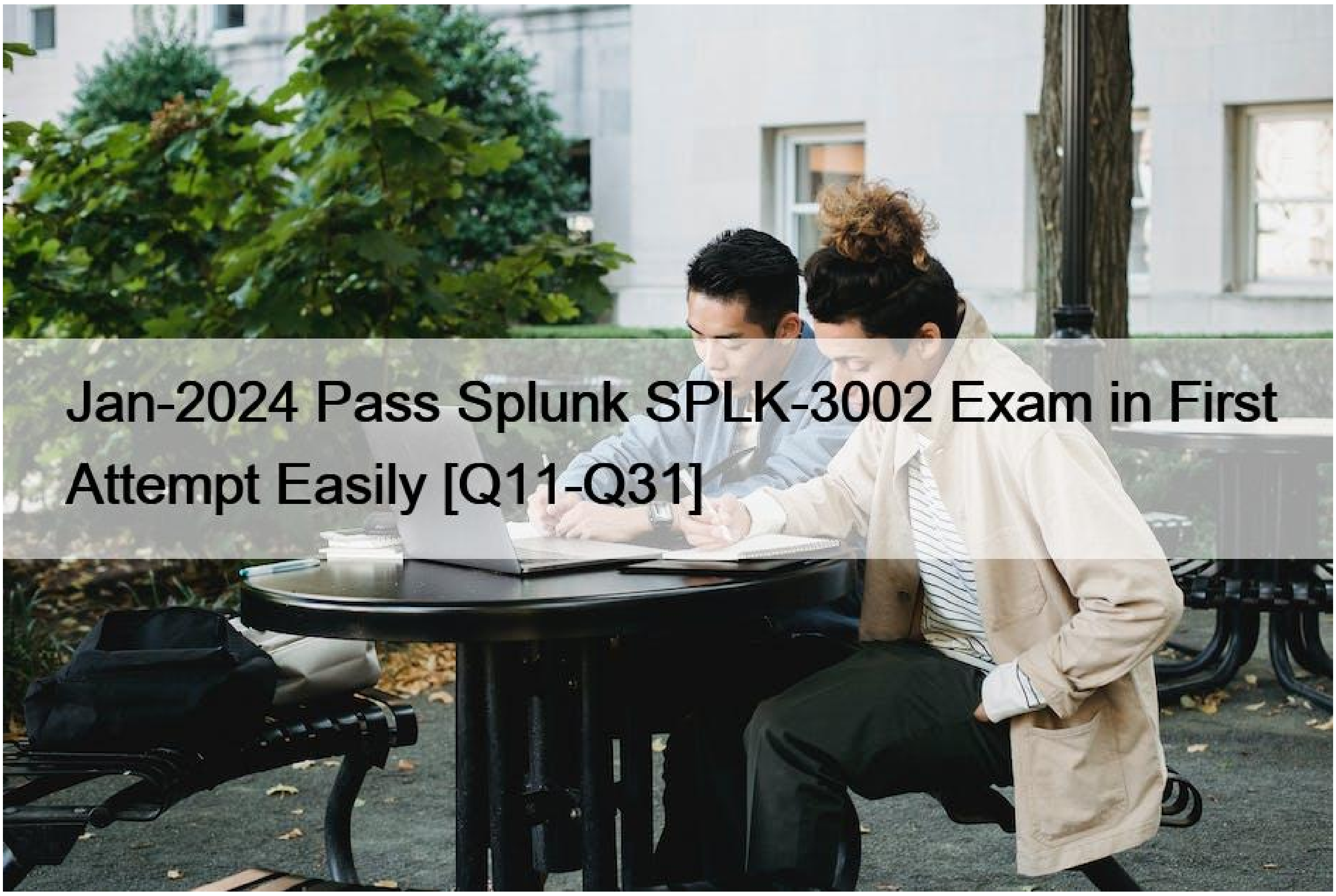
Jan-2024 Pass Splunk SPLK-3002 Exam in First Attempt Easily [Q11-Q31



Jan-2024 Pass Splunk SPLK-3002 Exam in First Attempt Easily
Free SPLK-3002 Exam Files Downloaded Instantly 100% Dumps & Practice Exam

The SPLK-3002 exam is a vendor-specific certification that is recognized globally as a valuable credential for IT professionals. It is designed for individuals who have already completed the Splunk Certified Power User certification and have experience working with Splunk IT Service Intelligence. Splunk IT Service Intelligence Certified Admin certification exam consists of 65 multiple-choice questions that must be completed within 90 minutes. Candidates must achieve a minimum score of 70% to pass the exam and earn the certification.

QUESTION 11

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.

Reference:

The service analyzer is a dashboard that allows you to monitor the overall service and KPI status in ITSI. The service analyzer displays a list of all services and their health scores, which indicate how well each service is performing based on its KPIs. You can also view the status and values of each KPI within a service, as well as drill down into deep dives or glass tables for further analysis. The service analyzer helps you identify issues affecting your services and prioritize them based on their impact and urgency. The main purpose of the service analyzer is:

D) Monitor overall service and KPI status. This is true because the service analyzer provides a comprehensive view of the health and performance of your services and KPIs in real time.

The other options are not the main purpose of the service analyzer because:

A) Display a list of all services and entities. This is not true because the service analyzer does not display entities, which are IT components that require management to deliver an IT service. Entities are displayed in other dashboards, such as entity management or entity health overview.

B) Trigger external alerts based on threshold violations. This is not true because the service analyzer does not trigger alerts, which are notifications sent to external systems or users when certain conditions are met. Alerts are triggered by correlation searches or alert actions configured in ITSI.

