

Splunk

Exam Questions SPLK-1001

Splunk Core Certified User Exam



NEW QUESTION 1

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.

Answer: C

NEW QUESTION 2

Which of the following is true about user account settings and preferences?

- A. Search & Reporting is the only app that can be set as the default application.
- B. Full names can only be changed by accounts with a Power User or Admin role.
- C. Time zones are automatically updated based on the setting of the computer accessing Splunk.
- D. Full name, time zone, and default app can be defined by clicking the login name in the Splunk bar.

Answer: B

NEW QUESTION 3

What must be done in order to use a lookup table in Splunk?

- A. The lookup must be configured to run automatically.
- B. The contents of the lookup file must be copied and pasted into the search bar.
- C. The lookup file must be uploaded to Splunk and a lookup definition must be created.
- D. The lookup file must be uploaded to the etc/apps/lookups folder for automatic ingestion.

Answer: C

NEW QUESTION 4

Which stats command function provides a count of how many unique values exist for a given field in the result set?

- A. dc(field)
- B. count(field)
- C. count-by(field)
- D. distinct-count(field)

Answer: A

NEW QUESTION 5

A collection of items containing things such as data inputs, UI elements, and knowledge objects is known as what?

- A. An app
- B. JSON
- C. A role
- D. An enhanced solution

Answer: A

NEW QUESTION 6

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.

Answer: A

NEW QUESTION 7

What is the main requirement for creating visualizations using the Splunk UI?

- A. Your search must transform event data into Excel file format first.
- B. Your search must transform event data into XML formatted data first.
- C. Your search must transform event data into statistical data tables first.
- D. Your search must transform event data into JSON formatted data first.

Answer: B

NEW QUESTION 8

What type of search can be saved as a report?

- A. Any search can be saved as a report.
- B. Only searches that generate visualizations.
- C. Only searches containing a transforming command.
- D. Only searches that generate statistics or visualizations.

Answer: A

NEW QUESTION 9

When viewing the results of a search, what is an Interesting Field?

- A. A field that appears in any event.
- B. A field that appears in every event.
- C. A field that appears in the top 10 events.
- D. A field that appears in at least 20% of the events.

Answer: D

NEW QUESTION 10

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

Answer: B

NEW QUESTION 10

Which is 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.

Answer: D

NEW QUESTION 15

What happens when a field is added to the Selected Fields list in the fields sidebar?

- A. Splunk will re-run the search job in Verbose Mode to prioritize the new Selected Field.
- B. Splunk will highlight related fields as a suggestion to add them to the Selected Fields list.
- C. Custom selections will replace the Interesting Fields that Splunk populated into the list at search time.
- D. The selected field and its corresponding values will appear underneath the events in the search results.

Answer: D

NEW QUESTION 20

What is Splunk?

- A. Splunk is a software platform to search, analyze and visualize the machine-generated data.
- B. Database management tool.
- C. Security Information and Event Management (SIEM).
- D. Cloud based application that help in analyzing logs.

Answer: A

NEW QUESTION 23

Splunk Enterprise is used as a Scalable service in Splunk Cloud.

- A. True
- B. False

Answer: A

NEW QUESTION 26

Which component of Splunk let us write SPL query to find the required data?

- A. Forwarders
- B. Indexer
- C. Heavy Forwarders
- D. Search head

Answer: D

NEW QUESTION 31

Log filtering/parsing can be done from _____.

- A. Index Forwarders (IF)
- B. Universal Forwarders (UF)
- C. Super Forwarder (SF)
- D. Heavy Forwarders (HF)

Answer: D

NEW QUESTION 33

Which is the default app for Splunk Enterprise?

- A. Splunk Enterprise Security Suite
- B. Searching and Reporting
- C. Reporting and Searching
- D. Splunk apps for Security

Answer: B

NEW QUESTION 38

What result will you get with following search index=test sourcetype="The_Questionnaire_P*" ?

- A. the_questionnaire _pedia
- B. the_questionnaire pedia
- C. the_questionnaire_pedia
- D. the_questionnaire Pedia

Answer: C

NEW QUESTION 39

You can on-board data to Splunk using following means (Choose four.):

- A. Props
- B. CLI
- C. Splunk Web
- D. savedsearches.conf
- E. Splunk apps and add-ons
- F. indexes.conf
- G. inputs.conf
- H. metadata.conf

Answer: BCEG

NEW QUESTION 40

Data sources being opened and read applies to:

- A. None of the above
- B. Indexing Phase
- C. Parsing Phase
- D. Input Phase
- E. License Metering

Answer: D

NEW QUESTION 43

Select the correct option that applies to Index time processing (Choose three.).

- A. Indexing
- B. Searching
- C. Parsing
- D. Settings
- E. Input

Answer: ACE

NEW QUESTION 45

Upload option creates inputs.conf

- A. Yes
- B. No

Answer: B

NEW QUESTION 49

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

- A. 3
- B. 2
- C. 4
- D. 1

Answer: A

NEW QUESTION 54

In monitor option you can select the following options in GUI.

- A. Only HTTP Event Collector (HEC) and TCP/UDP
- B. None of the above
- C. Only TCP/UDP
- D. Only Scripts
- E. Filed & Directories, HTTP Event Collector (HEC), TCP/UDP and Scripts

Answer: E

NEW QUESTION 58

Which of the statements are correct about HF? (Choose three.)

- A. Parsing
- B. Masking
- C. Searching
- D. Forwarding

Answer: ABD

NEW QUESTION 60

Where does Licensing meter happen?

- A. Indexer
- B. Parsing
- C. Heavy Forwarder
- D. Input

Answer: A

NEW QUESTION 63

Matching search terms are highlighted.

- A. Yes
- B. No

Answer: A

NEW QUESTION 68

Splunk Parses data into individual events, extracts time, and assigns metadata.

- A. False
- B. True

Answer: B

NEW QUESTION 70

Which symbol is used to snap the time?

- A. @
- B. &
- C. *
- D. #

Answer: A

NEW QUESTION 73

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SPLK-1001 Practice Exam Features:

- * SPLK-1001 Questions and Answers Updated Frequently
- * SPLK-1001 Practice Questions Verified by Expert Senior Certified Staff
- * SPLK-1001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SPLK-1001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SPLK-1001 Practice Test Here](#)