



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

Which of the following about reports is/are true?

- A. Reports are knowledge objects.
- B. Reports can be scheduled.
- C. Reports can run a script.
- D. All of the above.

Correct Answer: D

Explanation: A report is a way to save a search and its results in a format that you can reuse and share with others². A report is also a type of knowledge object, which is an entity that you create to add knowledge to your data and make it easier to search and analyze². Therefore, option A is correct. A report can be scheduled, which means that you can configure it to run at regular intervals and send the results to yourself or others via email or other methods². Therefore, option B is correct. A report can run a script, which means that you can specify a script file to execute when the report runs and use it to perform custom actions or integrations². Therefore, option C is correct. Therefore, option D is correct because all of the above statements are true for reports.

QUESTION 2

Which of the following objects can a calculated field use as a source?

- A. An alias of a field.
- B. A field added by an automatic lookup.
- C. The tag field.
- D. The eventtype field.

Correct Answer: B

Explanation: The correct answer is B. A field added by an automatic lookup.

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 use any field as a source, as long as the field is extracted before the calculated field is defined¹. An automatic lookup is a way to enrich events with additional fields from an external source, such as a CSV file or a database. An automatic lookup can add fields to events based on the values of existing fields, such as host, source, sourcetype, or any other extracted field². An automatic lookup is performed before the calculated fields are defined, so the fields added by the lookup can be used as sources for the calculated fields³. Therefore, a calculated field can use a field added by an automatic lookup as a source. References: About calculated fields About lookups Search time processing

QUESTION 3

In the following eval statement, what is the value of description if the status is 503? `index=main | eval description=case(status==200, "OK", status==404, "Not found", status==500, "Internal Server Error")`



- A. The description field would contain no value.
- B. The description field would contain the value 0.
- C. The description field would contain the value "Internal Server Error".
- D. This statement would produce an error in Splunk because it is incomplete.

Correct Answer: A

<https://docs.splunk.com/Documentation/Splunk/8.1.1/SearchReference/ConditionalFunctions>

QUESTION 4

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 5

Which of the following eval command function is valid?

- A. Int ()
- B. Count ()
- C. Print ()
- D. ToString ()



Correct Answer: D

Explanation: The eval command supports a number of functions that you can use in your expressions to perform calculations, conversions, string manipulations and more². One of the eval command functions is tostring(), which converts a numeric value to a string value². Therefore, option D is correct, while options A, B and C are incorrect because they are not valid eval command functions.

[SPLK-1002 PDF Dumps](#)

[SPLK-1002 VCE Dumps](#)

[SPLK-1002 Exam Questions](#)