Splunk SPLK-3002 Mock Exam

Shared by Everett on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Buttercup Retail sells t shirts both online and in stores. The IT Operations team is effectively monitoring the digital infrastructure. However, the executive leadership has expressed frustration in understanding what the related business impacts are of IT incidents.

Which option best entities would give Buttercup Retail executives the most impactful visibility?

Options:

A- store, product, payment type
B- store, season, customer age
C- host, browser type, software version
D- host, network interface, datacenter

Answer:

A

Explanation:

Splunk IT Service Intelligence (ITSI) is designed to align IT monitoring with the business outcomes that matter to stakeholders --- especially executives who are focused on service performance and its impact on revenue, customer experience, and operational goals. In ITSI, entities represent the individual components that make up services and contribute to Key Performance Indicators (KPIs). Selecting the right entities for service modeling is critical: technical entities (like hosts or network interfaces) are useful for IT operations troubleshooting, but they don't inherently represent business outcomes. Executive leadership cares about how incidents affect business capabilities and outcomes --- such as sales performance, customer transactions, and channel health. Therefore, entities that reflect business context (for example, store locations, product categories, or payment types) map IT issues directly to business performance indicators. When executives can see service health and incidents broken down by these business centric entities, they gain impactful visibility into how issues affect revenue, customer interactions, and overall business operations. In contrast, purely technical entities such as hosts or network interfaces do not provide that business impact perspective, and demographic slices like season or customer age --- while potentially valuable for marketing --- don't directly connect IT service health to business service performance in ITSI modeling.

Question 2

Question Type: MultipleChoice

How should entities be handled during the data audit phase of requirements gathering?

Options:

A- Entity meta-data for info and aliases should be identified and recorded as requirements.
B- Entities should be noted based upon Service KPI requirements such as 'by host' or 'by product line'.
C- Entities must be identified for every Service KPI defined and recorded in requirements.
D- Entities identified should be included in the entity filtering requirements, such as 'by processId' or 'by host'.

Answer:

A

Explanation:

During the data audit phase of requirements gathering for Splunk IT Service Intelligence (ITSI), it's crucial to identify and record the meta-data for entities, focusing on information (info) and aliases. This step involves understanding and documenting the key attributes and identifiers that describe each entity, such as host names, IP addresses, device types, or other relevant characteristics. These attributes are used to categorize and uniquely identify entities within ITSI, enabling more effective mapping of data to services and KPIs. By meticulously recording this meta-data, organizations ensure that their ITSI implementation is aligned with their specific monitoring needs and infrastructure, facilitating accurate service modeling and event management. This practice is foundational for setting up ITSI to reflect the actual IT environment, enhancing the relevance and effectiveness of the monitoring and analysis capabilities.

Question 3

Question Type: MultipleChoice

Which option best is a recommended best practice for service and glass table design?

Options:

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.

Answer:

A

Explanation:

A is the correct answer because it is recommended to plan and implement services first, then build detailed glass tables that reflect the service hierarchy and dependencies. This way, you can ensure that your glass tables provide accurate and meaningful service-level insights. Building glass tables first might lead to unnecessary or irrelevant KPIs that do not align with your service goals. Reference:Splunk IT Service Intelligence Service Design Best Practices

Question 4

Question Type: MultipleChoice

How can admins manually control groupings of notable events?

Options:

A- Correlation searches.
B- Multi-KPI alerts.
C- notable_event_grouping.conf
D- Aggregation policies.

Answer:

D

Explanation:

In Splunk IT Service Intelligence (ITSI), administrators can manually control the grouping of notable events using aggregation policies. Aggregation policies allow for the definition of criteria

based on which notable events are grouped together. This includes configuring rules based on event fields, severity, source, or other event attributes. Through these policies, administrators can tailor the event grouping logic to meet the specific needs of their environment, ensuring that related events are grouped in a manner that facilitates efficient analysis and response. This feature is crucial for managing the volume of events and focusing on the most critical issues by effectively organizing related events into manageable groups.

