Free Questions for SPLK-3002 by actualtestdumps

Shared by Pitts on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following is a good use case for creating a custom module?

Options:

A- Modules are required to create entity and service import searches.

B- Modules are required to be able to create custom visualizations for deep dives.

C- Making it easy to migrate KPI base searches and related visualizations to other ITSI installations.

D- Creating a service template to make it easy to automatically create new services during service and entity import.

Answer:

C

Explanation:

Creating a custom module in Splunk IT Service Intelligence (ITSI) is particularly beneficial for the purpose of migrating KPI base searches and related visualizations to other ITSI installations. Custom modules can encapsulate a set of configurations, searches, and visualizations that are tailored to specific monitoring needs or environments. By packaging these elements into a module, it becomes

easier to transfer, deploy, and maintain consistency across different ITSI instances. This modularity supports the reuse of developed components, simplifying the process of scaling and replicating monitoring setups in diverse operational contexts. The ability to migrate these components seamlessly enhances operational efficiency and ensures that best practices and custom configurations can be shared across an organization's ITSI deployments.

Question 2

Question Type: **MultipleChoice**

How can Service Now incidents be created automatically when a Multi-KPI alert triggers? (select all that apply)

Options:

A- By creating a custom etc/apps/SA-ITOA/workflow_rules. conf

B- By linking Entities to Service-Now configuration items.

C- By creating a notable event aggregation policy with a SNOW incident action.

D- By editing the associated correlation search and specifying an alert action.

Answer:

C, D

Explanation:

To automatically create ServiceNow incidents when a Multi-KPI alert triggers in Splunk IT Service Intelligence (ITSI), the following approaches can be used:

C) By creating a notable event aggregation policy with a ServiceNow (SNOW) incident action: ITSI allows the creation of notable event aggregation policies that can specify actions to be taken when certain conditions are met. One of these actions can be the creation of an incident in ServiceNow, directly linking the alerting mechanism in ITSI with incident management in ServiceNow.

D) By editing the associated correlation search and specifying an alert action: Correlation searches in ITSI are used to identify patterns or conditions that signify notable events. These searches can be configured to include alert actions, such as creating a ServiceNow incident, whenever the search conditions are met. This direct integration ensures that incidents are automatically generated in ServiceNow, based on the specific criteria defined in the correlation search.

Options A and B are not standard practices for integrating ITSI with ServiceNow for automatic incident creation. The configuration typically involves setting up actionable alert mechanisms within ITSI that are specifically designed to integrate with external systems like ServiceNow.

Question 3

Question Type: MultipleChoice

Which is the least permissive role required to modify default deep dives?

Options:

A- itoa_analyst

B- admin

C- power

D- itoa_admin

Answer:

D

Explanation:

To modify default deep dives in Splunk IT Service Intelligence (ITSI), the least permissive role typically required is the itoa_admin role. This role is specifically designed within ITSI to provide administrative capabilities, including the ability to configure and customize various aspects of ITSI, such as services, KPIs, and deep dives. The itoa_admin role has the necessary permissions to edit and manage default deep dives, enabling users with this role to tailor the deep dives to meet specific operational requirements and preferences. Other roles like itoa_analyst, admin, or power might not have sufficient privileges to modify default deep dives, as these roles are generally more restricted in terms of their ability to make broad changes within ITSI.

Question 4

Question Type: MultipleChoice

Which ITSI components are required before a module can be created?

Options:

A- One or more entity import saved searches.

B- One or more services with KPIs and their associated base searches.

C- One or more datamodels.

D- One or more correlation searches and their associated entities.

Answer:

C

Explanation:

Before a module can be created in Splunk IT Service Intelligence (ITSI), it is essential to have one or more datamodels established. Datamodels in Splunk provide a structured format for organizing and interpreting data, which is crucial for modules within ITSI. Modules often rely on datamodels to extract, transform, and present data in a meaningful way, especially when dealing with complex datasets across various sources. Datamodels serve as the foundation for the module's ability to categorize and analyze data efficiently, enabling the creation of KPIs, services, and visualizations that are aligned with the specific needs of the module. Having these datamodels in place ensures that the module can function correctly and provide valuable insights into the monitored IT environments.

Question 5

Question Type: MultipleChoice

Which anomaly detection algorithm is included within ITSI?

Options:

A- Entity cohesion

B- Standard deviation

C- Linear regression

D- Infantile regression

Answer:

A

Explanation:

Among the anomaly detection algorithms included within Splunk IT Service Intelligence (ITSI), 'Entity Cohesion' is a notable option. The Entity Cohesion algorithm is designed to detect anomalies by comparing the behavior of one entity against the collective behavior of a group of similar entities. This approach is particularly useful in scenarios where entities are expected to exhibit similar patterns of behavior under normal conditions. Anomalies are identified when an entity's metrics deviate significantly from the group norm, suggesting a potential issue with that specific entity. This method leverages the concept of cohesion among similar entities to enhance the accuracy and relevance of anomaly detection within ITSI environments.