C) Allow analysts to add comments to alerts. This is not true because the service analyzer does not allow analysts to add comments to alerts, which are notifications sent to external systems or users

QUESTION 12

ITSI Saved Search Scheduling is configured to use realtime_schedule = 0. Which statement is accurate about this configuration?
* If this value is set to 0, the scheduler bases its determination of the next scheduled search execution time on the current time.
* If this value is set to 0, the scheduler bases its determination of the next scheduled search on the last search execution time.
* If this value is set to 0, the scheduler may skip scheduled execution periods.
* If this value is set to 0, the scheduler might skip some execution periods to make sure that the scheduler is executing the searches running over the most recent time range.
Explanation

If set to 0, the scheduler determines the next scheduled search run time based on the last run time for the search. This is called continuous scheduling.

QUESTION 13

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

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

QUESTION 14

In maintenance mode, which features of KPIs still function?
* KPI searches will execute but will be buffered until the maintenance window is over.
* KPI searches still run during maintenance mode, but results go to itsi_maintenance_summary index.
* New KPIs can be created, but existing KPIs are locked.
* KPI calculations and threshold settings can be modified.
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.

Reference:

A is the correct answer because KPI searches still run during maintenance mode, but the results are buffered until the maintenance window is over. This means that no alerts are triggered during maintenance mode, but once it ends, the buffered results are processed and alerts are generated if necessary. You cannot create new KPIs or modify existing KPIs during maintenance mode. Reference: [Overview of maintenance windows in ITSI]

QUESTION 15

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

QUESTION 16

When in maintenance mode, which of the following is accurate?
* Once the window is over, KPIs and notable events will begin to be generated again.
* KPIs are shown in blue while in maintenance mode.
* Maintenance mode slots are scheduled on a per hour basis.
* Service health scores and KPI events are deleted until the window is over.
Reference:

A is the correct answer because when in maintenance mode, KPIs and notable events will begin to be generated again once the window is over. Maintenance mode is a feature of ITSI that allows you to temporarily suspend alerts and health score calculations for a service or an entity during planned maintenance or downtime. During maintenance mode, KPI searches still run, but the results are buffered until the window is over. Once the window is over, the buffered results are processed and alerts and health scores are generated if necessary. Reference: [Overview of maintenance windows in ITSI]

QUESTION 17

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;.

QUESTION 18

Which capabilities are enabled through &#8220;teams&#8221;?
* Teams allow searches against the itsi_summary index.
* Teams restrict notable event alert actions.
* Teams restrict searches against the itsi_notable_audit index.
* Teams allow restrictions to service content in UI views.
Explanation

Teams provide presentation-layer security only and not data-level security. It&#8217;s still possible for a user with access to the Splunk search bar to look up ITSI summary index data.

QUESTION 19

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.

QUESTION 20

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.

QUESTION 21

Which of the following best describes a default deep dive?
* It initially shows the health scores for all services.
* It initially shows the highest importance KPIs.
* It initially shows all of the KPIs for a selected service.
* It initially shows all the entity swim lanes.
Reference:

C is the correct answer because a default deep dive initially shows all of the KPIs for a selected service. You can create a default deep dive by drilling down from another dashboard or by selecting a service from the deep dive lister page. A default deep dive does not show health scores, importance scores, or entity swim lanes by default. Reference: [Create default deep dives for services in ITSI]

QUESTION 22

Which index will contain useful error messages when troubleshooting ITSI issues?
* _introspection
* _internal
* itsi_summary
* itsi_notable_audit

QUESTION 23

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.

QUESTION 24

Which of the following is a valid type of Multi-KPI Alert?

* Score over composite.
* Value over time.
* Status over time.
* Rise over run.

QUESTION 25

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.

QUESTION 26

What is the default importance value for dependent services&#8217; health scores?
* 11
* 1
* Unassigned
* 10
Explanation

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

QUESTION 27

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.

QUESTION 28

When changing a service template, which of the following will be added to linked services by default?
* Thresholds.
* Entity Rules.
* New KPIs.
* Health score.
C) New KPIs. This is true because when you add new KPIs to a service template, they will be automatically added to all the services that are linked to that template. This helps you keep your services consistent and up-to-date with the latest KPI definitions.

The other options will not be added to linked services by default because:

A) Thresholds. This is not true because when you change thresholds in a service template, they will not affect the existing thresholds in the linked services. You need to manually apply the threshold changes to each linked service if you want them to inherit the new thresholds from the template.

B) Entity rules. This is not true because when you change entity rules in a service template, they will not affect the existing entity rules in the linked services. You need to manually apply the entity rule changes to each linked service if you want them to inherit the new entity rules from the template.

D) Health score. This is not true because when you change health score settings in a service template, they will not affect the existing health score settings in the linked services. You need to manually apply the health score changes to each linked service if you want them to inherit the new health score settings from the template.

QUESTION 29

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.

QUESTION 30

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.

QUESTION 31

What are valid considerations when designing an ITSI Service? (Choose all that apply.)
* Service access control requirements for ITSI Team Access should be considered, and appropriate teams provisioned prior to creating the ITSI Service.
* Entities, entity meta-data, and entity rules should be planned carefully to support the service design and configuration.

* Services, entities, and saved searches are stored in the ITSI app, while events created by KPI execution are stored in the itsi_summary index.
* Backfill of a KPI should always be selected so historical data points can be used immediately and alerts based on that data can occur.

Free Exam Updates SPLK-3002 dumps with test Engine Practice:
https://www.dumpsmaterials.com/SPLK-3002-real-torrent.html]