SPLK-3001 Q&As

Splunk Enterprise Security Certified Admin

Pass Splunk SPLK-3001 Exam with 100% Guarantee

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

https://www.geekcert.com/splk-3001.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

To which of the following should the ES application be uploaded?

A. The indexer.

B. The KV Store.

C. The search head.

D. The dedicated forwarder.

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallEnterpriseSecuritySHC

QUESTION 2

An administrator wants to ensure that none of the ES indexed data could be compromised through tampering. What feature would satisfy this requirement?

A. Index consistency.

B. Data integrity control.

C. Indexer acknowledgement.

D. Index access permissions.

Correct Answer: B

Reference: https://answers.splunk.com/answers/790783/anti-tampering-features-to-protect-splunk-logsthe.html

QUESTION 3

An administrator is provisioning one search head prior to installing ES. What are the reference minimum requirements for OS, CPU, and RAM for that machine?

A. OS: 32 bit, RAM: 16 MB, CPU: 12 cores

B. OS: 64 bit, RAM: 32 MB, CPU: 12 cores

C. OS: 64 bit, RAM: 12 MB, CPU: 16 cores

D. OS: 64 bit, RAM: 32 MB, CPU: 16 cores

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Capacity/Referencehardware

QUESTION 4

Which of the following actions may be necessary before installing ES?

A. Redirect distributed search connections.

B. Purge KV Store.

C. Add additional indexers.

D. Add additional forwarders.

Correct Answer: C

QUESTION 5

Following the installation of ES, an admin configured users with the ess_user role the ability to close notable events.

How would the admin restrict these users from being able to change the status of Resolved notable events to Closed?

A. In Enterprise Security, give the ess_user role the Own Notable Events permission.

B. From the Status Configuration window select the Closed status. Remove ess_user from the status transitions for the Resolved status.

C. From the Status Configuration window select the Resolved status. Remove ess_user from the status transitions for the Closed status.

D. From Splunk Access Controls, select the ess_user role and remove the edit_notable_events capability.

Correct Answer: C