

Exam Questions SPLK-3002

Splunk IT Service Intelligence Certified Admin Exam

<https://www.2passeasy.com/dumps/SPLK-3002/>



NEW QUESTION 1

What happens when an anomaly is detected?

- A. A separate correlation search needs to be created in order to see it.
- B. A SNMP trap will be sent.
- C. An anomaly alert will appear in core splunk, in index=main.
- D. An anomaly alert will appear as a notable event in Episode Review.

Answer: D

Explanation:

When an anomaly is detected in Splunk IT Service Intelligence (ITSI), it typically generates a notable event that can be reviewed and managed in the Episode Review dashboard. The Episode Review is part of ITSI's Event Analytics framework and serves as a centralized location for reviewing, annotating, and managing notable events, including those generated by anomaly detection. This process enables IT operators and analysts to efficiently identify, prioritize, and respond to potential issues highlighted by the anomaly alerts. The integration of anomaly alerts into the Episode Review dashboard streamlines the workflow for managing and investigating these alerts within the broader context of IT service management and operational intelligence.

NEW QUESTION 2

Which of the following describes default deep dives?

- A. Are manually generated and can be accessed via the Service Analyzer.
- B. Include all KPIs of all services.
- C. Are auto-generated and can be accessed via the Service Analyzer.
- D. Include health scores of all services.

Answer: C

Explanation:

In Splunk IT Service Intelligence (ITSI), default deep dives are auto-generated and can be accessed via the Service Analyzer. Deep dives are an essential feature of ITSI that provide an in-depth, granular view into the health and performance of services and their associated KPIs. These default deep dives are automatically created for each service, allowing users to quickly drill down into the detailed operational metrics and performance data of their services. By accessing these deep dives through the Service Analyzer, ITSI users can efficiently investigate issues, understand service dependencies, and make informed decisions to maintain optimal service health. The auto-generated nature of these default deep dives simplifies the monitoring and analysis process, providing immediate insights into service performance without the need for manual setup or configuration.

NEW QUESTION 3

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

- 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.

NEW QUESTION 4

In distributed search, which components need to be installed on instances other than the search head?

- A. SA-IndexCreation and SA-ITSI-Licensechecker on indexers.
- B. SA-IndexCreation and SA-ITOA on indexers; SA-ITSI-Licensechecker and SA- UserAccess on the license master.
- C. SA-IndexCreation on indexers; SA-ITSI-Licensechecker and SA-UserAccess on the license master.
- D. SA-ITSI-Licensechecker on indexers.

Answer: A

Explanation:

SA-IndexCreation is required on all indexers. For non-clustered, distributed environments, copy SA-IndexCreation to \$SPLUNK_HOME/etc/apps/ on individual indexers. Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/Install/InstallIDD>

In distributed search, the components that need to be installed on instances other than the search head are SA-IndexCreation and SA-ITSI-Licensechecker on indexers. SA- IndexCreation is an add-on that creates the indexes required by ITSI, such as itsi_summary and itsi_tracked_alerts. SA-ITSI-Licensechecker is an add-on that monitors the license usage of ITSI and generates alerts when the license limit is exceeded or about to expire. These components need to be installed on indexers because they handle the data ingestion and storage functions for ITSI. The other components, such as ITSI app and SA-ITOA, need to be installed on the search head(s) because they handle the search management and presentation functions for ITSI. References: Install IT Service Intelligence in a distributed environment

NEW QUESTION 5

Which of the following best describes a default deep dive?

- A. It initially shows the health scores for all services.
- B. It initially shows the highest importance KPIs.
- C. It initially shows all of the KPIs for a selected service.
- D. It initially shows all the entity swim lanes.

Answer: C

Explanation:

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/DeepDives>

C is the correct answer because a default deep dive initially shows all of the KPIs for a selected service. You can create a default deep dive by drilling down from another dashboard or by selecting a service from the deep dive lister page. A default deep dive does not show health scores, importance scores, or entity swim lanes by default. References: [Create default deep dives for services in ITSI]

NEW QUESTION 6

For which ITSI function is it a best practice to use a 15-30 minute time buffer?

