SPLK-1002 Q&As

Splunk Core Certified Power User

Pass Splunk SPLK-1002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/splk-1002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

QUESTION 1

What other syntax will produce exactly the same results as | chart count over vendor_action by user?

A. | chart count by vendor_action, user

B. | chart count over vendor_action, user

C. | chart count by vendor_action over user

D. | chart count over user by vendor_action

Correct Answer: A

Explanation: https://docs.splunk.com/Documentation/Splunk/8.1.2/SearchReference/Chart

QUESTION 2

Data model are composed of one or more of which of the following datasets? (select all that apply.)

A. Events datasets

B. Search datasets

C. Transaction datasets

D. Any child of event, transaction, and search datasets

Correct Answer: ABC

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Aboutdatamodels

Data models are collections of datasets that represent your data in a structured and hierarchical way. Data models define how your data is organized into objects and fields. Data models can be composed of one or more of the following datasets:

Events datasets: These are the base datasets that represent raw events in Splunk. Events datasets can be filtered by constraints, such as search terms, sourcetypes, indexes, etc.

Search datasets: These are derived datasets that represent the results of a search on events or other datasets. Search datasets can use any search command, such as stats, eval, rex, etc., to transform the data.

Transaction datasets: These are derived datasets that represent groups of events that are related by fields, time, or both. Transaction datasets can use the transaction command or event types with transactiontype=true to create transactions.

QUESTION 3

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.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Abouttransactions

A transaction is a group of events that share some common characteristics, such as fields, time, or both. A transaction can be created by using the transaction command or by defining an event type with transactiontype=true in props.conf. Events in a transaction have one or more fields in common that relate them to each other. For example, you can create a transaction based on JSESSIONID, which is a unique identifier for each user session in web logs. Events in a transaction do not have to have the same timestamp, sourcetype, or exact same set of fields. They only have to share one or more fields that define the transaction.

QUESTION 4

What is a limitation of searches generated by workflow actions?

A. Searches generated by workflow action cannot use macros.

B. Searches generated by workflow actions must be less than 256 characters long.

C. Searches generated by workflow action must run in the same app as the workflow action.

D. Searches generated by workflow action run with the same permissions as the user running them.

Correct Answer: D

QUESTION 5

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

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields

A calculated field is a field that you create based on the value of another field or fields1. You can use calculated fields to enrich your data with additional information or to transform your data into a more useful format1. Calculated fields can be based on extracted fields, which are fields that are extracted from your raw data using various methods such as regular expressions, delimiters, or key-value pairs1. Therefore, option B is correct, while options A, C and D are incorrect because tags, output fields for a lookup, and fields generated from a search string are not types of extracted fields.

QUESTION 6

When creating a data model, which root dataset requires at least one constraint?

A. Root transaction dataset

B. Root event dataset

C. Root child dataset

D. Root search dataset

Correct Answer: B

Explanation: The correct answer is B. Root event dataset. This is because root event datasets are defined by a constraint that filters out events that are not relevant to the dataset. A constraint for a root event dataset is a simple search that returns a fairly wide range of data, such as sourcetype=access_combined. Without a constraint, a root event dataset would include all the events in the index, which is not useful for data modeling. You can learn more about how to design data models and add root event datasets from the Splunk documentation1. The other options are incorrect because root transaction datasets and root search datasets have different ways of defining their datasets, such as transaction definitions or complex searches, and root child datasets are not a valid type of root dataset.

QUESTION 7

Which of the following statements about calculated fields in Splunk is true?

A. Calculated fields cannot be chained together to create more complex fields

B. Calculated fields can be chained together to create more complex fields.

C. Calculated fields can only be used in dashboards.

D. Calculated fields can only be used in saved reports.

Correct Answer: B

The correct answer is B. Calculated fields can be chained together to create more complex fields.

Calculated fields are fields that are added to events at search time by using eval expressions. They can be used to perform calculations with the values of two or more fields already present in those events. Calculated fields can be defined with Splunk Web or in the props.conf file. They can be used in searches, reports, dashboards, and data models like any other extracted field1. Calculated fields can also be chained together to create more complex fields. This means that you can use a calculated field as an input for another calculated field. For example, if you have a calculated field named total that sums up the values of two fields named price and tax, you can use the total field to create another calculated field named discount that applies a percentage discount to the total field. To do this, you need to define the discount field with an eval expression that references the total field, such as: discount = total * 0.9 This will create a new field named discount that is equal to 90% of the total field value for each event2. References: About calculated fields Chaining calculated fields

QUESTION 8

Which of the following commands support the same set of functions?

A. stats, eval, table

B. search, where, eval

C. stats, chart, timechart

D. transaction, chart, timechart

Correct Answer: C

QUESTION 9

A field alias has been created based on an original field. A search without any transforming commands is then executed in Smart Mode. Which field name appears in the results?

