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.passapply.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

What do threat gen searches produce?

A. Threat Intel in KV Store collections.

B. Threat correlation searches.

C. Threat notables in the notable index.

D. Events in the threat_activity index.

Correct Answer: D

https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Createthreatmatchspecs

QUESTION 2

When using distributed configuration management to create the Splunk_TA_ForIndexers package, which three files can be included?

A. indexes.conf, props.conf, transforms.conf

B. web.conf, props.conf, transforms.conf

C. inputs.conf, props.conf, transforms.conf

D. eventtypes.conf, indexes.conf, tags.conf

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Install/InstallTechnologyAdd-ons

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

Where is it possible to export content, such as correlation searches, from ES?

A. Content exporter

B. Configure -> Content Management

C. Export content dashboard

D. Settings Menu -> ES -> Export

Correct Answer: B

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

QUESTION 5

After data is ingested, which data management step is essential to ensure raw data can be accelerated by a Data Model and used by ES?

A. Applying Tags.

B. Normalization to Customer Standard.

C. Normalization to the Splunk Common Information Model.

D. Extracting Fields.

Correct Answer: C