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.leads4pass.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

How does IT Service Intelligence (ITSI) impact the planning of a Splunk deployment?

A. ITSI requires a dedicated deployment server.

B. The amount of users using ITSI will not impact performance.

C. ITSI in a Splunk deployment does not require additional hardware resources.

D. Depending on the Key Performance Indicators that are being tracked, additional infrastructure may be needed.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/ITSI/4.3.1/Install/Plan

QUESTION 2

A customer plans to ingest 600 GB of data per day into Splunk. They will have six concurrent users, and they also want high data availability and high search performance. The customer is concerned about cost and wants to spend the minimum amount on the hardware for Splunk.

How many indexers are recommended for this deployment?

A. Two indexers not in a cluster, assuming users run many long searches.

B. Three indexers not in a cluster, assuming a long data retention period.

C. Two indexers clustered, assuming high availability is the greatest priority.

D. Two indexers clustered, assuming a high volume of saved/scheduled searches.

Correct Answer: D

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

QUESTION 3

Which command will permanently decommission a peer node operating in an indexer cluster?

A. splunk stop -f

B. splunk offline -f

C. splunk offline --enforce-counts

D. splunk decommission --enforce counts

Correct Answer: C

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

QUESTION 4

To optimize the distribution of primary buckets; when does primary rebalancing automatically occur? (Select all that apply.)

A. Rolling restart completes.

B. Master node rejoins the cluster.

C. Captain joins or rejoins cluster.

D. A peer node joins or rejoins the cluster.

Correct Answer: ABD

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

QUESTION 5

Which of the following is a best practice to maximize indexing performance?

A. Use automatic sourcetyping.

B. Use the Splunk default settings.

C. Not use pre-trained source types.

D. Minimize configuration generality.

Correct Answer: D

QUESTION 6

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 7

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 8

Which Splunk tool offers a health check for administrators to evaluate the health of their Splunk deployment?

A. btool

B. DiagGen

C. SPL Clinic

D. Monitoring Console

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/DMC/DMCoverview

QUESTION 9

Which search head cluster component is responsible for pushing knowledge bundles to search peers, replicating configuration changes to search head cluster members, and scheduling jobs across the search head cluster?

A. Master

B. Captain

C. Deployer

D. Deployment server

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/DistSearch/SHCarchitecture

QUESTION 10

In the deployment planning process, when should a person identify who gets to see network data?

A. Deployment schedule

B. Topology diagramming

C. Data source inventory

D. Data policy definition

Correct Answer: C

QUESTION 11

Which CLI command converts a Splunk instance to a license slave?

A. splunk add licenses

B. splunk list licenser-slaves

C. splunk edit licenser-localslave

D. splunk list licenser-localslave

Correct Answer: C

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

QUESTION 12

Which of the following are true statements about Splunk indexer clustering?

A. All peer nodes must run exactly the same Splunk version.

B. The master node must run the same or a later Splunk version than search heads.

C. The peer nodes must run the same or a later Splunk version than the master node.

D. The search head must run the same or a later Splunk version than the peer nodes.

Correct Answer: B

Reference: https://answers.splunk.com/answers/760348/search-head-version-compatibility.html

QUESTION 13

A search head has successfully joined a single site indexer cluster. Which command is used to configure the same search head to join another indexer cluster?

A. splunk add cluster-config

B. splunk add cluster-master

C. splunk edit cluster-config

D. splunk edit cluster-master

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.2/Indexer/Configuremulti-clustersearch

QUESTION 14

A customer has installed a 500GB Enterprise license. They also purchased and installed a 300GB, no enforcement license on the same license master. How much data can the customer ingest before search is locked out?

A. 300GB. After this limit, search is locked out.

B. 500GB. After this limit, search is locked out.

C. 800GB. After this limit, search is locked out.

D. Search is not locked out. Violations are still recorded.

Correct Answer: D

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

QUESTION 15

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