.  
The goal is to gain hands-on skills in cybersecurity monitoring using Splunk.

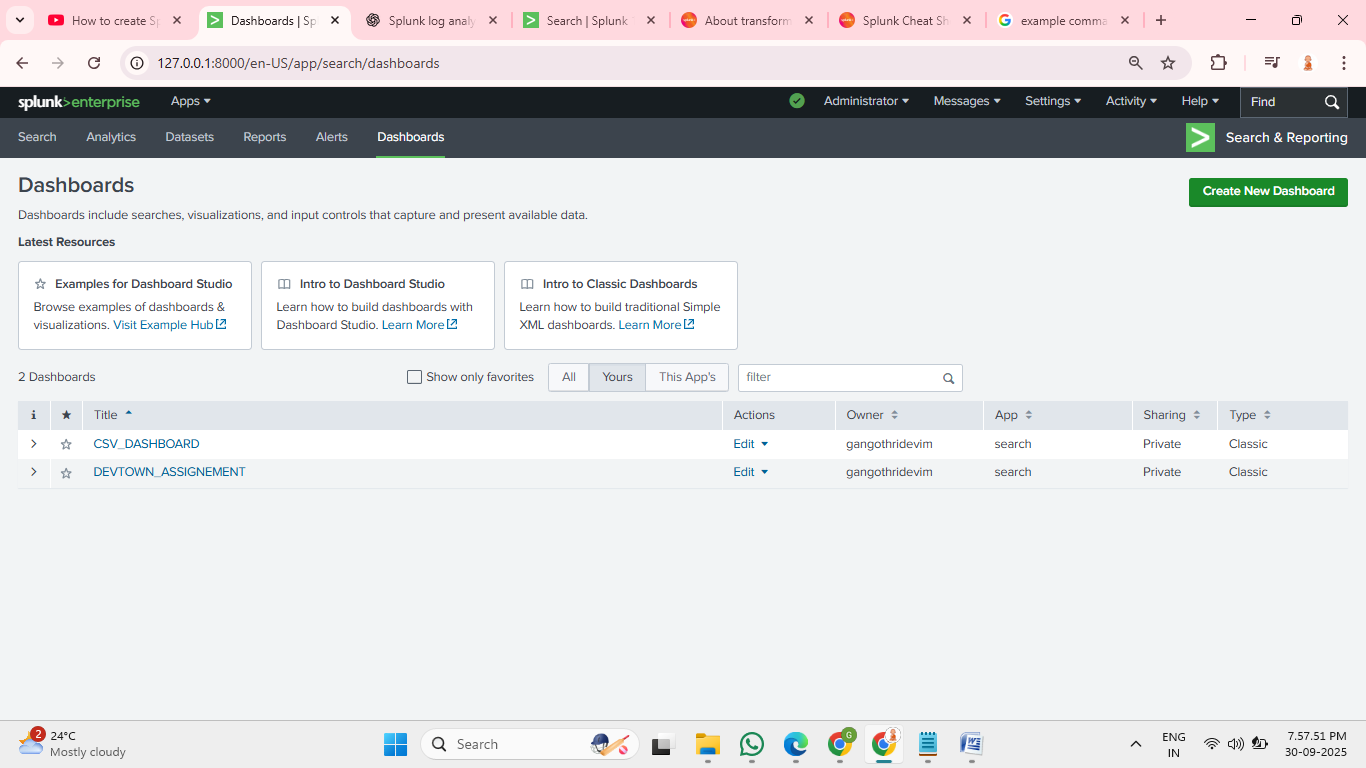
**2. Dataset Used**

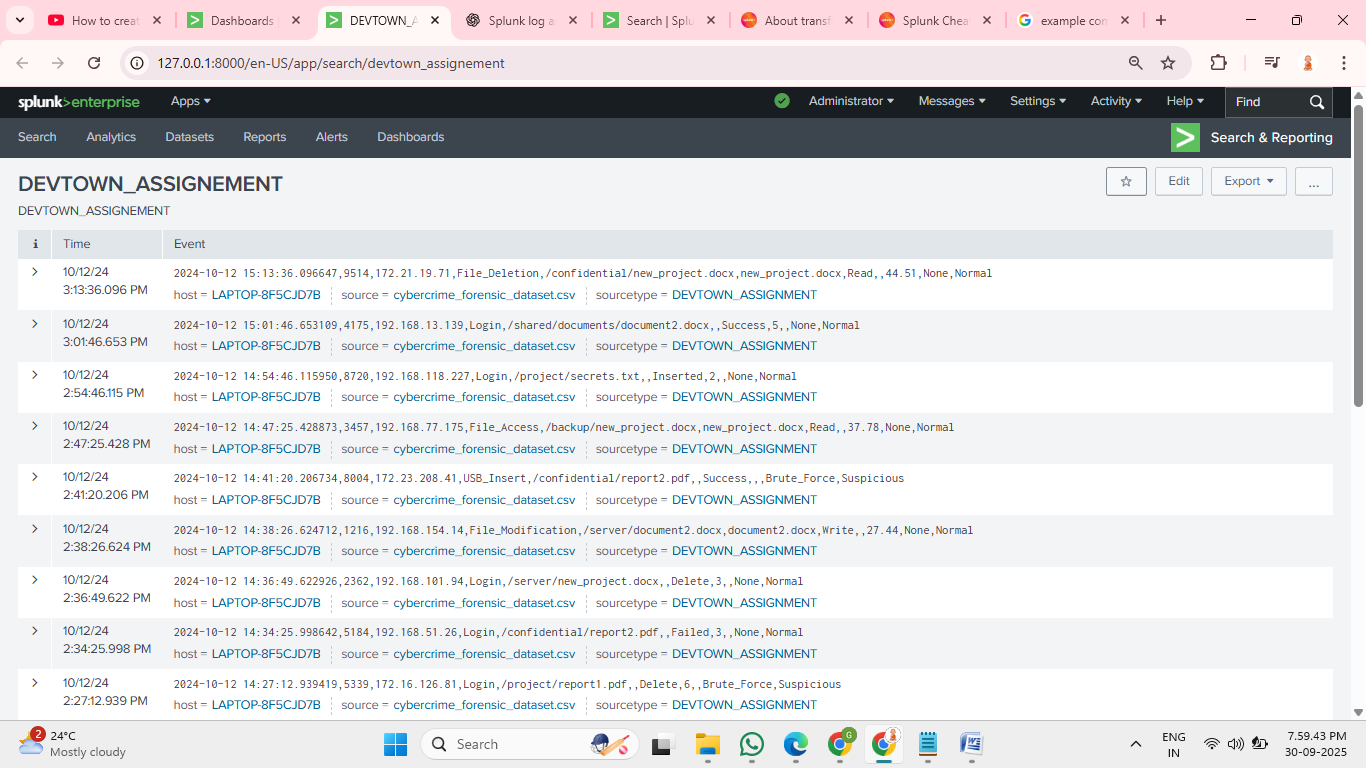
* **Dataset Name:** sample\_login\_events.csv
* **Source:** Created sample log file with structured fields.
* **Fields:**
  + timestamp (login time)
  + username (user ID)
  + ip\_address (source IP)
  + status (Success/Failure)

