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

The Add-On Builder creates Splunk Apps that start with what?

A. DA

B. SA

C. TA

D. App-

Correct Answer: C

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

QUESTION 2

Where should an ES search head be installed?

A. On a Splunk server with top level visibility.

B. On any Splunk server.

C. On a server with a new install of Splunk.

D. On a Splunk server running Splunk DB Connect.

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Export

QUESTION 3

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

QUESTION 4

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

QUESTION 5

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