SPLK-1002 Q&As

Splunk Core Certified Power User

QUESTION 1

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

A. Orchestrating

B. Transforming

C. Statistical

D. Generating

Correct Answer: B

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 2

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

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.

Correct Answer: A

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 3

When performing a regular expression (regex) field extraction using the Field Extractor (FX), what happens when the require option is used?

A. The regex can no longer be edited.

B. The field being extracted will be required for all future events.

C. The events without the required field will not display in searches.

D. Only events with the required string will be included in the extraction.

Correct Answer: D

The Field Extractor (FX) allows you to use regular expressions (regex) to extract fields from your events using a graphical interface or by manually editing the regex2. When you use the FX to perform a regex field extraction, you can use the require option to specify a string that must be present in an event for it to be included in the extraction2. This way, you can filter out events that do not contain the required string and focus on the events that are relevant for your extraction2. Therefore, option D is correct, while options A, B and C are incorrect.

QUESTION 4

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.

Correct Answer: C

The Splunk Common Information Model (CIM) add-on is a Splunk app that contains data models to help you normalize data from different sources and formats. The CIM add-on defines a common and consistent way of naming and categorizing fields and events in Splunk. This makes it easier to correlate and analyze data across different domains, such as network, security, web, etc. The CIM add-on does not use machine learning to normalize data, but rather relies on predefined field names and values. The CIM add-on does not contain dashboards that show how to map data, but rather provides documentation and examples on how to use the data models. The CIM add-on is not automatically installed in a Splunk environment, but rather needs to be downloaded and installed from Splunkbase.

QUESTION 5

Which of the following is true about a datamodel that has been accelerated?

A. They can be used with Pivot, the | tstats command, or the | datamodel command.

B. They can still be used in the Pivot tool but only with the accelerate_pivot capability.

C. They can no longer be used in the Pivot tool.

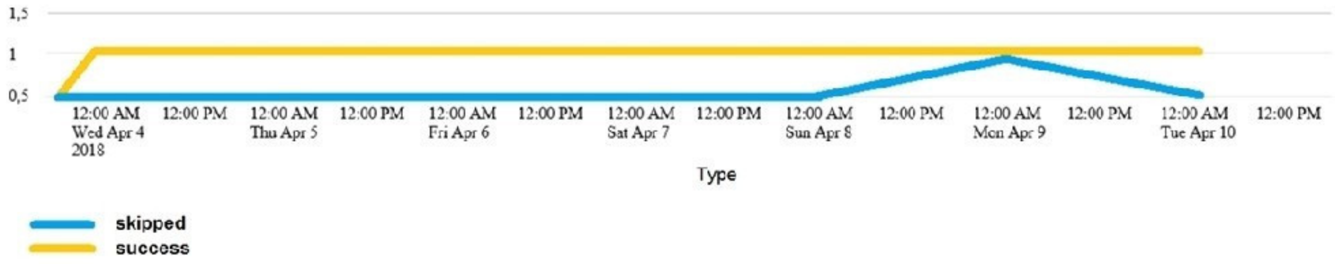
D. They can be used with the |tstats command, but will only return that data which has been accelerated.

Correct Answer: A

A data model that has been accelerated can be used with Pivot, the | tstats command, or the | datamodel command (Option A). Acceleration pre-computes and stores results for quicker access, enhancing the performance of searches and analyses that utilize the data model, especially for large datasets. This makes accelerated data models highly efficient for use in various analytical tools and commands within Splunk.

QUESTION 6

Which of the following searches would create a graph similar to the one below?



A. index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | start count states

B. index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | chart count states by -time

C. index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | timechart count by status

D. None of these searches would generate a similart graph.

Correct Answer: C

The following search would create a graph similar to the one below:

index_internal sourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan=1d | timechart count by status

The search does the following:

It uses index_internal to specify the internal index that contains Splunk logs and metrics.

It uses sourcetype=Savesplunker to filter events by the sourcetype that indicates the Splunk Enterprise Security app.

It uses fields sourcetype, status to keep only the sourcetype and status fields in the events.

It uses transaction status maxspan=1d to group events into transactions based on the status field with a maximum time span of one day between the first and last events in a transaction. It uses timechart count by status to create a time-based chart that shows the count of transactions for each status value over time.

The graph shows the following:

It is a line graph with two lines, one yellow and one blue. The x-axis is labeled with dates from Wed, Apr 4, 2018 to Tue, Apr 10, 2018.

The y-axis is labeled with numbers from 0 to 15.

The yellow line represents "shipped" and the blue line represents "success". The yellow line has a steady increase from 0 to 15, while the blue line has a sharp increase from 0 to 5, then a decrease to 0, and then a sharp increase to 10.

The graph is titled "Type".

Therefore, option C is the correct answer.

QUESTION 7

Which of the following statements about event types is true? (select all that apply)

A. Event types can be tagged.

B. Event types must include a time range,

C. Event types categorize events based on a search.

D. Event types can be a useful method for capturing and sharing knowledge.

Correct Answer: ACD

Reference: https://www.edureka.co/blog/splunk-events-event-types-and-tags/

As mentioned before, an event type is a way to categorize events based on a search string that matches the events2. Event types can be tagged, which means that you can apply descriptive labels to event types and use them in your searches2. Therefore, option A is correct. Event types categorize events based on a search string, which means that you can define an event type by specifying a search string that matches the events you want to include in the event type2. Therefore, option C is correct. Event types can be a useful method for capturing and sharing knowledge, which means that you can use event types to organize your data into meaningful categories and share them with other users in your organization2. Therefore, option D is correct. Event types do not have to include a time range, which means that you can create an event type without specifying a time range for the events2. Therefore, option B is incorrect.

