Actual exam question from Splunk's SPLK-2002

Question #: 4

Topic #: 1

[All SPLK-2002 Questions]

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.

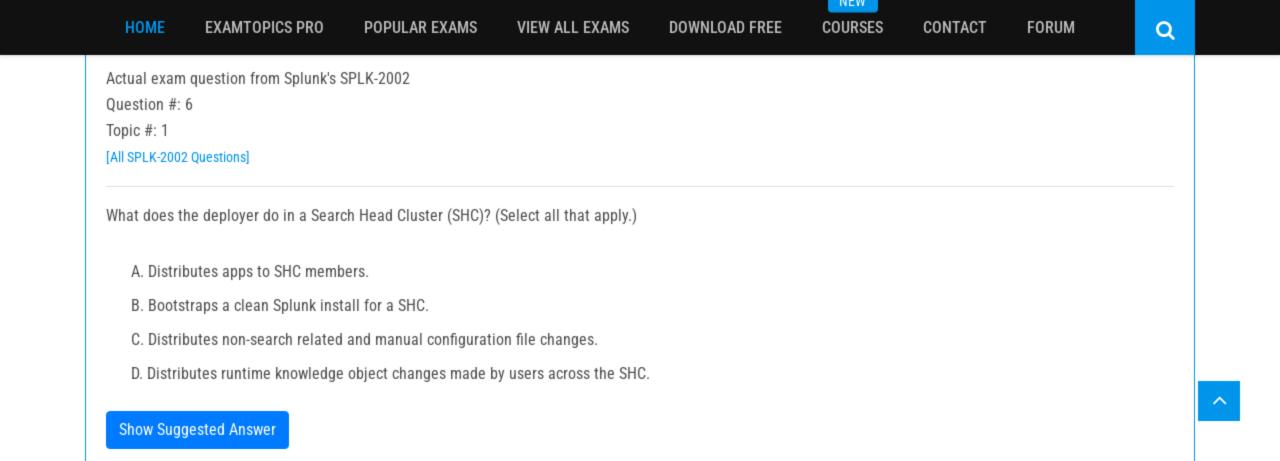
FORUM

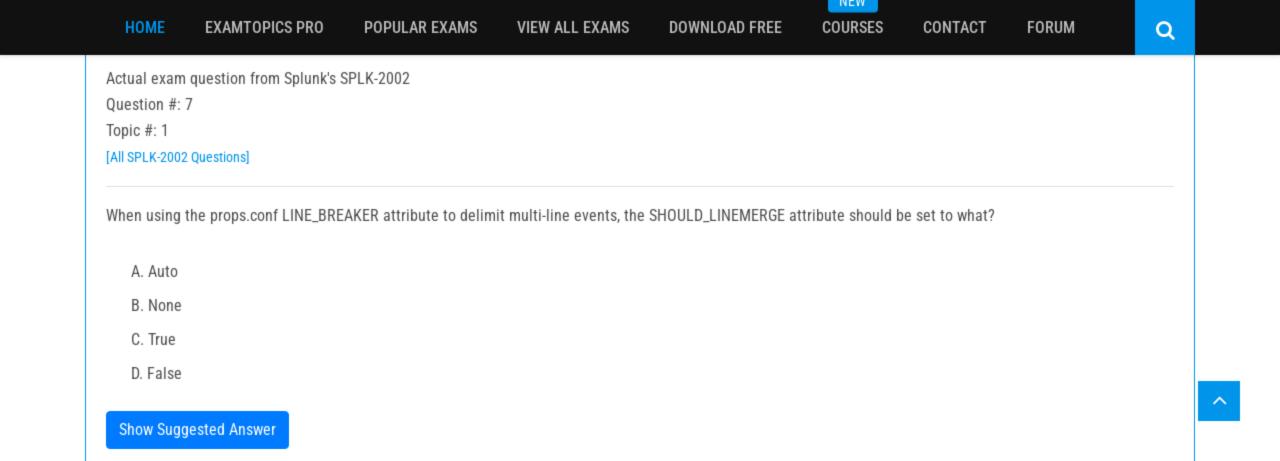
Q

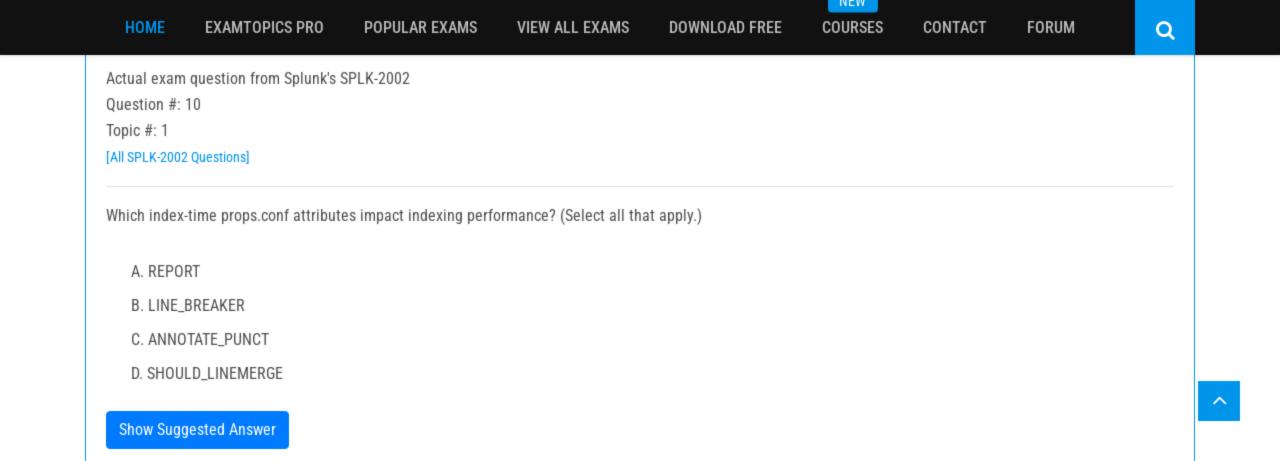
Which of the following items might be the cause for this issue?

