

Splunk

Exam Questions SPLK-2002

Splunk Enterprise Certified Architect



NEW QUESTION 1

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 2

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 3

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 4

Which Splunk server role regulates the functioning of indexer cluster?

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

Answer: C

NEW QUESTION 5

Which of the following commands is used to clear the KV store?

- A. splunk clean kvstore
- B. splunk clear kvstore
- C. splunk delete kvstore
- D. splunk reinitialize kvstore

Answer: A

NEW QUESTION 6

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 7

What is the minimum reference server specification for a Splunk indexer?

- A. 12 CPU cores, 12GB RAM, 800 IOPS
- B. 16 CPU cores, 16GB RAM, 800 IOPS
- C. 24 CPU cores, 16GB RAM, 1200 IOPS
- D. 28 CPU cores, 32GB RAM, 1200 IOPS

Answer: A

NEW QUESTION 8

Which of the following artifacts are included in a Splunk diag file? (Select all that apply.)

- A. OS settings.
- B. Internal logs.
- C. Customer data.
- D. Configuration files.

Answer: BD

NEW QUESTION 9

Which of the following can a Splunk diag contain?

- A. Search history, Splunk users and their roles, running processes, indexed data
- B. Server specs, current open connections, internal Splunk log files, index listings
- C. KV store listings, internal Splunk log files, search peer bundles listings, indexed data
- D. Splunk platform configuration details, Splunk users and their roles, current open connections, index listings

Answer: B

NEW QUESTION 10

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 10

Which Splunk internal index contains licenserelated events?

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

Answer: C

NEW QUESTION 15

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 20

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 23

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 25

Which of the following statements describe licensing in a clustered Splunk deployment? (Select all that apply.)

- A. Free licenses do not support clustering.
- B. Replicated data does not count against licensing.

- C. Each cluster member requires its own clustering license.
- D. Cluster members must share the same license pool and license master.

Answer: BD

NEW QUESTION 27

When planning a search head cluster, which of the following is true?

- A. All search heads must use the same operating system.
- B. All search heads must be members of the cluster (no standalone search heads).
- C. The search head captain must be assigned to the largest search head in the cluster.
- D. All indexers must belong to the underlying indexer cluster (no standalone indexers).

Answer: C

NEW QUESTION 29

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 32

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 37

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 40

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 45

When configuring a Splunk indexer cluster, what are the default values for replication and search factor?

- A. replication_factor = 2 search_factor = 2
- B. replication_factor = 2 searchfactor = 3
- C. replication_factor = 3 search_factor = 2
- D. replication_factor = 3 searchfactor = 3

Answer: A

NEW QUESTION 47

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 48

.....

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](#)