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

A new Splunk customer is using syslog to collect data from their network devices on port 514. What is the best practice for ingesting this data into Splunk?

A. Configure syslog to send the data to multiple Splunk indexers.

B. Use a Splunk indexer to collect a network input on port 514 directly.

C. Use a Splunk forwarder to collect the input on port 514 and forward the data.

D. Configure syslog to write logs and use a Splunk forwarder to collect the logs.

Correct Answer: C

Reference: https://wiki.splunk.com/Community:BestPracticeForConfiguringSyslogInput

QUESTION 2

In which phase of the Splunk Enterprise data pipeline are indexed extraction configurations processed?

A. Input

B. Search

C. Parsing

D. Indexing

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Admin/ Configurationparametersandthedatapipeline

QUESTION 3

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 4

How does the average run time of all searches relate to the available CPU cores on the indexers?

A. Average run time is independent of the number of CPU cores on the indexers.

B. Average run time decreases as the number of CPU cores on the indexers decreases.

C. Average run time increases as the number of CPU cores on the indexers decreases.

D. Average run time increases as the number of CPU cores on the indexers increases.

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Capacity/ Accommodatemanysimultaneoussearches

QUESTION 5

When configuring a Splunk indexer cluster, what are the default values for replication and search factor?

A. replication_factor = 2 search_factor = 2

B. replication_factor = 2 search factor = 3

C. replication_factor = 3 search_factor = 2

D. replication_factor = 3 search factor = 3

Correct Answer: C