SPLK-3002Q&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

Which of the following items apply to anomaly detection? (Choose all that apply.)

A. Use AD on KPIs that have an unestablished baseline of data points. This allows the ML pattern to perform it\\'s magic.

B. A minimum of 24 hours of data is needed for anomaly detection, and a minimum of 4 entities for cohesive analysis.

C. Anomaly detection automatically generates notable events when KPI data diverges from the pattern.

D. There are 3 types of anomaly detection supported in ITSI: adhoc, trending, and cohesive.

Correct Answer: BC

The KPI must be split by entity, and a minimum of four entities is required.

If the KPI diverges from the normal pattern, ITSI creates a notable event in Episode Review.

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

QUESTION 2

Which of the following describes enabling smart mode for an aggregation policy?

A. Configure –andgt; Policies –andgt; Smart Mode –andgt; Enable, select “fields”, click “Save”

B. Enable grouping in Notable Event Review, select “Smart Mode”, select “fields”, and click “Save”

C. Edit the aggregation policy, enable smart mode, select fields to analyze, click “Save”

D. Edit the notable event view, enable smart mode, select “fields”, and click “Save”

Correct Answer: A

1.

From the ITSI main menu, click Configuration > Notable Event Aggregation Policies.

2.

Select a custom policy or the Default Policy.

3.

Under Smart Mode grouping, enable Smart Mode.

4.

Click Select fields. A dialog displays the fields found in your notable events from the last 24 hours. Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/EA/SmartMode

QUESTION 3

Which index is used to store KPI values?

A. itsi_summary_metrics

B. itsi_metrics

C. itsia_service_health

D. itsi_summary

Correct Answer: A

The IT Service Intelligence (ITSI) metrics summary index, itsi_summary_metrics, is a metrics-based summary index that stores KPI data.

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

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

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

SPLK-3002 PDF Dumps | SPLK-3002 Exam Questions | SPLK-3002 Braindumps