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

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

QUESTION 2

To observe what network services are in use in a network\\'s activity overall, which of the following dashboards in Enterprise Security will contain the most relevant data?

A. Intrusion Center

B. Protocol Analysis

C. User Intelligence

D. Threat Intelligence

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/NetworkProtectionDomaindashboards

QUESTION 3

Following the Installation of ES, an admin configured Leers with the ?s_uso r 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. From the Status Configuration window select the Resolved status. Remove ess_user from the status transitions for the closed status.

B. From the Status Configuration windows select the closed status. Remove ess_use r from the status transitions for the Resolved status.

C. In Enterprise Security, give the ess_user role the own Notable Events permission.

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

Correct Answer: B

QUESTION 4

How should an administrator add a new lookup through the ES app?

A. Upload the lookup file in Settings -> Lookups -> Lookup Definitions

B. Upload the lookup file in Settings -> Lookups -> Lookup table files

C. Add the lookup file to /etc/apps/SplunkEnterpriseSecuritySuite/lookups

D. Upload the lookup file using Configure -> Content Management -> Create New Content -> Managed Lookup

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Createlookups

QUESTION 5

Which argument to the | tstats command restricts the search to summarized data only?

A. summaries=t

B. summaries=all

C. summariesonly=t

D. summariesonly=all

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels