1001_M4_Using_Fields_In_Searches_Quiz

1. What search string returns only events from the host WWW3?
   A. host=*
   [✓ B.] host=WWW3
   C. host=WWW*
   D. Host=WWW3

2. Which search query would return events containing “failure” in the netfw index or “warn” or “critical” in the netops index?
   A. (index=netfw failure) AND index=netops warn OR critical
   [✓ B.] (index=netfw failure) OR (index=netops (warn OR critical))
   C. (index=netfw failure) AND (index=netops (warn OR critical))
   D. (index=netfw failure) OR index=netops OR (warn OR critical))

3. Which of the following represents a Splunk search best practice?
   [✓ A.] Filter as early as possible
   B. Always specify exactly one index
   C. Limit the number of search teams to improve performance
   D. Use wildcards to return more search results.

4. By default, which field is displayed in the sidebar under Interesting Fields?
   A. host
   [✓ B.] index
   C. source
   D. sourcetype

5. Which statement about case sensitivity in Splunk is correct?
   A. Both field names and field values ARE case sensitive.
   [✓ B.] Field names ARE case sensitive; field values are NOT.
   C. Field values are case sensitive; field names are NOT.
   D. Both field names and field values ARE NOT case sensitive.

6. If a field exists in the search results but is not shown in the fields sidebar, how can you add it?
   [✓ A.] Click All Fields and select the field to add it to Selected Fields.
   B. Click interesting Fields and select the field to add it to Selected Fields.
   C. Click selected Fields and select the field to add it to Interesting Fields.

D. This scenario isn’t possible because all fields returned from a search always appear in the fields sidebar.

7. In the fields sidebar, which character identifies alphanumeric field values?

A. #
B. %
[✓ C.] ɑ
D. $

8. What syntax is used to connect key/value pairs in a search string?

A. action+purchase
[✓ B.] action=purchase
C. action | purchase
D. action equal purchase

9. Which of the following is the most efficient way to filter searches in Splunk?

[✓ A.] Time
B. Smart mode
C. Sourcetype
D. Selected Fields

10. How does Splunk decide which fields to extract from incoming data?

A. Splunk only extracts the most important fields based on data type
B. Splunk only extracts fields at index time
C. Splunk automatically extracts any fields that generate interesting visualizations
[✓ D.] Splunk automatically discovers many fields based on sourcetype and key/value pairs found in the data

11. What syntax is required to link key/value pairs in search strings?

A. Square brackets
B. @ or # symbols
C. Quotation marks
[✓ D.] Relational operators such as =, <, or >

12. Which search query retrieves events from the “access_combined” sourcetype?

A. Sourcetype=access_combined
B. Sourcetype=Access_Combined

- [✓ C.] sourcetype=Access_Combined
- D. SOURCETYPE=access_combined

13. Among the following, which index search delivers the best performance efficiency?
    - A. index=*
    - B. index=security OR index=w*
    - [✓ C.] (index=security OR index=web)
    - D. *index=sales AND index=web*

14. In the fields sidebar, what indicates that a field contains numeric values?
    - A. A number to the right of the field name.
    - [✓ B.] A # symbol to the left of the field name.
    - C. A lowercase n to the left of the field name.
    - D. A lowercase n to the right of the field name.

15. At index time, in which field does Splunk store the timestamp?
    - A. time
    - [✓ B.] _time
    - C. EventTime
    - D. Timestamp

16. Which events are returned by this search string: “host=www3 status=400”?
    - A. All events that either have a host of www3 or a status of 400.
    - [✓ B.] All events with a host of www3 that also have a status of 400.
    - C. We need more information; we cannot tell without knowing the time range.
    - D. We need more information; a search cannot be run without specifying an index.