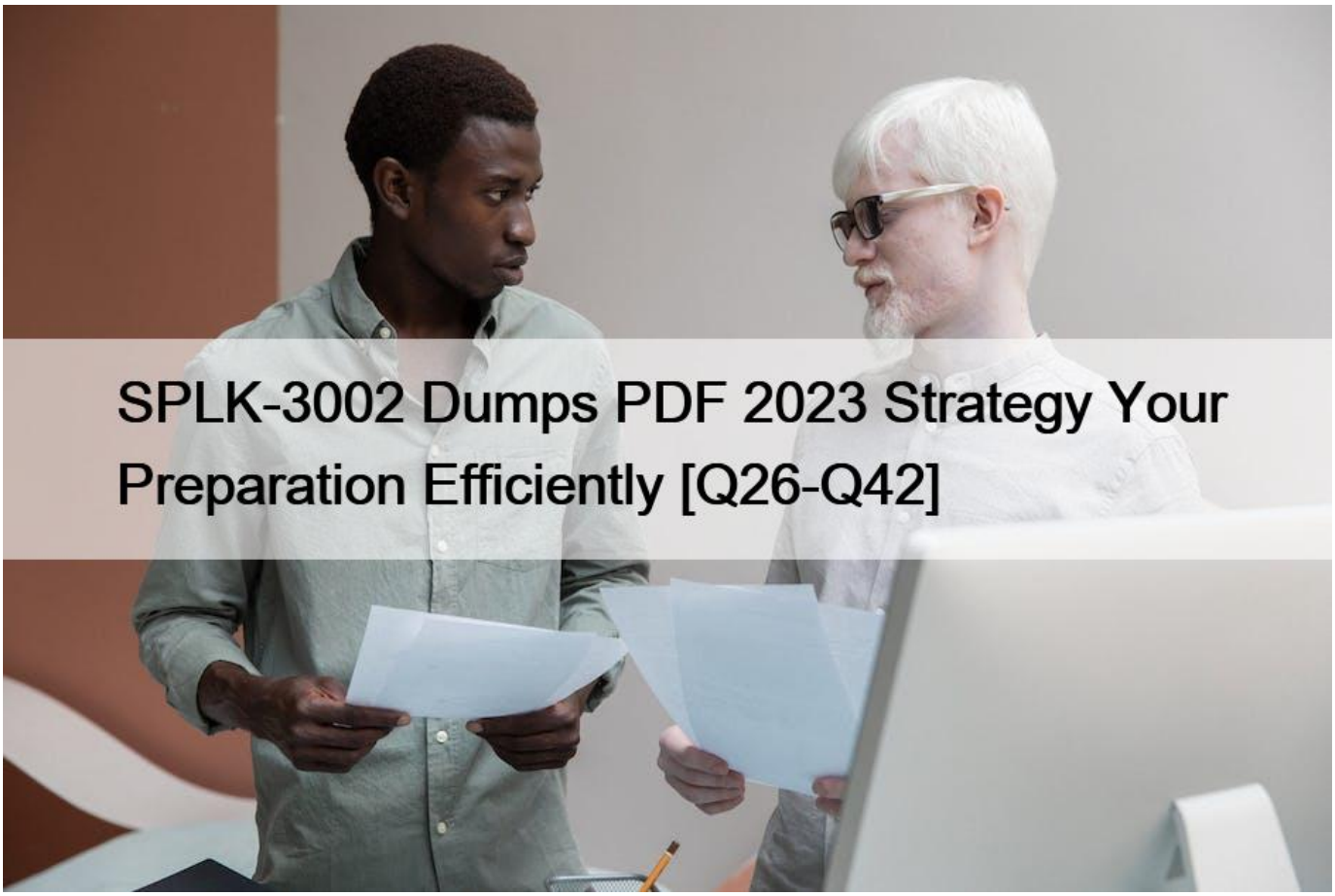
SPLK-3002 Dumps PDF 2023 Strategy Your Preparation Efficiently [Q26-Q42



SPLK-3002 Dumps PDF 2023 Strategy Your Preparation Efficiently
Latest Verified & Correct Splunk SPLK-3002 Questions