Question 5

Question Type: MultipleChoice

Besides creating notable events, what are the default alert actions a correlation search can execute? (Choose all that apply.)

Options:

A- Ping a host.
B- Send email.
C- Include in RSS feed.
D- Run a script.

Answer:

B, C, D

Explanation:

Throttling applies to any correlation search alert type, including notable events and actions (RSS feed, email, run script, and ticketing).

B, C, and D are correct answers because they are the default alert actions that a correlation search can execute besides creating notable events. You can configure a correlation search to send an email, include the results in an RSS feed, or run a custom script when the search matches a defined pattern. Ping a host is not a default alert action for correlation searches. Reference:Configure correlation search settings in ITSI

Question 6

Question Type: MultipleChoice

Which views would help an analyst identify that a memory usage KPI is going critical? (select all that apply)

Options:

A- Memory KPI in a glass table.
B- Memory panel of the OS Host Details view in the Operating System module.
C- Memory swim lane in a Deep Dive.
D- Service & KPI tiles in the Service Analyzer.

Answer:

A, B, C, D

Explanation:

To identify that a memory usage KPI is going critical, an analyst can leverage multiple views within Splunk IT Service Intelligence (ITSI), each offering a different perspective or level of detail:

A . Memory KPI in a glass table: A glass table can display the current status of the memory usage KPI, along with other related KPIs and services, providing a high-level overview of system health.

B . Memory panel of the OS Host Details view in the Operating System module: This specific panel within the OS Host Details view offers detailed metrics and trends related to memory usage, allowing for in-depth analysis.

C . Memory swim lane in a Deep Dive: Deep Dives allow analysts to visually track the performance and status of KPIs over time. A swim lane dedicated to memory usage can highlight periods where the KPI goes critical, along with the context of other related KPIs.

D . Service & KPI tiles in the Service Analyzer: The Service Analyzer provides a comprehensive overview of all services and their KPIs. The tiles related to memory usage can quickly alert analysts to critical conditions through color-coded indicators.

Each of these views contributes to a comprehensive monitoring strategy, enabling analysts to detect and respond to critical memory usage conditions from various analytical perspectives.

Question 7

Question Type: MultipleChoice

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

Options:

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.

Answer:

A

Explanation:

Adaptive thresholds are thresholds calculated by machine learning algorithms that dynamically adapt and change based on the KPI's observed behavior. Adaptive thresholds are useful for monitoring KPIs that have unpredictable or seasonal patterns that are difficult to capture with static thresholds. For example, you might use adaptive thresholds for a KPI that measures web traffic volume, which can vary depending on factors such as holidays, promotions, events, and so on. The advantage of using adaptive thresholds is:

A . Automatically update thresholds daily to manage dynamic changes to KPI values. This is true because adaptive thresholds use historical data from a training window to generate threshold values for each time block in a threshold template. Each night at midnight, ITSI recalculates adaptive threshold values for a KPI by organizing the data from the training window into distinct buckets and then analyzing each bucket separately. This way, the thresholds reflect the most recent changes in the KPI data and account for any anomalies or trends.

The other options are not advantages of using adaptive thresholds because:

B . Automatically adjust KPI calculation to manage dynamic event data. This is not true because adaptive thresholds do not affect the KPI calculation, which is based on the base search and the aggregation method. Adaptive thresholds only affect the threshold values that are used to determine the KPI severity level.

C . Automatically adjust aggregation policy grouping to manage escalating severity. This is not true because adaptive thresholds do not affect the aggregation policy, which is a set of rules that determines how to group notable events into episodes. Adaptive thresholds only affect the threshold values that are used to generate notable events based on KPI severity level.

D . Automatically adjust correlation search thresholds to adjust sensitivity over time. This is not true because adaptive thresholds do not affect the correlation search, which is a search that looks for relationships between data points and generates notable events. Adaptive thresholds only affect the threshold values that are used by KPIs, which can be used as inputs for correlation

searches.

P2P exams