



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

When changing a service template, which of the following will be added to linked services by default?

- A. Thresholds.
- B. Entity Rules.
- C. New KPIs.
- D. Health score.

Correct Answer: B

Link multiple services to a service template to manage them collectively in IT Service Intelligence (ITSI). A service can only be linked to one service template at a time. When you link a service to a service template, any existing KPIs in the service are preserved and KPIs in the template are added to the service. You can choose to append, replace, or keep entity rules.

Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/LinkST>

QUESTION 2

What are valid considerations when designing an ITSI Service? (Choose all that apply.)

- A. Service access control requirements for ITSI Team Access should be considered, and appropriate teams provisioned prior to creating the ITSI Service.
- B. Entities, entity meta-data, and entity rules should be planned carefully to support the service design and configuration.
- C. Services, entities, and saved searches are stored in the ITSI app, while events created by KPI execution are stored in the itsi_summaryindex.
- D. Backfill of a KPI should always be selected so historical data points can be used immediately and alerts based on that data can occur.

Correct Answer: AC

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

QUESTION 3

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>

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

When installing ITSI to support a Distributed Search Architecture, which of the following items apply? (Choose all that apply.)

- A. Copy SA-IndexCreation to all indexers.
- B. Copy SA-IndexCreation to the etc/apps directory on the index cluster master node.
- C. Extract installer package into etc/apps directory of the cluster deployer node.
- D. Extract ITSI app package into etc/apps directory of search head.

Correct Answer: A

Copy SA-IndexCreation to \$SPLUNK_HOME/etc/apps/ on all individual indexers in your environment. Reference: <https://docs.splunk.com/Documentation/ITSI/4.10.2/Install/InstallSHC>



VCE & PDF

GeekCert.com

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

2024 Latest geekcert SPLK-3002 PDF and VCE dumps Download

[Questions](#)