Actual exam question from Splunk's SPLK-2002

Question #: 1

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 2

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 3

Topic #: 1

[All SPLK-2002 Questions]

Search dashboards in the Monitoring Console indicate that the distributed deployment is approaching its capacity. Which of the following options will provide the most search performance improvement?

A. Replace the indexer storage to solid state drives (SSD).

B. Add more search heads and redistribute users based on the search type.

C. Look for slow searches and reschedule them to run during an off-peak time.

D. Add more search peers and make sure forwarders distribute data evenly across all indexers.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 4

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 5

Topic #: 1

[All SPLK-2002 Questions]

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. 300GB. After this limit, search is locked out.

B. 500GB. After this limit, search is locked out.

C. 800GB. After this limit, search is locked out.

D. Search is not locked out. Violations are still recorded.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 6

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 7

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 8

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 9

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 10

Topic #: 1

[All SPLK-2002 Questions]

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

A. REPORT

B. LINE_BREAKER

C. ANNOTATE_PUNCT

D. SHOULD_LINEMERGE

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 11

Topic #: 1

[All SPLK-2002 Questions]

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).

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 12

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 13

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 14

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 15

Topic #: 1

[All SPLK-2002 Questions]

Which Splunk Enterprise offering has its own license?

A. Splunk Cloud Forwarder

B. Splunk Heavy Forwarder

C. Splunk Universal Forwarder

D. Splunk Forwarder Management

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 16

Topic #: 1

[All SPLK-2002 Questions]

Which component in the splunkd.log will log information related to bad event breaking?

A. Audittrail

B. EventBreaking

C. IndexingPipeline

D. AggregatorMiningProcessor

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 17

Topic #: 1

[All SPLK-2002 Questions]

Which Splunk server role regulates the functioning of indexer cluster?

A. Indexer

B. Deployer

C. Master Node

D. Monitoring Console

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 18

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 19

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 20

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 21

Topic #: 1

[All SPLK-2002 Questions]

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%

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 22

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 23

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 24

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 25

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 26

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 27

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 28

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 29

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 30

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 31

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 32

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 33

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 34

Topic #: 1

[All SPLK-2002 Questions]

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)

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 35

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 36

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 37

Topic #: 1

[All SPLK-2002 Questions]

A new Splunk customer is using syslog to collect data from their network devices on port 514. What is the best practice for ingesting this data into Splunk?

A. Configure syslog to send the data to multiple Splunk indexers.

B. Use a Splunk indexer to collect a network input on port 514 directly.

C. Use a Splunk forwarder to collect the input on port 514 and forward the data.

D. Configure syslog to write logs and use a Splunk forwarder to collect the logs.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 38

Topic #: 1

[All SPLK-2002 Questions]

Which Splunk internal index contains license-related events?

A. _audit

B. _license

C. _internal

D. _introspection

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 39

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 40

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 41

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 42

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 43

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 44

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 45

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 46

Topic #: 1

[All SPLK-2002 Questions]

The KV store forms its own cluster within a SHC. What is the maximum number of SHC members KV store will form?

A. 25

B. 50

C. 100

D. Unlimited

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 47

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 48

Topic #: 1

[All SPLK-2002 Questions]

Which command is used for thawing the archive bucket?

A. Splunk collect

B. Splunk convert

C. Splunk rebuild

D. Splunk dbinspect

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 49

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 50

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 51

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 52

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 53

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 54

Topic #: 1

[All SPLK-2002 Questions]

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).

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 55

Topic #: 1

[All SPLK-2002 Questions]

In which phase of the Splunk Enterprise data pipeline are indexed extraction configurations processed?

A. Input

B. Search

C. Parsing

D. Indexing

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 56

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 57

Topic #: 1

[All SPLK-2002 Questions]

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

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 58

Topic #: 1

[All SPLK-2002 Questions]

A search head has successfully joined a single site indexer cluster. Which command is used to configure the same search head to join another indexer cluster?

A. splunk add cluster-config

B. splunk add cluster-master

C. splunk edit cluster-config

D. splunk edit cluster-master

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 59

Topic #: 1

[All SPLK-2002 Questions]

To improve Splunk performance, parallelIngestionPipelines setting can be adjusted on which of the following components in the Splunk architecture? (Select all that apply.)

A. Indexers

B. Forwarders

C. Search head

D. Cluster master

Show Suggested Answer

Actual exam question from Splunk's SPLK-2002

Question #: 60

Topic #: 1

[All SPLK-2002 Questions]

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.

Show Suggested Answer