- A. Correlation searches.
- B. Adaptive thresholding.
- C. Maintenance windows
- D. Anomaly detection.

Answer: B

Explanation:

B is the correct answer because adaptive thresholding is a feature of ITSI that allows you to dynamically adjust KPI thresholds based on historical patterns and trends. Adaptive thresholding requires a time buffer of at least 15 minutes to calculate the thresholds based on the previous data points. The time buffer ensures that there is enough data to perform the calculations and avoid false positives or negatives. References: Configure adaptive thresholding for a KPI in ITSI

NEW QUESTION 7

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

- 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.

NEW QUESTION 8

Which of the following best describes an ITSI Glass Table?

- 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.

NEW QUESTION 9

Anomaly detection can be enabled on which one of the following?

- A. KPI
- B. Multi-KPI alert
- C. Entity
- D. Service

Answer: A

Explanation:

A is the correct answer because anomaly detection can be enabled on a KPI level in ITSI. Anomaly detection allows you to identify trends and outliers in KPI search results that might indicate an issue with your system. You can enable anomaly detection for a KPI by selecting one of the two anomaly detection algorithms in the KPI configuration panel. References: Apply anomaly detection to a KPI in ITSI

NEW QUESTION 10

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

- 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.

NEW QUESTION 10

Which index contains ITSI Episodes?

- A. itsi_tracked_alerts
- B. itsi_grouped_alerts
- C. itsi_notable_archive
- D. itsi_summary

Answer: B

Explanation:

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/IndexOverview>

B is the correct answer because ITSI episodes are stored in the itsi_grouped_alerts index. This index contains notable events that have been grouped together based on predefined aggregation policies. Episodes help you reduce alert noise and focus on resolving incidents faster. References: [Overview of episodes in ITSI]

NEW QUESTION 14

Which anomaly detection algorithm is included within ITSI?

- 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.

NEW QUESTION 19

What are valid considerations when designing an ITSI Service? (Choose all that apply.)

- A. Service access control requirements for ITSI Team Access should be considered, and appropriate teams provisioned prior to creating the ITSI Service.
- B. Entities, entity meta-data, and entity rules should be planned carefully to support the service design and configuration.
- C. Services, entities, and saved searches are stored in the ITSI app, while events created by KPI execution are stored in the itsi_summary index.
- D. Backfill of a KPI should always be selected so historical data points can be used immediately and alerts based on that data can occur.

Answer: ABC

Explanation:

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/ImplementPerms>

A, B, and C are correct answers because service access control requirements for ITSI Team Access should be considered before creating the ITSI Service, as different teams may have different permissions and views of the service data. Entities, entity meta-data, and entity rules should also be planned carefully to support the service design and configuration, as they determine how ITSI maps data sources to services and KPIs. Services, entities, and saved searches are stored in the ITSI app, while events created by KPI execution are stored in the itsi_summary index for faster retrieval and analysis. References: ITSI service design best practices, Overview of ITSI indexes

NEW QUESTION 20

Which deep dive swim lane type does not require writing SPL?

- A. Event lane.
- B. Automatic lane.
- C. Metric lane.
- D. KPI lane.

Answer:

D

Explanation:

A KPI lane is a type of deep dive swim lane that does not require writing SPL. You can simply select a service and a KPI from a drop-down list and ITSI will automatically populate the lane with the corresponding data. You can also adjust the threshold settings and time range for the KPI lane. References: [KPI Lanes]

NEW QUESTION 24

What are valid ITSI Glass Table editor capabilities? (Choose all that apply.)

- A. Creating glass tables.
- B. Correlation search creation.
- C. Service swapping configuration.
- D. Adding KPI metric lanes to glass tables.

