



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.passapply.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 is true regarding Splunk Enterprise performance? (Select all that apply.)

- A. Adding search peers increases the maximum size of search results.
- B. Adding RAM to an existing search heads provides additional search capacity.
- C. Adding search peers increases the search throughput as search load increases.
- D. Adding search heads provides additional CPU cores to run more concurrent searches.

Correct Answer: BD

Reference: <https://docs.splunk.com/Documentation/Splunk/7.3.2/Capacity/HowsavedsearchesaffectSplunkEnterpriseperformance>

QUESTION 2

What is the logical first step when starting a deployment plan?

- A. Inventory the currently deployed logging infrastructure.
- B. Determine what apps and use cases will be implemented.
- C. Gather statistics on the expected adoption of Splunk for sizing.
- D. Collect the initial requirements for the deployment from all stakeholders.

Correct Answer: D

QUESTION 3

When adding or rejoining a member to a search head cluster, the following error is displayed: Error pulling configurations from the search head cluster captain; consider performing a destructive configuration resync on this search head cluster member.

What corrective action should be taken?

- A. Restart the search head.
- B. Run the splunk apply shcluster-bundle command from the deployer.
- C. Run the clean raft command on all members of the search head cluster.
- D. Run the splunk resync shcluster-replicated-config command on this member.

Correct Answer: B



QUESTION 4

What log file would you search to verify if you suspect there is a problem interpreting a regular expression in a monitor stanza?

- A. btool.log
- B. metrics.log
- C. splunkd.log
- D. tailing_processor.log

Correct Answer: C

Reference: <https://answers.splunk.com/answers/479312/how-to-edit-inputsconf-to-monitor-multiple-files-w-1.html>

QUESTION 5

Which of the following is a good practice for a search head cluster deployer?

- A. The deployer only distributes configurations to search head cluster members when they "phone home".
- B. The deployer must be used to distribute non-replicable configurations to search head cluster members.
- C. The deployer must distribute configurations to search head cluster members to be valid configurations.
- D. The deployer only distributes configurations to search head cluster members with splunk apply shcluster-bundle.

Correct Answer: A

[SPLK-2002 PDF Dumps](#)

[SPLK-2002 Study Guide](#)

[SPLK-2002 Brindumps](#)