

Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

<https://www.2passeasy.com/dumps/SPLK-1002/>



NEW QUESTION 1

- (Exam Topic 1)

Which of the following data model are included In the Splunk Common Information Model (CIM) add-on? (select all that apply)

- A. Alerts
- B. Email
- C. Database
- D. User permissions

Answer: ABC

NEW QUESTION 2

- (Exam Topic 1)

Which of the following statements describes field aliases?

- A. Field alias names replace the original field name.
- B. Field aliases can be used in lookup file definitions.
- C. Field aliases only normalize data across sources and sourcetypes.
- D. Field alias names are not case sensitive when used as part of a search.

Answer: A

NEW QUESTION 3

- (Exam Topic 1)

Which of the following searches will return events contains a tag name Privileged?

- A. Tag= Priv
- B. Tag= Priv*
- C. Tag= Priv*
- D. Tag= Privileged

Answer: D

NEW QUESTION 4

- (Exam Topic 1)

Data model are composed of one or more of which of the fo-owing datasets? (select all that apply.)

- A. Events datasets
- B. Search datasets
- C. Transaction datasets
- D. Any child of event, transaction, and search datasets

Answer: ABC

NEW QUESTION 5

- (Exam Topic 1)

Based on the macro definition shown below, what is the correct way to execute the macro in a search string?

- A. Convert_sales (euro, €, 79)"
- B. Convert_sales (euro, €, .79)
- C. Convert_sales (\$euro,\$€\$,s79\$
- D. Convert_sales (\$euro, \$€\$,S,79\$)

Answer: B

NEW QUESTION 6

- (Exam Topic 1)

Which one of the following statements about the search command is true?

- A. It does not allow the use of wildcards.
- B. It treats field values in a case-sensitive manner.
- C. It can only be used at the beginning of the search pipeline.

D. It behaves exactly like search strings before the first pipe.

Answer: C

NEW QUESTION 7

- (Exam Topic 1)

A field alias has been created based on an original field. A search without any transforming commands is then executed in Smart Mode. Which field name appears in the results?

- A. Both will appear in the All Fields list, but only if the alias is specified in the search.
- B. Both will appear in the Interesting Fields list, but only if they appear in at least 20 percent of events.
- C. The original field only appears in All Fields list and the alias only appears in the Interesting Fields list.
- D. The alias only appears in the All Fields list and the original field only appears in the Interesting Fields list.

Answer: B

NEW QUESTION 8

- (Exam Topic 1)

Which of the following can be used with the eval command tostring function (select all that apply)

- A. "hex"
- B. "commas"
- C. "Decimal"
- D. "duration"

Answer: ABD

NEW QUESTION 9

- (Exam Topic 1)

The Field Extractor (FX) is used to extract a custom field. A report can be created using this custom field. The created report can then be shared with other people in the organization. If another person in the organization runs the shared report and no results are returned, why might this be? (select all that apply)

- A. Fast mode is enabled.
- B. The dashboard is private.
- C. The extraction is private
- D. The person in the organization running the report does not have access to the index.

Answer: BD

NEW QUESTION 10

- (Exam Topic 1)

Which of the following are required to create a POST workflow action?

- A. Label, URI, search string.
- B. XMI attributes, URI, name.
- C. Label, URI, post arguments.
- D. URI, search string, time range picker.

Answer: B

NEW QUESTION 10

- (Exam Topic 1)

Data model fields can be added using the Auto-Extracted method. Which of the following statements describe Auto-Extracted fields? (select all that apply)

- A. Auto-Extracted fields can be hidden in Pivot.
- B. Auto-Extracted fields can have their data type changed.
- C. Auto-Extracted fields can be given a friendly name for use in Pivot.
- D. Auto-Extracted fields can be added if they already exist in the dataset with constraints.

Answer: B

NEW QUESTION 14

- (Exam Topic 1)

A calculated field maybe based on which of the following?

- A. Lookup tables
- B. Extracted fields
- C. Regular expressions
- D. Fields generated within a search string

Answer: B

NEW QUESTION 15

- (Exam Topic 2)

The eval command 'if' function requires the following three arguments (in order):

- A. Boolean expression, result if true, result if false
- B. Result if true, result if false, boolean expression
- C. Result if false, result if true, boolean expression
- D. Boolean expression, result if false, result if true

Answer: A

NEW QUESTION 17

- (Exam Topic 2)

By default search results are not returned in _____ order.

- A. Chronological
- B. Reverser chronological
- C. ASCIE
- D. Alphabetical

Answer: AD

NEW QUESTION 19

- (Exam Topic 2)

Using the export function, you can export search results as _____.(Select all that apply)

- A. Xml
- B. Json
- C. Html
- D. A php file

Answer: AB

NEW QUESTION 22

- (Exam Topic 2)

What is a limitation of searches generated by workflow actions?

- A. Searches generated by workflow action cannot use macros.
- B. Searches generated by workflow actions must be less than 256 characters long.
- C. Searches generated by workflow action must run in the same app as the workflow action.
- D. Searches generated by workflow action run with the same permissions as the user running them.

Answer: D

NEW QUESTION 26

- (Exam Topic 2)

Clicking a SEGMENT on a chart, _____.

- A. drills down for that value
- B. highlights the field value across the chart
- C. adds the highlighted value to the search criteria

Answer: C

NEW QUESTION 27

- (Exam Topic 2)

Which search would limit an "alert" tag to the "host" field?

- A. tag=alert
- B. host::tag::alert
- C. tag==alert
- D. tag::host=alert

Answer: D

NEW QUESTION 29

- (Exam Topic 2)

Which is not a comparison operator in Splunk

- A. <=
- B. =
- C. !=
- D. >
- E. ?=

Answer: E

NEW QUESTION 31

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-1002 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-1002 Product From:

<https://www.2passeasy.com/dumps/SPLK-1002/>

Money Back Guarantee

SPLK-1002 Practice Exam Features:

- * SPLK-1002 Questions and Answers Updated Frequently
- * SPLK-1002 Practice Questions Verified by Expert Senior Certified Staff
- * SPLK-1002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SPLK-1002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year