

# Splunk

## Exam Questions SPLK-1002

Splunk Core Certified Power User Exam



### NEW QUESTION 1

- (Exam Topic 1)

What does the Splunk Common Information Model (CIM) add-on include? (select all that apply)

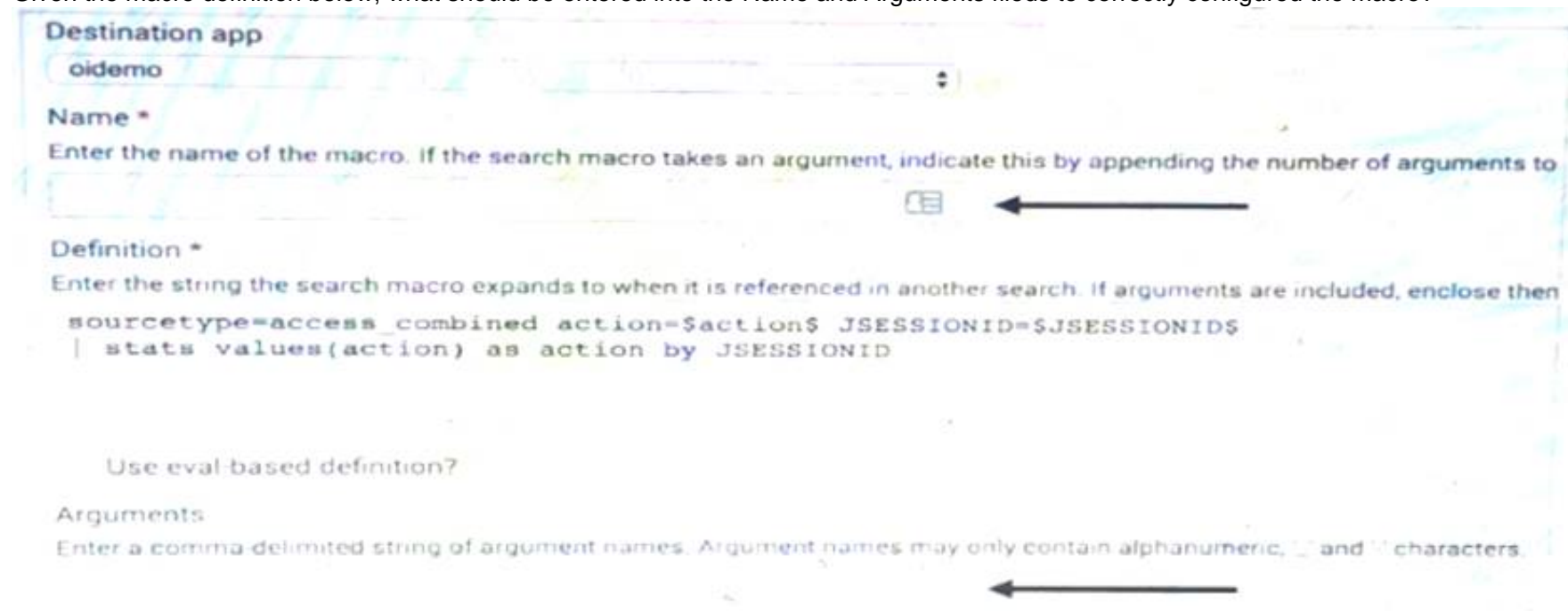
- A. Custom visualizations
- B. Pre-configured data models
- C. Fields and event category tags
- D. Automatic data model acceleration

**Answer: AC**

### NEW QUESTION 2

- (Exam Topic 1)

Given the macro definition below, what should be entered into the Name and Arguments fields to correctly configured the macro?



- A. The macro name is sessiontracker and the argument are action, JSESSION.
- B. The macro name is sessiontracker (2) and the action JSESSIONID
- C. The macro name is sessiontracker and the argument are sectional , \$ JSESSIONIDS.
- D. The macro name is sessiontracker (2) and the argument are \$action , \$JSESSIONIDS.

**Answer: B**

### NEW QUESTION 3

- (Exam Topic 1)

Which of the following Statements about macros is true? (select all that apply)

- A. Arguments are defined at execution time.
- B. Arguments are defined when the macro is created.
- C. Argument values are used to resolve the search string at execution time.
- D. Argument values are used to resolve the search string when the macro is created.

**Answer: AC**

### NEW QUESTION 4

- (Exam Topic 1)

Which of the following eval command function is valid?

- A. Int ()
- B. Count ( )
- C. Print ()
- D. ToString ()

**Answer: D**

### NEW QUESTION 5

- (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 6

- (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 7

- (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 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 15

- (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 .

