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.certbus.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

What should be considered when onboarding data into a Splunk index, assuming that ITSI will need to use this data?

A. Use | stats functions in custom fields to prepare the data for KPI calculations.

B. Check if the data could leverage pre-built KPIs from modules, then use the correct TA to onboard the data.

C. Make sure that all fields conform to CIM, then use the corresponding module to import related services.

D. Plan to build as many data models as possible for ITSI to leverage

Correct Answer: B

Reference: https://newoutlook.it/download/book/splunk/advanced-splunk.pdf

QUESTION 2

Which of the following accurately describes base searches used for KPIs in a service?

A. Base searches can be used for multiple services.

B. A base search can only be used by its service and all dependent services.

C. All the metrics in a base search are used by one service.

D. All the KPIs in a service use the same base search.

Correct Answer: A

KPI base searches let you share a search definition across multiple KPIs in IT Service Intelligence (ITSI). Create base searches to consolidate multiple similar KPIs, reduce search load, and improve search performance.

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

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

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 5

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 6

Which of the following best describes a default deep dive?

A. It initially shows the health scores for all services.

B. It initially shows the highest importance KPIs.

C. It initially shows all of the KPIs for a selected service.

D. It initially shows all the entity swim lanes.

Correct Answer: D

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

QUESTION 7

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 8

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 9

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 10

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