Free Questions for SPLK-1004 by actualtestdumps

Shared by Phelps on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What default Splunk role can use the Log Event alert action?

Options:

A- Power

B- User

C- can_delete

D- Admin

Answer:

D

Explanation:

In Splunk, the Admin role (Option D) has the capability to use the Log Event alert action among many other administrative privileges. The Log Event alert action allows Splunk to create an event in an index based on the triggering of an alert, providing a way to log and track alert occurrences over time. The Admin role typically encompasses a wide range of permissions, including the ability to configure

and manage alert actions.

Question 2

Question Type: MultipleChoice

When using a nested search macro, how can an argument value be passed to the inner macro?

Options:

A- The argument value may be passed to the outer macro.

B- An argument cannot be used with an inner nested macro.

C- An argument cannot be used with an outer nested macro.

D- The argument value must be specified in the outer macro.

Answer:

A

Explanation:

When using a nested search macro in Splunk, an argument value can be passed to the inner macro by specifying the argument in the outer macro's invocation (Option A). This allows the outer macro to accept arguments from the user or another search command and then pass those arguments into the inner macro, enabling dynamic and flexible macro compositions that can adapt based on input parameters.

Question 3

Question Type: MultipleChoice

What does the query | makeresults generate?

Options:

A- A timestamp

B- A results field

C- An error message

D- The results of the previously run search.

Answer:

B

Explanation:

The | makeresults command in Splunk generates a single event containing default fields, with the primary purpose of creating sample data or a placeholder event for testing and development purposes. The most notable field it generates is _time, but it does not create a specific 'results' field per se. However, it's commonly used to create a base event for further manipulation with eval or other commands in search queries for demonstration, testing, or constructing specific scenarios.

Question 4

Question Type: MultipleChoice

When running a search, which Splunk component retrieves the individual results?

Options:

A- Indexer

B- Search head

C- Universal forwarder

D- Master node

Answer:

B

Explanation:

The Search head (Option B) in Splunk architecture is responsible for initiating and coordinating search activities across a distributed environment. When a search is run, the search head parses the search query, distributes the search tasks to the appropriate indexers (which hold the actual data), and then consolidates the results retrieved by the indexers. The search head is the component that interacts with the user, presenting the final search results

Question 5

Question Type: MultipleChoice

What type of drilldown passes a value from a user click into another dashboard or external page?

Options:

A- Visualization

B- Event

C- Dynamic

D- Contextual

Answer:

D

Explanation:

Contextual drilldown (Option D) is the type of drilldown that allows passing a value from a user click (e.g., from a table row or chart element) into another dashboard or an external page. This feature enables the creation of interactive dashboards where clicking on a specific element dynamically updates another part of the dashboard or navigates to a different page with relevant information, using the clicked value as a context for the subsequent view.

Question 6

Question Type: MultipleChoice

What order of incoming events must be supplied to the transaction command to ensure correct results?

Options:

A- Reverse lexicographical order

B- Ascending lexicographical order

C- Ascending chronological order

D- Reverse chronological order

Answer:

C

Explanation:

The transaction command in Splunk groups events into transactions based on common fields or characteristics. For the transaction command to function correctly and group events into meaningful transactions, the incoming events must be supplied in ascending chronological order (Option C). This ensures that related events are sequenced correctly according to their occurrence over time, allowing for accurate transaction grouping and analysis