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 is the correct way to use the data model command to search field in the data model within the web dataset?

A. | datamodel web search | filed web *
B. | Search datamodel web web | filed web*
C. | datamodel web web field | search web*
D. Datamodel=web | search web | filed web*

Answer: A

NEW QUESTION 3
- (Exam Topic 1)
Which of the following searches show a valid use of macro? (Select all that apply)

```
index=main source=mySource oldField=* |`makeMyField(oldField)`| table _time newField

index=main source=mySource oldField=* | stats if(`makeMyField(oldField)`) | table _time
newField

index=main source=mySource oldField=* | eval newField=`makeMyField(oldField)`| table _time
newField

index=main source=mySource oldField=* | "`newField(`makeMyField(oldField)`)`" | table _time
newField
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: AC

NEW QUESTION 4
- (Exam Topic 1)
Which of the following statements about event types is true? (select all that apply)

A. Event types can be tagged.
B. Event types must include a time range,
C. Event types categorize events based on a search.
D. Event types can be a useful method for capturing and sharing knowledge.

Answer: AC

NEW QUESTION 5
- (Exam Topic 1)
Which of the following statements describe the search string below?
dacamodel Application_State All_Application_State search

A. Events will be returned from dataset named Application_state.
B. Events will be returned from the data model named Application_State.
C. Events will be returned from the data model named All_Application_state.
D. No events will be returned because the pipe should occur after the datamodel command

Answer: C

NEW QUESTION 6
- (Exam Topic 1)
Which of the following statements is true, especially in large environments?

A. Use the scats command when you next to group events by two or more fields.
B. The stats command is faster and more efficient than the transaction command
C. The transaction command is faster and more efficient than the stats command.
D. Use the transaction command when you want to see the results of a calculation.

Answer: B

NEW QUESTION 7
- (Exam Topic 1)
Which of the following statements describes the command below (select all that apply) sourcetype-access_combined | transaction JSESSIONID

A. An additional filed named maxspan is created.
B. An additional Held named duration is created.
C. An additional field named eventcount is created.
D. Events with the same JSESSIONID will be grouped together into a single event.

Answer: BCD

NEW QUESTION 8
- (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 9
- (Exam Topic 1)
When creating a Search workflow action, which field is required?

A. Search string
B. Data model name
C. Permission setting
D. An eval statement

Answer: A

NEW QUESTION 10
- (Exam Topic 1)
Which of the following statements describes POST workflow actions?

A. POST workflow actions are always encrypted.
B. POST workflow actions cannot use field values in their URI.
C. POST workflow actions cannot be created on custom sourcetypes.
D. POST workflow actions can open a web page in either the same window or a new .

Answer: D

NEW QUESTION 10
- (Exam Topic 1)
Calculated fields can be based on which of the following?

A. Tags
B. Extracted fields
C. Output fields for a lookup
D. Fields generated from a search string

Answer: B

NEW QUESTION 11
- (Exam Topic 1)
Which of the following knowledge objects represents the output of an oval expression?

A. Eval fields
B. Calculated fields
C. Field extractions
D. Calculated lookups

Answer: C

NEW QUESTION 14
- (Exam Topic 1)
What is the correct syntax to search for a tag associated with a value on a specific fields?

A. Tag-<field?
B. Tag<filed(tagname.)
C. Tag=<filed>::<tagname>

D. Tag::<filed>=<tagname>

Answer: D

NEW QUESTION 18
- (Exam Topic 1)
Which of the following statements describes macros?

A. A macro is a reusable search string that must contain the full search.
B. A macro is a reusable search string that must have a fixed time range.
C. A macro Is a reusable search string that may have a flexible time range.
D. A macro Is a reusable search string that must contain only a portion of the search.

Answer: C

NEW QUESTION 22
- (Exam Topic 1)
A user wants to convert field values to string and also to sort on those value. Which command should be used first, the eval or the sort?

A. It doesn't matter whether eval or sort is used first.
B. Convert the numeric to a string with eval first, then sort.
C. Use sort first, then convert the numeric to a string with eval.
D. You cannot use the sort command and the eval command on the same field.

Answer: B

NEW QUESTION 26
- (Exam Topic 1)
To identify all of the contributing events within a transaction that contains at least one REJECT event, which syntax is correct?

