SPLK-1002 Q&As

Splunk Core Certified Power User

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

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 searches show a valid use of a macro? (Choose all that apply.)

A. index=main source=mySource oldField=* |\\'makeMyField(oldField)\\'| table _time newField

B. index=main source=mySource oldField=* | stats if(`makeMyField(oldField)\\') | table _time newField

C. index=main source=mySource oldField=* | eval newField=\\'makeMyField(oldField)\\'| table _time newField

D. index=main source=mySource oldField=* | "\\'newField(`makeMyField(oldField)\\')\\'" | table _time newField

Correct Answer: AC

The searches A and C show a valid use of a macro. A macro is a reusable piece of SPL code that can be called by using single quotes (`\\'). A macro can take arguments, which are passed inside parentheses after the macro name. For example, `makeMyField(oldField)\\' calls a macro named makeMyField with an argument oldField. The searches B and D are not valid because they use double quotes ("") instead of single quotes (`\\').

QUESTION 3

In which Settings section are macros defined?

A. Fields

B. Tokens

C. Advanced Search

D. Searches, Reports, Alerts

Correct Answer: C

QUESTION 4

In the Field Extractor Utility, this button will display events that do not contain extracted fields.

Select your answer.

A. Selected-Fields

B. Non-Matches

C. Non-Extractions

D. Matches

Correct Answer: B

The Field Extractor Utility (FX) is a tool that helps you extract fields from your events using a graphical interface or by manually editing the regular expression2. The FX has a button that displays events that do not contain extracted fields, which is the Non- Matches button2. The Non-Matches button shows you the events that do not match the regular expression that you have defined for your field extraction2. This way, you can check if your field extraction is accurate and complete2. Therefore, option B is correct, while options A, C and D are incorrect because they are not buttons that display events that do not contain extracted fields.

QUESTION 5

The Field Extractor (FX) is used to extract a custom field. A report can be created using this custom field. The created report can then be shared with other people in the organization. If another person in the organization runs the shared report and no results are returned, why might this be? (select all that apply)

A. Fast mode is enabled.

B. The dashboard is private.

C. The extraction is private-

D. The person in the organization running the report does not have access to the index.

Correct Answer: CD

The Field Extractor (FX) is a tool that helps you extract fields from your events using a graphical interface2. You can create a report using a custom field extracted by the FX and share it with other users in your organization2. However, if another user runs the shared report and no results are returned, there could be two possible reasons. One reason is that the extraction is private, which means that only you can see and use the extracted field2. To make the extraction available to other users, you need to make it global or app-level2. Therefore, option C is correct. Another reason is that the other user does not have access to the index where the events are stored2. To fix this issue, you need to grant the appropriate permissions to the other user for the index2. Therefore, option D is correct. Options A and B are incorrect because they are not related to the field extraction or the report.

Latest SPLK-1002 Dumps SPLK-1002 Study Guide SPLK-1002 Exam Questions