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

Which of the following artifacts are included in a Splunk diag file? (Select all that apply.)

A. OS settings.

B. Internal logs.

C. Customer data.

D. Configuration files.

Correct Answer: BD

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Troubleshooting/Generateadiag

QUESTION 3

In a four site indexer cluster, which configuration stores two searchable copies at the origin site, one searchable copy at site2, and a total of four searchable copies?

A. site_search_factor = origin:2, site1:2, total:4

B. site_search_factor = origin:2, site2:1, total:4

C. site_replication_factor = origin:2, site1:2, total:4

D. site_replication_factor = origin:2, site2:1, total:4

Correct Answer: D

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

QUESTION 4

The guidance Splunk gives for estimating size on for syslog data is 50% of original data size. How does this divide between files in the index?

A. rawdata is: 10%, tsidx is: 40%

B. rawdata is: 15%, tsidx is: 35%

C. rawdata is: 35%, tsidx is: 15%

D. rawdata is: 40%, tsidx is: 10%

Correct Answer: B

Reference: https://answers.splunk.com/answers/147951/what-is-the-compression-ratio-of-raw-data-insplunk.html

QUESTION 5

A Splunk user successfully extracted an ip address into a field called src_ip. Their colleague cannot see that field in their search results with events known to have src_ip. Which of the following may explain the problem? (Select all that apply.)

A. The field was extracted as a private knowledge object.

B. The events are tagged as communicate, but are missing the network tag.

C. The Typing Queue, which does regular expression replacements, is blocked.

D. The colleague did not explicitly use the field in the search and the search was set to Fast Mode.

Correct Answer: D

Reference: https://answers.splunk.com/answers/657187/map-command-field-not-being-evaluated.html