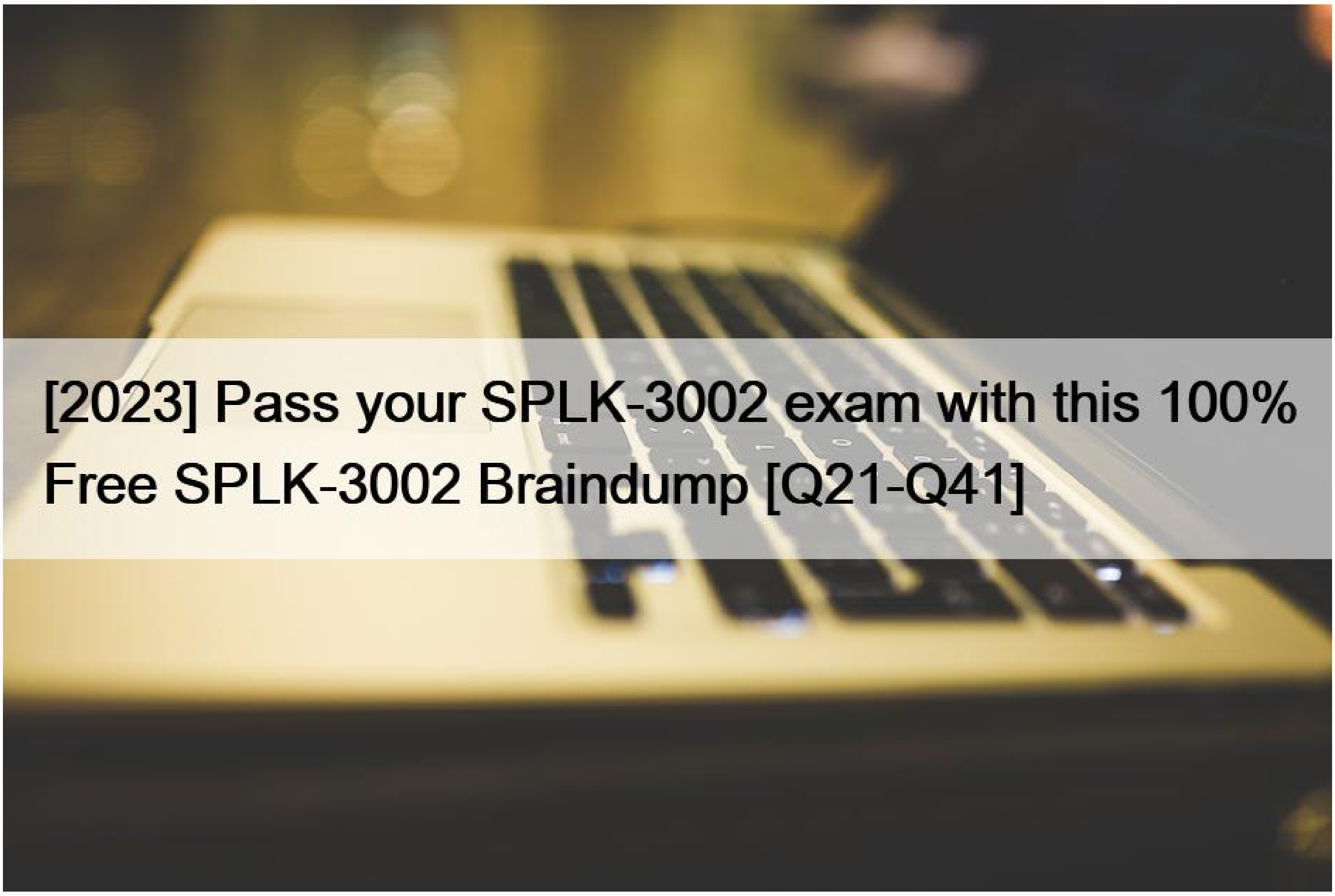
[2023 Pass your SPLK-3002 exam with this 100% Free SPLK-3002 Braindump [Q21-Q41



