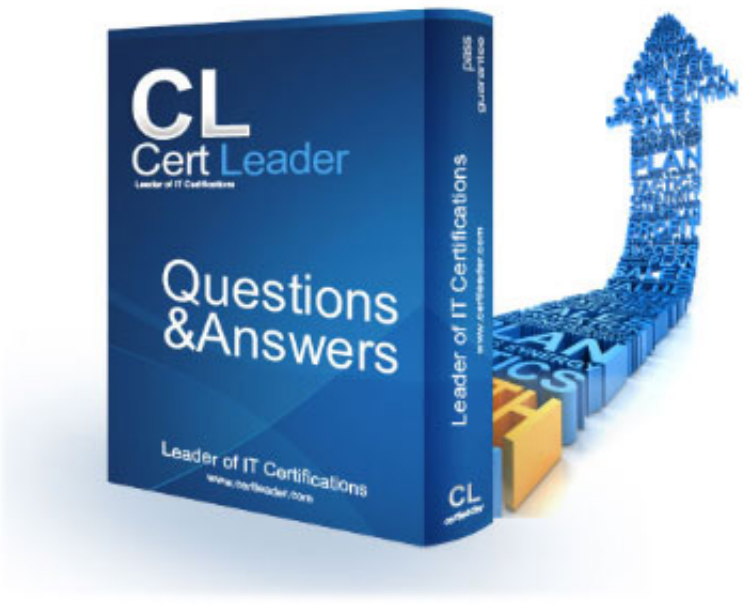
SPLK-2002 Dumps

Splunk Enterprise Certified Architect

https://www.certleader.com/SPLK-2002-dumps.html



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 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 5
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 6
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 7
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 8
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 9
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 10
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
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 14
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 18
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 22
Which of the following security options must be explicitly configured (i.e. which options are not enabled by default)?

A. Data encryption between Splunk Web and splunkd.
B. Certificate authentication between forwarders and indexers.
C. Certificate authentication between Splunk Web and search head.
D. Data encryption for distributed search between search heads and indexers.

Answer: B

NEW QUESTION 24
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 28
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 31
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 34
Which Splunk internal index contains licenserelated events?

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

Answer: C

NEW QUESTION 39
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 43
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 45
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 46
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 50
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 51
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 53
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 57
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 62
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 64
A search head has successfully joined a single site indexer cluster. Which command is used to configure the same search head to join another indexer cluster?

A. splunk add cluster-config
B. splunk add cluster-master
C. splunk edit cluster-config
D. splunk edit cluster-master

Answer: B

NEW QUESTION 67
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 71
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 73
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 75
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 80
Which of the following should be done when installing Enterprise Security on a Search Head Cluster? (Select all that apply.)

A. Install Enterprise Security on the deployer.
B. Install Enterprise Security on a staging instance.
C. Copy the Enterprise Security configurations to the deployer.
D. Use the deployer to deploy Enterprise Security to the cluster members.

Answer: AD

NEW QUESTION 84
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 86
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 90
How does the average run time of all searches relate to the available CPU cores on the indexers?

A. Average run time is independent of the number of CPU cores on the indexers.
B. Average run time decreases as the number of CPU cores on the indexers decreases.
C. Average run time increases as the number of CPU cores on the indexers decreases.
D. Average run time increases as the number of CPU cores on the indexers increases.

Answer: C

NEW QUESTION 95

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 99
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 103
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 104
Because Splunk indexing is read/write intensive, it is important to select the appropriate disk storage solution for each deployment. Which of the following statements is accurate about disk storage?

A. High performance SAN should never be used.
B. Enable NFS for storing hot and warm buckets.
C. The recommended RAID setup is RAID 10 (1 + 0).
D. Virtualized environments are usually preferred over bare metal for Splunk indexers.

Answer: C

NEW QUESTION 109
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SPLK-2002 Exam with Our Prep Materials Via below:

https://www.certleader.com/SPLK-2002-dumps.html