**Lab Exercise 8- Complex Search Queries on \_internal Index in Splunk**

**Objective**

**Lab Exercise: Search Queries on \_internal Index in Splunk**

The \_internal index in Splunk contains logs generated by Splunk itself, including information about system activity, indexing performance, searches, and user activity. This exercise focuses on creating queries to extract meaningful insights from the \_internal index.

**Objective**

Perform searches on the \_internal index to:

1. Monitor Splunk performance.
2. Analyze user activity.
3. Understand indexing behavior.
4. Detect potential errors.

**Exercise Steps**

**1. General Search**

* **Query 1: Search All Events in \_internal**

index=\_internal

**Goal:** View all raw events in the \_internal index.

* **Query 2: Search for Events Related to Errors**

index=\_internal log\_level=ERROR

**Goal:** Retrieve all logs with the log level set to ERROR.

**2. Monitoring Splunk Performance**

* **Query 3: Monitor Indexing Performance**

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

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

**Goal:** Analyze average and maximum indexing throughput (in kilobits per second) per index.

* **Query 4: Check License Usage**

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

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

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

**Goal:** View the total amount of data ingested per index in GB.

**3. Analyzing Search Activity**

* **Query 5: Count Searches by User**

index=\_internal sourcetype=splunkd component=SearchExecutor

| stats count by user

**Goal:** Count how many searches each user has run.

* **Query 6: Identify Long-Running Searches**

index=\_internal sourcetype=splunkd component=SearchExecutor

| where total\_run\_time > 60

| stats count by user search total\_run\_time

**Goal:** Identify searches that took longer than 60 seconds to execute.

**4. Error Detection and Troubleshooting**

* **Query 7: Identify the Most Common Errors**

index=\_internal log\_level=ERROR

| stats count by log\_message

| sort -count

**Goal:** List the most frequently occurring errors.

* **Query 8: Detect Configuration Issues**

index=\_internal sourcetype=splunkd component=ConfChanges

**Goal:** Retrieve logs related to configuration changes.

**5. Time-Based Analysis**

* **Query 9: Errors Over Time**

index=\_internal log\_level=ERROR

| timechart span=1m count

**Goal:** Create a timechart showing the count of error logs per minute.

* **Query 10: Indexing Volume Over Time**

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

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

**Goal:** Visualize indexing throughput over time.

**Deliverables**

1. **Search Queries**: Submit the SPL queries used in the lab.
2. **Query Results**: Provide screenshots of the query results.
3. **Analysis**: Write a short summary of findings, such as:
   * Errors detected.
   * Indexing performance trends.
   * User activity insights.
4. **Dashboard (Optional)**: Create a dashboard with at least 3 panels:
   * Errors over time.
   * Indexing throughput.
   * Searches by user.

**Insights**

This lab exercise demonstrates how the \_internal index can be a powerful tool for monitoring and troubleshooting Splunk's operation. By leveraging the built-in logs, administrators can ensure the system's health and performance. Let me know if you'd like additional guidance!