Splunk

SPLK-3002 Exam

Splunk IT Service Intelligence Certified Admin

Questions & Answers
Demo

Version: 4.0

Question: 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

Question: 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: A

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

Question: 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:
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

Question: 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: B

Explanation:
Among all the search configurations, automatic lane doesn't need to be written in Splunk Processing language.

Question: 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

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