SPLK-3003 Q&As

Splunk Core Certified Consultant

Pass Splunk SPLK-3003 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/splk-3003.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

In which directory should base config app(s) be placed to initialize an indexer?

A. $SPLUNK_HOME/etc/

B. $SPLUNK_HOME/etc/apps

C. $SPLUNK_HOME/etc/system/local

D. $SPLUNK_HOME/etc/slave-apps

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/Indexer/Manageappdeployment

QUESTION 2

In addition to the normal responsibilities of a search head cluster captain, which of the following is a default behavior?

A. The captain is not a cluster member and does not perform normal search activities.

B. The captain is a cluster member who performs normal search activities.

C. The captain is not a cluster member but does perform normal search activities.

D. The captain is a cluster member but does not perform normal search activities.

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/Splunk/8.1.0/DistSearch/SHCarchitecture#Search_head_cluster_captain

QUESTION 3

A customer would like to remove the output_file capability from users with the default user role to stop them from filling up the disk on the search head with lookup files. What is the best way to remove this capability from users?

A. Create a new role without the output_file capability that inherits the default user role and assign it to the users.

B. Create a new role with the output_file capability that inherits the default user role and assign it to the users.

C. Edit the default user role and remove the output_file capability.

D. Clone the default user role, remove the output_file capability, and assign it to the users.

Correct Answer: C

QUESTION 4

Which of the following server roles should be configured for a host which indexes its internal logs locally?

A. Cluster master

B. Indexer

C. Monitoring Console (MC)

D. Search head

Correct Answer: B

Reference: https://community.splunk.com/t5/Deployment-Architecture/How-to-identify-Splunk-Instancerole-by-internal-logs/m-p/365555

QUESTION 5

A customer is using regex to whitelist access logs and secure logs from a web server, but only the access logs are being ingested. Which troubleshooting resource would provide insight into why the secure logs are not being ingested?

A. list monitor

B. oneshot

C. btprobe

D. tailingprocessor

Correct Answer: B

Latest SPLK-3003 Dumps SPLK-3003 PDF Dumps SPLK-3003 VCE Dumps