Vendor: Splunk

Exam Code:SPLK-3002

Exam Name: Splunk IT Service Intelligence Certified Admin

Version: Demo

QUESTION 1

How do you automatically restrict a KPI to only the entities in its service, and generate KPI values for each entity?

A. Select “Yes” for both “Split by Entity” and “Filter to Entities in Service”.

B. Select “No” for “Split by Entity” and “Yes” for “Filter to Entities in Service”.

C. Select “Yes” for “Split by Entity” and “No” for “Filter to Entities in Service”.

D. Select “No” for both “Split by Entity” and “Filter to Entities in Service”.

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/BaseSearch

---

QUESTION 2

Which index is used to store KPI values?

A. itsi_summary_metrics

B. itsi_metrics

C. itsia_service_health

D. itsi_summary

Correct Answer: A

The IT Service Intelligence (ITSI) metrics summary index, itsi_summary_metrics, is a metrics-based summary index that stores KPI data.

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/MetricsIndexRef

---

QUESTION 3

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.

Correct Answer: BC

The KPI must be split by entity, and a minimum of four entities is required.

If the KPI diverges from the normal pattern, ITSI creates a notable event in Episode Review.

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

QUESTION 4

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.

Correct Answer: B

If set to 0, the scheduler determines the next scheduled search run time based on the last run time for the search. This is called continuous scheduling.

Reference: https://docs.splunk.com/Documentation/DFS/1.1.2/DFS/Savedsearchesconf

---

QUESTION 5

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.

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/BaseSearch

---

QUESTION 6

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.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/KPIImportance#:~:text=ITSI%20considers%20KPIs%20that%20have,other%20KPIs%20in%20the%20service

---

QUESTION 7

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.

Correct Answer: C

Alerts and Sharing Reference: https://docs.splunk.com/Documentation/MSExchange/4.0.3/Reference/ServiceAnalyzer

---

QUESTION 8

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.

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/MKA

QUESTION 9

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.

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/AboutSI

QUESTION 10

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”.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/KPIfilter

---

QUESTION 11

In maintenance mode, which features of KPIs still function?

A. KPI searches will execute but will be buffered until the maintenance window is over.

B. KPI searches still run during maintenance mode, but results go to itsi_maintenance_summaryindex.

C. New KPIs can be created, but existing KPIs are locked.

D. KPI calculations and threshold settings can be modified.

Correct Answer: A

It\\'s a best practice to schedule maintenance windows with a 15- to 30-minute time buffer before and after you start and stop your maintenance work. This gives the system an opportunity to catch up with the maintenance state and reduces the chances of ITSI generating false positives during maintenance operations.

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/AboutMW

QUESTION 12

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

Correct Answer: A

Services, entities, and KPIs that are fully or partially impacted by a maintenance window appear in a dark gray color on pages that display health scores, including service analyzers, service and entity details pages, glass tables, multi-KPI alerts, and deep dives.

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/AboutMW