Vendor: Splunk

Exam Code:SPLK-1001

Exam Name: Splunk Core Certified User

Version: Demo

QUESTION 1

Which search would return events from the access_combined sourcetype?

A. Sourcetype=access_combined

B. Sourcetype=Access_Combined

C. sourcetype=Access_Combined

D. SOURCETYPE=access_combined

Correct Answer: C

QUESTION 2

Which command is used to validate a lookup file?

A. | lookup products.csv

B. inputlookup products.csv

C. I inputlookup products.csv

D. | lookup definition products.csv

Correct Answer: C

QUESTION 3

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 4

This function of the stats command allows you to return the sample standard deviation of a field.

A. stdev

B. dev

C. count deviation

D. by standarddev

Correct Answer: A

QUESTION 5

What is the primary use for the rare command?

A. To sort field values in descending order.

B. To return only fields containing five of fewer values.

C. To find the least common values of a field in a dataset.

D. To find the fields with the fewest number of values across a dataset.

Correct Answer: C

QUESTION 6

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

A. No

B. Yes

Correct Answer: B

QUESTION 7

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 8

Which statement is true about the top command?

A. It returns the top 10 results

B. It displays the output in table format

C. It returns the count and percent columns per row

D. All of the above

Correct Answer: D

QUESTION 9

Documentations for Splunk can be found at docs.splunk.com

A. True

B. False

Correct Answer: A

QUESTION 10

Which is a primary function of the timeline located under the search bar?

A. To differentiate between structured and unstructured events in the data

B. To sort the events returned by the search command in chronological order

C. To zoom in and zoom out. although this does not change the scale of the chart

D. To show peaks and/or valleys in the timeline, which can indicate spikes in activity or downtime

Correct Answer: D

QUESTION 11

Splunk internal fields contains general information about events and starts from underscore i.e. _ .

A. True

B. False

Correct Answer: A

QUESTION 12

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