SPLK-3002^{Q&As}

Splunk IT Service Intelligence Certified Admin

Pass Splunk SPLK-3002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/splk-3002.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

Besides creating notable events, what are the default alert actions a correlation search can execute? (Choose all that apply.)

A. Ping a host.

B. Send email.

C. Include in RSS feed.

D. Run a script.

Correct Answer: BCD

Throttling applies to any correlation search alert type, including notable events and actions (RSS feed, email, run script, and ticketing).

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/EA/ConfigCS

QUESTION 2

Within a correlation search, dynamic field values can be specified with what syntax?

A. fieldname

B.

C. %fieldname% D. eval(fieldname)

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/8.2.2/Search/Searchindexes

QUESTION 3

ITSI Saved Search Scheduling is configured to use realtime_schedule = 0. Which statement is accurate about this configuration?

A. If this value is set to 0, the scheduler bases its determination of the next scheduled search execution time on the current time.

B. If this value is set to 0, the scheduler bases its determination of the next scheduled search on the last search execution time.

C. If this value is set to 0, the scheduler may skip scheduled execution periods.

D. If this value is set to 0, the scheduler might skip some execution periods to make sure that the scheduler is executing the searches running over the most recent time range.

Correct Answer: B

If set to 0, the scheduler determines the next scheduled search run time based on the last run time for the search. This is called continuous scheduling.

Reference: https://docs.splunk.com/Documentation/DFS/1.1.2/DFS/Savedsearchesconf

QUESTION 4

Which of the following is an advantage of using adaptive time thresholds?

A. Automatically update thresholds daily to manage dynamic changes to KPI values.

B. Automatically adjust KPI calculation to manage dynamic event data.

C. Automatically adjust aggregation policy grouping to manage escalating severity.

D. Automatically adjust correlation search thresholds to adjust sensitivity over time.

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/TimePolicies

QUESTION 5

Anomaly detection can be enabled on which one of the following?

A. KPI

B. Multi-KPI alert

C. Entity

D. Service

Correct Answer: A

Enable anomaly detection to identify trends and outliers in KPI search results that might indicate an issue with your system.

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/AD

SPLK-3002 PDF Dumps   SPLK-3002 VCE Dumps   SPLK-3002 Study Guide