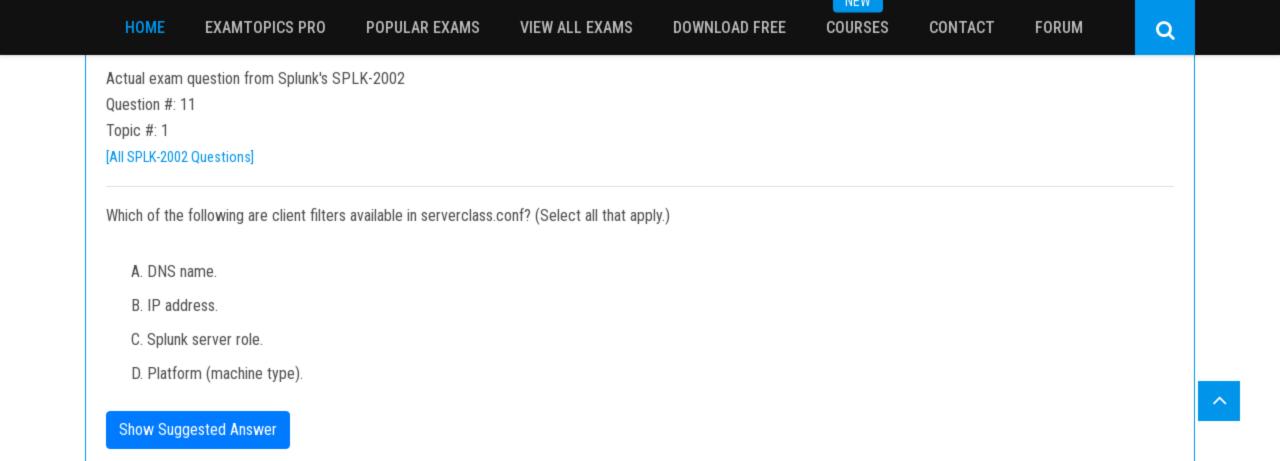
- A. The search head may have different configurations than the indexers.
- B. The data inputs are not properly configured across all the forwarders.
- C. The indexers may have different configurations than the heavy forwarders.
- D. The forwarders managed by the other department are an older version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

