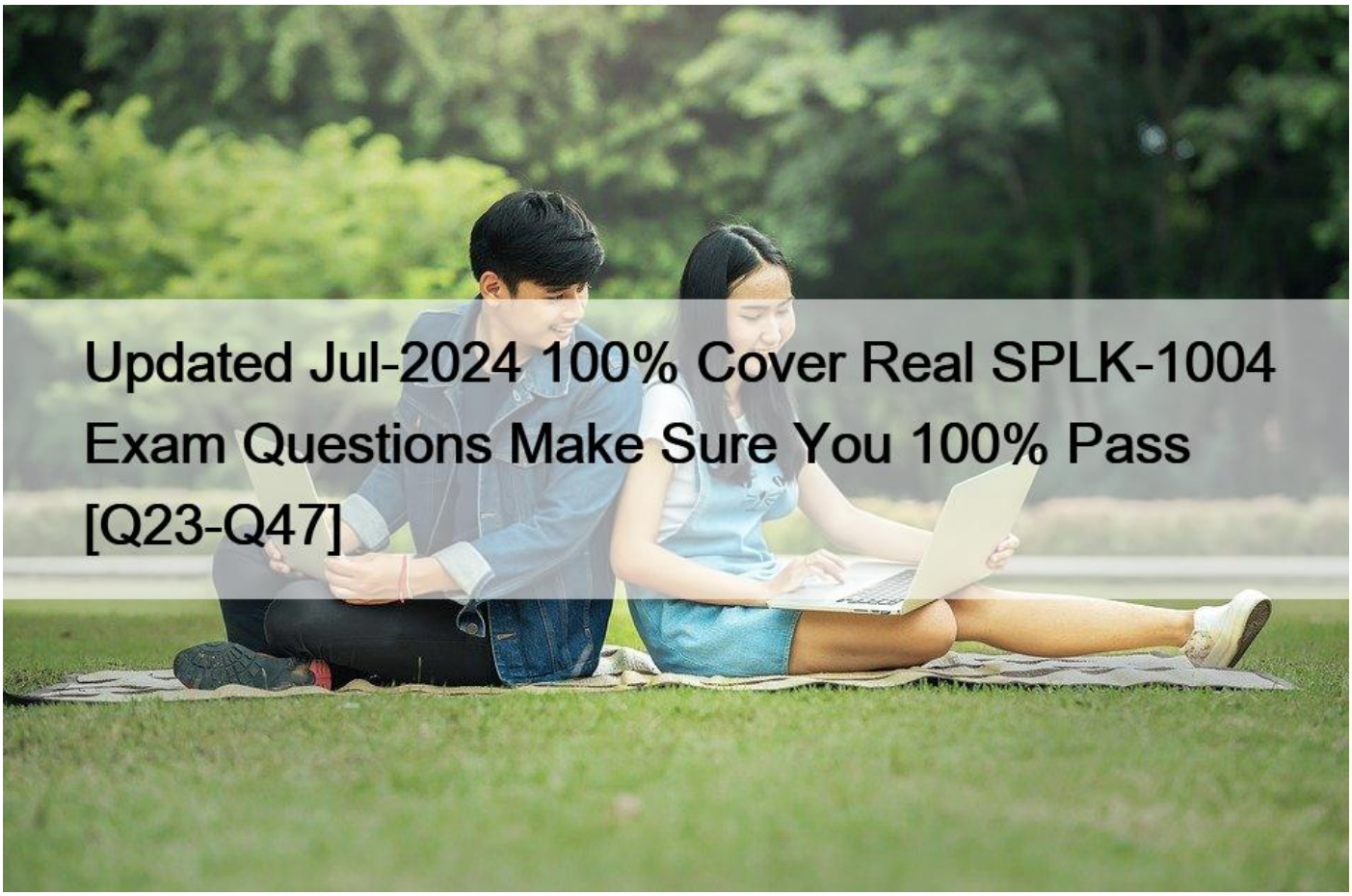
Updated Jul-2024 100% Cover Real SPLK-1004 Exam Questions Make Sure You 100% Pass [Q23-Q47



Updated Jul-2024 100% Cover Real SPLK-1004 Exam Questions Make Sure You 100% Pass SPLK-1004 dumps Accurate Questions and Answers with Free and Fast Updates

Splunk SPLK-1004 exam is designed to test the skills and knowledge of advanced power users who work with data in Splunk. SPLK-1004 exam is the highest level of certification for power users in Splunk and requires a deep understanding of the platform's various features and capabilities. SPLK-1004 exam is intended for professionals who have already achieved the Splunk Core Certified User credential and want to further advance their career in Splunk.