A. Both will appear in the All Fields list, but only if the alias is specified in the search.

B. Both will appear in the Interesting Fields list, but only if they appear in at least 20 percent of events.

C. The original field only appears in All Fields list and the alias only appears in the Interesting Fields list.

D. The alias only appears in the All Fields list and the original field only appears in the Interesting Fields list.

Correct Answer: B

Explanation: A field alias is a way to assign an alternative name to an existing field without changing the original field name or value2. You can use field aliases to make your field names more consistent or descriptive across different sources or sourcetypes2. When you run a search without any transforming commands in Smart Mode, Splunk automatically identifies and displays interesting fields in your results2. Interesting fields are fields that appear in at least 20 percent of events or have high variability among values2. If you have created a field alias based on an original field, both the original field name and the alias name will appear in the Interesting Fields list if they meet these criteria2. However, only one of them will appear in each event depending on which one you have specified in your search string2. Therefore, option B is correct, while options A, C and D are incorrect.

QUESTION 10

What is the Splunk Common Information Model (CIM)?

A. The CIM is a prerequisite that any data source must meet to be successfully onboarded into Splunk.

B. The CIM provides a methodology to normalize data from different sources and source types.

C. The CIM defines an ecosystem of apps that can be fully supported by Splunk.

D. The CIM is a data exchange initiative between software vendors.

Correct Answer: B

Explanation: The Splunk Common Information Model (CIM) provides a methodology to normalize data from different sources and source types. The CIM defines a common set of fields and tags for different types of data, such as web, network, email, etc. This allows you to search and analyze data from different sources in a consistent way.

QUESTION 11

The macro weekly sales (2) contains the search string:

index=games | eval ProductSales = $Price$ * $AmountSold$

Which of the following will return results?

A. `weekly sales (3)\\'

B. `weekly_sales($3.995, $108)\\'

C. \\'weekly_sales (3.99, 10)\\'

D. `weekly sales (3.99, 10)\\'

Correct Answer: C

Explanation: To use a search macro in a search string, you need to place a back tick character (`) before and after the macro name1. You also need to use the same number of arguments as defined in the macro2. The macro weekly sales (2)

has two arguments: Price and AmountSold. Therefore, you need to provide two values for these arguments when you call the macro.

The option A is incorrect because it uses parentheses instead of back ticks around the macro name. The option B is incorrect because it uses underscores instead of spaces in the macro name. The option D is incorrect because it uses

spaces instead of commas to separate the argument values.

Reference: 1 Use search macros in searches - Splunk Documentation 2 Define search macros in Settings - Splunk Documentation

QUESTION 12

Which of the following searches will return events contains a tag name Privileged?

A. Tag= Priv

B. Tag= Pri*

C. Tag= Priv*

D. Tag= Privileged

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/PCI/4.1.0/Install/PrivilegedUserActivity

A tag is a descriptive label that you can apply to one or more fields or field values in your events1. You can use tags to simplify your searches by replacing long or complex field names or values with short and simple tags1. To search for events that contain a tag name, you can use the tag keyword followed by an equal sign and the tag name1. You can also use wildcards (*) to match partial tag names1. Therefore, option B is correct because it will return events that

contain a tag name that starts with Pri. Options A and D are incorrect because they will only return events that contain an exact tag name match. Option C is incorrect because it will return events that contain a tag name that starts with Priv, not Privileged.

QUESTION 13

Which of the following is a function of the Splunk Common Information Model (CIM)?

A. Normalizing data across a Splunk deployment.

B. Providing templates for reports and dashboards.

C. Algorithmically shifting events to other indexes.

D. Reingesting previously indexed data with new field names.

Correct Answer: A

QUESTION 14

Which of the following objects can a calculated field use as a source?

A. An alias of a field.

B. A field added by an automatic lookup.

C. The tag field.

D. The eventtype field.

Correct Answer: B

Explanation: The correct answer is B. A field added by an automatic lookup.

A calculated field is a field that is added to events at search time by using an eval expression. A calculated field can use the values of two or more fields that are already present in the events to perform calculations. A calculated field can use any field as a source, as long as the field is extracted before the calculated field is defined1. An automatic lookup is a way to enrich events with additional fields from an external source, such as a CSV file or a database. An automatic lookup can add fields to events based on the values of existing fields, such as host, source, sourcetype, or any other extracted field2. An automatic lookup is performed before the calculated fields are defined, so the fields added by the lookup can be used as sources for the calculated fields3. Therefore, a calculated field can use a field added by an automatic lookup as a source. References: About calculated fields About lookups Search time processing

QUESTION 15

How is a macro referenced in a search?

A. By using the macroname command.

B. By using the macro command.

C. By enclosing the macro name in backtick characters (`).

D. By enclosing the macro name in single-quote characters (`).

Correct Answer: C

Explanation: The correct answer is C. By enclosing the macro name in backtick characters (`).

A macro is a way to reuse a piece of SPL code in different searches. A macro can take arguments, which are variables that can be replaced by different values when the macro is called. A macro can also contain another macro within it,

which is called a nested macro1. To reference a macro in a search, you need to enclose the macro name in backtick characters (). For example, if you have a macro named my_macro` that takes one argument, you can reference it in a

search by using the following syntax:

| my_macro(argument) | ...

This will replace the macro name and argument with the SPL code contained in the macro definition. For example, if the macro definition is:

[my_macro(argument)] search sourcetype=$argument$ And you reference it in a search with:

index=main | my_macro(web) | stats count by host This will expand the macro and run the following SPL code:

index=main | search sourcetype=web | stats count by host References:

Use search macros in searches