

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

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

QUESTION 2

What is the default log size for Splunk internal logs?

- A. 10MB
- B. 20 MB
- C. 25MB
- D. 30MB

Correct Answer: C

Reference: <https://answers.splunk.com/answers/959/how-can-i-control-the-size-and-number-of-splunksinternal-logs.html>

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

What does setting site=site0 on all Search Head Cluster members do in a multi-site indexer cluster?

- A. Disables search site affinity.
- B. Sets all members to dynamic captaincy.
- C. Enables multisite search artifact replication.
- D. Enables automatic search site affinity discovery.

Correct Answer: A

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

QUESTION 5

Which of the following security options must be explicitly configured (i.e. which options are not enabled by default)?

- A. Data encryption between Splunk Web and splunkd.
- B. Certificate authentication between forwarders and indexers.
- C. Certificate authentication between Splunk Web and search head.
- D. Data encryption for distributed search between search heads and indexers.

Correct Answer: B

[Latest SPLK-2002 Dumps](#)

[SPLK-2002 VCE Dumps](#)

[SPLK-2002 Study Guide](#)