



# Splunk

## Exam Questions SPLK-1002

Splunk Core Certified Power User Exam

### 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)

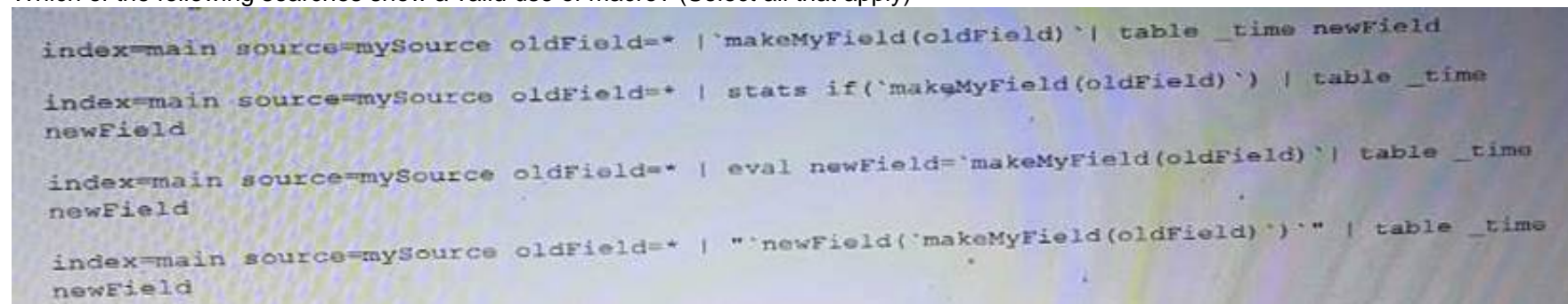
- A. Alerts
- B. Email
- C. Database
- D. User permissions

**Answer:** ABC

### NEW QUESTION 2

- (Exam Topic 1)

Which of the following 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 3

- (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 4

- (Exam Topic 1)

Which of the following statements describe calculated fields? (select all that apply)

- A. Calculated fields can be used in the search bar.
- B. Calculated fields can be based on an extracted field.
- C. Calculated fields can only be applied to host and sourcetype.
- D. Calculated fields are shortcuts for performing calculations using the eval command.

**Answer:** BD

### NEW QUESTION 5

- (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 6

- (Exam Topic 1)

When multiple event types with different color values are assigned to the same event, what determines the color displayed for the events?

- A. Rank
- B. Weight
- C. Priority
- D. Precedence

**Answer:** C

#### NEW QUESTION 7

- (Exam Topic 1)

Which of the following statements describe the Common Information Model (QM)? (select all that apply)

- A. CIM is a methodology for normalizing data.
- B. CIM can correlate data from different sources.
- C. The Knowledge Manager uses the CIM to create knowledge objects.
- D. CIM is an app that can coexist with other apps on a single Splunk deployment.

**Answer:** AC

#### 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)

Which of the following statements describe GET workflow actions?

- A. GET workflow actions must be configured with POST arguments.
- B. Configuration of GET workflow actions includes choosing a sourcetype.
- C. Label names for GET workflow actions must include a field name surrounded by dollar signs.
- D. GET workflow actions can be configured to open the URT link in the current window or in a new window

**Answer:** D

#### NEW QUESTION 10

- (Exam Topic 1)

What is the relationship between data models and pivots?

- A. Data models provide the datasets for pivots.
- B. Pivots and data models have no relationship.
- C. Pivots and data models are the same thing.
- D. Pivots provide the datasets for data models.

**Answer:** D

#### NEW QUESTION 10

- (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 14

- (Exam Topic 1)

Which of the following actions can the eval command perform?

