Free Questions for SPLK-3002

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

Options:

A- itoa_analyst
B- admin
C- power
D- itoa_admin

P2P exams

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.

P2P exams

Question 2

Question Type: MultipleChoice

Which of the following statements is accurate when using multiple policies?

Options:

A- New policies are applied after the default policy.
B- Policy processing is applied in a defined order.
C- An event can be processed by only a single policy.

D- New policies are applied before the default policy.

Answer:

B

Explanation:

In Splunk IT Service Intelligence (ITSI), when using multiple event management policies, it is important to understand that policy processing is applied in a defined order. This order is crucial because it determines how events are processed and aggregated, and which rules are applied to events first. The order of policies can be customized, allowing administrators to prioritize certain policies over others based on the specific needs and operational logic of their IT environment. This feature provides flexibility in event management, enabling more precise control over event processing and ensuring that the most critical events are handled according to the desired precedence. This structured approach to policy processing helps in maintaining the efficiency and effectiveness of event management within ITSI.

Question 3

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 4

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 5

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 6

Question Type: MultipleChoice

Which of the following items describe ITSI Deep Dive capabilities? (Choose all that apply.)

Options:

A- Comparing a service's notable events over a time period.
B- Visualizing one or more Service KPIs values by time.
C- Examining and comparing alert levels for KPIs in a service over time.
D- Comparing swim lane values for a slice of time.

Answer:

B, C, D

Explanation:

A deep dive is a dashboard that allows you to analyze the historical trends and anomalies of your KPIs and metrics in ITSI. A deep dive displays a timeline of events and swim lanes of data that you can customize and filter to investigate issues and perform root cause analysis. Some of the capabilities of deep dives are:

B) Visualizing one or more service KPIs values by time. This is true because you can add KPI swim lanes to a deep dive to show the values and severity levels of one or more KPIs over time. You can also compare KPIs from different services or entities using service swapping or entity splitting.

C) Examining and comparing alert levels for KPIs in a service over time. This is true because you can add alert swim lanes to a deep dive to show the alert levels and counts for one or more KPIs over time. You can also drill down into the alert details and view the notable events associated with each alert.

D) Comparing swim lane values for a slice of time. This is true because you can use the time range selector to zoom in or out of a specific time range in a deep dive. You can also use the time brush to select a slice of time and compare the swim lane values for that time period.

The other option is not a capability of deep dives because:

A) Comparing a service's notable events over a time period. This is not true because deep dives do not display notable events, which are alerts generated by ITSI based on certain conditions or correlations. Notable events are displayed in other dashboards, such as episode review or glass tables.

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

