Prepare Important Exam with SPLK-1002 Exam Dumps(2022) [Q41-Q56

Prepare Important Exam with SPLK-1002 Exam Dumps(2022)
Pass Exam Questions Efficiently With SPLK-1002 Questions

NEW QUESTION 41

When using a field value variable with a Workflow Action, which punctuation mark will escape the data
* *
* !
*
* #

NEW QUESTION 42

Which of the following searches would return a report of sales by product-name?
* chart sales by product_name
* chart sum(price) as sales by product_name
* stats sum(price) as sales over product_name
* timechart list(sales), values(product_name)

NEW QUESTION 43

The limit attribute will_____.
* override default of 10
* only work with top command
* override default of 20
* override default of 15

NEW QUESTION 44

When creating a Search workflow action, which field is required?
* Search string
* Data model name
* Permission setting
* An eval statement

Reference:https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Setupasearchworkflowaction

NEW QUESTION 45

What does the fillnull command replace null values with, if the value argument is not specified?
* 0
* N/A
* NaN
* NULL

NEW QUESTION 46

Which of the following statements describe data model acceleration? (select all that apply)
* Root events cannot be accelerated.
* Accelerated data models cannot be edited.
* Private data models cannot be accelerated.
* You must have administrative permissions or the accelerate_dacamodel capability to accelerate a data model.

NEW QUESTION 47

When using timechart, how many fields can be listed after a byclause?
* 0, because timechart doesn’t support using a by clause.
* 1, because _time is already implied as the x-axis.
* 2, because one field would represent the x-axis and the other would represent the y-axis.
* There is no limit specific to timechart.

NEW QUESTION 48

When multiple event types with different color values are assigned to the same event, what determines the color displayed for the event?
* Rank
* Weight
* Priority
* Precedence

Explanation/Reference: https://docs.splunk.com/Documentation/SplunkCloud/8.0.2003/Knowledge/Defineeventtypes

NEW QUESTION 49

The following searches will return the same results. SEARCH 1: ssh error SEARCH 2: ssh AND error
* True
* False

NEW QUESTION 50

In which Settings section are macros defined?
* Fields
* Tokens
* Advanced Search
* Searches, Reports, Alerts

NEW QUESTION 51

What does the fillnull command replace null values with, it the value argument is not specified?
* 0
* N/A
* NaN
* NULL

Reference:

https://answers.splunk.com/answers/653427/fillnull-doesnt-work-without-specfying-a-field.html

NEW QUESTION 52

Which of the following statements describes macros?
* A macro is a reusable search string that must contain the full search.
* A macro is a reusable search string that must have a fixed time range.
* A macro Is a reusable search string that may have a flexible time range.
* A macro Is a reusable search string that must contain only a portion of the search.

NEW QUESTION 53

Which of the following search control will not re-rerun the search? (Select all that apply.)
* zoom out
* selecting a bar on the timeline
* deselect
* selecting a range of bars on the timelines

NEW QUESTION 54

O: 97

which of the following are valid options with the chart command
* useother
* usenull

* fillfield
* usefiled

NEW QUESTION 55

This clause is used to group the output of a stats command by a specific name.
* Rex
* As
* List
* By

NEW QUESTION 56

Which of the following knowledge objects represents the output of an oval expression?
* Eval fields
* Calculated fields
* Field extractions
* Calculated lookups

Exam Details **SPLK-1002 has 65 multiple-select and multiple-choice questions that should be answered in 57 minutes, with an addition of 3 minutes that are given one to get familiar with the exam agreement. Taking this test will cost $ The applicants will be rated on a variety of knowledge areas, such as the following:** - Macros- CIM- Correlating events- Tags as well as event types- Workflow actions- Filtering as well as formatting of results- Data models
Candidates are advised to take the training courses provided by the vendor when preparing for SPLK-1002 exam. To succeed on the first attempt, they should tackle all the lectures, hands-on sessions, and practice questions to ensure they are adequately ready.

SPLK-1002 Questions - Truly Beneficial For Your Splunk Exam: https://www.validexam.com/SPLK-1002-latest-dumps.html]