

# 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 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 3

- (Exam Topic 1)

Which of the following statements describes the command below (select all that apply) sourcetype-access\_combined | transaction JSESSIONID

- A. An additional field named maxspan is created.
- B. An additional field 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 4

- (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 5

- (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 6

- (Exam Topic 1)

After manually editing; a regular expression (regex), which of the following statements is true?

- A. Changes made manually can be reverted in the Field Extractor (FX) UI.
- B. It is no longer possible to edit the field extraction in the Field Extractor (FX) UI.
- C. It is not possible to manually edit a regular expression (regex) that was created using the Field Extractor (FX) UI.
- D. The Field Extractor (FX) UI keeps its own version of the field extraction in addition to the one that was manually edited.

**Answer:** D

#### NEW QUESTION 7

- (Exam Topic 1)

Which of the following knowledge objects represents the output of an eval expression?

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

**Answer:** C

**NEW QUESTION 8**

- (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 9**

- (Exam Topic 1)

Which of the following describes the Splunk Common Information Model (CIM) add-on?

- A. The CIM add-on uses machine learning to normalize data.
- B. The CIM add-on contains dashboards that show how to map data.
- C. The CIM add-on contains data models to help you normalize data.
- D. The CIM add-on is automatically installed in a Splunk environment.

**Answer:** C

**NEW QUESTION 10**

- (Exam Topic 1)

When should you use the transaction command instead of the scats command?

- A. When you need to group on multiple values.
- B. When duration is irrelevant in search result
- C. .
- D. When you have over 1000 events in a transaction.
- E. When you need to group based on start and end constraints.

**Answer:** C

**NEW QUESTION 10**

- (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 14**

- (Exam Topic 1)

What is required for a macro to accept three arguments?

- A. The macro's name ends with (3).
- B. The macro's name starts with (3).
- C. The macro's argument count setting is 3 or more.
- D. Nothing, all macros can accept any number of arguments.

**Answer:** A

**NEW QUESTION 15**

- (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 17**

- (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 20

- (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 21

- (Exam Topic 2)

Which of the following searches will show the number of categoryId used by each host?

- A. Sourcetype=access\_\* |sum bytes by host
- B. Sourcetype=access\_\* |stats sum(categoryId) by host
- C. by host
- D. Sourcetype=access\_\* |sum(bytes) by host
- E. Sourcetype=access\_\* |stats sum by host

**Answer:** B

#### NEW QUESTION 24

- (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 26

.....

## 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](#)**