SPLK-1003Q&As

Splunk Enterprise Certified Admin

Pass Splunk SPLK-1003 Exam with 100% Guarantee

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

https://www.pass2lead.com/splk-1003.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

Which feature in Splunk allows Event Breaking, Timestamp extractions, and any advanced configurations found in props.conf to be validated all through the UI?

A. Apps

B. Search

C. Data preview

D. Forwarder inputs

Correct Answer: C

http://www.splunk.com/view/SP-CAAAGPR

QUESTION 2

What hardware attribute would need to be changed to increase the number of simultaneous searches (ad-hoc and scheduled) on a single search head?

A. Disk

B. CPUs

C. Memory

D. Network interface cards

Correct Answer: B

https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/SHCarchitecture Scroll down to section titled, How the cluster handles concurrent search quotas, "Overall search quota. This quota determines the maximum number of historical searches (combined scheduled and ad hoc) that the cluster can run concurrently. This quota is configured with max_Searches_per_cpu and related settings in limits.conf."

QUESTION 3

A log file contains 193 days worth of timestamped events. Which monitor stanza would be used to collect data 45 days old and newer from that log file?

A. followTail = -45d

B. ignore = 45d

C. includeNewerThan = 45d

D. ignoreOlderThan = 45d

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/8.2.1/Data/Configuretimestamprecognition

QUESTION 4

How do you remove missing forwarders from the Monitoring Console?

A. By restarting Splunk.

B. By rescanning active forwarders.

C. By reloading the deployment server.

D. By rebuilding the forwarder asset table.

Correct Answer: D

QUESTION 5

Which of the following is accurate regarding the input phase?

A. Breaks data into events with timestamps.

B. Applies event-level transformations.

C. Fine-tunes metadata.

D. Performs character encoding.

Correct Answer: D

"The data pipeline segments in depth. INPUT - In the input segment, Splunk software consumes data. It acquires the raw data stream from its source, breaks it into 64K blocks, and annotates each block with some metadata keys. The keys can also include values that are used internally, such as the character encoding of the data stream, and values that control later processing of the data, such as the index into which the events should be stored. PARSING Annotating individual events with metadata copied from the source-wide keys. Transforming event data and metadata according to regex transform rules."