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

QUESTION 1

Which correlation search feature is used to throttle the creation of notable events?

A. Schedule priority.

B. Window interval.

C. Window duration.

D. Schedule windows.

Correct Answer: C

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

QUESTION 2

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 3

What kind of value is in the red box in this picture?

A. A risk score.

B. A source ranking.

C. An event priority.

D. An IP address rating.

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Data/FormateventsforHTTPEventCollector

QUESTION 4

Glass tables can display static images and text, the results of ad-hoc searches, and which of the following objects?

A. Lookup searches.

B. Summarized data.

C. Security metrics.

D. Metrics store searches.

Correct Answer: C

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

QUESTION 5

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