Exam Questions SPLK-2002

Splunk Enterprise Certified Architect

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

NEW QUESTION 1
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 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
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 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
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 7
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 8
Which of the following clarification steps should be taken if apps are not appearing on a deployment client? (Select all that apply.)

A. Check serverclass.conf of the deployment server.
B. Check deploymentclient.conf of the deployment client.
C. Check the content of SPLUNK_HOME/etc/apps of the deployment server.
D. Search for relevant events in splunkd.log of the deployment server.

Answer: ABC

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 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 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 13
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 18
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 20
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 25
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 28
Which Splunk internal index contains licenserelated events?

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

Answer: C

NEW QUESTION 32
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 35
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 39
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 44
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 49
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
In search head clustering, which of the following methods can you use to transfer captaincy to a different member? (Select all that apply.)

A. Use the Monitoring Console.

B. Use the Search Head Clustering settings menu from Splunk Web on any member.
C. Run the splunk transfer shcluster-captain command from the current captain.
D. Run the splunk transfer shcluster-captain command from the member you would like to become the captain.

Answer: BD

NEW QUESTION 56
Which command is used for thawing the archive bucket?

A. Splunk collect
B. Splunk convert
C. Splunk rebuild
D. Splunk dbinspect

Answer: C

NEW QUESTION 58
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 63
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 68
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 70
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 74
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 76
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 81
As a best practice, where should the internal licensing logs be stored?

A. Indexing layer.
B. License server.
C. Deployment layer.
D. Search head layer.

Answer: D

NEW QUESTION 84
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 88
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 93
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 96
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 97
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 102
......