SPLK-3002Q&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.pass2lead.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 capabilities are enabled through “teams”?

A. Teams allow searches against the itsi_summaryindex.

B. Teams restrict notable event alert actions.

C. Teams restrict searches against the itsi_notable_auditindex.

D. Teams allow restrictions to service content in UI views.

Correct Answer: A

Teams provide presentation-layer security only and not data-level security. It\\'s still possible for a user with access to the Splunk search bar to look up ITSI summary index data.

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/ServicePerms

QUESTION 2

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 3

Which index will contain useful error messages when troubleshooting ITSI issues?

A. _introspection

B. _internal

C. itsi_summary

D. itsi_notable_audit

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/EA/TroubleshootRE

QUESTION 4

Which of the following items describe ITSI Deep Dive capabilities? (Choose all that apply.)

A. Comparing a service\\'s notable events over a time period.

B. Visualizing one or more Service KPIs values by time.

C. Examining and comparing alert levels for KPIs in a service over time.

D. Comparing swim lane values for a slice of time.

Correct Answer: BCD

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

QUESTION 5

When creating a custom deep dive, what color are services/KPIs in maintenance mode within the topology view?

A. Gray

B. Purple

C. Gear Icon

D. Blue

Correct Answer: A

Services, entities, and KPIs that are fully or partially impacted by a maintenance window appear in a dark gray color on pages that display health scores, including service analyzers, service and entity details pages, glass tables, multi-KPI alerts, and deep dives.

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

QUESTION 6

Which of the following is a good use case regarding defining entities for a service?

A. Automatically associate entities to services using multiple entity aliases.

B. All of the entities have the same identifying field name.

C. Being able to split a CPU usage KPI by host name.

D. KPI total values are aggregated from multiple different category values in the source events.

Correct Answer: A

Define entities before creating services. When you configure a service, you can specify entity matching rules based on

entity aliases that automatically add the entities to your service.

Reference: https://docs.splunk.com/Documentation/ITSI/4.10.2/Entity/About

QUESTION 7

Which of the following is a best practice when configuring maintenance windows?

A. Disable any glass tables that reference a KPI that is part of an open maintenance window.

B. Develop a strategy for configuring a service\\'s notable event generation when the service\\'s maintenance window is open.

C. Give the maintenance window a buffer, for example, 15 minutes before and after actual maintenance work.

D. Change the color of services and entities that are part of an open maintenance window in the service analyzer.

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.

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

QUESTION 8

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

A. Copy SA-IndexCreationto all indexers.

B. Copy SA-IndexCreationto 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

QUESTION 9

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 10

Which of the following applies when configuring time policies for KPI thresholds?

A. A person can only configure 24 policies, one for each hour of the day.

B. They are great if you expect normal behavior at 1:00 to be different than normal behavior at 5:00

C. If a person expects a KPI to change significantly through a cycle on a daily basis, don\\'t use it.

D. It is possible for multiple time policies to overlap.

Correct Answer: D

If you\\'re creating multiple time policies that require the same threshold values, you can save time by copying the threshold levels and their corresponding values from one policy to another

Reference: https://docs.splunk.com/Documentation/ITSI/4.9.1/SI/TimePolicies