SPLK-3003$^{Q\&As}$

Splunk Core Certified Consultant

Pass Splunk SPLK-3003 Exam with 100% Guarantee

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

https://www.geekcert.com/splk-3003.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 of the following statements is true, as it pertains to search head clustering (SHC)?

A. SHC is supported on AIX, Linux, and Windows operating systems.

B. Maximum number of nodes for a SHC is 10.

C. SHC members must run on the same hardware specifications.

D. Minimum number of nodes for a SHC is 5.

Correct Answer: B

QUESTION 2

Which statement is correct?

A. In general, search commands that can be distributed to the search peers should occur as early as possible in a well-tuned search.

B. As a streaming command, streamstats performs better than stats since stats is just a reporting command.

C. When trying to reduce a search result to unique elements, the dedup command is the only way to achieve this.

D. Formatting commands such as fieldformat should occur as early as possible in the search to take full advantage of the often larger number of search peers.

Correct Answer: D

QUESTION 3

The data in Splunk is now subject to auditing and compliance controls. A customer would like to ensure that at least one year of logs are retained for both Windows and Firewall events. What data retention controls must be configured?

A. maxTotalDataSizeMB and frozenTimePeriodInSecs

B. coldToFrozenDir and coldToFrozenScript

C. Splunk Volume and maxTotalDataSizMB

D. Splunk Volume and frozenTimePeriodInSecs

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/Indexer/Setaretirementandarchivingpolicy

QUESTION 4

What is the default push mode for a search head cluster deployer app configuration bundle?

A. full

B. merge_to_default

C. default_only

D. local_only

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/DistSearch/PropagateSHCconfigurationchanges#:~:text=The%20deployer%20push%20mode%20determines,default%20push%20mode%20is%20merge_to_default%20

QUESTION 5

A customer has 30 indexers in an indexer cluster configuration and two search heads. They are working on writing SPL search for a particular use-case, but are concerned that it takes too long to run for short time durations.

How can the Search Job Inspector capabilities be used to help validate and understand the customer concerns?

A. Search Job Inspector provides statistics to show how much time and the number of events each indexer has processed.

B. Search Job Inspector provides a Search Health Check capability that provides an optimized SPL query the customer should try instead.

C. Search Job Inspector cannot be used to help troubleshoot the slow performing search; customer should review index=_introspection instead.

D. The customer is using the transaction SPL search command, which is known to be slow.

Correct Answer: A

Latest SPLK-3003 Dumps SPLK-3003 VCE Dumps SPLK-3003 Study Guide