VCE & PDF
Pass4itSure.com

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.pass4itsure.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

A three-node search head cluster is skipping a large number of searches across time. What should be done to increase scheduled search capacity on the search head cluster?

A. Create a job server on the cluster.

B. Add another search head to the cluster.

C. server.conf captain_is_adhoc_searchhead = true.

D. Change limits.conf value for max_searches_per_cpu to a higher value.

Correct Answer: D

QUESTION 3

Which Splunk Enterprise offering has its own license?

A. Splunk Cloud Forwarder

B. Splunk Heavy Forwarder

C. Splunk Universal Forwarder

D. Splunk Forwarder Management

Correct Answer: C

Reference: https://docs.splunk.com/Splexicon:Forwardinglicense

QUESTION 4

Which of the following statements about integrating with third-party systems is true? (Select all that apply.)

A. A Hadoop application can search data in Splunk.

B. Splunk can search data in the Hadoop File System (HDFS).

C. You can use Splunk alerts to provision actions on a third-party system.

D. You can forward data from Splunk forwarder to a third-party system without indexing it first.

Correct Answer: CD

QUESTION 5

Which of the following statements describe licensing in a clustered Splunk deployment? (Select all that apply.)

A. Free licenses do not support clustering.

B. Replicated data does not count against licensing.

C. Each cluster member requires its own clustering license.

D. Cluster members must share the same license pool and license master.

Correct Answer: BD

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

[SPLK-2002 PDF Dumps](#)   [SPLK-2002 Practice Test](#)   [SPLK-2002 Exam Questions](#)