Scenario-Based Multiple Choice Questions (MCQs) on Splunk Queries

1. Identifying Failed Logins

You need to find failed login attempts in Splunk logs for a specific user named john_doe. Which query should you use?

A) index=security sourcetype=auth "john_doe" status="success"
B) index=security sourcetype=auth user="john_doe" status="failed"
C) index=security sourcetype=auth user="john_doe" | stats count by status
D) index=security sourcetype=auth status="failed" | stats count by user

Answer: B

---

2. Extracting IP Addresses

Which query extracts IP addresses using regex?

A) index=web_logs | rex field=_raw "(?P<ip>\d+\.\d+\.\d+\.\d+)"
B) index=web_logs | extract field=ip pattern="\d+\.\d+\.\d+\.\d+"
C) index=web_logs | regex ip="\d+\.\d+\.\d+\.\d+"
D) index=web_logs | fields ip

Answer: A

---

3. Filtering Specific Error Codes

You want to find all occurrences of HTTP 500 errors. Which query is correct?

A) index=web_logs status="500"
B) index=web_logs | where status==500
C) index=web_logs | search status=500
D) index=web_logs | where status=500

Answer: C

---

4. Counting Events per Host

Which query provides the number of events per host?

A) index=system_logs | stats count by host
B) index=system_logs | timechart count by host
C) index=system_logs | chart count by host
D) index=system_logs | count host

Answer: A

---

5. Identifying the Top 5 Hosts with Most Errors

How can you find the top 5 hosts generating error logs?

A) index=logs error | stats count by host | sort -count | head 5
B) index=logs error | top limit=5 host
C) index=logs error | rare limit=5 host
D) index=logs error | chart count by host limit=5

Answer: B

---

6. Finding Unique Users

Which query returns a list of unique users from the logs?

A) index=auth_logs | unique user
B) index=auth_logs | dedup user
C) index=auth_logs | stats distinct_count(user)
D) index=auth_logs | stats count(user)

Answer: C

---

7. Formatting Timestamps

How do you convert _time to a readable format?

A) index=logs | eval time=strftime(_time, "%Y-%m-%d %H:%M:%S")
B) index=logs | convert timeformat="%Y-%m-%d %H:%M:%S" _time
C) index=logs | format_time(_time, "%Y-%m-%d %H:%M:%S")
D) index=logs | timechart format="%Y-%m-%d %H:%M:%S"

Answer: A

---

8. Calculating Average Response Time

Which query calculates the average response time?

A) index=web_logs | stats avg(response_time)
B) index=web_logs | chart mean(response_time)
C) index=web_logs | timechart avg(response_time)
D) All of the above

Answer: D

---

9. Merging Two Fields

You want to create a new field full_name by combining first_name and last_name. What is the correct query?

A) index=users | eval full_name=first_name+last_name
B) index=users | eval full_name=first_name." ".last_name
C) index=users | eval full_name=first_name." ".last_name | table full_name
D) index=users | merge first_name last_name into full_name

Answer: C

---

10. Identifying the Slowest Query

Which query helps find the slowest queries?

A) index=database_logs | stats max(query_time) by query
B) index=database_logs | chart max(query_time) by query
C) index=database_logs | sort -query_time | table query, query_time
D) All of the above

Answer: D

---

11. Calculating Percentage of Errors

How do you calculate the percentage of errors in logs?

A) index=logs | eventstats count as total | where status="error" | eval percentage=(count/total)*100
B) index=logs | stats count as total, count(eval(status="error")) as error_count | eval error_pct=(error_count/total)*100
C) index=logs | where status="error" | stats percent(count)
D) index=logs | eval error_rate=(count(eval(status="error"))/count)*100

Answer: B

---

12. Extracting a Specific Field

How do you extract a custom field from raw logs?

A) index=logs | rex field=_raw "(?P<field_name>\w+)"
B) index=logs | extract field=field_name
C) index=logs | define field=field_name
D) index=logs | regex extract=field_name

Answer: A

---

13. Searching Last 30 Minutes of Logs

Which command retrieves logs from the last 30 minutes?

A) index=logs earliest=-30m latest=now
B) index=logs | timewindow -30m
C) index=logs | where time>-30m
D) index=logs since -30m

Answer: A

---

14. Finding IPs Generating the Most Requests

Which query shows the top 10 IPs making requests?

A) index=web_logs | top limit=10 ip
B) index=web_logs | stats count by ip | sort -count | head 10
C) index=web_logs | rare limit=10 ip
D) Both A and B

Answer: D

---

15. Identifying Anomalous Activity

Which function helps detect anomalies?

A) index=security | anomaly_detection user
B) index=security | stats count by user | anomalydetect
C) index=security | anomalydetection
D) index=security | anomalydetection

Answer: B

---

16. Parsing JSON Logs

How do you extract fields from JSON logs?

A) index=json_logs | spath
B) index=json_logs | json extract
C) index=json_logs | parse json
D) index=json_logs | extract fields=json

Answer: A

---

17. Converting String to Number

Which function converts a string field to a number?

A) index=logs | convert num(field)
B) index=logs | eval field=tonumber(field)
C) index=logs | cast field as number
D) index=logs | eval field=toint(field)

Answer: A

---

18. Renaming a Field

How do you rename the field old_name to new_name?

A) index=logs | rename old_name as new_name
B) index=logs | replace old_name with new_name
C) index=logs | change old_name to new_name
D) index=logs | eval new_name=old_name

Answer: A

---

19. Finding Logs for Specific Dates

Which query retrieves logs from Feb 1 to Feb 5, 2025?

A) index=logs earliest="02/01/2025" latest="02/05/2025"
B) index=logs earliest=2025-02-01 latest=2025-02-05
C) index=logs range 2025-02-01 to 2025-02-05
D) index=logs date>=2025-02-01 AND date<=2025-02-05

Answer: B

---

20. Removing Duplicates

Which command removes duplicate results?

A) index=logs | dedup field
B) index=logs | unique field
C) index=logs | distinct field
D) index=logs | filter distinct field

Answer: A