SPLK-2002 Q&As

Splunk Enterprise Certified Architect

Pass Splunk SPLK-2002 Exam with 100% Guarantee

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

https://www.pass4itsure.com/splk-2002.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

When troubleshooting monitor inputs, which command checks the status of the tailed files?

A. splunk cmd btool inputs list | tail

B. splunk cmd btool check inputs layer

C. curl https://serverhost:8089/services/admin/inputstatus/TailingProcessor:FileStatus

D. curl https://serverhost:8089/services/admin/inputstatus/TailingProcessor:Tailstatus

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Troubleshoottheinputprocess#Troubleshoot_your_tailed_files

QUESTION 2

Which component in the splunkd.log will log information related to bad event breaking?

A. Audittrail

B. EventBreaking

C. IndexingPipeline

D. AggregatorMiningProcessor

Correct Answer: D

Reference: https://answers.splunk.com/answers/141721/error-in-splunkd-log-breaking-event-becauselimit-of-256-has-been-exceeded.html

QUESTION 3

What is the algorithm used to determine captaincy in a Splunk search head cluster?

A. Raft distributed consensus.

B. Rapt distributed consensus.

C. Rift distributed consensus.

D. Round-robin distribution consensus.

Correct Answer: A

Reference: https://answers.splunk.com/answers/664102/need-to-know-about-raft-directory-on-searchhead-c.html

QUESTION 4

Of the following types of files within an index bucket, which file type may consume the most disk?

A. Rawdata

B. Bloom filter

C. Metadata (.data)

D. Inverted index (.tsidx)

Correct Answer: B

QUESTION 5

Which of the following statements describe licensing in a clustered Splunk deployment? (Select all that apply.)

A. Free licenses do not support clustering.

B. Replicated data does not count against licensing.

C. Each cluster member requires its own clustering license.

D. Cluster members must share the same license pool and license master.

Correct Answer: BD

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Admin/Distdeploylicenses