



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.geekcert.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 tasks should the architect perform when building a deployment plan? (Select all that apply.)

- A. Use case checklist.
- B. Install Splunk apps.
- C. Inventory data sources.
- D. Review network topology.

Correct Answer: D

QUESTION 2

When planning a search head cluster, which of the following is true?

- A. All search heads must use the same operating system.
- B. All search heads must be members of the cluster (no standalone search heads).
- C. The search head captain must be assigned to the largest search head in the cluster.
- D. All indexers must belong to the underlying indexer cluster (no standalone indexers).

Correct Answer: C

QUESTION 3

Splunk Enterprise platform instrumentation refers to data that the Splunk Enterprise deployment logs in the `_introspection` index. Which of the following logs are included in this index? (Select all that apply.)

- A. audit.log
- B. metrics.log
- C. disk_objects.log
- D. resource_usage.log

Correct Answer: CD

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.1/Troubleshooting/Abouttheplatforminstrumentationframework>

QUESTION 4

Before users can use a KV store, an admin must create a collection. Where is a collection is defined?



- A. kvstore.conf
- B. collection.conf
- C. collections.conf
- D. kvcollections.conf

Correct Answer: C

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.2/Knowledge/DefineaKVStorelookupinSplunkWeb>

QUESTION 5

Which of the following will cause the greatest reduction in disk size requirements for a cluster of N indexers running Splunk Enterprise Security?

- A. Setting the cluster search factor to N-1.
- B. Increasing the number of buckets per index.
- C. Decreasing the data model acceleration range.
- D. Setting the cluster replication factor to N-1.

Correct Answer: D

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Systemrequirements>

[SPLK-2002 PDF Dumps](#)

[SPLK-2002 VCE Dumps](#)

[SPLK-2002 Study Guide](#)