



# SPLK-3001<sup>Q&As</sup>

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

How is it possible to specify an alternate location for accelerated storage?

- A. Configure storage optimization settings for the index.
- B. Update the Home Path setting in indexes, conf
- C. Use the tstatsHomePath setting in props, conf
- D. Use the tstatsHomePath Setting in indexes, conf

Correct Answer: C

---

### QUESTION 2

Where is the Add-On Builder available from?

- A. GitHub
- B. SplunkBase
- C. [www.splunk.com](http://www.splunk.com)
- D. The ES installation package

Correct Answer: B

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

---

### QUESTION 3

Which lookup table does the Default Account Activity Detected correlation search use to flag known default accounts?

- A. Administrative Identities
- B. Local User Intel
- C. Identities
- D. Privileged Accounts

Correct Answer: C

---

### QUESTION 4

Where are attachments to investigations stored?

- A. KV Store



B. notable index

C. attachments.csv lookup D. /etc/apps/SA-Investigations/default/ui/views/attachments

Correct Answer: A

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Manageinvestigations>

---

## QUESTION 5

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%20Content%20Management%20page.andtext=You%20can%20export%20any%20type,%2C%20data%20models%2C%20and%20views.>

[SPLK-3001 Study Guide](#)

[SPLK-3001 Exam  
Questions](#)

[SPLK-3001 Braindumps](#)