

Splunk

Exam Questions SPLK-1001

Splunk Core Certified User Exam



NEW QUESTION 1

After running a search, what effect does clicking and dragging across the timeline have?

- A. Executes a new search.
- B. Filters current search results.
- C. Moves to past or future events.
- D. Expands the time range of the search.

Answer: C

NEW QUESTION 2

What does the values function of the stats command do?

- A. Lists all values of a given field.
- B. Lists unique values of a given field.
- C. Returns a count of unique values for a given field.
- D. Returns the number of events that match the search.

Answer: C

NEW QUESTION 3

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 4

Which statement is true about Splunk alerts?

- A. Alerts are based on searches that are either run on a scheduled interval or in real-time.
- B. Alerts are based on searches and when triggered will only send an email notification.
- C. Alerts are based on searches and require cron to run on scheduled interval.
- D. Alerts are based on searches that are run exclusively as real-time.

Answer: A

NEW QUESTION 5

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 6

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

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

Answer: B

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

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 9

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 the most efficient filter for running searches in Splunk?

- A. Time
- B. Fast mode
- C. Sourcetype
- D. Selected Fields

Answer: C

NEW QUESTION 10

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 12

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 17

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 19

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

- A. True
- B. False

Answer: A

NEW QUESTION 20

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 22

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

- A. False
- B. True

Answer: B

NEW QUESTION 27

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 29

Parsing of data can happen both in HF and UF.

- A. Yes
- B. No

Answer: B

NEW QUESTION 32

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

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

Answer: A

NEW QUESTION 36

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

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

Answer: ABD

NEW QUESTION 40

Matching search terms are highlighted.

- A. Yes
- B. No

Answer: A

NEW QUESTION 41

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

- A. False
- B. True

Answer: A

NEW QUESTION 44

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

- A. False
- B. True

Answer: B

NEW QUESTION 49

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

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

Answer: BCD

NEW QUESTION 54

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 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 62

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 64

.....

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](#)