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

Splunk Enterprise Certified Architect

QUESTION 1

Which of the following is a good practice for a search head cluster deployer?

A. The deployer only distributes configurations to search head cluster members when they "phone home".

B. The deployer must be used to distribute non-replicable configurations to search head cluster members.

C. The deployer must distribute configurations to search head cluster members to be valid configurations.

D. The deployer only distributes configurations to search head cluster members with splunk apply shcluster-bundle.

Correct Answer: A

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

Which command is used for thawing the archive bucket?

A. Splunk collect

B. Splunk convert

C. Splunk rebuild

D. Splunk dbinspect

Correct Answer: C

Reference: https://answers.splunk.com/answers/337025/after-frozen-data-restore-thawed-data-notworking.html

QUESTION 4

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

QUESTION 5

Which two sections can be expanded using the Search Job Inspector?

A. Execution costs.

B. Saved search history.

C. Search job properties.

D. Optimization suggestions.

Correct Answer: BC

SPLK-2002 VCE Dumps SPLK-2002 Study Guide SPLK-2002 Braindumps