SPLK-2002^Q&As

Splunk Enterprise Certified Architect

Pass Splunk SPLK-2002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/splk-2002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

QUESTION 1

In search head clustering, which of the following methods can you use to transfer captaincy to a different member? (Select all that apply.)

A. Use the Monitoring Console.

B. Use the Search Head Clustering settings menu from Splunk Web on any member.

C. Run the splunk transfer shcluster-captain command from the current captain.

D. Run the splunk transfer shcluster-captain command from the member you would like to become the captain.

Correct Answer: BD

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/Transfercaptain

QUESTION 2

In which phase of the Splunk Enterprise data pipeline are indexed extraction configurations processed?

A. Input

B. Search

C. Parsing

D. Indexing

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Admin/ Configurationparametersandthedatapipeline

QUESTION 3

When adding or rejoining a member to a search head cluster, the following error is displayed: Error pulling configurations from the search head cluster captain; consider performing a destructive configuration resync on this search head cluster member.

What corrective action should be taken?

A. Restart the search head.

B. Run the splunk apply shcluster-bundle command from the deployer.

C. Run the clean raft command on all members of the search head cluster.

D. Run the splunk resync shcluster-replicated-config command on this member.

Correct Answer: B

QUESTION 4

Which Splunk internal index contains license-related events?

A. _audit

B. _license

C. _internal

D. _introspection

Correct Answer: C

Reference: https://answers.splunk.com/answers/579494/how-to-display-license-consumed-by-an-indexover-2.html

QUESTION 5

A new Splunk customer is using syslog to collect data from their network devices on port 514. What is the best practice for ingesting this data into Splunk?

A. Configure syslog to send the data to multiple Splunk indexers.

B. Use a Splunk indexer to collect a network input on port 514 directly.

C. Use a Splunk forwarder to collect the input on port 514 and forward the data.

D. Configure syslog to write logs and use a Splunk forwarder to collect the logs.

Correct Answer: C

Reference: https://wiki.splunk.com/Community:BestPracticeForConfiguringSyslogInput

QUESTION 6

The guidance Splunk gives for estimating size on for syslog data is 50% of original data size. How does this divide between files in the index?

A. rawdata is: 10%, tsidx is: 40%

B. rawdata is: 15%, tsidx is: 35%

C. rawdata is: 35%, tsidx is: 15%

D. rawdata is: 40%, tsidx is: 10%

Correct Answer: B

Reference: https://answers.splunk.com/answers/147951/what-is-the-compression-ratio-of-raw-data-insplunk.html

QUESTION 7

Which of the following will cause the greatest reduction in disk size requirements for a cluster of N indexers running Splunk Enterprise Security?

A. Setting the cluster search factor to N-1.

B. Increasing the number of buckets per index.

C. Decreasing the data model acceleration range.

D. Setting the cluster replication factor to N-1.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Systemrequirements

QUESTION 8

Which of the following clarification steps should be taken if apps are not appearing on a deployment client? (Select all that apply.)

A. Check serverclass.conf of the deployment server.

B. Check deploymentclient.conf of the deployment client.

C. Check the content of SPLUNK_HOME/etc/apps of the deployment server.

D. Search for relevant events in splunkd.log of the deployment server.

Correct Answer: ABC

Reference: https://answers.splunk.com/answers/177021/why-is-deployment-client-not-picking-upchanges-to.html

QUESTION 9

How does the average run time of all searches relate to the available CPU cores on the indexers?

A. Average run time is independent of the number of CPU cores on the indexers.

B. Average run time decreases as the number of CPU cores on the indexers decreases.

C. Average run time increases as the number of CPU cores on the indexers decreases.

D. Average run time increases as the number of CPU cores on the indexers increases.

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Capacity/ Accommodatemanysimultaneoussearches

QUESTION 10

A Splunk architect has inherited the Splunk deployment at Buttercup Games and end users are complaining that the events are inconsistently formatted for a web sourcetype. Further investigation reveals that not all web logs flow through the same infrastructure: some of the data goes through heavy forwarders and some of the forwarders are managed by another department. Which of the following items might be the cause for this issue?

A. The search head may have different configurations than the indexers.

B. The data inputs are not properly configured across all the forwarders.

C. The indexers may have different configurations than the heavy forwarders.

D. The forwarders managed by the other department are an older version than the rest.

Correct Answer: D

QUESTION 11

When troubleshooting monitor inputs, which command checks the status of the tailed files?

A. splunk cmd btool inputs list | tail

B. splunk cmd btool check inputs layer

C. curl https://serverhost:8089/services/admin/inputstatus/TailingProcessor:FileStatus

D. curl https://serverhost:8089/services/admin/inputstatus/TailingProcessor:Tailstatus

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/
Troubleshoottheinputprocess#Troubleshoot_your_tailed_files

QUESTION 12

Which server.conf attribute should be added to the master node\\'s server.conf file when decommissioning a site in an indexer cluster?

A. site_mappings

B. available_sites

C. site_search_factor

D. site_replication_factor

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Decommissionasite

QUESTION 13

A Splunk instance has the following settings in SPLUNK_HOME/etc/system/local/server.conf:

[clustering] mode = master replication_factor = 2 pass4SymmKey = password123

Which of the following statements describe this Splunk instance? (Select all that apply.)

A. This is a multi-site cluster.

B. This cluster\\'s search factor is 2.

C. This Splunk instance needs to be restarted.

D. This instance is missing the master_uri attribute.

Correct Answer: AC

QUESTION 14

What is the algorithm used to determine captaincy in a Splunk search head cluster?

A. Raft distributed consensus.

B. Rapt distributed consensus.

C. Rift distributed consensus.

D. Round-robin distribution consensus.

Correct Answer: A

Reference: https://answers.splunk.com/answers/664102/need-to-know-about-raft-directory-on-searchhead-c.html

QUESTION 15

What is the default log size for Splunk internal logs?

A. 10MB

B. 20 MB

C. 25MB

D. 30MB

Correct Answer: C

Reference: https://answers.splunk.com/answers/959/how-can-i-control-the-size-and-number-of-splunksinternal-logs.html