Splunk Certified Power User - Pretest MCQs

1. What is Splunk primarily used for?
A) Database management
B) Log analysis and monitoring
C) Cloud computing
D) Web development

Answer: B) Log analysis and monitoring

---

2. Which of the following is NOT a default Splunk role?
A) Admin
B) User
C) Developer
D) Power User

Answer: C) Developer

---

3. What is the primary purpose of the index in Splunk?
A) Store and retrieve event data
B) Control user access
C) Generate reports
D) Convert data into JSON format

Answer: A) Store and retrieve event data

---

4. Which command is used to filter results based on field values?
A) eval
B) where
C) stats
D) table

Answer: B) where

---

5. What does the timechart command do?
A) Creates a statistical summary of data over time
B) Converts timestamps to readable formats
C) Displays event logs in chronological order
D) Joins two different indexes

Answer: A) Creates a statistical summary of data over time

---

6. Which function is used to extract fields from raw event data?
A) rex
B) eval
C) timechart
D) join

Answer: A) rex

---

7. What is the default retention period for the main index in Splunk?
A) 7 days
B) 30 days
C) 90 days
D) 365 days

Answer: C) 90 days

---

8. What type of search does Splunk use to find specific terms in raw event data?
A) Boolean search
B) Wildcard search
C) Keyword search
D) Index search

Answer: C) Keyword search

---

9. Which command is used to group results by a field and apply aggregate functions?
A) stats
B) table
C) sort
D) eval

Answer: A) stats

---

10. What does the dedup command do in Splunk?
A) Removes duplicate events based on specified fields
B) Sorts events in ascending order
C) Merges multiple searches into one
D) Converts timestamps into human-readable format

Answer: A) Removes duplicate events based on specified fields

---

11. What is the purpose of the eval command?
A) Evaluate mathematical expressions and create new fields
B) Merge two datasets

C) Delete specific fields from events
D) Convert time formats

Answer: A) Evaluate mathematical expressions and create new fields

---

12. Which Splunk role has full administrative privileges?
A) Power User
B) Admin
C) User
D) Developer

Answer: B) Admin

---

13. How can you create a new field in Splunk?
A) Using the eval command
B) Using the stats command
C) Editing the Splunk configuration files
D) Running a join command

Answer: A) Using the eval command

---

14. What does the transaction command do?
A) Combines multiple events into a single event based on a field
B) Merges two different indexes
C) Deletes events from the index
D) Runs a background process

Answer: A) Combines multiple events into a single event based on a field

---

15. In which order does Splunk process search commands?
A) From left to right
B) From right to left
C) Based on command priority
D) In alphabetical order

Answer: A) From left to right

---

16. What is the purpose of the lookup command?
A) Retrieve additional field values from a lookup table
B) Join two different indexes
C) Filter out unwanted events
D) Sort events in descending order

Answer: A) Retrieve additional field values from a lookup table

17. How do you convert a string field to an integer in Splunk?
A) convert num(fieldname)
B) eval fieldname = tostring(fieldname)
C) timechart fieldname
D) stats count(fieldname)

Answer: A) convert num(fieldname)

18. What is the purpose of props.conf in Splunk?
A) Define how data is parsed and indexed
B) Control user permissions
C) Store lookup tables
D) Define dashboard layouts

Answer: A) Define how data is parsed and indexed

19. Which Splunk feature allows users to create reports with visualizations?
A) Data Models
B) Pivot
C) Alerts
D) Indexing

Answer: B) Pivot

20. What is the purpose of an accelerated data model?
A) Improve search performance on large datasets
B) Store indexed data permanently
C) Convert raw data into logs
D) Remove duplicate records

Answer: A) Improve search performance on large datasets