SPLK-3003$^{Q\&As}$

Splunk Core Certified Consultant

QUESTION 1

Which configuration item should be set to false to significantly improve data ingestion performance?

A. AUTO_KV_JSON

B. BREAK_ONLY_BEFORE_DATE

C. SHOULD_LINEMERGE

D. ANNOTATE_PUNCT

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.6/Data/Configureeventlinebreaking

QUESTION 2

When can the Search Job Inspector be used to debug searches?

A. If the search has not expired.

B. If the search is currently running.

C. If the search has been queued.

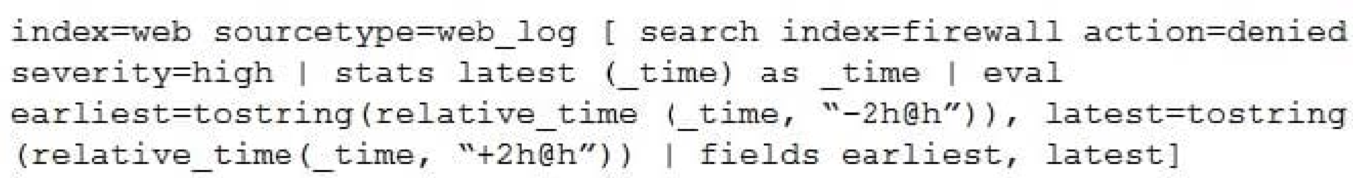
D. If the search has expired.

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/Search/ ViewsearchjobpropertieswiththeJobInspector

QUESTION 3

Consider the search shown below.



```
index=web sourcetype=web_log [ search index=firewall action=denied
severity=high | stats latest (_time) as _time | eval
earliest=tostring(relative_time (_time, "-2h@h")), latest=tostring
(relative_time(_time, "+2h@h")) | fields earliest, latest]
```

What is this search\\'s intended function?

A. To return all the web_log events from the web index that occur two hours before and after the most recent high severity, denied event found in the firewall index.

B. To find all the denied, high severity events in the firewall index, and use those events to further search for lateral movement within the web index.

C. To return all the web_log events from the web index that occur two hours before and after all high severity, denied events found in the firewall index.

D. To search the firewall index for web logs that have been denied and are of high severity.

Correct Answer: C

QUESTION 4

When setting up a multisite search head and indexer cluster, which nodes are required to declare site membership?

A. Search head cluster members, deployer, indexers, cluster master

B. Search head cluster members, deployment server, deployer, indexers, cluster master

C. All splunk nodes, including forwarders, must declare site membership

D. Search head cluster members, indexers, cluster master

Correct Answer: D

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

QUESTION 5

As data enters the indexer, it proceeds through a pipeline where event processing occurs. In which pipeline does line breaking occur?

A. Indexing

B. Typing

C. Merging

D. Parsing

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/Indexer/Howindexingworks#Event_processing_and_the_data_pipeline