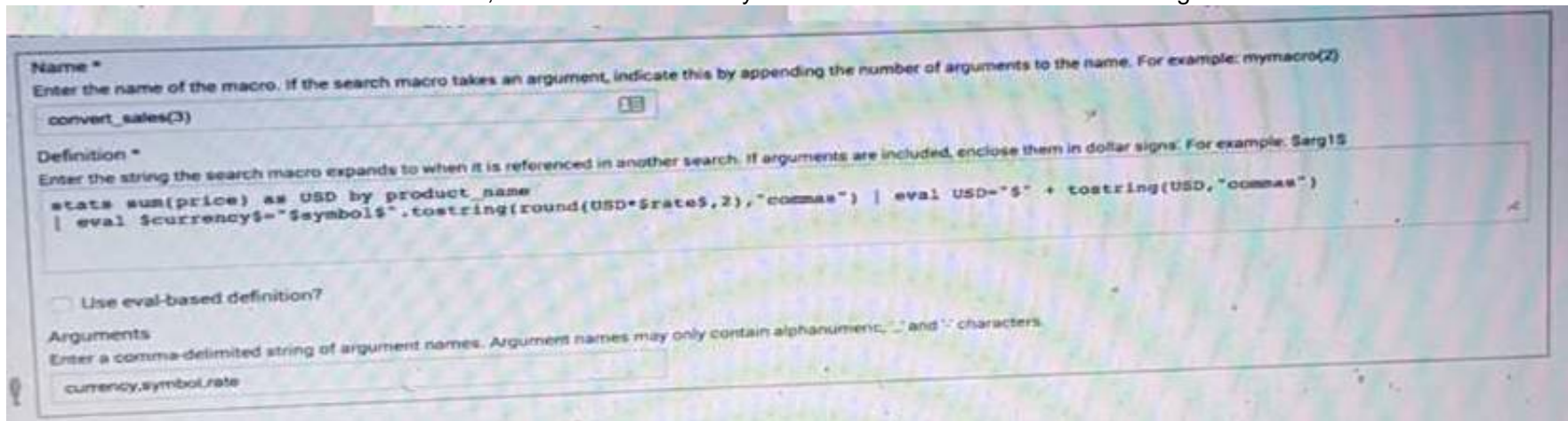
**Answer:**

D

#### NEW QUESTION 19

- (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 contains '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 contains 'currency,symbol,rate'. There is a checkbox for 'Use eval-based definition?' which is currently 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 20

- (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 24

- (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 29

- (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 31

- (Exam Topic 1)

Which of the following file formats can be extracted using a delimiter field extraction?

- A. CSV
- B. PDF
- C. XML
- D. JSON

**Answer: A**

#### NEW QUESTION 35

- (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 38

- (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 40

- (Exam Topic 1)

What does the fillnull command replace null values with, if the value argument is not specified?

- A. N/A
- B. NaN
- C. NULL

**Answer:** A

#### NEW QUESTION 45

- (Exam Topic 1)

Selected fields are displayed \_\_\_\_\_ each event in the search results.

- A. below
- B. interesting fields
- C. other fields
- D. above

**Answer:** A

#### NEW QUESTION 47

- (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 52

- (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 57

- (Exam Topic 1)

A space is an implied \_\_\_\_\_ in a search string.

- A. OR
- B. AND
- C. ()
- D. NOT

**Answer:** B

#### NEW QUESTION 60

- (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 64

- (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 65

- (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 66

- (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 69

- (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 74

- (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 75

- (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 77

- (Exam Topic 2)

Which of the following commands will show the maximum bytes?

- A. sourcetype=access\_\* | maximum totals by bytes
- B. sourcetype=access\_\* | avg (bytes)
- C. sourcetype=access\_\* | stats max(bytes)
- D. sourcetype=access\_\* | max(bytes)

**Answer:** C

#### NEW QUESTION 79

- (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 83

- (Exam Topic 2)

The transaction command allows you to \_\_\_\_\_ events across multiple sources

- A. duplicate
- B. correlate
- C. persist
- D. tag

**Answer:** B

#### NEW QUESTION 87

- (Exam Topic 2)

Which of the following are valid options to speed up reports? (Select all the apply.)

- A. Edit permissions
- B. Edit description
- C. Edit acceleration
- D. Edit schedule

**Answer:** C

#### NEW QUESTION 88

- (Exam Topic 2)

The gauge command:

- A. creates a single-value visualization
- B. allows you to set colored ranges for a single-value visualization
- C. creates a radial gauge visualization

**Answer:** B

#### NEW QUESTION 93

- (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 97

- (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 98**

- (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 102**

- (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 105**

- (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 110**

- (Exam Topic 2)

Which is not a comparison operator in Splunk

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

**Answer:** E

**NEW QUESTION 112**

- (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 116**

.....



## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### 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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SPLK-1002 Practice Test Here](#)**