Exam Questions SPLK-1001

Splunk Core Certified User Exam

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

NEW QUESTION 1
Which of the following is a Splunk search best practice?
Splunk Core Certified User

A. Filter as early as possible.
B. Never specify more than one index.
C. Include as few search terms as possible.
D. Use wildcards to return more search results.

Answer: A

NEW QUESTION 2
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 3
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 4
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 5
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 6
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 7
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 8
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 9
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 10
Portal for Splunk apps can be accessed through www.splunkbase.com

A. False
B. True

Answer: B

NEW QUESTION 10
Splunk shows data in _____ .

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

Answer: B

NEW QUESTION 12
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 15
Data sources being opened and read applies to:

A. None of the above
B. Indexing Phase
C. Parsing Phase
D. Input Phase
E. License Metering

Answer: D

NEW QUESTION 18
Parsing of data can happen both in HF and UF.

A. Yes
B. No

Answer: B

NEW QUESTION 21
Splunk index time process can be broken down into _____ phases.

A. 3
B. 2

C. 4
D. 1

Answer: A

NEW QUESTION 23
You are able to create new Index in Data Input settings.

A. No
B. Yes

Answer: B

NEW QUESTION 28
......

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