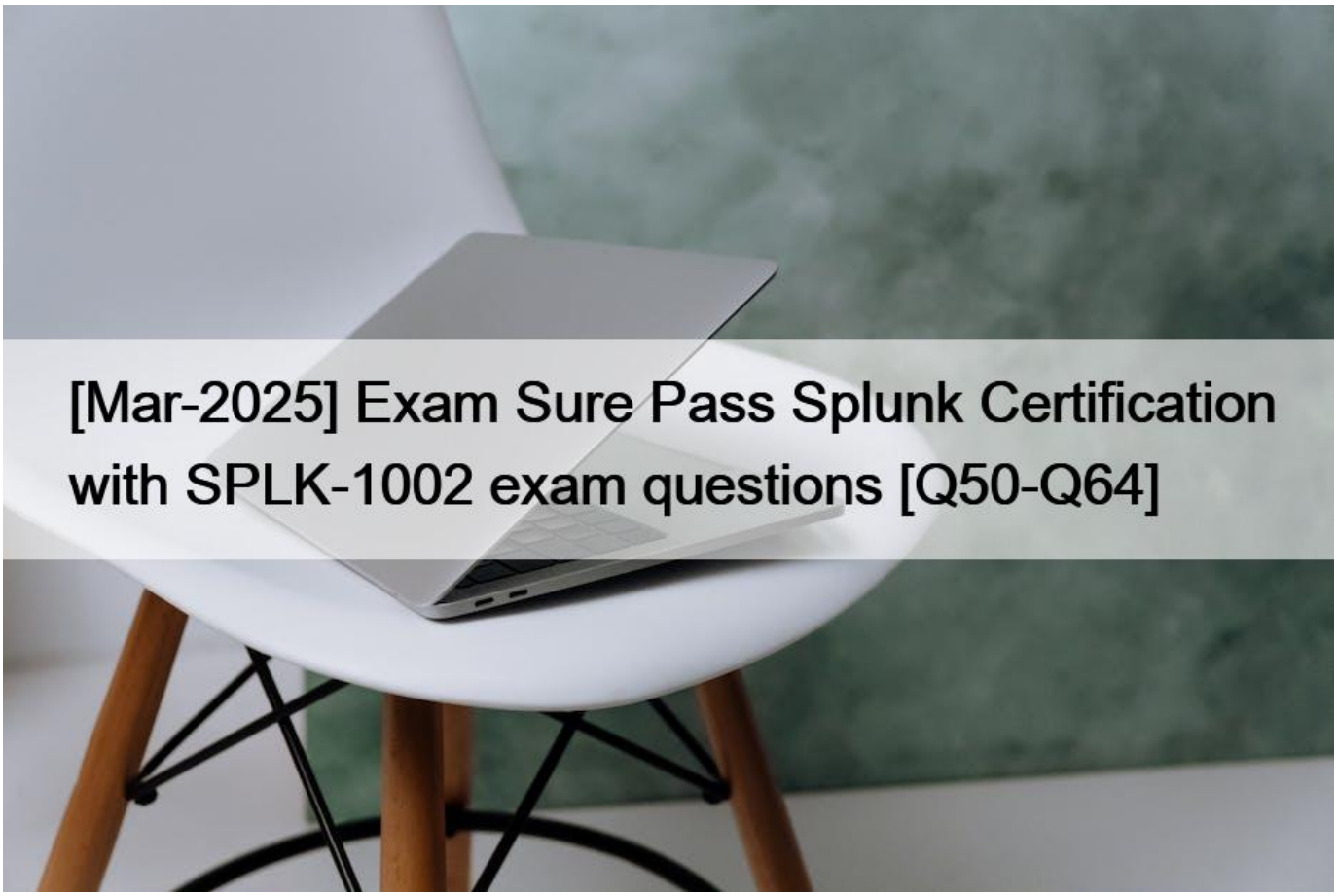
[Mar-2025 Exam Sure Pass Splunk Certification with SPLK-1002 exam questions [Q50-Q64



[Mar-2025] Exam Sure Pass Splunk Certification with SPLK-1002 exam questions
Real Splunk SPLK-1002 Exam Questions Study Guide

Who should take the splk-1002 exam

The Splunk Core Certified Power User **splk-1002 Exam** certification is an internationally-recognized validation that identifies persons who earn it as possessing skilled as Splunk Core Certified Power Users.

