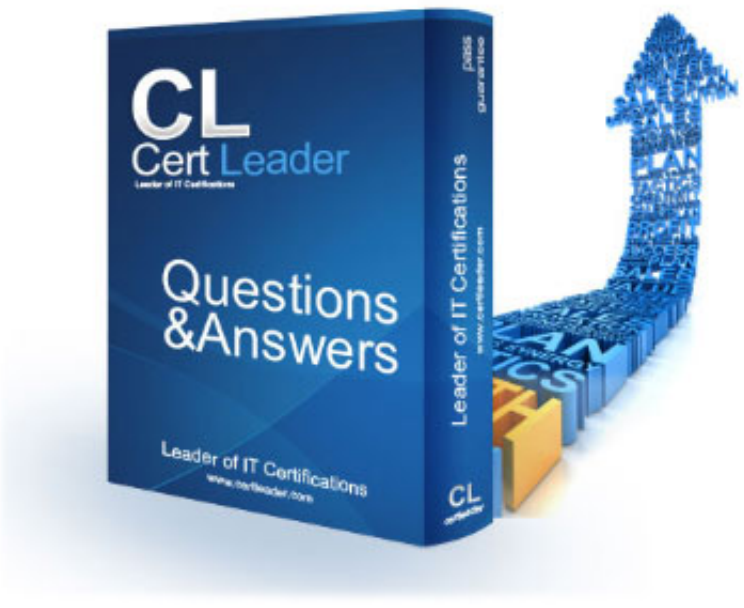
SPLK-2002 Dumps

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
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 4
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 5
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 6
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 7
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 8
Which Splunk server role regulates the functioning of indexer cluster?

A. Indexer
B. Deployer
C. Master Node
D. Monitoring Console

Answer: C

NEW QUESTION 9
Which of the following commands is used to clear the KV store?

A. splunk clean kvstore
B. splunk clear kvstore
C. splunk delete kvstore
D. splunk reinitialize kvstore

Answer: A

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
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 13
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 15
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 18
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 22
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 26
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 30
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 34
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 36
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 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 51
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 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 61
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 62
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 65
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 68
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 73
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 75
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 77
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 78
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 82
.....

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