



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

What does the deployer do in a Search Head Cluster (SHC)? (Select all that apply.)

- A. Distributes apps to SHC members.
- B. Bootstraps a clean Splunk install for a SHC.
- C. Distributes non-search related and manual configuration file changes.
- D. Distributes runtime knowledge object changes made by users across the SHC.

Answer: A

NEW QUESTION 4

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 5

Which index-time props.conf attributes impact indexing performance? (Select all that apply.)

- A. REPORT
- B. LINE_BREAKER
- C. ANNOTATE_PUNCT
- D. SHOULD_LINEMERGE

Answer: BD

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

In a four site indexer cluster, which configuration stores two searchable copies at the origin site, one searchable copy at site2, and a total of four searchable copies?

- A. site_search_factor = origin:2, site1:2, total:4
- B. site_search_factor = origin:2, site2:1, total:4
- C. site_replication_factor = origin:2, site1:2, total:4
- D. site_replication_factor = origin:2, site2:1, total:4

Answer: D

NEW QUESTION 8

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 9

Which Splunk server role regulates the functioning of indexer cluster?

- A. Indexer
- B. Deployer
- C. Master Node
- D. Monitoring Console

Answer: C

NEW QUESTION 10

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 10

The frequency in which a deployment client contacts the deployment server is controlled by what?

- A. polling_interval attribute in outputs.conf
- B. phoneHomeIntervalInSecs attribute in outputs.conf
- C. polling_interval attribute in deploymentclient.conf
- D. phoneHomeIntervalInSecs attribute in deploymentclient.conf

Answer: D

NEW QUESTION 12

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

Answer: C

NEW QUESTION 13

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.

Answer: D

NEW QUESTION 15

Which Splunk internal index contains licenserelated events?

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

Answer: C

NEW QUESTION 16

Which of the following statements describe a Search Head Cluster (SHC) captain? (Select all that apply.)

- A. Is the job scheduler for the entire SHC.
- B. Manages alert action suppressions (throttling).
- C. Synchronizes the member list with the KV store primary.
- D. Replicates the SHC's knowledge bundle to the search peers.

Answer: AD

NEW QUESTION 18

Before users can use a KV store, an admin must create a collection. Where is a collection is defined?

- A. kvstore.conf
- B. collection.conf
- C. collections.conf
- D. kvcollections.conf

Answer: C

NEW QUESTION 22

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 24

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.

Answer: D

NEW QUESTION 29

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.

Answer: BD

NEW QUESTION 34

Which of the following describe migration from single-site to multisite index replication?

- A. A master node is required at each site.
- B. Multisite policies apply to new data only.
- C. Single-site buckets instantly receive the multisite policies.
- D. Multisite total values should not exceed any single-site factors.

Answer: D

NEW QUESTION 36

Which of the following is a way to exclude search artifacts when creating a diag?

- A. SPLUNK_HOME/bin/splunk diag --exclude
- B. SPLUNK_HOME/bin/splunk diag --debug --refresh
- C. SPLUNK_HOME/bin/splunk diag --disable=dispatch
- D. SPLUNK_HOME/bin/splunk diag --filter-searchstrings

Answer: A

NEW QUESTION 40

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 42

Which tool(s) can be leveraged to diagnose connection problems between an indexer and forwarder? (Select all that apply.)

- A. telnet
- B. tcpdump
- C. splunk btool
- D. splunk btprobe

Answer: BC

NEW QUESTION 44

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

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

Answer: D

NEW QUESTION 47

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 51

Of the following types of files within an index bucket, which file type may consume the most disk?

- A. Rawdata
- B. Bloom filter
- C. Metadata (.data)
- D. Inverted index (.tsidx)

Answer: B

NEW QUESTION 52

When converting from a single-site to a multi-site cluster, what happens to existing single-site clustered buckets?

- A. They will continue to replicate within the origin site and age out based on existing policies.
- B. They will maintain replication as required according to the single-site policies, but never age out.
- C. They will be replicated across all peers in the multi-site cluster and age out based on existing policies.
- D. They will stop replicating within the single-site and remain on the indexer they reside on and age out according to existing policies.

Answer: B

NEW QUESTION 55

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 60

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.

Answer: C

NEW QUESTION 61

In a distributed environment, knowledge object bundles are replicated from the search head to which location on the search peer(s)?

- A. SPLUNK_HOME/var/lib/searchpeers
- B. SPLUNK_HOME/var/log/searchpeers
- C. SPLUNK_HOME/var/run/searchpeers
- D. SPLUNK_HOME/var/spool/searchpeers

Answer: C

NEW QUESTION 66

Consider a use case involving firewall data. There is no Splunk-supported Technical Add-On, but the vendor has built one. What are the items that must be evaluated before installing the add-on? (Select all that apply.)

- A. Identify number of scheduled or real-time searches.
- B. Validate if this Technical Add-On enables event data for a data model.
- C. Identify the maximum number of forwarders Technical Add-On can support.
- D. Verify if Technical Add-On needs to be installed onto both a search head or indexer.

Answer: AC

NEW QUESTION 69

Which two sections can be expanded using the Search Job Inspector?

- A. Execution costs.
- B. Saved search history.
- C. Search job properties.
- D. Optimization suggestions.

Answer: BC

NEW QUESTION 70

What is the logical first step when starting a deployment plan?

- A. Inventory the currently deployed logging infrastructure.
- B. Determine what apps and use cases will be implemented.
- C. Gather statistics on the expected adoption of Splunk for sizing.
- D. Collect the initial requirements for the deployment from all stakeholders.

Answer: D

NEW QUESTION 73

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 76

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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](#)