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

Snapping rounds down to the nearest specified unit.

A. Yes

B. No

Correct Answer: A

QUESTION 2

Will the queries following below get the same result?

1.

 index=log sourcetype=error_log status !=100

2.

 index=log sourcetype=error_log NOT status =100

A. Yes

B. No

Correct Answer: B

QUESTION 3

When is an alert triggered?

A. When Splunk encounters a syntax error in a search

B. When a trigger action meets the predefined conditions

C. When an event in a search matches up with a data model

D. When results of a search meet a specifically defined condition

Correct Answer: D

Reference: https://books.google.com.pk/books?id=sNwkBQAAQBAJandpg=PT525andlpg=PT525anddq=splunk+alert
+triggered+When+results+of+a+search+meet+a+specifically+defined
+conditionandsource=blandots=avtEx5luxoandsig=ACfU3U1ZVob_j9nU243Te2vhqwxI3YvJuAandhl=enandsa=X
andved=2a hUKEwjm48rmkfXoAhUIMewKHb_FAbkQ6AEwB3oECBYQJg

QUESTION 4

Monitor option in Add Data provides _____.

A. Only continuous monitoring.

B. Only One-time monitoring.

C. None of the above.

D. Both One-time and continuous monitoring

Correct Answer: D

QUESTION 5

Matching search terms are highlighted.

A. Yes

B. No

Correct Answer: A

[SPLK-1001 VCE Dumps](#)   [SPLK-1001 Practice Test](#)   [SPLK-1001 Study Guide](#)