**Lab Exercise 9- Creating Multiple Reports Using Splunk’s \_internal Index**

This lab exercise guides you through creating multiple reports using the \_internal index in Splunk. These reports help monitor Splunk performance, user activity, and system health.

**Objective**

1. Create reports from the \_internal index.
2. Use reports to gain insights into Splunk system activity.
3. Save and organize reports for future use.

**Exercise Steps**

**Step 1: Access Splunk and Search the \_internal Index**

1. Log in to Splunk Web.
2. Navigate to the **Search & Reporting** app.
3. Use the index=\_internal query to explore available data.

**Step 2: Create Individual Reports**

**Report 1: Indexing Throughput**

* **Query**:

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

| stats avg(kbps) as avg\_throughput max(kbps) as max\_throughput by series

* **Description**: Displays average and maximum indexing throughput (in kbps) per index.
* **Steps**:
  + Run the query in the search bar.
  + Click **Save As > Report**.
  + Name the report: *Indexing Throughput Report*.
  + Add a description and save.

**Report 2: Errors Over Time**

* **Query**:

index=\_internal log\_level=ERROR

| timechart span=1m count

* **Description**: Displays a timechart of error events per minute.
* **Steps**:
  + Run the query.
  + Save it as a report named *Errors Over Time*.

**Report 3: User Search Activity**

* **Query**:

index=\_internal sourcetype=splunkd

| stats count by user

* **Description**: Shows the number of searches performed by each user.
* **Steps**:
  + Run the query.
  + Save it as a report named *User Search Activity*.

**Report 4: Top Errors**

* **Query**:

index=\_internal log\_level=ERROR

| stats count by event\_message

| sort -count

| head 5

* **Description**: Lists the top 5 most common error messages.
* **Steps**:
  + Run the query.
  + Save it as a report named *Top Errors*.

**Report 5: License Usage**

* **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

* **Description**: Shows the amount of data ingested (in GB) per index.
* **Steps**:
  + Run the query.
  + Save it as a report named *License Usage by Index*.

**Step 3: Organize Reports**

1. Navigate to **Reports** in Splunk.
2. Verify that all saved reports are listed.
3. Optionally, add the reports to a new or existing **dashboard** for easier visualization.

**Deliverables**

1. **Reports Created**:
   * *Indexing Throughput Report*.
   * *Errors Over Time*.
   * *User Search Activity*.
   * *Top Errors*.
   * *License Usage by Index*.
2. **Screenshots**: Include screenshots of each report’s output.
3. **Insights**: Write a short summary for each report highlighting key findings.

**Expected Outcomes**

* **Indexing Throughput**: Identify trends in Splunk’s indexing performance.
* **Errors Over Time**: Detect spikes in error events and their timings.
* **User Search Activity**: Understand user behavior and activity levels.
* **Top Errors**: Highlight the most frequent errors for troubleshooting.
* **License Usage**: Monitor data ingestion and ensure compliance with license limits.

This lab provides a simple and structured approach to creating and leveraging reports for Splunk monitoring and analysis.