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.pass4itsure.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

Splunk shows data in _____.

A. ASCII Character order.

B. Reverse chronological order.

C. Alphanumeric order.

D. Chronological order.

Correct Answer: B

QUESTION 2

This function of the stats command allows you to return the middle-most value of field X.

A. Median(X)

B. Eval by X

C. Fields(X)

D. Values(X)

Correct Answer: A

QUESTION 3

Given the following SPL search, how many rows of results would you expect to be returned by default? index=security sourcetype=linux_secure (fail* OR invalid) I top src__ip

A. 10

B. 50

C. 100

D. 20

Correct Answer: A

The SPL search specified above will return 10 rows of results by default, as the "top" command specifies a limit of 10 results. The query will search for all events in the security index with a sourcetype of linuxsecure that contain either the terms fail* or invalid and will display the top 10 results according to the src_ip field.

QUESTION 4

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

QUESTION 5

When an alert action is configured to run a script, Splunk must be able to locate the script. Which is one of the directories Splunk will look in to find the script?

A. $SPLUNK_HOME/bin/scripts

B. $SPLUNK_HOME/etc/scripts

C. $SPLUNK_HOME/bin/etc/scripts

D. $SPLUNK_HOME/etc/scripts/bin

Correct Answer: A