SPLK-3003 Q&As

Splunk Core Certified Consultant

Pass Splunk SPLK-3003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/splk-3003.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

What is the Splunk PS recommendation when using the deployment server and building deployment apps?

A. Carefully design smaller apps with specific configuration that can be reused.

B. Only deploy Splunk PS base configurations via the deployment server.

C. Use $SPLUNK_HOME/etc/system/local configurations on forwarders and only deploy TAs via the deployment server.

D. Carefully design bigger apps containing multiple configs.

Correct Answer: B

Reference: https://www.splunk.com/en_us/blog/platform/adding-a-deployment-server-forwardermanagement-to-a-new-or-existing-splunk-cloud-or-splunk-enterprise-deployment.html

QUESTION 2

A customer wants to understand how Splunk bucket types (hot, warm, cold) impact search performance within their environment. Their indexers have a single storage device for all data. What is the proper message to communicate to the customer?

A. The bucket types (hot, warm, or cold) have the same search performance characteristics within the customer\\'s environment.

B. While hot, warm, and cold buckets have the same search performance characteristics within the customers environment, due to their optimized structure, the thawed buckets are the most performant.

C. Searching hot and warm buckets result in best performance because by default the cold buckets are miniaturized by removing TSIDX files to save on storage cost.

D. Because the cold buckets are written to a cheaper/slower storage volume, they will be slower to search compared to hot and warm buckets which are written to Solid State Disk (SSD).

Correct Answer: D

QUESTION 3

The customer has an indexer cluster supporting a wide variety of search needs, including scheduled search, data model acceleration, and summary indexing. Here is an excerpt from the cluster mater\\'s server.conf:

```
[clustering]
replication_factor=2
search_factor=1
summary_replication-false
```

Which strategy represents the minimum and least disruptive change necessary to protect the searchability of the

indexer cluster in case of indexer failure?

A. Enable maintenance mode on the CM to prevent excessive fix-up and bring the failed indexer back online.

B. Leave replication_factor=2, increase search_factor=2 and enable summary_replication.

C. Convert the cluster to multi-site and modify the server.conf to be site_replication_factor=2, site_search_factor=2.

D. Increase replication_factor=3, search_factor=2 to protect the data, and allow there to always be a searchable copy.

Correct Answer: D

QUESTION 4

The data in Splunk is now subject to auditing and compliance controls. A customer would like to ensure that at least one year of logs are retained for both Windows and Firewall events. What data retention controls must be configured?

A. maxTotalDataSizeMB and frozenTimePeriodInSecs

B. coldToFrozenDir and coldToFrozenScript

C. Splunk Volume and maxTotalDataSizMB

D. Splunk Volume and frozenTimePeriodInSecs

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/Indexer/Setaretirementandarchivingpolicy

QUESTION 5

What is the primary driver behind implementing indexer clustering in a customer\\'s environment?

A. To improve resiliency as the search load increases.

B. To reduce indexing latency.

C. To scale out a Splunk environment to offer higher performance capability.

D. To provide higher availability for buckets of data.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/Indexer/Howclusteredsearchworks

SPLK-3003 Study Guide SPLK-3003 Exam Questions SPLK-3003 Braindumps