



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

When in maintenance mode, which of the following is accurate?

- A. Once the window is over, KPIs and notable events will begin to be generated again.
- B. KPIs are shown in blue while in maintenance mode.
- C. Maintenance mode slots are scheduled on a per hour basis.
- D. Service health scores and KPI events are deleted until the window is over.

Correct Answer: A

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

QUESTION 3

In maintenance mode, which features of KPIs still function?

- A. KPI searches will execute but will be buffered until the maintenance window is over.
- B. KPI searches still run during maintenance mode, but results go to itsi_maintenance_summaryindex.
- C. New KPIs can be created, but existing KPIs are locked.
- D. KPI calculations and threshold settings can be modified.

Correct Answer: A

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. This gives the system an opportunity to catch up with the maintenance state and reduces the chances of ITSI generating false positives during maintenance operations.



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

QUESTION 4

When deploying ITSI on a distributed Splunk installation, which component must be installed on the search head(s)?

- A. SA-ITOA
- B. ITSI app
- C. All ITSI components
- D. SA-ITSI-Licensechecker

Correct Answer: D

Install SA-ITSI-Licensechecker and SA-UserAccess on any license master in a distributed or search head cluster environment. If a search head in your environment is also a license master, the license master components are installed when you install ITSI on the search heads.

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

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>