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

QUESTION 1

By default, which of the following is a Selected Field?

A. action

B. clientip

C. categoryId

D. sourcetype

Correct Answer: D

QUESTION 2

Which search string returns a filed containing the number of matching events and names that field Event Count?

A. index=security failure | stats sum as "Event Count"

B. index=security failure | stats count as "Event Count"

C. index=security failure | stats count by "Event Count"

D. index=security failure | stats dc(count) as "Event Count"

Correct Answer: B

QUESTION 3

What kind of logs can Splunk Index?

A. Only A, B

B. Router and Switch Logs

C. Firewall and Web Server Logs

D. Only C

E. Database logs

F. All firewall, web server, database, router and switch logs

Correct Answer: F

QUESTION 4

Which command is used to review the contents of a specified static lookup file?

A. lookup

B. csvlookup

C. inputlookup

D. outputlookup

Correct Answer: C

QUESTION 5

What is the correct syntax to count the number of events containing a vendor_action field?

A. count stats vendor_action

B. count stats (vendor_action)

C. stats count (vendor_action)

D. stats vendor_action (count)

Correct Answer: C