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

Which of the following is a way to test for a property normalized data model?

A. Use Audit -> Normalization Audit and check the Errors panel.

B. Run a | datamodel search, compare results to the CIM documentation for the datamodel.

C. Run a | loadjob search, look at tag values and compare them to known tags based on the encoding.

D. Run a | datamodel search and compare the results to the list of data models in the ES normalization guide.

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime

QUESTION 2

Which of these Is a benefit of data normalization?

A. Reports run faster because normalized data models can be optimized for better performance.

B. Dashboards take longer to build.

C. Searches can be built no matter the specific source technology for a normalized data type.

D. Forwarder-based inputs are more efficient.

Correct Answer: A

QUESTION 3

Which of the following steps will make the Threat Activity dashboard the default landing page in ES?

A. From the Edit Navigation page, drag and drop the Threat Activity view to the top of the page.

B. From the Preferences menu for the user, select Enterprise Security as the default application.

C. From the Edit Navigation page, click the \\'Set this as the default view" checkmark for Threat Activity.

D. Edit the Threat Activity view settings and checkmark the Default View option.

Correct Answer: C

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

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