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
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.

Answer: B

NEW QUESTION 3
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 4
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. 300G
B. After this limit, search is locked ou
C. B.500G
D. After this limit, search is locked out.
E. 800G
F. After this limit, search is locked out.
G. Search is not locked ou
H. Violations are still recorded.

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
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 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 9
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 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
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 11
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 16
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 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 24
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 27
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 30
Which Splunk internal index contains licenserelated events?

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

Answer: C

NEW QUESTION 35
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 39
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 44
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 47
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 52
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 53
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 56
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 59
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 60
Which of the following statements about integrating with third-party systems is true? (Select all that apply.)

A. A Hadoop application can search data in Splunk.
B. Splunk can search data in the Hadoop File System (HDFS).
C. You can use Splunk alerts to provision actions on a third-party system.
D. You can forward data from Splunk forwarder to a third-party system without indexing it first.

Answer: CD

NEW QUESTION 63
In a distributed environment, knowledge object bundles are replicated from the search head to which location on the search peer(s)?

A. SPLUNK_HOME/var/lib/searchpeers
B. SPLUNK_HOME/var/log/searchpeers
C. SPLUNK_HOME/var/run/searchpeers
D. SPLUNK_HOME/var/spool/searchpeers

Answer: C

NEW QUESTION 66
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 67
What is a Splunk Job? (Select all that apply.)

A. A user-defined Splunk capability.
B. Searches that are subjected to some usage quota.
C. A search process kicked off via a report or an alert.
D. A child OS process manifested from the splunkd process.

Answer: A

NEW QUESTION 70
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 73
What is the logical first step when starting a deployment plan?

A. Inventory the currently deployed logging infrastructure.
B. Determine what apps and use cases will be implemented.
C. Gather statistics on the expected adoption of Splunk for sizing.
D. Collect the initial requirements for the deployment from all stakeholders.

Answer: D

NEW QUESTION 77
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 81
......