Free Questions for SPLK-3003 by go4braindumps

Shared by Castillo on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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.)

Options:

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.

Answer:

B

Question 2

Question Type: MultipleChoice

The universal forwarder (UF) should be used whenever possible, as it is smaller and more efficient. In which of the following scenarios would a heavy forwarder (HF) be a more appropriate choice?

Options:

A- When a predictable version of Python is required.

B- When filtering 10%--15% of incoming events.

C- When monitoring a log file.

D- When running a script.

Answer:

B

Question 3

Question Type: MultipleChoice

A non-ES customer has a concern about data availability during a disaster recovery event. Which of the following Splunk Validated Architectures (SVAs) would be recommended for that use case?

Options:

A- Topology Category Code: M4

B- Topology Category Code: M14

C- Topology Category Code: C13

D- Topology Category Code: C3

Answer:

B

Question 4

Question Type: MultipleChoice

Which statement is correct?

Options:

A- In general, search commands that can be distributed to the search peers should occur as early as possible in a well-tuned search.

B- As a streaming command, streamstats performs better than stats since stats is just a reporting command.

C- When trying to reduce a search result to unique elements, the dedup command is the only way to achieve this.

D- Formatting commands such as fieldformat should occur as early as possible in the search to take full advantage of the often larger number of search peers.

Answer:

D

Question 5

Question Type: **MultipleChoice**

Which event processing pipeline contains the regex replacement processor that would be called upon to run event masking routines on events as they are ingested?

Options:

A- Merging pipeline

B- Indexing pipeline

C- Typing pipeline

D- Parsing pipeline

Answer:

A

Question 6

Question Type: **MultipleChoice**

What happens to the indexer cluster when the indexer Cluster Master (CM) runs out of disk space?

Options:

A- A warm standby CM needs to be brought online as soon as possible before an indexer has an outage.

B- The indexer cluster will continue to operate as long as no indexers fail.

C- If the indexer cluster has site failover configured in the CM, the second cluster master will take over.

D- The indexer cluster will continue to operate as long as a replacement CM is deployed within 24 hours.

Answer:

C

Question 7

Question Type: **MultipleChoice**

In addition to the normal responsibilities of a search head cluster captain, which of the following is a default behavior?

Options:

A- The captain is not a cluster member and does not perform normal search activities.

B- The captain is a cluster member who performs normal search activities.

C- The captain is not a cluster member but does perform normal search activities.

D- The captain is a cluster member but does not perform normal search activities.

Answer:

B

Question 8

Question Type: **MultipleChoice**

In an environment that has Indexer Clustering, the Monitoring Console (MC) provides dashboards to monitor environment health. As the environment grows over time and new indexers are added, which steps would ensure the MC is aware of the additional indexers?

Options:

A- No changes are necessary, the Monitoring Console has self-configuration capabilities.

B- Using the MC setup UI, review and apply the changes.

C- Remove and re-add the cluster master from the indexer clustering UI page to add new peers, then apply the changes under the MC setup UI.

D- Each new indexer needs to be added using the distributed search UI, then settings must be saved under the MC setup UI.

Answer:

B

To Get Premium Files for SPLK-3003 Visit

https://www.p2pexams.com/products/splk-3003

For More Free Questions Visit

https://www.p2pexams.com/splunk/pdf/splk-3003