

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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

A customer has three users and is planning to ingest 250GB of data per day. They are concerned with search uptime, can tolerate up to a two-hour downtime for the search tier, and want advice on single search head versus a search head cluster. (SHC).

Which recommendation is the most appropriate?

- A. The customer should deploy two active search heads behind a load balancer to support HA.
- B. The customer should deploy a SHC with a single member for HA; more members can be added later.
- C. The customer should deploy a SHC, because it will be required to support the high volume of data.
- D. The customer should deploy a single search head with a warm standby search head and an rsync process to synchronize configurations.

Correct Answer: D

QUESTION 2

When monitoring and forwarding events collected from a file containing unstructured textual events, what is the difference in the Splunk2Splunk payload traffic sent between a universal forwarder (UF) and indexer compared to the Splunk2Splunk payload sent between a heavy forwarder (HF) and the indexer layer? (Assume that the file is being monitored locally on the forwarder.)

- A. The payload format sent from the UF versus the HF is exactly the same. The payload size is identical because they're both sending 64K chunks.
- B. The UF sends a stream of data containing one set of metadata fields to represent the entire stream, whereas the HF sends individual events, each with their own metadata fields attached, resulting in a larger payload.
- C. The UF will generally send the payload in the same format, but only when the sourcetype is specified in the inputs.conf and EVENT_BREAKER_ENABLE is set to true.
- D. The HF sends a stream of 64K TCP chunks with one set of metadata fields attached to represent the entire stream, whereas the UF sends individual events, each with their own metadata fields attached.

Correct Answer: B

QUESTION 3

In an environment that has Indexer Clustering, the Monitoring Console (MC) provides dashboards to monitor environment health. As the environment grows over time and new indexers are added, which steps would ensure the MC is aware of the additional indexers?

- A. No changes are necessary, the Monitoring Console has self-configuration capabilities.
- B. Using the MC setup UI, review and apply the changes.
- C. Remove and re-add the cluster master from the indexer clustering UI page to add new peers, then apply the changes

under the MC setup UI.

D. Each new indexer needs to be added using the distributed search UI, then settings must be saved under the MC setup UI.

Correct Answer: B

QUESTION 4

Which statement is true about subsearches?

- A. Subsearches are faster than other types of searches.
- B. Subsearches work best for joining two large result sets.
- C. Subsearches run at the same time as their outer search.
- D. Subsearches work best for small result sets.

Correct Answer: A

Reference: <https://community.splunk.com/t5/Archive/Looking-for-way-to-explain-why-subsearches-are-soslow/m-p/479133>

QUESTION 5

A customer's deployment server is overwhelmed with forwarder connections after adding an additional 1000 clients. The default phone home interval is set to 60 seconds. To reduce the number of connection failures to the DS what is recommended?

- A. Create a tiered deployment server topology.
- B. Reduce the phone home interval to 6 seconds.
- C. Leave the phone home interval at 60 seconds.
- D. Increase the phone home interval to 600 seconds.

Correct Answer: A

[Latest SPLK-3003 Dumps](#)

[SPLK-3003 PDF Dumps](#)

[SPLK-3003 VCE Dumps](#)