

DUMPS ARENA

Splunk Enterprise Security Certified Admin Exam

Splunk SPLK-3001

Version Demo

Total Demo Questions: 7

Total Premium Questions: 97

Buy Premium PDF

<https://dumpsarena.com>

sales@dumpsarena.com

dumpsarena.com

QUESTION NO: 1

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.

ANSWER: D**Explanation:**

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 NO: 2

A site has a single existing search head which hosts a mix of both CIM and non-CIM compliant applications.

All of the applications are mission-critical. The customer wants to carefully control cost, but wants good ES performance. What is the best practice for installing ES?

- A. Install ES on the existing search head.
- B. Add a new search head and install ES on it.
- C. Increase the number of CPUs and amount of memory on the search head, then install ES.
- D. Delete the non-CIM-compliant apps from the search head, then install ES.

ANSWER: B**QUESTION NO: 3**

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

- A. Text
- B. STIX/TAXII

- C. VulnScanSPL
- D. SplunkEnterpriseThreatGenerator

ANSWER: A B

QUESTION NO: 4

Which argument to the | tstats command restricts the search to summarized data only?

- A. summaries=t
- B. summaries=all
- C. summariesonly=t
- D. summariesonly=all

ANSWER: C

QUESTION NO: 5

Which of the following are data models used by ES? (Choose all that apply)

- A. Web
- B. Anomalies
- C. Authentication
- D. Network Traffic

ANSWER: A C D

QUESTION NO: 6

“10.22.63.159”, “websvr4”, and “00:26:08:18: CF:1D” would be matched against what in ES?

- A. A user.
- B. A device.
- C. An asset.

D. An identity.

ANSWER: B

QUESTION NO: 7

Both "Recommended Actions" and "Adaptive Response Actions" use adaptive response. How do they differ?

- A. Recommended Actions show a textual description to an analyst, Adaptive Response Actions show them encoded.
- B. Recommended Actions show a list of Adaptive Responses to an analyst, Adaptive Response Actions run them automatically.
- C. Recommended Actions show a list of Adaptive Responses that have already been run, Adaptive Response Actions run them automatically.
- D. Recommended Actions show a list of Adaptive Responses to an analyst, Adaptive Response Actions run manually with analyst intervention.

ANSWER: D