[2023] Pass your SPLK-3002 exam with this 100% Free SPLK-3002 Braindump
View All SPLK-3002 Actual Exam Questions, Answers and Explanations for Free

NO.21 Which of the following describes enabling smart mode for an aggregation policy?
* Configure -> Policies -> Smart Mode -> Enable, select &#8220;fields&#8221;, click &#8220;Save&#8221;
* Enable grouping in Notable Event Review, select &#8220;Smart Mode&#8221;, select &#8220;fields&#8221;, and click &#8220;Save&#8221;
* Edit the aggregation policy, enable smart mode, select fields to analyze, click &#8220;Save&#8221;
* Edit the notable event view, enable smart mode, select &#8220;fields&#8221;, and click &#8220;Save&#8221;
Explanation

1. From the ITSI main menu, click Configuration > Notable Event Aggregation Policies.

2. Select a custom policy or the Default Policy.

3. Under Smart Mode grouping, enable Smart Mode.

4. Click Select fields. A dialog displays the fields found in your notable events from the last 24 hours.

NO.22 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&#8217;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.
Reference:

A base search is a search definition that can be shared across multiple KPIs that use the same data source. Base searches can improve search performance and reduce search load by consolidating multiple similar KPIs. One of the characteristics of base searches is that it is possible to filter to entities assigned to the service for calculating the metrics for the service&#8217;s KPIs. This means that you can use entity filtering rules to specify which entities are relevant for each KPI based on the base search results. Reference: Create KPI base searches in ITSI, [Filter entities for KPIs based on base searches]

NO.23 Which of the following is a recommended best practice for service and glass table design?
* Plan and implement services first, then build detailed glass tables.
* Always use the standard icons for glass table widgets to improve portability.
* Start with base searches, then services, and then glass tables.
* Design glass tables first to discover which KPIs are important.

NO.24 For which ITSI function is it a best practice to use a 15-30 minute time buffer?
* Correlation searches.
* Adaptive thresholding.
* Maintenance windows
* Anomaly detection.
B is the correct answer because adaptive thresholding is a feature of ITSI that allows you to dynamically adjust KPI thresholds based on historical patterns and trends. Adaptive thresholding requires a time buffer of at least 15 minutes to calculate the thresholds based on the previous data points. The time buffer ensures that there is enough data to perform the calculations and avoid false positives or negatives. Reference: Configure adaptive thresholding for a KPI in ITSI

NO.25 Which of the following describes entities? (Choose all that apply.)
* Entities must be IT devices, such as routers and switches, and must be identified by either IP value, host name, or mac address.
* An abstract (pseudo/logical) entity can be used to split by for a KPI, although no entity rules or filtering can be used to limit data to a specific service.
* Multiple entities can share the same alias value, but must have different role values.
* To automatically restrict the KPI to only the entities in a particular service, select &#8220;Filter to Entities in Service&#8221;.

NO.26 Which of the following is an advantage of using adaptive time thresholds?
* Automatically update thresholds daily to manage dynamic changes to KPI values.
* Automatically adjust KPI calculation to manage dynamic event data.
* Automatically adjust aggregation policy grouping to manage escalating severity.
* Automatically adjust correlation search thresholds to adjust sensitivity over time.

NO.27 Which index will contain useful error messages when troubleshooting ITSI issues?
* _introspection
* _internal
* itsi_summary
* itsi_notable_audit

NO.28 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.
Copy SA-IndexCreation to $SPLUNK_HOME/etc/apps/ on all individual indexers in your environment.