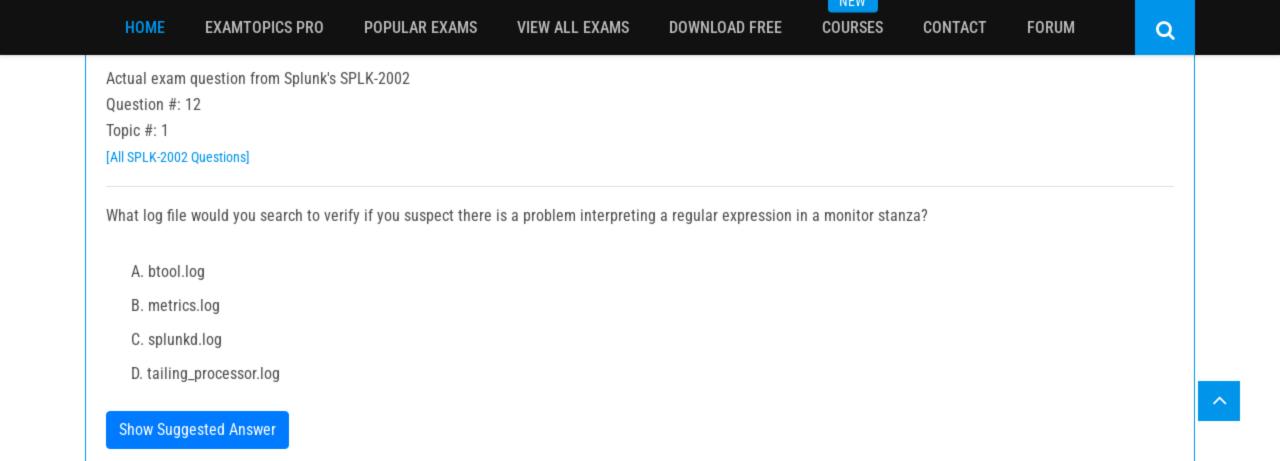
Show Suggested Answer

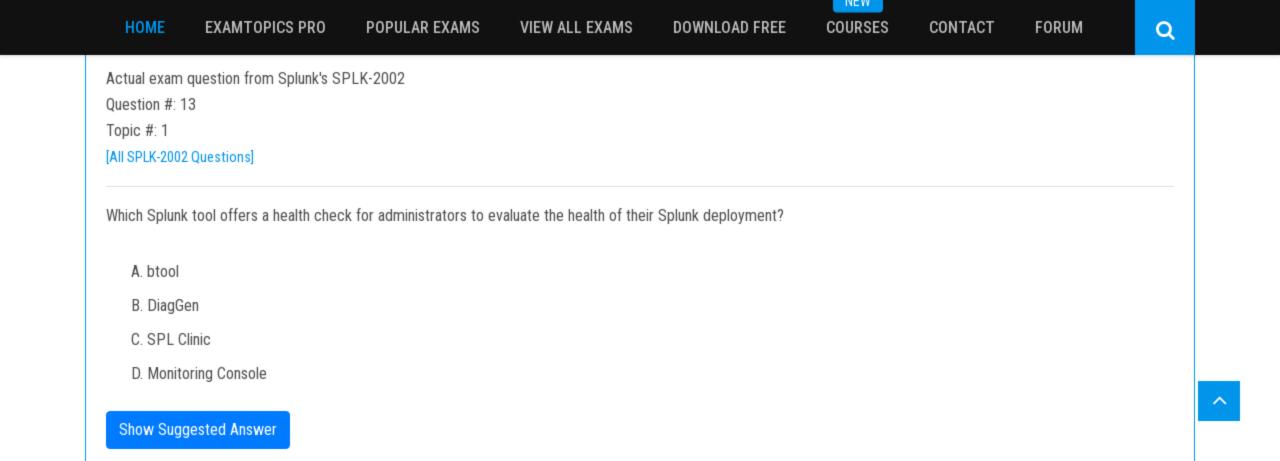


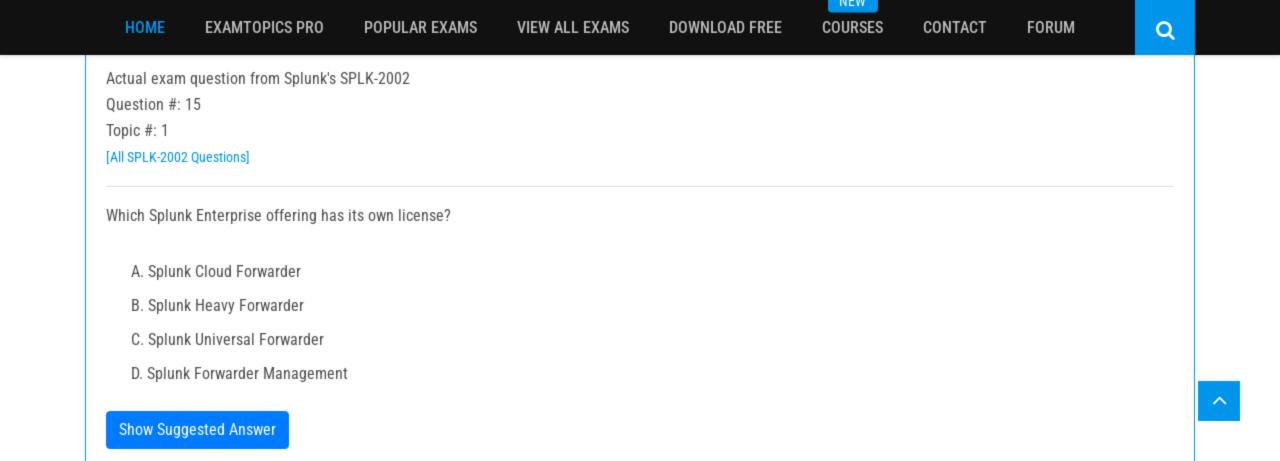