Q23. When using a nested search macro, how can an argument value be passed to the inner macro?
* The argument value may be passed to the outer macro.
* An argument cannot be used with an inner nested macro.
* An argument cannot be used with an outer nested macro.
* The argument value must be specified in the outer macro.

When using a nested search macro in Splunk, an argument value can be passed to the inner macro by specifying the argument in the outer macro’s invocation (Option A). This allows the outer macro to accept arguments from the user or another search

command and then pass those arguments into the inner macro, enabling dynamic and flexible macro compositions that can adapt based on input parameters.

Q24. How can form inputs impact dashboard panels using inline searches?
* Panels powered by an inline search require a minimum of one form input.
* Form inputs can not impact panels using inline searches.
* Adding a form input to a dashboard converts all panels to prebuilt panels.
* A token in a search can be replaced by a form input value.

Form inputs in Splunk dashboards can dynamically impact the panels using inline searches by allowing a token in the search to be replaced by a form input value (Option D). This capability enables dashboard panels to update their content based on user interaction with the form elements. When a user makes a selection or enters data into a form input, the corresponding token in the search string of a dashboard panel is replaced with this value, effectively customizing the search based on user input. This feature makes dashboards more interactive and adaptable to different user needs or questions.

Q25. Where can wildcards be used in the tstats command?
* No wildcards can be used with
* In the where to clause.
* In the from clause.
* In the by clause.

Wildcards can be used in the from clause of the tstats command in Splunk (Option C). The from clause specifies the data model or dataset from which to retrieve the statistics, and using wildcards here allows users to query across multiple data models or datasets that share a common naming pattern, making the search more flexible and encompassing.

Q26. What are the four types of event actions?
* stats, target, set, and unset
* stats, target, change, and clear
* eval, link, change, and clear
* eval, link, set, and unset

The four types of event actions in Splunk are eval, link, change, and clear (Option C). These actions can be used in dashboard panel configurations to dynamically interact with or manipulate event data based on user inputs or other criteria. Eval is used for calculating fields, link for creating hyperlinks, change for modifying field values, and clear for removing field values or other data elements.

Q27. which function of the stats command creates a multivalue entry?
* mvcombine
* eval
* makemv
* list

Q28. Which field Is requited for an event annotation?
* annotation_category
* _time
* eventype
* annotation_label

For an event annotation in Splunk, the required field is time (Option B). The time field specifies the point or range in time that the annotation should be applied to in timeline visualizations, making it essential for correlating the annotation with the correct temporal context within the data.

Q29. Which of the following functions’ primary purpose is to convert epoch time to a string format?
* tostring

* strptime
* tonumber
* strftime

The strftime function in Splunk is used to convert epoch time (also known as POSIX time or Unix time, which is a system for describing points in time as the number of seconds elapsed since January 1, 1970) into a human-readable string format. This function is particularly useful when formatting timestamps in search results or when creating more readable time representations in dashboards and reports. The strftime function takes an epoch time value and a format string asarguments and returns the formatted time as a string according to the specified format. The other options (tostring, strptime, and tonumber) serve different purposes: tostring converts values to strings, strptime converts string representations of time into epoch format, and tonumber converts values to numbers.

Q30. How is regex passed to the makemv command?

* makemv be preceded by the erex command.
* It is specified by the delim argument.
* It Is specified by the tokenizer argument.
* Makemv must be preceded by the rex command.

The regex is passed to the makemv command in Splunk using the delim argument (Option B). This argument specifies the delimiter used to split a single string field into multiple values, effectively creating a multivalue field from a field that contains delimited data.

Q31. What is the correct hierarchy of XML elements in a dashboard panel?

* <panel><dashboard><row>
* <dashboard><row><panel>
* <dashboard><panel><row>
* <panel><row><dashboard>

In a Splunk dashboard, the correct hierarchy of XML elements for a dashboard panel is

<dashboard><row><panel> (Option B). A Splunk dashboard is defined within the <dashboard> element.

Within this, <row> elements are used to organize the layout into rows, and each <panel> element within a row defines an individual panel that can contain visualizations, searches, or other content. This hierarchical structure allows for organized and customizable layouts of dashboard elements, facilitating clear presentation of data and analyses. The other options provided do not represent the correct hierarchical order for defining dashboard panels in Splunk’s XML dashboard syntax.

Q32. What command is used la compute find write summary statistic, to a new field in the event results?