A. Index-main | REJECT trans sessionid
B. Index-main | transaction sessionid | search REJECT
C. Index=main | transaction sessionid | whose transaction=reject
D. Index=main | transaction sessionid | where transaction=reject''

Answer: D

NEW QUESTION 28
- (Exam Topic 1)
What do events in a transaction have In common?

A. All events In a transaction must have the same timestamp.
B. All events in a transaction must have the same sourcetype.
C. All events in a transaction must have the exact same set of fields.
D. All events in a transaction must be related by one or more fields.

Answer: B

NEW QUESTION 31
- (Exam Topic 1)
In what order arc the following knowledge objects/configurations applied?

A. Field Aliases, Field Extractions, Lookups
B. Field Extractions, Field Aliases, Lookups
C. Field Extractions, Lookups, Field Aliases
D. Lookups, Field Aliases, Field Extractions

Answer: B

NEW QUESTION 32
- (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 34
- (Exam Topic 1)
A space is an implied _____ in a search string.

A. OR

B. AND
C. ()
D. NOT

Answer: B

NEW QUESTION 39
- (Exam Topic 1)
Which of the following statements describe the search below? (select all that apply) Index=main I transaction clientip host maxspan=30s maxpause=5s

A. Events in the transaction occurred within 5 seconds.
B. It groups events that share the same clientip and host.
C. The first and last events are no more than 5 seconds apart.
D. The first and last events are no more than 30 seconds apart.

Answer: B

NEW QUESTION 43
- (Exam Topic 1)
When using timechart, how many fields can be listed after a by clause? (Choose Two)

A. because timechart doesn't support using a by clause.
B. because _time is already implied as the x-axis.
C. because one field would represent the x-axis and the other would represent the y-axis.
D. There is no limit specific to timechart.

Answer: BD

NEW QUESTION 44
- (Exam Topic 1)
Which of the following statements describe data model acceleration? (select all that apply)

A. Root events cannot be accelerated.
B. Accelerated data models cannot be edited.
C. Private data models cannot be accelerated.
D. You must have administrative permissions or the accelerate_dacamodel capability to accelerate a data model.

Answer: BCD

NEW QUESTION 45
- (Exam Topic 1)
Which delimiters can the Field Extractor (FX) detect? (select all that apply)

A. Tabs
B. Pipes
C. Spaces
D. Commas

Answer: ABCD

NEW QUESTION 47
- (Exam Topic 1)
What does the following search do?

index=corndog type=mysterymeat action=eaten | stats count as corndog_count by user

A. Creates a table of the total count of users and split by corndogs.
B. Creates a table of the total count of mysterymeat corndogs split by user.
C. Creates a table with the count of all types of corndogs eaten split by user.
D. Creates a table that groups the total number of users by vegetarian corndogs.

Answer: A

NEW QUESTION 49
- (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 54
- (Exam Topic 1)
What does the transaction command do?

A. Groups a set of transactions based on time.
B. Creates a single event from a group of events.
C. Separates two events based on one or more values.
D. Returns the number of credit card transactions found in the event logs.

Answer: B

NEW QUESTION 55
- (Exam Topic 2)
which of the following are valid options with the chart command

A. useother
B. usenull
C. fillfield
D. usefiled

Answer: AB

NEW QUESTION 58
- (Exam Topic 2)
This tab shows you the event patterns in the results of a specific search.

A. statistics
B. visualization
C. patterns

Answer: C

NEW QUESTION 61
- (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 66
- (Exam Topic 2)
When using the transaction command, what does the argument maxspan do?

A. Sets the maximum total time between events in a transaction.
B. Sets the maximum length of all events within a transaction.
C. Sets the maximum total time between the earliest and latest events in a transaction.
D. Sets the maximum length that any single event can reach to be included in the transaction.

Answer: B

NEW QUESTION 70
- (Exam Topic 2)
Which of the following statements describes the use of the Filed Extractor (FX)?

A. The Field Extractor automatically extracts all field at search time.
B. The Field Extractor uses PERL to extract field from the raw events.
C. Field extracted using the Extracted persist as knowledge objects.
D. Fields extracted using the Field Extractor do not persist and must be defined for each search.

Answer: C

NEW QUESTION 73
- (Exam Topic 2)
These allow you to categorize events based on search terms. Select your answer.

A. Groups
B. Event Types
C. Macros
D. Tags

Answer: B

NEW QUESTION 78
......

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