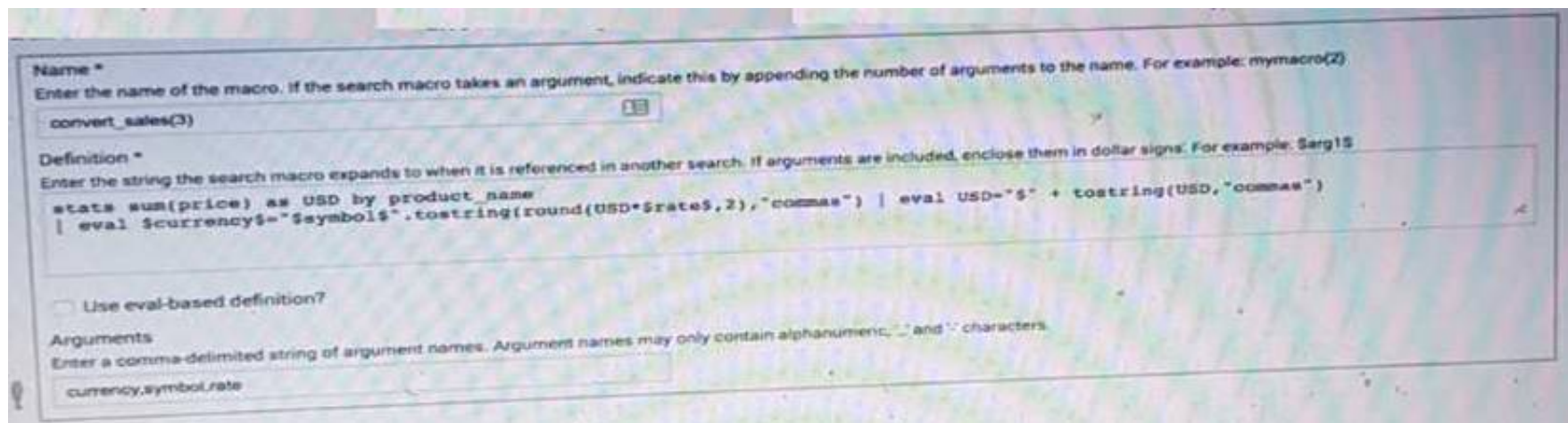
- A. Remove fields from results.
- B. Create or replace an existing field.
- C. Group transactions by one or more fields.
- D. Save SPL commands to be reused in other searches.

**Answer:** B

#### NEW QUESTION 15

- (Exam Topic 1)

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



The screenshot shows the 'Macro Definition' form in Splunk. The 'Name' field is 'convert\_sales(3)'. The 'Definition' field contains the following code: `stats sum(price) as USD by product_name  
| eval $currency$="$symbol$".tostring(round(USD*$rate$,2),"comma") | eval USD="$" + tostring(USD,"comma")`. The 'Arguments' field is 'currency,symbol,rate'. There is a checkbox for 'Use eval-based definition?' which is unchecked.

- 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 16

- (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 21

- (Exam Topic 1)

Which are valid ways to create an event type? (select all that apply)

- A. By using the searchtypes command in the search bar.
- B. By editing the event\_type stanza in the props.conf file.
- C. By going to the Settings menu and clicking Event Types > New.
- D. By selecting an event in search results and clicking Event Actions > Build Event Type.

**Answer:** CD

#### NEW QUESTION 25

- (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 30

- (Exam Topic 1)

Which group of users would most likely use pivots?

- A. Users
- B. Architects
- C. Administrators
- D. Knowledge Managers

**Answer:** D

#### NEW QUESTION 35

- (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 39

- (Exam Topic 1)

Which of the following statements describes Search workflow actions?

- A. By default
- B. Search workflow actions will run as a real-time search.
- C. Search workflow actions can be configured as scheduled searches,
- D. The user can define the time range of the search when created the workflow action.
- E. Search workflow actions cannot be configured with a search string that includes the transaction command

**Answer:** C

#### 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 46

- (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 51

- (Exam Topic 2)

Which workflow uses field values to perform a secondary search?

- A. POST
- B. Action
- C. Search
- D. Sub-Search

**Answer:** C

#### Explanation:

<https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/CreateworkflowactionsinSplunkWeb>

#### NEW QUESTION 52

- (Exam Topic 2)

Which of the following search modes automatically returns all extracted fields in the fields sidebar?

- A. Fast
- B. Smart
- C. Verbose

**Answer:** C

#### NEW QUESTION 55

- (Exam Topic 2)

Splunk alerts can be based on search that run \_\_\_\_\_. (Select all that apply.)

- A. in real-time
- B. on a regular schedule
- C. and have no matching events

**Answer:** AB

#### NEW QUESTION 60

- (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 61

- (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 62

- (Exam Topic 2)

Which is not a comparison operator in Splunk

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

**Answer:** E

#### NEW QUESTION 65

- (Exam Topic 2)

What will you learn from the results of the following search? sourcetype=cisco\_esa | transaction mid, dcid, icid | timechart avg(duration)

- A. The average time elapsed during each transaction for all transactions
- B. The average time for each event within each transaction
- C. The average time between each transaction

**Answer:** A

#### NEW QUESTION 67

.....



## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

### 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)

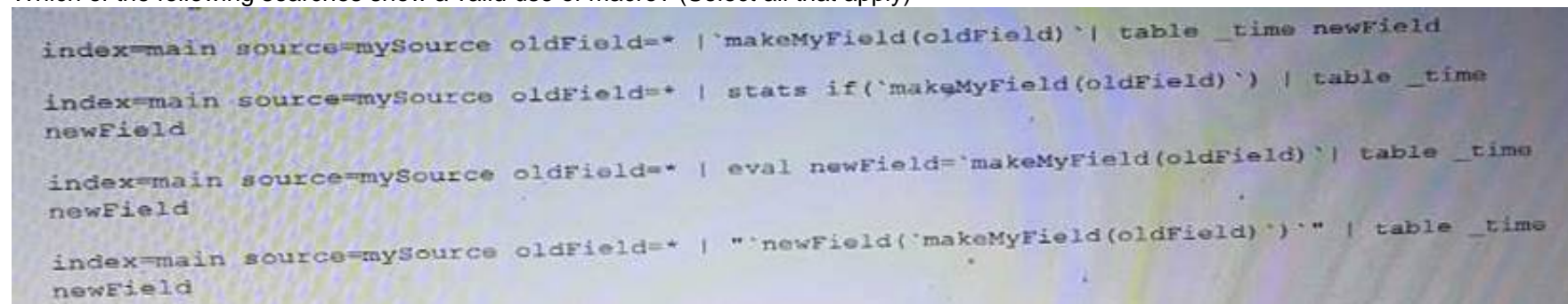
- A. Alerts
- B. Email
- C. Database
- D. User permissions

**Answer:** ABC

### NEW QUESTION 2

- (Exam Topic 1)

Which of the following 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 3

- (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 4

- (Exam Topic 1)

Which of the following statements describe calculated fields? (select all that apply)

- A. Calculated fields can be used in the search bar.
- B. Calculated fields can be based on an extracted field.
- C. Calculated fields can only be applied to host and sourcetype.
- D. Calculated fields are shortcuts for performing calculations using the eval command.

**Answer:** BD

### NEW QUESTION 5

- (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 6

- (Exam Topic 1)

When multiple event types with different color values are assigned to the same event, what determines the color displayed for the events?

- A. Rank
- B. Weight
- C. Priority
- D. Precedence



**Answer:** C

#### NEW QUESTION 7

- (Exam Topic 1)

Which of the following statements describe the Common Information Model (QM)? (select all that apply)

- A. CIM is a methodology for normalizing data.
- B. CIM can correlate data from different sources.
- C. The Knowledge Manager uses the CIM to create knowledge objects.
- D. CIM is an app that can coexist with other apps on a single Splunk deployment.

**Answer:** AC

#### 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)

Which of the following statements describe GET workflow actions?

- A. GET workflow actions must be configured with POST arguments.
- B. Configuration of GET workflow actions includes choosing a sourcetype.
- C. Label names for GET workflow actions must include a field name surrounded by dollar signs.
- D. GET workflow actions can be configured to open the URT link in the current window or in a new window

**Answer:** D

#### NEW QUESTION 10

- (Exam Topic 1)

What is the relationship between data models and pivots?

- A. Data models provide the datasets for pivots.
- B. Pivots and data models have no relationship.
- C. Pivots and data models are the same thing.
- D. Pivots provide the datasets for data models.

**Answer:** D

#### NEW QUESTION 10

- (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 14

- (Exam Topic 1)

Which of the following actions can the eval command perform?

