SPLK-3002 Q&As

Splunk IT Service Intelligence Certified Admin

Pass Splunk SPLK-3002 Exam with 100% Guarantee

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

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

Which of the following is a recommended best practice for service and glass table design?

A. Plan and implement services first, then build detailed glass tables.

B. Always use the standard icons for glass table widgets to improve portability.

C. Start with base searches, then services, and then glass tables.

D. Design glass tables first to discover which KPIs are important.

Correct Answer: D

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

QUESTION 3

When in maintenance mode, which of the following is accurate?

A. Once the window is over, KPIs and notable events will begin to be generated again.

B. KPIs are shown in blue while in maintenance mode.

C. Maintenance mode slots are scheduled on a per hour basis.

D. Service health scores and KPI events are deleted until the window is over.

Correct Answer: A

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

QUESTION 4

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 5

Which of the following describes a way to delete multiple duplicate entities in ITSI?

A. Via c CSV upload.

B. Via the entity lister page.

C. Via a search using the | deleteentity command.

D. All of the above.

Correct Answer: A

Import entities from CSV files that contain one or more entity definitions. Importing entities from CSV files is an efficient way to define multiple entities.

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/Entity/ImportCSV

QUESTION 6

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 7

Which of the following describes entities? (Choose all that apply.)

A. Entities must be IT devices, such as routers and switches, and must be identified by either IP value, host name, or mac address.

B. An abstract (pseudo/logical) entity can be used to split by for a KPI, although no entity rules or filtering can be used to limit data to a specific service.

C. Multiple entities can share the same alias value, but must have different role values.

D. To automatically restrict the KPI to only the entities in a particular service, select “Filter to Entities in

Service”.

Correct Answer: D

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

QUESTION 8

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 9

Which of the following are deployment recommendations for ITSI? (Choose all that apply.)

A. Deployments often require an increase of hardware resources above base Splunk requirements.

B. Deployments require a dedicated ITSI search head.

C. Deployments may increase the number of required indexers based on the number of KPI searches.

D. Deployments should use fastest possible disk arrays for indexers.

Correct Answer: ABC

You might need to increase the hardware specifications of your own Enterprise Security deployment above the minimum hardware requirements depending on your environment.

Install Splunk Enterprise Security on a dedicated search head or search head cluster.

The Splunk platform uses indexers to scale horizontally. The number of indexers required in an Enterprise Security deployment varies based on the data volume, data type, retention requirements, search type, and search concurrency.

Reference: https://docs.splunk.com/Documentation/ES/latest/Install/DeploymentPlanning

QUESTION 10

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

Latest SPLK-3002 Dumps SPLK-3002 VCE Dumps SPLK-3002 Study Guide