Splunk SPLK-3002 Practice Questions

Shared by Beard on 18-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following describes default deep dives?

Options:

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.

Question 2

Question Type: MultipleChoice

Which of the following describes default deep dives?

Options:

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.

Question 3

Question Type: MultipleChoice

Which option best describes enabling smart mode for an aggregation policy?

Options:

A- Configure --> Policies --> Smart Mode --> Enable, select ''fields'', click ''Save''
B- Enable grouping in Notable Event Review, select ''Smart Mode'', select ''fields'', and click ''Save''
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'', and click ''Save''

Answer:

C

Explanation:

1. From the ITSI main menu, clickConfiguration>Notable Event Aggregation Policies.

2. Select a custom policy or the Default Policy.

3. Under Smart Mode grouping, enableSmart Mode.

4. ClickSelect fields. A dialog displays the fields found in your notable events from the last 24 hours.

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. Reference:Configure smart mode for aggregation policies in ITSI

Question 4

Question Type: MultipleChoice

Which option best items apply to anomaly detection? (Choose all that apply.)

Options:

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

Answer:

B, C

Explanation:

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. Reference: [Anomaly Detection]

Question 5

Question Type: MultipleChoice

Within a correlation search, dynamic field values can be specified with what syntax?

Options:

A- fieldname
B- By editing the associated correlation search and specifying an alert action.
C- %fieldname%
D- eval(fieldname)

Answer:

B

Explanation:

B is the correct answer because dynamic field values can be specified with <fieldname /fieldname> syntax within a correlation search. This syntax allows you to insert values from fields returned by the correlation search into alert actions such as email subject or body. For example, <host /host> inserts the value of the host field into the email. Reference: [Use dynamic field values in correlation searches in ITSI]

Question 6

Question Type: MultipleChoice

Which scenario would benefit most by implementing ITSI?

Options:

A- Monitoring of business services functionality.
B- Monitoring of system hardware.
C- Monitoring of system process statuses
D- Monitoring of retail sales metrics.

Answer:

A

Explanation:

Splunk IT Service Intelligence (ITSI) is a monitoring and analytics solution that uses artificial intelligence and machine learning to provide insights into the health and performance of IT services. ITSI lets you create services that represent the critical components of your IT infrastructure, such as applications, databases, servers, networks, and so on. You can then monitor the status and performance of these services using key performance indicators (KPIs), which are metrics that measure aspects of service health, such as availability, latency, error rate, and so on. ITSI also provides tools for visualizing, investigating, and alerting on service issues, such as service analyzers, glass tables, deep dives, episode review, and so on. The scenario that would benefit most by implementing ITSI is monitoring of business service functionality, because ITSI enables you to measure and improve the quality and reliability of your IT services and align them with your business objectives. Reference:What is Splunk IT Service Intelligence?

Question 7

Question Type: MultipleChoice

Which of the following describes entities? (Choose all that apply.)

Options:

A- Entities must be IT devices, such as routers and switches, and must be identified by either IP value, host name, or mac address.
B- An abstract (pseudo/logical) entity can be used to split by for a KPI, although no entity rules or filtering can be used to limit data to a specific service.
C- Multiple entities can share the same alias value, but must have different role values.
D- To automatically restrict the KPI to only the entities in a particular service, select ''Filter to Entities in Service''.

Answer:

B, D

Explanation:

Entities are IT components that require management to deliver an IT service. Each entity has specific attributes and relationships to other IT processes that uniquely identify it. Entities contain alias fields and informational fields that ITSI associates with indexed events. Some statements that describe entities are:

B . An abstract (pseudo/logical) entity can be used to split by for a KPI, although no entity rules or filtering can be used to limit data to a specific service. An abstract entity is an entity that does not represent a physical host or device, but rather a logical grouping of data sources. For example, you can create an abstract entity for each business unit in your organization and use it to split by for a KPI that measures revenue or customer satisfaction. However, you cannot use entity rules or filtering to limit data to a specific service based on abstract entities, because they do not have alias fields that match indexed events.

D . To automatically restrict the KPI to only the entities in a particular service, select ''Filter to Entities in Service''. This option allows you to filter the data sources for a KPI by the entities that are assigned to the service. For example, if you have a service for web servers and you want to monitor the CPU load percent for each web server entity, you can select this option to ensure that only the events from those entities are used for the KPI calculation.

Question 8

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 9

Question Type: MultipleChoice

Which of the following is a characteristic of base searches?

Options:

A- Search expression, entity splitting rules, and thresholds are configured at the base search level.
B- It is possible to filter to entities assigned to the service for calculating the metrics for the service's KPIs.
C- The fewer KPIs that share a common base search, the more efficiency a base search provides, and anomaly detection is more efficient.
D- The base search will execute whether or not a KPI needs it.

Answer:

B

Explanation:

A base search is a search definition that can be shared across multiple KPIs that use the same data source. Base searches can improve search performance and reduce search load by consolidating multiple similar KPIs. One of the characteristics of base searches is that it is possible to filter to entities assigned to the service for calculating the metrics for the service's KPIs. This means that you can use entity filtering rules to specify which entities are relevant for each KPI based on the base search results. Reference:Create KPI base searches in ITSI, [Filter entities for KPIs based on base searches]

Question 10

Question Type: MultipleChoice

Which option best 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.