Reference:

A is the correct answer because when installing ITSI to support a distributed search architecture, you need to copy SA-IndexCreation to all indexers. SA-IndexCreation is an app that contains the definitions of the ITSI indexes, such as itsi_summary, itsi_tracked_alerts, itsi_grouped_alerts, etc. You need to copy this app to all indexers to ensure that they can store and search the ITSI data. B is not a correct answer because you do not need to copy SA-IndexCreation to the etc/apps directory on the index cluster master node. The index cluster master node does not store or search data, it only manages the replication and availability of data across the index cluster peers. C is not a correct answer because you do not need to extract the installer package into etc/apps directory of the cluster deployer node. The cluster deployer node is used to distribute apps and configuration updates to the search head cluster members. You need to extract the installer package into etc/shcluster/apps directory of the cluster deployer node instead. D is not a correct answer because you do not need to extract the ITSI app package into etc/apps directory of search head. You need to extract the ITSI app package into etc/shcluster/apps directory of the cluster deployer node and use the deployer to push the app to all search head cluster members. Reference: [Install Splunk IT Service Intelligence on a search head cluster], [Install Splunk IT Service Intelligence on an indexer cluster]

NO.29 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.
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.

Reference:

https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/kvstorejson

https://docs.splunk.com/Documentation/ITSI/4.10.2/Configure/BackupandRestoreITSIconfig C and D are correct answers because ITSI backup and restore functionality uses kvstore_to_json.py as a command line script or as part of custom scripts to backup ITSI data for full or partial backups. ITSI backups are also stored as a collection of JSON formatted files that contain KV store objects such as services, KPIs, glass tables, etc. A is not a correct answer because there is no pre-configured default ITSI backup job provided. You can create your own backup jobs or use the command line script or custom scripts to backup ITSI data. B is not a correct answer because ITSI backup is not inclusive of index dependencies. ITSI backup only includes KV store objects and optionally some .conf files. You need to use other methods to backup index data. Reference: [Overview of backing up and restoring ITSI KV store data], [Create a full backup of ITSI], [Create a partial backup of ITSI]

NO.30 What are valid ITSI Glass Table editor capabilities? (Choose all that apply.)
* Creating glass tables.
* Correlation search creation.

* Service swapping configuration.
* Adding KPI metric lanes to glass tables.
Explanation

Create a glass table to visualize and monitor the interrelationships and dependencies across your IT and business services.

The service swapping settings are saved and apply the next time you open the glass table.

You can add metrics like KPIs, ad hoc searches, and service health scores that update in real time against a background that you design. Glass tables show real-time data generated by KPIs and services.

NO.31 Which of the following is a good use case regarding defining entities for a service?
* Automatically associate entities to services using multiple entity aliases.
* All of the entities have the same identifying field name.
* Being able to split a CPU usage KPI by host name.
* KPI total values are aggregated from multiple different category values in the source events.
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:

A is the correct answer because defining entities for a service allows you to automatically associate entities to services using multiple entity aliases. Entity aliases are alternative names or identifiers for an entity, such as host name, IP address, MAC address, or DNS name. ITSI matches entity aliases to fields in your data sources and assigns entities to services accordingly. This way, you can avoid manually adding entities to each service and ensure that your services reflect the latest changes in your environment.
Reference: Define entities for a service in ITSI

NO.32 Which of the following is an advantage of using adaptive time thresholds?
* Automatically update thresholds daily to manage dynamic changes to KPI values.
* Automatically adjust KPI calculation to manage dynamic event data.
* Automatically adjust aggregation policy grouping to manage escalating severity.
* Automatically adjust correlation search thresholds to adjust sensitivity over time.
Reference:

Adaptive thresholds are thresholds calculated by machine learning algorithms that dynamically adapt and change based on the KPI&#8217;s observed behavior. Adaptive thresholds are useful for monitoring KPIs that have unpredictable or seasonal patterns that are difficult to capture with static thresholds. For example, you might use adaptive thresholds for a KPI that measures web traffic volume, which can vary depending on factors such as holidays, promotions, events, and so on. The advantage of using adaptive thresholds is:

A) Automatically update thresholds daily to manage dynamic changes to KPI values. This is true because adaptive thresholds use historical data from a training window to generate threshold values for each time block in a threshold template. Each night at midnight, ITSI recalculates adaptive threshold values for a KPI by organizing the data from the training window into distinct buckets and then analyzing each bucket separately. This way, the thresholds reflect the most recent changes in the KPI data and account for any anomalies or trends.

