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

QUESTION 1

When investigating, what is the best way to store a newly-found IOC?

A. Paste it into Notepad.

B. Click the "Add IOC" button.

C. Click the "Add Artifact" button.

D. Add it in a text note to the investigation.

Correct Answer: C

QUESTION 2

Which of the following features can the Add-on Builder configure in a new add-on?

A. Expire data.

B. Normalize data.

C. Summarize data.

D. Translate data.

Correct Answer: B

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

QUESTION 3

What can be exported from ES using the Content Management page?

A. Only correlation searches, managed lookups, and glass tables.

B. Only correlation searches.

C. Any content type listed in the Content Management page.

D. Only correlation searches, glass tables, and workbench panels.

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Export#:~:text=as%20an%20app-,Export%20content%20from%20Splunk%20Enterprise%20Security%20as,from%20the%20Conte nt%20Management%20page.andtext=You%20can%20export%20any%20type,%2C%20data%20models%2C%20and%20views.

QUESTION 4

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 5

What feature of Enterprise Security downloads threat intelligence data from a web server?

A. Threat Service Manager

B. Threat Download Manager

C. Threat Intelligence Parser

D. Therat Intelligence Enforcement

Correct Answer: B

"The Threat Intelligence Framework provides a modular input (Threat Intelligence Downloads) that handles the majority of configurations typically needed for downloading intelligence files and data. To access this modular input, you simply need to create a stanza in your Inputs.conf file called "threatlist"."