# Free Questions for SPLK-1002 by actualtestdumps

## Shared by Collins on 29-01-2024

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

Which type of workflow action sends field values to an external resource (e.g. a ticketing system)?

## Options:

**A-** POST

**B-** Search

**C-** GET

**D-** Format

## Answer:

A

## Explanation:

The type of workflow action that sends field values to an external resource (e.g. a ticketing system) is POST. A POST workflow action allows you to send a POST request to a URI location with field values or static values as arguments. For example, you can use a POST workflow action to create a ticket in an external system with information from an event.

# Question 2

**Question Type:** MultipleChoice

The timechart command is an example of which of the following command types?

## Options:

**A-** Orchestrating

**B-** Transforming

**C-** Statistical

**D-** Generating

## Answer:

B

## Explanation:

The correct answer is B. Transforming.

The explanation is as follows:

The timechart command is a Splunk command that creates a time series chart with corresponding table of statistics12.

A timechart is a statistical aggregation applied to a field to produce a chart, with time used as the X-axis1. You can specify a split-by field, where each distinct value of the split-by field becomes a series in the chart1.

Transforming commands are commands that change the format of the search results into a data structure that can be easily visualized3. Transforming commands often use stats functions to aggregate and summarize data3.

Therefore, the timechart command is an example of a transforming command, as it transforms the search results into a chart and a table using stats functions123.

# Question 3

**Question Type:** MultipleChoice

Which of the following options will define the first event in a transaction?

## Options:

**A-** startswith

**B-** with

**C-** startingwith

**D-** firstevent

## Answer:

A

## Explanation:

The correct answer is A. startswith.

The explanation is as follows:

The transaction command is used to find transactions based on events that meet various constraints12.

Transactions are made up of the raw text (the _raw field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member1.

The startswith option is used to define the first event in a transaction by specifying a search term or an expression that matches the event13.

For example, | transaction clientip JSESSIONID startswith='view' will create transactions based on the clientip and JSESSIONID fields, and the first event in each transaction will contain the term "view" in the _raw field2.

# Question 4

**Question Type:** MultipleChoice

What are search macros?

## Options:

**A-** Lookup definitions in lookup tables.

**B-** Reusable pieces of search processing language.

**C-** A method to normalize fields.

**D-** Categories of search results.

## Answer:

B

## Explanation:

The correct answer is B. Reusable pieces of search processing language.

The explanation is as follows:

Search macros are knowledge objects that allow you to insert chunks of SPL into other searches12.

Search macros can be any part of a search, such as an eval statement or a search term, and do not need to be a complete command12.

You can also specify whether the macro field takes any arguments and define validation expressions for them12.

Search macros can help you make your SPL searches shorter and easier to understand3.

To use a search macro in a search string, you need to put a backtick character () before and after the macro name[^1^][1]. For example, mymacro`.

# Question 5

**Question Type:** **MultipleChoice**

Which of the following searches will return all clientip addresses that start with 108?

## Options:

**A-** ... | where like (clientip, "108.% )

**B-** ... | where (clientip, '108. %')

**C-** ... | where (clientip=108. % )

**D-** ... | search clientip=108

### Answer:

A

# Question 6

**Question Type:** **MultipleChoice**

In the Field Extractor, when would the regular expression method be used?

### Options:

**A-** When events contain JSON data.

**B-** When events contain comma-separated data.

**C-** When events contain unstructured data.

**D-** When events contain table-based data.

## Answer:

C

## Explanation:

The correct answer is C. When events contain unstructured data.

The regular expression method works best with unstructured event data, such as log files or text messages, where the fields are not separated by a common delimiter, such as a comma or space1. You select a sample event and highlight one or more fields to extract from that event, and the field extractor generates a regular expression that matches similar events in your dataset and extracts the fields from them1. The regular expression method provides several tools for testing and refining the accuracy of the regular expression. It also allows you to manually edit the regular expression1.

The delimiters method is designed for structured event data: data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma or space1. You select a sample event, identify the delimiter, and then rename the fields that the field extractor finds1. This method is simpler and faster than the regular expression method, but it may not work well with complex or irregular data formats1.

1: Build field extractions with the field extractor - Splunk Documentation

# Question 7

**Question Type:** MultipleChoice

For the following search, which field populates the x-axis?

index=security sourcetype=linux secure | timechart count by action

## Options:

**A-** action

**B-** source type

**C-** _time

**D-** time

## Answer:

C

## Explanation:

The correct answer is C. _time.

The timechart command creates a time series chart with corresponding table of statistics, with time used as the X-axis1. You can specify a split-by field, where each distinct value of the split-by field becomes a series in the chart1. In this case, the split-by field is action, which means that the chart will have different lines for different actions, such as accept, reject, or fail2. The count function will calculate the number of events for each action in each time bin1.

For example, the following image shows a timechart of the count by action for a similar search3:

As you can see, the x-axis is populated by the _time field, which represents the time range of the search. The y-axis is populated by the count function, which represents the number of events for each action. The legend shows the different values of the action field, which are used to split the chart into different series.

