Exam Questions SPLK-2002

Splunk Enterprise Certified Architect

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

NEW QUESTION 1
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 2
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.

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 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
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 9
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 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
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 13
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

Answer: C

NEW QUESTION 15
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

Answer: B

NEW QUESTION 16
Which Splunk internal index contains licenserelated events?

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

Answer: C

NEW QUESTION 17

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 19
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 24
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 26
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 30
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.

Answer: A

NEW QUESTION 33
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 38
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 42
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 45
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 47
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 50
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 54
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 55
......