* tstats
* stats
* eventstats
* transaction

The eventstats command in Splunk is used to compute and add summary statistics to all events in the search results, similar to the stats command, but without grouping the results into a single event(Option C). This command adds the computed summary statistics as new fields to each event, allowing those fields to be used in subsequent search operations or for display purposes. Unlike the transaction command, which groups events into transactions, eventstats retains individual events while enriching them with statistical information.

Q33. How can a lookup be referenced in an alert?

* Use the lookup dropdown in the alert configuration window.
* Follow a lookup with an alert command in the search bar.
* Run a search that uses a lookup and save as an alert.
* Upload a lookup file directly to the alert.

To reference a lookup in an alert in Splunk, you would run a search that uses a lookup and then save that search as an alert (Option

C). This method integrates the lookup within the search logic, and when the search conditions meet the alert’s trigger conditions, the alert is activated. This approach allows the alert to leverage the enriched data provided by the lookup for more accurate and informative alerting.

Q34. What type of drilldown passes a value from a user click into another dashboard or external page?
* Visualization
* Event
* Dynamic
* Contextual

Contextual drilldown (Option D) is the type of drilldown that allows passing a value from a user click (e.g., from a table row or chart element) into another dashboard or an external page. This feature enables the creation of interactive dashboards where clicking on a specific element dynamically updates another part of the dashboard or navigates to a different page with relevant information, using the clicked value as a context for the subsequent view.

Q35. What XML element is used to pass multiple fields into another dashboard using a dynamic drilldown?
* <drilldown field_”sources_Field_name”>
* <condition field_”sources_Field_name”>
* <pas_token field_”sources_field_name”>
* <link field_”sources_field_name”>

In Splunk Simple XML for dashboards, dynamic drilldowns are configured within the<drilldown>element, not<link>,<condition>, or<pass_token>. To pass multiple fields to another dashboard, you would use a combination of<set>tokens within the<drilldown>element. Each<set>token specifies a field or value to be passed. The correct configuration might look something like this within the<drilldown>element:

<drilldown>

<set token=”token1″>$row.field1$</set>

<set token=”token2″>$row.field2$</set>

<link target=”_blank”>/app/search/new_dashboard</link>

</drilldown>

In this configuration,$row.field1$and$row.field2$are placeholders for the field values from the clicked event, which are assigned to tokenstoken1andtoken2. These tokens can then be used in the target dashboard to receive the values. The<link>element specifiesthe target dashboard. Note that the exact syntax can vary based on the specific requirements of the drilldown and the dashboard configuration.

Q36. What is a performance improvement technique unique to dashboards?
* Using stats instead of transaction
* Using global searches
* Using report acceleration
* Using datamodel acceleration

Using report acceleration (Option C) is a performance improvement technique unique to dashboards in Splunk.

Report acceleration involves pre-computing the results of a report (which can be a saved search or a dashboard panel) and storing these results in a summary index, allowing dashboards to load faster by retrieving the pre-computed data instead of running the full search each time. This technique is especially useful for dashboards that rely on complex searches or searches over large datasets.

Q37. Which command processes a template for a set of related fields?
* bin
* xyseries
* foreach
* untable

The foreach command in Splunk is used to apply a processing step to each field in a set of related fields, making it ideal for performing repetitive tasks across multiple fields without having to specify each field individually. This command can process a template of commands or functions to apply to each specified field, thereby streamlining operations that need to be applied uniformly across multiple data points.

Q38. Why is the transaction command slow in large splunk deployments?
* It forces the search to run in fast mode.
* transaction or runs on each Indexer in parallel.
* It forces all event data to be returned to the search head.
* transaction runs a hidden eval to format fields.

The transaction command can be slow in large Splunk deployments because it requires all event data relevant to the transaction to be returned to the search head (Option C). This process can be resource-intensive, especially for transactions that span a large volume of data or time, as it involves aggregating and sorting events across potentially many indexers before the transaction logic can be applied.

Q39. what is the result of the xyseries command?
* To transform single series output into a multi-series output
* To transform a stats-like output into chart-like output.
* To transform a multi-series output into single series output.
* To transform a chart-like output into a stats-like output.

The result of the xyseries command in Splunk is to transform a stats-like output into chart-like output (Option B). The xyseries command restructures the search results so that each row represents a unique combination of x and y values, suitable for plotting in a chart, making it easier to visualize complex relationships between multiple data points.

