

SPLK-3002 Valid Test Answers & Real SPLK-3002 Exam Questions

Splunk SPLK-3002 Practice Questions

Splunk IT Service Intelligence Certified Admin Exam

Order our SPLK-3002 Practice Questions Today and Get Ready to Pass with Flying Colors!



SPLK-3002 Practice Exam Features | QuestionsTube

- Latest & Updated Exam Questions
- Subscribe to FREE Updates
- Both PDF & Exam Engine
- Download Directly Without Waiting

<https://www.questionstube.com/exam/splk-3002/>

At QuestionsTube, you can read SPLK-3002 free demo questions in pdf file, so you can check the questions and answers before deciding to download the Splunk SPLK-3002 practice questions. These free demo questions are parts of the SPLK-3002 exam questions. Download and read them carefully, you will find that the SPLK-3002 test questions of QuestionsTube will be your great learning materials online. Share some SPLK-3002 exam online questions below.

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

DOWNLOAD the newest ValidExam SPLK-3002 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1HcTS7pn7Hs9bk2AlwLN_3vVxjBEfktE

What is your reason for wanting to be certified with SPLK-3002? I believe you must want to get more opportunities. As long as you use SPLK-3002 learning materials and get a SPLK-3002 certificate, you will certainly be appreciated by the leaders. As you can imagine that you can get a promotion sooner or latter, not only on the salary but also on the position, so what are you waiting for? Just come and buy our SPLK-3002 study braindumps.

Splunk SPLK-3002 Certification Exam is a challenging and comprehensive exam that is designed to test the knowledge and skills of IT professionals in using Splunk IT Service Intelligence (ITSI) to manage and monitor their IT environments. Splunk ITSI is a powerful platform that provides real-time visibility and insights into IT operations, allowing organizations to quickly identify and resolve issues before they impact business operations.

>> SPLK-3002 Valid Test Answers <<

Free PDF SPLK-3002 - High-quality Splunk IT Service Intelligence Certified Admin Valid Test Answers

We prepare everything you need to prepare, and help you pass the exam easily. The SPLK-3002 exam braindumps of us have the

significant information for the exam, if you use it, you will learn the basic knowledge as well as some ways. We offer free update for you, and you will get the latest version timely, and you just need to practice the SPLK-3002 Exam Dumps. We believe that with the joint efforts of both us, you will gain a satisfactory result.

Splunk SPLK-3002 exam is intended for IT professionals who are responsible for monitoring and managing IT services in their organization. This includes IT managers, system administrators, network engineers, security analysts, and other IT professionals who are involved in the management of IT services. Splunk IT Service Intelligence Certified Admin certification provides a credential that validates the candidate's knowledge and skills in using Splunk ITSI to monitor and manage IT services.

Splunk SPLK-3002 Certification Exam is ideal for IT professionals who are responsible for managing and administering ITSI solutions in their organization. This includes IT administrators, system administrators, and IT operations professionals. Splunk IT Service Intelligence Certified Admin certification is also useful for professionals who are looking to enhance their careers in the field of IT service management and monitoring.

Splunk IT Service Intelligence Certified Admin Sample Questions (Q62-Q67):

NEW QUESTION # 62

Which of the following are deployment recommendations for ITSI? (Choose all that apply.)

- A. Deployments should use fastest possible disk arrays for indexers.
- B. Deployments often require an increase of hardware resources above base Splunk requirements.
- C. Deployments require a dedicated ITSI search head.
- D. Deployments may increase the number of required indexers based on the number of KPI searches.

Answer: B,C,D

Explanation:

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:

A, B, and C are correct answers because ITSI deployments often require more hardware resources than base Splunk requirements due to the high volume of data ingestion and processing. ITSI deployments also require a dedicated search head that runs the ITSI app and handles all ITSI-related searches and dashboards. ITSI deployments may also increase the number of required indexers based on the number and frequency of KPI searches, which can generate a large amount of summary data. Reference: ITSI deployment overview, ITSI deployment planning

NEW QUESTION # 63

Which of the following describes a way to delete multiple duplicate entities in ITSI?