Sample data format:

| **timestamp** | **username** | **ip\_address** | **status** |
| --- | --- | --- | --- |
| 2025-09-27 09:32:15 | alice | 192.168.1.10 | Success |
| 2025-09-27 09:34:42 | bob | 10.0.0.12 | Failure |
| 2025-09-27 09:35:10 | alice | 192.168.1.10 | Failure |
| 2025-09-27 09:37:25 | charlie | 203.0.113.22 | Success |
|  |  |  |  |

Reference Screenshots of Inserted DataSets:

**



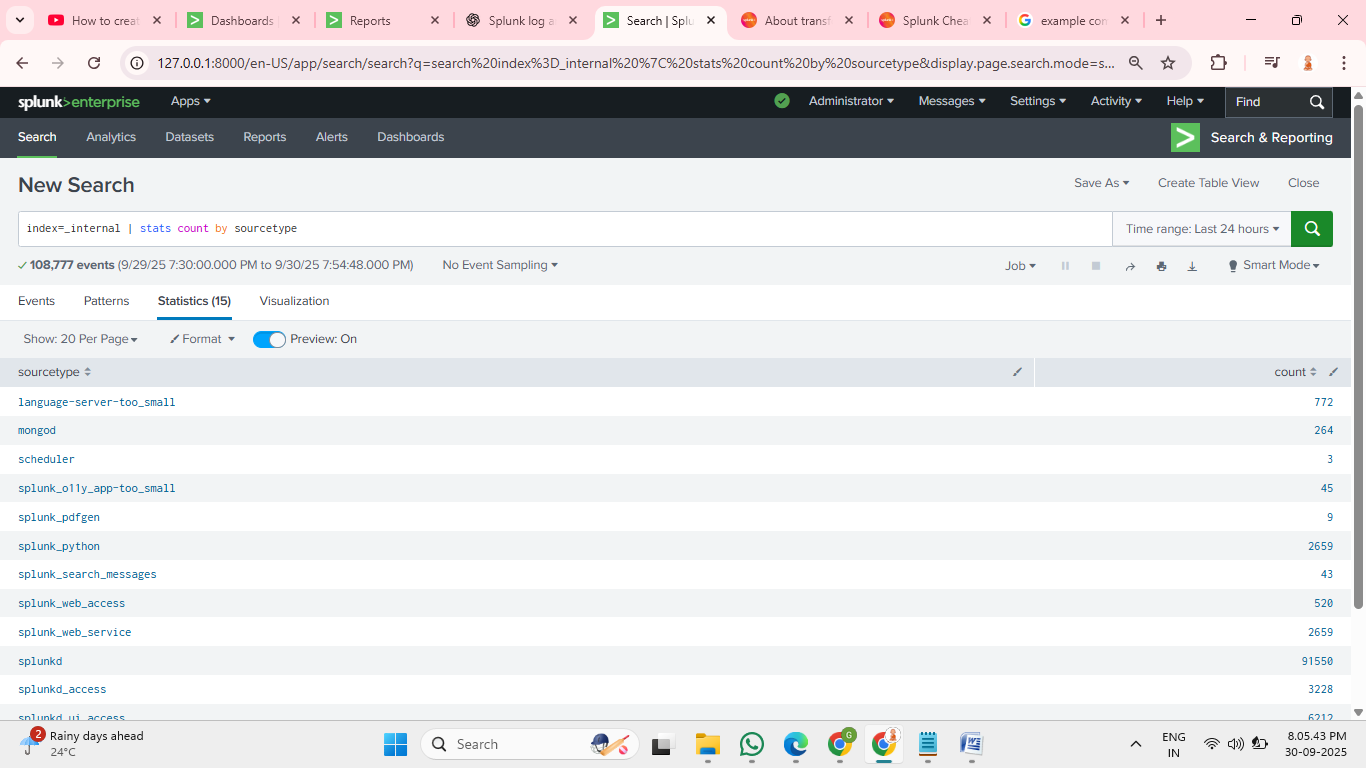
**3. Data Ingestion in Splunk**

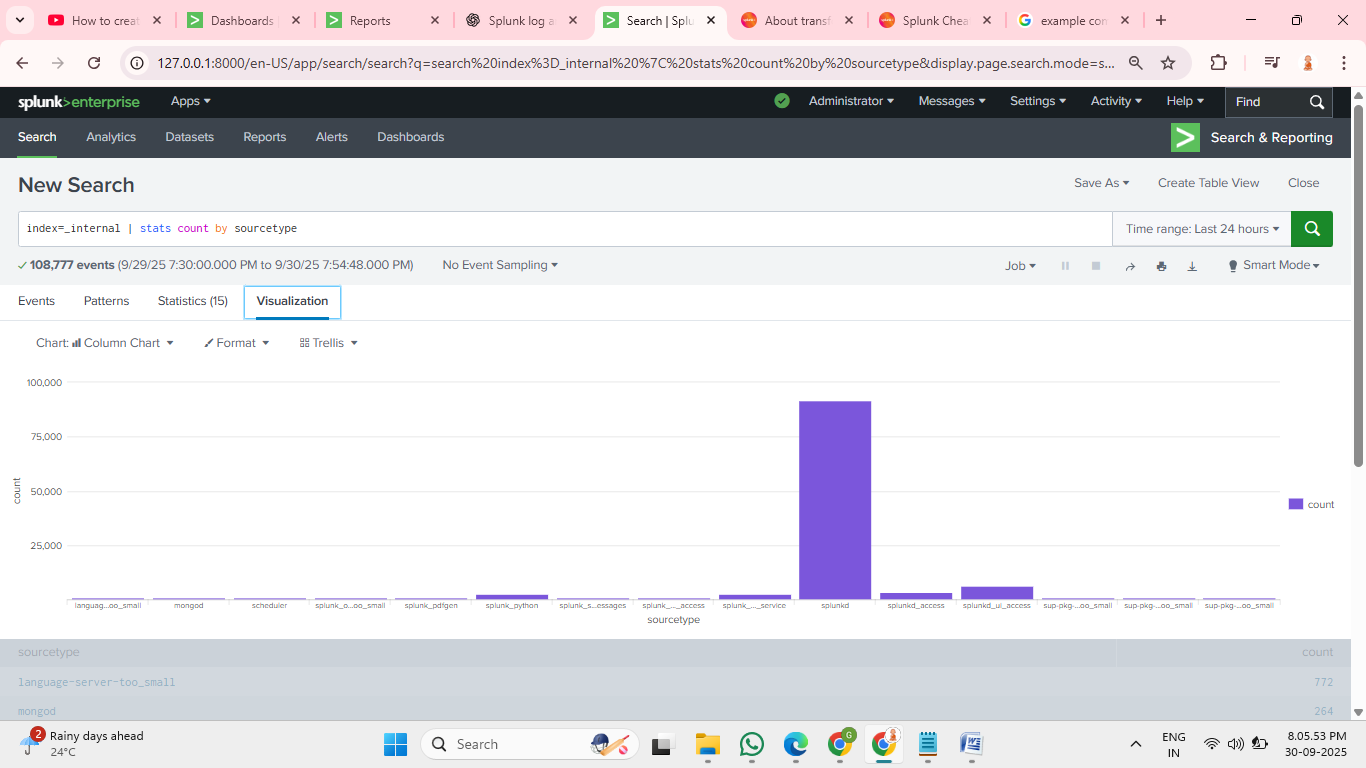
Steps followed:

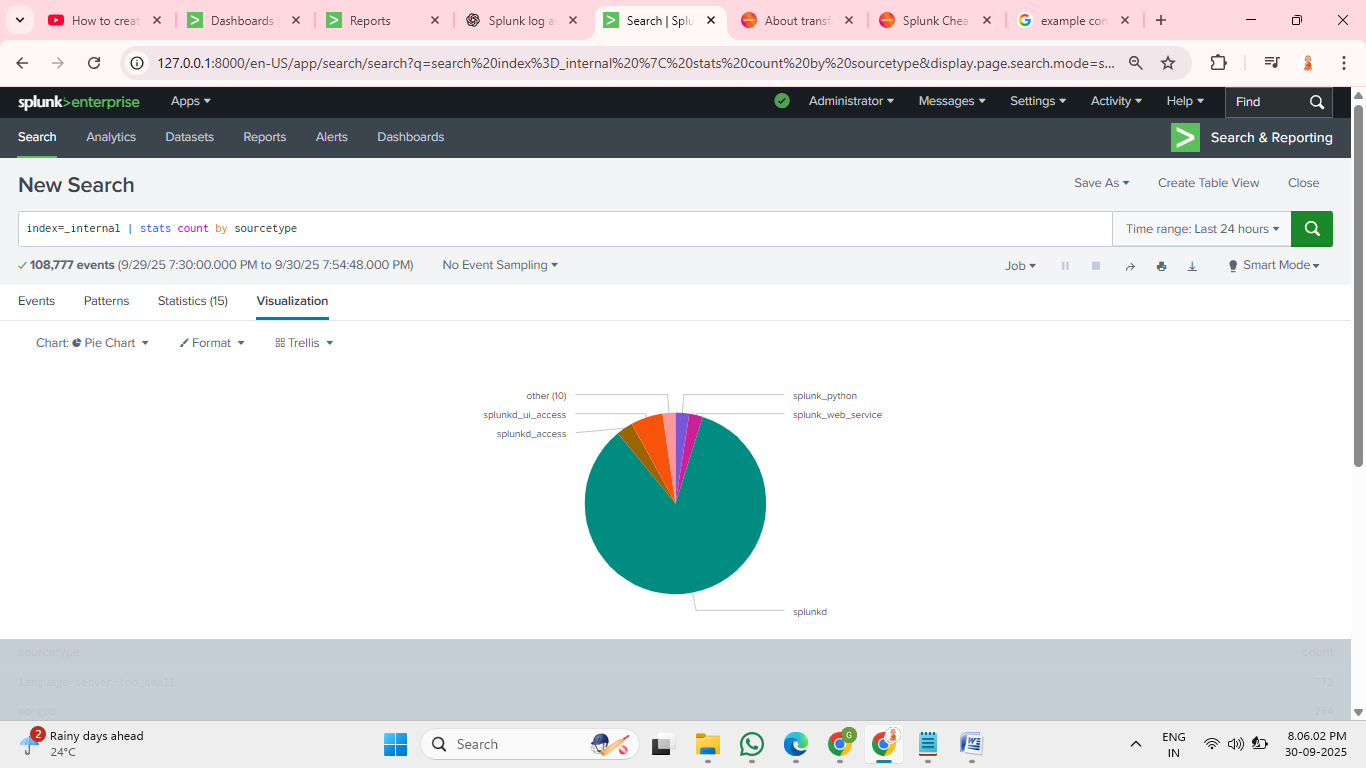
* Open Splunk Search & Reporting app.
* Go to **Settings → Add Data → Upload**.
* Upload sample\_login\_events.csv.
* Choose **Source Type:** csv.
* Assign to **Index:** bootcamp\_logs.
* Click **Submit** to complete ingestion.

