**Lab Exercise 6- Create a Dashboard in Splunk with Detailed Log Data**

**Dashboard Creation Exercise Using \_internal Index with 5 Different Types of Charts**

This exercise will guide you through creating a simple Splunk dashboard using the \_internal index. You’ll use five different types of visualizations: **line chart**, **bar chart**, **pie chart**, **table**, and **area chart**.

**Objective**

Learn to:

1. Create a dashboard in Splunk.
2. Use the \_internal index to generate insights.
3. Visualize data using multiple chart types.

**Steps**

**1. Create a Dashboard**

1. Log in to Splunk.
2. Navigate to **Dashboards > Create New Dashboard**.
3. Provide a name (e.g., Internal Monitoring Dashboard) and click **Create**.

**2. Add Panels with Queries**

**Panel 1: Line Chart - Indexing Throughput Over Time**

* **Query**:

index=\_internal sourcetype=splunkd group=per\_index\_thruput

| timechart span=1m sum(kbps) as indexing\_throughput

* **Visualization**: Line Chart
* **Goal**: Show the sum of indexing throughput (in kbps) over time.

**Panel 2: Bar Chart - Top 5 Indexes by Data Ingested**

* **Query**:

index=\_internal source=\*license\_usage.log\* type=Usage

| stats sum(b) as bytes\_ingested by idx

| eval GB\_ingested=bytes\_ingested/1024/1024/1024

| sort -GB\_ingested

| head 5

* **Visualization**: Bar Chart
* **Goal**: Display the top 5 indexes with the highest data ingestion (in GB).

**Panel 3: Pie Chart - Error Distribution**

* **Query**:

index=\_internal log\_level=ERROR

| stats count by sourcetype

* **Visualization**: Pie Chart
* **Goal**: Show the distribution of error events across different source types.

**Panel 4: Table - Search Activity by User**

* **Query**:

index=\_internal sourcetype=splunkd

| stats count by user

* **Visualization**: Table
* **Goal**: List the number of searches performed by each user.

**Panel 5: Area Chart - Errors Over Time**

* **Query**:

index=\_internal log\_level=ERROR

| timechart span=1m count

* **Visualization**: Area Chart
* **Goal**: Display the count of error events over time.

**3. Configure Panel Settings**

* After adding each query to the respective panel:
  + Click **Visualization** and select the appropriate chart type.
  + Customize chart settings (e.g., labels, legends, and colors).
  + Save each panel.

**Deliverables**

1. **Dashboard Name**: Provide the name of the created dashboard (e.g., Internal Monitoring Dashboard).
2. **Panels**:
   * Line Chart: Indexing Throughput Over Time.
   * Bar Chart: Top 5 Indexes by Data Ingested.
   * Pie Chart: Error Distribution.
   * Table: Search Activity by User.
   * Area Chart: Errors Over Time.
3. **Screenshots**: Include screenshots of each panel and the complete dashboard.