Answer: ACD

Explanation:

Create a glass table to visualize and monitor the interrelationships and dependencies across your IT and business services.

The service swapping settings are saved and apply the next time you open the glass table. You can add metrics like KPIs, ad hoc searches, and service health scores that update in real time against a background that you design. Glass tables show real-time data generated by KPIs and services.

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/GTOverview>

The glass table editor is a tool that allows you to create and edit glass tables in ITSI. Some of the capabilities of the glass table editor are:

Creating glass tables from scratch or from existing templates.

Configuring service swapping on widgets to toggle displaying metrics from different services.

Adding KPI metric lanes to glass tables to show historical trends of KPI values.

The glass table editor does not support correlation search creation, which is a separate feature in ITSI that allows you to create searches that look for relationships between data points and generate notable events. References: Overview of the glass table editor in ITSI,

[Configure service swapping on glass tables], [Add KPI metric lanes to glass tables], [Overview of correlation searches in ITSI]

NEW QUESTION 27

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

- 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.

NEW QUESTION 32

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

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

Answer: BCD

Explanation:

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

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/EA/ConfigCS>

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. References: Configure correlation search settings in ITSI

NEW QUESTION 33

Which of the following items apply to anomaly detection? (Choose all that apply.)

- A. Use AD on KPIs that have an unestablished baseline of data point
- B. This allows the ML pattern to perform it??s magic.
- C. A minimum of 24 hours of data is needed for anomaly detection, and a minimum of 4 entities for cohesive analysis.
- D. Anomaly detection automatically generates notable events when KPI data diverges from the pattern.
- E. There are 3 types of anomaly detection supported in ITSI: adhoc, trending, and cohesive.

Answer: BC

Explanation:

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/AD>

Anomaly detection is a feature of ITSI that uses machine learning to detect when KPI data deviates from a normal pattern. The following items apply to anomaly detection:

- * B. A minimum of 24 hours of data is needed for anomaly detection, and a minimum of 4 entities for cohesive analysis. This ensures that there is enough data to establish a baseline pattern and compare different entities within a service.
- * C. Anomaly detection automatically generates notable events when KPI data diverges from the pattern. You can configure the sensitivity and severity of the anomaly detection alerts and assign them to episodes or teams. References: [Anomaly Detection]

NEW QUESTION 36

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

- 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.

NEW QUESTION 37

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

- 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: BC

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.

NEW QUESTION 40

Which of the following describes enabling smart mode for an aggregation policy?

- A. Configure → Policies → Smart Mode → Enable, select ??fields??.
- B. Enable grouping in Notable Event Review, select ??Smart Mode??.
- C. Edit the aggregation policy, enable smart mode, select fields to analyze, click ??Save??.
- D. Edit the notable event view, enable smart mode, select ??fields??.

Answer: C

Explanation:

- * 1. From the ITSI main menu, click Configuration > Notable Event Aggregation Policies.

- * 2. Select a custom policy or the Default Policy.

- * 3. Under Smart Mode grouping, enable Smart Mode.

- * 4. Click Select fields. A dialog displays the fields found in your notable events from the last 24 hours.

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/EA/SmartMode>

C is the correct answer because smart mode is a feature of aggregation policies that allows ITSI to automatically group notable events based on the fields that have the most impact on the event occurrence. You can enable smart mode for an aggregation policy by editing the policy, selecting the smart mode option, and choosing the fields to analyze. You can also specify a minimum number of events to trigger smart mode and a maximum number of groups to create. References: Configure smart mode for aggregation policies in ITSI

NEW QUESTION 43

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SPLK-3002 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SPLK-3002 Product From:

<https://www.2passeasy.com/dumps/SPLK-3002/>

Money Back Guarantee

SPLK-3002 Practice Exam Features:

- * SPLK-3002 Questions and Answers Updated Frequently
- * SPLK-3002 Practice Questions Verified by Expert Senior Certified Staff
- * SPLK-3002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SPLK-3002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year