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.pass4itsure.com/splk-3002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

QUESTION 1

Which of the following is an advantage of using adaptive time thresholds?

A. Automatically update thresholds daily to manage dynamic changes to KPI values.

B. Automatically adjust KPI calculation to manage dynamic event data.

C. Automatically adjust aggregation policy grouping to manage escalating severity.

D. Automatically adjust correlation search thresholds to adjust sensitivity over time.

Correct Answer: A

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

QUESTION 2

What is the default importance value for dependent services' health scores?

A. 11

B. 1

C. Unassigned

D. 10

Correct Answer: A

By default, impacting service health scores have an importance value of 11. Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/Dependencies

QUESTION 3

Which of the following applies when configuring time policies for KPI thresholds?

A. A person can only configure 24 policies, one for each hour of the day.

B. They are great if you expect normal behavior at 1:00 to be different than normal behavior at 5:00

C. If a person expects a KPI to change significantly through a cycle on a daily basis, don\\'t use it.

D. It is possible for multiple time policies to overlap.

Correct Answer: D

If you\\'re creating multiple time policies that require the same threshold values, you can save time by copying the threshold levels and their corresponding values from one policy to another

Reference: https://docs.splunk.com/Documentation/ITSI/4.9.1/SI/TimePolicies

QUESTION 4

In maintenance mode, which features of KPIs still function?

A. KPI searches will execute but will be buffered until the maintenance window is over.

B. KPI searches still run during maintenance mode, but results go to itsi_maintenance_summaryindex.

C. New KPIs can be created, but existing KPIs are locked.

D. KPI calculations and threshold settings can be modified.

Correct Answer: A

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 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

QUESTION 6

In Episode Review, what is the result of clicking an episode\\'s Acknowledge button?

A. Assign the current user as owner.

B. Change status from New to Acknowledged.

C. Change status from New to In Progress and assign the current user as owner.

D. Change status from New to Acknowledged and assign the current user as owner.

Correct Answer: C

When an episode warrants investigation, the analyst acknowledges the episode, which moves the status from New to In Progress.

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

QUESTION 7

When deploying ITSI on a distributed Splunk installation, which component must be installed on the search head(s)?

A. SA-ITOA

B. ITSI app

C. All ITSI components

D. SA-ITSI-Licensechecker

Correct Answer: D

Install SA-ITSI-Licensechecker and SA-UserAccess on any license master in a distributed or search head cluster environment. If a search head in your environment is also a license master, the license master components are installed when you install ITSI on the search heads.

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

QUESTION 8

When creating a custom deep dive, what color are services/KPIs in maintenance mode within the topology view?

A. Gray

B. Purple

C. Gear Icon

D. Blue

Correct Answer: A

Services, entities, and KPIs that are fully or partially impacted by a maintenance window appear in a dark gray color on pages that display health scores, including service analyzers, service and entity details pages, glass tables, multi-KPI alerts, and deep dives.

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

QUESTION 9

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 10

Which index will contain useful error messages when troubleshooting ITSI issues?

A. _introspection

B. _internal

C. itsi_summary

D. itsi_notable_audit

Correct Answer: B

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