SPLK-3001$^{Q\&As}$

Splunk Enterprise Security Certified Admin

Pass Splunk SPLK-3001 Exam with 100% Guarantee

Following Questions and Answers are all new published by Splunk Official Exam Center

QUESTION 1

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 2

Which of the following threat intelligence types can ES download? (Choose all that apply)

A. Text

B. STIX/TAXII

C. VulnScanSPL

D. SplunkEnterpriseThreatGenerator

Correct Answer: AB

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

QUESTION 3

Which tool Is used to update indexers In E5?

A. Index Updater

B. Distributed Configuration Management

C. indexes.conf

D. Splunk_TA_ForIndexeres. spl

Correct Answer: B

QUESTION 4

What is the maximum recommended volume of indexing per day, per indexer, for a non-cloud (on-prem) ES deployment?

A. 50 GB

B. 100 GB

C. 300 GB

D. 500 MB

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/ITSI/4.4.2/Install/Plan

QUESTION 5

Where is the Add-On Builder available from?

A. GitHub

B. SplunkBase

C. www.splunk.com

D. The ES installation package

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Installation

Latest SPLK-3001 Dumps SPLK-3001 Practice Test SPLK-3001 Braindumps