



Pass4IT

Splunk
splk-2002

QUESTIONS AND ANSWERS

FREE VERSION

(LIMITED CONTENT)

Thank you for downloading our reliable exam questions
for more exams you can visit:

<https://www.pass4it.com/all-vendors>

Dumps Questions splk-2002

Exam Name: Splunk Enterprise Certified Architect

Certification Provider: Splunk

Exam: Splunk Enterprise Certified Architect

Question #1

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>

Question #2

Stakeholders have identified high availability for searchable data as their top priority. Which of the following best addresses this requirement?

- A. Increasing the search factor in the cluster.
- B. Increasing the replication factor in the cluster.
- C. Increasing the number of search heads in the cluster.
- D. Increasing the number of CPUs on the indexers in the cluster.

Correct Answer: B

Reference:

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

Question #3

Search dashboards in the Monitoring Console indicate that the distributed deployment is approaching its capacity. Which of the following options will provide the most search performance improvement?

- A. Replace the indexer storage to solid state drives (SSD).
- B. Add more search heads and redistribute users based on the search type.
- C. Look for slow searches and reschedule them to run during an off-peak time.
- D. Add more search peers and make sure forwarders distribute data evenly across all indexers.

Correct Answer: C

Question #4

A Splunk architect has inherited the Splunk deployment at Buttercup Games and end users are complaining that the events are inconsistently formatted for a web sourcetype. Further investigation reveals that not all web logs flow through the same infrastructure: some of the data goes through heavy forwarders and some of the forwarders are managed by another department. Which of the following items might be the cause for this issue?

- A. The search head may have different configurations than the indexers.
- B. The data inputs are not properly configured across all the forwarders.
- C. The indexers may have different configurations than the heavy forwarders.
- D. The forwarders managed by the other department are an older version than the rest.

Correct Answer: C

Question #5

A customer has installed a 500GB Enterprise license. They also purchased and installed a 300GB, no enforcement license on the same license master. How much data can the customer ingest before search is locked out?

- A. 300GB. After this limit, search is locked out.
- B. 500GB. After this limit, search is locked out.
- C. 800GB. After this limit, search is locked out.
- D. Search is not locked out. Violations are still recorded.

Correct Answer: D

Reference:

<https://docs.splunk.com/Documentation/Splunk/7.3.2/Admin/TypesofSplunklicenses>