NEW QUESTION 26

How do you automatically restrict a KPI to only the entities in its service, and generate KPI values for each entity?
* Select “Yes” for both “Split by Entity” and “Filter to Entities in Service”.
* Select “No” for “Split by Entity” and “Yes” for “Filter to Entities in Service”.
* Select “Yes” for “Split by Entity” and “No” for “Filter to Entities in Service”.
* Select “No” for both “Split by Entity” and “Filter to Entities in Service”.
Reference:

A is the correct answer because selecting “Yes” for both “Split by Entity” and “Filter to Entities in Service” allows you to automatically restrict a KPI to only the entities in its service and generate KPI values for each entity. Split by Entity splits the KPI search results by entity alias fields and calculates a separate KPI value for each entity. Filter to Entities in Service filters out any entities that are not part of the service from the KPI search results. This way, you can

ensure that your KPI reflects only the relevant entities for your service and provides granular information for each entity. Reference: [Configure KPI settings in ITSI]

NEW QUESTION 27

What is the default importance value for dependent services’ health scores?
* 11
* 1
* Unassigned
* 10
Explanation

By default, impacting service health scores have an importance value of 11.

NEW QUESTION 28

How do you automatically restrict a KPI to only the entities in its service, and generate KPI values for each entity?
* Select “Yes” for both “Split by Entity” and “Filter to Entities in Service”.
* Select “No” for “Split by Entity” and “Yes” for “Filter to Entities in Service”.
* Select “Yes” for “Split by Entity” and “No” for “Filter to Entities in Service”.
* Select “No” for both “Split by Entity” and “Filter to Entities in Service”.

NEW QUESTION 29

In distributed search, which components need to be installed on instances other than the search head?
* SA-IndexCreation and SA-ITSI-Licensechecker on indexers.
* SA-IndexCreation and SA-ITOA on indexers; SA-ITSI-Licensechecker and SA-UserAccess on the license master.
* SA-IndexCreation on idexers; SA-ITSI-Licensechecker and SA-UserAccess on the license master.
* SA-ITSI-Licensechecker on indexers.
SA-IndexCreation is required on all indexers. For non-clustered, distributed environments, copy SA-IndexCreation to $SPLUNK_HOME/etc/apps/ on individual indexers.

Reference:

In distributed search, the components that need to be installed on instances other than the search head are SA-IndexCreation and SA-ITSI-Licensechecker on indexers. SA-IndexCreation is an add-on that creates the indexes required by ITSI, such as itsi_summary and itsi_tracked_alerts. SA-ITSI-Licensechecker is an add-on that monitors the license usage of ITSI and generates alerts when the license limit is exceeded or about to expire. These components need to be installed on indexers because they handle the data ingestion and storage functions for ITSI. The other components, such as ITSI app and SA-ITOA, need to be installed on the search head(s) because they handle the search management and presentation functions for ITSI. Reference: Install IT Service Intelligence in a distributed environment

NEW QUESTION 30

When installing ITSI to support a Distributed Search Architecture, which of the following items apply?

(Choose all that apply.)
* Copy SA-IndexCreation to all indexers.

* Copy SA-IndexCreation to the etc/apps directory on the index cluster master node.
* Extract installer package into etc/apps directory of the cluster deployer node.
* Extract ITSI app package into etc/apps directory of search head.

Explanation

Copy SA-IndexCreation to $SPLUNK_HOME/etc/apps/ on all individual indexers in your environment.

NEW QUESTION 31

Which of the following is a best practice for identifying the most effective services with which to start an iterative ITSI deployment?
* Only include KPIs if they will be used in multiple services.
* Analyze the business to determine the most critical services.
* Focus on low-level services.
* Define a large number of key services early.

Reference:

A best practice for identifying the most effective services with which to start an iterative ITSI deployment is to analyze the business to determine the most critical services that have the most impact on revenue, customer satisfaction, or other key performance indicators. You can use the Service Analyzer to prioritize and monitor these services. Reference: Service Analyzer

NEW QUESTION 32

What effects does the KPI importance weight of 11 have on the overall health score of a service?
* At least 10% of the KPIs will go critical.
* Importance weight is unused for health scoring.
* The service will go critical.
* It is a minimum health indicator KPI.

