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

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

An administrator is provisioning one search head prior to installing ES. What are the reference minimum requirements for OS, CPU, and RAM for that machine?

A. OS: 32 bit, RAM: 16 MB, CPU: 12 cores

B. OS: 64 bit, RAM: 32 MB, CPU: 12 cores

C. OS: 64 bit, RAM: 12 MB, CPU: 16 cores

D. OS: 64 bit, RAM: 32 MB, CPU: 16 cores

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Capacity/Referencehardware

QUESTION 3

A customer site is experiencing poor performance. The UI response time is high and searches take a very long time to run. Some operations time out and there are errors in the scheduler logs, indicating too many concurrent searches are being started. 6 total correlation searches are scheduled and they have already been tuned to weed out false positives.

Which of the following options is most likely to help performance?

A. Change the search heads to do local indexing of summary searches.

B. Add heavy forwarders between the universal forwarders and indexers so inputs can be parsed before indexing.

C. Increase memory and CPUs on the search head(s) and add additional indexers.

D. If indexed realtime search is enabled, disable it for the notable index.

Correct Answer: C

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

Which of the following ES features would a security analyst use while investigating a network anomaly notable?

A. Correlation editor.

B. Key indicator search.

C. Threat download dashboard.

D. Protocol intelligence dashboard.

Correct Answer: D

Reference: https://www.splunk.com/en_us/products/premium-solutions/splunk-enterprise-security/ features.html