

Exam Questions SPLK-2002

Splunk Enterprise Certified Architect

<https://www.2passeasy.com/dumps/SPLK-2002/>



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 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

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

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 6

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 7

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 8

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 9

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 10

Which Splunk Enterprise offering has its own license?

- A. Splunk Cloud Forwarder
- B. Splunk Heavy Forwarder
- C. Splunk Universal Forwarder
- D. Splunk Forwarder Management

Answer: C

NEW QUESTION 10

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 12

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 16

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 21

Which of the following clarification steps should be taken if apps are not appearing on a deployment client? (Select all that apply.)

- A. Check serverclass.conf of the deployment server.
- B. Check deploymentclient.conf of the deployment client.
- C. Check the content of SPLUNK_HOME/etc/apps of the deployment server.
- D. Search for relevant events in splunkd.log of the deployment server.

Answer: ABC

NEW QUESTION 22

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 24

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 28

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

Answer: C

NEW QUESTION 29

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 30

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 32

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 35

Which Splunk internal index contains licenserelated events?

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

Answer: C

NEW QUESTION 38

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 41

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 42

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 46

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

Answer: C

NEW QUESTION 47

A Splunk instance has the following settings in SPLUNK_HOME/etc/system/local/server.conf:

```
[clustering] mode = master
replication_factor = 2
pass4SymmKey = password123
```

Which of the following statements describe this Splunk instance? (Select all that apply.)

- A. This is a multi-site cluster.
- B. This cluster's search factor is 2.
- C. This Splunk instance needs to be restarted.
- D. This instance is missing the master_uri attribute.

Answer: AC

NEW QUESTION 51

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 55

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 57

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 59

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 64

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 67

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 71

Which of the following should be done when installing Enterprise Security on a Search Head Cluster? (Select all that apply.)

- A. Install Enterprise Security on the deployer.
- B. Install Enterprise Security on a staging instance.
- C. Copy the Enterprise Security configurations to the deployer.
- D. Use the deployer to deploy Enterprise Security to the cluster members.

Answer: AD

NEW QUESTION 72

Splunk configuration parameter settings can differ between multiple .conf files of the same name contained within different apps. Which of the following directories has the highest precedence?

- A. System local directory.
- B. System default directory.
- C. App local directories, in ASCII order.
- D. App default directories, in ASCII order.

Answer: A

NEW QUESTION 73

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 76

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 77

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 79

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 83

What is the default log size for Splunk internal logs?

- A. 10MB
- B. 20 MB
- C. 25MB
- D. 30MB

Answer: C

NEW QUESTION 86

What is a Splunk Job? (Select all that apply.)

- A. A user-defined Splunk capability.
- B. Searches that are subjected to some usage quota.
- C. A search process kicked off via a report or an alert.
- D. A child OS process manifested from the splunkd process.

Answer: A

NEW QUESTION 90

When Splunk is installed, where are the internal indexes stored by default?

- A. SPLUNK_HOME/bin
- B. SPLUNK_HOME/var/lib
- C. SPLUNK_HOME/var/run
- D. SPLUNK_HOME/etc/system/default

Answer: B

NEW QUESTION 93

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 97

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-2002 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-2002 Product From:

<https://www.2passeasy.com/dumps/SPLK-2002/>

Money Back Guarantee

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