Reference:

The KPI importance weight is a value that indicates how much a KPI contributes to the overall health score of a service. The importance weight can range from 1 (lowest) to 10 (highest). The statement that applies when configuring a KPI importance weight of 11 is:

B) Importance weight is unused for health scoring. This is true because an importance weight of 11 is invalid and cannot be used for health scoring. The maximum value for importance weight is 10.

The other statements do not apply because:

A) At least 10% of the KPIs will go critical. This is not true because an importance weight of 11 does not affect the severity level of any KPIs.

C) The service will go critical. This is not true because an importance weight of 11 does not affect the health score or status of any service.

D) It is a minimum health indicator KPI. This is not true because an importance weight of 11 does not indicate anything about the minimum health level of a KPI.

NEW QUESTION 33

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

* Comparing a service’s notable events over a time period.
* Visualizing one or more Service KPIs values by time.
* Examining and comparing alert levels for KPIs in a service over time.
* Comparing swim lane values for a slice of time.

NEW QUESTION 34

What is an episode?
* A workflow task.
* A deep dive.
* A notable event group.
* A notable event.

Explanation

It’s a deduplicated group of notable events occurring as part of a larger sequence, or an incident or period considered in isolation.

NEW QUESTION 35

Which of the following is the best use case for configuring a Multi-KPI Alert?
* Comparing content between two notable events.
* Using machine learning to evaluate when data falls outside of an expected pattern.
* Comparing anomaly detection between two KPIs.
* Raising an alert when one or more KPIs indicate an outage is occurring.

Reference:

A multi-KPI alert is a type of correlation search that is based on defined trigger conditions for two or more KPIs. When trigger conditions occur simultaneously for each KPI, the search generates a notable event. For example, you might create a multi-KPI alert based on two common KPIs: CPU load percent and web requests. A sudden simultaneous spike in both CPU load percent and web request KPIs might indicate a DDOS (Distributed Denial of Service) attack. Multi-KPI alerts can bring such trending behaviors to your attention early, so that you can take action to minimize any impact on performance. Multi-KPI alerts are useful for correlating the status of multiple KPIs across multiple services. They help you identify causal relationships, investigate root cause, and provide insights into behaviors across your infrastructure. The best use case for configuring a multi-KPI alert is to raise an alert when one or more KPIs indicate an outage is occurring, such as when the service health score drops below a certain threshold or when multiple KPIs have critical severity levels. Reference: Create multi-KPI alerts in ITSI

NEW QUESTION 36

Which index is used to store KPI values?
* itsi_summary_metrics
* itsi_metrics
* itsi_service_health
* itsi_summary

The IT Service Intelligence (ITSI) metrics summary index, itsi_summary_metrics, is a metrics-based summary index that stores KPI data.

Reference:

A is the correct answer because the itsi_summary_metrics index is used to store KPI values in ITSI. This index improves the performance of the searches dispatched by ITSI, particularly for very large environments. Every KPI is summarized in both the

itsi_summary events index and the itsi_summary_metrics metrics index. Reference: Overview of ITSI indexes

NEW QUESTION 37

There are two departments using ITSI. Finance and Sales. Analysts in each department should not be allowed to see each other’s services. What are the role configuration steps required to accomplish this?
* itoa_finance_admin, inherited from itoa_admin; itoa_sales_admin, inherited from itoa_team_admin; itoa_finance_analyst, inherited from itoa_analyst; itoa_sales_analyst, inherited from itoa_analyst.
* itoa_finance_admin, inherited from itoa_admin; itoa_sales_admin, inherited from itoa_team_admin; itoa_finance_analyst, inherited from itoa_team_analyst; itoa_sales_analyst, inherited from itoa_team_analyst.
* itoa_finance_admin, inherited from itoa_admin; itoa_sales_admin, inherited from itoa_team_admin; itoa_finance_analyst, inherited from itoa_analyst; itoa_sales_analyst, inherited from itoa_team_analyst.
* itoa_finance_admin, inherited from itoa_team_admin; itoa_sales_admin, inherited from itoa_team_admin; itoa_finance_analyst, inherited from itoa_analyst; itoa_sales_analyst, inherited from itoa_analyst.
C is the correct answer because teams are a feature of ITSI that allow you to restrict access to service content in UI views based on user roles. To create separate teams for finance and sales analysts, you need to create custom roles that inherit from the itoa_analyst role, which has read-only access to ITSI content. For example, you can create itoa_finance_analyst and itoa_sales_analyst roles that inherit from itoa_analyst. Then, you need to create custom teams that include these roles and assign them to the relevant services. For example, you can create a finance team that includes the itoa_finance_analyst role and assign it to the finance services. Similarly, you can create a sales team that includes the itoa_sales_analyst role and assign it to the sales services. This way, analysts in each department can only see their own services and not each other’s. Reference: Create teams in ITSI, Assign teams to services in ITSI

