

# SPLK-2002<sup>Q&As</sup>

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

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

---

## QUESTION 2

Which of the following clarification steps should be taken if apps are not appearing on a deployment client? (Select all that apply.)

- A. Check serverclass.conf of the deployment server.
- B. Check deploymentclient.conf of the deployment client.
- C. Check the content of SPLUNK\_HOME/etc/apps of the deployment server.
- D. Search for relevant events in splunkd.log of the deployment server.

Correct Answer: ABC

Reference: <https://answers.splunk.com/answers/177021/why-is-deployment-client-not-picking-upchanges-to.html>

---

## QUESTION 3

Which search head cluster component is responsible for pushing knowledge bundles to search peers, replicating configuration changes to search head cluster members, and scheduling jobs across the search head cluster?

- A. Master
- B. Captain
- C. Deployer
- D. Deployment server

Correct Answer: B

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/SHCArchitecture>

---

## QUESTION 4

Which Splunk Enterprise offering has its own license?

- A. Splunk Cloud Forwarder
- B. Splunk Heavy Forwarder
- C. Splunk Universal Forwarder
- D. Splunk Forwarder Management

Correct Answer: C

Reference: <https://docs.splunk.com/Splexicon:Forwardinglicense>

---

## QUESTION 5

Indexing is slow and real-time search results are delayed in a Splunk environment with two indexers and one search head. There is ample CPU and memory available on the indexers. Which of the following is most likely to improve indexing performance?

- A. Increase the maximum number of hot buckets in indexes.conf
- B. Increase the number of parallel ingestion pipelines in server.conf
- C. Decrease the maximum size of the search pipelines in limits.conf
- D. Decrease the maximum concurrent scheduled searches in limits.conf

Correct Answer: D

[Latest SPLK-2002 Dumps](#)

[SPLK-2002 PDF Dumps](#)

[SPLK-2002 Practice Test](#)