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.certbus.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

Which of the following data models are included in the Splunk Common Information Model (CIM) add-on? (select all that apply)

A. User permissions

B. Alerts

C. Databases

D. Email

Correct Answer: BD

The Splunk Common Information Model (CIM) Add-on includes a variety of data models designed to normalize data from different sources to allow for cross-source reporting and analysis. Among the data models included, Alerts (Option B) and Email (Option D) are part of the CIM. The Alerts data model is used for data related to alerts and incidents, while the Email data model is used for data pertaining to email messages and transactions. User permissions (Option A) and Databases (Option C) are not data models included in the CIM; rather, they pertain to aspects of data access control and specific types of data sources, respectively, which are outside the scope of the CIM\\'s predefined data models.

QUESTION 2

In which Settings section are macros defined?

A. Fields

B. Tokens

C. Advanced Search

D. Searches, Reports, Alerts

Correct Answer: C

QUESTION 3

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

A. POST

B. Search

C. GET

D. Format

Correct Answer: A

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 4

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

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

A. action

B. source type

C. _time

D. time

Correct Answer: C

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.

Reference:

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

QUESTION 5

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 6

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

A. Creates lookups without using SPL.

B. Data Models are not required.

C. Creates reports without using SPL

D. Datasets are not required.

Correct Answer: C

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.

QUESTION 7

Which statement is true?

A. Pivot is used for creating datasets.

B. Data models are randomly structured datasets.

C. Pivot is used for creating reports and dashboards.

D. In most cases, each Splunk user will create their own data model.

Correct Answer: C

The statement that pivot is used for creating reports and dashboards is true. Pivot is a graphical interface that allows you to create tables, charts, and visualizations from data models. Data models are structured datasets that define how data is organized and categorized. Pivot does not create datasets, but uses existing ones.

QUESTION 8

A user wants to create a workflow action that will retrieve a specific field value from an event and run a search in a new browser window

in the user\\'s Splunk instance. What kind of workflow action should they create?

A. A Run workflow action, because the user is running a new search with a specific field value from an event returned in the user\\'s search.

B. A Search workflow action, because the user is running a new search with a specific field value from an event returned in the user\\'s search.

C. A POST workflow action, because the search is being sent to the user\\'s current Splunk instance.

D. A GET workflow action, because a field value needs to be retrieved from the events returned in the user\\'s search.

Correct Answer: B

A Search workflow action is the appropriate choice when a user wants to retrieve a specific field value from an event and run a search in a new browser window within their Splunk instance (Option B). This type of workflow action allows users to define a search that utilizes field values from selected events as parameters, enabling more detailed investigation or context-specific analysis based on the original search results.

QUESTION 9

which of the following commands are used when creating visualizations(select all that apply.)

A. Geom

B. Choropleth

C. Geostats

D. iplocation

Correct Answer: ACD

The following commands are used when creating visualizations: geom, geostats, and iplocation. Visualizations are graphical representations of data that show trends, patterns, or comparisons. Visualizations can have different types, such as charts, tables, maps, etc. Visualizations can be created by using various commands that transform the data into a suitable format for the visualization type. Some of the commands that are used when creating visualizations are: geom: This command is used to create choropleth maps that show geographic regions with different colors based on some metric. The geom command takes a KMZ file as an argument that defines the geographic regions and their boundaries. The geom command also takes a field name as an argument that specifies the metric to use for coloring the regions. geostats: This command is used to create cluster maps that show groups of events with different sizes and colors based on some metric. The geostats command takes a latitude and longitude field as arguments that specify the

location of the events. The geostats command also takes a statistical function as an argument that specifies the metric to use for sizing and coloring the clusters. iplocation: This command is used to create location-based visualizations that show events with different attributes based on their IP addresses. The iplocation command takes an IP address field as an argument and adds some additional fields to the events, such as Country, City, Latitude, Longitude, etc. The iplocation command can be used with other commands such as geom or geostats to create maps based on IP addresses.

QUESTION 10

Which knowledge object is used to normalize field names to comply with the Splunk Common Information Model (CIM)?

A. Field alias

B. Event types

C. Search workflow action

D. Tags

Correct Answer: A

The correct answer is A. Field alias123.

In Splunk, a field alias is a knowledge object that you can use to assign an alternate name to a field3. This can be particularly useful when you want to normalize your data to comply with the Splunk Common Information Model (CIM)12. The

CIM provides a methodology for normalizing values to a common field name1. It acts as a search-time schema to define relationships in the event data while leaving the raw machine data intact2. By using field aliases, you can map vendor

fields to common fields that are the same for each data source in a given domain4. This allows you to correlate events from different source types by normalizing these different occurrences to a common structure and naming convention1.

QUESTION 11

Which of the following statements describes Search workflow actions?

A. By default. Search workflow actions will run as a real-time search.

B. Search workflow actions can be configured as scheduled searches,

C. The user can define the time range of the search when created the workflow action.

D. Search workflow actions cannot be configured with a search string that includes the transaction command

Correct Answer: C

Search workflow actions are custom actions that run a search when you click on a field value in your search results. Search workflow actions can be configured with various options, such as label name, search string, time range, app context, etc. One of the options is to define the time range of the search when creating the workflow action. You can choose from predefined time ranges, such as Last 24 hours, Last 7 days, etc., or specify a custom time range using relative or absolute time modifiers. Search workflow actions do not run as real-time searches by default, but rather use

the same time range as the original search unless specified otherwise. Search workflow actions cannot be configured as scheduled searches, as they are only triggered by user interaction. Search workflow actions can be configured with any valid search string that includes any search command, such as transaction.

QUESTION 12

Which knowledge Object does the Splunk Common Information Model (CIM) use to normalize data. in addition to field aliases, event types, and tags?

A. Macros

B. Lookups

C. Workflow actions

D. Field extractions

Correct Answer: B

Normalize your data for each of these fields using a combination of field aliases, field extractions, and lookups. https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsear chtime

QUESTION 13

A calculated field may be based on which of the following?

A. Fields generated within a search string

B. Lookup tables

C. Regular expressions

D. Extracted fields

Correct Answer: D

In Splunk, calculated fields allow you to create new fields using expressions that can transform or combine the values of existing fields. Although all options provided might seem viable, when selecting only one option that is most representative of a calculated field, we typically refer to:

D. Extracted fields: Calculated fields are often based on fields that have already been extracted from your data. Extracted fields are those that Splunk has identified and pulled out from the event data based on patterns, delimiters, or other methods such as regular expressions or automatic extractions. These fields can then be used in expressions to create calculated fields. For example, you might have an extracted field for the time in seconds, and you want to create a calculated field for the time in minutes. You would use the extracted field in a calculation to create the new field. It\\'s important to note that although fields generated within a search string (A) and regular expressions (C) can also be used in the calculation of a new field, and lookup tables (B) can be used to enrich data, option D is typically what one refers to when discussing calculated fields, as it implies a direct transformation or calculation based on fields that have been extracted from the raw data.

QUESTION 14

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

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 15

Which of the following eval command functions is valid?

A. int()

B. count()

C. print()

D. tostring()

Correct Answer: D

https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/CommonEvalFunct ions

The eval command function tostring() is valid. The tostring() function converts a numeric value to a string value. For example, tostring(3.14) returns "3.14". The other functions are not valid eval command functions.