2: Timechart Command In Splunk With Example - Mindmajix 1: timechart - Splunk Documentation 3: timechart command examples - Splunk Documentation

# Question 8

**Question Type:** **MultipleChoice**

Which of the following is included with the Common Information Model (CIM) add-on?

## Options:

**A-** Search macros

**B-** Event category tags

**C-** Workflow actions

**D-** tsidx files

## Answer:

B

## Explanation:

The correct answer is B. Event category tags. This is because the CIM add-on contains a collection of preconfigured data models that you can apply to your data at search time. Each data model in the CIM consists of a set of field names and tags that define the least common denominator of a domain of interest. Event category tags are used to classify events into high-level categories, such as authentication, network traffic, or web activity. You can use these tags to filter and analyze events based on their category. You can learn more about event category tags from the Splunk documentation12. The other options are incorrect because they are not included with the CIM add-on. Search macros are reusable pieces of search syntax that you can invoke from other searches. They are not specific to the CIM add-on, although some Splunk apps may provide their own search macros. Workflow actions are custom links or scripts that you can run on specific fields or events. They are also not specific to the CIM add-on, although some Splunk apps may provide their own workflow actions. tsidx files are index files that store the terms and pointers to the raw data in Splunk buckets. They are part of the Splunk indexing process and have nothing to do with the CIM add-on.

# Question 9

**Question Type:** MultipleChoice

What approach is recommended when using the Splunk Common Information Model (CIM) add-on to normalize data?

## Options:

**A-** Consult the CIM data model reference tables.

**B-** Run a search using the authentication command.

**C-** Consult the CIM event type reference tables.

**D-** Run a search using the correlation command.

## Answer:

A

## Explanation:

The recommended approach when using the Splunk Common Information Model (CIM) add-on to normalize data is A. Consult the CIM data model reference tables. This is because the CIM data model reference tables provide detailed information about the fields and tags that are expected for each dataset in a data model. By consulting the reference tables, you can determine which data models are

relevant for your data source and how to map your data fields to the CIM fields. You can also use the reference tables to validate your data and troubleshoot any issues with normalization. You can find the CIM data model reference tables in the Splunk documentation1 or in the Data Model Editor page in Splunk Web2. The other options are incorrect because they are not related to the CIM add-on or data normalization. The authentication command is a custom command that validates events against the Authentication data model, but it does not help you to normalize other types of data. The correlation command is a search command that performs statistical analysis on event fields, but it does not help you to map your data fields to the CIM fields. The CIM event type reference tables do not exist, as event types are not part of the CIM add-on.

# Question 10

**Question Type:** MultipleChoice

Which field extraction method should be selected for comma-separated data?

## Options:

**A-** Regular expression

**B-** Delimiters

**C-** eval expression

**D-** table extraction

## Answer:

B

## Explanation:

The correct answer is B. Delimiters. This is because the delimiters method is designed for structured event data, such as data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma or space. You can select a sample event, identify the delimiter, and then rename the fields that the field extractor finds. You can learn more about the delimiters method from the Splunk documentation1. The other options are incorrect because they are not suitable for comma-separated data. The regular expression method works best with unstructured event data, where you select and highlight one or more fields to extract from a sample event, and the field extractor generates a regular expression that matches similar events and extracts the fields from them. The eval expression is a command that lets you calculate new fields or modify existing fields using arithmetic, string, and logical operations. The table extraction is a feature that lets you extract tabular data from PDF files or web pages. You can learn more about these methods from the Splunk documentation23 .

# Question 11

**Question Type:** MultipleChoice

When used with the timechart command, which value of the limit argument returns all values?

## Options:

**A-** limit=*

**B-** limit=all

**C-** limit=none

**D-** limit=0

## Answer:

D

## Explanation:

The correct answer is D. limit=0. This is because the limit argument specifies the maximum number of series to display in the chart. If you set limit=0, no series filtering occurs and all values are returned. You can learn more about the limit argument and how it works with the agg argument from the Splunk documentation1. The other options are incorrect because they are not valid values for the limit argument. The limit argument expects an integer value, not a string or a wildcard. You can learn more about the syntax and usage of the timechart command from the Splunk documentation23.

# Question 12

**Question Type:** MultipleChoice

Which of the following is a feature of the Pivot tool?

## Options:

**A-** Creates lookups without using SPL.

**B-** Data Models are not required.

**C-** Creates reports without using SPL

**D-** Datasets are not required.

## Answer:

C

## Explanation:

The correct answer is C. Creates reports without using SPL. This is because the Pivot tool is a feature of Splunk that allows you to report on a specific data set without using the Splunk Search Processing Language (SPL). You can use a drag-and-drop interface to design and generate pivots that present different aspects of your data in the form of tables, charts, and other visualizations. You can learn more

about the Pivot tool from the Splunk documentation1 or watch a video tutorial2. The other options are incorrect because they do not describe the features of the Pivot tool. The Pivot tool requires data models and datasets to define the data that you want to work with. Data models and datasets are designed by the knowledge managers in your organization. You can learn more about data models and datasets from the Splunk documentation3. The Pivot tool does not create lookups, which are tables that match field values to other field values. You can create lookups using SPL or the Lookup Editor. You can learn more about lookups from the Splunk documentation.