Splunk Multiple-Choice Post Quiz Questions (MCQs)

---

1. Splunk Basics (10 Questions)

1.1 What is Splunk primarily used for?
A) Data visualization
B) Log analysis and monitoring
C) Software development
D) Network security

Answer: B) Log analysis and monitoring

1.2 Which Splunk component is responsible for collecting and forwarding data?
A) Search Head
B) Indexer
C) Forwarder
D) Deployment Server

Answer: C) Forwarder

1.3 What is the primary function of an Indexer in Splunk?
A) Searching data
B) Parsing and storing data
C) Managing dashboards
D) Forwarding data

Answer: B) Parsing and storing data

1.4 What type of data does Splunk process?
A) Structured data only
B) Unstructured data only
C) Both structured and unstructured data
D) Only real-time data

Answer: C) Both structured and unstructured data

1.5 What is the default Splunk web interface port?
A) 8080
B) 443
C) 8000
D) 9999

Answer: C) 8000

1.6 What command is used to stop Splunk?
A) splunk shutdown
B) splunk stop
C) service splunk stop
D) splunk terminate

Answer: B) splunk stop

1.7 Splunk Free allows a maximum of how much data per day?
A) 500 MB
B) 1 GB
C) 5 GB
D) Unlimited

Answer: A) 500 MB

1.8 What are Splunk indexes used for?
A) Storing and retrieving event data
B) Generating dashboards
C) Configuring Splunk settings
D) Managing forwarders

Answer: A) Storing and retrieving event data

1.9 Which file is used to configure data inputs in Splunk?
A) inputs.conf
B) indexes.conf
C) server.conf
D) props.conf

Answer: A) inputs.conf

1.10 Splunk can ingest data from which of the following sources?
A) Syslog
B) JSON logs
C) Windows Event Logs
D) All of the above

Answer: D) All of the above

---

2. Splunk SPL Query (10 Questions)

2.1 What does SPL stand for in Splunk?
A) System Processing Language
B) Search Processing Language

C) Splunk Programming Language
D) Script Processing Language

Answer: B) Search Processing Language

2.2 Which command is used to filter data in Splunk searches?
A) table
B) stats
C) search
D) where

Answer: C) search

2.3 How do you rename a field in Splunk SPL?
A) rename fieldX AS fieldY
B) rename fieldY AS fieldX
C) set fieldX = fieldY
D) replace fieldX WITH fieldY

Answer: A) rename fieldX AS fieldY

2.4 Which SPL command is used to count occurrences of a field?
A) table
B) count
C) stats count
D) eval

Answer: C) stats count

2.5 What does the "| top 5 user" command do?
A) Displays the top 5 most frequent users
B) Shows the first 5 occurrences of "user"
C) Sorts users in descending order
D) Returns 5 random users

Answer: A) Displays the top 5 most frequent users

2.6 What is the purpose of the "rex" command?
A) Extract fields using regex
B) Replace field values
C) Count field values
D) Remove duplicate values

Answer: A) Extract fields using regex

2.7 What does the "| dedup host" command do?
A) Removes duplicate host values
B) Sorts hosts alphabetically
C) Filters host events
D) Counts unique hosts

Answer: A) Removes duplicate host values

2.8 Which function is used in SPL to calculate the sum of a field?
A) stats sum(field)
B) eval sum(field)
C) sum(field)
D) aggregate sum(field)

Answer: A) stats sum(field)

2.9 What is the use of "| fields -" in an SPL query?
A) Include specific fields
B) Exclude specific fields
C) Filter results
D) Sort fields

Answer: B) Exclude specific fields

2.10 What command would you use to display event timestamps in human-readable format?
A) strftime()
B) timechart
C) convert
D) eval

Answer: C) convert

3. Splunk Knowledge Objects

3.1 What are Knowledge Objects in Splunk?
A) Data inputs
B) Configurations that enrich searches
C) Machine learning models
D) Internal logs

Answer: B) Configurations that enrich searches

3.2 Which Knowledge Object is used to categorize event data?
A) Tags
B) Lookups
C) Event Types
D) Macros

Answer: C) Event Types

3.3 What is the purpose of a lookup table in Splunk?
A) Store user credentials
B) Map event data to external data sources
C) Backup indexed data
D) Monitor user sessions

Answer: B) Map event data to external data sources

---

4. Splunk Dashboards

4.1 What is a Splunk Dashboard?
A) A graphical representation of logs
B) A script execution panel
C) A command-line interface
D) A configuration file

Answer: A) A graphical representation of logs

4.2 What is the purpose of a Splunk Panel?
A) To visualize search results
B) To store raw logs
C) To index data
D) To monitor Splunk servers

Answer: A) To visualize search results

---

5. Splunk Advanced Questions

5.1 What is the difference between a Splunk Summary Index and a Normal Index?
A) A summary index stores summarized data, reducing search time
B) A normal index stores raw events only
C) Both store data the same way
D) A summary index cannot be queried

Answer: A) A summary index stores summarized data, reducing search time

---

5.2 What is the role of the Deployment Server in Splunk?

A) It manages distributed Splunk deployments
B) It stores configuration files
C) It indexes logs
D) It searches across multiple indexes

Answer: A) It manages distributed Splunk deployments
