

# Splunk

## Exam Questions SPLK-2002

Splunk Enterprise Certified Architect





#### NEW QUESTION 1

Stakeholders have identified high availability for searchable data as their top priority. Which of the following best addresses this requirement?

- A. Increasing the search factor in the cluster.
- B. Increasing the replication factor in the cluster.
- C. Increasing the number of search heads in the cluster.
- D. Increasing the number of CPUs on the indexers in the cluster.

**Answer: B**

#### NEW QUESTION 2

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 3

When using the props.conf LINE\_BREAKER attribute to delimit multi-line events, the SHOULD\_LINEMERGE attribute should be set to what?

- A. Auto
- B. None
- C. True
- D. False

**Answer: C**

#### NEW QUESTION 4

A multi-site indexer cluster can be configured using which of the following? (Select all that apply.)

- A. Via Splunk Web.
- B. Directly edit SPLUNK\_HOME/etc/system/local/server.conf
- C. Run a splunk edit cluster-config command from the CLI.
- D. Directly edit SPLUNK\_HOME/etc/system/default/server.conf

**Answer: AB**

#### NEW QUESTION 5

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 6

What log file would you search to verify if you suspect there is a problem interpreting a regular expression in a monitor stanza?

- A. btool.log
- B. metrics.log
- C. splunkd.log
- D. tailing\_processor.log

**Answer: C**

#### NEW QUESTION 7

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.

**Answer: B**



#### NEW QUESTION 8

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 9

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 10

Which of the following security options must be explicitly configured (i.e. which options are not enabled by default)?

- A. Data encryption between Splunk Web and splunkd.
- B. Certificate authentication between forwarders and indexers.
- C. Certificate authentication between Splunk Web and search head.
- D. Data encryption for distributed search between search heads and indexers.

**Answer: B**

#### NEW QUESTION 10

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.

**Answer: B**

#### NEW QUESTION 11

To reduce the captain's work load in a search head cluster, what setting will prevent scheduled searches from running on the captain?

- A. `adhoc_searchhead = true` (on all members)
- B. `adhoc_searchhead = true` (on the current captain)
- C. `captain_is_adhoc_searchhead = true` (on all members)
- D. `captain_is_adhoc_searchhead = true` (on the current captain)

**Answer: D**

#### NEW QUESTION 15

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 17

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.

**Answer: C**

#### NEW QUESTION 18

Which Splunk internal index contains licenserelated events?



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

**Answer:** C

#### NEW QUESTION 19

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 20

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 25

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

**Answer:** B

#### NEW QUESTION 29

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 32

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 33

The KV store forms its own cluster within a SHC. What is the maximum number of SHC members KV store will form?

- A. 25
- B. 50
- C. 100
- D. Unlimited

**Answer:** D

#### NEW QUESTION 34

Which command is used for thawing the archive bucket?

- A. Splunk collect
- B. Splunk convert
- C. Splunk rebuild



D. Splunk dbinspect

**Answer:** C

**NEW QUESTION 36**

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

**Answer:** A

**NEW QUESTION 39**

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 42**

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 47**

Which of the following statements about integrating with third-party systems is true? (Select all that apply.)

- A. A Hadoop application can search data in Splunk.
- B. Splunk can search data in the Hadoop File System (HDFS).
- C. You can use Splunk alerts to provision actions on a third-party system.
- D. You can forward data from Splunk forwarder to a third-party system without indexing it first.

**Answer:** CD

**NEW QUESTION 50**

Which of the following statements describe search head clustering? (Select all that apply.)

- A. A deployer is required.
- B. At least three search heads are needed.
- C. Search heads must meet the high-performance reference server requirements.
- D. The deployer must have sufficient CPU and network resources to process service requests and push configurations.

**Answer:** AC

**NEW QUESTION 55**

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 57**

.....



## 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](#)**