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

In the fields sidebar, which character denotes alphanumeric field values?

A. #

B. %

C. a

D. a#

Correct Answer: B

QUESTION 2

When refining search results, what is the difference in the time picker between real-time and relative time ranges?

A. Real-time searches happen instantly, while relative searches happen at a scheduled time.

B. Real-time searches display results from a rolling time window, while relative searches display results from a set length of time.

C. Real-time searches run constantly in the background, while relative searches only run when certain criteria are met.

D. Real-time represents events that have happened in a set time window, while relative will display results from a rolling time window.

Correct Answer: B

The difference between real-time and relative time ranges in the time picker is that real-time searches display results from a rolling time window, such as the last 15 minutes, while relative searches display results from a set length of time, such as yesterday or last week. Real-time searches do not happen instantly, but rather update periodically based on the refresh interval. Relative searches do not happen at a scheduled time, but rather when the user runs them. Real-time searches do not run constantly in the background, but rather when the user starts them. Real-time searches do not represent events that have happened in a set time window, but rather events that are happening now.

QUESTION 3

Which is the default app for Splunk Enterprise?

A. Splunk Enterprise Security Suite

B. Searching and Reporting

C. Reporting and Searching

D. Splunk apps for Security

Correct Answer: B

QUESTION 4

Which of the following are common constraints of the top command?

A. limit, count

B. limit, showpercent

C. limits, countfield

D. showperc, countfield

Correct Answer: B

QUESTION 5

Which of the following are Splunk premium enhanced solutions? (Choose three.)

A. Splunk User Behavior Analytics (UBA)

B. Splunk IT Service Intelligence (ITSI)

C. Splunk Enterprise Security (ES)

D. Splunk Analytics Security (AS)

Correct Answer: ABC