Splunk SPLK-1002 Mock Exam

Shared by Mcleod on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What are the expected results for a search that contains the command | where A=B?

Options:

A- Events that contain the string value where A=B.
B- Events that contain the string value A=B.
C- Events where values of field are equal to values of field B.
D- Events where field A contains the string value B.

Answer:

C

Explanation:

The correct answer is C. Events where values of field A are equal to values of field B.

The where command is used to filter the search results based on an expression that evaluates to true or false. The where command can compare two fields, two values, or a field and a value. The where command can also use functions, operators, and wildcards to create complex expressions1.

The syntax for the where command is:

| where <expression>

The expression can be a comparison, a calculation, a logical operation, or a combination of these. The expression must evaluate to true or false for each event.

To compare two fields with the where command, you need to use the field names without any quotation marks. For example, if you want to find events where the values for the field A match the values for the field B, you can use the following syntax:

| where A=B

This will return only the events where the two fields have the same value.

The other options are not correct because they use different syntax or fields that are not related to the where command. These options are:

A) Events that contain the string value where A=B: This option uses the string value where A=B as a search term, which is not valid syntax for the where command. This option will return events

that have the literal text ''where A=B'' in them.

B) Events that contain the string value A=B: This option uses the string value A=B as a search term, which is not valid syntax for the where command. This option will return events that have the literal text ''A=B'' in them.

D) Events where field A contains the string value B: This option uses quotation marks around the value B, which is not valid syntax for comparing fields with the where command. Quotation marks are used to enclose phrases or exact matches in a search2. This option will return events where the field A contains the string value ''B''.

where command usage

Search command cheatsheet

Question 2

Question Type: MultipleChoice

What do events in a transaction have In common?

Options:

A- All events In a transaction must have the same timestamp.
B- All events in a transaction must have the same sourcetype.
C- All events in a transaction must have the exact same set of fields.
D- All events in a transaction must be related by one or more fields.

Answer:

D

Explanation:

A transaction is a group of events that share some common characteristics, such as fields, time, or both. A transaction can be created by using the transaction command or by defining an event type with transactiontype=true in props.conf. Events in a transaction have one or more fields in common that relate them to each other. For example, you can create a transaction based on JSESSIONID, which is a unique identifier for each user session in web logs. Events in a transaction do not have to have the same timestamp, sourcetype, or exact same set of fields. They only have to share one or more fields that define the transaction.

Question 3

Question Type: MultipleChoice

Clicking a SEGMENT on a chart, _____.

Options:

A- drills down for that value
B- highlights the field value across the chart
C- adds the highlighted value to the search criteria

Answer:

C

Question 4

Question Type: MultipleChoice

When using timechart, how many fields can be listed after a by clause?

Options:

A- because timechart doesn't support using a by clause.
B- because _time is already implied as the x-axis.
C- because one field would represent the x-axis and the other would represent the y-axis.
D- There is no limit specific to timechart.

Answer:

B

Explanation:

The timechart command is used to create a time-series chart of statistical values based on your search results2.You can use the timechart command with a by clause to split the results by one or more fields and create multiple series in the chart2.However, you can only list one field after the by clause when using the timechart command because _time is already implied as the x-axis of the chart2. Therefore, option B is correct, while options A, C and D are incorrect.

Question 5

Question Type: MultipleChoice

This clause is used to group the output of a stats command by a specific name.

Options:

A- Rex
B- As
C- List
D- By

Answer:

B

Question 6

Question Type: MultipleChoice

Which tool uses data models to generate reports and dashboard panels without using SPL?

Options:

A- Visualization tab
B- Pivot
C- Datasets
D- splunk CIM

Answer:

B

Explanation:

The correct answer is B. Pivot1.

In Splunk, Pivot is a tool that uses data models to generate reports and dashboard panels without

the need for users to write or understand Splunk's Search Processing Language (SPL)1. Data models enable users of Pivot to create compelling reports and dashboards1. When a Pivot user designs a pivot report, they select the data model that represents the category of event data that they want to work with1. Then they select a dataset within that data model that represents the specific dataset on which they want to report1. This makes Pivot a powerful tool for users who need to create visualizations but do not have a deep understanding of SPL1.

Question 7

Question Type: MultipleChoice

What will you learn from the results of the following search?

sourcetype=cisco_esa | transaction mid, dcid, icid | timechart avg(duration)

Options:

A- The average time elapsed during each transaction for all transactions
B- The average time for each event within each transaction
C- The average time between each transaction

Answer:

A

Question 8

Question Type: MultipleChoice

A POST workflow action will pass which types of arguments to an external website?

Options:

A- Clear text only.
B- A mix of clear text strings and variables.
C- It can only send raw event data.
D- Variables only.

Answer:

B

Explanation:

A POST workflow action in Splunk is designed to send data to an external web service by using HTTP POST requests. This type of workflow action can pass a combination of clear text strings and variables derived from the search results or event data. The clear text strings might include static text or predefined values, while the variables are dynamic elements that represent specific fields or values extracted from the Splunk events. This flexibility allows for constructing detailed and context-specific requests to external systems, enabling various integration and automation scenarios. The POST request can include both types of data, making it versatile for different use cases.

Question 9

Question Type: MultipleChoice

What fields does the transaction command add to the raw events? (Choose all that apply)

Options:

A- count
B- duration
C- eventcount
D- transaction id

Answer:

B, D

Explanation:

Hello, this is Bing. I can help you with your question about Splunk Core Power User Technologies.

The correct answers are B. duration and D. transaction id.

The explanation is as follows:

The transaction command is a Splunk command that finds transactions based on events that

meet various constraints12.

Transactions are made up of the raw text (the _raw field) of each member, the time and date fields of the earliest member, as well as the union of all other fields of each member12.

The transaction command adds some fields to the raw events that are part of the transaction123. These fields are:

duration: The difference, in seconds, between the timestamps for the first and last events in the transaction123.

eventcount: The number of events in the transaction123.

transaction_id: A unique identifier for each transaction3. This field is useful for filtering or joining transactions3.

Therefore, the fields that the transaction command adds to the raw events are duration and transaction_id, which are options B and D in your question.