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

Splunk alerts can be based on search that run_____. (Select all that apply.)

A. in real-time

B. on a regular schedule

C. and have no matching events

Correct Answer: AB

Explanation: Splunk alerts can be based on searches that run in real-time or on a regular schedule3. An alert is a way to monitor your data and get notified when certain conditions are met3. You can create an alert by specifying a search and a triggering condition3. You can also specify how often you want to run the search and how you want to receive the alert notifications3. You can run the alert search in real-time, which means that it continuously monitors your data as it streams into Splunk3. Alternatively, you can run the alert search on a regular schedule, which means that it runs at fixed intervals such as every hour or every day3. Therefore, options A and B are correct, while option C is incorrect because it is not a way to run an alert search.

QUESTION 2

Which command is used to create choropleth maps?

A. geostats

B. cluster

C. geom

Correct Answer: C

QUESTION 3

Which of the following is included with the Common Information Model (CIM) add-on?

A. Search macros

B. Event category tags

C. Workflow actions

D. tsidx files

Correct Answer: B

Explanation: The correct answer is B. Event category tags. This is because the CIM add- on contains a collection of preconfigured data models that you can apply to your data at search time. Each data model in the CIM consists of a set of field names and tags that define the least common denominator of a domain of interest. Event category tags are used to classify events into high-level categories, such as authentication, network traffic, or web activity. You can use these tags to filter and analyze events based on their category. You can learn more about event category tags from the Splunk

documentation12. The other options are incorrect because they are not included with the CIM add-on. Search macros are reusable pieces of search syntax that you can invoke from other searches. They are not specific to the CIM add-on, although some Splunk apps may provide their own search macros. Workflow actions are custom links or scripts that you can run on specific fields or events. They are also not specific to the CIM add-on, although some Splunk apps may provide their own workflow actions. tsidx files are index files that store the terms and pointers to the raw data in Splunk buckets. They are part of the Splunk indexing process and have nothing to do with the CIM add-on.

QUESTION 4

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

Explanation: 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 5

When would a user select delimited field extractions using the Field Extractor (FX)?

A. When a log file has values that are separated by the same character, for example, commas.

B. When a log file contains empty lines or comments.

C. With structured files such as JSON or XML.

D. When the file has a header that might provide information about its structure or format.

Correct Answer: A

The correct answer is A. When a log file has values that are separated by the same character, for example, commas.

The Field Extractor (FX) is a utility in Splunk Web that allows you to create new fields from your events by using either regular expressions or delimiters. The FX provides a graphical interface that guides you through the steps of defining and testing your field extractions1. The FX supports two field extraction methods: regular expression and delimited. The regular expression method works best with unstructured event data, such as logs or messages, that do not have a consistent format or structure. You select a sample event and highlight one or more fields to extract from that event, and the FX generates a regular expression that matches similar events in your data set and extracts the fields from them1. The delimited method is designed for structured event data: data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma, a tab, or a space. You select a sample event, identify the delimiter, and then rename the fields that the FX finds1. Therefore, you would select the delimited field extraction

method when you have a log file that has values that are separated by the same character, for example, commas. This method will allow you to easily extract the fields based on the delimiter without writing complex regular expressions. The other options are not correct because they are not suitable for the delimited field extraction method. These options are:

B. When a log file contains empty lines or comments: This option does not indicate that the log file has a structured format or a common delimiter. The delimited method might not work well with this type of data, as it might miss some fields or

include some unwanted values.

C. With structured files such as JSON or XML: This option does not require the delimited method, as Splunk can automatically extract fields from JSON or XML files by using indexed extractions or search-time extractions2. The delimited

method might not work well with this type of data, as it might not recognize the nested structure or the special characters.

D. When the file has a header that might provide information about its structure or format: This option does not indicate that the file has a common delimiter between the fields. The delimited method might not work well with this type of data,

as it might not be able to identify the fields based on the header information.

References:

Build field extractions with the field extractor Configure indexed field extraction