

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 is a primary function of a scheduled report?

- A. Auto-detect changes in performance.
- B. Auto-generated PDF reports of overall data trends.
- C. Regularly scheduled archiving to keep disk space use low.
- D. Triggering an alert in your Splunk instance when certain conditions are met.

Answer: D

NEW QUESTION 4

Which command is used to review the contents of a specified static lookup file?

- A. lookup
- B. csvlookup
- C. inputlookup
- D. outputlookup

Answer: C

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

How do you add or remove fields from search results?

- A. Use field +to add and field -to remove.
- B. Use table +to add and table -to remove.
- C. Use fields +to add and fields -to remove.
- D. Use fields Plus to add and fields Minus to remove.

Answer: C

NEW QUESTION 8

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

- A. #
- B. %
- C. a
- D. a#

Answer: B

NEW QUESTION 9

What syntax is used to link key/value pairs in search strings?

- A. action+purchase
- B. action=purchase
- C. action | purchase
- D. action equal purchase

Answer: B

NEW QUESTION 10

When placed early in a search, which command is most effective at reducing search execution time?

- A. dedup
- B. rename
- C. sort -
- D. fields +

Answer: A

NEW QUESTION 10

Which of the following is a best practice when writing a search string?

- A. Include all formatting commands before any search terms.
- B. Include at least one function as this is a search requirement.
- C. Include the search terms at the beginning of the search string.
- D. Avoid using formatting clauses, as they add too much overhead.

Answer: D

NEW QUESTION 13

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 16

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 18

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

- A. user
- B. source
- C. location
- D. sourceip

Answer: B

NEW QUESTION 22

Which of the following is the recommended way to create multiple dashboards displaying data from the same search?

- A. Save the search as a report and use it in multiple dashboards as needed.
- B. Save the search as a dashboard panel for each dashboard that needs the data.
- C. Save the search as a scheduled alert and use it in multiple dashboards as needed.
- D. Export the results of the search to an XML file and use the file as the basis of the dashboards.

Answer: D

NEW QUESTION 23

What does the following specified time range do?
earliest=-72h@h latest=@d

- A. Look back 3 days ago and prior.
- B. Look back 72 hours, up to one day ago.
- C. Look back 72 hours, up to the end of today.
- D. Look back from 3 days ago, up to the beginning of today.

Answer: C

NEW QUESTION 27

What can be configured using the Edit Job Settings menu?

- A. Export the result to CSV format.
- B. Add the Job results to a dashboard.
- C. Schedule the Job to re-run in 10 minutes.
- D. Change Job Lifetime from 10 minutes to 7 days.

Answer: B

NEW QUESTION 31

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 35

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 40

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 43

Forward Option gather and forward data to indexers over a receiving port from remote machines.

- A. False
- B. True

Answer: B

NEW QUESTION 45

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 47

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 50

Upload option creates inputs.conf

- A. Yes
- B. No

Answer: B

NEW QUESTION 55

You are able to create new Index in Data Input settings.

- A. No
- B. Yes

Answer: B

NEW QUESTION 57

You can view the search result in following format (Choose three.):

- A. Table
- B. Raw
- C. Pie Chart
- D. List

Answer: ABD

NEW QUESTION 61

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

- A. Hosts
- B. Sourcetypes
- C. Sources
- D. Indexes

Answer: ABC

NEW QUESTION 63

.....

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](#)