Actual exam question from Splunk's SPLK-3002

Question #: 1

Topic #: 1

[All SPLK-3002 Questions]

After a notable event has been closed, how long will the meta data for that event remain in the KV Store by default?

A. 6 months.

B. 9 months.

C. 1 year.

D. 3 months.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 2

Topic #: 1

[All SPLK-3002 Questions]

Which of the following is a best practice for identifying the most effective services with which to start an iterative ITSI deployment?

A. Only include KPIs if they will be used in multiple services.

B. Analyze the business to determine the most critical services.

C. Focus on low-level services.

D. Define a large number of key services early.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 3

Topic #: 1

[All SPLK-3002 Questions]

When creating a custom deep dive, what color are services/KPIs in maintenance mode within the topology view?

A. Gray

B. Purple

C. Gear Icon

D. Blue

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 4

Topic #: 1

[All SPLK-3002 Questions]

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

A. Event lane.

B. Automatic lane.

C. Metric lane.

D. KPI lane.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 5

Topic #: 1

[All SPLK-3002 Questions]

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 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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 6

Topic #: 1

[All SPLK-3002 Questions]

Which of the following is a best practice when configuring maintenance windows?

A. Disable any glass tables that reference a KPI that is part of an open maintenance window.

B. Develop a strategy for configuring a service's notable event generation when the service's maintenance window is open.

C. Give the maintenance window a buffer, for example, 15 minutes before and after actual maintenance work.

D. Change the color of services and entities that are part of an open maintenance window in the service analyzer.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 7

Topic #: 1

[All SPLK-3002 Questions]

In Episode Review, what is the result of clicking an episode's Acknowledge button?

A. Assign the current user as owner.

B. Change status from New to Acknowledged.

C. Change status from New to In Progress and assign the current user as owner.

D. Change status from New to Acknowledged and assign the current user as owner.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 8

Topic #: 1

[All SPLK-3002 Questions]

Which glass table feature can be used to toggle displaying KPI values from more than one service on a single widget?

A. Service templates.

B. Service dependencies.

C. Ad-hoc search.

D. Service swapping.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 9

Topic #: 1

[All SPLK-3002 Questions]

Which of the following is a characteristic of base searches?

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 10

Topic #: 1

[All SPLK-3002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 11

Topic #: 1

[All SPLK-3002 Questions]

Which of the following is the best use case for configuring a Multi-KPI Alert?

A. Comparing content between two notable events.

B. Using machine learning to evaluate when data falls outside of an expected pattern.

C. Comparing anomaly detection between two KPIs.

D. Raising an alert when one or more KPIs indicate an outage is occurring.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 12

Topic #: 1

[All SPLK-3002 Questions]

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 idexers; SA-ITSI-Licensechecker and SA-UserAccess on the license master.

D. SA-ITSI-Licensechecker on indexers.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 13

Topic #: 1

[All SPLK-3002 Questions]

When deploying ITSI on a distributed Splunk installation, which component must be installed on the search head(s)?

A. SA-ITOA

B. ITSI app

C. All ITSI components

D. SA-ITSI-Licensechecker

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 14

Topic #: 1

[All SPLK-3002 Questions]

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

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”.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 15

Topic #: 1

[All SPLK-3002 Questions]

Which of the following describes a realistic troubleshooting workflow in ITSI?

A. Correlation Search –> Deep Dive –> Notable Event

B. Service Analyzer –> Notable Event Review –> Deep Dive

C. Service Analyzer –> Aggregation Policy –> Deep Dive

D. Correlation search –> KPI –> Aggregation Policy

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 16

Topic #: 1

[All SPLK-3002 Questions]

Which of the following accurately describes base searches used for KPIs in a service?

A. Base searches can be used for multiple services.

B. A base search can only be used by its service and all dependent services.

C. All the metrics in a base search are used by one service.

D. All the KPIs in a service use the same base search.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 17

Topic #: 1

[All SPLK-3002 Questions]

Which scenario would benefit most by implementing ITSI?

A. Monitoring of business services functionality.

B. Monitoring of system hardware.

C. Monitoring of system process statuses.

D. Monitoring of retail sales metrics.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 18

Topic #: 1

[All SPLK-3002 Questions]

ITSI Saved Search Scheduling is configured to use realtime_schedule = 0. Which statement is accurate about this configuration?

A. If this value is set to 0, the scheduler bases its determination of the next scheduled search execution time on the current time.

B. If this value is set to 0, the scheduler bases its determination of the next scheduled search on the last search execution time.

