# SPLK-3002<sup>Q&As</sup>

## 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**

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

**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**

In distributed search, which components need to be installed on instances other than the search head?

A. SA-IndexCreationand SA-ITSI-Licensecheckeron indexers.

B. SA-IndexCreationand SA-ITOA on indexers; SA-ITSI-Licensecheckerand SA-UserAccess on the license master.

C. SA-IndexCreationon idexers; SA-ITSI-Licensecheckerand SA-UserAccesson the license master.

D. SA-ITSI-Licensecheckeron indexers.

Correct Answer: A

SA-IndexCreation is required on all indexers. For non-clustered, distributed environments, copy SA-IndexCreation to $SPLUNK_HOME/etc/apps/ on individual indexers.

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/Install/InstallDD

**QUESTION 4**

Which ITSI functions generate notable events? (Choose all that apply.)

A. KPI threshold breaches.

B. KPI anomaly detection.

C. Multi-KPI alert.

D. Correlation search.

Correct Answer: ABD

After you configure KPI thresholds, you can set up alerts to notify you when aggregate KPI severities

change. ITSI generates notable events in Episode Review based on the alerting rules you configure.

Anomaly detection generates notable events when a KPI IT Service Intelligence (ITSI) deviates from an

expected pattern.

Notable events are typically generated by a correlation search.

Reference:

https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/KPIthresholds

https://docs.splunk.com/Documentation/ITSI/4.10.1/SI/AboutSI

https://docs.splunk.com/Documentation/ITSI/4.10.2/EA/NotableEvents

**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