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.geekcert.com/splk-1002.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

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

A. Transaction datasets

B. Events datasets

C. Search datasets

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

Correct Answer: ABC

Data model datasets have a hierarchical relationship with each other, meaning they have parent-child relationships. Data models can contain multiple dataset hierarchies. There are three types of dataset hierarchies: event, search, and transaction. https://docs.splunk.com/Splexicon:Datamodeldataset

QUESTION 2

What does the Splunk Common Information Model (CIM) add-on include? (select all that apply)

A. Custom visualizations

B. Pre-configured data models

C. Fields and event category tags

D. Automatic data model acceleration

Correct Answer: BC

The Splunk Common Information Model (CIM) add-on is a collection of pre- built data models and knowledge objects that help you normalize your data from different sources and make it easier to analyze and report on it3. The CIM add-on includes pre- configured data models that cover various domains such as Alerts, Email, Database, Network Traffic, Web and more3. Therefore, option B is correct. The CIM add-on also includes fields and event category tags that define the common attributes and labels for the data models3. Therefore, option C is correct. The CIM add-on does not include custom visualizations or automatic data model acceleration. Therefore, options A and D are incorrect.

QUESTION 3

When should transaction be used?

A. Only in a large distributed Splunk environment.

B. When calculating results from one or more fields.

C. When event grouping is based on start/end values.

D. When grouping events results in over 1000 events in each group.

Correct Answer: C

QUESTION 4

Which of the following statements describes calculated fields?

A. Calculated fields are only used on fields added by lookups.

B. Calculated fields are a shortcut for repetitive and complex eval commands.

C. Calculated fields are a shortcut for repetitive and complex calc commands.

D. Calculated fields automatically calculate the simple moving average for indexed fields.

Correct Answer: B

QUESTION 5

Which of the following statements about tags is true? (select all that apply.)

A. Tags are case-insensitive.

B. Tags are based on field/vale pairs.

C. Tags categorize events based on a search.

D. Tags are designed to make data more understandable.

Correct Answer: BD

The following statements about tags are true: tags are based on field/value pairs and tags categorize events based on a search. Tags are custom labels that can be applied to fields or field values to provide additional context or meaning for your data. Tags can be used to filter or analyze your data based on common concepts or themes. Tags can be created by using various methods, such as search commands, configuration files, user interfaces, etc. Some of the characteristics of tags are: Tags are based on field/value pairs: This means that tags are associated with a specific field name and a specific field value. For example, you can create a tag called "alert" for the field name "status" and the field value "critical". This means that only events that have status=critical will have the "alert" tag applied to them. Tags categorize events based on a search: This means that tags are defined by a search string that matches the events that you want to tag. For example, you can create a tag called "web" for the search string sourcetype=access_combined. This means that only events that match the search string sourcetype=access_combined will have the "web" tag applied to them. The following statements about tags are false: tags are case-insensitive and tags are designed to make data more understandable. Tags are case-sensitive and tags are designed to make data more searchable. Tags are case-sensitive: This means that tags must match the exact case of the field name and field value that they are associated with. For example, if you create a tag called "alert" for the field name "status" and the field value "critical", it will not apply to events that have status=CRITICAL or Status=critical. Tags are designed to make data more searchable: This means that tags can help you find relevant events or patterns in your data by using common concepts or themes. For example, if you create a tag called "web" for the search string sourcetype=access_combined, you can use tag=web to find all events related to web activity.

SPLK-1002 VCE Dumps   SPLK-1002 Practice Test   SPLK-1002 Study Guide