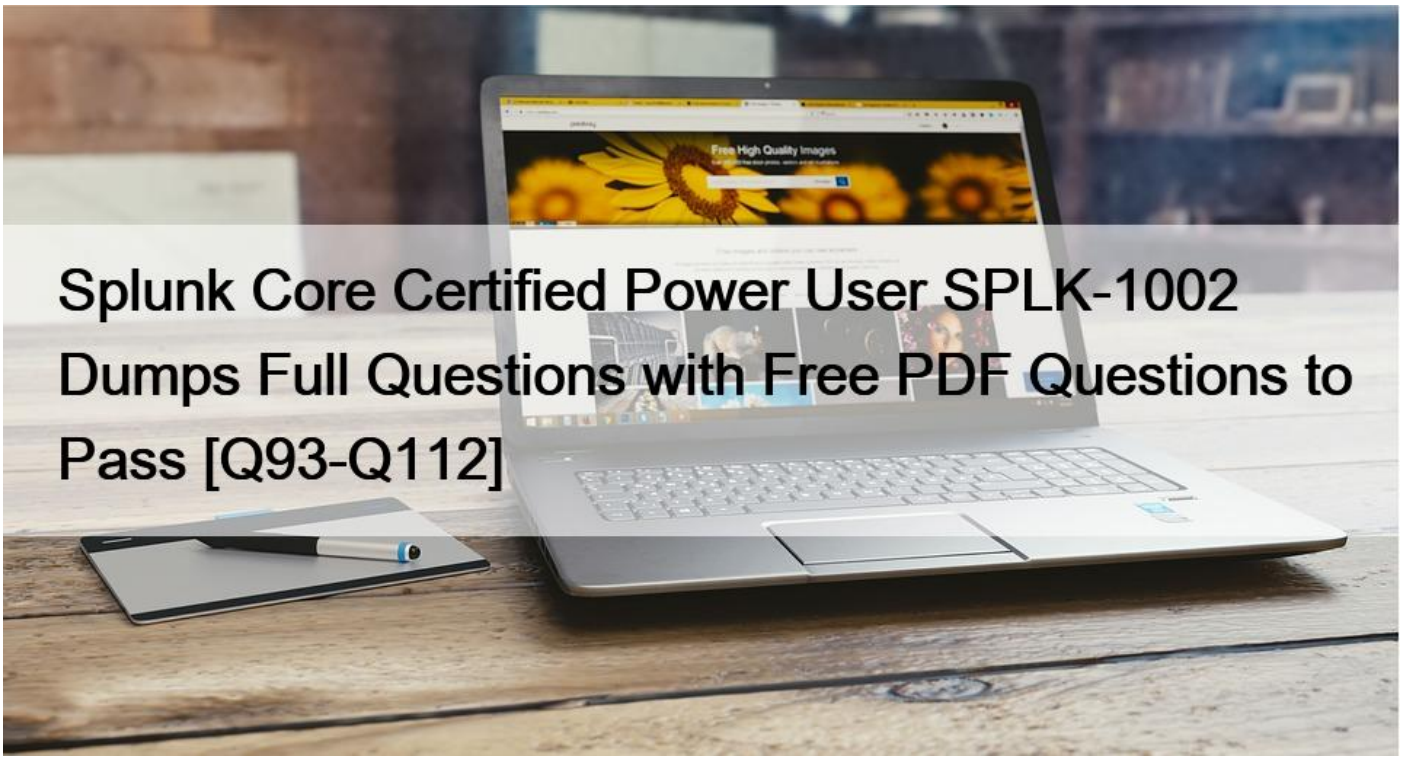
Splunk Core Certified Power User SPLK-1002 Dumps Full Questions with Free PDF Questions to Pass [Q93-Q112



Splunk Core Certified Power User SPLK-1002 Dumps Full Questions with Free PDF Questions to Pass
100% Updated Splunk SPLK-1002 Enterprise PDF Dumps

NEW QUESTION 93

Which group of users would most likely use pivots?
* Users
* Architects
* Administrators
* Knowledge Managers
Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.0.3/Pivot/IntroductiontoPivot

NEW QUESTION 94

The Field Extractor (FX) is used to extract a custom field. A report can be created using this custom field. The created report can then be shared with other people in the organization. If another person in the organization runs the shared report and no results are returned, why might this be? (select all that apply)
* Fast mode is enabled.
* The dashboard is private.
* The extraction is private-
* The person in the organization running the report does not have access to the index.