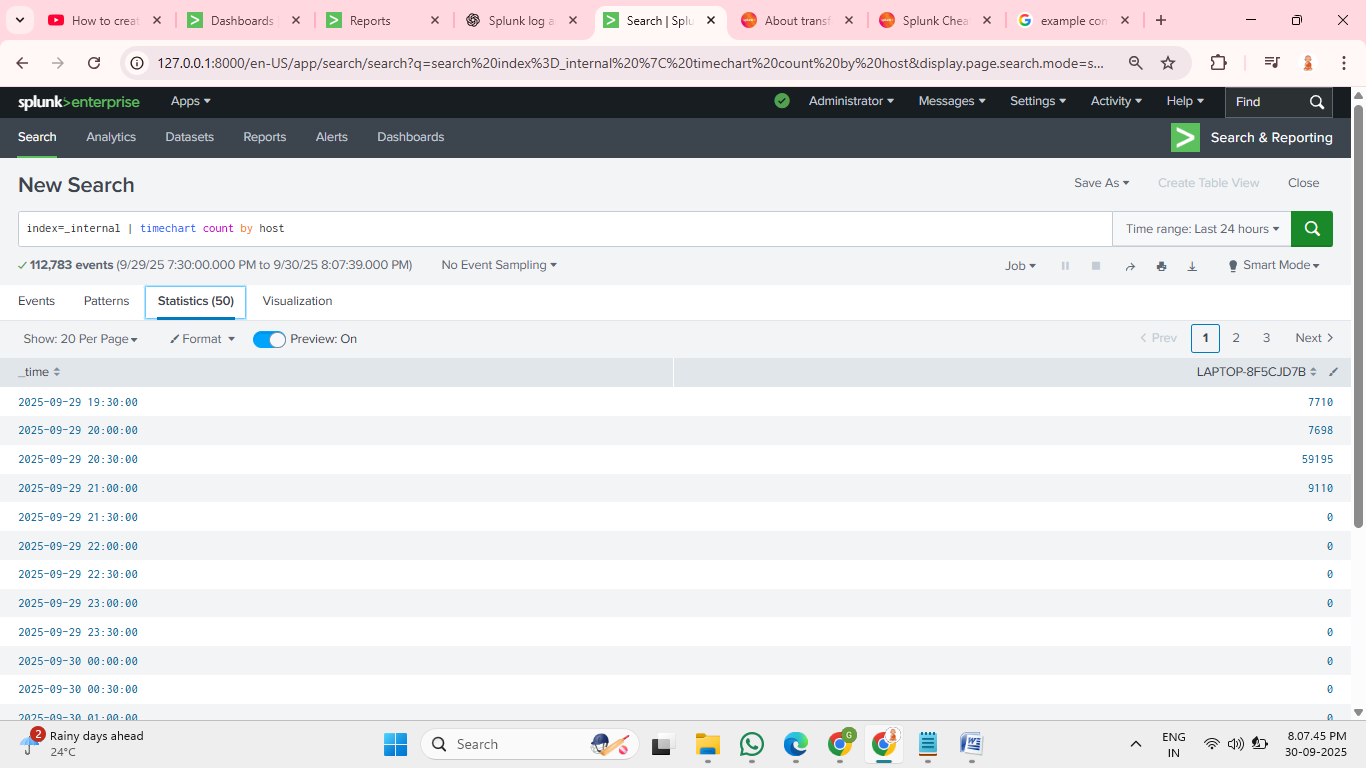
**4. SPL Queries and Explanation**

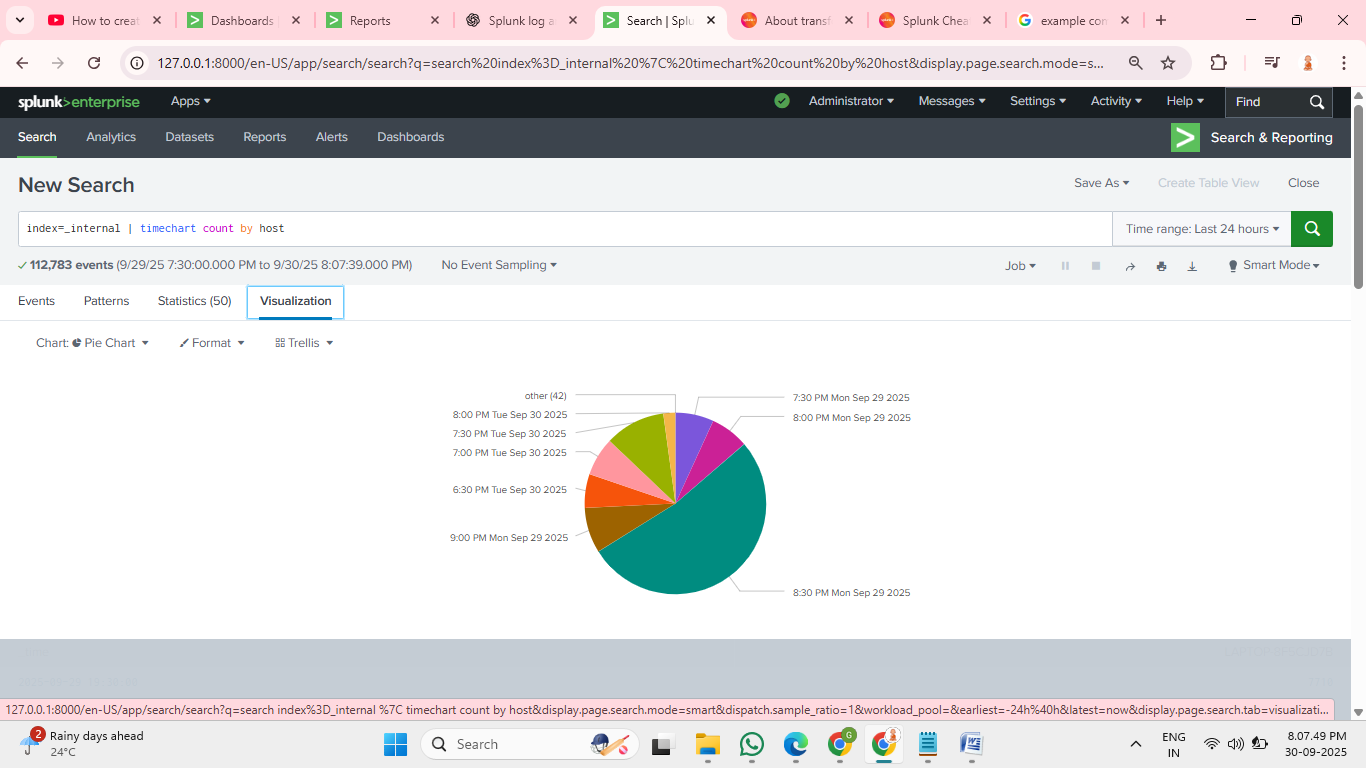
| **Query** | **Purpose / What it shows** |
| --- | --- |
| `index=bootcamp\_logs | stats count by status` |
| `index=bootcamp\_logs status=Failure | top username` |
| `index=bootcamp\_logs status=Failure | top ip\_address` |
| `index=bootcamp\_logs | timechart count by status` |
| `index=bootcamp\_logs status=Failure | stats dc(ip\_address) as UniqueIPs by username` |

