SPLK-1001 Q&As

Splunk Core Certified User

Pass Splunk SPLK-1001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/splk-1001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

QUESTION 1

Which of the following statements are correct about Search and Reporting App? (Choose three.)

A. Can be accessed by Apps > Search and Reporting.

B. Provides default interface for searching and analyzing logs.

C. Enables the user to create knowledge object, reports, alerts and dashboards.

D. It only gives us search functionality.

Correct Answer: ABC

QUESTION 2

At the time of searching the start time is 03:35:08. Will it look back to 03:00:00 if we use -30m@h in searching?

A. Yes

B. No

Correct Answer: A

QUESTION 3

Which of the statements is correct regarding click and drag option in timeline?

A. The new result after selecting the range by dragging filters the events and displays the most recent first.

B. There is no functionality like click and drag in Splunk\\'s timeline.

C. Using this option executes a new query.

D. This doesn\\'t execute a new query

Correct Answer: A

QUESTION 4

In a deployment with multiple indexes, what will happen when a search is run and an index is not specified in the search string?

A. No events will be returned.

B. Splunk will prompt you to specify an index.

C. All non-indexed events to which the user has access will be returned.

D. Events from every index searched by default to which the user has access will be returned.

Correct Answer: D

QUESTION 5

Which of the following Splunk components typically resides on the machines where data originates?

A. Indexer

B. Forwarder

C. Search head

D. Deployment server

Correct Answer: B

QUESTION 6

What happens when a field is added to the Selected Fields list in the fields sidebar\\'?

A. Splunk will re-run the search job in Verbose Mode to prioritize the new Selected Field

B. Splunk will highlight related fields as a suggestion to add them to the Selected Fields list.

C. Custom selections will replace the Interesting Fields that Splunk populated into the list at search time

D. The selected field and its corresponding values will appear underneath the events in the search results

Correct Answer: D

QUESTION 7

Splunk automatically determines the source type for major data types.

A. False

B. True

Correct Answer: B

QUESTION 8

When is the pipe character, I, used in search strings?

A. Before clauses. For example: stats sum(bytes) | by host

B. Before commands. For example: | stats sum(bytes) by host

C. Before arguments. For example: stats sum| (bytes) by host

D. Before functions. For example: stats |sum(bytes) by host

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Aboutsearchlanguagesyntax#Quotes_and_escaping_characters

QUESTION 9

Beginning parentheses is automatically highlighted to guide you on the presence of complimenting parentheses.

A. No

B. Yes

Correct Answer: B

QUESTION 10

Matching search terms are highlighted.

A. Yes

B. No

Correct Answer: A

QUESTION 11

After running a search, what effect does clicking and dragging across the timeline have?

A. Executes a new search.

B. Filters current search results.

C. Moves to past or future events.

D. Expands the time range of the search.

Correct Answer: B

QUESTION 12

The stats command will create a _____ by default.

A. Table

B. Report

C. Pie chart

Correct Answer: A

QUESTION 13

When editing a dashboard, which of the following are possible options? (select all that apply)

A. Add an output.

B. Export a dashboard panel.

C. Modify the chart type displayed in a dashboard panel.

D. Drag a dashboard panel to a different location on the dashboard.

Correct Answer: CD

QUESTION 14

Which command automatically returns percent and count columns when executing searches?

A. top

B. stats

C. table

D. percent

Correct Answer: A

QUESTION 15

Zoom Out and Zoom to Selection re-executes the search.

A. No

B. Yes

Correct Answer: B