Download Free Splunk SPLK-1002 Exam Questions & Answer [Q48-Q62

Download Free Splunk SPLK-1002 Exam Questions & Answer
Online VALID SPLK-1002 Exam Dumps File Instantly

Earning a Splunk SPLK-1002 certification can open up many career opportunities for individuals. It demonstrates a high level of expertise in using Splunk software for data analysis and troubleshooting, making individuals more valuable to potential employers. Additionally, certified professionals are often considered for higher-paying jobs and more challenging projects.

Q48. Which of the following statements describes Search workflow actions?
* By default. Search workflow actions will run as a real-time search.
* Search workflow actions can be configured as scheduled searches,
* The user can define the time range of the search when created the workflow action.
* Search workflow actions cannot be configured with a search string that includes the transaction command

Q49. Which function should you use with the transaction command to set the maximum total time between the earliest and latest events returned?

* maxpause
* endswith
* maxduration
* maxspan

The maxspan function of the transaction command allows you to set the maximum total time between the earliest and latest events returned. The maxspan function is an argument that can be used with the transaction command to specify the start and end constraints for the transactions. The maxspan function takes a time modifier as its value, such as 30s, 5m, 1h, etc. The maxspan function sets the maximum time span between the first and last events in a transaction. If the time span between the first and last events exceeds the maxspan value, the transaction will be split into multiple transactions.

Q50. Use this command to use lookup fields in a search and see the lookup fields in the field sidebar.

* inputlookup
* lookup

Q51. When would a user select delimited field extractions using the Field Extractor (FX)?

* When a log file has values that are separated by the same character, for example, commas.
* When a log file contains empty lines or comments.
* With structured files such as JSON or XML.
* When the file has a header that might provide information about its structure or format.

The correct answer is A. When a log file has values that are separated by the same character, for example, commas.

The Field Extractor (FX) is a utility in Splunk Web that allows you to create new fields from your events by using either regular expressions or delimiters. The FX provides a graphical interface that guides you through the steps of defining and testing your field extractions1.

The FX supports two field extraction methods: regular expression and delimited. The regular expression method works best with unstructured event data, such as logs or messages, that do not have a consistent format or structure. You select a sample event and highlight one or more fields to extract from that event, and the FX generates a regular expression that matches similar events in your data set and extracts the fields from them1.

The delimited method is designed for structured event data: data from files with headers, where all of the fields in the events are separated by a common delimiter, such as a comma, a tab, or a space. You select a sample event, identify the delimiter, and then rename the fields that the FX finds1.

Therefore, you would select the delimited field extraction method when you have a log file that has values that are separated by the same character, for example, commas. This method will allow you to easily extract the fields based on the delimiter without writing complex regular expressions.

The other options are not correct because they are not suitable for the delimited field extraction method. These options are:

B) When a log file contains empty lines or comments: This option does not indicate that the log file has a structured format or a common delimiter. The delimited method might not work well with this type of data, as it might miss some fields or include some unwanted values.

C) With structured files such as JSON or XML: This option does not require the delimited method, as Splunk can automatically extract fields from JSON or XML files by using indexed extractions or search-time extractions2. The delimited method might not work well with this type of data, as it might not recognize the nested structure or the special characters.

D) When the file has a header that might provide information about its structure or format: This option does not indicate that the file has a common delimiter between the fields. The delimited method might not work well with this type of data, as it might not be able

to identify the fields based on the header information.

Reference:

Build field extractions with the field extractor

Configure indexed field extraction

Q52. 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.

Explanation

Data model fields are fields that describe the attributes of a dataset in a data model2. Data model fields can be added using various methods such as Auto-Extracted, Evaluated or Lookup2. Auto-Extracted fields are fields that are automatically extracted from your raw data using various techniques such as regular expressions, delimiters or key-value pairs2. Auto-Extracted fields can be hidden in Pivot, which means that you can choose whether to display them or not in the Pivot interface2. Therefore, option A is correct. Auto-Extracted fields can have their data type changed, which means that you can specify whether they are strings, numbers, booleans or timestamps2. Therefore, option B is correct. Auto-Extracted fields can be given a friendly name for use in Pivot, which means that you can assign an alternative name to them that is more descriptive or user-friendly than the original field name2. Therefore, option C is correct. Auto-Extracted fields can be added if they already exist in the dataset with constraints, which means that you can include them in your data model even if they are already extracted from your raw data by applying filters or constraints to limit the scope of your dataset2. Therefore, option D is correct.

Q53. When creating a Search workflow action, which field is required?
* Search string
* Data model name
* Permission setting
* An eval statement

Reference:

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.

