Leads4Pass

SPLK-1001^{Q&As}

Splunk Core Certified User

Pass Splunk SPLK-1001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/splk-1001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk
Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

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

Correct Answer: A

QUESTION 2

In the Splunk interface, the list of alerts can be filtered based on which characteristics?

A. App, Owner, Severity, and Type

B. App, Owner, Priority, and Status

C. App, Dashboard, Severity, and Type

D. App, Time Window, Type, and Severity

Correct Answer: D

QUESTION 3

Which of the following statements about case sensitivity is true?

A. Both field names and field values ARE case sensitive.

B. Field names ARE case sensitive; field values are NOT.

C. Field values ARE case sensitive; field names ARE NOT.

D. Both field names and field values ARE NOT case sensitive.

Correct Answer: B

QUESTION 4

When is the pipe character, I, used in search strings?

A. Before clauses. For example: stats sum(bytes) | by host

B. Before commands. For example: | stats sum(bytes) by host

C. Before arguments. For example: stats sum| (bytes) by host

D. Before functions. For example: stats |sum(bytes) by host

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/
Aboutsearchlanguagesyntax#Quotes_and_escaping_characters

QUESTION 5

When a search returns _____, you can view the results as a list.

A. a list of events

B. transactions

C. statistical values

Correct Answer: C

[SPLK-1001 PDF Dumps](#)   [SPLK-1001 Study Guide](#)   [SPLK-1001 Braindumps](#)