# SPLK-1004 Q&As

Splunk Core Certified Advanced Power User

## Pass Splunk SPLK-1004 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.pass4itsure.com/splk-1004.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

**QUESTION 1**

Which of the following is an event handler action?

A. Run an eval statement based on a user clicking a value on a form.

B. Set a token to select a value from the time range picker.

C. Pass a token from a drilldown to modify index settings.

D. Cancel all jobs based on the number of search job results captured.

Correct Answer: A

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.

**QUESTION 2**

Which of the following statements is accurate regarding the append command?

A. It is used with a subsearch and only accesses real-lime searches.

B. It is used with a subsearch and oily accesses historical data.

C. It cannot be used with a subsearch and only accesses historical data.

D. It cannot be used with a subsearch and only accesses real-time searches.

Correct Answer: B

The append command in Splunk is often used with a subsearch to add additional data to the end of the primary search results, and it can access historical data (Option B). This capability is useful for combining datasets from different time ranges or sources, enriching the primary search results with supplementary information.

**QUESTION 3**

When possible, what is the best choice for summarizing data to improve search performance?

A. Us the fieldsummary command.

B. Data model acceleration

C. Report acceleration

D. Summary indexing

Correct Answer: D

**QUESTION 4**

Which is a regex best practice?

A. Use complex expressions rather than simple ones.

B. Avoid backtracking.

C. Use greedy operators (. *) instead of non-greedy operators (. *? ).

D. Use * rather than +.

Correct Answer: B

In regex (regular expressions), one of the best practices is to avoid backtracking when possible. Backtracking occurs when the regex engine revisits previous parts of the input string to attempt different permutations of the pattern, which can significantly degrade performance, especially with complex patterns on large inputs. Designing regex patterns to minimize or avoid backtracking can lead to more efficient and faster evaluations.

**QUESTION 5**

What does the query | makeresults generate?

A. A timestamp

B. A results field

C. An error message

D. The results of the previously run search.

Correct Answer: B

The | makeresults command in Splunk generates a single event containing default fields, with theprimary purpose of creating sample data or a placeholder event for testing and development purposes. The most notable field it generates is _time, but it does not create a specific \\'results\\' field per se. However, it\\'s commonly used to create a base event for further manipulation with eval or other commands in search queries for demonstration, testing, or constructing specific scenarios.

**QUESTION 6**

Which statement about the coalesce function is accurate?

A. It can take only a single argument.

B. It can take a maximum of two arguments.

C. It can be used to create a new field in the results set.

D. It can return null or non-null values.

Correct Answer: C

The coalesce function in Splunk is used to evaluate each argument in order and return the first non-null value. This function can be used within an eval expression to create a new field in the results set, which will contain the first non-null value from the list of fields provided as arguments to coalesce. This makes it particularly useful in situations where data may be missing or inconsistently populated across multiple fields, as it allows for a fallback mechanism to ensure that some value is always presented.

**QUESTION 7**

What XML element is used to pass multiple fields into another dashboard using a dynamic drilldown?

A.

B.

C.

D.

Correct Answer: D

In Splunk Simple XML for dashboards, dynamic drilldowns are configured within the element, not,, or. To pass multiple fields to another dashboard, you would use a combination oftokens

within the element. Eachtoken specifies a field or value to be passed. The correct configuration might look something like this within theelement:

$row.field1$

$row.field2$

/app/search/new_dashboard

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.

Theelement specifiesthe target dashboard. Note that the exact syntax can vary based on the specific requirements of the drilldown and the dashboard configuration.

**QUESTION 8**

Why use the tstats command?

A. As an alternative to the summary command.

B. To generate statistics on indexed fields.

C. To generate an accelerated datamodel.

D. To generate statistics on search-time fields.

Correct Answer: B

The tstats command in Splunk is used to generate statistics on indexed fields, particularly from data models that have been accelerated (Option B). This command is highly efficient for summarizing large volumes of data because it operates on indexed-time summarizations rather than raw data, enabling faster search performance and reduced processing time. The tstats command is especially useful in scenarios where quick aggregation and analysis of indexed data are required, making it a powerful tool for exploring and reporting on data model information. While tstats can be seen as an alternative to some uses of the summary command (Option A), its primary utility is in its ability to leverage data model accelerations and indexed field statistics, rather than creating or referring to summary indexes. It does not specifically generate statistics on search-time fields (Option D) or create an accelerated data model (Option C), but rather it queries against existing accelerated data models.

**QUESTION 9**

How can the inspect button be disabled on a dashboard panel?

A. Set inspect.link.disabled to 1

B. Set link.inspect .visible to 0

C. Set link.inspectSearch.visible too

D. Set link.search.disabled to 1

Correct Answer: B

To disable the inspect button on a dashboard panel in Splunk, you can set the link.inspect.visible attribute to 0 (Option B) in the panel\\'s source code. This attribute controls the visibility of the inspect button, and setting it to 0 hides the button, preventing users from accessing the search inspector for that panel.

**QUESTION 10**

Which of these generates a summary index containing a count of events by productId?

A. | stats count by productId

B. | stats sum (productId)

C. | sistats count by productId

D. sistats summary_index by productid

Correct Answer: A

To generate a summary index containing a count of events by productId, the correct search command would be | stats count by productId (Option A). This command aggregates the events by productId, counting the number of events for each unique productId value. The stats command is a fundamental Splunk command used for aggregation and summarization, making it suitable for creating summary data like counts by specific fields.

**QUESTION 11**

If a search contains a subsearch, what is the order of execution?

A. The order of execution depends on whether either search uses a stats command.

B. The inner search executes first.

C. The otter search executes first.

D. The two searches are executed in parallel.

Correct Answer: B

In a Splunk search containing a subsearch, the inner subsearch executes first (Option B). The result of the subsearch is then passed to the outer search. This is because the outer search often depends on the results of the inner subsearch to complete its execution. For example, a subsearch might be used to identify a list of relevant terms or values which are then used by the outer search to filter or manipulate the main dataset.

**QUESTION 12**

what is the result of the xyseries command?

A. To transform single series output into a multi-series output

B. To transform a stats-like output into chart-like output.

C. To transform a multi-series output into single series output.

D. To transform a chart-like output into a stats-like output.

Correct Answer: B

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.

**QUESTION 13**

Which of the following would exclude all entries contained in the lookup file baditems. csv from search results?

A. NOT [inputlookup baditems.csv]

B. NOT (lookup baditems.csv OUTPUT item)

C. WHERE item NOT IN (baditems.csv)

D. [NOT inputlookup baditems.csv]

Correct Answer: A

The correct syntax to exclude all entries contained in the lookup file baditems.csv from search results is NOT [inputlookup baditems.csv]. This syntax uses a subsearch with the inputlookup command to retrieve the contents of the baditems.csv lookup file and then uses the NOT operator to exclude those results from the main search. This approach is efficient for filtering out unwanted data based on a predefined list of criteria stored in a lookup file.

**QUESTION 14**

Which of the following functions\\' primary purpose is to convert epoch time to a string format?

A. tostring

B. strptime

C. tonumber

D. strftime

Correct Answer: D

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.

**QUESTION 15**

What happens to panels with post-processing searches when their base search Is refreshed?

A. The parcels are deleted.

B. The panels are only refreshed If they have also been configured.

C. The panels are refreshed automatically.

D. Nothing happens to the panels.

Correct Answer: C

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.