Free Questions for SPLK-3002 by braindumpscollection

Shared by Lucas on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following best describes a default deep dive?

Options:

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.

Answer:

C

Explanation:

C is the correct answer because a default deep dive initially shows all of the KPIs for a selected service. You can create a default deep dive by drilling down from another dashboard or by selecting a service from the deep dive lister page. A default deep dive does not show

health scores, importance scores, or entity swim lanes by default. Reference: [Create default deep dives for services in ITSI]

Question 2

Question Type: MultipleChoice

Which index contains ITSI Episodes?

Options:

A- itsi_tracked_alerts

B- itsi_grouped_alerts

C- itsi_notable_archive

D- itsi_summary

Answer:

B

Explanation:

B is the correct answer because ITSI episodes are stored in the itsi_grouped_alerts index. This index contains notable events that have been grouped together based on predefined aggregation policies. Episodes help you reduce alert noise and focus on resolving incidents faster. Reference: [Overview of episodes in ITSI]

Question 3

Question Type: MultipleChoice

In maintenance mode, which features of KPIs still function?

Options:

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_summary index.

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

D- KPI calculations and threshold settings can be modified.

Answer:

A

Explanation:

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.

A is the correct answer because KPI searches still run during maintenance mode, but the results are buffered until the maintenance window is over. This means that no alerts are triggered during maintenance mode, but once it ends, the buffered results are processed and alerts are generated if necessary. You cannot create new KPIs or modify existing KPIs during maintenance mode. Reference: [Overview of maintenance windows in ITSI]

Question 4

Question Type: MultipleChoice

Which capabilities are enabled through "teams"?

Options:

A- Teams allow searches against the itsi_summary index.

B- Teams restrict notable event alert actions.

C- Teams restrict searches against the itsi_notable_audit index.

D- Teams allow restrictions to service content in UI views.

Answer:

D

Explanation:

D is the correct answer because teams allow you to restrict access to service content in UI views such as service analyzers, glass tables, deep dives, and episode review. Teams also control access to services and KPIs for editing and viewing purposes. Teams do not affect the ability to search against the itsi_summary index, restrict notable event alert actions, or restrict searches against the itsi_notable_audit index. Reference:Overview of teams in ITSI

Question 5

Question Type: MultipleChoice

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

Options:

A- Via c CSV upload.

B- Via the entity lister page.

C- Via a search using the | deleteentity command.

D- All of the above.

Answer:

D

Explanation:

D is the correct answer because ITSI provides multiple ways to delete multiple duplicate entities. You can use a CSV upload to overwrite existing entities with new or updated information, or delete them by setting the action field to delete. You can also use the entity lister page to select multiple entities and delete them in bulk. Alternatively, you can use a search command called | deleteentity to delete entities that match certain criteria. Reference:Create and update entities using a CSV file in ITSI,Delete entities in bulk in ITSI,Delete entities using the | deleteentity command in ITSI

Question 6

Question Type: MultipleChoice

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

Options:

A- KPI threshold breaches.

B- KPI anomaly detection.

C- Multi-KPI alert.

D- Correlation search.

Answer:

A, B, D

Explanation:

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.

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

A, B, and D are correct answers because ITSI can generate notable events when a KPI breaches a threshold, when a KPI detects an anomaly, or when a correlation search matches a defined pattern. These are the main ways that ITSI can alert you to potential issues or incidents in your IT environment. Reference:Configure KPI thresholds in ITSI,Apply anomaly detection to a KPI in ITSI,Generate events with correlation searches in ITSI