Splunk SPLK-1001 Practice Questions

Shared by Williams on 18-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

By default, all users have DELETE permission to ALL knowledge objects.

Options:

A- True
B- False

Answer:

B

Question 2

Question Type: MultipleChoice

When viewing the results of a search, what is an Interesting Field?

Options:

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

Question 3

Question Type: MultipleChoice

Which search string only returns events from hostWWW3?

Options:

A- B. host=WWW3
B- C. host=WWW*
C- D. Host=WWW3

Answer:

B

Question 4

Question Type: MultipleChoice

Which of the following searches would return events with failure in index netfw or warn or critical in index netops?

Options:

A- (index=netfw failure) AND index=netops warn OR critical
B- (index=netfw failure) OR (index=netops (warn OR critical))
C- (index=netfw failure) AND (index=netops (warn OR critical))
D- (index=netfw failure) OR index=netops OR (warn OR critical)

Answer:

B

Question 5

Question Type: MultipleChoice

At index time, in which field does Splunk store the timestamp value?

Options:

A- time
B- _time
C- EventTime
D- timestamp

Answer:

B

Question 6

Question Type: MultipleChoice

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

Options:

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

Answer:

A, B, D

Question 7

Question Type: MultipleChoice

Which of the following represents the Splunk recommended naming convention for dashboards?

Options:

A- Description_Group_Object
B- Group_Description_Object
C- Group_Object_Description
D- Object_Group_Description

Answer:

C

Question 8

Question Type: MultipleChoice

Events in Splunk are automatically segregated using data and time.

Options:

A- Yes
B- No

Answer:

A

Question 9

Question Type: MultipleChoice

A field exists in search results, but isn't being displayed in the fields sidebar. How can it be added to the fields sidebar?

Options:

A- Click All Fields and select the field to add it to Selected Fields.
B- Click Interesting Fields and select the field to add it to Selected Fields.
C- Click Selected Fields and select the field to add it to Interesting Fields.
D- This scenario isn't possible because all fields returned from a search always appear in the fields sidebar.

Answer:

A

Question 10

Question Type: MultipleChoice

What result will you get with following search index=test sourcetype="The_Questionnaire_P*" ?

Options:

A- the_questionnaire _pedia
B- index=security sourcetype=access_* status=200 stats | count by price
C- the_questionnaire_pedia
D- the_questionnaire Pedia

Answer:

C

P2P exams