EndExam

QUESTION & ANSWER

Accurate study guides, High passing rate!

We offer free update service for one year!

http://www.endexam.com

Exam : **SPLK-3002**

Title : Splunk IT Service Intelligence Certified Admin Exam

Version : DEMO

1.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.
Answer: A
Explanation:
By default, notable event metadata is archived after six months to keep the KV store from growing too large.
Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/EA/TrimNECollections

2.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.
Answer: B
Explanation:
Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/MKA
A best practice for identifying the most effective services with which to start an iterative ITSI deployment is to analyze the business to determine the most critical services that have the most impact on revenue, customer satisfaction, or other key performance indicators. You can use the Service Analyzer to prioritize and monitor these services.
Reference: Service Analyzer

3.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
Answer: A
Explanation:
When creating a custom deep dive, services or KPIs that are in maintenance mode are shown in gray color in the topology view. This indicates that they are not actively monitored and do not generate alerts or notable events.
Reference: Deep Dives

4.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.
Reference: [KPI Lanes]

5.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.
Answer: B, C
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.
Reference: [Anomaly Detection]