Free Questions for SPLK-1002 by braindumpscollection

Shared by Bowers on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

How are arguments defined within the macro search string?

Options:

A- arg$

B- 'arg'

C- %arg%

D- 'arg'

Answer:

A

Explanation:

Arguments are defined within the macro search string by using dollar signs on either side of the argument name, such as arg1 or fragment.

Reference

Search macro examples

Define search macros in Settings

Use search macros in searches

Question 2

Question Type: MultipleChoice

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

Options:

A- User permissions

B- Alerts

C- Databases

D- Email

Answer:

B, D

Explanation:

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 3

Question Type: MultipleChoice

To create a tag, which of the following conditions must be met by the user?

Options:

A- Identify at least one field:value pair.

B- Have the Power role at a minimum.

C- Be able to edit the sourcetype the tag applies to.

D- Must have the tag capability associated with their user role.

Answer:

D

Explanation:

To create a tag, the user must have the tag capability associated with their user role. The tag capability allows the user to create, edit, and delete tags. The user does not need to identify a field:value pair, have the Power role, or be able to edit the sourcetype the tag applies to. Reference SeeDefine and manage tags in Settingsand [About capabilities] in the Splunk Documentation.

Question 4

Question Type: MultipleChoice

Which of the following describes this search?

New Search

'third_party_outages(EMEA,-24h)'

Options:

A- This search will find all events for the third_party_outages event type that have 'EMEA' or '-24h' in the raw event data.

B- This search will run the third_party_outages saved search and filter for events containing 'EMEA' and '-24h' in the raw event data.

C- This search will run the third_party_outages macro and pass the arguments EMEA and -24h to the macro definition.

D- This search will find all events in the third_party_outages index with the tags EMEA and -24h.

Answer:

C

Explanation:

This search will run the third_party_outages macro and pass the arguments EMEA and -24h to the macro definition. A search macro is a reusable chunk of SPL that can be inserted into other searches. A search macro can take arguments that are used to resolve the search string at execution time. The syntax for using a search macro ismacro_name (argument1, argument2, ...). Reference SeeUse search macros in searchesandSearch macro examplesin the Splunk Documentation.

Question 5

Question Type: MultipleChoice

Which of the following is true about data model attributes?

Options:

A- They cannot be created within the data model.

B- They can only be added into a root search dataset.

C- They cannot be edited if inherited from a parent dataset.

D- They can be added to a dataset from search time field extractions.

Answer:

D

Explanation:

Data model attributes are fields that are added to a dataset from search time field extractions, calculated fields, lookups, or aliases. They can be created within the data model editor or inherited from a parent dataset. They can be edited or removed unless they are required by the data model. They can be added to any type of dataset, not just root search datasets. Reference SeeAbout data models, [Define

data model attributes], and [Edit data model datasets] in the Splunk Documentation.

Question 6

Question Type: MultipleChoice

When should the regular expression mode of Field Extractor (FX) be used? (select all that apply)

Options:

A- For data cleanly separated by a space, a comma, or a pipe character.

B- For data in a CSV (comma-separated value) file.

C- For data with multiple, different characters separating fields.

D- For unstructured data.

Answer:

C, D

Explanation:

The regular expression mode of Field Extractor (FX) should be used for data with multiple, different characters separating fields or for unstructured dat

a. The regular expression mode allows you to select a sample event and highlight the fields that you want to extract, and the field extractor generates a regular expression that matches similar events and extracts the fields from them. Reference SeeBuild field extractions with the field extractor - Splunk DocumentationandField Extractor: Select Method step - Splunk Documentation.

Question 7

Question Type: MultipleChoice

What type of command is eval?

Options:

A- Streaming in some modes

B- Report generating

C- Distributable streaming

D- Centralized streaming

Answer:

C

Explanation:

The correct answer is C. Distributable streaming. This is because the eval command is a type of command that can run on the indexers before the results are sent to the search head. This reduces the amount of data that needs to be transferred and improves the search performance. Distributable streaming commands can operate on each event or result individually, without depending on other events or results. You can learn more about the types of commands and how they affect search performance from the Splunk documentation1.

Question 8

Question Type: MultipleChoice

Which of the following statements describes an event type?

Options:

A- A log level measurement: info, warn, error.

B- A knowledge object that is applied before fields are extracted.

C- A field for categorizing events based on a search string.

D- Either a log, a metric, or a trace.

Answer:

C

Explanation:

This is because an event type is a knowledge object that assigns a user-defined name to a set of events that match a specific search criteria. For example, you can create an event type named successful_purchase for events that have sourcetype=access_combined, status=200, and action=purchase. Then, you can use eventtype=successful_purchase as a search term to find those events. You can also use event types to create alerts, reports, and dashboards.You can learn more about event types from the Splunk documentation1. The other options are incorrect because they do not describe what an event type is. A log level measurement is a field that indicates the severity of an event, such as info, warn, or error. A knowledge object that is applied before fields are extracted is a source type, which identifies the format and structure of the data. Either a log, a metric, or a trace is a type of data that Splunk can ingest and analyze, but not an event type.

Question 9

Question Type: MultipleChoice

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

Options:

A- Root transaction dataset

B- Root event dataset

C- Root child dataset

D- Root search dataset

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.