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.pass2lead.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

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 2

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 3

Which of the following is a valid type of Multi-KPI Alert?

A. Score over composite.

B. Value over time.

C. Status over time.

D. Rise over run.

Correct Answer: C

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

QUESTION 4

Which index contains ITSI Episodes?

A. itsi_tracked_alerts

B. itsi_grouped_alerts

C. itsi_notable_archive

D. itsi_summary

Correct Answer: C

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

QUESTION 5

Which of the following are the default ports that must be configured on Splunk to use ITSI?

A. SplunkWeb (8405), SplunkD (8519), and HTTP Collector (8628)

B. SplunkWeb (8089), SplunkD (8088), and HTTP Collector (8000)

C. SplunkWeb (8000), SplunkD (8089), and HTTP Collector (8088)

D. SplunkWeb (8088), SplunkD (8089), and HTTP Collector (8000)

Correct Answer: C

Reference: https://splunk.github.io/docker-splunk/ARCHITECTURE.html