

Splunk

Exam Questions SPLK-2002

Splunk Enterprise Certified Architect



NEW QUESTION 1

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.

Answer: D

NEW QUESTION 2

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. 300G
- B. After this limit, search is locked out
- C. B.500G
- D. After this limit, search is locked out.
- E. 800G
- F. After this limit, search is locked out.
- G. Search is not locked out
- H. Violations are still recorded.

Answer: D

NEW QUESTION 3

Which of the following are client filters available in serverclass.conf? (Select all that apply.)

- A. DNS name.
- B. IP address.
- C. Splunk server role.
- D. Platform (machine type).

Answer: AB

NEW QUESTION 4

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

Answer: D

NEW QUESTION 5

Which component in the splunkd.log will log information related to bad event breaking?

- A. Audittrail
- B. EventBreaking
- C. IndexingPipeline
- D. AggregatorMiningProcessor

Answer: D

NEW QUESTION 6

Indexing is slow and real-time search results are delayed in a Splunk environment with two indexers and one search head. There is ample CPU and memory available on the indexers. Which of the following is most likely to improve indexing performance?

- A. Increase the maximum number of hot buckets in indexes.conf
- B. Increase the number of parallel ingestion pipelines in server.conf
- C. Decrease the maximum size of the search pipelines in limits.conf
- D. Decrease the maximum concurrent scheduled searches in limits.conf

Answer: D

NEW QUESTION 7

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%

Answer: B

NEW QUESTION 8

In an existing Splunk environment, the new index buckets that are created each day are about half the size of the incoming data. Within each bucket, about 30% of the space is used for rawdata and about 70% for index files.

What additional information is needed to calculate the daily disk consumption, per indexer, if indexer clustering is implemented?

- A. Total daily indexing volume, number of peer nodes, and number of accelerated searches.
- B. Total daily indexing volume, number of peer nodes, replication factor, and search factor.
- C. Total daily indexing volume, replication factor, search factor, and number of search heads.
- D. Replication factor, search factor, number of accelerated searches, and total disk size across cluster.

Answer: D

NEW QUESTION 9

A three-node search head cluster is skipping a large number of searches across time. What should be done to increase scheduled search capacity on the search head cluster?

- A. Create a job server on the cluster.
- B. Add another search head to the cluster.
- C. `server.conf` `captain_is_adhoc_searchhead = true`.
- D. Change `limits.conf` value for `max_searches_per_cpu` to a higher value.

Answer: D

NEW QUESTION 10

To activate replication for an index in an indexer cluster, what attribute must be configured in `indexes.conf` on all peer nodes?

- A. `repFactor = 0`
- B. `replicate = 0`
- C. `repFactor = auto`
- D. `replicate = auto`

Answer: C

NEW QUESTION 10

Which of the following is a good practice for a search head cluster deployer?

- A. The deployer only distributes configurations to search head cluster members when they "phone home".
- B. The deployer must be used to distribute non-replicable configurations to search head cluster members.
- C. The deployer must distribute configurations to search head cluster members to be valid configurations.
- D. The deployer only distributes configurations to search head cluster members with `splunk apply shcluster-bundle`.

Answer: A

NEW QUESTION 12

Which Splunk internal index contains licenserelated events?

- A. `_audit`
- B. `_license`
- C. `_internal`
- D. `_introspection`

Answer: C

NEW QUESTION 16

Which search will show all deployment client messages from the client (UF)?

- A. `index=_audit component=DC* host=<ds> | stats count by message`
- B. `index=_audit component=DC* host=<uf> | stats count by message`
- C. `index=_internal component= DC* host=<uf> | stats count by message`
- D. `index=_internal component=DS* host=<ds> | stats count by message`

Answer: D

NEW QUESTION 17

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.

Answer: ABD

NEW QUESTION 21

Configurations from the deployer are merged into which location on the search head cluster member?

- A. SPLUNK_HOME/etc/system/local
- B. SPLUNK_HOME/etc/apps/APP_HOME/local
- C. SPLUNK_HOME/etc/apps/search/default
- D. SPLUNK_HOME/etc/apps/APP_HOME/default

Answer: A

NEW QUESTION 25

When Splunk indexes data in a non clustered environment, what kind of files does it create by default?

