Free Questions for SPLK-3003 by dumpssheet

Shared by Sellers on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is the default push mode for a search head cluster deployer app configuration bundle?

Options:

A- full

B- merge_to_default

C- default_only

D- local_only

Answer:

B

Question 2

Question Type: MultipleChoice

What does Splunk do when it indexes events?

Options:

A- Extracts the top 10 fields.

B- Extracts metadata fields such as host, source, sourcetype.

C- Performs parsing, merging, and typing processes on universal forwarders.

D- Create report acceleration summaries.

Answer:

B

Question 3

Question Type: **MultipleChoice**

A customer has the following Splunk instances within their environment: An indexer cluster consisting of a cluster master/master node and five clustered indexers, two search heads (no search head clustering), a deployment server, and a license master. The deployment server and license master are running on their own single-purpose instances. The customer would like to start using the Monitoring Console (MC) to monitor the whole environment.

On the MC instance, which instances will need to be configured as distributed search peers by specifying them via the UI using the settings menu?

Options:

A- Just the cluster master/master node.

B- Indexers, search heads, deployment server, license master, cluster master/master node.

C- Search heads, deployment server, license master, cluster master/master node

D- Deployment server, license master

Answer:

C

Question 4

Question Type: **MultipleChoice**

What happens when an index cluster peer freezes a bucket?

Options:

A- All indexers with a copy of the bucket will delete it.

B- The cluster master will ensure another copy of the bucket is made on the other peers to meet the replication settings.

C- The cluster master will no longer perform fix-up activities for the bucket.

D- All indexers with a copy of the bucket will immediately roll it to frozen.

Answer:

C

Question 5

Question Type: **MultipleChoice**

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?

Options:

A- maxTotalDataSizeMB and frozenTimePeriodInSecs

B- coldToFrozenDir and coldToFrozenScript

C- Splunk Volume and maxTotalDataSizMB

D- Splunk Volume and frozenTimePeriodInSecs

Answer:

A

Question 6

Question Type: **MultipleChoice**

Which of the following statements applies to indexer discovery?

Options:

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.

Answer:

D

Question 7

Question Type: MultipleChoice

Data can be onboarded using apps, Splunk Web, or the CLI.

Which is the PS preferred method?

Options:

A- Create UDP input port 9997 on a UF.

B- Use the add data wizard in Splunk Web.

C- Use the inputs.conf file.

D- Use a scripted input to monitor a log file.

Answer:

B