



# 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

What is an example of an ES asset?

- A. MAC address
- B. User name
- C. Server
- D. People

Correct Answer: A

---

### QUESTION 2

What is the first step when preparing to install ES?

- A. Install ES.
- B. Determine the data sources used.
- C. Determine the hardware required.
- D. Determine the size and scope of installation.

Correct Answer: D

---

### QUESTION 3

Which columns in the Assets lookup are used to identify an asset in an event?

- A. src, dvc, dest
- B. cidr, port, netbios, saml
- C. ip, mac, dns, nt\_host
- D. host, hostname, url, address

Correct Answer: C

Reference: <https://docs.splunk.com/Documentation/ES/6.4.1/Admin/Formatassetoridentitylist>

---

### QUESTION 4

When ES content is exported, an app with a .spl extension is automatically created. What is the best practice when exporting and importing updates to ES content?



- A. Use new app names each time content is exported.
- B. Do not use the .spl extension when naming an export.
- C. Always include existing and new content for each export.
- D. Either use new app names or always include both existing and new content.

Correct Answer: D

Either use new app names each time (which could be difficult to manage) or make sure you always include all content (old and new) each time you export.

---

#### QUESTION 5

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>

[Latest SPLK-3001 Dumps](#)

[SPLK-3001 PDF Dumps](#)

[SPLK-3001 Braindumps](#)