Exam Questions SPLK-2002

Splunk Enterprise Certified Architect

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

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
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 3
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 4
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 5
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 6
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 7
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

Answer: D

NEW QUESTION 8

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 9
Which Splunk server role regulates the functioning of
indexer cluster?

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

Answer: C

NEW QUESTION 10
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 10
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 13
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 17
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 21
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 23
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.

Answer: D

NEW QUESTION 26
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 30
Which Splunk internal index contains licenserelated events?

A. audit
B. _license
C. _internal
D. _introspection

Answer: C

NEW QUESTION 32
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

Answer: C

NEW QUESTION 36
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

Answer: D

NEW QUESTION 37
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 38
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 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
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

Answer: D

NEW QUESTION 51
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 52
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 56
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 58
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 62
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 65
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 66
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

Answer: AB

NEW QUESTION 70
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 72
Which of the following is a best practice to maximize indexing performance?

A. Use automatic sourcetyping.
B. Use the Splunk default settings.
C. Not use pre-trained source types.
D. Minimize configuration generality.

Answer: D

NEW QUESTION 73
When converting from a single-site to a multi-site cluster, what happens to existing single-site clustered buckets?

A. They will continue to replicate within the origin site and age out based on existing policies.
B. They will maintain replication as required according to the single-site policies, but never age out.
C. They will be replicated across all peers in the multi-site cluster and age out based on existing policies.
D. They will stop replicating within the single-site and remain on the indexer they reside on and age out according to existing policies.

Answer: B

NEW QUESTION 76
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 79
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 82
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 83
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 88
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 90
.....

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