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.passapply.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 index contains ITSI Episodes?

A. itsi_tracked_alerts

B. itsi_grouped_alerts

C. itsi_notable_archive

D. itsi_summary

Correct Answer: C

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

QUESTION 2

Which of the following is a best practice for identifying the most effective services with which to start an iterative ITSI deployment?

A. Only include KPIs if they will be used in multiple services.

B. Analyze the business to determine the most critical services.

C. Focus on low-level services.

D. Define a large number of key services early.

Correct Answer: A

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

QUESTION 3

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 4

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 5

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