- A. Index and .tsidx files.
- B. Rawdata and index files.
- C. Compressed and .tsidx files.
- D. Compressed and meta data files.

Answer: B

NEW QUESTION 26

What does setting site=site0 on all Search Head Cluster members do in a multi-site indexer cluster?

- A. Disables search site affinity.
- B. Sets all members to dynamic captaincy.
- C. Enables multisite search artifact replication.
- D. Enables automatic search site affinity discovery.

Answer: A

NEW QUESTION 27

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

- A. Input
- B. Search
- C. Parsing
- D. Indexing

Answer: C

NEW QUESTION 31

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

Answer: B

NEW QUESTION 33

To improve Splunk performance, parallelIngestionPipelines setting can be adjusted on which of the following components in the Splunk architecture? (Select all that apply.)

- A. Indexers
- B. Forwarders
- C. Search head
- D. Cluster master

Answer: AB

NEW QUESTION 35

When adding or decommissioning a member from a Search Head Cluster (SHC), what is the proper order of operations?

- A. 1. Delete Splunk Enterprise, if it exists.2. Install and initialize the instance.3. Join the SHC.
- B. 1. Install and initialize the instance.2. Delete Splunk Enterprise, if it exists.3. Join the SHC.
- C. 1. Initialize cluster rebalance operation.2. Remove master node from cluster.3. Trigger replication.
- D. 1. Trigger replication.2. Remove master node from cluster.3. Initialize cluster rebalance operation.

Answer: B

NEW QUESTION 37

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

- A. Use automatic sourcetypes.
- B. Use the Splunk default settings.
- C. Not use pre-trained source types.
- D. Minimize configuration generality.

Answer: D

NEW QUESTION 41

When should multiple search pipelines be enabled?

- A. Only if disk IOPS is at 800 or better.
- B. Only if there are fewer than twelve concurrent users.
- C. Only if running Splunk Enterprise version 6.6 or later.
- D. Only if CPU and memory resources are significantly under-utilized.

Answer: D

NEW QUESTION 46

Which of the following is an indexer clustering requirement?

- A. Must use shared storage.
- B. Must reside on a dedicated rack.
- C. Must have at least three members.
- D. Must share the same license pool.

Answer: D

NEW QUESTION 51

As a best practice, where should the internal licensing logs be stored?

- A. Indexing layer.
- B. License server.
- C. Deployment layer.
- D. Search head layer.

Answer: D

NEW QUESTION 54

A Splunk user successfully extracted an ip address into a field called src_ip. Their colleague cannot see that field in their search results with events known to have src_ip. Which of the following may explain the problem? (Select all that apply.)

- A. The field was extracted as a private knowledge object.
- B. The events are tagged as communicate, but are missing the network tag.
- C. The Typing Queue, which does regular expression replacements, is blocked.
- D. The colleague did not explicitly use the field in the search and the search was set to Fast Mode.

Answer: D

NEW QUESTION 57

Which of the following tasks should the architect perform when building a deployment plan? (Select all that apply.)

- A. Use case checklist.
- B. Install Splunk apps.
- C. Inventory data sources.
- D. Review network topology.

Answer: D

NEW QUESTION 59

Because Splunk indexing is read/write intensive, it is important to select the appropriate disk storage solution for each deployment. Which of the following statements is accurate about disk storage?

- A. High performance SAN should never be used.
- B. Enable NFS for storing hot and warm buckets.
- C. The recommended RAID setup is RAID 10 (1 + 0).
- D. Virtualized environments are usually preferred over bare metal for Splunk indexers.

Answer: C

NEW QUESTION 60

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SPLK-2002 Practice Exam Features:

- * SPLK-2002 Questions and Answers Updated Frequently
- * SPLK-2002 Practice Questions Verified by Expert Senior Certified Staff
- * SPLK-2002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SPLK-2002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SPLK-2002 Practice Test Here](#)