Q40. Which element attribute is required for event annotation?
* <search type=”event_annotation”>
* <search style=”annotation”>
* <search type=$annotation$>
* <search type=”annotation”>

In Splunk dashboards, event annotations are used to add informative overlays on timeline visualizations to mark significant events. The required element attribute to define an event annotation within a dashboard panel is <search type=”annotation”> (Option D). This attribute specifies that the search within this element is intended to generate annotations, which are then overlaid on the timeline based on the time and information provided by the search results.

Q41. Which of the following is an event handler action?
* Run an eval statement based on a user clicking a value on a form.
* Set a token to select a value from the time range picker.
* Pass a token from a drilldown to modify index settings.
* Cancel all jobs based on the number of search job results captured.

An event handler action in Splunk is an action that is triggered based on user interaction with dashboard elements. Running an eval statement based on a user clicking a value on a form (Option A) is an example of an event handler action. This capability allows dashboards to be interactive and dynamic, responding to user inputs or actions to modify displayed data, visuals, or other elements in real-time.

Q42. How is a muitlvalue Add treated from product-“a, b, c, d”?

* . . . | makemv delim{product, “,”}
* . . . | eval mvexpand{makemv{product, “,”})
* . . . | mvexpand product
* . . . | makemv delim=”,” product

To treat a multivalue field product=”a, b, c, d” in Splunk, the correct command is …| makemv delim=”,” product (Option D).The makemv command with the delim argument specifies the delimiter (in this case, a comma) to split the field values into a multivalue field. This allows for easier manipulation and analysis of each value within the product field as separate entities.

Q43. Which of the following is not a common default time field?
* date_zone
* date minute
* date_year
* date_day

In Splunk, common default time fields include date_minute, date_year, and date_day, which represent the minute, year, and day parts of event timestamps, respectively. date_zone (Option A) is not recognized as a common default time field in Splunk. The platform typically uses fields like _time and various date_* fields for time-related information but does not use date_zone as a standard time field.

Q44. Repeating JSON data structures within one event will be extracted as what type of fields?
* Single value
* Lexicographical
* Multivalue
* Mvindex

Repeating JSON data structures within a single event in Splunk are extracted as multivalue fields (Option C).

Multivalue fields allow a single field to contain multiple distinct values, which is common with JSON data structures that include arrays or repeated elements. Splunk’s field extraction capabilities automatically recognize and parse these structures, allowing users to work with each value within the multivalue field for analysis and reporting

Q45. What happens to panels with post-processing searches when their base search Is refreshed?
* The parcels are deleted.
* The panels are only refreshed If they have also been configured.
* The panels are refreshed automatically.
* Nothing happens to the panels.

When the base search of a dashboard panel with post-processing searches is refreshed, the panels with these post-processing searches are refreshed automatically (Option C). Post-processing searches inherit the scope and results of the base search, and when the base search is updated or rerun, the post-processed results are recalculated to reflect the latest data.

Q46. What file types does Splunk use to define geospatial lookups?
* GPX or GML files
* TXT files
* KMZ or KML files
* CSV files

For defining geospatial lookups, Splunk uses KMZ or KML files (Option C). KML (Keyhole Markup Language) is an XML notation for expressing geographic annotation and visualization within Internet-based maps and Earth browsers like Google Earth. KMZ is a compressed version of KML files. These file types allow Splunk to map data points to geographic locations, enabling the creation of geospatial visualizations and analyses. GPX or GML files (Option A), TXT files (Option B), and CSV files (Option D) are not specifically used for geospatial lookups in Splunk, although CSV files are commonly used for other types of lookups.

Q47. What is one way to troubleshoot dashboards?
* Run the | previous_searches command to troubleshoot your SPL queries.
* Go to the Troubleshooting dashboard of me Searching and Reporting app.
* Delete the dashboard and start over.
* Create an HTML panel using tokens to verify that they are being set.

To troubleshoot dashboards in Splunk, one effective approach is to go to the Troubleshooting dashboard of the Search & Reporting app (Option B). This dashboard provides insights into the performance and potential issues of other dashboards and searches, offering a centralized place to diagnose and address problems. This method allows for a structured approach to troubleshooting, leveraging built-in tools and reports to identify and resolve issues.

Splunk is a leading software platform that helps organizations to analyze and make sense of large amounts of data. As more and more companies rely on Splunk to drive their business, the demand for certified Splunk professionals is increasing. The SPLK-1004 (Splunk Core Certified Advanced Power User) certification exam is designed to validate the skills and knowledge of individuals in this domain.

Real SPLK-1004 Quesions Pass Certification Exams Easily:
https://www.test4engine.com/SPLK-1004_exam-latest-braindumps.html]