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.geekcert.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

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 2

When should multiple search pipelines be enabled?

A. Only if disk IOPS is at 800 or better.

B. Only if there are fewer than twelve concurrent users.

C. Only if running Splunk Enterprise version 6.6 or later.

D. Only if CPU and memory resources are significantly under-utilized.

Correct Answer: D

Reference: https://answers.splunk.com/answers/617608/can-we-increase-parallelingestionpipelines-in-ahe.html

QUESTION 3

Which of the following will cause the greatest reduction in disk size requirements for a cluster of N indexers running Splunk Enterprise Security?

A. Setting the cluster search factor to N-1.

B. Increasing the number of buckets per index.

C. Decreasing the data model acceleration range.

D. Setting the cluster replication factor to N-1.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Systemrequirements

QUESTION 4

A customer has installed a 500GB Enterprise license. They also purchased and installed a 300GB, no enforcement license on the same license master. How much data can the customer ingest before search is locked out?

A. 300GB. After this limit, search is locked out.

B. 500GB. After this limit, search is locked out.

C. 800GB. After this limit, search is locked out.

D. Search is not locked out. Violations are still recorded.

Correct Answer: D

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

QUESTION 5

A search head has successfully joined a single site indexer cluster. Which command is used to configure the same search head to join another indexer cluster?

A. splunk add cluster-config

B. splunk add cluster-master

C. splunk edit cluster-config

D. splunk edit cluster-master

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Configuremulti-clustersearch

[SPLK-2002 Study Guide](#)   [SPLK-2002 Exam Questions](#)   [SPLK-2002 Braindumps](#)