



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.geekcert.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 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 2

Which of the following actions can improve overall search performance?

- A. Disable indexed real-time search.
- B. Increase priority of all correlation searches.
- C. Reduce the frequency (schedule) of lower-priority correlation searches.
- D. Add notable event suppressions for correlation searches with high numbers of false positives.

Correct Answer: A

QUESTION 3

How is notable event urgency calculated?

- A. Asset priority and threat weight.
- B. Alert severity found by the correlation search.
- C. Asset or identity risk and severity found by the correlation search.
- D. Severity set by the correlation search and priority assigned to the associated asset or identity.

Correct Answer: D

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned>

QUESTION 4

Which two fields combine to create the Urgency of a notable event?

- A. Priority and Severity.



- B. Priority and Criticality.
- C. Criticality and Severity.
- D. Precedence and Time.

Correct Answer: A

Reference: <https://docs.splunk.com/Documentation/ES/6.4.1/User/Howurgencyisassigned>

QUESTION 5

Which data model populated the panels on the Risk Analysis dashboard?

- A. Risk
- B. Audit
- C. Domain analysis
- D. Threat intelligence

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskAnalysis#Dashboard_panels

[Latest SPLK-3001 Dumps](#)

[SPLK-3001 Practice Test](#)

[SPLK-3001 Study Guide](#)