



Splunk

Exam Questions SPLK-1001

Splunk Core Certified User Exam

NEW QUESTION 1

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 2

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

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

Answer: B

NEW QUESTION 3

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 4

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 5

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 6

What does the stats command do?

- A. Automatically correlates related fields.
- B. Converts field values into numerical values.
- C. Calculates statistics on data that matches the search criteria.
- D. Analyzes numerical fields for their ability to predict another discrete field.

Answer: C

NEW QUESTION 7

How can another user gain access to a saved report?

- A. The owner of the report can edit permissions from the Edit dropdown.
- B. Only users with an Admin or Power User role can access other users' reports.
- C. Anyone can access any reports marked as public within a shared Splunk deployment.
- D. The owner of the report must clone the original report and save it to their user account.

Answer: A

NEW QUESTION 8

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 9

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 10

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 10

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

- A. False
- B. True

Answer: B

NEW QUESTION 11

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. Files & Directories, HTTP Event Collector (HEC), TCP/UDP and Scripts

Answer: E

NEW QUESTION 12

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

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

Answer: ABD

NEW QUESTION 15

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

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

Answer: BCD

NEW QUESTION 17

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 21

.....

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](#)