Splunk Core Certified Power User

Splunk SPLK-1002 Dumps Available Here at:

https://www.certification-questions.com/splunk-exam/splk-1002-dumps.html

Enrolling now you will get access to 155 questions in a unique set of SPLK-1002 dumps

Question 1

When using a split series on a chart, the series MUST be displayed using the STACKED option.

Options:

A. True

B. False

Answer: B

Question 2

What is a limitation of searches generated by workflow actions?

Options:

A. Searches generated by workflow action cannot use macros.

B. Searches generated by workflow actions must be less than 256 characters long.

C. Searches generated by workflow action must run in the same app as the workflow action.

D. Searches generated by workflow action run with the same permissions as the user running them.

Answer: D

Question 3

Which of the following statements describes Search workflow actions?

Options:

A. By default. Search workflow actions will run as a real-time search.

B. Search workflow actions can be configured as scheduled searches,

C. The user can define the time range of the search when created the workflow action.

D. Search workflow actions cannot be configured with a search string that includes the transaction

command

Answer: C

Question 4

Which of the following Statements about macros is true? (select all that apply)

Options:

A. Arguments are defined at execution time.

B. Arguments are defined when the macro is created.

C. Argument values are used to resolve the search string at execution time.

D. Argument values are used to resolve the search string when the macro is created.

Answer: B, D

Question 5

Which of the following statements describes this search?
sourcetype=access_combined I transaction JSESSIONID | timechart avg (duration)

Options:

A. This is a valid search and will display a timechart of the average duration, of each transaction

event.

B. This is a valid search and will display a stats table showing the maximum pause among

transactions.

C. No results will be returned because the transaction command must include the startswith and

endswith options.

D. No results will be returned because the transaction command must be the last command used in

the search pipeline.

Answer: A

Question 6

Which of the following statements is true, especially in large environments?

Options:

A. Use the scats command when you next to group events by two or more fields.

B. The stats command is faster and more efficient than the transaction command

C. The transaction command is faster and more efficient than the stats command.

D. Use the transaction command when you want to see the results of a calculation.

Answer: B

Explanation:
ps://answers.splunk.com/answers/103/transaction-vs-stats-commands.html
Explanation:

Question 7

What functionality does the Splunk Common Information Model (CIM) rely on to normalize fields with different names?

Options:

A. Macros.

B. Field aliases.

C. The rename command.

D. CIM does not work with different names for the same field.

Answer: B

Question 8

What is required for a macro to accept three arguments?

Options:

A. The macro's name ends with (3).

B. The macro's name starts with (3).

C. The macro's argument count setting is 3 or more.

D. Nothing, all macros can accept any number of arguments.

Answer: A

Question 9

Data model fields can be added using the Auto-Extracted method. Which of the following statements describe Auto-Extracted fields? (select all that apply)

Options:

A. Auto-Extracted fields can be hidden in Pivot.

B. Auto-Extracted fields can have their data type changed.

C. Auto-Extracted fields can be given a friendly name for use in Pivot.

D. Auto-Extracted fields can be added if they already exist in the dataset with constraints.

Answer: A, C, D

Question 10

Which of the following statements about tags is true?

Options:

A. Tags are case insensitive.

B. Tags are created at index time.

C. Tags can make your data more understandable.

D. Tags are searched by using the syntax tag: : <fieldneme>

Answer: C