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.pass4itsure.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 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 2

Which of the following is the best use case for configuring a Multi-KPI Alert?

A. Comparing content between two notable events.

B. Using machine learning to evaluate when data falls outside of an expected pattern.

C. Comparing anomaly detection between two KPIs.

D. Raising an alert when one or more KPIs indicate an outage is occurring.

Correct Answer: A

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

QUESTION 3

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 4

Which of the following is an advantage of using adaptive time thresholds?

A. Automatically update thresholds daily to manage dynamic changes to KPI values.

B. Automatically adjust KPI calculation to manage dynamic event data.

C. Automatically adjust aggregation policy grouping to manage escalating severity.

D. Automatically adjust correlation search thresholds to adjust sensitivity over time.

Correct Answer: A

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

QUESTION 5

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