# Pass2Lead
https://Pass2Lead.com

# SPLK-3002<sup>Q&As</sup>

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.pass2lead.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**

Besides creating notable events, what are the default alert actions a correlation search can execute? (Choose all that apply.)

A. Ping a host.

B. Send email.

C. Include in RSS feed.

D. Run a script.

Correct Answer: BCD

Throttling applies to any correlation search alert type, including notable events and actions (RSS feed, email, run script, and ticketing).

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/EA/ConfigCS

**QUESTION 3**

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 4**

Within a correlation search, dynamic field values can be specified with what syntax?

A. fieldname

B.

C. %fieldname% D. eval(fieldname)

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/8.2.2/Search/Searchindexes

**QUESTION 5**

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.

Correct Answer: ABC

You might need to increase the hardware specifications of your own Enterprise Security deployment above

the minimum hardware requirements depending on your environment.

Install Splunk Enterprise Security on a dedicated search head or search head cluster.

The Splunk platform uses indexers to scale horizontally. The number of indexers required in an Enterprise

Security deployment varies based on the data volume, data type, retention requirements, search type, and

search concurrency.

Reference: https://docs.splunk.com/Documentation/ES/latest/Install/DeploymentPlanning

SPLK-3002 Study Guide

SPLK-3002 Exam Questions

SPLK-3002 Braindumps