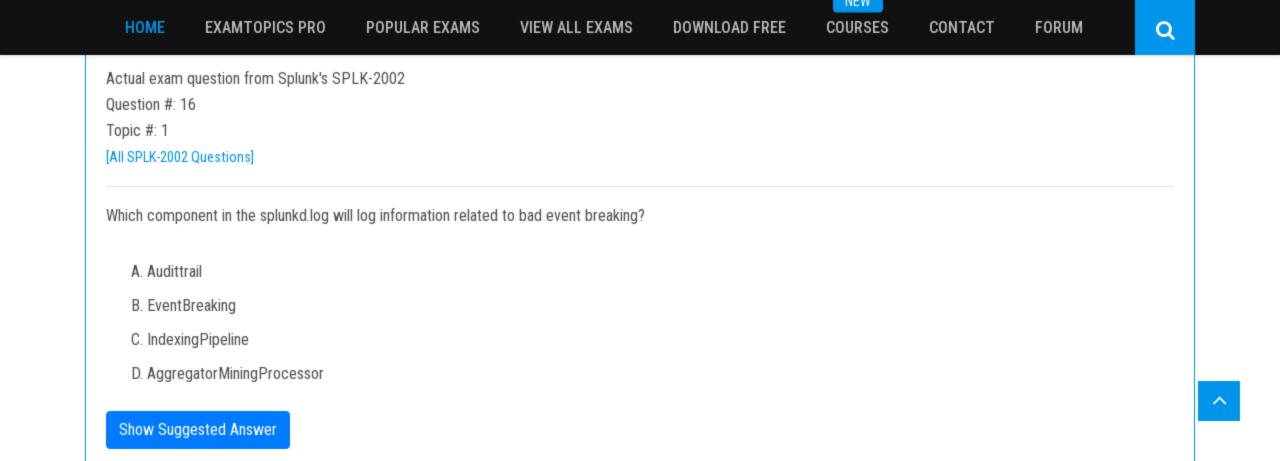


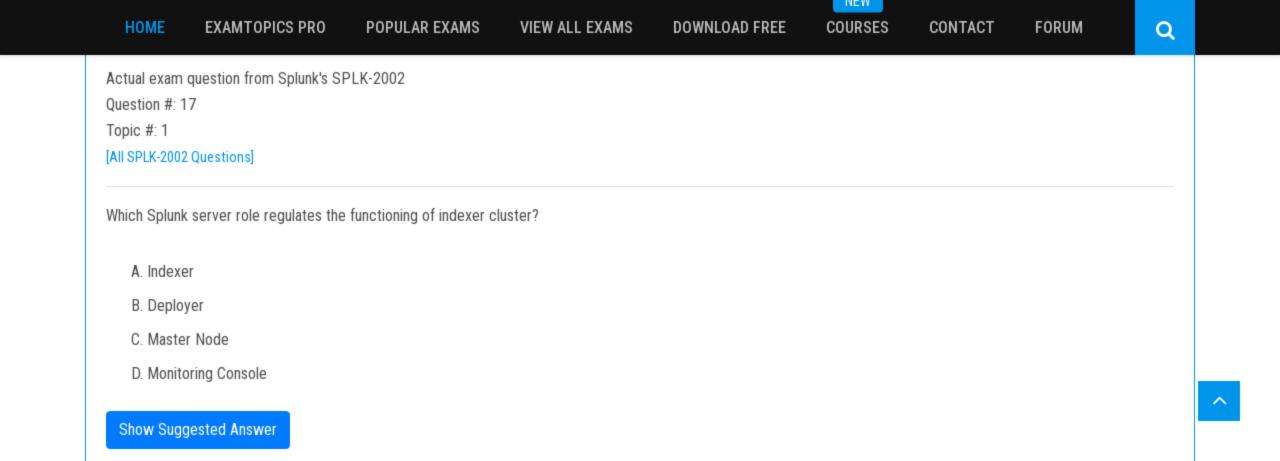


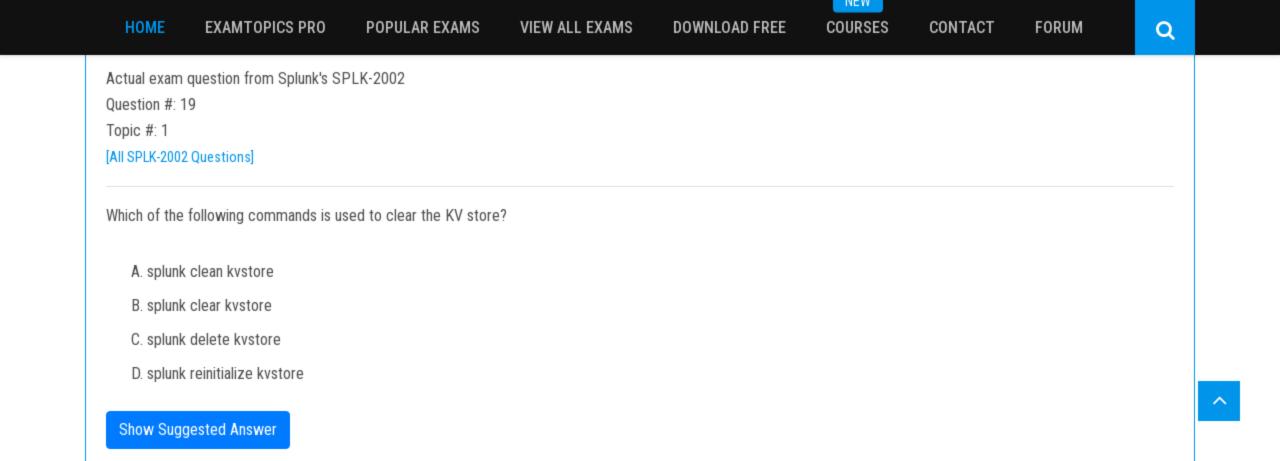


