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.leads4pass.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

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 2

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

A. SA-IndexCreationand SA-ITSI-Licensecheckeron indexers.

B. SA-IndexCreationand SA-ITOA on indexers; SA-ITSI-Licensecheckerand SA-UserAccess on the license master.

C. SA-IndexCreationon idexers; SA-ITSI-Licensecheckerand SA-UserAccesson the license master.

D. SA-ITSI-Licensecheckeron 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/InstallDD

QUESTION 3

Which scenario would benefit most by implementing ITSI?

A. Monitoring of business services functionality.

B. Monitoring of system hardware.

C. Monitoring of system process statuses.

D. Monitoring of retail sales metrics.

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/AboutSI

QUESTION 4

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 5

Which of the following are the default ports that must be configured on Splunk to use ITSI?

A. SplunkWeb (8405), SplunkD (8519), and HTTP Collector (8628)

B. SplunkWeb (8089), SplunkD (8088), and HTTP Collector (8000)

C. SplunkWeb (8000), SplunkD (8089), and HTTP Collector (8088)

D. SplunkWeb (8088), SplunkD (8089), and HTTP Collector (8000)

Correct Answer: C

Reference: https://splunk.github.io/docker-splunk/ARCHITECTURE.html

QUESTION 6

Anomaly detection can be enabled on which one of the following?

A. KPI

B. Multi-KPI alert

C. Entity

D. Service

Correct Answer: A

Enable anomaly detection to identify trends and outliers in KPI search results that might indicate an issue with your system.

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/AD

QUESTION 7

For which ITSI function is it a best practice to use a 15-30 minute time buffer?

A. Correlation searches.

B. Adaptive thresholding.

C. Maintenance windows

D. Anomaly detection.

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. 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 8

How do you automatically restrict a KPI to only the entities in its service, and generate KPI values for each entity?

A. Select “Yes” for both “Split by Entity” and “Filter to Entities in Service”.

B. Select “No” for “Split by Entity” and “Yes” for “Filter to Entities in Service”.

C. Select “Yes” for “Split by Entity” and “No” for “Filter to Entities in Service”.

D. Select “No” for both “Split by Entity” and “Filter to Entities in Service”.

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/BaseSearch

QUESTION 9

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 10

What effects does the KPI importance weight of 11 have on the overall health score of a service?

A. At least 10% of the KPIs will go critical.

B. Importance weight is unused for health scoring.

C. The service will go critical.

D. It is a minimum health indicator KPI.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/SI/KPIImportance#:~:text=ITSI%20considers%20KPIs%20that%20have,other%20KPIs%20in%20the%20service