SPLK-1001 Q&As

Splunk Core Certified User

Pass Splunk SPLK-1001 Exam with 100% Guarantee

QUESTION 1

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 2

Three basic components of Splunk are (Choose three.):

A. Forwarders

B. Deployment Server

C. Indexer

D. Knowledge Objects

E. Index

F. Search Head

Correct Answer: ACF

QUESTION 3

Where does Licensing meter happen?

A. Indexer

B. Parsing

C. Heavy Forwarder

D. Input

Correct Answer: A

QUESTION 4

The default host name used in Inputs general settings can not be changed.

A. False

B. True

Correct Answer: A

QUESTION 5

What is a quick, comprehensive way to learn what data is present in a Splunk deployment?

A. Review Splunk reports

B. Run ./splunk show

C. Click Data Summary in Splunk Web

D. Search index=* sourcetype=* host=*

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/InheritedDeployment/Yourdata

QUESTION 6

By default, all users have DELETE permission to ALL knowledge objects.

A. True

B. False

Correct Answer: B

QUESTION 7

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

QUESTION 8

What is Search Assistant in Splunk?

A. It is only available to Admins.

B. Such feature does not exist in Splunk.

C. Shows options to complete the search string

Correct Answer: C

QUESTION 9

Which of the following reports is available in the Fields window?

A. Top values by time

B. Rare values by time

C. Events with top value fields

D. Events with rare value fields

Correct Answer: C

QUESTION 10

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 11

What is the purpose of using a by clause with the stats command?

A. To group the results by one or more fields.

B. To compute numerical statistics on each field.

C. To specify how the values in a list are delimited.

D. To partition the input data based on the split-by fields.

Correct Answer: A

QUESTION 12

Clicking a SEGMENT on a chart, ________.

A. drills down for that value

B. highlights the field value across the chart

C. adds the highlighted value to the search criteria

Correct Answer: C

QUESTION 13

When a Splunk search generates calculated data that appears in the Statistics tab. in what formats can the results be exported?

A. CSV, JSON, PDF

B. CSV, XML JSON

C. Raw Events, XML, JSON

D. Raw Events, CSV, XML, JSON

Correct Answer: D

QUESTION 14

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 15

Which events will be returned by the following search string? host=www3 status=503

A. All events that either have a host of www3 or a status of 503.

B. All events with a host of www3 that also have a status of 503

C. We need more information: we cannot tell without knowing the time range

D. We need more information a search cannot be run without specifying an index

Correct Answer: B