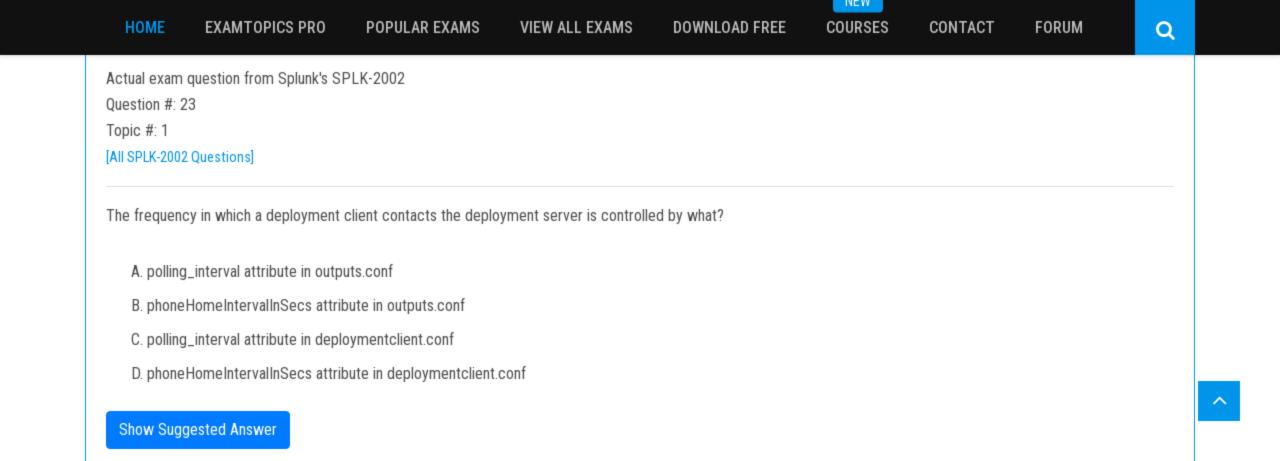


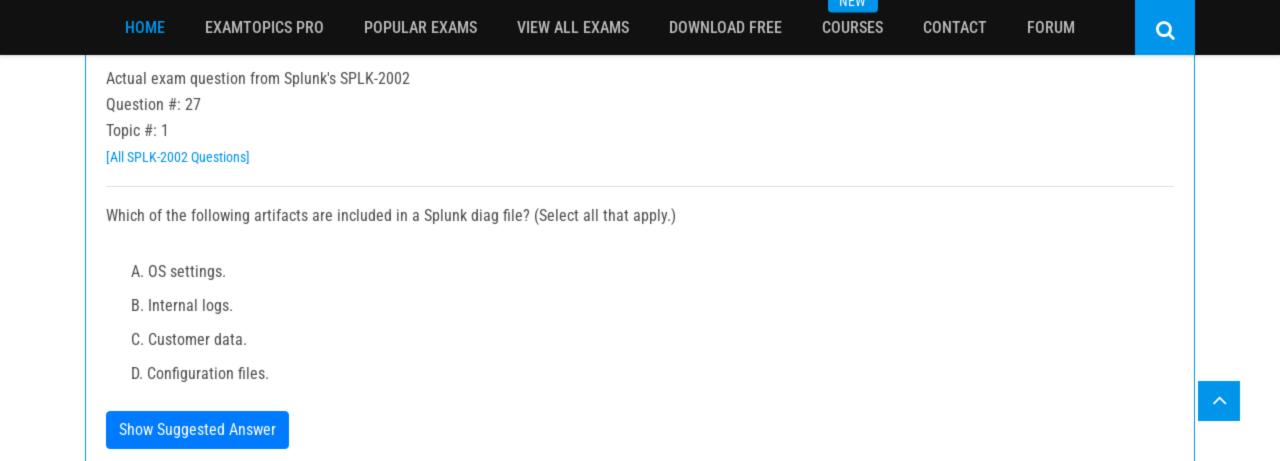


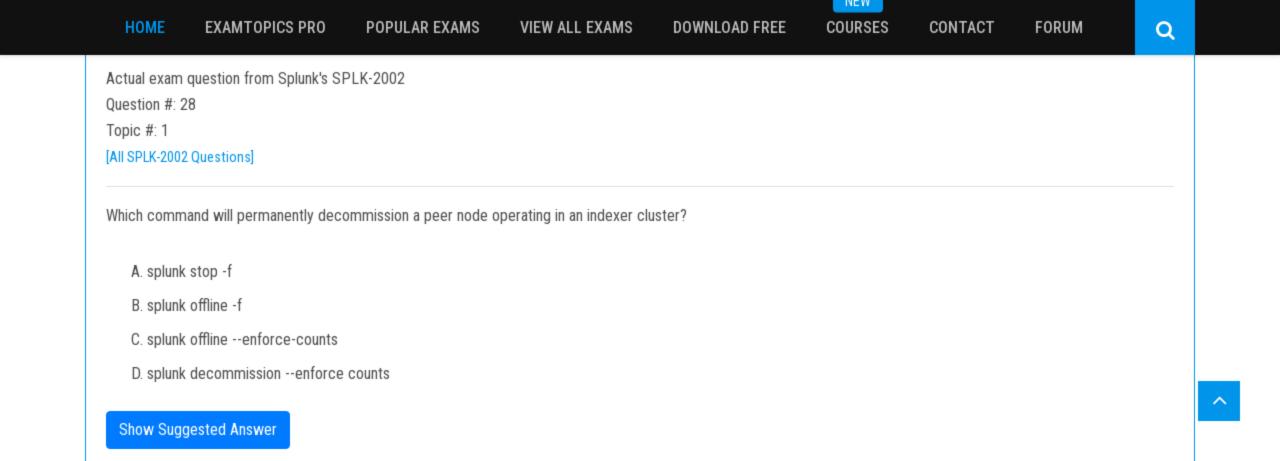


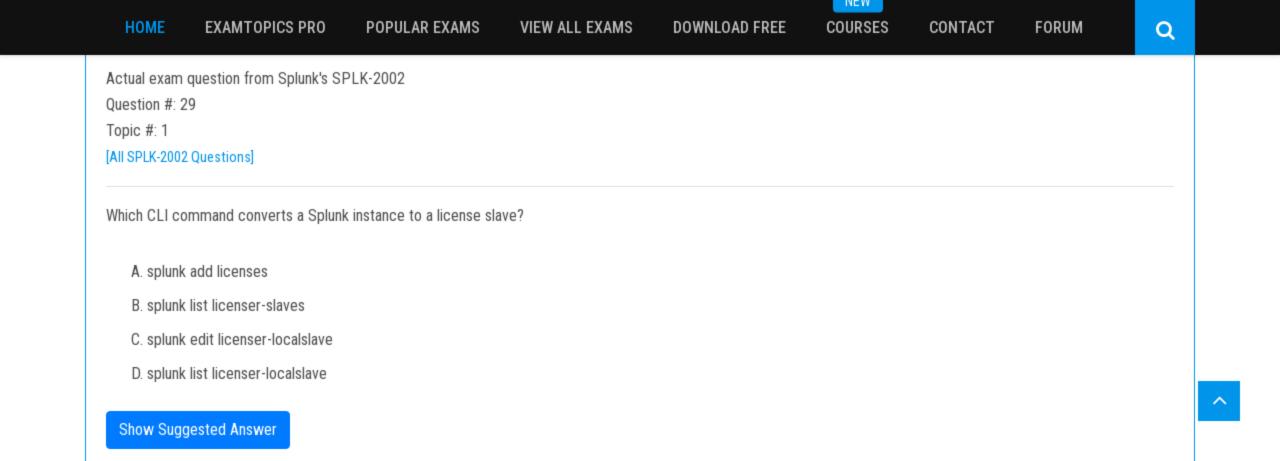












