

Splunk

Exam Questions SPLK-2002

Splunk Enterprise Certified Architect



NEW QUESTION 1

Which of the following will cause the greatest reduction in disk size requirements for a cluster of N indexers running Splunk Enterprise Security?

- A. Setting the cluster search factor to N-1.
- B. Increasing the number of buckets per index.
- C. Decreasing the data model acceleration range.
- D. Setting the cluster replication factor to N-1.

Answer: D

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

Which of the following should be included in a deployment plan?

- A. Business continuity and disaster recovery plans.
- B. Current logging details and data source inventory.
- C. Current and future topology diagrams of the IT environment.
- D. A comprehensive list of stakeholders, either direct or indirect.

Answer: D

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

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 7

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 8

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 9

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 10

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 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 13

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 17

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 22

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 25

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 26

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 29

Which Splunk internal index contains licenserelated events?

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

Answer: C

NEW QUESTION 30

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 34

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 37

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 42

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 46

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 49

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 50

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 54

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 58

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 59

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 61

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 65

What is the algorithm used to determine captaincy in a Splunk search head cluster?

- A. Raft distributed consensus.
- B. Rapt distributed consensus.
- C. Rift distributed consensus.
- D. Round-robin distribution consensus.

Answer: A

NEW QUESTION 70

As a best practice, where should the internal licensing logs be stored?

- A. Indexing layer.

- B. License server.
- C. Deployment layer.
- D. Search head layer.

Answer: D

NEW QUESTION 73

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 76

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 81

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 85

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 86

What is the default log size for Splunk internal logs?

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

Answer: C

NEW QUESTION 91

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 96

.....

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](#)