

Splunk

Exam Questions SPLK-2002

Splunk Enterprise Certified Architect



NEW QUESTION 1

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 2

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 3

Which of the following is true regarding Splunk Enterprise performance? (Select all that apply.)

- A. Adding search peers increases the maximum size of search results.
- B. Adding RAM to an existing search heads provides additional search capacity.
- C. Adding search peers increases the search throughput as search load increases.
- D. Adding search heads provides additional CPU cores to run more concurrent searches.

Answer: BD

NEW QUESTION 4

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 5

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 6

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 7

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

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

Answer: D

NEW QUESTION 8

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 9

Splunk Enterprise platform instrumentation refers to data that the Splunk Enterprise deployment logs in the _introspection index. Which of the following logs are included in this index? (Select all that apply.)

- A. audit.log
- B. metrics.log
- C. disk_objects.log
- D. resource_usage.log

Answer: CD

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 10

At which default interval does metrics.log generate a periodic report regarding license utilization?

- A. 10 seconds
- B. 30 seconds
- C. 60 seconds
- D. 300 seconds

Answer: B

NEW QUESTION 11

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 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 17

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 22

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 26

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 28

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 32

When troubleshooting monitor inputs, which command checks the status of the tailed files?

- A. splunk cmd btool inputs list | tail
- B. splunk cmd btool check inputs layer
- C. curl https://serverhost:8089/services/admin/inputstatus/TailingProcessor:FileStatus
- D. curl https://serverhost:8089/services/admin/inputstatus/TailingProcessor:Tailstatus

Answer: C

NEW QUESTION 33

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 34

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 38

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 43

Which of the following options can improve reliability of syslog delivery to Splunk? (Select all that apply.)

- A. Use TCP syslog.
- B. Configure UDP inputs on each Splunk indexer to receive data directly.
- C. Use a network load balancer to direct syslog traffic to active backend syslog listeners.
- D. Use one or more syslog servers to persist data with a Universal Forwarder to send the data to Splunk indexers.

Answer: CD

NEW QUESTION 48

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 50

.....

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](#)