Obtaining the Splunk Core Certified Power User certification can be beneficial for IT professionals who work with Splunk or plan to work with the platform in the future. Splunk Core Certified Power User Exam certification demonstrates the candidate's proficiency in using Splunk to analyze and visualize data, which can be valuable for organizations that rely on data-driven decision-making. Additionally, the certification can help individuals advance their career as a Splunk administrator, analyst, or developer.

NO.50 Which of the following is included with the Common Information Model (CIM) add-on?
* Search macros
* Event category tags

* Workflow actions
* tsidx files

The correct answer is B. Event category tags. This is because the CIM add-on contains a collection of preconfigured data models that you can apply to your data at search time. Each data model in the CIM consists of a set of field names and tags that define the least common denominator of a domain of interest.

Event category tags are used to classify events into high-level categories, such as authentication, network traffic, or web activity. You can use these tags to filter and analyze events based on their category.You can learn more about event category tags from the Splunk documentation12. The other options are incorrect because they are not included with the CIM add-on. Search macros are reusable pieces of search syntax that you can invoke from other searches. They are not specific to the CIM add-on, although some Splunk apps may provide their own search macros. Workflow actions are custom links or scripts that you can run on specific fields or events. They are also not specific to the CIM add-on, although some Splunk apps may provide their own workflow actions. tsidx files are index files that store the terms and pointers to the raw data in Splunk buckets. They are part of the Splunk indexing process and have nothing to do with the CIM add-on.

NO.51 Which of the following is the correct way to use the data model command to search field in the data model

within the web dataset?

* | datamodel web search | filed web *
* | Search datamodel web web | filed web*
* | datamodel web web field | search web*
* Datamodel=web | search web | filed web*

The data model command allows you to run searches on data models that have been accelerated1. The syntax

for using the data model command is | datamodel <model_name> <dataset_name> [search <search_string>]1.

Therefore, option A is the correct way to use the data model command to search fields in the data model

within the web dataset. Options B and C are incorrect because they do not follow the syntax for the data model

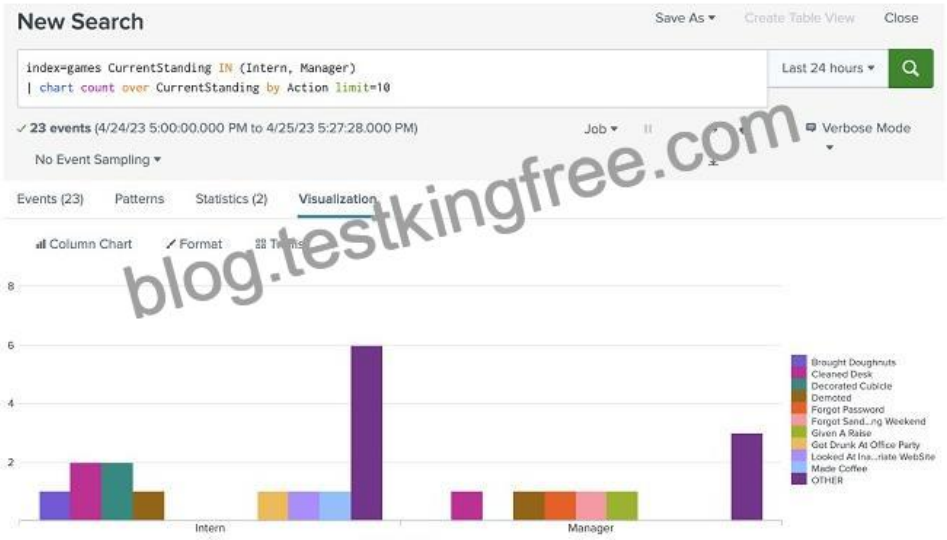
command. Option D is incorrect because it does not use the data model command at all.

NO.52 A user wants to convert numeric field values to strings and also to sort on those values.