- A. Via a CSV upload.
- B. Via the entity lister page.
- C. Via a search using the `| deleteentity` command.
- D. All of the above.

Answer: D

Explanation:

D is the correct answer because ITSI provides multiple ways to delete multiple duplicate entities. You can use a CSV upload to overwrite existing entities with new or updated information, or delete them by setting the action field to delete. You can also use the entity lister page to select multiple entities and delete them in bulk.

Alternatively, you can use a search command called `| deleteentity` to delete entities that match certain criteria.

References: Create and update entities using a CSV file in ITSI, Delete entities in bulk in ITSI, Delete entities using the `| deleteentity` command in ITSI

NEW QUESTION # 64

Fritz is looking at a Deep Dive with a lane showing the average percent of CPU usage across the four web servers in the web farm.

Seeing a spike, he wants to add the graphs of each server on the swim lane, and selects the Lane Overlay Options to do so. No entity overlays are available for the KPI.

What is wrong with his KPI configuration?

- A. He configured the service with only three entities.
- B. He did not enable entity filtering.
- **C. He did not split the KPI by entity.**
- D. He configured the KPI to split by pseudo#entity.

Answer: C

Explanation:

In Splunk ITSI, swim lane overlays depend on a KPI being split by entity so that each entity's individual time series can be displayed separately in the Deep Dive view. When a KPI is aggregated without an entity split, it produces a single time series value at each timestamp representing the entire group (in this case, the average CPU across all web servers). Because that KPI does not contain per#entity values, ITSI has nothing to overlay

- therefore no entity overlays appear in the Lane Overlay Options. This configuration mistake often happens when a KPI is defined to average values across sources without specifying an entity dimension on which to split results. Entity filtering is a separate feature that enables restricting which entities are considered in display or analytics and does not control availability of swim lane overlays; pseudo#entities are artificial names that do not reflect actual system identities and are not relevant to this error; and having only three entities versus four would not prevent overlays from appearing if the KPI were correctly split by entity. The correct fix is to edit the KPI definition and configure it to split the metric results by the server entity field, such that each server has its own time series. This then enables Fritz to overlay the individual server CPU graphs on the swim lane as intended.

NEW QUESTION # 65

Which of the following items apply to anomaly detection? (Choose all that apply.)

- A. There are 3 types of anomaly detection supported in ITSI: adhoc, trending, and cohesive.
- B. Use AD on KPIs that have an unestablished baseline of data points. This allows the ML pattern to perform its magic.
- **C. A minimum of 24 hours of data is needed for anomaly detection, and a minimum of 4 entities for cohesive analysis.**
- **D. Anomaly detection automatically generates notable events when KPI data diverges from the pattern.**

Answer: C,D

Explanation:

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

Anomaly detection is a feature of ITSI that uses machine learning to detect when KPI data deviates from a normal pattern. The following items apply to anomaly detection:

B). A minimum of 24 hours of data is needed for anomaly detection, and a minimum of 4 entities for cohesive analysis. This ensures that there is enough data to establish a baseline pattern and compare different entities within a service.

C). Anomaly detection automatically generates notable events when KPI data diverges from the pattern. You can configure the sensitivity and severity of the anomaly detection alerts and assign them to episodes or teams. References: [Anomaly Detection]

NEW QUESTION # 66

Which of the following statements describe default glass tables in ITSI?

- A. The Service Health Score default glass table.
- **B. There are no default glass tables.**
- C. There is one default glass table per service.
- D. There is one service template default glass table.

Answer: B

Explanation:

In Splunk IT Service Intelligence (ITSI), glass tables are fully customizable dashboards that provide a visual representation of an organization's IT environment, along with the health and status of services and KPIs.

Unlike some pre-configured views or dashboards that might come with default setups in various platforms, ITSI does not provide default glass tables out of the box. Instead, users are encouraged to create their own glass tables tailored to their specific monitoring needs and operational views. This approach ensures that each organization can design glass tables that best represent their unique

- DOWNLOAD the newest ValidExam SPLK-3002 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1HcTS7pn7Hs9bk2AlwLN_3vVxjBEfkItE