Free Questions for SPLK-3003 by dumpshq

Shared by Delaney on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A customer with a large distributed environment has blacklisted a large lookup from the search bundle to decrease the bundle size using distsearch.conf. After this change, when running searches utilizing the lookup that was blacklisted they see error messages in the Splunk Search UI stating the lookup file does not exist.

What can the customer do to resolve the issue?

Options:

A- The search needs to be modified to ensure the lookup command specifies parameter local=true.

B- The blacklisted lookup definition stanza needs to be modified to specify setting allow_caching=true.

C- The search needs to be modified to ensure the lookup command specified parameter blacklist=false.

D- The lookup cannot be blacklisted; the change must be reverted.

Answer:

A

Question 2

Question Type: MultipleChoice

A customer is using regex to whitelist access logs and secure logs from a web server, but only the access logs are being ingested.
Which troubleshooting resource would provide insight into why the secure logs are not being ingested?

Options:

A- list monitor

B- oneshot

C- btprobe

D- tailingprocessor

Section: (none)

Explanation

Answer:

B

Question 3

Question Type: MultipleChoice

A customer has a multisite cluster (two sites, each site in its own data center) and users experiencing a slow response when searches are run on search heads located in either site. The Search Job Inspector shows the delay is being caused by search heads on either site waiting for results to be returned by indexers on the opposing site. The network team has confirmed that there is limited bandwidth available between the two data centers, which are in different geographic locations.

Which of the following would be the least expensive and easiest way to improve search performance?

Options:

A- Configure site_search_factor to ensure a searchable copy exists in the local site for each search head.

B- Move all indexers and search heads in one of the data centers into the same site.

C- Install a network pipe with more bandwidth between the two data centers.

D- Set the site setting on each indexer in the server.conf clustering stanza to be the same for all indexers regardless of site.

Answer:

A

Question 4

Question Type: MultipleChoice

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

Options:

A- Indexing

B- Typing

C- Merging

D- Parsing

Answer:

D

Question 5

Question Type: MultipleChoice

A customer has a network device that transmits logs directly with UDP or TCP over SSL. Using PS best practices, which ingestion method should be used?

Options:

A- Open a TCP port with SSL on a heavy forwarder to parse and transmit the data to the indexing tier.

B- Open a UDP port on a universal forwarder to parse and transmit the data to the indexing tier.

C- Use a syslog server to aggregate the data to files and use a heavy forwarder to read and transmit the data to the indexing tier.

D- Use a syslog server to aggregate the data to files and use a universal forwarder to read and transmit the data to the indexing tier.

Answer:

D

Question 6

Question Type: MultipleChoice

A customer is having issues with truncated events greater than 64K. What configuration should be deployed to a universal forwarder (UF) to fix the issue?

Options:

A- None. Splunk default configurations will process the events as needed; the UF is not causing truncation.

B- Configure the best practice magic 6 or great 8 props.conf settings.

C- EVENT_BREAKER_ENABLE and EVENT_BREAKER regular expression settings per sourcetype.

D- Global EVENT_BREAKER_ENABLE and EVENT_BREAKER regular expression settings.

Answer:

C

Question 7

Question Type: **MultipleChoice**

Where does the bloomfilter reside?

Options:

A- $SPLUNK_HOME/var/lib/splunk/indexfoo/db/db_1553504858_1553504507_8

B- $SPLUNK_HOME/var/lib/splunk/indexfoo/db/db_1553504858_1553504507_8/*.tsidx

C- $SPLUNK_HOME/var/lib/splunk/fishbucket

D- $SPLUNK_HOME/var/lib/splunk/indexfoo/db/db_1553504858_1553504507_8/rawdata

Answer:

C

Question 8

Question Type: MultipleChoice

Which command is most efficient in finding the pass4SymmKey of an index cluster?

Options:

A- find / -name server.conf --print | grep pass4SymKey

B- $SPLUNK_HOME/bin/splunk search | rest splunk_server=local /servicesNS/-/ unhash_app/storage/passwords

C- $SPLUNK_HOME/bin/splunk btool server list clustering | grep pass4SymmKey

D- $SPLUNK_HOME/bin/splunk btool clustering list clustering --debug | grep pass4SymmKey

Answer:

D

Question 9

Question Type: MultipleChoice

Report acceleration has been enabled for a specific use case. In which bucket location is the corresponding CSV file located?

Options:

A- thawedPath

B- summaryHomePath

C- tstatsHomePath

D- homePath, coldPath

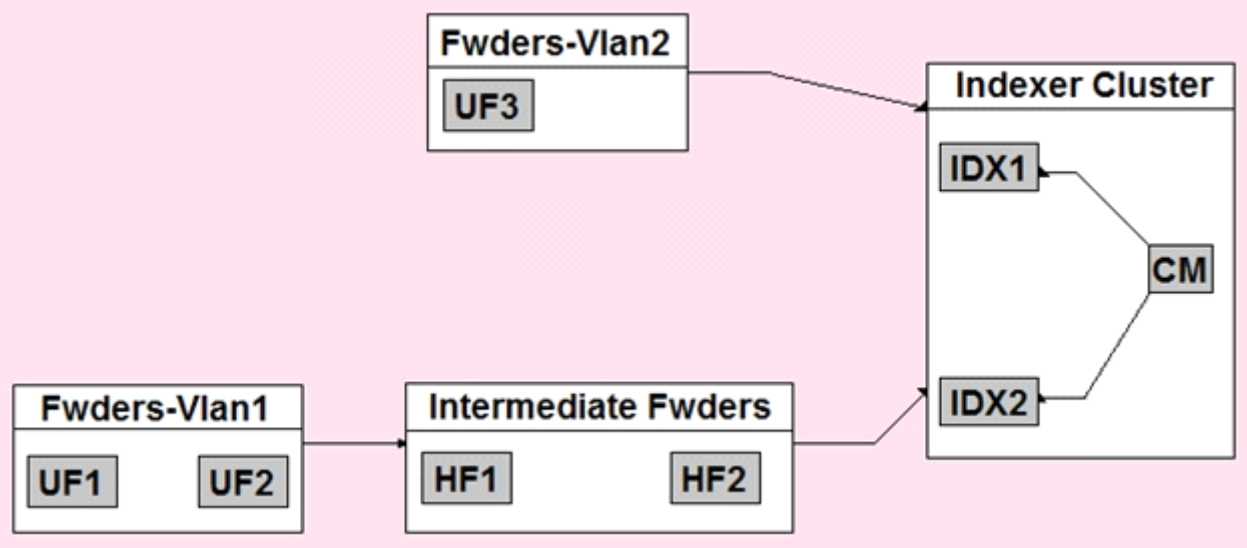
Answer:

B

Question 10

Question Type: MultipleChoice

In the diagrammed environment shown below, the customer would like the data read by the universal forwarders to set an indexed field containing the UF's host name. Where would the parsing configurations need to be installed for this to work?



Options:

A- All universal forwarders.

B- Only the indexers.

C- All heavy forwarders.

D- On all parsing Splunk instances.

Answer:

D