Perfect Splunk - SPLK-2002 - Splunk Enterprise Certified Architect Valid Test Bootcamp

CertWizard.com
splunk>
CERTIFIED
Splunk Enterprise Certified Architect
Splunk Enterprise Certified Architect
Exam: SPLK-2002
CertWizard.com
Get Splunk SPLK-2002 exam passing assistance!
Pass your SPLK-2002 exam at home without stress!

P.S. Free & New SPLK-2002 dumps are available on Google Drive shared by PassLeader: https://drive.google.com/open?id=1Df9YUsCNMgUoNugGKxsBtw4WEHTL40X7

Everyone wants to stand out in such a competitive environment, but they don't know how to act. Maybe our SPLK-2002 exam questions can help you. Having a certificate may be something you have always dreamed of, because it can prove that you have a certain capacity. Our SPLK-2002 learning materials can provide you with meticulous help and help you get your certificate. Our SPLK-2002 training prep is credible and their quality can stand the test. Therefore, our SPLK-2002 practice materials can help you get a great financial return in the future and you will have a good quality of life.

The Splunk SPLK-2002 Exam is divided into two parts: the written exam and the practical lab exam. The written exam consists of 60 multiple-choice questions that cover topics such as Splunk Enterprise architecture, deployment planning, data ingestion, and search optimization. Candidates have 90 minutes to complete the written exam, and they must achieve a score of 70% or higher to pass.

>> SPLK-2002 Valid Test Bootcamp <<

Reliable SPLK-2002 Braindumps Sheet - Certification SPLK-2002 Cost

Of course, when we review a qualifying exam, we can't be closed-door. We should pay attention to the new policies and information related to the test SPLK-2002 certification. For the convenience of the users, the SPLK-2002 test materials will be updated on the homepage and timely update the information related to the qualification examination. Annual qualification examination, although content broadly may be the same, but as the policy of each year, the corresponding examination pattern grading standards and hot spots will be changed, as a result, the SPLK-2002 Test Prep can help users to spend the least time, you can know the test information directly what you care about on the learning platform that provided by us, let users save time and used their time in learning the new hot spot concerning about the knowledge content.

The Splunk Enterprise Certified Architect certification exam is an advanced-level certification that is intended for experienced Splunk professionals who have a deep understanding of the platform's architecture and deployment. SPLK-2002 exam covers various topics such as Splunk architecture, distributed search, indexing, data management, and deployment management. SPLK-2002 Exam Format consists of 60 multiple-choice questions that the candidate has to complete in 2 hours.

Splunk Enterprise Certified Architect Sample Questions (Q58-Q63):

NEW QUESTION # 58
Which search will show all deployment client messages from the client (UF)?

- A. index=_internal component=DS* host=<ds> | stats count by message
- B. index=_internal component= DC* host=<uf> | stats count by message
- C. index=_audit component=DC* host=<ds> | stats count by message
- D. index=_audit component=DC* host=<uf> | stats count by message

Answer: A

NEW QUESTION # 59

(A customer has a Splunk Enterprise deployment and wants to collect data from universal forwarders. What is the best step to secure log traffic?)

- A. Use the Splunk provided SSL certificates to encrypt data between the forwarders and indexers.
- B. Create signed SSL certificates and use them to encrypt data between the search heads and indexers.
- C. Create signed SSL certificates and use them to encrypt data between the forwarders and indexers.
- D. Ensure all forwarder traffic is routed through a web application firewall (WAF).

Answer: C

Explanation:
Splunk Enterprise documentation clearly states that the best method to secure log traffic between Universal Forwarders (UFs) and Indexers is to implement Transport Layer Security (TLS) using signed SSL certificates.
When Universal Forwarders send data to Indexers, this communication can be encrypted using SSL/TLS to prevent eavesdropping, data tampering, or interception while in transit.
Splunk provides default self-signed certificates out of the box, but these are only for testing or lab environments and should not be used in production. Production-grade security requires custom, signed SSL certificates - either from an internal Certificate Authority (CA) or a trusted public CA. These certificates validate both the sender (forwarder) and receiver (indexer), ensuring data integrity and authenticity.
In practice, this involves:
* Generating or obtaining CA-signed certificates.
* Configuring the forwarder's outputs.conf to use SSL encryption (sslCertPath, sslPassword, and sslRootCAPath).
* Configuring the indexer's inputs.conf and server.conf to require and validate client certificates.
This configuration ensures end-to-end encryption for all log data transmitted from forwarders to indexers.
Routing traffic through a WAF (Option C) does not provide end-to-end encryption for Splunk's internal communication, and securing search head-to-indexer communication (Option D) is unrelated to forwarder data flow.
References (Splunk Enterprise Documentation):
* Securing Splunk Enterprise: Encrypting Data in Transit Using SSL/TLS
* Configure Forwarder-to-Indexer Encryption
* Server and Forwarder Authentication with Signed Certificates
* Best Practices for Forwarder Management and Security Configuration

NEW QUESTION # 60

When adding or decommissioning a member from a Search Head Cluster (SHC), what is the proper order of operations?

- A. 1. Trigger replication.2. Remove master node from cluster.3. Initialize cluster rebalance operation.
- B. 1. Initialize cluster rebalance operation.2. Remove master node from cluster.3. Trigger replication.
- C. 1. Delete Splunk Enterprise, if it exists.2. Install and initialize the instance.3. Join the SHC.
- D. 1. Install and initialize the instance.2. Delete Splunk Enterprise, if it exists.3. Join the SHC.

Answer: D

NEW QUESTION # 61

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 the current captain)
- B. captain_is_adhoc_searchhead = true (on all members)
- C. adhoc_searchhead = true (on all members)
- D. captain_is_adhoc_searchhead = true (on the current captain)

Answer: D

Explanation:
Explanation
To reduce the captain's work load in a search head cluster, the setting that will prevent scheduled searches from running on the

captain is captain_is_adhoc_searchhead = true (on the current captain). This setting will designate the current captain as an ad hoc search head, which means that it will not run any scheduled searches, but only ad hoc searches initiated by users. This will reduce the captain's work load and improve the search head cluster performance. The adhoc_searchhead = true (on all members) setting will designate all search head cluster members as ad hoc search heads, which means that none of them will run any scheduled searches, which is not desirable. The adhoc_searchhead = true (on the current captain) setting will have no effect, as this setting is ignored by the captain. The captain_is_adhoc_searchhead = true (on all members) setting will have no effect, as this setting is only applied to the current captain. For more information, see Configure the captain as an ad hoc search head in the Splunk documentation.

NEW QUESTION # 62

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. Decrease the maximum size of the search pipelines in limits.conf
- C. Increase the number of parallel ingestion pipelines in server.conf
- D. Decrease the maximum concurrent scheduled searches in limits.conf

Answer: D

NEW QUESTION # 63

......