Question #: 33

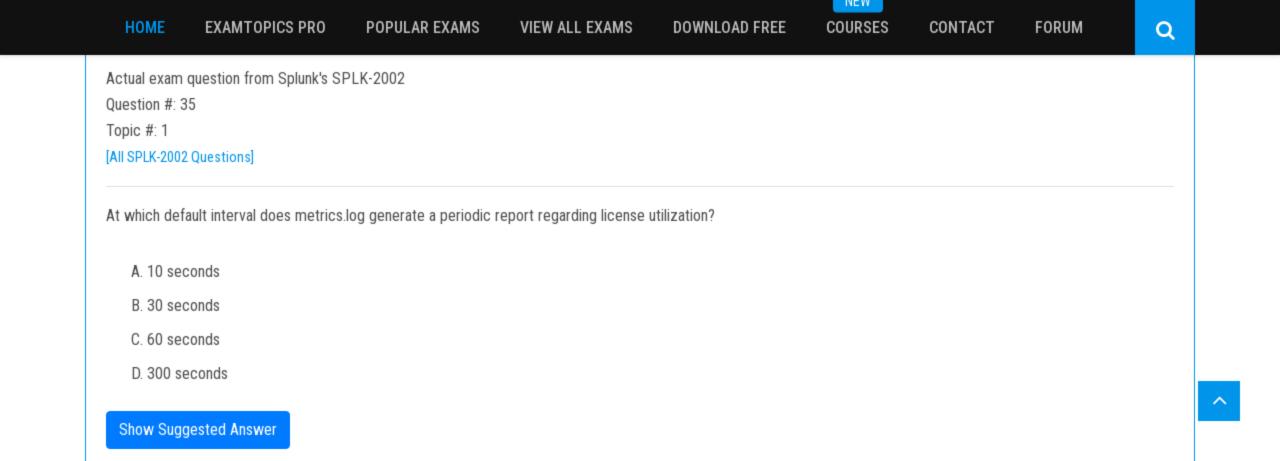
Topic #: 1

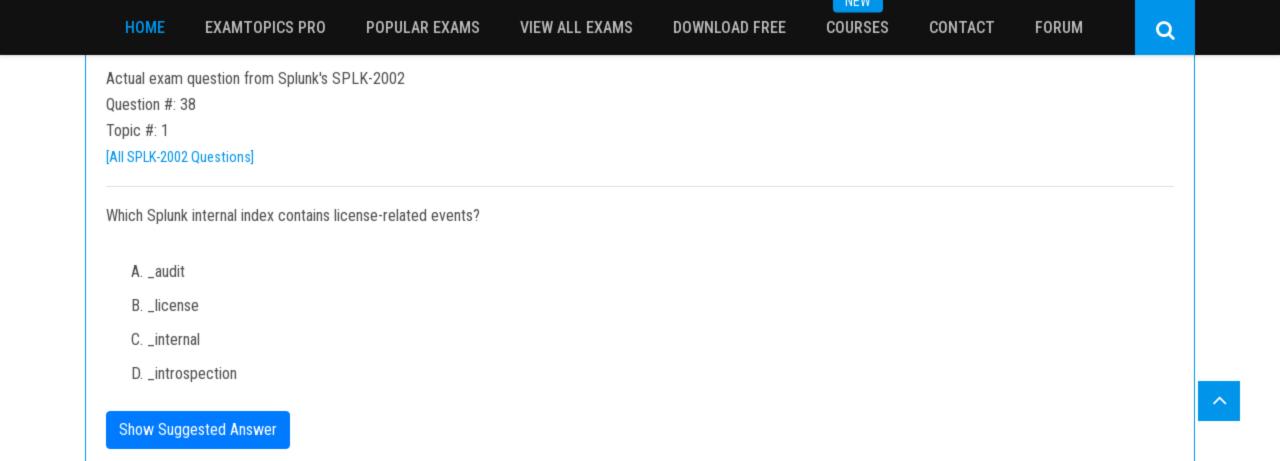
[All SPLK-2002 Questions]

