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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

QUESTION 2

"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.

Correct Answer: B

QUESTION 3

ES needs to be installed on a search head with which of the following options?

A. No other apps.

B. Any other apps installed.

C. All apps removed except for TA-*.

D. Only default built-in and CIM-compliant apps.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallEnterpriseSecurity

QUESTION 4

Who can delete an investigation?

A. ess_admin users only.

B. The investigation owner only.

C. The investigation owner and ess-admin.

D. The investigation owner and collaborators.

Correct Answer: A

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

QUESTION 5

Which of the following are examples of sources for events in the endpoint security domain dashboards?

A. REST API invocations.

B. Investigation final results status.

C. Workstations, notebooks, and point-of-sale systems.

D. Lifecycle auditing of incidents, from assignment to resolution.

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/EndpointProtectionDomaindashboards