EndExam

QUESTION & ANSWER

Accurate study guides, High passing rate!

We offer free update service for one year!

http://www.endexam.com

Exam : SPLK-1001

Title : Splunk Core Certified User

Version : DEMO

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: C
Explanation:
The stats command calculates statistics based on fields in the events. The count function counts the number of events that match the criteria. The syntax is stats count (field_name), where field_name is the name of the field that contains the value to be counted. In this case, vendor_action is the field name, so stats count (vendor_action) is the correct syntax.
Reference: Splunk Core User Certification Exam Study Guide, page 23.

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: D
Explanation:
The fields sidebar in Splunk shows the default fields and the interesting fields for the events that match your search. The default fields are host, source, and sourcetype, which are extracted for every event at index time. The interesting fields are fields that appear in at least 20% of the events in your search results. You can also select additional fields to display in the fields sidebar1.
By default, the index field is not listed in the fields sidebar, because it is not a default field nor an interesting field. The index field is a metadata field that indicates which index the event belongs to. Metadata fields are not extracted from the event data, but are added by the indexer as part of the indexing process. Metadata fields are not shown in the fields sidebar, but you can use them in your search queries2.
Therefore, among the four options, only sourcetype would be listed in the fields sidebar under interesting fields by default.
Reference
Use fields to search
About default fields

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: C
Explanation:
When looking at a dashboard panel that is based on a report, you cannot modify the search string in the

panel, but you can change and configure the visualization. This is because the dashboard panel inherits the search string from the report, and any changes to the search string will affect the report as well. However, you can customize the visualization settings for the dashboard panel without affecting the report.
Reference: Splunk Core User Certification Exam Study Guide, page 37.

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: C
Explanation:
A best practice when writing a search string is to include the search terms at the beginning of the search string. This helps Splunk narrow down the events that match your search criteria and improve the search performance. Formatting commands and functions can be added later in the search pipeline to manipulate and display the results.
Reference: Splunk Core User Certification Exam Study Guide, page 13.

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: D
Explanation:
Only searches that generate statistics or visualizations can be saved as a report. These are searches that contain a transforming command, such as stats, chart, timechart, top, rare, etc. Transforming commands create a data table from the events and enable various types of visualizations. Searches that do not contain a transforming command can only be saved as an alert or a dashboard panel.
Reference: Splunk Core User Certification Exam Study Guide, page 35.