Free Questions for SPLK-2002 by ebraindumps

Shared by Wolf on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Which search head cluster component is responsible for pushing knowledge bundles to search peers, replicating configuration changes to search head cluster members, and scheduling jobs across the search head cluster?

Options:

A- Master

B- Captain

C- Deployer

D- Deployment server

Answer:

B

Question 2

Question Type: **MultipleChoice**

To optimize the distribution of primary buckets; when does primary rebalancing automatically occur? (Select all that apply.)

Options:

A- Rolling restart completes.

B- Master node rejoins the cluster.

C- Captain joins or rejoins cluster.

D- A peer node joins or rejoins the cluster.

Answer:

A, B, D

Question 3

Question Type: **MultipleChoice**

Which search will show all deployment client messages from the client (UF)?

Options:

A- index=_audit component=DC* host=<ds> | stats count by message

B- index=_audit component=DC* host=<uf> | stats count by message

C- index=_internal component= DC* host=<uf> | stats count by message

D- index=_internal component=DS* host=<ds> | stats count by message

Answer:

D

Question 4

Question Type: **MultipleChoice**

Before users can use a KV store, an admin must create a collection. Where is a collection is defined?

Options:

A- kvstore.conf

B- collection.conf

C- collections.conf

D- kvcollections.conf

Answer:

C

Question 5

Question Type: **MultipleChoice**

Which of the following statements describe a Search Head Cluster (SHC) captain? (Select all that apply.)

Options:

A- Is the job scheduler for the entire SHC.

B- Manages alert action suppressions (throttling).

C- Synchronizes the member list with the KV store primary.

D- Replicates the SHC's knowledge bundle to the search peers.

Answer:

A, D

Question 6

Question Type: MultipleChoice

Which Splunk internal index contains license-related events?

Options:

A- _audit

B- _license

C- _internal

D- _introspection

Answer:

C

Question 7

Question Type: **MultipleChoice**

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?

Options:

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.

Answer:

C

Question 8

Question Type: **MultipleChoice**

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

Options:

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.

Answer:

A

Question 9

Question Type: MultipleChoice

At which default interval does metrics.log generate a periodic report regarding license utilization?

Options:

A- 10 seconds

B- 30 seconds

C- 60 seconds

D- 300 seconds

Answer:

B

Question 10

Question Type: **MultipleChoice**

To reduce the captain's work load in a search head cluster, what setting will prevent scheduled searches from running on the captain?

Options:

A- adhoc_searchhead = true (on all members)

B- adhoc_searchhead = true (on the current captain)

C- captain_is_adhoc_searchhead = true (on all members)

D- captain_is_adhoc_searchhead = true (on the current captain)

Answer:

D