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.leads4pass.com/splk-3003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

QUESTION 1

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 2

Which of the following statements applies to indexer discovery?

A. The Cluster Master (CM) can automatically discover new indexers added to the cluster.

B. Forwarders can automatically discover new indexers added to the cluster.

C. Deployment servers can automatically configure new indexers added to the cluster.

D. Search heads can automatically discover new indexers added to the cluster.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/DistSearch/
Connectclustersearchheadstosearchpeers

QUESTION 3

An index receives approximately 50GB of data per day per indexer at an even and consistent rate. The customer would like to keep this data searchable for a minimum of 30 days. In addition, they have hourly scheduled searches that process a week\\'s worth of data and are quite sensitive to search performance.

Given ideal conditions (no restarts, nor drops/bursts in data volume), and following PS best practices, which of the following sets of indexes.conf settings can be leveraged to meet the requirements?

A. frozenTimePeriodInSecs, maxDataSize, maxVolumeDataSizeMB, maxHotBuckets

B. maxDataSize, maxTotalDataSizeMB, maxHotBuckets, maxGlobalDataSizeMB

C. maxDataSize, frozenTimePeriodInSecs, maxVolumeDataSizeMB

D. frozenTimePeriodInSecs, maxWarmDBCount, homePath.maxDataSizeMB, maxHotSpanSecs

Correct Answer: B

QUESTION 4

When monitoring and forwarding events collected from a file containing unstructured textual events, what is the difference in the Splunk2Splunk payload traffic sent between a universal forwarder (UF) and indexer compared to the Splunk2Splunk payload sent between a heavy forwarder (HF) and the indexer layer? (Assume that the file is being monitored locally on the forwarder.)

A. The payload format sent from the UF versus the HF is exactly the same. The payload size is identical because they\\'re both sending 64K chunks.

B. The UF sends a stream of data containing one set of medata fields to represent the entire stream, whereas the HF sends individual events, each with their own metadata fields attached, resulting in a lager payload.

C. The UF will generally send the payload in the same format, but only when the sourcetype is specified in the inputs.conf and EVENT_BREAKER_ENABLE is set to true.

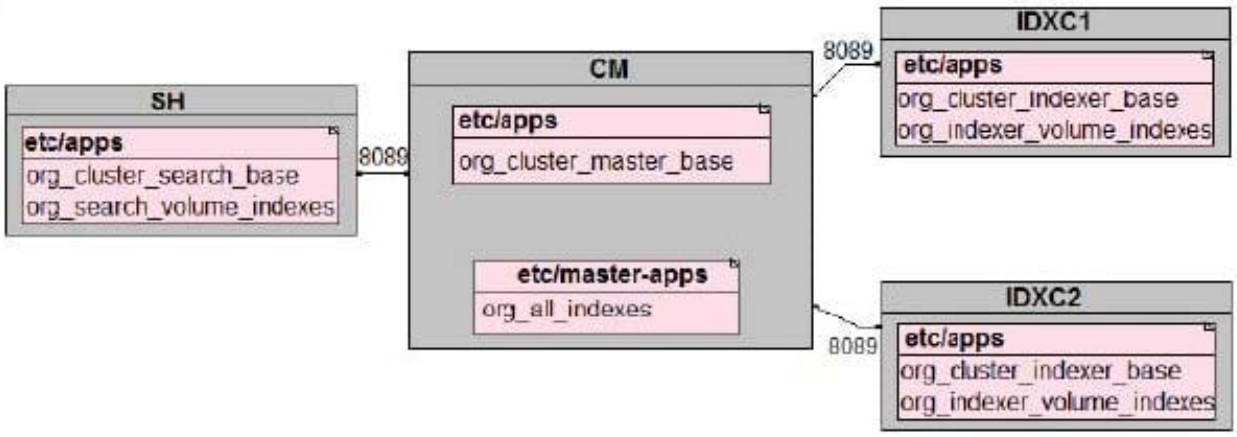
D. The HF sends a stream of 64K TCP chunks with one set of metadata fields attached to represent the entire stream, whereas the UF sends individual events, each with their own metadata fields attached.

Correct Answer: B

QUESTION 5

In preparation for the deployment of a new environment for a customer, which of the following mappings are correct per PS best practices?

