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.certbus.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 constraints can be used with the top command?

A. limit

B. useperc

C. addtotals

D. fieldcount

Correct Answer: A

QUESTION 2

What will always appear in the Selected Fields list?

A. index

B. action

C. clientip

D. sourcetype

Correct Answer: D

QUESTION 3

_____ is the default web port used by Splunk.

A. 8089

B. 8000

C. 8080

D. 443

Correct Answer: B

QUESTION 4

This is what Splunk uses to categorize the data that is being indexed.

A. Host

B. Sourcetype

C. Index

D. Source

Correct Answer: B

QUESTION 5

Which of the following statements about case sensitivity is true?

A. Both field names and field values ARE case sensitive.

B. Field names ARE case sensitive; field values are NOT.

C. Field values ARE case sensitive; field names ARE NOT.

D. Both field names and field values ARE NOT case sensitive.

Correct Answer: B

QUESTION 6

Keywords are highlighted when you mouse over search results and you can click this search result to (Choose three.):

A. Open new search.

B. Exclude the item from search.

C. None of the above.

D. Add the item to search

Correct Answer: ABD

QUESTION 7

Which of the following is the most efficient filter for running searches in Splunk?

A. Time

B. Fast mode

C. Sourcetype

D. Selected Fields

Correct Answer: A

QUESTION 8

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 9

What are the steps to schedule a report?

A. After saving the report, click Schedule.

B. After saving the report, click Event Type.

C. After saving the report, click Scheduling.

D. After saving the report, click Dashboard Panel.

Correct Answer: A

QUESTION 10

Which statement is true about Splunk alerts?

A. Alerts are based on searches that are either run on a scheduled interval or in real-time.

B. Alerts are based on searches and when triggered will only send an email notification.

C. Alerts are based on searches and require cron to run on scheduled interval.

D. Alerts are based on searches that are run exclusively as real-time.

Correct Answer: A

QUESTION 11

Which of the following fields is stored with the events in the index?

A. user

B. source

C. location

D. sourcelp

Correct Answer: B

QUESTION 12

It is no possible for a single instance of Splunk to manage the input, parsing and indexing of machine data.

A. True

B. False

Correct Answer: B

QUESTION 13

Following are the time selection option while making search:

(Choose all that apply.)

A. Date and Time Range

B. Advanced

C. Date Range

D. Presets

E. Relative

Correct Answer: B

QUESTION 14

Prefix wildcards might cause performance issues.

A. False

B. True

Correct Answer: B

QUESTION 15

When looking at a dashboard panel that is based on a report, which of the following is true?

A. You can modify the search string in the panel, and you can change and configure the visualization.

B. You can modify the search string in the panel, but you cannot change and configure the visualization.

C. You cannot modify the search string in the panel, but you can change and configure the visualization.

D. You cannot modify the search string in the panel, and you cannot change and configure the visualization.

Correct Answer: C

When looking at a dashboard panel that is based on a report, you cannot modify the search string in the panel, but you can change and configure the visualization. This is because the dashboard panel inherits the search string from the report, and any changes to the search string will affect the report as well. However, you can customize the visualization settings for the dashboard panel without affecting the report. References: Splunk Core User Certification Exam Study Guide, page 37.