



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.geekcert.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

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 2

In distributed search, which components need to be installed on instances other than the search head?

- A. SA-IndexCreation and SA-ITSI-Licensechecker on indexers.
- B. SA-IndexCreation and SA-ITOA on indexers; SA-ITSI-Licensechecker and SA-UserAccess on the license master.
- C. SA-IndexCreation on indexers; SA-ITSI-Licensechecker and SA-UserAccess on the license master.
- D. SA-ITSI-Licensechecker on indexers.

Correct Answer: A

SA-IndexCreation is required on all indexers. For non-clustered, distributed environments, copy SA-IndexCreation to \$SPLUNK_HOME/etc/apps/ on individual indexers.

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/Install/InstallIDD>

QUESTION 3

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 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 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>

[SPLK-3002 PDF Dumps](#)

[SPLK-3002 Practice Test](#)

[SPLK-3002 Study Guide](#)