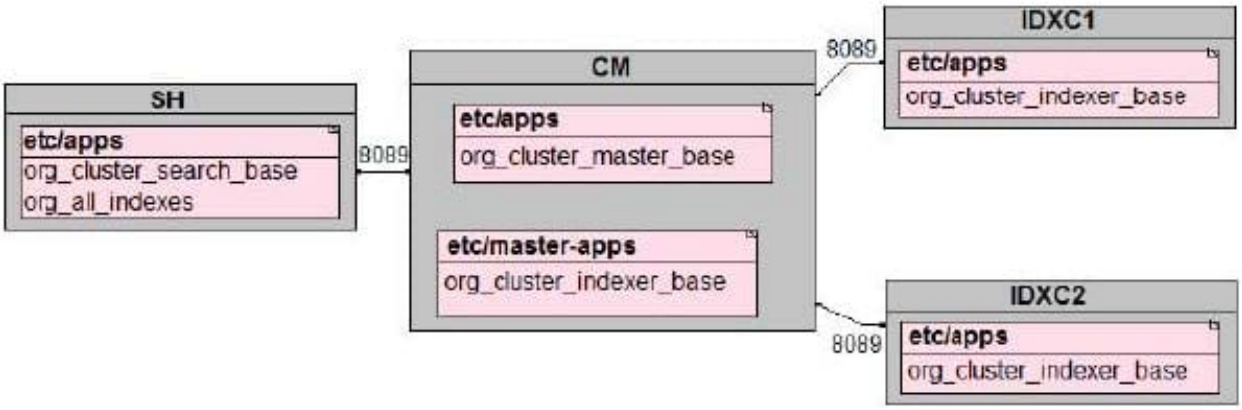
A.


SH
etc/apps
org_cluster_search_base
org_search_volume_indexes
8089
CM
etc/apps
org_cluster_master_base
etc/master-apps
org_all_indexes
8089
IDXC1
etc/apps
org_cluster_indexer_base
org_indexer_volume_indexes
8089
IDXC2
etc/apps
org_cluster_indexer_base
org_indexer_volume_indexes

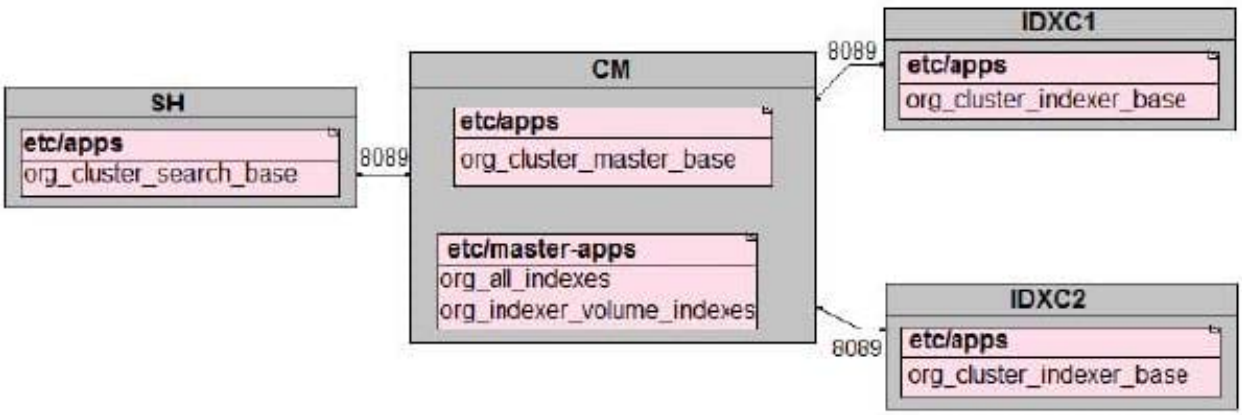
B.


SH
etc/apps
org_cluster_search_base
org_search_volume_indexes
org_all_indexes
8089
CM
etc/apps
org_cluster_master_base
etc/master-apps
org_all_indexes
org_indexer_volume_indexes
8089
IDXC1
etc/apps
org_cluster_indexer_base
8089
IDXC2
etc/apps
org_cluster_indexer_base

C.


SH
etc/apps
org_cluster_search_base
org_all_indexes
8089
CM
etc/apps
org_cluster_master_base
etc/master-apps
org_cluster_indexer_base
8089
IDXC1
etc/apps
org_cluster_indexer_base
8089
IDXC2
etc/apps
org_cluster_indexer_base

D.


SH
etc/apps
org_cluster_search_base
8089
CM
etc/apps
org_cluster_master_base
etc/master-apps
org_all_indexes
org_indexer_volume_indexes
8089
IDXC1
etc/apps
org_cluster_indexer_base
8089
IDXC2
etc/apps
org_cluster_indexer_base

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B