Q54. Which of the following statements about data models and pivot are true? (select all that apply)
* They are both knowledge objects.
* Data models are created out of datasets called pivots.
* Pivot requires users to input SPL searches on data models.
* Pivot allows the creation of data visualizations that present different aspects of a data model.

Q55. Which of the following statements are true for this search? (Select all that apply.) SEARCH:

sourcetype=access* |fields action productld status
* is looking for all events that include the search terms: fields AND action AND productld AND status
* users the table command to improve performance
* limits the fields are extracted
* returns a table with 3 columns

Q56. 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.

Reference:

As mentioned before, an event type is a way to categorize events based on a search string that matches the events2. Event types can be tagged, which means that you can apply descriptive labels to event types and use them in your searches2. Therefore, option A is correct. Event types categorize events based on a search string, which means that you can define an event type by specifying a search string that matches the events you want to include in the event type2. Therefore, option C is correct. Event types can be a useful method for capturing and sharing knowledge, which means that you can use event types to organize your data into meaningful categories and share them with other users in your organization2. Therefore, option D is correct. Event types do not have to include a time range, which means that you can create an event type without specifying a time range for the events2. Therefore, option B is incorrect.

Q57. In what order arc the following knowledge objects/configurations applied?
* Field Aliases, Field Extractions, Lookups
* Field Extractions, Field Aliases, Lookups
* Field Extractions, Lookups, Field Aliases
* Lookups, Field Aliases, Field Extractions

Q58. In which of the following scenarios is an event type more effective than a saved search?
* When a search should always include the same time range.
* When a search needs to be added to other users’ dashboards.
* When the search string needs to be used in future searches.
* When formatting needs to be included with the search string.

Reference: https://answers.splunk.com/answers/4993/eventtype-vs-saved-search.html An event type is a way to categorize events based on a search string that matches the events2. You can use event types to simplify your searches by replacing long or complex search strings with short and simple event type names2. An event type is more effective than a saved search when the search string needs to be used in future searches because it allows you to reuse the search string without having to remember or type it again2.

Therefore, option C is correct, while options A, B and D are incorrect because they are not scenarios where an event type is more effective than a saved search.

Q59. Which of the following statements describe the search string below?

| datamodel Application_State All_Application_State search
* Evenrches would return a report of sales by 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

Q60. Which of the following statements about calculated fields in Splunk is true?

* Calculated fields cannot be chained together to create more complex fields
* Calculated fields can be chained together to create more complex fields.
* Calculated fields can only be used in dashboards.
* Calculated fields can only be used in saved reports.

Explanation

The correct answer is B. Calculated fields can be chained together to create more complex fields.

Calculated fields are fields that are added to events at search time by using eval expressions. They can be used to perform calculations with the values of two or more fields already present in those events. Calculated fields can be defined with Splunk Web or in the props.conf file. They can be used in searches, reports, dashboards, and data models like any other extracted field1.

Calculated fields can also be chained together to create more complex fields. This means that you can use a calculated field as an input for another calculated field. For example, if you have a calculated field named total that sums up the values of two fields named price and tax, you can use the total field to create another calculated field named discount that applies a percentage discount to the total field. To do this, you need to define the discount field with an eval expression that references the total field, such as:

discount = total * 0.9

This will create a new field named discount that is equal to 90% of the total field value for each event2.

References:

About calculated fields

Chaining calculated fields

Q61. Selected fields are displayed _____each event in the search results.

* below
* interesting fields
* other fields
* above

Q62. 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.

The Field Extractor (FX) is a tool that helps you extract fields from your events using a graphical interface2. You can create a report using a custom field extracted by the FX and share it with other users in your organization2. However, if another user runs the shared report and no results are returned, there could be two possible reasons. One reason is that the extraction is private, which means that only you can see and use the extracted field2. To make the extraction available to other users, you need to make it global or app-level2. Therefore, option C is correct. Another reason is that the other user does not have access to the index where the events are stored2. To fix this issue, you need to grant the appropriate permissions to the other user for the index2. Therefore, option D is correct. Options A and B are incorrect because they are not related to the field extraction or the report.

The SPLK-1002 certification exam is a comprehensive test designed to evaluate a candidate's proficiency in using Splunk Core. SPLK-1002 exam focuses on the skills and knowledge required to operate and troubleshoot a Splunk environment. Splunk Core Certified Power User Exam certification is aimed at IT professionals, data analysts, and system administrators who work with Splunk and want to demonstrate their expertise in the platform.

SPLK-1002 Exam Dumps For Certification Exam Preparation: https://www.vceprep.com/SPLK-1002-latest-vce-prep.html]