QUESTION 8

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.

Correct Answer: ABD

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

Calculated fields are fields that are created by performing calculations on existing fields using the eval command. Calculated fields can be used in the search bar to filter and transform events based on the calculated values. Calculated fields can also be based on an extracted field, which is a field that is extracted from raw data using various methods, such as regex, delimiters, lookups, etc. Calculated fields are not shortcuts for performing calculations using the eval command, but rather results of performing calculations using the eval command. Calculated fields can be applied to any field in Splunk, not only host and sourcetype.

Therefore, statements A, B, and D are true about calculated fields.

QUESTION 9

Which of the following statements describes POST workflow actions?

A. Configuration of a POST workflow action includes choosing a sourcetype.

B. POST workflow actions can be configured to send email to the URI location.

C. By default, POST workflow action are shown in both the event and field menus.

D. POST workflow actions can be configured to send POST arguments to the URI location.

Correct Answer: D

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

QUESTION 10

What are search macros?

A. Lookup definitions in lookup tables.

B. Reusable pieces of search processing language.

C. A method to normalize fields.

D. Categories of search results.

Correct Answer: B

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 11

A calculated field is a shortcut for performing repetitive, long, or complex transformations using which of the following commands?

A. transaction

B. lookup

C. stats

D. eval

Correct Answer: D

The correct answer is D. eval.

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 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. A calculated field is a shortcut for performing repetitive, long, or complex transformations using the eval command. The eval command is used to create or modify fields by using expressions. The eval command can perform mathematical, string, date and time, comparison, logical, and other operations on fields or values2. For example, if you want to create a new field named total that is the sum of two fields named price and tax, you can use the eval command as follows: | eval total=price+tax However, if you want to use this new field in multiple searches, reports, or dashboards, you can create a calculated field instead of writing the eval command every time. To create a calculated field with Splunk Web, you need to go to Settings > Fields > Calculated Fields and enter the name of the new field (total), the name of the sourcetype (sales), and the eval expression (price+tax). This will create a calculated field named total that will be added to all events with the sourcetype sales at search time. You can then use the total field like any other extracted field without writing the eval expression1. The other options are not correct because they are not related to calculated fields. These options are:

A. transaction: This command is used to group events that share some common values into a single record, called a transaction. A transaction can span multiple events and multiple sources, and can be useful for correlating events that are

related but not contiguous3.

B. lookup: This command is used to enrich events with additional fields from an external source, such as a CSV file or a database. A lookup can add fields to events based on the values of existing fields, such as host, source, sourcetype, or

any other extracted field.

C. stats: This command is used to calculate summary statistics on the fields in the search results, such as count, sum, average, etc. It can be used to group and aggregate data by one or more fields.

References:

About calculated fields

eval command overview

transaction command overview

[lookup command overview]

[stats command overview]

QUESTION 12

Use the dedup command to _____.

A. Rename a field in the index

B. remove duplicate values

C. provide an additional alias for the field that can D.be used in the search criteria

Correct Answer: B

QUESTION 13

The gauge command:

A. creates a single-value visualization

B. allows you to set colored ranges for a single-value visualization

C. creates a radial gauge visualization

Correct Answer: B

QUESTION 14

Consider the following search:

index=web sourcetype=access_corabined

The log shows several events that share the same jsesszonid value (SD462K101O2F267).

View the events as a group.

From the following list, which search groups events by jSSESSIONID?

A. index=web sourcetype=access_combined I transaction JSESSZONID I search SD462K101C2F267

B. index=web sourcetype=access_combined SD462K101O2F267 | table JSESSIONID

C. index=web sourcetype=access_combined | highlight JSESSIONID | search SD462K101O2F267

D. index=web sourcetype=access_combined JSESSTONID

Correct Answer: A

The transaction command groups events that share a common value in a specified field, such as JSESSIONID, and that occur within a specified time range. The search command filters the results to show only the events that match the given value of JSESSIONID. This search groups the events by JSESSIONID and then shows only the events that have the value SD462K101C2F267 for JSESSIONID2

1: Splunk Core Certified Power User Track, page 9. 2: Splunk Documentation, transaction command.

QUESTION 15

__________ datasets can be added to root dataset to narrow down the search

A. parent

B. extracted

C. event

D. child

Correct Answer: D

Child datasets can be added to root datasets to narrow down the search. Datasets are collections of events that represent your data in a structured and hierarchical way. Datasets can be created by using commands such as datamodel or pivot. Datasets can have different types, such as events, search, transaction, etc. Datasets can also have different levels, such as root or child. Root datasets are base datasets that contain all events from a data model or an index. Child datasets are derived datasets that contain a subset of events from a parent dataset based on some constraints, such as search terms, fields, time range, etc. Child datasets can be added to root datasets to narrow down the search and filter out irrelevant events.