

# SPLK-3003<sup>Q&As</sup>

Splunk Core Certified Consultant

## Pass Splunk SPLK-3003 Exam with 100% Guarantee

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

<https://www.pass2lead.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 wants to understand how Splunk bucket types (hot, warm, cold) impact search performance within their environment. Their indexers have a single storage device for all data. What is the proper message to communicate to the customer?

- A. The bucket types (hot, warm, or cold) have the same search performance characteristics within the customer's environment.
- B. While hot, warm, and cold buckets have the same search performance characteristics within the customer's environment, due to their optimized structure, the thawed buckets are the most performant.
- C. Searching hot and warm buckets result in best performance because by default the cold buckets are miniaturized by removing TSIDX files to save on storage cost.
- D. Because the cold buckets are written to a cheaper/slower storage volume, they will be slower to search compared to hot and warm buckets which are written to Solid State Disk (SSD).

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

A customer has the following Splunk instances within their environment: An indexer cluster consisting of a cluster master/master node and five clustered indexers, two search heads (no search head clustering), a deployment server, and a license master. The deployment server and license master are running on their own single-purpose instances. The customer would like to start using the Monitoring Console (MC) to monitor the whole environment.

On the MC instance, which instances will need to be configured as distributed search peers by specifying them via the UI using the settings menu?

- A. Just the cluster master/master node.
- B. Indexers, search heads, deployment server, license master, cluster master/master node.
- C. Search heads, deployment server, license master, cluster master/master node
- D. Deployment server, license master

Correct Answer: C

---

#### QUESTION 4

What is the primary driver behind implementing indexer clustering in a customer's environment?

- A. To improve resiliency as the search load increases.
- B. To reduce indexing latency.
- C. To scale out a Splunk environment to offer higher performance capability.
- D. To provide higher availability for buckets of data.

Correct Answer: D

Reference: <https://docs.splunk.com/Documentation/Splunk/8.1.0/Indexer/Howclusteredsearchworks>

---

#### QUESTION 5

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

[SPLK-3003 PDF Dumps](#)

[SPLK-3003 VCE Dumps](#)

[SPLK-3003 Practice Test](#)