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.geekcert.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

After a notable event has been closed, how long will the meta data for that event remain in the KV Store by default?

A. 6 months.

B. 9 months.

C. 1 year.

D. 3 months.

Correct Answer: A

By default, notable event metadata is archived after six months to keep the KV store from growing too large.

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

QUESTION 2

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

QUESTION 3

Which of the following is the best use case for configuring a Multi-KPI Alert?

A. Comparing content between two notable events.

B. Using machine learning to evaluate when data falls outside of an expected pattern.

C. Comparing anomaly detection between two KPIs.

D. Raising an alert when one or more KPIs indicate an outage is occurring.

Correct Answer: A

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

QUESTION 4

Which glass table feature can be used to toggle displaying KPI values from more than one service on a single widget?

A. Service templates.

B. Service dependencies.

C. Ad-hoc search.

D. Service swapping.

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/Visualizations#collapseDesktop8

QUESTION 5

For which ITSI function is it a best practice to use a 15-30 minute time buffer?

A. Correlation searches.

B. Adaptive thresholding.

C. Maintenance windows

D. Anomaly detection.

Correct Answer: C

It\\'s a best practice to schedule maintenance windows with a 15- to 30-minute time buffer before and after you start and stop your maintenance work. This gives the system an opportunity to catch up with the maintenance state and reduces the chances of ITSI generating false positives during maintenance operations.

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/AboutMW

Latest SPLK-3002 Dumps   SPLK-3002 VCE Dumps   SPLK-3002 Study Guide