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.leads4pass.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 using the props.conf LINE_BREAKER attribute to delimit multi-line events, the SHOULD_LINEMERGE attribute should be set to what?

A. Auto

B. None

C. True

D. False

Correct Answer: C

Reference: https://answers.splunk.com/answers/6926/how-to-keep-data-together-as-one-event.html

QUESTION 2

Which of the following is a best practice to maximize indexing performance?

A. Use automatic sourcetyping.

B. Use the Splunk default settings.

C. Not use pre-trained source types.

D. Minimize configuration generality.

Correct Answer: D

QUESTION 3

A Splunk instance has the following settings in SPLUNK_HOME/etc/system/local/server.conf:

[clustering] mode = master replication_factor = 2 pass4SymmKey = password123

Which of the following statements describe this Splunk instance? (Select all that apply.)

A. This is a multi-site cluster.

B. This cluster\\'s search factor is 2.

C. This Splunk instance needs to be restarted.

D. This instance is missing the master_uri attribute.

Correct Answer: AC

QUESTION 4

To reduce the captain\\'s work load in a search head cluster, what setting will prevent scheduled searches from running on the captain?

A. adhoc_searchhead = true (on all members)

B. adhoc_searchhead = true (on the current captain)

C. captain_is_adhoc_searchhead = true (on all members)

D. captain_is_adhoc_searchhead = true (on the current captain)

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/Adhocclustermember

QUESTION 5

Which of the following options can improve reliability of syslog delivery to Splunk? (Select all that apply.)

A. Use TCP syslog.

B. Configure UDP inputs on each Splunk indexer to receive data directly.

C. Use a network load balancer to direct syslog traffic to active backend syslog listeners.

D. Use one or more syslog servers to persist data with a Universal Forwarder to send the data to Splunk indexers.

Correct Answer: CD