Which command should be used first, theevalor thesort?

* It doesn’t matter whether eval or sort is used first.
* Convert the numeric to a string with eval first, then sort.
* Use sort first, then convert the numeric to a string with eval.
* You cannot use the sort command and the eval command on the same field.

NO.53 How could the following syntax for the chart command be rewritten to remove the OTHER category? (select all that apply)



* | chart count over CurrentStanding by Action useother=f
* | chart count over CurrentStanding by Action usenull-f useother-t
* | chart count over CurrentStanding by Action limit=10 useother=f
* | chart count over CurrentStanding by Action limit-10

In Splunk, when using the chart command, the useother parameter can be set to false (f) to remove the ‘OTHER’ category, which is a bucket that Splunk uses to aggregate low-cardinality groups into a single group to simplify visualization. Here’s how the options break down:

A . | chart count over CurrentStanding by Action useother=f

This command correctly sets the useother parameter to false, which would prevent the ‘OTHER’ category from being displayed in the resulting visualization.

B . | chart count over CurrentStanding by Action usenull=f useother=t

This command has useother set to true (t), which means the ‘OTHER’ category would still be included, so this is not a correct option.

C . | chart count over CurrentStanding by Action limit=10 useother=f

Similar to option A, this command also sets useother to false, additionally imposing a limit to the top 10 results, which is a way to control the granularity of the chart but also to remove the ‘OTHER’ category.

D . | chart count over CurrentStanding by Action limit-10

This command has a syntax error (limit-10 should be limit=10) and does not include the useother=f clause. Therefore, it would not remove the ‘OTHER’ category, making it incorrect.

NO.54 How does a user display a chart in stack mode?
* By changing Stack Mode in the Format menu.
* You cannot display a chart in stack mode, only a timechart.
* By using the stack command.
* By turning on the Use Trellis Layout option.

A chart is a graphical representation of your search results that shows the relationship between two or more fields2. You can display a chart in stack mode by changing the Stack Mode option in the Format menu2. Stack mode allows you to stack multiple series on top of each other in a chart to show the cumulative values of each series2. Therefore, option C is correct, while options A, B and D are incorrect because they are not ways to display a chart in stack mode.

NO.55 Calculated fields can be based on which of the following?
* Tags
* Extracted fields
* Output fields for a lookup
* Fields generated from a search string

NO.56 These kinds of charts represent a series in a single bar with multiple sections
* Multi-Series
* Split-Series
* Omit nulls
* Stacked

Stacked charts represent a series in a single bar with multiple sections. A chart is a graphical representation of

data that shows trends, patterns, or comparisons. A chart can have different types, such as column, bar, line,

area, pie, etc. A chart can also have different modes, such as split-series, multi-series, stacked, etc. A stacked

chart is a type of chart that shows multiple series in a single bar or area with different sections for each series

NO.57 Which of the following are required to create a POST workflow action?
* Label, URI, search string.
* XML attributes, URI, name.
* Label, URI, post arguments.
* URI, search string, time range picker.

Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.1.1/Knowledge/SetupaPOSTworkflowaction

NO.58 Which of the following statements describe calculated fields? (select all that apply)
* Calculated fields can be used in the search bar.
* Calculated fields can be based on an extracted field.
* Calculated fields can only be applied to host and sourcetype.
* Calculated fields are shortcuts for performing calculations using the eval command.

Reference:https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/definecalcfields

Calculated fields are fields that are created by performing calculations on existing fields using the eval

command. Calculated fields can be used in the search bar to filter and transform events based on the calculated

values. Calculated fields can also be based on an extracted field, which is a field that is extracted from raw

data using various methods, such as regex, delimiters, lookups, etc. Calculated fields are not shortcuts for

performing calculations using the eval command, but rather results of performing calculations using the eval

command. Calculated fields can be applied to any field in Splunk, not only host and sourcetype.

Therefore, statements A, B, and D are true about calculated fields.