C. If this value is set to 0, the scheduler may skip scheduled execution periods.

D. If this value is set to 0, the scheduler might skip some execution periods to make sure that the scheduler is executing the searches running over the most recent time range.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 19

Topic #: 1

[All SPLK-3002 Questions]

What effects does the KPI importance weight of 11 have on the overall health score of a service?

A. At least 10% of the KPIs will go critical.

B. Importance weight is unused for health scoring.

C. The service will go critical.

D. It is a minimum health indicator KPI.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 20

Topic #: 1

[All SPLK-3002 Questions]

Which of the following is an advantage of using adaptive time thresholds?

A. Automatically update thresholds daily to manage dynamic changes to KPI values.

B. Automatically adjust KPI calculation to manage dynamic event data.

C. Automatically adjust aggregation policy grouping to manage escalating severity.

D. Automatically adjust correlation search thresholds to adjust sensitivity over time.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 21

Topic #: 1

[All SPLK-3002 Questions]

Which of the following applies when configuring time policies for KPI thresholds?

A. A person can only configure 24 policies, one for each hour of the day.

B. They are great if you expect normal behavior at 1:00 to be different than normal behavior at 5:00

C. If a person expects a KPI to change significantly through a cycle on a daily basis, don't use it.

D. It is possible for multiple time policies to overlap.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 22

Topic #: 1

[All SPLK-3002 Questions]

What is the main purpose of the service analyzer?

A. Display a list of All Services and Entities.

B. Trigger external alerts based on threshold violations.

C. Allow Analysts to add comments to Alerts.

D. Monitor overall Service and KPI status.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 23

Topic #: 1

[All SPLK-3002 Questions]

What is the default importance value for dependent services' health scores?

A. 11

B. 1

C. Unassigned

D. 10

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 24

Topic #: 1

[All SPLK-3002 Questions]

What should be considered when onboarding data into a Splunk index, assuming that ITSI will need to use this data?

A. Use | stats functions in custom fields to prepare the data for KPI calculations.

B. Check if the data could leverage pre-built KPIs from modules, then use the correct TA to onboard the data.

C. Make sure that all fields conform to CIM, then use the corresponding module to import related services.

D. Plan to build as many data models as possible for ITSI to leverage

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 25

Topic #: 1

[All SPLK-3002 Questions]

When changing a service template, which of the following will be added to linked services by default?

A. Thresholds.

B. Entity Rules.

C. New KPIs.

D. Health score.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 26

Topic #: 1

[All SPLK-3002 Questions]

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

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 27

Topic #: 1

[All SPLK-3002 Questions]

What is an episode?

A. A workflow task.

B. A deep dive.

C. A notable event group.

D. A notable event.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 28

Topic #: 1

[All SPLK-3002 Questions]

Which index will contain useful error messages when troubleshooting ITSI issues?

A. _introspection

B. _internal

C. itsi_summary

D. itsi_notable_audit

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 29

Topic #: 1

[All SPLK-3002 Questions]

Which of the following is a recommended best practice for service and glass table design?

A. Plan and implement services first, then build detailed glass tables.

B. Always use the standard icons for glass table widgets to improve portability.

C. Start with base searches, then services, and then glass tables.

D. Design glass tables first to discover which KPIs are important.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 30

Topic #: 1

[All SPLK-3002 Questions]

Which of the following are deployment recommendations for ITSI? (Choose all that apply.)

A. Deployments often require an increase of hardware resources above base Splunk requirements.

B. Deployments require a dedicated ITSI search head.

C. Deployments may increase the number of required indexers based on the number of KPI searches.

D. Deployments should use fastest possible disk arrays for indexers.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 31

Topic #: 1

[All SPLK-3002 Questions]

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.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 32

Topic #: 1

[All SPLK-3002 Questions]

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

A. KPI

B. Multi-KPI alert

C. Entity

D. Service

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 33

Topic #: 1

[All SPLK-3002 Questions]

Which index is used to store KPI values?

A. itsi_summary_metrics

B. itsi_metrics

C. itsi_service_health

D. itsi_summary

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 34

Topic #: 1

[All SPLK-3002 Questions]

Where are KPI search results stored?

A. The default index.

B. KV Store.

C. Output to a CSV lookup.

D. The itsi_summary index.

Show Suggested Answer

Actual exam question from Splunk's SPLK-3002

Question #: 35

Topic #: 1

[All SPLK-3002 Questions]

Which ITSI functions generate notable events? (Choose all that apply.)

A. KPI threshold breaches.

B. KPI anomaly detection.

C. Multi-KPI alert.

D. Correlation search.

Show Suggested Answer