**Lab Exercise 10- Monitoring Splunk’s Health and Maintaining Performance**

Monitoring and maintaining Splunk’s health is critical for ensuring optimal performance, preventing system failures, and efficiently managing resources. Below are key areas to focus on, along with specific methods and tools for monitoring and maintaining Splunk's performance.

**1. Key Areas to Monitor**

**a. Indexing Performance**

* **Monitor Data Throughput**:
  + Keep track of data ingestion rates to avoid exceeding license limits.
  + Use per\_index\_thruput to monitor throughput per index.
  + Query:

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

| stats sum(kbps) as total\_kbps by series

* **Check Queue Sizes**:
  + Monitor the size of input, parsing, merging, and indexing queues to detect bottlenecks.
  + Query:

index=\_internal sourcetype=splunkd component=metrics group=queue

| stats avg(current\_size) as avg\_size by name

**b. Search Performance**

* **Long-Running Searches**:
  + Identify and optimize slow searches to prevent resource hogging.
  + Query:

index=\_internal sourcetype=splunkd component=SearchExecutor

| where total\_run\_time > 60

| stats avg(total\_run\_time) as avg\_runtime, count by user

* **Concurrent Searches**:
  + Monitor search concurrency to ensure the system handles multiple searches efficiently.
  + Use the Monitoring Console’s Search Activity: Instance panel.

**d. License Usage**

* **Track Daily License Usage**:
  + Avoid exceeding the daily ingestion limits.
  + 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

**e. Errors and Warnings**

* **Monitor System Errors**:
  + Check for error logs to identify misconfigurations or failures.
  + Query:

index=\_internal log\_level=ERROR

| stats count by component

* **Track Warnings**:
  + Identify warnings that could escalate into issues.
  + Query:

index=\_internal log\_level=WARN

| stats count by component

**2. Tools for Monitoring Splunk’s Health**

**a. Splunk Monitoring Console**

* Provides out-of-the-box dashboards to monitor:
  + Indexing performance.
  + Search performance.
  + System resources (CPU, memory, disk).
  + Forwarder activity.
* **How to Access**:
  + Navigate to **Settings > Monitoring Console**.

**b. Alerts and Notifications**

* Set up alerts for critical metrics such as:
  + High queue sizes.
  + License violations.
  + Disk space running low.
* Example Alert Query:

index=\_internal sourcetype=splunkd log\_level=ERROR

| stats count by component

| where count > 10

**c. External Tools**

* Use third-party tools for enhanced monitoring:
  + **Splunk ITSI**: For advanced insights into Splunk performance.
  + **Nagios/Zabbix**: For system-level monitoring (CPU, memory, etc.).

**3. Maintenance Best Practices**

**a. Regularly Update Splunk**

* Keep Splunk and its apps updated to ensure you have the latest features and security patches.

**b. Optimize Search Queries**

* Use best practices for search queries to reduce resource usage:
  + Avoid wildcard searches (e.g., \*).
  + Use indexed fields for filtering.

**c. Manage Data Retention**

* Define appropriate retention policies to avoid excessive storage use.
* Adjust frozenTimePeriodInSecs and ensure older data is archived or deleted.

**d. Clean Old Data**

* Use splunk clean commands to remove unused data and logs:

splunk clean eventdata

**e. Monitor Forwarders**

* Ensure forwarders are active and sending data to the indexer:

index=\_internal sourcetype=splunkd component=Forwarder

| stats count by hostname

**4. Actionable Checklist**

| **Area** | **Task** | **Frequency** |
| --- | --- | --- |
| Indexing Performance | Check queue sizes and throughput. | Daily |
| Search Performance | Monitor long-running and concurrent searches. | Weekly |
| Disk Usage | Verify hot/warm/cold bucket sizes and free disk space. | Weekly |
| License Usage | Review daily license consumption. | Daily |
| Errors and Warnings | Investigate system errors and warnings. | Daily |
| System Updates | Update Splunk software and apps. | Quarterly |

By consistently monitoring these metrics and following maintenance best practices, you can ensure Splunk remains healthy and performs optimally.