SPLK-2002$^{\text{Q\&As}}$

Splunk Enterprise Certified Architect

QUESTION 1

Which of the following can a Splunk diag contain?

A. Search history, Splunk users and their roles, running processes, indexed data

B. Server specs, current open connections, internal Splunk log files, index listings

C. KV store listings, internal Splunk log files, search peer bundles listings, indexed data

D. Splunk platform configuration details, Splunk users and their roles, current open connections, index listings

Correct Answer: B

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

QUESTION 2

In an existing Splunk environment, the new index buckets that are created each day are about half the size of the incoming data. Within each bucket, about 30% of the space is used for rawdata and about 70% for index files.

What additional information is needed to calculate the daily disk consumption, per indexer, if indexer clustering is implemented?

A. Total daily indexing volume, number of peer nodes, and number of accelerated searches.

B. Total daily indexing volume, number of peer nodes, replication factor, and search factor.

C. Total daily indexing volume, replication factor, search factor, and number of search heads.

D. Replication factor, search factor, number of accelerated searches, and total disk size across cluster.

Correct Answer: D

QUESTION 3

When adding or decommissioning a member from a Search Head Cluster (SHC), what is the proper order of operations?

A. 1. Delete Splunk Enterprise, if it exists.

2.

Install and initialize the instance.

3.

Join the SHC.

B. 1. Install and initialize the instance.

2.

Delete Splunk Enterprise, if it exists.

3.

Join the SHC.

C. 1. Initialize cluster rebalance operation.

2.

Remove master node from cluster.

3.

Trigger replication.

D. 1. Trigger replication.

2.

Remove master node from cluster.

3.

Initialize cluster rebalance operation.

Correct Answer: B

QUESTION 4

Which of the following will cause the greatest reduction in disk size requirements for a cluster of N indexers running Splunk Enterprise Security?

A. Setting the cluster search factor to N-1.

B. Increasing the number of buckets per index.

C. Decreasing the data model acceleration range.

D. Setting the cluster replication factor to N-1.

Correct Answer: D

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

QUESTION 5

Because Splunk indexing is read/write intensive, it is important to select the appropriate disk storage solution for each deployment. Which of the following statements is accurate about disk storage?

A. High performance SAN should never be used.

B. Enable NFS for storing hot and warm buckets.

C. The recommended RAID setup is RAID 10 (1 + 0).

D. Virtualized environments are usually preferred over bare metal for Splunk indexers.

Correct Answer: C

Reference: https://www.splunk.com/pdfs/technical-briefs/splunk-deploying-vmware-tech-brief.pdf