Question 6

Question Type: MultipleChoice

When working with a notable event group in the Notable Events Review dashboard, which of the following can be set at the individual or group level?

Options:

A- Service, status, owner.

B- Severity, status, owner.

C- Severity, comments, service.

D- Severity, status, service.

Answer:

B

Explanation:

In the Notable Events Review dashboard within Splunk IT Service Intelligence (ITSI), when working with a notable event group, users can set or adjust certain attributes at the individual event level or at the group level. These attributes include:

Severity: The importance or impact level of the notable event or group, which can be adjusted to reflect the current assessment of the situation.

Status: The current state of the notable event or group, such as 'New,' 'In Progress,' or 'Resolved,' indicating the progress in addressing the event or group.

Owner: The user or team responsible for managing and resolving the notable event or group.

These settings allow for effective management and tracking of notable events, ensuring that they are appropriately prioritized, acted upon, and resolved by the responsible parties.

Question 7

Question Type: MultipleChoice

Which of the following services often has KPIs but no entities?

Options:

A- Security Service.

B- Network Service.

C- Business Service.

D- Technical Service.

Answer:

C

Explanation:

In the context of Splunk IT Service Intelligence (ITSI), a Business Service often has Key Performance Indicators (KPIs) but might not have directly associated entities. Business Services represent high-level aggregations of organizational functions or processes and are typically measured by KPIs that reflect the performance of underlying technical services or components rather than direct infrastructure entities. For example, a Business Service might monitor overall transaction completion times or customer satisfaction scores, which are abstracted from the specific technical entities that underlie these metrics. This abstraction allows Business Services to provide a business-centric view of IT health and performance, focusing on outcomes rather than specific technical components.

Question 8

Question Type: MultipleChoice

Which of the following is a characteristic of notable event groups?

Options:

A- Notable event groups combine independent notable events.

B- Notable event groups are created in the itsi_tracked_alerts index.

C- Notable event groups allow users to adjust threshold settings.

D- All of the above.

Answer:

A

Explanation:

In Splunk IT Service Intelligence (ITSI), notable event groups are used to logically group related notable events, which enhances the manageability and analysis of events:

A) Notable event groups combine independent notable events: This characteristic allows for the aggregation of related events into a single group, making it easier for users to manage and investigate related issues. By grouping events, users can focus on the broader context of an issue rather than getting lost in the details of individual events.

While notable event groups play a critical role in organizing and managing events in ITSI, they do not inherently allow users to adjust threshold settings, which is typically handled at the KPI or service level. Additionally, while notable event groups are utilized within the ITSI framework, the statement that they are created in the 'itsi_tracked_alerts' index might not fully capture the complexity of how event groups are managed and stored within the ITSI architecture.

Question 9

Question Type: MultipleChoice

What can a KPI widget on a glass table drill down into?

Options:

A- Another glass table.

B- A Splunk dashboard.

C- A custom deep dive.

D- Any of the above.

Answer:

D

Explanation:

In Splunk IT Service Intelligence (ITSI), a KPI widget on a glass table can be configured to drill down into a variety of destinations based on the needs of the user and the design of the glass table. This flexibility allows users to dive deeper into the data or analysis represented by the KPI widget, providing context and additional insights. The destinations for drill-downs from a KPI widget can include:

A) Another glass table, offering a different perspective or more detailed view related to the KPI. B. A Splunk dashboard that provides broader analysis or incorporates data from multiple sources. C. A custom deep dive for in-depth, time-series analysis of the KPI and related metrics.

This versatility makes KPI widgets powerful tools for navigating through the wealth of operational data and insights available in ITSI, facilitating effective monitoring and decision-making.

Question 10

Question Type: MultipleChoice

Which of the following are characteristics of service templates? (select all that apply)

Options:

A- Service templates can be modified after services are instantiated from it.

B- Service templates contain KPIs and KPI thresholds.

C- Service templates can contain specific or generic entity rules.

D- Service templates contain domain specific dashboards and deep dives.

Answer:

B, C

Explanation:

Service templates in Splunk IT Service Intelligence (ITSI) are designed to streamline the creation of services by providing pre-defined configurations:

B) Service templates contain KPIs and KPI thresholds: This allows for the standardized deployment of services with predefined performance indicators and their associated thresholds, ensuring consistency across similar services.

C) Service templates can contain specific or generic entity rules: These rules define how entities are associated with services created from the template, allowing for both broad and targeted applicability.

While service templates contain configurations for KPIs, thresholds, and entity rules, the ability to modify templates after services have been instantiated from them is limited. Changes to a template do not retroactively affect services already created from that template. Moreover, service templates do not inherently contain domain-specific dashboards or deep dives; these are created separately within ITSI.