NEW QUESTION 95

Which of the following is true about Pivot?
* Users can save reports from Pivot.
* Users cannot share visualizations created with Pivot.
* Users must use SPL to find events in a Pivot.
* Users cannot create visualizations with Pivot.

In Splunk, Pivot is a tool that allows you to report on a specific data set without using the Splunk Search Processing Language (SPL?)1. You can use a drag-and-drop interface to design and generate pivots that present different aspects of your data in the form of tables, charts, and other visualizations12.

One of the features of Pivot is that it allows you to save your reports1. This can be useful when you want to reuse a report or share it with others1. Therefore, it’s not true that users cannot share visualizations created with Pivot or that they must use SPL to find events in a Pivot12. It’s also not true that users cannot create visualizations with Pivot, as creating visualizations is one of the main functions of Pivot12.

NEW QUESTION 96

How is a Search Workflow Action configured to run at the same time range as the original search?
* Set the earliest time to match the original search.
* Select the same time range from the time-range picker.
* Select the “Use the same time range as the search that created the field listing” checkbox.
* Select the “Overwrite time range with the original search” checkbox.

To configure a Search Workflow Action to run at the same time range as the original search, you need to select the “Use the same time range as the search that created the field listing” checkbox. This will ensure that the workflow action search uses the same earliest and latest time parameters as the original search.

NEW QUESTION 97

What is required for a macro to accept three arguments?
* The macro’s name ends with (3).
* The macro’s name starts with (3).
* The macro’s argument count setting is 3 or more.
* Nothing, all macros can accept any number of arguments.

Explanation

To create a macro that accepts arguments, you must include the number of arguments in parentheses at the end of the macro name1. For example, my_macro(3) is a macro that accepts three arguments. The number of arguments in the macro name must match the number of arguments in the definition1. Therefore, option A is correct, while options B, C and D are incorrect.

NEW QUESTION 98

When should transaction be used?
* Only in a large distributed Splunk environment.
* When calculating results from one or more fields.
* When event grouping is based on start/end values.
* When grouping events results in over 1000 events in each group.

Reference:https://docs.splunk.com/Documentation/Splunk/8.0.3/Search/Abouttransactions

NEW QUESTION 99

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.

It’s important to note that although fields generated within a search string (A) and regular expressions (C) can also be used in the calculation of a new field, and lookup tables (B) can be used to enrich data, option D is typically what one refers to when discussing calculated fields, as it implies a direct transformation or calculation based on fields that have been extracted from the raw data.

NEW QUESTION 100

Data model fields can be added using the Auto-Extracted method. Which of the following statements describe Auto-Extracted fields? (select all that apply)
* Auto-Extracted fields can be hidden in Pivot.
* Auto-Extracted fields can have their data type changed.
* Auto-Extracted fields can be given a friendly name for use in Pivot.
* Auto-Extracted fields can be added if they already exist in the dataset with constraints.

Auto-Extracted fields in Splunk Data Models are derived directly from the indexed data based on the existing fields within the events. These fields are identified and extracted by Splunk automatically, without the need for explicit field extractions configured by the user. Understanding the characteristics of Auto-Extracted fields is crucial for effectively managing Data Models and utilizing them in Pivot tables for analysis.

A: Auto-Extracted fields can be hidden in Pivot. This is true. When building a Data Model, you have the option to hide certain fields from appearing in Pivot, making the Pivot table cleaner and more focused on the fields that are most relevant for analysis. This helps in reducing clutter and focusing on the data that matters most to the users.

B: Auto-Extracted fields can have their data type changed. This statement is not typically accurate for Auto-Extracted fields. The data type of an Auto-Extracted field is determined by Splunk based on the field’s content in the indexed data. While you can assign a type to a field when you manually create a field in a data model, the inherent data type of Auto-Extracted fields is not something that is changed within the Data Model itself.

C: Auto-Extracted fields can be given a friendly name for use in Pivot. This is correct. Within Data Models, you can assign a more user-friendly, descriptive name to an Auto-Extracted field. This feature is particularly useful in making Data Models more intuitive and easier to use for those who may not be familiar with the original field names or when the original field names are not descriptive or user-friendly.

D: Auto-Extracted fields can be added if they already exist in the dataset with constraints. This is true.

