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.leads4pass.com/splk-3003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

QUESTION 1

A customer is having issues with truncated events greater than 64K. What configuration should be deployed to a universal forwarder (UF) to fix the issue?

A. None. Splunk default configurations will process the events as needed; the UF is not causing truncation.

B. Configure the best practice magic 6 or great 8 props.conf settings.

C. EVENT_BREAKER_ENABLE and EVENT_BREAKER regular expression settings per sourcetype.

D. Global EVENT_BREAKER_ENABLE and EVENT_BREAKER regular expression settings.

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/Resolvedataqualityissues

QUESTION 2

A customer has asked for a five-node search head cluster (SHC), but does not have the storage budget to use a replication factor greater than 2. They would like to understand what might happen in terms of the users\\' ability to view historic scheduled search results if they log onto a search head which doesn\\'t contain one of the 2 copies of a given search artifact.

Which of the following statements best describes what would happen in this scenario?

A. The search head that the user has logged onto will proxy the required artifact over to itself from a search head that currently holds a copy. A copy will also be replicated from that search head permanently, so it is available for future use.

B. Because the dispatch folder containing the search results is not present on the search head, the user will not be able to view the search results.

C. The user will not be able to see the results of the search until one of the search heads is restarted, forcing synchronization of all dispatched artifacts across all search heads.

D. The user will not be able to see the results of the search until the Splunk administrator issues the apply shcluster-bundle command on the search head deployer, forcing synchronization of all dispatched artifacts across all search heads.

Correct Answer: A

QUESTION 3

A customer would like to remove the output_file capability from users with the default user role to stop them from filling up the disk on the search head with lookup files. What is the best way to remove this capability from users?

A. Create a new role without the output_file capability that inherits the default user role and assign it to the users.

B. Create a new role with the output_file capability that inherits the default user role and assign it to the users.

C. Edit the default user role and remove the output_file capability.

D. Clone the default user role, remove the output_file capability, and assign it to the users.

Correct Answer: C

QUESTION 4

A site from a multi-site indexer cluster needs to be decommissioned. Which of the following actions must be taken?

A. Nothing. Decommissioning a site is not possible.

B. Create an alias for where the new data should be sent.

C. Remove the site from the list of available sites.

D. Remove the site from the list of available sites and create an alias for where the new data should be sent.

Correct Answer: D

QUESTION 5

When can the Search Job Inspector be used to debug searches?

A. If the search has not expired.

B. If the search is currently running.

C. If the search has been queued.

D. If the search has expired.

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/Search/ ViewsearchjobpropertieswiththeJobInspector