Free Questions for SPLK-1002 by dumpssheet

Shared by Dean on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

The Splunk Common Information Model (CIM) is a collection of what type of knowledge object?

Options:

A- KV Store

B- Lookups

C- Saved searches

D- Data models

Answer:

D

Explanation:

The Splunk Common Information Model (CIM) is a collection of data models that apply a common structure and naming convention to data from any source. A data model is a type of knowledge object that defines the structure and relationships of fields in a dataset. A

data model can have one or more datasets, which are subsets of the data model that represent different aspects of the data. For example, the Network Traffic data model has datasets such as All Traffic, DNS, HTTP, etc. The CIM contains 28 pre-configured data models that cover various domains such as authentication, network traffic, web, email, etc.The CIM is implemented as an add-on that contains the JSON files for the data models, documentation, and tools that support the consistent, normalized treatment of data for maximum efficiency at search time23

1: Splunk Core Certified Power User Track, page 10.2: Splunk Documentation, Overview of the Splunk Common Information Model1.3: Splunkbase, Splunk Common Information Model (CIM)2.

Question 2

Question Type: **MultipleChoice**

Why are tags useful in Splunk?

Options:

A- Tags look for less specific data.

B- Tags visualize data with graphs and charts.

C- Tags group related data together.

D- Tags add fields to the raw event data.

Answer:

C

Explanation:

Tags are a type of knowledge object that enable you to assign descriptive keywords to events based on the values of their fields. Tags can help you to search more efficiently for groups of event data that share common characteristics, such as functionality, location, priority, etc. For example, you can tag all the IP addresses of your routers as router, and then search for tag=router to find all the events related to your routers. Tags can also help you to normalize data from different sources by using the same tag name for equivalent field values.For example, you can tag the field values error, fail, and critical as severity=high, and then search for severity=high to find all the events with high severity level2

1: Splunk Core Certified Power User Track, page 10.2: Splunk Documentation, About tags and aliases.

Question 3

Question Type: MultipleChoice

Given the following eval statement:

...| eval fieldl - if(isnotnull(fieldl),fieldl,0), field2 = if(isnull, "NO-VALUE", fieid2)

Which of the following is the equivalent using f ilinull?

Options:

A- There is no equivalent expression using f ilinull

B- ... t filinull values=(0,'NO-VALUE') fields=(fieldl,field2)

C- ... I filinull value=0 fieldl I fillnull fields

D- ... I fillnull fieldl I filinull value='NO-VALUE' field2

Answer:

B

Explanation:

The fillnull command replaces null values in one or more fields with a specified value. The values option allows you to specify a comma-separated list of values to fill the null values in the corresponding fields. The fields option allows you to specify a comma-separated list of fields to apply the fillnull command to. The eval statement in the question uses the if and isnull functions to check if field1 and field2 have

null values and replace them with 0 and "NO-VALUE" respectively.The equivalent expression using fillnull is to use the values option to specify 0 and "NO-VALUE" and the fields option to specify field1 and field22

1: Splunk Core Certified Power User Track, page 9.2: Splunk Documentation, fillnull command.

Question 4

Question Type: MultipleChoice

If a calculated field has the same name as an extracted field, what happens to the extracted field?

Options:

A- The calculated field will override the extracted field.

B- The calculated and extracted fields will be combined.

C- The calculated field will duplicate the extracted field.

D- An error will be returned and the search will fail.

Answer:

A

Explanation:

When you define a calculated field, you can specify the name of the field that the eval expression will create or modify. If the name of the calculated field matches the name of an existing extracted field, the calculated field will override the extracted field and replace its value with the result of the eval expression. This means that the original value of the extracted field will not be available for searching or analysis.To avoid this, you should use a unique name for your calculated field or use a different name for your extracted field2

1: Splunk Core Certified Power User Track, page 9.2: Splunk Documentation, Configure calculated fields with props.conf.

Question 5

Question Type: MultipleChoice

Tags can reference which of the following knowledge objects?

Options:

A- Lookups and event types only.

B- Extracted fields, field aliases, calculated fields, lookups, and event types.

C- Tags cannot reference any of these knowledge objects because tags are the last knowledge objects generated in the search-time operation sequence.

D- Extracted fields, calculated fields, and field aliases only.

Answer:

B

Explanation:

Tags are a type of knowledge object that enable you to assign descriptive keywords to events. Tags can reference any of the following knowledge objects: extracted fields, field aliases, calculated fields, lookups, and event types. Tags cannot reference other tags or search macros.Tags are applied to events at search time based on the values of the fields that they reference2

1: Splunk Core Certified Power User Track, page 10.2: Splunk Documentation, About tags and aliases.

Question 6

Question Type: MultipleChoice

What commands can be used to group events from one or more data sources?

Options:

A- eval, coalesce

B- transaction, stats

C- stats, format

D- top, rare

Answer:

B

Explanation:

The transaction and stats commands are two ways to group events from one or more data sources based on common fields or time ranges. The transaction command creates a single event out of a group of related events, while the stats command calculates summary statistics over a group of events. The eval and coalesce commands are used to create or combine fields, not to group events. The format command is used to format the results of a subsearch, not to group events.The top and rare commands are used to rank the most or least common values of a field, not to group events23

1: Splunk Core Certified Power User Track, page 9.2: Splunk Documentation, transaction command.3: Splunk Documentation, stats command.

Question 7

Question Type: MultipleChoice

Consider the the following search run over a time range of last 7 days:

index=web sourcetype=access_conbined | timechart avg(bytes) by product_nane

Which option is used to change the default time span so that results are grouped into 12 hour intervals?

Options:

A- span=12h

B- timespan=12h

C- span=12

D- timespan=12

Answer:

A

Explanation:

The span option is used to specify the time span for the timechart command. The span value can be a number followed by a time unit, such as h for hour, d for day, w for week, etc. The span value determines how the data is grouped into time buckets. For example, span=12h means that the data is grouped into 12-hour intervals.The timespan option is not a valid option for the timechart command2

1: Splunk Core Certified Power User Track, page 9.2: Splunk Documentation, timechart command.

Question 8

Question Type: MultipleChoice

Which of the following expressions could be used to create a calculated field called gigabytes?

Options:

A- eval sc_bytes(1024/1024)

B- | eval negabytes=sc_bytes(1024/1024)

C- megabytes=sc_bytes(1024/1024)

D- sc_bytas(1024/1024)

Answer:

B

Question 9

Question Type: MultipleChoice

When defining a macro, what are the required elements?

Options:

A- Name and arguments.

B- Name and a validation error message.

C- Name and definition.

D- Definition and arguments.

Answer:

C

Explanation:

When defining a search macro, the required elements are the name and the definition of the macro. The name is a unique identifier for the macro that can be used to invoke it in other searches. The definition is the search string that the macro expands to when referenced.The arguments, validation expression, and validation error message are optional elements that can be used to customize the macro behavior and input validation2

1: Splunk Core Certified Power User Track, page 9.2: Splunk Documentation, Define search macros in Settings.