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)
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 3
- (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 4
- (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 5
- (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 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)
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 9
- (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 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)
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 15
- (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 18
- (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 19
- (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 23
- (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 28
- (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 30
- (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 31
- (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 33
- (Exam Topic 1)
Which of the following statements about data models and pivot are true? (select all that apply)

A. They are both knowledge objects.
B. Data models are created out of datasets called pivots.
C. Pivot requires users to input SPL searches on data models.
D. Pivot allows the creation of data visualizations that present different aspects of a data model.

Answer: BD

NEW QUESTION 35
- (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 40
- (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 44
- (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 47
- (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 51
- (Exam Topic 1)
In which of the following scenarios is an event type more effective than a saved search?

A. When a search should always include the same time range.
B. When a search needs to be added to other users' dashboards.
C. When the search string needs to be used in future searches.
D. When formatting needs to be included with the search string.

Answer: D

NEW QUESTION 56
- (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 60
- (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 61
- (Exam Topic 1)
What functionality does the Splunk Common Information Model (CIM) rely on to normalize fields with different names?

A. Macros.
B. Field aliases.
C. The rename command.
D. CIM does not work with different names for the same field.

Answer: B

NEW QUESTION 65
- (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 67
- (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 69
- (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 70
- (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 71
- (Exam Topic 2)
These users can create global knowledge objects. (Select all that apply.)

A. users
B. power users
C. administrators

Answer: BC

NEW QUESTION 74
- (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 78
- (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 79
- (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 81
- (Exam Topic 2)
Which is not a comparison operator in Splunk

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

Answer: E

NEW QUESTION 83
- (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 84
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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](https://www.certshared.com/exam/SPLK-1002/)