



SPLK-3002^{Q&As}

Splunk IT Service Intelligence Certified Admin

Pass Splunk SPLK-3002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/splk-3002.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

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 2

Which of the following is a good use case regarding defining entities for a service?

- A. Automatically associate entities to services using multiple entity aliases.
- B. All of the entities have the same identifying field name.
- C. Being able to split a CPU usage KPI by host name.
- D. KPI total values are aggregated from multiple different category values in the source events.

Correct Answer: A

Define entities before creating services. When you configure a service, you can specify entity matching rules based on entity aliases that automatically add the entities to your service.

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/Entity/About>

QUESTION 3

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.

Correct Answer: C

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.

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

QUESTION 4

What is an episode?

- A. A workflow task.
- B. A deep dive.
- C. A notable event group.
- D. A notable event.

Correct Answer: D

It's a deduplicated group of notable events occurring as part of a larger sequence, or an incident or period considered in isolation.

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/EA/EpisodeOverview>

QUESTION 5

Which index contains ITSI Episodes?

- A. itsi_tracked_alerts
- B. itsi_grouped_alerts
- C. itsi_notable_archive
- D. itsi_summary

Correct Answer: C

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/IndexOverview>

[SPLK-3002 VCE Dumps](#)

[SPLK-3002 Exam
Questions](#)

[SPLK-3002 Braindumps](#)