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

When using the props.conf LINE_BREAKER attribute to delimit multi-line events, the SHOULD_LINEMERGE attribute should be set to what?

A. Auto

B. None

C. True

D. False

Correct Answer: C

Reference: https://answers.splunk.com/answers/6926/how-to-keep-data-together-as-one-event.html

QUESTION 2

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 3

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

QUESTION 4

When should multiple search pipelines be enabled?

A. Only if disk IOPS is at 800 or better.

B. Only if there are fewer than twelve concurrent users.

C. Only if running Splunk Enterprise version 6.6 or later.

D. Only if CPU and memory resources are significantly under-utilized.

Correct Answer: D

Reference: https://answers.splunk.com/answers/617608/can-we-increase-parallelingestionpipelines-in-ahe.html

---

QUESTION 5

What does the deployer do in a Search Head Cluster (SHC)? (Select all that apply.)

A. Distributes apps to SHC members.

B. Bootstraps a clean Splunk install for a SHC.

C. Distributes non-search related and manual configuration file changes.

D. Distributes runtime knowledge object changes made by users across the SHC.

Correct Answer: A

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

Latest SPLK-2002 Dumps   SPLK-2002 PDF Dumps   SPLK-2002 Exam
                                                             Questions