Auto-Extracted fields are based on fields that already exist in the data. When you define a dataset within a Data Model, you can apply constraints to narrow down the events that the dataset includes. The Auto-Extracted fields are then identified from this constrained dataset. This means that the fields must already be present in the data that meets the dataset’s constraints to be available for auto-extraction.

In summary, Auto-Extracted fields in Splunk Data Models offer a flexible and efficient way to utilize existing data fields within Pivot tables, with options to rename them for clarity and hide unnecessary fields to streamline data analysis.

NEW QUESTION 101

Which of the following file formats can be extracted using a delimiter field extraction?
* CSV
* PDF
* XML
* JSON
Explanation

Explanation/Reference: https://docs.splunk.com/Documentation/Splunk/8.1.1/Data/Extractfieldsfromfileswithstructureddata

NEW QUESTION 102

These are the default selected fields.
* source, sourcetype, host
* source, sourcetype, index
* source, sourcetype, timestamp
* host, source, _raw

NEW QUESTION 103

When should you use the transaction command instead of the scats command?
* When you need to group on multiple values.
* When duration is irrelevant in search results. .
* When you have over 1000 events in a transaction.
* When you need to group based on start and end constraints.
The transaction command is used to group events into transactions based on some common characteristics,

such as fields, time, or both. The transaction command can also specify start and end constraints for the

transactions, such as a field value that indicates the beginning or the end of a transaction. The stats command

is used to calculate summary statistics on the events, such as count, sum, average, etc. The stats command

cannot group events based on start and end constraints, but only on fields or time buckets. Therefore, the

transaction command should be used instead of the stats command when you need to group events based on

start and end constraints.

NEW QUESTION 104

What is the correct syntax to search for a tag associated with a value on a specific fields?
* Tag-<field?
* Tag<filed(tagname.)
* Tag=<filed>::<tagname>
* Tag::<filed>=<tagname>
Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.3/Knowledge/TagandaliasfieldvaluesinSplunkWeb

NEW QUESTION 105

How many ways are there to access the Field Extractor Utility?
* 3
* 4
* 1
* 5

NEW QUESTION 106

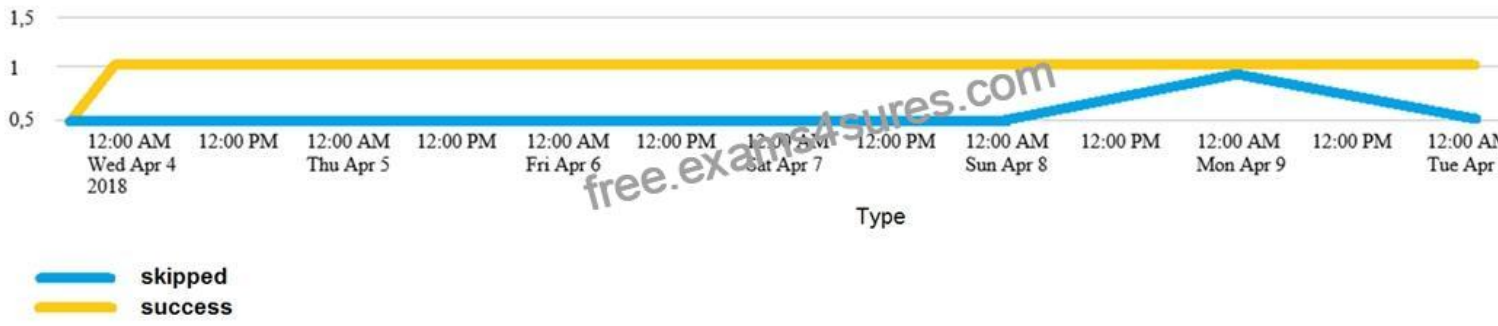
What other syntax will produce exactly the same results as | chart count over vendor_action by user?
* | chart count by vendor_action, user
* | chart count over vendor_action, user
* | chart count by vendor_action over user
* | chart count over user by vendor_action

NEW QUESTION 107

Which of the following statements about event types is true? (select all that apply)
* Event types can be tagged.
* Event types must include a time range,
* Event types categorize events based on a search.
* Event types can be a useful method for capturing and sharing knowledge.

NEW QUESTION 108

Which of the following searches would create a graph similar to the one below?



* index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | start count states
* index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | chart count states by -time
* index_internal seourcetype=Savesplunker | fields sourcetype, status | transaction status maxspan-id | timechart count by status
* None of these searches would generate a similart graph.

