Free Questions for SPLK-3002 by dumpshq

Shared by Doyle on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Which of the following items describe ITSI teams? (select all that apply)

Options:

A- Teams should have itoa admin roles added with read-only permissions for services and entities.

B- Services should be assigned to the 'global' team if all users need access to it.

C- By default, all services are owned by the built-in 'global' team and administered by the 'itoa_admin' role.

D- A new team admin role should be created for each team. The new role should inherit the 'itoa_team_admin' role.

Answer:

B, C, D

Explanation:

In Splunk IT Service Intelligence (ITSI), teams are used to organize services, KPIs, and other objects within ITSI to facilitate access control and management:

B) Services should be assigned to the 'global' team if all users need access to it: The 'global' team in ITSI is a built-in concept that denotes universal accessibility. Assigning services to the 'global' team makes them accessible to all ITSI users, irrespective of their specific team memberships. This is useful for services that are relevant across the entire organization.

C) By default, all services are owned by the built-in 'global' team and administered by the 'itoa_admin' role: This default setting ensures that upon creation, services are accessible to administrators and can be further re-assigned or refined for access by specific teams as needed.

D) A new team admin role should be created for each team. The new role should inherit the 'itoa_team_admin' role: This best practice allows for granular access control and management within teams. Each team can have its own administrators with the appropriate level of access and permissions tailored to the needs of that team, derived from the capabilities of the 'itoa_team_admin' role.

The concept of adding 'itoa admin roles' with read-only permissions contradicts the typical use case for administrative roles, which usually require more than read-only access to manage services and entities effectively.

Question 2

Question Type: MultipleChoice

When troubleshooting KPI search performance, which search names in job activity identify base searches?

Options:

A- Indicator - XXXX - Base Search

B- Indicator - Shared - xxxx - ITSI Search

C- Indicator - Base - xxxx - ITSI Search

D- Indicator - Base - XXXX - Shared Search

Answer:

B

Explanation:

In the context of troubleshooting KPI search performance in Splunk IT Service Intelligence (ITSI), the search names in the job activity that identify base searches typically follow the pattern 'Indicator - Shared - xxxx - ITSI Search.' These base searches are fundamental components of the KPI calculation process, aggregating and preparing data for further analysis by KPIs. Identifying these base searches in the job activity is crucial for diagnosing performance issues, as these searches can be resource-intensive and impact overall system performance. Understanding the naming convention helps administrators and analysts quickly pinpoint the base searches related to specific KPIs, facilitating more effective troubleshooting and optimization of search performance within the ITSI environment.

Question 3

Question Type: **MultipleChoice**

Which of the following is a characteristic of custom deep dives?

Options:

A- Allows itoa_analyst roles to add comments.

B- Requires at least 7 days' data to show anomalies.

C- Combines metric, event, KPI, and service health score lanes.

D- Uses drilldown to generate notable events via anomaly detection.

Answer:

C

Explanation:

Custom deep dives in Splunk IT Service Intelligence (ITSI) are versatile and highly customizable dashboards that allow users to analyze various types of data in a unified view. One of the key characteristics of custom deep dives is their ability to combine lanes of different data types, such as metrics, events, Key Performance Indicators (KPIs), and service health scores. This multifaceted approach provides a comprehensive and layered view of the IT environment, enabling analysts and operators to correlate different data types and gain deeper insights into the health and performance of services. By incorporating these diverse data lanes, custom deep dives facilitate a more holistic understanding of the operational landscape, aiding in more effective troubleshooting and decision-making.

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

There are two Smart Mode configuration settings that control how fields affect grouping. Which of these is correct?

Options:

A- Text deviation and category deviation.

B- Text similarity and category deviation.

C- Text similarity and category similarity.

D- Text deviation and category similarity.

Answer:

C

Explanation:

In the context of Smart Mode configuration within Splunk IT Service Intelligence (ITSI), the two settings that control how fields affect grouping are 'Text similarity' and 'Category similarity.' Smart Mode is a feature used in event grouping that leverages machine learning to automatically group related events. 'Text similarity' refers to how closely the textual content of event fields must match for those events to be grouped together, taking into account commonalities in strings or narratives within the event data. 'Category similarity,' on the other hand, relates to the similarity in the categorical attributes of events, such as event types or source types, which helps in clustering events that are similar in nature or origin. Both of these settings are crucial in determining how events are grouped in ITSI, influencing the granularity and relevance of the event groupings based on textual and categorical similarities.

Question 6

Question Type: MultipleChoice

To use Adaptive Threshholding, what is the minimum requirement for a set of KPI data?

Options:

A- 14 days old.

B- 7 days old.

C- 30 days old.

D- 10 days old.

Answer:

B

Explanation:

To utilize Adaptive Thresholding in Splunk IT Service Intelligence (ITSI), the minimum requirement for a set of Key Performance Indicator (KPI) data is that it must be at least 7 days old. Adaptive Thresholding uses historical data to dynamically adjust thresholds based on observed patterns and trends. Having a minimum of 7 days worth of data allows the system to analyze a sufficient amount of information to identify normal ranges and variances in KPI behavior, thereby setting more accurate and contextually relevant thresholds. This requirement ensures that the adaptive thresholds are based on a meaningful data set that reflects the typical operational conditions of the monitored services.

Question 7

Question Type: **MultipleChoice**

Which of the following can generate notable events?

Options:

A- Through ad-hoc search results which get processed by adaptive thresholds.

B- When two entity aliases have a matching value.

C- Through scheduled correlation searches which link to their respective services.

D- Manually selected using the Notable Event Review panel.

Answer:

C

Explanation:

Notable events in Splunk IT Service Intelligence (ITSI) are primarily generated through scheduled correlation searches. These searches are designed to monitor data for specific conditions or patterns defined by the ITSI administrator, and when these conditions are met, a notable event is created. These correlation searches are often linked to specific services or groups of services, allowing for targeted monitoring and alerting based on the operational needs of those services. This mechanism enables ITSI to provide timely and relevant alerts that can be further investigated and managed through the Episode Review dashboard, facilitating efficient incident response and management within the IT environment.