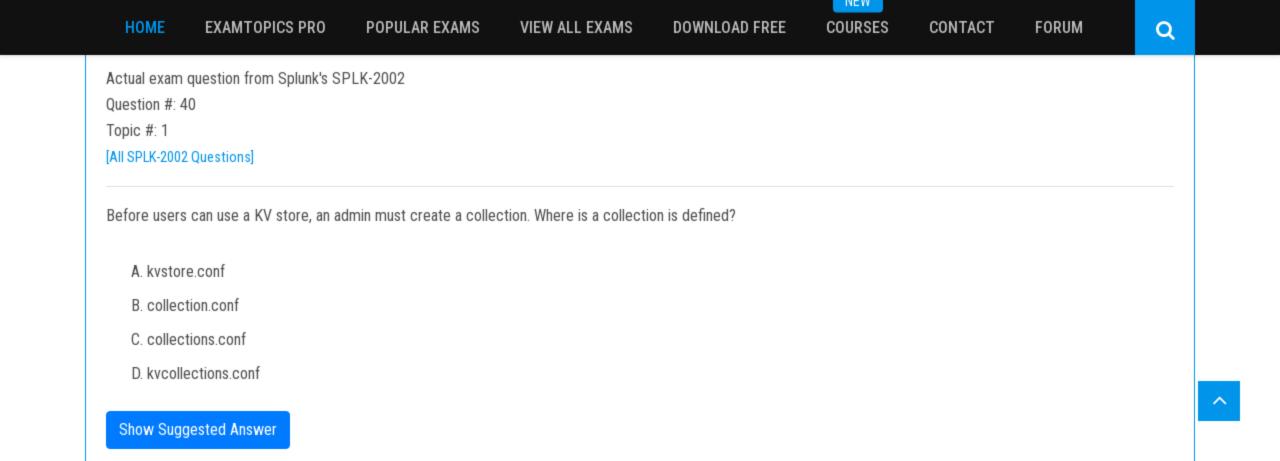
A customer plans to ingest 600 GB of data per day into Splunk. They will have six concurrent users, and they also want high data availability and high search performance. The customer is concerned about cost and wants to spend the minimum amount on the hardware for Splunk. How many indexers are recommended for this deployment?

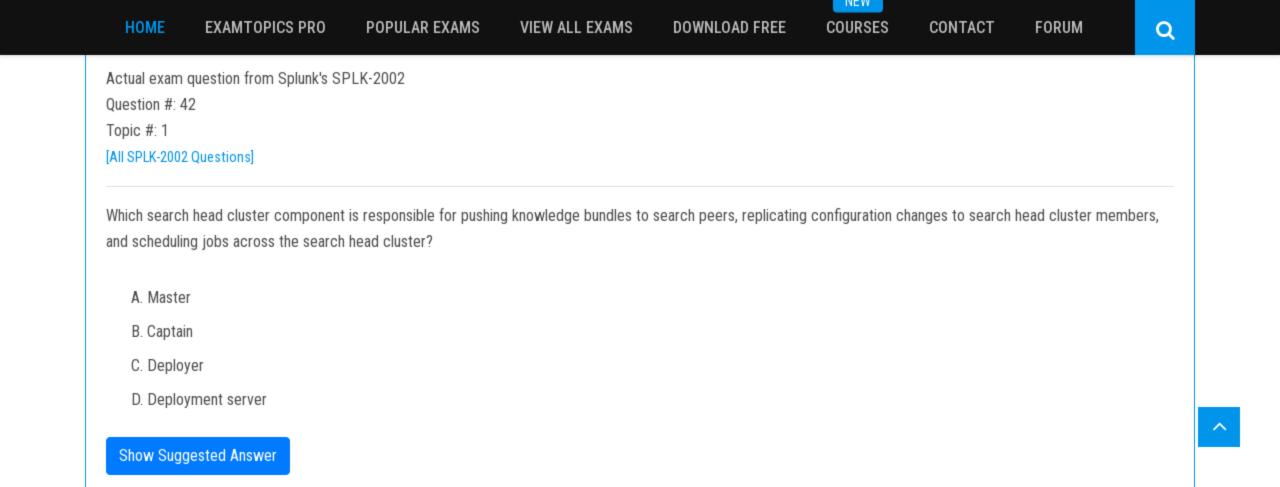
- A. Two indexers not in a cluster, assuming users run many long searches.
- B. Three indexers not in a cluster, assuming a long data retention period.
- C. Two indexers clustered, assuming high availability is the greatest priority.
- D. Two indexers clustered, assuming a high volume of saved/scheduled searches.

