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.pass4itsure.com/splk-1001.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Search Assistant is enabled by default in the SPL editor with compact settings.

A. No

B. Yes

Correct Answer: B

QUESTION 2

What can be configured using the Edit Job Settings menu?

A. Export the results to CSV format

B. Add the Job results to a dashboard

C. Schedule the Job to re-run in 10 minutes

D. Change Job Lifetime from 10 minutes to 7 days.

Correct Answer: D

QUESTION 3

Portal for Splunk apps can be accessed through www.splunkbase.com

A. False

B. True

Correct Answer: B

QUESTION 4

Select the statements that are true for timeline in Splunk (Choose four.):

A. Timeline shows distribution of events specified in the time range in the form of bars.

B. Single click to see the result for particular time period.

C. You can click and drag across the bar for selecting the range.

D. This is default view and you can\\'t make any changes to it.

E. You can hover your mouse for details like total events, time and date.

Correct Answer: ABCE

QUESTION 5

When sorting on multiple fields with the sort command, what delimiter can be used between the field names in the search?

A. |

B. $

C. !

D. ,

Correct Answer: D

QUESTION 6

In the Fields sidebar, what does the number directly to the right of the field name indicate?

A. The value of the field

B. The number of values for the field

C. The number of unique values for the field

D. The numeric non-unique values of the field

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/SearchTutorial/Usefieldstosearch

QUESTION 7

Which search string only returns events from hostWWW3?

A. B. host=WWW3

B. C. host=WWW*

C. D. Host=WWW3

Correct Answer: B

QUESTION 8

When displaying results of a search, which of the following is true about line charts?

A. Line charts are optimal for single and multiple series.

B. Line charts are optimal for single series when using Fast mode.

C. Line charts are optimal for multiple series with 3 or more columns.

D. Line charts are optimal for multiseries searches with at least 2 or more columns.

Correct Answer: C

QUESTION 9

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

A. Rex

B. As

C. List D. By

Correct Answer: D

QUESTION 10

It is mandatory for the lookup file to have this for an automatic lookup to work.

A. Source type

B. At least five columns

C. Timestamp

D. Input filed

Correct Answer: D

QUESTION 11

Fields are searchable key value pairs in your event data.

A. True

B. False

Correct Answer: A

QUESTION 12

You can view the search result in following format (Choose three.):

A. Table

B. Raw

C. Pie Chart

D. List

Correct Answer: ABD

QUESTION 13

What is one benefit of creating dashboard panels from reports?

A. Any newly created dashboard will include that report.

B. There are no benefits to creating dashboard panels from reports.

C. It makes the dashboard more efficient because it only has to run one search string.

D. Any change to the underlying report will affect every dashboard that utilizes that report.

Correct Answer: C

QUESTION 14

Which Field/Value pair will return only events found in the index named security?

A. Index=Security

B. index=Security

C. Index=security

D. index!=Security

Correct Answer: B

Reference: https://answers.splunk.com/answers/712164/why-are-the-wineventlogssecurity- indexing-indiffe.html

QUESTION 15

What are the two most efficient search filters?

A. _time and host

B. _time and index

C. host and sourcetype

D. index and sourcetype

Correct Answer: B

This is the correct answer because these two filters can help you limit the amount of data that Splunk retrieves from disk, which is the key to fast searching1. The _time filter allows you to specify a narrow time window for your search, which reduces the number of buckets that Splunk scans2. The index filter allows you to specify which index or indexes contain the data that you want to search, which reduces the number of files that Splunk reads3.