DUMPSQUEEN

Splunk Core Certified Consultant

Splunk SPLK-3003

Version Demo

Total Demo Questions: 10

Total Premium Questions: 85

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

QUESTION NO: 1

In a single indexer cluster, where should the Monitoring Console (MC) be installed?

A. Deployer sharing with master cluster.

B. License master that has 50 clients or more.

C. Cluster master node

D. Production Search Head

ANSWER: C

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/DMC/WheretohostDMC

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

A new single-site three indexer cluster is being stood up with replication_factor:2, search_factor:2. At which step would the Indexer Cluster be classed as ‘Indexing Ready’ and be able to ingest new data?

Step 1: Install and configure Cluster Master (CM)/Master Node with base clustering stanza settings, restarting CM.

Step 2: Configure a base app in etc/master-apps on the CM to enable a splunktcp input on port 9997 and deploy index creation configurations.

Step 3: Install and configure Indexer 1 so that once restarted, it contacts the CM, download the latest config bundle.

Step 4: Indexer 1 restarts and has successfully joined the cluster.

Step 5: Install and configure Indexer 2 so that once restarted, it contacts the CM, downloads the latest config bundle Step 6: Indexer 2 restarts and has successfully joined the cluster.

Step 7: Install and configure Indexer 3 so that once restarted, it contacts the CM, downloads the latest config bundle. Step 8: Indexer 3 restarts and has successfully joined the cluster.

A. Step 2

B. Step 4

C. Step 6

D. Step 8

ANSWER: A

QUESTION NO: 4

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

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

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/DistSearch/SHCarchitecture#Search_head_cluster_captain

QUESTION NO: 5

What does Splunk do when it indexes events?

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

Explanation:

Reference:
https://docs.splunk.com/Documentation/Splunk/8.1.0/Indexer/Howindexingworks#:~:text=Splunk%20Enterprise%20can%20index%20any,events%20indexes%20and%20metrics% 20indexes

QUESTION NO: 6

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?

A. Merging pipeline

B. Indexing pipeline

C. Typing pipeline

D. Parsing pipeline

ANSWER: A

QUESTION NO: 7

A [script://] input sends data to a Splunk forwarder using which method?

A. UDP stream

B. TCP stream

C. Temporary file

D. STDOUT/STDERR

ANSWER: C

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/latest/Admin/inputsconf

QUESTION NO: 8

A customer has a number of inefficient regex replacement transforms being applied. When under heavy load the indexers are struggling to maintain the expected indexing rate. In a worst case scenario, which queue(s) would be expected to fill up?

A. Typing, merging, parsing, input

B. Parsing

C. Typing

D. Indexing, typing, merging, parsing, input

ANSWER: B

QUESTION NO: 9

A customer has been using Splunk for one year, utilizing a single/all-in-one instance. This single Splunk server is now struggling to cope with the daily ingest rate. Also, Splunk has become a vital system in day-to-day operations making high availability a consideration for the Splunk service. The customer is unsure how to design the new environment topology in order to provide this.

Which resource would help the customer gather the requirements for their new architecture?

A. Direct the customer to the docs.splunk.com and tell them that all the information to help them select the right design is documented there.

B. Ask the customer to engage with the sales team immediately as they probably need a larger license.

C. Refer the customer to answers.splunk.com as someone else has probably already designed a system that meets their requirements.

D. Refer the customer to the Splunk Validated Architectures document in order to guide them through which approved architectures could meet their requirements.

ANSWER: D

Explanation:

Reference: https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf

QUESTION NO: 10

What happens when an index cluster peer freezes a bucket?

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

Explanation:

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/Indexer/Bucketsandclusters