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

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: D

QUESTION 2

Which command will permanently decommission a peer node operating in an indexer cluster?

A. splunk stop -f

B. splunk offline -f

C. splunk offline --enforce-counts

D. splunk decommission --enforce counts

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Takeapeeroffline

QUESTION 3

Which search head cluster component is responsible for pushing knowledge bundles to search peers, replicating configuration changes to search head cluster members, and scheduling jobs across the search head cluster?

A. Master

B. Captain

C. Deployer

D. Deployment server

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/SHCarchitecture

QUESTION 4

When Splunk is installed, where are the internal indexes stored by default?

A. SPLUNK_HOME/bin

B. SPLUNK_HOME/var/lib

C. SPLUNK_HOME/var/run

D. SPLUNK_HOME/etc/system/default

Correct Answer: B

Reference: https://answers.splunk.com/answers/3806/where-does-splunk-store-the-logs.html

QUESTION 5

What is a Splunk Job? (Select all that apply.)

A. A user-defined Splunk capability.

B. Searches that are subjected to some usage quota.

C. A search process kicked off via a report or an alert.

D. A child OS process manifested from the splunkd process.

Correct Answer: A