NO.59 When creating a Search workflow action, which field is required?
* Search string
* Data model name
* Permission setting
* An eval statement

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/Setupasearchworkflowaction A workflow action is a link that appears when you click an event field value in your search results2. A workflow action can open a web page or run another search based on the field value2. There are two types of workflow actions: GET and POST2. A GET workflow action appends the field value to the end of a URI and opens it in a web browser2. A POST workflow action sends the field value as part of an HTTP request to a web server2. When creating a Search workflow action, which is a type of GET workflow action that runs another search based on the field value, the only required field is the search string2. The search string defines the search that will be run when the workflow action is clicked2. Therefore, option A is correct, while options B, C and D are incorrect because they are not required fields for creating a Search workflow action.

NO.60 Which of the following statements best describes a macro?
* A macro is a method of categorizing events based on a search.
* A macro is a way to associate an additional (new) name with an existing field name.
* A macro is a portion of a search that can be reused in multiple place
* A macro is a knowledge object that enables you to schedule searches for specific events.

The correct answer is C. A macro is a portion of a search that can be reused in multiple places.

A macro is a way to reuse a piece of SPL code in different searches. A macro can be any part of a search, such as an eval statement or a search term, and does not need to be a complete command. A macro can also take arguments, which are variables that can be replaced by different values when the macro is called. A macro can also contain another macro within it, which is called a nested macro1.

To create a macro, you need to define its name, definition, arguments, and description in the Settings > Advanced Search > Search Macros page in Splunk Web or in the macros.conf file. To use a macro in a search, you need to enclose the macro name in backtick characters (`) and provide values for the arguments if any1.

For example, if you have a macro named my_macro that takes one argument named object and has the following definition:

search sourcetype= object

You can use it in a search by writing:

my_macro(web)

This will expand the macro and run the following SPL code:

search sourcetype=web

The benefits of using macros are that they can simplify complex searches, reduce errors, improve readability, and promote consistency1.

The other options are not correct because they describe other types of knowledge objects in Splunk, not macros. These objects are:

A) An event type is a method of categorizing events based on a search. An event type assigns a label to events that match a specific

search criteria. Event types can be used to filter and group events, create alerts, or generate reports2.

B) A field alias is a way to associate an additional (new) name with an existing field name. A field alias can be used to normalize fields from different sources that have different names but represent the same data. Field aliases can also be used to rename fields for clarity or convenience3.

D) An alert is a knowledge object that enables you to schedule searches for specific events and trigger actions when certain conditions are met. An alert can be used to monitor your data for anomalies, errors, or other patterns of interest and notify you or others when they occur4.

Reference:

About event types

About field aliases

About alerts

Define search macros in Settings

Use search macros in searches

NO.61 A calculated field may be based on which of the following?
* Fields generated within a search string
* Lookup tables
* Regular expressions
* Extracted fields

In Splunk, calculated fields allow you to create new fields using expressions that can transform or combine the values of existing fields. Although all options provided might seem viable, when selecting only one option that is most representative of a calculated field, we typically refer to:

D . Extracted fields: Calculated fields are often based on fields that have already been extracted from your data.

Extracted fields are those that Splunk has identified and pulled out from the event data based on patterns, delimiters, or other methods such as regular expressions or automatic extractions. These fields can then be used in expressions to create calculated fields.

For example, you might have an extracted field for the time in seconds, and you want to create a calculated field for the time in minutes. You would use the extracted field in a calculation to create the new field.

NO.62 When using the transaction command, what does the argument maxspan do?
* Sets the maximum total time between events in a transaction.
* Sets the maximum length of all events within a transaction.
* Sets the maximum total time between the earliest and latest events in a transaction.
* Sets the maximum length that any single event can reach to be included in the transaction.

NO.63 Which of the following searches would return a report of sales by product-name?
* chart sales by product_name
* chart sum(price) as sales by product_name
* stats sum(price) as sales over product_name

* timechart list(sales), values(product_name)

Reference:http://hilllaneconsulting.co.uk/blog/?p=640

NO.64 In most large Splunk environments, what is the most efficient command that can be used to group events by fields?

* join
* stats
* streamstats
* transaction

Explanation/Reference: https://answers.splunk.com/answers/103/transaction-vs-stats-commands.html