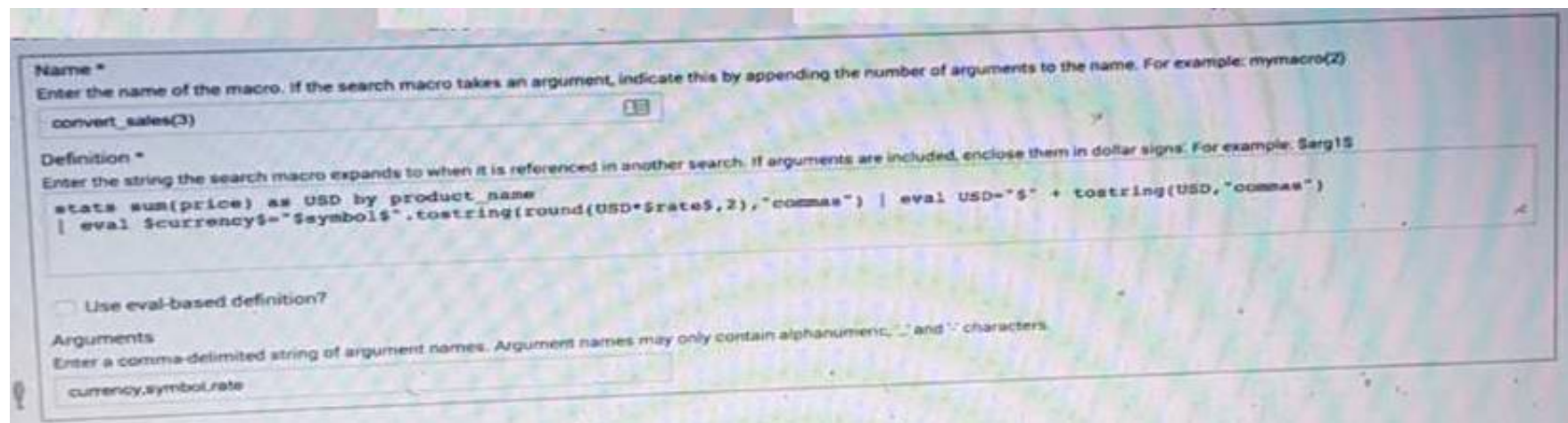
- A. Remove fields from results.
- B. Create or replace an existing field.
- C. Group transactions by one or more fields.
- D. Save SPL commands to be reused in other searches.

**Answer:** B

#### NEW QUESTION 15

- (Exam Topic 1)

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



The screenshot shows the 'Macro Definition' form in Splunk. The 'Name' field is 'convert\_sales(3)'. The 'Definition' field contains the following code: `stats sum(price) as USD by product_name | eval $currency$="$symbol$".tostring(round(USD*$rate$,2),"comma") | eval USD="$" + tostring(USD,"comma")`. The 'Arguments' field is 'currency,symbol,rate'. There is a checkbox for 'Use eval-based definition?' which is unchecked.

- 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 16

- (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 21

- (Exam Topic 1)

Which are valid ways to create an event type? (select all that apply)

- A. By using the searchtypes command in the search bar.
- B. By editing the event\_type stanza in the props.conf file.
- C. By going to the Settings menu and clicking Event Types > New.
- D. By selecting an event in search results and clicking Event Actions > Build Event Type.

**Answer: CD**

#### NEW QUESTION 25

- (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 30

- (Exam Topic 1)

Which group of users would most likely use pivots?

- A. Users
- B. Architects
- C. Administrators
- D. Knowledge Managers

**Answer: D**

#### NEW QUESTION 35

- (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 39

- (Exam Topic 1)

Which of the following statements describes Search workflow actions?

- A. By default
- B. Search workflow actions will run as a real-time search.
- C. Search workflow actions can be configured as scheduled searches,
- D. The user can define the time range of the search when created the workflow action.
- E. Search workflow actions cannot be configured with a search string that includes the transaction command

**Answer:** C

#### 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 46

- (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 51

- (Exam Topic 2)

Which workflow uses field values to perform a secondary search?

- A. POST
- B. Action
- C. Search
- D. Sub-Search

**Answer:** C

#### Explanation:

<https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/CreateworkflowactionsinSplunkWeb>

#### NEW QUESTION 52

- (Exam Topic 2)

Which of the following search modes automatically returns all extracted fields in the fields sidebar?

- A. Fast
- B. Smart
- C. Verbose

**Answer:** C

#### NEW QUESTION 55

- (Exam Topic 2)

Splunk alerts can be based on search that run \_\_\_\_\_. (Select all that apply.)

- A. in real-time
- B. on a regular schedule
- C. and have no matching events

**Answer:** AB

#### NEW QUESTION 60

- (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 61

- (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 62

- (Exam Topic 2)

Which is not a comparison operator in Splunk

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

**Answer:** E

#### NEW QUESTION 65

- (Exam Topic 2)

What will you learn from the results of the following search? sourcetype=cisco\_esa | transaction mid, dcid, icid | timechart avg(duration)

- A. The average time elapsed during each transaction for all transactions
- B. The average time for each event within each transaction
- C. The average time between each transaction

**Answer:** A

#### NEW QUESTION 67

.....

## Relate Links

**100% Pass Your SPLK-1002 Exam with Exambible Prep Materials**

<https://www.exambible.com/SPLK-1002-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>