



Free Questions for [SPLK-3002](#) by [certsdeals](#)

Shared by [Evans](#) on [09-08-2024](#)

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)

Question 1

Question Type: MultipleChoice

What is the minimum number of entities a KPI must be split by in order to use Entity Cohesion anomaly detection?

Options:

A- 3

B- 4

C- 5

D- 2

Answer:

D

Explanation:

For Entity Cohesion anomaly detection in Splunk IT Service Intelligence (ITSI), the minimum number of entities a KPI must be split by is 2. Entity Cohesion as a method of anomaly detection focuses on identifying anomalies based on the deviation of an entity's behavior in comparison to other entities within the same group or cohort. By requiring a minimum of only two entities, ITSI allows for the comparison

of entities to detect significant deviations in one entity's performance or behavior, which could indicate potential issues. This method leverages the idea that entities performing similar functions or within the same service should exhibit similar patterns of behavior, and significant deviations could be indicative of anomalies. The low minimum requirement of two entities ensures that this powerful anomaly detection feature can be utilized even in smaller environments.

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 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 4

Question Type: MultipleChoice

Which of the following is a recommended best practice for ITSI installation?

Options:

- A-** ITSI should not be installed on search heads that have Enterprise Security installed.
- B-** Before installing ITSI, make sure the Common Information Model (CIM) is installed.
- C-** Install the Machine Learning Toolkit app if anomaly detection must be configured.
- D-** Install ITSI on one search head in a search head cluster and migrate the configuration bundle to other search heads.

Answer:

A

Explanation:

One of the recommended best practices for Splunk IT Service Intelligence (ITSI) installation is to avoid installing ITSI on search heads that already have Splunk Enterprise Security (ES) installed. This recommendation stems from potential resource conflicts and performance issues that can arise when both resource-intensive applications are deployed on the same instance. Both ITSI and ES are complex applications that require significant system resources to function effectively, and running them concurrently on the same search head can lead to degraded performance, conflicts in resource allocation, and potential stability issues. It's generally advised to segregate these applications onto separate Splunk instances to ensure optimal performance and stability for both platforms.

Question 5

Question Type: MultipleChoice

Which of the following is part of setting up a new aggregation policy?

Options:

- A-** Filtering criteria
- B-** Policy version

C- Review order

D- Module rules

Answer:

A

Explanation:

When setting up a new aggregation policy in Splunk IT Service Intelligence (ITSI), one of the crucial components is defining the filtering criteria. This aspect of the aggregation policy determines which events should be included in the aggregation based on specific conditions or attributes. The filtering criteria can be based on various event fields such as severity, source, event type, and other custom fields relevant to the organization's monitoring strategy. By specifying the filtering criteria, ITSI administrators can ensure that the aggregation policy is applied only to the pertinent events, thus facilitating more targeted and effective event management and reducing noise in the operational environment. This helps in organizing and prioritizing events more efficiently, enhancing the overall incident management process within ITSI.

Question 6

Question Type: MultipleChoice

Which of the following statements describe default glass tables in ITSI?

Options:

- A- The Service Health Score default glass table.
- B- There is one default glass table per service.
- C- There is one service template default glass table.
- D- There are no default glass tables.

Answer:

D

Explanation:

In Splunk IT Service Intelligence (ITSI), glass tables are fully customizable dashboards that provide a visual representation of an organization's IT environment, along with the health and status of services and KPIs. Unlike some pre-configured views or dashboards that might come with default setups in various platforms, ITSI does not provide default glass tables out of the box. Instead, users are encouraged to create their own glass tables tailored to their specific monitoring needs and operational views. This approach ensures that each organization can design glass tables that best represent their unique infrastructure, applications, and service landscapes, providing a more personalized and relevant operational overview.

Question 7

Question Type: MultipleChoice

Which of the following best describes an ITSI Glass Table?

Options:

- A-** A view which displays a system topology overlaid with KPI metrics.
- B-** A view which describes a topology.
- C-** A dashboard which displays a system topology.
- D-** A view showing KPI values in a variety of visual styles.

Answer:

A

Explanation:

An ITSI Glass Table provides a customizable, high-level view that can display a system's topology overlaid with real-time Key Performance Indicator (KPI) metrics and service health scores. This visualization tool allows users to create a visual representation of their IT infrastructure, applications, and services, integrating live data to monitor the health and performance of each component in

context. The ability to overlay KPI metrics on the system topology enables IT and business stakeholders to quickly understand the operational status and health of various elements within their environment, facilitating more informed decision-making and rapid response to issues.

To Get Premium Files for SPLK-3002 Visit

<https://www.p2pexams.com/products/splk-3002>

For More Free Questions Visit

<https://www.p2pexams.com/splunk/pdf/splk-3002>