The other options are not advantages of using adaptive thresholds because:

B) Automatically adjust KPI calculation to manage dynamic event data. This is not true because adaptive thresholds do not affect the KPI calculation, which is based on the base search and the aggregation method. Adaptive thresholds only affect the threshold values that are used to determine the KPI severity level.

C) Automatically adjust aggregation policy grouping to manage escalating severity. This is not true because adaptive thresholds do not affect the aggregation policy, which is a set of rules that determines how to group notable events into episodes. Adaptive thresholds only affect the threshold values that are used to generate notable events based on KPI severity level.

D) Automatically adjust correlation search thresholds to adjust sensitivity over time. This is not true because adaptive thresholds do not affect the correlation search, which is a search that looks for relationships between data points and generates notable events. Adaptive thresholds only affect the threshold values that are used by KPIs, which can be used as inputs for correlation searches.

NO.33 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.

NO.34 Anomaly detection can be enabled on which one of the following?
* KPI
* Multi-KPI alert
* Entity
* Service
Explanation

Enable anomaly detection to identify trends and outliers in KPI search results that might indicate an issue with your system.

NO.35 Which of the following is a best practice when configuring maintenance windows?
* Disable any glass tables that reference a KPI that is part of an open maintenance window.
* Develop a strategy for configuring a service&#8217;s notable event generation when the service&#8217;s maintenance window is open.
* Give the maintenance window a buffer, for example, 15 minutes before and after actual maintenance work.
* Change the color of services and entities that are part of an open maintenance window in the service analyzer.

Explanation

It&#8217;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.

NO.36 For which ITSI function is it a best practice to use a 15-30 minute time buffer?
* Correlation searches.
* Adaptive thresholding.
* Maintenance windows
* Anomaly detection.
Explanation

It&#8217;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.

NO.37 Besides creating notable events, what are the default alert actions a correlation search can execute? (Choose all that apply.)
* Ping a host.
* Send email.
* Include in RSS feed.
* Run a script.
Explanation

Throttling applies to any correlation search alert type, including notable events and actions (RSS feed, email, run script, and ticketing).

NO.38 After a notable event has been closed, how long will the meta data for that event remain in the KV Store by default?
* 6 months.
* 9 months.
* 1 year.
* 3 months.
Explanation

By default, notable event metadata is archived after six months to keep the KV store from growing too large.

NO.39 Which of the following accurately describes base searches used for KPIs in a service?
* Base searches can be used for multiple services.
* A base search can only be used by its service and all dependent services.
* All the metrics in a base search are used by one service.
* All the KPIs in a service use the same base search.
KPI base searches let you share a search definition across multiple KPIs in IT Service Intelligence (ITSI). Create base searches to consolidate multiple similar KPIs, reduce search load, and improve search performance.

Reference:

A base search is a search definition that can be shared across multiple KPIs that use the same data source. Base searches can improve search performance and reduce search load by consolidating multiple similar KPIs. The statement that accurately describes base searches used for KPIs in a service is:

A) Base searches can be used for multiple services. This means that you can create a base search for a service and use it for other services that have similar data sources and KPIs. For example, if you have multiple services that monitor web server performance, you can create a base search that queries the web server logs and use it for all the services that need to calculate KPIs based on those logs.

NO.40 Which of the following describes a realistic troubleshooting workflow in ITSI?
* Correlation Search -> Deep Dive -> Notable Event
* Service Analyzer -> Notable Event Review -> Deep Dive
* Service Analyzer -> Aggregation Policy -> Deep Dive
* Correlation search -> KPI -> Aggregation Policy

NO.41 What is the main purpose of the service analyzer?
* Display a list of All Services and Entities.
* Trigger external alerts based on threshold violations.
* Allow Analysts to add comments to Alerts.
* Monitor overall Service and KPI status.