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
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.

Answer: C

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
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 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
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 7
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 8
Which Splunk server role regulates the functioning of

indexer cluster?

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

Answer: C

NEW QUESTION 9
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 10
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.

Answer: D

NEW QUESTION 10
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 13
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 18
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 19
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 21
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 25
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 26
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 29
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 32
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.

Answer: D

NEW QUESTION 33
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 36
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 38
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 41
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 43
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 46
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 48
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 49
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 51
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 56
What is the default log size for Splunk internal logs?

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

Answer: C

NEW QUESTION 58
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 61
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 66
.....

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