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.leads4pass.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

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 2

What is the main purpose of the service analyzer?

A. Display a list of All Services and Entities.

B. Trigger external alerts based on threshold violations.

C. Allow Analysts to add comments to Alerts.

D. Monitor overall Service and KPI status.

Correct Answer: C

Alerts and Sharing Reference: https://docs.splunk.com/Documentation/MSExchange/4.0.3/Reference/ServiceAnalyzer

QUESTION 3

Where are KPI search results stored?

A. The default index.

B. KV Store.

C. Output to a CSV lookup.

D. The itsi_summaryindex.

Correct Answer: D

Search results are processed, created, and written to the itsi_summary index via an alert action.

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

QUESTION 4

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 5

Which deep dive swim lane type does not require writing SPL?

A. Event lane.

B. Automatic lane.

C. Metric lane.

D. KPI lane.

Correct Answer: B

Among all the search configurations, automatic lane doesn\\'t need to be written in Splunk Processing language.

QUESTION 6

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 7

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 8

Which of the following is a characteristic of base searches?

A. Search expression, entity splitting rules, and thresholds are configured at the base search level.

B. It is possible to filter to entities assigned to the service for calculating the metrics for the service\\'s KPIs.

C. The fewer KPIs that share a common base search, the more efficiency a base search provides, and anomaly detection is more efficient.

D. The base search will execute whether or not a KPI needs it.

Correct Answer: B

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

QUESTION 9

Which scenario would benefit most by implementing ITSI?

A. Monitoring of business services functionality.

B. Monitoring of system hardware.

C. Monitoring of system process statuses.

D. Monitoring of retail sales metrics.

Correct Answer: A

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

QUESTION 10

What is an episode?

A. A workflow task.

B. A deep dive.

C. A notable event group.

D. A notable event.

Correct Answer: D

It\\'s a deduplicated group of notable events occurring as part of a larger sequence, or an incident or period considered in isolation.

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