Free Questions for SPLK-1002 by ebraindumps

Shared by Lara on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which option of the transaction command would be used to specify the maximum time between events in a transaction?

Options:

A- maxpause

B- maxspan

C- duration

D- eventcount

Answer:

A

Explanation:

The maxpause option of the transaction command in Splunk is used to specify the maximum time allowed between events in a transaction. If the time between events exceeds the maxpause value, those events are not considered part of the same transaction.

Splunk Docs: transaction command

Splunk Answers: maxpause option in transaction

Question 2

Question Type: **MultipleChoice**

A Splunk app is configured to extract domain names in web service logs and specify them as a field named domain.

What workflow action would return an external IP lookup for the field named domain?

Options:

A- POST

B- PUT

C- GET

D- Search

Answer:

C

Explanation:

In Splunk, a workflow action that returns an external IP lookup for a field named domain would typically use the GET method. This HTTP method is used to retrieve data from a specified resource, which is appropriate for looking up information based on the domain field.

Splunk Docs: Define workflow actions

Splunk Answers: Workflow actions for external lookups

Question 3

Question Type: MultipleChoice

When using multiple expressions in a single eval command, which delimiter is used?

Options:

A- , (comma)

B- I (pipe)

C- / (forward slash)

D- : (colon)

Answer:

A

Explanation:

When using multiple expressions in a single eval command in Splunk, the delimiter used is a comma (,). This allows for the execution of multiple operations within a single eval statement, separating each operation clearly.

Splunk Docs: Eval command

Splunk Answers: Multiple expressions in eval

Question 4

Question Type: **MultipleChoice**

When creating an event type, which is allowed in the search string?

Options:

A- Tags

B- Joins

C- Subsearches

D- Pipes

Answer:

C

Explanation:

When creating an event type in Splunk, subsearches are allowed in the search string. Subsearches enable users to perform a secondary search whose results are used as input for the main search. This functionality is useful for more complex event type definitions that require additional filtering or criteria based on another search.

Splunk Docs: About subsearches

Splunk Docs: Event type creation

Splunk Answers: Using subsearches in event types

Question 5

Question Type: MultipleChoice

What is the purpose of a calculated field?

Options:

A- To automatically add fields to the index using an eval expression rather than manually including an eval command.

B- To manually add and remove fields at search time related to statistical functions.

C- To automatically add fields at search time using an eval expression rather than manually including an eval command.

D- To manually add fields at search time and check for syntax errors.

Answer:

C

Explanation:

A calculated field in Splunk is designed to automatically add fields at search time using an eval expression. This feature allows users to define new fields based on existing data without needing to manually include an eval command in every search. Calculated fields simplify repeated search tasks by embedding the eval logic directly into the field configuration.

Splunk Docs: Calculated fields

Splunk Answers: Purpose of calculated fields

Question 6

Question Type: MultipleChoice

When using the Field Extractor (FX) to perform a field extraction, which delimiter can be used?

Options:

A- A period or comma.

B- A comma.

C- A tab or space.

D- Any consistent character.

Answer:

D

Explanation:

When using the Field Extractor (FX) in Splunk to perform field extraction, any consistent character can be used as a delimiter. The Field Extractor allows users to define how fields are separated in the raw event data, and as long as the delimiter is consistent, the FX tool can parse and extract the fields correctly.

Splunk Docs: Field Extractor

Splunk Answers: Field extraction delimiters