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

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

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 3

An administrator is asked to configure an "Nslookup" adaptive response action, so that it appears as a selectable option in the notable event\\'s action menu when an analyst is working in the Incident Review dashboard. What steps would the administrator take to configure this option?

A. Configure -> Content Management -> Type: Correlation Search -> Notable -> Nslookup

B. Configure -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup

C. Configure -> Content Management -> Type: Correlation Search -> Notable -> Next Steps -> Nslookup

D. Configure -> Content Management -> Type: Correlation Search -> Notable -> Recommended Actions > Nslookup

Correct Answer: D

QUESTION 4

What is an example of an ES asset?

A. MAC address

B. User name

C. Server

D. People

Correct Answer: A

QUESTION 5

Which of the following is a key feature of a glass table?

A. Rigidity.

B. Customization.

C. Interactive investigations.

D. Strong data for later retrieval.

Correct Answer: B