SPLK-2002Q&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.pass2lead.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

Which of the following is a way to exclude search artifacts when creating a diag?

A. SPLUNK_HOME/bin/splunk diag --exclude

B. SPLUNK_HOME/bin/splunk diag --debug --refresh

C. SPLUNK_HOME/bin/splunk diag --disable=dispatch

D. SPLUNK_HOME/bin/splunk diag --filter-searchstrings

Correct Answer: A

Reference: https://splunkonbigdata.com/2018/10/01/splunk-diag/

QUESTION 2

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 3

Which of the following is an indexer clustering requirement?

A. Must use shared storage.

B. Must reside on a dedicated rack.

C. Must have at least three members.

D. Must share the same license pool.

Correct Answer: D

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

QUESTION 4

What is the minimum reference server specification for a Splunk indexer?

A. 12 CPU cores, 12GB RAM, 800 IOPS

B. 16 CPU cores, 16GB RAM, 800 IOPS

C. 24 CPU cores, 16GB RAM, 1200 IOPS

D. 28 CPU cores, 32GB RAM, 1200 IOPS

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Capacity/Referencehardware#Reference_host_specification

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