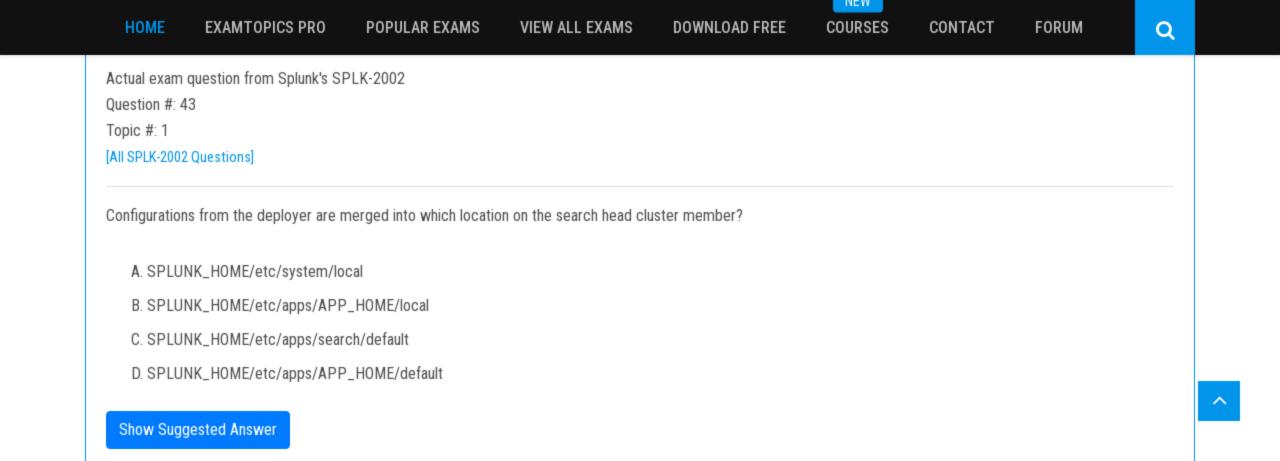
Show Suggested Answer

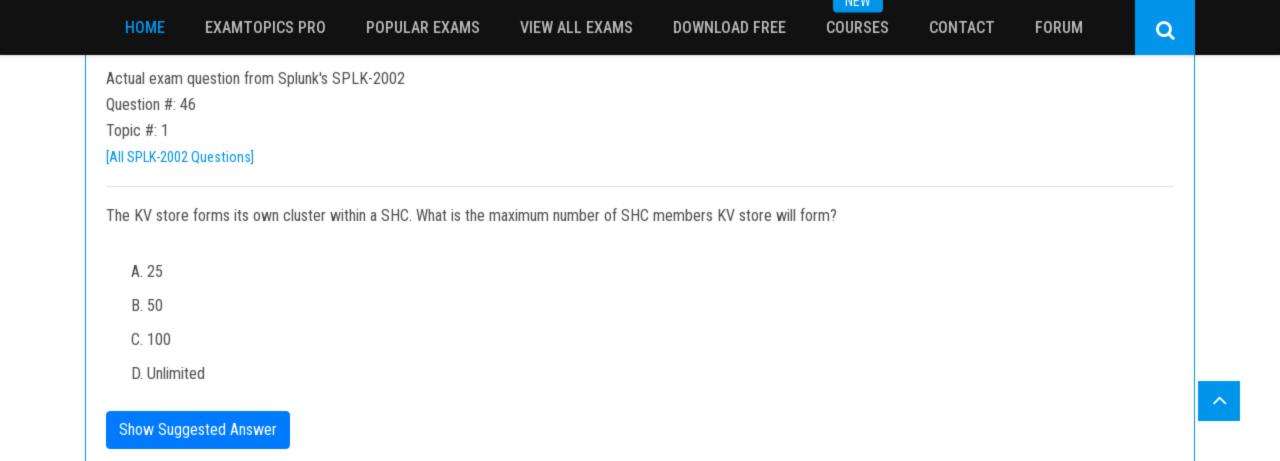


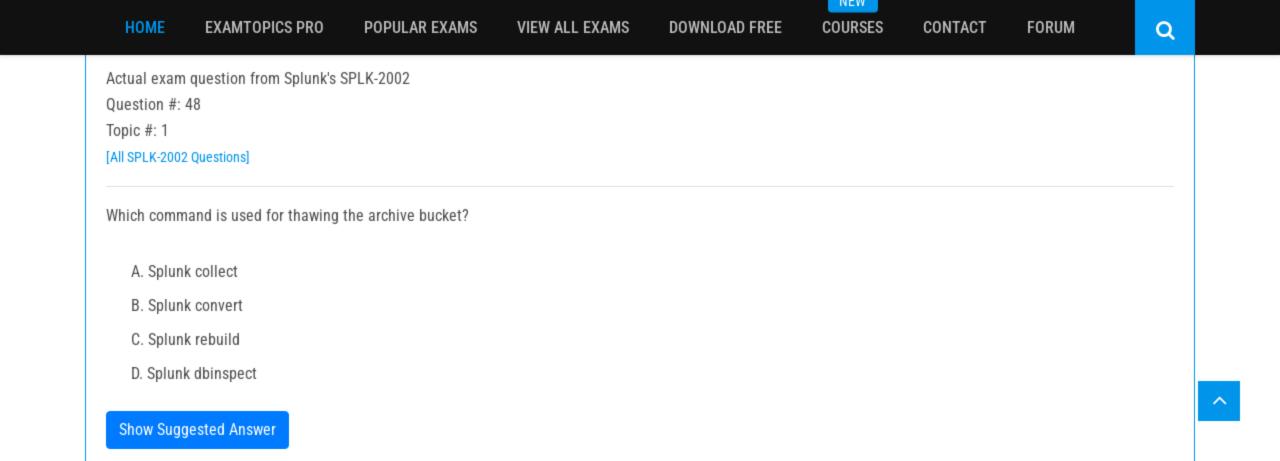












Actual exam question from Splunk's SPLK-2002

Question #: 49

Topic #: 1

[All SPLK-2002 Questions]

A Splunk instance has the following settings in SPLUNK_HOME/etc/system/local/server.conf:

[clustering]

mode = master

replication_factor = 2

pass4SymmKey = password123

Which of the following statements describe this Splunk instance? (Select all that apply.)

- A. This is a multi-site cluster.
- B. This cluster's search factor is 2.
- C. This Splunk instance needs to be restarted.
- D. This instance is missing the master_uri attribute.

Show Suggested Answer

