SPLK-1001^Q&As^

Splunk Core Certified User

Pass Splunk SPLK-1001 Exam with 100% Guarantee

QUESTION 1

The stats command will create a _____________ by default.

A. Table

B. Report

C. Pie chart

Correct Answer: A

QUESTION 2

Splunk index time process can be broken down into __________ phases.

A. 3

B. 2

C. 4

D. 1

Correct Answer: A

QUESTION 3

Lookups allow you to overwrite your raw event.

A. True

B. False

Correct Answer: A

QUESTION 4

In the fields sidebar, which character denotes alphanumeric field values?

A. #

B. %

C. a

D. a#

Correct Answer: B

QUESTION 5

Parsing of data can happen both in HF and UF.

A. Yes

B. No

Correct Answer: B

QUESTION 6

How many main user roles do you have in Splunk?

A. 2

B. 4

C. 1

D. 3

Correct Answer: D

QUESTION 7

You can also specify a time range in the search bar. You can use the following for beginning and ending for a time range (Choose two.):

A. Not possible to specify time manually in Search query

B. end=

C. start=

D. earliest=

E. latest=

Correct Answer: DE

QUESTION 8

By default, how long does Splunk retain a search job?

A. 10 Minutes

B. 15 Minutes

C. 1 Day

D. 7 Days

Correct Answer: A

QUESTION 9

Which of the following is an accurate definition of fields within Splunk?

A. Inherent entities that exist in event data.

B. A searchable key/value pair in event data.

C. Values pulled exclusively from lookup tables.

D. A non-searchable name/value pair used while indexing data.

Correct Answer: A

Fields are searchable key/value pairs in event data. They allow you to specify criteria for your searches and filter out unwanted events. Fields can be extracted automatically by Splunk software during indexing or searching, or manually by users using various methods. Fields are not inherent entities that exist in event data, but rather interpretations of data by Splunk software or users. Fields are not values pulled exclusively from lookup tables, although lookup tables can be used to add fields to events based on existing fields. Fields are not non-searchable name/value pairs used while indexing data, but rather searchable attributes that can be used to refine searches5.

QUESTION 10

Selected fields are a set of configurable fields displayed for each event.

A. True

B. False

Correct Answer: A

QUESTION 11

Which of the following commands will show the maximum bytes?

A. sourcetype=access_* | maximum totals by bytes

B. sourcetype=access_* | avg (bytes)

C. sourcetype=access_* | stats max(bytes)

D. sourcetype=access_* | max(bytes)

Correct Answer: C

QUESTION 12

What will always appear in the Selected Fields list?

A. index

B. action

C. clientip

D. sourcetype

Correct Answer: D

QUESTION 13

Splunk Components:

Which of the following are responsible for parsing incoming data and storing data on disc?

A. forwarders

B. indexers

C. search heads

Correct Answer: B

QUESTION 14

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

QUESTION 15

Data summary button just below the search bar gives you the following (Choose three.):

A. Hosts

B. Sourcetypes

C. Sources

D. Indexes

Correct Answer: ABD