Splunk POST Quiz Questionnaire

Splunk Certified Core Power User Certification - MCQs

1. What is Splunk primarily used for?
A) Database Management
B) Log Analysis and Monitoring ✅
C) Cloud Computing
D) Image Processing

2. Which of the following is NOT a valid search mode in Splunk?
A) Fast Mode
B) Smart Mode
C) Slow Mode ✅
D) Verbose Mode

3. Which command is used to extract fields from raw event data?
A) extract ✅
B) eval
C) search
D) stats

4. What is the default time range for a Splunk search?
A) Last 24 hours ✅
B) Last 7 days
C) Last 60 minutes
D) Last 30 days

5. What does the 'stats' command do in Splunk?
A) Computes statistical summaries ✅
B) Filters data
C) Extracts fields
D) Sorts events

6. In Splunk, what is the purpose of the 'rex' command?
A) Extract fields using regular expressions ✅
B) Format time values
C) Convert logs to JSON
D) Create summary indexes

7. What is a Splunk sourcetype?
A) The name of the index
B) The format of the incoming data ✅
C) A field that identifies an event
D) A type of dashboard panel

8. Which search command is used to group events into transactions?
A) stats
B) transaction ✅
C) table
D) dedup

9. What is the primary function of Splunk indexer?
A) Store and retrieve indexed data ✅
B) Generate reports
C) Forward events to another system
D) Manage user authentication

10. Which command removes duplicate events from search results?
A) dedup ✅
B) sort
C) unique
D) eval

11. Which of the following is NOT a valid time modifier in Splunk?
A) earliest
B) latest
C) timespan ✅
D) before

12. What does the 'eval' command do?
A) Assigns values to a field using expressions ✅
B) Filters out null values
C) Displays raw log data
D) Converts logs into a table

13. Which field contains the index time of an event?
A) _index
B) _indextime ✅

C) _time
D) _raw

14. What is the purpose of a lookup table in Splunk?
A) Store additional data to enrich search results ✅
B) Store indexes
C) Create scheduled reports
D) Monitor system logs

15. Which of the following is NOT an option in the 'stats' command?
A) count
B) avg
C) min
D) exclude ✅

16. How can you schedule a report in Splunk?
A) Using the "Save As" option ✅
B) Using the "eval" command
C) Using the "table" command
D) By modifying the event logs

17. What is a Splunk Knowledge Object?
A) Any saved search, report, or field extraction ✅
B) A type of dashboard
C) A user-defined alert
D) A monitoring agent

18. What does the 'timechart' command do?
A) Displays time-series data in a chart ✅
B) Filters data
C) Joins different data sources
D) Converts timestamps

19. What is the function of Splunk forwarder?
A) Collects and forwards data to Splunk indexer ✅
B) Queries data from indexes
C) Manages dashboards
D) Monitors Splunk performance

20. What is the purpose of event sampling in Splunk?
A) Reduce data volume for faster searches ✅

B) Remove duplicates
C) Encrypt log files
D) Create index partitions

21. What is the role of Splunk Deployment Server?

A) Manages configuration of Splunk forwarders ✅
B) Stores index data
C) Runs searches
D) Generates reports

22. Which of the following is an example of a Boolean operator in Splunk?

A) AND ✅
B) MATCH
C) FILTER
D) EXTRACT

23. How do you exclude specific events from search results?

A) Using NOT in the search ✅
B) Using the filter command
C) Using the ignore command
D) Using the drop command

24. What is an accelerated data model in Splunk?

A) Pre-calculated summaries for faster search performance ✅
B) A method for real-time indexing
C) A type of alert
D) A dashboard panel

25. What does the 'fillnull' command do?

A) Replaces NULL values with a specified value ✅
B) Removes NULL values
C) Filters out empty events
D) Converts NULL values to zero

26. What is a Splunk macro?

A) A reusable search expression ✅
B) A special dashboard
C) A report scheduler
D) A log management feature

27. What is the function of the 'spath' command?

A) Extracts fields from JSON and XML data ✅

B) Sorts data

C) Converts timestamps

D) Joins multiple events

28. How can you combine multiple search results in Splunk?

A) Using the append command ✅

B) Using the merge command

C) Using the stats command

D) Using the rex command

29. Which component is responsible for storing indexed data in Splunk?

A) Indexer ✅

B) Search Head

C) Forwarder

D) Deployment Server

30. Which of the following Splunk roles has full administrative privileges?

A) Admin ✅

B) Power User

C) User

D) Auditor