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 are data models used by ES? (Choose all that apply)

A. Web

B. Anomalies

C. Authentication

D. Network Traffic

Correct Answer: ACD

Reference: https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/datamodelsusedbyes/

QUESTION 2

What is the default schedule for accelerating ES Datamodels?

A. 1 minute

B. 5 minutes

C. 15 minutes

D. 1 hour

Correct Answer: B

QUESTION 3

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 4

Glass tables can display static images and text, the results of ad-hoc searches, and which of the following objects?

A. Lookup searches.

B. Summarized data.

C. Security metrics.

D. Metrics store searches.

Correct Answer: C

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

QUESTION 5

A security manager has been working with the executive team en long-range security goals. A primary goal for the team Is to Improve managing user risk in the organization. Which of the following ES features can help identify users accessing inappropriate web sites?

A. Configuring the identities lookup with user details to enrich notable event Information for forensic analysis.

B. Make sure the Authentication data model contains up-to-date events and is properly accelerated.

C. Configuring user and website watchlists so the User Activity dashboard will highlight unwanted user actions.

D. Use the Access Anomalies dashboard to identify unusual protocols being used to access corporate sites.

Correct Answer: C