



# 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

Which of the following is a risk of using the Auto Deployment feature of Distributed Configuration Management to distribute indexes.conf?

- A. Indexes might crash.
- B. Indexes might be processing.
- C. Indexes might not be reachable.
- D. Indexes have different settings.

Correct Answer: A

Reference: <https://docs.splunk.com/Documentation/Splunk/8.0.2/Admin/Indexesconf>

---

### QUESTION 2

Which of the following would allow an add-on to be automatically imported into Splunk Enterprise Security?

- A. A prefix of CIM\_
- B. A suffix of .spl
- C. A prefix of TECH\_
- D. A prefix of Splunk\_TA\_

Correct Answer: D

Reference: <https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/planintegrationes/>

---

### QUESTION 3

What is the main purpose of the Dashboard Requirements Matrix document?

- A. Identifies on which data model(s) each dashboard depends.
- B. Provides instructions for customizing each dashboard for local data models.
- C. Identifies the searches used by the dashboards.
- D. Identifies which data model(s) depend on each dashboard.

Correct Answer: D

---

### QUESTION 4



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 5

How should an administrator add a new lookup through the ES app?

- A. Upload the lookup file in Settings -> Lookups -> Lookup Definitions
- B. Upload the lookup file in Settings -> Lookups -> Lookup table files
- C. Add the lookup file to /etc/apps/SplunkEnterpriseSecuritySuite/lookups
- D. Upload the lookup file using Configure -> Content Management -> Create New Content -> Managed Lookup

Correct Answer: D

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

[Latest SPLK-3001 Dumps](#)

[SPLK-3001 VCE Dumps](#)

[SPLK-3001 Braindumps](#)