NEW QUESTION 38

Which scenario would benefit most by implementing ITSI?
* Monitoring of business services functionality.
* Monitoring of system hardware.
* Monitoring of system process statuses
* Monitoring of retail sales metrics.

NEW QUESTION 39

Which of the following items describe ITSI Backup and Restore functionality? (Choose all that apply.)
* A pre-configured default ITSI backup job is provided that can be modified, but not deleted.
* ITSI backup is inclusive of KV Store, ITSI Configurations, and index dependencies.
* kvstore_to_json.py can be used in scripts or command line to backup ITSI for full or partial backups.
* ITSI backups are stored as a collection of JSON formatted files.
Explanation

ITSI provides a kvstore_to_json.py script that lets you backup/restore ITSI configuration data, perform bulk service KPI operations, apply time zone offsets for ITSI objects, and regenerate KPI search schedules.

When you run a backup job, ITSI saves your data to a set of JSON files compressed into a single ZIP file.

NEW QUESTION 40

When deploying ITSI on a distributed Splunk installation, which component must be installed on the search head(s)?
* SA-ITOA
* ITSI app

* All ITSI components
* SA-ITSI-Licensechecker

Install SA-ITSI-Licensechecker and SA-UserAccess on any license master in a distributed or search head cluster environment. If a search head in your environment is also a license master, the license master components are installed when you install ITSI on the search heads.

Reference:

When deploying ITSI on a distributed Splunk installation, the component that must be installed on the search head(s) is the ITSI app. The ITSI app contains the main features and functionality of ITSI, such as service creation and management, KPI configuration, glass table creation and editing, episode review, deep dives, and so on. The ITSI app also contains some add-ons that provide additional functionality, such as SA-ITOA (IT Operations Analytics), SA-UserAccess (User Access Management), and SA-Utils (Utility Functions). The ITSI app must be installed on the search head(s) because it handles the search management and presentation functions for ITSI. Reference: Install IT Service Intelligence in a distributed environment

NEW QUESTION 41

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

* _introspection
* _internal
* itsi_summary
* itsi_notable_audit

NEW QUESTION 42

Which of the following is a characteristic of base searches?

* Search expression, entity splitting rules, and thresholds are configured at the base search level.
* It is possible to filter to entities assigned to the service for calculating the metrics for the service’s KPIs.
* The fewer KPIs that share a common base search, the more efficiency a base search provides, and anomaly detection is more efficient.
* The base search will execute whether or not a KPI needs it.

Certification Topics of Splunk SPLK-3002 Exam

Our **SPLK-3002 Dumps** covers the following objectives of Splunk SPLK-3002 Exam

- Data Audit and Base Searches (5%)- Investigating Issues with Deep Dives (10%)- Implementing Services (5%)- Introducing ITSI (5%)- Designing Services (5%)- Installing and Configuring ITSI (10%)- Correlation and Multi KPI Searches (5%)- Thresholds and Time Policies (5%)- Anomaly Detection (5%)- Managing Notable Events (10%)- Entities and Modules (5%)- Aggregation Policies (5%)- Templates and Dependencies (5%) **SPLK-3002 PDF Dumps Are Helpful To produce Your Dreams Correct QA's:** https://www.dumpsmaterials.com/SPLK-3002-real-torrent.html]