NEW QUESTION 109

Which of the following statements describe the search string below?

| datamodel Application_State All_Application_State search
* Events will be returned from dataset named Application_state.
* Events will be returned from the data model named Application_State.
* Events will be returned from the data model named All_Application_state.
* No events will be returned because the pipe should occur after the datamodel command

NEW QUESTION 110

The timechart command is an example of which of the following command types?
* Orchestrating
* Transforming
* Statistical
* Generating
The correct answer is B. Transforming.

The explanation is as follows:

* The timechart command is a Splunk command that creates a time series chart with corresponding table of statistics12.

* A timechart is a statistical aggregation applied to a field to produce a chart, with time used as the X-axis1. You can specify a split-by field, where each distinct value of the split-by field becomes a series in the chart1.

* Transforming commands are commands that change the format of the search results into a data structure that can be easily visualized3. Transforming commands often use stats functions to aggregate and summarize data3.

* Therefore, the timechart command is an example of a transforming command, as it transforms the search

* results into a chart and a table using stats functions123.

NEW QUESTION 111

A field alias has been created based on an original field. A search without any transforming commands is then executed in Smart Mode. Which field name appears in the results?
* Both will appear in the All Fields list, but only if the alias is specified in the search.
* Both will appear in the Interesting Fields list, but only if they appear in at least 20 percent of events.
* The original field only appears in All Fields list and the alias only appears in the Interesting Fields list.
* The alias only appears in the All Fields list and the original field only appears in the Interesting Fields list.
Explanation

A field alias is a way to assign an alternative name to an existing field without changing the original field name or value2. You can use field aliases to make your field names more consistent or descriptive across different sources or sourcetypes2. When you run a

search without any transforming commands in Smart Mode, Splunk automatically identifies and displays interesting fields in your results2. Interesting fields are fields that appear in at least 20 percent of events or have high variability among values2. If you have created a field alias based on an original field, both the original field name and the alias name will appear in the Interesting Fields list if they meet these criteria2. However, only one of them will appear in each event depending on which one you have specified in your search string2. Therefore, option B is correct, while options A, C and D are incorrect.

NEW QUESTION 112

Which of the following searches will return events contains a tag name Privileged?
* Tag= Priv
* Tag= Pri*
* Tag= Priv*
* Tag= Privileged
Reference:https://docs.splunk.com/Documentation/PCI/4.1.0/Install/PrivilegedUserActivity

A tag is a descriptive label that you can apply to one or more fields or field values in your events1. You can

use tags to simplify your searches by replacing long or complex field names or values with short and simple

tags1. To search for events that contain a tag name, you can use the tag keyword followed by an equal sign

and the tag name1. You can also use wildcards (*) to match partial tag names1. Therefore, option B is correct

because it will return events that contain a tag name that starts with Pri. Options A and D are incorrect because

they will only return events that contain an exact tag name match. Option C is incorrect because it will return

events that contain a tag name that starts with Priv, not Privileged.

Splunk Core Certified Power User (SPLK-1002) Exam is designed to validate the skills and knowledge of individuals who use Splunk to analyze and interpret data. Splunk is a powerful platform that allows organizations to collect, monitor, and analyze machine-generated data from various sources. The SPLK-1002 Exam is intended for professionals who use Splunk on a daily basis and are responsible for managing and manipulating data within the platform.

Splunk SPLK-1002 (Splunk Core Certified Power User) Exam is a certification exam that tests the knowledge and skills of the candidates in using Splunk Core for data analysis and troubleshooting. Splunk is a popular software platform that enables organizations to analyze and monitor their machine-generated data in real-time. The SPLK-1002 exam is designed for individuals who have a deep understanding of Splunk's functionality and are proficient in using its features to manage and manipulate data.

Exam Details **SPLK-1002 has 65 multiple-select and multiple-choice questions that should be answered in 57 minutes, with an addition of 3 minutes that are given one to get familiar with the exam agreement. Taking this test will cost $ The applicants will be rated on a variety of knowledge areas, such as the following:** - Transformation of commands as well as visualizations- Macros- CIM- Filtering as well as formatting of results- Knowledge objects

Candidates are advised to take the training courses provided by the vendor when preparing for SPLK-1002 exam. To succeed on the first attempt, they should tackle all the lectures, hands-on sessions, and practice questions to ensure they are adequately ready.

Use Valid Exam SPLK-1002 by Exams4sures Books For Free Website:
https://www.exams4sures.com/Splunk/SPLK-1002-practice-exam-dumps.html]