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 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 3
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

Answer: C

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 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 6
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 7
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

Answer:

D

NEW QUESTION 8
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 9
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 10
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 10
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 12
Which Splunk internal index contains licenserelated events?

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

Answer: C

NEW QUESTION 14
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 16
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 18
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 23
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 26
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 31
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 35
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.

Answer: BD

NEW QUESTION 37
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 41
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
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 48
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 51
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 54
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 59
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 63
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 66
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 67
When Splunk is installed, where are the internal indexes
stored by default?

A. SPLUNK_HOME/bin
B. SPLUNK_HOME/var/lib
C. SPLUNK_HOME/var/run

D. SPLUNK_HOME/etc/system/default

Answer: B

NEW QUESTION 68
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 72
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 77
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons 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