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

Stakeholders have identified high availability for searchable data as their top priority. Which of the following best addresses this requirement?

A. Increasing the search factor in the cluster.

B. Increasing the replication factor in the cluster.

C. Increasing the number of search heads in the cluster.

D. Increasing the number of CPUs on the indexers in the cluster.

Correct Answer: B

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

---

QUESTION 2

Of the following types of files within an index bucket, which file type may consume the most disk?

A. Rawdata

B. Bloom filter

C. Metadata (.data)

D. Inverted index (.tsidx)

Correct Answer: B

QUESTION 3

Which of the following options can improve reliability of syslog delivery to Splunk? (Select all that apply.)

A. Use TCP syslog.

B. Configure UDP inputs on each Splunk indexer to receive data directly.

C. Use a network load balancer to direct syslog traffic to active backend syslog listeners.

D. Use one or more syslog servers to persist data with a Universal Forwarder to send the data to Splunk indexers.

Correct Answer: CD

QUESTION 4

Which of the following should be done when installing Enterprise Security on a Search Head Cluster? (Select all that apply.)

A. Install Enterprise Security on the deployer.

B. Install Enterprise Security on a staging instance.

C. Copy the Enterprise Security configurations to the deployer.

D. Use the deployer to deploy Enterprise Security to the cluster members.

Correct Answer: AD

Reference: https://docs.splunk.com/Documentation/ES/5.3.1/Install/InstallEnterpriseSecuritySHC

QUESTION 5

In a distributed environment, knowledge object bundles are replicated from the search head to which location on the search peer(s)?

A. SPLUNK_HOME/var/lib/searchpeers

B. SPLUNK_HOME/var/log/searchpeers

C. SPLUNK_HOME/var/run/searchpeers

D. SPLUNK_HOME/var/spool/searchpeers

Correct Answer: C

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

SPLK-2002 Practice Test SPLK-2002 Study Guide SPLK-2002 Exam Questions