Splunk Core Certified User

1. What is the correct syntax to count the number of events containing a vendor_action field?

A. count stats vendor_action

B. count stats (vendor_action)

C. stats count (vendor_action)

D. stats vendor_action (count)

Answer(s): C

---

2. By default, which of the following fields would be listed in the fields sidebar under interesting Fields?

A. host

B. index

C. source

D. sourcetype

Answer(s): D

---

3. When looking at a dashboard panel that is based on a report, which of the following is true?

A. You can modify the search string in the panel, and you can change and configure the visualization.

B. You can modify the search string in the panel, but you cannot change and configure the visualization.

C. You cannot modify the search string in the panel, but you can change and configure the visualization.

D. You cannot modify the search string in the panel, and you cannot change and configure the visualization.

Answer(s): C

---

4. Which of the following is a best practice when writing a search string?

A. Include all formatting commands before any search terms

B. Include at least one function as this is a search requirement

C. Include the search terms at the beginning of the search string

D. Avoid using formatting clauses as they add too much overhead

Answer(s): C

---

5. What type of search can be saved as a report?

A. Any search can be saved as a report

B. Only searches that generate visualizations

C. Only searches containing a transforming command

D. Only searches that generate statistics or visualizations

Answer(s): D

---

6. What can be included in the All Fields option in the sidebar?

A. Dashboards

B. Metadata only

C. Non-interesting fields

D. Field descriptions

Answer(s): C

---

7. What syntax is used to link key/value pairs in search strings?

A. action+purchase

B. action=purchase

C. action | purchase

D. action equal purchase

Answer(s): B

---

8. When viewing the results of a search, what is an Interesting Field?

A. A field that appears in any event

B. A field that appears in every event

C. A field that appears in the top 10 events

D. A field that appears in at least 20% of the events

Answer(s): D

---

9. When a Splunk search generates calculated data that appears in the Statistics tab. in what formats can the results be exported?

A. CSV, JSON, PDF

B. CSV, XML JSON

C. Raw Events, XML, JSON

D. Raw Events, CSV, XML, JSON

Answer(s): D

---

10. Which of the following are functions of the stats command?

A. count, sum, add

B. count, sum, less

C. sum, avg, values

D. sum, values, table

Answer(s): C

---

11. In a deployment with multiple indexes, what will happen when a search is run and an index is not specified in the search string?

A. No events will be returned.

B. Splunk will prompt you to specify an index.

C. All non-indexed events to which the user has access will be returned.

D. Events from every index searched by default to which the user has access will be returned.

Answer(s): D

---

12. Which search matches the events containing the terms "error" and "fail"?

A. index=security Error Fail

B. index=security error OR fail

C. index=security "error failure"

D. index=security NOT error NOT fail

Answer(s): A

---

13. Which of the following is an option after clicking an item in search results?

A. Saving the item to a report

B. Adding the item to the search.

C. Adding the item to a dashboard

D. Saving the search to a JSON file.

Answer(s): A

---

14. When placed early in a search, which command is most effective at reducing search execution time?

A. dedup

B. rename

C. sort -

D. fields +

Answer(s): A

---

15. In the Splunk interface, the list of alerts can be filtered based on which characteristics?

A. App, Owner, Severity, and Type

B. App, Owner, Priority, and Status

C. App, Dashboard, Severity, and Type

D. App, Time Window, Type, and Severity

Answer(s): D

---

16. When displaying results of a search, which of the following is true about line charts?

A. Line charts are optimal for single and multiple series.

B. Line charts are optimal for single series when using Fast mode.

C. Line charts are optimal for multiple series with 3 or more columns.

D. Line charts are optimal for multiseries searches with at least 2 or more columns.

Answer(s): C

---

17. A collection of items containing things such as data inputs, UI elements, and knowledge objects is known as what?

A. An app

B. JSON

C. A role

D. An enhanced solution

Answer(s): A

---

18. Which of the following fields is stored with the events in the index?

A. user

B. source

C. location

D. sourcelp

Answer(s): B

---

19. Which of the following is the recommended way to create multiple dashboards displaying data from the same search?

A. Save the search as a report and use it in multiple dashboards as needed

B. Save the search as a dashboard panel for each dashboard that needs the data

C. Save the search as a scheduled alert and use it in multiple dashboards as needed

D. Export the results of the search to an XML file and use the file as the basis of the dashboards

Answer(s): A

---

20. What must be done in order to use a lookup table in Splunk?

A. The lookup must be configured to run automatically.

B. The contents of the lookup file must be copied and pasted into the search bar.

C. The lookup file must be uploaded to Splunk and a lookup definition must be created.

D. The lookup file must be uploaded to the etc/apps/lookups folder for automatic ingestion.

Answer(s): C