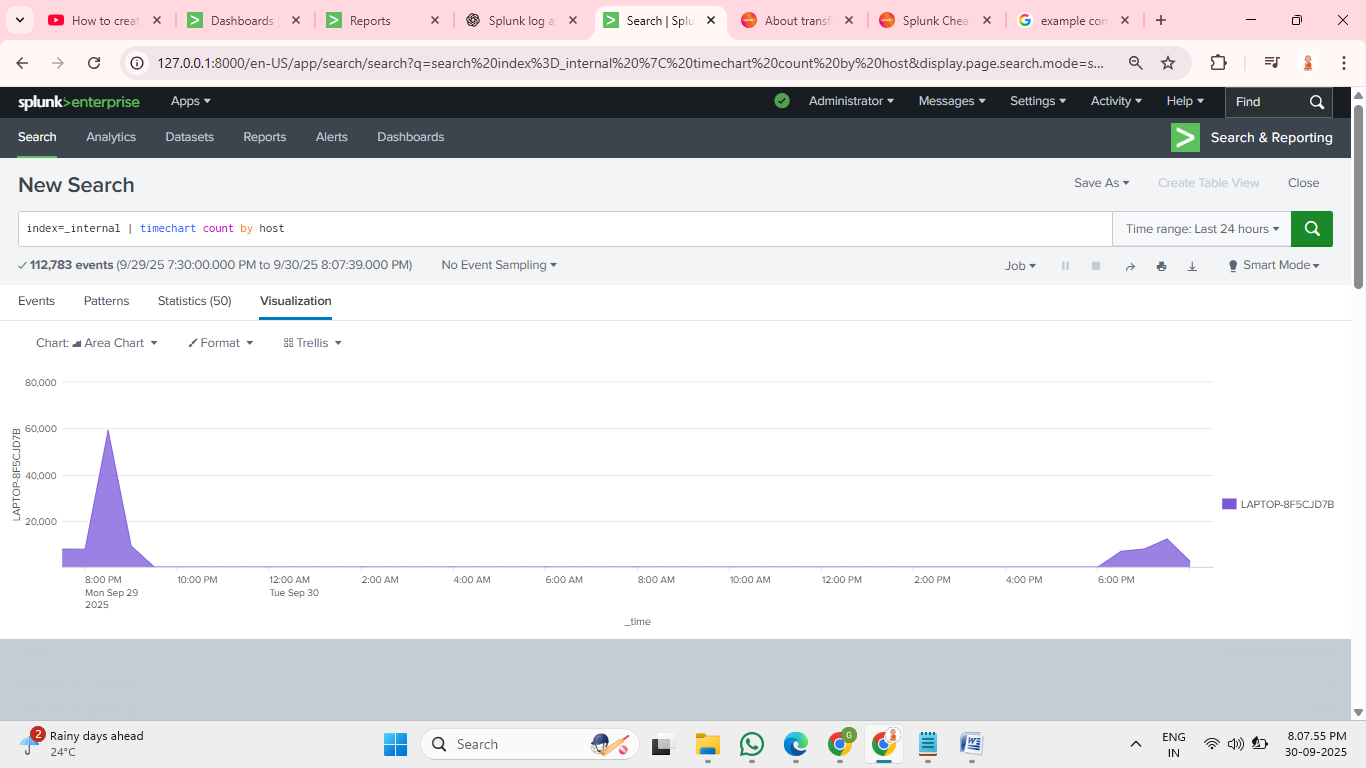
****

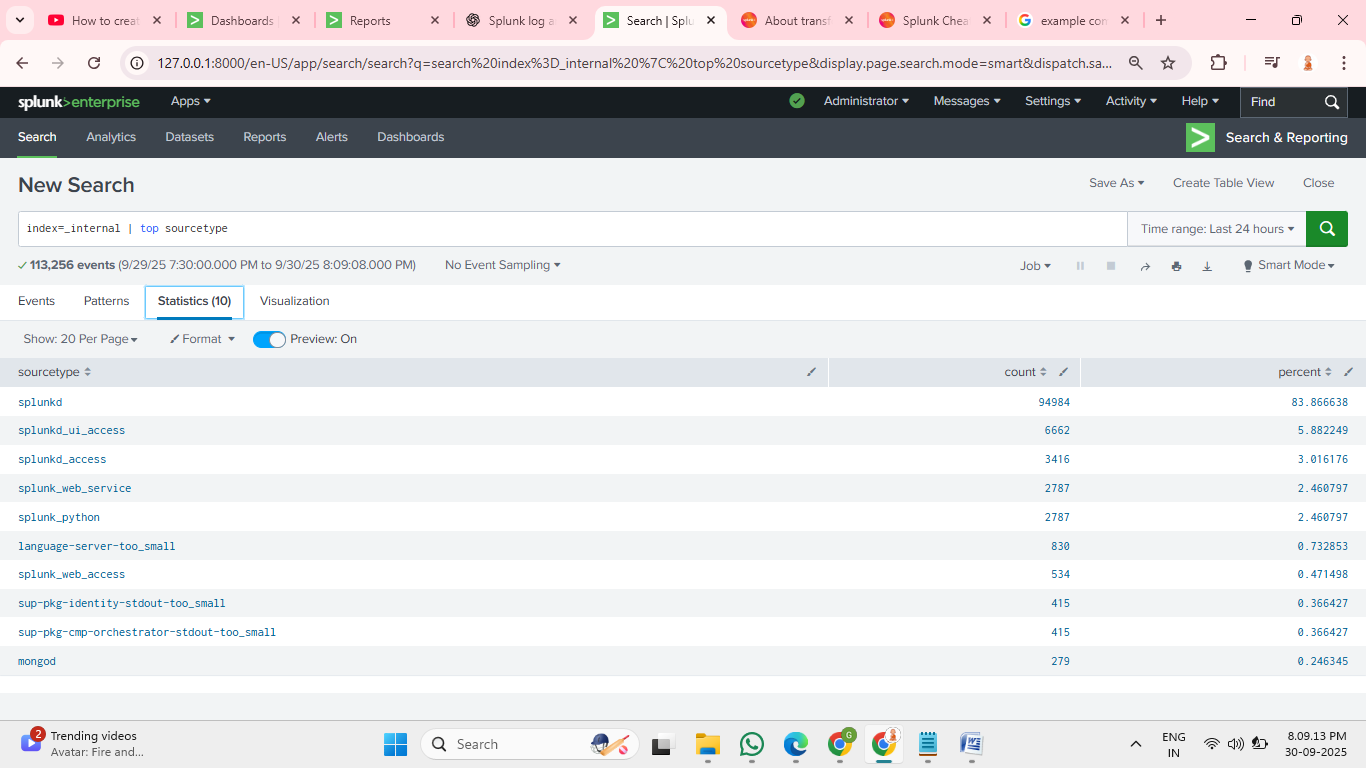
****

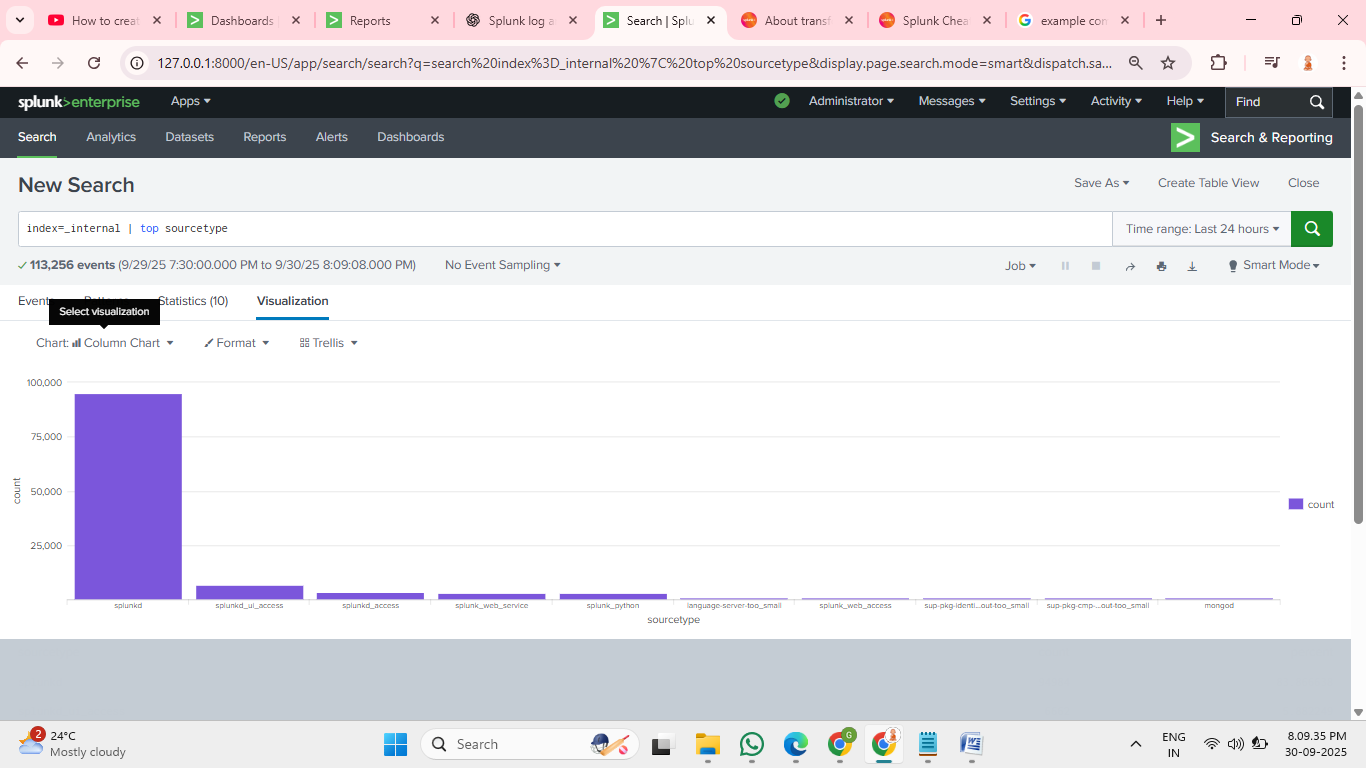
****

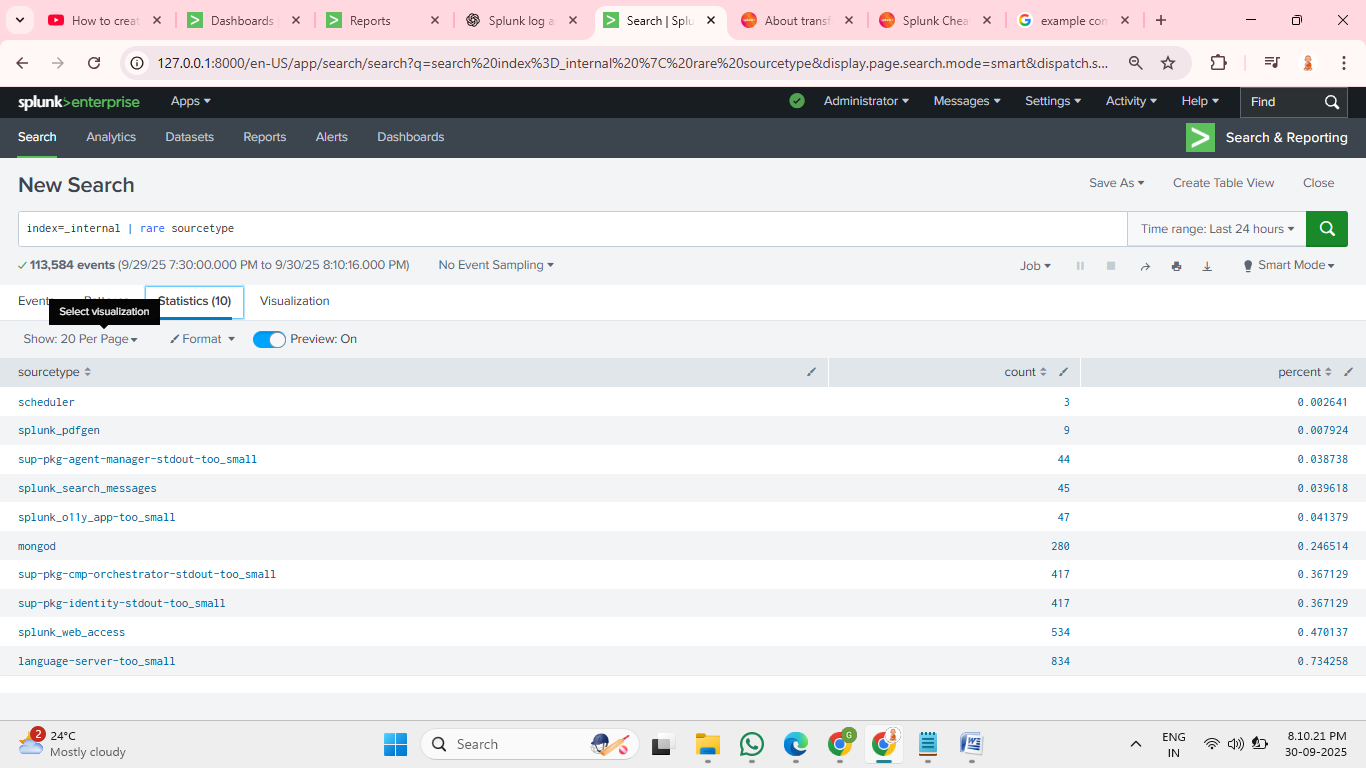
****

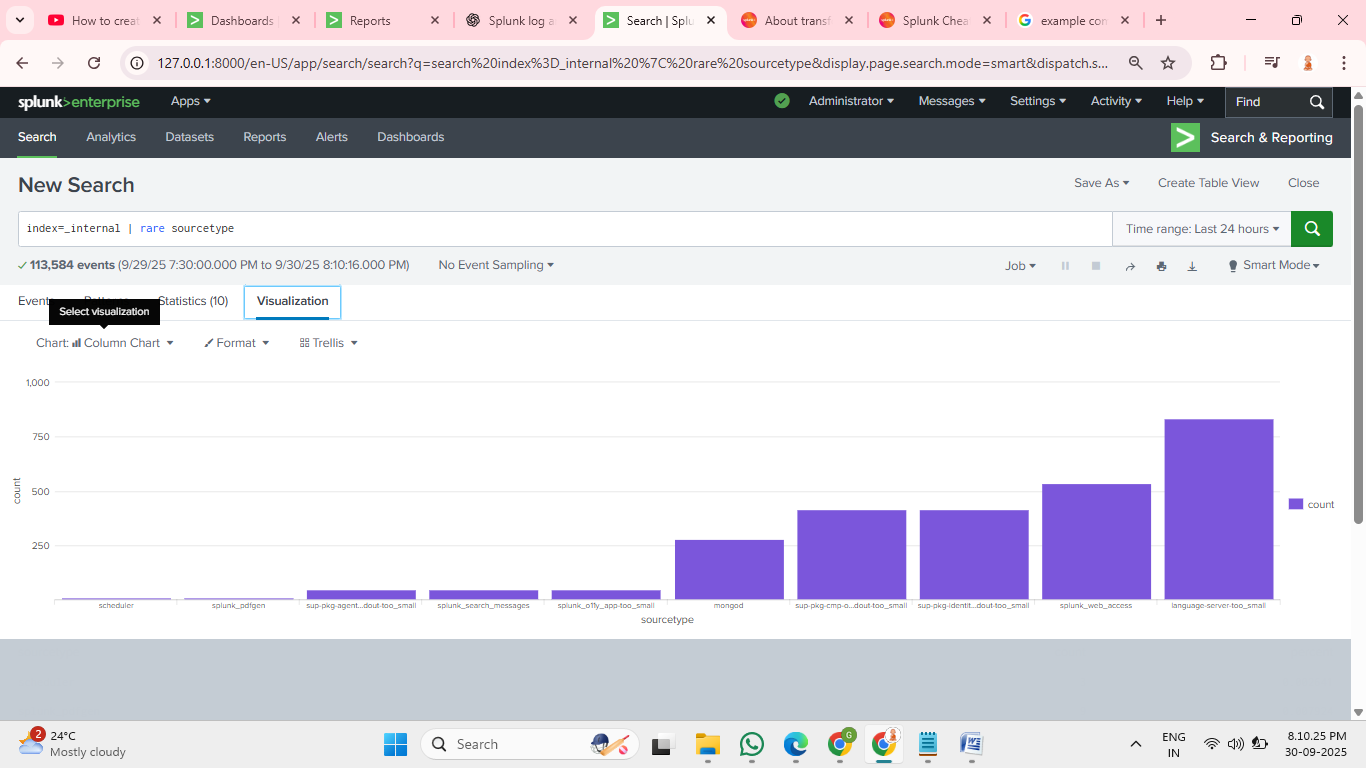
****

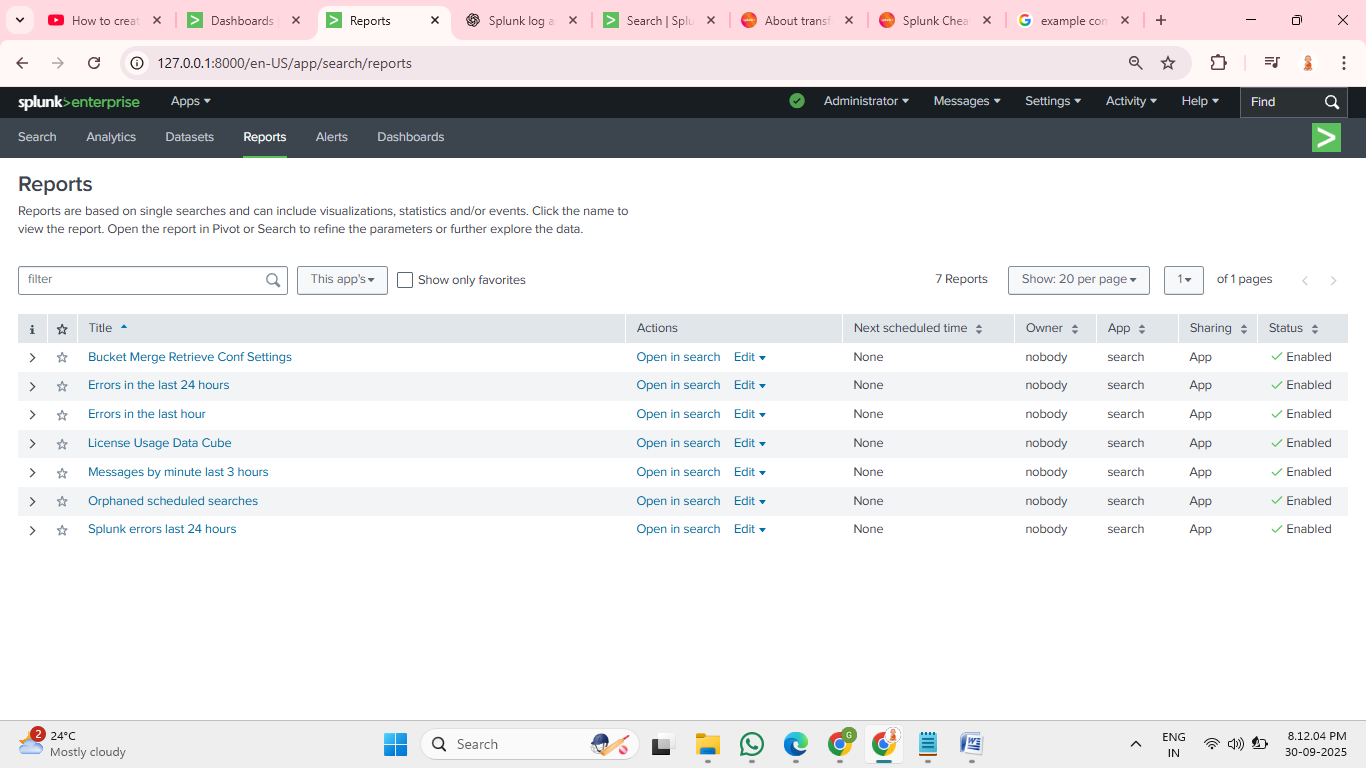
****

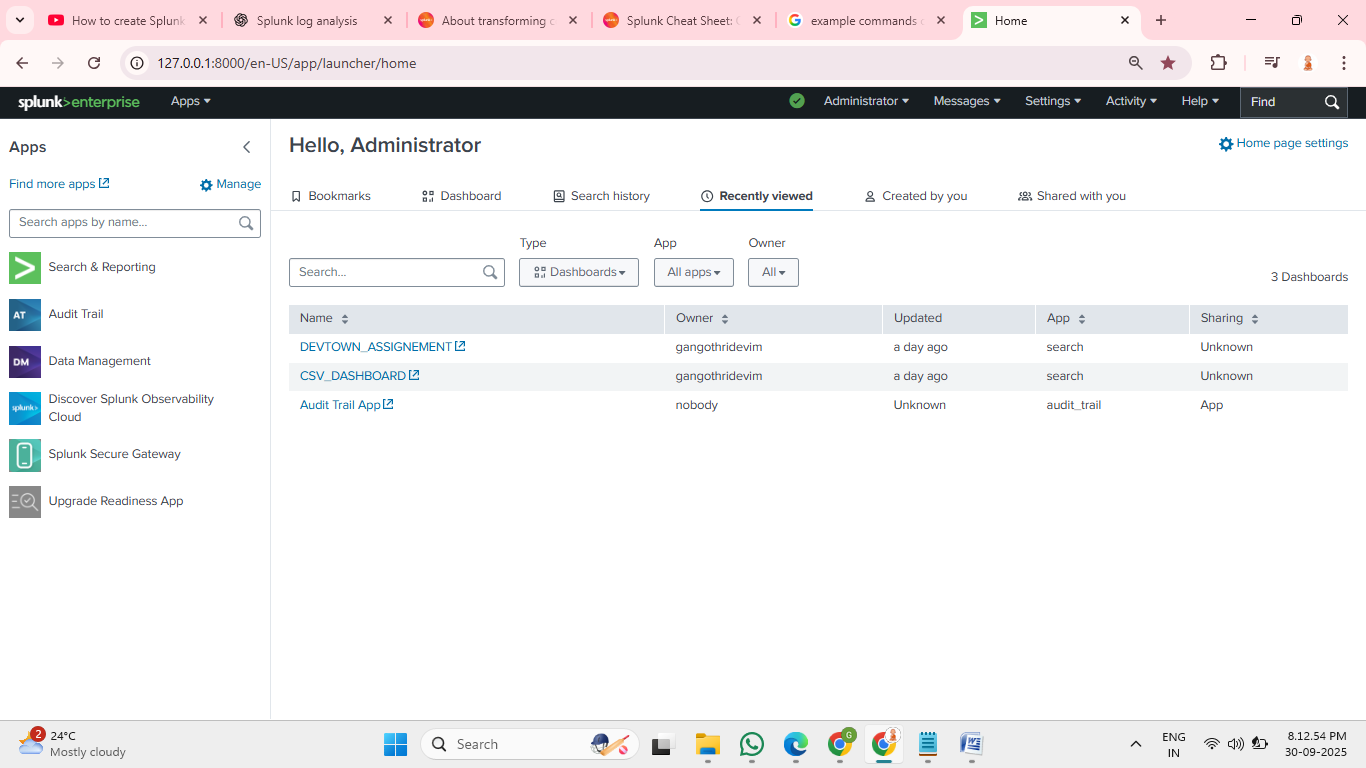
****

****

****

****

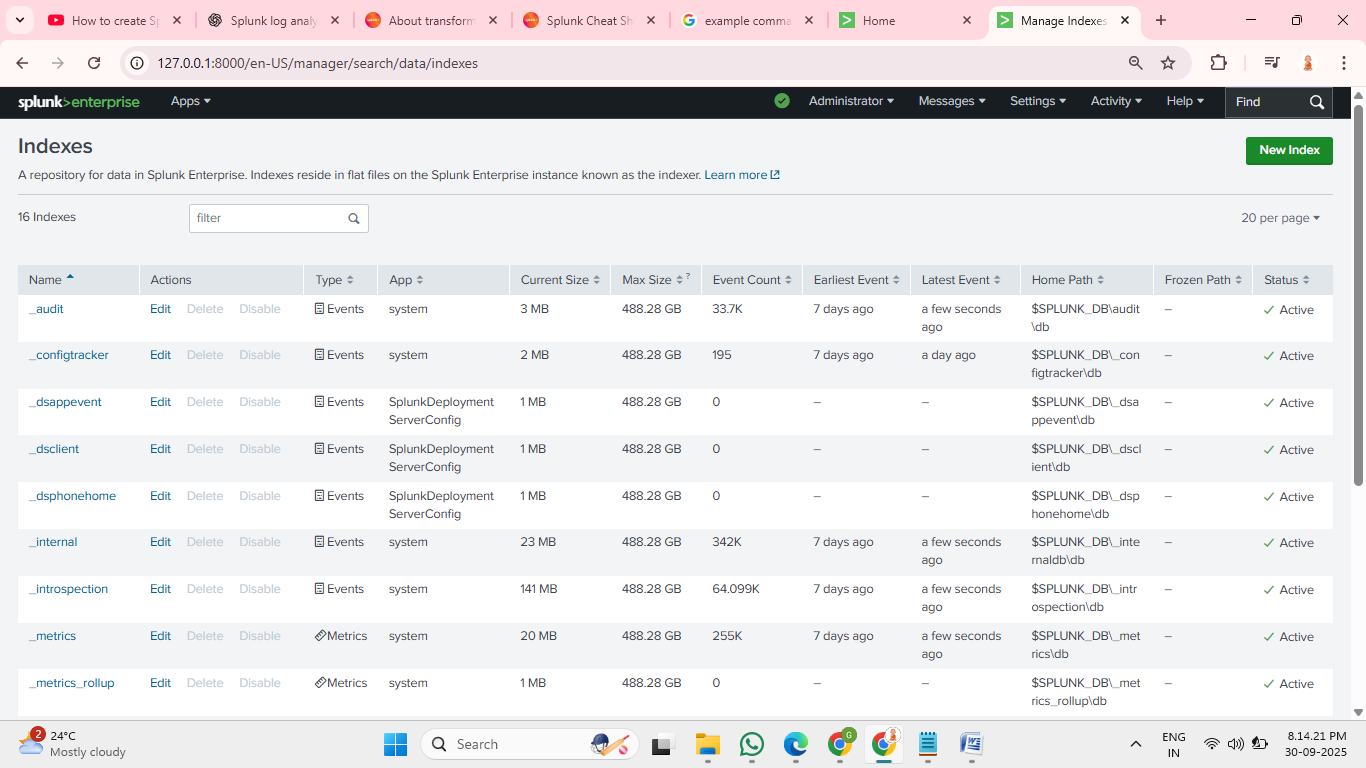
****

****

**5. Dashboard Panels Created**

Dashboard Title: **“Login Analysis”**  
Panels added:

| **Panel Name** | **Visualization** | **Description** |
| --- | --- | --- |
| Login Success vs Failure Count | Pie Chart | Quick view of ratio of successful and failed logins. |
| Failed Logins by Username | Bar Chart | Highlights users with most failed attempts. |
| Failed Logins by IP Address | Bar Chart | Shows suspicious IPs generating failed logins. |
| Login Trends Over Time | Timechart | Visualizes spikes or anomalies in authentication activity. |



**6. Observed Patterns & Findings**

* **High Failure Count for User “bob”:** Could indicate a brute-force attack or forgotten password.
* **Multiple Failures from IP 10.0.0.12:** Possible attacker or misconfigured script.
* **Success vs Failure Ratio:** 70% Success, 30% Failure; normally failure rate is <5%, so this spike needs investigation.
* **Anomalous Spike on 27-Sep-2025 at 09:35 AM:** A sudden increase in failures observed in timechart panel.

**7. Conclusion**

This project successfully demonstrates:

* Ingesting structured log data into Splunk.
* Writing SPL queries to analyze authentication events.
* Building dashboards to visualize and detect anomalies.

Practical outcome: **Improved capability to perform data-driven security investigations** using Splunk dashboards.