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
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
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 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
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 6
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 7
What user interface component allows for time selection?

A. Time summary
B. Time range picker
C. Search time picker
D. Data source time statistics

Answer: B

NEW QUESTION 8
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 9
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 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 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 15
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
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 25
What is the primary use for the rare command?

A. To sort field values in descending order.
B. To return only fields containing five of 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 29
Splunk Enterprise is used as a Scalable service in Splunk Cloud.

A. True
B. False

Answer: A

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 35
Portal for Splunk apps can be accessed through www.splunkbase.com

A. False
B. True

Answer: B

NEW QUESTION 36
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 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
Parsing of data can happen both in HF and UF.

A. Yes
B. No

Answer: B

NEW QUESTION 45
Upload option creates inputs.conf

A. Yes
B. No

Answer: B

NEW QUESTION 48
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 51
Where does Licensing meter happen?

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

Answer: A

NEW QUESTION 53
Matching search terms are highlighted.

A. Yes
B. No

Answer: A

NEW QUESTION 54
You are able to create new Index in Data Input settings.

A. No
B. Yes

Answer: B

NEW QUESTION 57
Which symbol is used to snap the time?

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

Answer: A

NEW QUESTION 59
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 63
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 66
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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