DUMPSARENA

Splunk Core Certified Consultant

Splunk SPLK-3003

Version Demo

Total Demo Questions: 10

Total Premium Questions: 85

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Where are Splunk Data Model Acceleration (DMA) summaries stored?

A. In tstatsHomePath

B. In the .tsidx files.

C. In summaryHomePath

D. In journal.gz

ANSWER: A

Explanation:

Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.0/Knowledge/Acceleratedatamodels#:~:text=Splunk%20software%20creates%20ad%20hoc,your%20indexes%20alongside% 20index%20buckets

QUESTION NO: 2

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

ANSWER: D

Explanation:

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

QUESTION NO: 3

When adding a new search head to a search head cluster (SHC), which of the following scenarios occurs?

A. The new search head connects to the captain and replays any recent configuration changes to bring it up to date.

B. The new search head connects to the deployer and replays any recent configuration changes to bring it up to date.

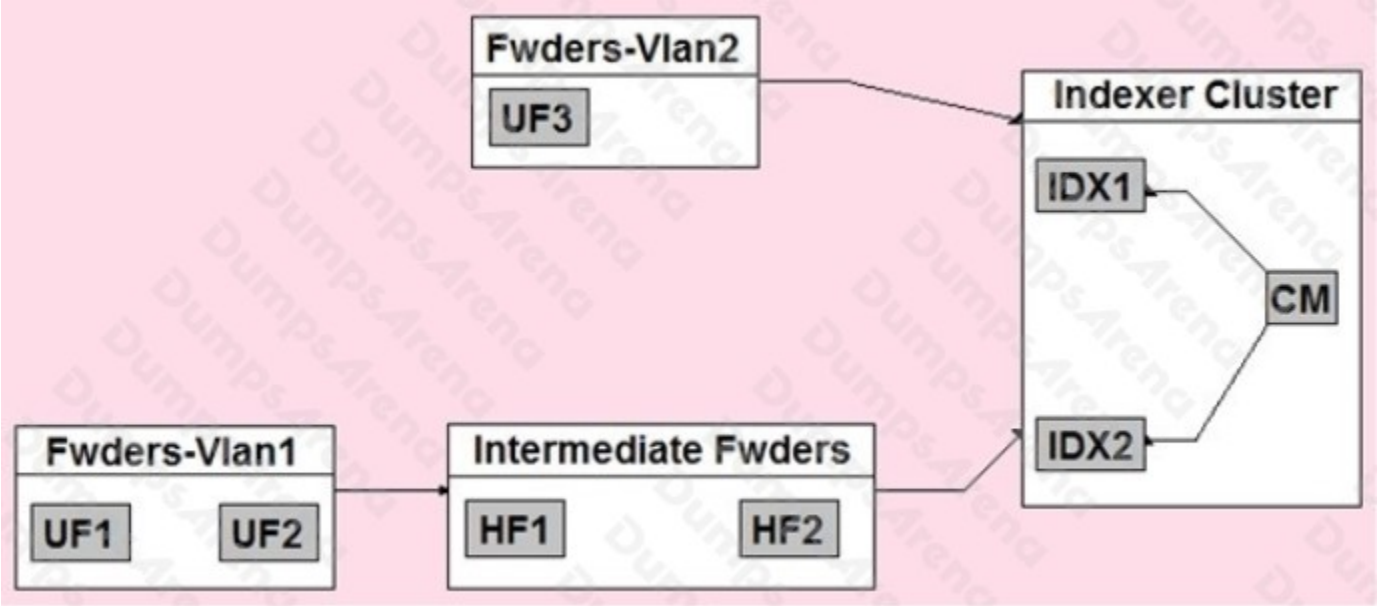
C. The new search head connects to the captain and pulls the most recently deployed bundle. It then connects to the deployer and replays any recent configuration changes to bring it up to date.

D. The new search head connects to the deployer and pulls the most recently deployed bundle. It then connects to the captain and replays any recent configuration changes to bring it up to date.

ANSWER: C

QUESTION NO: 4

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?



A. All universal forwarders.

B. Only the indexers.

C. All heavy forwarders.

D. On all parsing Splunk instances.

ANSWER: D

QUESTION NO: 5

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

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

Explanation:

Reference: https://community.splunk.com/t5/Deployment-Architecture/Which-instance-or-configuration-file-in-my-Splunk-environment/m-p/241486

QUESTION NO: 6

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?

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 NO: 7

Which of the following is the most efficient search?

A. index=www status=200 uri=/cart/checkout | append [search index = sales] | stats count, sum(revenue) as total_revenue by session_id | table total_revenue session_id

B. (index=www status=200 uri=/cart/checkout) OR (index=sales) | stats count, sum(revenue) as total_revenue by session_id | table total_revenue session_id

C. index=www | append [search index = sales] | stats count, sum(revenue) as total_revenue by session_id | table total_revenue session_id

D. (index=www) OR (index=sales) | search (index=www status=200 uri=/cart/checkout) OR (index=sales) | stats count, sum(revenue) as total_revenue by session_id | table total_revenue session_id

ANSWER: B

QUESTION NO: 8

A customer's deployment server is overwhelmed with forwarder connections after adding an additional 1000 clients. The default phone home interval is set to 60 seconds. To reduce the number of connection failures to the DS what is recommended?

A. Create a tiered deployment server topology.

B. Reduce the phone home interval to 6 seconds.

C. Leave the phone home interval at 60 seconds.

D. Increase the phone home interval to 600 seconds.

ANSWER: A

QUESTION NO: 9

The Splunk Validated Architectures (SVAs) document provides a series of approved Splunk topologies. Which statement accurately describes how it should be used by a customer?

A. Customer should look at the category tables, pick the highest number that their budget permits, then select this design topology as the chosen design.

B. Customers should identify their requirements, provisionally choose an approved design that meets them, then consider design principles and best practices to come to an informed design decision.

C. Using the guided requirements gathering in the SVAs document, choose a topology that suits requirements, and be sure not to deviate from the specified design.

D. Choose an SVA topology code that includes Search Head and Indexer Clustering because it offers the highest level of resilience.

ANSWER: B

Explanation:

Reference: https://www.splunk.com/en_us/blog/tips-and-tricks/splunk-validated-architectures.html

QUESTION NO: 10

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?

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