

Exam Questions SPLK-1001

Splunk Core Certified User Exam

<https://www.2passeasy.com/dumps/SPLK-1001/>



NEW QUESTION 1

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 2

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 3

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 4

Which of the following searches will return results where fail, 400, and error exist in every event?

- A. error AND (fail AND 400)
- B. error OR (fail and 400)
- C. error AND (fail OR 400)
- D. error OR fail OR 400

Answer: C

NEW QUESTION 5

How does Splunk determine which fields to extract from data?

- A. Splunk only extracts the most interesting data from the last 24 hours.
- B. Splunk only extracts fields users have manually specified in their data.
- C. Splunk automatically extracts any fields that generate interesting visualizations.
- D. Splunk automatically discovers many fields based on sourcetype and key/value pairs found in the data.

Answer: D

NEW QUESTION 6

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 7

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 8

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 9

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 search matches the events containing the terms "error" and "fail"?

- A. index=security Error Fail
- B. index=security error OR fail
- C. index=security "error failure"
- D. index=security NOT error NOT fail

Answer: B

NEW QUESTION 10

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

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

Answer: B

NEW QUESTION 12

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 17

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 22

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.

Answer: B

NEW QUESTION 24

What is the primary use for the rare command?

- A. To sort field values in descending order.
- B. To return only fields containing five or 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.

Answer: C

NEW QUESTION 28

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 32

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

- A. Forwarders
- B. Deployment Server
- C. Indexer
- D. Knowledge Objects
- E. Index
- F. Search Head

Answer: ACF

NEW QUESTION 35

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 39

Splunk shows data in _____ .

- A. ASCII Character order.
- B. Reverse chronological order.
- C. Alphanumeric order.
- D. Chronological order.

Answer: B

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 41

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 43

Upload option creates inputs.conf

- A. Yes
- B. No

Answer: B

NEW QUESTION 46

Where does Licensing meter happen?

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

Answer: A

NEW QUESTION 49

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

- A. False
- B. True

Answer: A

NEW QUESTION 52

There are three different search modes in Splunk (Choose three.):

- A. Automatic
- B. Smart
- C. Fast
- D. Verbose

Answer: BCD

NEW QUESTION 57

Keywords are highlighted when you mouse over search results and you can click this search result to (Choose three.):

- A. Open new search.
- B. Exclude the item from search.
- C. None of the above.
- D. Add the item to search.

Answer: ABD

NEW QUESTION 62

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 67

What options do you get after selecting timeline? (Choose four.)

- A. Zoom to selection
- B. Format Timeline
- C. Deselect
- D. Delete
- E. Zoom Out

Answer: ABCE

NEW QUESTION 71

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-1001 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-1001 Product From:

<https://www.2passeasy.com/dumps/SPLK-1001/>

Money Back Guarantee

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